§18. División de polinomios

Recuerdo: Sean $A, B \in k[X]$ polinomios. Decimos que B divide a A (o que A es un múltiplo de B) si $\exists\, Q \in k[X]$ tq $A = BQ$.

Teorema (división euclideana): Sean $A, B \in k[X]$. Si $B \neq 0$, existen únicos polinomios Q (cociente) y R (resto) tq

$$A = BQ + R \quad \text{y} \quad gr(R) < gr(B).$$

Dem: Unicidad: Si $A = BQ + R = BQ' + R' \Rightarrow R - R' = B(Q' - Q)$ y luego B divide $R - R'$. $\underset{gr(R-R') < gr(B)}{\Rightarrow} R' - R = 0$, ie, $R = R' \underset{B \neq 0}{\Rightarrow} Q = Q'$ ✓

Existencia: Por inducción en $n = gr(A)$: Si $A = 0$, consideramos $Q = R = 0$ ✓
Sup. que $A \neq 0$. Si $n < gr(B)$ consideramos $Q = 0$ y $R = A$, sino:
$n \geq gr(B) =: m$ y escribimos $A = \sum_{i=0}^{n} a_i X^i$ y $B = \sum_{i=0}^{m} b_i X^i$, con $a_m \neq 0$ y $b_m \neq 0$.
$\Rightarrow A' := A - \frac{a_m}{b_m} X^{n-m} B = (a_m X^n + \dots) - \frac{a_m}{\cancel{b_m}} X^{n-m} (\cancel{b_m} X^m + \dots)$ tiene grado $< n$.
Hipótesis de inducción $\Rightarrow A' = BQ' + R'$ con $gr(R') < gr(B)$
$\Rightarrow A = B \cdot \left(\frac{a_m}{b_m} X^{n-m} + Q' \right) + R'$ y luego $Q = \frac{a_m}{b_m} X^{n-m} + Q'$ y $R = R'$ ■

Ejemplo: La división euclideana de $A(X) = X^3 + X + 1$ por $B(X) = X + 1$ es:

$$\begin{array}{l} X^3 + X + 1 : (X+1) = X^2 - X + 2 \\ \underline{-(X^3 + X^2)} \\ \quad -X^2 + X + 1 \\ \quad \underline{-(-X^2 - X)} \\ \qquad 2X + 1 \\ \qquad \underline{-(2X+2)} \\ \qquad\quad -1 \end{array}$$

$$\Rightarrow A(X) = B(X)\underbrace{(X^2 - X + 2)}_{Q(X)} \underbrace{-1}_{R(X)}.$$

Corolario: Sea $P \in k[X]$. Entonces, $a \in k$ es una raíz de P (ie, $P(a) = 0$) $\Leftrightarrow$ P es divisible por $X - a$.

Dem: La división euclideana de P por $X - a$ nos da $P = (X-a)Q + R$, donde $gr(R) < 1$ y luego $R \in k$ es constante $\Rightarrow P(a) = 0 + R$, de donde concluimos ■

Recuerdo: Sea $P \in k[X]$, y sea $a \in k$ una raíz de P. La multiplicidad de la raíz $a \in k$ es el máximo $m \in \mathbb{N}^{\geq 1}$ tal que $(X-a)^m$ divide a $P(X)$. En caso que $m = 1$ (resp $m = 2$, resp. $m = 3$, etc) decimos que a es una raíz simple (resp. raíz doble, resp. raíz triple, etc).

Ejemplo: Sea $P \in \mathbb{C}[X]$ dado por $P(X) = X^n - 1$, para cierto $n \in \mathbb{N}^{\geq 1}$.
$\Rightarrow P(X) = (X-1)(X-\xi)(X-\xi^2)\cdots(X-\xi^{n-1})$ con $\xi = e^{2\pi i/n}$ (raíces simples).

