Capítulo 7

Polinomios.

7.1 El anillo de polinomios $K[X]$: generalidades.

Sea K un cuerpo, por ejemplo $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}/p\mathbb{Z}$, donde p es un número primo (positivo). Se dice que f es un *polinomio con coeficientes en* K si f es de la forma

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = \sum_{i=0}^{n} a_i X^i,$$

para algún $n \in \mathbb{N}_0$, donde X es una indeterminada sobre K y $a_i \in K$ para $0 \leq i \leq n$. Los elementos $a_i \in K$ se llaman los *coeficientes* de f. Se conviene que dos polinomios son iguales si y solo si coinciden todos sus coeficientes, es decir si $f = \sum_{i=0}^{n} a_i X^i$ y $g = \sum_{i=0}^{n} b_i X^i$, entonces $f = g \Leftrightarrow a_i = b_i,\ 0 \leq i \leq n$.

El conjunto de todos los polinomios f con coeficientes en K se nota $K[X]$.

Si f no es el polinomio nulo, es decir $f \neq 0$, entonces se puede escribir para algún $n \in \mathbb{N}_0$ en la forma

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{con} \quad a_n \neq 0.$$

En ese caso n es el *grado* de f y se nota $\mathrm{gr}(f)$, a_n es el *coeficiente principal* de f y lo notaremos aquí $\mathrm{cp}(f)$, y a_0 se denomina el *coeficiente constante* o *término independiente* de f. El polinomio nulo no tiene grado. Cuando el coeficiente principal de f es igual a 1, se dice que el polinomio es *mónico*. Notemos que para todo $f \in K[X] - \{0\}$, se tiene $\mathrm{gr}(f) \in \mathbb{N}_0$.

7.1.1 Operaciones en $K[X]$.

Las operaciones $+$ y $\cdot$ del cuerpo K se trasladan al conjunto $K[X]$ en forma natural, se suma coeficiente a coeficiente y se multiplica aplicando la distributividad:

- Si $f = \sum_{i=0}^{n} a_i X^i,\ g = \sum_{i=0}^{n} b_i X^i \in K[X]$, entonces

$$f + g = \sum_{i=0}^{n} (a_i + b_i) X^i \in K[X].$$

- Si $f = \sum_{i=0}^{n} a_i X^i,\ g = \sum_{j=0}^{m} b_j X^j \in K[X]$, entonces

$$f \cdot g = \sum_{k=0}^{n+m} c_k X^k \in K[X] \quad \text{donde } c_k = \sum_{i+j=k} a_i b_j.$$

Ejemplos:

- Sean $f = 5X^4 - 2X^3 + 3X^2 - X + 1$ y $g = 3X^3 - X^2 + X - 3$. Entonces

  $f + g = 5X^4 + X^3 + 2X^2 - 2,$
  $f \cdot g = 15X^7 - 11X^6 + 16X^5 - 23X^4 + 13X^3 - 11X^2 + 4X - 3.$

  En este caso, $\operatorname{gr}(f+g) = 4 = \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$, y $\operatorname{gr}(f \cdot g) = 7 = \operatorname{gr}(f) + \operatorname{gr}(g)$, más aún, $\operatorname{cp}(f \cdot g) = 15 = 5 \cdot 3 = \operatorname{cp}(f) \cdot \operatorname{cp}(g)$.

- Sean $f = 2X^3 + 3X - 1$, $g = -2X^3 + 2X^2 - 1$ y $h = -3X^3 - 2$. Entonces $f + g = 2X^2 + 3X - 2$ y $f + h = -X^3 + 3X - 3$. En este caso $\operatorname{gr}(f+g) = 2 < \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$ pues los dos polinomios tienen el mismo grado y se cancelaron los coeficientes principales, pero $\operatorname{gr}(f+h) = 3 = \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$ pues por más que los dos polinomios tienen mismo grado, no se cancelaron los coeficientes principales.

Observación 7.1.1. (Grado de la suma y del producto.)

Sea K un cuerpo y sean $f, g \in K[X]$ *no nulos*. Entonces

- Si $f + g \neq 0$, entonces $\operatorname{gr}(f+g) \leq \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$. Más precisamente,

  $\operatorname{gr}(f+g) = \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$ si $\operatorname{gr}(f) \neq \operatorname{gr}(g)$ o $\operatorname{gr}(f) = \operatorname{gr}(g)$ pero $\operatorname{cp}(f) + \operatorname{cp}(g) \neq 0$.

  $\operatorname{gr}(f+g) < \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$ si $\operatorname{gr}(f) = \operatorname{gr}(g)$ y $\operatorname{cp}(f) + \operatorname{cp}(g) = 0$.

- $\operatorname{cp}(f \cdot g) = \operatorname{cp}(f) \cdot \operatorname{cp}(g)$. En particular, $f \cdot g \neq 0$ y $\operatorname{gr}(f \cdot g) = \operatorname{gr}(f) + \operatorname{gr}(g)$.

Ejemplo: Calcular el coeficiente principal, el coeficiente constante y el que acompaña a X de

$$f = (X^3 + 2)^{10}(2X + 3)^5$$

- El coeficiente principal de f se obtiene multiplicando los coeficientes principales de los factores:

$$\mathrm{cp}(f) = \mathrm{cp}(X^3 + 2)^{10}\mathrm{cp}(2X + 3)^5 = 1^{10} \cdot 2^5 = 2^5.$$

- El coeficiente constante de f se obtiene multiplicando los coeficientes constantes de los factores, en este caso:

$$2^{10} \cdot 3^5.$$

- ¿Cómo se obtiene el coeficiente que acompaña a X en este producto? La única forma es eligiendo el coeficiente constante en $(X^3 + 2)^{10}$, esto es 2^{10}, y calculando en $(2X + 3)^5$ el coeficiente que acompaña a X, es decir eligiendo en uno de los 5 paréntesis de $(2X + 3)^5$ una vez el $2X$ y 4 veces el 3, esto es $\binom{5}{1}2 \cdot 3^4 = 5 \cdot 2 \cdot 3^4$. El resultado es entonces:

$$2^{10} \cdot 5 \cdot 2 \cdot 3^4 = 2^{11} \cdot 3^4 \cdot 5.$$

Teorema 7.1.2. (El anillo $(K[X], +, \cdot)$.)

Sea K un cuerpo. Entonces, $(K[X], +, \cdot)$ es un anillo conmutativo *(al igual que $\mathbb{Z}$). Más aún, al igual que en $\mathbb{Z}$, si se multiplican dos elementos no nulos, el resultado es no nulo, o dicho de otra manera:*

$$\forall\, f, g \in K[X], \quad f \cdot g = 0 \implies f = 0 \ o \ g = 0.$$

(Esto se llama ser un dominio íntegro*.)*

Demostración. Las propiedades conmutativa y asociativa de las operaciones $+$ y $\cdot$ son consecuencia de las definiciones de las operaciones y del hecho que valen las mismas propiedades en K. El elemento neutro para la suma es el polinomio 0, y el opuesto aditivo de $f = \sum_{i=0}^{n} a_i X^i$ es $-f = \sum_{i=0}^{n}(-a_i)X^i$. El elemento neutro para el producto es el polinimio 1. Pero en ese caso no todo $f \neq 0$ tiene inverso multiplicativo, como veremos a continuación.

La segunda afirmación es una consecuencia de la observación anterior: si f y g son no nulos, entonces fg es no nulo. □

Como consecuencia de la observación sobre el grado del producto se deduce inmediatamente quiénes son los polinomios en $K[X]$ que tienen inverso multiplicativo.

Observación 7.1.3. (Inversibles de $K[X]$.)

Sea K un cuerpo. Entonces $f \in K[X]$ es inversible si y solo si $f \in K^\times$. O sea los elementos inversibles de $K[X]$ son los polinomios de grado 0.

Demostración.

- ($\Rightarrow$) Sea $f \in K[X]$ inversible. Es decir existe $g \in K[X]$ tal que $f \cdot g = 1$. Por lo tanto tanto f como g son no nulos, y $\mathrm{gr}(1) = \mathrm{gr}(f \cdot g)$, es decir $0 = \mathrm{gr}(f) + \mathrm{gr}(g)$. Como $\mathrm{gr}(f), \mathrm{gr}(g) \in \mathbb{N}_0$, la única posibilidad es $\mathrm{gr}(f) = 0 = \mathrm{gr}(g)$ y por lo tanto $f, g \in K$, y no nulos.

- ($\Leftarrow$) Sea $f \in K - \{0\}$, o sea f es una constante no nula de K. Por lo tanto, como K es un cuerpo, f es inversible y existe $g \in K - \{0\}$ tal que $f \cdot g = 1$, es decir f es inversible.

□

7.1.2 Divisibilidad, Algoritmo de División y MCD en $K[X]$.

Por lo que vimos en la sección anterior, $K[X]$ es un anillo conmutativo (más bien un dominio íntegro) que, al igual que $\mathbb{Z}$, no es un cuerpo ya que no todo elemento no nulo es inversible: sabemos que los únicos polinomios inversibles son los polinomios constantes (no nulos). Tiene sentido entonces estudiar la *divisibilidad* así como hicimos en $\mathbb{Z}$. En esta sección haremos todo un paralelismo con la teoría desarrollada en $\mathbb{Z}$.

Definición 7.1.4. (Divisibilidad.)

Sean $f, g \in K[X]$ con $g \neq 0$. Se dice que g *divide a* f, y se nota $g \mid f$, si existe un polinomio $q \in K[X]$ tal que $f = q \cdot g$. O sea:

$$g \mid f \iff \exists\, q \in K[X] \,:\, f = q \cdot g.$$

En caso contrario, se dice que g no divide a f, y se nota $g \nmid f$.

Propiedades 7.1.5. (Propiedades de la divisibilidad.)

- Todo polinomio $g \neq 0$ satisface que $g \mid 0$ pues $0 = 0 \cdot g$ (aquí $q = 0$).
- $g \mid f \Leftrightarrow c\,g \mid f$, $\forall\, c \in K^\times$ (pues $f = q \cdot g \Leftrightarrow f = (c^{-1}q) \cdot (c\,g)$).
  De la misma manera $g \mid f \Leftrightarrow g \mid d\,f, \forall\, d \in K^\times$.
  Se concluye que si $f, g \in K[X]$ son no nulos,

$$g \mid f \iff c\,g \mid d\,f,\ \forall\, c, d \in K^\times \iff \frac{g}{\mathrm{cp}(g)} \mid \frac{f}{\mathrm{cp}(f)}.$$

Es decir la divisibilidad no depende de constantes no nulas (que son los elementos inversibles de K), y por lo tanto todo polinomio tiene infinitos divisores. Pero todo divisor g de f tiene un divisor mónico asociado, que es $g/\mathrm{cp}(g)$.

- Sean $f, g \in K[X]$ no nulos tales que $g \mid f$ y $\mathrm{gr}(g) = \mathrm{gr}(f)$. Entonces $g = c\,f$ para algún $c \in K^\times$ (pues $f = q\,g$ con $q \neq 0$ y $\mathrm{gr}(g) = \mathrm{gr}(f) \Rightarrow \mathrm{gr}(q) = 0$, i.e. $q = c \in K^\times$).

- $g \mid f$ y $f \mid g \Leftrightarrow f = c\,g$ para algún $c \in K^\times$ (pues tienen el mismo grado).

- Para todo $f \in K[X]$, $f \notin K$, se tiene $c \mid f$ y $c\,f \mid f$, $\forall\, c \in K^\times$.

  Así, todo f en esas condiciones tiene esas dos categorías distintas de divisores asegurados (los de grado 0 y los de su mismo grado que son de la forma $c\,f$, con $c \in K^\times$).

  Hay polinomios que tienen únicamente esos divisores, y otros que tienen más. Esto motiva la separación de los polinomios en $K[X]$ no constantes en dos categorías, la de polinomios *irreducibles* y la de los polinomios *reducibles* :

Definición 7.1.6. (Polinomios irreducibles y reducibles.)

Sea $f \in K[X]$.

- Se dice que f es *irreducible* en $K[X]$ cuando $f \notin K$ y los únicos divisores de f son de la forma $g = c$ o $g = c\,f$ para algún $c \in K^\times$. O sea f tiene únicamente dos divisores mónicos (distintos), que son 1 y $f/\mathrm{cp}(f)$.

- Se dice que f es *reducible* en $K[X]$ cuando $f \notin K$ y f tiene algún divisor $g \in K[X]$ con $g \neq c$ y $g \neq c\,f$, $\forall\, c \in K^\times$, es decir f tiene algún divisor $g \in K[X]$ (no nulo por definición) con $0 < \mathrm{gr}(g) < \mathrm{gr}(f)$.

En particular, todo polinomio de grado 1 en $K[X]$ es irreducible.

