Revista Eletrônica Paulista de Matemática

ISSN 2316-9664
Volume 12, jul. 2018

Construção do anel de polinômios em uma indeterminada utilizando módulos

Construction of the ring of polynomials in one indeterminate using modules

Christian José Santos Gonçalves
Universidade Estadual de Maringá - DMA - UEM
chrisssgoncalves@gmail.com

Renan Willian Prado
Universidade Estadual de Campinas - Imecc - Unicamp
renanwillianprado@gmail.com

Resumo

O conceito de módulos sobre um anel comutativo com unidade A é uma generalização da noção de espaço vetorial. Como em álgebra linear, é possível definir conjunto linearmente independente, base e dimensão de maneira bem semelhante. O objetivo deste artigo é construir o anel de polinômios $A[X]$. Ele será gerado como A-módulo pelo conjunto linearmente independente $\{1, X, X^2, \dots\}$ de elementos de $S(A)$, conjunto das sequências em A.

Palavras-chave: Anéis de polinômios. Módulos. Sequências quase nulas.

Abstract

The concept of modules over a commutative ring with identity A is a generalization of the notion of vector space. As in linear algebra, it is possible to define linearly independent set, base and dimension in a very similar way. The objective of this article is construct the ring of polynomials $A[X]$. It will be generated as A-module by the linearly independent set $\{1, X, X^2, \dots\}$ of elements of $S(A)$, set of the sequences in A.

Keywords: Ring of polynomials. Modules. Sequences almost null.

Artigo recebido em abr. 2018 e aceito em jul. 2018

1 Introdução

É fato que em toda a história da matemática, os primeiros conceitos sobre polinômios, sobretudo as equações polinomiais se deram antes mesmo do formalismo matemático moderno. Um polinômio é uma expressão da forma $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, onde os coeficientes $a_n, a_{n-1}, \ldots a_0$ são elementos de um anel comutativo com unidade e o x é chamado de *indeterminada*. Nosso objetivo será formalizar este conceito, assim como fez *Peano* com os números naturais no século XIX, por exemplo.

O estudo de anéis se originou a partir de duas importantes classes, a classe dos anéis de polinômios em n variáveis sobre o corpo dos números complexos, e a classe dos anéis de inteiros algébricos de um corpo de números algébricos. Essas duas classes são responsáveis por vários resultados, muito sofisticados e um tanto quanto elegantes.

Neste artigo, precisaremos somente de alguns conceitos básicos de módulos, na qual introduziremos na primeira seção. Para um estudo mais aprofundado veja [1] ou [2].

Na seção seguinte, o conjunto $S(A)$ das sequências de elementos em A, será ainda um anel comutativo com unidade. O subconjunto $X^{\mathbb{N}} := \{X^n \in S(A) \mid n \in \mathbb{N}\}$ de elementos de $S(A)$ definido pelas potências de $X = (x_n)$ tal que $x_n = 0$, se $n \neq 1$ e $x_n = 1$, se $n = 1$, será um conjunto linearmente independente, assim, definiremos $A[X]$ como sendo o conjunto gerado por $X^{\mathbb{N}}$. Tal sequência X, é chamada de indeterminada.

É possível construir o anel de polinômios apenas com o conceito de sequências quase nulas como feito em [2] e [3], ou de modo mais intuitivo, como em [4]. No entanto, a construção feita aqui é mais algébrica do que em termos de sequências, um conceito mais analítico.

2 A-módulos

Definição 1. *Seja $A = (A, +, \cdot)$ um anel comutativo com unidade e $M = (M, \oplus)$ um grupo comutativo. Dizemos que M é um A-modulo se existe uma operação adicional, $\odot : A \times M \to M$, tal que dados $a_1, a_2 \in A$ e dados $m_1, m_2 \in M$ vale*

- $1 \odot m_1 = m_1$,
- $(a_1 \cdot a_2) \odot m_1 = a_1 \odot (a_2 \odot m_1)$,
- $(a_1 + a_2) \odot m_1 = a_1 \odot m_1 \oplus a_2 \odot m_1$;
- $a_1 \odot (m_1 \oplus m_2) = a_1 \odot m_1 \oplus a_1 \oplus m_2$.

  Para simplificar, daqui em diante escreveremos $a_1 \odot m_1 = a_1 m_1$ e $m_1 \oplus m_2 = m_1 + m_2$.

