GyA - Teoría 1ª Parte

Jose Antonio Lorencio Abril

2019/2020

1 Anillos

Teorema 1.23. De la Correspondencia

Sea A un anillo, e I un ideal de A. Entonces

$$\left\{Ideales\ de\ \frac{A}{I}\right\} = \left\{\frac{J}{I} : I \subset J \trianglelefteq A\right\}$$

Y la siguiente aplicación es biyectiva

$$\begin{array}{ccc} \left\{\frac{J}{I} : I \subset J \trianglelefteq A\right\} & \to & \left\{Ideales\ de\ \frac{A}{I}\right\} \\ J & \mapsto & \frac{J}{I} \end{array}$$

Demostración

- **Sobreyectividad**

  $\underline{\frac{J}{I} \trianglelefteq \frac{A}{I}}$

  Como $J \trianglelefteq A$, entonces $0 \in J \implies 0 + I \in \frac{J}{I}$

  Dados $x, y \in J$, tenemos que $(x + I) + (y + I) = (x + y) + I \in \frac{J}{I}$, pues $x + y \in J$

  Dado $a \in A$, entonces $(a + I)(x + I) = ax + I \in \frac{J}{I}$, pues $ax \in J$

  <u>Sea ahora $K \trianglelefteq \frac{A}{I}$ y sea $J = \{a \in A/a + I \in K\}$</u>, y definimos

  $$\begin{array}{ccccc} A & \xrightarrow{f} & \frac{A}{I} & \xrightarrow{g} & \frac{\left(\frac{A}{I}\right)}{K} \\ a & \mapsto & a + I & & \\ & & x & \mapsto & x + K \end{array}$$

  Y sea $h = g \circ f$. Calculemos su núcleo:

  $$a \in Kerh \iff f(a) + K = g(f(a)) = 0_{\frac{\left(\frac{A}{I}\right)}{K}} = K = 0 + K \iff a + I = f(a) \in K \iff a \in J$$

  Es decir, $Kerh = J \overset{Def\ 1.20}{\implies} J \trianglelefteq A$.

  Además, si $a \in I \implies a + I = I = 0_{\frac{A}{I}} \in K \implies a \in J$. Es decir, $I \subset J$.

$¿\frac{J}{I} = K?$

'$\subseteq$' $x \in \frac{J}{I} \implies x = a + I,\ a \in J \implies x = a + I \in K$ (por la definición de J)

'$\supseteq$' $x \in K \subset \frac{A}{I} \implies x = a + I \in K,\ a \in A \implies a \in J \implies x = a + I \in \frac{J}{I}$

Recapitulando: dado un ideal de $\frac{A}{I}$, podemos escribir este como $\frac{J}{I}$, donde $I \subset J \trianglelefteq A$, por lo que nuestra aplicación es suprayectiva.

- **Inyectividad**

  Sean J_1, J_2 ideales de A que contienen a I tales que $\frac{J_1}{I} \subseteq \frac{J_2}{I}$. Entonces

  $$x \in J_1 \implies x{+}I \in \frac{J_1}{I} \subset \frac{J_2}{I} \implies x{+}I = y{+}I,\ y \in J_2 \implies x{-}y \in I \subset J_2 \implies x = x{-}y{+}y \in J_2 \implies J_1 \subseteq$$

  $$\text{Por tanto, si } \frac{J_1}{I} = \frac{J_2}{I} \implies \begin{cases} \frac{J_1}{I} \subseteq \frac{J_2}{I} \implies J_1 \subseteq J_2 \\ \frac{J_2}{I} \subseteq \frac{J_1}{I} \implies J_2 \subseteq J_1 \end{cases} \implies J_1 = J_2$$

  Y la aplicación es inyectiva.

Es decir, que la aplicación del enunciado es biyectiva. Pero esto quiere demuestra también la igualdad de los dos conjuntos de ideales.

Teorema 1.27. Primer teorema de isomorfía

Sea $f : A \to B$ un homomorfismo de anillos. Entonces existe un único isomorfismo de anillos $\overline{f} : \frac{A}{Kerf} \to Imf$ que hace conmutativo el diagrama

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p"'] & B \\ \frac{A}{Kerf} \arrow[r, dashed, "\overline{f}"] & Imf \arrow[u, "i"'] \end{tikzcd}$$

es decir, $i \circ \overline{f} \circ p = f$, donde i es la inclusión y p es la proyección.

En particular

$$\frac{A}{Kerf} \simeq Imf$$

Demostración

La aplicación $\overline{f} : \frac{A}{Kerf} \to Imf$ dada por $\overline{f}(x + Kerf) = f(x)$ está bien definida. Es decir, no depende de representantes. Veámoslo:

Si $x + Kerf = y + Kerf$ entonces $x - y \in Kerf$ y así $f(x) - f(y) = f(x - y) = 0 \implies f(x) = f(y)$.

Veamos ahora que es homomorfismo:

- $\overline{f}\left((x + Kerf) + (y + Kerf)\right) = \overline{f}\left((x + y) + Kerf\right) = f(x + y) = f(x) + f(y) =$
  $\overline{f}\left(x + Kerf\right) + \overline{f}\left(y + Kerf\right)$

- $\overline{f}\left((x+Kerf)(y+Kerf)\right)=\overline{f}\left((xy)+Kerf\right)=f(xy)=f(x)f(y)=$ $\overline{f}\left(x+Kerf\right)\overline{f}\left(y+Kerf\right)$
- $\overline{f}\left(1+Kerf\right)=f(1)=1$

Queda ver la biyectividad.

Comenzamos por la supreyectividad:

Dado $x\in Imf \implies \exists a\in A/x=f(a)=\overline{f}\left(a+Kerf\right)$

Para ver que es inyectiva usamos la Proposición 1.21 (un homomorfismo de anillos es inyectivo sii $Kerf=0$):

Si $x+Kerf\in Ker\overline{f} \implies 0=\overline{f}\left(x+K\right)=f(x) \implies x\in Kerf \implies x+Kerf=0+Kerf$. Es decir, $Ker\overline{f}=0$ y, por tanto, $\overline{f}$ es inyectiva.

Así, $\overline{f}$ es un isomorfismo y los conjuntos $\frac{A}{Kerf}$, Imf son isomorfos.

¿Hace conmutativo el diagrama?

Dado $x\in Kerf$, se tiene que

$$i\left(\overline{f}\left(p(x)\right)\right)=\overline{f}\left(x+Kerf\right)=f(x)$$

¿Es único?

Supongamos que otro homomorfismo $\overline{g}:\frac{A}{Kerf}\to Imf$ verifica $i\circ\overline{g}\circ p=f$, entonces $\forall x\in Kerf$, se tiene $\overline{g}(x+Kerf)=i\left(\overline{g}\left(p(x)\right)\right)=f(x)=\overline{f}\left(x+Kerf\right)$, y así $\overline{g}=\overline{f}$.