$\boxed{\text{Ejercicio}}$ Sea $P \in k[X]$ y $a \in k$. Probar que a es una raíz múltiple de P (ie, de multiplicidad ≥ 2) $\Leftrightarrow P(a) = P'(a) = 0$.

Def: Sea $I \subseteq k[X]$ sub-conjunto. Decimos que I es un <u>ideal</u> de $k[X]$ si:
(i) I es un sub-e.v. de $k[X]$.
(ii) $\forall P \in I$ y $\forall Q \in k[X]$ se tiene que $PQ \in$ [redacted] I.

<u>Ejemplo</u>: Sean $P_1, \dots, P_r \in k[X]$ y sea $I = \{P_1 Q_1 + \dots + P_r Q_r$ donde $Q_i \in k[X]\}$. Entonces I es el ideal más pequeño que contiene los $P_1, \dots, P_r$ y es llamado el <u>ideal generado</u> por $P_1, \dots, P_r$, que denotamos $\langle P_1, \dots, P_r \rangle$.

<u>Terminología</u>: Decimos que un ideal $I \subseteq k[X]$ es un <u>ideal principal</u> si $\exists P \in k[X]$ tq $I = \langle P \rangle$, ie, si I está formado por todos los múltiplos PQ de P.

Teorema: Todo ideal I de $k[X]$ es principal. Más aún, si $I \neq \{0\}$ es un ideal, entonces existe un <u>único</u> polinomio <u>unitario</u> $P \in I$ tq $I = \langle P \rangle$.

<u>Dem</u>: Si $I = \{0\}$ entonces $I = \langle 0 \rangle$ está generado por el polinomio nulo ✓
Sup. que $I \neq \{0\}$. En este caso, el conjunto

$$\{gr(Q),\ Q \in I - \{0\}\} \subseteq \mathbb{N}$$

es un sub-conjunto no-vacío de $\mathbb{N}$. $\Rightarrow$ Admite un elemento minimal d.
Sea $P \in I - \{0\}$ tq $gr(P) = d$. Reemplazando P por $a^{-1}P$ si fuese necesario, donde $a \in k - \{0\}$ es el coeficiente principal de P, podemos suponer que P es <u>unitario</u>. Veamos que $I = \langle P \rangle$:

Sea $F \in I$ arbitrario. La división euclideana de F por P nos da $F = PQ + R$, con $gr(R) < gr(P) = d$. Como I es un ideal: $R = \underbrace{F}_{\in I} - \underbrace{PQ}_{\in I} \in I$.
Luego, por minimalidad de d, necesariamente $R = 0$.
$\Rightarrow F = PQ$ y luego $I = \langle P \rangle$ ✓

Veamos que P es único:
Si $I = \langle P \rangle = \langle P' \rangle$ con P' unitario, entonces $\exists Q, Q' \in k[X]$ tq $P' = PQ$ (pues $I = \langle P \rangle$) y $P = P'Q'$ (pues $I = \langle P' \rangle$) $\Rightarrow gr(Q) = gr(Q') = 0$, ie, $Q, Q' \in k$. Como P y P' son unitarios, la igualdad $P' = PQ$ implica que $Q = 1$ y luego $P' = P$. ■

Def: Sean $A, B \in k[X] \setminus \{0\}$ <u>no-nulos</u>. Decimos que $D \in k[X]$ es un <u>máximo común divisor</u> (mcd) de A y B si D divide A y B, y si todo divisor común de A y B divide a D. Diremos que A y B son "<u>primos entre sí</u>" si 1 es un mcd de A y B.

⚠ El mcd <u>no</u> es único: si D es un mcd de A y B, entonces λD también lo es para todo escalar $\lambda \neq 0$. Por maximalidad, todos los mcd (en caso de existir) se obtienen de este modo y en particular $\exists!$ $mcd(A,B)$ <u>unitario</u>.

Prop: Sean $A, B \in k[X]-\{0\}$ no nulos. Entonces, existe $D \in k[X]$ un mcd de A y B. Dicho D se escribe como $D = AU + BV$ para ciertos $U, V \in k[X]$. En part, $\exists!$ $\text{mcd}(A,B) \in k[X]$ unitario.

