Algebra Superior 2

11·05·20

Teo. Sean $p(x), q(x) \in \mathbb{R}[x]$. Entonces:

1. Si $p(x) \mid q(x)$ entonces $\alpha p(x) \mid q(x)$ $\forall \alpha \in \mathbb{R}, \alpha \neq 0$.
2. Si $p(x) \mid q(x)$ entonces $p(x) \mid s(x) q(x)$ para cualquier polinomio $s(x) \in \mathbb{R}[x]$.
3. Si $\alpha \in \mathbb{R}$, $\alpha \neq 0$, entonces α divide a cualquier polinomio en $\mathbb{R}[x]$.
4. Si $p(x) \mid q(x)$ y $q(x) \neq 0$, entonces $\text{Grad}(p(x)) \leq \text{Grad}(q(x))$.
5. Si $p(x) \mid q(x)$ y $\text{Grad}(p(x)) = \text{Grad}(q(x))$ entonces existe $\alpha \in \mathbb{R}$ tal que $\alpha p(x) = q(x)$.
6. Si $s(x) \mid p(x)$ y $s(x) \mid q(x)$ entonces $s(x) \mid (t(x) p(x) + u(x) q(x))$ para cualesquiera polinomios $t(x), u(x) \in \mathbb{R}[x]$.

Dem. 1 y 2: como $p(x) \mid q(x)$ se tiene que $q(x) = p(x) \cdot r(x)$ para algún $r(x) \in \mathbb{R}[x]$. Entonces $q(x) = (\alpha \cdot p(x)) \cdot (\alpha^{-1} r(x))$ y $s(x) \cdot q(x) = p(x) \cdot r(x) \cdot s(x)$ que es lo que se quería.

Ejercicio: Demueste los incisos 3-6 tomando como base los resultados análogos para $\mathbb{Z}$.

Def. Sean $a(x), b(x) \in \mathbb{R}[x]$ no ambas cero. Entonces $d(x) \in \mathbb{R}[x]$ es el máximo común divisor de $(a(x))$ y $b(x)$ si:

1. $d(x) \mid a(x)$ y $d(x) \mid b(x)$
2. si $c(x) \in \mathbb{R}[x]$ es tal que $c(x) \mid a(x)$ y $c(x) \mid b(x)$ entonces $c(x) \mid d(x)$.

Nota: El máximo común divisor de 2 polinomios no es único y esto contrasta con lo que pasa en $\mathbb{Z}$.

Def. Un polinomio distinto de cero es llamado mónico si su coeficiente principal es 1.

Teo. Sean $(a(x)), b(x) \in \mathbb{R}[x]$ no ambos cero. Entonces existe un único polinomio mónico $d(x) \in \mathbb{R}[x]$ que es un máximo común divisor de $(a(x))$ y $(b(x))$. Además se tiene que

$$d(x) = g(x)\,a(x) + h(x)\,b(x)$$

para algunos $g(x), h(x) \in \mathbb{R}[x]$.

Dem. Supongamos que $a(x) = 0$, entonces $b(x) \neq 0$ y es fácil ver que el polinomio mónico buscado existe y puede ser expresado en la forma deseada. Lo mismo ocurre si $a(x) \neq 0$ y $b(x) = 0$.
Por tanto, supongamos que $a(x) \neq 0$ y $b(x) \neq 0$: probaremos el resultado por inducción.

Consideremos el número $\min\{\text{Grad}(a(x)), \text{Grad}(b(x))\}$.

Si $\min\{\text{Grad}(a(x)), \text{Grad}(b(x))\} = 0$ entonces o $a(x)$ o $b(x)$ es una constante distinta de cero y los únicos divisores comunes de $(a(x))$ y $(b(x))$ son las constantes no cero.
Por tanto 1 es un máxmo común divisor mónico y si $a(x) = a \in \mathbb{R}$ entonces $1 = a^{-1} \cdot a + 0 \cdot b(x)$.
Si $b(x) = b \in \mathbb{R}$ entonces $1 = 0 \cdot a(x) + b^{-1} \cdot b$.

