Universidad de la República
Facultad de Ciencias
Centro de Matemática

Divisibilidad en dominios

Notas adaptadas por Mariana Haim para el curso "Anillos y Módulos" 2021.

En este capítulo D siempre será un dominio, es decir un anillo conmutativo $D \neq \{0\}$ sin divisores de cero.

0.1. Generalidades

Definición 0.1.1. Sean $a, b \in D$. Decimos que a *divide a* b, que a *es divisor de* b o que b *es múltiplo de* a si existe $c \in D$ tal que $b = ac$. En este caso notamos $a \mid b$.

Ejemplos 0.1.1. Para todo $a \in D$, se tiene:

$$1 \mid a, \qquad a \mid a, \qquad a \mid 0, \qquad 0 \mid a \quad \text{si y sólo si } a = 0, \qquad a \mid 1 \quad \text{si y sólo si } a \in D^\times.$$

Observación 0.1.1.

- Las siguientes propiedades se verifican fácilmente:

  Si $a \mid b$ y $a \mid b'$ entonces $a \mid (b + b')$, $a \mid (b - b')$ y $a^2 \mid bb'$.

  Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

- La relación "divide a.$^{\text{es}}$ entonces lo que se conoce como un preorden en D^* (es reflexiva y transitiva, pero en general no antisimétrica: $1 \mid -1 \mid 1$). Como todo preorden induce una relación de equilalencia definida por $a \sim b$ si y sólo si $a \mid b$ y $b \mid a$.

Proposición 0.1.1. *Sea $\sim$ la relación en D definida en la observación anterior. Se tiene $a \sim b$ si y sólo si existe $u \in D^\times$ tal que $a = ub$.*

Demostración. Si existe $u \in D^\times$ tal que $a = ub$, se tiene también $b = u^{-1}a$ y por lo tanto $a \sim b$. Recíprocamente, supongamos que $a = xb$ y que $b = ya$. Entonces $a = xya$ y por tanto $a(1 - xy) = 0$. Como D es un dominio, tenemos dos posibilidades: $a = 0$ o $xy = 1$. Si $a = 0$, entonces $b = ya = 0$ y se deduce $a \sim b$. Si $xy = 1$, entonces $x \in D^\times$ y por tanto $a = xb \sim b$. □

Definición 0.1.2. Sean $a, b \in D$. Decimos que a y b *son asociados* si $a \sim b$.

Observación 0.1.2. La prueba de la proposición anterior permite afirmar además que si $b \in D$ es no nulo, entonces

$$xb \sim b \Rightarrow x \in D^\times.$$

La siguiente proposición traduce estas nociones de divisibilidad en términos de ideales principales.

Proposición 0.1.2. *Sean $a, b \in D$. Entonces:*

1. *$a \mid b$ si y sólo si $(b) \subseteq (a)$,*
2. *$a \sim b$ si y sólo si $(a) = (b)$,*
3. *$a \mid b$ y $a \not\sim b$ si y sólo si $(b) \subsetneq (a)$,*
4. *$a \in D^\times$ si y sólo si $(a) = D$.*

Demostración. A cargo del lector. □

Definición 0.1.3. Sea $a \in D$ no nulo y no invertible. Decimos que a es:

- *irreducible* si $\forall b, c \in D : a = bc$ implica $b \in D^\times$ o $c \in D^\times$,
- *primo* si $\forall b, c \in D : a \mid bc$ implica $a \mid b$ o $a \mid c$.

Observación 0.1.3.
1. Sea $a \in D$ no nulo y no invertible. Entonces a es irreducible si y sólo si $\forall b \in D : b \mid a$ implica $b \in D^\times$ o $b \sim a$.
2. Todo primo es irreducible.
3. Supongamos $p \sim q$. Si p es irreducible, también lo es q. Si p es primo también lo es q.

Ejemplos 0.1.2.
1. En $\mathbb{Z}$ y $\Bbbk[x]$ ($\Bbbk$ cuerpo) los primos y los irreducibles coinciden.
2. Sea $\Bbbk$ un cuerpo. Pongamos $D = \{a + x^2 p(x) \mid a \in \Bbbk, p(x) \in \Bbbk[x]\} \subseteq \Bbbk[x]$. El elemento $x^2 \in D$ es irreducible pero no es primo. En efecto $x^2 \mid x^3 x^3 = x^2 x^4$ pero $x^2 \nmid x^3$.
3. El polinomio $x^2 - 2$ es irreducible y primo como elemento de $\mathbb{Z}[x]$ pero no lo es como elemento de $\mathbb{R}[x]$.
4. El polinomio $2x - 2$ es irreducible y primo como elemento de $\mathbb{R}[x]$ pero no lo es como elemento de $\mathbb{Z}[x]$.

Proposición 0.1.3. *Sea $a \in D$ no nulo y no invertible. Entonces:*

1. *a es primo si y sólo si (a) es un ideal primo en D,*
2. *a es irreducible si y sólo si (a) es maximal (respecto de la inclusión) en la familia de ideales principales propios de D.*

Demostración. A cargo del lector. □

Definición 0.1.4. Si $a, b \in D$ no son simultáneamente nulos, decimos que $d \in D$ es un *máximo común divisor* de a y b si verifica

$$d \mid a, \quad d \mid b, \quad \text{y} \quad \forall c \in D \;\; c \mid a,\; c \mid b \Rightarrow c \mid d.$$

Observación 0.1.4.
1. En un dominio cualquiera no tiene por qué existir el máximo común divisor. En efecto, en el ejemplo 0.1.2.2, los elementos x^5 y x^6 tienen como conjunto de divisores comunes a $\{a \mid a \in \mathbb{R}\} \cup \{ax^2 \mid a \in \mathbb{R}\} \cup \{ax^3 \mid a \in \mathbb{R}\}$. Sin embargo ninguno de los elementos de este conjunto es múltiplo de todos los demás.
2. Si d y d' son máximos comunes divisores de a y b, entonces $d \sim d'$. Notamos $\operatorname{mcd}(a, b)$ a la clase de equivalencia definida por a y b.

Abuso de notación: En caso de existir máximos comunes divisores de a y b, notaremos $\operatorname{mcd}(a, b) = d$ en lugar de $d \in \operatorname{mcd}(a, b)$.

