UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Livea Cichito Esteves

Uma introdução à teoria de Galois sobre anéis comutativos e aplicações

São José do Rio Preto
2020

Livea Cichito Esteves

Uma introdução à teoria de Galois sobre anéis comutativos e aplicações

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Financiadora: CAPES

São José do Rio Preto
2020

E79i

Esteves, Livea Cichito

Uma introdução à teoria de Galois sobre anéis comutativos e aplicações / Livea Cichito Esteves. -- São José do Rio Preto, 2020

104 f.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto

Orientador: Antonio Aparecido de Andrade

1. Módulo. 2. Álgebra semi-simples. 3. Álgebra separável. 4. Teoria de Galois. 5. Códigos sobre anéis. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Livea Cichito Esteves

Uma introdução à teoria de Galois sobre anéis comutativos e aplicações

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Financiadora: CAPES

Comissão Examinadora

Prof. Dr. Antonio Aparecido de Andrade
UNESP – Câmpus de São José do Rio Preto
Orientador

Prof. Dr. Edson Donizete de Carvalho
UNESP – Câmpus de Ilha Solteira

Profª. Drª. Carina Alves Severo
UNESP – Câmpus de Rio Claro

São José do Rio Preto
28 de fevereiro de 2020

Aos meus pais, Maria Ines e João Carlos
e ao meu irmão, Rafael.

AGRADECIMENTOS

No decorrer de todo o mestrado e na elaboração desta dissertação tive o apoio de várias pessoas que foram fundamentais para realização deste sonho, e por isso quero expressar aqui a minha gratidão.

Agradeço primeiramente a Deus, por me dar saúde, força e sabedoria para superar os momentos de dificuldade.

Ao meu orientador, Toninho, por toda paciência e dedicação em me orientar e pelos valiosos ensinamentos.

Aos membros da comissão examinadora, Prof. Dr. Edson Donizete de Carvalho e Prof.ª Dr.ª Carina Alves Severo, por aceitarem o convite e pelas valiosas contribuições ao trabalho.

Aos meus amigos do mestrado, pelos momentos de descontração que tornaram a caminhada mais leve e por estarem sempre dispostos a ajudar.

Aos meus pais, João Carlos e Maria Ines, e ao meu irmão, Rafael, por todo amor, apoio e carinho em todos os momentos.

Ao meu namorado, Murilo, por estar sempre comigo mesmo quando longe, me animando, incentivando e encorajando, além de todo amor e carinho.

A todos que direta ou indiretamente contribuíram na realização deste trabalho.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, a qual agradeço.

Sábio é o ser humano que tem coragem de ir diante do espelho da sua alma para reconhecer seus erros e fracassos e utilizá-los para plantar as mais belas sementes no terreno de sua inteligência.

Augusto Cury

RESUMO

O principal objetivo deste trabalho é apresentar a teoria de Galois sobre anéis comutativos, exibindo uma definição adequada para uma extensão de anéis ser galoisiana, de modo que esta seja uma generalização natural da definição conhecida da teoria de Galois sobre corpos. Além disso, é apresentado sob quais condições resultados importantes da teoria de corpos, como o teorema da correspondência de Galois, são válidos neste caso. Por último, é feita uma investigação acerca dos códigos sobre o anel $\mathbb{Z}_m$ via anel de grupos utilizando as propriedades das álgebras semi-simples.

Palavras-chave: Módulo, Álgebra semi-simples, Álgebra separável, Teoria de Galois, Códigos sobre $\mathbb{Z}_m$.

ABSTRACT

The aim of the present work is to present the Galois theory of commutative rings, showing a proper definition for an extension of rings to be galoisian, so that it is a natural generalization of the known definition of Galois theory of fields. Furthermore, is presented under which conditions important results of field theory, as the classical Galois correspondence theorem, are valid in this case. In the last part, we made a investigation about the codes over the ring $\mathbb{Z}_m$ by groups ring using the properties of semisimple algebras.

Keywords: Module, Semisimple algebra, Separable algebra, Galois theory, Codes over $\mathbb{Z}_m$.

Sumário

Introdução

A teoria de Galois sobre corpos tem grande importância na álgebra e em outras áreas da matemática e é possível encontrar muitos estudos sobre esta teoria na literatura atual. Como na matemática sempre somos tentados a generalizar os resultados, com esta teoria não foi diferente, e desse modo, começaram a surgir os seguintes questionamentos:

1. Será que é possível criar uma teoria consistente como a teoria de Galois para corpos pensando em um anel comutativo qualquer?

2. Quais as especificidades que o anel em questão deve ter?

Responder a essas questões é o principal objeto do presente trabalho.

Ao considerar anéis, diferentemente de quando se considera corpos, um estudo pode serguir várias vertentes distintas, pois existem várias classificações para os anéis. É possível estudar a teoria de Galois sobre anéis não comutativos, sobre anéis de divisão, anéis de característica p, entre outros. Para este trabalho, nós escolhemos os anéis comutativos.

A primeira definição de extensão galoisiana de um anel apareceu na literatura em 1960 no trabalho "The Brauer group of a commutative ring" de M. Auslander e O. Goldman. Mas a teoria de Galois para anéis comutativos surgiu a partir de 1965 como parte de um trabalho de S.U Chase, D.K. Harrison e A. Rosenberg intitulado "Galois Theory and Galois Cohomology of Commutative Rings", onde foram apresentadas outras definições equivalentes para uma extensão galoisiana de anéis dada por Auslander e Goldman, além de conter resultados importantes, inclusive um Teorema Fundamental para esta teoria.

Sendo assim, o principal objetivo deste trabalho é apresentar uma definição apropriada para que uma extensão de anéis seja de Galois de modo que esta definição seja uma generalização natural da teoria de Galois para corpos e que os principais resultados, como por exemplo, o Teorema Fundamental da Teoria de Galois, que estabelece uma correspondência entre os corpos intermediários e os subgrupos do grupo de Ga-

lois, também possa ser estendido para o caso dos anéis. Para isso, iremos apresentar algumas das definições equivalentes de extensão galoisiana de corpos existentes na literatura e analisar se é possível adaptar os conceitos abordados ao contexto dos anéis, sempre evidenciando as semelhanças e as diferenças entre as teorias e as perdas que a substituição de um corpo para um anel comutativo acarretam. Além disso, salvo menção contrária, os anéis considerados neste trabalho serão sempre comutativos com unidade.

A presente dissertação está dividida em cinco capítulos, onde os dois primeiros contém todo o embasamento teórico sobre anéis, módulos e álgebras necessários para a compreensão dos demais capítulos.

No primeiro, é feita uma revisão sobre a teoria de módulos, explorando mais profundamente assuntos como o produto tensorial, módulos projetivos e módulos semi-simples que serão de suma importância para o desenvolvimento do próximo capítulo. Este capítulo também foi escrito com o intuito de servir como base e auxílio a estudantes que estejam iniciando seus estudos no assunto de módulos.

O segundo capítulo é dividido em três seções. A primeira seção apresenta a definição de álgebra e alguns exemplos, além de conter a definição do produto tensorial entre álgebras, propriedade que será muito utilizada. Na segunda seção o foco está nas álgebras semi-simples sobre um corpo, onde todo o trabalho é feito com o objetivo de dar uma caracterização a elas através do famoso Teorema de Wedderburn. Por último, exploramos as álgebras separáveis, que serão apresentadas por meio de duas abordagens distintas, uma que envolve extensão de corpos e semi-simplicidade e outra que pode ser generalizada para anéis quaisquer. Este será um dos conceitos mais importantes na generalização da teoria de Galois.