Pero no solo ellos, dependiendo del cuerpo K: por ejemplo el polinomio $X^2 + 1 \in \mathbb{R}[X]$ es irreducible en $\mathbb{R}[X]$, pues si fuera reducible, tendría un divisor mónico de grado 1 (grado intermedio), y luego se tendría $X^2 + 1 = (X + a)\,(X + b)$ con $a, b \in \mathbb{R}$, lo que implica $a + b = 0$, i.e. $b = -a$ y $a\,b = 1$, i.e. $-a^2 = 1$, lo que es imposible para $a \in \mathbb{R}$. Pero es reducible en $\mathbb{C}[X]$ ya que $X^2 + 1 = (x - i)(x + i)$, i.e. $X - i \mid X^2 + 1$ en $\mathbb{C}[X]$.

Y el polinomio $X^2 - 2 \in \mathbb{Q}[X]$ es irreducible en $\mathbb{Q}[X]$, pues si fuera reducible, tendría un divisor mónico de grado 1, y luego se tendría $X^2 - 2 =$

$(X+a)\,(X+b)$ con $a, b \in \mathbb{Q}$, lo que implica $a+b=0$, i.e. $b=-a$ y $a\,b=-2$, i.e. $a^2=2$, lo que es imposible para $a \in \mathbb{Q}$. Pero es reducible en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$ ya que $X^2+2=(x-\sqrt{2})(x+\sqrt{2})$, i.e. $X-\sqrt{2} \mid X^2-2$ en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$.

La divisibilidad de polinomios cumple exactamente las mismas propiedades que la divisibilidad de números enteros. Repasar esas propiedades.

Continuamos entonces el paralelismo con $\mathbb{Z}$ para $K[X]$:

Teorema 7.1.7. (Algoritmo de división.)

Dados $f, g \in K[X]$ no nulos, existen únicos $q, r \in K[X]$ que satisfacen

$$f = q \cdot g + r \quad \textit{con} \quad r = 0 \quad o \quad \mathrm{gr}(r) < \mathrm{gr}(g).$$

Se dice que q es el *cociente* y r es el *resto* de la división de f por g, que notaremos $r_g(f)$.

<u>*Ejemplo:*</u> Sean $f = X^5+X^4-3X^3+4X^2+2X$ y $g = X^4+3X^3-X^2-6X-2$, entonces

$$f = (X-2)g + r \quad \text{con } r = 4X^3+8X^2-8X-4.$$

Demostración. • *Existencia de q y r:*

La demostración es calcada del caso $\mathbb{Z}$. Dados $f, g \in K[X]$ no nulos, consideramos el conjunto

$$A = \{f - \tilde{q}\,g;\ \tilde{q} \in K[X]\} \ \subset\ K[X],$$

que es claramente un conjunto $\neq \emptyset$ pues por ejemplo $f \in A$ tomando $\tilde{q}=0$. Si $0 \notin A$, elijamos un polinomio $r \in A$ de grado mínimo, y si $0 \in A$, elijamos $r=0$. Es decir

$$\exists\, q \in K[X] \text{ tal que } \quad r = f - q\,g \quad \text{ y } \quad r=0 \text{ o } \mathrm{gr}(r) \le \mathrm{gr}(\tilde{r}),\ \forall\, \tilde{r} \in A.$$

Por lo tanto, $f = q\,g + r$ y se afirma que si $r \neq 0$, entonces $\mathrm{gr}(r) < \mathrm{gr}(g)$. Pues si fuera $\mathrm{gr}(r) \ge \mathrm{gr}(g)$, puedo considerar el polinomio

$$\begin{aligned}\tilde{r} &= r - \frac{\mathrm{cp}(r)}{\mathrm{cp}(g)} X^{\mathrm{gr}(r)-\mathrm{gr}(g)}\, g \\ &= f - q\,g - \frac{\mathrm{cp}(r)}{\mathrm{cp}(g)} X^{\mathrm{gr}(r)-\mathrm{gr}(g)}\, g \\ &= f - \big(q + \frac{\mathrm{cp}(r)}{\mathrm{cp}(g)} X^{\mathrm{gr}(r)-\mathrm{gr}(g)}\big)\, g \ \in\ A.\end{aligned}$$

Es fácil verificar que los dos sumandos tienen el mismo grado, y en esta resta, se cancela el coeficiente principal de r. Por lo tanto $\mathrm{gr}(\tilde{r}) < \mathrm{gr}(r)$, lo que contradice el hecho que r tenía grado mínimo en A.

- *Unicidad de q y r:*

  Supongamos que existen $q_1, r_1, q_2, r_2 \in K[X]$ con $r_1 = 0$ o $\mathrm{gr}(r_1) < \mathrm{gr}(g)$ y $r_2 = 0$ o $\mathrm{gr}(r_2) < \mathrm{gr}(g)$ tales que

  $$f = q_1\, g + r_1 = q_2\, g + r_2.$$

  Entonces $(q_1 - q_2)\, g = r_2 - r_1$ implica $g \mid r_2 - r_1$. Pero si $r_2 - r_1 \neq 0$, se tiene que $\mathrm{gr}(r_2 - r_1) \leq \max\{\mathrm{gr}(r_2), \mathrm{gr}(r_1)\} < \mathrm{gr}(g)$, luego no puede ser divisible por g. Por lo tanto $r_2 - r_1 = 0$, i.e. $r_1 = r_2$ de lo que se deduce que $q_1 = q_2$ pues $(q_1 - q_2)\, g = 0$ con $g \neq 0$ implica $q_1 - q_2 = 0$.

□

Observación 7.1.8. (Algoritmo de división en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.)

Una consecuencia tal vez impensada pero importante de la unicidad del cociente y el resto en el algoritmo de división es que si $f, g \in \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$, entonces **el** cociente y **el** resto de dividir a f por g pertenecen a $\mathbb{Q}[X]$ independientemente de si miramos a los polinomios en $\mathbb{Q}[X]$, en $\mathbb{R}[X]$ o en $\mathbb{C}[X]$ (pues el cociente y el resto en $\mathbb{Q}[X]$ cumplen la propiedad de cociente y resto también en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$). Y análogamente para $f, g \in \mathbb{R}[X] \subset \mathbb{C}[X]$.

Definición 7.1.9. (Máximo Común Divisor.)

Sean $f, g \in K[X]$ no ambos nulos. El *máximo común divisor* entre f y g, que se nota $(f : g)$, es el polinomio mónico de mayor grado que divide simultáneamente a f y a g.

Observación 7.1.10. No es obvio en este caso que este polinomio es único, de hecho es una consecuencia de las propiedades siguientes que se cumplen para un polinomio mónico de mayor grado que es divisor común de f y g, y de los resultados que se deducen de esas propiedades.

- $(f : 0) = f/\mathrm{cp}(f)$, $\forall\, f \in K[X]$ no nulo.
- Sean $f, g \in K[X]$ con g no nulo. Si $f = q \cdot g + r$ para $q, r \in K[X]$, entonces $(f : g) = (g : r)$.

<u>*Ejemplos:*</u> Sean $f, g \in K[X]$, $g \neq 0$. Entonces :

- Sea $c \in K^\times$, $(c : g) = 1$
- Si $g \mid f$, entonces $(f : g) = \frac{g}{\mathrm{cp}(g)}$.

A continuación deducimos el Algoritmo de Euclides, que al igual que en el caso $\mathbb{Z}$, permite calcular el máximo común divisor entre dos polinomios (y es de hecho la única forma de calcular el máximo común divisor de polinomios arbitrarios).

Teorema 7.1.11. (Algoritmo de Euclides.)

Sean $f, g \in K[X]$ no nulos. Entonces $(f : g)$ es el último resto r_k no nulo (dividido por su coeficiente principal para volverlo mónico) que aparece en la sucesión de divisiones siguiente:

$$\begin{array}{lcll} f & = & q_1\, g + r_1 & \textit{con} \quad r_1 \neq 0 \quad \textit{y} \quad \mathrm{gr}(r_1) < \mathrm{gr}(g), \\ g & = & q_2\, r_1 + r_2 & \textit{con} \quad r_2 \neq 0 \quad \textit{y} \quad \mathrm{gr}(r_2) < \mathrm{gr}(r_1), \\ r_1 & = & q_3\, r_2 + r_3 & \textit{con} \quad r_3 \neq 0 \quad \textit{y} \quad \mathrm{gr}(r_3) < \mathrm{gr}(r_2), \\ & \vdots & & \\ r_{k-2} & = & q_k\, r_{k-1} + r_k & \textit{con} \quad r_k \neq 0 \quad \textit{y} \quad \mathrm{gr}(r_k) < \mathrm{gr}(r_{k-1}), \\ r_{k-1} & = & q_{k+1}\, r_k & \end{array}$$

(pues resulta

$$(f : g) = (g : r_1) = (r_1 : r_2) = \cdots = (r_{k-2} : r_{k-1}) = (r_{k-1} : r_k) = \frac{r_k}{\mathrm{cp}(r_k)},$$

ya que $r_k \mid r_{k-1}$).

Observación 7.1.12. (Mcd en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.)

El hecho que el algoritmo de Euclides para calcular $(f : g)$ se basa en el algoritmo de división tiene una consecuencia no inmediata tal vez, pero fundamental, que es que si $f, g \in \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$, entonces $(f : g) \in \mathbb{Q}[X]$ (y es siempre el mismo) independientemente de si miramos a $f, g \in \mathbb{Q}[X]$, en $\mathbb{R}[X]$ o en $\mathbb{C}[X]$. Y análogamente para $f, g \in \mathbb{R}[X] \subset \mathbb{C}[X]$.

Si despejamos en el algoritmo de Euclides para el cálculo del mcd el polinomio r_k de la anteúltima igualdad, y volviendo hacia arriba despejando paso a paso r_{k-1}, $r_{k-2}, \ldots$, r_2, r_1 en las igualdades anteriores, se logra escribir r_k en la forma $r_k = s'f + t'g$ (al igual que hicimos en el caso de $\mathbb{Z}$). Finalmente, dividiendo toda la expresión por la constante $\mathrm{cp}(r_k)$, se obtienen $s, t \in K[X]$ tales que $(f : g) = sf + tg$.

<u>*Ejemplo:*</u> Sean $f = X^5+X^4-3X^3+4X^2+2X$ y $g = X^4+3X^3-X^2-6X-2$. Se tiene :

$$\begin{array}{lcll} f & = & (X-2)g + r_1 & \text{con} \quad r_1 = 4X^3 + 8X^2 - 8X - 4 \\ g & = & (\frac{1}{4}X + \frac{1}{4})r_1 + r_2 & \text{con} \quad r_2 = -X^2 - 3X - 1 \\ r_1 & = & (-4X + 4)r_2 & \end{array}$$

Luego $(f:g) = \frac{r_2}{\mathrm{cp}(r_2)} = X^2 + 3X + 1$ y

$$\begin{aligned} r_2 &= g - (\tfrac{1}{4}X + \tfrac{1}{4})r_1 \\ &= g - (\tfrac{1}{4}X + \tfrac{1}{4})(f - (X-2)g) \\ &= -(\tfrac{1}{4}X + \tfrac{1}{4})f + [1 + (\tfrac{1}{4}X + \tfrac{1}{4})(X-2)]g \\ &= -(\tfrac{1}{4}X + \tfrac{1}{4})f + (\tfrac{1}{4}X^2 - \tfrac{1}{4}X + \tfrac{1}{2})g \end{aligned}$$

Así : $(f:g) = -r_2 = (\frac{1}{4}X + \frac{1}{4})f - (\frac{1}{4}X^2 - \frac{1}{4}X + \frac{1}{2})g$.

Corolario 7.1.13. (Mcd y combinación polinomial.)

Sean $f, g \in K[X]$ no ambos nulos. El máximo común divisor entre f y g es el (único) polinomio mónico $h \in K[X]$ que satisface simultáneamente las dos condiciones siguientes :

- $h \mid f$ *y* $h \mid g$,
- *Existen* $s, t \in K[X]$ *tales que* $h = sf + tg$.

También se puede deducir, como en el caso de los enteros, la propiedad siguiente que relaciona el máximo común divisor con los divisores comunes mediante divisibilidad.

Corolario 7.1.14. (Mcd y divisores comunes.)

Sean $f, g \in K[X]$ no ambos nulos. El máximo común divisor entre f y g es el (único) polinomio mónico $h \in K[X]$ que satisface simultáneamente las dos condiciones siguientes :

- $h \mid f$ *y* $h \mid g$,
- *Si* $\tilde{h} \in K[X]$ *satisface que* $\tilde{h} \mid f$ *y* $\tilde{h} \mid g$, *entonces* $\tilde{h} \mid h$.

Definición 7.1.15. (Polinomios coprimos)

Sean $f, g \in K[X]$ no ambos nulos. Se dice que son *coprimos* si satisfacen

$$(f:g) = 1.$$

Es decir si ningún polinomio de grado ≥ 1 divide simultáneamente a f y a g . O equivalentemente si existen polinomios $s, t \in K[X]$ tales que

$$1 = sf + tg.$$

Proposición 7.1.16. (Divisibilidad con coprimalidad.)