Definição 2. *Seja A um anel e M um A-módulo. Um subgrupo N de M é um A-submódulo, se a multiplicação por escalar do módulo M preserva N, isto é, se*

$$a \odot n \in N, \ \forall a \in A \ e \ \forall \ n \in N.$$

Abaixo segue dois exemplos clásicos de A-módulos. Estes exemplos mostram que A-módulos generalizam a noção de espaço vetorial e que nem todos os A-módulos são espaços vetoriais.

Exemplo 3. *Seja K um corpo e V um espaço vetorial. Então V é um K-módulo, onde $\odot$ é o produto por escalar e V é grupo abeliano com a soma $\oplus$ de vetores.*

Exemplo 4. *Todo grupo $G = (G, +)$ comutativo é um $\mathbb{Z}$ módulo dotado da operação $\odot : \mathbb{Z} \times G \to G$ com $n \odot g = ng \equiv \sum_{i=1}^{n} g$.*

Motivado pelos conceitos em espaços vetoriais, podemos definir um subconjunto gerado por um subconjunto S, subconjunto linearmente independente e base.

Definição 5. *Seja $S \subset M$, M um A-módulo, então o gerado por S é o conjunto (S) tal que*

$$(S) = \{v \in M \mid \exists \{a_{s'}\}_{s' \in S'} \subset A,\ v = \sum_{s' \in S'} a_{s'} s' \text{ e } S' \subset S \text{ é finito}\}.$$

Quando $(A) = M$, diremos que M é gerado por S ou que S é um gerador de M e quando S é finito diremos que M é finitamente gerado, ou quando se quer explicitar S, diremos que M é finitamente gerado por S. Além disso, se $v \in S$ diremos que v é combinação linear de elementos de S.

Claramente (S) é um submódulo de M, assim temos a mesma noção que em espaços vetoriais onde o gerado por um subconjunto também é subespaço.

Definição 6. *Seja S um subconjunto de M, um A-módulo, dizemos que S é linearmente independente se para qualquer família finita $\{s'_i\}_{i \in I}$ de elementos de S e qualquer família $\{a_i\}_{i \in I}$ de elementos de A vale que*

$$\sum_{i \in I} a_i s_i = 0 \Rightarrow a_i = 0,\ \forall\, i \in I.$$

Exemplo 7. *Todo subconjunto S linearmente independente de V, um K espaço vetorial, é linearmente independente de vendo V como K-módulo.*

Definição 8. *Uma base S de um A-módulo M, é um subconjunto linearmente independente e gerador de M. Nesse caso, diremos que M é um A-módulo livre. Chamamos a cardinalidade de S, denotamos por $|S| = \#S$, um posto de M ou uma dimensão de M.*

O Lema abaixo será essencial para demonstrar que a dimensão de um A-módulo está bem definido.

Lema 9. *Seja M um A-módulo e I um ideal de A. Então $IM = \{\sum_{j=1}^{n} i_j m_j \mid i_j \in I \text{ e } m_j \in M, \forall 1 \leq j \leq n\}$ é um A-módulo e M/IM é um A/I-módulo segundo a operação:*

$$\begin{array}{rccc} \odot : & A/I \times M/IM & \longrightarrow & M/IM \\ & (\lambda + I, m + IM) & \longmapsto & \lambda m + IM. \end{array}$$

Demonstração. Temos inicialmente que

$$IM = \{\sum_{j=1}^{n} i_j m_j \mid i_j \in I \text{ e } m_j \in M, \forall 1 \leq j \leq n\}.$$

Temos que IM é fechado para soma por um oposto, pois dados dois elementos $x, y \in IM$ temos que $x = \sum_{i=1}^{n} i_j m_j$ e $-y = -\sum_{i=n+1}^{n+m} i_j m_j = \sum_{i=n+1}^{n+m} (-i_j) m_j$ e assim $x - y = \sum_{i=1}^{n} i_j m_j + \sum_{i=n+1}^{n+m} (-i_j) m_j = \sum_{i=1}^{n+m} \text{sign}(n-j) i_j m_j$. Portanto IM é também grupo abeliano. Além disso, dado $a \in A$, vale que $ax = a(\sum_{i=1}^{n} i_j m_j) = \sum_{i=1}^{n} a(i_j m_j) = \sum_{i=1}^{n} (a i_j) m_j$, mas para cada j, com $1 \leq j \leq n$, temos $a i_j \in I$, pois I é um ideal de A. Logo vale que a operação $\odot|_{A \times IM}$ tem imagem contida em IM, logo IM é, também, um A-módulo.

