Journal homepage http://revistas.unitru.edu.pe/index.php/SSMM

SELECCIONES MATEMÁTICAS
Universidad Nacional de Trujillo
ISSN: 2411-1783 (Online)
2022; Vol. 9(2): 323-335.

Classification of abelian groups finitely generated and applications

Clasificacão de grupos abelianos finitamente gerados e algumas aplicacões

Elisângela Valéria de Jesus, Aislan Leal Fontes and Carlos Mejía Alemán

Received, Oct. 30, 2022 *Accepted, Dec. 05, 2022*

How to cite this article:
Valéria de Jesus E. et. al *Classification of abelian groups finitely generated and applications*. Selecciones Matemáticas. 2022;9(2):323–335. http://dx.doi.org/10.17268/sel.mat.2022.02.16

Abstract

In this work we establishe relations between modules over a ring and vector spaces, we show results of linear algebra that can be extended to modules and we present counterexamples to those ones that cannot be extended. By identify abelian groups with $\mathbb{Z}$-modules we classify every the finitely generated abelian groups and we show a decomposition in direct sum of ciclic subgroups. Finally, we apply the results about finitely generated abelian groups to determine the rational canonical form of an endomorphism of finitely generated $K[t]$-modules and simplify the computation of associated numbers to the endomorphism, for example: the rank and the determinant.

Keywords. Modules, vector spaces, abelian groups, ciclic decomposition.

Resumo

Nesse trabalho estabelecemos relações entre módulos sobre um anel e espaços vetoriais, exibimos resultados de álgebra linear que podem ser estendidos para módulos e apresentamos contraexemplos para aqueles resultados que não podem ser estendidos. Identificando grupos abelianos com $\mathbb{Z}$-módulos, classificamos todos os grupos abelianos finitamente gerados e exibimos uma decomposição em soma direta de subgrupos cíclicos. Finalmente, aplicamos os resultados acerca de grupos abelianos finitos para determinar a forma canônica racional de um endomorfismo de $K[t]$-módulos finitamente gerados e simplificar o cálculo de números associados ao endomorfismo, por exemplo: o posto e o determinante.

Palavras-chave . Módulos, espaços vetoriais, grupos abelianos, decomposição cíclica.

1. Introducción. O presente artigo constitui-se de um fragmento da pesquisa de Jesus (2017) referente à dissertação de Mestrado Profissional em Matemática da Fundação Universidade Federal de Sergipe, intitulada "Módulos e grupos abelianos finitamente gerados". Para este artigo, estabelecemos como objetivo principal, detalhar os principais resultados desse assunto para torná-lo mais acessível a iniciantes interessados em compreender tal teoria.

A resolução de sistemas lineares é um problema básico de álgebra linear trabalhado no ensino médio onde procuramos as soluções sobre um corpo, geralmente, $\mathbb{R}$ ou $\mathbb{C}$. Esse problema se torna mais difícil se consideramos sistemas lineares com entradas em um anel A e procuramos por soluções nesse anel, por consequência do número reduzido de propriedades que caracteriza A. Com o intuito de tratar esse assunto de forma mais compreensível, foram detalhados os principais resultados associado ao tema encontrados principalmente em [1] e distribuídos da seguinte forma:
Na seção 2, apresentamos alguns resultados básicos de Álgebra Linear e salientamos algumas considerações importantes. Tais resultados geralmente são abordados nas disciplinas da área de Álgebra em cursos de Licenciatura em Matemática, mas sem destacar algumas particularidades. Por exemplo: ao considerar o

*Escola Municipal Cecílio Eugênio Alves, Brasil. (eli.vjesus01@gmail.com).
†Universidade Federal de Sergipe, Brasil. (aislan@ufs.br).
‡Universidad de Lima, Perú. (c.mejia.aleman@gmail.com).

conjunto dos coeficientes sendo um anel, estamos trabalhando com o conceito de módulos sobre um anel e obtemos resultados análogos aos de espaço vetorial. No entanto, existem afirmações verdadeiras em espaço vetorial que não se estendem a um módulo. Pois, não é verdade que todo conjunto gerador de um A-módulo contém uma base e é falso que todo subconjunto linearmente independente de um A-módulo possa ser completado a uma base. Ainda podemos citar o fato de que um módulo finitamente gerado sobre um anel não comutativo pode ter bases com cardinalidade diferentes (ver exemplo 2.9).

Ademais, destacamos outro ponto importante em Álgebra Linear que é desenvolver técnicas para conseguir diagonalizar um operador linear sobre um espaço vetorial de dimensão finita usando o fato de que números associados a uma operador linear, como o posto ou o determinante, podem ser determinados através de uma simples análise de sua matriz associada. Também citamos o teorema espectral o qual afirma que toda matriz simétrica é equivalente a uma matriz diagonal. Inclusive, é estudado a forma canônica de Jordan de uma matriz que sobre condições específicas fornece uma matriz diagonal em blocos equivalente a matriz considerada.

Ainda na seção 2, introduzimos fatos conhecidos acerca de módulos e apresentamos vários exemplos com objetivo de fazer um comparativo desses resultados com exemplos em espaços vetoriais.

Finalmente, podemos destacar que o exemplo 2.2 garante que um grupo abeliano é simplesmente um $\mathbb{Z}$-módulo. Já na seção 4, usamos essa identificação para classificar os grupos abelianos finitamente gerados conforme teorema 4.1. Anteriormente, na seção 3 descrevemos as operações elementares que podem ser aplicadas a linhas e colunas de uma matriz, além de evidenciarmos a existência de uma matriz diagonal associada a uma matriz dada B com a condição de essas duas matrizes apresentarem o mesmo módulo. Por fim, na seção 5 aplicamos os resultados de módulos aqui obtidos para encontrar a forma racional de um endomorfismo de $K[t]$-módulos, K um corpo.

Enfim, esperamos que esse trabalho contribua para o melhor amadurecimento do profissional da área de Matemática ou área fim, especialmente dos aspirantes a professor de Matemática, quanto ao conhecimento e abstração dessa teoria, tendo em vista as diversas aplicações em conteúdos trabalhados na educação básica, nos quais o docente poderá ministrar com mais domínio e desenvoltura.

2. Fatos sobre Módulos. Vamos apresentar algumas definições básicas de módulos bem como exemplos e alguns resultados que consideramos significativos. Neste trabalho, vamos considerar A um anel com unidade.

