Polinomios

1. Estructuras algebraicas.

Sea G un conjunto y sea $*$ una operación en G, es decir, una función de $G \times G$ en G que a cada par de elementos $g, h \in G$ le asigna un elemento de G al que denotaremos $g*h$. Diremos que $(G, *)$ es un *grupo* si se satisfacen:

i) $g*(h*p) = (g*h)*p \ \ \forall\, g, h, p \in G$ ($*$ es asociativa)
ii) Existe $g_0 \in G$ tal que $h*g_0 = g_0*h = h$ para todo $h \in G$ (hay un elemento neutro)
iii) Para todo $g \in G$ existe $h \in G$ tal que $g*h = h*g = g_0$ (todo elemento tiene inverso)

Es fácil ver que si $(G, *)$ es un grupo entonces el elemento neutro y el inverso de cada $g \in G$ son únicos.
Diremos que un grupo $(G, *)$ es *abeliano* (o *conmutativo*) si $*$ es conmutativa, es decir, $g*h = h*g \ \ \forall\, g, h \in G$.

Ejemplos.

1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$ son grupos abelianos
2) $(\mathbb{N}, +)$ no es un grupo (no hay elemento neutro)
3) $(\mathbb{N} \cup \{0\}, +)$ no es un grupo (no todo elemento tiene inverso: el único elemento inversible es 0).
4) $(\mathbb{Q} - \{0\}, .)$, $(\mathbb{R} - \{0\}, .)$ y $(\mathbb{C} - \{0\}, .)$ son grupos abelianos
5) $(\mathbb{Z} - \{0\}, .)$ no es un grupo (no todo elemento tiene inverso: los únicos elementos inversibles son 1 y -1).
6) $(G_n, .)$ es un grupo abeliano

Sea A un conjunto y sean $+$ y $.$ dos operaciones en A. Diremos que $(A, +, .)$ es un *anillo* (con identidad) si se satisfacen:

i) $(A, +)$ es un grupo abeliano
ii) $.$ es asociativa
iii) $.$ tiene un elemento neutro y $1 \neq 0$, donde 1 denota el elemento neutro de $.$ y 0 denota el elemento neutro de $+$
iv) $a.(b + c) = a.b + a.c$ y $(a + b).c = a.c + b.c$, $\forall\, a, b, c \in A$ (propiedades distributivas)

Ejercicio. Sea $(A, +, .)$ un anillo. Probar que $a.0 = 0$ para todo $a \in A$.

Diremos que un anillo $(A, +, .)$ es *conmutativo* si $.$ es conmutativa, es decir, $a.b = b.a$ $\forall a, b \in A$.

Ejemplo. Si A es el conjunto de matrices de 2×2 con coeficientes reales y $+$ y $.$ son la suma y el producto de matrices respectivamente, entonces $(A, +, .)$ es un anillo no conmutativo.

Diremos que un anillo $(A, +, .)$ es *íntegro* si $\forall a, b \in A$ vale: $a.b = 0 \iff a = 0$ o $b = 0$. Notar que esto es equivalente a decir que si $a \neq 0$ y $b \neq 0$ entonces $a.b \neq 0$.

Sea $(A, +, .)$ un anillo. Diremos que $a \in A$ es una *unidad* si a es inversible respecto del producto, es decir, si existe $b \in A$ tal que $a.b = b.a = 1$. Si a es inversible respecto del producto entonces el inverso de a es único. Denotaremos por $\mathcal{U}(A)$ al conjunto de las unidades de A, es decir, al conjunto de todos los elementos de A que son inversibles respecto del producto.
Si $(A, +, .)$ es un anillo y $a \in A$, denotaremos por $-a$ al inverso de a respecto de $+$ y por a^{-1} al inverso de a respecto de . cuando $a \in \mathcal{U}(A)$.

Ejemplos. $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$ $(\mathbb{R}, +, .)$ y $(\mathbb{C}, +, .)$ son anillos conmutativos e íntegros. Sus unidades son $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$, $\mathcal{U}(\mathbb{Q}) = \mathbb{Q} - \{0\}$, $\mathcal{U}(\mathbb{R}) = \mathbb{R} - \{0\}$, y $\mathcal{U}(\mathbb{C}) = \mathbb{C} - \{0\}$.

Sea $n \in \mathbb{N}$, $n > 1$. Si consideramos el conjunto de los posibles restos en la división por n

$$\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$$

y definimos la suma $+_n$ y el producto $._n$ de dos elementos de $\mathbb{Z}_n$ en la forma

$$a +_n b = r_n(a+b)$$
$$a ._n b = r_n(a.b)$$

entonces $(\mathbb{Z}_n, +_n, ._n)$ es un anillo conmutativo.

Ejemplos.

1) Calculemos las tablas de suma y producto para $\mathbb{Z}_4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Como se observa en la tabla del producto, $\mathbb{Z}_4$ no es íntegro. Además, las unidades de $\mathbb{Z}_4$ son $\mathcal{U}(\mathbb{Z}_4) = \{1, 3\}$.

2) Calculemos las tablas de suma y producto para $\mathbb{Z}_5$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Como se observa en la tabla del producto, $\mathbb{Z}_5$ es íntegro. Además, las unidades de $\mathbb{Z}_5$ son $\mathcal{U}(\mathbb{Z}_5) = \{1, 2, 3, 4\}$.

3) $\mathbb{Z}_{15}$ no es íntegro pues $3 \neq 0$, $5 \neq 0$ y $3 ._{15} 5 = r_{15}(3.5) = 0$. Dejamos como ejercicio verificar que $\mathcal{U}(\mathbb{Z}_{15}) = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Proposición. Sea n un número natural mayor que 1. Entonces $a \in \mathbb{Z}_n$ es una unidad si y sólo si a y n son coprimos, es decir, $\mathcal{U}(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \,/\, (a : n) = 1\}$.

Demostración: $a \in \mathcal{U}(\mathbb{Z}_n)$ si y sólo si $\exists\, b \in \mathbb{Z}_n$ tal que $a ._n b = 1$ si y sólo si $\exists\, b \in \mathbb{Z}_n$ tal que $r_n(a.b) = 1$ si y sólo si $\exists\, b \in \mathbb{Z}_n$ tal que $a.b \equiv 1\ (n)$ si y sólo si la ecuación de congruencia $ax \equiv 1\,(n)$ tiene solución, si y sólo si $(a : n) \mid 1$ si y sólo si $(a : n) = 1$. □

Sea $\mathbb{K}$ un conjunto y sean $+$ y $.$ dos operaciones en $\mathbb{K}$. Diremos que $(\mathbb{K}, +, .)$ es un *cuerpo* si se satisfacen:

i) $(\mathbb{K}, +, .)$ es un anillo conmutativo
ii) Todo $a \in \mathbb{K}$ no nulo es inversible respecto del producto, es decir, si $\mathcal{U}(\mathbb{K}) = \mathbb{K} - \{0\}$.

Ejemplos.

1) $(\mathbb{Q}, +, .)$ $(\mathbb{R}, +, .)$ y $(\mathbb{C}, +, .)$ son cuerpos
2) $(\mathbb{Z}, +, .)$ no es un cuerpo

Ejercicio. 1) Probar que si $(\mathbb{K}, +, .)$ es un cuerpo entonces es un anillo íntegro.
2) Probar que $\mathbb{Z}_n$ es íntegro si y sólo si n es primo.
3) Probar que $\mathbb{Z}_n$ es un cuerpo si y sólo si n es primo.

Sea $(\mathbb{K}, +, .)$ un cuerpo. Diremos que $\mathbb{K}$ tiene *característica cero* si $\underbrace{1 + 1 + \cdots + 1}_{n \text{ sumandos}} \neq 0$ para todo $n \in \mathbb{N}$.

Ejemplos.

1) $(\mathbb{Q}, +, .)$ $(\mathbb{R}, +, .)$ y $(\mathbb{C}, +, .)$ son cuerpos de característica cero
2) $(\mathbb{Z}_p, +, .)$ (p primo) no es un cuerpo de característica cero pues $\underbrace{1 + 1 + \cdots + 1}_{p \text{ sumandos}} = 0$

2. El anillo de polinomios.

Sea $(A, +, .)$ un anillo conmutativo (por ejemplo, $A = \mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$) y sea X una indeterminada sobre A, es decir, X satisface

$$a_0 + a_1X + \cdots + a_nX^n = b_0 + b_1X + \cdots + b_mX^m \Longleftrightarrow a_0 = b_0, a_1 = b_1, a_2 = b_2, \ldots$$

(Por ejemplo, si $A = \mathbb{Q}$ entonces los números reales e y π satisfacen esta propiedad).

Definimos el *anillo de polinomios* con coeficientes en A, al que denotaremos por $A[X]$, en la forma

$$A[X] = \{a_0 + a_1X + \cdots + a_nX^n \,/\, n \in \mathbb{N}_0 \text{ y } a_i \in A \ (0 \leq i \leq n)\}$$

con las operaciones + y . definidas por

$$\sum_{i=0}^{n} a_iX^i + \sum_{i=0}^{m} b_iX^i = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)X^i$$

$$\left(\sum_{i=0}^{n} a_iX^i\right) . \left(\sum_{i=0}^{m} b_iX^i\right) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_ib_j\right) X^k$$

donde $a_i = 0$ para $i > n$ y $b_i = 0$ para $i > m$ y, por convención, $X^0 = 1$.
A los elementos de $A[X]$ los llamaremos *polinomios* con coeficientes en A.

Ejercicio. Probar que $(A[X], +, .)$ es un anillo conmutativo.

Si $f \in A[X]$ es el polinomio $f = \sum\limits_{i=0}^{n} a_iX^i$, el elemento $a_i \in A$ se llama el coeficiente de X^i de f.

Observación. $A \subseteq A[X]$ ya que si $a \in A$ entonces $a = \sum\limits_{i=0}^{n} a_iX^i$ donde $a_0 = a$ y $n = 0$. Además, la suma y el producto de elementos de A es la misma vistos como elementos de A o como elementos de $A[X]$.

Observación. Sean $f, g \in A[X]$. Si $f = \sum\limits_{i=0}^{n} a_iX^i$ y $g = \sum\limits_{i=0}^{m} b_iX^i$ entonces $f = g$ si y sólo si $a_i = b_i$ para todo i. En particular, $f = 0$ si y sólo si $a_i = 0$ para todo i.

Ejemplos.

1) Sean $f, g \in \mathbb{Z}[X]$ los polinomios

$$f = X^4 + 2X^3 + 3X^2 - 2X + 1$$
$$g = 3X^2 + 5X - 7$$

Entonces

$$f + g = X^4 + 2X^3 + 6X^2 + 3X - 6$$
$$\begin{aligned} f.g = {} & 3X^6 + (1.5 + 2.3)X^5 + (1.(-7) + 2.5 + 3.3)X^4 + (2.(-7) + 3.5 + (-2).3)X^3 + \\ & + (3.(-7) + (-2).5 + 1.3)X^2 + ((-2).(-7) + 1.5)X + 1.(-7) = \\ & = 3X^6 + 11X^5 + 12X^4 - 5X^3 - 28X^2 + 19X - 7 \end{aligned}$$

2) Sean $f, g \in \mathbb{Z}_{30}[X]$ los polinomios

$$f = 21X^2 + 9$$
$$g = 20X^4 + 10X$$

Entonces

$$\begin{aligned} f.g &= 21._{30}20X_6 + 9._{30}20X^4 + 21._{30}10X^3 + 9._{30}10X = \\ &= r_{30}(21.20)X^6 + r_{30}(9.20)X^4 + r_{30}(21.10)X^3 + r_{30}(9.10)X = \\ &= 0X^6 + 0X^4 + 0X^3 + 0X = 0 \end{aligned}$$

Como vemos, en $\mathbb{Z}_{30}[X]$ el producto de dos polinomios no nulos puede ser el polinomio nulo. Luego, $\mathbb{Z}_{30}[X]$ no es íntegro.

Proposición. $A[X]$ es íntegro si y sólo si A es íntegro.

Demostración: ($\Longrightarrow$) Sean $a, b \in A$ tales que $a \neq 0$ y $b \neq 0$. Como $a, b \in A[X]$ y $A[X]$ es íntegro entonces $a.b \neq 0$.