Sean f, g, $h \in K[X]$, entonces:

1. *Si g y h son* coprimos, *entonces $g \mid f$ y $h \mid f \iff gh \mid f$*

2. Si g *y* h *son* coprimos, *entonces* $g \mid h\,f \iff g \mid f$.

Demostración. $(g : h) = 1 \Longrightarrow \exists\, s, t \in K[X]$ tales que $1 = sg + th$. Luego

$$f = sgf + thf. \tag{7.1}$$

1. ($\Leftarrow$) vale siempre.

   ($\Rightarrow$) $g\,h$ divide al primer sumando a la derecha en (7.1) pues $h \mid f$ por hipótesis, y $g\,h$ divide también al segundo sumando pues $g \mid f$ por hipótesis. Por lo tanto $g\,h$ divide a la suma que es igual a f.

2. ($\Leftarrow$) vale siempre.

   ($\Rightarrow$) g divide claramente al primer sumando a la derecha en (7.1), y también divide al segundo sumando pues $g \mid hf$ por hipótesis. Por lo tanto g divide a la suma que es igual a f. divide a f.

□

7.1.3 El Teorema Fundamental de la Aritmética para Polinomios.

Observación 7.1.17. (Primalidad de los polinomios irreducibles.)

Sea f un polinomio *irreducible* en $K[X]$. Entonces

- Para todo $g \in K[X]$, $(f : g) = \frac{f}{\mathrm{cp}(f)}$ si $f \mid g$ y $(f : g) = 1$ si $f \nmid g$.
- Para todo $g, h \in K[X]$, $f \mid g\,h \implies f \mid g$ o $f \mid h$.

Teorema 7.1.18. (Teorema Fundamental de la Aritmética para polinomios.)

Sea K *un cuerpo, y sea* $f \in K[X]$ *un polinomio no constante. Entonces* existen únicos polinomios irreducibles mónicos distintos $g_1, \ldots, g_r$ *en* $K[X]$ *tales que*

$$f = c\,{g_1}^{m_1} \ldots {g_r}^{m_r} \quad \text{donde} \quad c \in K \setminus \{0\} \text{ y } m_1, \ldots, m_r \in \mathbb{N}$$

(La unicidad de los factores irreducibles g_i *es salvo el orden de los factores.) La constante* c *resulta ser el coeficiente principal de* f.

<u>*Ejemplo:*</u> El polinomio $(X^2+1)(X^2-2)$ está factorizado en factores irreducibles en $\mathbb{Q}[X]$ (pues ambos factores son irreducibles) pero su factorización en $\mathbb{R}[X]$ es $(X^2+1)(X-\sqrt{2})(X+\sqrt{2})$ y su factorización en $\mathbb{C}[X]$ es $(X-i)(X+i)(X-\sqrt{2})(X+\sqrt{2})$. Notemos que en $\mathbb{Q}[X]$ el polinomio

$(X^2+1)(X^2-2)$ es **reducible** en $\mathbb{Q}[X]$, pues $X^2+1 \mid f$ en $\mathbb{Q}[X]$ pero sin embargo **no tiene raíces** en $\mathbb{Q}$. Pero de todos modos como veremos en lo que sigue la búsqueda de raíces de f, si tenemos la suerte de encontrar, ayuda para la factorización.

7.2 Evaluación y Raíces.

Sea $f = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$ un polinomio, entonces f define en forma natural una función

$$f : K \to K, \quad f(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \forall\, x \in K$$

que se llama la función *evaluación*.

Esta función evaluación cumple las dos propiedades siguientes para todo $f, g \in K[X]$:

$$\big(f+g\big)(x) = f(x) + g(x) \quad \text{y} \quad \big(f \cdot g\big)(x) = f(x) \cdot g(x), \quad \forall\, x \in K.$$

En particular, si $f = q\,g + r$ con $q, r \in K[X]$, entonces

$$f(x) = q(x)\,g(x) + r(x), \ \forall\, x \in K.$$

<u>*Ejemplos:*</u>

- Sea $f = X^2 + X - 2 \in \mathbb{Q}[X]$. Entonces $f(3) = 3^2 + 3 - 2 = 10$, $f(0) = -2$ y $f(1) = 1^2 + 1 - 2 = 0$.
- Sea $f = \sum_{i=0}^{n} a_i X^i \in K[X]$. Entonces $f(0) = a_0$ y $f(1) = \sum_{i=0}^{n} a_i$.
- Sea $f = c$ un polinomio constante en $K[X]$. Entonces $f(x) = c$, $\forall\, x \in K$.
- Determinar todos los polinomios $f \in \mathbb{R}[X]$ de grado ≤ 2 (o nulo) tales que $f(0) = 1$ y $f(1) = f(2)$:

  El polinomio f es de la forma $f = aX^2 + bX + c \in \mathbb{R}[X]$. Se tiene $f(0) = 1 \ \Leftrightarrow \ c = 1$ y $f(1) = f(2) \ \Leftrightarrow \ a + b + c = 4a + 2b + c$, es decir $3a + b = 0$. En definitiva, $b = -3a$ y $c = 1$, lo que implica que $f = aX^2 - 3aX + 1$, $a \in \mathbb{R}$.
- Sea $f \in \mathbb{Q}[X]$ tal que $f(0) = 1$ y $f(1) = f(2) = 3$. Calcular el resto de dividir f por $X(X-1)(X-2)$:

  El polinomio f se escribe por el Algoritmo de División como

  $$f = q \cdot X(X-1)(X-2) + r \ \text{ con } \ r = 0 \ \text{ o } \ \operatorname{gr}(r) < 3,$$

o sea $r = aX^2 + bX + c \in \mathbb{Q}[X]$. Por lo tanto, dado que el polinomio $X(X-1)(X-2)$ se anula en 0, 1 y 2, si evaluamos en $x = 0$, $x = 1$ y $x = 2$ obtenemos $f(0) = r(0)$, $f(1) = r(1)$ y $f(2) = r(2)$. O sea $r(0) = 1$, $r(1) = r(2) = 3$. Por el inciso anterior, $r = aX^2 - 3aX + 1$, con $r(1) = a - 3a + 1 = 3$, es decir $-2a = 2$, o sea $a = -1$. Se concluye $r = -X^2 + 3X + 1$.

Definición 7.2.1. (Raíz de un polinomio.)

Sean $f \in K[X]$ un polinomio y $x \in K$. Si $f(x) = 0$, se dice que x es una *raíz* de f (en K).

Proposición 7.2.2. (Equivalencias de raíz.)

$$\begin{aligned} x \in K \text{ es raíz de } f &\iff f(x) = 0 \\ &\iff X - x \mid f \\ &\iff f = q \cdot (X - x) \text{ para algún } q \in K[X]. \end{aligned}$$

Es decir, si $f \neq 0$, $X - x$ es un factor irreducible (mónico) en la descomposición en irreducibles de $f \in K[X]$.

Demostración. Las equivalencia $X - x \mid f \iff f = q\,(X - x)$ para algún $q \in K[X]$ es simplemente por la definición de divisibilidad. Probemos la equivalencia $f(x) = 0 \iff f = q \cdot (X - x)$ para algún $q \in K[X]$:
Por el algoritmo de división, $f = q \cdot (X - x) + r$ donde o bien $r = 0$ o bien $\mathrm{gr}(r) < \mathrm{gr}(X - x) = 1$, es decir $r = 0$ o $\mathrm{gr}(r) = 0$. Así, en todo caso, $r \in K$: r es un polinomio constante. Y por lo tanto cuando evaluamos la expresión en $X = x$ obtenemos

$$f(x) = q(x) \cdot (x - x) + r(x) = q(x) \cdot 0 + r = r$$

ya que $x - x = 0$ y el polinomio constante r evaluado en x da r.
Por lo tanto $f(x) = 0 \iff r = 0$, es decir $f(x) = 0 \iff f = q\,(X - x)$ como se quería probar. □

El razonamiento que acabamos de hacer muestra también el resultado un poco más general siguiente.

Proposición 7.2.3. (Teorema del resto.)

Dados $f \in K[X]$ y $x \in K$, se tiene que $r_{X-x}(f) = f(x)$.

Demostración. Si dividimos al polinomio f por el polinomio $X - x \in K[X]$, obtenemos

$$f = q \cdot (X - x) + r \quad \text{con} \quad r = 0 \text{ o } \mathrm{gr}(r) = 0,$$

o sea $r \in K$ es un polinomio constante. Evaluando como arriba la expresión en $x \in K$ se obtiene $f(x) = r$, y por lo tanto $f = q \cdot (X - x) + f(x)$. Es decir $r_{X-x}(f) = f(x)$. □

Observación 7.2.4. Sean $f, g \in K[X]$ con $g \neq 0$ tal que $g \mid f$ en $K[X]$. Sea $x \in K$. Si x es raíz de g, entonces x es raíz de f también. (Pues $g \mid f$ implica existe $q \in K[X]$ tal que $f = q\,g$ y por lo tanto $f(x) = q(x)\,g(x) = q(x) \cdot 0 = 0$.)

Ejemplos:

- 1 es raíz del polinomio $X^2 + X - 2 \in \mathbb{Q}[X]$.
- 0 es raíz de $f \in K[X]$ si y solo si el coeficiente constante de f es igual a 0.
- f constante: $f = c$ con $c \in K$.

  Entonces, o bien $c = 0$ y todo $x \in K$ es raíz de f, ó bien $c \neq 0$ y f no tiene ninguna raíz en K.
- f de grado 1: $f = aX + b$ con $a, b \in K$, $a \neq 0$. Entonces $x = -\frac{b}{a}$ es raíz de f y $f = a\big(X - (-\frac{b}{a})\big) = a(X - x)$ es la factorización del polinomio irreducible f en $K[X]$.

El resultado siguiente puede ser útil a la hora de buscar raíces si se tiene alguna información adicional sobre el polinomio.

Proposición 7.2.5. (Raíz común y Mcd.)

Sean $f, g \in K[X]$ no ambos nulos y sea $x \in K$. Entonces

$$f(x) = 0 \;\; y \;\; g(x) = 0 \iff (f : g)(x) = 0.$$

Demostración.

- ($\Rightarrow$) Se sabe que existen $s, t \in K[X]$ tales que $(f : g) = s\,f + t\,g$. Por lo tanto $(f : g)(x) = s(x)f(x) + t(x)g(x) = 0$ si $f(x) = g(x) = 0$.
- ($\Leftarrow$) Como $(f : g) \mid f$ y $(f : g) \mid g$ en $K[X]$, si $(f : g)(x) = 0$, entonces $f(x) = 0$ y $g(x) = 0$.

□

7.2.1 Multiplicidad de las raíces.

Vimos en los ejemplos anteriores que a veces una raíz puede aparecer "repetida". Por ejemplo si consideramos el polinomio

$$f = 10(X - 1)^2(X + 1)(X - 2)^3$$

tenemos que la raíz 1 "aparece" dos veces, la raíz -1 una sola, y la raíz 2 tres veces. Esto sugiere la noción de multiplicidad de una raíz de un polinomio.

Definición 7.2.6. (Multiplicidad de una raíz).

Sea $f \in K[X]$ *no nulo.*

- Sea $m \in \mathbb{N}_0$. Se dice que $x \in K$ es una *raíz de multiplicidad* m *de* f si $(X-x)^m \mid f$ y $(X-x)^{m+1} \nmid f$, o lo que equivalente, existe $q \in K[X]$ tal que

  $$f = (X-x)^m\, q \quad \text{con} \quad q(x) \neq 0.$$

  Notamos aquí $\text{mult}(x; f) = m$.

- Se dice que $x \in K$ es una *raíz simple de* f cuando $\text{mult}(x; f) = 1$, es decir $X-x \mid f$ pero $(X-x)^2 \nmid f$, o lo que es equivalente $f = (X-x)\, q$ con $q(x) \neq 0$.

- Se dice que $x \in K$ es una *raíz múltiple de* f cuando $\text{mult}(x; f) > 1$, es decir $(X-x)^2 \mid f$.

- Se dice que $x \in K$ es una *raíz doble de* f cuando $\text{mult}(x; f) = 2$ y que es una *raíz triple de* f cuando $\text{mult}(x; f) = 3$.

Está claro de la definición que dado un polinomio $f \in K[X]$ *no nulo* y $x \in K$ una raíz de f, su multiplicidad m siempre está acotada por el grado del polinomio: $\text{mult}(x; f) \leq \text{gr}(f)$.

Ejemplos:

- En el ejemplo $f = 10(X-1)^2(X+1)(X-2)^3$, 1 es raíz doble de f, -1 es simple y 2 es triple.

- $\text{mult}(x; f) = 0$ si y solo si x no es raíz de f.

Proposición 7.2.7. (Multiplicidad en suma y producto.)