Teorema 1.28. Segundo Teorema de Isomorfía

Sea A un anillo y sean I,J dos ideales tales que $I\subset J$. Entonces $\frac{J}{I}\trianglelefteq\frac{A}{I}$ y existe un isomorfismo de anillos

$$\frac{\left(\frac{A}{I}\right)}{\left(\frac{J}{I}\right)}\simeq\frac{A}{J}$$

Demostración

Por el teorema de correspondencia, $\frac{J}{I}\trianglelefteq\frac{A}{I}$.

Sea $f:\frac{A}{I}\to\frac{A}{J}$ la aplicación definida por $f(a+I)=a+J$.

f está bien definida: si $a+I=b+I$, entonces
$a-b\in I \implies a-b\in J \implies a+J=b+J \implies f(a+I)=f(b+I)$

Homomorfismo:

- $f\left((a+I)+(b+I)\right)=f\left((a+b)+I\right)=(a+b)+J=(a+J)+(b+J)=f\left(a+I\right)+f\left(b+I\right)$
- $f\left((a+I)(b+I)\right)=f\left(ab+I\right)=ab+J=(a+J)(b+J)=f\left(a+I\right)f\left(b+I\right)$
- $f(1+I)=f(1+J)$

Suprayectividad: dado $b\in\frac{A}{J}$, entonces $\exists a\in A/b=a+J \implies b=f(a+I)$. Al ser suprayectiva $Imf=\frac{A}{J}$

Núcleo: $f(a+I)=0=0+J \iff a+J=0+J \iff a\in J$. Es decir, $Kerf=\frac{J}{I}$.

Por el primer teorema de isomorfía, tenemos que

$$\frac{\left(\frac{A}{I}\right)}{\left(\frac{J}{I}\right)}\simeq\frac{A}{J}$$

Teorema 1.29. Tercer Teorema de Isomorfía

Sea A un anillo con un subanillo B y un ideal I. Entonces:

1. $B \cap I \trianglelefteq B$
2. $B + I$ es un subanillo de A que contiene a I como ideal
3. Se tiene un isomorfismo de anillos $\frac{B}{B \cap I} \simeq \frac{B+I}{I}$

Demostración

1. No vacío: como B es subanillo de A, entonces $0 \in B$. Como $I \trianglelefteq A$, entonces $0 \in I$. Así, $0 \in B \cap I \implies B \cap I \neq \emptyset$

   Suma: dados $x, y \in B \cap I \implies \begin{cases} x, y \in B \implies x + y \in B \\ x, y \in I \implies x + y \in I \end{cases} \implies x + y \in B \cap I$

   Producto: dados $x \in B \cap I,\ b \in B \implies \begin{cases} xb \in B \\ xb \in I \end{cases} \implies xb \in B \cap I$

   Por tanto, $B \cap I \trianglelefteq B$.

2. Por la proposición 1.7, para ver que $B + I$ es subanillo de A, basta ver que contiene al 1 y es cerrado para restas y productos

   Contiene al 1: Como B es subanillo, entonces $1 \in B \implies 1 = 1 + 0 \in B + I$

   Cerrado para restas: Sean
   $x, y \in B+I \implies x = x_1+x_2,\ y = y_1+y_2,\ x_1, y_1 \in B,\ x_2, y_2 \in I \implies x-y = (x_1-y_1)+(x_2-y_2)$.

   Pero B es cerrado para restas, por lo que $x_1 - y_1 \in B$, y también
   $y_2 \in I \implies -y_2 \in I \implies x_2 - y_2 \in I$. Por tanto $x - y \in B + I$

   Cerrado para productos: Sean
   $x, y \in B + I \implies xy = (x_1 + x_2)(y_1 + y_2) = x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$

   Como B es cerrado para productos, entonces $x_1y_1 \in B$.

   Como I es un ideal en A, entonces $x_1y_2, x_2y_1, x_2y_2 \in I \implies x_1y_2 + x_2y_1 + x_2y_2 \in I$

   Por tanto, $xy \in B + I$, y así, este es subanillo de A.

   Además, contiene a I pues dado $x \in I \implies x = 0 + x \in B + I$

3. Sea $f : B \to \frac{A}{I}$ la composición de la inclusión $j : B \to A$ con la proyección $p : A \to \frac{A}{I}$.

   Calculemos $Kerf$:

   $x \in Kerf \iff f(x) = 0 = 0+I \iff p \circ j(x) = 0+I \iff p(x) = 0+I \iff x+I = 0+I \iff x \in I$

Pero $x \in B$, por tanto $Kerf = B \cap I$.

$\underline{Imf}$:

$$x \in B \implies f(x) = p \circ j(x) = p(x) = x + I$$

Es decir, $Imf = \frac{B}{I}$, pero $\frac{B}{I} = \frac{B+I}{I}$:

'$\subseteq$' $x + I \in \frac{B}{I} \implies x + I = (x+0) + I \in \frac{B+I}{I}$

'$\supseteq$' $(x+y) + I \in \frac{B+I}{I} \implies (x+y) + I = (x+I) + (y+I) = x + I \in \frac{B}{I}$

Así, por el primer teorema de isomorfía:

$$\frac{B}{B \cap I} \simeq \frac{B+I}{I}$$

Teorema 1.33. Teorema Chino de los Restos para anillos

Sea A un anillo y sea $I_1, ..., I_n$ ideales de A tales que $I_i + I_j = A$ para todo $i \neq j$.

Entonces $I_1 \cap ... \cap I_n = I_1 ... I_n$. Además

$$\frac{A}{I_1 \cap ... \cap I_n} \simeq \frac{A}{I_1} \times ... \times \frac{A}{I_n}$$

Demostración

Razonamos por inducción sobre n, empezando por caso $n = 2$, pues el caso $n = 1$ es trivial.

'$\subseteq$' La hipótesis $I_1 + I_2 = A = (1)$ nos dice que existen $x_1 \in I_1, x_2 \in I_2 / x_1 + x_2 = 1$, entonces $\forall a \in I_1 \cap I_2$ se tiene $a = ax_1 + ax_2 \in I_1 I_2$, por lo que $I_1 \cap I_2 \subseteq I_1 I_2$

'$\supseteq$' $x \in I_1 I_2 \implies x = \sum_{i=0}^{k} x_i y_i,\ x_i \in I_1, y_i \in I_2 \implies x_i y_i \in I_1 \cap I_2 \implies x \in I_1 \cap I_2$

Veamos la <u>isomorfía:</u> sea

$$\begin{array}{rcc} f : A & \rightarrow & \frac{A}{I_1} \times \frac{A}{I_2} \\ a & \mapsto & (a + I_1, a + I_2) \end{array}$$

- $f(a+b) = ((a+b) + I_1, (a+b) + I_2) = ((a + I_1) + (b + I_1), (a + I_2) + (b + I_2)) = (a + I_1, a + I_2) + (b + I_1, b + I_2) = f(a) + f(b)$
- $f(ab) = (ab + I_1, ab + I_2) = ((a+I_1)(b+I_1), (a+I_2)(b+I_2)) = (a+I_1, a+I_2)(b+I_1, b+I_2) = f(a)f(b)$
- $f(1) = (1 + I_1, 1 + I_j)$, que es la unidad en $\frac{A}{I_1} \times \frac{A}{I_2}$

El núcleo:

$$f(a) = 0 \iff (a + I_1, a + I_2) = (0,0) = (0 + I_1, 0 + I_2) \iff a \in I_1, a \in I_2 \iff a \in I_1 \cap I_2$$

La imagen, es todo $\frac{A}{I_1} \times \frac{A}{I_2}$, pues f es suprayectiva.