Definição 2.1. Seja A um anel. Um A-módulo M é um grupo abeliano aditivo $(M,+)$ dotado de uma multiplicação escalar

$$\begin{aligned} A \times M &\longrightarrow M \\ (a,m) &\longmapsto a \cdot m \end{aligned}$$

que satisfaz

$$1 \cdot m = m, \quad (ab) \cdot m = a \cdot (bm), \quad (a+b) \cdot m = a \cdot m + b \cdot m, \quad a \cdot (m+n) = a \cdot m + a \cdot n,$$

para todos a, b em A e para todos m, n em M.

Example 2.1. Seja $(A,+,\cdot)$ um anel.

1 Todo espaço vetorial sobre um corpo K é um K-módulo.

2 Considere

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A\}.$$

Com as operações usuais de soma de n-uplas e multiplicação por escalar temos que A^n é um A-módulo.

3 Seja $M = \mathcal{M}_{m\times n}(A)$ o conjunto de todas matrizes de ordem $m \times n$ com entradas em A. Definindo a adição usual das matrizes e a multiplicação usual de matrizes por escalar, temos que M é um A-módulo.

Example 2.2. Sejam $A = (\mathbb{Z},+,\cdot)$ um anel e $(G,+)$ grupo abeliano. Defina a multiplicação escalar por

$$\begin{aligned} * : \mathbb{Z} \times G &\longrightarrow G \\ (a,v) \longmapsto a * v &:= \begin{cases} \underbrace{v + v + \cdots + v}_{a \text{ vezes}}, & \text{se } a \geq 0, \\ \underbrace{(-v) + (-v) + \cdots + (-v)}_{-a \text{ vezes}}, & \text{se } a < 0. \end{cases} \end{aligned}$$

Com essa operação temos que G é um $\mathbb{Z}$-módulo. Vamos provar a propriedade 2 e as demais ficam para o leitor. Para todo a e b em z e v, v_1 e v_2 em G, temos dois casos a analisar: $a \cdot b \geq 0$ ou $a \cdot b < 0$. Se $a \cdot b \geq 0$, então $a, b \geq 0$ ou $a, b < 0$. Quando $a, b \geq 0$ (se $a, b < 0$, então $-ab > 0$)

$$\begin{aligned}(a \cdot b) * v &= \underbrace{v + \cdots + v}_{ab \text{ vezes}} \\ &= \underbrace{\underbrace{v + \cdots + v}_{b \text{ vezes}} + \cdots + \underbrace{v + \cdots + v}_{b \text{ vezes}}}_{a \text{ vezes}} \\ &= b * v + \cdots + b * v = a \cdot (bv).\end{aligned}$$

Obsdervação 2.1. Da definição 2.1 e do exemplo 2.2 vemos que

grupos abelianos = $\mathbb{Z}$-módulos.

Definição 2.2. Sejam A um anel, M um A-módulo e W um subconjunto não vazio de M. Dizemos que W é um submódulo do A-módulo M ou um A-submódulo de M se para todos w_1, w_2 em W e $a \in A$ vale

$$aw_1 + w_2 \in W.$$

1 Seja V um espaço vetorial sobre um corpo K. Um subconjunto $S \subseteq V$ é um K-submódulo de V se, e somente se, S é um subespaço vetorial de V.
2 Seja $(G, +)$ um grupo abeliano. Então os $\mathbb{Z}$-submódulos são exatamente os seus subgrupos.
3 Os submódulos do A-módulo A são os ideais de A.

Definição 2.3. Sejam $W_1, \ldots, W_k$ A-submódulos de M. Dizemos que M é a soma direta dos submódulos $W_1, \ldots, W_k$, e escrevemos $M = W_1 \oplus \cdots \oplus W_k$ se:

- $M = W_1 + \cdots + W_k$;
- Se $w_1 + \cdots + w_k = 0$, com w_i em W_i, então $w_i = 0$ para todo i.

Em outras palavras, M é a soma direta dos submódulos W_i, se cada elemento v em M pode ser escrito unicamente na forma $v = w_1 + \cdots + w_k$, com w_i em W_i.

Example 2.3. Consideremos o $\mathbb{Z}$-módulo $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Os subconjuntos $N_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $N_2 = \{\overline{0}, \overline{3}\}$ são submódulos de $\mathbb{Z}_6$ tais que

$$N_1 \cap N_2 = \{\overline{0}\} \text{ e } \mathbb{Z}_6 = N_1 + N_2.$$

Portanto, $\mathbb{Z}_6 = N_1 \oplus N_2$.

Definição 2.4. *Sejam $(M, +)$ e $(M', \uplus)$ dois A-módulos. Uma aplicação $\varphi : M \to M'$ é homomorfismo de A-módulos ou um A-homomorfismo se para todos a em A, v_1, v_2 em M temos que :*

i. $\varphi(v_1 + v_2) = \varphi(v_1) \uplus \varphi(v_2)$, para todos v_1, v_2 em M;

ii. $\varphi(a \cdot v) = a \odot \varphi(v)$, para todos a em A, v em M.

Example 2.4. Se K é um corpo, os homomorfismos de K-módulos são as transformações lineares entre espaços vetoriais sobre K.

Definição 2.5. Dizemos que um homomorfismo de A-módulos é isomorfismo de A-módulos se ele é bijetivo. Quando existe um isomorfismo entre dois A-módulos M e M', dizemos que M é isomorfo à M', e denotamos por $M \simeq M'$.

Definição 2.6. Dado um homomorfismo de A-módulos $\varphi : M \to M'$, definimos o núcleo de φ e a imagem de φ, respectivamente, como os seguinte conjuntos:

$$ker(\varphi) = \{v \in M \mid \varphi(v) = 0\}$$

e

$$Im(\varphi) = \{\varphi(v) \in M' \mid v \in M\}.$$

Segue da definição que o núcleo de um homomorfismo $\varphi : M \to M'$ é um submódulo de M e a imagem $Im(\varphi)$ um submódulo de M'. Seja M um A-módulo e N um submódulo de M. Então, o grupo quociente $(M/N, +)$, isto é, o conjunto de $\{m + N \mid m \in M\}$ das classes laterais de N em M, munido de uma multiplicação por escalar de A

$$r \cdot \overline{v} = r \cdot (v + N) = rv + N = \overline{rv}, \forall r \in A, \forall v \in M$$

hereda uma estrutura de A-módulo de M. O A-módulo M/N chamado de *A-módulo quociente* de M por N. O teorema a seguir é o analogo ao teorema do isomorfismo para grupos cuja prova pode ser encontrada em [3].