Temos que se $(\lambda_1 + I, m_1 + IM) = (\lambda_2 + I, m_2 + IM)$, então $\lambda_1 - \lambda_2 \in I$ e $m_1 - m_2 \in IM$. Assim, como $\lambda_1 m_1 - \lambda_2 m_2 = \lambda_1 m_1 - \lambda_1 m_2 + \lambda_1 m_2 - \lambda_2 m_2 = \lambda_1(m_1 - m_2) + (\lambda_1 - \lambda_2)m_2$, então como cada parcela está em IM, temos que a soma também está. Assim, M/IM é um A/I-módulo. □

Proposição 10. *Sejam S e S' duas bases de M, um A-módulo, então $|S| = |S'|$, isto é, o posto é único e está bem definido.*

Demonstração. Seja I um ideal maximal de A, que existe pelo lema de Zorn, e seja Z qualquer base de M, um A-módulo.

Considere $\{z + IM\}_{z \in Z}$. Temos que é base de M/IM, um A/I-módulo, e $|Z| = |\{z + IM\}_{z \in Z}|$. De fato, dada $\{z + IM\}_{z \in Z_i}$ uma família finita de elementos de $\{z + IM\}_{z \in Z}$ e $\{a_z + I\}_{z \in Z_i}$ também uma família finita de elementos de A/I, se

$$\sum_{z \in Z_i} (\alpha_z + I)(z + IM) = 0 + IM,$$

então $\sum_{z \in Z_i} \alpha_z z \in IM$. Logo, como Z é base de M e reagrupando, caso necessário, existe um segundo subconjunto finito Z_j de Z e existem $i_z \in I \ \forall z \in Z_j$ tal que ainda vale

$$\sum_{z \in Z_i} \alpha_z z = \sum_{z \in Z_j} i_z z.$$

Assim, cada $\alpha_z \in I$, com $z \in Z_i$. Temos portanto, $\alpha_z + I = 0 + I$ para todo $z \in Z_i$.

Mostraremos que $\{z + IM\}_{z \in Z}$ gera M/IM. De fato, seja $m \in M$, temos que existe subconjunto finito Z_k de Z, por Z ser base de M, e elementos $a_z \in A$ para todo $z \in Z_k$, tal que

$$m = \sum_{z \in Z_k} a_z z.$$

Assim, $m + IM = (\sum_{z \in Z_k} a_z z) + IM = \sum_{z \in Z_k} (a_z z + IM) = \sum_{z \in Z_k} (a_z + I)(z + IM)$.

Falta mostrar que $|Z| = \{z + IM\}_{z \in Z}$, mas isso é claro, pois, como $\{z + IM\}_{z \in Z}$ é base de M/IM, se $z \neq z'$, então $z + IM \neq z' + IM$. Logo $|Z| = |\{z + IM\}_{z \in Z}|$.

Como I é ideal maximal, temos que A/I é corpo, assim M/IM é corpo sobre A/I, segue, portanto, que toda base de M/IM tem a mesma cardinalidade. Assim, finalmente, dadas duas bases S e S' de um A-módulo M, segue que, pelos comentários anteriores, $|S'| = |\{s' + IM\}_{s' \in S'}| = |\{s + IM\}_{s \in S}| = |S|$, como queríamos demonstrar. □

Abaixo daremos um exemplo de um módulo M que não é livre, isto é, um módulo que não possui base.

Exemplo 11. *Seja $n > 1$ um número inteiro, o grupo abeliano $\mathbb{Z}_n$ não é um $\mathbb{Z}$-módulo livre. Apesar de ser, claramente, um $\mathbb{Z}$-módulo, $\mathbb{Z}_n$, $n > 1$, não é livre. De fato, dado $\overline{z} \in \mathbb{Z}_n$, $n \cdot \overline{z} = \overline{0}$. Logo nenhum subconjunto S de $\mathbb{Z}_n$ pode ser linearmente independente sobre $\mathbb{Z}$.*

A proposição seguinte diz que, como em espaços vetoriais, que todo elemento é escrito de modo único como combinação linear de vetores da base.

