Cor. Si D es un DFU y $f(x), g(x) \in D[x]$, entonces $c(fg)=c(f)c(g)$. Se sigue que todo factor de un polinomio primitivo en $D[x]$ también es primitivo.

Dem:
$f(x)=c(f)f'(x)$, $g(x)=c(g)g'(x)$ donde $f'(x)$, $g'(x)$ son primitivos. Así $c(fg)h'(x)=f(x)g(x)=c(f)c(g)f'(x)g'(x)$ por el lema anterior $f'(x)g'(x)$ es primitivo. Esto implica que $c(fg)=c(f)c(g)$.

Cor. [Lema de Gauss] Sea D un DFU con campo de fracciones K. Si un polinomio $f(x)$ en $D[x]$ es irreducible, entonces considerado como polinomio en $K[x]$ también es irreducible.

Dem:

Supongamos que $f(x) \in D[x]$ es primitivo. Si $f(x)=p(x)q(x)$ con $p(x), q(x) \in K[x]$.

Escribimos:

$p(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_m}{b_m}x^m$, $q(x) = \frac{a'_0}{b'_0} + \frac{a'_1}{b'_1}x + \cdots + \frac{a'_n}{b'_n}x^n$ con $\frac{a_i}{b_i}, \frac{a'_j}{b'_j} \in K$

Si $b = b_0 b_1 \cdots b_m$ y $b' = b'_0 b'_1 \cdots b'_n$, entonces $p(x) = \left(\frac{1}{b}\right) b p(x)$ y $q(x) = \left(\frac{1}{b'}\right) b' q(x)$ con $bp(x), b'q(x) \in D[x]$. Sean d y d' los contenidos de $bp(x)$ y $b'q(x)$ respectivamente. Así $bp(x) = d u(x)$ y $b'q(x) = d' v(x)$ con $u(x), v(x) \in D[x]$ primitivos. Por lo tanto:

$$f(x) = p(x)q(x) = \frac{1}{bb'}\left(bp(x)\right)\left(b'q(x)\right) = \frac{dd'}{bb'} u(x)v(x) = \frac{s}{t} u(x)v(x)$$

Entonces $tf(x) = s u(x)v(x)$. Por el lema anterior $c(tf(x)) = t$ y $c(su(x)v(x)) = s$ $\therefore$ $s = t$

Por lo tanto $f(x) = u(x)v(x) \in D[x]$.

Si $f(x)\in D[x]$ no es primitivo, escribimos $f(x)=dg(x)$ con $g(x)\in D[x]$ primitivo. Si $f(x)=p(x)q(x)$ con $p(x),q(x)\in K[x]$, entonces $dg(x)=f(x)=p(x)q(x)$. Se sigue que $g(x)=\left(\frac{1}{d}p(x)\right)q(x)\in K[x]$ con $g(x)\in D[x]$ primitivo. Por el paso anterior $g(x)=u(x)v(x)$ en $D[x]$. Por lo tanto $f(x)=dg(x)=\left(du(x)\right)v(x)\in D[x]$.

Teorema. Si D es un DFU, entonces $D[x]$ también lo es.

Dem:

Dado un polinomio $f(x)\in D[x]$, tenemos la factorización $f(x)=c(f)g(x)$ con $g(x)$ un polinomio primitivo. Si $f(x)$ es irreducible, $c(f)$ es unidad ó $g(x)$ es unidad. Si $c(f)$ es unidad, $f(x)$ es primitivo. Si $g(x)$ es unidad, entonces $g(x)$ es constante y por lo

$$1=g(x)h(x)\Rightarrow 0=gr(g)+gr(h)\Rightarrow gr(g)=0$$

tanto $f(x)$ también. Esto nos dice que los polinomios irreducibles son constantes o polinomios primitivos.

Obs1: Un polinomio constante c es irreducible si y solo si c es irreducible en D.

$\Rightarrow$) Si $c = ab \in D$, ent $c = ab \in D \hookrightarrow D[x]$

$\Leftarrow$) Sup. $c = p(x)q(x) \in D[x]$. Ent $0 = gr(c) = gr(p) + gr(q)$ lo que implica que $gr(p) = 0 = gr(q)$ i.e, $p(x) = p$ $q(x) = q$ son constantes. Por lo tanto $c = pq \in D$.