Dem: El conjunto $I = \langle A, B\rangle = \{AP + BQ \text{ donde } P, Q \in k[X]\}$ es un ideal $\neq \{0\}$.
$\Rightarrow I = \langle D\rangle$ para cierto $D \in k[X]$ (único si lo suponemos unitario).
En part, $D = AU + BV$ para ciertos $U, V \in k[X]$. Como $A, B \in I = \langle D\rangle$, ellos son múltiplos de D. Más aún, todo polinomio que divide tanto A y B también divide $AU + BV = D$ $\Rightarrow D$ es un mcd de A y B. ■

Teorema de Bézout: Sean $A, B \in k[X]-\{0\}$ no nulos. Entonces, A y B son primos entre sí $\Leftrightarrow \exists\, U, V \in k[X]$ tq $AU + BV = 1$.

Dem: A y B son primos entre sí $\overset{\text{def}}{\Longleftrightarrow}$ 1 es un mcd de A y B
$\Leftrightarrow \text{mcd}(A,B) = 1 \underset{\text{Prop}}{\Longrightarrow} \exists\, U, V \in k[X]$ tq $AU + BV = 1$ ✓
Recíprocamente, si $AU + BV = 1$ entonces todo mcd de A y B divide 1 y es por lo tanto constante $\Rightarrow \text{mcd}(A,B) = 1$ ✓ ■

Lema de Gauss: Sean $A, B, C \in k[X]-\{0\}$ polinomios no nulos. Entonces:
① Si $\text{mcd}(A,B) = 1$ y A divide BC $\Rightarrow A$ divide C.
② Si $\text{mcd}(A,B) = 1$ y $\text{mcd}(A,C) = 1$ $\Rightarrow \text{mcd}(A, BC) = 1$.

Dem: ① Como $\text{mcd}(A,B) = 1 \Rightarrow \exists\, U, V \in k[X]$ tq $AU + BV = 1$.
Como A divide BC, $\exists P \in k[X]$ tq $BC = AP$.
$$\Rightarrow C = C \cdot 1 = C(AU + BV) = ACU + \underbrace{BC}_{=AP}V = ACU + APV = A\underbrace{(CU + PV)}_{Q \in k[X]}$$
$\Rightarrow A$ divide C ✓

② Sea $D = \text{mcd}(A, BC)$. Notar que $\text{mcd}(B, D) = 1$, pues todo divisor común a D y B divide A y B, y estos últimos son primos entre sí.
Como $\text{mcd}(B,D) = 1$ y D divide $BC \overset{①}{\Longrightarrow} D$ divide C
Luego, D divide A y D divide C $\Rightarrow D = 1$ ✓ ■

Corolario: Sean $P, P_1, \ldots, P_m \in k[X]-\{0\}$ polinomios no nulos. Entonces:
① Si $\text{mcd}(P_i, P_j) = 1$ para todo $i \neq j$ y si P_i divide P para todo i
$\Rightarrow$ El producto $P_1 \cdots P_m$ divide P.
② Si $\text{mcd}(P, P_i) = 1$ para todo i $\Rightarrow \text{mcd}(P, P_1 \cdots P_m) = 1$.

Dem: ① Por inducción en m: si $P = P_1 Q$ y si P_j con $j \geq 2$ divide P y $\text{mcd}(P_j, P_1) = 1 \Rightarrow P_j$ divide Q (Lema de Gauss)
Por hipótesis de inducción, Q es divisible por $P_2 \cdots P_m$ ✓
② Por inducción en m: el caso base ($m=2$) dado por el Lema de Gauss ✓ ■

<u>Ejemplo importante</u>: Sea $P \in k[X]$ un polinomio. Vimos que $a \in k$ es una raíz de P (ie, $P(a)=0$) $\Leftrightarrow$ $X-a$ divide a P.