Proposición 0.1.4.
1. *Si $a, b \in D$ son tales que $a \mid b$, entonces $\operatorname{mcd}(a, b) = a$. En particular $\operatorname{mcd}(a, 0) = a$ y $\operatorname{mcd}(a, b) = 1$ siempre que $a \in D^\times$.*
2. *Si $p \in D$ es irreducible, entonces $\operatorname{mcd}(a, p) = 1$ o $\operatorname{mcd}(a, p) = p$.*

Demostración. 1. La afirmación y el primer caso particular son claros. Si a es invertible, entonces $b = aa^{-1}b$ y por tanto $a \mid b$. Se deduce que $\operatorname{mcd}(a, b) = a$ y como $a \sim 1$, entonces $\operatorname{mcd}(a, b) = 1$.

2. Como p es irreducible, sus divisores son 1, p o sus asociados, en particular $\operatorname{mcd}(a, p)$ es uno de estos. □

Definición 0.1.5. Sean $a_1, a_2, \ldots, a_n \in D$ no simultáneamente nulos. Decimos que $d \in D$ es un *máximo común divisor* de $a_1, a_2, \ldots, a_n$ y notamos $d = \operatorname{mcd}(a_1, \ldots, a_n)$ si

$$d \mid a_i \ \ \forall i \in \{1, 2, \ldots, n\} \quad \text{y} \quad \forall c \in D \ \ c \mid a_i \ \forall i \Rightarrow c \mid d.$$

Observación 0.1.5. 1. Aquí también vale la unicidad a menos de asociados y haremos un abuso de notación análogo.

2. Sin pérdida de generalidad, se puede asumir que todos los a_i son no nulos puesto que si $a_i = 0$, es fácil ver que se tiene $\operatorname{mcd}(a_1, a_2, \ldots, a_n) = \operatorname{mcd}(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$.

3. Supongamos que $a_i \neq 0$ para todo $i \leqslant n$. Entonces si $d_1 := \operatorname{mcd}(a_1, a_2, \ldots, a_{n-1})$, se tiene $\operatorname{mcd}(a_1, a_2, \ldots, a_n) = \operatorname{mcd}(d_1, a_n)$.

4. De la observación anterior se deduce que si existe $\operatorname{mcd}(a, b)$ para cualesquiera $a, b \in D$, entonces existe $\operatorname{mcd}(a_1, a_2, \ldots, a_n)$ cualesquiera sean $a_1, a_2, \ldots, a_n \in D$, $n \geqslant 3$.

0.1.1. Dominios de factorización única

Definición 0.1.6. Un dominio D se dice *dominio factorial* o *dominio de factorización única* (abreviado DFU) si verifica:

- (Existencia de la descomposición factorial) Para cada $a \in D$ no nulo y no invertible, existen $p_1, p_2, \ldots, p_n$ irreducibles tales que $a = p_1 p_2 \cdots p_n$.
- (Unicidad de la descomposición factorial) Si $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, con p_i, q_j irreducibles para cada $i \in \{1, 2, \ldots, n\}, j \in \{1, 2, \ldots, m\}$, entonces $n = m$ y existe una función $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ tal que $p_i \sim q_{\sigma(i)}$.

Observación 0.1.6. 1. La unicidad de la factorización implica que puede asumirse σ inyectiva. En efecto, si $n = 1$ es claro. Supongamos que σ es inyectiva para n_0 y probémoslo para $n_0 + 1$. Tomemos

$$p_1 p_2 \cdots p_{n_0} p_{n_0+1} = q_1 q_2 \cdots q_m.$$

Existe $j \in \{1, 2, \ldots, m\}$ tal que $q_j \sim p_{n_0+1}$, por lo que se tiene $x p_{n_0+1} = q_j$ para cierto x invertible. Cancelando p_{n_0+1} en la igualdad de arriba, se deduce:

$$p_1 p_2 \cdots p_{n_0} = x^{-1} q_1 q_2 \cdots q_{j-1} q_{j+1} \cdots q_m.$$

Tomando $\sigma : \{1, 2, \ldots, n_0\} \to \{1, 2, \ldots, m\} \backslash \{j\}$ inyectiva y extendiéndola a $\overline{\sigma} : \{1, 2, \cdots, n_0 + 1\} \to \{1, 2, \ldots, m\}$ mediante $\overline{\sigma}(i) = \sigma(i), \forall i \leqslant n_0$, $\overline{\sigma}(n_0 + 1) = j$, obtenemos $\overline{\sigma}$ inyectiva.

2. En la prueba de la observación anterior no se usó la condición $n = m$ exigida para la unicidad de la descomposición factorial. De hecho, esta condición puede eliminarse de la definición. En efecto, por la observación anterior se deduce $n \leqslant m$, y luego intercambiando los roles de los p_i y los q_j se deduce $m \leqslant n$ y se obtiene $m = n$ (y por lo tanto σ es, de hecho, biyectiva).

3. La existencia de la factorización implica que todo elemento no nulo $a \in D$ es de la forma $a = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, con $u \in D^\times$, $n \in \mathbb{Z}^+$, p_i irreducibles no asociados dos a dos y $\alpha_i \in \mathbb{N}$ para todo $i \in \{1, \ldots, n\}$.

   En efecto, si a es invertible, se toma n cualquiera y $\alpha_i = 0$ para todo $i \in \{1, \ldots, n\}$. Si a no es invertible, se tiene $a = q_1 q_2 \cdots q_m$, con q_i irreducible para todo $j \in \{1, \ldots, m\}$. Agrupando los q_i que sean asociados y usando que el producto de invertibles es invertible, se tiene el resultado.

La siguiente proposición muestra que $a \mid b$ si y sólo si "la factorización de a está contenida en la de b".

Proposición 0.1.5. *Sean D un DFU y $a, b \in D$ no nulos y no invertibles. Si $a = p_1 p_2 \cdots p_n$ y $b = q_1 q_2 \cdots q_m$, entonces son equivalentes:*

(i) $a \mid b$

(ii) existe una función inyectiva $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ tal que $p_i \sim q_{\sigma(i)}$.

Demostración. Si $a \mid b$, entonces existe $x \in D$ tal que $ax = b$. Poniendo $x = r_1 r_2 \cdots r_t$, se tiene

$$p_1 p_2 \cdots p_n r_1 r_2 \cdots r_t = q_1 q_2 \cdots q_m$$

y se deduce la tesis, a partir de la Observación 0.1.6.

