Demostraciones Pendientes de la Unidad 5

En este documento se presentarán las demostraciones de dos resultados de la Unidad de Polinomios, el Algoritmo de la División de Polinomios, y el Teorema de Gauss sobre raíces de Polinomios a coeficientes enteros.

Para la primera, será necesario comenzar introduciendo una propiedad algebráica de las operaciones sobre un conjunto, de la que gozan muchos de los conjuntos conocidos, en los cuales pueden definirse operaciones de sumas y multiplicación (como en cada caso particular pueda esto ser hecho), la no existencia de divisores de 0.

Ésta afirma que $\mathbb{C}$ (y todos los conjuntos numéricos usuales, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$), no tiene divisores de 0, dicho en dos formas equivalentes, para cualesquiera $x, y \in \mathbb{C}$,

$$(x, y \neq 0 \;\Rightarrow\; x \cdot y \neq 0) \quad \text{o} \quad (x \cdot y = 0 \;\Rightarrow\; x = 0 \text{ o } y = 0) \,.$$

En efecto, para mostrarlo a través de la segunda forma de presentar la definición, tomando $xy = 0$, si $y = 0$, y vale $x = 0$ o $y = 0$, y si $y \neq 0$, entonces

$$xy = 0 \;\Rightarrow\; xy \cdot y^{-1} = 0 \cdot y^{-1} \;\Rightarrow\; x = x \cdot 1 = x(y \cdot y^{-1}) = 0 \,.$$

y también vale y vale $x = 0$ o $y = 0$. La misma prueba sirve para verificar que en $\mathbb{R}$ tampoco existen divisores de 0.

Ahora bien, estas ideas no servirán para mostrar que en $\mathbb{C}[x]$ o $\mathbb{R}[x]$ no hay divisores de 0, porque hemos visto que no todo polinomio no nulo admite un inverso multiplicativo (de paso, tampoco sirve esa demostración para demostrar que $\mathbb{N}$ o $\mathbb{Z}$ tiene la propiedad), pero en concreto para el caso de interés, para mostrar que

$$p(x), q(x) \in \mathbb{C}[x] \;\; (\text{o}\mathbb{R}[x]) \,, \quad \text{entonces} \;\; p \cdot q = \bar{0} \;\; \Rightarrow \;\; p = \bar{0} \;\; \text{o} \;\; q = \bar{0} \,,$$

puede hacerse por contradicción. En efecto, si p y q son tales que $p \cdot q = \bar{0}$ y son dos polinomios no nulos, entonces ambos tienen grado, n y m respectivamente, y serán de la forma

$$p(x) = a_n x^n + \cdots \quad \text{y} \quad q(x) = b_m x^m + \cdots \,,$$

con $a_n \neq 0$ y $b_m \neq 0$, pero con esas formas de p y q, será

$$(p \cdot q)(x) = a_n \cdot b_m \cdot x^{m+n} + \cdots$$

el cual, para coincidir con el polinomio nulo, deberá ser tal que en particular resulte $a_n \cdot b_m = 0$, pero esto ocurrirá, como $\mathbb{C}$ no tiene divisores de 0, si $a_n = 0$ o $b_m = 0$, lo cual contradice la conclusión previa $a_n \neq 0$ y $b_m \neq 0$.

Teorema 1. *Dados $p(x), q(x) \in \mathbb{C}[x]$, donde $q \neq \bar{0}$, existen únicos $c, r \in \mathbb{C}[x]$, tales que*

$$p(x) = c(x) \cdot q(x) + r(x) \quad \textit{siendo} \quad r(x) = \bar{0} \;\; \textit{o} \;\; 0 \leq gr(r) < gr(q) \,.$$

Demostración. Primero se mostrará la existencia de tales polinomios c y r, considerando para ello el conjunto de polinomios, formado cuya definición depende de los polinomios p y q dados,

$$P = \{p - q \cdot h \;\; , \;\; h \in \mathbb{C}[x]\} \subseteq \mathbb{C}[x] \;\; ,$$

para el cual existe dos posibilidades:

1. o bien $\overline{0} \in P$,
2. o bien $\overline{0} \notin P$.

En el primer caso, 1), se tiene que existe un polinomio $\tilde{h} \in \mathbb{C}[x]$ tal que

$$p - q \cdot \hat{h} \;=\; \bar{0}\,, \quad \text{con lo que} \quad p \;=\; q \cdot \tilde{h}\,,$$

y considerando $c = \tilde{h}$ y $r = \bar{0}$, queda probada la existencia de cociente y resto.