Dado $(a + I_1, b + I_2) \in \frac{A}{I_1} \times \frac{A}{I_2}$, entonces $c = ax_2 + bx_1,\ x_1, x_2$ los de más atrás, entonces $f(c) = (ax_2 + bx_1 + I_1, ax_2 + bx_1 + I_2) = (ax_2 + I_1, bx_1 + I_2) = ((a + I_1)(x_2 + I), (b + I_2)(x_1 + I_2)) = (a + I_1, b + I_2)$.

Entonces, por el primer teorema de isomorfía, tenemos que

$$\frac{A}{I_1 \cap I_2} \simeq \frac{A}{I_1} \times \frac{A}{I_2}$$

Pasemos al caso general, $n > 2$.

Nótese que si demostramos que $(I_1 \cap ... \cap I_{n-1}) + I_n = A$ ya lo tenemos, pues, por la hipótesis de inducción

$$I_1 \cap ... \cap I_{n-1} \cap I_n \overset{n=2}{=} (I_1 \cap ... \cap I_{n-1})I_n \overset{n-1}{=} I_1 ... I_{n-1} I_n$$

y que

$$\frac{A}{I_1 \cap ... \cap I_n} = \frac{A}{(\cap_{i=1}^{n-1} I_i) \cap I_n} \overset{n=2}{\simeq} \frac{A}{\cap_{i=1}^{n-1} I_i} \times \frac{A}{I_n} \overset{n-1}{\simeq} \frac{A}{I_1} \times ... \times \frac{A}{I_{n-1}} \times \frac{A}{I_n}$$

Para ver lo que necesitemos, nótese que $\forall i \leq n-1,\ \exists a_i \in I_i,\ b_i \in I_n / 1 = a_i + b_i$, entonces, multiplicando todas esas expresiones, obtenemos

$$1 = 1 \cdot 1 \cdot ... \cdot 1 = \prod_{i=1}^{n-1} (a_i + b_i) = a_1 \cdot ... \cdot a_{n-1} + b$$

donde b engloba a todos los sumandos que se obtendrían desarrollando los productos, excepto el que hemos dejado fuera, y está en I_n porque en cada sumando hay al menos un b_i, de I_n. Como, además, $a_1 \cdot ... \cdot a_{n-1} \in I_1 \cap ... \cap I_{n-1}$, entonces $1 \in (I_1 \cap ... \cap I_{n-1}) + I_n$, por lo que $(I_1 \cap ... \cap I_{n-1}) + I_n = A$, como queríamos ver.

2 Divisibilidad en Dominios

Caracterización de DFU

Lema 2.21

Si D es un DFU, entonces todo elemento irreducible de D es primo.

Demostración

Sea $p \in D$ irreducible, y sean $a, b \in D$ tales que $p|ab$. <u>*¿$p|a$ ó $p|b$?*</u>

Si alguno de los dos es 0 es claro que sí. Supongamos que ninguno es nulo.

Entonces $ab = tp$ para algún $t \in D$. Si

$$t = up_1...p_n$$

$$a = vq_1...q_m$$

$$b = wr_1...r_k$$

son factorizaciones en irreducibles, con $u, v, w \in D^*$, entonces

$$upp_1...p_n = (vw)q_1...q_m r_1...r_k$$

y por la unicidad de la factorización, p es asociado de algún q_i y entonces $p|a$ o de algún r_i y entonces $p|b$.

Proposición 2.22

Para un dominio D, las condiciones siguientes son equivalentes:

1. D es un DFU
2. Todo elemento no nulo de D es producto de primos
3. D es un DF en el que todo irreducible es primo

Demostración

'$1 \implies 2$' D DFU $\Longrightarrow$ todo elemento no nulo de D es producto de irreducibles $\overset{Lema\ 2.21}{\Longrightarrow}$ todo elemento no nulo de D es producto de primos

'$2 \implies 3$' En un dominio todo primo es irreducible (proposición 2.13), por lo que si todo no nulo de D es producto de primos entonces todo no nulo es producto de irreducibles y, por tanto, D es un DF..

Supongamos ahora que p es irreducible y sea $p = q_1...q_k$ con $q_1, ..., q_k$ primos.

Como p es irreducible, entonces algún q_i debe ser asociado de p, podemos suponer que es q_1. Así, $p|q_1$ y $q_1|p$. Entonces, como q_1 es primo, también lo es p.

'$3 \implies 1$' Por hipótesis, todo elemento no nulo de D se factoriza como un producto de primos. Solo falta ver la unicidad de las factorizaciones.

Sean $up_1...p_n = vq_1...q_m$, con p_i, q_i irreducibles $\forall i,\ u, v \in D^*$. Suponemos que $n \leq m$ y razonamos por inducción sobre n.

Si $n = 0$, entonces $m = 0$, ya que los divisores de las unidades son unidades.

Supongamos $n > 0$ y la hipótesis de inducción. Tenemos entonces que p_n es primo, por hipótesis, por lo que divide a algún q_i y de hecho son asociados (porque p_n también es irreducible). Reordenando si es necesario, podemos suponer $i = m$.

Es decir, $\exists w \in D^*/q_m = wp_n$. Entonces

$$up_1...p_{n-1} = (vw)q_1...q_{m-1}$$

Por la hipótesis de inducción se tiene $n - 1 = m - 1 \implies n = m$ y existe una biyección

$$\tau : \{1, ..., n-1\} \to \{1, ..., n-1\}$$

tal que p_i y $q_{\tau(i)}$ son asociados $\forall i = 1, ..., n-1$.

La extensión de τ a una permutación σ de $\mathbb{N}_n$ tal que p_i y $q_{\sigma(i)}$ son asociados $\forall i$ es la evidente:

$$\sigma(i) = \begin{cases} \tau(i) & i < n \\ n & i = n \end{cases}$$

Y así, obtenemos que las factorizaciones iniciales son equivalentes.

DIP implica DFU

Proposición 2.24

Si D es un DIP y $0 \neq a \in D \setminus D^*$, las siguientes condiciones son equivalentes:

1. a es irreducible
2. (a) es un ideal maximal
3. $\frac{A}{(a)}$ es un cuerpo
4. a es primo
5. (a) es un ideal primo
6. $\frac{a}{(a)}$ es un dominio

Demostración

'1 $\iff$ 2' Por la proposición 2.15.(6)

- a irreducible si y solo si (a) es maximal entre los ideales principales propios no nulos de D

  ' $\implies$ ' a irreducible si, y solo si, $a = bc \implies b \in A^*$ *ó* $c \in A*$. Entonces, supongamos que $(a) \subset (b) \iff a \in (b) \iff a = bc$.

