Tema 4

Polinomios

4.1 Anillo de polinomios con coeficientes en un cuerpo

Aunque se puede definir el conjunto de los polinomios con coeficientes en un anillo, nuestro estudio se va a centrar en el conjunto de los polinomios con coeficientes en un cuerpo.

Definición 4.1 (Anillo de polinomios) *El anillo de polinomios con coeficientes en un cuerpo K, es el conjunto*

$$K[X] = \{ a_0 + a_1X + \ldots + a_nX^n, a_i \in K \}$$

junto con las operaciones suma y producto definidos en la forma usual.
Dados $f(X) = \sum_{i=}^{r} a_iX^i$ y $g(X) = \sum_{i=0}^{s} b_iX^i \in K[X]$, se definen:

Suma: $f(X) + g(X) = \sum_{i=0}^{n}(a_i + b_i)X^i$, siendo $n = \max\{r, s\}$

Producto: $f(X).g(X) = \sum_{i=0}^{r+s}\left(\sum_{j=0}^{i} a_j\, b_{i-j}\right)X^i$

$K[X]$ con las dos operaciones definidas tiene estructura de anillo conmutativo con identidad.

Todo polinomio no nulo puede escribirse en la forma $f(X) = \sum_{i=}^{d} a_iX^i$ con $a_d \neq 0$ para algún $d \geq 0$. En este caso, el número natural d se dice grado del polinomio y lo denotaremos por $gr(f)$. Al coeficiente a_d se le dice *coeficiente director*.
De lo anterior se deduce que las constantes (los elementos de K) son polinomios de grado cero. Asimismo, se define $gr(0) = -\infty$.
El grado verifica:

I) $gr(f + g)) \leq \max\{ gr(f), gr(g)\}$
II) $gr(f \,.\, g)) = gr(f) + gr(g)$

En lo referente a divisibilidad, el anillo de polinomios tiene un comportamiento análogo al anillo de los números enteros. Es un dominio de integridad y posee división euclídea, el papel del valor absoluto lo juega ahora el grado.

Proposición 4.2 *El anillo* $(K[X], +, .)$ *es un dominio de integridad. Esto significa que el producto de dos polinomios no puede ser 0 si ambos son no nulos.*

Demostración.
Dados $f(x) = \sum_{i=0}^{r} a_iX^i$, $g(x) = \sum_{i=0}^{s} b_iX^i \in K[x]$, $f(x) \neq 0$ y verificando $f(x).g(x) = 0$, veamos que $g(x) = 0$.
Al ser $f(x) \neq 0$, tiene algún coeficiente no nulo. Se puede suponer, sin pérdida de generalidad, que $a_0 \neq 0$. Si fuese a_k el primer coeficiente no nulo, esto es $a_k \neq 0$ y $a_i = 0$

$\forall\ i$ con $0 \le i \le k$-1, se tendría $f(x) = \sum_{i=k}^{r} a_i X^i = X^k\left(\sum_{i=k}^{r} a_i X^{i-k}\right)$, y se podría trabajar con el polinomio$\sum_{i=k}^{r} a_i X^{i-k}$.
Supongamos que $a_0 \neq 0$
Si $f(x).g(x) = \sum_{i=0}^{r+s}\left(\sum_{j=0}^{i} a_j\, b_{i-j}\right)X^i = 0$, todos los coeficientes son nulos, esto es, $\sum_{j=0}^{i} a_j\, b_{i-j} = 0$, para $i \in \{0, \ldots, r+s\}$. Veamos por inducción que $b_i = 0$.
Para $i = 0$, se tiene $0 = a_0 b_0$. De $a_0 \neq 0$ se deduce $b_0 = 0$.
Supongamos cierto que $b_j = 0$ para $1 \le j \le k-1$, veamos que $b_k = 0$:
$0 = \sum_{j=0}^{k} a_j\, b_{k-j} = a_0 b_k$, De $a_0 \neq 0$ se deduce $b_k = 0$. Por tanto $g(x) = 0$ ■

Todo lo que sabemos de $\mathbb{Z}$ con respecto al máximo común divisor, algoritmo de Euclides, identidad de Bézout, factorización única de primos, ecuaciones diofánticas lineales, … funciona exactamente igual en el caso de los anillos de polinomios $K[X]$.