Proposição 12. *Seja $S \subset M$ uma base para M. Todo elemento de M se escreve, de modo único, como combinação linear não nula de elementos de S, i.e., dados X e Y, dois pares de subconjuntos finitos de S, $\{a_x\}_{x \in X}$ e $\{b_y\}_{y \in Y}$, dois subconjuntos finitos de elementos não nulos de A, tais que $\sum_{x \in X} a_x x = \sum_{y \in Y} b_y y$, então $X = Y$ e $\{a_x\}_{x \in X} = \{b_y\}_{y \in Y}$.*

Demonstração. Dados X e Y, $\{a_x\}_{x\in X}$ e $\{b_y\}_{y\in Y}$ tais como o enunciado, então $\sum_{x\in X} a_x x = \sum_{y\in Y} b_y y$. Logo,

$$\sum_{x\in X} a_x x - \sum_{y\in Y} b_y y = 0.$$

Dado $x^* \in X$, suponha, por absurdo, que x^* não está em Y, então, $(\sum_{x\in X-\{x^*\}} a_x x - \sum_{y\in Y} b_y y) + a_{x^*} x^* = 0$. Como $\sum_{x\in X-\{x^*\}} a_x x - \sum_{y\in Y} b_y y \in ((X-\{x^*\})\cup Y)$, i.e., está no espaço gerado por $(X-\{x^*\})\cup Y$, segue que existe uma família finita $\{c_z\}_{z\in(X-\{x^*\})\cup Y}$ de elementos de A tal que $\sum_{x\in X-\{x^*\}} a_x x - \sum_{y\in Y} b_y y = \sum_{z\in(X-\{x^*\})\cup Y} c_z z$. Logo,

$$\sum_{z\in(X-\{x^*\})\cup Y} c_z z + a_{x^*} x^* = 0.$$

Assim, necessariamente $a_{x^*} = 0$, o que é um absurdo. Da mesma forma, se prova que dado $y^* \in Y$, então $y^* \in X$. Temos, portanto, que $X = Y$. Agora como $X = Y$,

$$\sum_{x\in X} a_x x - \sum_{y\in Y} b_y y = \sum_{x\in X} (a_x - b_x) x = 0.$$

Assim, $a_x = b_x$, $\forall x \in X$, donde $\{a_x\}_{x\in X} = \{b_y\}_{y\in Y}$, como queríamos demonstrar. □

Finalmente temos todas as ferramentas necessárias para se definir polinômios em uma indeterminada.

3 Polinômios em uma indeterminada

Seja um anel A comutativo com unidade e considere o conjunto $S(A)$ das sequências com elementos em A, isto é,

$$S(A) = \{\, s \subset \mathbb{N}\times A \mid s \text{ é função}\}.$$

Denotaremos s, um elemento de $S(A)$, por $(s_n)_n$ para dizer que $s(n) = s_n$ para todo $n \in \mathbb{N}$.

Definição 13. *Em $S(A)$ consideremos duas operações $\oplus$ e $\odot$, chamadas de adição e produto por escalar respectivamente, da seguinte forma: $\forall f, g \in S(A)$ e $a \in A$,*

$$\begin{aligned} \oplus : S(A)\times S(A) &\to S(A) \\ (f,g) &\longmapsto f\oplus g \end{aligned} \qquad \begin{aligned} \odot : A\times S(A) &\to S(A) \\ (a,f) &\longmapsto a\odot f \end{aligned}$$

Com $(f\oplus g)_n = (f_n + g_n)_n$ e $(a\odot f)_n = (af_n)$.

Em algumas momentos usaremos as notações $f+g$ e af para as operações $f\oplus g$ e $a\odot f$ respectivamente.

Proposição 14. *Com as operações $\oplus$ e $\odot$ definidas acima segue que $S(A)$ é um A-módulo.*

Demonstração. De fato, é fácil provar que $S(A)$ é grupo comutativo com a operação $\oplus$. Falta mostrar que $\forall a, b \in A$ e $\forall f, g \in S(A)$, vale as condições da definição (1):

- $1f = (1f_n)_n = (f_n)_n = f$,
- $(ab)f = ((ab)f_n)_n = (a(bf_n))_n = a(bf_n)_n = a(bf)$,

- $(a+b)f = ((a+b)f_n)_n = (af_n + bf_n)_n = (af_n)_n + (bf_n)_n = a(f_n)_n + b(f_n)_n = af + bf$,
- $a(f+g) = a(f_n+g_n)_n = (a(f_n+g_n))_n = (af_n+ag_n) = (af_n)_n + (ag_n)_n = a(f_n)_n + a(g_n)_n = af + af$.