($\Longleftarrow$) Sean $f, g \in A[X]$ tales que $f \neq 0$ y $g \neq 0$. Entonces, $f = a_n X^n + \cdots + a_1 X + a_0$ con $a_n \neq 0$ y $g = b_m X^m + \cdots + b_1 X + b_0$ con $b_m \neq 0$. Como A es íntegro entonces $a_n.b_m \neq 0$. Luego

$$f.g = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) X^k = a_n.b_m X^{n+m} + \sum_{k=0}^{n+m-1} \left(\sum_{i+j=k} a_i b_j \right) X^k$$

Por lo tanto, $f.g \neq 0$ pues el coeficiente de X^{n+m} es $a_n.b_m \neq 0$. □

Corolario. Si $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}_p$ (p primo) y $f, g \in A[X]$ son no nulos entonces $f.g \neq 0$.

Ejercicio. Sea A un anillo íntegro y sean $f, g, h \in A[X]$. Probar que si $f.g = f.h$ y $f \neq 0$ entonces $g = h$.

Sea A un anillo conmutativo y sea $f \in A[X]$. Si $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, donde $a_n \neq 0$ entonces decimos que n es el *grado* de f y escribimos $\operatorname{gr} f = n$. Además diremos que a_n es el *coeficiente principal* de f y, diremos que f es *mónico* si $a_n = 1$.

Proposición. Sea A un anillo íntegro (por ejemplo, $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}_p$ con p primo). Si $f, g \in A[X]$ son no nulos entonces

i) $f.g \neq 0$ y $\operatorname{gr}(f.g) = \operatorname{gr} f + \operatorname{gr} g$.
ii) Para todo $k \in \mathbb{N}$ vale $f^k \neq 0$ y $\operatorname{gr}(f^k) = k.\operatorname{gr} f$
iii) Si $f + g \neq 0$ entonces $\operatorname{gr}(f + g) \leq \max\{\operatorname{gr} f, \operatorname{gr} g\}$
iv) Si $\operatorname{gr} f \neq \operatorname{gr} g$ entonces $f + g \neq 0$ y $\operatorname{gr}(f + g) = \max\{\operatorname{gr} f, \operatorname{gr} g\}$

Dejamos la demostración como ejercicio.

Observación. Si A no es íntegro entonces dados $f, g \in A[X]$ no nulos puede ocurrir que $f.g = 0$ y también que $f.g \neq 0$ pero $\mathrm{gr}\,(f.g) < \mathrm{gr}\, f + \mathrm{gr}\, g$. Por ejemplo, si $A = \mathbb{Z}_{14}$ y $f, g \in A[X]$ son los polinomios $f = 2X^5+3$ y $g = 7X^3+X$ entonces $f.g = 2X^6+7X^3+3X$, que tiene grado $6 < 8$.

Ejemplo. Hallemos todos los $f \in \mathbb{C}[X]$ tales que $Xf^2 - X^3 = (2X-1)f + 1$.

Sea $f \in \mathbb{C}[X]$, tal que $Xf^2 - X^3 = (2X-1)f+1$ y sea $n = \mathrm{gr}\, f$ (notar que $f \neq 0$). Entonces, tomando grado en ambos miembros de la igualdad, $\mathrm{gr}\,(Xf^2 - X^3) = \mathrm{gr}\,((2X-1)f+1)$. Si $n > 1$ entonces, por i) y ii), $\mathrm{gr}\,(Xf^2) = \mathrm{gr}\, X + 2.\mathrm{gr}\, f = 1 + 2n > 3$. Luego, por iv), $\mathrm{gr}\,(Xf^2 - X^3) = 1 + 2n$. Además, como $\mathrm{gr}\,((2X-1)f) = 1 + n > 0$, entonces $\mathrm{gr}\,((2X-1)f+1) = \mathrm{gr}\,((2X+1)f = 1 + n$ por iv).

Por lo tanto, $1 + 2n = \mathrm{gr}\,(Xf^2 - X^3) = \mathrm{gr}\,((2X-1)f+1) = 1 + n$, pero esto no puede ocurrir pues $n > 1$. Hemos probado entonces que $\mathrm{gr}\, f \leq 1$, es decir, $f = aX + b$ para ciertos $a, b \in \mathbb{C}$. Ahora determinemos a y b.

$$\begin{aligned}
&Xf^2 - X^3 = (2X-1)f + 1 \iff X(aX+b)^2 - X^3 = (2X-1)(aX+b) + 1 \iff \\
&\iff (a^2-1)X^3 + 2abX^2 + b^2X = 2aX^2 + (2b-a)X - b + 1 \iff \\
&\iff a^2 - 1 = 0,\ 2ab = 2a,\ b^2 = 2b - a \ \text{ y } \ -b+1 = 0 \iff a = 1 = b
\end{aligned}$$

Luego, el único polinomio que satisface lo pedido es $f = X + 1$.

Proposición. Sea A un anillo íntegro (por ejemplo, $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}_p$ con p primo). Entonces $\mathcal{U}(A[X]) = \mathcal{U}(A)$.

Demostración: Es trivial que $\mathcal{U}(A) \subseteq \mathcal{U}(A[X])$. Veamos la otra inclusión: sea $f \in \mathcal{U}(A[X])$. Entonces existe $g \in A[X]$ tal que $f.g = 1$. De esta igualdad resulta que $f, g \neq 0$ y $\mathrm{gr}\,(f.g) = 0$. Luego, por la proposición anterior, $\mathrm{gr}\, f + \mathrm{gr}\, g = 0$ de donde resulta que $\mathrm{gr}\, f = 0 = \mathrm{gr}\, g$. Luego, $f, g \in A$ y $f.g = 1$, por lo tanto $f \in \mathcal{U}(A)$. ◻

Ejemplos.

1) $\mathcal{U}(\mathbb{Z}[X]) = \{1, -1\}$

2) Si $\mathbb{K}$ es un cuerpo (por ejemplo, $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}_p$) entonces $\mathcal{U}(\mathbb{K}[X]) = \mathbb{K} - \{0\}$, es decir, las unidades de $\mathbb{K}[X]$ son los polinomios no nulos de grado cero.

3) $2X^n + 1 \in \mathcal{U}(\mathbb{Z}_4[X])$ para todo $n \in \mathbb{N}$ pues $(2X^n+1)(2X^n+1) = 1$. Luego, si $A = \mathbb{Z}_4$ entonces en $A[X]$ hay unidades de grado tan grande como se quiera. Esto se debe a que $A = \mathbb{Z}_4$ no es íntegro. En general, si A no es íntegro, hallar $\mathcal{U}(A[X])$ no es un problema fácil.

3. Aritmética en $\mathbb{K}[X]$.

Sea $\mathbb{K}$ un cuerpo (por ejemplo, $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}_p$ con p primo). Veremos en esta sección nociones de aritmética análogas a las que vimos para los enteros, que también pueden definirse en $\mathbb{K}[X]$ tales como divisibilidad, congruencia, máximo común divisor, etc.

Divisibilidad. Dados $f, g \in \mathbb{K}[X]$ decimos que f *divide* a g (y escribimos $f \mid g$) si existe $h \in \mathbb{K}[X]$ tal que $g = f.h$.

Ejemplos.

1) Si $\mathbb{K} = \mathbb{Q}$ entonces $X - 1 \mid X^3 - 1$ pues $X^3 - 1 = (X - 1)(X^2 + X + 1)$

2) Si $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$ entonces $2X^2 + 1 \mid X^3 - 2X^2 + \frac{1}{2}X - 1$ pues

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

3) Si $\mathbb{K} = \mathbb{Z}_5$ entonces $3X^2 + 2X + 1 \mid X^5 + 4X^4 + X^3 + X^2 + 3X$ pues

$$X^5 + 4X^4 + X^3 + X^2 + 3X = (3X^2 + 2X + 1)(2X^3 + 3X)$$

A continuación veremos que las propiedades de la divisibilidad en $\mathbb{K}[X]$ son semejantes a las propiedades de la divisibilidad en $\mathbb{Z}$, teniendo en cuenta que ahora $\mathbb{K} - \{0\}$ (los polinomios no nulos de grado cero) juegan el papel que en $\mathbb{Z}$ jugaban 1 y -1. Esto se debe a que $\{1, -1\} = \mathcal{U}(\mathbb{Z})$ y $\mathbb{K} - \{0\} = \mathcal{U}(\mathbb{K}[X])$. Además, $|a|$ para $a \in \mathbb{Z}$ se traduce en $\operatorname{gr} f$ para $f \in \mathbb{K}[X]$.

Propiedades de la divisibilidad.

En $\mathbb{Z}$	En $\mathbb{K}[X]$
i) $\pm a \mid a \quad \forall a \in \mathbb{Z}$	i') $c.f \mid f \quad \forall f \in \mathbb{K}[X]$, $c \in \mathbb{K} - \{0\}$
ii) $a \mid b$ y $b \mid c \Longrightarrow a \mid c$	ii') $f \mid g$ y $g \mid h \Longrightarrow f \mid h$
iii) $a \mid b \Longrightarrow a \mid b.c \quad \forall c \in \mathbb{Z}$	iii') $f \mid g \Longrightarrow f \mid g.h \quad \forall h \in \mathbb{K}[X]$
iv) $a \mid b$ y $a \mid c \Longrightarrow a \mid b + c$	iv') $f \mid g$ y $f \mid h \Longrightarrow f \mid g + h$
v) $\pm 1 \mid a \quad \forall a \in \mathbb{Z}$	v') $c \mid f \quad \forall c \in \mathbb{K} - \{0\}, f \in \mathbb{K}[X]$
vi) $a \mid \pm 1 \Longrightarrow a = \pm 1$	vi') $f \mid c$ con $c \in \mathbb{K} - \{0\} \Longrightarrow f \in \mathbb{K} - \{0\}$
vii) $a \mid 0 \quad \forall a \in \mathbb{Z}$	vii') $f \mid 0 \quad \forall f \in \mathbb{K}[X]$
viii) $0 \mid a \Longleftrightarrow a = 0$	viii') $0 \mid f \Longleftrightarrow f = 0$
ix) Si $b \neq 0$ y $a \mid b$ entonces $\lvert a\rvert \leq \lvert b\rvert$	ix') Si $g \neq 0$ y $f \mid g$ entonces $\operatorname{gr} f \leq \operatorname{gr} g$
x) $a \mid b$ y $b \mid a \Longleftrightarrow a = \pm b$	x') $f \mid g$ y $g \mid f \Longleftrightarrow \exists\, c \in \mathbb{K} - \{0\} \,/\, f = c.g$
xi) $a \mid b \Longleftrightarrow -a \mid b \Longleftrightarrow$	xi') $f \mid g \Longleftrightarrow c.f \mid g \Longleftrightarrow f \mid d.g \Longleftrightarrow$
$\Longleftrightarrow a \mid -b \Longleftrightarrow -a \mid -b$	$\Longleftrightarrow c.f \mid d.g \quad \forall c, d \in \mathbb{K} - \{0\}$

Dejamos las demostraciones como ejercicio.

Irreducibles. Sean $f, g \in \mathbb{K}[X]$. Diremos que f y g son *asociados* si $\exists\, c \in \mathbb{K} - \{0\}$ (es decir, una unidad de $\mathbb{K}[X]$) tal que $f = c.g$ (notar que si $f = c.g \iff g = c^{-1}.f$, donde $c^{-1} \in \mathbb{K} - \{0\}$). Observemos que f y g son asociados si y sólo si $f \mid g$ y $g \mid f$.

Observación. Así como todo entero a siempre es divisible por 1, -1, a y $-a$, todo polinomio en $f \in \mathbb{K}[X]$ siempre es divisible por las unidades de $\mathbb{K}[X]$ y por los asociados de f (propiedades i') y v')).

Sea $f \in \mathbb{K}[X]$. Diremos que f es *irreducible* si $f \neq 0$, f no es una unidad y f es divisible sólo por unidades de $\mathbb{K}[X]$ y asociados de f. Notemos que la noción de irreducible en $\mathbb{K}[X]$ es análoga a la noción de primo en $\mathbb{Z}$: $p \in \mathbb{Z}$ es primo si y sólo si $p \neq 0, 1, -1$ y p es divisible sólo por 1,-1, p y $-p$.

Proposición. Sea $f \in \mathbb{K}[X]$, $f \neq 0$. Si $\operatorname{gr} f = 1$ entonces f es irreducible.

