Universidade Federal de Sergipe
Centro de Ciências Exatas e Tecnologia
Departamento de Matemática
Graduação em Matemática

Sizígias de Um Módulo

São Cristóvão - SE
Setembro de 2025

IGOR DE SANTANA LOPES

Sizígias de Um Módulo

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade Federal de Sergipe para obtenção do título de Licenciado em matemática.

Orientador: Prof. Dr. Zaqueu Alves Ramos

Universidade Federal de Sergipe
Setembro, 2025

Sizígias de Um Módulo

Por

IGOR DE SANTANA LOPES

Área de Conhecimento: Ciências Exatas e da Terra
Subárea de Conhecimento: Matemática
Especialidade de Conhecimento: Álgebra Comutativa

Banca Examinadora:

Prof. Dr. Zaqueu Alves Ramos
(Orientador: UFS)

Prof. Dr. Diego Alves da Costa
(1º Examinador: IFS)

Prof. Me. Samuel Brito Silva
(2º Examinador: UFS)

Dedico este trabalho a Deus, ao meu pai e ao meu orientador.

Agradecimentos

Agradeço primeiramente a Deus, pela vida, pela saúde e pela força que me sustentaram em todos os momentos da minha vida.

Ao meu pai, Pedro, que não está aqui em presença física, mas que vive eternamente em minha memória e em meu coração. Pai, o senhor é e sempre será minha maior referência de ser humano. Sou grato por todos os momentos que tivemos juntos. Espero por este momento desde aquele dia em que estávamos fechando um bag de latinhas, com o sol a pino, e o senhor me disse exatamente estas palavras: “Meu filho, quando você se formar, lembre que um dia você já amarrou um bag de latinha com seu pai.” Hoje, escrevo isso sentindo como se meu peito fosse esmagado pela saudade, mas também aquecido pela honra de ter sido seu filho. Esta conquista é também sua, e sei que, de onde estiver, o senhor sorri orgulhoso. Sempre te amarei, meu pai.

À minha mãe, Gilvanda, por todo o amor, apoio e ensinamentos que me guiaram até aqui. Sou grato por tudo que a senhora enfrentou e suportou para que eu pudesse chegar a este momento.

À minha noiva, Ingrid, que esteve ao meu lado em cada passo desta jornada, oferecendo amor, paciência e apoio incondicional. Sua presença foi um porto seguro nos dias difíceis e uma luz que iluminou minha jornada até aqui.

Aos meus irmãos, Juliandersson, Alisson, Elaine, Alessandro e Pablo, por fazerem parte da minha vida e da minha história, compartilhando momentos e me incentivando, direta ou indiretamente, a chegar até aqui.

À minha vó-sogra Dona Marta, à minha sogra Rose e minha cunhada Iris, pelo carinho, apoio e acolhimento que recebi, tornando essa caminhada mais leve e especial.

Ao meu orientador, Prof. Dr. Zaqueu Ramos, pela paciência, confiança e por todo o conhecimento compartilhado ao longo deste processo. Sua orientação foi fundamental para o desenvolvimento deste trabalho e para o meu crescimento acadêmico e pessoal.

Aos meus amigos Adiclarque, Alisson, Camille, Carlos, Daniele, David, Ellen, Enoque, Girlaine, Jamilly e Saulo. Uma jornada como esta não se faz sozinho e eu tive a sorte de contar com amigos incríveis. Minha gratidão por me apoiar em nos momentos mais desafiadores, oferecendo não apenas palavras de encorajamento, mas também as risadas e a leveza que tornaram o caminho mais agradável.

Aos professores do curso, que contribuíram com palavras de incentivo, debates enriquecedores e momentos de aprendizado compartilhados, em especial à Profª. Dra. Denize Souza, que sutilmente, mudou minha visão como é ser professor.

À banca examinadora, Prof. Dr. Diego Costa e Prof. Me. Samuel Silva, por aceitarem o convite para compor a banca e pelas valiosas contribuições na avaliação deste trabalho.

Por fim, a todos que, de alguma forma, participaram desta etapa da minha vida, minha sincera gratidão.

A busca pelo conhecimento pode ser resumida pela célebre frase: "O que sabemos é uma gota; o que ignoramos é um oceano"(Isaac Newton).

Resumo

Este trabalho tem por objetivo analisar as *sizígias* de um módulo sobre um anel comutativo, enfatizando a estrutura e as propriedades do *módulo de sizígias*. Partindo da definição e caracterização das relações lineares não triviais entre geradores, demonstra-se como essas estruturas permitem mensurar o afastamento de um módulo em relação à condição de ser livre. A pesquisa contempla o estudo de propriedades e comportamentos das sizígias, bem como suas implicações para a compreensão das estruturas modulares no contexto da álgebra comutativa. São apresentados exemplos que ilustram e fundamentam os resultados teóricos, de modo a oferecer uma abordagem clara sobre o tema.

Palavras-chave: Módulo livre; Sizígia; Resolução Livre.

Abstract

This work aims to analyze the *syzygies* of a module over a commutative ring, emphasizing the structure and properties of the *syzygies module*. Starting from the definition and characterization of nontrivial linear relations between generators, we demonstrate how these structures allow us to measure the distance of a module from the condition of being free. The research includes the study of the properties and behavior of syzygies, as well as their implications for understanding modular structures in the context of commutative algebra. Examples are presented to illustrate and substantiate the theoretical results, thus providing a clear approach to the topic.

Keywords: Free module; Syzygy; Free Resolution.

Conteúdo

Introdução

Uma generalização natural do conceito de espaço vetorial é a de *módulo*. Enquanto, em um espaço vetorial, os escalares são elementos de um corpo; na definição de módulo, supomos apenas que os escalares pertencem a um anel comutativo com identidade. Essa flexibilização na escolha do anel de escalares abre caminho para possibilidades teóricas mais amplas, porém, também mais complexas e desafiadoras.

Parte substancial dessa complexidade decorre do fato de que, em muitos módulos, qualquer conjunto de geradores satisfaz relações lineares não triviais, o que impede a existência de base e, consequentemente, a representação única de seus elementos. Essas relações são denominadas *sizígias* e o conjunto de todas elas constitui o chamado *módulo de sizígias*. De forma intuitiva, pode-se entender esse módulo como uma medida do afastamento em relação à condição de ser livre, isto é, de possuir uma base.

O estudo das sizígias, no entanto, não se encerra em um único passo. O módulo de sizígias, que pode ser finitamente gerado e, portanto, pode possuir suas próprias sizígias e, assim, sucessivamente. Este processo iterativo de análise das relações entre geradores está na base da construção das *resoluções livres*, uma ferramenta central da álgebra comutativa. Uma resolução livre decompõe a estrutura de um módulo complexo em uma sequência exata de módulos livres, que são mais simples de compreender.

O objetivo deste trabalho é, portanto, investigar formalmente o conceito de sizígia no contexto da álgebra comutativa. Para alcançar tal objetivo, o texto foi organizado em quatro capítulos. Os Capítulos 1 e 2 são dedicados as preliminares, seções nas quais revisamos conceitos essenciais da teoria de anéis, como ideais e homomorfismos, que constituem o alicerce para o desenvolvimento subsequente. No Capítulo 3, introduzimos a teoria de módulos, com ênfase nos módulos livres e nos módulos noetherianos, que são importantes para a compreensão das relações entre geradores.

Por último, o Capítulo 4 aborda o tema central deste trabalho. Nele, o conceito de sizígia é formalmente definido, e é ilustrado com exemplos. As sequências exatas são introduzidas como a ferramentas para descrever a relação entre um módulo, seus geradores e suas sizígias, culminando na definição e construção de resoluções livres. Desse modo, este trabalho busca não apenas apresentar uma análise teórica, mas também contribuir para uma compreensão das conexões entre sizígias e outras áreas da matemática, como a geometria algébrica, oferecendo uma base para trabalhos

futuros.

Capítulo 1

Preliminares

Nesta seção, abordaremos a estrutura de anéis e seus subanéis, apresentando conceitos e resultados que servirão de base para o restante do trabalho. O estudo desses objetos é fundamental para a álgebra comutativa, pois grande parte das construções e resultados posteriores, como a teoria de módulos e o cálculo de sizígias, baseia-se nas propriedades dos anéis e de suas subestruturas.

1.1 A estrutura de anel

Definição 1.1.1. Um *anel* é um grupo aditivo R, munido de uma multiplicação

$$R \times R \longrightarrow R, (a, b) \mapsto ab$$

satisfazendo:

$$(ab)c = a(bc),\ \ c(a + b) = ca + cb, (a + b)c = ac + bc \tag{1.1}$$

para todo a, b, c em R.

Dizemos que um anel R é *comutativo* se a multiplicação é comutativa, ou seja,

$$ab = ba \tag{1.2}$$

para cada $a, b \in R$.

Dizemos que um anel R é *anel com identidade* se existe $1 \in R$ tal que

$$1a = a1 = a \tag{1.3}$$

para cada $a \in R$.

Observação 1.1.2. Neste texto, estaremos interessados apenas nos anéis comutativos com identidade. Assim, para efeito de facilitação da escrita, cometeremos o abuso de linguagem de usar

apenas a palavra "anel"para designar um *anel comutativo com identidade.*

Exemplo 1.1.3. Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, tão familiares desde o ensino elementar, são exemplos fundamentais de anéis quando considerados com suas operações usuais de adição e multiplicação.

Exemplo 1.1.4 (Anel de resíduos módulo n)**.** Seja $n \geq 1$ um número inteiro. Dados $a, b \in \mathbb{Z}$, dizemos que a é *congruente* a b módulo n se n divide $a - b$. Pode-se mostrar que esta é uma relação de equivalência em $\mathbb{Z}$. Denotaremos a classe de equivalência de um elemento $a \in \mathbb{Z}$ por $\overline{a}$, ou seja,

$$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}.$$

O conjunto quociente de $\mathbb{Z}$ por essa relação é denotado por $\mathbb{Z}_n = \{\overline{a} \mid a \in \mathbb{Z}\}$. Pode ser deduzido que o conjunto $\mathbb{Z}_n$ é completamente determinado pelas classes dos restos da divisão por n. Em outras palavras,

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Definimos as operações de adição e multiplicação em $\mathbb{Z}_n$ da seguinte maneira:

$$\overline{a} + \overline{b} := \overline{a+b} \quad \text{e} \quad \overline{a} \cdot \overline{b} := \overline{ab}.$$

Essas operações estão bem definidas, ou seja, o resultado não depende da escolha dos representantes a e b, e conferem a $\mathbb{Z}_n$ a estrutura de um *anel*.

O anel $\mathbb{Z}_n$ não apenas ilustra a aplicação de conceitos fundamentais como relações de equivalência e operações sobre classes, mas também serve como uma ponte natural entre a aritmética elementar e a álgebra abstrata. Além disso, devido à sua estrutura finita, $\mathbb{Z}_n$ é um dos exemplos preferidos no estudo de anéis.

Exemplo 1.1.5 (Anel das funções de um conjunto em um anel)**.** Seja X um conjunto não vazio e R um anel. Denotamos o conjunto de todas as funções de X em R por $F(X, R)$. Dados $f, g \in F(X, R)$, definimos as operações de adição e multiplicação ponto a ponto da seguinte maneira:

$$(f+g)(x) := f(x) + g(x) \quad \text{e} \quad (fg)(x) := f(x)g(x).$$

Essas operações estão bem definidas, ou seja, os resultados pertencem novamente a $F(X, R)$ e conferem a $F(X, R)$ estrutura de *anel*. Nesse anel, o elemento neutro da adição é a função nula

$$0(x) := 0 \quad \text{para todo } x \in X,$$

enquanto a identidade multiplicativa é a função constante

$$1(x) := 1 \quad \text{para todo } x \in X.$$

Exemplo 1.1.6. Seja R um anel. Um polinômio em n variáveis $x_1, \ldots, x_n$ com coeficientes em R é uma soma

$$f = \sum_{\underline{\alpha} \in \mathbb{N}^n} a_{\underline{\alpha}} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

onde os $a_{\underline{\alpha}}$ pertencem a R e são distintos de zero apenas para uma quantidade finita de índices $\underline{\alpha}$. Dizemos que dois polinômios

$$f = \sum_{\underline{\alpha} \in \mathbb{N}^n} a_{\underline{\alpha}} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \quad \text{e} \quad g = \sum_{\underline{\alpha} \in \mathbb{N}^n} b_{\underline{\alpha}} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

são iguais se $a_{\underline{\alpha}} = b_{\underline{\alpha}}$ para cada $\underline{\alpha} \in \mathbb{N}^n$. Dados dois polinômios

$$f = \sum_{\underline{\alpha} \in \mathbb{N}^n} a_{\underline{\alpha}} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \quad \text{e} \quad g = \sum_{\underline{\alpha} \in \mathbb{N}^n} b_{\underline{\alpha}} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

definimos:

$$f + g = \sum_{\underline{\alpha} \in \mathbb{N}^n} (a_\alpha + b_\alpha) x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

e

$$fg = \sum_{\underline{\gamma} \in \mathbb{N}^n} c_\gamma x_1^{\gamma_1} \cdots x_n^{\gamma_n}, \quad \text{em que} \quad c_\gamma = \sum_{\alpha+\beta=\gamma} a_\alpha b_\beta.$$

É possível verificar que $f + g$ e gf também são polinômios em n variáveis com coeficientes em R. De fato, é possível mostrar que o conjunto de todos os polinômios em n variáveis com coeficientes em R munido das operações acima é um anel, chamado *anel de polinômios* em n variáveis com coeficientes em R. Denotamos este anel por $R[x_1, \ldots, x_n]$. Vale destacar que o zero de $R[x_1, \ldots, x_n]$ é o polinômio tal que todos os coeficientes são iguais a zero e que a identidade de $R[x_1, \ldots, x_n]$ é o polinômio em que o coeficiente da n-upla nula de $\mathbb{N}^n$ é 1 e os demais coeficientes são iguais a zero.