□

Nosso próximo passo será fazer com que $S(A)$ passe a ser um anel comutativo com unidade, para isso precisaremos definir uma segunda operação em $S(A)$:

Definição 15. *Em $S(A)$ definimos $\circ : S(A) \times S(A) \to S(A)$ tal que se f e g estão em $S(A)$, então $f \circ g = c$, onde*

$$c_n = \sum_{i=0}^{n} f_i g_{n-i},\ \forall\, n \in \mathbb{N}.$$

Denotamos $f \circ g$ por fg, isto é, $f \circ g = fg$.

Proposição 16. *$S(A) = (S(A), \oplus, \circ)$ é um anel comutativo com unidade.*

Demonstração. Já sabemos que $S(A)$ é grupo comutativo com a operação $\oplus$ e portanto falta mostrar que existe $1 \in S(A)$ tal que para quaisquer $f, g, h \in S(A)$ vale

1. $1 \circ f = f$,
2. $f \circ g = g \circ f$,
3. $(f \circ g) \circ h = f \circ (g \circ h)$,
4. $f \circ (g+h) = f \circ g + f \circ h$.

Tome $1 = (s_n)_n$, $s_n = 1$, se $n = 0$, e $s_n = 0$, caso contrário. Temos que para quaisquer f, g, h em $S(A)$ vale

1. $1 \circ f = f$. De fato, $1f = (s_n)_n (f_n)_n = (\sum_{j=0}^{n} s_j f_{n-j})_n = (s_0 f_n)_n = (1 f_n)_n = (f_n) = f$. Da mesma forma, $f1 = (\sum_{j=0}^{n} f_j s_{n-j})_n = (f_n s_{n-n}) = (f_n 1)_n = (f_n)_n = f$,
2. $f \circ g = g \circ f$. De fato, temos que $f \circ g = (f_n)_n (g_n)_n = (\sum_{j=0}^{n} f_j g_{n-j})_n = (\sum_{j=0}^{n} f_{n-j} g_j)_n = (\sum_{j=0}^{n} g_j f_{n-j})_n = (g_n)_n (f_n)_n = g \circ f$,
3. $(f \circ g) \circ h = f \circ (g \circ h)$. Temos que

$$\begin{aligned}
(fg)h &= (\sum_{i=0}^{n} f_i g_{n-i})_n h = (\sum_{i=0}^{n} f_i g_{n-i})_n (h_n)_n = \\
&= (\sum_{j=0}^{n} (\sum_{i=0}^{j} f_i g_{j-i}) h_{n-j})_n = (\sum_{j=0}^{n} \sum_{i=0}^{j} f_i g_{j-i} h_{n-j})_n = \\
&= (\sum_{i=0}^{n} \sum_{j=i}^{n} f_i g_{j-i} h_{n-j})_n = \\
&= (\sum_{i=0}^{n} \sum_{j=i}^{n} f_i g_{j-i} h_{n-j})_n = (\sum_{i=0}^{n} f_i (\sum_{j=i}^{n} g_{j-i} h_{n-j}))_n = \\
&= (\sum_{i=0}^{n} f_i (\sum_{k=0}^{n-i} g_k h_{n-i-k}))_n = (f_n)_n (\sum_{k=0}^{n} g_k h_{n-k})_n = \\
&= (f_n)_n ((g_n)_n (h_n)_n) = f(gh).
\end{aligned}$$

Aqui vale a pena fazer um comentário do que foi feito. Note que $\{(i,j) \in \mathbb{Z}\times\mathbb{Z} \mid 0 \leq j \leq n, 0 \leq i \leq j\} = \{(i,j) \in \mathbb{Z}\times\mathbb{Z} \mid 0 \leq i \leq n, i \leq j \leq n\}$, fazendo uma mudança de coordenadas tal como feita em Cálculo ao trocar a ordem de integração da integral dupla. Por essa razão $\sum_{j=0}^{n}\sum_{i=0}^{j} a_{i,j} = \sum_{i=0}^{n}\sum_{j=i}^{n} a_{i,j}$, pela comutatividade da operação adição.