No terceiro capítulo, o mais importante deste trabalho, relembramos um pouco dos fatos mais relevantes da teoria de Galois sobre corpos e em seguida vamos preparando o terreno para enfim chegarmos à generalização que queríamos, onde são demonstradas cinco definições equivalentes para uma extensão de anel ser galoisiana, que junto com a adaptação e a demonstração do teorema fundamental, integra a parte principal deste trabalho. Também são dados alguns exemplos de extensões galoisiana de anéis a fim de que haja um melhor esclarecimento. A referência [16] foi a principal utilizada neste capítulo, e a riqueza de detalhes nas demonstrações e exemplos constituem a principal contribuição deste trabalho.

O quarto capítulo é dedicado à análise da estrutura e construção de códigos sobre $\mathbb{Z}_m$, onde m é um inteiro qualquer. Estas construções utilizam fortemente os conceitos e resultados de álgebra semi-simples apresentadas no segundo capítulo, de modo que esta parte é uma aplicação desta teoria. Primeiramente, é feita a construção para

o caso onde m é o produto de primos distintos, que torna-se mais simples pelo fato de que nestas condições a álgebra de grupo $\mathbb{Z}_m G$, onde G é um grupo cíclico, é semi-simples. Em seguida, utilizando o Teorema de Wedderburn, adaptamos estes resultados para o caso onde m é uma potência de um primo, e uma vez que estes dois casos estão resolvidos, conseguimos encontrar códigos sobre $\mathbb{Z}_m$, onde m é qualquer inteiro positivo.

No último capítulo, foi feita uma revisão geral do trabalho, apontando as principais conclusões e perspectivas futuras.

1 Anéis e módulos

Este capítulo aborda definições e resultados importantes sobre módulos, destacando alguns casos particulares, como módulos livres, módulos projetivos, módulos simples e semi-simples, que serão úteis no decorrer do texto. Também, apresentamos uma construção detalhada do produto tensorial para módulos e exibimos alguns dos mais importantes radicais de um anel. Os anéis considerados neste capítulo serão sempre comutativos. As definições e os resultados apresentados neste capítulo baseiam-se essencialmente em [4], [12], [14] e [15].

1.1 Módulos

Nesta seção, introduzimos a noção de módulo, que trata-se de uma generalização de espaço vetorial, onde a multiplicação por escalar é definida sobre um anel, ao invés de ser definida sobre um corpo como nos espaços vetoriais.

Veremos ao longo do presente texto como a perda de características básicas, como o fato de que todo elemento é inversível, no conjunto escalar, acarreta em diversas mudanças na estrutura, fazendo com que algumas propriedades que funcionam bem nos espaços vetoriais deixem de valer nesse caso mais geral.

Definição 1.1. *Sejam R um anel e M um conjunto não vazio. Se M é grupo abeliano em relação à adição e está definida uma operação externa que a cada par $(a, m) \in R \times M$ associa o elemento $am \in M$ e de modo que para todo $a, b \in A$ e para todo $x, y \in M$ são válidas as condições*

i) $a(bx) = (ab)x$,

ii) $a(x + y) = ax + ay$,

iii) $(a + b)x = ax + bx$, *e*

iv) $1x = x$,

M é dito um ***R-módulo*** *à esquerda.*

Observação 1.2. Considerando a multiplicação por escalar à direita, define-se de forma análoga um R-módulo à direita. Quando o anel R é comutativo não existe distinção entre módulos à direita e módulos à esquerda. Nesse trabalho, a menos de menção contrária, consideramos um R-módulo à esquerda.

Exemplo 1.3. Seja K um corpo. Todo K-espaço vetorial é um K-módulo.

Exemplo 1.4. Todo anel R pode ser visto como um R-módulo. Além disso, o produto direto $R^n = R \times R \times ... \times R$ de um anel R é um R-módulo.

Exemplo 1.5. Para todo $n \in \mathbb{Z}$, o anel $n\mathbb{Z}$ é um $\mathbb{Z}$-módulo.

Definição 1.6. *Sejam M um R-módulo e $N \subseteq M$ um subconjunto não vazio. Dizemos que N é um R-**submódulo** de M se N é um subgrupo aditivo de M e é fechado em relação ao produto por escalar. Na maioria das vezes, por simplicidade, dizemos apenas que N é um submódulo de M e denotamos como $N \leq M$.*

Sejam M um R-módulo e N um R-submódulo de M. No grupo quociente M/N definimos a seguinte operação: $a(m + N) = am + N$, onde $a \in R$ e $m \in M$. Com essa operação, M/N tem uma estrutura de um R-módulo que recebe o nome de **módulo quociente** de M por N.

Sabemos que todo espaço vetorial possui uma base, entretanto, a mesma afirmação não se estende para os módulos. Um R-módulo M pode nem sequer possuir um gerador, por exemplo, $4\mathbb{Z}$ visto como um $2\mathbb{Z}$-módulo não possui um conjunto de geradores. Por esta razão, módulos com essas propriedades são especiais, como veremos a seguir.

Definição 1.7. *Sejam um R-módulo M e $S \subseteq M$ um subconjunto não vazio. O conjunto*

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} a_i s_i : a_i \in R, s_i \in S \right\}$$

é um R-submódulo de M chamado de submódulo gerado por S, sendo o menor submódulo de M que contém S.

Sempre que escrevermos $\langle S \rangle$, estamos nos referindo ao conjunto gerado por S. Se $\langle S \rangle = M$, dizemos que S gera M e sendo S finito, ou seja, $S = \{s_1, s_2, \ldots, s_n\}$, dizemos que M é finitamente gerado. Além disso, se S for linearmente independente, isto é, se $\sum_{i=1}^{n} a_i s_i = 0$ implicar que $a_i = 0$, para $i = 1, \ldots, n$, dizemos que S forma uma base para M, e neste caso, M é chamado de **módulo livre**.

Definição 1.8. *Sejam M e N dois R-módulos. Uma função $f : M \longrightarrow N$ é um **homomorfismo** de R-módulos se satisfaz:*

$$f(am_1 + m_2) = af(m_1) + f(m_2),$$

para todo $a \in R,\ m_1, m_2 \in M$.

Um submódulo importante de M, chamado **Kernel** de f, é definido como $\mathrm{Ker}(f) = \{x \in M : f(x) = 0_N\}$. A **imagem** de f é definida como $\mathrm{Im}(f) = \{f(x) : x \in M\}$, e é um submódulo de N. Ao conjunto de todos os homomorfismos de R-módulos M em N, denotamos por $\mathrm{Hom}_R(M, N)$, que também é um R-módulo.

Naturalmente, a partir da definição de um homomorfismo de R-módulos, segue o seguinte Teorema do Homomorfismo para R-módulos.

Teorema 1.9. *Se M e N são dois R-módulos, $f : M \to N$ um homomorfismo de R-módulos, $j : M \to M/Ker(f)$ a função projeção e $i : Im(f) \to N$ a inclusão, então existe uma única função $f^* : M/Ker(f) \to Im(f)$ tal que*

1. $f = i \circ f^* \circ j$,
2. f^* *é um isomorfismo.*

Demonstração. A aplicação

$$\begin{array}{rccl} f^* : & M/\mathrm{Ker}(f) & \to & \mathrm{Im}(f) \\ & x + \mathrm{Ker}(f) & \mapsto & f^*(x + \mathrm{Ker}(f)) = f(x), \end{array}$$

está bem definida e é bijetora, donde segue que f^* é um isomorfismo de R-módulos. Também, f^* satisfaz a igualdade $f = i \circ f^* \circ j$. □

Definição 1.10. *Sejam $\{M_i\}_{i \in I}$ uma família de R-módulos e $f_i \in Hom_R(M_i, M_{i+1})$, para todo $i \in I$. Dizemos que a sequência*

$$\ldots M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \longrightarrow \ldots$$

é ***exata*** *em M_{i+1} se $Im(f_i) = Ker(f_{i+1})$. Se a sequência for exata em M_i para todo i, dizemos simplesmente que a sequência é exata.*

Exemplo 1.11. Sejam R um anel, M um R-módulo e N um R-submódulo de M. Considere sequência $0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$, onde i é a função inclusão e π é a projeção canônica dada por $\pi(m) = m + N$. Essa sequência é exata, pois i é injetora, π é sobrejetora e $\mathrm{Im}(i) = N = \mathrm{Ker}(\pi)$.