Observação 1.1.7. O conjunto $M_{n\times n}(\mathbb{R})$, formado por todas as matrizes quadradas de ordem n com entradas reais, é um exemplo clássico e bastante familiar de estrutura algébrica. Com as operações usuais de adição e multiplicação de matrizes:

$$A + B = (a_{ij} + b_{ij}) \quad \text{e} \quad AB = \left(\sum_{k=1}^{n} a_{ik} b_{kj} \right),$$

$M_{n\times n}(\mathbb{R})$ constitui um *anel com identidade*. No entanto, para $n \geq 2$, a multiplicação de matrizes não é comutativa, ou seja, em geral $AB \neq BA$. Apesar de sua relevância e do fato de ser um exemplo recorrente desde a educação básica, não estamos interessados nesse tipo de anel neste trabalho, pois restringiremos nossa análise apenas aos anéis comutativos.

Proposição 1.1.8. *Seja R um anel. Então, $R = \{0\}$ se, e somente se, $1 = 0$.*

Demonstração. Suponha que $R = \{0\}$. Como R é anel, então a identidade 1 coincide com 0. Reciprocamente, como R é anel a inclusão $\{0\} \subseteq R$ é óbvia. Considere $a \in R$. Assim,

$$a = a1 = a0 = 0.$$

Portanto, $R \subseteq \{0\}$, e a demonstração se verifica. □

Observação 1.1.9. Daqui em diante, estaremos desconsiderando anéis como o da proposição anterior. Ou seja, sempre que nos referirmos a um anel estará subentendido que $1 \neq 0$.

1.2 Subanéis

Sempre que definimos uma estrutura algébrica, é conveniente também definirmos o conceito de *subestrutura*, ou seja, um subconjunto que, com as operações herdadas, também forma uma estrutura do mesmo tipo. Com base nisso, apresentaremos a seguir a estrutura de *subanel*.

Definição 1.2.1. Seja S um subconjunto de um anel R. Dizemos que S é *subanel* de R se:

(i) $-1, 1 \in S$;

(ii) S é fechado em relação às operações de adição e multiplicação de R.

Observação 1.2.2. A condição (ii) garante que as operações de adição e multiplicação de R permanecem bem definidas em R. Já a condição (i) assegura que S contém os elementos neutros e seus opostos, de modo que, com as operações herdadas de R, o conjunto S também possui estrutura de anel.

Exemplo 1.2.3. Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, que vimos anteriormente formam uma cadeia de inclusões, na qual cada conjunto é subanel do seguinte:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Exemplo 1.2.4. Seja $F(\mathbb{R}, \mathbb{R})$ o conjunto de todas as funções de $\mathbb{R}$ em $\mathbb{R}$, dizemos que uma função $f : \mathbb{R} \to \mathbb{R}$ é *derivável* se existe a sua derivada $f'(x)$ para todo $x \in \mathbb{R}$. Mais geralmente, dizemos que f é de classe C^k, com $k \in \mathbb{N}$, se admite derivadas contínuas até a ordem k. Por fim, uma função é de classe C^∞ se admite derivadas contínuas de todas as ordens.

Essas funções formam subconjuntos importantes de $F(\mathbb{R}, \mathbb{R})$ e que naturalmente possuem estrutura de subanéis, pois são fechados sob as operações de adição e multiplicação ponto a ponto e contêm os elementos -1 e 1. Assim, temos a seguinte cadeia de subanéis:

$$C^\infty(\mathbb{R}, \mathbb{R}) \subset \cdots \subset C^2(\mathbb{R}, \mathbb{R}) \subset C^1(\mathbb{R}, \mathbb{R}) \subset F(\mathbb{R}, \mathbb{R}).$$

Cada conjunto da cadeia representa um subanel do próximo.

Exemplo 1.2.5. O conjunto dos *inteiros Gaussianos* é definido pela seguinte igualdade:

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z},\ i^2 = -1\}.$$

Podemos verificar facilmente que $\mathbb{Z}[i]$ é um subanel de $\mathbb{C}$, munido com as operações usuais de adição e multiplicação de $\mathbb{C}$.

Exemplo 1.2.6. Seja R um anel. Um polinômio

$$f = \sum_{\underline{\alpha} \in \mathbb{N}^n} a_{\underline{\alpha}} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

de $R[x_1, \ldots, x_n]$ é dito *constante* se $a_{\underline{\alpha}} = 0$ para cada n-upla não nula $\underline{\alpha} \in \mathbb{N}^n$. O conjunto de todos os polinômios constantes de $R[x_1, \ldots, x_n]$ é um subanel de $R[x_1, \ldots, x_n]$. Ele se identifica naturalmente com R e é dessa maneira que enxergamos R como subanel de $R[x_1, \ldots, x_n]$.

1.3 Divisores de zero e o conceito de domínio de integridade

Definição 1.3.1. Seja R um anel. Dizemos que um elemento $a \in R$ é *divisor de zero* de R, se existe $b \in A$ não nulo tal que $ab = 0$.

Exemplo 1.3.2. Sejam $f, g \in F(X, R)$ funções definidas pelas seguintes regras:

$$f(x) = \begin{cases} 0, & \text{se } x = 0 \\ 1, & \text{se } x \neq 0 \end{cases} \quad \text{e} \quad g(x) = \begin{cases} 1, & \text{se } x = 0 \\ 0, & \text{se } x \neq 0 \end{cases} \tag{1.4}$$

Observe que ambas as funções são diferentes de zero. Contudo,

$$(fg)(x) = f(x)g(x) = 0 \quad \text{para todo } x \in R.$$

Ou seja, o produto fg é a função nula. Portanto, f e g são *divisores de zero do anel* $F(X, R)$.

Esse exemplo é interessante porque mostra que, mesmo em anéis formados por objetos familiares como funções, podem existir elementos não nulos cujo produto é nulo.

Definição 1.3.3. Dizemos que um anel D é um *domínio de integridade* (ou simplesmente *domínio*) se, dados quaisquer $a, b \in D$, tais que $ab = 0$ então $a = 0$ ou $b = 0$.

Ou seja, um domínio é um anel que não possui divisores de zero não nulo. Essa propriedade garante um comportamento mais próximo do que ocorre nos inteiros $\mathbb{Z}$.

Exemplo 1.3.4. Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ com suas operações usuais de adição e multiplicação são exemplos de domínios.

Proposição 1.3.5. *Se S é subanel de um domínio R então S é domínio.*

Demonstração. Como R é um domínio de integridade, temos que R é um anel comutativo com identidade e não possui divisores de zero.

Agora, seja $S \subseteq R$ um subanel. Então S herda de R a comutatividade e o elemento identidade. Resta verificar que S também não tem divisores de zero.

De fato, se $a, b \in S$ satisfazem $ab = 0$ em S, essa igualdade também vale em R, pois as operações em S são restrições das operações em R. Mas como R é domínio, disso segue que $a = 0$ ou $b = 0$.

Portanto, S não possui divisores de zero e é um domínio de integridade. □

Proposição 1.3.6. *Se R é um domínio então o anel de polinômios $R[x_1, \ldots, x_n]$ é um domínio.*

Demonstração. Ver [3, Proposition 156]. □

1.4 Elementos invertíveis e o conceito de corpo

Definição 1.4.1. Seja R um anel. Dizemos que $a \in R$ é *invertível* em R se existe $b \in R$ tal que $ab = 1$.

Proposição 1.4.2. *O inverso multiplicativo de um elemento invertível é único. Além disso, temos*

$$(a^{-1})^{-1} = a.$$

Demonstração. Suponha que b e c são ambos inversos de a, isto é, $ab = 1$ e $ac = 1$. Queremos mostrar que $b = c$. De fato:

$$b = b \cdot 1 = b \cdot (ac) = (ba) \cdot c = 1 \cdot c = c.$$

Logo, o inverso de a é único. □

Denotaremos o conjunto de todos os elementos invertíveis de R por R^*, também chamado de *conjunto das unidades* de R.

Exemplo 1.4.3. Apresentamos agora alguns exemplos de conjuntos de unidades em anéis bem conhecidos:

1. Em $\mathbb{Z}$, temos $\mathbb{Z}^* = \{-1, 1\}$, pois são os únicos inteiros que possuem inversos também inteiros.

2. No anel dos números racionais, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, já que todo racional não nulo possui inverso racional.

3. De modo análogo, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ e $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, pois os elementos não nulos desses anéis também admitem inversos neles mesmos.

Esses exemplos ilustram como o conjunto das unidades varia conforme a estrutura do anel em questão.

Definição 1.4.4. Um anel R é chamado de *corpo* se todo elemento não nulo de R é invertível em R. Ou seja, um anel R é corpo se, e somente se, $R^* = R\backslash\{0\}$.

Exemplo 1.4.5. Os conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ com suas operações usuais de adição e multiplicação são exemplos de corpos.

Observação 1.4.6. Note que, o anel $\mathbb{Z}$ não é um corpo. De fato, os únicos elementos invertíveis em $\mathbb{Z}$ são -1 e 1, ou seja, $\mathbb{Z}^* = \{-1, 1\}$.

Proposição 1.4.7. *Se R é corpo, então R é domínio.*

Demonstração. Sejam $a, b \in R$ tais que $ab = 0$. Suponha $a \neq 0$. Como R é um corpo, então a admite inverso multiplicativo, isto é, existe $a^{-1} \in R$ tal que $a^{-1}a = 1$. Multiplicando ambos os lados da igualdade $ab = 0$ à esquerda por a^{-1}, obtemos:

$$a^{-1}(ab) = a^{-1} \cdot 0.$$

Pela associatividade da multiplicação, temos:

$$(a^{-1}a)b = 0 \quad \Rightarrow \quad 1 \cdot b = 0.$$

Logo, $b = 0$. Portanto, se $ab = 0$, então $a = 0$ ou $b = 0$, o que mostra que R não possui divisores de zero. Assim, R é um domínio. □

Observação 1.4.8. Note que a recíproca não é verdadeira, embora todo corpo seja um domínio, o contrário nem sempre ocorre, como foi observado em (1.4.6).

1.5 Ideais e o conceito de domínio de ideais principais

Definição 1.5.1. Seja R um anel. Um subconjunto $I \subseteq R$ é chamado de *ideal* de R se satisfaz as seguintes propriedades:

1. $0 \in I$;
2. se $a, b \in I$, então $a + b \in I$;
3. se $a \in R$ e $b \in I$, então $ab \in I$.

Observação 1.5.2. Todo anel R admite ao menos dois ideais: o ideal $\{0\}$ e o próprio anel R. Esses são chamados de *ideais triviais de* R.

Exemplo 1.5.3. Seja $F(\mathbb{R},\mathbb{R})$ o conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$, com operações definidas ponto a ponto. Consideremos o subconjunto

$$I = \{f \in F(\mathbb{R},\mathbb{R}) \mid f(\pi) = 0\}.$$

Mostraremos que I é um ideal de $F(\mathbb{R},\mathbb{R})$.

(i) A função nula pertence a I, pois $0(\pi) = 0$.

(ii) Se $f, g \in I$, então $(f+g)(\pi) = f(\pi) + g(\pi) = 0 + 0 = 0$, logo $f + g \in I$.

(iii) Se $h \in F(\mathbb{R},\mathbb{R})$ e $f \in I$, então $(hf)(\pi) = h(\pi) \cdot f(\pi) = h(\pi) \cdot 0 = 0$, logo $hf \in I$.

Como I satisfaz todas as condições, concluímos que se trata de um ideal de $F(\mathbb{R},\mathbb{R})$.

Exemplo 1.5.4. Seja $S \subseteq R$ um subconjunto não vazio qualquer de um anel R. O *ideal gerado por* S é definido por:

$$(S) = \left\{ \sum_{i=1}^{n} a_i s_i \mid n \in \mathbb{N}, a_i \in R,\ s_i \in S \right\}.$$

Mostraremos que (S) é um ideal de R.

(i) O elemento nulo pertence a (S), pois $0 = \sum 0 \cdot s_i$, no qual s é um elemento qualquer de S (que é não vazio).

(ii) Se $x = \sum a_i s_i$ e $y = \sum b_i s_i$ pertencem a (S), então

$$x + y = \sum a_i s_i + \sum b_i s_i = \sum (a_i + b_i) s_i \in (S).$$

(iii) Se $r \in R$ e $x = \sum a_i s_i \in (S)$, então

$$rx = r \sum a_i s_i = \sum (r a_i) s_i \in (S).$$

Assim, (S) satisfaz as propriedades de ideal.

O ideal do exemplo anterior é chamado de *ideal gerado pelo conjunto* S. Quando S é finito, digamos $S = \{s_1, \ldots, s_n\}$, denotamos o ideal por $(s_1, \ldots, s_n)$ e dizemos que ele é *finitamente gerado*. Em particular, se o ideal é gerado por um único elemento $s \in R$, ou seja, da forma (s), dizemos que se trata de um *ideal principal*.

Definição 1.5.5. Seja R um domínio. Dizemos que R é um *domínio de ideais principais* se todo ideal de R é principal.