Demostración: Sabemos que $f \neq 0$ y, como $\operatorname{gr} f = 1$ entonces f no es una unidad. Veamos cuáles son los divisores de f: sea $g \in \mathbb{K}[X]$ tal que $g \mid f$. Entonces $f = g.h$ para algún $h \in \mathbb{K}[X]$. Ahora, tomando grado en esta igualdad, resulta que $1 = \operatorname{gr} f = \operatorname{gr} g + \operatorname{gr} h$. Luego $\operatorname{gr} g = 0$ o $\operatorname{gr} g = 1$. Si $\operatorname{gr} g = 0$ entonces g es una unidad. Y si $\operatorname{gr} g = 1$ entonces $\operatorname{gr} h = 0$ de donde resulta que h es una unidad y por lo tanto f y g son asociados ya que $f = g.h$. □

Ejercicio. Probar que f es irreducible si y sólo si se verifican las dos siguientes condiciones:
i) $f \neq 0$ y $\operatorname{gr} f \geq 1$
ii) Dado $g \in \mathbb{K}[X]$, si $g \mid f$ entonces $\operatorname{gr} g = 0$ o $\operatorname{gr} g = \operatorname{gr} f$

Recordemos que todo entero $a \neq 0, 1, -1$ es divisible por algún primo. La siguiente proposición es el resultado análogo para $\mathbb{K}[X]$.

Proposición. Sea $f \in \mathbb{K}[X]$ tal que $f \neq 0$ y $\operatorname{gr} f > 0$ (es decir, si f no es cero ni una unidad). Entonces existe $h \in \mathbb{K}[X]$ irreducible tal que $h \mid f$.

Demostración: Notemos que si $g \mid f$ entonces $g \neq 0$ pues $f \neq 0$. Por lo tanto, para todo g que divide a f está definido $\operatorname{gr} g$. Sea

$$S = \{\operatorname{gr} g \,/\, g \in \mathbb{K}[X],\ g \mid f \text{ y } \operatorname{gr} g \geq 1\}$$

Entonces S es un subconjunto no vacío de $\mathbb{N}$ pues $\operatorname{gr} f \in S$ y por lo tanto, por el principio de buena ordenación, posee un primer elemento n. Es decir, $n \in S$ y $n \leq m$ para todo $m \in S$.
Como $n \in S$ entonces $n = \operatorname{gr} h$ para algún $h \in \mathbb{K}[X]$ tal que $h \mid f$ y $\operatorname{gr} h \geq 1$. Veremos que h es irreducible.
Es trivial que h satisface la condición i) del ejercicio anterior, veamos que también satisface ii). Sea $g \in \mathbb{K}[X]$ tal que $g \mid h$. Debemos probar que si $\operatorname{gr} g \neq 0$ entonces $\operatorname{gr} g = \operatorname{gr} h$. Supongamos que $\operatorname{gr} g \neq 0$. Entonces, $\operatorname{gr} g \geq 1$ y como $g \mid h$ y $h \mid f$ entonces $g \mid f$. Luego,

$m = \operatorname{gr} g \in S$ y por lo tanto $\operatorname{gr} h = n \leq m = \operatorname{gr} g$. Pero como $g \mid h$ entonces $\operatorname{gr} g \leq \operatorname{gr} h$, de donde $\operatorname{gr} g = \operatorname{gr} h$ como queríamos probar. Luego, h es irreducible y $h \mid f$. □

Algoritmo de división. El algoritmo de división en $\mathbb{Z}$ dice que dados $a, b \in \mathbb{Z}$, $b \neq 0$, existen únicos $q, r \in \mathbb{Z} \,/\, a = b.q + r$ y $0 \leq r < |b|$. Teniendo en cuenta que el valor absoluto de un número entero se traduce para los polinomios en la noción de grado, el resultado análogo para $\mathbb{K}[X]$ es el siguiente

Teorema. Sean $f, g \in \mathbb{K}[X]$, $g \neq 0$. Entonces existen únicos $q, r \in \mathbb{K}[X]$ tales que $f = g.q + r$ y $r = 0$ o $\operatorname{gr} r < \operatorname{gr} g$.

Demostración: <u>Existencia</u>: Si $g \mid f$ entonces existe $h \in \mathbb{K}[X]$ tal que $f = g.h$. En este caso basta tomar $q = h$ y $r = 0$. Supongamos ahora que $g \not| f$. Entonces $f - g.q \neq 0$ para todo $q \in \mathbb{K}[X]$ y por lo tanto está definido $\operatorname{gr}(f - g.q)$ para todo $q \in \mathbb{K}[X]$. Sea

$$S = \{\operatorname{gr}(f - g.q) \,/\, q \in \mathbb{K}[X]\}$$

Entonces S es un subconjunto no vacío de $\mathbb{N}_0$ pues $\operatorname{gr} f \in S$ y por lo tanto posee un primer elemento n (si $0 \in S$ entonces 0 es el primer elemento de S y si $0 \notin S$ entonces S es un subconjunto no vacío de $\mathbb{N}$ y por lo tanto posee un primer elemento). Luego $n \in S$ y $n \leq m$ para todo $m \in S$.

Como $n \in S$ entonces $n = gr(f - g.q)$ para algún $q \in \mathbb{K}[X]$. Luego, tomando $r = f - g.q$ se tiene $\operatorname{gr} r = n$ y $f = g.q + r$. Debemos probar que $n < \operatorname{gr} g$. Sea $m = \operatorname{gr} g$, entonces

$$\begin{aligned} r &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \text{ con } a_n \neq 0 \\ g &= b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0, \text{ con } b_m \neq 0 \end{aligned}$$

Si fuese $n \geq m$ entonces $n - m \geq 0$ y tomando $r' = r - a_n {b_m}^{-1} X^{n-m}.g$ se tiene que

$$\begin{aligned} r' &= r - a_n {b_m}^{-1} X^{n-m}.g = \\ &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 - \\ &\quad - a_n {b_m}^{-1} X^{n-m}.(b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0) = \\ &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 - a_n X^n - a_n {b_m}^{-1} b_{m-1} X^{n-1} - \cdots - \\ &\qquad - a_n {b_m}^{-1} b_1 X^{n-m+1} - a_n {b_m}^{-1} b_0 X^{n-m} = \\ &= a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 - a_n {b_m}^{-1} b_{m-1} X^{n-1} - \cdots - \\ &\qquad - a_n {b_m}^{-1} b_1 X^{n-m+1} - a_n {b_m}^{-1} b_0 X^{n-m} \end{aligned}$$

de donde $\operatorname{gr} r' < n$. Pero esto no puede ocurrir pues n era el primer elemento de S y $\operatorname{gr} r' \in S$ ya que

$$r' = r - a_n {b_m}^{-1} X^{n-m}.g = f - g.q - a_n {b_m}^{-1} X^{n-m}.g = f - g.[q + a_n {b_m}^{-1} X^{n-m}]$$

Por lo tanto $\operatorname{gr} r = n < \operatorname{gr} g$.

Unicidad: Supongamos que $f = g.q_1 + r_1$, con $q_1, r_1 \in \mathbb{K}[X]$ y $r_1 = 0$ o $\operatorname{gr} r_1 < \operatorname{gr} g$ y que $f = g.q_2 + r_2$, con $q_2, r_2 \in \mathbb{K}[X]$ y $r_2 = 0$ o $\operatorname{gr} r_2 < \operatorname{gr} g$. Debemos ver que $r_1 = r_2$ y $q_1 = q_2$.
Si $r_1 = r_2$ entonces $g.q_1 = f = g.q_2$, de donde $g(q_1 - q_2) = 0$ y como $g \neq 0$ y $\mathbb{K}[X]$ es íntegro entonces resulta que $q_1 - q_2 = 0$, es decir, $q_1 = q_2$.
Supongamos ahora que $r_1 \neq r_2$. Como $g.q_1 + r_1 = g.q_2 + r_2$ entonces $g(q_1 - q_2) = r_2 - r_1 \neq 0$. Luego, tomando grado en esta igualdad, resulta que $\operatorname{gr} g + \operatorname{gr}(q_1 - q_2) = \operatorname{gr}(r_1 - r_2)$. Como $\operatorname{gr}(q_1 - q_2) \geq 0$, $\operatorname{gr}(r_1 - r_2) \leq \max\{\operatorname{gr} r_1, \operatorname{gr} r_2\}$, $\operatorname{gr} r_1 < \operatorname{gr} g$ y $\operatorname{gr} r_2 < \operatorname{gr} g$ entonces

$$\operatorname{gr} g \leq \operatorname{gr} g + \operatorname{gr}(q_1 - q_2) = \operatorname{gr}(r_1 - r_2) \leq \max\{\operatorname{gr} r_1, \operatorname{gr} r_2\} < \operatorname{gr} g$$

lo que es una contradicción. □

Observación. Si $f, g \in \mathbb{Z}[X]$, $g \neq 0$ entonces, en particular, $f, g \in \mathbb{Q}[X]$ y por lo tanto existen $q, r \in \mathbb{Q}[X]$ tales que $f = g.q + r$ con $r = 0$ o $\operatorname{gr} r < \operatorname{gr} g$. Pero, en general, q y r no son polinomios con coeficientes enteros. Por ejemplo, si $f = X^2 + 3$ y $g = 2X + 1$ entonces $q = \frac{1}{2}X - \frac{1}{4}$ y $r = \frac{13}{4}$. Pero si g es mónico (es decir, su coeficiente principal es igual a 1) entonces resulta que $q, r \in \mathbb{Z}[X]$. Más generalmente, si A es un anillo íntegro, dados $f, g \in A[X]$, $g = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$, con $b_m \in \mathcal{U}(A)$ entonces podemos repetir para f y g la demostración del teorema anterior. Por lo tanto podemos concluír que dados $f, g \in A[X]$, $g \neq 0$, si el coeficiente principal de g es una unidad de A entonces existen únicos $q, r \in A[X]$ tales que $f = g.q + r$ y $r = 0$ o $\operatorname{gr} r < \operatorname{gr} g$.

Los polinomios q y r del teorema anterior se llaman el *cociente* y el *resto* de la división de f por g. Notar que por la unicidad del cociente y el resto, si $f = g.q + r$ con $r = 0$ o $\operatorname{gr} r < \operatorname{gr} g$ entonces necesariamente q y r son, respectivamente, el cociente y el resto de la división de f por g.

Ejemplos.

1) Sean $f, g \in \mathbb{R}[X]$, $f = 2X^4 + 3X^2 - X + 5$ y $g = X^3 + X^2 + 1$. Entonces el cociente y el resto de la división de f por g son $q = 2X - 2$ y $r = 5X^2 - 3X + 7$.

2) Sean $f, g \in \mathbb{Z}_7[X]$, $f = 2X^4 + 3X^3 + 2X + 4$, $g = 3X^2 + 5$. Entonces el cociente y el resto de la división de f por g son $q = 3X^2 + X + 2$ y $r = 4X + 1$.

Ejercicio. Sea $f \in \mathbb{C}[X]$, sea $g \in \mathbb{C}[X]$ tal que $g \neq 0$ y sean $q, r \in \mathbb{C}[X]$ el cociente y el resto de la división de f por g. Probar que

i) Si $f, g \in \mathbb{R}[X]$ entonces $q, r \in \mathbb{R}[X]$

ii) Si $f, g \in \mathbb{Q}[X]$ entonces $q, r \in \mathbb{Q}[X]$

Sea $f \in \mathbb{K}[X]$, $f = \sum_{i=0}^{n} a_i X^i$ y sea $c \in \mathbb{K}$. Llamaremos *especialización* de f en c al elemento de $\mathbb{K}$

$$f(c) = \sum_{i=0}^{n} a_i c^i$$

Propiedades de la especialización. Para todo $f, g \in \mathbb{K}[X]$, $c \in \mathbb{K}$ se verifican

i) $(f+g)(c) = f(c) + g(c)$
ii) $(f.g)(c) = f(c).g(c)$

Dejamos la demostración como ejercicio.

Teorema del resto. Sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces el resto de la división de f por $X - a$ es $f(a)$.

Demostración: Por el algoritmo de división, $\exists!\, q, r \in \mathbb{K}[X]$ tales que $f = (X-a).q + r$ y $r = 0$ o $\operatorname{gr} r < 1$. Ahora, especializando en a resulta que $f(a) = (a-a).q(a) + r(a) = r(a)$ y como $r = 0$ o $\operatorname{gr} r = 0$ entonces $r(a) = r$. Por lo tanto $r = f(a)$. □

Ejemplo. Sea $f \in \mathbb{Q}[X]$. Sabiendo que $f(1) = 2$, $f(-1) = 1$ y $f(-2) = -1$ podemos hallar el resto de la división de f por $g = (X-1)(X+1)(X+2)$. Notar que, por el teorema del resto, esto es lo mismo que decir que si conocemos el resto de la división de f por $X-1$, por $X+1$ y por $X+2$ entonces podemos calcular el resto de la división de f por $g = (X-1)(X+1)(X+2)$. (¿Esto no le recuerda el teorema chino del resto?)

