Capítulo 2

Anéis de polinómios a várias indeterminadas

Todos os resultados, e respectivas demonstrações, deste capítulo são transcritos do livro

POLINÓMIOS, Textos de Matemática, Vol. 20, Universidade de Lisboa, 2010

da autoria de Pedro Jorge Freitas.

1. Polinómios a várias indeterminadas

Seja A um anel. Como sabemos, o anel $A[x]$ dos *polinómios a uma indeterminada* x é o conjunto das sucessões

$$\boldsymbol{p} = (p_0, p_1, \ldots, p_n, 0, 0, \ldots), \quad p_i \in A$$

ou, equivalentemente, das somas formais

$$\boldsymbol{p} = p_0 + p_1 x + p_2 x^2 + \cdots + p_n x^n = \sum_{i=0}^{n} p_i x^i,$$

munido das operações de *soma* e *produto de convolução* definidas por

$$(\boldsymbol{p} + \boldsymbol{q})_i = p_i + q_i \quad \text{e} \quad (\boldsymbol{p} \star \boldsymbol{q})_i = \sum_{j=0}^{i} p_j q_{i-j}.$$

Agora, o anel $A[x_1, \ldots, x_n]$ dos *polinómios a* n *indeterminadas* $x_1, \ldots, x_n$ define-se simplesmente por iteração: $A[x_1, \ldots, x_n] \colon = A[x_1, \ldots, x_{n-1}][x_n]$.

Esta definição corresponde à ideia que uma soma de monómios a n indeterminadas se deve escrever como um polinómio na última, pondo-a em evidência em cada monómio. Por exemplo, o polinómio $2x^2y^3 + x^3y + 2y^3 + 5x + 2y \in \mathbb{R}[x,y]$ pode escrever-se como um polinómio em y com coeficientes em $\mathbb{R}[x]$:

$$(2x^2 + 2)y^3 + (x^3 + 2)y + 5x.$$

Proposição 1.1. *Seja $p \in A[x_1, \ldots, x_n]$. Então existem um natural m e coeficientes $a_{i_1 \ldots i_n}$ $(0 \le i_1, \ldots, i_n \le m)$ tais que*

$$p = \sum_{i_1,\ldots,i_n=0}^{m} a_{i_1 \ldots i_n}\, x_1^{i_1} \cdots x_n^{i_n}.$$

Além disso, os coeficientes $a_{i_1 \ldots i_n}$ nesta representação canónica são únicos.

Demonstração. Demonstremos o resultado por indução sobre n.

Se $n = 1$, o resultado é válido (como sabemos do estudo do anel $A[x]$). Suponhamos então o resultado válido para $n-1$ e consideremos $p \in A[x_1, \ldots, x_n]$. Como, por definição, $A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$ então, usando o caso $n = 1$, podemos assumir que existem polinómios $p_1, \ldots, p_k \in A[x_1, \ldots, x_{n-1}]$ tais que

$$p = \sum_{j=0}^{k} p_k x_n^j.$$

Agora, pela hipótese de indução, para cada p_j existem coeficientes $a_{i_1 \ldots i_{n-1}, j}$, com $0 \le i_1, \ldots, i_{n-1} \le l_j$ tais que

$$p_j = \sum_{i_1,\ldots,i_{n-1}=0}^{l_j} a_{i_1 \ldots i_{n-1}, j}\, x_1^{i_1} \cdots x_{n-1}^{i_{n-1}}.$$

Seja m o maior dos inteiros l_j $(1 \le j \le n-1)$ e k. Introduzindo monómios com coeficientes nulos se necessário, e chamando i_n ao índice j, obtemos

$$p = \sum_{i_n=0}^{m} \Big(\sum_{i_1,\ldots,i_{n-1}=0}^{m} a_{i_1 \ldots i_{n-1} i_n}\, x_1^{i_1} \cdots x_{n-1}^{i_{n-1}} \Big) x_n^{i_n} = \sum_{i_1,\ldots,i_n=0}^{m} a_{i_1 \ldots i_n}\, x_1^{i_1} \cdots x_n^{i_n},$$

o que prove a primeira parte do resultado.

