Prop. Si D es un DIP entonces D es un DFU.

Dem:

Como todo DIP es Noetheriano tenemos que todo elemento distinto de cero de D que no es unidad se escribe como un producto de irreducibles. Para la unicidad, supongamos que:

$$a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m \text{ dos descomposiciones}$$

en irreducibles. $\therefore$, a_i y b_j son irreducibles. Como D es un DIP, cada a_i es un elemento primo de D. Por un lema anterior, tomando $u=1$, $n=m$ y $b_i = u_i a_i$ con u_i unidad.

Por lo tanto, D es un DFU.

Cor. Sea D un DFU y $a \in D$ un elemento irreducible. Entonces a es primo.

Dem:

Tenemos que a no es unidad. Sup. que $a \mid xy$ con $x, y \in D$. Entonces existe $b \in D$ tal que $ab = xy$. Podemos suponer que x y y no son cero ni unidades. También podemos suponer que $b \neq 0$. Si b es unidad, ent $a = x(yb^{-1})$ ∇. Por lo tanto b no es una unidad. Como D es un DFU, podemos escribir $b = b_1 \cdots b_n$, $x = x_1 \cdots x_m$ y $y = y_1 \cdots y_\ell$ con b_i, x_j, y_k irreducibles. Así

$$a(b_1 \cdots b_n) = x_1 \cdots x_m y_1 \cdots y_\ell.$$

Por la unicidad $a = x_j u_j$ ó $a = y_k v_k$, con u_j y v_k unidades

$\therefore a \mid x$ ó $a \mid y$.

Ejemplos de DFU's: $\mathbb{Z}$, $K[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

Como en un DFU se tiene un "teorema fundamental de la aritmetica" podemos hablar de conceptos como el siguiente:

Def: Sean $a,b \in D$ con D un dominio. Un maximo comun divisor de a y b en D es un elemento $d \in D$ tal que:

i) $d \mid a$ y $d \mid b$

ii) Siempre que $g \mid a$ y $g \mid b$ se tiene que $g \mid d$.

Notemos que si d_1 y d_2 son m.c.d de a y de b ent, $d_1 \mid a$ y $d_1 \mid b$ así que $d_1 \mid d_2$. De la misma forma $d_2 \mid d_1$. Por lo tanto $d_1 = u d_2$ con u unidad.

Prop. Sea D un DFU y $a,b \in D$. Entonces $\text{mcd}(a,b)$ en D existe.

Dem:

Como D es DFU, $a = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ $b = p_1^{\beta_1} \cdots p_m^{\beta_m}$ donde cada p_i es irreducible y $\alpha_i, \beta_i \geq 0$. Consideremos $d = p_1^{\gamma_1} \cdots p_m^{\gamma_m}$ con $\gamma_i = \min\{\alpha_i, \beta_i\}$. Es claro que $d \mid a$ y $d \mid b$. Sea g tal que $g \mid a$ y $g \mid b$. Escribimos $g = p_1^{\delta_1} \cdots p_m^{\delta_m}$. Así $\delta_i \leq \alpha_i$ y $\delta_i \leq \beta_i$. Por lo tanto $\delta_i \leq \min\{\alpha_i, \beta_i\} = \gamma_i$ así que $g \mid d$.

Cuando D es un DIP tenemos una mejor descripción del mcd.

Prop. Sea D un DIP y $a, b \in D$. Entonces $\mathrm{mcd}(a,b)$ es el elemento de D tal que

$$D\,\mathrm{mcd}(a,b) = \{ar + bs \mid r, s \in D\} = Da + Db.$$

Dem:

Escribamos $Dd = Da + Db$. Entonces $Da \subseteq Dd$ y $Db \subseteq Dd$. Por lo tanto, $d|a$ y $d|b$. Sup. que $g \in D$ es tal que $g|a$ y $g|b$. Esto implica que $Da \subseteq Dg$ y $Db \subseteq Dg$. Así que $Da + Db \subseteq Dg$

ie. $Dd \subseteq Dg$ $\therefore g|d$. $\therefore d = mcd(a,b)$.

Def. Sea D un DFU. Dos elementos $a, b \in D$ son primos relativos (coprimos) si $mcd(a,b) = 1$.