Proposição 1.5.6. *O domínio dos números inteiros $\mathbb{Z}$ é um domínio de ideais principais.*

Demonstração. Se $I = \{0\}$, então $I = (0)$ e nada há a provar. Suponha $I \neq \{0\}$. Considere o conjunto $S = \{s \in I \mid s > 0\}$. Como $I \neq \{0\}$, existe algum inteiro não nulo em I e, portanto, $S \neq \emptyset$. Pelo princípio da boa ordem, S possui um menor elemento; denote-o por $n > 0$. Mostraremos que $I = (n)$. Primeiro, como $n \in I$ e I é ideal, para todo $k \in \mathbb{Z}$ temos $kn \in I$, logo $(n) \subseteq I$. Para a inclusão oposta, seja $a \in I$. Fazendo a divisão euclidiana de a por n, existem $q, r \in \mathbb{Z}$ com

$$a = qn + r, \qquad 0 \leq r < n.$$

Como $a, qn \in I$ (pois $n \in I$ e I é ideal), segue que $r = a - qn \in I$. Pela escolha de n como o menor positivo em I, a condição $0 \leq r < n$ implica $r = 0$. Logo $a = qn \in (n)$. □

Proposição 1.5.7. *Um anel de polinômios em uma única variável com coeficientes em um corpo é um domínio de ideais principais.*

Demonstração. Seja k um corpo e considere o anel $k[x]$. Primeiro observamos que $k[x]$ é um domínio de integridade, pois k é corpo e o anel de polinômios sobre um corpo é domínio.

Seja $I \subseteq k[x]$ um ideal. Se $I = \{0\}$ então $I = (0)$ é principal. Suponha $I \neq \{0\}$ e escolha $f \in I$ não nulo com o menor grau entre todos os polinômios não nulos de I (essa escolha é possível; pois, os graus são números inteiros não negativos).

Tomemos um polinômio arbitrário $g \in I$. Pelo algoritmo da divisão em $k[x]$ (que existe porque k é um corpo), existem únicos polinômios $q, r \in k[x]$ tais que

$$g = fq + r \qquad \text{com} \qquad r = 0 \text{ ou } \operatorname{gr}(r) < \operatorname{gr}(f).$$

Como $f, q \in I$ e $g \in I$, segue que $r = g - fq \in I$. Pela minimalidade de $\operatorname{gr}(f)$, a única possibilidade é $r = 0$. Assim $g = -fq$, ou seja, $g \in (f)$.

Portanto $I \subseteq (f)$. A inclusão inversa $(f) \subseteq I$ é óbvia; pois, $f \in I$. Logo $I = (f)$, mostrando que I é principal.

Como I era um ideal arbitrário de $k[x]$, concluímos que todo ideal de $k[x]$ é principal, isto é, $k[x]$ é um domínio de ideais principais. □

1.6 Ideais primos e maximais

Definição 1.6.1. Sejam R um anel e I um ideal de R que está propriamente contido em R.

(a) Dizemos que I é ideal *primo* de R se $ab \in I$, com $a, b \in R$, implicar $a \in I$ ou $b \in I$.

(b) Dizemos que I é ideal *maximal* de R se para cada ideal J de R tal que $I \subset J \subset R$ tivermos $I = J$ ou $J = R$.

Os conceitos de ideal primo e maximal estão relacionados da seguinte maneira

Proposição 1.6.2. *Todo ideal maximal é ideal primo.*

Demonstração. Seja R um anel e seja $I \subset R$ um ideal maximal. Queremos mostrar que I é primo, ou seja, se $a, b \in R$ são tais que $ab \in I$, então $a \in I$ ou $b \in I$. Suponha, que $ab \in I$, mas $a \notin I$. Devemos mostrar que $b \in I$. Consideremos o ideal $J = \{m + ra \mid m \in I, r \in R\}$. Note que $I \subsetneq J$, pois $a \in J$ mas $a \notin I$. Pela maximalidade de I, temos que $J = R$. Assim, $1 \in J$, ou seja, existem $m \in I$ e $r \in R$ tais que:

$$1 = m + ra.$$

Multiplicando ambos os lados por b, temos:

$$b = b \cdot 1 = b(m + ra) = bm + rab.$$

Como I é ideal e $m, ab \in I$ então $bm \in I$ e $rab \in I$. Também do fato de I ser ideal segue que $b = bm + rab \in I$. □

Exemplo 1.6.3. Seja D um domínio. Mostraremos que o ideal $P = \{0\}$ é um ideal primo de D. De fato, seja $a, b \in D$ tais que $ab \in P = \{0\}$, ou seja, $ab = 0$. Como D é um domínio, isso implica que $a = 0$ ou $b = 0$. Portanto, $a \in P$ ou $b \in P$. Logo, $P = \{0\}$ satisfaz a condição da definição de ideal primo, e assim concluímos que $\{0\}$ é um ideal primo de D.

Exemplo 1.6.4. Seja $\mathbb{Z}$ o anel dos inteiros. Consideremos o ideal $(5) = \{5k \mid k \in \mathbb{Z}\}$. Afirmamos que (5) é um ideal maximal de $\mathbb{Z}$. De fato, se J é um ideal de $\mathbb{Z}$ tal que $(5) \subseteq J \subseteq \mathbb{Z}$, então $J = (d)$ para algum divisor d de 5, já que todo ideal de $\mathbb{Z}$ é principal. Como os únicos divisores positivos de 5 são 1 e 5, temos que $J = (5)$ ou $J = (1) = \mathbb{Z}$. Logo, (5) não está contido propriamente em nenhum ideal que não seja o anel inteiro $\mathbb{Z}$, o que mostra que (5) é maximal.

Capítulo 2

Anéis quocientes e homomorfismos de anéis

A partir desta capítulo, passaremos a explorar uma nova perspectiva, a de estabelecer relações entre diferentes anéis. Para isso, introduziremos um conceito fundamental, o de *homomorfismo de anéis*. A ideia central de um homomorfismo é permitir a comparação entre distintas estruturas algébricas, por meio de uma aplicação que preserve as operações de adição e multiplicação e respeitando a identidade do anel.

2.1 Anéis quocientes

Definição 2.1.1. Seja R um anel e $I \subsetneq R$ um ideal de R. Dizemos que dois elementos $a, b \in R$ são *congruentes módulo* I se $a - b \in I$.

Escrevemos $a \equiv b \pmod{I}$ para dizer que a é congruente a b módulo I.

Proposição 2.1.2. *Congruência módulo I define uma relação de equivalência em R.*

Demonstração. Para cada $a \in R$ temos $a - a = 0 \in I$; logo, $a \equiv a \pmod{I}$. Isso nos mostra que congruência é uma relação reflexiva.

Para a simetria, suponha $a, b \in R$ tais que $a \equiv b \pmod{I}$, então $a - b \in I$. Como I é um ideal,$(-1)(a - b) = b - a \in I$. Logo, $b \equiv a \pmod{I}$.

Finalmente, para provar a transitividade, suponha $a, b, c \in R$ tai que $a \equiv b \pmod{I}$ e $b \equiv c \pmod{I}$. Então $a - b \in I$ e $b - c \in I$. Como I é fechado sob adição, segue que: $(a - b) + (b - c) = a - c \in I$. Logo $a \equiv c \pmod{I}$. □

A classe de equivalência de um elemento de R pela relação de congruência módulo I será denotada por $\overline{a}$ ou $(a + I)$. O espaço quociente de R pela relação de congruência módulo I será denotado por R/I.

Definimos operações de adição e multiplicação em R/I da seguinte maneira:

$$\overline{a} + \overline{b} := \overline{a+b} \quad \text{e} \quad \overline{a} \cdot \overline{b} := \overline{ab}.$$

Essas operações estão bem definidas, ou seja, o resultado não dependem da escolha dos representantes das classes. Em outras palavras, se $a \equiv a' \pmod{I}$ e $b \equiv b' \pmod{I}$, então:

$$a + b \equiv a' + b' \pmod{I} \quad \text{e} \quad ab \equiv a'b' \pmod{I},$$

o que garante que $\overline{a+b} = \overline{a'+b'}$ e $\overline{ab} = \overline{a'b'}$.

É possível verificar que o conjunto R/I, com as operações definidas anteriormente, forma um anel. Nesse contexto, valem as seguintes observações:

(i) $\overline{0}$ é o elemento neutro da adição em R/I.

(ii) O inverso aditivo de $\overline{a}$ em R/I é dado por $\overline{-a}$, pois $\overline{a} + \overline{-a} = \overline{a-a} = \overline{0}$;

(iii) A identidade multiplicativa de R/I é o elemento $\overline{1}$, já que $\overline{1} \cdot \overline{a} = \overline{a}$ para todo $a \in R$.

Teorema 2.1.3. *Seja R um anel e I um ideal de R. Então:*

(i) *O anel R/I é domínio se, e somente se, I for um ideal primo;*

(ii) *O anel R/I é corpo se, e somente se, I for um ideal maximal.*

Demonstração. (i) Suponha que I seja um ideal primo de R. Vamos mostrar que R/I é um domínio. Sejam $\overline{a}, \overline{b} \in R/I$ tais que $\overline{a} \cdot \overline{b} = \overline{0}$. Isso significa que $ab \in I$. Como I é primo, temos $a \in I$ ou $b \in I$, ou seja, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Logo, R/I não possui divisores de zero, e portanto é um domínio. Reciprocamente, suponha que R/I é um domínio. Se $ab \in I$, então $\overline{a} \cdot \overline{b} = \overline{0}$, e como não há divisores de zero em R/I, temos $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, isto é, $a \in I$ ou $b \in I$. Portanto, I é um ideal primo.

(ii) Suponha que I seja um ideal maximal. Vamos provar que R/I é um corpo. Seja $\overline{a} \in R/I$ com $\overline{a} \neq \overline{0}$, ou seja, $a \notin I$. Como I é maximal, o ideal gerado por I e a é igual a R. Assim, existem $i \in I$ e $r \in R$ tais que:

$$1 = i + ra.$$

Igualando as classes:

$$\overline{1} = \overline{i + ra} = \overline{i} + \overline{r} \cdot \overline{a} = \overline{0} + \overline{r} \cdot \overline{a} = \overline{r} \cdot \overline{a}.$$

Logo, $\overline{a}$ admite inverso em R/I, e como isso vale para todo elemento não nulo, R/I é um corpo. Reciprocamente, suponha que R/I é um corpo. Suponha, por absurdo, que exista um ideal J de R tal que $I \subsetneq J \subsetneq R$. Seja $a \in J \setminus I$. Então $\overline{a} \neq \overline{0}$, e como R/I é corpo, $\overline{a}$ é invertível. Assim, existe $\overline{r} \in R/I$ tal que $\overline{r} \cdot \overline{a} = \overline{1}$, o que implica que $ra - 1 \in I \subseteq J$. Como $ra \in J$ e J é ideal, então $1 \in J$, e portanto $J = R$, o que contradiz $J \subsetneq R$. Portanto, I é maximal. □

2.2 Homomorfismo de anéis

Definição 2.2.1. Sejam R e S anéis. Uma aplicação $\varphi : R \longrightarrow S$ é chamada de *homomorfismo de anéis* se,

$$\varphi(a+b) = \varphi(a) + \varphi(b) \text{ e } \varphi(ab) = \varphi(a)\varphi(b)$$

para todos $a, b \in R$ e $\varphi(1) = 1$.

Exemplo 2.2.2. Seja R um anel. Temos os seguintes exemplos básicos de homomorfismos:

1. A aplicação identidade $id_R : R \longrightarrow R$ definida por $id_R(a) = a$, para todo $a \in R$, é um homomorfismo de anéis.

2. Seja I um ideal de R. A aplicação $\pi : R \longrightarrow R/I$ definida por $\pi(a) = \overline{a}$ é também um homomorfismo de anéis, chamado de *projeção canônica*.

2.2.1 Núcleo e imagem de um homomorfismo

Seja $\varphi : R \longrightarrow S$ um homomorfismo de anéis. O *núcleo* de φ, denotado por $\mathrm{Ker}(\varphi)$, é o conjunto formado por todos os elementos de R que são enviados em 0 por φ, isto é,

$$\ker(\varphi) = \{\, a \in R \mid \varphi(a) = 0 \,\} \subseteq A.$$

A *imagem* de φ, denotada por $\mathrm{Im}(\varphi)$, é o conjunto de todos os elementos de S que podem ser escritos como $\varphi(a)$ para algum $a \in R$, isto é,

$$\mathrm{Im}(\varphi) = \{\, \varphi(a) \in S \mid a \in R \,\} \subseteq S.$$

O conjunto $\mathrm{Im}\,\varphi$ mede a sobrejetividade do homomorfismo. Mais adiante, veremos que o núcleo $\mathrm{Ker}\,\varphi$ está relacionado à injetividade de φ.

Exemplo 2.2.3. Considere o homomorfismo de anéis $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_k$ definido por:

$$\phi(n) = \overline{n} \text{ (mód } k),$$

isto é, $\phi(n)$ é a classe de equivalência de n módulo k. Temos

$$\mathrm{Im}(\phi) = \{\phi(n) \in \mathbb{Z}_k \mid n \in \mathbb{Z}\} = \mathbb{Z}_k,$$

pois toda classe $\overline{r} \in \mathbb{Z}_k$, com $0 \leq r < k$, possui um representante inteiro. O núcleo de ϕ é dado por

$$\ker(\phi) = \{n \in \mathbb{Z} \mid \phi(n) = \overline{0}\} = \{n \in \mathbb{Z} \mid k \mid n\} = k\mathbb{Z}.$$

Ou seja, o núcleo é o ideal (k) de $\mathbb{Z}$.