Dados N_1, N_2 dois R-submódulos de um R-módulo M, podemos definir um novo R-submódulo dado por:

$$N_1 + N_2 = \{n_1 + n_2 : n_1 \in N_1, n_2 \in N_2\}.$$

A representação dos elementos de $N_1 + N_2$ nem sempre é única. De fato, se $N_1 = N_2 = 4\mathbb{Z} \leq \mathbb{Z}$ como $\mathbb{Z}$-módulos, então $16 = 4 + 12 = 8 + 8$. Assim, quando a representação é única? Isso acontece quando $N_1 \cap N_2 = \{0\}$, e nesse caso, denotamos por $N_1 \oplus N_2$. Quando $N_1 + N_2 = M$ e $N_1 \cap N_2 = \{0\}$, dizemos que M é a **soma direta** de N_1 e N_2, e denotamos, $M = N_1 \oplus N_2$.

Este conceito estende-se para uma família qualquer $\{N_i\}_{i\in I}$ de R-submódulos de M, e nesse caso, M é a soma direta de $\{N_i\}_{i\in I}$, se satisfazer uma das seguintes afirmações equivalentes

i) Todo elemento $m \in M$ se escreve de maneira única na forma $m = \sum_{i\in I} n_i$, onde $n_i \in N_i$ e $(n_i)_{i\in I}$ é uma família quase nula, isto é, $n_i = 0$, exceto para um número finito de elementos;

ii) $M = \sum_{i\in I} N_i$ e se $\sum_{i\in I} n_i = 0$, então $n_i = 0$, para todo $i \in I$;

iii) $M = \sum_{i\in I} N_i$ e $N_j \cap (\sum_{i\neq j} N_i) = \{0\}$.

Também, a partir de dois R-módulos M e N, considerando

$$M \times N = \{(x, y), \quad \text{onde} \quad x \in M, y \in N\}$$

com as operações

1. $(x, y) + (x', y') = (x + x', y + y')$, e
2. $a(x, y) = (ax, ay)$,

o conjunto $M \times N$ possui estrutura de um R-módulo, chamado de **produto cartesiano** de M e N. Mais geralmente, dada uma família de R-módulos $\{M_i\}_{i\in I}$, podemos definir seu produto cartesiano

$$\prod_{i\in I} M_i = \{(m_i)_{i\in I} : m_i \in M_i, \quad \text{para todo} \quad i \in I\}.$$

Denotando por $\dot{\otimes}_{i\in I} M_i$ o conjunto das famílias quase-nulas de $\prod_{i\in I} M_i$, e considerando as mesmas operações, o conjunto $\dot{\otimes}_{i\in I} M_i$ é chamado de **produto direto** da família $\{M_i\}_{i\in I}$. Observe que quando o conjunto de índices I for finito, os dois R-módulos coincidem, ou seja, o produto direto e o produto cartesiano coincidem.

Definição 1.12. *Seja N um submódulo de um R-módulo M. Dizemos que um submódulo $N_1 \subseteq M$ é um* ***suplementar*** *de N em M se $M = N \oplus N_1$. Se N admite suplementar, N é dito somando direto de M.*

Embora essa propriedade seja válida para todo subespaço de um espaço vetorial, para módulos não podemos afirmar o mesmo, ou seja, nem todo submódulo possui um suplementar e mesmo quando possui, a unicidade não é garantida, motivo pelo qual usamos "um suplementar" na Definição 1.12.

Proposição 1.13. *Seja M um R-módulo. Se N_1 e N_2 são dois submódulos de M tal que $M = N_1 \oplus N_2$, então $M/N_1 \cong N_2$.*

Demonstração. Dado $x \in M$, por hipótese, existem $n_1 \in N_1$ e $n_2 \in N_2$ tal que $x = n_1 + n_2$. Considere a função projeção sobre a segunda coordenada, que é o epimorfismo

$$\begin{array}{rccc} p: & M & \to & N_2 \\ & x & \mapsto & n_2. \end{array}$$

Pelo Teorema 1.9, segue que $M/\mathrm{Ker}(p) = N_2$. Como $\mathrm{Ker}(p) \cong N_1$, segue que $M/N_1 \cong N_2$. □

Agora, vamos analisar algumas relações entre somas diretas e sequências exatas. Dados dois R-módulos M_1, M_2, a sequência $0 \longrightarrow M_1 \xrightarrow{i_1} M_1 \oplus M_2 \xrightarrow{p_2} M_2 \longrightarrow 0$, onde $i_1(m_1) = (m_1, 0)$ é a inclusão natural, e $p_2(m_1, m_2) = m_2$ é a projeção sobre a segunda coordenada, é uma sequência exata. Mas, dada uma sequência exata qualquer, $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$, será que sempre temos que $F = E \oplus G$? No que segue tentamos responder a essa questão.

Definição 1.14. *Uma sequência exata de R-módulos $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$* ***cinde*** *se $Im(f) = Ker(g)$ é um somando direto de F.*

Pelo Teorema 1.9, segue que $\mathrm{Im}(f) \cong E/\mathrm{Ker}(f) = E$, e uma vez que f é injetora, podemos dizer que a sequência exata da Definição 1.14 cinde se E é um somando direto de F. Também, é possível mostrar que seu suplementar é isomorfo a G, ou seja, pela sequência exata $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$, segue que $G \cong F/\mathrm{Ker}(g)$, pois g é sobrejetora. Além disso, da igualdade $F = E' \oplus E''$, pela Proposição 1.13, segue que $E'' \cong F/E' = F/\mathrm{Ker}(g)$. Portanto, $E'' \cong G$. Feito isso podemos responder ao nosso questionamento, ou seja, será que sempre temos que $F = E \oplus G$? Isso nem sempre ocorre, mas quando acontece dizemos que a sequência cinde.

Proposição 1.15. *Seja $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$ uma sequência exata. As seguintes afirmações são equivalentes:*

i) *A sequência cinde;*

ii) *Existe um homomorfismo $\psi : F \longrightarrow E$ tal que $\psi \circ f = 1_E$;*

iii) *Existe um homomorfismo* $\phi : G \longrightarrow F$ *tal que* $g \circ \phi = 1_G$.

Demonstração. **i)** $\Rightarrow$ **ii)** Como por hipótese a sequência cinde, segue que existe E'' tal que $F = E' \oplus E''$ e $E' = \mathrm{Im}(f)$. Assim, se $x \in F$, então $x = x' + x''$, para únicos $x' \in E'$ e $x'' \in E''$ e se $x' \in E'$, então existe um único $y \in E$ tal que $f(y) = x'$, uma vez que f é injetora. Assim, podemos definir o seguinte homomorfismo:

$$\begin{array}{rccc} \psi : & F & \to & E \\ & x & \mapsto & y. \end{array}$$

Desse modo, $(\psi \circ f)(y) = \psi(f(y)) = \psi(x') = y$, isto é, existe um homomorfismo $\psi : F \longrightarrow E$ tal que $\psi \circ f = 1_E$.

