[Conclusão da aula anterior: isomorfismos de anéis e característica]

2. Anéis Polinomiais

A aritmética de polinómios de coeficientes reais é governada por regras familiares. Como generalizá-la a um anel arbitrário?

Na Análise têm trabalhado com polinómios com coeficientes reais, definidos como as *funções* $p : \mathbb{R} \to \mathbb{R}$ da forma

$$p(x) = \sum_{i=0}^{n} p_i x^i,$$

onde os números reais p_i são os coeficientes do polinómio. A coeficientes distintos correspondem polinómios (funções polinomiais) distintos. Não podemos definir de modo análogo os polinómios com coeficientes num anel arbitrário A, se desejarmos que polinómios com coeficientes distintos sejam necessariamente polinómios distintos. De facto, desde que A tenha mais de um elemento ($a \neq 0$), existe uma infinidade de possibilidades distintas para os coeficientes de um possível polinómio (por ex., $a, ax, ax^2, ax^3, \ldots$), mas, no caso de A ser finito, existe apenas um número finito de funções $f : A \to A$, pelo que não podem ser usadas para definir todos os polinómios com coeficientes em A.

Por exemplo, se A for o anel $\mathbb{Z}_2$, só existem quatro funções $f : \mathbb{Z}_2 \to \mathbb{Z}_2$

$$\begin{array}{cccc} f_1 & f_2 & f_3 & f_4 \\ 0 \mapsto 0 & 0 \mapsto 0 & 0 \mapsto 1 & 0 \mapsto 1 \\ 1 \mapsto 0 \quad , & 1 \mapsto 1 \quad , & 1 \mapsto 0 \quad , & 1 \mapsto 1 \end{array}$$

[Observe: os polinómios $1 + x$ e $1 + x + x^2 + x^3$ definem ambos f_3]

mas se quisermos que polinómios com coeficientes distintos sejam de facto polinómios distintos, existe um número infinito de polinómios com coeficientes em $\mathbb{Z}_2$:

$$0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2, x^3, 1+x^3, x+x^3, x^2+x^3, 1+x+x^3, 1+x^2+x^3,$$

$$x + x^2 + x^3, 1 + x + x^2 + x^3, \ldots$$

Resolvemos este problema identificando um polinómio com a sucessão dos seus próprios coeficientes, esquecendo a sua relação com funções de tipo especial.

No que se segue A designa um anel comutativo com identidade.

POLINÓMIO

Uma sucessão

$$\begin{aligned} p : \mathbb{N}_0 &\to A \\ i &\mapsto p(i) := p_i \end{aligned}$$

em A diz-se um *polinómio* se existe $n \in \mathbb{N}_0$ tal que $p(i) = 0$ para todo o $i > n$. O menor número $n \in \mathbb{N}_0$ nessas condições chama-se *grau* do polinómio (no caso em que o polinómio não é o polinómio nulo $(0, 0, 0, \ldots)$; quando se trata do polinómio nulo, convenciona-se que o seu grau é $-\infty$). Os termos $p(i) := p_i$ dizem-se os *coeficientes* do polinómio. Denotaremos por $A[x]$ o conjunto de todos os polinómios com coeficientes no anel A.

Exemplos:

$\mathbf{0} := (0, 0, 0, \ldots)$ é o *polinómio zero* ou *nulo*.

$\mathbf{1} := (1, 0, 0, \ldots)$ é o *polinómio um* ou *identidade*.

$\boldsymbol{a} := (a, 0, 0, \ldots)$ diz-se um *polinómio constante* ($a \in A$).

A soma e produto de polinómios com coeficientes reais (isto é, em $\mathbb{R}[x]$) é-nos seguramente familiar e baseiam-se nas operações de soma e produto dos coeficientes reais. Reconhecendo que essas operações sobre os coeficientes são possíveis em qualquer anel, podemos estender essas operações a qualquer $A[x]$. Note que a soma assim introduzida não passa da soma usual de sucessões, mas o produto já não é o habitual. Quando há risco de ambiguidade, referimo-nos ao produto definido abaixo como o *produto de convolução*, e representamo-lo por $p \star q$ em lugar de pq.

SOMA E PRODUTO (DE CONVOLUÇÃO) DE POLINÓMIOS

Sendo $p, q : \mathbb{N}_0 \to A$ polinómios, a *soma* $\boldsymbol{p + q}$ e o *produto (de convolução)* $\boldsymbol{p \star q}$ são os polinómios dados por

$$(\boldsymbol{p} + \boldsymbol{q})_i = p_i + q_i$$

$$(\boldsymbol{p} \star \boldsymbol{q})_i = \sum_{j=0}^{i} p_j q_{i-j}.$$

Exemplos: (1) Se $\boldsymbol{a} = (a, 0, 0, \ldots)$ é um polinómio constante e

$$\boldsymbol{p} = (p_0, p_1, \ldots, p_n, 0, 0, \ldots)$$

é um polinómio arbitrário, o produto $\boldsymbol{a} \star \boldsymbol{p}$ é o polinómio

$$(ap_0, ap_1, ap_2, \ldots, ap_n, 0, 0, \ldots),$$

porque a soma $\sum_{j=0}^{i} a_j p_{i-j}$ se reduz sempre à parcela com $j = 0$.

(2) Se $\boldsymbol{a} = (a, 0, 0, \ldots)$ e $\boldsymbol{b} = (b, 0, 0, \ldots)$ são polinómios constantes, a sua soma e o seu produto são dados por $\boldsymbol{a} + \boldsymbol{b} = (a + b, 0, 0, \ldots)$ e $\boldsymbol{a} \star \boldsymbol{b} = (ab, 0, 0, \ldots)$. Portanto, o conjunto dos polinómios constantes com as operações acima indicadas é um anel isomorfo a A.

`[Confirme: o isomorfismo é dado pela aplicação` $a \mapsto (a, 0, 0, \ldots)$`]`

(3) Em $\mathbb{Z}_2[x]$, se $\boldsymbol{p} = (1, 1, \ldots, 1, 0, 0, \ldots)$ é de grau $n \geq 0$, então

$$\boldsymbol{pp} = (1, 0, 1, 0, \ldots, 1, 0, 0, \ldots),$$

de grau $2n$, pois

$$(\boldsymbol{pp})_i = \sum_{j=0}^{i} p_j p_{i-j} = \sum_{j=0}^{i} 1 = (i + 1) \bmod 2.$$

O resultado seguinte é evidente, pelo que a sua demonstração fica como exercício.

Proposição. *Se A é um anel comutativo com identidade, $(A[x], +, \star)$ é também um anel comutativo com identidade. Além disso, $(A[x], +, \star)$ é um domínio de integridade se e só se A é um domínio de integridade.* ∎

O anel $A[x]$ chama-se *anel polinomial* sobre A.

Observámos no exemplo (2) acima que o anel $A[x]$ contém um subanel isomorfo a A (o conjunto dos polinómios constantes), o que justifica que se possa usar o mesmo símbolo a para designar um dado elemento do anel A e o correspondente polinómio constante $(a, 0, 0, \ldots)$. Dizemos então que $A[x]$ é uma *extensão* de A.