Proposição 2.2.4. *Seja $\phi : R \longrightarrow S$ um homomorfismo de anéis. Então:*

(a) $\mathrm{Im}\,\phi$ *é subanel de* S*;*

(b) $\ker \phi$ *é ideal de* R*.*

Demonstração. (a) Vamos verificar que $\mathrm{Im}\,\phi$ satisfaz as condições para ser um subanel de S. Como ϕ é homomorfismo de anéis, temos que $\phi(1) = 1$ e $\phi(0) = \phi(1 + (-1)) = \phi(1) + \phi(-1)$. Mas também, como ϕ é homomorfismo, $\phi(0) = 0$. Logo,

$$0 = \phi(1) + \phi(-1) = 1 + \phi(-1),$$

donde segue que $\phi(-1)$ é o inverso aditivo de 1, isto é, $\phi(-1) = -1$. Logo os elementos 1 e -1 pertencem à imagem de ϕ. Sejam $b_1 = \phi(a_1)$ e $b_2 = \phi(a_2)$, com $a_1, a_2 \in R$. A aplicação ϕ preserva as operações, então:

$$b_1 + b_2 = \phi(a_1) + \phi(a_2) = \phi(a_1 + a_2),$$

$$b_1 \cdot b_2 = \phi(a_1) \cdot \phi(a_2) = \phi(a_1 a_2).$$

Como $a_1 + a_2$ e $a_1 a_2$ pertencem a R, segue que $\phi(a_1 + a_2)$ e $\phi(a_1 a_2)$ pertencem à imagem de ϕ. Assim, $\mathrm{Im}\,\phi$ é fechada em relação à adição e à multiplicação. Logo, $\mathrm{Im}\,\phi$ é um subanel de S.

(b) Agora, vamos mostrar que o núcleo de ϕ, forma um ideal de R. Temos que $\phi(0) = 0$, então $0 \in \ker \phi$. Se $x, y \in \ker \phi$, então $\phi(x) = \phi(y) = 0$. Como ϕ preserva a adição:

$$\phi(x + y) = \phi(x) + \phi(y) = 0 + 0 = 0,$$

logo, $x + y \in \mathrm{Ker}\,\phi$. Seja $r \in R$ e $x \in \mathrm{Ker}\,\phi$. Como ϕ é homomorfismo, temos:

$$\phi(rx) = \phi(r) \cdot \phi(x) = \phi(r) \cdot 0 = 0,$$

assim, $rx \in \mathrm{Ker}\,\phi$. Portanto, $\mathrm{Ker}\,\phi$ satisfaz todas as condições para ser um ideal de R. □

Proposição 2.2.5. *Seja $\phi : R \longrightarrow S$ um homomorfismo de anéis. Então, ϕ é injetora se, e somente se,* $\ker \phi = \{0\}$.

Demonstração. Suponha que ϕ é injetora. Se $x \in \ker \phi$, então $\phi(x) = 0 = \phi(0)$. Pela injetividade, segue que $x = 0$. Logo, $\ker \phi = \{0\}$. Reciprocamente, suponha agora que $\ker \phi = \{0\}$ e que $\phi(a) = \phi(b)$ para alguns $a, b \in R$. Então:

$$\phi(a - b) = \phi(a) - \phi(b) = 0 \quad \Rightarrow \quad a - b \in \ker \phi.$$

Mas como $\ker \phi = \{0\}$, então $a - b = 0$, isto é, $a = b$. Logo, ϕ é injetora. □

2.2.2 Isomorfismo de anéis

Definição 2.2.6. Sejam R e S anéis. Um homomorfismo $\phi : R \longrightarrow S$ é dito *isomorfismo de anéis* se for bijetor.

Exemplo 2.2.7. Seja R um anel. A aplicação identidade

$$\mathrm{id}_R : R \longrightarrow R, \quad \mathrm{id}_R(x) = x, \text{ para todo } x \in R,$$

é um isomorfismo de anéis. De fato, id_R é homomorfismo, pois preserva as operações de adição e multiplicação, além disso, $\mathrm{id}_R(1) = 1$ e é, claramente, bijetora.

Proposição 2.2.8. *Seja $\phi : R \longrightarrow S$ um isomorfismo de anéis. Então, $\phi^{-1} : S \longrightarrow R$ também o é.*

Demonstração. Sabemos que a inversa de uma bijeção também é uma bijeção. Assim, ϕ^{-1} é uma aplicação bijetora de S em R. Resta verificar que ϕ^{-1} é um homomorfismo de anéis, isto é, que ela preserva a identidade, a adição e a multiplicação. Como ϕ é homomorfismo, temos $\phi(1) = 1$. Aplicando ϕ^{-1} dos dois lados, obtemos:

$$\phi^{-1}(\phi(1)) = \phi^{-1} \circ \phi(1) = \mathrm{id}_R(1) = 1.$$

Portanto, ϕ^{-1} preserva a identidade do anel. Suponha agora $a', b' \in S$. Como ϕ é bijetora, existem $a, b \in R$ tais que $a' = \phi(a)$ e $b' = \phi(b)$. Então:

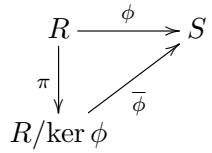
$$\phi^{-1}(a' + b') = \phi^{-1}(\phi(a) + \phi(b)) = \phi^{-1}(\phi(a + b)) = \mathrm{id}_R(a + b) = a + b = \phi^{-1}(a') + \phi^{-1}(b').$$

Da mesma forma, temos:

$$\phi^{-1}(a'b') = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = \mathrm{id}_R(ab) = ab = \phi^{-1}(a')\phi^{-1}(b').$$

Portanto, ϕ^{-1} preserva as operações e a identidade do anel, além de ser bijetora. Logo, é um isomorfismo de anéis. □

Teorema 2.2.9 (Primeiro Teorema dos Isomorfismos)**.** *Seja $\phi : R \longrightarrow S$ um homomorfismo de anéis. Então, existe um único homomorfismo injetor $\overline{\phi} : R/\ker \phi \longrightarrow S$ tal que o diagrama*



comuta. Além disso, temos um isomorfismo de anéis:

$$R/\ker \phi \simeq \mathrm{Im}\ \phi.$$

Demonstração. Seja $\phi : R \longrightarrow S$ um homomorfismo de anéis. Definimos a aplicação

$$\overline{\phi} : R/\ker\phi \longrightarrow S, \quad \overline{\phi}(\overline{a}) := \phi(a), \quad a \in R.$$

Primeiro, verificamos que $\overline{\phi}$ está bem definida. Se $\overline{a} = \overline{a'}$, então $a - a' \in \ker\phi$, o que implica $\phi(a-a') = 0$. Assim, $\phi(a) = \phi(a')$, logo $\overline{\phi}(\overline{a}) = \overline{\phi}(\overline{a'})$. Mostremos agora que $\overline{\phi}$ é homomorfismo. Para todo $a, b \in R$, tem-se

$$\overline{\phi}(\overline{a} + \overline{b}) = \overline{\phi}(\overline{a+b}) = \phi(a+b) = \phi(a) + \phi(b) = \overline{\phi}(\overline{a}) + \overline{\phi}(\overline{b}),$$

e

$$\overline{\phi}(\overline{a} \cdot \overline{b}) = \overline{\phi}(\overline{ab}) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(\overline{a}) \cdot \overline{\phi}(\overline{b}).$$

Além disso, como $\phi(1) = 1$, segue que $\overline{\phi}(\overline{1}) = 1$. Logo, $\overline{\phi}$ é um homomorfismo de anéis. A injetividade é imediata: se $\overline{\phi}(\overline{a}) = 0$, então $\phi(a) = 0$, ou seja, $a \in \ker\phi$, e portanto $\overline{a} = \overline{0}$. Seja agora $\pi : R \to R/\ker\phi$ a projeção canônica, dada por $\pi(a) = \overline{a}$. Para todo $a \in R$ temos

$$(\overline{\phi} \circ \pi)(a) = \overline{\phi}(\overline{a}) = \phi(a),$$

isto é, $\phi = \overline{\phi} \circ \pi$, o que mostra a comutatividade do diagrama. Por fim, notemos que

$$\mathrm{Im}(\overline{\phi}) = \{\overline{\phi}(\overline{a}) \mid a \in R\} = \{\phi(a) \mid a \in R\} = \mathrm{Im}(\phi).$$

Concluímos, portanto, que $\overline{\phi}$ é um homomorfismo injetor de $R/\ker\phi$ em S, com imagem igual a $\mathrm{Im}(\phi)$. Assim,

$$R/\ker\phi \simeq \mathrm{Im}(\phi)$$

como desejado □

O Primeiro Teorema dos Isomorfismos pode ser usado para caracterizar ideais importantes em anéis de polinômios. Um exemplo é o *homomorfismo de avaliação*, que nos permite provar que o ideal gerado pela variável x é primo no anel de polinômios $R[x]$.

Proposição 2.2.10. *Seja R um domínio de integridade. Então, o ideal principal $\langle x \rangle$ é um ideal primo no anel de polinômios $R[x]$.*

Demonstração. Para provar este resultado, definimos um homomorfismo sobrejetor $\phi : R[x] \to R$ e usamos o Primeiro Teorema dos Isomorfismos para analisar a estrutura do anel quociente $R[x]/\langle x \rangle$.

Considere a aplicação $\phi : R[x] \to R$ tal que

$$\phi(f(x)) = f(0).$$

Se $f(x) = a_n x^n + \cdots + a_1 x + a_0$, então $\phi(f(x)) = a_0$. Essa aplicação é um homomorfismo de anéis sobrejetor, pois para qualquer $r \in R$, o polinômio constante $f(x) = r$ é mapeado para r.

O núcleo de ϕ é o conjunto de todos os polinômios $f(x) \in R[x]$ tais que $f(0) = 0$. Um polinômio satisfaz esta condição se, e somente se, seu termo constante for nulo, o que significa que o polinômio é um múltiplo de x. Portanto, o núcleo é o ideal principal gerado por x:

$$\ker(\phi) = \langle x \rangle.$$

Pelo Primeiro Teorema dos Isomorfismos, temos o isomorfismo $R[x]/\ker(\phi) \simeq \mathrm{Im}(\phi)$. Como $\mathrm{Im}(\phi) = R$, obtemos:

$$R[x]/\langle x \rangle \simeq R.$$

Por hipótese, o anel R é um domínio de integridade. Como o anel quociente $R[x]/\langle x \rangle$ é isomorfo a R, ele também deve ser um domínio de integridade. Aplicando (2.1.3) ao nosso caso, concluímos que o ideal $\langle x \rangle$ é um ideal primo em $R[x]$. □

Teorema 2.2.11 (Segundo teorema dos isomorfismos)**.** *Seja R um anel e $I \subseteq J$ ideais de R. Então,*

$$(R/I)/(J/I) \simeq R/J.$$

Demonstração. Sejam R um anel e $I \subseteq J$ ideais de R. Definimos a aplicação

$$\varphi : R/I \longrightarrow R/J, \qquad \varphi(a + I) = a + J.$$

Queremos mostrar que φ é bem definida e é um homomorfismo cujo núcleo é J/I. Se $a+I = b+I$ então $a - b \in I$. Como $I \subseteq J$, segue $a - b \in J$, logo $a + J = b + J$. Assim $\varphi(a + I) = \varphi(b + I)$. Para $a, b \in R$ temos,

$$\varphi((a + I) + (b + I)) = \varphi((a + b) + I) = (a + b) + J = (a + J) + (b + J),$$
$$\varphi((a + I)(b + I)) = \varphi((ab) + I) = (ab) + J = (a + J)(b + J).$$

E também $\varphi(1 + I) = 1 + J$. Portanto φ é homomorfismo de anéis. Agora iremos calcular o núcleo de φ. Primeiro, se $a + I \in \ker\varphi$ então

$$\varphi(a + I) = a + J = 0 + J,$$

ou seja $a \in J$. Logo $a + I \in J/I$, mostrando $\ker\varphi \subseteq J/I$. Reciprocamente, se $a + I \in J/I$ então $a \in J$ e portanto

$$\varphi(a + I) = a + J = 0 + J,$$

isto é $a + I \in \ker\varphi$. Assim $\ker\varphi = J/I$. Pelo Teorema (2.2.9), $(R/I)/\ker\varphi \cong \mathrm{Im}\,\varphi$. Como

$\ker \varphi = J/I$ e φ é sobrejetora, obtemos

$$(R/I)/(J/I) \cong R/J.$$

□

Definição 2.2.12. Seja D um domínio, e sejam $a, b \in D$. Dizemos que b divide a em D e denotamos por $b \mid a$ se existe $c \in D$ tal que $a = bc$. Caso contrário, escrevemos $b \nmid a$, ou seja, b não divide a.

Definição 2.2.13. Seja D um domínio e $a, b \in D$, com $a \neq 0$ ou $b \neq 0$. Um *máximo divisor comum* de a e b, ou simplesmente $\mathrm{mdc}(a, b)$, é um elemento $d \in D$ que satisfaz:

1. $d \mid a$ e $d \mid b$;
2. se d' é tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

Definição 2.2.14. Seja D um domínio. Dois elementos $a, b \in D \setminus \{0\}$ são ditos *associados* se existe $u \in D^*$ tal que $a = ub$.

Observação 2.2.15. Se o máximo divisor comum de dois elementos existe, ele é único a menos de associados.

Proposição 2.2.16. *Se D é um domínio de ideais principais, então, quaisquer que sejam $a, b \in D$ não ambos nulos, o $\mathrm{mdc}(a, b)$ sempre existe.*

Demonstração. Como D é um domínio de ideais principais, temos que o ideal gerado por a e b é principal, isto é, $(a, b) = (d)$ para algum $d \in D$. Em particular, $a, b \in (d)$, o que implica que $d \mid a$ e $d \mid b$. Agora, seja $d' \in D$ tal que $d' \mid a$ e $d' \mid b$. Então existem $l, k \in D$ tais que $a = ld'$ e $b = kd'$. Como $d \in (a, b)$, existem $x, y \in D$ com $d = ax + by$. Substituindo as expressões de a e b, obtemos:

$$d = (ld')x + (kd')y = (lx + ky)d',$$

o que mostra que $d' \mid d$. Assim, d satisfaz a definição de máximo divisor comum de a e b. □

2.3 Domínio de fatoração única

Definição 2.3.1. Seja p um elemento não nulo e não invertível de um domínio D.

