LA REGLA DE RUFFINI

En el desolador panorama que nos ofrece la enseñanza en España, es particularmente dramática la falta o ausencia de conocimiento matemático de nuestros estudiantes. Siempre he sospechado que a ello contribuye mucho unos contenidos superfluos, sin profundidad, impartidos muchas veces por profesores incompetentes que se preocupan más por aspectos prácticos que por transmitir la belleza de lo que exponen. Por eso han convertido la enseñanza de las matemáticas en un recetario algorítmico para ser aplicado con poca base reflexiva. Un lamentable ejemplo es lo mal que se explica la *Regla de Ruffini* (me horrorizan las reglas en matemáticas). Si los alumnos no saben el porqué de lo que se les enseña mal aprenderán. En la medida de lo posible es preferible demostrar todo lo que se pueda. Puntualmente se nos puede presentar un resultado cuya demostración sea larga y tediosa o incluso que el alumno no tenga los conocimientos suficientes para llevarla a cabo, solo en estos casos estaría justificada la ausencia de la demostración.

Lo primero que necesitamos saber es en qué consiste la división en el conjunto $\mathbb{Z}$ de los números enteros, si tan sólo sabemos el mísero algoritmo de la división no podemos avanzar. Damos la definición del cociente de números enteros.

Definición: Sean $a, b \in \mathbb{Z}$, $a > b$. Se dice que al dividir a por b el cociente es c y el resto es r , $b > r$ si se puede expresar $a = b.c + r$ con la caja de división esto lo expresábamos así:

$$\begin{array}{r|l} a & b \\ \hline r & c \end{array}$$

La definición de división en el anillo de los números enteros $\mathbb{Z}$ se puede extender al anillo $\mathbb{R}[X]$ de los polinomios con coeficientes reales:

$$\mathbb{R}[X] = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_n, a_{n-1}, \dots, a_1, a_0 \in \mathbb{R}\}$$

Dedición: Sean $P(X), Q(X) \in \mathbb{R}[X]$ tal que $\text{grado } Q(X) \leq \text{grado } P(X)$. Se dice que el cociente al dividir $P(X)$ por $Q(X)$ es $C(X)$ con resto $R(X)$, siendo $\text{grado } R(X) < \text{grado } Q(X)$ si se verifica que $P(X) = Q(X)C(X) + R(X)$ Con la caja de la división esto lo expresamos así:

$$\frac{P(X)}{R(X)} \quad \left| \frac{Q(X)}{C(X)} \right.$$

La *Regla de Ruffini* es un algoritmo para dividir un polinomio $P(X)$ por $x-a$. Para fijar ideas sea el polinomio $P(X) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ y supongamos que:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \left| \begin{array}{l} x-a \\ \hline b_{n-1} x^{n-1} + \dots + b_1 x + b_0 \end{array} \right.$$

r

Observese que el grado del cociente debe ser (n-1) y que el resto ha de ser un número r. Según la definición de división ha de cumplirse que:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = (x-a)(b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \dots + b_1 x + b_0) + r$$

Si desarrollamos el producto y agrupamos términos obtenemos:

$$b_{n-1} x^n + (b_{n-2} - ab_{n-1}) x^{n-1} + \dots + (b_{n-3} - ab_{n-2}) x^{n-2} + \dots + (b_0 - ab_1) x + (r - ab_0) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Según el principio de identidad de polinomios, dos polinomios son iguales si y solo si tienen el mismo grado y son iguales los coeficientes de los términos del mismo grado, con lo que:

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} - ab_{n-1} &= a_{n-1} \implies b_{n-2} = a_{n-1} + ab_{n-1} = a_{n-1} + aa_n \\ b_{n-3} - ab_{n-2} &= a_{n-2} \implies b_{n-3} = a_{n-2} + ab_{n-2} = a_{n-2} + a(a_{n-1} + aa_n) \\ &\dots \\ &\dots \\ &\dots \\ b_0 - ab_1 &= a_1 \implies b_0 = a_1 + ab_1 = a_1 + a(a_2 + a(\dots)) \\ r - ab_0 &= a_0 \implies r = a_0 + ab_0 = \dots \end{aligned}$$