Anillos de polinomios

Sea R un anillo. Consideremos el conjunto de polinomios con coeficientes en R, $R[x]$, es decir, expresiones de la forma $f(x)=a_0+a_1x+\cdots+a_nx^n$ con $n\geq 0$ y $a_i\in R$. Es rutina probar que $R[x]$ es un anillo conmutativo con unidad con las operaciones que conocemos de polinomios.

Si D es un dominio euclidiano, $D[x]$ no tiene porqué ser un anillo euclidiano El ejemplo es $\mathbb{Z}[x]$ (lo discutiremos más adelante).

Prop. Si D es un dominio entero, entonces $D[x]$ también.

Dem:

Sean $f(x)=a_0+a_1x+\cdots+a_mx^m$ y $g(x)=b_0+b_1x+\cdots+b_nx^n$ dos polinomios no cero en $D[x]$. Sup. $a_m\neq 0$ y $b_n\neq 0$. Entonces:

$$f(x)g(x)=c_0+c_1x+\cdots+c_rx^r \quad \text{donde:}$$

$$c_k = \sum_{i+j=k} a_i b_j \qquad 0 \leq k \leq r$$

Si $k > m+n$, entonces $i > m$ ó $j > n$ ya que $i+j > m+n$. Así que $a_i = 0$ ó $b_j = 0$. Por lo tanto $c_k = 0$.

Si $k = m+n$, entonces $\underline{c_k = a_m b_n}$ ya que $i+j = m+n$. Si $i < m$ entonces $j > n$ y así $b_j = 0$. De la misma forma si $j < n$, ent $i > m$ y por lo tanto $a_i = 0$. Como D es un dominio entero y $a_m \neq 0$ y $b_n \neq 0$, se tiene que $c_{m+n} = a_m b_n \neq 0$

$\therefore f(x)g(x) \neq 0$.

El anillo $\mathbb{Z}[x]$, también es un ejemplo de que si D es DIP, $D[x]$ no necesariamente lo es. Entonces, la siguiente pregunta sería:

¿Si D es un DFU, se tiene que $D[x]$ es DFU? Sí

Def: Sea D un DFU. Un polinomio $f(x)=a_0+a_1x+\cdots+a_nx^n$ en $D[x]$ se llama primitivo si $\text{mcd}(a_0,a_1,\ldots,a_n)=1$ (o una unidad).

Def: Sea D un DFU. El contenido de un polinomio $g(x)=b_0+b_1x+\cdots+b_mx^m$ en $D[x]$ se define como $c(g):=\text{mcd}(b_0,b_1,\ldots,b_m)$.

Entonces un polinomio $f(x)$ es primitivo $\Leftrightarrow c(f)=1$

Notemos que si $g(x)\in D[x]$, entonces $g(x)$ se puede escribir como $g(x)=c(g)f(x)$ con $f(x)$ primitivo.

Lema (Gauss). Si D es un DFU y $f(x), g(x)$ en $D[x]$ son primitivos, entonces $f(x)g(x)$ también es primitivo.

Dem:

Escribamos $f(x)=a_0+a_1x+\cdots+a_mx^m$, $g(x)=b_0+b_1x+\cdots+b_nx^n$ y $f(x)g(x)=c_0+c_1x+\cdots+c_rx^r$. Supongamos que $f(x)g(x)$ no es primitio, es decir, $\mcd(c_0,c_1,\ldots,c_r)$ no es una unidad. Como D es un DFU, existe un irreducible $\pi\in D$ tal que $\pi \mid c_k$ $\forall 1\leq k\leq r$. Como $f(x)$ es primitivo, π no divide a todos los a_i. Sea s el menor indice tal que π no divide a a_s. De la misma forma sea t el menor indice tal que π no divide a b_t. Consideremos $c_{s+t}=\sum_{i+j=s+t} a_ib_j$

$$= \left(\underline{a_0} b_{s+t} + \underline{a_1} b_{(s-1)+t} + \cdots + \underline{a_{s-1}} b_{1+t}\right) + a_s b_t$$

$$+ \left(a_{s+1} \underline{b_{t-1}} + \cdots + a_{s+t} \underline{b_0}\right)$$

Sabemos que $\pi \mid C_{s+t}$. Por la forma en que se escogieron s y t, π a lo que está entre parentesis. Por lo tanto, π tiene que dividir a $a_s b_t$. Como π es primo

$\pi \mid a_s$ ó $\pi \mid b_t$ ∇ $\therefore$ $c(f_g) = 1$.