Quanto à unicidade dos coeficientes, pode ser provada de modo similar, usando indução sobre n. Para $n = 1$, o resultado é consequência da definição. Supondo que o resultado vale para $n-1$, consideremos duas possíveis representações canónicas do mesmo polinómio p:

$$p = \sum_{i_1,\ldots,i_n=0}^{m} a_{i_1 \ldots i_n}\, x_1^{i_1} \cdots x_n^{i_n} = \sum_{i_1,\ldots,i_n=0}^{m} a'_{i_1 \ldots i_n}\, x_1^{i_1} \cdots x_n^{i_n}.$$

Olhando cada membro como polinómio de $A[x_1, \ldots, x_{n-1}][x_n]$, temos

$$\sum_{i_n=0}^{m}\Big(\sum_{i_1,\ldots,i_{n-1}=0}^{m} a_{i_1\ldots i_{n-1}i_n}\, x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}\Big)x_n^{i_n} = \sum_{i_n=0}^{m}\Big(\sum_{i_1,\ldots,i_{n-1}=0}^{m} a'_{i_1\ldots i_{n-1}i_n}\, x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}\Big)x_n^{i_n}.$$

Então, pelo caso $n = 1$, podemos concluir que

$$\sum_{i_1,\ldots,i_{n-1}=0}^{m} a_{i_1\ldots i_{n-1}i_n}\, x_1^{i_1}\cdots x_{n-1}^{i_{n-1}} = \sum_{i_1,\ldots,i_{n-1}=0}^{m} a'_{i_1\ldots i_{n-1}i_n}\, x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}$$

para qualquer i_n entre 1 e m. Finalmente, pela hipótese de indução,

$$a_{i_1\ldots i_{n-1}i_n} = a'_{i_1\ldots i_{n-1}i_n}$$

para quaisquer $1 \le i_1, \ldots, i_{n-1} \le m$. ∎

Notação. Em questões teóricas é útil simplificar a escrita usando *expoentes e índices múltiplos* (permitindo recuperar a notação usada nos polinómios a uma indeterminada). Basta para cada n-úplo de inteiros não negativos $i = (i_1, \ldots, i_n)$ abreviar $x_1^{i_1}\cdots x_n^{i_n}$ por $\overline{x}^i$.

Por exemplo, o polinómio $x_1^2x_2 - x_1x_2 + 4x_1 \in \mathbb{R}[x_1, x_2]$ abrevia-se por

$$\overline{x}^{(2,1)} - \overline{x}^{(1,1)} + 4\overline{x}^{(1,0)}.$$

Vamos também denotar $A[x_1, \ldots, x_n]$ simplesmente por $A[\overline{x}]$ sempre que isso não cause confusão.

Note que se i e j forem dois expoentes múltiplos, então $\overline{x}^i\overline{x}^j = \overline{x}^{i+j}$ (onde a soma $i + j$ é feita coordenada a coordenada), pela comutatividade do anel $A[\overline{x}]$. Isto permite recuperar o formalismo da soma e do produto de polinómios a uma indeterminada:

Proposição 1.2. *Sejam $p = \sum_{i\in\mathbb{N}_0^n} a_i\, \overline{x}^i$ e $q = \sum_{i\in\mathbb{N}_0^n} b_i\, \overline{x}^i$ em $A[\overline{x}]$. Então*

$$p + q = \sum_{i\in\mathbb{N}_0^n} (a_i + b_i)\, \overline{x}^i \qquad e \qquad pq = \sum_{k\in\mathbb{N}_0^n}\Big(\sum_{i+j=k} a_ib_j\Big)\, \overline{x}^k.$$

Demonstração. A primeira identidade é simples de verificar. Quanto à da multiplicação, é consequência da distributividade:

$$pq = \Big(\sum_{i\in\mathbb{N}_0^n} a_i\, \overline{x}^i\Big)\Big(\sum_{j\in\mathbb{N}_0^n} b_j\, \overline{x}^j\Big) = \sum_{i,j\in\mathbb{N}_0^n} a_ib_j\, \overline{x}^i\overline{x}^j = \sum_{i,j\in\mathbb{N}_0^n} a_ib_j\, \overline{x}^{i+j}.$$

Agrupando as parcelas comuns onde ocorre $\overline{x}^k$, obtemos

$$pq = \sum_{k\in\mathbb{N}_0^n} \Big(\sum_{i+j=k} a_i b_j \Big) \overline{x}^k. \qquad \blacksquare$$

Os polinómios da forma $ax_1^{i_1} \cdots x_n^{i_n}$ são chamados *monómios* e os da forma $x_1^{i_1} \cdots x_n^{i_n}$ *monómio primitivos*. Diz-se que um monómio primitivo *ocorre* num polinómio p se o seu coeficiente em p for diferente de zero.