Sea K un cuerpo y sean $f, g \in K[X]$ no nulos. Sea $x \in K$. Entonces

1. *Si* $\text{mult}(x; f) \neq \text{mult}(x; g)$, *entonces* $\text{mult}(x; f+g) = \min\{\text{mult}(x; f), \text{mult}(x; g)\}$.
2. $\text{mult}(x; fg) = \text{mult}(x; f) + \text{mult}(x; g)$.

Demostración. Pongamos $m_1 := \text{mult}(x; f)$ y $m_2 = \text{mult}(x; g)$ donde $m_1, m_2 \in \mathbb{N}_0$, o sea $f = (X-x)^{m_1} q_1$ con $q_1(x) \neq 0$ y $g = (X-x)^{m_2} q_2$ con $q_2(x) \neq 0$.

1. Supongamos sin pérdida de generalidad que $m_1 < m_2$. Entonces

   $$f+g = (X-x)^{m_1}\big(q_1 + (X-x)^{m_2-m_1} q_2\big) \quad \text{donde} \quad \big(q_1 + (X-x)^{m_2-m_1} q_2\big)(x) \neq 0$$

pues $\big(q_1 + (X-x)^{m_2-m_1}q_2\big)(x) = q_1(x) \neq 0$ al ser $m_2 - m_1 \geq 1$, y por lo tanto $\text{mult}(x; f+g) = m_1$.

Notar que si $\text{mult}(x; f) = \text{mult}(x; g)$ puede pasar cualquier cosa. Por ejemplo $\text{mult}(0; 1) = 0 = \text{mult}(0; X^n - 1)$ pero

$$\text{mult}(0; 1 + (X^n - 1)) = \text{mult}(0; X^n) = n.$$

2. Se tiene

$$f\,g = (X-x)^{m_1+m_2}q_1q_2 \quad \text{donde} \quad (q_1q_2)(x) \neq 0$$

pues $(q_1q_2)(x) = q_1(x)q_2(x) \neq 0$ al ser $q_1(x) \neq 0$ y $q_2(x) \neq 0$, y por lo tanto $\text{mult}(x; fg) = m_1 + m_2$.

□

Se recuerda que si $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ entonces

$$f' = n\,a_nX^{n-1} + (n-1)\,a_{n-1}X^{n-2} + \cdots + a_1 \in K[X]$$

es la *derivada* de f, que satisface:

- $(f+g)' = f' + g'$ y $(fg)' = f'g + fg'$, $\forall\, f, g \in K[X]$.
- $(g \circ f)' = g'(f)f'$, $\forall\, f, g \in K[X]$.
  En particular $\big((X-x)^k\big)' = k(X-x)^{k-1}$.
- $f'' = (f')'$ y en general $f^{(m)} = (f')^{(m-1)}$, $\forall\, m \in \mathbb{N}$.

Observemos que si x es una raíz múltiple de f, es decir $f = (X-x)^2q$ para algún $q \in K[X]$, entonces

$$f' = 2(X-x)q + (X-x)^2q' = (X-x)\big(2\,q + (X-x)\,q'\big).$$

Por lo tanto $f'(x) = 0$ también. O sea no sólo vale que $f(x) = 0$ pero también $f'(x) = 0$. Esto es la base de la siguiente proposición que relaciona la multiplicidad con las derivadas de f.

Proposición 7.2.8. (Raíz múltiple y derivada.)

Sea $f \in K[X]$ y sea $x \in K$. Entonces

- *x es raíz múltiple de f si y solo si $f(x) = 0$ y $f'(x) = 0$.*
- *x es raíz simple de f si y solo si $f(x) = 0$ y $f'(x) \neq 0$.*

Demostración. Alcanza con probar el primer inciso, ya que el segundo es decir que x es raíz de f pero no múltiple.

Sabemos que $x \in K$ es raíz de f si y solo si $f = (X - x)\, q$ para algún $q \in K[X]$. Derivando, $f' = q + (X - x)q'$ satisface $f'(x) = q(x)$. En particular $f'(x) = 0 \Leftrightarrow q(x) = 0$.

Por lo tanto,

$$f(x) = 0 \text{ y } f'(x) = 0 \implies (X - x)^2 \mid f.$$

La recíproca fue observada antes de enunciar la proposición: si $(X-x)^2 \mid f$, entonces $f(x) = f'(x) = 0$. □

Ejemplos:

- Probar que el polinomio $2X^{15}+7X^7+2X^3+1$ no tiene raíces múltiples reales.

  Supongamos que sí: Sea $x \in \mathbb{R}$ tal que $f(x) = f'(x) = 0$. En particular, dado que $f' = 30X^{14}+49X^6+6X^2$, se tendría $0 = f'(x) = 30x^{14} + 49x^6 + 6x^2$. Lo que implica que $x = 0$ dado que todos los exponentes en f' son pares (luego $\forall\, x \in \mathbb{R}$, $f'(x) \geq 0$ y $f'(x) = 0 \Leftrightarrow x = 0$.) Pero claramente $f(0) = 1 \neq 0$.

- Hallar para qué valores de $a \in \mathbb{C}$ el polinomio $f = X^8 - 2X^4 + a$ tiene raíces múltiples en $\mathbb{C}$.

  Sea $x \in \mathbb{C}$ una raíz múltiple. Equivalentemente, $f(x) = f'(x) = 0$. Es decir, dado que $f' = 8X^7 - 8X^3$, $8x^7 - 8x^3 = 8x^3(x^4 - 1) = 0$. O sea $x = 0$ o $x^4 = 1$.

  - $f(0) = 0 \Leftrightarrow a = 0$: en ese caso $f = X^8 - 2X^4 = X^4(X^4 - 2)$, o sea f tiene la raíz 0 con multiplicidad 4.
  - Si $x^4 = 1$, entonces

    $$f(x) = x^8 - 2x^4 + a = (x^4)^2 - 2x^4 + a = 1 - 2 \cdot 1 + a = -1 + a$$

    implica que $f(x) = 0 \Leftrightarrow a = 1$. Por lo tanto $f = X^8-2X^4+1 = (X^4 - 1)^2$ tiene claramente la raíz 1 que es múltiple.

Se puede ser más explícito cuando se trabaja sobre $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$ (pero atención, el argumento no es válido para los cuerpos finitos $\mathbb{Z}/p\mathbb{Z}$).

Proposición 7.2.9. (Multiplicidad en f y multiplicidad en f'.)
Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, sea $x \in K$ y sea $m \in \mathbb{N}$. Entonces

$$\text{mult}(x; f) = m \quad \Longleftrightarrow \quad f(x) = 0 \;\; y \;\; \text{mult}(x; f') = m - 1.$$

Demostración.

($\Rightarrow$)

$$\begin{aligned}
\text{mult}(x;f) = m \iff & \exists\, q \in K[X] \text{ tal que } f = (X-x)^m\, q \text{ con } q(x) \neq 0 \\
\implies & f' = m(X-x)^{m-1}q + (X-x)^m q' \\
& = (X-x)^{m-1}\big(m\,q + (X-x)\,q'\big) \\
\implies & f' = (X-x)^{m-1}h, \\
& \text{donde } h = m\,q + (X-x)\,q' \in K[X] \text{ es tal que} \\
& h(x) = m\,q(x) \neq 0 \text{ pues } q(x) \neq 0.
\end{aligned}$$

Por lo tanto, $f(x) = 0$ y $\text{mult}(x;f') = m-1$.

(Este argumento no es válido en un cuerpo finito $\mathbb{Z}/p\mathbb{Z}$ si $p \mid m$ pues en ese caso $h(x) = 0$.)

($\Leftarrow$) Queremos probar que si $f(x) = 0$ y $\text{mult}(x;f') = m-1$, entonces $\text{mult}(x;f) = m$. Como $f(x) = 0$, x es raíz de f con cierta multiplicidad $k \geq 1$ (y queremos probar que en realidad $k = m$). Por lo tanto por la implicación que acabamos de probar, $\text{mult}(x;f') = k-1$. Pero por hipótesis, $\text{mult}(x;f') = m-1$, de lo cual se deduce $k-1 = m-1$ y por lo tanto $k = m$ como se quería probar. □

Se obtiene el corolario siguiente en términos del máximo común divisor entre f y f'.

Corolario 7.2.10. (Multiplicidad en f y multiplicidad en $(f : f')$.)

Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, sea $x \in K$ y sea $m \geq 2$. Entonces

$$\text{mult}(x;f) = m \quad \iff \quad \text{mult}(x;(f:f')) = m-1.$$

Demostración.

($\Rightarrow$) Tenemos que probar que $(X-x)^{m-1} \mid (f : f')$ pero $(X-x)^m \nmid (f : f')$. Como $\text{mult}(x;f) = m$, entonces $\text{mult}(x;f') = m-1$ por la proposición anterior, y por lo tanto $(X-x)^{m-1} \mid f'$. Por otro lado $(X-x)^{m-1} \mid f$ también pues $(X-x)^m \mid f$, con lo cual $(X-x)^{m-1} \mid (f : f')$. Pero $(X-x)^m \nmid (f : f')$ pues si $(X-x)^m$ dividiera a $(f : f')$, dividiría en particular a f', lo que contradice que $\text{mult}(x;f') = m-1$.

($\Leftarrow$) $\text{mult}(x;(f:f')) = m-1$ implica en particular que $(X-x)^{m-1} \mid f$, y como $m \geq 2$ entonces $m-1 \geq 1$, lo que implica $f(x) = 0$. Por otro lado $(X-x)^{m-1} \mid f'$ y por lo tanto $\text{mult}(x;f') = k \geq m-1$. Estos dos hechos implican por la proposición anterior que $\text{mult}(x;f) = k+1 \geq m$. Ahora bien, por ($\Rightarrow$), $\text{mult}(x;f) = k+1 \geq m \geq 2$ implica $\text{mult}(x;(f:f')) = k$. Pero por hipótesis $\text{mult}(x;(f:f')) = m-1$, o sea $k = m-1$ y por lo tanto $k+1 = m$, es decir $\text{mult}(x;f) = m$ como se quería probar. □

Finalmente podemos presentar también la importante caracterización de la multiplicidad en términos de la derivadas.

Proposición 7.2.11. (Raíz de multiplicidad m y derivadas hasta orden m.)

Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, sea $x \in K$ y sea $m \in \mathbb{N}$. Entonces

$$\text{mult}(x; f) = m \iff \begin{cases} f(x) = 0 \\ f'(x) = 0 \\ \vdots \\ f^{(m-1)}(x) = 0 \\ f^{(m)}(x) \neq 0. \end{cases}$$

Demostración. Por inducción en $m \in \mathbb{N}$:

$p(m)$: Dado $g \in K[X]$,

$$x \in K \text{ es t.q. } \text{mult}(x; g) = m \iff \begin{cases} g(x) = 0 \\ g'(x) = 0 \\ \vdots \\ g^{(m-1)}(x) = 0 \\ g^{(m)}(x) \neq 0. \end{cases}$$

- Caso base, $m = 1$: $p(1)$ es V? Sí pues $\text{mult}(x; g) = 1 \Leftrightarrow g(x) = 0$ y $g'(x) \neq 0$ por la Proposicíón 7.2.8.

- Paso inductivo, $p(k)$ V $\rightarrow$ $p(k+1)$ V:

  Por la Proposición 7.2.9,

  $$\text{mult}(x, f) = k + 1 \Leftrightarrow f(x) = 0 \text{ y } \text{mult}(x, f') = k.$$

  Por HI, para $g = f'$ se tiene que

  $$f'(x) = 0, (f')'(x) = 0, \ldots, (f')^{(k-1)}(x) = 0 \text{ y } (f')^{(k)}(x) \neq 0,$$

  es decir

  $$f'(x) = 0, f''(x) = 0, \ldots, f^{(k)}(x) = 0 \text{ y } f^{(k+1)}(x) \neq 0.$$

  Así concluimos

  $$\text{mult}(x, f) = k + 1 \Leftrightarrow f(x) = 0, f'(x) = 0, \ldots, f^{(k)}(x) = 0 \text{ y } f^{(k+1)}(x) \neq 0.$$

  Hemos probado el paso inductivo.

Por lo tanto $p(m)$ es Verdadera para todo $m \in \mathbb{N}$. □

7.2.2 Cantidad de raíces en K.

Vamos a probar ahora que un polinomio $f \in K[X]$ no nulo no puede tener más raíces en el cuerpo K, aún contadas con su multiplicidad, que su grado.

Proposición 7.2.12. (Raíces de f y factores.)

Sea $f \in K[X]$ no nulo.