Recíprocamente si existe tal σ se tiene que

$$b = \prod_{j=1}^{m} q_j = x \prod_{i=1}^{n} p_i \prod_{j \notin \mathrm{Im}\,(\sigma)} q_j = xa \prod_{j \notin \mathrm{Im}\,(\sigma)} q_j$$

para cierto $x \in D^\times$. □

Proposición 0.1.6. *Sea D un dominio en el que todo elemento no nulo y no invertible se descompone en producto de irreducibles. Entonces son equivalentes:*

- *D es un DFU,*
- *todo irreducible en D es primo.*

Demostración. Supongamos primero que D es un DFU y que p es irreducible y que $p \mid ab$. Pongamos $a = p_1 p_2 \cdots p_n$ y $b = q_1 q_2 \cdots q_m$. Se tiene $ab = pc$ para cierto $c = r_1 r_2 \cdots r_t \in D$. De la igualdad

$$p r_1 r_2 \cdots r_t = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m,$$

y la unicidad de la descomposición en irreducibles, se deduce que existe $i \in \{1, \ldots, n\}$ tal que $p \sim p_i$ o existe $j \in \{1, \ldots, m\}$ tal que $p \sim q_j$. En el primer caso $p \mid a$ y en el segundo $p \mid b$.

Recíprocamente, supongamos que todo irreducible en D es primo y que $p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$, con $p_i, q_j \in D$ irreducibles $\forall i \leqslant n, j \leqslant m$. Para cada $i \leqslant n$, como p_i es primo y divide al término de la derecha, se tiene que $p_i \mid q_j$ para cierto $j \leqslant m$. Como además q_j es irreducible, se deduce $p_i \sim q_j$. □

0.1.2. Dominios a ideales principales

Definición 0.1.7. Un dominio D se dice *dominio a ideales principales* (DIP) si todo ideal de D es principal, es decir, si todo ideal de D está generado por un elemento.

Ejemplos 0.1.3.

- El anillo de enteros $\mathbb{Z}$ es un DIP puesto que sus ideales son de la forma $n\mathbb{Z}$, es decir principales.
- El anillo de polinomios $\Bbbk[x]$ es un DIP si y sólo si $\Bbbk$ es un cuerpo.

  Observemos primero que si $\Bbbk$ no es un cuerpo, existe $a \in \Bbbk$ no invertible y no nulo. Es fácil ver que el ideal $I = \{p \in \Bbbk[x] \mid p(0) \text{ es múltiplo de } a\}$ no es principal. En efecto, $a \in I$ y $x \in I$, pero el único divisor común entre ellos es 1, por lo que si I fuera principal sería $I = (1) = \Bbbk[x]$.

  Recíprocamente, si $\Bbbk$ es un cuerpo, la división euclídea de polinomios nos permite probar de manera análoga que en el caso de $\mathbb{Z}$ que todos los ideales de $\Bbbk[x]$ son principales[1]. En efecto, dado un ideal I, consideremos un polinomio $f \in I$ de grado mínimo entre los grados de los polinomios en I. Sea $g \in I$ cualquiera. Como $\operatorname{gr}(g) \geqslant \operatorname{gr}(f)$ se tiene $g = fq + r$, con $\operatorname{gr}(r) < \operatorname{gr}(f)$ o $r = 0$. Pero $r = g - fq \in I$, por lo que no puede tener grado menor que el grado de f. Se deduce $r = 0$ y por tanto $I = (f)$.

Proposición 0.1.7. *Sean D un DIP, $I \lhd D$. Son equivalentes:*

1. *I es maximal,*
2. *I es primo.*

Demostración. Ya sabemos que (1) implica (2) en un anillo conmutativo. Para (2) implica (1), supongamos que I es primo y que $I \subsetneq M \subseteq D$. Sean $p, q \in D$ tales que $I = (p)$ y $M = (q)$. Se tiene $p = xq$ para cierto $x \in D$ no invertible. Por ser I primo y como $q \notin I$, se deduce $x \in I$, de donde $x = py$ y por tanto $x \sim p$. Pero entonces q es invertible y por tanto $M = D$. □

Corolario 0.1.8. *En un dominio a ideales principales, todo irreducible es primo (y recíprocamente).*

Demostración. Si $p \in D$ es irreducible, entonces $I = (p)$ es maximal respecto de la inclusión en la familia de ideales principales propios; como D es un DIP, se deduce que I es maximal y por tanto primo. En consecuencia, p es primo. □

Queremos probar que todo dominio a ideales principales es un dominio de factorización única. El lector podrá observar que, existiendo la descomposición en producto de irreducibles, el corolario anterior asegura la unicidad de la descomposición a menos de asociados (esto quedará claro de todas formas en la prueba del Teorema 0.1.9). Queremos entonces estudiar qué particularidad de los dominios a ideales principales es la que asegura la existencia de la descomposición. Esta es el hecho de que todo ideal sea finitamente generado. Los anillos que verifican esto tienen su importancia propia en teoría de anillos, es por esto que les dedicamos el próximo apartado.

[1] Estos dos son casos particulares de una observación más general, y es que cualquier *dominio euclídeo* es a ideales principales: ver práctico 5.

Anillos noetherianos

En esta sección, estudiamos una condición de finitud de anillos, que se muestra ligada a la existencia de la descomposición factorial en dominios (ver Teorema 0.1.11).

Proposición 0.1.9. *Consideremos un anillo conmutativo A. Las siguientes proposiciones son equivalentes:*

1. *Todo ideal de A es finitamente generado.*
2. *Toda sucesión creciente de ideales en A estabiliza. Esto es, si $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ es una cadena de ideales de A, entonces existe $n \in \mathbb{Z}^+$ tal que $I_n = I_{n+1} = \cdots$.*
3. *Toda familia no vacía de ideales de A contiene un elemento maximal respecto de la inclusión.*

Demostración. Supongamos primero que todo ideal de A es finitamente generado y tomemos una sucesión creciente de ideales:

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots \subset A.$$

Sea $I = \bigcup_{n \geqslant 0} I_n$. Como los I_k están encajados, I es un ideal de A (como en la demostración de la existencia de ideales maximales). Existen entonces $x_1, x_2, \ldots, x_k \in A$ tales que el conjunto $\{x_1, x_2, \ldots, x_k\}$ genera al ideal I. Para cada $i \in \{1, \ldots, k\}$ se tiene que $x_i \in I$, luego existe $n_i \in \mathbb{Z}^+$ tal que $x_i \in I_{n_i}$. Por lo tanto si $N = \text{máx}\{n_1, \ldots, n_k\}$ entonces $I \subseteq I_N$. Se deduce que $I_n = I$ para todo $n \geqslant N$.