Teorema 2.1 (Teorema do Isomorfismo). *Seja $\varphi : M \to M'$ um homomorfismo sobrejetor de A-módulos cujo $ker(\varphi) = N$. Então ψ é um isomorfismo de A-módulos entre o quociente M/N e a imagem do homomorfismo φ.*

Definição 2.7. Dizemos que β é um conjunto de geradores de M, ou simplesmente, que β gera M se qualquer elemento $v \in M$ pode ser escrito como combinação linear finita (em geral, não única) de elementos de β, isto é, existem $a_i, \ldots, a_{i+j} \in A$ e $v_i, \ldots, v_{i+j} \in \beta$ tais que

$$v = a_i v_i + \cdots + a_{i+j} v_{i+j}.$$

Um A-módulos M é dito *finitamente gerado* se existe um conjunto finito de elementos que gera M.

Definição 2.8. Seja M um A-módulo. Um conjunto $\beta \subseteq M$ é linearmente independente se, para todo subconjunto $\{v_i, \ldots, v_{i+j}\}$ finito de β, sempre que

$$a_i v_i + \cdots + a_{i+j} v_{i+j} = 0,$$

implica $a_i = \ldots = a_{i+j} = 0$.

Definição 2.9. Um conjunto β de elementos de um A-módulos M que é linearmente independente e gera M é dito ser uma base de M.

Example 2.5. O conjunto $\beta = \{(1,0),(0,1)\}$ é uma base do $\mathbb{Z}$-módulo $\mathbb{Z} \times \mathbb{Z}$.

Definição 2.10. Um A-módulo M é dito livre se ele admite uma base. Se o A-módulo livre M é finitamente gerado então o módulo M é isomorfo a A^n para algum n.

Example 2.6. Todo espaço vetorial não nulo de dimensão finita é um módulo livre.

Em seguida, apresentamos alguns exemplos para mostrar que nem sempre os módulos se comportam como um espaço vetorial.

Example 2.7. Não é verdade que todo subconjunto linearmente independente de um módulo livre possa ser ampliado a uma base. De fato, o $\mathbb{Z}$-módulo $\mathbb{Z}$ é livre e o conjunto $\{2\}$ é linearmente independente. Entretanto, esse conjunto não é e não pode ser ampliado a uma base.

Example 2.8. Não é verdade que todo conjunto de gerador pode ser reduzido a uma base. Novamente, considerando o $\mathbb{Z}$-módulo $\mathbb{Z}$ temos o conjunto gerado por $\{2,3\}$ não pode ser reduzido a uma base.

Teorema 2.2. *Se A é um anel comutativo e M é um A-módulo livre com bases $\{v_1, \ldots, v_n\}$ e $\{w_1, \ldots, w_m\}$ então $m = n$.*

Demonstração: Ver [6], Exercício 3.10.

□

Como consequência do teorema 2.2, definimos o *posto* de um A-módulo livre M, quando A é um anel comutativo, como sendo o número de elementos de uma base de M. A hipótese do anel ser comutativo no teorema 2.2 é necessária, vejamos um exemplo.

Example 2.9. Seja $\mathbb{Z}[X]$ o $\mathbb{Z}$-módulo dos polinômios na indeterminada X com coeficientes inteiros. Considere o anel de endomorfismos $A := \in_{\mathbb{Z}} \mathbb{Z}[X]$. O anel não comutativo A, considerado como um A-módulo, possui duas bases finitas com diferente cardinalidade. De fato, A como um A-módulo é finitamente gerado por apenas um elemento, tendo o endomorfismo identidade como base. Definamos agora $f_1, f_2 \in A$ da seguinte forma: para todo $n \in \mathbb{N}_0$, seja

$$\begin{cases} f_1(X^{2n+1}) = X^n \\ f_1(X^{2n}) = 0 \end{cases} \quad \text{e} \quad \begin{cases} f_2(X^{2n+1}) = 0 \\ f_2(X^{2n}) = X^n. \end{cases}$$

Estendendo linearmente, temos que cada elemento $f \in A$ fica definido pelas suas imagens nos monômios X^n, pois estes elementos formam uma base de $\mathbb{Z}[X]$. Assim, expandimos as aplicações linearmente a todos os elementos de $\mathbb{Z}[X]$. Verifiquemos que $\{f_1, f_2\}$ é uma base de A. Sejam $\alpha_1, \alpha_2 \in A$ e considere $\alpha_1 f_1 + \alpha_2 f_2 \equiv 0$. Então, para todo $n \in \mathbb{N}_0$, temos que

$$\begin{aligned} 0 &= (\alpha_1 f_1 + \alpha_2 f_2)(X^{2n+1}) \\ &= \alpha_1(f_1(X^{2n+1})) + \alpha_2(f_2(X^{2n+1})) \\ &= \alpha_1(X^n). \end{aligned}$$

Assim, $\alpha_1(p) = 0$ para todo $p \in \mathbb{Z}[X]$. Portanto, $\alpha_1 \equiv 0$. Fazendo o mesmo cálculo para cada X^{2n} temos $\alpha_2 \equiv 0$. Logo, $\{f_1, f_2\}$ é linearmente independente. Agora, seja $f \in A$. Consideremos $\beta_1, \beta_2 \in A$ definidos da seguinte maneira: para todo $n \in \mathbb{N}_0$,

$$\begin{cases} \beta_1(X^n) := f(X^{2n+1}) \\ \beta_2(X^n) := f(X^{2n}), \end{cases}$$

e estendemos por linearidade. Temos que, para todo $n \in \mathbb{N}_0$,

$$\begin{aligned}(\beta_1 f_1 + \beta_2 f_2)(X^{2n+1}) &= \beta_1(f_1(X^{2n+1})) + \beta_2(f_2(X^{2n+1})) \\ &= \beta_1(X^n) \\ &= f(X^{2n+1}).\end{aligned}$$

Do mesmo modo, calculando $(\beta_1 f_1 + \beta_2 f_2)(X^{2n})$ vemos que coincide com $f(X^{2n})$. Assim, por linearidade, temos que $f = \beta_1 f_1 + \beta_2 f_2$. Portanto, $\{f_1, f_2\}$ gera A. Logo, $\{f_1, f_2\}$ é uma base de A.

Definição 2.11. Seja A um anel. Um A-módulo M em que todos os seus submódulos são finitamente gerados é chamado Noetheriano.