Si nos fijamos esto es lo que hacemos con la regla de Ruffini.

a	a _n	a _{n-1}		a ₁	a ₀
	aa _n				
	a _n	aa _n + a _{n-1}			

Queda claro que la regla de Ruffini no es más que una forma rápida de dividir un polinomio por $(x - a)$. Veamos algunos resultados interesantes que se desprenden de la división de un polinomio por $(x - a)$

Teorema del Resto.- El resto r al dividir un polinomio $P(x)$ por $x - a$ es el valor numérico del polinomio en $x = a$, es decir $r = P(a)$

Demostración:

Sea $c(x)$ el cociente de la división de $P(x)$ por $x - a$:

$$\begin{array}{r} P(x) \\ r \end{array} \quad \left| \begin{array}{l} x-a \\ \hline c(x) \end{array} \right.$$

Entonces $P(x) = c(x)(x - a) + r \Rightarrow P(a) = c(a)(a - a) + r \Rightarrow P(a) = r$

Proposición.- Sea $P(x)$ un polinomio y sea r el resto al dividir $P(x)$ por $x - a$. Entonces a es raíz de $P(x) \iff r = 0$

Demostración

Según el teorema del resto $r = P(a)$. Por tanto si a es raíz de $P(x) \iff \iff P(a) = 0 \iff r = 0$

Proposición.- Sea el polinomio $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. Entonces las posibles raíces enteras de $P(x)$ son divisores del término independiente a_0 .

Demostración

Si a es raíz de $P(x)$ entonces $P(a) = a_n a^n + a_{n-1} a^{n-1} + \dots + a_1 a + a_0 = 0 \iff a_0 = -a_n a^n - a_{n-1} a^{n-1} - \dots - a_1 a \iff a_0 = a(-a_n a^{n-1} - a_{n-1} a^{n-2} - \dots - a_1) \iff a_0$ es múltiplo de $a \iff a$ es divisor de a_0 .

Vamos a necesitar las siguientes propiedades de números enteros. Cuando a es divisor de b pondremos $a|b$

Propiedad 1.- Sean $a, b, c \in \mathbb{Z}$ tales que $a|(bc)$. Entonces $a|b$ o bien $a|c$.

Demostración

si $a|(bc) \Rightarrow \exists d \in \mathbb{Z}$ tal que $bc = ad$. Supongamos que $a \nmid b$, como $d = b \frac{c}{a} \Rightarrow a|c$.

Propiedad 2.- Si $a \nmid b \Rightarrow a \nmid b^n \forall n \in \mathbb{Z}$. La demostración se hace por inducción sobre n .

Proposición.- Sea $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ un polinomio con coeficientes enteros. Supongamos que $x = \frac{p}{q} \in \mathbb{Q}$ donde $\text{mcd}(p, q) = 1$, es raíz de $P(x)$. Entonces $p|a_0$ y $q|a_n$

Demostración

Por definición de raíz $P\left(\frac{p}{q}\right) = a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_1 \frac{p}{q} + a_0 = 0$. Si despejamos $-a_0 q^n = p(a_n p^{n-1} + a_{n-1} q p^{n-2} + \dots + a_1 q^{n-1})$, como $\text{mcd}(p, q) = 1$ se verifica que $p \nmid q$, al ser $a_n p^{n-1} + a_{n-1} q p^{n-2} + \dots + a_1 q^{n-1} = -\frac{a_0 q^n}{p} \Rightarrow p|a_0$. Análogamente $-a_n p^n = q(a_{n-1} p^{n-1} + a_{n-2} q p^{n-2} + \dots + a_1 q^{n-1} + a_0 q^n)$. Por tanto $a_{n-1} p^{n-1} + a_{n-2} q p^{n-2} + \dots + a_1 q^{n-1} + a_0 q^n = -\frac{a_n p^n}{q}$ y como $q \nmid p \Rightarrow q|a_n$