4. $f\circ(g+h) = f\circ g + f\circ h$. De fato,

$$\begin{aligned} f(g+h) = (f_n)_n((g_n)+(h_n)_n) = (f_n)_n((g_n+h_n)_n) = (\sum_{i=0}^{n} f_i(g_{n-i}+h_{n-i}))_n = \\ = (\sum_{i=0}^{n} f_i g_{n-i} + f_i h_{n-i}))_n = (\sum_{i=0}^{n} f_i g_{n-i} + \sum_{i=0}^{n} f_i h_{n-i})_n = \\ = (\sum_{i=0}^{n} f_i g_{n-i})_n + (\sum_{i=0}^{n} f_i h_{n-i})_n = \\ = (f_n)_n(g_n) + (f_n)_n(h_n)_n = fg + fh. \end{aligned}$$

Portanto $S(A)$ é anel com as operações dadas, como queríamos demonstrar. □

Definição 17. *A sequência $X = (x_n)$ tal que $x_n = 0$, se $n \neq 1$ e $x_n = 1$, se $n = 1$, é chamada indeterminada.*

Definição 18. *Para manter a uniformidade daqui em diante, defina $X^0 = 1$, onde $1 \in S(A)$ é a unidade deste anel.*

Definição 19. *Defina, indutivamente, para cada $n \geq 1$, $X^{n+1} = XX^n$.*

A proposição seguinte descreve como é a lei da sequência X^n e será importante nas próximas proposições e demonstrações.

Proposição 20. *Dado $n \geq 1$, vale $X^n = (\delta_{m,n})_m$, onde $\delta_{m,n}$ é a função delta de Kronecker, definida por, $\delta_{m,n} = 0$, se $m \neq n$ e $\delta_{m,n} = 1$, se $m = n$.*

Demonstração. A lei, por definição, vale para $n = 1$. Assim, suponha por indução que a lei valha para n, qualquer natural dado, temos que $X^{n+1} = XX^n = (x_m)_m(\delta_{m,n})_m = (\sum_{i=0}^{m} x_i\delta_{m-i,n})_m = (x_1\delta_{m-1,n})_m = (1\delta_{m-1,n})_m = (\delta_{m-1,n})_m = (\delta_{m,n+1})_m$, como queríamos demonstrar. □

Abaixo vamos provar que vale a regra da soma da potência da indeterminada.

Proposição 21. *Dados $i, j \in \mathbb{N}$, $X^iX^j = X^{i+j}$.*

Demonstração. Dados $i, j \in \mathbb{N}$, temos que

$$X^iX^j = (\delta_{n,i})_n(\delta_{n,j})_n = (\sum_{k=1}^{n} \delta_{k,i}\delta_{n-k,j})_n = (\delta_{i,i}\delta_{n-i,j})_n$$

$$= (\delta_{n-i,j})_n = (\delta_{n,i+j})_n = X^{i+j},$$

como queríamos demonstrar. □

Proposição 22. *O subconjunto de elementos de $S(A)$ dado por $\{X^n \in S(A) \mid n \in \mathbb{N}\}$ é um conjunto linearmente independente de $S(A)$.*

Demonstração. Seja $\{X^n\}_{n\in\eta}$ uma família finita de elementos de $\{X^n \in S(A) \mid n \in \mathbb{N}\}$ e seja $\{a_n\}_{n\in\eta}$ uma família finita de elementos de A tal que $\sum_{n\in\eta} a_n X^n = 0$. Claramente, $\eta \subset \mathbb{N}$ é finito. Pela Proposição 21, $\sum_{n\in\eta} a_n X^n = \sum_{n\in\eta} a_n(\delta_{m,n})_m = \sum_{n\in\eta}(a_n\delta_{m,n})_m = (\sum_{n\in\eta} a_n\delta_{m,n})_m = 0$. Logo,

$$\sum_{n\in\eta} a_n\delta_{m,n} = 0, \ \forall\, m \in \mathbb{N}. \tag{1}$$

Seja $n' \in \eta$, por 1, $\sum_{n\in\eta} a_n\delta_{n',n} = 0$, assim $\sum_{n\in\eta} a_n\delta_{n',n} = a'_n\delta_{n',n'} = a'_n = 0$, como queríamos demonstrar. □

A seguir vem a principal definição do presente artigo, onde a definição vem de modo natural.