Considere A um anel Noetheriano e seja M um A-módulo finitamente gerado por $\{v_1, \ldots, v_m\}$. Então, existe um A-homomorfismo sobrejetor $\pi : A^m \to M$ com

$$\pi(x_1, \ldots, x_m) = x_1 v_1 + \cdots + x_m v_m.$$

Como $ker(\pi) = N$ é um submódulo de A^m e portanto, finitamente gerado, sendo $\beta = \{w_1, \ldots, w_n\}$ um conjunto de geradores de N temos um A-homomorfismo sobrejetor $\varphi : A^n \to N$, mas os elementos de β pertencem à A^m, dessa forma obtemos um A-homomorfismo

$$\begin{aligned}\psi : A^n &\to A^m \\ X &\mapsto BX,\end{aligned}$$

onde B é uma $m \times n$ matriz com entradas em A. Note que $ker(\pi) = Im(\psi) = BA^n$ e pelo teorema do isomorfismo 2.1,

$$M \cong A^m / BA^n.$$

Neste caso, dizemos que a matriz B é uma *matriz de apresentação* de M.

Definição 2.12. Seja M um A-módulo finitamente gerado por um conjunto $\beta = \{v_1, \ldots, v_m\}$. Chamamos um elemento $Y = (y_1, \ldots, y_m)^t$ em A^m, tal que $y_1 v_1 + \cdots + y_m v_m = 0$, um vetor relação ou uma relação entre geradores de M.

Definição 2.13. Um conjunto S de relações de M é um conjunto maximal de M se cada relação de M é uma combinação linear de elementos de S com coeficientes em A.

Example 2.10. O $\mathbb{Z}$-módulo que é gerado por três elementos v_1, v_2 e v_3 com o conjunto completo de relações

$$\begin{aligned}3v_1 + 2v_2 + v_3 &= 0 \\ 8v_1 + 4v_2 + 2v_3 &= 0 \\ 7v_1 + 6v_2 + 2v_3 &= 0 \\ 9v_1 + 6v_2 + v_3 &= 0\end{aligned}$$

é apresentado pela matriz

$$B = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix}.$$

Obsdervação 2.2. Note que a quantidade de linhas da matriz de apresentação de um módulo é igual a quantidade de geradores. Uma vez que várias matrizes apresentam o mesmo módulo ou módulos isomorfos, exibiremos, a seguir, algumas regras para manipular uma matriz B sem alterar a classe do isomorfismo do módulo que essa matriz apresenta:

Proposição 2.1. Sejam B uma matriz de apresentação $m \times n$ de um A-módulo M e P, Q matrizes elementares de tamanho adequado conforme o teorema 3.1. As seguintes regras não modificam o módulo em que B apresenta:

- Multiplicar à esquerda de B por Q^{-1}, com Q em $GL_m(A)$;
- Multiplicar à direita de B por P, com P em $GL_n(A)$;
- Exclusão de uma coluna de zeros da matriz B;
- Exclusão da linha i e da coluna j, caso a j-ésima coluna de B seja e_i.

Utilizando essas regras com a matriz de apresentação B do exemplo 2.10, podemos reduzi-la a matriz

$$B = \begin{bmatrix} 4 \end{bmatrix}$$

e isso significa $M \simeq \mathbb{Z}$.

3. Diagonalização de Matrizes com Entradas Inteiras. Seja $B = (b_{ij})$ uma $m \times n$ matriz com entradas b_{ij} nos inteiros. São operações elementares em suas linhas e colunas:

1 Permutação de duas linhas $L_i \leftrightarrow L_j$ (resp. de duas colunas $C^i \leftrightarrow C^j$).

2 Substituição de uma linha (resp. de uma coluna) pela soma desta linha com um múltiplo inteiro de uma outra linha $L_i \leftrightarrow L_i + cL_j, c \in \mathbb{Z}$ (resp. pela soma desta coluna com um múltiplo inteiro de uma outra coluna).

3 Multiplicar uma linha ou coluna por -1.

Vejamos, através de exemplos, que essas operações elementares são obtidas por multiplicação, à direita ou à esquerda, da matriz B por certas matrizes invertíveis.

Example 3.1. Seja $B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}$. Para permutar as colunas 2 e 3 de B fazemos o produto

$$\begin{pmatrix} b_{11} & b_{13} & b_{12} \\ b_{21} & b_{23} & b_{22} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

em que a última matriz desse produto é uma matriz elementar de determinante -1. Se queremos permutar as linhas de B então realizamos o produto

$$\begin{pmatrix} b_{21} & b_{23} & b_{22} \\ b_{11} & b_{13} & b_{12} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}.$$

Por fim, para a substituição de uma coluna pela soma desta coluna com um múltiplo inteiro de uma outra coluna, por exemplo substituir a coluna 3 de B pela soma da coluna 3 mais d vezes a coluna 1 de B fazemos

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} + db_{11} \\ b_{21} & b_{22} & b_{23} + db_{21} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix} \begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Teorema 3.1. *Seja B uma matriz com coeficientes inteiros. Existem produtos Q e P de matrizes elementares, de tamanhos adequados, de modo que $Q^{-1}BP$ é diagonal, digamos*

$$\begin{bmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix} & \\ & 0 \end{bmatrix}, \tag{3.1}$$

onde as entradas da diagonal d_i são positivas, e $d_i \mid d_{i+1}$ para cada $i = 1, \ldots, k-1$.

Demonstração: Se $B = 0$, não temos nada a fazer. Suponhamos que B seja não nula. Por meio de permutações de linhas e colunas, podemos considerar uma entrada não nula e positiva na posição b_{11}. Em seguida, vamos zerar a primeira linha e a primeira coluna de B. Se a primeira coluna contém uma entrada b_{i1} não nula $i > 1$, aplicando o algoritmo da divisão, existem únicos q_i e r_i inteiros tais que

$$b_{i1} = b_{11}q_i + r_i,$$

com $0 \leq r_i < b_{11}$. Depois, substituímos a i-ésima linha L_i de B por $L_i - q_iL_1$ e mudamos b_{i1} para r_i. Se $r_i = 0$, então produzimos um 0 na primeira coluna. Se $r_i \neq 0$, repetimos o processo acima.

