TEMA 1. POLINOMIOS

Apuntamentos de clase da materia de Álxebra Linear e Multilinear.

O obxectivo deste tema é introducir algúns conceptos básicos sobre polinomios que serán útiles posteriormente no estudo e clasificación de endomorfismos.

Sexa K un corpo.

Definición. O anel de polinomios nunha variable con coeficientes en K é o conxunto

$$K[X] = \{f(X) = a_0 + a_1X + \ldots + a_nX^n \text{ con } a_i \in K\}$$

coas operacións de suma e multiplicación habituais.

Non faremos a comprobación de que efectivamente é un anel conmutativo, por tratarse dunha comprobación rutineira. Ademais, $K[X]$ pode verse como un K-espazo vectorial de dimensión infinita.

Definición. O grao dun polinomio $f \neq 0$ é o maior enteiro n tal que $a_n \neq 0$. Escribiremos $\text{gr}(f)$ ou $\deg(f)$ (polo termo inglés *degree*). O polinomio $f = 0$ non ten grao definido; por convenio, poremos $\deg(0) = -\infty$.
Un polinomio de grao n con $a_n = 1$ chámase mónico.

Proposición. O grao ten as seguintes propiedades.

(a) $\deg(f + g) \leq \text{máx}\{\deg(f), \deg(g)\}$, con igualdade se $\deg(f) \neq \deg(g)$.

(b) $\deg(fg) = \deg(f) + \deg(g)$.

O resultado anterior tamén se aplica cando algún dos polinomios (ou ámbolos dous) é igual a 0.
A seguinte proposición afirma que o algoritmo da división de números enteiros tamén funciona no anel de polinomios. A demostración basearase en reproducir o algoritmo.

Proposición. Dados polinomios $f(X), g(X) \in K[X]$ con $g \neq 0$, existen polinomios $q(X)$ e $r(X)$ únicos e tales que

$$f(X) = g(X)q(X) + r(X), \quad \deg(r) < \deg(g).$$

Demostración. Vamos comezar vendo que se existen, os polinomios necesariamente son únicos. De ter dúas igualdades da forma

$$f(X) = g(X)q_1(X) + r_1(X)$$
$$f(X) = g(X)q_2(X) + r_2(X),$$

podemos restar unha da outra e obter

$$g(X)(q_1(X) - q_2(X)) = r_2(X) - r_1(X).$$

Porén, se $q_1(X) - q_2(X) \neq 0$, temos que

$$\deg(g(X)) > \deg(r_2(X) - r_1(X)) = \deg(g(X)(q_1(X) - q_2(X))) \geq \deg(g(X)).$$

Polo tanto, $q_1(X) - q_2(X)$ e de aquí deducimos que $r_1(X) = r_2(X)$.

Imos comprobar agora a existencia. Se $f = 0$, o resultado é trivial pondo $q(X) = r(X) = 0$. Senón, pomos

$$f(X) = a_0 + a_1X + \ldots + a_nX^n, \quad g(X) = b_0 + b_1X + \ldots + b_mX^m,$$

con $a_n, b_m \neq 0$. Se $n < m$, entón $f(X) = g(X) \cdot 0 + f(X)$ e o resultado é certo. Se $n \geq m$, podemos escribir

$$f(X) - g(X) \cdot \frac{a_n}{b_m} X^{n-m} = r_1(X),$$

onde o polinomio $r_1(X)$ é 0 ou ten grao $n_1 < n$. Se $r_1(X) = 0$ ou $n_1 < m$, pomos $q(X) = \frac{a_n}{b_m} X^{n-m}$ e $r(X) = r_1(X)$.
No caso $n_1 \geq m$, iteramos o proceso novamente e pomos $r_1(X) = c_0 + c_1X + \ldots + c_{n_1}X^{n_1}$, con $c_{n_1} \neq 0$; novamente,

$$r_1(X) - g(X)\frac{c_{n_1}}{b_m} X^{n_1-m} = r_2(X),$$

con $r_2(X) = 0$ ou de grao $n_2 < n_1$. En calquera caso,

$$f(X) = g(X)\Big(\frac{a_n}{b_m} X^{n-m} + \frac{c_{n_1}}{b_m} X^{n_1-m}\Big) + r_2(X).$$

Se $n_2 \geq m$, hai que repetir o proceso novamente, pero como o valor $n_i - m$ é estritamente menor despois de cada iteración, acabaremos despois dun número finito de pasos cun polinomio que será ou ben 0 ou ben de grao menor que n. Polo tanto, despois de k pasos teremos

$$f(X) = g(X)\Big(\frac{a_n}{b_m} X^{n-m} + \frac{c_{n-1}}{b_m} X^{n_1-m} + \ldots + \frac{c_{n_{k-1}}}{b_m} X^{n_{k-1}-m}\Big) + r_k(X).$$