Proposição 1.3. *Sejam A e B anéis, $A \subseteq B$, e $b_1, \ldots, b_n \in B$. Existe um (único) homomorfismo de anéis $\varphi_{b_1,\ldots,b_n} : A[x_1, \ldots, x_n] \to B$ que*

- *deixa fixos os elementos de $A \subseteq A[x_1, \ldots, x_n]$ e*
- *aplica x_i em b_i, para cada $1 \leq i \leq n$.*

Demonstração. A existência pode ser provada por indução sobre n. O caso $n = 1$ é conhecido do ano passado. Supondo válido o resultado para $n-1$, existe um homomorfismo de anéis $\sigma\colon A[x_1, \ldots, x_{n-1}] \to B$ que fixa os elementos de A e tal que $\sigma(x_i) = b_i$ para $i = 1, 2, \ldots, n-1$. Mas (como vimos no ano passado), para cada homomorfismo de anéis $f\colon A \to B$, a aplicação $\overline{f}\colon A[x] \to B[x]$ definida por $\overline{f}(\sum_{i=0}^n a_i\, x^i) = \sum_{i=0}^n f(a_i)\, x^i$ é também um homomorfismo de anéis. Aplicando este resultado à nossa situação obtemos um homomorfismo $\overline{\sigma}\colon A[x_1, \ldots, x_{n-1}][x_n] \to B[x_n]$ dado pela correspondência

$$p_0 + p_1 x_n + \cdots + p_m x_n^m \longmapsto \sigma(p_0) + \sigma(p_1) x_n + \cdots + \sigma(p_m) x_n^m.$$

Por outro lado, pelo resultado a uma variável, existe um homomorfismo $\tau\colon B[x_n] \to B$ tal que $\tau(b) = b$ para qualquer $b \in B$ e $\tau(x_n) = b_n$. Compondo τ com $\overline{\sigma}$ obtemos um homomorfismo nas condições do enunciado. De facto, para cada $a \in A$, $\tau\overline{\sigma}(a) = \tau(a) = a$, $\tau\overline{\sigma}(x_i) = \tau(\sigma(x_i)) = \tau(b_i) = b_i$ para $i = 1, \ldots, n-1$ e $\tau\overline{\sigma}(x_n) = \tau(x_n) = b_n$.

Quanto à unicidade, suponhamos que ψ era outro homomorfismo nessas condições. Então

$$\begin{aligned}
\psi\Big(\sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, x_1^{i_1} \cdots x_n^{i_n} \Big) &= \sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, \psi(x_1^{i_1} \cdots x_n^{i_n}) \\
&= \sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, \psi(x_1)^{i_1} \cdots \psi(x_n)^{i_n} \\
&= \sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, b_1^{i_1} \cdots b_n^{i_n} \\
&= \tau\overline{\sigma}\Big(\sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, x_1^{i_1} \cdots x_n^{i_n} \Big),
\end{aligned}$$

o que termina a demonstração. ∎

O homomorfismo $\varphi_{b_1,\dots,b_n}$ é o designado *homomorfismo de substituição*. Denotaremos a imagem $\varphi_{b_1,\dots,b_n}(p)$ por $p(b_1,\dots,b_n)$.

A imagem de $A[x_1,\dots,x_n]$ por $\varphi_{b_1,\dots,b_n}$ é exactamente o subanel de B gerado por $A\cup\{b_1,\dots,b_n\}$, que denotamos por $A[b_1,\dots,b_n]$. Sendo A um domínio de integridade, denotamos por $A(b_1,\dots,b_n)$ o corpo das fracções de $A[b_1,\dots,b_n]$ (que podemos considerar contido em B, a menos de isomorfismo, se B for um corpo; neste caso, $A(b_1,\dots,b_n)$ é o menor subcorpo de B que contém $A\cup\{b_1,\dots,b_n\}$).

Como os coeficientes dos polinómios a várias indeterminadas são eles próprios polinómios, então uma raiz de um elemento de $A[x_1,\dots,x_n]=A[x_1,\dots,x_{n-1}][x_n]$ é um polinómio nas indeterminadas $x_1,\dots,x_{n-1}$. Temos assim que usar outro nome ("zero") para os n-úplos que anulam o polinómio:

ZEROS de um polinómio

$(b_1,\dots,b_n)\in B^n$ é um *zero* de $p\in A[\overline{x}]$ se $\varphi_{b_1,\dots,b_n}(p)=0$, ou seja, $p(b_1,\dots,b_n)=0$.

Dado $p\in A[\overline{x}]$, a função $A^n\to A$ definida por $a\mapsto p(a)=\varphi_a(p)$ é chamada a *função polinomial* associada a p.