Para probar (2) implica (3), consideremos una familia $\mathcal{F}$ no vacía de ideales y un elemento $I_1 \in \mathcal{F}$. Si I_1 no es maximal, está propiamente contenido en otro ideal $I_2 \in \mathcal{F}$. Si I_2 no es maximal, está propiamente contenido en otro ideal $I_3 \in \mathcal{F}$. Se construye así una cadena estrictamente creciente de ideales en $\mathcal{F}$: $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots$, lo que contradice (2). Se deduce que para algún n, I_n es maximal en $\mathcal{F}$.

Finalmente, supongamos que vale (3) y que I es un ideal de A. Consideremos la familia $\{J \subseteq I \mid J \lhd A, J \text{ finitamente generado}\}$. Es no vacía porque contiene al ideal $\{0\}$ y tiene por tanto un elemento maximal M. Si $M \neq I$, entonces existe $x \in I \backslash M$ y el ideal generado por $M \cup \{x\}$ es finitamente generado y está incluido en I. Esto contradice la maximalidad de M como elemento de la familia. Se deduce entonces que $M = I$ y por tanto que I es finitamente generado. □

Definición 0.1.8. Un anillo conmutativo que verifica una de las condiciones de la Proposición 0.1.9 se dice *noetheriano*.

Ejemplos 0.1.4.

- Todo DIP es noetheriano.
- El anillo de polinomios en infinitas variables $\Bbbk[x_1, x_2, \ldots, x_n, \ldots]$ no es noetheriano.
- Más adelante (Teorema 0.1.10) probaremos el *teorema de la base de Hilbert* que afirma que si A es un anillo noetheriano, entonces $A[x_1, \ldots, x_n]$ es noetheriano.

Observación 0.1.7. La noción de noetherianidad tiene su versión lateral (considerando ideales a izquierda o a derecha), pero estamos interesados en el caso de anillos conmutativos, y por eso así la definimos.

El siguiente teorema permite deducir que los anillos de polinomios en finitas variables $A[x_1, x_2 \cdots, x_n]$ sí son noetherianos siempre que A lo sea.

Teorema 0.1.10 (Teorema de la base de Hilbert)**.** *Sea A un anillo conmutativo. Si A es noetheriano, entonces $A[x]$ también lo es.*

Demostración. Tomemos un ideal $J \lhd A[x]$. Vamos a probar que J es finitamente generado. Para esto, consideramos $I_n = \{a \in A \mid \text{ existe } f \in J \text{ con } \operatorname{gr}(f) = n, a = \ell(f)\} \cup \{0\}$: en otras palabras, el conjunto de los coeficientes líderes de los polinomios de grado n de J. Es fácil ver que I_n es un ideal de A y que $I_n \subseteq I_{n+1}, \forall n \in \mathbb{N}$. Como A es noetheriano, la sucesión estabiliza en algún $I_{\bar{n}}$.

Para cada $i \leqslant \bar{n}$, el ideal I_i es finitamente generado, pongamos que está generado por ciertos $\{a_{i1}, a_{i2}, \ldots, a_{ik_i}\}$. Sean $f_{ij} \in J$ de grado i tales que $\ell(f_{ij}) = a_{ij}$.

Tomemos $f \in J$ no nulo. Probaremos por inducción en $\operatorname{gr}(f)$ que f está generado por los f_{ij}. Si $\operatorname{gr}(f) = 0$, entonces $f \in I_0$ y está generado por $\{f_{0j} \mid j \leqslant k_0\}$. Supongamos que todos los polinomios en J de grado menor que n están generados por los f_{ij} y probemos que los de grado n también lo están.

Sea $f \in J$, con $\operatorname{gr}(f) = n$. Se tiene $\ell(f) \in I_n \subseteq I_{\bar{n}}$, por lo que $\ell(f) = \sum_{j \leqslant k_{\bar{n}}} \lambda_{\bar{n}j} a_{\bar{n}j}$. Si $n \leqslant \bar{n}$, el polinomio $f - \sum \lambda_{\bar{n}j} f_{\bar{n}j} \in J$ es nulo o de grado estrictamente menor que n, por lo que está generado por los f_{ij}. Se deduce que f también lo está. Si $n > \bar{n}$, el polinomio $f - \sum x^{n-\bar{n}} \lambda_{\bar{n}j} f_{\bar{n}j} \in J$ es nulo o de grado estrictamente menor que n, por lo que se deduce otra vez que f está generado por los f_{ij}. □

Todo DIP es un DFU

Teorema 0.1.11. *Si D es un dominio tal que:*

1. *D es noetheriano,*
2. *todo irreducible en D es primo,*

entonces D es un dominio de factorización única.

Demostración. Vamos a ver que la primera condición implica la existencia de la descomposición, y que la segunda implica la unicidad.

Para la existencia, consideremos la familia

$$\mathcal{F} = \{(a) \mid a \notin D^\times, a \neq 0, a \text{ no se descompone en producto de irreducibles}\}.$$

Queremos ver que $\mathcal{F} = \varnothing$. Si fuera no vacía, como D es noetheriano, existe $a_M \in D$ tal que (a_M) es un elemento maximal en $\mathcal{F}$. En particular se tiene que a_M es no nulo y no invertible y que a_M no es irreducible (por no ser producto de irreducibles). Por tanto a_M se descompone en producto de dos elementos no nulos y no invertibles de D: $a_M = xy$. Además, como a_M no es producto de irreducibles, o bien x o bien y no es producto de irreducibles. Supongamos sin pérdida de generalidad que x no es producto de irreducibles. Se tiene entonces

$$(x) \in \mathcal{F} \text{ y } (a_M) \subsetneq (x),$$

lo que contradice la maximalidad de (a_M) como elemento de $\mathcal{F}$.

Para la unicidad de la descomposición, alcanza con aplicar la Proposición 0.1.6.

Recordamos que puede deducirse $n = m$ como se muestra en la observación 0.1.6.2. □

Como todo dominio a ideales principales es noetheriano y verifica la condición de que los irreducibles son (los) primos, se deduce el siguiente corolario.

Corolario 0.1.12. *Todo dominio a ideales principales es un dominio de factorización única.*

El recíproco no es cierto, i.e. hay dominios de factorización única que no son dominios a ideales principales. Un ejemplo es el anillo de polinomios $\mathbb{Z}[x]$ y generalizaciones de éste. Entenderemos bien este hecho en la próxima sección, dedicada a divisibilidad en anillos de polinomios. Pero antes, una última observación general.

