RESUMEN ALGEBRA 1

FINAL

POLINOMIOS:

Polinomios.

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

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 $K[X]$

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 $\mathrm{gr}(f+g) \leq \max\{\mathrm{gr}(f), \mathrm{gr}(g)\}$. Más precisamente,

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

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

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

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:*

$$\forall f,g\in K[X],\quad f\cdot g=0 \quad\Longrightarrow\quad f=0 \text{ o } g=0.$$

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

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.

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

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.)

- $g\mid f$ 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 $0 < \mathrm{gr}(g) < \mathrm{gr}(f)$.

Teorema 7.1.7. **(Algoritmo de división.)**

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

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

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

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.

- $(f : 0) = f/\mathrm{cp}(f)$, $\forall\, f \in K[X]$ 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 $(f : g) = \frac{g}{\mathrm{cp}(g)}$.

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:*

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

(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 $r_k \mid r_{k-1}$*).*

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* $h = sf + tg$.

Corolario 7.1.14. **(Mcd y divisores comunes.)** (El máximo común divisor entre f y g es el (único) polinomio mónico h perteneciente a K[X] que satisface:)

- *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* $g \mid hf \iff g \mid f$.

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 $g, h \in K[X]$, $f \mid gh \implies f \mid g$ 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*

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

(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.

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 $f, g \in K[X]$:

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

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

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

EJEMPLOS IMPORTANTES:

- 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

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

  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.)

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

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

Proposición 7.2.3. (Teorema del resto.)

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

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 $f(x) = q(x)\, g(x) = q(x) \cdot 0 = 0$.)

Proposición 7.2.5. **(Raíz común y Mcd.)**

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

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

7.2.1 Multiplicidad de las raíces.

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

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

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

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 $f'(x) \neq 0$.*

<u>EJEMPLOS IMPORTANTES</u>

- 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 $f(0) = 1 \neq 0$.

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

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

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

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

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

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

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* $\operatorname{mult}(x_1; f) = m_1$ *y* $\operatorname{mult}(x_2; f) = m_2$. *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*

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

Entonces

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

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.*

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...*

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

Lema 7.2.15. **(Lema de Gauss.)**

Sea $f = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ 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 $\alpha \mid a_0$ y $\beta \mid a_n$.*

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.

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.

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

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

- 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

- 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

- 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

- 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

- 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.

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* $\mathrm{gr}(f) = 1$, *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 $z_1, \dots, z_r \in \mathbb{C}$ *son distintos,* $m_1, \dots, m_r \in \mathbb{N}$ *y* $c \in \mathbb{C}^{\times}$.

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

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* $\mathbb{R}$.

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* $m \in \mathbb{N}$, $\mathrm{mult}(z; f) = m \iff \mathrm{mult}(\overline{z}; f) = m$.
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. $\mathrm{mult}(z; f) = m \implies \big((X - z)(X - \overline{z})\big)^m \mid f$ *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

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*

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

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

Pero ser reducible en $\mathbb{Q}[X]$ no implica tener raíz en $\mathbb{Q}$:

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 $\mathbb{Q}[X]$!

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

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* $m \in \mathbb{N}$, $\operatorname{mult}(a+b\sqrt{d}; f) = m \Leftrightarrow \operatorname{mult}(a-b\sqrt{d}; f) = m$.

<u>EJERCICIOS</u> <u>DE</u> <u>FINALES</u>:

FINAL 13/9/22

4. (a) Hallar todos los polinomios de grado 2 irreducibles en $(\mathbb{Z}/2\mathbb{Z})[X]$.
   (b) Probar que el polinomio $f(X) = X^4 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ es irreducible.

FINAL 3/8/22

4) Factorizar el polinomio
$$3X^2 + 210X + 5 \in (\mathbb{Z}/239\mathbb{Z})[X]$$
como producto de polinomios irreducibles en $(\mathbb{Z}/239\mathbb{Z})[X]$ (239 es primo).

FINAL 27/7/22

4. Sea $f \in \mathbb{Q}[X]$ un polinomio de grado mínimo entre los polinomios **mónicos** que satisfacen simultáneamente que:

- $(X^2 + 2X + 5) \mid (f : f')$.
- $(X^2 - 4X + 1) \mid (f : f'')$.
- $f'(2 - \sqrt{3}) = 0$.

Hallar la facorización de f como producto de polinomios irreducibles en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

FINAL 20/7/22

4. Factorizar en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ el polinomio

$$X^6 - 6X^5 + 14X^4 - 8X^3 - 14X^2 + 10X + 7$$

sabiendo que tiene dos raíces cuya suma es 1 y cuyo producto es -1, que además son múltiples.