ii) $\Rightarrow$ **i)** Devemos mostrar que a sequência $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$ cinde, isto é, que existe E'' tal que $F = \mathrm{Im}(f) \oplus E''$. Vamos mostrar que $E'' = \mathrm{Ker}(\psi)$ satisfaz essa condição, onde ψ é o homomorfismo da hipótese. Para isso, seja $x \in F$. Considere $y = (f \circ \psi)(x) = f(\psi(x))$ e tome $z = x - y \Rightarrow x = y + z$. Como $y \in \mathrm{Im}(f)$, segue que $z \in \mathrm{Ker}(\psi)$, uma vez que $\psi(z) = \psi(x - y) = \psi(x) - \psi(y) = \psi(x) - (\psi \circ f \circ \psi)(x) = 0$. Agora, verificamos que a soma é direta. Se $a \in \mathrm{Im}(f) \cap \mathrm{Ker}(\psi)$, então $a \in \mathrm{Im}(f)$ e $a \in \mathrm{Ker}(\psi)$. Assim, existe $x \in E$ tal que $f(x) = a$. Como $a \in \mathrm{Ker}(\psi)$, segue que $\psi(y) = 0 \Rightarrow \psi(f(x)) = 0 \Rightarrow x = 0$. Logo, $f(0) = a = 0$. Portanto, $F = \mathrm{Im}(f) \oplus \mathrm{Ker}(\psi)$, ou seja, a sequência cinde.

i) $\Rightarrow$ **iii)** Para mostrar que essa implicação é válida, precisamos definir um homomorfismo $\phi : G \longrightarrow F$ tal que $g \circ \phi = 1_G$. Seja $u \in G$. Como g é sobrejetora, segue que existe $v \in F$ tal que $g(v) = u$. Por hipótese, podemos escrever $F = E' \oplus E''$. Assim, se $v \in F$, então $v = x' + x''$, onde $x' \in E'$ e $x'' \in E''$. Como $x' \in E' = \mathrm{Im}(f)$, segue que existe $x \in E$ tal que $f(x) = x'$. Para mostrar que o homomorfismo está bem definido, devemos mostrar que dado $u \in G$ existe um único $x'' \in E''$ tal que $g(x'') = u$. A existência segue do fato que $u = g(v) = g(f(x) + x'') = g(f(x)) + g(x'') \overset{\mathrm{Im}(f)=\mathrm{Ker}(g)}{=} g(x'')$. Para a unicidade, suponhamos que existam $x'', y'' \in E''$ tal que $g(x'') = u = g(y'')$. Assim, $g(x'' - y'') = 0 \Rightarrow x'' - y'' \in \mathrm{Ker}(g) = \mathrm{Im}(f)$. Logo, $x'' - y'' \in E'' \cap \mathrm{Im}(f) = \{0\}$, ou seja, $x'' = y''$. Assim, podemos definir o homomorfismo

$$\begin{array}{rccc} \phi : & G & \to & F \\ & u & \mapsto & x''. \end{array}$$

Logo, $(g \circ \phi)(u) = g(\phi(u)) = g(x'') = u$, ou seja, $g \circ \phi = 1_G$.

iii) $\Rightarrow$ **i)** Agora, vamos mostrar que $F = \mathrm{Im}(f) \oplus \mathrm{Im}(\phi)$. Se $x \in F$, então po-

demos escrever $x = x - \phi(g(x)) + \phi(g(x))$, onde $x - \phi(g(x)) \in \mathrm{Im}(f) = \mathrm{Ker}(g)$, pois $g(x - \phi(g(x))) = g(x) - g(\phi(g(x))) \overset{g\circ\phi=1_G}{=} g(x) - g(x) = 0$, e desse modo, $\phi(g(x)) \in \mathrm{Im}(\phi)$. Além disso, a soma é direta, pois supondo que $a \in \mathrm{Im}(f) \cap \mathrm{Im}(\phi)$, segue que existe $x \in G$ tal que $a = \phi(x)$ e como $a \in \mathrm{Im}(f) = \mathrm{Ker}(g)$, segue que $g(a) = 0$, ou seja, $g(\phi(x)) = 0$. Como $(g \circ \phi) = 1_G$, segue que $x = 0$. Portanto, $a = 0$, e assim, $F = \mathrm{Im}(f) \oplus \mathrm{Im}(\phi)$, ou seja, a sequência cinde. □

A seguir, veremos uma sequência de proposições envolvendo sequência exata e módulos livres que será muito útil na Seção 3 deste capítulo ao provar as equivalências para módulo projetivo e que também usamos para provar alguns fatos sobre R-módulos particulares, por exemplo, quando R é um domínio principal.

Proposição 1.16. *Todo R-módulo M é isomorfo a um quociente de um R-módulo livre.*

Demonstração. Seja $\{m_i\}_{i\in I}$ um conjunto de geradores de M (note que este conjunto de geradores sempre existe, pois pelo menos o próprio M o é). Podemos definir a aplicação

$$\begin{array}{rccc} f: & R^I & \to & M \\ & a & \mapsto & \displaystyle\sum_{i=1}^{n} a_i m_i, \end{array}$$

onde $R^I = \bigoplus_{i\in I} R_i$, com $R_i = R$, para todo $i \in I$. A aplicação f é um homomorfismo e f é sobrejetora, pois $\{m_i\}_{i\in I}$ gera M. Logo, pelo Teorema 1.9, segue que $M \cong R^I/\mathrm{Ker}(f)$. O anel R pode sempre ser visto como um R-módulo e este é livre pois $\{1_R\}$ é uma base. O produto direto R^I também é livre, pois $B = \{e_k\}$, onde $e_k = (x_i)_{i\in I}$, $x_k = 1_R$ e $x_i = 0$, para todo $i \neq k$, é uma base de R^I. Portanto, M é isomorfo a um quociente do R-módulo livre R^I, como queríamos. Se M for livre, isto é, se $\{m_i\}_{i\in I}$ for uma base de M, então f é injetora, e assim, $M \cong \oplus R^I$, para algum conjunto I. Para o caso em que I é finito e $\{m_1, m_2, \ldots, m_k\}$ é um conjunto de geradores, segue que $M \cong R^k/\mathrm{Ker}(f)$. Em geral, k não é único, pois depende da quantidade de elementos da base que tomamos, que pode variar em anéis não comutativos. Mas, como aqui assumimos que o anel é comutativo, segue que k é único. □

Proposição 1.17. *Seja L um R-módulo livre. Se M e N são dois R-módulos, $f : M \longrightarrow N$ um epimorfismo e $g : L \longrightarrow N$ um homomorfismo, então existe um homomorfismo $\bar{g} : L \longrightarrow M$ tal que $f \circ \bar{g} = g$.*

Demonstração. Seja $\{x_i\}_{i\in I}$ uma base de L. Como f é sobrejetora, segue que existe $m_i \in M$ tal que $f(m_i) = g(x_i)$, para todo $i \in I$. Definindo $\bar{g}(x_i) = m_i$ para os elementos da base, podemos estender ao homomorfismo $\bar{g}(m) = \sum \lambda_i m_i$, onde $m = \sum \lambda_i x_i$ é um elemento de M. Assim, $f \circ \bar{g} = g$, o que prova o resultado. □

Proposição 1.18. *Se L é um R-módulo livre e $f : M \longrightarrow L$ um epimorfismo, então $M = Ker(f) \oplus L$.*

Demonstração. Consideramos a sequência exata

$$\begin{array}{ccccccccc} & & & & L & & & & \\ & & & & \vdots h & \searrow^{id_L} & & & \\ 0 & \longrightarrow & \mathrm{Ker}(f) & \xrightarrow[i]{} & M & \xrightarrow[f]{} & L & \longrightarrow & 0. \end{array}$$

Se mostrarmos que esta sequência cinde, segue que $M = \mathrm{Ker}(f) \oplus L$. Para isso consideramos o homomorfismo id_L. Podemos ver com o auxílio do diagrama que estamos nas hipóteses da Proposição 1.17, e portanto, existe um homomorfismo $h : L \longrightarrow M$ tal que $f \circ h = id_L$. Desta forma, pela Proposição 1.15, segue que a sequência cinde, isto é, que $M = \mathrm{Ker}(f) \oplus L$. □

Corolário 1.19. *Seja $0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0$ uma sequência exata de R-módulos. Se L é livre, então a sequência cinde.*

Demonstração. Através do diagrama

$$\begin{array}{ccccccccc} & & & & L & & & & \\ & & & & \vdots h & \searrow^{id_L} & & & \\ 0 & \longrightarrow & M & \longrightarrow & N & \xrightarrow[f]{} & L & \longrightarrow & 0 \end{array}$$

segue que este resultado é uma consequência direta das Proposições 1.17 e 1.15. □

A partir daqui até o final dessa seção analisamos alguns fatos sobre os R-módulos M, onde R é um domínio de integridade. Para o último teorema, precisamos também da hipótese extra de que R é principal.