- *Sean $x_1, x_2 \in K$ raíces* distintas *de f tales que* $\text{mult}(x_1; f) = m_1$ *y* $\text{mult}(x_2; f) = m_2$. *Entonces* $(X - x_1)^{m_1}(X - x_2)^{m_2} \mid f$.
- *Sean $x_1, \ldots, x_r \in K$ raíces* distintas *de f tales que*

$$\text{mult}(x_1; f) = m_1, \ldots, \text{mult}(x_r; f) = m_r.$$

Entonces

$$(X - x_1)^{m_1} \cdots (X - x_r)^{m_r} \mid f.$$

Demostración. • Esto es porque $(X - x_1)^{m_1}$ y $(X - x_2)^{m_2}$ son polinomios coprimos al ser potencias de polinomios irreducibles distintos. Luego,

$$(X - x_1)^{m_1} \mid f \text{ y } (X - x_2)^{m_2} \mid f \implies (X - x_1)^{m_1}(X - x_2)^{m_2} \mid f.$$

- Por inducción en la cantidad de raíces distintas.

□

En esas condiciones se tiene que si $f \neq 0$, $\text{gr}\left((X - x_1)^{m_1} \cdots (X - x_r)^{m_r}\right) \leq \text{gr}(f)$, es decir $m_1 + \cdots + m_r \leq \text{gr}(f)$. Se obtuvo:

Proposición 7.2.13. (Cantidad de raíces en K.)

Sea K un cuerpo y sea $f \in K[X]$ un polinomio no nulo *de grado n. Entonces f tiene a lo sumo n raíces en K contadas con multiplicidad.*

Esto implica que sobre un cuerpo *infinito* K, dos polinomios son iguales si y sólo si coinciden como función de K en K.

Corolario 7.2.14. (Igualdad de polinomios.)

1. *Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, y sean $f, g \in K[X]$. Entonces*

$$f = g \text{ en } K[X] \iff f(x) = g(x), \ \forall\, x \in K.$$

2. *¡Ojo que no esto no es cierto en $\mathbb{Z}/p\mathbb{Z}[X]$! Por ejemplo el polinomio $X^p - X$ coincide con el polinomio 0 en todos los elementos de $\mathbb{Z}/p\mathbb{Z}$ (verificarlo) pero sin embargo no son el mismo polinomio...*

Demostración. Probamos solo (i), y alcanza con probar la vuelta, ya que si dos polinomios son iguales, tienen los mismos coeficientes y por lo tanto coinciden en todos los valores de K.
Supongamos entonces que $f, g \in K[X]$ satisfacen $f(x) = g(x)$, $\forall\, x \in K$, y definamos el polinomio $h := f - g \in K[X]$. Por lo tanto,

$$h(x) = f(x) - g(x) = 0, \ \forall\, x \in K.$$

O sea ¡todos los elementos de K (que es infinito al ser $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$) son raíces de h! Pero esto es imposible si $h \neq 0$ pues h no puede tener más raíces que su grado.... Por lo tanto $h = 0$ en $K[X]$, es decir, $f = g$ en $K[X]$. □

7.2.3 Cálculo de raíces en $\mathbb{Q}$ de polinomios en $\mathbb{Q}[X]$.

Un hecho notorio es que se pueden encontrar todas las raíces racionales de un polinomio $f \in \mathbb{Q}[X]$ por medio de un algoritmo. Este hecho es una consecuencia de que todo número entero $a \in \mathbb{Z} \setminus \{0\}$ tiene un número finito de divisores posibles, que se pueden calcular.

Sea $f = a_n X_n + \cdots + a_0 \in \mathbb{Q}[X]$. Entonces existe $c \in \mathbb{Z} \setminus \{0\}$ tal que $g = c\, f \in \mathbb{Z}[X]$, es decir g tiene todos sus coeficientes enteros (por ejemplo, eligiendo c como el mínimo común múltiplo de los denominadores de los coeficientes de f), y además las raíces de f claramente coinciden con las de g.

Por ejemplo, $f = \frac{3}{2}X^5 - \frac{1}{3}X^4 + X^2 - \frac{5}{4} \in \mathbb{Q}[X]$ y $g = 12\, f = 18X^5 - 4X^4 + 12X^2 - 15 \in \mathbb{Z}[X]$ tienen exactamente las mismas raíces.

Por consiguiente para encontrar las raíces racionales de un polinomio en $\mathbb{Q}[X]$, nos podemos restringir a estudiar cómo encontrar las raíces racionales de un polinomio en $\mathbb{Z}[X]$.

Lema 7.2.15. (Lema de Gauss.)

Sea $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ con $a_n,\ a_0 \neq 0$. Si $\frac{\alpha}{\beta} \in \mathbb{Q}$ es una raíz racional de f, con α y $\beta \in \mathbb{Z}$ coprimos, *entonces $\alpha \,|\, a_0$ y $\beta \,|\, a_n$.*

Demostración.

$$\begin{aligned} f\left(\frac{\alpha}{\beta}\right) = 0 \quad &\iff \quad a_n \left(\frac{\alpha}{\beta}\right)^n + a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \cdots + a_1\left(\frac{\alpha}{\beta}\right) + a_0 = 0 \\ &\iff \quad \frac{a_n\alpha^n + a_{n-1}\alpha^{n-1}\beta + \cdots + a_1\alpha\beta^{n-1} + a_0\beta^n}{\beta^n} = 0 \\ &\iff \quad a_n\alpha^n + a_{n-1}\alpha^{n-1}\beta + \cdots + a_1\alpha\beta^{n-1} + a_0\beta^n = 0. \end{aligned}$$

Por lo tanto, $\alpha\left(a_n\alpha^{n-1}+\cdots+a_1\beta^{n-1}\right)=-a_0\beta^n$.

Esto implica $\alpha\,|\,-a_0\beta^n$ en $\mathbb{Z}$. Pero al ser α y β enteros coprimos, α es coprimo con β^n también, y por lo tanto $\alpha\,|\,a_0$.

De la misma manera, $\beta\left(a_{n-1}\alpha^{n-1}+\cdots+a_0\beta^{n-1}\right)=-a_n\alpha^n$ implica que $\beta\,|\,-a_n\alpha^n$ pero al ser coprimo con α, resulta $\beta\,|\,a_n$. □

Observación 7.2.16. (Algoritmo para calcular las raíces en $\mathbb{Q}$ de $f\in\mathbb{Z}[X]$.)

En las condiciones del teorema anterior, el Lema de Gauss implica que si se construye el conjunto (finito) $\mathcal{N}$ (por numerador) de los divisores positivos y negativos de a_0 y el conjunto $\mathcal{D}$ (por denominador) de los de a_n, las raíces del polinomio f se encuentran en el conjunto de todas las fracciones coprimas $\frac{\alpha}{\beta}$, eligiendo α en $\mathcal{N}$ y β en $\mathcal{D}$. Chequeando para cada fracción $\frac{\alpha}{\beta}$ así construída si $f(\frac{\alpha}{\beta})=0$, se obtienen todas las raíces racionales de f.

Simplemente hay que tener un poco de cuidado en que este procedimiento no aclara la multiplicidad de cada raíz.

Ejemplo: Hallar las raíces racionales del polinomio racional

$$f=X^8+\frac{8}{3}X^7+\frac{1}{3}X^6-\frac{14}{3}X^5-\frac{14}{3}X^4-\frac{4}{3}X^3.$$

Limpiando los denominadores de f se obtiene el polinomio entero g con las mismas raíces:

$$g=3X^8+8X^7+X^6-14X^5-14X^4-4X^3=X^3(3X^5+8X^4+X^3-14X^2-14X-4).$$

Claramente, $\mathrm{mult}(0;g)=3$ (y por lo tanto $\mathrm{mult}(0;f)=3$ también pues $g=3\,f$), y las restantes raíces racionales de g (o f) son las de

$$h=3X^5+8X^4+X^3-14X^2-14X-4.$$

Aquí, $a_0=-4$ y $a_n=3$.

Los divisores de a_0 son $\pm1,\pm2,\pm4$ y los divisores de a_n son $\pm1,\pm3$, luego las raíces racionales se buscan en el conjunto :

$$\{\,\pm1,\pm2,\pm4,\pm\frac{1}{3},\pm\frac{2}{3},\pm\frac{4}{3}\,\}$$

Chequeando se obtiene que $h(-1)=0$ y $h(-2/3)=0$, y éstas son las únicas raíces racionales (distintas) de h.

Para conocer con qué multiplicidad son éstas raíces de h, se puede o bien dividir h por $(X+1)(X+\frac{2}{3})$ y volver a evaluar el cociente en -1 y $-2/3$, o bien también se puede derivar h:

$h' = 15X^4 + 32X^3 + 3X^2 - 28X - 14$ y se tiene que $h'(-1) = 0$ mientras que $h'(-2/3) \neq 0$.

O sea -1 es raíz de multiplicidad ≥ 2 y $-2/3$ es raíz simple.

Volviendo a derivar h: $h'' = 60X^3 + 96X + 6X - 28$ y $h''(-1) \neq 0$.

Se concluye que -1 es raíz doble de h.

Finalmente la factorización de h en $\mathbb{Q}[X]$ es:

$$h = 3(X+1)^2(X+\frac{2}{3})(X^2-2)$$

ya que $X^2 - 2$ es irreducible en $\mathbb{Q}[X]$.

Y dado que $f = \frac{1}{3}X^3\, h$, obtenemos la siguiente factorización de f en $\mathbb{Q}[X]$:

$$f = X^3(X+1)^2(X+\frac{2}{3})(X^2-2).$$

Observación 7.2.17. El Lema de Gauss provee un algoritmo para calcular todas las raíces racionales de un polinomio racional, pero se ve claramente que éste es extremadamente costoso, pues hay que evaluar el polinomio de entrada en un gran número de fracciones $\dfrac{\alpha}{\beta}$ (la cantidad de fracciones está relacionada con la cantidad de divisores de a_0 y a_n).

7.3 Factorización en $K[X]$.

Como ya se mencionó, todo polinomio no constante en $K[X]$ se factoriza en forma única como producto de polinomios irreducibles mónicos en $K[X]$, multiplicados por su coeficiente principal en $K^\times$. Estudiaremos en lo que sigue más en detalle como puede ser esa factorización según quién es el cuerpo K.

7.3.1 Polinomios cuadráticos en $K[X]$.

Sea $f = aX^2 + bX + c$ con $a, b, c \in K$, $a \neq 0$.

Como f tiene grado 2, es reducible si y solo si tiene un factor en $K[X]$ de grado 1, que podemos asumir mónico de la forma $X - x$ con $x \in K$. Así que en este caso f es reducible en $K[X]$ si y solo si f tiene una raíz $x \in K$.

Asumimos en lo que sigue que $1 + 1 \neq 0$ en K, es decir $2 \neq 0 \in K$ (por ejemplo $K \neq \mathbb{Z}/2\mathbb{Z}$) para que tenga sentido dividir por 2 en la cuenta que hacemos a continuación.

Luego

$$\begin{aligned} f &= a\left(X^2 + \frac{b}{a}X + \frac{c}{a}\right) \\ &= a\left(\left(X + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right) \\ &= a\left(\left(X + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right). \end{aligned}$$

Se define el *discriminante* de f como $\Delta = \Delta(f) := b^2 - 4ac \in K$.

Si existe $\omega \in K$ tal que $\omega^2 = \Delta$, o sea tal que $\left(\frac{w}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$, se tiene que :

$$f = a\left(\left(X + \frac{b}{2a}\right)^2 - \left(\frac{\omega}{2a}\right)^2\right) = a\left(X + \frac{b}{2a} - \frac{\omega}{2a}\right)\left(X + \frac{b}{2a} + \frac{\omega}{2a}\right)$$

por diferencia de cuadrados. Por lo tanto

$$f = a\left(X - \frac{-b + \omega}{2a}\right)\left(X - \frac{-b - \omega}{2a}\right),$$

lo que implica, dado que K es un cuerpo, $f(x) = 0 \Leftrightarrow x - \frac{-b + \omega}{2a} = 0$ o $x - \frac{-b - \omega}{2a} = 0$. Es decir, se obtienen las 2 raíces (a lo mejor la misma repetida si $\omega = 0$):

$$x_\pm = \frac{-b \pm \omega}{2a}.$$

Lo que probamos hasta ahora es que si $\Delta \in K$ es un cuadrado en K, entonces el polinomio cuadrático $f = aX^2 + bX + c$ tiene (al menos) una raíz en K. Podemos probar la recíproca también: que si f tiene una raíz en K, entonces Δ es un cuadrado en K:

En efecto, si $f = aX^2 + bX + c$ tiene una raíz $x_1 \in K$, $X - x_1 \mid f$ y el cociente, que tiene grado 1, se puede escribir en la forma $a(X - x_2)$. Por lo tanto

$$f = a(X - x_1)(X - x_2) = aX^2 - a(x_1 + x_2)X + ax_1x_2.$$

Igualando coeficiente a coeficiente, resulta que $b = -a(x_1 + x_2)$ y $c = ax_1x_2$. Por lo tanto,

$$\begin{aligned} \Delta = b^2 - 4ac &= a^2(x_1 + x_2)^2 - 4a^2x_1x_2 \\ &= a^2(x_1^2 + x_2^2 - 2x_1x_2) = \big(a(x_1 - x_2)\big)^2 = \omega^2 \end{aligned}$$

donde $\omega = a(x_1 - x_2) \in K$: Δ resulta ser un cuadrado en K!