□

Cando $r(X) = 0$ diremos que $f(X)$ é un múltiplo de $g(X)$. Grazas á existencia de división euclidiana, podemos considerar os conceptos habituais de divisibilidade sobre os enteiros como mínimo común múltiplo, máximo común divisor, algoritmo de Euclides ou identidade de Bézout.
Coas notacións do resultado anterior, o algoritmo de Euclides di que $\gcd(f(X), g(X)) = \gcd(g(X), r(X))$; por outro lado, a identidade de Bézout asegura que existen polinomios $u(X)$ e $v(X)$ tales que

$$u(X) \cdot f(X) + v(X) \cdot g(X) = \gcd(f(X), g(X)).$$

Ademais, o algoritmo de Euclides proporciona unha maneira construtiva de achar os polinomios $u(X)$ e $v(X)$. A modo de exemplos, consideremos o caso $f(X) = X^4 + X^3 + 1$ e $g(X) = X^2 + 1$. Entón, en dúas iteracións, o algoritmo de Euclides danos que

$$\begin{aligned} x^4 + x^3 + 1 &= (x^2 + 1)(x^2 + x - 1) + (-x + 2) \\ x^2 + 1 &= (-x + 2)(-x - 2) + 5 \end{aligned}.$$

Polo tanto, $\gcd(x^4 + x^3 + 1, x^2 + 1) = 1$, dado que calquera constante do corpo (en particular o 5) divide un polinomio arbitrario. Procedendo agora en sentido inverso,

$$\begin{aligned} 5 &= 1 \cdot (x^2 + 1) + (x + 2) \cdot (-x + 2) \\ &= 1 \cdot (x^2 + 1) + (x + 2) \cdot (x^4 + x^3 + 1 - (x^2 + 1) \cdot (x^2 + x - 1)) \\ &= (x + 2) \cdot (x^4 + x^3 + 1) + (-x^3 - 3x^2 - x + 3) \cdot (x^2 + 1). \end{aligned}$$

Alternativamente,

$$1 = \frac{x+2}{5} \cdot (x^4 + x^3 + 1) + \frac{-x^3 - 3x^2 - x + 3}{5} \cdot (x^2 + 1).$$

Definición. Un polinomio $f(X) \neq 0$ de grao maior que 0 é irredutible se os seus únicos divisores son da forma k e $k \cdot f(X)$, con $k \in K$.

En teoría de aneis, é habitual definir unha noción de primo, dicindo que $f(X)$ é primo se sempre que divide a un produto $g(X)h(X)$, entón divide a $g(X)$ ou a $h(X)$. Neste caso, os dous conceptos son equivalentes, pero imos traballar polo de agora coa noción de irredutible.

Proposición. Todo polinomio $f(X) \neq 0$ de grao maior que 0 é produto de irredutibles

Demostración. Se $f(X)$ é irredutible, o resultado é certo. En caso contrario, sexa $g_1(X)$ un divisor de grao mínimo entre os de $f(X)$. Entón, $g_1(X)$ é irredutible, xa que todos os seus divisores tamén o son de $f(X)$. Podemos pór entón $f(X) = g_1(X) \cdot f_1(X)$. Se $f_1(X)$ é irredutible, acabamos; en caso contrario, consideramos novamente un dos seus divisores de grao mínimo, $g_2(X)$, e escribimos $f(X) = g_1(X) \cdot g_2(X) \cdot f_2(X)$. Como $\deg(f) > \deg(f_1) > \deg(f_2) > \ldots$, o proceso remata despois dun número finito de pasos. □

Por último, é importante observar que a descomposición en irredutibles, como sucede no caso dos enteiros, é única (salvo multiplicación por constantes). Para demostrar o resultado, imos usar que se $p(X)$ divide o produto $q(X)r(X)$ e $\gcd(p(X), q(X)) = 1$, entón $p(X)$ divide $r(X)$. Isto vese aplicando a identidade de Bézout, que nos permite considerar polinomios $u(X)$ e $v(X)$ tales que $1 = p(X)u(X) + q(X)v(X)$. Polo tanto,

$$r(X) = p(X)r(X)u(X) + q(X)r(X)v(X),$$

e o polinomio $p(X)$ divide os dous sumandos da dereita e por conseguinte tamén divide $r(X)$.

Proposición. Se $f(X) = p_1(X) \cdots p_n(X) = q_1(X) \cdots q_m(X)$ e tódolos factores son polinomios irredutibles, entón $n = m$ e os polinomios $\{p_i(X)\}$ son os mesmos que os $\{q_j(X)\}$ salvo factores do corpo K.