Proposición 0.1.13. *Si D es un DFU, entonces existe* $\operatorname{mcd}(a,b)$ *para cualesquiera $a, b \in D$ no simultáneamente nulos.*

Demostración. Pongamos

$$a = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}, \qquad b = vp_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m},$$

con $u, v \in D^\times$, y para cada $i \leqslant m$, p_i irreducible tal que $p_i \nsim p_j$ si $i \neq j$, y $\alpha_i, \beta_i \in \mathbb{N}$. Si tomamos para cada $i \leqslant m$, $\gamma_i = \min\{\alpha_i, \beta_i\}$, entonces es fácil (y queda a cargo del lector) verificar que

$$\operatorname{mcd}(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_m^{\gamma_m}. \qquad \square$$

Definición 0.1.9. Si $a, b \in D$ son no simultáneamente nulos, decimos que a y b son *primos entre sí* si existe $\operatorname{mcd}(a,b)$ y $\operatorname{mcd}(a,b) = 1$.

Proposición 0.1.14 (Lema de Euclides)**.** *Sean a, b, c elementos no nulos en un dominio factorial. Si $a \mid bc$ y $\operatorname{mcd}(a,b) = 1$, entonces $a \mid c$.*

Demostración. Supongamos $a = p_1 p_2 \cdots p_m$ una descomposición en irreducibles de a. Para cada $i \in \{1, \ldots, m\}$, se tiene que $p_i \mid bc$ y como p_i es primo, se tiene que p_i divide a b o divide a c. Ahora bien, $\operatorname{mcd}(a,b) = 1$, por lo que si $p_i \mid b$, como también $p_i \mid a$ se tendría $p_i \mid 1$ y por tanto sería p_i invertible. Entonces $p_i \mid c$ para todo $i \in \{1, \ldots, m\}$, de donde $a \mid c$. $\square$

Proposición 0.1.15. *Sean D un dominio a ideales principales y $a, b \in D$ no simultáneamente nulos. Entonces:*

1. *existe* $\operatorname{mcd}(a,b)$,
2. *si* $\operatorname{mcd}(a,b) = d$ *entonces* $(a,b) = (d)$. *En particular existen $x, y \in D$ tales que $ax + by = d$* (identidad de Bézout).

Demostración. La existencia de $\operatorname{mcd}(a,b)$ se debe a que D es en particular un dominio de factorización única. Además, si consideramos el ideal

$$I = (a,b) = \{ax + by \mid x, y \in D\},$$

como D es un dominio a ideales principales, existe $c \in D$ tal que $I = (c)$.

Como $(a) \subseteq I$, se tiene que $c \mid a$. Análogamente se tiene que $c \mid b$ y por lo tanto $c \mid d$.

Por otra parte $d \mid ax + by$ para todo $x, y \in D$, en particular $d \mid c$. Se deduce $I = (d)$, por lo que existen $x, y \in D$ tales que $ax + by = d$. $\square$

0.2. Divisibilidad en anillos de polinomios

Polinomios como funciones

Recordemos que la propiedad universal de los anillos de polinomios da lugar a la existencia, para cada $a \in A$, del morfismo de anillos *evaluación en a* $\varepsilon_a : A[x] \to A$ que verifica $\varepsilon_a(d) = d$ para todo $d \in D$, y $\varepsilon_a(x) = a$.

Para $p \in A[x]$ y $a \in D$, usamos la notación $p(a) := \varepsilon_a(p)$. Observar que el hecho de que ε_a sea morfismo de anillos se interpreta con la nueva notación mediante $(p+q)(a) = p(a) + q(a), (pq)(a) = p(a)q(a)$ para todo $p, q \in A[x]$. Además si $p = c \in A$ es un polinomio constante entonces $p(a) = c$ para todo $a \in A$.

Haciendo variar $a \in A$, se obtiene una función

$$\varphi : A[x] \to A^A, \text{ definida por } \varphi(p)(a) = p(a),$$

que resulta ser un morfismo de anillos si ponemos en el conjunto de funciones A^A la estructura dada por la suma y el producto punto a punto.

Ahora bien, es claro que φ en general no es sobreyectiva (no toda función de D en D es un polinomio: la función $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = \begin{cases} 1 & \text{si } x \geqslant 0 \\ 0 & \text{si no} \end{cases}$ no es un polinomio, pues $\lim_{x \to +\infty} f(x) = 1$ y eso implicaría que fuera el polinomio constante 1).

En cuanto a la inyectividad, el siguiente ejemplo muestra que φ en general no es inyectiva:

$$p(x) = x^3 - x \in \mathbb{Z}_3[x] \text{ es no nulo; sin embargo, } p(a) = 0 \ \ \forall a \in \mathbb{Z}_3, \text{ es decir } \varphi(p) = 0.$$

De hecho vamos a probar en la próxima sección, para el caso de polinomios sobre dominios, que φ es inyectiva si y sólo si D es infinito. Por lo tanto podemos identificar D con su imagen $\varphi(D)$ de *funciones polinómicas* sólo en el caso que D sea un dominio infinito.

Raíces

Se tiene la función $deg : A[x]^* \to \mathbb{N}$ que asocia a cada polinomio no nulo el máximo exponente en x de los monomios que lo conforman que nota $deg(p)$ y se llama **grado de p**. Al coeficiente asociado a $x^deg(p)$ se le llama **coeficiente líder de** p. Notar que $deg(p) = 0$ si y solo si p es constante.

Si $A = D$ es un dominio y $p, qsonnonulos$, se verifica $deg(pq) = deg(p) + deg(q), \forall p, q \in D[x]$ y esto permite deducir que $D[x]$ también es un dominio.

Además, si $A = \Bbbk$ es un cuerpo, se tiene que para todos $p, d \in \Bbbk[x], d \neq 0$, existen $q, r \in \Bbbk[x]$ tales que $p = dq + r$ y $r = 0$ o $deg(r) < deg(d)$. (esto asegura que $\Bbbk[x]$ es un dominio euclídeo como se vio en un ejercicio de práctico, y por tanto un dominio a ideales principales).

Observación 0.2.1. Si $t \in D[x]$ es un polinomio con coeficiente líder invertible, entonces para cualquier $p \in D[x]$, existen $q, r \in D[x]$ tales que $p = qt + r$ y $r = 0$ o $\operatorname{gr}(r) < \operatorname{gr}(t)$.