  Entonces, o bien $(b) = A$, o bien b es asociado de a, lo que implica $a|b$, y entonces $b \in (a)$, por lo que $(b) \subset (a)$, y así $(a) = (b)$. Es decir, si a es irreducible, no puede haber ningún ideal principal que contenga propiamente al ideal que genera.

' $\Longleftarrow$ ' No existe ningún $0 \neq b \in A \setminus A^*/(a) \subsetneq (b)$, entonces, si $a = bc$, se tiene que

$$\begin{cases} b|a \implies a \in (b) \implies (a) \subset (b) \implies \begin{cases} (a) = (b) \implies a, b \text{ asociados} \implies c \in A^* \checkmark \\ (b) = A \implies b \in A^* \checkmark \end{cases} \\ c|a \implies a \in (c) \implies (a) \subset (c) \implies \begin{cases} (a) = (c) \implies a, c \text{ asociados} \implies b \in A^* \checkmark \\ (c) = A \implies c \in A^* \checkmark \end{cases} \end{cases}$$

'2 $\iff$ 3' Por la proposición 2.6.(1)

- I es maximal si y solo si $\frac{A}{I}$ es un cuerpo

  $\frac{A}{I}$ es un cuerpo si, y solo si, sus únicos ideales son el 0 y el total.

  I es maximal si, y solo si, no existe ningún ideal propio que lo contenga.

  ' $\implies$ ' Por el teorema de la correspondencia, los ideales de $\frac{A}{I}$ son los ideales de A que contienen a I, módulo I. Como el único ideal de A que contiene a I es el total, entonces los ideales de $\frac{A}{I}$ son el total y el 0 y es un cuerpo.

  ' $\Longleftarrow$ ' Si es un cuerpo, entonces los únicos ideales son el 0 y el total. La biyección del teorema de correspondencia nos da los ideales de A que contienen a I como $\pi^{-1}(J)$, J ideal de $\frac{A}{I}$. Pero $\pi^{-1}(0) = 0$, $\pi^{-1}(\frac{A}{I}) = A$. Por lo que I es maximal.

'4 $\iff$ 5' Por la proposición 2.15.(5)

- a primo si y solo si (a) es un ideal primo no nulo de D

  $a \text{ primo} \iff (a|bc \implies a|b \text{ ó } a|c) \iff (bc \in (a) \implies b \in (a) \text{ ó } c \in (a)) \iff (a) \text{ primo}$

'5 $\iff$ 6' Por la proposición 2.6.(2)

- I es primo si y solo si $\frac{A}{I}$ es un dominio

  ' $\implies$ ' Sean $a + I$, $b + I$ dos elementos no nulos de $\frac{A}{I}$. Entonces $a, b \notin I \overset{I \text{ primo}}{\implies} ab \notin I$, por lo que $(a + I)(b + I) = ab + I \neq 0$. Por la proposición 2.3.(3), $\frac{A}{I}$ es un dominio.

  ' $\Longleftarrow$ ' Si $\frac{A}{I}$ es un dominio, por la proposición 2.3.(3), si $(a + I), (b + I) \in \frac{A}{I}$ no nulos, entonces $ab + I \neq 0$. Es decir, que si $a, b \notin I \implies ab \notin I$. Usando el contrarrecíproco obtenemos $ab \in I \implies a \in I \text{ ó } b \in I$. Por lo que I es primo.

'2 $\implies$ 5' Por la proposición 2.6.(3)

- Si I es maximal entonces es primo

  $I \text{ maximal} \overset{2.6.(1)}{\iff} \frac{A}{I} \text{ cuerpo} \implies \frac{A}{I} \text{ dominio} \overset{2.6.(2)}{\iff} I \text{ primo}$

'4 $\implies$ 1' Por la proposición 2.13

- En un dominio todo elemento primo es irreducible

  Si $a = bc$, entonces $b|a$ y $c|a$. Como $a|a \implies a|bc \overset{a \text{ primo}}{\implies} a|b \text{ ó } a|c$.

  - Si $a|b$, entonces a, b son asociados
  - Si $a|c$, entonces a, c son asociados

  Por lo que a es irreducible.

Teorema 2.25

Todo DIP es un DFU.

Demostración

Si demostramos que D es un DF, entonces, por la proposición 2.24, al ser D un DIP, tenemos que todo irreducible es primo. Entonces D es un DF con todo irreducible primo, por la proposición 2.22.$(3 \implies 1)$, tenemos el resultado.

Es decir, basta ver que D es DF.

Por reducción al absurdo, supongamos que D no es DF.

Vamos a construir, por recurrencia, una sucesión $a_1, a_2, ...$ de elementos de D que no admiten factorización y tales que $(a_1) \subset (a_2) \subset ...$ es una cadena estrictamente creciente de ideales de D.

Así, sea $a_1 \in D$ un elemento que no admite factorización en irreducibles, que existe pues suponemos que D no es DF.

Supongamos, entonces, que hemos seleccionado $a_1, ..., a_n,\ n \geq 1$, satisfaciendo las condiciones anteriores. Entonces a_n no es irreducible (pues en tal caso sería producto de irreducibles), luego existen $x, y \in D \setminus D^*/a_n = xy$.

Como a_n no es producto de irreducibles, al menos uno de los factores x, y no es producto de irreducibles. Supongamos que es x.

Entonces, haciendo $a_{n+1} = x$, tenemos que $a_{n+1}|a_n \implies (a_n) \subset (a_{n+1})$ y la inclusión es estricta, pues $y \in D \setminus D^*$, no es unidad.

Una vez construida la sucesión, tomamos

$$I = (a_1, a_2, ...) = \cup_{i \in \mathbb{N}}(a_i)$$

Esta igualdad se debe a que $(a_i) \subset (a_{i+1})$, luego $(a_1, ..., a_k) = (a_k) = \cup_{i=1}^{k}(a_i)$. Tomando límites la tenemos.

Como D es DIP, $\exists x \in D/I = (x)$. En particular, $x \in I$, por tanto, existe un índice, i, tal que $x \in (a_i)$ (y de hecho pertenece a todos los posteriores también). Además, dado que
$(a_i) \subset I = (x) \implies a_i \in (x)$. O sea, que x y a_i son asociados. Pero esto quiere decir que $(a_i) = (x)$, y por lo tanto $(a_i) = (a_{i+1})\#$ Esto es una contradicción, ya que los hemos construido de forma que estuvieran estrictamente contenidos. Por tanto, D debe ser un DF y, como explicamos al principio, es un DFU.

DE implica DIP

Lema 2.28

Sea δ una función euclídea en D, sea I un ideal de D y $0 \neq a \in D$, $a \in I$. Entonces
$I = (a) \iff \delta(a) \leq \delta(x),\ \forall x \in I.$

Demostración

'$\implies$' $I = (a) \implies \forall x \in I,\ a|x \overset{DE1}{\implies} \delta(a) \leq \delta(x)$

' $\Longleftarrow$ ' Como $a \in I \implies (a) \subset I$.