(a) Dizemos que p é *irredutível* em D se $p = ab$, com $a, b \in D$, implicar que a ou b é invertível em D.

(b) Dizemos que p é *primo* em D se $p|ab$, com $b \in D$, implicar que $p|a$ ou $p|b$

Os conceitos de elemento irredutível e primo estão relacionados da seguinte maneira

Proposição 2.3.2. *Seja p um elemento primo em um domínio D. Então p é irredutível em D.*

Demonstração. Suponha que $p = ab$ para certos $a, b \in D$. Obviamente, $p|p$. Assim, $p \mid ab$. Da primalidade de p segue que $p \mid a$ ou $p \mid b$. Sem perda de generalidade, suponha que $p \mid a$. Então existe $l \in D$ tal que $a = lp$. Substituindo na igualdade inicial $p = ab$, obtemos

$$p = (lp)b = l(pb).$$

Como D é um domínio e $p \neq 0$, podemos cancelar p dos dois lados, obtendo

$$1 = lb.$$

Isso mostra que b é inversível em D. Logo, sempre que $p = ab$, um dos fatores é invertível em D. Portanto, p é irredutível em D. □

Proposição 2.3.3. *Seja D um domínio. Então, um elemento $p \in D \setminus \{0\}$ é primo se, e somente se, o ideal (p) é um ideal primo.*

Demonstração. ($\Rightarrow$) Suponha que p seja primo em D. Queremos mostrar que (p) é um ideal primo. Seja $ab \in (p)$, com $a, b \in D$. Isso significa que existe $c \in D$ tal que $ab = pc$. Assim, $p \mid ab$. Como p é primo, segue que $p \mid a$ ou $p \mid b$. Se $p \mid a$, então $a \in (p)$; se $p \mid b$, então $b \in (p)$. Portanto, (p) satisfaz a condição de ideal primo.

Observação: se p for unidade, então $(p) = D$ e não é ideal próprio; por isso, exige na definição de elemento primo que p seja não nulo e diferente da unidade.

($\Leftarrow$) Suponha agora que (p) seja um ideal primo. Primeiro notemos que $(p) \neq D$, pois um ideal primo é próprio; portanto p não é unidade. Além disso, $p \neq 0$, pois se $p = 0$ então $(p) = (0)$ e (0) sempre é um ideal primo em um domínio, inclusive, esse fato foi mostrado em (1.6.3), o que não é o caso aqui; assim, na hipótese usual, $p \neq 0$. Seja $a, b \in D$ tal que $p \mid ab$, isto é, $ab \in (p)$. Como (p) é primo, temos $a \in (p)$ ou $b \in (p)$. Em ambos os casos conclui-se que $p \mid a$ ou $p \mid b$. Portanto p é um elemento primo. Juntando as duas implicações, obtemos a equivalência desejada. □

Definição 2.3.4. Dizemos que um domínio D é um *domínio de fatoração única* (denotado por DFU) se todo elemento $a \in D \setminus D^*$, $a \neq 0$, pode ser escrito como um produto finito de elementos irredutíveis, isto é,

$$a = p_1 p_2 \cdots p_r,$$

com p_i irredutível para todo i.

Além disso, tal fatoração é única no seguinte sentido: se

$$a = p_1 p_2 \cdots p_r \quad \text{e} \quad a = q_1 q_2 \cdots q_s,$$

em que todos p_i e q_j são irredutíveis, então $r = s$ e, a menos de reordenação dos fatores, cada p_i é associado a q_i, isto é, $p_i = u_i q_i$ para alguma unidade $u_i \in D^*$.

Exemplo 2.3.5. O anel $\mathbb{Z}$ é um DFU, pois todo inteiro não nulo e diferente da unidade admite fatoração única em números primos (a menos de sinal). Por exemplo:

$$30 = 2 \cdot 3 \cdot 5 = (-5) \cdot (-2) \cdot 3,$$

em que as duas fatorações diferem apenas por unidades (± 1).

Capítulo 3

Módulos

Um conceito fundamental em toda álgebra comutativa é o de módulo. Nesta etapa, destacaremos os principais aspectos da teoria de módulos que serão relevantes para o desenvolvimento das investigações propostas neste trabalho, fornecendo a base teórica necessária para a compreensão dos resultados que virão a seguir.

3.1 Definição e Exemplos de Módulos

Definição 3.1.1. Seja R um anel. Um *módulo* sobre R (ou simplesmente, *R-módulo*) é um grupo abeliano M, com operação denotada por $+$, e com uma multiplicação por escalar

$$R \times M \longrightarrow M \quad (a, x) \mapsto ax$$

satisfazendo:

$$(ab)x = a(bx),\ (a+b)x = ax + bx,\ a(x+y) = ax + ay,\ 1x = x \tag{3.1}$$

para qualquer $a, b \in R$ e para qualquer $x, y \in M$.

Observação 3.1.2. Notemos que os espaços vetoriais são módulos sobre os corpos. Assim, a teoria de módulos é uma generalização da teoria dos espaços vetoriais.

Exemplo 3.1.3. Seja n um número inteiro positivo. Denotamos o conjunto de todas as n-uplas ordenadas de elementos de R por R^n, ou seja,

$$R^n = \{(a_1, \ldots, a_n) \mid a_i \in R,\ 1 \leq i \leq n\}.$$

Nesse conjunto, a adição é definida coordenada a coordenada:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$

e a multiplicação por escalar $r \in R$ é dada por

$$r(a_1, \ldots, a_n) = (ra_1, \ldots, ra_n).$$

Com essas operações é possível verificar que R^n é um *R-módulo*.

Exemplo 3.1.4. Seja R um anel. O conjunto $M_{m\times n}(R)$ de todas as matrizes $m \times n$ com entradas em R, munido da adição usual de matrizes e da multiplicação por escalar feita elemento a elemento, é um R-módulo.

Exemplo 3.1.5. O anel de polinômios $R[x_1, \ldots, x_n]$, com a adição usual de polinômios e a multiplicação por escalar dada pela multiplicação usual por elementos de R, é um R-módulo.

Exemplo 3.1.6. Seja I um ideal de um anel R. O anel quociente R/I possui uma estrutura natural de R-módulo. A adição é a usual, e a multiplicação por escalar é dada por

$$r(x + I) = rx + I$$

para todo $r \in R$ e $x + I \in R/I$.

3.2 Submódulos

Definição 3.2.1. Seja M um *R-módulo*. Um subconjunto $N \subseteq M$ é chamado de *R-submódulo* ou simplesmente *submódulo* de M se:

(i) $0 \in N$;

(ii) $u + av \in N$, para todo $a \in R$ e para todos $u, v \in N$.

Exemplo 3.2.2. Seja M um R-módulo. Os conjuntos $\{0\}$ e M são submódulos de M, sendo chamados de *submódulos triviais*.

Exemplo 3.2.3. Todo anel R pode ser visto como um R-módulo sobre si mesmo, onde as operações de adição e multiplicação por escalar coincidem com a adição e multiplicação de R como anel. Nesse caso, os submódulos de R são exatamente os ideais de R.

Exemplo 3.2.4. Seja I um ideal de um anel R e M um módulo sobre R. O subconjunto

$$IM = \{a_1x_1 + \cdots + a_rx_r \,|\, r \in \mathbb{N},\, a_i \in I \text{ e } x_i \in M\}$$

é um submódulo de M.

3.3 Módulos quocientes

Seja M um R-módulo e $N \subseteq M$ um submódulo. Dados elementos $x, y \in M$, dizemos que x é *congruente* a y módulo N se $x - y \in N$. Pode-se verificar, que essa relação é de equivalência. A classe de equivalência de um elemento x de M por essa relação é denotada por $\overline{x}$ ou $x + N$. O conjunto de todas as classes é denotado por M/N. Definimos em M/N as seguintes operações

$$\overline{x} + \overline{y} := \overline{x + y}, \quad \text{e} \quad a \cdot \overline{x} := \overline{ax}, \;\; a \in R.$$

Estas operações estão bem definidas e conferem a M/N a estrutura de R-módulo, chamado *módulo quociente* de M por N. É importante destacar os seguintes fatos sobre o módulo quociente M/N :

(i) O zero de M/N corresponde a classe do 0 de M. Mais geralmente, temos que $\overline{0} = \overline{x}$ se, e somente se, $x \in N$.

(ii) Para qualquer $x \in M$, a classe $\overline{-x}$ é inverso aditivo de $\overline{x}$.

Teorema 3.3.1 (Correspondência de Módulos)**.** *Sejam M um R-módulo e $N \subseteq M$ um submódulo. Existe uma bijeção entre os submódulos de M/N e os submódulos de M que contém N. Em particular, todo submódulo de M/N é da forma N'/N, onde N' é um submódulo de M que contém N.*

Demonstração. Ver [1, Theorem 11.4.3]. □

3.4 Homomorfismos de Módulos

Definição 3.4.1. Sejam M e N dois *R-módulos*. Uma aplicação $f : M \longrightarrow N$ chama-se *homomorfismo de R-módulos*, se

$$f(x + y) = f(x) + f(y) \quad \text{e} \quad f(ax) = af(x)$$

para cada $x, y \in M$ e para cada $a \in R$.

Exemplo 3.4.2. Sejam M um R-módulo e N um R-submódulo de M. A função *inclusão*, definida por

$$i : N \longrightarrow M, \quad i(x) = x,$$

é um homomorfismo de R-módulos.

Exemplo 3.4.3. Seja M um módulo sobre um anel R e N um submódulo de M. A aplicação

$$\pi : M \to M/N, \quad x \mapsto \overline{x}$$

é um homomorfismo de módulos, chamado de *projeção canônica* de M sobre M/N.

Definição 3.4.4. Uma função $f : M \longrightarrow N$ entre dois R-módulos M e N é chamada *isomorfismo de M em N* se f for um homomorfismo bijetor.

Dizemos que dois R-módulos M e N são *isomorfos* se existe um isomorfismo entre eles e denotamos esse fato pela notação $M \cong N$.

Exemplo 3.4.5. O homomorfismo identidade $\mathrm{id}_M : M \longrightarrow M$ é, obviamente, um isomorfismo.

3.4.1 Núcleo e imagem de um homomorfismo

De maneira análoga ao que ocorre na teoria de anéis, também na teoria de módulos podemos associar a um homomorfismo as noções de *núcleo* e *imagem*. Esses dois conceitos têm o papel de analisar as propriedades do homomorfismo. O núcleo está diretamente relacionado à injetividade, enquanto a imagem mede a sobrejetividade da aplicação.

Sejam M e N dois R-módulos e $f : M \to N$ um homomorfismo de R-módulos. O *núcleo* e a *imagem* de f são, respectivamente, os seguintes conjuntos:

$$\ker f = \{x \in M \,|\, f(x) = 0\} \quad \text{e} \quad \mathrm{Im}\, f = \{y \in N \,|\, y = f(x), \text{ para algun } x \in M\}.$$

Proposição 3.4.6. *Sejam M e N dois R-módulos e $f : M \longrightarrow N$ um homomorfismo. Então,*

(i) $\ker f$ *é submódulo de* M.

(ii) $\mathrm{Im}\, f$ *é submódulo de* N.

Demonstração. (i) Como f é homomorfismo,

$$f(0) = f(0 + 0) = f(0) + f(0).$$

Subtraindo $f(0)$ em ambos os lados, obtemos $f(0) = 0$. Logo, $0 \in \mathrm{Ker}(f)$.

Se $x, y \in \mathrm{Ker}(f)$ e $r \in R$, então $f(x) = 0$ e $f(y) = 0$. Assim,

$$f(x + ry) = f(x) + rf(y) = 0 + r \cdot 0 = 0,$$

o que implica $x + ry \in \ker(f)$. Portanto, $\ker(f)$ é submódulo de M.

(ii) Pelo cálculo anterior, $f(0) = 0$. Logo, $0 \in \mathrm{Im}(f)$.

Sejam $r \in R$ e $u, v \in \mathrm{Im}(f)$. Então, existem $x, y \in M$ tais que $u = f(x)$ e $v = f(y)$. Assim:

$$u + rv = f(x) + rf(y) = f(x + ry) \in \mathrm{Im}(f).$$

Portanto, $\mathrm{Im}(f)$ é submódulo de N. □

Proposição 3.4.7. *Sejam M e N dois R-módulos e $f : M \longrightarrow N$ um homomorfismo. Então, f é injetora se, e somente se,* $\ker f = \{0\}$.

Demonstração. Suponha que f é injetora. Dado $x \in \ker f$ temos

$$f(x) = 0 = f(0).$$

Da injetividade de f segue que $x = 0$. Logo, $\ker f = \{0\}$.