Por exemplo, o polinómio $x\in\mathbb{R}[x,y]$ tem infinitos zeros (todos os pares $(0,b)$ com $b\in\mathbb{R}$) mas como elemento de $\mathbb{R}[y][x]$ tem grau 1 logo não pode ter mais do que uma raiz em $\mathbb{R}[y]$ (e como polinómio de grau zero em $\mathbb{R}[x][y]$ não pode ter raízes em $\mathbb{R}[x]$).

Proposição 1.4. *Seja D um domínio de integridade infinito, e sejam $B_1,\dots,B_n\subseteq D$ conjuntos infinitos. Se $p\in D[x_1,\dots,x_n]$ é tal que $p(b_1,\dots,b_n)=0$ para qualquer $(b_1,\dots,b_n)\in B_1\times\cdots\times B_n$, então $p=0$.*

Demonstração. Mais uma vez demonstramos o resultado por indução sobre n. O caso $n=1$ foi provado no ano passado ("*um polinómio $p(x)\in D[x]$ de grau $n\geq 0$ não pode ter mais do que n raízes em D*"). Suponhamos então o resultado válido para $n-1$, e seja

$$p=\sum_{i\in\mathbb{N}_0} p_i(x_1,\dots,x_{n-1})\,x_n^i\in D[x_1,\dots,x_n].$$

Para cada $1\leq i\leq n-1$ sejam $b_i\in B_i$ quaisquer e consideremos $h(x_n)=p(b_1,\dots,b_{n-1},x_n)\in D[x_n]$. É claro que h se anula em $B_n\subseteq A$, um conjunto infinito. Como num domínio infinito D dois polinómios em $D[x]$ diferentes definem funções polinomiais diferentes, então $h(x_n) = 0$ em $D[x_n]$, o que quer dizer que os seus coeficientes são nulos, isto é, $p_i(b_1, \ldots, b_{n-1}) = 0$ para qualquer $i \in \mathbb{N}_0$. Como os elementos $b_1, \ldots, b_{n-1}$ são arbitrários, concluimos que os polinómios $p_i \in D[x_1, \ldots, x_{n-1}]$ se anulam sempre que $b_1 \in B_1, \ldots, b_{n-1} \in B_{n-1}$. Por hipótese de indução, isso significa que são nulos. Assim, $p = 0$ como pretendíamos. ∎

Portanto, se $p, q \in D[x_1, \ldots, x_n]$ definem a mesma função polinomial, então $p = q$. De facto, basta ver que $p - q$ se anula em D^n, com D infinito; daí decorre, pelo resultado, que $p - q = 0$, isto é, $p = q$.

2. Factorização de polinómios a várias indeterminadas

Proposição 2.1. *Se D é um domínio de integridade (resp. DFU) então $D[x_1, \ldots, x_n]$ é também um domínio de integridade (resp. DFU).*

Demonstração. Capítulo 1. ∎

Assim, se D for um domínio de integridade, podemos formar o corpo das fracções de $A[x_1, \ldots, x_n]$, que denotaremos por $A(x_1, \ldots, x_n)$.

GRAU de um polinómio

(1) Seja $x_1^{i_1} \cdots x_n^{i_n}$ um monómio de $A[x_1, \ldots, x_n]$. Chama-se *grau* deste monómio à soma dos expoentes dos x_i's:

$$\mathrm{gr}(x_1^{i_1} \cdots x_n^{i_n}) := i_1 + \cdots + i_n.$$

(2) Seja $p \in A[x_1, \ldots, x_n]$ um polinómio não nulo. Chama-se *grau* de p ao máximo dos graus dos monómios que ocorrem em p. Por convenção, diz-se que o grau do polinómio nulo é $-\infty$.
(3) Um polinómio diz-se *homogéneo* se todos os seus monómios tiverem o mesmo grau.

Tal como nos polinómios a uma indeterminada, é verdade que

$$\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q)$$

quando os coeficientes pertencem a um domínio de integridade. No entanto, não podemos usar indução para provar isso. Necessitaremos então do seguinte resultado envolvendo polinómios homogéneos:

Proposição 2.2. *Seja A um anel comutativo. Então qualquer polinómio $p \in A[x_1, \dots, x_n]$ se escreve, de modo único, como soma de parcelas homogéneas.*

Demonstração. Para provar a existência, basta partir da representação canónica de p como soma de monómios, e agrupar os monómios do mesmo grau numa mesma parcela: se $p = \sum_{i \in \mathbb{N}_0^n} a_i \, \overline{x}^i$, então

$$p = a_{(0,\dots,0)} + \sum_{i_1+\cdots+i_n=1} a_i \, \overline{x}^i + \sum_{i_1+\cdots+i_n=2} a_i \, \overline{x}^i + \cdots$$