En efecto, se puede ver que la división euclídea en $\Bbbk[x]$ da lugar a $q \in D[x]$ y por tanto $r = p - qt \in D[x]$. Decimos que r *es el resto de dividir* p *por* q.

En particular, como el coeficiente líder de $x - a$ es 1 y por tanto invertible, para cualquier polinomio $p \in D[x]$ existen $q, r \in D[x]$ tales que $p = (x-a)q + r$ y $r \in D$.

Definición 0.2.1. Sea $p \in D[x]$. Un elemento $a \in D$ se dice *raíz* de p si $p(a) = 0$.

Proposición 0.2.1 (Teorema del resto)**.** *El resto de dividir un polinomio $p \in D[x]$ por $x - a$ es $p(a)$.*

Demostración. Basta aplicar el morfismo de anillos ε_a a la igualdad $p(x) = q(x)(x-a) + r$. □

Corolario 0.2.2. *Un polinomio $p \in D[x]$ se escribe como $(x-a)q$ para algún $q \in D[x]$ si y sólo si $p(a) = 0$.*

De este corolario sacamos dos corolarios:

Corolario 0.2.3. *Todo polinomio no nulo $p \in D[x]$ tiene una cantidad finita de raíces.*

Demostración. Sea $p \in D[x]$ un polinomio de grado n. Sean $c_1, c_2, \ldots$ las raíces diferentes de p en D. Entonces $p(x) = q_1(x)(x - c_1)$, de donde $0 = p(c_2) = q_1(c_2)(c_2 - c_1)$. Como $c_1 \neq c_2$ y D es un dominio, entonces $q_1(c_2) = 0$. Por lo tanto $x - c_2$ divide a q_2, y $p(x) = q_3(x)(x - c_2)(x - c_1)$. Por inducción llegamos a que dadas m raíces diferentes $c_1, \ldots, c_m$ de p, el polinomio $g_m = (x - c_1)(x - c_2)\cdots(x - c_m)$ divide a p. Pero gr $g_m = m$, de donde $m \leqslant n$. □

Proposición 0.2.4. *El morfismo $\varphi : D[x] \to D^D$ definido por $\varphi(p)(a) = p(a)$ es inyectivo si y sólo si D es infinito.*

Demostración. Si D es finito, entonces D^D también lo es, pero $D[x]$ es infinito, por lo que φ no es inyectivo.

Si D es infinito y $p \in D[x]$ es no nulo, entonces p tiene una cantidad finita de raíces y por lo tanto algún elemento de D no es raíz de p, de lo que se deduce $\varphi(p) \neq 0$. □

Contenido

Definición 0.2.2. Sea D un dominio de factorización única y $f = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ no nulo. Se define el *contenido* de f como $\operatorname{cont}(f) = \operatorname{mcd}(a_n, \ldots, a_1, a_0)$. Decimos que f es *primitivo* si $\operatorname{cont}(f) = 1$.

Ejemplo 0.2.1.

- Todo polinomio mónico es primitivo.
- $f = 2x + 3$ es primitivo en $\mathbb{Z}[x]$, pero $g = 2x + 4$ no lo es, de hecho $\operatorname{cont}(g) = 2 \not\sim 1$.

Observación 0.2.2.

1. Notar que hacemos el mismo abuso de notación que para el máximo común divisor. Si bien $\operatorname{cont}(f)$ es una $\sim$-clase de equivalencia en D, usamos la notación para referirnos a cualquiera de sus representantes.
2. Si $f \in D[x]$ y $a \in D, a \neq 0$, entonces $\operatorname{cont}(af) = a \operatorname{cont}(f)$. Además siempre existe un (único a menos de multiplicar por un invertible de D) polinomio $\overline{f} \in D[x]$ tal que $f = \operatorname{cont}(f)\overline{f}$. Este polinomio $\overline{f}$ resulta obviamente primitivo.

Lema 0.2.5 (Lema de Gauss)**.** *Sean $f, g \in D[X]$, donde D es un dominio de factorización única.*

1. *Si f y g son primitivos, su producto fg también lo es.*
2. *Más en general, se tiene* $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$.

Demostración.

1. Supongamos primero que f y g son primitivos y que $p \in D$ es primo. Pongamos $f = a_n x^n + \cdots + a_1 x + a_0$ y $g = b_m x^m + \cdots + b_1 x + b_0$. Por ser f y g primitivos, $p \nmid \operatorname{cont}(f)$ y $p \nmid \operatorname{cont}(g)$, por lo que existen $i \in \{0, \ldots, n\}, j \in \{0, \ldots, m\}$ tales que

a_i y b_j no son múltiplos de p. Podemos entonces considerar $\bar{i}_0 := \text{mín}\{i \mid p \nmid a_i\}$ y $j_0 = \text{mín}\{j \mid p \nmid b_j\}$. Ahora bien, sea $k = i_0 + j_0$; el término k-ésimo de fg es

$$a_0 b_k + a_1 b_{k-1} + \cdots + a_{i_0} b_{j_0} + \cdots + a_{k-1} b_1 + a_k b_0.$$

Tenemos tres tipos de sumandos $a_i b_j$ en el término de arriba:

- sumandos en que $i < i_0$: $p \mid a_i$ y por tanto el sumando es múltiplo de p;
- sumandos en que $j < j_0$: $p \mid b_j$ y por tanto el sumando es múltiplo de p:
- el sumando $a_{i_0} b_{j_0}$: $p \nmid a_{i_0}$ y $p \nmid b_{j_0}$, por lo que el sumando no es múltiplo de p.

Para cada primo p, existe entonces un coeficiente que no es múltiplo de p (el k-ésimo, según la construcción de arriba). Se deduce $\text{cont}\,(fg) = 1$.

2. Supongamos ahora que f y g son polinomios cualesquiera y pongamos $f = \text{cont}\,(f)\bar{f}$ y $g = \text{cont}\,(g)\bar{g}$, con $\bar{f}, \bar{g}$ primitivos. Se tiene $fg = \text{cont}\,(f)\,\text{cont}\,(g)\bar{f}\bar{g}$, y como $\bar{f}\bar{g}$ es primitivo (por la parte anterior) se deduce que

$$\text{cont}\,(fg) = \text{cont}\,(f)\,\text{cont}\,(g)\,\text{cont}\,(\bar{f}\bar{g}) = \text{cont}\,(f)\,\text{cont}\,(g). \qquad \square$$

Criterios de irreducibilidad

Proposición 0.2.6. *Sea K un cuerpo y $p \in K[x]$ un polinomio de grado dos o tres. Entonces p es reducible si y sólo si tiene una raíz en K.*

Demostración. Un polinomio de grado dos o tres con coeficientes en un cuerpo es reducible si y sólo si tiene un factor lineal, pues $K[x]^\times = K^\times = K\backslash\{0\}$. Por el corolario 0.2.2 esto ocurre si y sólo si f tiene una raíz en K. $\square$

En lo queda de esta sección, D será un dominio y $\Bbbk$ denotará al cuerpo de fracciones de D.