Hemos probado el siguiente resultado:

Proposición 7.3.1. (Polinomios cuadráticos en $K[X]$.)

Sea K un cuerpo y sea $f = aX^2+bX+c \in K[X]$, con $a \neq 0$, un polinomio cuadrático. Entonces f es reducible en $K[X]$ si y solo si f tiene una raíz en K.

Si $2 \neq 0$ en K, f es reducible en $K[X]$ (o equivalentemente tiene raíz en K) si y solo si $\Delta = b^2 - 4ac$ es un cuadrado en K. En ese caso, sea $\omega \in K$ tal que $\omega^2 = \Delta$. Entonces las raíces de f en K son

$$x_\pm = \frac{-b \pm \omega}{2a}$$

(donde si $\Delta = 0$, $x_+ = x_-$), y $f = a(X - x_+)(X - x_-)$ es la factorización de f en $K[X]$.

<u>*Ejemplos:*</u> Sea $f = aX^2 + bX + c \in K[X]$, con $a \neq 0$, un polinomio cuadrático.

- Cuando $K = \mathbb{C}$, sabemos que siempre existe $\omega \in \mathbb{C}$ tal que $\omega^2 = \Delta \in \mathbb{C}$ (pues todo número complejo tiene raíz cuadrada), luego todo polinomio de grado 2 es reducible en $\mathbb{C}[X]$, o equivalentemente tiene dos raíces en $\mathbb{C}$ (que pueden ser distintas o la misma repetida dos veces cuando $\Delta = 0$).

  Por ejemplo si $f = X^2 - iX + (-1 + i)$, entonces $\Delta = 3 - 4i = \omega^2$ con $\omega = 2 - i$. Se obtiene

  $$x_+ = \frac{i + (2 - i)}{2} = 1 \quad \text{y} \quad x_- = \frac{i - (2 - i)}{2} = -1 + i.$$

  La factorización de f en polinomios irreducibles en $\mathbb{C}[X]$ es

  $$f = (X - x_+)(X - x_-) = (X - 1)(X - (-1 + i)).$$

- Cuando $K = \mathbb{R}$, existe $\omega \in \mathbb{R}$ tal que $\omega^2 = \Delta$ si y sólo si $\Delta \geq 0$. Por lo tanto, f es reducible en $\mathbb{R}[X]$ si y solo si $\Delta \geq 0$. Los polinomios cuadráticos tales que $\Delta < 0$ son irreducibles en $\mathbb{R}[X]$, como por ejemplo los polinomios de la forma $X^2 + c$ con $c \in \mathbb{R}$ positivo, y los que son tales que $\Delta \geq 0$ son reducibles en $\mathbb{R}[X]$, o equivalentemente en este caso tienen dos raíces reales contadas con multiplicidad.

- Cuando $K = \mathbb{Q}$, f es reducible en $\mathbb{Q}[X]$ (o tiene raíz en $\mathbb{Q}$) si y solo si Δ es un cuadrado en $\mathbb{Q}$. Existen luego polinomios de grado 2 irreducibles en $\mathbb{Q}[X]$ (o equivalentemente en este caso sin raíces racionales), como por ejemplo los polinomios de la forma $X^2 + c$ con $c > 0$, o también $X^2 - 2$.

- Cuando $K = \mathbb{Z}/p\mathbb{Z}$ con p primo $\neq 2$, f puede ser reducible o no según si Δ es un cuadrado o no en $\mathbb{Z}/p\mathbb{Z}$. Por ejemplo el polinomio $f = X^2 + \overline{2}X + \overline{5}$ es irreducible en $\mathbb{Z}/7\mathbb{Z}$ pues $\Delta = \overline{2}^2 - 4 \cdot \overline{5} = \overline{4 - 20} = \overline{-16} = \overline{5}$ no es un cuadrado en $\mathbb{Z}/7\mathbb{Z}$, mientras que el polinomio $X^2 + X + \overline{1}$ es reducible pues $\Delta = \overline{1}^2 - 4 \cdot \overline{1} = \overline{-3} = \overline{4} = \overline{2}^2$ es un cuadrado en $\mathbb{Z}/7\mathbb{Z}$ (aquí $\omega = \overline{2}$): se tiene

$$x_+ = \frac{-\overline{1} + \overline{2}}{2} = \frac{\overline{1}}{2} = \overline{4} \quad \text{y} \quad x_- = \frac{-\overline{1} - \overline{2}}{2} = \frac{\overline{-3}}{2} = \frac{\overline{4}}{2} = \overline{2},$$

y por lo tanto $f = (X - x_+)(X - x_-) = (X - \overline{4})(X - \overline{2})$ es la factorización de f en $\mathbb{Z}/7\mathbb{Z}$.

- Cuando $K = \mathbb{Z}/2\mathbb{Z}$, hay pocos polinomios de grado 2. Estos son $f_1 = X^2$, $f_2 = X^2 + \overline{1}$, $f_3 = X^2 + X$ y $f_4 = X^2 + X + \overline{1}$. Se puede ver que los tres primeros son reducibles (por ejemplo $f_2 = (X - \overline{1})^2$) mientras que el último no lo es, pues ni $\overline{0}$ ni $\overline{1}$ son raíces de f_4. (Sin embargo $\Delta = \overline{1} - 4 \cdot \overline{1} = \overline{1}$ es un cuadrado en $\mathbb{Z}/2\mathbb{Z}$.)

7.3.2 Polinomios en $\mathbb{C}[X]$ y el Teorema Fundamental del Álgebra.

Acabamos de ver que todo polinomio cuadrático $f = aX^2 + bX + c \in \mathbb{C}[X]$, con $a \neq 0$, tiene exactamente 2 raíces en $\mathbb{C}$ (contadas con multiplicidad), que son

$$z_\pm = \frac{-b \pm \omega}{2a} \quad \text{donde } \omega \in \mathbb{C} \text{ es tal que } \omega^2 = b^2 - 4ac,$$

y por lo tanto el polinomio f se factoriza en $\mathbb{C}[X]$ en la forma

$$f = (X - z_+)(X - z_-).$$

También podemos deducir inmediatamente de nuestro estudio sobre las raíces n-ésimas de números complejos en el capítulo anterior que todo polinomio de la forma $X^n - z$ en $\mathbb{C}[X]$ tiene exactamente n raíces en $\mathbb{C}$ (contadas con multiplicidad):

- Si $z = 0$, el polinomio es X^n que tiene la raíz 0 con multiplicidad n.
- Si $z \neq 0$, determinar las raíces de $X^n - z$ equivale a hallar los $\omega \in \mathbb{C}$ tales que $\omega^n - z = 0$, es decir hallar los $\omega \in \mathbb{C}$ tales que $\omega^n = z$, o sea determinar las raíces n-ésimas de z. Sabemos que $z \neq 0$ tiene n raíces n-ésimas distintas en $\mathbb{C}$, que son $\omega_0, \omega_1, \ldots, \omega_{n-1}$ descritas en el capítulo anterior. Por lo tanto estas n raíces son simples (ya que el

polinomio tiene a lo sumo n raíces contadas con multiplicidad), y el polinomio $X^n - z$ se factoriza en $\mathbb{C}[X]$ en la forma

$$X^n - z = (X - \omega_0) \cdots (X - \omega_{n-1}).$$

De hecho vale un resultado general al respecto, conocido como el Teorema Fundamental del Álgebra: todo polinomio no constante en $\mathbb{C}[X]$ tiene (al menos) una raíz en $\mathbb{C}$, o, lo que es equivalente aplicando divisiones sucesivas, todo polinomio de grado $n \geq 1$ en $\mathbb{C}[X]$ tiene exactamente n raíces contadas con multiplicidad! (Se dice que $\mathbb{C}$ es *algebraicamente cerrado*.)

Teorema 7.3.2. (Teorema Fundamental del Álgebra.)

Sea $f \in \mathbb{C}[X]$ un polinomio no constante. Entonces existe $z \in \mathbb{C}$ tal que $f(z) = 0$.

Equivalentemente, todo polinomio no constante en $\mathbb{C}[X]$ de grado n tiene exactamente n raíces contadas con multiplicidad en $\mathbb{C}$.

El Teorema Fundamental del Álgebra es equivalente a que los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de grado 1, de lo cual se deduce la factorización de polinomios en $\mathbb{C}[X]$.

Teorema 7.3.3. (Irreducibles y factorización en $\mathbb{C}[X]$.)

- *Sea $f \in \mathbb{C}[X]$. Entonces f es irreducible en $\mathbb{C}[X]$ si y solo si $\operatorname{gr}(f) = 1$, es decir $f = aX + b \in \mathbb{C}[X]$ con $a \neq 0$.*
- *Sea $f \in \mathbb{C}[X] - \mathbb{C}$. Entonces la factorización en irreducibles de f en $\mathbb{C}[X]$ es de la forma*

  $$f = c\,(X - z_1)^{m_1} \cdots (X - z_r)^{m_r}$$

  donde $z_1, \ldots, z_r \in \mathbb{C}$ son distintos, $m_1, \ldots, m_r \in \mathbb{N}$ y $c \in \mathbb{C}^\times$.

El Teorema Fundamental del Álgebra, que enunciamos en este curso sin demostración (se ven varias demostraciones en nuestra licenciatura en Matemática, pero hacen falta más herramientas que las que disponemos a este nivel) fue enunciado y demostrado en varias etapas a lo largo del tiempo, empezando con el matemático francés Albert Girard quién lo enunció en alguna forma en 1629. Una primera demostración, incompleta, fue esbozada por Jean le Rond D'Alembert en 1746. Aparecieron luego muchas demostraciones entre 1749 y 1795, pero con "agujeros" (argumentos no claros, que necesitan una demostración en sí mismo) ya que todas asumían que las raíces existen en "algún lado". Gauss también presentó una demostración con un agujero en 1799. En 1814, el librero y matemático amateur de origen suizo Jean-Robert Argand publicó la primera demostración completa, y

luego Gauss presentó otra en 1816. Existen hoy en día numerosas demostraciones distintas de este teorema, aunque todas ellas usan algún ingrediente indispensable de la rama de la matemática que se suele llamar *Análisis*, la completitud de los números reales en una u otra forma (como por ejemplo el Teorema de Bolzano, que establece que toda función continua en $\mathbb{R}$ que toma un valor positivo y un valor negativo obligatoriamente toma el valor 0).

Ejemplos: (para información nomás)

- f de grado 3: (Scipione del Ferro 1515?, Tartaglia 1535, Cardano 1545.)

$$f = aX^3 + bX^2 + cX + d \ \in \mathbb{C}[X], \quad a \neq 0.$$

Haciendo el cambio de variables $Y = X - \dfrac{b}{3a}$, el problema se traduce en buscar las raíces del polinomio :

$$g = Y^3 + pY + q.$$

Buscando las soluciones de la forma $y = u + v$, con $u^3 + v^3 = -q$ y $u^3v^3 = -\dfrac{p^3}{27}$, se observa que u^3 y v^3 son las raíces del polinomio (*resolvente*):

$$Z^2 + qZ - \frac{p^3}{27}.$$

Por lo tanto hay 3 posibilidades para u y 3 posibilidades para v, o sea 6 posibilidades para $y = u + v$: las 3 raíces y del polinomio son 3 de entre esas 6 posibilidades, las 3 que son dadas por las elecciones de u y v que satisfacen $u\,v = -p/3$.

Pero puede ocurrir que calcular las raíces de un polinomio de esa forma puede dar una expresión muy engorrosa para algo mucho más sencillo! Por ejemplo la raíz $x = 1$ del polinomio X^3+X-2 aparece expresada en la forma

$$1 = \sqrt[3]{1 + \frac{2}{9}\sqrt{21}} + \sqrt[3]{1 - \frac{2}{9}\sqrt{21}}.$$

- f de grado 4: (Ludovico Ferrari, 1540?)

$$f = X^4 + pX^2 + qX + r.$$

Las 4 raíces son del tipo $\alpha = \frac{1}{2}(\pm u \pm v \pm \omega)$, donde $-u^2$, $-v^2$, $-\omega^2$ son las tres raíces del polinomio *resolvente*:

$$Z^3 - 2pZ^2 + (p^2 - 4r)Z + q^2.$$

La condición aquí para determinar las 4 raíces complejas entre las 8 posibles expresiones es $(\pm u)(\pm v)(\pm\omega) = -q$.

Hasta ahora se obtuvieron las raíces complejas de polinomios $f \in \mathbb{C}[X]$ de grado ≤ 4, por medio de fórmulas que se obtienen a partir de los coeficientes del polinomio f mediante las operaciones $+$, $-$, $\cdot$, $/$ y extracción de raíces cuadradas y cúbicas.