Quanto à unicidade, consideremos $p = p_0 + p_1 \cdots + p_m = p'_0 + p'_1 + \cdots + p'_k$ onde p_j e p'_j são homogéneos de grau j para cada j. Reagrupando as parcelas podemos escrever

$$p_0 - p'_0 = (p'_1 + \cdots + p'_k) - (p_1 + \cdots + p_m),$$

em que, sendo não nulos, o polinómio da esquerda tem grau 0 e o da direita tem grau ≥ 1, um absurdo. Assim, têm de ser nulos, pelo que $p_0 = p'_0$ e $p_1 + \cdots + p_m = p'_1 + \cdots + p'_k$. Iterando o argumento para as parcelas de grau 1, concluímos que também são iguais e podemos cortá-las. E assim sucessivamente, chegaremos à conclusão que para $j \leq \min\{m, k\}$, $p_j = p'_j$. Suponhamos, sem perda de generalidade, que $k \leq m$. Se $k < m$ teríamos $p_{k+1} + \cdots + p_m = 0$, o que é impossível por p_j ser homogéneo de grau j. Logo $m = k$. ■

Teorema 2.3. *Seja D um domínio de integridade. Então* $\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q)$ *para quaisquer polinómios $p, q \in D[x_1, \dots, x_n]$.*

Demonstração. Se $p = 0$ ou $q = 0$ o resultado é óbvio. Suponhamos então $p \neq 0$, $q \neq 0$, $\mathrm{gr}(p) = n$ e $\mathrm{gr}(q) = m$. Provaremos primeiro o caso em que p e q são homogéneos. É simples de verificar que o grau de qualquer monómio que ocorra em pq é igual a $n + m$, por causa da homogeneidade. Temos pois de garantir apenas que, depois das simplificações, o produto pq não é zero. Isso é garantido pelo facto de $D[x_1, \dots, x_n]$ ser um domínio de integridade.

No caso geral, decompomos p e q em parcelas homogéneas (usando a proposição anterior) $p = p_0 + \cdots + p_n$ e $q = q_0 + \cdots + q_m$ onde $\mathrm{gr}(p_i) = i$, $\mathrm{gr}(q_j) = j$ e $p_n, q_m \neq 0$. Então

$$pq = p_n q_m + p_n \Big(\sum_{i=0}^{m-1} q_j \Big) + \Big(\sum_{i=0}^{n-1} p_i \Big) q_m + \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} p_i q_j,$$

onde todos os polinómios que aparecem nos somatórios à direita têm grau menor que $p_n q_m$, pelo caso já demonstrado. Logo $\mathrm{gr}(pq) = \mathrm{gr}(p_n q_m) = n + m$, pelo mesmo motivo. ■

A Proposição 2.1, no caso dos DFU, diz-nos que faz sentido falar da decomposição de um polinómio em factores irredutíveis.

[RECORDE que esses irredutíveis estão descritos no Teorema 3.3 do Capítulo 1.]

Exemplos. (1) É fácil de ver, usando o Teorema 3.3 do Capítulo 1, que polinómios como $xy+1$ ou $x+1$ são irredutíveis em $\mathbb{Z}[x,y]$. Por exemplo, o polinómio $xy+1$, considerado como elemento de $\mathbb{Z}[x][y]$, é primitivo pois os seus coeficientes, x e 1, são co-primos e não tem factorizações próprias (por ter grau 1). Assim, pelo Teorema 3.3, o polinómio é irredutível em $\mathbb{Z}[x,y]$. Quanto a $x+1 \in \mathbb{Z}[x][y]$, é um elemento do anel de coeficientes $\mathbb{Z}[x]$, e é irredutível por ser primitivo e não admitir factorizações próprias. Assim, sendo irredutível em $\mathbb{Z}[x]$, é irredutível em $\mathbb{Z}[x][y] = \mathbb{Z}[x,y]$, pelo mesmo teorema.

(2) O polinómio $xy^2 - x \in \mathbb{Z}[x,y] = \mathbb{Z}[x][y]$ admite a factorização $x(y^2-1)$. No entanto, não é própria pois $x \in \mathbb{Z}[x]$ (que é o anel dos coeficientes). Uma factorização própria seria por exemplo $(xy-x)(y+1)$. A factorização completa em irredutíveis é $x(y-1)(y+1)$.