En el segundo caso, 2), para todo $h \in \mathbb{C}[x]$ se tiene $p - q \cdot h \neq \bar{0}$, y como consecuencia, todo polinomio de P tiene grado. Luego, habrá un nṁero t que será el menor de todos los grados de los polinomios de P, y un polinomio h_0 tal que $p - q \cdot h_0$ es de grado t, es decir, tal que para cada $h \in \mathbb{C}[x]$

$$gr(\; \underbrace{p - q \cdot h_0}_{\tilde{r}} \;) \;\leq\; gr(p - q \cdot h)\,.$$

Notando $\tilde{r}$ al polinomio $p - q \cdot h_0$, resulta $p = q \cdot h_0 + \tilde{r}$, con $\tilde{r} \neq \bar{0}$ y $gr(\tilde{r}) = t$. Queda probar $gr(\tilde{r}) < gr(q)$ para que quede demostrada la existencia en el caso que se está analizando. Esto será hecho por contradicción, notando

$$q(x) = \sum_{i=0}^{m} q_i \cdot x^i, \quad \tilde{r}(x) = \sum_{i=0}^{t} r_i \cdot x^i, \qquad t = gr(\tilde{r}), \quad m = gr(q)$$

y suponiendo que $t \geq m$. Si éste fuera el caso, construyendo el polinomio

$$r_0(x) = \tilde{r}(x) - \frac{r_t}{q_m} \cdot x^{t-m} \cdot q(x)\,,$$

resultará $gr(r_0) \leq t$ y

$$r_0(x) \;=\; p(x) - q(x) \cdot h_0(x) - \frac{r_t}{q_m} \cdot x^{t-m} \cdot q(x) \;=\; p(x) - q(x) \cdot \underbrace{\left(h_0(x) + \frac{r_t}{q_m} \cdot x^{t-m} \right)}_{\in \mathbb{C}[x]}\,,$$

siendo $r_0 \in P$, $gr(r_0) \leq t$ y el término de r_0 que corresponde a x^t igual a

$$r_t x^t - \frac{r_t}{q_m} \cdot x^{t-m} \cdot q_m x^m \;=\; r_t x^t - r_t x^t = 0 x^t$$

se tendría que $gr(r_0) < gr(\tilde{r})$, lo cual genera la constración anticipada. Dado que todo se basó en la suposición de que $gr(\tilde{r}) \geq gr(q)$ resulta que $gr(\tilde{r}) < gr(q)$.

Respecto de la unicidad, si se suponen polinomios c_1, r_1 y c_2, r_2 tales que

$$p \;=\; q \cdot c_1 + r_1\,, \quad r_1 \;=\; \bar{0} \quad \text{o} \quad gr(r_1) < gr(q)$$

$$p \;=\; q \cdot c_1 + r_1\,, \quad r_1 \;=\; \bar{0} \quad \text{o} \quad gr(r_1) < gr(q)$$

al restar miembro a miembro, quedará $\bar{0} = q \cdot (c_1 - c_2) + r_1 - r_2$ y por lo tanto $q \cdot (c_1 - c_2) = (r_2 - r_1)$.
Si fuera $r_2 - r_1 \neq \bar{0}$ entonces por un lado, debería ser $gr(r_2 - r_1) = \text{máx}\{gr(r_1), gr(r_2)\} < gr(q)$, y por el otro,

$$\bar{0} \;\neq\; r_2 - r_1 \;=\; q \cdot (c_1 - c_2) \;\;\Rightarrow\;\; gr(r_2 - r_1) gr[q \cdot (c_1 - c_2)] \;=\; gr(q) + gr(c_1 - c_2) \geq gr(q)\,,$$

que genera contradicción con lo anterior, permintiendo afirmar $r_2 - r_1 = \bar{0}$ y se deduce, y luego, al ser q no nulo, que $c_1 = c_2$.

Q.E.D.