Por el algoritmo de división, $f = g.q + r$, con $r = 0$ o $\operatorname{gr} r < 3$. Luego, $r = aX^2 + bX + c$ donde $a, b, c \in \mathbb{Q}$. Como $g(1) = g(-1) = g(-2) = 0$ entonces, especializando en 1, -1 y -2 se tienen el sistema de 3 ecuaciones con 3 incógnitas

$$\begin{aligned} 2 &= a + b + c \\ 1 &= a - b + c \\ -1 &= 4a - 2b + c \end{aligned}$$

cuyas soluciones son $a = -\frac{1}{2}$, $b = \frac{1}{2}$ y $c = 2$. Luego, el resto buscado es $-\frac{1}{2}X^2 + \frac{1}{2}X + 2$.

Congruencias. Dados $f, g, h \in \mathbb{K}[X]$ decimos que f es *congruente* a g *módulo* h, y escribimos $f \equiv g\ (h)$, si $h \mid g - f$. En tal caso escribimos $f \equiv g\ (h)$

Propiedades de la congruencia.

1) $f \equiv f\ (h)$ para todo $f, h \in \mathbb{K}[X]$
2) $f \equiv g\ (h) \Longrightarrow g \equiv f\ (h)$
3) $f \equiv g\ (h)$ y $g \equiv p\ (h) \Longrightarrow f \equiv p\ (h)$
4) $f \equiv g\ (h) \Longrightarrow f + p \equiv g + p\ (h)$ para todo $p \in \mathbb{K}[X]$
5) $f \equiv g\ (h) \Longrightarrow f.p \equiv g.p\ (h)$ para todo $p \in \mathbb{K}[X]$
6) $f \equiv g\ (h)$ y $p \equiv q\ (h) \Longrightarrow f + p \equiv g + q\ (h)$ y $f.p \equiv g.q\ (h)$
7) $f \equiv g\ (h) \Longrightarrow f^n \equiv g^n\ (h)$ para todo $n \in \mathbb{N}$
8) Si $h \neq 0$ y r es el resto de la división de f por h entonces $f \equiv r\ (h)$
9) Si $h \neq 0$ y $f \equiv r\ (h)$ donde $r = 0$ o $\operatorname{gr} r < \operatorname{gr} h$ entonces r es el resto de la división de f por h
10) $f \equiv 0\ (h) \Longleftrightarrow h \mid f$

11) $f \equiv f + hq\ (h)$ para todo $q \in \mathbb{K}[X]$
12) Sea $p \in \mathbb{K}[X]$. Entonces $f \equiv g\ (h) \iff f.p \equiv g.p\ (h.p)$

Dejamos las demostraciones de estas propiedades como ejercicio.

Ejemplo. Sea $f \in \mathbb{Q}[X]$, $f = 3X^{101} - 15X^{16} - 2X^7 - 5X^4 + 3X^3 + 2X^2 + 1$. Hallemos el resto de la división de f por $X^3 + 1$

Como $X^3 \equiv -1\ (X^3 + 1)$ entonces

$$\begin{aligned} X^{101} &= (X^3)^{33}X^2 \equiv (-1)^{33}X^2 = -X^2\ \ (X^3+1) \\ X^{16} &= (X^3)^5 X \equiv (-1)^5 X = -X\ \ (X^3+1) \\ X^7 &= (X^3)^2 X \equiv (-1)^2 X = X\ \ (X^3+1) \\ X^4 &= X^3 X \equiv -X\ \ (X^3+1) \end{aligned}$$

Luego, módulo $X^3 + 1$,

$$\begin{aligned} f &= 3X^{101} - 15X^{16} - 2X^7 - 5X^4 + 3X^3 + 2X^2 + 1 \equiv \\ &\equiv -3X^2 + 15X - 2X + 5X - 3 + 2X^2 + 1 = \\ &= -X^2 + 18X - 2 \end{aligned}$$

Como $f \equiv -X^2 + 18X - 2\ \ (X^3+1)$ y $\mathrm{gr}\,(-X^2 + 18X - 2) = 2 < 3 = \mathrm{gr}\,(X^3+1)$ entonces el resto de la división de f por $X^3 + 1$ es $-X^2 + 18X - 2$

Proposición. Sea $f \in \mathbb{K}[X]$ y sea $c \in \mathbb{K}$. Entonces existen únicos $a_0, a_1, \dots, a_n \in \mathbb{K}$ tales que

$$f = \sum_{i=0}^{n} a_i (X - c)^i$$

Notemos que esta proposición es el resultado análogo al desarrollo en base s para números enteros.

Observación. La proposición anterior puede formularse de la siguiente manera: Sea $f \in \mathbb{K}[X]$ y sea $c \in \mathbb{K}$. Entonces existe un único $g \in \mathbb{K}[X]$ tal que $f = g(X - c)$.

Ejemplo. Escribamos a $f = X^3 - 11X^2 + 19X + 20 \in \mathbb{Q}[X]$ en potencias de $X - 3$, es decir, hallemos $a_0, a_1, \dots, a_n \in \mathbb{Q}$ tales que $f = \sum_{i=0}^{n} a_i (X-3)^i$.

Tal como hacíamos para hallar el desarrollo en base s de un número entero, los a_i son los restos de divisiones sucesivas por $X - 3$

$$\begin{aligned} &X^3 - 11X^2 + 19X + 20 = (X-3).(X^2 - 8X - 5) + 5 \\ &X^2 - 8X - 5 = (X-3).(X-5) + (-20) \\ &X - 5 = (X-3).1 + (-2) \end{aligned}$$

de donde

$$\begin{aligned} f &= X^3 - 11X^2 + 19X + 20 = (X-3).(X^2 - 8X - 5) + 5 = \\ &= (X-3).[(X-3).(X-5) - 20] + 5 = \\ &= (X-3)^2.(X-5) - 20(X-3) + 5 = \\ &= (X-3)^2.[(X-3) - 2] - 20(X-3) + 5 = \\ &= (X-3)^3 - 2(X-3)^2 - 20(X-3) + 5 \end{aligned}$$

Luego, tomando $a_0 = 5$, $a_1 = -20$, $a_2 = -2$ y $a_1 = 1$ se tiene que $f = \sum_{i=0}^{n} a_i(X-3)^i$

Observación. Notemos que si $f \in \mathbb{Z}[X]$ y $c \in \mathbb{Z}$ entonces los cocientes y los restos de las sucesivas divisiones por $X - c$ son polinomios con coeficientes enteros ya que $X - c$ es mónico. Luego, los a_i así obtenidos son números enteros.

Máximo común divisor. Si $a, b \in \mathbb{Z}$, alguno de ellos no nulo, habíamos definido el máximo común divisor entre a y b como el único $d \in \mathbb{Z}$ tal que

i) $d \in \mathbb{N}$
ii) $d \mid a$ y $d \mid b$
iii) $c \mid a$ y $c \mid b \Longrightarrow c \mid d$
Si queremos dar una definición análoga para dos polinomios $f, g \in \mathbb{K}[X]$, está claro que las dos últimas condiciones se traducirán en
2) $d \mid f$ y $d \mid g$
3) $h \mid f$ y $h \mid g \Longrightarrow h \mid d$
pero necesitaremos reformular adecuadamente la condición i).
Si repasamos la demostración de la existencia y unicidad del máximo común divisor en $\mathbb{Z}$ observamos que i) sólo se usa para demostrar la unicidad: probamos que si d y d' satisfacen ii) y iii) entonces $d \mid d'$ y $d' \mid d$ lo que implica que $d = d'$ o $d = -d'$, es decir, $d = u.d'$ donde $u \in \mathcal{U}(\mathbb{Z})$. De la misma manera se ve que si $d, d' \in \mathbb{K}[X]$ satisfacen 2) y 3) entonces $d \mid d'$ y $d' \mid d$, de donde resulta que $\exists\, c \in \mathbb{K} - \{0\} = \mathcal{U}(\mathbb{K}[X])$ tal que $d = c.d'$, es decir, d y d' son asociados. Para garantizar la unicidad pediremos entonces que d sea mónico, ya que si $d = c.d'$ y ambos son mónicos entonces necesariamente $c = 1$ y por lo tanto $d = d'$.

Por lo tanto, dados dos polinomios $f, g \in \mathbb{K}[X]$, alguno de ellos no nulo, definimos el máximo común divisor entre f y g como el único $d \in \mathbb{K}[X]$ que es mónico y satisface las condiciones 2) y 3).

El siguiente teorema garantiza que un tal d existe y es único.

Teorema. Sean $f, g \in \mathbb{K}[X]$ tales que $f \neq 0$ o $g \neq 0$. Entonces $\exists!\, d \in \mathbb{K}[X]$ que satisface:

1) d es mónico
2) $d \mid f$ y $d \mid g$
3) $h \mid f$ y $h \mid g \Longrightarrow h \mid d$

Dejamos la demostración como ejercicio. Para probar la existencia probar que el conjunto

$$H = \{\mathrm{gr}\,(f.t + g.s) \,/\, t, s \in \mathbb{K}[X] \text{ y } f.t + g.s \text{ es mónico}\}$$

es un subconjunto no vacío de $\mathbb{N}_0$ y por lo tanto posee un primer elemento n. Luego, existen $t, s \in \mathbb{K}[X]$ tales que $n = \mathrm{gr}\,(f.t + g.s)$ y $f.t + g.s$ es mónico. Probar que $d = f.t + g.s$ satisface 1), 2) y 3).

Notación. Denotaremos por $(f : g)$ al máximo común divisor entre f y g, es decir, al único $d \in \mathbb{K}[X]$ que satisface las condiciones 1), 2) y 3) del teorema.

Corolario. Sean $f, g \in \mathbb{K}[X]$ tales que $f \neq 0$ o $g \neq 0$. Entonces $\exists\, t, s \in \mathbb{K}[X]$ tales que $(f : g) = f.t + g.s$.

Observación. Los polinomios t y s del corolario no son únicos.

Diremos que f y g son *coprimos* si $(f : g) = 1$.

Ejercicio. Probar que f y g no son coprimos si y sólo si existe un irreducible mónico $p \in \mathbb{K}[X]$ tal que $p \mid f$ y $p \mid g$.

Los irreducibles mónicos en $\mathbb{K}[X]$ son análogos a los primos positivos en $\mathbb{Z}$.

Propiedades del máximo común divisor. Sean $f, g \in \mathbb{K}[X]$ tales que $f \neq 0$ o $g \neq 0$. Entonces valen

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

2) Si f y f' son asociados y g y g' también son asociados entonces $(f : g) = (f' : g')$

3) Si p es un irreducible mónico entonces

$$(f : p) = \begin{cases} p & \text{si } p \mid f \\ 1 & \text{en otro caso} \end{cases}$$

4) Si $f \mid g$ entonces $(f : g) = a^{-1}.f$, donde a es el coeficiente principal de f. En particular, $(f : 0) = a^{-1}.f$, donde a es el coeficiente principal de f.

5) f y g son coprimos si y sólo si $\exists\, r, s \in \mathbb{K}[X]$ tales que $1 = rf + sg$

6) Si $d = (f : g)$ entonces $\frac{f}{d}, \frac{g}{d} \in \mathbb{K}[X]$ y $\left(\frac{f}{d} : \frac{g}{d}\right) = 1$

7) Sean $a, b \in \mathbb{K}$. Si $a \neq b$ entonces los polinomios $X - a$ y $X - b$ son coprimos.

Dejamos las demostraciones como ejercicio.

Proposición. Sean $f, g \in \mathbb{K}[X]$, $g \neq 0$. Si $f = g.q + r$, con $q, r \in \mathbb{K}[X]$, entonces $(f : g) = (g : r)$.