Proposição 1.20. *Sejam R domínio e M um R-módulo. Se $\{x_i\}_{1 \leq i \leq n}$ é linearmente independente em M e $\{y_i\}_{1 \leq j \leq m}$ é um conjunto gerador de M, então $n \leq m$.*

Demonstração. Como $\{y_i\}_{1 \leq j \leq m}$ é um gerador de M, segue que cada x_i pode ser escrito da forma $x_i = \sum_{j=1}^{m} a_{ij} y_j$, com $a_{ij} \in A$, para $1 \leq i \leq n$. Considere a expressão $\sum_{i=1}^{n} \lambda_i x_i = 0$. Substituindo x_i, segue que

$$0 = \sum_{i=1}^{n} \lambda_i \left(\sum_{j=1}^{m} a_{ij} y_j \right) = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \lambda_i a_{ij} \right) y_j.$$

Seja o sistema $\sum_{i=1}^{n} \lambda_i a_{ij} = 0$, onde $j = 1, 2, \ldots, m$. Vamos supor que $n > m$ e que as soluções do sistema de n variáveis e m equações estão no corpo de frações de R. Como

$n > m$, segue que esse sistema admite uma solução não trivial, mas isso contraria o fato de $\{x_i\}_{1\leq i\leq n}$ ser linearmente independente. Portanto, $n \leq m$. □

Teorema 1.21. *Se R é domínio e M é um R-módulo finitamente gerado, então todas as bases de M tem o mesmo número de elementos.*

Demonstração. Sejam $B_1 = \{x_i\}_{i=1}^{n_1}$ e $B_2 = \{y_j\}_{j=1}^{n_2}$ duas bases de M. Como B_1 é linearmente independente e B_2 é um gerador de M, pela Proposição 1.20, segue que $n_1 \leq n_2$. Mas também, B_2 é linearmente independente e B_1 é um gerador, que implica que $n_2 \leq n_1$. Portanto, $n_1 = n_2$. □

Definição 1.22. *Dado M um R-módulo finitamente gerado, chamamos de **posto** de M ao número de elementos de uma base de M.*

Para o próximo resultado, precisamos assumir que R é um domínio principal. Antes, vejamos através de um exemplo, que o resultado não vale em geral. Seja o $\mathbb{Z}_6$-módulo livre $\mathbb{Z}_6$, onde $\{\bar{1}\}$ é uma base. O submódulo $H = \{\bar{0}, \bar{3}\}$ não é livre, pois $\bar{3}$ é linearmente dependente, uma vez que $\bar{3}.\bar{2} = \bar{0}$.

Teorema 1.23. *Se M é um R-módulo livre de posto n, onde R é um domínio principal, então todo submódulo de M é livre com posto menor ou igual a n.*

Demonstração. Faremos a prova por indução sobre n, o posto de M. Se $n = 1$, então M tem uma base com um elemento, e suponhamos que essa base é $\{u\}$. Definindo $f : A \longrightarrow M$ por $f(a) = au$, onde $a \in A$, segue que f é um homomorfismo bijetivo (direto do fato de $\{u\}$ ser base), e assim, $R \cong M$. Como R é principal, segue que os submódulos de R (que coincidem com os ideais de R) são livres de posto 1, com exceção do módulo nulo que por convenção tem posto 0. Suponhamos, agora, que a afirmação vale para todo módulo com posto menor que n, e com isso provamos que vale para M com posto n. Se $\{v_i\}_{i=1,\ldots,n}$ é uma de base M, então, todo elemento $m \in M$ se escreve de maneira única na forma $m = \sum_{i=1}^{n} a_i v_i$, com $a_i \in A$. Considere o isomorfismo $f : M \longrightarrow A^{(n)}$ dado por $f(m) = (a_1, \ldots, a_n)$. Considere, também, $\bar{f} : M \longrightarrow A$, onde $\bar{f} = p_1 \circ f$, sendo p_1 a projeção na primeira coordenada, ou seja, $\bar{f}(m) = a_1$. Seja N um submódulo de M. Podemos definir $f_N : N \longrightarrow A$, onde $f_N = \bar{f}|_N$, e assim, obtemos a sequência exata

$$0 \longrightarrow \mathrm{Ker}(f) \xrightarrow{i} N \xrightarrow{f_N} \mathrm{Im}(f_N) \longrightarrow 0.$$

Como $\mathrm{Im}(f_N) \subseteq A$, segue que $\mathrm{Im}(f_N)$ é livre, e assim, pelo Corolário 1.19, segue que a sequência cinde. Portanto, $N = \mathrm{Im}(f_N) \oplus \mathrm{Ker}(f_N)$. Se M_1 é um submódulo de M gerado

por $\{v_2, \ldots, v_n\}$, então M_1 é livre e $\mathrm{Ker}(f_N) \subseteq M_1$. De fato, se $x = \sum_{i=1}^{n} \lambda_i v_i \in \mathrm{Ker}(f_N)$, então

$$f_N(x) = 0 \Rightarrow \bar{f}(x) = 0 \Rightarrow (p_1 \circ f)(x) = 0 \Rightarrow \lambda_1 = 0 \Rightarrow x = \sum_{i=2}^{n} \lambda_i v_i.$$

Pela hipótese de indução, segue que todo submódulo de M_1, portanto $\mathrm{Ker}(f_N)$, é livre com posto menor ou igual a $n-1$. Assim, N é livre de posto menor ou igual a n. □

1.2 Produto tensorial

Nesta seção, definimos uma aplicação bilinear para módulos e apresentamos um caso particular dessas aplicações que será muito importante para o nosso trabalho, o produto tensorial.

Definição 1.24. *Sejam M, N, T três A-módulos. Uma aplicação $f : M \times N \longrightarrow T$ é chamada bilinear, se para todo $m_1, m_2 \in M, n_1, n_2 \in N$ e $a \in A$, vale as seguintes propriedades:*

1. $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$;
2. $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$;
3. $f(am, n) = f(m, an) = af(m, n)$.

Em outras palavras, uma aplicação f é bilinear se f for linear em relação à primeira e à segunda variável.

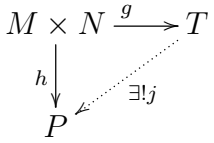
Agora, apresentamos uma construção do produto tensorial, que é dada a partir de uma propriedade universal para módulos. Nas funções, em geral, não podemos afirmar que valem as propriedades listadas na Definição 1.24. O produto tensorial é uma aplicação onde essas propriedades são satisfeitas. Assim, é natural que usemos algum tipo de quociente, pois necessitamos que muitas operações nessa estrutura resulte em zero.