Depois de um número finito de operações elementares nas linhas dessa matriz, obtemos uma matriz equivalente a B com $b_{i1} = 0$ para todo $i > 1$. Analogamente, usando as operações elementares nas colunas, conseguimos $b_{1j} = 0$ para todo $j > 1$. Assim, obtemos uma matriz equivalente a matriz original B que é da forma

$$\begin{bmatrix} d_1' & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathcal{M}_1 & \\ 0 & & & \end{bmatrix} = B_1.$$

Agora, suponhamos que alguma entrada b de $\mathcal{M}_1$, situada na posição ij da matriz B_1 não é divisível por d_1'. Então, substituímos a primeira coluna C^1 de B_1 por $C^1 + C^j$ produzindo uma entrada b na primeira coluna de B_1. Com isso, repetimos todo o processo acima e ao final temos uma matriz equivalente a matriz B_1 da forma

$$\begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \mathcal{M}_2 & \\ 0 & 0 & & \end{bmatrix},$$

onde $d_1 \mid d_2$ e d_2 divide todas as entradas de $\mathcal{M}_2$. Então, aplicaremos todo o processo na matriz $\mathcal{M}_2$. Procedendo dessa forma chegamos a uma matriz da forma (3.1) como afirma o teorema. □

Example 3.2. Seja $B = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 6 \end{bmatrix}$. Determinemos as matrizes B', Q^{-1} e P, tal que $B' = Q^{-1}BP$, onde Q e P são invertíveis. Realizando operações elementares nas linhas e colunas de B

$$\begin{bmatrix} 1 & 0 \\ -4 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & -2 & -6 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & -2 & -6 \end{bmatrix}\begin{bmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & -6 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & -6 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 6 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 6 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} = B'.$$

Portanto

$$B' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 4 & -1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 6 \end{bmatrix}\begin{bmatrix} 1 & -2 & 3 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} = Q^{-1}BP.$$

Observe que, para obter a matriz Q^{-1} basta multiplicar na ordem inversa as matrizes elementares que produzem as operações em linhas. Já para obter a matriz P, basta multiplicar as matrizes elementares na ordem em que suas respectivas as operações em colunas são feitas.

Corolario 3.1. *Seja $\varphi : M \to M'$ um homomorfismo de grupos abelianos livres. Existem bases de M e M' de tal modo que a matriz do homomorfismo tem a forma diagonal do teorema 3.1.*

Teorema 3.2. *Seja M um grupo abeliano livre de posto m, e seja N um subgrupo de M. Então N é um grupo abeliano livre e seu posto é menor do que ou igual a m.*

Demonstração: Sendo M um $\mathbb{Z}$-módulo finitamente gerado tem-se N é finitamente gerado e podemos considerar $\beta' = \{u_1, \ldots, u_n\}$ um conjunto de geradores de N. Sejam $\beta = \{w_1, \ldots, w_m\}$ uma base de M e $i : N \hookrightarrow M$ um homomorfismo inclusão. Escrevemos

$$u_j = b_{1j}w_1 + \cdots + b_{mj}w_m$$

e consideramos a matriz $B = (b_{ij})_{m\times n}$. Pelo Teorema 3.1, existe uma matriz $B' = Q^{-1}BP$ diagonal da forma

$$\begin{bmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix} & \\ & 0 \end{bmatrix},$$

onde $d_1 \mid d_2 \mid \cdots \mid d_k$. Além disso, podemos interpretar P como sendo a matriz de mudança de base de $\mathbb{Z}^n$ e Q é a matriz de mudança de base de $\mathbb{Z}^m$. Como β e β' foram considerados arbitrários, podemos considerar uma base β_1 de M e um conjunto de geradores β_1' de N de modo que temos $B' = Q^{-1}BP$. Assim, $u_j = d_j w_j$, para $1 \leq j \leq k$.

No entanto, a matriz B pode conter alguma coluna nula, a qual corresponde a um gerador u_j cujo vetor de coordenadas na base β é o vetor nulo e portanto $u_j = 0$. Assim, podemos descartá-lo de β'. Fazendo isso para todas as colunas nulas de B temos que a quantidade de geradores de N, que por abuso de notação vamos chamar de n, é k e $n \leq m$. Agora, mostremos que o conjunto $\beta' = \{u_1, \ldots, u_n\}$ é uma base de N. Como β' gera N, basta mostrar que β' é linearmente independente. Sejam $b_1, \ldots, b_n \in \mathbb{Z}$ tais que

$$b_1 u_1 + \cdots + b_n u_n = 0,$$

ou seja,

$$b_1 d_1 w_1 + \cdots + b_n d_n w_n = 0.$$

Visto que $w_1, \ldots, w_n$ são linearmente independentes tem-se $b_j d_j = 0$, para cada $1 \leq j \leq n$. Como $d_j \neq 0$ para todo $1 \leq j \leq n$, concluímos que $b_j = 0$ para $j = 1, \ldots, n$. Logo, β' é linearmente independente e portanto, uma base de N. □

4. Classificação de grupos abelianos finitamente gerados. Desde que um grupo abeliano finitamente gerado M admite uma matriz de apresentação diagonal 3.1, vamos mostrar que M é a soma direta de subgrupos cíclicos e um módulo livre. Vale lembrar que um grupo C é *cíclico* quando é gerado por apenas um elemento.

Teorema 4.1 (Teorema de Estrutura para Grupos Abelianos). *Um grupo abeliano finitamente gerado M é uma soma direta de subgrupos cíclicos $C_{d_1}, \ldots, C_{d_r}$ e um grupo abeliano livre L, ou seja,*

$$M = C_{d_1} \oplus \cdots \oplus C_{d_r} \oplus L,$$

onde a ordem d_i de C_{d_i} é maior que 1 e d_i divide d_{i+1} para $i = 1, \ldots, r-1$.

Demonstração: Seja M um grupo abeliano finitamente gerado por $\beta = \{v_1, \ldots, v_m\}$. Consideramos B uma matriz de apresentação para M determinada pelo conjunto de geradores β e Y um conjunto completo de relações de M. Pelo teorema 3.1, a matriz B apresenta o mesmo módulo que a matriz

$$\begin{bmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix} & \\ & 0 \end{bmatrix}_{m \times n},$$

com $d_1 \mid d_2 \mid \cdots \mid d_k$.

Vamos eliminar qualquer linha i e coluna j cuja entrada da diagonal seja igual a 1 pois nesse caso temos a relação $v_i = 0$ que não contribui no conjunto dos geradores. Além disso, eliminamos qualquer coluna de zeros pois não impõe relação. Assim, depois de reordenar os d_i's, a matria B tem a forma

$$B = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_r \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix}_{m \times r},$$

onde $d_1 > 1$ e $d_1 \mid d_2 \mid \cdots \mid d_r$, com $r \leq k \leq m$. Como isso,

$$d_1 v_1 = 0, \ldots d_r v_r = 0,$$

formando um conjunto completo de relações de M. Agora, seja C_j o subgrupo cíclico gerado por v_j, para $1 \leq j \leq m$. Então, C_j é cíclico de ordem d_j se $j \leq r$ e C_j é cíclico infinito se $j > r$.