Demostración: Es igual que la de la proposición análoga para los enteros. □

Algoritmo de Euclides. Sean $f, g \in \mathbb{Q}[X]$, $f = X^4 + 2X^3 - X^2 - X + 1$ y $g = X^3 + 1$. Veamos cómo calcular $(f : g)$ y escribirlo como combinación lineal de f y g.

$$\begin{aligned} f &= g(X+2) + (-X^2 - 2X - 1) \\ g &= (-X^2 - 2X - 1)(-X+2) + (3X+3) \\ -X^2 - 2X - 1 &= (3X+3)\left(-\frac{1}{3}X - \frac{1}{3}\right) + 0 \end{aligned}$$

Luego, por la proposición anterior,

$$(f:g) = (g:-X^2-2X-1) = (-X^2-2X-1:3X+3) = (3X+3:0) = X+1$$

En general, si h es el último resto no nulo y c es el coeficiente principal de h entonces $d = c^{-1}.h$. Ahora escribimos a $3X+3$ como combinación lineal de f y g

$$\begin{aligned} 3X+3 =& g + (-X^2-2X-1)(X-2) = g + [f - g(X+2)](X-2) = \\ &= g[1-(X+2)(X-2)] + f(X-2) = \\ &= g(-X^2+5) + f((X-2) \end{aligned}$$

y finalmente escribimos a $(f:g) = X+1$ como combinación lineal de f y g en la forma

$$(f:g) = X+1 = g\left(-\frac{1}{3}X^2 + \frac{5}{3}\right) + f\left(\frac{1}{3}X - \frac{2}{3}\right)$$

Proposición. Sean $f, g, h \in \mathbb{K}[X]$. Si $f \mid g.h$ y $(f:g) = 1$ entonces $f \mid h$

Corolario. Sean $f, g \in \mathbb{K}[X]$ y sea $p \in \mathbb{K}[X]$ irreducible. Si $p \mid f.g$ entonces $p \mid f$ o $p \mid g$.

Ejercicio. Sean $a, b \in \mathbb{K}$, $a \neq b$ y sean $n, m \in \mathbb{N}$. Probar que $((X-a)^n : (X-b)^m) = 1$.

Proposición. Sean $f, g, h \in \mathbb{K}[X]$ tales que $(f:g) = 1$. Si $f \mid h$ y $g \mid h$ entonces $f.g \mid h$

Teorema fundamental de la aritmética. Recordemos que dado $a \in \mathbb{Z}$, $a \neq 0, 1, -1$, entonces a puede escribirse, de manera única, en la forma

$$a = \delta \prod_{i=1}^{r} p_i^{n_i}$$

donde $p_1 < p_2 < \ldots < p_r$ son primos positivos, $n_1, n_2, \ldots, n_r \in \mathbb{N}$ y $\delta \in \{1, -1\} = \mathcal{U}(\mathbb{Z})$. El resultado análogo para $\mathbb{K}[X]$ es el siguiente

Teorema. Sea $f \in \mathbb{K}[X]$. Si $f \neq 0$ y $\operatorname{gr} f > 0$ entonces existen $p_1, p_2, \ldots, p_r \in \mathbb{K}[X]$ irreducibles mónicos, $c \in \mathbb{K} - \{0\}$ y $n_1, n_2, \ldots, n_r \in \mathbb{N}$ tales que

$$f = c \prod_{i=1}^{r} p_i^{n_i}$$

Además, esta escritura es única salvo el orden de los factores.

4. Raíces.

Sea $\mathbb{K}$ un cuerpo (por ejemplo, $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}_p$ con p primo). Dado $f \in \mathbb{K}[X]$ diremos que $a \in \mathbb{K}$ es una *raíz* de f si $f(a) = 0$.

El hecho de conocer las raíces en $\mathbb{K}$ de un polinomio $f \in \mathbb{K}[X]$ nos será luego de gran utilidad para poder factorizarlo como producto de irreducibles.

Observación. Si $f \in \mathbb{K}[X]$ tal que $\operatorname{gr} f = 1$ entonces f tiene una raíz en $\mathbb{K}$. En efecto, si $f = aX + b$, con $a, b \in \mathbb{K}$, $a \neq 0$, entonces $-a^{-1}b \in \mathbb{K}$ es raíz de f. Pero si $\operatorname{gr} f > 1$ entonces puede ocurrir que f no tenga ninguna raíz en $\mathbb{K}$. Por ejemplo, $X^n - 3 \in \mathbb{Q}[X]$ $(n \geq 2)$ no tiene ninguna raíz en $\mathbb{Q}$ y $X^2 + 1 \in \mathbb{R}[X]$ no tiene ninguna raíz en $\mathbb{R}$.

Ejemplos.

1) Si $f = X^3 + 2X^2 - X - 2 \in \mathbb{Q}[X]$ entonces 1, -1 y -2 son raíces de f
2) Si p es primo y $f = X^p - X \in \mathbb{Z}_p[X]$ entonces a es raíz de f para todo $a \in \mathbb{Z}_p$
3) Si $f = X^8 - 1 \in \mathbb{C}[X]$ entonces $w \in \mathbb{C}$ es raíz de f si y sólo si $w \in G_8$
4) Si $f = X^2 + 1 \in \mathbb{C}[X]$ entonces las raíces de f en $\mathbb{C}$ son i y $-i$.
5) Sea $f = X^{1000} + 4X + 1 \in \mathbb{Z}_5[X]$. Hallemos las raíces de f en $\mathbb{Z}_5$.
Si $a \in \mathbb{Z}_5$ es raíz de f entonces $a \neq 0$. Luego, $a^4 = 1$ y por lo tanto $a^{1000} = 1$. Entonces $a \in \mathbb{Z}_5$ es raíz de f si y sólo si $1 + 4a + 1 = 0$, si y sólo si $a = 2$.

Criterio de Gauss. El siguiente teorema nos da un método para hallar las raíces racionales de un polinomio con coeficientes enteros.

Teorema. Sea $f \in \mathbb{Z}[X]$, $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, con $a_n \neq 0$ y sean $p \in \mathbb{Z}$ y $q \in \mathbb{N}$ tales que $(p : q) = 1$.

Si $\frac{p}{q}$ es raíz de f entonces $p \mid a_0$, $q \mid a_n$ y $p - kq \mid f(k)$ para todo $k \in \mathbb{Z}$.

Demostración: Si $\frac{p}{q}$ es raíz de f entonces

$$0 = f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0$$

Luego, $a_n\,p^n + a_{n-1}\,p^{n-1}q + a_{n-2}\,p^{n-2}q^2 + \cdots + a_1\,p\,q^{n-1} + a_0\,q^n = 0$ de donde resulta que

$$a_0\,q^n = -a_n\,p^n - a_{n-1}\,p^{n-1}q - a_{n-2}\,p^{n-2}q^2 - \cdots - a_1\,p\,q^{n-1}$$

y

$$a_n\,p^n = -a_{n-1}\,p^{n-1}q - a_{n-2}\,p^{n-2}q^2 - \cdots - a_1\,p\,q^{n-1} - a_0\,q^n$$

Luego, $p \mid a_0\,q^n$ y $q \mid a_n\,p^n$. Por lo tanto, como p y q son enteros coprimos, $p \mid a_0$ y $q \mid a_n$. Además, dado $k \in \mathbb{Z}$,

$$\begin{aligned}
q^n\,f(k) &= q^n[a_nk^n + a_{n-1}k^{n-1} + a_{n-2}\,k^{n-2} + \cdots + a_1k + a_0] = \\
&= a_n\,q^nk^n + a_{n-1}\,q^nk^{n-1} + a_{n-2}\,q^nk^{n-2} + \cdots + a_1q^nk + a_0\,q^n = \\
&= a_n\,q^nk^n + a_{n-1}\,q^nk^{n-1} + a_{n-2}\,q^nk^{n-2} + \cdots + a_1q^nk - a_n\,p^n - a_{n-1}\,p^{n-1}q- \\
&\qquad - a_{n-2}\,p^{n-2}q^2 - \cdots - a_2\,p^2q^{n-2} - a_1\,p\,q^{n-1} = \\
&= a_n\,(q^nk^n - p^n) + a_{n-1}\,q\,(q^{n-1}k^{n-1} - p^{n-1}) + a_{n-2}\,q^2\,(q^{n-2}k^{n-2} - p^{n-2}) + \\
&\qquad + \cdots + a_2\,q^{n-2}\,(q^2k^2 - p^2) + a_1q^{n-1}\,(qk - p)
\end{aligned}$$

y como $p-kq \mid (qk)^j - p^j$ para todo $j \in \mathbb{N}$ (recordar que si $a, b \in \mathbb{Z}$ entonces $a-b \mid a^m - b^m$ $\forall\, m \in \mathbb{N}$) entonces resulta que $p - kq \mid q^n\,f(k)$. Luego, observando que $p - kq$ y q^n son coprimos pues $(p : q) = 1$ concluímos que $p - kq \mid f(k)$. □

Corolario. Sea $f \in \mathbb{Z}[X]$, $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, con $a_n \neq 0$ y sean $p \in \mathbb{Z}$ y $q \in \mathbb{N}$ tales que $(p : q) = 1$. Si $\frac{p}{q}$ es raíz de f entonces $p \mid a_0$, $q \mid a_n$, $p - q \mid f(1)$ y $p + q \mid f(-1)$.

Ejemplos.

1) Hallemos todas las raíces racionales de $f \in \mathbb{Z}[X]$, $f = 2X^4 - 3X^3 - 3X - 2$
Si $\frac{p}{q}$ es raíz de f, con $p \in \mathbb{Z}$, $q \in \mathbb{N}$ y $(p : q) = 1$ entonces $p \mid 2$ y $q \mid 2$. Luego, $\frac{p}{q} = \pm 1, \pm 2, \pm\frac{1}{2}$. Veamos cuáles son raíces de f.
$f(1) = -6 \neq 0$
$f(-1) = 6 \neq 0$
$f(2) = 32 - 24 - 6 - 2 = 0$
$f(-2) = 32 + 24 + 6 - 2 \neq 0$
$f(\frac{1}{2}) = \frac{1}{8} - \frac{3}{8} - \frac{3}{2} - 2 \neq 0$ y
$f(-\frac{1}{2}) = \frac{1}{8} + \frac{3}{8} + \frac{3}{2} - 2 = 0$
Luego, las raíces racionales de f son 2 y $-\frac{1}{2}$.

2) Hallemos todas las raíces racionales de $f \in \mathbb{Q}[X]$, $f = 2X^6 + \frac{1}{3}X^5 + \frac{2}{3}X^4 + \frac{1}{2}X - 1$
Notemos que $f \notin \mathbb{Z}[X]$ pero si consideramos $g = 6f$ entonces f y g tienen las mismas raíces y $g = 12X^6 + 2X^5 + 4X^4 + 3X - 6 \in \mathbb{Z}[X]$. Luego, las raíces racionales de f son las raíces racionales de g y a éstas las podemos hallar aplicando el criterio de Gauss pues $g \in \mathbb{Z}[X]$.
Si $\frac{p}{q}$ es raíz de g, con $p \in \mathbb{Z}$, $q \in \mathbb{N}$ y $(p : q) = 1$ entonces $p \mid -6$ y $q \mid 12$. Además, $p-q \mid g(1)$ y $p+q \mid g(-1)$. Luego, las posibles raíces racionales son $\frac{p}{q} = \pm 1, \pm 2, \pm 3, \pm 6, \pm\frac{1}{2}$, $\pm\frac{1}{3}$, $\pm\frac{1}{4}$, $\pm\frac{1}{6}$, $\pm\frac{1}{12}$, $\pm\frac{2}{3}$, $\pm\frac{3}{2}$, $\pm\frac{3}{4}$, y como $g(1) = 15$ y $g(-1) = 5$ entonces 1 y -1 no son raíces de g, $p - q \mid 15$ y $p + q \mid 5$.
Por otra parte, notando que si $a > 1$ entonces $12a^6 + 2a^5 + 4a^4 + 3a > 12 + 2 + 4 + 3$ resulta que $2, 3, 6 y \frac{3}{2}$ no pueden ser raíces de g. Veamos qué ocurre con cada una de las restantes

posibles raíces:

$$
\begin{array}{l}
-3 \text{ no satisface } p-q \mid 15 \text{ pues } p-q=-4 \\
-6 \text{ no satisface } p-q \mid 15 \text{ pues } p-q=-7 \\
\frac{1}{2} \text{ no satisface } p+q \mid 5 \text{ pues } p+q=3 \\
\frac{1}{3} \text{ no satisface } p+q \mid 5 \text{ pues } p+q=4 \\
\frac{1}{6} \text{ no satisface } p+q \mid 5 \text{ pues } p+q=7 \\
-\frac{1}{3} \text{ no satisface } p-q \mid 15 \text{ pues } p-q=-4 \\
-\frac{1}{6} \text{ no satisface } p-q \mid 15 \text{ pues } p-q=-7 \\
\frac{3}{4} \text{ no satisface } p+q \mid 5 \text{ pues } p+q=-7 \\
-\frac{3}{4} \text{ no satisface } p-q \mid 15 \text{ pues } p-q=-7 \\
\frac{1}{12} \text{ no satisface } p+q \mid 5 \text{ pues } p+q=13 \\
-\frac{1}{12} \text{ no satisface } p+q \mid 5 \text{ pues } p+q=11
\end{array}
$$

