Definició de l'anell de polinomis

Direm simplement "cos" per indicar un cos commutatiu.

Una *successió* d'elements de K és una aplicació

$$\{0,1,2,\ldots\} \to K$$

Si indiquem per a_n la imatge de n, està clar que la successió queda determinada donant

$$(a_0, a_1, \ldots, a_n, \ldots),$$

que denotarem abreujadament per (a_n).

Un *polinomi amb coeficients a* K és una successió (a_n) amb $a_i = 0$ per a tot i llevat d'un nombre finit. Si $a_m \neq 0$, però $a_i = 0$ per a tot $i > m$ direm que m és el *grau* del polinomi (a_n): $gr(a_n)$. Els a_i es diuen els *coeficients* del polinomi.

Designarem per $K[x]$ el conjunt de polinomis amb coeficients a K. Definim dues operacions a $K[x]$ de la següent manera:

$$(a_0, a_1, \ldots, a_n, \ldots) + (b_0, b_1, \ldots, b_n, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$$
$$(a_0, a_1, \ldots, a_n, \ldots) \cdot (b_0, b_1, \ldots, b_n, \ldots) = (a_0 \cdot b_0, a_0 \cdot b_1 + a_1 \cdot b_0, \ldots, c_n, \ldots)$$

on $c_n = \sum_{i+j=n} a_i \cdot b_j$

Amb aquestes operacions $K[x]$ és un anell commutatiu amb unitat. El zero d'aquest anell és $(0) = (0,0,\ldots)$ i la unitat $(1,0,\ldots)$. Es compleix també que si $(a_n) \neq (0)$, $(b_n) \neq (0)$,

$$gr[(a_n) + (b_n)] \leq màx[gr(a_n), gr(b_n)]$$
$$gr[(a_n) \cdot (b_n)] = gr(a_n) + gr(b_n)$$

La segona igualtat té com a conseqüències interessants:

- $(a_n) \cdot (b_n) = (0) \Rightarrow (a_n) = (0)$ o $(b_n) = (0)$
- $(a_n) \cdot (b_n) = (a_n) \cdot (c_n) \neq 0 \Rightarrow (b_n) = (c_n)$.
- Els únics elements invertibles de $K[x]$ són els de grau 0.

Si a cada $a \in K$ li fem correspondre el polinomi $(a,0,\ldots)$ obtenim una aplicació injectiva

$$K \to K[x]$$

Divisió entera i ideals a $K[x]$

Teorema 2.1 (de la divisió entera) *Donats dos polinomis* $a(x)$ *i* $b(x)$ *diferents de zero de* $K[x]$*, existeixen dos únics polinomis* $q(x)$ *i* $r(x)$ *tals que:*

$$\boxed{a(x)=b(x)\cdot q(x)+r(x)}$$

amb $r(x)=0$ o $gr\, r(x)<gr\, b(x)$.

Si la resta de la divisió entera de $a(x)$ per $b(x)$ és 0, es diu que $a(x)$ és un *múltiple* de $b(x)$ (i escriurem $a(x)=\overline{b(x)}$), o que $b(x)$ és un *divisor* de $a(x)$ (i escriurem $b(x)\mid a(x)$). Indicarem per

$$(b(x))$$

el conjunt dels múltiples de $b(x)$.

Observem que $(b(x))$ compleix les dues propietats següents:

- És tancat per la suma (és a dir, $a(x),c(x)\in(b(x))\Rightarrow a(x)+c(x)\in(b(x))$) .
- Si $a(x)\in(b(x))$ i $c(x)\in K[x]$, aleshores $a(x)\cdot c(x)\in(b(x))$.

Anomenarem *ideal* de $K[x]$ tot subconjunt $I\subset K[x]$ que compleixi:

1. $a(x),b(x)\in I\Rightarrow a(x)+b(x)\in I$
2. $a(x)\in I$ i $c(x)\in K[x]\Rightarrow a(x)\cdot c(x)\in I$

$(b(x))$ és doncs, un ideal.

Proposició 2.2 *Si* I *és un ideal de* $K[x]$*, existeix sempre un polinomi* $b(x)$ *tal que* $(b(x))=I$.

Polinomis irreductibles i polinomis primers entre ells

Dos polinomis $a(x)$, $b(x)$ són *primers entre ells* quan $m.c.d.(a(x),b(x))=1$.

Proposició 4.1 (Teorema d'Euclides) *Si* $a(x)\mid b(x)\cdot c(x)$ i $m.c.d.(a(x),b(x))=1$, *aleshores* $a(x)\mid c(x)$.

Proposició 4.2 *Si* $m(x)=m.c.m.(a(x),b(x))$, *llavors* $m(x)\cdot d(x)=ka(x)\cdot b(x)$. *Amb* $k\in K$.

Proposició 4.3 *Tot polinomi* $a(x)\neq 0$ *de* $grau>0$ *és el producte de polinomis irredectibles.*

Proposició 4.4 *Si*

$$p_1(x)\cdots p_n(x)=q_1(x)\cdots q_m(x)$$

i tots els factors són polinomis irreductibles, llavors $n=m$ *i els polinomis* $\{p_i(x)\}$ *són els mateixos que els de* $\{q_j(x)\}$ *llevat de factors del cos* K.

Zeros d'un polinomi

Si $a(x)=a_0+a_1x+\ldots+a_nx^n$ és un polinomi de $K[x]$ i $k\in K$, anomenarem *valor de* $a(x)$ *a* k.

$$a(k)=a_0+a_1k+\ldots+a_nk^n\in K$$

Si $a(k)=0$ direm que k és un *zero* o una arrel de $a(x)$.