Definição 23. *O conjunto gerado, veja Definição 5, por $X^{\mathbb{N}} = \{X^n \in S(A) \mid n \in \mathbb{N}\}$ denotado por $A[X]$, isto é, $A[X] = (\{X^n \in S(A) \mid n \in \mathbb{N}\}) = \{\sum_{x\in X^*} a_x x \mid \{a_x\}_{x\in X^*} \subset A$ com $X^* \subset X^{\mathbb{N}}$ finito $\}$ é o conjunto dos polinômios com coeficiente em A. O conjunto $A[X]$ é chamado anel dos polinômios em uma indeterminada.*

Segue que, como o esperado, pela Proposição 22, o conjunto $X^{\mathbb{N}}$ é base para o anel dos polinômios. Assim, os polinômios tem dimensão infinita enumerável e, pela Proposição 10, todas as bases tem dimensão infinita enumerável. Além disso, note que dado $x \in X^{\mathbb{N}}$, existe um único $i \in \mathbb{N}$ tal que $x = X^i$, assim podemos escrever as somas $\sum_{x\in X^*} a_x x$ por $\sum_{i\in\eta} a'_i X^i$, onde η é um subconjunto finito dos naturais e $a_x = a'_i$, quando $x = X^i$. Além disso, como η é finito segue que η é limitado, digamos por $n \in \mathbb{N}$, logo defina $b_i = 0$, se $i \leq n$ e $i \notin \eta$ e $b_i = a'_i$, se $i \leq n$ e $i \in \eta$. Portanto, $\sum_{x\in X^*} a_x x = \sum_{i\in\eta} a'_i X^i = \sum_{i=0}^n b_i X^i$. Assim, os polinômios tem a forma usual de se escrever. Por essa razão, em geral, denotamos um polinômio por $P(X)$.

Definição 24. *Seja $P(X) = \sum_{i=0}^n a_i X^i \in A[X]$ um polinômio não nulo. Dizemos que um número $gr(P(X)) \in \mathbb{N}$ é o grau do polinômio $P(X)$, se $P(X) = \sum_{i=1}^{gr(P(X))} a_i X^i$ e $a_{gr(P(X))} \neq 0$, isto é, $gr(P(X))$ é o maior n, tal que a_n não é nulo.*

Definição 25. *Diz-se que uma sequência $(s_n)_{n\in\mathbb{N}} \in S(A)$ é quase nula se existe $n_0 \in \mathbb{N}$ tal que $s_n = 0$, $\forall\, n \geq n_0$ ou, equivalentemente, o conjunto $\{n \in \mathbb{N} \mid s_n \neq 0\}$ é finito. O conjunto dessas sequências denotaremos por E.*

Proposição 26. *O conjunto dos polinômios em uma indeterminada é o conjunto das sequências quase nulas.*

Demonstração. Seja $P(X) = \sum_{i=0}^n a_i X^i \in A[X]$ um polinômio. Pela Proposição 20,

$$P(X) = \sum_{i=0}^n a_i X^i = \sum_{i=0}^n a_i(\delta_{m,i})_m = \sum_{i=0}^n (a_i\delta_{m,i})_m = (\sum_{i=0}^n a_i\delta_{m,i})_m.$$

Tome $m \geq n+1$, para que $\delta_{m,i} = 0$, para todo $0 \leq i \leq n$, logo $\sum_{i=0}^n a_i\delta_{m,i} = \sum_{i=0}^n a_i 0 = 0$ e assim $P(X) \in E$. Logo $A[X] \subset E$. Seja $(s_n)_n \in E$, temos que existe $n_0 \in \mathbb{N}$ tal que $s_n = 0$, $\forall\, n \geq n_0$, mas assim temos que $(s_n)_n = \sum_{i=0}^n s_i(\delta_{m,i})_m = \sum_{i=0}^n s_i X^i$. Portanto, $(s_n)_n \in A[X]$. Logo $E \subset A[X]$. Donde $A[X] = E$. □

Abaixo daremos uma aplicação imediata da proposição acima.

Corolário 27. *O conjunto das sequências quase nulas nos racionais é enumerável.*

Demonstração. Pela Proposição 26, temos que as sequências quase nulas são exatamente os polinômios com coeficientes racionais. Como $\mathbb{Q}[X]$ tem base enumerável e os racionais são enumeráveis, segue que o o conjunto das sequências é enumerável. □

A definição de polinômios, como gerado por $X^{\mathbb{N}}$, permite provar facilmente que produtos de polinômios é também um polinômio, como demonstrado na proposição seguinte.