(3) Vimos que se um polinómio a uma indeterminada tivesse uma raiz a então era divisível por $(x-a)$. Apliquemos este resultado ao polinómio $y^n - x^n \in \mathbb{Z}[x,y] = \mathbb{Z}[x][y]$ $(n>1)$. Como polinómio em y tem apenas termo de grau n e termo independente. Além disso, se substituirmos a indeterminada y por x (um elemento do anel dos coeficientes), verificamos que x é raiz do polinómio. Assim, o polinómio é divisível por $y-x$ em $\mathbb{Z}[x,y]$. Usando a regra de Ruffini para fazer a divisão obtemos

$$\begin{array}{c|cccccc}
 & (n) & (n-1) & (n-2) & \cdots & (1) & (0) \\
 & 1 & 0 & 0 & \cdots & 0 & -x^n \\
x & & x & x^2 & \cdots & x^{n-1} & x^n \\
\hline
 & 1 & x & x^2 & \cdots & x^{n-1} & 0
\end{array}$$

Portanto

$$y^n - x^n = (y-x)(y^{n-1} + xy^{n-2} + x^2y^{n-3} + \cdots + x^{n-2}y + x^{n-1}).$$

Logo, $y^n - x^n$ nunca é irredutível para $n > 1$.

Proposição 2.4. *Sejam A um anel, $\sigma \in S_n$ e $k < n$ um inteiro. Então $A[x_1,\ldots,x_n]$ é isomorfo a $A[x_{\sigma(1)},\ldots,x_{\sigma(n)}]$ e igual a $A[x_1,\ldots,x_k][x_{k+1},\ldots,x_n]$. Portanto,*

$$A[x_1,\ldots,x_n] \cong A[x_{\sigma(1)},\ldots,x_{\sigma(k)}][x_{\sigma(k+1)},\ldots,x_{\sigma(n)}].$$

Demonstração. Consideremos o homomorfismo de substituição

$$\varphi\colon A[x_1,\ldots,x_n] \to A[x_{\sigma(1)},\ldots,x_{\sigma(n)}]$$

que aplica x_i em x_i (não se trata da aplicação identidade pois cada indeterminada x_i desempenha um papel diferente no primeiro anel e no segundo). Este homomorfismo tem como inverso o homomorfismo de substituição ψ com a mesma correspondência $x_i \mapsto x_i$, desta vez de $A[x_{\sigma(1)},\ldots,x_{\sigma(n)}]$ para $A[x_1,\ldots,x_n]$. A conclusão de que são inversos um do outro segue do facto de que $\psi\varphi$ vai de $A[x_1,\ldots,x_n]$ para si próprio, aplica x_i em x_i e fixa A: como a identidade é outro homomorfismo de substituição verificando as mesmas condições, tem de ser o mesmo, pela unicidade. Assim, $\psi\varphi = \mathrm{id}$. Analogamente, $\varphi\psi = \mathrm{id}$.

A segunda parte do resultado segue por indução: o caso $n = 2$ é evidente e supondo o resultado válido para $n-1$ temos

$$\begin{aligned} A[x_1,\ldots,x_k][x_{k+1},\ldots,x_n] &= (A[x_1,\ldots,x_k][x_{k+1},\ldots,x_{n-1}])[x_n] \\ &\overset{\text{hip. ind.}}{=} A[x_1,\ldots,x_{n-1}][x_n] = A[x_1,\ldots,x_n]. \end{aligned}$$ ∎

Este resultado diz-nos que podemos, a menos de isomorfismo, considerar quaisquer indeterminadas como coeficientes, e quaisquer outras como indeterminadas propriamente ditas.

Seja $p \in A[x_1,\ldots,x_n]$. Chama-se *grau* de p em x_i ao grau de p considerado como elemento de $A[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n][x_i]$.

Apresentamos agora vários exemplos que ilustram como se podem aplicar os critérios de irredutibilidade estudados para provar que certos polinómios de $A[x_1,\ldots,x_n]$ são irredutíveis, ou para os factorizar. Note que as definições de elemento irredutível e elemento primo dependem apenas dos conceitos de factorização e de unidade num anel, pelo que são conservadas por isomorfismo. Assim, por exemplo, quando estamos a discutir a irredutibilidade ou primalidade de um polinómio em $\mathbb{C}[x,y,z]$ podemos considerá-lo como pertencendo a $\mathbb{C}[x,z][y]$ ou a $\mathbb{C}[z][x,y]$, por exemplo, conforme der mais jeito.

É preciso, porém, algum cuidado com o conceito de factorização própria pois esta depende do anel de coeficientes que estejamos a considerar.