Proposició 5.1 k *és un zero del polinomi* $a(x)\neq 0$ *si i només si* $a(x)$ *és divisible per* $x-k$.

Direm que $k\in K$ és un *zero de multiplicitat* p del polinomi $a(x)\in K[x]$ si $a(x)=(x-k)^p b(x)$ i $b(k)\neq 0$, és a dir , si $a(x)$ és divisible per $(x-k)^p$ però no ho és per $(x-k)^{p+1}$.

Corol·lari 5.2 *Si* $gr\,a(x)=n$*, la suma de les multiplicitats dels zeros de* $a(x)$ *és* $\leq n$.

Proposició 5.3 *Si* K *és infinit i* $a(k)=b(k)$ *per a tot* $k\in K$*, llavors* $a(x)=b(x)$.

El polinomi $ma(x)$ té els mateixos zeros que $a(x)$ i els coeficients enters.

Polinomis irreductibles de $\mathbb{R}[x]$

Teorema 6.1 (fonamental de l'Àlgebra) *Tot polinomi de* $grau>1$ *amb coeficients complexos té un zero.*

Corol·lari 6.2 *Els polinomis irreductibles de* $\mathbb{R}[x]$ *són els de grau 1.*

Estudiarem ara els polinomis irreductibles de $\mathbb{R}[x]$. Tot polinomi real $a(x)=a_0+a_1x+\ldots a_nx^n$ pot considerar-se també com un polinomi amb coeficients complexos. En general, si $a(x)=a_0+a_1x+\ldots a_nx^n$ és de $\mathbb{R}[x]$ indicarem per $\overline{a}(x)$

$$\overline{a}_0+\overline{a}_1x+\ldots\overline{a}_nx^n$$

Si $z=a+bi\in\mathbb{C}$, $\bar{z}=a-bi$ indica el seu conjugat. Aleshores $a(x)$ té coeficients reals si i només si

$$\boxed{\bar{a}(x)=a(x)}$$

Quan $a(x)$ té coeficients reals, resulta que sempre que z sigui un zero, $\bar{z}$ també ho és. Aleshores, o bé $z=\bar{z}$, és a dir, z és un zero real de $a(x)$, o bé $z\neq\bar{z}$ i $a(x)$ és divisible per

$$(x-z)(x-\bar{z})=x^2-(z+\bar{z})x+z\bar{z},$$

que és un polinomi amb coeficients reals. A més a més, $x^2-(z+\bar{z})x+z\bar{z}$ és irreductible a $\mathbb{C}[x]$, ja que en cas contrari tindria un divisor de primer grau i per tant un zero real.

Així doncs els polinomis irreductibles de $\mathbb{R}[x]$ són de grau ≤ 2.

Nota:

A l'anell $\mathbf{Q}[x]$ es poden trobar polinomis irreductibles de grau tan gran com es vulgui.

Els anells $K[x]/(m(x))$

Sigui $m(x)$ un polinomi de $K[x]$. Direm que dos polinomis $a(x)$ i $b(x)$ són *congruents mòdul* $m(x)$ si $a(x)-b(x)\in m(x)$. Això equivalm a dir que les restes de les divisions enteres de $a(x)$ i $b(x)$ per $m(x)$ són iguals. Escriurem aleshores

$$a(x)\equiv b(x) \qquad m(x)$$

Aquesta relació és clarament d'equivalència. Designem per $[a(x)]$ la classe d'equivalència de $a(x)$, és a dir, el conjunt de polinomis congruents amb $a(x)$ mòdul $m(x)$.

El conjunt d'aquestes classes d'equivalència el denotarem per

$$K(x)/(m(x))$$

i en direm *quocient* de $K(x)$ per $(m(x))$. A cada classe d'equivalència hi ha un i només un polinomi de grau més petit que el de $m(x)$.

En el conjunt $K(x)/(m(x))$ podem definir dues operacions, suma:

$$[a(x)]+[b(x)]=[a(x)+b(x)],$$

i producte:

$$[a(x)]\cdot[b(x)]=[a(x)\cdot b(x)].$$

$K(x)/(m(x))$ té, amb aquestes operacions, l'estructura d'un anell commutatiu amb unitat; ara bé aquest anell posseeix algunes propietats que no tenia $K[x]$. Per exemple,

Proposició 7.1 *Si* $a(x), m(x)=(1)$, $[a(x)]$ *té un invers a* $K(x)/(m(x))$. *Si* $(a(x), m(x))=(d(x))$ *amb* $gr\, d(x)\geq 1$, $[a(x)]$ *és un divisor de* 0 *a* $K[x]/(m(x))$.

Corol·lari 7.2 *Si* $p(x)\in Kx$ *és irreductible,* $K[x]/(p(x))$ *és un cos.*

El cos $K[x]/(p(x))$ es denota per $K(\alpha)$ i es diu una *extensió algebraica* de K.

Existeix doncs, una correspondència bijectiva entre el cos $|[x]/(x^2+1)$ i el cos $|$ dels nombres complexos, que conserva les operacions. Podem dir, doncs que el cos $|[x]/(x^2+1)$ no és una altra cosa que el cos $|$ dels nombres complexos. Amb més precisió, es diu que $|[x]/(x^2+1)$ i $|$ són dos cossos *issomorfs*.