Proposición 0.2.7 (Criterio de la raíz racional)**.** *Sea $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in D[X]$ con $a_n \neq 0$, y sea $\frac{p}{q} \in \Bbbk$ una raíz de f, con $\operatorname{mcd}(p,q) = 1$. Entonces $p \mid a_0$ y $q \mid a_n$ en D.*

Demostración. Tenemos que $a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0 = 0$, por lo tanto $a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0$ y entonces:

$$a_0 q^n = -p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1 q^{n-1})$$

Esto prueba que $p \mid a_0 q^n$. Como $\operatorname{mcd}(p,q) = 1$, entonces $\operatorname{mcd}(p,q^n) = 1$. El lema de Euclides (Proposición 0.1.14) nos da que $p \mid a_0$. Análogamente $q \mid a_n$. □

Corolario 0.2.8. *Si $f \in D[X]$ es un polinomio mónico y $\alpha \in \Bbbk$ es raíz de f, entonces $\alpha \in D$.*

El siguiente es un lema técnico que será de utilidad en los resultados que le siguen:

Lema 0.2.9. *Si $f \in D[x]$ es tal que $f = gh$ para ciertos $g, h \in \Bbbk[x]$, entonces existen $g', h' \in D[x]$ y $\lambda, \mu \in \Bbbk$ no nulos, tales que $f = g'h'$, $g = \lambda g'$ y $h = \mu h'$.*

Demostración. Tomando $a, b \in D^*$ como los respectivos productos de los denominadores de los coeficientes de g y h, surge que existen $\tilde{g}, \tilde{h} \in D[x]$ tales que $g = \frac{1}{a}\tilde{g}, h = \frac{1}{b}\tilde{h}$ (observar que para esto alcanza con que D sea un dominio).
Obtenemos la igualdad en D: $abf = \tilde{g}\tilde{h} = cont(\tilde{g})cont(\tilde{h})g''h''$, con $g'', h'' \in D[x]$ primitivos. Tomando contenidos de ambos lados, se deduce que $abcont(f) = \operatorname{cont}(g'')\operatorname{cont}(h'')$ y por tanto, cancelando ab, se tiene $f = cont(f)g''h''$. La prueba termina considerando por ejemplo $g' = cont(f)g'' = \frac{acont(f)}{cont(\tilde{g})}g$, $h' = h'' = \frac{b}{cont(\tilde{h})}$. □

Teorema 0.2.10 (Criterio de irreducibilidad de Gauss)**.** [2] *Sea $f \in D[x]$ no constante. Entonces f es irreducible en $D[x]$ si y sólo si es irreducible en $\Bbbk[x]$ y es primitivo en $D[x]$.*

Demostración. Supongamos primero que f es irreducible como polinomio en $\Bbbk[x]$ y es primitivo como polinomio en $D[x]$. Si $f = gh$ es una descomposición de f en producto de polinomios $g, h \in D[x]$, también lo es en $\Bbbk[x]$ y por tanto g o h es invertible en $\Bbbk[x]$. Supongamos sin perder generalidad que g lo es. Esto implica que $g \in \Bbbk^\times \cap D[x] = D\backslash\{0\}$. Pero en ese caso $\operatorname{cont}(f) = g\operatorname{cont}(h)$, y como $\operatorname{cont}(f) = 1$ se tiene que $g \in D$ es invertible. Se deduce que f es irreducible en $D[x]$.

Recíprocamente, supongamos que f es irreducible y no constante como polinomio en $D[x]$. Por la descomposición $f = \operatorname{cont}(f)\overline{f}$ con $\overline{f}$ primitivo, debe ser f primitivo.

Supongamos que $f = gh$ es una descomposición de f en producto de polinomios $g, h \in \Bbbk[x]$. Usando el Lema 0.2.9, se deduce $f = g'h'$ para ciertos $g', h' \in D[x]$ primitivos (porque f es primitivo) tales que $g = \lambda g', h = \mu h'$ para ciertos $\lambda, \mu \in \Bbbk$ no nulos.

Como f es irreducible en $D[x]$ se deduce que g' o h' son invertibles. Supongamos sin perder generalidad que g' es invertible en $D[x]$. Entonces $g' \in D\backslash\{0\}$, por lo que $g' \in D$ y por tanto $g \in \Bbbk$. Esto implica que en la descomposición original $f = gh$, el polinomio $g \in \Bbbk[x]$ es invertible. □

Ejemplo 0.2.2. Sea $f = x^3 + x^2 + 10x + 1 \in \mathbb{Z}[x]$. Por el criterio de la raíz racional, sus únicas posibles raíces racionales son ± 1. Se verifica fácilmente que $f(\pm 1) \neq 0$, luego f no tiene raíces racionales. En particular, por la Proposición 0.2.6, al ser f de grado tres, es irreducible en $\mathbb{Q}$ (y como es primitivo, es irreducible también en $\mathbb{Z}$, por el criterio de irreducibilidad de Gauss).

[2] En muchos textos se llama también a este resultado *lema de Gauss*.

Proposición 0.2.11 (Criterio de irreducibilidad de Eisenstein)**.** *Sea* $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in D[X]$ *con* $a_n \neq 0$*. Supongamos que existe* $p \in D$ *irreducible tal que:*

- $p \mid a_1, \ldots, p \mid a_{n-1}$,
- $p \nmid a_n$,
- $p \mid a_0, p^2 \nmid a_0$.

Entonces f *es irreducible en* $\Bbbk[x]$.[3]

Demostración. Supongamos $f = gh \in D[x]$ con $g, h \in \Bbbk[x]$. Veamos que $g \in \Bbbk\backslash\{0\}$ o $h \in \Bbbk\backslash\{0\}$. Escribamos $g = b_r x^r + \cdots + b_1 x + b_0$, $h = c_s x^s + \cdots + c_1 x + c_0$, con $b_r c_s \neq 0$. Ahora bien, por hipótesis $a_0 = b_0 c_0$ es múltiplo de p y no es múltiplo de p^2. Podemos suponer entonces sin pérdida de generalidad que $p \mid b_0$ y $p \nmid c_0$.