Obs2: Un polinomio primitivo es irreducible si y solo si no tiene un factor primitivo no constante de grado menor.

$\Rightarrow$) Sea $f(x)$ primitivo irreducible y sup. $g(x)$ no es constante y $g(x) \mid f(x)$, i.e, $g(x)h(x) = f(x)$. Como $f(x)$ es irreducible y $g(x)$ no es constante, se tiene que $h(x)$ es una unidad. Por lo tanto

$g(f) = gr(g) + gr(h) = gr(g) + 0 = gr(g)$

$\Leftarrow$) Si $f(x) = g(x)h(x)$, $gr(f) = gr(g) + gr(h)$. Si h no es unidad, $gr(h) \geq 1$. Si $g(x)$ no es unidad $gr(g(x)) \geq 1$

Entonces $gr(g) < gr(f)$!

Tenemos $f(x) = c(f)g(x)$. Si $g(x)$ no es irreducible, $g(x) = h_1(x)h_2(x)$ con $gr(h_1) < gr(g)$ y $gr(h_2) < gr(g)$. Como $g(x)$ es primitivo, h_1 y h_2 también lo son. Si $h_1(x)$ no es irreducible $h_1(x) = h_{11}(x)h_{12}(x)$ con $gr(h_{11}), g(h_{12}) < gr(h_1) < gr(g)$. Si $h_2(x)$ no es irreducible $h_2(x) = h_{21}(x)h_{22}(x)$ con $gr(h_{21}), gr(h_{22}) < gr(h_2) < gr(g)$. Siguiendo de esta manera tenemos que terminar.

Supongamos ahora que se tienen dos factorizaciones en irreducibles de $f(x)$, ie,

$$f(x) = c_1 \cdots c_m f_1(x) \cdots f_r(x) = d_1 \cdots d_n g_1(x) \cdots g_s(x) \text{ con } c_i, d_j \in D \text{ y } f_i, g_j \text{ primitivos.}$$

Como los f_i y g_j son primitivos, se tiene
$c_1 \cdots c_m = c(f) = d_1 \cdots d_n \in D$ Como D es un DFU
$m=n$ y $c_i = d_i u_i$ con u_i unidad. Así
$d_1 u_1 \cdots d_n u_n f_1(x) \cdots f_r(x) = \underline{d_1 \cdots d_n} g_1(x) \cdots g_s(x)$

Cancelando

$$u f_1(x) \cdots f_r(x) = g_1(x) \cdots g_s(x) \in D[x] \hookrightarrow K[x]$$

Por el lema de Gauss cada f_i, g_j es irreducible en $K[x]$ donde K es el campo de fracciones de D. Como $K[x]$ es un DFU, $r=s$ y

$$f_i(x) = \frac{v_i}{w_i} g_i(x) \quad \text{con } \frac{v_i}{w_i} \in K \quad \text{unidad. Así}$$

$$w_i f_i(x) = v_i g_i(x)$$

como f_i y g_i son primitivos, $c(w_i f_i) = w_i$ y $c(v_i g_i) = v_i$. Por lo tanto $v_i = w_i$ lo que implica que $\frac{v_i}{w_i}$ es unidad en D

$\therefore D[x]$ es un DFU.

El anillo $\mathbb{Z}[x]$ es un DFU, por el Teorema anterior. Sup. que $\mathbb{Z}[x]$ es un DIP. y consideremos el ideal generado por 2 y x i.e.,

$$\langle 2, x \rangle = \{ 2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x] \}.$$

Como $\mathbb{Z}[x]$ es un DIP, $\langle 2, x\rangle = \langle h(x)\rangle$.

En particular $2 = h(x) f(x) \Rightarrow gr(h(x)) = 0$

$$x = h(x)\, g(x)$$

ent $h(x)$ es constante, $h(x) = h \in \mathbb{Z}$. y

$h \mid 2$. Como h no es unidad, $h = 2$

$$x = 2g(x) \ !$$ ∇ Por lo tanto $\mathbb{Z}[x]$

no es un DIP, en particular tampoco es un dominio euclidiano.