Sea $x \in I$, por $DE2$ se tiene que $\exists q, r \in D / x = aq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(a)$.

Entonces $r = x - aq \in I$, y entonces $\delta(a) \leq \delta(r)$. Por tanto, ha de ser $r = 0$. Es decir, $x = aq \implies x \in (a)$. Así, $I \subset (a)$.

Y deducimos que $(a) = I$.

Teorema 2.29

Todo dominio euclídeo es DIP.

Demostración

Sea D un DE, δ un función euclídea en D y sea $I \triangleleft D$. <u>¿Existe $0 \neq a \in I$ tal que $\delta(a) \leq \delta(x),\ \forall x \in I$?</u>

Sea $a/\delta(a) = \min\{\delta(r) | r \in I, r \neq 0\}$, nótese que esto es posible porque δ está acotada inferiormente por 0 y toma valores discretos. Como $a \in I \implies (a) \subset I$.

Ahora bien, si $y \in I$, entonces $\exists q, r \in D / y = qa + r$, con $r = 0$ o $\delta(r) < \delta(a)$.

Entonces $r = y - qx \in I$, por tanto, como a presenta el mínimo de los δ, ha de ser $r = 0$. Es decir, $y = qx \implies y \in (x)$.

Así, $I \subset (a)$ y tenemos las dos inclusiones.

Propiedad universal del cuerpo de fracciones

Proposición 2.34

Sean D un dominio, $Q(D)$ su cuerpo de fracciones y $u : D \to Q(D)$ la aplicación dada por $u(a) = \frac{a}{1}$. Entonces:

1. **Propiedad universal del cuerpo de fracciones:** Para toda pareja (K, f) formada por un cuerpo K y un homomorfismo inyectivo de anillos $f : D \to K$, existe un único homomorfismo de cuerpos $\overline{f} : Q(D) \to K$ tal que $\overline{f} \circ u = f$. Se dice que $\overline{f}$ completa de modo único el diagrama

$$\begin{tikzcd} D \arrow[r, "u"] \arrow[dr, "f"'] & Q(D) \arrow[d, dashed, "\overline{f}"] \\ & K \end{tikzcd}$$

2. Si dos homomorfismos de cuerpos $g, h : Q(D) \to K$ coinciden sobre D entonces son iguales. Es decir, si $g \circ u = h \circ u$ entonces $g = h$

3. $Q(D)$ está determinado salvo isomorfismos por la propiedad universal. Explícitamente: supongamos que existen un cuerpo F y un homomorfismo inyectivo de anillos $v : D \to F$ tales que, para todo cuerpo K y todo homomorfismo inyectivo de anillos $f : D \to K$, existe un único homomorfismo de cuerpos $\overline{f} : F \to K$ tal que $\overline{f} \circ v = f$. Entonces existe un isomorfismo $\phi : F \to Q(D)$ tal que $\phi \circ v = u$.

Demostración

1) Sea f como en el enunciado. Si $\overline{f} : Q(D) \to K$ es un homomorfismo de cuerpos tal que $\overline{f} \circ u = f$, entonces, $\forall \frac{a}{s} \in Q(D)$, se verifica

$$\overline{f}\left(\frac{a}{s}\right) = \overline{f}\left(u(a)u(s)^{-1}\right) = \left(\overline{f} \circ u\right)(a)\left(\overline{f} \circ u\right)(s)^{-1} = f(a)f(s)^{-1}$$

Esto prueba que el único homomorfismo de cuerpos $\overline{f}$ que puede satisfacer $\overline{f} \circ u = f$ tiene que venir dado por $\overline{f}\left(\frac{a}{s}\right) = f(a)f(s)^{-1}$.

Solo falta comprobar que la aplicación $\overline{f}$ así dada está bien definida y es un homomorfismo.

Si $\frac{a_1}{s_1} = \frac{a_2}{s_2}$ entonces $a_1 s_2 = a_2 s_1$, luego $f(a_1)f(s_2) = f(a_2)f(s_1) \iff f(a_1)f(s_1)^{-1} = f(a_2)f(s_2)^{-1}$. Luego $\overline{f}$ está bien definida.

Veamos que es un homomorfismo:

- $\overline{f}\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}\right) = \overline{f}\left(\frac{a_1 s_2 + a_2 s_1}{s_1 s_2}\right) = f(a_1 s_2 + a_2 s_1) f(s_1 s_2)^{-1} =$ $\left(f(a_1 s_2) + f(a_2 s_1)\right) f(s_1)^{-1} f(s_2)^{-1} = f(a_1)f(s_2)f(s_1)^{-1}f(s_2)^{-1} + f(a_2)f(s_1)f(s_1)^{-1}f(s_2)^{-1} =$ $f(a_1)f(s_1)^{-1} + f(a_2)f(s_2)^{-1} = \overline{f}\left(\frac{a_1}{s_1}\right) + \overline{f}\left(\frac{a_2}{s_2}\right)$
- $\overline{f}\left(\frac{a_1}{s_1}\frac{a_2}{s_2}\right) = f(a_1 a_2) f(s_1 s_2)^{-1} = f(a_1)f(a_2)f(s_1)^{-1}f(s_2)^{-1} = \overline{f}\left(\frac{a_1}{s_1}\right)\overline{f}\left(\frac{a_2}{s_2}\right)$
- $\overline{f}(1) = \overline{f}\left(\frac{1}{1}\right) = f(1)f(1)^{-1} = 1 \cdot 1^{-1} = 1 \cdot 1 = 1$

Y ya lo tenemos.

2) Si ponemos $f = g \circ u = h \circ u : D \to K$, los homomorfismos g, h completan el diagrama de **1)** y por la unicidad se tiene $g = h$.

3) Aplicando **1)** a v del enunciado, encontramos un homomorfismo $\overline{v} : Q(D) \to F$ tal que $\overline{v} \circ u = v$, y aplicando la hipótesis de **3)** sobre u, encontramos un homomorfismo $\overline{u} : F \to Q(D)$ tal que $\overline{u} \circ v = u$. Entonces la composición $\overline{u} \circ \overline{v} : Q(D) \to Q(D)$ verifica $(\overline{u} \circ \overline{v}) \circ u = \overline{u} \circ v = u = Id_{Q(D)} u$. Por **2)**, obtenemos que $\overline{u} \circ \overline{v} = Id_{Q(D)}$.

En particular $\overline{u}$ es suprayectiva, y es inyectiva por ser homomorfismo de cuerpos (el núcleo es un ideal y los únicos ideales en un cuerpo son el 0 y el total, entonces el núcleo es 0 y es inyectiva), y entonces $\phi = \overline{u}$ es el isomorfismo buscado.

$$\begin{tikzcd} D \arrow[r, "u"] \arrow[dr, "v"'] & Q(D) \arrow[d, dashed, "\overline{v}"] \\ & F \end{tikzcd} \qquad \begin{tikzcd} D \arrow[r, "v"] \arrow[dr, "u"'] & F \arrow[d, dashed, "\overline{u}"] \\ & Q(D) \end{tikzcd}$$

3 Polinomios

Propiedad Universal de Anillo de Polinomios (PUAP)

Proposición 3.3

Sean A un anillo, $A[X]$ el anillo de polinomios con coeficientes en A en la indeterminada X y $u : A \to A[X]$ el homomorfismo de inclusión.