Reciprocamente, suponhamos que $\ker f = \{0\}$. Dados $x, y \in M$ tais que $f(x) = f(y)$ temos que $f(x) - f(y) = 0$. Como f é homomorfismo temos $f(x - y) = 0$. Logo, $x - y \in \ker f = \{0\}$. Desse modo,

$$x - y = 0.$$

Equivalentemente, $x = y$. Portanto, f é injetora. □

Teorema 3.4.8 (Primeiro Teorema dos Isomorfismos)**.** *Seja $f : M \longrightarrow N$ um homomorfismo de R-módulos. Então*

$$M/\ker(f) \cong \mathrm{Im}(f).$$

Demonstração. Ver [1, Theorem 11.4.2]. □

Teorema 3.4.9 (Segundo Teorema dos Isomorfismos)**.** *Seja M um R-módulo, e sejam $N, L \subseteq M$ submódulos. Então*

$$(N + L)/L \cong N/(N \cap L).$$

Demonstração. Ver [1, Theorem 11.4.2]. □

3.5 Conjunto de geradores

Definição 3.5.1. Seja M um R-módulo e $v_1, \ldots, v_m \in M$. Dados $r_1, \ldots, r_m \in R$, chamamos a expressão

$$r_1 v_1 + \cdots + r_m v_m$$

de *combinação linear* dos elementos $v_1, \ldots, v_m$ com coeficientes em R.

Seja $S \subseteq M$ um subconjunto de um R-módulo M. Denotamos por $\langle S \rangle$ o conjunto formado por todas as combinações lineares de elementos de S com coeficientes em R.

Proposição 3.5.2. *O conjunto $\langle S \rangle$ é um submódulo de M.*

Demonstração. Observe inicialmente que

$$0 \cdot v_1 + \cdots + 0 \cdot v_m = 0.$$

Logo, $0 \in \langle S \rangle$. Sejam agora $x, y \in \langle S \rangle$ e $r \in R$. Por definição, existem $v_1, \ldots, v_k \in S$ e coeficientes $a_1, \ldots, a_k \in R$ tais que

$$x = a_1 v_1 + \cdots + a_k v_k.$$

Analogamente, existem $w_1, \ldots, w_t \in S$ e coeficientes $b_1, \ldots, b_t \in R$ tais que

$$y = b_1 w_1 + \cdots + b_t w_t.$$

Então,

$$\begin{aligned} x + ry &= a_1 v_1 + \cdots + a_k v_k + r(b_1 w_1 + \cdots + b_t w_t) \\ &= a_1 v_1 + \cdots + a_k v_k + (rb_1) w_1 + \cdots + (rb_t) w_t, \end{aligned}$$

que é uma combinação linear de elementos de S. Logo, $x + ry \in \langle S \rangle$. Assim, $\langle S \rangle$ é submódulo de M. □

Todo submódulo N de M é da forma $N = \langle S \rangle$ para algum subconjunto S de N. Chamamos $\langle S \rangle$ de *submódulo gerado por* S. Se $M = \langle S \rangle$, dizemos que S é um *conjunto de geradores* do R-módulo M. Além disso, se $S = \{v_1, \ldots, v_m\}$, escrevemos $\langle v_1, \ldots, v_m \rangle$ em vez de $\langle S \rangle$. Dizemos também que um R-módulo M é *finitamente gerado* se existem $v_1, \ldots, v_m \in M$ tais que $\langle v_1, \ldots, v_m \rangle = M$.

Definição 3.5.3. Seja M um R-módulo. Dizemos que um subconjunto $S \subseteq M$ é *linearmente independente* se para quaisquer $r_1, \ldots, r_m \in M$ e $v_1, \ldots, v_m \in R$ tais que

$$r_1 v_1 + \cdots + r_m v_m = 0$$

tem-se que $r_1 = \cdots = r_m = 0$. Caso contrário, dizemos que S é *linearmente dependente*.

3.6 Módulos Livres

Um conceito central na teoria de módulos é o de *módulo livre*. De maneira análoga ao caso dos espaços vetoriais sobre corpos, um módulo livre é aquele que possui uma *base*, isto é, um conjunto de geradores linearmente independente.

Definição 3.6.1. Seja M um R-módulo. Dizemos que M é um *R-módulo livre* se M possui uma base.

Exemplo 3.6.2. Para cada $1 \leq i \leq n$, denotemos por e_i a n-upla de R^n cuja i-ésima coordenada é 1 a as demais são iguais a zero. O conjunto $\{e_1, \ldots, e_n\}$ é uma base para o R^n. Assim, R^n é um módulo livre.

Exemplo 3.6.3. O anel $R[x]$ é um R-módulo livre. Uma base para este R-módulo é o conjunto

$$\{1, x, x^2, x^3, \ldots\}.$$

No próximo exemplo veremos que para um anel R que não é corpo sempre existirá um R-módulo que não é livre.

Exemplo 3.6.4. Seja R um anel que não é um corpo. Então existe um ideal I de R que não é trivial. Considere o R módulo R/I. Suponha S um subconjunto não vazio de R/I e a um elemento não nulo de I. Para um elemento $\alpha + I$ de S temos

$$a(\alpha + I) = 0.$$

Isso nos dá uma combinação linear não trivial dos elementos de S, mostrando que S é linearmente dependente. Isso nos mostra que qualquer conjunto não vazio de R/I é linearmente dependente. Logo. R/I não possui base e, portanto, não é livre.

Proposição 3.6.5. *Seja M um R-módulo livre. Quaisquer duas bases de M tem a mesma cardinalidade.*

Demonstração. Ver [1, Proposition 14.2.6 (b)]. □

Devido a essa proposição temos a seguinte definição

Definição 3.6.6. Seja M um R-módulo livre. A cardinalidade de uma base de M (e, portanto, todas as bases de M) é chamada de *posto* de M.

Exemplo 3.6.7. Pelo Exemplo 3.6.2 concluímos que R^n é um R-módulo livre de posto n.

Proposição 3.6.8. *Seja M um R-módulo e $u_1, \ldots, u_n \in M$. Dado um R-módulo livre F de posto n com base $\{e_1, \ldots, e_n\}$, existe um único homomorfismo de R-módulos $\Phi : F \to M$ tal que $\Phi(e_i) = u_i$ para todo $i = 1, \ldots, n$.*

Demonstração. **Existência:** Como F é livre de posto n com base $\{e_1, \ldots, e_n\}$, todo $v \in F$ admite uma única escrita

$$v = r_1 e_1 + \cdots + r_n e_n, \quad r_i \in R.$$

Definimos

$$\Phi(v) := r_1 u_1 + \cdots + r_n u_n.$$

Essa aplicação é bem definida e é linear pela construção, logo é um homomorfismo com $\Phi(e_i) = u_i$ para todo $i = 1, \ldots, n$.

Unicidade: Suponha agora $\Psi : F \to M$ ser um homomorfismo com $\Psi(e_i) = u_i$ para todo $i = 1, \ldots, n$. Dado $v = r_1 e_1 + \cdots + r_n e_n$, segue pelo fato de Ψ ser homomorfismo que

$$\Psi(v) = r_1 \Psi(e_1) + \cdots + r_n \Psi(e_n) = r_1 u_1 + \cdots + r_n u_n = \Phi(v).$$

Portanto, $\Phi = \Psi$. □

Observação 3.6.9. Homomorfismos entre R-módulos livres de postos finitos podem ser representados por matrizes, de modo análogo às transformações lineares entre espaços vetoriais.

Sejam F e G dois R-módulos livres de postos finitos e seja $f : F \to G$ um homomorfismo de R-módulos. Suponha que $B = \{e_1 \dots e_n\}$ e $B' = \{e'_1 \dots e'_m\}$ são bases para F e G, respectivamente. Para cada elemento e_j da base de F, calculamos sua imagem $f(e_j)$ em G através de f. Em particular, cada $f(e_j)$ pode ser escrito de forma única como uma combinação linear dos elementos da base B' com coeficientes em R. Precisamente,

$$\begin{aligned} f(e_1) &= a_{11}e'_1 + a_{21}e'_2 + \cdots + a_{m1}e'_m \\ f(e_2) &= a_{12}e'_1 + a_{22}e'_2 + \cdots + a_{m2}e'_m \\ &\vdots \\ f(e_n) &= a_{1n}e'_1 + a_{2n}e'_2 + \cdots + a_{mn}e'_m \end{aligned}$$

cada $a_{ij} \in R$. A matriz $[f]_B^{B'} := (a_{i,j})$ é chamada de *representação matricial* do homomorfismo f com respeito as bases B e B'. De acordo com a Proposição 3.6.8, o homomorifismo f é completamente determinado pela matriz $[f]_B^{B'}$. Observe que $[f]_B^{B'}$ é uma matriz de ordem $m \times n$ cuja a j-ésima coluna da matriz é composta pelos coeficientes da imagem do j-ésimo elemento da base, $f(e_j)$.

Exemplo 3.6.10. Seja $R = k[x, y]$ o anel de polinômios em duas variáveis com coeficientes em um corpo k e seja $f : R^2 \to R^3$ o homommorfismo dado por

$$f(p, q) = (py, px + qy, qx).$$

Denotemos por $B = \{e_1, e_2\}$ a base canônica de R^2 e por $B' = \{e'_1, e'_2, e'_3\}$ a base canônica de R^3. Calculando a imagem dos elementos da base canônica B de R^2 e escrevendo-os como combinação linear da base B', temos:

$$f(e_1) = f(1, 0) = (y, x, 0) = ye'_1 + xe'_2 + 0e'_3$$

$$f(e_2) = f(0, 1) = (0, y, x) = 0e'_1 + ye'_2 + xe'_3$$

Daí, a matriz de f em relação às bases canônicas B e B' é:

$$[f]_B^{B'} = \begin{pmatrix} y & 0 \\ x & y \\ 0 & x \end{pmatrix}.$$

3.7 Módulos Noetherianos

Definição 3.7.1. Um R-módulo M é dito *Noetheriano* se todo submódulo de M é finitamente gerado. Um anel R é dito *Noetheriano* se o for como R-módulo (ou seja, todo ideal de R é finitamente

gerado).

Exemplo 3.7.2. Todo domínio de ideais principais é um anel Noetheriano. Em particular, domínios euclidianos, corpos e o anel dos inteiros são anéis Noetherianos.

Exemplo 3.7.3. Todo anel finito é Noetheriano.

Exemplo 3.7.4. Se M é R-módulo Noetheriano e N é submódulo Noetheriano então M/N é R-módulo Noetheriano.

Teorema 3.7.5 (Caracterização dos Módulos Noetherianos)**.** *Seja A um anel e M um A-módulo. São equivalentes:*

(i) *M é Noetheriano.*

(ii) *Toda cadeia ascendente de submódulos de M se estabiliza.*

(iii) *Toda família não vazia de submódulos de M possui um elemento maximal com respeito à inclusão.*

Demonstração. Ver [7, Definition 2.1 e Theorem 2.9]. □

Exemplo 3.7.6. Seja $F(\mathbb{R},\mathbb{R})$ o anel das funções de $\mathbb{R}$ em $\mathbb{R}$. Para cada inteiro positivo n, defina I_n em $F(\mathbb{R},\mathbb{R})$, como sendo o conjunto das funções f em $F(\mathbb{R},\mathbb{R})$ tal que $f(x)=0$ para todo $x \geq n$. Pode-se verificar que I_n é ideal de $F(\mathbb{R},\mathbb{R})$. A cadeia ascendente

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

não estabiliza. De fato, para cada inteiro positivo n temos que a função

$$f_{n+1}(x) = \begin{cases} x-(n+1) & , x \leq n+1 \\ 0 & , x \geq n+1 \end{cases}$$

pertence a I_{n+1} mas não pertence a I_n. Portanto, $F(\mathbb{R},\mathbb{R})$ não é Noetheriano.

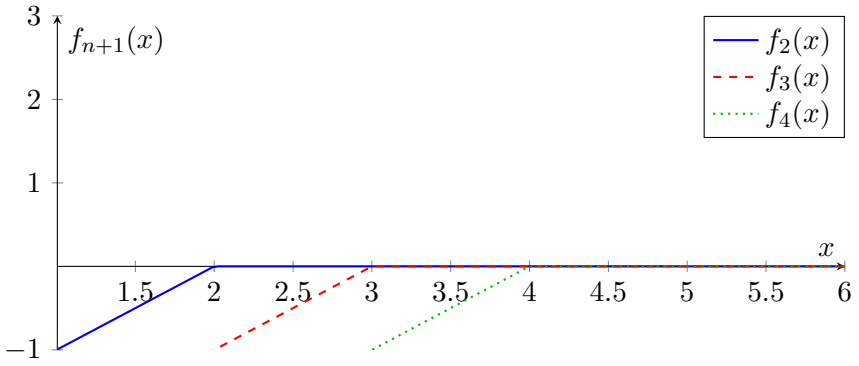


Figura 3.1: Gráfico das funções f_2, f_3, f_4 em $F(\mathbb{R}, \mathbb{R})$. Cada função anula-se após $x = n + 1$, mostrando que a cadeia $I_1 \subset I_2 \subset I_3 \subset \cdots$ não estabiliza.

Proposição 3.7.7. *Se R é um anel Noetheriano e M é um R-módulo finitamente gerado, então M é Noetheriano.*

Demonstração. Ver [4, Proposition 1.4] □

Teorema 3.7.8 (Teorema da base de Hilbert)**.** *Se R é um anel Noetheriano, então o anel de polinômios $R[x_1, \ldots, x_n]$ também o é.*

Demonstração. Ver [7, Theorem 2.11 e Corollary 2.13]. □

Capítulo 4

Sizígias

No estudo da álgebra comutativa e, em particular, na teoria de módulos, surge naturalmente a necessidade de compreender não apenas como um conjunto de elementos gera um módulo, mas também quais são as relações existentes entre esses geradores. Essas relações, que expressam combinações lineares dos geradores que resultam no elemento nulo, de maneira mais formal, são chamadas *sizígias*. A análise das sizígias permite investigar a estrutura interna de um módulo com mais profundidade, indo além da simples descrição por um conjunto de geradores. Esse estudo está intimamente ligado à construção de resoluções livres. Além de sua importância teórica, o conceito de sizígias encontra aplicações em várias áreas. O objetivo deste capítulo é introduzir formalmente o conceito de sizígia, apresentar exemplos e estabelecer ferramentas para seu cálculo no contexto de módulos sobre anéis comutativos.