Mostremos que M é a soma direta destes grupos cíclicos. Como β gera M, temos que $M = C_1 + \cdots + C_m$. Basta mostrar que $w_1 + ... + w_m = 0$ implica $w_j = 0$, para w_j em C_j. De fato, considere a equação $w_1 + \cdots + w_m = 0$, com w_j em C_j. Uma vez que v_j gera C_j segue que $w_j = y_j v_j$, para algum inteiro y_j. Assim, $Y = (y_1, \ldots, y_m)^t$ é uma relação de M. Visto que as colunas de B formam um conjunto completo de relações de M, $Y = BX$ para algum vetor X. Isto significa que y_j é um múltiplo de d_j, se $j \leq r$ e $y_j = 0$, se $j > r$. Como $d_j v_j = 0$ se $j \leq r$, temos que $w_j = 0$ se $j \leq r$. Portanto, $w_j = 0$ para $1 \leq j \leq m$. Logo,

$$M = C_{d_1} \oplus \cdots \oplus C_{d_r} \oplus L,$$

onde o grupo abeliano livre L é a soma direta dos grupos cíclicos infinitos C_j, com $j > r$. □

Example 4.1. Seja M um grupo abeliano finitamente gerado por v_1, v_2 e v_3, com conjunto completo de relações

$$\begin{aligned} 2v_1 + 2v_2 + 2v_3 &= 0 \\ 2v_1 + 2v_2 &= 0 \\ 2v_1 + 2v_3 &= 0. \end{aligned}$$

A 3×3 matriz de apresentação de M é dada por

$$B = \begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{bmatrix}.$$

Diagonalizando B, obtemos

$$B \sim \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Portanto, $M \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Example 4.2. Considere M um grupo abeliano finitamente gerado por v_1, v_2 e v_3, com as relações

$$\begin{aligned} 7v_1 + 5v_2 + 2v_3 &= 0 \\ 3v_1 + 3v_2 &= 0 \\ 13v_1 + 11v_2 + 2v_3 &= 0. \end{aligned}$$

Vamos escrever M como soma direta de grupos cíclicos. Temos a matriz de apresentação do $\mathbb{Z}$-módulo M

$$B = \begin{bmatrix} 7 & 3 & 13 \\ 5 & 3 & 11 \\ 2 & 0 & 2 \end{bmatrix}.$$

Ao diagonalizar B, obtemos $B \sim \begin{bmatrix} 6 \\ 0 \end{bmatrix}$ e portanto, $M \simeq \mathbb{Z}_6 \oplus \mathbb{Z}$. Com o objetivo de mostrar a unicidade do teorema de estrutura 4.1 vamos enunciar o seguinte resultado cuja demonstração pode ser encontrada em [1, proposição 2.11.3].

Proposição 4.1. *Se a e b são inteiros relativamente primos, então o grupo cíclico C_{ab} é isomorfo a soma direta $C_a \oplus C_b$.*

Demonstração:
Combinando o teorema 4.1 com a proposição 4.1. □

Corolario 4.1 (Forma Alternativa do Teorema de Estrutura). *Todo grupo abeliano finito é uma soma direta de grupos cíclicos de ordem potência de um primo, ou seja,*

$$M \simeq C_{p_1^{u_{11}}} \oplus \cdots \oplus C_{p_s^{u_{1s}}} \oplus \cdots \oplus C_{p_1^{u_{r1}}} \oplus \cdots \oplus C_{p_s^{u_{rs}}},$$

onde $u_{1j} \leq u_{2j} \leq \cdots \leq u_{rj}$ e $1 \leq j \leq s$.

Teorema 4.2 (Unicidade do Teorema de Estrutura). *Se um grupo abeliano finito M é uma soma direta de subgrupos cíclicos de ordens potência de um primo $p_j^{r_{ij}}$, com $1 \leq i \leq r$ e $1 \leq j \leq s$, então os inteiros d_j do teorema 4.1 são unicamente determinados pelo grupo M.*

Demonstração: Sejam $p_1, \ldots, p_s$ os primos distintos na decomposição de M. Vamos listar todas as potências de um primo que aparecem na decomposição de M da seguinte maneira:

$$\begin{matrix} p_1^{u_{11}} & p_2^{u_{12}} & \cdots & p_s^{u_{1s}} \\ p_1^{u_{21}} & p_2^{u_{22}} & \cdots & p_s^{u_{2s}} \\ \vdots & \vdots & & \vdots \\ p_1^{u_{r1}} & p_2^{u_{r2}} & \cdots & p_s^{u_{rs}} \end{matrix},$$

onde r é o número de ocorrência dos primos que aparecem mais vezes e $u_{1j} \leq u_{2j} \leq \cdots \leq u_{rj}$, $1 \leq j \leq s$. Eventualmente, alguns dos u_{ij} terão que ser nulos. Seja d_i o produto das potências de um primo na linha i, ou seja,

$$d_i = p_1^{u_{i1}} \cdot p_2^{u_{i2}} \ldots p_s^{u_{is}},$$

onde $1 \leq i \leq r$. É claro que $d_1 \mid d_2 \mid \cdots \mid d_r$. Como as potências de um primo que aparecem em cada d_i são primas entre si, pela proposição 4.1 podemos concluir

$$C_{d_i} = C_{p_1^{u_{i1}}} \oplus C_{p_2^{u_{i2}}} \oplus \cdots \oplus C_{p_s^{u_{is}}}.$$

Daí, segue que

$$M \simeq C_{p_1^{u_{11}}} \oplus \cdots \oplus C_{p_s^{u_{1s}}} \oplus \cdots \oplus C_{p_1^{u_{r1}}} \oplus \cdots \oplus C_{p_s^{u_{rs}}} \simeq C_{d_1} \oplus \cdots \oplus C_{d_r}.$$

Resumindo, dado uma lista dos $p_j^{u_{ij}}$ vemos que cada d_i fica determinado,a menos de associados. Reciprocamente, dado uma lista dos $d_i, i = 1 \ldots, r$, os $p_j^{u_{ij}}$ são as potências de um primo que aparece na decomposição do respectivo d_i. Logo, os d_i são unicamente determinados por M. □

Example 4.3. Seja o grupo abeliano finito $G = \mathbb{Z}_{20} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{108}$. Pelo corolário 4.1, G é uma soma direta de subgrupos cíclicos de ordens potência de um primo, ou seja,

$$G = \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{2^3} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^3}.$$

Assim, as potências de um primo que aparecem na decomposição de G são 2^2, 5, 2^3, 5, 2^2 e 3^3 e dispõem-se de acordo com a seguinte tabela:

$$\begin{matrix} 2^2 & 3^0 & 5^0 \\ 2^2 & 3^0 & 5 \\ 2^3 & 3^3 & 5 \end{matrix}.$$

Portanto,

$$\begin{aligned} d_1 &= 2^2 = 4 \\ d_2 &= 2^2 \cdot 5 = 20 \\ d_3 &= 2^3 \cdot 3^3 \cdot 5 = 1080. \end{aligned}$$

Logo, $G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{1080}$.