Continuando por inducción, supongamos que $s(x)$ y $t(x)$ son polinomios tales que
$\min\{\text{Grad}(s(x)), \text{Grad}(t(x))\} < n$,

entonces $s(x)$ y $t(x)$ tienen un máximo común divisor mónico, $d(x)$ que puede ser expresado de la forma

$$d(x) = e(x)s(x) + f(x)t(x) \quad \text{para}$$

$e(x), f(x) \in \mathbb{R}[x]$.

Supongamos que $n = \text{Grad}(b(x)) \leq \text{Grad}(a(x))$.

(La prueba en el caso $n = \text{Grad}(a(x)) \leq \text{Grad}(b(x))$ es análoga).

Por el algoritmo de la división

$$a(x) = g(x) \cdot b(x) + r(x) \qquad \text{con } r(x) = 0 \text{ o } r(x) \neq 0 \text{ y } \text{Grad}(r(x)) < \text{Grad}(b(x))$$

Si $r(x) = 0$, entonces $b(x) \mid a(x)$ y se puede tomar el polinomio siguiente:

si $b(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$

entonces consideremos $\beta(x) = x^n + \frac{b_{n-1}}{b_n} x^{n-1} + \cdots + \frac{b_1}{b_n} + \frac{b_0}{b_n}$.

$\beta(x)$ es un máximo común divisor de $a(x)$ y $b(x)$ y $\beta(x)$ tiene la forma $g(x)a(x) + h(x)b(x)$ donde $g(x) = 0$ y $h(x)$ es una constante no cero ✓

Si $r(x) \neq 0$, entonces

$$\min\{\text{Grad}(r(x)), \text{Grad}(b(x))\} = \text{Grad}(r(x)) < \text{Grad}(b(x))$$

$$= \min\{\text{Grad}(a(x)), \text{Grad}(b(x))\} = n.$$

Entonces, por la hipótesis de inducción, $r(x)$ y $b(x)$ tienen un máximo común divisor mónico, $d(x)$, que se puede escribir de la forma

$$d(x) = e(x)r(x) + f(x)\,b(x).$$

Como $d(x) \mid b(x)$ y $d(x) \mid r(x)$ se sigue que

$$d(x) \mid \left(q(x)b(x) + r(x) \right).$$

Es decir, $d(x) \mid a(x)$.

Supongamos que $c(x) \in \mathbb{R}[x]$ es tal que $c(x) \mid a(x)$ y $c(x) \mid b(x)$. Entonces $c(x)$ divide a $a(x) - q(x)b(x) = r(x)$. Por tanto, como $d(x)$ es un máximo común divisor de $b(x)$ y $r(x)$, se tiene que $c(x) \mid d(x)$ por definición.

Así $d(x)$ es un máximo común divisor de $(a(x))$ y $(b(x))$. Además

$$\begin{aligned} d(x) &= e(x)r(x) + f(x)b(x) = e(x)\left(a(x) - q(x)b(x)\right) + f(x)b(x) \\ &= g(x)a(x) + h(x)\,b(x) \end{aligned}$$

donde $g(x) = e(x)$ y $h(x) = f(x) - e(x)q(x)$.

Ahora solo resta probar que $d(x)$ es el único máximo común divisor mónico de $(a(x))$ y $(b(x))$. Supongamos que existe $d_1(x)$ que satisface lo mismo: se tiene entonces, por la definición, que $d(x) \mid d_1(x)$ y también $d_1(x) \mid d(x)$.

Y entonces exuste $k \in \mathbb{R}$ tal que $d_1 = k\,d(x)$ con $k \neq 0$. Como $d_1(x)$ y $d(x)$ ambos tienen coeficiente principal igual a 1 se sigue que $k = 1$ y $\therefore \quad d_1(x) = d(x)$.

Esto es lo que se quería demostrar. ∎