4.1 Definição e Exemplos de Sizígias

Sejam R um anel, M um R-módulo finitamente gerado e $G = \{g_1, \ldots, g_m\}$ um conjunto de geradores para M. Considere o homomorfismo sobrejetor

$$\phi : R^m \twoheadrightarrow M,\ e_i \mapsto g_i.$$

Dado $v = \alpha_1 e_1 + \cdots + \alpha_m e_m \in R^m$ temos

$$\phi(v) = \alpha_1 g_1 + \cdots + \alpha_m g_m.$$

Dizemos que $v = (\alpha_1, \ldots, \alpha_m)$ é *sizígia* de M com respeito ao conjunto de geradores G se $v \in \ker \phi$, ou seja,

$$\alpha_1 g_1 + \cdots + \alpha_m g_m = 0.$$

Chamamos o núcleo de ϕ de *módulo de sizígias* do R-módulo M com respeito ao conjunto de geradores G e o denotamos por $\mathrm{Syz}_G(M)$. Em particular, segue do primeiro teorema dos isomorfismos a seguinte representação para o módulo M

$$M \simeq R^m/\mathrm{Syz}_G(M).$$

Graças a esse homomorfismo, podemos estudar M em termos do R-módulo livre R^m e do seu submódulo $\mathrm{Syz}_G(M)$. Uma questão natural nesse contexto é como descrever os geradores de $\mathrm{Syz}_G(M)$. Tipicamente, essa é uma questão de natureza muito difícil. A seguir, apresentamos um exemplo bastante ilustrativo.

Exemplo 4.1.1. Para qualquer ideal I gerado por um conjunto $G = \{f_1, \ldots, f_m\}$ em um anel comutativo R, podemos encontrar um conjunto de sizígias de forma imediata. Essas relações surgem diretamente da propriedade comutativa da multiplicação do anel ($f_i f_j = f_j f_i$). Para qualquer par de índices $1 \leq i < j \leq m$, a seguinte relação é sempre verdadeira:

$$(-f_j)f_i + (f_i)f_j = 0.$$

Essa relação corresponde a uma sizígia em R^m. Se considerarmos a base canônica $G = \{e_1, \ldots, e_m\}$ de R^m, onde cada e_k é uma n-upla com 1 na k-ésima posição e 0 nas demais, podemos escrever esta sizígia da seguinte maneira:

$$\mathfrak{z}_{i,j} = -f_j e_i + f_i e_j.$$

Essa sizígia tem o elemento $-f_j$ na i-ésima posição, f_i na j-ésima posição, e zeros em todas as outras. Por exemplo,

$$\mathfrak{z}_{i,j} = (0, \ldots, -f_j, \ldots, f_i, \ldots, 0) \in R^m.$$

Essas sizígias, que existem para qualquer ideal, são conhecidas como *sizígias de Koszul*. Elas formam o primeiro conjunto de relações que se pode identificar entre os geradores de um ideal.

Exemplo 4.1.2. Seja $R = k[x, y]$ o anel de polinômios em duas variáveis sobre um corpo K e considere o ideal I gerado pelo conjunto $G = \{x, y\}$. Vamos calcular um conjunto de geradores para o módulo de sizígias $\mathrm{Syz}_G(I)$. Definimos o homomorfismo

$$\phi : R^2 \twoheadrightarrow I, \quad e_1 \mapsto x, \quad e_2 \mapsto y,$$

o qual, para um par arbitrário $(a, b) \in R^2$, é dado por

$$\phi(a, b) = ax + by.$$

Observemos que

$$(-y) \cdot x + (x) \cdot y = -yx + xy = 0,$$

ou seja, $\mathfrak{z}_{1,2} = (-y, x)$ pertence a $\mathrm{Syz}_G(I)$. Assim,

$$\langle \mathfrak{z}_{1,2} \rangle \subseteq \mathrm{Syz}_G(I).$$

Mostremos agora a inclusão contrária. Seja $\mathfrak{z} = (p, q) \in \mathrm{Syz}_G(I)$. Por definição, temos

$$px + qy = 0. \tag{4.1}$$

Equivalentemente,

$$px = -qy. \tag{4.2}$$

Como $\langle y \rangle$ é um ideal primo em R e $x \notin \langle y \rangle$, a equação (4.2) implica que $q \in \langle x \rangle$. Logo, existe $u \in R$ tal que

$$q = ux. \tag{4.3}$$

Substituindo (4.3) em (4.2), obtemos

$$px = -uxy,$$

e como x é não nulo em R, podemos cancelar x, obtendo

$$p = -uy. \tag{4.4}$$

Portanto, a sizígia $\mathfrak{z}$ pode ser escrita como

$$\mathfrak{z} = (p, q) = (-uy, ux) = u(-y, x) = u\mathfrak{z}_{1,2}.$$

Logo, $\mathfrak{z} \in \langle \mathfrak{z}_{1,2} \rangle$. Assim, concluímos que

$$\mathrm{Syz}_G(I) = \langle \mathfrak{z}_{1,2} \rangle.$$

Exemplo 4.1.3. Seja $R = k[x, y]$ um anel de polinômios em duas variáveis com coeficientes em um corpo k e I o ideal gerado pelo conjunto $G = \{x^2, xy, y^2\}$. Vamos calcular um conjunto de geradores para o módulo de sizígias $\mathrm{Syz}_G(I)$. Nosso objetivo é estudar o módulo de sizígias $\mathrm{Syz}_G(I)$. Definimos o homomorfismo

$$\phi : R^3 \twoheadrightarrow I, \quad e_1 \mapsto x^2, \quad e_2 \mapsto xy, \quad e_3 \mapsto y^2,$$

o qual, para $(a, b, c) \in R^3$, é dado por

$$\phi(a, b, c) = ax^2 + bxy + cy^2.$$

As relações triviais de Koszul entre os geradores x^2, xy, y^2 produzem as seguintes sizígias:

$$\mathfrak{z}_{1,2} = (-xy,\, x^2,\, 0), \quad \mathfrak{z}_{1,3} = (-y^2,\, 0,\, x^2), \quad \mathfrak{z}_{2,3} = (0,\, -y^2,\, xy).$$

Portanto, temos

$$\langle \mathfrak{z}_{1,2}, \mathfrak{z}_{1,3}, \mathfrak{z}_{2,3} \rangle \subseteq \mathrm{Syz}_G(I).$$

Entretanto, diferentemente dos exemplos anteriores, essas sizígias de Koszul não geram todo o módulo de sizígias. De fato, considere $q = (-y,\, x,\, 0)$. Temos que

$$(-y) \cdot x^2 + x \cdot xy + 0 \cdot y^2 = -x^2y + x^2y = 0,$$

logo $q \in \mathrm{Syz}_G(I)$. Contudo, diferentemente do exemplo anterior, essas sizígias de Koszul não geram todo o módulo de sizígias. Por exemplo,

$$q = (-y, x, 0)$$

é uma sizígia de I, pois

$$(-y)x^2 + (x)xy + (0)y^2 = -x^2y + x^2y = 0.$$

No entanto, q não pode ser escrito como uma combinação linear das sizígias de Koszul.

Suponha, por contradição, que q pertença ao submódulo gerado pelas sizígias de Koszul. Então, existiriam polinômios $\alpha, \beta, \gamma \in k[x, y]$ tais que:

$$q = \alpha \cdot \mathfrak{z}_{1,2} + \beta \cdot \mathfrak{z}_{1,3} + \gamma \cdot \mathfrak{z}_{2,3}$$

Escrevendo a primeira coordenada desta equação, teríamos:

$$-y = \alpha(-xy) + \beta(-y^2) + \gamma(0) = -\alpha xy - \beta y^2.$$

Isso implica que $\alpha x + \beta y = 1$, em particular, os termos independentes em ambos os lados devem ser iguais, donde seguiria que $1 = 0$, o que é um absurdo. Assim, concluímos que

$$\mathrm{Syz}_G(I) \subsetneq \langle \mathfrak{z}_{1,2}, \mathfrak{z}_{1,3}, \mathfrak{z}_{2,3} \rangle,$$

isto é, as sizígias de Koszul não são suficientes para gerar todo o módulo de sizígias neste caso.

Exemplo 4.1.4. Seja $R = k[x, y, z]$ um anel de polinômios em três variáveis com coeficientes em um corpo k e I o ideal gerado pelo conjunto $G = \{yz, xz, xy\}$.Vamos calcular um conjunto de geradores para o módulo de sizígias $\mathrm{Syz}_G(I)$. Primeiro consideramos o homomorfismo

$$\phi : R^3 \twoheadrightarrow I, \quad e_1 \mapsto yz, \quad e_2 \mapsto xz, \quad e_3 \mapsto xy,$$

o qual, para um $(a, b, c) \in R^3$ arbitrário, é dado por

$$\phi(a, b, c) = ayz + bxz + cxy.$$

Observemos que

$$-x \cdot yz + y \cdot xz + 0 \cdot xy = 0 \quad \text{e} \quad 0 \cdot yz - y \cdot xz + z \cdot xy = 0.$$

Concluímos então dessas duas igualdades que $\mathfrak{z}_1 = (-x, y, 0)$ e $\mathfrak{z}_2 = (0, -y, z)$ pertencem a $\mathrm{Syz}_G(I)$. Em particular,

$$\langle \mathfrak{z}_1, \mathfrak{z}_2 \rangle \subseteq \mathrm{Syz}_G(I).$$

Iremos mostrar aqui que esta inclusão é uma igualdade. Para isso, considere $\mathfrak{z} = (a, b, c) \in \mathrm{Syz}_G(I)$. Então, $ayz + bxz + cxy = 0$. Equivalentemente,

$$ayz = -x(bz + cy) \tag{4.5}$$

Como x é elemento primo de R segue que

$$a = px \tag{4.6}$$

para algum $p \in R$. Substituindo essa expressão de a em (4.5) e efetuando os devidos cancelamentos obtemos $pyz = -bz - cy$. Mas, essa igualdade pode ser reescrita como

$$bz = -y(pz + c) \tag{4.7}$$

Dessa igualdade e da primalidade de y em R segue que

$$b = qy \tag{4.8}$$

para algum $q \in R$. Substituindo essa expressão de b em (4.7) e efetuando cancelamentos obtemos $qz = -pz - c$, ou seja,

$$c = -(q + p)z. \tag{4.9}$$

Assim, das equações (4.6), (4.8) e (4.9) obtemos:

$$\mathfrak{z} = (a, b, c) = (px, qy, -(q + p)z) = -p\mathfrak{z}_1 - q\mathfrak{z}_2$$

Logo, $\mathfrak{z} \in \langle \mathfrak{z}_1, \mathfrak{z}_2 \rangle$. Portanto,

$$\mathrm{Syz}_G(I) = \langle \mathfrak{z}_1, \mathfrak{z}_2 \rangle.$$

Exemplo 4.1.5. Seja $R = k[x, y, z]$ um anel de polinômios em três variáveis com coeficientes em um corpo k e I o ideal gerado pelo conjunto $G = \{x, y, z\}$. Vamos calcular um conjunto de geradores para o módulo de sizígias $\mathrm{Syz}_G(I)$. Primeiro consideramos o homomorfismo

$$\phi : R^3 \twoheadrightarrow I, \quad e_1 \mapsto x, \quad e_2 \mapsto y, \quad e_3 \mapsto z,$$

o qual, para um $(a, b, c) \in R^3$ arbitrário, é dado por

$$\phi(a, b, c) = ax + by + cz.$$

Observemos que

$$0 \cdot x - z \cdot y + y \cdot z = 0, \quad -z \cdot x + 0 \cdot y + x \cdot z = 0 \quad \text{e} \quad -y \cdot x + x \cdot y + 0 \cdot z = 0.$$

Concluímos então dessas três igualdades que $\mathfrak{z}_1 = (0, -z, y)$, $\mathfrak{z}_2 = (-z, 0, x)$ e $\mathfrak{z}_3 = (-y, x, 0)$ pertencem a $\mathrm{Syz}_G(I)$. Em particular,

$$\langle \mathfrak{z}_1, \mathfrak{z}_2, \mathfrak{z}_3 \rangle \subseteq \mathrm{Syz}_G(I).$$

Iremos mostrar que esta inclusão é uma igualdade. Para isso, considere $\mathfrak{z} = (a, b, c) \in \mathrm{Syz}_G(I)$. Então, $ax + by + cz = 0$. Equivalentemente,

$$ax = -by - cz \tag{4.10}$$

Como $\langle y, z \rangle$ é um ideal primo em R e $x \notin \langle y, z \rangle$, a equação (4.10) implica que $a \in \langle y, z \rangle$. Assim, existem polinômios $p, q \in R$ tais que

$$a = py + qz. \tag{4.11}$$

Substituindo essa expressão de a na relação de sizígia original, temos $(py + qz)x + by + cz = 0$. Reorganizando os termos, obtemos

$$y(px + b) = -z(qx + c). \tag{4.12}$$

Como y e z são elementos primos distintos em R, a igualdade (4.12) implica que y deve dividir

$(qx + c)$. Portanto, existe um polinômio $r \in R$ tal que

$$qx + c = ry. \tag{4.13}$$

Substituindo (4.13) em (4.12), temos $y(px + b) = -z(ry)$. Como R é um domínio, podemos cancelar y para obter $px + b = -rz$. Agora, podemos expressar b e c em termos de p, q, r:

$$b = -px - rz \tag{4.14}$$

$$c = ry - qx \tag{4.15}$$

Reunindo as equações (4.11), (4.14) e (4.15), temos:

$$\begin{aligned} \mathfrak{z} = (a, b, c) &= (py + qz, -px - rz, ry - qx) \\ &= r(0, -z, y) - q(-z, 0, x) - p(-y, x, 0) \\ &= r\mathfrak{z}_1 - q\mathfrak{z}_2 - p\mathfrak{z}_3. \end{aligned}$$