Example 4.4. Vamos encontrar explicitamente todos os grupos abelianos (a menos de isomorfismo) de ordem $400 = 2^4 \cdot 5^2$. Existem exatamente 5 grupos abelianos de ordem 2^4, são eles

$$\mathbb{Z}_{2^4}, \mathbb{Z}_2 \oplus \mathbb{Z}_{2^3}, \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2}, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \text{ e } \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

e existem exatamente 2 grupos abelianos de ordem 5^2, a saber $\mathbb{Z}_{5^2}$ e $\mathbb{Z}_5 \oplus \mathbb{Z}_5$. Então, os grupos abelianos de ordem 400 são

$$\begin{aligned}
G_1 &= \mathbb{Z}_{2^4} \oplus \mathbb{Z}_{5^2} \simeq \mathbb{Z}_{400},\\
G_2 &= \mathbb{Z}_{2^4} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_5 \oplus \mathbb{Z}_{80},\\
G_3 &= \mathbb{Z}_2 \oplus \mathbb{Z}_{2^3} \oplus z_{5^2} \simeq z_2 \oplus \mathbb{Z}_{200},\\
G_4 &= \mathbb{Z}_2 \oplus \mathbb{Z}_{2^3} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_{10} \oplus \mathbb{Z}_{40},\\
G_5 &= \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{5^2} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_{100},\\
G_6 &= \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_{20} \oplus \mathbb{Z}_{20},\\
G_7 &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{5^2} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{100},\\
G_8 &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{20},\\
G_9 &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{5^2} \simeq \mathbb{Z}_2 \oplus z_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{50},\\
G_{10} &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{10}.
\end{aligned}$$

5. Aplicação a operadores lineares. Podemos fazer uma classificação análoga a de grupos abelianos para o anel de polinômios em uma variável $A = K[t]$, sobre um corpo K. Lembremos que o principal argumento usado na demonstração do teorema 3.1 para a diagonalização de matrizes com coeficientes inteiros foi o algoritmo da divisão e como A é um anel Euclidiano temos uma versão do algoritmo da divisão [4, section 3.7] . Por outro lado, segue do teorema da base de Hilbert [1] que A é um anel Noetheriano, e assim todo A-módulo V é finitamente gerado e tem uma matriz de apresentação. Reescrevemos o teorema 3.1 para uma matriz com entradas em A como segue.

Teorema 5.1. *Sejam $A = K[t]$ o anel de polinômios na variável t sobre um corpo K e B uma A-matriz de tamanho $m \times n$. Existem matrizes P e Q, produto de A-matrizes elementares, tal que $B' = Q^{-1}BP$ é diagonal, sendo que cada entrada não nula da diagonal d_i de B' é um polinômio mônico, e ainda $d_1|d_2 \ldots |d_k$.*

Example 5.1.

$$B = \begin{bmatrix} t^2-3t+1 & t-2 \\ (t-1)^3 & t^2-3t+2 \end{bmatrix} \overset{linha}{\to} \begin{bmatrix} t^2-3t+1 & t-2 \\ t^2-t & 0 \end{bmatrix} \overset{col}{\to}$$

$$\overset{col}{\to} \begin{bmatrix} -1 & t-2 \\ t^2-t & 0 \end{bmatrix} \overset{col}{\to} \begin{bmatrix} -1 & 0 \\ t^2-t & t^3-3t^2+2t \end{bmatrix} \overset{linha}{\to} \begin{bmatrix} 1 & 0 \\ 0 & t^3-3t^2+2t \end{bmatrix} := B'$$

Assim como feito para $\mathbb{Z}$-módulos, vamos considerar um A-modulo cíclico C, digamos que seja gerado por $v \in A$. Dessa forma, existe um homomorfismo sobrejetor $\varphi : A \longrightarrow C$ tal que $r \mapsto rv$, onde o núcleo $I = ker(\varphi)$ é um ideal principal de A e pelo teorema do isomorfismo $C \simeq A/(d)$, para algum polinômio $d \in A$. Isso significa que o módulo de relações é gerado por um único elemento.

Teorema 5.2. *Seja $A = K[t]$ o anel de polinômios em uma variável sobre o corpo K. Seja V um A-módulo finitamente gerado. Então o A-módulo V é uma soma direta de módulos cíclicos $C_1, \ldots, C_k$ com um A-módulo livre L, onde C_i é isomorfo a $A/(d_i)$, os elementos d_i são polinômios mônicos de grau positivo com $d_1|d_2 \ldots |d_k$.*

Voltando ao exemplo 5.1, com $A = \mathbb{Q}[t]$, o A-módulo V apresentado pela matriz B é isomorfo ao módulo apresentado pela matriz B' que segundo a propriedade (2.1) obtemos $V \simeq A/(f)$. Mas como os fatores $t, t-1, t-2$ são polinômios irredutíveis sobre $\mathbb{Q}$ os mesmos são relativamente primos e então

$$V \simeq A/(t) \oplus A/(t-1) \oplus A/(t-2).$$

Agora vamos ao objetivo desta seção que é aplicar esse conceito a operadores lineares. Dado um operador linear $T : V \longrightarrow V$ em um espaço vetorial V sobre um corpo K podemos definir nesse espaço vetorial V uma estrutura de A-módulo por

$$\begin{aligned}
\cdot : \quad A \times V &\longrightarrow V \\
(f(t), v) &\longmapsto f(t) \cdot v,
\end{aligned}$$

em que dado $f(t) = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in A$ consideramos

$$f(t) \cdot v := [f(T)]v = a_n T^n(v) + a_{n-1}T^{n-1}(v) + \ldots + a_1 T(v) + a_0 v.$$

Com essa notação tem-se $t \cdot v = T(v)$ e $(V, \cdot)$ é um A-módulo. Reciprocamente,