Luego, falta ver si $g(\frac{p}{q})=0$ para $\frac{p}{q}=-2,-\frac{1}{2},\frac{2}{3},-\frac{2}{3},-\frac{3}{2},\ \frac{1}{4},\ -\frac{1}{4}$
$g(-2)=12.2^6-2.2^5+4.2^4-3.2-6=(12-1+1).2^6-12=12(2^6-1)\neq 0$
$g(-\frac{1}{2})=12\frac{1}{2^6}-2\frac{1}{2^5}+4\frac{1}{2^4}-\frac{3}{2}-6=\frac{3}{2^4}-\frac{1}{2^4}+\frac{4}{2^4}-\frac{3}{2}-6=\frac{6}{2^4}-\frac{3}{2}-6=\frac{3}{8}-\frac{12}{8}-6\neq 0$
$g(\frac{2}{3})=12\frac{2^6}{3^6}+2\frac{2^5}{3^5}+4\frac{2^4}{3^4}+3\frac{2}{3}-6=4\frac{2^6}{3^5}+\frac{2^6}{3^5}+3\frac{2^6}{3^5}+2-6=8\frac{2^6}{3^5}-4\neq 0$
$g(-\frac{2}{3})=12\frac{2^6}{3^6}-2\frac{2^5}{3^5}+4\frac{2^4}{3^4}-3\frac{2}{3}-6=4\frac{2^6}{3^5}-\frac{2^6}{3^5}+\frac{2^6}{3^4}-2-6=3\frac{2^6}{3^5}+\frac{2^6}{3^4}-8=2\frac{2^6}{3^4}-8\neq 0$
$g(-\frac{3}{2})=12\frac{3^6}{2^6}-2\frac{3^5}{2^5}+4\frac{3^4}{2^4}-3\frac{3}{2}-6=27\frac{3^4}{2^4}-3\frac{3^4}{2^4}+4\frac{3^4}{2^4}-\frac{9}{2}-6=28\frac{3^4}{2^4}-\frac{9}{2}-6=7\frac{3^4}{4}-\frac{21}{2}\neq 0$
Dejamos como tarea al lector verificar que $g(\frac{1}{4})<0$ y $g(-\frac{1}{4})<0$. Luego, g (y por lo tanto f) no tiene raíces en $\mathbb{Q}$.

Proposición. Sean $f\in\mathbb{R}[X]$ y $z\in\mathbb{C}$. Entonces z es raíz de f si y sólo si $\overline{z}$ es raíz de f.

Demostración: Como $f\in\mathbb{R}[X]$ entonces $f=\sum_{i=0}^{n}a_iX^i$ donde $a_i\in\mathbb{R}$. Luego,

$$
f(z)=0 \iff \sum_{i=0}^{n}a_iz^i=0 \iff \overline{\sum_{i=0}^{n}a_iz^i}=0 \iff \sum_{i=0}^{n}\overline{a_i}\,\overline{z^i}=0 \iff
$$
$$
\iff \sum_{i=0}^{n}a_i\overline{z}^i=0 \iff f(\overline{z})=0
$$

ya que $\overline{a_i}=a_i$ pues $a_i\in\mathbb{R}$. $\square$

Teorema fundamental del álgebra. Sea $f \in \mathbb{C}[X]$. Si $\operatorname{gr} f \geq 1$ entonces f tiene al menos una raíz en $\mathbb{C}$.

No veremos la demostración de este teorema ya que excede los alcances del curso.

Proposición. Sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces a es raíz de f si y sólo si $X - a \mid f$.

Demostración: Es consecuencia inmediata del teorema del resto. $\square$

Corolario 1. Sea $f \in \mathbb{K}[X]$ un polinomio no nulo de grado n. Entonces f tiene a lo sumo n raíces distintas en $\mathbb{K}$.

Demostración: Sean $a_1, a_2, \ldots, a_m$ las raíces distintas de f en $\mathbb{K}$. Entonces, por la proposición anteriror, $X - a_i \mid f$ $(1 \leq i \leq m)$ y, como $(X - a_i : X - a_j) = 1$ para $i \neq j$ entonces

$$(X - a_1)(X - a_2) \ldots (X - a_m) \mid f$$

Luego, $m = \operatorname{gr}((X - a_1)(X - a_2) \ldots (X - a_m)) \leq \operatorname{gr} f = n$. $\square$

Corolario 2. Sea $f \in \mathbb{C}[X]$. Entonces f es irreducible en $\mathbb{C}[X]$ si y sólo si $\operatorname{gr} f = 1$.

Demostración: $(\Longleftarrow)$ Vimos antes que esta implicación vale.
$(\Longrightarrow)$ Si f es irreducible en $\mathbb{C}[X]$ entonces, por el teorema fundamental del álgebra, f tiene una raíz $a \in \mathbb{C}$. Luego, $X - a \mid f$ y, como f es irreducible entonces f y $X - a$ deben ser asociados, de donde $\operatorname{gr} f = \operatorname{gr}(X - a) = 1$. $\square$

Corolario 3. Sea $f \in \mathbb{C}[X]$ tal que $\operatorname{gr} f \geq 1$. Entonces la factorización de f en $\mathbb{C}[X]$ es de la forma

$$f = c(X - a_1)(X - a_2) \ldots (X - a_n)$$

donde $a_1, a_2, \ldots, a_n \in \mathbb{C}$ (no necesariamente distintos) y $c \in \mathbb{C}$, $c \neq 0$.

Demostración: Es consecuencia inmediata del teorema fundamental de la aritmética y el corolario 2. $\square$

Observación. Sea $f \in \mathbb{K}[X]$. Si $f = c(X - a_1)(X - a_2) \ldots (X - a_n)$, con $a_1, a_2, \ldots, a_n \in \mathbb{K}$ y $c \in \mathbb{K}$, $c \neq 0$, entonces c es el coeficiente principal de f, $n = \operatorname{gr} f$ y $a_1, a_2, \ldots, a_n$ son las raíces de f en $\mathbb{K}$.

Ejemplo. Sean $a, b, c \in \mathbb{C}$ las raíces de $f = 2X^3 - X^2 + 3X + 4$. Hallar $a + b + c$, $a^2 + b^2 + c^2$, $a^3 + b^3 + c^3$, $a^4 + b^4 + c^4$, $\frac{1}{a} + \frac{1}{b} + \frac{1}{c}$ y $\frac{1}{ab} + \frac{1}{bc} + \frac{1}{ac}$

Como a, b y c son las raíces de f y el coeficiente principal de f es 2 entonces

$$f = 2(X - a)(X - b)(X - c) = 2[X^3 - (a + b + c)X^2 + (ab + bc + ac)X - abc]$$

Luego, $2X^3 - X^2 + 3X + 4 = 2X^3 - 2(a + b + c)X^2 + 2(ab + bc + ac)X - 2abc]$, de donde $-1 = -2(a + b + c)$, $3 = 2(ab + bc + ac)$ y $4 = -2abc$. Por lo tanto, $a + b + c = \frac{1}{2}$, $ab + bc + ac = \frac{3}{2}$ y $abc = -2$.

Luego,

$$a+b+c=\frac{1}{2}$$

$$a^2+b^2+c^2=(a+b+c)^2-2(ab+bc+ac)=\frac{1}{4}-3=-\frac{11}{4}$$

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=\frac{bc+ac+ab}{abc}=\frac{\frac{3}{2}}{-2}=-\frac{3}{4}$$

Veamos cómo calcular $a^3+b^3+c^3$. Como a, b y c son raíces de f entonces

$$2a^3=a^2-3a-4$$
$$2b^3=b^2-3b-4$$
$$2c^3=c^2-3c-4$$

Por lo tanto $2(a^3+b^3+c^3)=a^2+b^2+c^2-3(a+b+c)-12=-\frac{11}{4}-\frac{3}{2}-12$. Dejamos como ejercicio hallar $a^4+b^4+c^4$. Sugerencia:

$$2a^3=a^2-3a-4\Longrightarrow 2a^4=a^3-3a^2-4a$$
$$2b^3=b^2-3b-4\Longrightarrow 2b^4=b^3-3b^2-4b$$
$$2c^3=c^2-3c-4\Longrightarrow 2c^4=c^3-3c^2-4c$$

de donde $2(a^4+b^4+c^4)=a^3+b^3+c^3-3(a^2+b^2+c^2)-4(a+b+c)$.

Finalmente, calculemos $\frac{1}{ab}+\frac{1}{bc}+\frac{1}{ac}=\frac{c+a+b}{abc}=\frac{\frac{1}{2}}{-2}=-\frac{1}{4}$

Corolario 4. Sea $f\in\mathbb{R}[X]$. Si $\operatorname{gr} f$ es impar entonces f tiene al menos una raíz en $\mathbb{R}$.

Demostración: Sea $n=\operatorname{gr} f$. Entonces $n=2k-1$ para algún $k\in\mathbb{N}$. Demostraremos el corolario por inducción en k.

Si $k=1$ entonces $\operatorname{gr} f=1$. Luego $f=aX+b$, con $a,b\in\mathbb{R}$, $a\neq 0$. En este caso $-a^{-1}b\in\mathbb{R}$ es raíz de f.

Supongamos ahora que el corolario vale para k y sea $f\in\mathbb{R}[X]$ un polinomio de grado $2(k+1)-1=2k+1$. Sea $z\in\mathbb{C}$ una raíz de f (teorema fundamental del álgebra). Si $z\in\mathbb{R}$ entonces f tiene una raíz real. Supongamos entonces que $z\notin\mathbb{R}$. Entonces, como $f\in\mathbb{R}[X]$, $\overline{z}$ es raíz de f y $\overline{z}\neq z$. Luego, $X-z\mid f$, $X-\overline{z}\mid f$ y $(X-z:X-\overline{z})=1$. Por lo tanto $(X-z)(X-\overline{z})\mid f$, es decir, existe $h\in\mathbb{C}[X]$ tal que $f=(X-z)(X-\overline{z}).h$. Pero como $f\in\mathbb{R}[X]$ y $(x-z)(X-\overline{z})=X^2-(z+\overline{z})X+z\,\overline{z}=X^2-2\mathrm{Re}(z)+|z|^2\in\mathbb{R}[X]$, entonces $h\in\mathbb{R}[X]$.

Usando ahora la hipótesis inductiva para h, que tiene grado $2k-1$, resulta que h tiene una raíz $a\in\mathbb{R}$, y por lo tanto f tiene una raíz en $\mathbb{R}$ pues $f(a)=(a-z)(a-\overline{z}).h(a)=0$. □

Corolario 5. Sea $f\in\mathbb{K}[X]$ tal que $\operatorname{gr} f\geq 2$. Si f es irreducible en $\mathbb{K}[X]$ entonces f no tiene raíces en $\mathbb{K}$.

Demostración: Sea f irreducible en $\mathbb{K}[X]$ y supongamos que f tiene una raíz $a \in \mathbb{K}$. Luego, $X - a \mid f$ en $\mathbb{K}[X]$ y, como f es irreducible entonces f y $X - a$ deben ser asociados, de donde $\operatorname{gr} f = \operatorname{gr}(X - a) = 1$. Luego esto no puede ocurrir cuando $\operatorname{gr} f \geq 2$. □

Observación. El polinomio $f = (X^2 + 1)(X^4 + 3) \in \mathbb{R}[X]$ no tiene raíces en $\mathbb{R}$ pero no es irreducible en $\mathbb{R}[X]$.

Proposición. Sea $f \in \mathbb{K}[X]$. Si $\operatorname{gr} f = 2$ o 3 entonces f es irreducible en $\mathbb{K}[X]$ si y sólo si f no tiene raíces en $\mathbb{K}$.