Logo, $\mathfrak{z} \in \langle \mathfrak{z}_1, \mathfrak{z}_2, \mathfrak{z}_3 \rangle$. Portanto,

$$\mathrm{Syz}_G(I) = \langle \mathfrak{z}_1, \mathfrak{z}_2, \mathfrak{z}_3 \rangle.$$

Para qualquer ideal I gerado por um conjunto $G = \{f_1, \ldots, f_m\}$ em um anel comutativo R, sempre existem as chamadas *sizígias de Koszul*, construídas a partir da comutatividade do produto $f_i f_j = f_j f_i$. Em alguns casos, essas sizígias são suficientes para gerar todo o módulo de sizígias. A saber, no exemplo (4.1.2), o qual o ideal

$$I = \langle x, y \rangle \subseteq K[x, y],$$

tem o módulo de sizígias gerado exatamente pela sizígia de Koszul $(-y, x)$. Todavia, em outros casos, as sizígias de Koszul não bastam. Isso ocorre, como vimos no exemplo (4.1.3), para o ideal

$$I = \langle x^2, xy, y^2 \rangle \subseteq K[x, y],$$

em que o módulo de sizígias contém elementos como

$$q = (-y, x, 0) \quad \text{e} \quad w = (0, -y, x),$$

os quais não pertencem ao submódulo gerado apenas pelas sizígias de Koszul. Nesse caso, é necessário adicionar geradores extras para descrever $\mathrm{Syz}_G(I)$ por completo. Sistemas computacional especializados, como o *Macaulay2*, são projetados exatamente para este fim. Utilizando implementações do *Algoritmo de Buchberger* para calcular uma *Base de Gröbner* do ideal, o Macaulay2 pode determinar de forma algorítmica um conjunto de geradores para o módulo de sizígias.

4.2 Sequências Exatas

As sequências exatas constituem uma ferramenta central na álgebra comutativa, permitindo descrever a relação entre diferentes módulos através de homomorfismos encadeados.

Definição 4.2.1. Uma sequência de homomorfismos de R-módulos

$$\cdots \longrightarrow M_{i+1} \xrightarrow{d_i} M_i \xrightarrow{d_{i-1}} M_{i-1} \longrightarrow \cdots$$

é chamada de *sequência exata* se, para todo i, tivermos

$$\mathrm{Im}(d_i) = \mathrm{Ker}(d_{i-1}).$$

Isso significa que, em cada termo da sequência, a imagem do homomorfismo que chega nele coincide com o núcleo do homomorfismo que sai dele.

Sejam M e N R-módulos.

O símbolo $M \longrightarrow 0$ representa o homomorfismo nulo de M para o módulo nulo, que envia todo elemento de M para 0. Já $0 \longrightarrow M$ representa o único homomorfismo possível do módulo nulo para M, que envia 0 em 0.

Uma sequência do tipo $M \xrightarrow{\varphi} N \longrightarrow 0$ é exata no ponto N se, e somente se, φ é sobrejetiva. De fato, a exatidão nesse ponto significa que $\mathrm{Im}(\varphi) = \mathrm{Ker}(0)$, mas o núcleo do homomorfismo $N \longrightarrow 0$ é o próprio N, logo $\mathrm{Ker}(0) = N$, e portanto $\mathrm{Im}(\varphi) = N$.

Uma sequência do tipo $0 \longrightarrow M \xrightarrow{\varphi} N$ é exata no ponto M se, e somente se, φ é injetiva. De fato, a exatidão nesse ponto exige que $\mathrm{Im}(0) = \mathrm{Ker}(\varphi)$, mas a imagem do homomorfismo $0 \longrightarrow M$ é o conjunto $\{0\}$, logo a condição se reduz a $\mathrm{Ker}(\varphi) = \{0\}$.

4.3 Sequências Exatas Curtas

Definição 4.3.1. Sejam M, N, P R-módulos. Dizemos que:

A sequência exata $0 \longrightarrow M \xrightarrow{d_1} N \xrightarrow{d_0} P$ é chamada de *sequência exata curta à esquerda*. Neste caso, a exatidão no primeiro termo significa que d_1 é injetiva.

A sequência exata $M \xrightarrow{d_1} N \xrightarrow{d_0} P \longrightarrow 0$ é chamada de *sequência exata curta à direita*. A exatidão no último termo implica que d_0 é sobrejetiva.

A sequência exata $0 \longrightarrow M \xrightarrow{d_1} N \xrightarrow{d_0} P \longrightarrow 0$ é chamada de *sequência exata curta*. Aqui, a exatidão no primeiro termo garante que d_1 é injetiva, e a exatidão no último termo garante que d_0 é sobrejetiva. Além disso, a exatidão no termo do meio implica que $\mathrm{im}(d_1) = \ker(d_0)$.

Exemplo 4.3.2. Seja M um R-módulo e N um R-submódulo de M. A sequência

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$$

é uma *sequência exata curta*. Aqui, i é o homomorfismo inclusão $i(n) = n$, que é claramente injetivo; já π é a projeção canônica $\pi(m) = m + N$, que é sobrejetiva porque toda classe $m + N$ tem representante em M. A exatidão em N significa que $\mathrm{Im}(0) = \mathrm{Ker}(i)$, o que é verdadeiro; pois, $\mathrm{Ker}(i) = \{0\}$; a exatidão em M significa que $\mathrm{Im}(i) = \mathrm{Ker}(\pi)$, e de fato $\mathrm{Ker}(\pi) = N$; e, por fim, a exatidão em M/N significa que $\mathrm{Im}(\pi) = \mathrm{Ker}(0) = M/N$.

Teorema 4.3.3. *Seja*

$$0 \longrightarrow M_n \xrightarrow{d_{n-1}} M_{n-1} \longrightarrow \cdots \xrightarrow{d_1} M_1 \xrightarrow{d_0} M_0 \longrightarrow 0$$

uma sequência exata de K-espaços vetoriais de dimensão finita. Então,

$$\sum_{i=0}^{n} (-1)^i \dim(M_i) = 0.$$

Demonstração. A sequência é exata, logo, para cada i temos: $\mathrm{Im}(d_i) = \mathrm{Ker}(d_{i-1})$, em que, por convenção, d_{-1} e d_n são os homomorfismos nulos das extremidades. Pelo Teorema do Núcleo e Imagem para espaços vetoriais, sabemos que:

$$\dim(M_i) = \dim(\mathrm{Ker}(d_i)) + \dim(\mathrm{Im}(d_i)).$$

Substituindo $\mathrm{Im}(d_i) = \mathrm{Ker}(d_{i-1})$, obtemos:

$$\dim(M_i) = \dim(\mathrm{Ker}(d_i)) + \dim(\mathrm{Ker}(d_{i-1})).$$

Agora, somamos essa igualdade para $i = 0, 1, \ldots, n$. O termo $\dim(\mathrm{Ker}(d_{i-1}))$ com $i > 0$ aparece novamente como $\dim(\mathrm{Ker}(d_i))$ na linha seguinte, fazendo com que a soma de todas as linhas produza cancelamentos simétricos. Nas extremidades, $\mathrm{Ker}(d_{-1}) = M_0$ e $\mathrm{Ker}(d_n) = M_n$, já que os mapas das extremidades são nulos. Com essa contagem, ao reorganizar os termos, obtemos exatamente $\dim(M_0) - \dim(M_1) + \dim(M_2) - \cdots + (-1)^n \dim(M_n) = 0$. Ou seja,

$$\sum_{i=0}^{n} (-1)^i \dim(M_i) = 0.$$

□

4.4 Resoluções Livres

As resoluções livres são ferramentas fundamentais na álgebra comutativa. A ideia central é descrever um módulo como um quociente de um módulo livre, e depois descrever o núcleo desse quociente também como um quociente de um módulo livre, e assim por diante.

Definição 4.4.1. Seja M um R-módulo. Uma *resolução livre* de M é uma sequência exata de R-módulos

$$F_o : \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \longrightarrow 0$$

em que cada F_i é R-módulo livre. F_o é finita se F_i é diferente de zero somente para uma quantidade finita de índices i.

Proposição 4.4.2. *Todo R-módulo admite uma resolução livre.*

Demonstração. Seja M um R-módulo. Vamos construir uma resolução livre de M.

Construção de F_0 e do mapa $F_0 \to M$. Escolha um conjunto gerador $S = \{m_i \mid i \in I\}$ de M. Defina

$$F_0 = \bigoplus_{i \in I} Re_i,$$

o R-módulo livre com base $\{e_i \mid i \in I\}$. Defina $\varphi_0 : F_0 \to M$ por $\varphi_0(e_i) = m_i$. Como S gera M, φ_0 é sobrejetivo.

Construção de F_1 e do mapa $F_1 \to F_0$. Considere $\ker(\varphi_0)$. Temos a sequência exata curta

$$0 \longrightarrow \ker(\varphi_0) \longrightarrow F_0 \xrightarrow{\varphi_0} M \longrightarrow 0.$$

Escolha um conjunto gerador $T = \{x_j \mid j \in J\}$ de $\ker(\varphi_0)$ e defina

$$F_1 = \bigoplus_{j \in J} Rf_j,$$

o R-módulo livre com base $\{f_j \mid j \in J\}$. Defina $\varphi_1 : F_1 \to F_0$ por $\varphi_1(f_j) = x_j$.

Continuação do processo. Repetimos o procedimento: para $\ker(\varphi_1)$, escolhemos um conjunto gerador e construímos um módulo livre F_2 com um mapa $\varphi_2 : F_2 \to F_1$. Continuando indefinidamente, obtemos

$$\cdots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0.$$

Por construção, cada F_i é livre e a sequência é exata em todos os termos. Portanto, M admite uma resolução livre. □

Exemplo 4.4.3. Seja o ideal $I = (x^2, xy)$ no anel $R = k[x, y]$, em que k é um corpo. Uma resolução livre de I é dada por

$$0 \longrightarrow R \xrightarrow{(y,-x)} R^2 \xrightarrow{(x^2,\,xy)} I \longrightarrow 0,$$

em que o módulo R^2 é livre, gerado pelos vetores $(1, 0)$ e $(0, 1)$, que correspondem aos geradores x^2 e xy de I. O mapeamento $R^2 \longrightarrow I$ envia $(1, 0) \mapsto x^2$ e $(0, 1) \mapsto xy$. Assim, sua matriz associada é $(x^2,\, xy)$. O mapeamento $R \longrightarrow R^2$ é dado pela matriz $(y, -x)$, que traduz a relação

$y \cdot x^2 = -x \cdot xy$ ou, equivalentemente,

$$y \cdot x^2 - x \cdot xy = 0.$$

Essa relação é precisamente a primeira *sizígia* entre os geradores de I. Dessa forma, a sequência acima é exata, e os módulos envolvidos são livres, caracterizando uma resolução livre de I.

Capítulo 5

Considerações Finais

O presente trabalho teve como principal objetivo introduzir as ferramentas fundamentais da álgebra comutativa necessárias para o estudo das sizígias. Nos Capítulos 1 e 2, exploramos as estruturas de anéis, ideais e anéis residuais, que servem de alicerce para a construção de conceitos mais complexos. A seguir, no Capítulo 3, avançamos para a teoria de módulos, com foco especial nos módulos livres e nos módulos noetherianos, que são categorias essenciais para a compreensão das relações entre geradores.

No Capítulo 4, o conceito central de sizígia foi formalmente definido como a relação linear não trivial entre os geradores de um módulo. Demonstramos que o módulo de sizígias atua como uma medida do quão distante um módulo está de ser livre, oferecendo uma visão mais profunda de sua estrutura interna. Concluímos nossa análise com o conceito de resoluções livres e provamos que todo módulo possui uma resolução livre. As resoluções livres são ferramentas poderosas que permitem decompor a complexidade de um módulo em uma sequência de módulos livres mais simples.

Em suma, este trabalho estabeleceu a base teórica para a compreensão da estrutura de um módulo para além de seu conjunto de geradores. O estudo das sizígias e das resoluções livres oferece um ponto de partida crucial para investigações futuras em áreas como a geometria algébrica, no qual a complexidade das relações entre geradores é um tema central.

Bibliografia

[1] ARTIN, M. *Algebra*. 2nd ed. Boston: Pearson, 2011.

[2] BRUNS, W.; HERZOG, J. *Cohen-Macaulay Rings*. Cambridge Studies in Advanced Mathematics, v. 60. Cambridge University Press, 1993.

[3] CLARK, A. *Elements of Abstract Algebra*. Reprint of the 1971 edition. Dover Publications, New York, 1984.

[4] EISENBUD, D. *Commutative Algebra with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics, v. 150. Springer-Verlag, New York, 1995.

[5] EISENBUD, D. *The Geometry of Syzygies: A Second Course in Commutative Algebra and Algebraic Geometry*. Graduate Texts in Mathematics, v. 229. Springer-Verlag, New York, 2005.

[6] HERZOG, J.; HIBI, T. *Monomial Ideals*. Graduate Texts in Mathematics, v. 260. Springer, London, 2010.

[7] KEMPER, G. *A Course in Commutative Algebra*. Graduate Texts in Mathematics, v. 256. Springer, 2011.

[8] MATSUMURA, H. *Commutative Ring Theory*. Cambridge University Press, 1986.

[9] SIMIS, A. *Commutative Algebra*. De Gruyter Textbook, 2020.