Demostración. Faremos indución sobre n. Cando $n = 1$, é obviamente certo que $m = 1$ e $p_1(X) = q_1(X)$. Supoñamos logo que o resultado é certo cando $n \leq r - 1$ e imos establecelo para $n = r$. Dada a igualdade $p_1(X) \cdots p_r(X) = q_1(X) \cdots q_m(X)$, temos que $p_r(X)$ divide o produto $q_1(X)(q_2(X) \cdots q_m(X))$. Se $p_r(X)$ non coincide con $q_1(X)$ (salvo multiplicación por factores de K), entón é relativamente primo con el e divide a $q_2(X) \cdots q_m(X)$. Repetindo o razoamento, chegamos a que un $q_j(X)$ é igual a $p_r(X)$ salvo un factor de K, isto é, $p_r(X) = k \cdot q_j(X)$, con $k \in K$ diferente de 0. Suprimindo este factor de ambos lados da igualdade, podemos aplicar a hipótese de inducción e concluír que cada un dos $p_i(X)$, con $1 \leq i \leq r - 1$ coincide cos $q_j(X)$ restantes e en particular $r = m$. □

Observamos que a proba deste resultado usa de forma esencial a existencia de división euclidiana no anel de polinomios, dado que usamos a identidade de Bézout para demostrar que se $p(X)$ divide o produto $q(X)r(X)$ e $\gcd(p(X), q(X)) = 1$, entón $p(X)$ divide $r(X)$.

Definición. Un elemento $k \in K$ é un cero do polinomio $f(X)$ se $f(k) = 0$. Ás veces tamén se usa o termo raíz.

É habitual introducir a aplicación lineal *avaliación en* k, que denotaremos por av_k e que está dada por

$$\mathrm{av}_k : K[X] \longrightarrow K, \quad f(X) \mapsto f(k).$$

Entón, k é un cero de $f(X)$ se e soamente se $f(X)$ está no núcleo de av_k.

Proposición. Un elemento $k \in K$ é un cero de $f(X)$ se e soamente se $X - k$ divide $f(X)$.

Demostración. Se $f(X) = (X - k)q(X)$, avaliando en $X = k$ temos que $f(k) = 0$. Reciprocamente, supoñamos que $k \in K$ é un cero de $f(X)$, con $f \neq 0$ (o caso $f = 0$ é trivial). Podemos considerar a división euclidiana e escribir $f(X) = (X-k) \cdot q(X) + r$, onde $r \in K$. Avaliando en $X = k$, temos que $0 = f(k) = r$, co cal $X - k$ divide $f(X)$. □

Definición. Se $f(X) = (X - k)^m \cdot g(X)$, con $\gcd(X - k, g(X)) = 1$, diremos que k é unha raíz de $f(X)$ de multiplicidade m. Se $m > 1$, diremos que k é unha raíz múltiple.

Definición. Un corpo K é alxebricamente pechado se todo polinomio $f(X)$ non constante ten unha raíz.

Enunciamos agora o coñecido como teorema fundamental da álxebra. As probas máis sinxelas do mesmo usan a teoría da variable complexa (o teorema de Liouville) ou o concepto de *grao* topolóxico. Por esta razón, ímola omitir polo de agora.

Teorema. O corpo dos números complexos, $\mathbb{C}$, é alxebricamente pechado.

Corolario. Os factores irredutibles dun polinomio $f(X) \in \mathbb{R}[X]$ teñen grao como moito dous.

Demostración. Sobre os números complexos, o polinomio $f(X)$ ten tantas raíces como o seu grao. Imos demostrar que se $X - \alpha \in \mathbb{C}[X]$ é un factor irredutible, entón $X - \bar{\alpha} \in \mathbb{C}[X]$ tamén o será; para iso, é suficiente con observar que

$$0 = f(\alpha) = \overline{f(\alpha)} = f(\bar{\alpha}).$$

Polo tanto, $(X - \alpha)(X - \bar{\alpha})$ é un factor de $f(X)$, que se pode escribir como

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha} \in \mathbb{R}[X].$$

Dividindo por este factor e iterando o proceso, concluímos a demostración. □

O caso dos polinomios sobre $\mathbb{Q}$ é polo xeral máis complicado. Se un polinomio ten coeficientes enteiros, diremos que é primitivo cando o máximo común divisor dos seus coeficientes é 1. Nese caso, cúmprese que o polinomio é irredutible sobre $\mathbb{Q}[X]$ se e soamente se o é tamén sobre $\mathbb{Z}[X]$ (é o coñecido como Lema de Gauss). Aí podemos aplicar os resultados habituais de divisibilidade; por exemplo, que un polinomio mónico ten tódalas súas raíces entre os divisores do termo independente.