Exemplo. O polinómio $x^n + y + 1$ considerado em $\mathbb{Z}[y][x]$ verifica as condições do critério de Eisenstein, com $p = y+1$ (irredutível em $\mathbb{Z}[y]$). Portanto o polinómio não admite factorização própria em $\mathbb{Z}[y][x]$. Como 1 é mdc dos seus coeficientes, 1 e $y+1$, o polinómio é irredutível em $\mathbb{Z}[y][x] = \mathbb{Z}[x,y]$.

Proposição 2.5. *Sejam A e B domínios de integridade, $f\colon A \to B$ um homomorfismo e $\overline{f}\colon A[x] \to B[x]$ a extensão definida na demonstração da Proposição 1.3. Seja $p(x) \in A[x]$, $p(x) \neq 0$, tal que $\operatorname{gr}(\overline{f}(p(x))) = \operatorname{gr}(p(x))$. Então, se $\overline{f}(p(x))$ não admitir uma factorização própria em $B[x]$, também $p(x)$ não admite factorizações próprias em $A[x]$.*

Demonstração. Suponhamos, por absurdo, que $p(x)$ tem uma factorização própia em $A[x]$:
$$p(x) = q(x)r(x), \quad \operatorname{gr}(q(x)), \operatorname{gr}(r(x)) < \operatorname{gr}(p(x)).$$
Então $\overline{f}(p(x)) = \overline{f}(q(x))\overline{f}(r(x))$, $\operatorname{gr}(\overline{f}(q(x))) \leq \operatorname{gr}(q(x)), \operatorname{gr}(\overline{f}(r(x))) \leq \operatorname{gr}(r(x))$, mas como $\operatorname{gr}(\overline{f}(p(x))) = \operatorname{gr}(p(x))$, temos de ter também igualdade nos graus dos factores e portanto $\operatorname{gr}(\overline{f}(q(x))), \operatorname{gr}(\overline{f}(r(x))) < \operatorname{gr}(\overline{f}(p(x)))$, o que contraria o facto de $\overline{f}(p(x))$ não admitir factorizações próprias em $B[x]$. ■

Aplicando este resultado ao homomorfismo de substituição, obtemos imediatamente o seguinte corolário:

Corolário 2.6. [Critério de substituição] *Seja D um DFU e*
$$p \in A[x_1, \ldots, x_n, y] = A[x_1, \ldots, x_n][y].$$
Suponhamos que, para certos elementos $a_1, \ldots, a_n \in A$, o polinómio $p(a_1, \ldots, a_n, y)$ ten o mesmo grau em y que p, e não tem factorizações próprias em $A[y]$. Então p não tem factorizações próprias em $A[x_1, \ldots, x_n][y]$.

Exemplos. (1) O polinómio
$$x^2y^2 - y^2 + x - 1 \in \mathbb{Z}[x, y],$$
escrito como elemento de $\mathbb{Z}[x][y]$ fica $(x^2-1)y^2+x-1$. Um mdc dos seus coeficientes é $x - 1$, que pode ser posto em evidência, obtendo
$$(x - 1)((x + 1)y^2 + 1) = (x - 1)(xy^2 + y^2 + 1).$$
O primeiro dos factores é claramente irredutível por ser primitivo em $\mathbb{Z}[x]$ e sem factorizações próprias (por ter grau 1). Assim, é irredutível em $\mathbb{Z}[x]$ e, portanto, irredutível em $\mathbb{Z}[x][y] = \mathbb{Z}[x, y]$. Quanto ao segundo factor, é primitivo em $\mathbb{Z}[x][y]$. Fazendo a substituição $x = 2$, obtemos o polinómio $3y^2 + 1$, que não admite factorizações próprias em $\mathbb{Z}[y]$: tem grau 2 e não tem raízes em $\mathbb{Q}$. Logo é irredutível em $\mathbb{Q}[x]$. Assim, o outro factor também é irredutível em $\mathbb{Z}[x][y]$, e terminámos a factorização.