1. **PUAP** Para todo homomorfismo de anillos $f : A \to B$ y todo elemento $b \in B$ existe un único homomorfismo de anillos $\overline{f} : A[X] \to B$ tal que $\overline{f}(X) = b$ y $\overline{f} \circ u = f$. Para expresar la última igualdad se dice que $\overline{f}$ completa de modo único el diagrama

$$\begin{tikzcd} A \arrow[r, "u"] \arrow[dr, "f"'] & A[X] \arrow[d, dashed, "\overline{f}"] \\ & B \end{tikzcd}$$

2. Si dos homomorfismos de anillos $g, h : A[X] \to B$ coinciden sobre A y en X entonces son iguales. Es decir, si $g \circ u = h \circ u$ y $g(X) = h(X)$ entonces $g = h$.

3. $A[X]$ y u están determinados salvo isomorfimos por la PUAP.

   Explícitamente: supongamos que existen un homomorfismo de anillos $v : A \to P$ y un elemento $T \in P$ tales que, para todo homomorfismo de anillos $f : A \to B$ y todo elemento $b \in B$, existe un único homomorfismo de anillos $\overline{f} : P \to B$ tal que $\overline{f} \circ v = f$ y $\overline{f}(T) = b$. Entonces existe un isomorfismo $\phi : A[X] \to P$ tal que $\phi \circ u = v$ y $\phi(X) = T$.

Demostración

1) Sean $f : A \to B$ y $b \in B$ como en el enunciado. Si existe un homomorfismo $\overline{f} : A[X] \to B$ tal que $\overline{f} \circ u = f$ y $\overline{f}(X) = b$, entonces, para un polinomio $P = \sum_{n\geq 0} p_n X^n$, se tendrá

$$\overline{f}\,(P) = \overline{f}\left(\sum_{n\geq 0} u\,(p_n)\,X^n\right) = \sum_{n\geq 0} f(p_n) b^n$$

Por tanto, la aplicación dada por $\overline{f}\,(P) = \sum_{n\geq 0} f(p_n) b^n$ es la única que puede cumplir tales condiciones.

<u>¿Homomorfismo?</u>

- $\overline{f}(P+Q) = \sum_{n\geq 0} f\,(p_n + q_n)\,b^n = \sum_{n\geq 0} \left(f\,(p_n)\,b^n + f\,(q_n)\,b^n\right) = \sum_{n\geq 0} f\,(p_n)\,b^n + \sum_{n\geq 0} f\,(q_n)\,b^n = \overline{f}(P) + \overline{f}(Q)$
- $\overline{f}(PQ) = \sum_{n\geq 0} f\left(\sum_{k=0}^{n} p_k q_{n-k}\right) b^n = \sum_{n\geq 0} \left(\sum_{k=0}^{n} f\,(p_k q_{n-k})\right) b^n = \sum_{n\geq 0} \left(\sum_{k=0}^{n} f\,(p_k)\, f\,(q_{n-k})\right) b^n = \overline{f}(P)\overline{f}(Q)$
- $\overline{f}(1) = f(1)b^0 = 1 \cdot 1 = 1$

$\underline{¿\overline{f}(X) = b?}$

$\overline{f}(X) = f(0)b^0 + f(1)b^1 = 0 \cdot 1 + 1 \cdot b = b$

$\underline{¿\overline{f} \circ u = f?}$ Es evidente, pues hemos construido $\overline{f}$ para que verifique esto.

2) Haciendo $f = g \circ u = h \circ u : A \to B$, los homomorfismos g, h completan el diagrama de **1)**, por la unicidad se tiene que $g = h$.

3) Tomemos $v : A \to P$ y $T \in P$ como en el enunciado. Fijémonos en estos diagramas:

$$\begin{tikzcd} A \arrow[r, "u"] \arrow[dr, "v"'] & A[X] \arrow[d, dashed, "\overline{v}"] \\ & P \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "v"] \arrow[dr, "u"'] & P \arrow[d, dashed, "\overline{u}"] \\ & A[X] \end{tikzcd}$$

Aplicando **1)** al primero, obtenemos $\overline{v} : A[X] \to P / \overline{v} \circ u = v \ y \ \overline{v}(X) = T$.

Aplicando las hipótesis de **3)** al segundo, obtenemos $\overline{u} : P \to A[X] / \overline{u} \circ v = u \ y \ \overline{u}(T) = X$.

Entonces, la composición, $\overline{u} \circ \overline{v} : A[X] \to A[X]$ verifica

$$(\overline{u} \circ \overline{v}) \circ u = \overline{u} \circ v = u = Id_{A[X]} u \qquad y \qquad (\overline{u} \circ \overline{v})(X) = \overline{u}(T) = X = Id_{A[X]}(X)$$

Luego, por **2)** obtenemos que $\overline{u} \circ \overline{v} = Id_{A[X]}$.

Análogamente se demuestra que $\overline{v} \circ \overline{u} = Id_P$.

Y así, el isomorfismo buscado es $\phi = \overline{v}$.

Relación entre la multiplicidad de una raíz de un polinomio y sus derivadas

Proposición 3.11

Un elemento $a \in A$ es una raíz múltiple de $P \in A[X]$ si y solo si $P(a) = P'(a) = 0$

Demostración

' $\Longleftarrow$ ' Por el teorema de Ruffini, a es una raíz de P si y solo si $P(a) = 0$.

Si a es raíz simple se tiene $P = (X - a)Q$ para $Q \in A[X]$ con $Q(a) \neq 0$, entonces

$$P' = Q + (X - a)Q'$$

y entonces $P'(a) = Q(a) + 0 \cdot Q'(a) = Q(a) \neq 0$.

' $\Longrightarrow$ ' Si a es raíz múltiple, entonces $P = (X - a)^2 Q$ para $Q \in A[X]$ con $Q(a) \neq 0$, entonces

$$P' = 2(X - a)Q + (X - a)^2 Q'$$

Y, así, $P'(a) = 0$.

Proposición 3.12

Sea D un dominio de característica 0, y sean $P \in D[X]$ y $a \in D$. Entonces la multiplicidad de a en P es el menor $m \in \mathbb{N}_0$ tal que $P^{(m)}(a) \neq 0$.

Demostración

Hagamos inducción en la multiplicidad m de a en P.

$\underline{m = 0}$ Es evidente, si la multiplicidad es 0, entonces no es raíz, por lo que $P(a) \neq 0$

$\underline{m \geq 1}$ Entonces a es raíz de P y por tanto $P = (X-a)Q$ para cierto $Q \in D[X]$. Entonces, la multiplicidad de a en Q es $m-1$, y por hipótesis de inducción $Q^{(i)}(a) = 0 \neq Q^{(m-1)}(a),\ \forall i < m-1$.