Proposição 5.1. *Seja $A = K[t]$ o anel de polinômios em uma variável sobre um corpo K. Se V é um A-módulo, então temos um operador linear $T : V \longrightarrow V$, sendo agora V um K-espaço vetorial.*

Demonstração: Desde que V é um A-módulo, podemos definir a multiplicação por polinômios constantes que são os elementos de K, e assim V se torna um espaço vetorial sobre K. Novamente pelo fato de V ser um A-módulo, podemos definir a multiplicação de elementos de V pelo elemento $t \in A$. Vamos denotar essa operação de multiplicação por t em V como sendo T, ou seja,

$$V \xrightarrow{T} V \text{ tal que } T(v) = tv. \tag{5.1}$$

Sendo V um A módulo, em particular vale a distributividade da soma sobre o produto e então $tc(v + v') = ctv + tv'$ o que significa $T(cv + v') = cT(v) + T(v')$, para todo $v, v' \in V, c \in K$. Portanto, a aplicação T é um operador linear sobre o espaço vetorial V. □

Corolario 5.1. *Com as hipóteses da proposição 5.1 as regras que associam a cada $K[t]$-módulo V um operador linear sobre V e vice-versa são operações inversas.*

Se V é um $K[t]$-módulo de dimensão finita n como K-espaço vetorial, então aplicando o teorema 5.2 tem-se uma decomposição de V em soma direta de submódulos cíclicos

$$V = C_1 \oplus \ldots \oplus C_k,$$

onde cada C_i é isomorfo a $K[t]/(f_i)$, f_i polinômio mônico em $K[t]$, e a parte livre é zero desde que V é de dimensão finita. Considerando β_i uma base de $C_i, i = 1, \ldots, k$, temos que $\beta = (\beta_1, \ldots, \beta_k)$ é uma base de V sendo que cada espaço C_i é invariante por T o que significa a matriz de T ser diagonal em blocos assim como acontece para um espaço vetorial.

Vamos escolher um dos módulos C_i e para um melhor entendimento omitimos o índice. Seja v o gerador do modulo C. Como $K[t]$ é um domínio de ideais principais já vimos que C é isomorfo a $K[t]/(f)$ para algum $f(t) = t^m + a_{m-1}t^{m-1} + \ldots + a_1 t + a_0 \in K[t]$ mônico de grau m. Mais precisamente, temos o isomorfismo $K[t]/(f) \longrightarrow C$ dado por $1 \mapsto v$. Pelo algoritmo da divisão,

$$K[t]/(f) = \{b_{m-1}t^{m-1} + \ldots + b_1 t + b_0 | b_i \in K\},$$

e portanto o conjunto $\{1, t, \ldots, t^{m-1}\}$ é uma base de $K[t]/(f)$ como $K[t]$-módulo, consequentemente o conjunto $\beta = \{v, tv, \ldots, t^{m-1}v_0\}$ é uma base de V como K-espaço vetorial. Considerando T o operador multiplicação por t definido em (5.1), ao escrevermos os vetores da base β da forma $(v_0, v_1, \ldots, v_{n-1})$, onde $v_i = T^i(v_0)$, temos

$$T(v_0) = v_1, T(v_1) = T^2(v_0) = v_2, \ldots, T(v_{n-2}) = T^{n-1}(v_0) = v_{n-1},$$

Mas como

$$\begin{aligned}[f(T)](v_0) &= T^n(v_0) + a_{n-1}T^{n-1}(v_0) + \ldots + a_1 T(v_0) + a_0 v_0 \\ &= T(v_{n-1}) + a_{n-1}v_{n-1} + \ldots + a_1 v_1 + a_0 v_0 = 0\end{aligned}$$

segue que

$$T(v_{n-1}) = -a_{n-1}v_{n-1} - \ldots - a_1 v_1 - a_0 v_0.$$

Dessa forma, vamos ter a matriz de T na base β

$$[T]_\beta = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix},$$

cujo polinômio característico é $f(t)$. Esse argumento é suficiente para demonstrar o seguinte resultado.

Teorema 5.3. *Seja T um operador linear em um espaço vetorial de dimensão finita V sobre um corpo K. Existe uma base para V tal que a matriz de T é composta de blocos do tipo descrito acima.*

Essa matriz é chamada de *forma canônica racional* do operador T.

Example 5.2. Seja $K = \mathbb{R}$. Considere a matriz B na forma racional

$$B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

que tem como polinômio característico $f(t) = t^3 - 1 = (t-1)(t^2+t+1)$. Desde que $(t-1)$ e t^2+t+1 são polinômios irredutíveis sobre K, o $K[t]$-módulo cíclico V que B representa é uma soma direta de módulos cíclicos, que mediante a consideração acima sua matriz de apresentação em blocos é dada por

$$B' = \left[\begin{array}{c|cc} 1 & & \\ \hline & 0 & -1 \\ & 1 & -1 \end{array}\right].$$

Sobre o corpo dos números complexos o polinômio $t^2 + t + 1$ é redutível com fatores irredutíveis $t - \omega, t - \omega^2$, onde $\omega = e^{\frac{2\pi i}{3}}$ e a matriz de apresentação do módulo V é diagonalizável, mais precisamente,

$$B'' = \begin{bmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{bmatrix}.$$

ORCID and License
Elisângela Valéria de Jesus https://orcid.org/0000-0002-7987-8240
Aislan Leal Fontes https://orcid.org/0000-0002-6701-8286
Carlos Mejía Alemán https://orcid.org/0000-0002-5081-9175

Referências

[1] Artin M. Algebra. 2ª ed., Pearson Prentice Hall: New Jersey; 1991.
[2] Freitas PJ, Galvão ML. Dimensão de Módulos Livres sobre Anéis Comutativos. Boletim da SPM 68[Internet]. 2013.[Acesso em: 15 novembro de 2016]. Disponível em: http://revistas.rcaap.pt/boletimspm/article/download/3831/2895.
[3] Garcia A, Lequain Y. Elementos de Álgebra. 4ª ed. IMPA, Projeto Euclides: Rio de Janeiro; 2006.
[4] Herstein IN. Topics in Algebra. 2da ed. John Wiley & Sons: New York; 1975.
[5] Jacobson N. Basic Algebra, vol.1, W.H. Freeman and Company: New York; 1910.
[6] Picardo J. Álgebra Comutativa [Internet]. Universidade de Coimbra; 2013 [Acesso em: 11 de outubro de 2016]. Disponível em http://www.mat.uc.pt/~picado/algcom/apontamentos/TextosApoio.pdf.