Demostración: ($\Longrightarrow$) Ya vimos que esta implicación vale (corolario 5).

($\Longleftarrow$) Supongamos que f no tiene raíces en $\mathbb{K}$. Sea $g \in \mathbb{K}[X]$ tal que $g \mid f$. Entonces $\operatorname{gr} g \leq \operatorname{gr} f$ y $f = g.h$ para algún $h \in \mathbb{K}[X]$.

Supongamos primero que $\operatorname{gr} f = 2$. Entonces $\operatorname{gr} g = 0, 1, 2$. Si $\operatorname{gr} g = 0$ entonces g es una unidad, si $\operatorname{gr} g = 1$ entonces g (y por lo tanto $f = g.h$) tendría una raíz en $\mathbb{K}$, lo cual no puede ocurrir y si $\operatorname{gr} g = 2$ entonces $\operatorname{gr} h = 0$ y por lo tanto h es una unidad. Luego, f y g son asociados.

Supongamos ahora que $\operatorname{gr} f = 3$. Entonces $\operatorname{gr} g = 0, 1, 2, 3$. Si $\operatorname{gr} g = 0$ entonces g es una unidad y si $\operatorname{gr} g = 3$ entonces f y g son asociados. Veamos que los casos $\operatorname{gr} g = 1, 2$ no pueden ocurrir. Si $\operatorname{gr} g = 1$ entonces g, y por lo tanto f, tendría una raíz en $\mathbb{K}$. Finalmente, si $\operatorname{gr} g = 2$, como $f = g.h$ entonces $\operatorname{gr} h = 1$ de donde h, y por lo tanto f, tendría una raíz en $\mathbb{K}$. □

Corolario. Sea $f \in \mathbb{R}[X]$. Entonces f es irreducible en $\mathbb{R}[X]$ si y sólo si $\operatorname{gr} f = 1$ o $\operatorname{gr} f = 2$ y f no tiene raíces reales.

Demostración: Ya vimos que los polinomios de grado 1 son irreducibles y la proposición anterior garantiza que si $\operatorname{gr} f = 2$ entonces f es irreducible en $\mathbb{R}[X]$ si y sólo si f no tiene raíces reales.

Veamos ahora que no puede haber polinomios de grado mayor que 2 en $\mathbb{R}[X]$ que sean irreducibles.

Supongamos que f es irreducible en $\mathbb{R}[X]$. Sea $z \in \mathbb{C}$ una raíz de f. Si $z \in \mathbb{R}$ entonces $X - z \mid f$ en $\mathbb{R}[X]$ y como f es irreducible entonces $\operatorname{gr} f = 1$. Y si $z \notin \mathbb{R}$ entonces existe $h \in \mathbb{R}[X]$ tal que $f = (X^2 - 2\mathrm{Re}(z)X - |z|^2).h$ (ver demostración del corolario 4). Luego, $X^2 - 2\mathrm{Re}(z)X - |z|^2 \in \mathbb{R}[X]$ y divide a f. Como f es irreducible en $\mathbb{R}[X]$ entonces f y $X^2 - 2\mathrm{Re}(z)X - |z|^2$ deben ser asociados y por lo tanto $\operatorname{gr} f = 2$. □

Observación. El corolario anterior no vale para $\mathbb{Q}[X]$. En $\mathbb{Q}[X]$ hay polinomios irreducibles de grado tan grande como se desee, por ejemplo el polinomio $X^n - 2$ es irreducible en $\mathbb{Q}[X]$ para todo $n \in \mathbb{N}$. No veremos la demostración de este hecho ya que excede los alcances de este curso.

Ejemplos.

1) Factoricemos en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ el polinomio $f = 2X^5+3X^4-X^2-2X+1$ sabiendo que $-\frac{1}{2}-\frac{\sqrt{3}}{2}\,i$ es raíz de f.

Sea $z = -\frac{1}{2}-\frac{\sqrt{3}}{2}\,i$. Como $f \in \mathbb{R}[X]$ y z es raíz de f entonces $\overline{z}$ es raíz de f. Luego, $X^2+X+1 = X^2-2\mathrm{Re}(z)X-|z|^2 \mid f$. Dividiendo f por X^2+X+1 (cuyas raíces son $-\frac{1}{2}\pm\frac{\sqrt{3}}{2}\,i$) se tiene que

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

Ahora buscamos las restantes raíces de f que son las raíces de $g = 2X^3+X^2-3X+1$. Como $g \in \mathbb{Z}[X]$, aplicando el criterio de Gauss vemos que $\frac{1}{2}$ es raíz de g. Luego, $X-\frac{1}{2} \mid g$. Dividimos ahora g por $X-\frac{1}{2}$:

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

Ahora buscamos las raíces de $2X^2+2X-2$ que son $-\frac{1}{2}\pm\frac{\sqrt{5}}{2}$.
Por lo tanto las raíces de f en $\mathbb{C}$ son $-\frac{1}{2}\pm\frac{\sqrt{3}}{2}\,i$, $\frac{1}{2}$ y $-\frac{1}{2}\pm\frac{\sqrt{5}}{2}$ y la factorización de f en $\mathbb{C}[X]$ es

$$f = 2(X-(-\frac{1}{2}-\frac{\sqrt{3}}{2}\,i))(X-(-\frac{1}{2}+\frac{\sqrt{3}}{2}\,i))(X-\frac{1}{2})(X-(-\frac{1}{2}+\frac{\sqrt{5}}{2}))(X-(-\frac{1}{2}-\frac{\sqrt{5}}{2}))$$

Los factores son irreducibles en $\mathbb{C}[X]$ porque tienen grado 1. La factorización de f en $\mathbb{R}[X]$ es

$$f = 2(X^2+X+1)(X-\frac{1}{2})(X-(-\frac{1}{2}+\frac{\sqrt{5}}{2}))(X-(-\frac{1}{2}-\frac{\sqrt{5}}{2}))$$

Los factores son irreducibles en $\mathbb{R}[X]$ por ser polinomios de grado 1 o polinomios de grado 2 que no tienen raíces reales. La factorización en $\mathbb{Q}[X]$ es

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

Los factores son irreducibles en $\mathbb{Q}[X]$ por ser polinomios de grado 1 o polinomios de grado 2 que no tienen raíces racionales.

2) Factoricemos en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ el polinomio $f = X^4-3$.

Las raíces de f en $\mathbb{C}$ son los $z \in \mathbb{C}$ tales que $z^4 = 3$, es decir, las raíces cuartas de 3 que son $\sqrt[4]{3}$, $-\sqrt[4]{3}$, $\sqrt[4]{3}\,i$ y $-\sqrt[4]{3}\,i$. Luego, la factorización de f en $\mathbb{C}[X]$ es

$$f = (X-\sqrt[4]{3})(X+\sqrt[4]{3})(X-\sqrt[4]{3}\,i)(X+\sqrt[4]{3}\,i)$$

Los factores son irreducibles en $\mathbb{C}[X]$ porque tienen grado 1. La factorización de f en $\mathbb{R}[X]$ es $f = (X-\sqrt[4]{3})(X+\sqrt[4]{3})(X^2+\sqrt{3})$. Los factores son irreducibles en $\mathbb{R}[X]$ por ser polinomios de grado 1 o polinomios de grado 2 que no tienen raíces reales. La factorización en $\mathbb{Q}[X]$ es $f = X^4-3$. Veamos que el polinomio X^4-3 es irreducible en $\mathbb{Q}[X]$. Supongamos que existe $g \in \mathbb{Q}[X]$ tal que $g \mid X^4 - 3$, con $\operatorname{gr} g = 1$, 2 o 3. Entonces $X^4 - 3 = g.h$ para algún $h \in \mathbb{Q}[X]$. Si $\operatorname{gr} g = 1$ entonces g, y por lo tanto $X^4 - 3$, tendría una raíz en $\mathbb{Q}$ y si $\operatorname{gr} g = 3$ entonces $\operatorname{gr} h = 1$ y por lo tanto h, y en consecuencia $X^4 - 3$, tendría una raíz en $\mathbb{Q}$. Luego, $\operatorname{gr} g = 2 = \operatorname{gr} h$, $g, h \in \mathbb{R}[X]$ y $f = X^4 - 3 = g.h$. Pero como $X^2 + \sqrt{3}$ es irreducible en $\mathbb{R}[X]$ y divide a f entonces, en $\mathbb{R}[X]$, $X^2 + \sqrt{3} \mid g$ o $X^2 + \sqrt{3} \mid h$. Luego, como todos tienen grado 2, $X^2 + \sqrt{3}$ y g son asociados o $X^2 + \sqrt{3}$ y h lo son. Por lo tanto, $c(X^2 + \sqrt{3}) = g \in \mathbb{Q}[X]$ para algún $c \in \mathbb{R}$ no nulo o $c(X^2 + \sqrt{3}) = h \in \mathbb{Q}[X]$ para algún $c \in \mathbb{R}$ no nulo. Luego debe ser $c \in \mathbb{Q}$ y $c\sqrt{3} \in \mathbb{Q}$, lo que implica que $\sqrt{3} \in \mathbb{Q}$, cosa que no es verdadera.

Como se ve en el ejemplo anterior, probar que un polinomio $f \in \mathbb{Q}[X]$ es irreducible no es sencillo.

Proposición. Sean $f, g \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces a es raíz de f y de g si y sólo si a es raíz de $(f : g)$.

Demostración: Sea $d = (f : g)$. Dado $a \in \mathbb{K}$, a es raíz de f y de g si y sólo si $X - a \mid f$ y $X - a \mid g$ si y sólo si $X - a \mid d$ si y sólo si a es raíz de d. $\square$

Corolario. Sean $f, g \in \mathbb{C}[X]$. Entonces f y g no tienen raíces comunes en $\mathbb{C}$ si y sólo si $(f : g) = 1$.

Demostración: ($\Longrightarrow$) Sea $d = (f : g)$. Si $d \neq 1$ entonces $\operatorname{gr} d \geq 1$. Luego, d tiene una raíz $a \in \mathbb{C}$ y por lo tanto a es raíz de f y de g.

($\Longleftarrow$) Si $(f : g) = 1$ entonces existen $s, t \in \mathbb{C}[X]$ tales que $1 = fs + tg$ y por lo tanto no puede existir $a \in \mathbb{C}$ tal que $f(a) = 0 = g(a)$. $\square$

Teorema de Wilson. Sea $p \in \mathbb{Z}$ un primo positivo. Entonces $(p-1)! \equiv -1\ (p)$.

Demostración: Consideremos el polinomio $f = X^{p-1} - 1 \in \mathbb{Z}_p[X]$. Por el teorema de Fermat, $1, 2, 3, \dots, p-1 \in \mathbb{Z}_p$ son $p-1$ raíces distintas de f.

Luego, $(X-1)(X-2)(X-3)\dots(X-(p-1)) \mid f$ en $\mathbb{Z}_p[X]$ y, como f tiene grado $p-1$ y es mónico entonces

$$f = (X-1)(X-2)(X-3)\dots(X-(p-1))$$

Por lo tanto, especializando en cero y multiplicando ambos miembros por $(-1)^{p-1}$ se tiene que, en $\mathbb{Z}_p$

$$(-1)^p = (-1)^{p-1} f(0) = 1.2.3\dots(p-1) = (p-1)!$$

es decir, $(p-1)! \equiv (-1)^p\ (p)$. Notando que cuando $p = 2$ entonces $(-1)^p = 1 \equiv -1 (p)$ y que cuando $p \neq 2$ entonces $(-1)^p = -1$ pues p es impar, resulta que $(p-1)! \equiv -1\ (p)$. $\square$

5. Polinomio derivado y multiplicidad de raíces.

Sea $\mathbb{K}$ un cuerpo. Dado $n \in \mathbb{N}$, podemos ver a n como el elemento de $\mathbb{K}$ que se obtiene sumando n veces el elemento neutro del producto, es decir, el elemento $\underbrace{1+1+\cdots+1}_{n \text{ sumandos}} \in \mathbb{K}$.

Sea $f \in \mathbb{K}[X]$, $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$. Definimos el *derivado* de f, al que denotaremos por f', como el polinomio en $\mathbb{K}[X]$

$$f' = n\,a_nX^{n-1} + (n-1)\,a_{n-1}X^{n-2} + \cdots + 2\,a_2X + a_1$$

Ejemplos.