Teorema 1.25. *Se M e N são dois R-módulos, então existe um par (T, g), onde T é um R-módulo e $g : M \times N \longrightarrow T$ é uma função bilinear satisfazendo:*

1. *Para todo R-módulo P e para toda aplicação bilinear $h : M \times N \longrightarrow P$, existe um único homomorfismo $j : T \longrightarrow P$ tal que h se fatora via g, isto é, $j \circ g = h$.*

2. *O par* (T, g) *é único a menos de isomorfismo, ou seja, se existe* (T', g') *que também satisfaz* (1)*, então existe um isomorfismo de* R*-módulos* $f : T \longrightarrow T'$ *tal que* $f \circ g = g'$*.*

Com o auxílio do diagrama



é mais fácil ver a situação imposta pelo Teorema, ou seja, partindo de uma função bilinear h*, sempre existe* (T, g) *de modo que existe um único* j *que faz o diagrama comutar.*

Demonstração. (1) Para a existência, considere o produto cartesiano $M \times N$ e C um R-módulo livre gerado por (a, b), com $a \in M, b \in N$, ou seja,

$$C = R^{M\times N} = \left\{ \sum_{finito} \lambda_i(a_i, b_i) : \lambda_i \in R \; a_i \in M, b_i \in N \right\}.$$

Definimos a soma entre elementos de C e a multiplicação por escalar sobre R como segue:

i) $\sum \lambda_i(a_i, b_i) + \sum \gamma_i(a_i, b_i) = \sum(\lambda_i + \gamma_i)(a_i, b_i)$;

ii) $\lambda \sum \lambda_i(a_i, b_i) = \sum \lambda\lambda_i(a_i, b_i)$.

Com estas operações, C é um R-módulo. Consideramos D um submódulo de C gerado pelos elementos de C da seguinte maneira:

- $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$;
- $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$;
- $(\lambda a, b) - \lambda(a, b)$;
- $(a, \lambda b) - \lambda(a, b)$.

Agora, consideramos o conjunto quociente C/D. Neste conjunto, segue que

- $\overline{(a_1 + a_2, b)} - \overline{(a_1, b)} - \overline{(a_2, b)} = \overline{0}$,
- $\overline{(a, b_1 + b_2)} - \overline{(a, b_1)} - \overline{(a, b_2)} = \overline{0}$,

- $\overline{(\lambda a, b)} - \lambda\overline{(a, b)} = \overline{0}$ e
- $\overline{(a, \lambda b)} - \lambda\overline{(a, b)} = \overline{0}$.

Denotamos a classe representada pelo par (a, b) por $a \otimes b := (a, b) + D$. Assim, pela forma que definimos esse conjunto, segue que

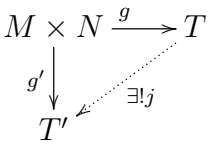
- $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$;
- $a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$;
- $\lambda a \otimes b = \lambda(a \otimes b) = a \otimes \lambda b$.

Agora, defina $T := C/D$ e $g : M \times N \longrightarrow T$ tal que $g(a, b) = a \otimes b$, onde (a, b) são elementos básicos de C. Assim, T é gerado por $a \otimes b$. Além disso, pela construção, segue que g é bilinear. Agora, resta apenas mostrar que T e g definidos dessa maneira satisfazem o item (1). Para isso, dada a função bilinear $h : M \times N \longrightarrow P$, segue que h pode ser estendida a uma função $\bar{h} : C \longrightarrow P$, uma vez que os elementos de $M \times N$ formam uma base para C. Como h é bilinear, segue que $\bar{h}$ se anula em todos os geradores de D, ou seja,

$$\begin{aligned} \bar{h}((a_1 + a_2, b) - (a_1, b) - (a_2, b)) &= h((a_1 + a_2, b) - (a_1, b) - (a_2, b)) \\ &= h((a_1, b) + (a_2, b) - (a_1, b) - (a_2, b)) \\ &= h(0) = 0. \end{aligned}$$

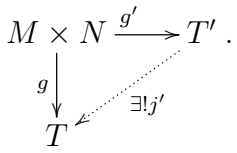
De modo análogo, segue que vale para todos os geradores de D, e portanto, vale em todo D. Assim, $D \subseteq \mathrm{Ker}(\bar{h})$. Portanto, h induz um homomorfismo $h' : T \longrightarrow P$ tal que $h'(a \otimes b) = h(a, b)$. Mostramos, agora, que h' está bem definida. Para isso, se $a \otimes b = a' \otimes b'$, então $(a, b) - (a', b') \in D$. Como $\bar{h}|_D = 0$, segue que $h'((a, b) - (a', b')) = 0$, ou seja, $h'(a, b) = h'(a', b')$. Tomando $h' = j$, segue que $j \circ g = h$, uma vez que $j \circ g(a, b) = j(a \otimes b) \overset{h'=j}{=} h(a, b)$. Além disso, h' é unicamente definida por esta condição. Portanto, o par (T, g) satisfaz o item (1).

(2) Para a unicidade, suponhamos que (T, g) e (T', g') são dois pares que satisfazem o item (1). Tomando $P = T'$ e $h = g'$ obtemos a situação representada pelo diagrama



onde pelo item (1), segue que existe um único homomorfismo j tal que $j \circ g = g'$. De modo análogo, para T', como por hipótese T' também satisfaz o item (1), segue que

existe um único homomorfismo j' tal que $j' \circ g' = g$, como representado no diagrama.



A partir dessas construções, segue que:

i) $j' \circ g' = g$ implica que $j' \circ j \circ g = g$, ou seja, $j' \circ j = id_T$;

ii) $j \circ g = g'$ implica que $j \circ j' \circ g' = g'$, ou seja, $j \circ j' = id_T$.

Por **i**) e **ii**), segue que $j : T \to T'$ é um isomorfismo que satisfaz $j \circ g = g'$, e portanto, o par (T, g) é único a menos de isomorfismo, o que prova a unicidade. □

O módulo T, assim definido, é chamado **produto tensorial** entre M e N e é denotado por $M \otimes_R N$, ou simplesmente, por $M \otimes N$ quando estiver claro qual o anel da operação. Por construção, segue que $M \otimes N$ é gerado por $a \otimes b$, onde $a \in M, b \in N$, ou seja, os elementos de $M \otimes N$ são da forma

$$\sum_{finito} \lambda_i(a_i \otimes b_i) = \sum_{finito} (\lambda_i a_i) \otimes b_i = \sum_{finito} a_i \otimes (\lambda_i b_i).$$

Exemplo 1.26. Considerando $\mathbb{Z}$ e $\mathbb{Z}_n$ vistos como $\mathbb{Z}$-módulos, segue que $\mathbb{Z} \otimes \mathbb{Z}_n \cong \mathbb{Z}_n$.

Exemplo 1.27. Se $\text{mdc}(m, n) = 1$, então $\mathbb{Z}_n \otimes \mathbb{Z}_m = 0$. De fato, como m e n são coprimos, segue que existem $r, s \in \mathbb{Z}$ tal que $mr + ns = 1$. Se $a \otimes b$ é um gerador de $\mathbb{Z}_n \otimes \mathbb{Z}_m$, então

$$\begin{aligned} a \otimes b &= 1(a \otimes b) = (mr + ns)(a \otimes b) = ((mr)a + (ns)a) \otimes b \\ &= mr(a) \otimes b + (ns)a \otimes b = mr(a) \otimes b + a \otimes ns(b) \\ &= 0 \otimes b + a \otimes 0 = 0 + 0 = 0. \end{aligned}$$

Como se anula nos geradores, segue que se anula em todo o conjunto, e portanto, $\mathbb{Z}_n \otimes \mathbb{Z}_m = 0$.

Tomando funções multilineares $f : M_1 \times \cdots \times M_r \to P$ ao invés de bilineares (as funções multilineares são definidas do mesmo modo que as bilineares, isto é, cada coordenada é linear), e seguindo os mesmos passos da prova do Teorema 1.25, obtemos o **produto multitensorial**

$$T = M_1 \otimes \cdots \otimes M_r,$$

gerado pelos elementos da forma $x_1 \otimes \cdots \otimes x_r$, onde $x_i \in M_i$, para todo $1 \leq i \leq r$. O resultado equivalente ao Teorema 1.25 para o produto multitensorial é dado pela próxima proposição.