Calculemos la derivada n-ésima de P, que es $P^{(n)} = nQ^{(n-1)} + (X-a)Q^{(t)}$, por inducción:

$\underline{n = 1}$ $P' = Q + (X-a)Q'$✓

Entonces, obtenemos la hipótesis de inducción, $P^{(n-1)} = (n-1)Q^{(n-2)} + (X-a)Q^{(n-1)}$

$\underline{n \geq 2}$ $P^{(n)} = \left(P^{(n-1)}\right)' = (n-1)Q^{(n-1)} + Q^{(n-1)} + (X-a)Q^{n} = nQ^{(n-1)} + (X-a)Q^{(n)}$✓

Entonces

$$P^{(m-1)} = (m-1)Q^{(m-2)} + (X-a)Q^{(m-1)}$$

Luego

$$P^{(m-1)}(a) = (m-1)Q^{(m-2)}(a) + 0 \cdot Q^{(m-1)}(a) = 0 + 0 = 0$$

y

$$P^{(m)}(a) = mQ^{(m-1)}(a) + (X-a)Q^{(m)}(a) = mQ^{(m-1)}(a) \neq 0$$

Y la multiplicidad es el menor natural m con la derivada m-ésima de P no nula.

D DFU implica D[X] DFU

Lema 3.15

Si $a \in D$ DFU y $f, g, h \in D[X]$ verifican $af = gh \neq 0$, entonces existen $g_1, h_1 \in D[X]$ tales que

$$f = g_1 h_1, \qquad gr(g_1) = gr(g), \qquad gr(h_1) = gr(h)$$

Demostración

Vamos a razonar por inducción en $\varphi(a)$.

Si $\varphi(a) = 0$, podemos tomar $g_1 = a^{-1}g$ y $h_1 = h$.

Si $\varphi(a) > 0$, existen $p, b \in D$ tales que $a = pb$ y p es primo (esto es porque en los DFU los irreducibles son primos).

Entonces $p|af = gh$ en $D[X]$ y, por el Lema 3.14 (si D es DFU, p primo en D sii p primo en $D[X]$), entonces $p|g$ *ó* $p|h$.

Podemos asumir que $p|g$ en $D[X]$, es decir, $\exists \overline{g}/g = \overline{g}p$ y $gr(g) = gr(\overline{g})$.

Tenemos, entonces, que

$$pbf = af = gh = p\overline{g}h$$

Cancelando p, tenemos que $bf = \overline{g}h$, pero ahora $\varphi(b) = \varphi(a) - 1 < \varphi(a)$, y la hipótesis de inducción nos dice que existen $g_1, h_1 \in D[X]$ tales que $f = g_1h_1$, con $gr(g_1) = gr(\overline{g}) = gr(g)$ y $gr(h_1) = gr(h)$. Y ya tenemos el resultado.

Lema 3.16

Si $f \in D[X] \setminus D$ es irreducible en $D[X]$ siendo D DFU, entonces es irreducible (y primo) en $K[X]$.

Demostración

Supongamos que f no es irreducible en $K[X]$.

Por la proposición 3.13 (f irred en $Q[X]$, Q cuerpo si y solo si es primo si y solo si $gr(f) > 0$ y f no es producto de dos polinomios de grado menor), entonces, como no es irreducible, deben existir $G, H \in K[X]$ tales que

$$f = GH, \qquad gr(G) > 0, \qquad gr(H) > 0$$

Si $0 \neq b \in D$ es un múltiplo común de los denoinadores de los coeficientes de G, entonces $g = bG \in D[X]$, y análogamente existe $0 \neq c \in D$ tal que $h = cH \in D[X]$.

Aplicando el lema anterior a la igualdad

$$(bc)f = gh$$

obtenemos $g_1, h_1 \in D[X]$ tales que

$$f = g_1 h_1, \qquad gr(g_1) = gr(g) = gr(G) > 0, \qquad gr(h_1) = gr(h) = gr(H) > 0$$

por lo que f no es irreducible en $D[X]$. Por tanto, el resultado queda demostrado por contrarrecíproco.

Teorema 3.17

D es DFU si y solo si lo es $D[X]$

Demostración

' $\Longleftarrow$ ' El corolario 3.2 nos dice que $D[X]$ dominio sii D dominio y en este caso $D[X]^* = D^*$.

Entonces D es un dominio y cada $0 \neq a \in D \setminus D^*$ es producto de irreducibles de $D[X]$, que tendrán grado 0 pues lo tiene a. Por el lema 3.14 (p irred en D sii p irred en $D[X]$), tenemos que esa misma factorización de $D[X]$ es una factorización en D por irreducibles. Como $D[X]$ es DFU, entonces los irreducibles son primos. Y el mismo lema 3.14 nos dice que los primos de $D[X]$ son los primos de D, por lo que, usando la caracterización de DFU, tenemos que, como D es DF y los irreducibles son primos, entonces D es DFU.

' $\Longrightarrow$ ' Vamos a empezar viendo que cada $a = a_0 + ... + a_n X^n \in D[X]$, no invertible y con $a_n \neq 0$, es producto de irreducibles. Lo haremos por inducción en $n + \varphi(a_n)$.

Obsérvese que a es invertible si, y solo si, $a \in D^*$, si, y solo si, $n + \varphi(a_n) = 0$.

$\underline{n + \varphi(a_n) = 1}$

- $n = 1, \varphi(a_n) = 0$, y en este caso $gr(f) = 1$ y a_1 es invertible. Si no fuera producto de irreducibles, entonces debe poder escribirse como $a = gh$, con $g, h \in D[X] \setminus D[X]^*$ y alguno de ellos no es producto de irreducibles. Uno debe ser de grado 0 y otro de grado 1, supongamos $gr(g) = 1, gr(h) = 0$. Entonces

$$a_0 + a_1 X = (b_0 + b_1 X)c_0 = b_0 c_0 + b_1 c_0 X$$

De donde $a_0 = b_0c_0$ y $a_1 = b_1c_0$. Como $a_1 \in D^* \implies b_1c_0 \in D^* \implies c_0 \in D^* = D[X]^*$. Luego d es invertible. # Esto contradice que a no sea producto de irreducibles.

- $n = 0, \varphi(a_n) = 1$ Entonces estamos en D y como D es DFU, entonces a es producto de irreducibles.

$\underline{n + \varphi(a_n) > 1}$ Supongamos que a no es irreducible. Entonces existen

$$b = b_0 + ... + b_mX^m \ (b_m \neq 0) \quad y \quad c = c_0 + ... + c_kX^k \ (c_k \neq 0)$$

en $D[X] \setminus D[X]^*$, con $a = bc$.

Entonces

$$0 < m + \varphi(b_m),\ 0 < k + \varphi(c_k) \quad y \quad n + \varphi(a_n) = m + k + \varphi(b_m) + \varphi(c_k)$$

En consecuencia, podemos aplicar la hipótesis de inducción a b y c y pegando las factorizaciones obtenemos una factorización de a.