En part, si $a \in k$ <u>no</u> es una raíz de P ($\Rightarrow P \neq 0$ es no-nulo) entonces $\mathrm{mcd}(P, X-a) = 1$ (este último es necesariamente de grado 0).

El Corolario anterior ② $\Rightarrow$ P y $(X-a)^n$ son primos entre sí $\forall n \in \mathbb{N}^{\geq 1}$.

Por otra parte, si $\lambda_1, \dots, \lambda_p \in k$ son raíces distintas de P, de multiplicidades $m_1, \dots, m_p \in \mathbb{N}^{\geq 1}$ entonces el Corolario anterior ① implica que P es divisible por el producto $\prod_{j=1}^{p} (X-\lambda_j)^{m_j} = (X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\cdots(X-\lambda_p)^{m_p}$.

<u>Def</u>: Sea $P \in k[X]-\{0\}$ polinomio no nulo. Decimos que P <u>escinde sobre k</u> si se factoriza (sobre k) como un producto de polinomios de grado 1:

$$P(X) = a \prod_{j=1}^{p} (X-\lambda_j)^{m_j} = a(X-\lambda_1)^{m_1}\cdots(X-\lambda_p)^{m_p}$$

donde $a \in k$ y $\lambda_1, \dots, \lambda_p \in k$. En otras palabras, P escinde sobre k si y sólo si la suma $s(P) = m_1 + \dots + m_p$ de las multiplicidades de sus raíces en k es igual al grado de P: $s(P) = gr(P)$.

<u>Lema útil</u>: Sean $P, Q \in k[X]-\{0\}$ no nulos. Si P escinde sobre k y si Q divide a P $\Rightarrow$ Q escinde sobre k.

<u>Dem</u>: Si $P = AQ$ $\Rightarrow$ $gr(P) = s(P) = s(A) + s(Q)$.
Como $gr(P) = gr(A) + gr(Q)$, $s(A) \leq gr(A)$ y $s(Q) \leq gr(Q)$, necesariamente $s(Q) = gr(Q)$ y luego Q escinde sobre k. ■

<u>Recuerdo</u>: El Teorema Fundamental del Álgebra asegura que <u>todo</u> polinomio complejo $P \in \mathbb{C}[X]$ de grado ≥ 1 posee al menos una raíz en $\mathbb{C}$.
Como consecuencia de la división euclideana, y usando la terminología anterior, esto último equivale a:

<u>Teorema Fundamental del Álgebra</u>: Todo polinomio $P \in \mathbb{C}[X]-\{0\}$ no nulo con coeficientes complejos escinde sobre $\mathbb{C}$.

<u>Ejemplo</u>: Esto último <u>no</u> es cierto sobre **otros cuerpos**:

① $P \in \mathbb{R}[X]$ dado por $P(X) = X^3 - 1 = (X-1)(X^2+X+1)$ <u>no</u> escinde sobre $\mathbb{R}$, pues X^2+X+1 no posee raíces reales.

② <u>Pequeño Teorema de Fermat</u> (1636): Sea $a \in \mathbb{N}$ y p un número primo, entonces $a^p \equiv a \pmod p$. En part, $a^{-1} \equiv a^{p-2}$ para todo $a \not\equiv 0 \pmod p$.

<u>Idea</u> (inducción): $a = 0$ ✓ y $(a+1)^p - (a+1) = \underbrace{a^p - a}_{\equiv 0 \pmod p} + \sum_{k=0}^{p-1} \underbrace{\binom{p}{k}}_{\equiv 0 \pmod p} a^{p-k}$ ■

Consecuencia: El polinomio $P \in \mathbb{F}_p[X]$ dado por $P(X) = X^p - X + 1$ <u>no</u> posee raíces en $\mathbb{F}_p$ (pues $P(a) = 1$ $\forall a \in \mathbb{F}_p$) y luego <u>no</u> escinde sobre $\mathbb{F}_p$.