Proposição 28. *Dados $P(X), Q(X) \in A[X]$, então $P(X)Q(X) \in A[X]$.*

Demonstração. Dados $P(X), Q(X)$, existe duas famílias finitas de elementos de A, digamos, $\{a_i\}_{0\leq i\leq m}$ e $\{b_j\}_{0\leq j\leq n}$, tais que $P(X) = \sum_{i=0}^{m} a_i X^i$ e $Q(X) = \sum_{j=0}^{n} b_j X^j$, logo

$$P(X)Q(X) = (\sum_{i=0}^{m} a_i X^i)(\sum_{j=0}^{n} b_j X^j) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j X^i X^j = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j X^{i+j}.$$

Assim, $P(X)Q(X)$ está no gerado por $X^{\mathbb{N}}$ e portanto está em $A[X]$. □

Até agora não está claro o motivo de se ter tomado um polinômio como uma sequência infinita e não como uma função $f : A \to A$ tal que $f(X) = \sum_{i=1}^{n} a_i X^i$. A importância de tal construção vai ser mostrada no exemplo a seguir.

Exemplo 29. *Seja $n \in \mathbb{N}$ e considere $\mathbb{Z}_n$ o conjunto dos inteiros módulo n. Seja $f : \mathbb{Z}_n \to \mathbb{Z}_n$ tal que $f(X) = \prod_{i=1}^{n}(X - \bar{i})$. Temos que $f(X) = \bar{0}$ para todo $X \in \mathbb{Z}_n$, isto é, a função f é a função identicamente nula. No entanto, o polinômio $\prod_{i=1}^{n}(X - \bar{i}) \in S(A)$ não é, claramente, polinômio nulo.*

O exemplo acima nos motiva a definir o valor de $f(X)$ aplicado num elemento de A.

Definição 30. *Seja $f(X) = \sum_{i=0}^{n} a_i X^i$ um polinômio em $A[X]$. Chamamos de valor do polinômio $f(X)$ em $x \in A$, denotado por $f(x)$, o escalar $f(x) \in A$ tal que $f(x) = \sum_{i=0}^{n} a_i x^i$. Quando $f(x) = 0$, chamamos x de uma raiz ou um zero do polinômio f.*

Note que, como a representação de um polinômio é única, pois $X^{\mathbb{N}}$ é base, pela Proposição 22, e pela unicidade da combinação linear, vide Proposição 12, dado um polinômio $P(X) \in A[x]$ e $x \in A$, existe um único valor $P(x) \in A$. Isso nos permite definir função polinomial:

Definição 31. *Chamamos de função polinomial qualquer função $f : A \to A$ com $f(\alpha) = P(\alpha)$ para todo $\alpha \in A$ com $P(X) \in A[X]$. Quando $f(\alpha) = 0$, chamamos α de uma raiz ou um zero do polinômio $P(X)$. Dizemos que, nesse caso, f é uma função polinomial determinada pelo polinômio $P(X)$.*

4 Conclusão

É possível construir o anel de polinômios apenas com o conceito de sequências quase nulas como feito em [2] e [3], ou de modo mais intuitivo, como em [4]. No entanto, a construção feita aqui é mais algébrica do que em termos de sequências, um conceito mais analítico. Além disso, nossa construção é bem mais geral, por exemplo, pode-se definir uma família finita elementos de um A-módulo M, digamos $\{X_i\}_{1\leq i\leq n}$ que comutam no produto de vetores, a fim de definir o conjunto polinômios de n indeterminadas como sendo o gerado pelo conjunto linearmente independente $\{\prod_{i=1}^{n} X_i^{\alpha_i} \mid \alpha_i \in \mathbb{N},\ \forall\ 1 \leq i \leq n\}$. Temos portanto uma grande liberdade de construção de estruturas somente com a teoria básica de A-módulos.

Referências

[1] ATIYAH, M. F.; MACDONALD, I. G. **Introduction to commutative algebra**. London: Addison-Wesley Publishing Co., 1969.

[2] GARCIA, A.; LEQUAIN, Y. **Elementos de álgebra**. 5. ed. Rio de Janeiro: Instituto Nacional de Matematica Pura e Aplicada, 2008.

[3] MONTEIRO, L. H. J. **Elementos de álgebra**. Rio de Janeiro: IMPA, 1969.

[4] FRALEIGH, J. B. **A first course in abstract algebra.** 7. ed. Boston. Pearson Education, Inc., 2003.

[5] HOFFMAN, K.; KUNZE, R. **Álgebra linear**. São Paulo: Editora Polígono, 1971.