Proposição 1.28. *Se $M_1, \ldots, M_r$ são R-módulos, então existe um par (T, g), onde T é um R-módulo e $g : M_1 \times \cdots \times M_r \to T$ é uma aplicação multilinear, satisfazendo:*

1. *Para todo R-módulo P e para toda aplicação multilinear $h : M_1 \times \cdots \times M_r \to P$, existe um único homomorfismo $j : T \to P$ tal que $j \circ g = h$.*

2. *O par (T,g) é único a menos de homomorfismo.*

Quando tensorizamos um R-módulo por um R-módulo que é também um anel, o produto tensorial ganha uma interpretação como mudança de base, isto é, mudamos o anel de escalares a partir da tensorização. Por exemplo, o anel de polinômios $\mathbb{R}[x]$ e $\mathbb{C}$ são $\mathbb{R}$-módulos. Tensorizando $\mathbb{C}$ por $\mathbb{R}[x]$, obtemos $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[x] \cong \mathbb{C}[x]$. O isomorfismo se dá pela função $\mathbb{R}$-bilinear $f : \mathbb{R}[x] \times \mathbb{C} \to \mathbb{C}[x]$, onde $f(p(x), z) = zp(x)$ que induz o isomorfismo $f : \mathbb{R}[x] \otimes \mathbb{C} \to \mathbb{C}[x]$ onde $f(p(x) \otimes z) = zp(x)$. Analogamente, se $L \supset K$ é uma extensão de corpos, então $K[x] \otimes_K L \cong L[x]$.

Vejamos, agora, alguns resultados envolvendo produto tensorial e sequências exatas.

Seja $f : M \longrightarrow N$ um homomorfismo de R-módulos. Dados P um R-módulo e $g : P \longrightarrow M$ um homomorfismo, a aplicação

$$\begin{array}{rccc} \hat{f} : & Hom_R(P, M) & \to & Hom_R(P, N) \\ & g & \mapsto & f \circ g \end{array}$$

é um homomorfismo. De forma análoga, dado $h \in Hom_R(N, P)$, a aplicação

$$\begin{array}{rccc} \bar{f} : & Hom_R(N, P) & \to & Hom_R(M, P) \\ & h & \mapsto & h \circ f \end{array} .$$

é um homomorfismo. Usando essas duas funções, obtemos a seguinte proposição:

Proposição 1.29. *Sejam M, M', M'' e P quatro R-módulos.*

i) *A sequência $M' \xrightarrow{g} M \xrightarrow{f} M'' \longrightarrow 0$ é exata $\Leftrightarrow$ a sequência $0 \longrightarrow Hom_R(M'', P) \xrightarrow{\bar{f}} Hom_R(M, P) \xrightarrow{\bar{g}} Hom_R(M', P)$ é exata, para todo R-módulo P.*

ii) *A sequência $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ é exata $\Leftrightarrow$ a sequência $0 \longrightarrow Hom_R(P, M') \xrightarrow{\hat{f}} Hom_R(P, M) \xrightarrow{\hat{g}} Hom_R(P, M'')$ é exata, para todo R-módulo P.*

Demonstração. **i**) : Suponhamos que $M' \xrightarrow{g} M \xrightarrow{f} M'' \longrightarrow 0$ é exata. Assim, $\mathrm{Im}(f) = \mathrm{Ker}(g)$ e g é sobrejetora. Falta mostrar que $\mathrm{Im}(\bar{g}) = \mathrm{Ker}(\bar{f})$ e que $\bar{g}$ é injetora.

- $\bar{g}$ injetora: Por definição, $\bar{g} = h \circ g$. Se $h \in \mathrm{Ker}(\bar{g})$, então $\bar{g}(h) = 0 \Rightarrow h \circ g = 0 \Rightarrow h(g(m)) = 0$, para todo $m \in M$. Como g é sobrejetora, segue que $g(M) = M''$. Logo, $h(M'') = 0 \Rightarrow h \equiv 0$, e portanto, $\bar{g}$ é injetora.

- $Im(\bar{g}) \subseteq \mathrm{Ker}(\bar{f})$: Se $u \in Im(\bar{g})$, então existe $h \in \mathrm{Hom}_R(M'', P)$ tal que $\bar{g}(h) = u \Rightarrow h \circ g = u$. Assim, $\bar{f}(u) = u \circ f = h \circ g \circ f \overset{\mathrm{Ker}(g)=Im(f)}{=} h \circ 0 = 0$, uma vez que $g \circ f = 0$.

- $\mathrm{Ker}(\bar{f}) \subseteq \mathrm{Im}(\bar{g})$: Seja $u \in \mathrm{Ker}(\bar{f})$. Queremos mostrar que $u \in \mathrm{Im}(\bar{g})$, isto é, que existe $h \in \mathrm{Hom}_R(M'', P)$ tal que $\bar{g}(h) = u$. Considere $h(m'') = u(m)$, onde $h \circ g(m) = m''$. Observe que como g é sobrejetora, segue que dado m'', este m sempre existe. Também, a função está bem definida: suponhamos que exista $m_1, m_2 \in M$ tal que $m'' = g(m_1) = g(m_2)$. Logo, $m_1 - m_2 \in \mathrm{Ker}(g) = \mathrm{Im}(f)$, e então, existe $m' \in M'$ tal que $f(m') = m_1 - m_2$, e assim, $u \circ f(m') = u(m_1 - m_2)$. Como $u \in \mathrm{Ker}(\bar{f})$, segue que $\bar{f}(u) = u \circ f = 0$, e assim, $u(m_1 - m_2) = 0 \Rightarrow u(m_1) = u(m_2)$. Além disso, h é homomorfismo, uma vez que f e g também são homomorfismos. Portanto, $\mathrm{Im}(\bar{g}) = \mathrm{Ker}(\bar{f})$.

  Agora, provamos a recíproca.

- g sobrejetora: Para isso, vamos usar o fato que $g : X \to Y$ é sobrejetora $\Leftrightarrow h \circ g = f \circ g \Rightarrow h = f$, para todo $f, h : Y \to Z$ (*). Suponhamos que existam $f, h : M'' \to P$ tal que $f \circ g = h \circ g$, ou seja, $\bar{g}(f) = \bar{g}(h)$. Como $\bar{g}$ é injetora, segue que $f = h$. Portanto, por (*), segue que g é sobrejetora.

- $Im(f) \subseteq \mathrm{Ker}(g)$: Como $\mathrm{Im}(\bar{g}) = \mathrm{Ker}(\bar{f})$ segue que $\bar{f} \circ \bar{g} = 0$. Logo, $u \circ g \circ f = 0$, para toda função $u : M'' \to P$. Tomando $P = M''$ e $u = \mathrm{Id}$, segue que $g \circ f = 0$. Logo, $\mathrm{Im}(f) \subset \mathrm{Ker}(g)$.

- $\mathrm{Ker}(g) \subseteq Im(f)$: Sejam $P = \frac{M}{Im(f)}$ e $\pi : M \to P$ a projeção canônica. Assim, $\bar{f}(\pi(m')) = (\pi \circ f)(m') = f(m') + Im(f) = 0$, para todo $m' \in M$. Logo, $\pi \in \mathrm{Ker}(\bar{f}) = Im(\bar{g})$, ou seja, existe $u : M'' \to P$ tal que $\pi = \bar{g}(u) = u \circ g \Rightarrow \mathrm{Ker}(g) \subseteq Im(f)$.

ii) Segue de modo análogo ao item i). □

Observemos que $\mathrm{Hom}_R(M \otimes N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$. Dada $f : M \times N \longrightarrow P$ uma aplicação bilinear, pelo Teorema 1.25, segue que f induz $\bar{f} : M \otimes N \longrightarrow P$. Para

cada $m \in M$, a aplicação $f_m : N \longrightarrow P$ é definida por $f_m(n) = f(x, n)$ que pertence a $\mathrm{Hom}_R(N, P)$, e assim, existe o homomorfismo $g : M \longrightarrow \mathrm{Hom}_R(N, P)$ definido por $g(m) = f_m$. Por outro lado, dada uma aplicação $g : M \longrightarrow \mathrm{Hom}_R(N, P)$, segue que a aplicação $\bar{g} : M \times N \longrightarrow P$ dada por $\bar{g}(m, n) = g(m)(n)$ é bilinear, pelo Teorema 1.25, segue que existe uma aplicação $f : M \otimes N \longrightarrow P$.