1) Sea $f \in \mathbb{Q}[X]$, $f = 2X^{11} - \frac{1}{4}X^8 + \frac{3}{5}X^6 + 5X^2 - \frac{2}{3}$. Entonces el derivado de f es $f' = 22X^{10} - 2X^7 + \frac{18}{5}X^5 + 10X$.

2) Sea $f = 4X^9 + 3X^7 + X^5 + 5X^4 + 4X^2 + 6X + 3 \in \mathbb{Z}_7[X]$. Entonces el derivado de f es $f' = X^8 + 5X^4 + 6X^3 + X + 6$.

Propiedades del derivado. Sean $f, g \in \mathbb{K}[X]$. Entonces se verifican

i) $(f+g)' = f' + g'$
ii) $(f.g)' = f'.g + f.g'$

Proposición. Sea $\mathbb{K}$ un cuerpo de característica cero, es decir, tal que $\underbrace{1+1+\cdots+1}_{n \text{ sumandos}} \neq 0$ para todo $n \in \mathbb{N}$ (por ejemplo, $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y sea $f \in \mathbb{K}[X]$.
Entonces se verifican

i) $f' = 0$ si y sólo si $f = c$ para algún $c \in \mathbb{K}$
ii) Si $f' \neq 0$ entonces $\operatorname{gr} f' = \operatorname{gr} f - 1$

Dejamos la demostración como ejercicio. Observemos que la hipótesis de que $\mathbb{K}$ tenga característica cero es esencial. En efecto, si $f \in \mathbb{Z}_p[X]$ es el polinomio $f = X^p - 1$ entonces $f' = 0$ (es decir, no se satisface i)) y si $f \in \mathbb{Z}_p[X]$ es el polinomio $f = X^p + X + 1$ entonces $f' = 1$ (es decir, no se satisface ii)).

Sea $\mathbb{K}$ un cuerpo (por ejemplo, $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{Z}_p$) y sea $f \in \mathbb{K}[X]$. Diremos que $a \in \mathbb{K}$ es raíz de f de *multiplicidad* m si existe $g \in \mathbb{K}[X]$ tal que $f = (X-a)^m.g$ y $g(a) \neq 0$, es decir, si $(X-a)^m \mid f$ y $(X-a)^{m+1} \nmid f$. En tal caso escribimos $m = \operatorname{mult}(a, f)$.

Diremos que $a \in \mathbb{K}$ es raíz *simple* de f si $\operatorname{mult}(a,f) = 1$, *doble* si $\operatorname{mult}(a,f) = 2$ y *triple* si $\operatorname{mult}(a,f) = 3$. Diremos que $a \in \mathbb{K}$ es raíz *múltiple* de f si $\operatorname{mult}(a,f) \geq 2$.

Ejemplo. Si $f \in \mathbb{Z}_5[X]$, $f = X^6 - X$ entonces 0 es raíz simple de f y 1 es raíz múltiple de f. Más aún, $\operatorname{mult}(1,f) = 5$ ya que $f = X\,(X-1)^5$

Observación. Sea $f \in \mathbb{K}[X]$ un polinomio de grado $n > 0$. Si $a_1, a_2, \ldots, a_r$ son las raíces de f en $\mathbb{K}$ y $m_i = \text{mult}(a_i, f)$ entonces $(X - a_i)^{m_i} \mid f$ $(1 \le i \le r)$. Luego, como $(X - a_i)^{m_i}$ y $(X - a_j)^{m_j}$ son coprimos para todo $i \neq j$, se tiene que

$$\prod_{i=1}^{r} (X - a_i)^{m_i} \mid f$$

y por lo tanto $m_1 + m_2 + \cdots + m_r \le \operatorname{gr} f = n$. Es decir, un polinomio $f \in \mathbb{K}[X]$ de grado n tiene a lo sumo n raíces en $\mathbb{K}$, contadas con multiplicidad.

En particular, si $\mathbb{K} = \mathbb{C}$, dado $f \in \mathbb{C}[X]$ polinomio de grado $n > 0$ cuyas raíces en $\mathbb{C}$ son $a_1, a_2, \ldots, a_r$ y $m_i = \text{mult}(a_i, f)$ entonces

$$\prod_{i=1}^{r} (X - a_i)^{m_i} \mid f$$

Por lo tanto,

$$f = g. \prod_{i=1}^{r} (X - a_i)^{m_i}$$

y $g(a_i) \neq 0$ $(1 \le i \le r)$ ya que $(X - a_i)^{m_i + 1} \not| f$. Luego debe ser $\operatorname{gr} g = 0$ pues si $\operatorname{gr} g \ge 1$ entonces g (y en consecuencia f) tendría una raíz $a \in \mathbb{C}$, con $a \neq a_1, a_2, \ldots, a_r$. Luego, la factorización de f en $\mathbb{C}[X]$ es

$$f = c. \prod_{i=1}^{r} (X - a_i)^{m_i}$$

$a_1, a_2, \ldots, a_r$ son las raíces de f en $\mathbb{C}$, $m_i = \text{mult}(a_i, f)$ y $c \in \mathbb{C}$ es el coeficiente principal de f.

Sea $f \in \mathbb{K}[X]$ y sea $n \in \mathbb{N}_0$. Definimos el *derivado n-ésimo* de f, al que denotaremos por $f^{(n)}$, inductivamente en la forma

$$f^{(n)} = \begin{cases} f & \text{si } n = 0 \\ (f^{(n-1)})' & \text{si } n \ge 1 \end{cases}$$

Proposición. Sea $\mathbb{K}$ un cuerpo de característica cero (por ejemplo, $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces, dado $m \in \mathbb{N}$, $m \ge 2$ se verifica:

a es raíz de f de multiplicidad $m \iff f(a) = 0$ y a es raíz de f' de multiplicidad $m - 1$

Demostración: $(\Longrightarrow)$ $f = (X - a)^m.g$, con $g \in \mathbb{K}[X]$ tal que $g(a) \neq 0$. Luego, $f(a) = 0$ y

$$f' = m(X - a)^{m-1}.g + (X - a)^m.g' = (X - a)^{m-1}(mg + (X - a)g')$$

Por lo tanto $f(a) = 0$ y $f' = (X - a)^{m-1} h$, donde $h = mg + (X - a)g' \in \mathbb{K}[X]$ y $h(a) = m.g(a) \neq 0$.

($\Longleftarrow$) Supongamos que $f(a) = 0$ y $f' = (X-a)^{m-1}.h$, donde $h(a) \neq 0$.
Por el algoritmo de división, existen $q, r \in \mathbb{K}[X]$ tales que $f = (X-a)^m.q + r$ y $r = 0$ o $\operatorname{gr} r < m$. Probaremos que $r = 0$ y que $q(a) \neq 0$.
Utilizando las propiedades del derivado se tiene que

$$f' = m(X-a)^{m-1}q + (X-a)^m q' + r' = (X-a)^{m-1}(mq + (X-a)q') + r'$$

y, como $\mathbb{K}$ tiene característica cero, $r' = 0$ o $\operatorname{gr} r' = \operatorname{gr} r - 1 < m-1$. Como $(X-a)^{m-1} \mid f'$ entonces $(X-a)^{m-1} \mid r'$. Luego debe ser $r' = 0$, de donde resulta que $r = c$ para algún $c \in \mathbb{K}$. Por lo tanto $(X-a)^{m-1}.h = f' = (X-a)^{m-1}(mq + (X-a)q')$ de donde resulta que $h = mq + (X-a)q'$ y, en consecuencia, $q(a) \neq 0$ pues $h(a) \neq 0$.
Luego, $f = (X-a)^m.q + c$, con $c \in \mathbb{K}$ y $q \in \mathbb{K}[X]$ tal que $q(a) \neq 0$. Finalmente, especializando en a y teniendo en cuenta que $f(a) = 0$, se tiene que $c = 0$. □

Proposición. Sea $\mathbb{K}$ un cuerpo de característica cero (por ejemplo, $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces, dado $m \in \mathbb{N}$, se verifica:

a es raíz de f de multiplicidad $m \Longleftrightarrow f^{(k)}(a) = 0 \ \ \forall\, 0 \leq k \leq m-1$ y $f^{(m)}(a) \neq 0$

Demostración: Por inducción en m. Veamos primero que vale para $m = 1$, es decir, debemos probar que a es raíz simple de f si y sólo si $f(a) = 0$ y $f'(a) \neq 0$.
Por el teorema del resto, $f = (X-a)g + f(a)$. Luego, $f' = g + (X-a)g'$ y por lo tanto $f'(a) = g(a)$. Entonces a es raíz simple de f si y sólo si $f = (X-a)\,g$ y $g(a) \neq 0$ si y sólo si $f(a) = 0$ y $f'(a) \neq 0$.

Supongamos ahora que la proposición vale para m y veamos que vale para $m+1$. Por la proposición anterior, a es raíz de f de multiplicidad $m+1 \Longleftrightarrow f(a) = 0$ y a es raíz de f' de multiplicidad m

Ahora, usando la hipótesis inductiva para f', resulta que a es raíz de f de multiplicidad $m+1 \Longleftrightarrow f(a) = 0$, $(f')^{(k)}(a) = 0 \ \ \forall\, 0 \leq k \leq m-1$ y $(f')^{(m)}(a) \neq 0 \Longleftrightarrow f^{(k)}(a) = 0$ $\forall\, 0 \leq k \leq m$ y $f^{(m+1)}(a) \neq 0$. □

Corolario 1. Sea $\mathbb{K}$ un cuerpo de característica cero (por ejemplo, $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces a es raíz múltiple de f si y sólo si a es raíz de f y de f'.

Corolario 2. Sea $\mathbb{K}$ un cuerpo de característica cero (por ejemplo, $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y sea $f \in \mathbb{K}[X]$. Entonces f tiene todas sus raíces simples si y sólo si f y f' son coprimos. Dejamos la demostración como ejercicio.

Corolario 3. Sea $f \in \mathbb{Q}[X]$. Si f es irreducible en $\mathbb{Q}[X]$ todas raíces de f en $\mathbb{C}$ son simples.

Demostración: Como f es irreducible entonces $(f : f') \neq 1$ si y sólo si $f \mid f'$. Pero como $\operatorname{gr} f' = \operatorname{gr} f - 1 < \operatorname{gr} f$ entonces no puede ocurrir que f divida a f'. Luego, $(f : f') = 1$. Por lo tanto, por el corolario 2, resulta que todas las raíces de f en $\mathbb{C}$ son simples. □

Ejemplos.

1) El polinomio $f = X^7 - X + 2$ tiene todas sus raíces simples.
En efecto, supongamos que $a \in \mathbb{C}$ es una raíz múltiple de f. Entonces, por el corolario 1, a es raíz de f y de f'. Por lo tanto, como $f' = 7X^6 - 1$ entonces $0 = f(a) = a^7 - a + 2$ y $0 = f'(a) = 7a^6 - 1$. Luego, $a^6 = \frac{1}{7}$ y

$$0 = a^7 - a + 2 = a^6\, a - a + 2 = \frac{1}{7}a - a + 2 = -\frac{6}{7}a + 2$$

Por lo tanto $a^6 = \frac{1}{7}$ y $a = \frac{7}{3}$, lo que es absurdo.

2) Sea $f = -X^5 + aX^4 + X^3 - 5X^2 + (a^2 - 3a + 6)X - (a^2 - 2a + 1)$. Hallar todos los $a \in \mathbb{C}$ tales que 1 es raíz doble de f
Debemos hallar los $a \in \mathbb{C}$ tales que $f(1) = 0$, $f'(1) = 0$ y $f''(1) \neq 0$.
Calculemos f' y f''.

$$\begin{aligned} f' &= -5X^4 + 4aX^3 + 3X^2 - 10X + a^2 - 3a + 6 \\ f'' &= -20X^3 + 12aX^2 + 6X - 10 \end{aligned}$$

Luego,

$$\begin{aligned} f(1) &= -1 + a + 1 - 5 + a^2 - 3a + 6 - (a^2 - 2a + 1) = 0 \\ f'(1) &= -5 + 4a + 3 - 10 + a^2 - 3a + 6 = a^2 + a - 6 \\ f''(1) &= -20 + 12a + 6 - 10 = -24 + 12a \end{aligned}$$

entonces $f(1) = 0$ para todo a y $f'(1) = 0 \iff a = 2$ o $a = -3$ y como debe valer $f''(1) \neq 0$ entonces el único $a \in \mathbb{C}$ que satisface lo pedido es $a = -3$.