La pregunta natural es entonces : ¿Existirá para cada polinomio f de grado arbitrario una fórmula para las raíces que involucre los coeficientes de f y las operaciones $+$, $-$, $\cdot$, $/$ y extracción de raíces n-ésimas para algunos n adecuados?

Durante más de 200 años, muchos matemáticos buscaron esas fórmulas. Pero a principios del S. XIX el joven matemático noruego Niels Abel, 1802-1829, probó que sorprendentemente la respuesta es NO:

Teorema 7.3.4. (Abel, 1824?)

No existe ninguna fórmula que describa las raíces (complejas) de un polinomio general cualquiera $f \in \mathbb{C}[X]$ de grado ≥ 5 a partir de sus coeficientes y de las operaciones elementales $+$, $-$, $\cdot$, $/$ y extracciones de raíces n-ésimas.

El aún más joven matemático francés Evariste Galois, 1811-1832, caracterizó en 1832, la noche antes de morir, al batirse en duelo, cuáles son los polinomios de grado ≥ 5 para los cuales existe tal fórmula (aunque no es fácilmente deducible de los coeficientes del polinomio, sino que tiene que ver con cierto grupo asociado a él).

Esto es parte de la hoy llamada Teoría de Galois, que además de su importancia en matemática, constituye también la base del funcionamiento de sistemas de navegación satelital como el GPS por ejemplo. Sus resultados fueron entendidos recién en 1846 por el matemático francés Joseph Liouville, 1809-1882.

Tanto Abel como Galois fueron los iniciadores de la Teoría de Grupos.

7.3.3 Polinomios en $\mathbb{R}[X]$.

Sabemos que un polinomio en $\mathbb{R}[X]$ de grado $n \geq 1$ tiene a lo sumo n raíces contadas con multiplicidad. También sabemos que si $f \in \mathbb{R}[X]$ tiene grado

≥ 2 y tiene una raíz $x \in \mathbb{R}$, entonces f es reducible en $\mathbb{R}[X]$ pues $X-x \mid f$ ($X-x$ es un factor no trivial de f en $\mathbb{R}[X]$). Pero ser reducible en $\mathbb{R}[X]$ no implica tener raíz en $\mathbb{R}$: existen polinomios reducibles en $\mathbb{R}[X]$ de cualquier grado (par) que no tienen raíces reales, como por ejemplo el polinomio $(X^2+1)^n$, $\forall\, n \geq 2$. Sin embargo no existen polinomios irreducibles en $\mathbb{R}[X]$ de cualquier grado. Es lo que estudiaremos a continuación, gracias al estudio ya realizado de los polinomios en $\mathbb{C}[X]$.

Primeramente volvamos a mencionar la consecuencia siguiente del famoso Teorema de Bolzano, probado en 1817 por el matemático bohemio Bernard Bolzano, 1781-1848.

Proposición 7.3.5. (Polinomios reales de grado impar.)

Sea $f \in \mathbb{R}[X]$ de grado impar. *Entonces f tiene al menos una raíz en $\mathbb{R}$.*

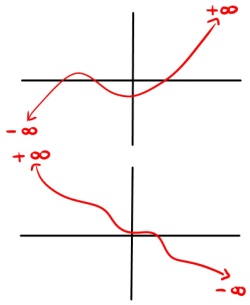
Demostración. Sea $f = a^n X^n + \cdots + a_0 \in \mathbb{R}[X]$, con n impar.

Si $a_n > 0$, entonces :

$$\lim_{x\to+\infty} f(x) = +\infty \quad \text{y} \quad \lim_{x\to-\infty} f(x) = -\infty :$$

Y si $a_n < 0$ se tiene :

$$\lim_{x\to+\infty} f(x) = -\infty \quad \text{y} \quad \lim_{x\to-\infty} f(x) = +\infty :$$



En ambos casos los signos son opuestos, y por lo tanto, por el Teorema de Bolzano (y dado que $f : \mathbb{R} \to \mathbb{R}$ define una función continua), debe existir $x \in \mathbb{R}$ tal que $f(x) = 0$. □

Pero se puede ser más explícito y precisar un poco más cuántas raíces reales puede tener f.

Proposición 7.3.6. (Raíces complejas conjugadas de polinomios reales.)

Sea $f \in \mathbb{R}[X]$, y sea $z \in \mathbb{C} - \mathbb{R}$ un número complejo no real. Entonces

1. $f(z) = 0 \iff f(\overline{z}) = 0$.
2. *Para todo* $m \in \mathbb{N}$, $\text{mult}(z; f) = m \iff \text{mult}(\overline{z}; f) = m$.
3. $(X - z)(X - \overline{z})$ *es un polinomio irreducible de* $\mathbb{R}[X]$.
4. $f(z) = 0 \implies (X - z)(X - \overline{z}) \mid f$ *en* $\mathbb{R}[X]$.

5. $\text{mult}(z;f) = m \implies \big((X-z)(X-\overline{z})\big)^m \mid f$ *en* $\mathbb{R}[X]$.

Demostración. 1. Sea $f = a_nX^n + \cdots + a_0 \in \mathbb{R}[X]$. Entonces

$$\begin{aligned} f(z) = 0 &\iff a_nz^n + \cdots + a_1z + a_0 = 0 \\ &\iff \overline{a_nz^n + \cdots + a_1z + a_0} = 0 \\ &\iff \overline{a_n}\,\overline{z}^n + \cdots + \overline{a_1}\,\overline{z} + \overline{a_0} = 0 \\ &\iff a_n\overline{z}^n + \cdots + a_1\overline{z} + a_0 = 0 \quad \text{pues } a_0,\ldots,a_n \in \mathbb{R} \\ &\iff f(\overline{z}) = 0 \end{aligned}$$

2. Por la Proposición 7.2.11,

$$\text{mult}(z;f) = m \iff f(z) = f'(z) = \cdots = f^{(m-1)}(z) = 0, f^{(m)}(z) \neq 0.$$

Pero $f', \ldots, f^{(m-1)}$, $f^{(m)}$ también son polinomios en $\mathbb{R}[X]$. Por lo tanto, por (1):

$$\begin{aligned} f(z) = \cdots = f^{(m-1)}(z) = 0, f^{(m)}(z) \neq 0 &\iff f(\overline{z}) = \cdots = f^{(m-1)}(\overline{z}) = 0, f^{(m)}(\overline{z}) \neq 0 \\ &\iff \text{mult}(\overline{z};f) = m. \end{aligned}$$

3. $(X-z)(X-\overline{z}) = X^2 - 2\,\Re e(z) + |z|^2 \in \mathbb{R}[X]$ pues sus coeficientes pertenecen a $\mathbb{R}$, y es irreducible por ser de grado 2 y no tener raíces reales.

4. $f(z) = 0 \Rightarrow f(\overline{z}) = 0$, por lo tanto $X - z \mid f$ y $X - \overline{z} \mid f$ en $\mathbb{C}[X]$. Luego, como son polinomios coprimos, su producto $(X-z)(X-\overline{z}) \mid f$ en $\mathbb{C}[X]$. Pero al ser $f \in \mathbb{R}[X]$ y $(X-z)(X-\overline{z}) \in \mathbb{R}[X]$, se concluye que $(X-z)(X-\overline{z}) \mid f$ en $\mathbb{R}[X]$.

5. Por inducción en $m \geq 1$. El caso base es el inciso anterior. Sea entonces $m > 1$ y sea $z \in \mathbb{C} - \mathbb{R}$ raíz de f de multiplicidad m. Entonces $(X-z)(X-\overline{z}) \mid f \in \mathbb{R}[X]$ y consideremos el cociente $q := \dfrac{f}{(X-z)(X-\overline{z})} \in \mathbb{R}[X]$. Se tiene que $\text{mult}(z;q) = m-1$ y por lo tanto, por hipótesis inductiva, $\big((X-z)(X-\overline{z})\big)^{m-1} \mid q$ en $\mathbb{R}[X]$. Es decir, $\big((X-z)(X-\overline{z})\big)^m \mid f$ en $\mathbb{R}[X]$.

□

La proposición anterior significa que las raíces complejas no reales de un polinomio real f vienen de a pares de complejos conjugados, o sea que un

polinomio real f de grado n, que tiene exactamente n raíces complejas contadas con multiplicidad, tiene un número par de ellas que son complejas no reales, y las restantes automáticamente tienen que ser reales. Por ejemplo, un polinomio real de grado impar tiene un número impar de raíces reales. Más aún, existen algoritmos que calculan la cantidad exacta de raíces reales que tiene un polinomio en $\mathbb{R}[X]$ (como por ejemplo el Algoritmo de Sturm), pero no los vamos a ver aquí. A continuación caracterizamos los polinomios irreducibles de $\mathbb{R}[X]$ y como es la factorización de polinomios en $\mathbb{R}[X]$.

Proposición 7.3.7. (Polinomios irreducibles en $\mathbb{R}[X]$.)

Los polinomios irreducibles en $\mathbb{R}[X]$ son exactamente los siguientes:

- *Los de grado 1, o sea de la forma $aX + b \in \mathbb{R}[X]$ con $a \neq 0$.*
- *Los de grado 2 con discriminante negativo, o sea de la forma*

$$aX^2 + bX + c \in \mathbb{R}[X] \quad con \quad a \neq 0 \quad y \quad \Delta := b^2 - 4ac < 0.$$

Demostración. Claramente los polinomios de grado 1 y los de grado 2 con discriminante negativo son irreducibles. Probemos que son los únicos.

- Si f tiene grado impar > 1, entonces tiene por lo menos una raíz real y por lo tanto es reducible.
- Si f es de grado 2, sabemos que es reducible si y solo si tiene discriminante ≥ 0.
- Si f tiene grado par ≥ 4, o bien tiene alguna raíz real, y en tal caso es reducible, o bien todas sus raíces son complejas no reales y vienen de a pares conjugados. Por lo tanto si z es una de esas raíces, el polinomio real $(X - z)(X - \overline{z})$ divide a f en $\mathbb{R}[X]$, y f resulta ser reducible.

□

Teorema 7.3.8. (Factorización en $\mathbb{R}[X]$.)

Sea $f \in \mathbb{R}[X] - \mathbb{R}$. Entonces la factorización en irreducibles de f en $\mathbb{R}[X]$ es de la forma

$$f = c\,(X - x_1)^{m_1} \dots (X - x_r)^{m_r} (X^2 + b_1 X + c_1)^{n_1} \dots (X^2 + b_s X + c_s)^{n_s}$$

donde $c \in \mathbb{R}^\times$, $r, s \in \mathbb{N}_0$, $m_i, n_j \in \mathbb{N}$ para $1 \leq i \leq r, 1 \leq j \leq s$, $x_1, \dots, x_r \in \mathbb{R}$, $b_1, c_1, \dots, b_s, c_s \in \mathbb{R}$ y $\Delta_j := {b_j}^2 - 4c_j < 0$.

Ejemplo: Factorizar en $\mathbb{R}[X]$ y $\mathbb{C}[X]$ el polinomio $f = X^4 - 2X^3 + X^2 - 4X - 2$ sabiendo que $\sqrt{2}\,i$ es raíz de f:

Como $f \in \mathbb{R}[X]$, por la Proposición 7.3.6, se tiene que $f(\sqrt{2}\,i) = 0 \Leftrightarrow f(-\sqrt{2}\,i) = 0$. Por lo tanto $(X - \sqrt{2}\,i)(X + \sqrt{2}\,i) = X^2 + 2 \mid f$. En efecto, $f = (X^2+2)(X^2 - 2X - 1)$. Las raíces de $X^2 - 2X - 1$ son reales: $1 + \sqrt{2}$ y $1 - \sqrt{2}$. Por lo tanto,

- $f = (X - \sqrt{2}\,i)(X + \sqrt{2}\,i)(X - (1+\sqrt{2}))(X - (1-\sqrt{2}))$ es la factorización de f en $\mathbb{C}[X]$

- $f = (X^2 + 2)(X - (1 + \sqrt{2}))(X - (1 - \sqrt{2}))$ es la factorización de f en $\mathbb{R}[X]$.

7.3.4 Polinomios en $\mathbb{Q}[X]$.

Sabemos que un polinomio en $\mathbb{Q}[X]$ de grado $n \geq 1$ tiene a lo sumo n raíces contadas con multiplicidad. También sabemos que si $f \in \mathbb{Q}[X]$ tiene grado ≥ 2 y tiene una raíz $x \in \mathbb{Q}$, entonces f es reducible en $\mathbb{Q}[X]$ pues $X - x \mid f$ (lo que implica $X - x$ es un factor no trivial de f en $\mathbb{Q}[X]$). Pero ser reducible en $\mathbb{Q}[X]$ no implica tener raíz en $\mathbb{Q}$: existen polinomios reducibles en $\mathbb{Q}[X]$ de cualquier grado que no tienen raíces racionales, como por ejemplo los polinomios $(X^2 - 2)^n$, $\forall\, n \geq 2$ y $(X^2 - 2)(X^3 - 2)$.