Definición 4.3 (División euclídea)
En el caso de los enteros se tenía una aplicación (el valor absoluto):

$$|\,.\,| : \mathbb{Z} \to \mathbb{N}$$

Y que dados cualesquiera a y b, $b \neq 0$, existirían q y r tales que:

$$a = b\,.\,q + r, \text{ con } 0 \le r < |\,b\,|,$$

en el caso del anillo de polinomios el papel de esa aplicación lo juega la aplicación grado:

$$gr(.)\ K[X] \to \mathbb{N}$$

se tiene que, *para cualesquiera polinomios* $f(X)$ y $g(X)$, $g(X) \neq 0$, *existen polinomios* $q(X)$ y $r(X)$, *tales que*

$$f(X) = g(X)q(X) + r(X),\ gr(r) < gr(g)$$

A $q(X)$ se le denomina cociente y $r(X)$ resto.

Ejemplo 4.4 *Hallar el cociente y el resto de dividir* $x^5 + x^4 + 2x^3 + x^2 + 4x + 2$ entre $x^2+2x + 3$ en $\mathbb{Z}_7[x]$.

$(x^5 + x^4 + 2x^3 + x^2 + 4x + 2) = (x^2 + 2x + 3)(\, x^3 - x^2 + x + 2) + (-3x - 4) \equiv$
$(x^2 + 2x + 3)(\, x^3 + 6x^2 + x + 2) + (4x + 3)$(mód 7)
Cociente $x^3 + 6x^2 + x + 2$, Resto $4x + 3$ ■

Proposición 4.5 *Los únicos elementos inversibles en el anillo* $K[X]$ *son las constantes.*

Demostración.
Es consecuencia de las propiedades del grado.
Sea $f(X) \in K[X]$ un elemento inversible, existe $g(X) \in K[X]$ verificando $f(X)g(X) = 1$.
En consecuencia, $f(X)$ y $g(X)$ son polinomios no nulos y $gr(f.g)\ ) = gr(f) + gr(g) = 0$. Por tanto $gr(f) = gr(g) = 0$, es decir, son constantes. ■

Definición 4.6 *Un polinomio* $g(X)$ *se dice* ***divisor*** *(o* ***factor****) de* $f(X)$ *en* $K[X]$ *si existe un polinomio* $h(X)$ *en* $K[X]$ *tal que* $f(X) = g(X)\ h(X)$.

Definición 4.7 (**Polinomios mónicos)** *Se llaman polinomios mónicos a aquellos cuyo coeficiente director es* 1.

Estos polinomios mónicos juegan el papel, que en el caso de los enteros juegan los números positivos. Del mismo modo que en $\mathbb{Z}$, todo entero se podía escribir como el producto de una unidad (±1) por un entero positivo, en este caso todo polinomio puede escribirse como una unidad en $K[X]$ por un polinomio Mónico. En efecto, $f(X) = \sum_{i=}^{d} a_i X^i$, al ser $a_d \neq 0$, se puede poner en la forma:

$$f(X) = a_d \left(X^d + \frac{a_{d-1}}{a_d} X^{d-1} + \frac{a_{d-2}}{a_d} X^{d-2} + \cdots + \frac{a_1}{a_d} X + \frac{a_0}{a_d} \right)$$

Definición 4.8 (**Polinomios irreducibles)** *Un polinomio mónico no constante se dice irreducible* (*o primo*) *si los únicos polinomios mónicos que lo dividen son el 1 y el propio polinomio.*