Así, sabemos que $D[X]$ es DF, si demostramos que en $D[X]$ todo irreducible es primo, entonces podremos asegurar, por la caracterización de DFU, que $D[X]$ es DFU.

Vamos a ver que todo f irreducible en $D[X]$ es primo en $D[X]$. El lema 3.14 nos dice que si D es DFU, entonces p irred en D sii p primo en D sii p primo en $D[X]$. Por tanto, podemos suponer que $gr(f) \geq 1$, pues el otro caso ya lo tenemos.

Sean entonces $g, h \in D[X]$ tales que $f|gh$ en $D[X]$ $\underline{¿f|g \text{ ó } f|h?}$

Se tiene que $f|gh$ en $K[X]$ y por el lema 3.16 f es primo en $K[X]$ y entonces $f|g$ ó $f|h$ en $K[X]$. Podemos suponer que divide a g. O sea, $\exists G \in K[X]$ tal que $g = fG$, si demostramos que $G \in D[X]$ habremos acabado.

Para esto, sea $a \in D / aG \in D[X]$ y $\varphi(a)$ mínimo.

<u>Basta ver que $\varphi(a) = 0$.</u> Supongamos que no es así, es decir, $\varphi(a) > 0$ y sean $p, b \in D$ con $a = pb$ con p primo. Entonces, en $D[X]$ se tiene que $p|ag = faG$. Como p es primo en $D[X]$ (Lema 3.14) y $p \nmid f$ (porque f es irreducible y $gr(f) \geq 1$), entonces ha de ser $p|aG$ en $D[X]$.

Si $g_1 \in D[X]$ verifica $aG = pg_1$entonces $bG = g_1 \in D[X]$, y $\varphi(b) < \varphi(a)$ # esto contradice la minimalidad de $\varphi(a)$. Por tanto, ha de ser $\varphi(a) = 0$. Esto implica que $G \in D[X]$ y que $f|g$ en $D[X]$, como queríamos ver. Así, f es primo en $D[X]$.

Por tanto, $D[X]$ es un DF en el que todo irreducible es primo, esto quiere decir (caracterización de DFU) que $D[X]$ es DFU.

Caracterización de los irreducibles del anillo de polinomios de un DFU

Lema 3.14

Sea D un dominio y sea $p \in D$

1. p irreducible en D si y solo si lo es en $D[X]$
2. p primo en $D[X]$ entonces p primo en D

3. Si D es DFU, entonces las siguientes condiciones son equivalentes

   (a) p irred en D
   (b) p irred en $D[X]$
   (c) p primo en D
   (d) p primo en $D[X]$

Demostración

1) ' $\Longleftarrow$ ' Obvio

' $\Longrightarrow$ ' Si no fuese irreducible en $D[X]$, debería ser producto de dos polinomios no invertibles con grado menor. Pero su grado es 0, luego estos polinomios deberían tener grado 0, por lo que p sería no irreducible en $D\#$

2) Si $p|ab$ en D, entonces $p|ab$ en $D[X]$, como es primo aquí, entonces $p|a$ o $p|b$ en $D[X]$, pero, como todos tienen grado 0, esto quiere decir que $p|a$ o $p|b$ en D.

3) (a) $\Longleftrightarrow$ (b) por **1)**

(a) $\Longleftrightarrow$ (c) Cierto, pues D es DFU, por el lema 2.21

(d) $\Longrightarrow$ (b) Cierto, porque primo en un dominio implica irreducible

Demostrando (c) $\Longrightarrow$ (d) lo tenemos.

Sea p primo en D y sean

$$a = a_0 + ... + a_n X^n \qquad b = b_0 + ... + b_m X^m$$

polinomios de $D[X]$ tales que $p \nmid a, p \nmid b$ y veamos que $p \nmid ab$.

Como p no divide a a, existe un menor índice i tal que $p \nmid a_i$ y un menor índice j tal que $p \nmid b_j$.

El coeficiente de grado $i + j$ de ab es

$$c_{i+j} = a_0 b_{i+j} + ... + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + ... + a_{i+j} b_0$$

Entonces p divide a todos los sumandos excepto al $a_i b_j$, porque los de la izquierda tienen un índice en la a menor que i y los de la derecha en la b menor que j. Así, $p \nmid c_{i+j} \implies p \nmid ab$.

Por tanto, p es primo en $D[X]$.

Lema 3.19. Lema de Gauss

Si $f, g \in K[X]$, entonces $c(fg) = c(f)c(g)$. En particular, fg es primitivo si y solo si f y g son primitivos.

Demostración

Tenemos $f = c(f)f_1$ y $g = c(g)g_1$ con f_1, g_1 primitivos.

Por tanto

$$fg = c(f)c(g)f_1g_1$$

Luego, para ver la igualdad basta ver que f_1g_1 es primitivo.

Si no fuera primitivo, entonces $c(f_1g_1)$ tendría un divisor irreducible p en D. Esto implica que $p|f_1g_1$.

Por el lema 3.14, p es primo en $D \overset{D\ DFU}{\Longrightarrow}$ p primo en $D[X]$ y por lo tanto $p|f_1$ o $p|g_1$, entonces $p|c(f_1)$ o $p|c(g_1)\#$ esto contradice que $c(f_1) = c(g_1) = 1$.

Así, $f_1g_1$es primitivo y el resultado queda demostrado.

Proposición 3.20

Para un polinomio primitivo $f \in D[X] \setminus D$, las siguientes condiciones son equivalentes:

1. f irreducible en $D[X]$
2. f irreducible en $K[X]$
3. $f = GH$, con $G, H \in K[X] \implies gr(G) = 0$ *ó* $gr(H) = 0$
4. $f = gh$, con $g, h \in D[X] \implies gr(g) = 0$ *ó* $gr(h) = 0$

Demostración

$1 \implies 2$ Por el lema 3.16

$2 \iff 3$ Por la proposición 3.13, que dice que f irreducible en $K[X]$ sii $gr(f) > 0$ y no puede escribirse como producto de polinomios de grado menor

$3 \implies 4$ Si $g, h \in D[X] \implies g, h \in K[X] \implies gr(g) = 0$ *ó* $gr(h) = 0$

$4 \implies 1$ Como f es primitivo, sus únicos divisores de grado 0 son unidades, por lo que no tiene divisores de grado 0, ni los tiene de grado mayor por la hipótesis 4. Por tanto, f es irreducible en $D[X]$

Corolario 3.21

Si D es un DFU y K es su cuerpo de fracciones, entonces los irreducibles de $D[X]$ son los irreducibles de D y los polinomios primitivos de $D[X] \setminus D$ que son irreducibles en $K[X]$.

Demostración

Por el lema 3.14 sabemos que los irreducibles de D son irreducibles en $D[X]$.

Si tenemos un polinomio $f \in D[X] \setminus D$ que no es primitivo, entonces no es irreducible, pues es divisible por un elemento de D y claramente no son asociados.

Si es primitivo, entonces es irreducible si y solo si lo es en $K[X]$, por el teorema 3.20.