Teorema 2 (Regla de Ruffini)**.** *Si $p(x) = a_n x^n + a_{n-1}x^n - 1 + ... + a_1 x + a_0$ y $q(x) = x - \alpha$, con $\alpha \in \mathbb{C}$, entonces $p(x) = c(x) \cdot q(x) + r$, con $c(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-1} + ... + b_1 x + b_0$, siendo*

$$r = a_0 + \alpha \cdot b_0 \quad y \quad b_i = a_{i+1} + \alpha b_{i+1} \ , \ \ i = 0, ..., n-2$$

Demostración. Siendo $gr(q) = 1$ resulta por el resultado anterior, que $gr(c) = n-1$ y $gr(r) = 0$, de donde r es un polinomio constante (o el polinomio nulo). Resta verificar que r y los b_i son los del enunciado.
Esto sale de observar que

$$\begin{aligned} p(x) &= c(x) \cdot (x-\alpha) + r = (b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1}x^{n-1}) \cdot (x-\alpha) + r \\ &= (b_0 x + b_1 x^2 + \cdots + b_{n-1}x^n) - (b_0\alpha + b_1 \alpha x + b_2 \alpha x^2 + \cdots + b_{n-1}\alpha x^{n+1}) + r \\ &= (r - b_0\alpha) + (b_0 - b_1\alpha)x + \cdots + (b_{n-2} - b_{n-1}\alpha)x^{n-1} + b_{n-1}x^n \ , \end{aligned}$$

y siendo que $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} + a_n x^n$, comparando coeficientes,

$$\left\{ \begin{array}{lcl} a_n &=& b_{n-1} \\ a_{n-1} &=& b_{n-2} - b_{n-1}\alpha \\ & \vdots & \\ a_1 &=& b_0 - b_1\alpha \\ a_0 &=& r - b_0\alpha \end{array} \right. \quad \text{de donde} \quad \left\{ \begin{array}{lcl} b_{n-1} &=& a_n \\ b_{n-2} &=& a_{n-1} + \alpha b_{n-1} \\ & \vdots & \\ b_0 &=& a_1 - \alpha b_1 \\ r &=& a_0 - \alpha b_0 \end{array} \right.$$

Q.E.D.

Teorema 3. ***Teorema de Gauss***

Sea $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ un polinomio a coeficientes enteros, con $a_0 \neq 0$. Si $\alpha = \dfrac{r}{s}$ es una raíz racional de p, con r y s primos relativos, entonces r divide a a_0 y s divide a a_n.

Demostración. Si $a_0 = 0$, basta sacar factor común x^m, para m el menor grado de los tÃ©rminos de p, y obtenemos $p(x) = x^m C(x)$, con c un polinomio a coeficientes enteros con término independiente no nulo.

Como $\alpha = \dfrac{r}{s}$ es una raÃz de p, debe ser $p(\alpha) = 0$, de manera que

$$a_n \frac{r^n}{s^n} + \cdots a_1 \frac{r}{s} + a_0 = 0 \ .$$

En este caso, multiplicando ambos miembros por s^n, se obtiene

$$a_n r^n + a_{n-1} s r^{n-1} 0 + \cdots a_1 s^{n-1} r + a_0 s^n = 0 \ , \tag{1}$$

de modo que

$$r(a_n r^{n-1} + \cdots a_1 s^{n-1}) = -a_0 s^n .$$

Como $a_0 \neq 0$, 0 no es raÃz de p y por lo tanto será $r \neq 0$. Por otro lado, como todos los $a_k \in \mathbb{Z}$ y $r \in \mathbb{Z}$, se tiene

$$\frac{-a_0 s^n}{r} = a_n r^{n-1} + \cdots a_1 s^{n-1} \in \mathbb{Z} \ \ \Rightarrow \ \ r | a_0 \ \ \text{o} \ \ r | s^n \ ,$$

pero r no puede dividir a s^n pues r y s son primos relativos (no tienen factores primos comunes), y en consecuencia será válido que $r|a_0$.
Por otro lado, puede sacarse factor común s en (1), para obtener

$$s(a_0 s^{n-1} + \cdots + a_{n-1} r^{n-1}) = -a_n r^n \ .$$

En este caso, como $s \neq 0$, resulta

$$\frac{-a_n r^n}{s} = a_0 s^{n-1} + \cdots + a_{n-1} r^{n-1} \in \mathbb{Z} \ \ \Rightarrow \ \ s | a_n \ \ \text{o} \ \ s | r^n \ ,$$

y siendo r y s coprimos, debe ser necesariamente $s|a_n$.

Q.E.D.

Con el mismo razonamiento que antes, concluimos que s divide a a_n.