Usando el mismo argumento que en el caso de los enteros, se puede demostrar que existen infinitos.
Los polinomios mónicos de grado 1 son todos irreducibles, independientemente del cuerpo de coeficientes *K*..
En general, la forma de los polinomios irreducibles depende del cuerpo de coeficientes. Así, se tiene:

- K = $\mathbb{Q}$. Existen polinomio irreducibles de cualquier grado. Por ejemplo, $X^n + p$ es irreducible para cualquier entero primo p (si no fuese primo tampoco lo sería p).
- K = $\mathbb{R}$. Los polinomios primos son de dos tipos:
  - $X - \alpha$, para cualquier $X - \alpha$, número real.
  - $(X - \alpha)^2 + \beta^2$. Los $\alpha \in \mathbb{R}$ y $\beta \in \mathbb{R}\setminus\{0\}$.
- K = $\mathbb{C}$. Los únicos polinomios irreducibles son los mónicos de grado uno. (Teorema fundamental del Álgebra).
- K = $\mathbb{Z}_p$. Existen polinomios irreducibles de cualquier grado.

Definición 4.9 (Máximo común divisor) *Dados dos polinomios el máximo común divisor es el único polinomio mónico que verifica:*

i) Divide a ambos.
ii) Todo divisor de ambos es también divisor de él.

Algoritmo 4.10 (Algoritmo de Euclides) En un anillo de polinomios existe un proceso similar al que conocemos en los enteros para el cálculo del máximo común divisor de dos polinomios. En este caso el polinomio resto tiene grado estrictamente menor que el divisor. El proceso termina cuando el resto es 0. También se cumple la identidad de Bézout.

Ejemplo 4.11 *Encontrar el máximo común divisor y una identidad de Bézout de los polinomios* $g(X) = X^3 + 1$ y $f(X) = X^4 + X^3 + 2X^2 + X + 1$ de $\mathbb{Q}[X]$.

Vamos a realizar el proceso matricial similar al que conocemos para los enteros, hay que ir anotando los cocientes en cada paso que se da en el algoritmo.

$$R_0 = \begin{pmatrix} X^4 + X^3 + 2X^2 + X + 1 & X^3 + 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Dado que $f(X) = X^4 + X^3 + 2X^2 + X + 1 = (X^3 + 1)(X + 1) + 2X^2$

$$Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & -(X + 1) \end{pmatrix}$$

$$R_1 = R_0Q_1 = \begin{pmatrix} X^3 + 1 & 2X^2 \\ 0 & 1 \\ 1 & -(X+1) \end{pmatrix}$$

Al ser $X^3 + 1 = (2\,X^2).\frac{1}{2}X + 1$

$$Q_2 = \begin{pmatrix} 0 & 1 \\ 1 & -\frac{1}{2}X \end{pmatrix}$$

$$R_2 = R_0Q_1Q_2 = \begin{pmatrix} 2X^2 & 1 \\ 1 & -\frac{1}{2}X \\ -(X-1) & \frac{1}{2}X^2 + \frac{1}{2}X + 1 \end{pmatrix}$$

Al ser $2\,X^2 = 1.2X^2$

$$Q_3 = \begin{pmatrix} 0 & 1 \\ 1 & -2X^2 \end{pmatrix}$$

$$R_3 = R_0Q_1Q_2Q_3 = \begin{pmatrix} 1 & 0 \\ -\frac{1}{2}X & \mathrm{X}^3 \\ \frac{1}{2}X^2 + \frac{1}{2}X + 1 & -X^4 - X^3 - 2X^2 - x + 1 \end{pmatrix}$$

El proceso ha terminado, el máximo común divisor es 1. Los polinomios son coprimos. Se deduce la siguiente identidad de Bézout

$$1 = \left(-\tfrac{1}{2}X\right)f(X) + \left(\tfrac{1}{2}X^2 + \tfrac{1}{2}X + 1\right)g(X) \qquad \blacksquare$$