(2) Aplicamos agora o critério das raízes fraccionárias a um polinómio a duas indeterminadas. Seja $p = x^2y^4 + y^4 - x^4 - xy^2$. Se o encararmos como elemento de $\mathbb{Z}[y][x]$, isto é, $-x^4 + y^4x^2 - y^2x + y^4$, vemos que se existirem raízes de p em $\mathbb{Z}[y]$ têm de dividir y^4 em $\mathbb{Z}[y]$. Experimentando as diversas potências de y (e as suas simétricas), vemos que y^2 é raiz e portanto o polinómio é divisível por $x - y^2$. Usando a regra de Ruffini encontramos

$$x^2y^4 + y^4 - x^4 - xy^2 = (x - y^2)(x^3 - y^2x^2 - y^2).$$

Sejam $A \subseteq B$ anéis e $b = (b_1, \ldots, b_n)$ uma família de elementos de B. A família b diz-se *algebricamente dependente* sobre A se existir um polinómio $p \in A[x_1, \ldots, x_n]$ com $p \neq 0$ tal que $p(b_1, \ldots, b_n) = 0$; caso contrário, diz-se que é *algebricamente independente.*

Exemplos. (1) É claro que as indeterminadas $(x_1, \ldots, x_n)$ são independentes sobre A (pela Proposição 1.1).

(2) O facto de π ser transcendente sobre $\mathbb{Q}$ significa nesta nova linguagem que π é algebricamente independente sobre $\mathbb{Q}$. No entanto, (π, π^2) é algebricamente dependente, pois o par é zero do polinómio $x^2 - y$.

Proposição 2.7. *Sejam $A \subseteq B$ anéis e $b_1, \ldots, b_n \in B$. Então $(b_1, \ldots, b_n)$ é uma família algebricamente independente se e só se o homomorfismo de substituição $\varphi_{b_1,\ldots,b_n}$ for injectivo. Nesse caso, este homomorfismo é um isomorfismo de $A[x_1, \ldots, x_n]$ em $A[b_1, \ldots, b_n]$.*

Demonstração. Se a família é algebricamente independente e $p \in A[\overline{x}]$ for não nulo, isto quer dizer que $\varphi_b(p) = p(b) \neq 0$, o que é equivalente a afirmar que $N(\varphi_b) = \{0\}$. A recíproca é imediata também. ∎

Exercícios

2.1. Prove que, sendo $A \subseteq B$ anéis e $b_1, \ldots, b_n \in B$, então $A[b_1, \ldots, b_n]$ é o menor subanel de B que contém A e os elementos $b_1, \ldots, b_n$ (isto é, é o subanel de B gerado por $A \cup \{b_1, \ldots, b_n\}$).

2.2. Quais dos seguintes polinómios têm factorizações próprias em $\mathbb{Z}[x][y]$? e em $\mathbb{Z}[y][x]$?

(a) $x^2 + xy + x + y$. (b) $xy^2 + x^2y + x^2 + y^2 + 2xy + x + y$.

2.3. Sabendo que $\mathbb{Z}[x, y]$ é um DFU, determine o

$$\text{mdc}\,(x^2y^2 - xy^2 + 2x^2y - 2y^2 - 2xy + x^2 - 4y - x - 2, xy^2 + x^2y + y^2 + 2xy + x^2 + y + x).$$

2.4. Determine a multiplicidade de a como raiz de $p \in A[x]$ nos seguintes casos:

(a) $p = x^3 - yx^2 - y^2x + y^3$, $a = y$, $A = \mathbb{Z}[y]$.

(b) $p = x^2y^2 + 2xy^2 + y^2 + x^2 + 2x + 1$, $a = -1$, $A = \mathbb{Z}[y]$.

2.5. Seja D um domínio de integridade. Mostre que $D[x_1, \ldots, x_n]^* = D^*$.

2.6. Seja D um DFU. Prove que se $p \in D$ é primo em D, então p é primo em $D[x_1, \ldots, x_n]$.

2.7. Factorize os seguintes polinómios num produto de irredutíveis em $\mathbb{Z}[x, y]$, $\mathbb{R}[x, y]$ e $\mathbb{C}[x, y]$.

(a) $x^2 + y^2$. (b) $x^3 - 2y^3$.

2.8. Factorize ou prove que são irredutíveis em $\mathbb{Z}[x, y]$:

(a) $xy^2 + 2x - 4y + 2$.

(b) $x^5y^2 + x^2y + 2xy + y + x$.

(c) $xy^2 + x^2y + xy + x + y + 1$.

2.9. Mostre que os seguintes polinómios são irredutíveis em $\mathbb{C}[x, y, z]$:

(a) $x^2 + y^2 - 1$. (b) $x^2 - y^2 + z^2$.

2.10. Seja C um corpo e $p(x, y) \in C[x, y]$. Prove que p tem um factor de grau 1 em $C[x, y]$ se e só se

- existir $q \in C[x]$ com $\text{gr}(q) \leq 1$ e $p(x, q(x)) = 0$ ou
- existir $r \in C[y]$ com $\text{gr}(r) \leq 1$ e $p(r(y), y) = 0$.