Por otra parte, como $p \nmid a_n = b_r c_s$, tenemos que b_r no es múltiplo de p. En particular, existe $i \in \{0, \ldots, r\}$ tal que $p \mid b_k$ para todo $k < i$ y $p \nmid b_i$. Se tiene entonces $p \nmid b_i c_0$ y por tanto $p \nmid a_i = b_i c_0 + b_{i-1}c_1 + \cdots + b_1 c_{i-1} + b_0 c_i$. Se deduce que $i = n$ y por tanto $\operatorname{gr}(h) = 0$, es decir $h \in \Bbbk\backslash\{0\}$. □

Ejemplos 0.2.1. 1. $f = x^4 + 2x^3 + 2x^2 + 2x + 2 \in \mathbb{Z}[x]$ es irreducible.

2. $f = x^n + p \in \mathbb{Z}[x]$, es irreducible para cualquier primo $p \in \mathbb{Z}$. Este ejemplo muestra que hay polinomios irreducibles en $\mathbb{Z}$ de grado arbitrario.

Preservación de la Factorización única

Lema 0.2.12. *Sean* D *un dominio y* $\Bbbk$ *su cuerpo de fracciones.*

1. *Si* $a \in D$ *es primo, entonces es primo en* $D[x]$.
2. *Sea* $f \in D[x]$ *es primitivo; si* f *es primo en* $\Bbbk[x]$ *entonces es primo en* $D[x]$.

Demostración. 1. Si $a \mid fg$, entonces $a \mid \operatorname{cont}(f)\operatorname{cont}(g)$ y por tanto $a \mid \operatorname{cont}(f)$ o $a \mid \operatorname{cont}(g)$. Se deduce que $a \mid f$ o $a \mid g$.

2. Si $f \mid gh$ en $D[x]$, entonces también $f \mid gh$ en $\Bbbk[x]$. Supongamos para fijar ideas que $f \mid g$ en $\Bbbk[x]$. Existe entonces $\varphi \in \Bbbk[x]$ tal que $f\varphi = g$. Multiplicando por el denominador común de los términos de φ se obtiene una igualdad en $D[x]$ de la forma $f\varphi' = ag$, con $a \in D$. Tomando contenidos y usando que f es primitivo, se deduce que $cont(\varphi') = acont(g)$, por lo que se tiene para cierto $h \in D[x]$, $acont(g)hf = ag$ en $D[x]$. Como D es un dominio, se deduce $cont(g)hf = g$ y por lo tanto $f \mid g$ en $D[x]$. □

Teorema 0.2.13. *Si* D *es un dominio de factorización única, entonces* $D[x]$ *también lo es.*

Demostración. Sabemos que $D[x]$ es también un dominio. Además, para $f \in D[x]$ no nulo y no invertible se tiene $f = \operatorname{cont}(f)\bar{f}$, con $\bar{f} \in D[x]$ no nulo y primitivo.

Sea $\Bbbk = Frac(D)$. Como $\Bbbk[x]$ es un dominio de factorización única (pues es un DIP), $\bar{f} \neq 0$ es invertible o se descompone en $\Bbbk[x]$ como producto de irreducibles. Cada irreducible en $\Bbbk[x]$ es de la forma $\frac{1}{a}h(x)$ con $h(x) \in D[x]$ irreducible en $\Bbbk[x]$ y $a \in D\backslash\{0\}$. Se tiene entonces que si $\bar{f}$ no es invertible, es de la forma $\bar{f} = \frac{1}{d}h_1 h_2 \ldots h_n$ con $d \in D\backslash\{0\}, h_i \in D[x]$ irreducible en $\Bbbk[x]$, para todo $i \in \{1, \ldots, n\}$. Para cada i podemos escribir $h_i = \operatorname{cont}(h_i)h_i'$ con h_i' primitivo. Se tiene entonces:

[3]En el práctico 5 aparece como ejercicio opcional una generalización del criterio de Eisenstein a dominios cualesquiera.

- h_i' es primitivo y por tanto irreducible en $D[x]$, para todo $i \in \{1, \dots, n\}$,
- $\frac{\operatorname{cont}(h_1)\cdots\operatorname{cont}(h_n)}{d} \in D$ es invertible en D,
- $cont(f)$ se descompone en irreducibles en D y por tanto en $D[x]$,
- $\bar{f} = \frac{\operatorname{cont}(h_1)\cdots\operatorname{cont}(h_n)}{d} h_1' h_2' \dots h_n'$,

por lo que $f = \frac{\operatorname{cont}(h_1)\cdots\operatorname{cont}(h_n)}{d} cont(f) h_1' h_2' \dots h_n'$.

Se deduce la existencia de la descomposición factorial en irreducibles.

Para la unicidad, por la Proposición 0.1.6, alcanza con probar que todo irreducible de $D[x]$ es primo. Sea $f \in D[x]$ irreducible.

Si $\operatorname{gr}(f) = 0$, entonces es claro que f es irreducible como elemento en D y por tanto primo en D, de lo que se deduce usando el Lema 0.2.12 que es primo en $D[x]$.

Si $\operatorname{gr}(f) > 0$, f es irreducible como elemento en $\Bbbk[x]$ y por tanto primo. Se deduce usando la otra parte del Lema 0.2.12 que es primo en $D[x]$. □

Este último teorema nos permite deducir que $\mathbb{Z}[x]$ y $\Bbbk[x, y] \cong \Bbbk[x][y]$ son dominios de factorización única (que no son dominios a ideales principales). Más en general, se tiene el siguiente corolario.

Corolario 0.2.14. *Si D es un dominio de factorización única $D[x_1, x_2, \dots, x_n]$ también lo es.*

Observación 0.2.3. El anillo de polinomios en infinitas variables $A = \Bbbk[x_1, x_2, \dots, x_n, \dots]$ es un dominio de factorización única. En efecto, si tomamos un polinomio $f \in A$, existe $n \in \mathbb{N}$ tal que $f \in A_n = \Bbbk[x_1, \dots, x_n]$ y por tanto f se descompone en producto de irreducibles de A_n. Es un ejercicio probar que los irreducibles de A_n son irreducibles en A. Usando argumentos similares, se prueba que los primos de A son irreducibles, de lo que se deduce la unicidad de la descomposición.

Este es un ejemplo de dominio de factorización única que no es noetheriano.