Sin embargo la situación no es como en $\mathbb{R}[X]$ donde no existen polinomios irreducibles de grado impar: en $\mathbb{Q}[X]$ se puede probar que existen polinomios irreducibles de cualquier grado, como por ejemplo el polinomio $X^n - 2$, $\forall\, n \in \mathbb{N}$: no sólo el polinomio $X^n - 2$ no tiene raíces en $\mathbb{Q}$ para todo $n \geq 2$, pero más aún no tiene ningún factor en $\mathbb{Q}[X]$ de cualquier grado d, $1 \leq d \leq n - 1$. También se puede probar que para p primo, el polinomio $X^{p-1} + \cdots + X + 1$ es irreducible en $\mathbb{Q}[X]$.

La situación parece desesperada. Pero al menos en $\mathbb{Q}$ existen algoritmos para encontrar (en forma exacta) todas las raíces racionales, como por ejemplo el algoritmo de Gauss, y más aún, también para decidir si el polinomio es irreducible o no en $\mathbb{Q}[X]$, y en caso de ser reducible, determinar su factorización en irreducibles de $\mathbb{Q}[X]$!

Una herramienta que puede ser útil si se tiene más información sobre el polinomio es la proposición siguiente que ayuda a determinar factores irreducibles cuadráticos de un polinomio cuando tiene una raíz real de la forma $a + b\sqrt{d}$ con $d \in \mathbb{Q}$ tal que $\sqrt{d} \notin \mathbb{Q}$:

Proposición 7.3.9. (Raíces de la forma $a + b\sqrt{d}$ de polinomios racionales.)

Sea $d \in \mathbb{Q}$ tal que $\sqrt{d} \notin \mathbb{Q}$, y sean $a, b \in \mathbb{Q}$ con $b \neq 0$. Sea $f \in \mathbb{Q}[X]$. Entonces

1. $g := \big(X - (a + b\sqrt{d})\big)\big(X - (a - b\sqrt{d})\big)$ *es un polinomio irreducible de* $\mathbb{Q}[X]$,
2. $f(a + b\sqrt{d}) = 0 \implies g \mid f$ *en* $\mathbb{Q}[X]$,
3. $f(a + b\sqrt{d}) = 0 \iff f(a - b\sqrt{d}) = 0$,
4. *Para todo* $m \in \mathbb{N}$, $\text{mult}(a + b\sqrt{d}; f) = m \Leftrightarrow \text{mult}(a - b\sqrt{d}; f) = m$.

Demostración. 1. Haciendo la cuenta,

$$g := \big(X - (a + b\sqrt{d})\big)\big(X - (a - b\sqrt{d})\big) = X^2 - 2aX + a^2 - b^2 d \in \mathbb{Q}[X]$$

porque todos sus coeficientes pertenecen a $\mathbb{Q}$, y es irreducible por ser de grado 2 y no tener raíz en $\mathbb{Q}$.

2. Dividamos a $f \in \mathbb{Q}[X]$ por el polinomio $g \in \mathbb{Q}[X]$:

$$g = q\,g + r \quad \text{con} \quad r = 0 \quad \text{o} \quad \text{gr}(r) < 2.$$

En todo caso se puede escribir en la forma $r = cX + e$ con $c, e \in \mathbb{Q}$. Ahora bien, como $a + b\sqrt{d}$ es raíz de f y de g, se obtiene que $a + b\sqrt{d}$ es raíz de r también. Es decir

$$\begin{aligned} 0 &= r(a + b\sqrt{d}) = c(a + b\sqrt{d}) + e = ca + e + cb\sqrt{d} \\ &\implies ca + e = -cb\sqrt{d}. \end{aligned}$$

Si fuera $c \neq 0$, como $b \neq 0$ se obtendría $\sqrt{d} = \dfrac{ca + e}{-cb} \in \mathbb{Q}$ lo que contradice la hipótesis $\sqrt{d} \notin \mathbb{Q}$. Por lo tanto $c = 0$, lo que implica también de la igualdad $0 = c(a + b\sqrt{d}) + e$ que $e = 0$. Se concluye que $r = cX + e$ es el polinomio nulo, y por lo tanto $g \mid f \in \mathbb{Q}[X]$.

3. Es una consecuencia directa del inciso anterior, ya que si $f(a + b\sqrt{d}) = 0$, entonces $g \mid f$ y por lo tanto $f(a - b\sqrt{d}) = 0$ también. La recíproca es análoga.

4. La misma multiplicidad se obtiene por inducción, aplicando la hipótesis inductiva al polinomio $f/g \in \mathbb{Q}[X]$ cuando $a + b\sqrt{d}$ es raíz de f.

□

Ejemplo: Factorizar en $\mathbb{C}[X]$, $\mathbb{R}[X]$ y $\mathbb{Q}[X]$ el polinomio $f = X^4 - X^3 - 2X^2 - 3X - 1$ sabiendo que tiene a $1 - \sqrt{2}$ como raíz.

Como $f \in \mathbb{Q}[X]$ y $1 - \sqrt{2}$ es raíz, también lo es $1 + \sqrt{2}$ y f es divisible por el polinomio $g = \big(X - (1 - \sqrt{2})\big)\big(X - (1 + \sqrt{2})\big) = X^2 - 2X - 1$. En efecto, al hacer la división se obtiene

$$f = (X^2 - 2X - 1)(X^2 + X + 1).$$

Ahora bien, las raíces de $X^2 + X + 1$ son las raíces cúbicas primitivas de la unidad, $\dfrac{-1 \pm \sqrt{3}i}{2}$, por lo tanto la factorización de f en $\mathbb{C}[X]$ es

$$f = \big(X - (1 - \sqrt{2})\big)\big(X - (1 + \sqrt{2})\big)\big(X - (\frac{-1 + \sqrt{3}}{2})\big)\big(X - (\frac{-1 - \sqrt{3}}{2})\big).$$

El polinomio X^2+X+1 es irreducible tanto en $\mathbb{R}[X]$ como en $\mathbb{Q}[X]$ al tener grado 2 y no tener raíces allí, y el polinomio $X^2 - 2X - 1$ es irreducible en $\mathbb{Q}[X]$ al tener grado 2 y no tener raíces en $\mathbb{Q}$. Por lo tanto la factorización de f en $\mathbb{R}[X]$ es

$$f = \big(X - (1 - \sqrt{2})\big)\big(X - (1 + \sqrt{2})\big)\big(X^2 + X + 1\big)$$

y la factorización de f en $\mathbb{Q}[X]$ es

$$\big(X^2 - 2X - 1\big)\big(X^2 + X + 1\big).$$

Con respecto a la factorización en general, en el caso de $\mathbb{Q}[X]$ no se puede decir nada más preciso que lo que ya dice el Teorema Fundamental de la Aritmética para polinomios:

Teorema 7.3.10. (Factorización en $\mathbb{Q}[X]$.)

Sea $f \in \mathbb{Q}[X] - \mathbb{Q}$. Entonces la factorización en irreducibles de f en $\mathbb{Q}[X]$ es de la forma

$$f = c\, g_1^{m_1} \dots g_r^{m_r}$$

donde $c \in \mathbb{Q}^\times$, $g_1, \dots, g_r$ son polinomios mónicos irreducibles distintos en $\mathbb{Q}[X]$ y $m_1, \dots, m_r \in \mathbb{N}$.

Notemos que cada factor irreducible $g_i \in \mathbb{Q}[X]$ cuando lo miremos como polinomio en $\mathbb{R}[X]$ o en $\mathbb{C}[X]$ va probablemente a dejar de ser irreducible para factorizarse como polinomios de grado 1 o 2 en el caso de $\mathbb{R}$, o todos de grado 1 en el caso de $\mathbb{C}$. En ese sentido la factorización de f en $\mathbb{R}[X]$ "refina" la factorización de f en $\mathbb{Q}[X]$, y la de f en $\mathbb{C}[X]$ la refina aún más.


Zassenhaus


Berlekamp


A. Lenstra


H. Lenstra


Lovasz

Por ejemplo el polinomio $f = X^4 - 2X^3 + X^2 - 4X - 2 \in \mathbb{Q}[X]$ que consideramos arriba se factoriza en $\mathbb{Q}[X]$ en la forma

$$f = (X^2 + 2)(X^2 - 2X - 1),$$

ya que ambos factores son irreducibles en $\mathbb{Q}[X]$ al no tener raíces en $\mathbb{Q}$ (por ser de grado 2).

Si bien no se sabe nada a priori sobre los factores irreducibles en $\mathbb{Q}[X]$ de un polinomio, en este caso existen algoritmos de factorización (exacta), contrariamente a lo que pasa en $\mathbb{C}[X]$ o $\mathbb{R}[X]$.

La historia de los algoritmos de factorización de polinomios en $\mathbb{Q}[X]$ comenzó con el astrónomo alemán Friedrich von Schubert en 1793, que presentó un algoritmo luego redescubierto por Leopold Kronecker en 1882 y y que se conoce hoy como el *Algoritmo de Kronecker*.

Para factorizar un polinomio en $\mathbb{Q}[X]$, dado que las constantes no influyen, alcanza con considerar el polinomio en $\mathbb{Z}[X]$ obtenido limpiando los denominadores comunes. Y en realidad se puede probar más: se puede probar que el problema de la factorización en $\mathbb{Q}[X]$ se reduce a encontrar factores con coeficientes enteros.

El algoritmo de Kronecker se basa en ese hecho, y en evaluación e interpolación de polinomios. Es muy sencillo teóricamente, aunque terriblemente costoso de implementar computacionalmente. Pero tiene la importante característica de indicar que existen algoritmos, y por lo tanto se pueden buscar algoritmos que funcionen mejor... Hubo posteriormente grandes mejoras en cuanto a la velocidad de los algoritmos de factorización en $\mathbb{Q}[X]$.

El primero de ellos, debido a Hans Zassenhaus, en 1969, se basa esencialmente en un algoritmo de Elwyn Berlekamp para factorizar rápidamente polinomios en cuerpos finitos, 1967. El algoritmo requiere en promedio un número de operaciones del orden de $\mathrm{gr}(f)^c$, donde c es una constante calculada, aunque en el peor de los casos puede necesitar un número exponencial en $\mathrm{gr}(f)$ operaciones como en el algoritmo de Kronecker mencionado más arriba.

El primer algoritmo polinomial para factorizar polinomios en $\mathbb{Q}[X]$, conoci-

do como algoritmo L^3, es debido a los hermanos holandeses Arjen Lenstra y Hendrik Lenstra y al húngaro László Lovász, en 1982. Establece exactamente lo siguiente :

Teorema 7.3.11. **(L^3.)**

Sea $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ un polinomio que satisface que sus coeficientes (enteros) no tienen ningún factor común no trivial en $\mathbb{Z}$. Sea H una cota superior para los módulos de los coeficientes $a_i \in \mathbb{Z}$. Entonces, se puede factorizar f en $\mathbb{Q}[X]$ realizando del orden de $n^{12} + n^9(\log_2 H)^3$ operaciones "bit" (es decir los números se representan en base 2, y se cuenta una operación cada vez que se suma, resta, multiplica o divide un bit "0" ó "1").

Este es el primer algoritmo *polinomial* que existe para factorizar en $\mathbb{Q}[X]$ polinomios racionales, donde polinomial significa que si el polinomio de entrada se mide a través de su grado n y del tamaño de sus coeficientes en representación binaria $\log_2 H$, la cantidad total de operaciones binarias que realiza el algoritmo está acotado por $(n \cdot \log_2 H)^c$ para algún $c \in \mathbb{N}$ calculado, y no del tipo 2^n como lo era hasta entonces.

El algoritmo utilizado hoy en día por la mayoría de los sistemas de álgebra computacional es un algoritmo más moderno, debido principalmente a Mark van Hoeij (que trabaja en él desde el 2002, y logró varias mejoras teóricas y prácticas): tiene la ventaja de ser polinomial en teoría y también eficiente en la práctica.

La descripción y la demostración de los algoritmos de Zassenhaus-Berlekamp, L^3 y van Hoeij quedan fuera de nuestro alcance, y utilizan fundamentalmente en el primer caso la reducción a factorizar polinomios módulo p para p primo, en el segundo caso la teoría de látices o reticulados en $\mathbb{Z}^n$, y en el último una combinación de ambos.

7.4 Ejercicios.

Generalidades.

1. Calcular el grado y el coeficiente principal de los siguientes polinomios

   i) $(4X^6 - 2X^5 + 3X^2 - 2X + 7)^{77}$,

   ii) $(-3X^7 + 5X^3 + X^2 - X + 5)^4 - (6X^4 + 2X^3 + X - 2)^7$,

   iii) $(-3X^5 + X^4 - X + 5)^4 - 81X^{20} + 19X^{19}$.