Def Una función euclidiana (o grado) es una aplicación $\delta : A \setminus \{0\} \to \mathbb{N}$

t.q.

1) $\delta(ab) \geq \delta(a)$

2) Si $a, b \in A$, $b \neq 0$

$\exists\, q, r \in A$ t.q.

$$a = bq + r$$

y o $R = 0$ o $\delta(r) < \delta(b)$

Un anillo A es un dominio euclídeo si admite una función euclídea.

Ej:

- $\mathbb{Z}$, $\delta = |\cdot|$
- $F[x]$, F cuerpo
- $\delta = \deg$

Ej: Mostramos que si $f(x), g(x) \in F(x)$ con $g(x) \neq 0$, $\exists\, q(x), r(x) \in F(x)$

t.q. $f(x) = g(x) \cdot q(x) + r(x)$

y $r(x) = 0$ ó $\deg r(x) \leq \deg g(x)$

Por inducción sobre $\deg f$:

P.B) Si $\deg f = 0$ y $\deg g \neq 0$

luego $f = \cancel{0 \cdot g}^{0} + f$

Si $\deg g = 0$

$$f = \frac{f}{g} \cdot g + 0$$

P.I)

- Si $\deg f < \deg g$

$q(x) = 0 \quad R(x) = f(x)$

$f = 0 \cdot g + f$

- Si $\deg f \geq \deg g$

Llamamos $f(x) = a_n x^n + \dots + a_1 x + a_0$

$g(x) = b_m x^m + \dots + b_1 x + b_0$

Definimos $f_1(x) = f(x) - (a_n b_m^{-1}) \cdot x^{n-m} \cdot g(x)$

Siendo $\deg f_1 < \deg f$ por inducción existen ... (falta)

// 153

Ej: $3x^2 + \quad + x + 2 \;\big|\; 4x+1$

$3x^2 + 2x^2$ $\qquad\qquad 2x^2+2x+1$

$// \quad -2x^2 + x + 2$

$-2x^2 - x$

$3x^2 + 2x$

$-x + 2$

$4x + 1$

$// \quad 1$

módulo $S = 0$ ←

$$3x^2 + x + 2 = (2x^2+2x+1)(4x+1) + 1$$

$$= 8x^3 + 2x^2 + 3x^2 + 2x + 4x + 1 + 1$$

$$= 3x^2 + x + 2.$$

Ej: $\gcd(373, 75)$

$373 = 4 \cdot 75 + 73$

$75 = 1 \cdot 73 + 2$

$73 = 36 \cdot 2 + 1$

$2 = 2 \cdot (1) + 0$

$$\gcd(a, b) = \gcd(b, R)$$

Si $a = bq + R$

$$\{\text{Divisores comunes } a \text{ y } b\} = \{\text{divisores comunes } b \text{ y } R\}$$

$(\subseteq:)$ Si $d \mid a$ y $d \mid b$
$\Rightarrow d \mid (a - bq) = R$

$(\supseteq:)$ Si $d \mid b$ y $d \mid r$
luego $d \mid (bq + r) = a$

Hay un algoritmo euclídeo extendido.

Lema Sea A un ED si $a \mid b$ y $d(a) = d(b)$ entonces a y b son asociados.

(degree)

Dem: Decimos que $b \mid a$ y $d(a) = d(b)$ escribimos:

$$a = bq + R$$

① Si $R \neq 0$, por def. nos queda: $d(R) \geq d(b)$:

Siendo $a \mid a$ y $a \mid b$

$$a \mid (a - bq) = R$$

$\exists t \in A$:

$$at = R$$

$$d(R) = d(a+b) \geq d(a) = d(b) > d(R)$$

$$d(R) > d(R) \quad (\Rightarrow\Leftarrow).$$

Contradicción que surge de asumir $R \neq 0$, luego $R = 0$ y $b \mid a$ siendo A dominio de integridad y $a \mid b$ y $b \mid a$.

Teorema $ED \Rightarrow PID$.

(Probar leerla/hacerla)