FINAL 17/6/22

4. Encuentre todos los $a, b \in \mathbb{Z}$ para los que el polinomio

$$X^5 + 15aX^4 + 12bX^3 - 18X^2 - 1$$

tiene una raíz racional. Pruebe además que, para cualquiera de los a y b hallados, esta raíz es única y tiene multiplicidad 1.

FINAL 27/5/22

4. Sea $P \in \mathbb{Q}[X]$ un polinomio de grado 8. Factorize P en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$, sabiendo que

- P tiene exactamente 5 raíces,
- $1 + i$ y $2 - \sqrt{3}$ son raíces simples de P,
- $P(2) = 0$ y $P(0) = 4$.

FINAL 29/4/22

4. Factorize en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ el polinomio

$$X^5 - X^4 + 4X^3 - 7X^2 - 5X - 10,$$

sabiendo que tiene una raíz en $\mathbb{C}$ cuya parte real es cero.

FINAL 4/3/22

4. (a) Determinar todos los números enteros a y b para los cuales el polinomio

$$X^{101} + 33\,a\,X^4 + X^3 + 12\,b\,X^2 - 18\,X + 1$$

tiene al menos una raíz racional.

(b) Decidir si existen números enteros a y b para los cuales el polinomio tiene una raíz racional múltiple.

3. Sea $(f_n)_{n\in\mathbb{N}}$ la sucesión de polinomios en $\mathbb{Q}[X]$ definida por:

$$f_1 := X - 1\,,\ f_2 = 2X^2 - X - 2 \quad \text{y} \quad f_{n+2} = X\,f_{n+1} + 2X^2 f_n - 2\,X + 3,\ \forall\, n \geq 1.$$

Conjeturar y probar fórmulas para el coeficiente principal y el grado de f_n para todo $n \in \mathbb{N}$.

Final 25/2/22

4. Describir todos los pares $(a, b) \in \mathbb{C}^2$ para los cuales el polinomio

$$f = X^4 + 2aX^2 + b$$

tiene raíces múltiples en $\mathbb{C}$, y para cada par (a, b) determinar la cantidad de raíces distintas y la multiplicidad de cada raíz. (No hace falta calcular exactamente las raíces.)

FINAL 18/2/22

3. Sea g un polinomio que satisface que $g(0) \neq 0$ y sea $(f_n)_{n\in\mathbb{N}}$ la sucesión de polinomios definida por:

$$f_1 := X\,g \quad \text{y} \quad f_{n+1} = (X\,f_n')^n,\ \forall\, n \in \mathbb{N}.$$

Determinar y probar una fórmula para la multiplicidad exacta de 0 como raíz de f_n, para todo $n \in \mathbb{N}$.

4. Determinar todos los números reales a, b para los cuales el polinomio

$$f = 3X^5 + 10X^4 + 12X^3 + 3X^2 + aX + b$$

satisface que $(f : X^3 + X^2 - 2)$ tiene grado 2, y para cada par de valores hallado factorizar f en $\mathbb{R}[X]$.

FINAL 22/12/21

Ejercicio 4

(a) Determinar todos los $a, b \in \mathbb{Z}$ **coprimos** y no nulos para los cuales el polinomio

$$X^4 + iX^3 + 2X^2 + aiX + b$$

tiene al menos una raíz **racional**.

(b) Para cada par de valores hallado, factorizar el polinomio obtenido en $\mathbb{C}[X]$.

FINAL 10/12/22

3. (a) Determinar todos los $n \in \mathbb{N}$ para los cuales

$$X^2 + X + 1 \mid X^{2n} + X^n + 1.$$

(b) Calcular el resto de dividir a $X^{6n} + X^{3n} + 1$ por $X^2 + X + 1$.

Final 21/10/21

4. Sea $f \in \mathbb{C}[X]$ un polinomio de grado $n \geq 3$ con una raíz $\alpha \in \mathbb{C}$ de multiplicidad (exactamente) 3. Probar que el resto de dividir a f' por $(X - \alpha)^3$ es de la forma $c(X - \alpha)^2$ donde $c \in \mathbb{C}$ es no nulo.

FINAL 28/7/21

4. Determinar todos los primos positivos p tales que el polinomio

$$f = X^4 - 2X^3 - 16X^2 + 2pX - p$$

admite al menos una raíz racional positiva. Para cada valor hallado factorizar el polinomio en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.