Dados M, N, P três R-módulos e $f : M \longrightarrow N$ um homomorfismo de R-módulos, seja a aplicação $g : M \times P \longrightarrow N \oplus P$ definida por $g(m, p) = f(m) \times p$. A aplicação g é -bilinear, e assim, pelo Teorema 1.25, segue que existe um homomorfismo $\bar{f} : M \otimes P \longrightarrow N \otimes P$ de R-módulos dado por $m \otimes p = f(m) \otimes p$. A aplicação $\bar{f}$ é denotada por $f \otimes id$. Assim, obtemos a seguinte proposição:

Proposição 1.30. *Seja P um R-módulo. Se a sequência $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ é exata, então a sequência $M' \otimes P \xrightarrow{f \otimes id} M \otimes P \xrightarrow{g \otimes id} M'' \otimes P \longrightarrow 0$ também é exata.*

Demonstração. Como a sequência é exata, pela Proposição 1.29, item i), segue que a sequência

$$0 \longrightarrow Hom_R(M'', N) \longrightarrow Hom_R(M, N) \longrightarrow Hom_R(M', N)$$

é exata, para todo R-módulo N. Assim, pela Proposição 1.29 item ii), segue que a sequência

$$0 \longrightarrow Hom_R(P, Hom_R(M'', N)) \longrightarrow Hom_R(P, Hom_R(M, N)) \longrightarrow Hom_R(P, Hom_R(M', N))$$

é exata para todo R-módulo P. Logo, a sequência

$$0 \longrightarrow Hom_R(P \otimes M'', N) \longrightarrow Hom_R(P \otimes M, N) \longrightarrow Hom_R(P \otimes M', N)$$

é exata. Assim, pela Proposição 1.29 item i), segue que a sequência

$$M' \otimes P \xrightarrow{f \otimes id} M \otimes P \xrightarrow{g \otimes id} M'' \otimes P \longrightarrow 0$$

é exata. □

Se a sequência $0 \longrightarrow M' \longrightarrow M \longrightarrow M''$ é exata, nem sempre podemos afirmar que a sequência $0 \longrightarrow M' \otimes P \longrightarrow M \otimes P \longrightarrow M'' \otimes P$ também é exata, como podemos ver através do próximo exemplo.

Exemplo 1.31. Seja a sequência $0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$, onde $f(x) = 2x$. A sequência $0 \longrightarrow \mathbb{Z} \otimes \mathbb{Z}_2 \xrightarrow{f \otimes id} \mathbb{Z} \otimes \mathbb{Z}_2$ não é exata, pois a injetividade não é mantida, uma vez que $f \otimes id(n \otimes \bar{a}) = 2n \otimes \bar{a} = n \otimes 2\bar{a} = 0$, para todo $n \in \mathbb{Z}$.

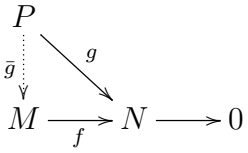
Definição 1.32. *Um R-módulo P é dito* ***plano*** *se para toda sequência exata $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, a sequência $0 \longrightarrow M' \otimes P \longrightarrow M \otimes P \longrightarrow M'' \otimes P \longrightarrow 0$ é exata.*

Através da Definição 1.32, segue que P é um R-módulo plano se, e somente se, para todo $f : M' \longrightarrow M$ homomorfismo, $f \otimes id : M' \otimes P \longrightarrow M \otimes P$ é injetiva, uma vez que a condição de ser exata é garantida pela Proposição 1.30.

1.3 Módulos projetivos

Nesta seção, apresentamos uma classe de módulos que é mais abrangente que a classe dos módulos livres, que são os módulos projetivos. Em geral, um submódulo de um R-módulo livre L, pode não ser livre e ser um somando direto de L. Mas sempre que o submódulo for livre, ele será um somando direto de L. É por isso que os módulos projetivos são uma generalização dos módulos livres.

Definição 1.33. *Um R-módulo P é chamado* ***projetivo****, se dados quaisquer R-módulos M, N, um epimorfismo $f : M \longrightarrow N$ e um homomorfismo $g : P \longrightarrow N$, existe um homomorfismo $\bar{g} : P \longrightarrow M$ tal que $f \circ \bar{g} = g$. Em outras palavras, P é projetivo se para todo diagrama*



existe homomorfismo $\bar{g}$ que faz com que o diagrama comute.

Um resultado importante sobre os módulos projetivos, que veremos na próxima proposição, é no sentido da caracterização dos mesmos, permitindo mostrar que um módulo é projetivo por meios que às vezes podem ser mais simples do que o apresentado na Definição 1.33.

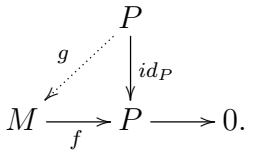
Proposição 1.34. *Seja P um R-módulo. As seguintes afirmações são equivalentes:*

i) *P é projetivo;*

ii) *se P é a imagem de um R-módulo M por um epimorfismo, então p é isomorfo a um somando direto de M;*

iii) *P é um somando direto de um R-módulo livre.*

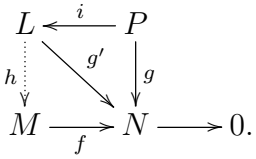
Demonstração. **i**) $\Rightarrow$ **ii**) Sejam P um R-módulo projetivo, M um R-módulo e $f : M \longrightarrow P$ um epimorfismo (existe pela hipótese). Utilizando o mesmo raciocínio usado da prova da Proposição 1.18, segue o diagrama



Como P é projetivo, segue que existe $g : P \longrightarrow M$ tal que $f \circ g = id_P$. Logo, pela Proposição 1.15, segue que a sequência exata $0 \longrightarrow \text{Ker}(f) \xrightarrow{i} M \xrightarrow{f} P \longrightarrow 0$ cinde, e portanto, P é um somando direto de M.

ii) $\Rightarrow$ **iii**) Pela Proposição 1.16, segue que todo R-módulo é a imagem de um R-módulo livre por um epimorfismo. Assim, dado um R-módulo P, segue que existe um epimorfismo $f : M \longrightarrow P$, onde M é livre. Por hipótese, P é isomorfo a um somando direto de M, isto é, existe N tal que $P \oplus N = M$, que é livre. Portanto, P é um somando direto de um R-módulo livre.

iii) $\Rightarrow$ **i**) Por hipótese, P é um somando direto de um R-módulo livre. Assim, existem um R-módulo livre L e um R-módulo S tal que $L = P \oplus S$. Sejam os R-módulos M e N, o epimorfismo $f : M \longrightarrow N$ e o homomorfismo $g : P \longrightarrow N$. Como $P \subseteq L$, podemos estender g a $g' : L \longrightarrow N$ definindo $g'(x) = g(x)$, para todo $x \in P$ e $g'(x) = 0$, para todo $x \in S$, que ainda será um homomorfismo. Como a soma $L = P \oplus S$ é direta, segue que dado $x \in L$ existem únicos $x_1 \in P, x_2 \in S$ tal que $x = x_1 + x_2$. Assim, $g(x) = g(x_1)$. Indicando por $i : P \longrightarrow L$ a inclusão, segue o diagrama:



Como L é livre, pela Proposição 1.17, segue que existe um homomorfismo $h : L \longrightarrow M$ tal que $f \circ h = g'$. Mas para mostrar que P é projetivo, devemos exibir um homomorfismo $\bar{h} : P \longrightarrow M$ tal que $f \circ \bar{h} = g$. Tomando $\bar{h} = h \circ i$ (h restrita a P), o resultado segue, isto é, $f \circ \bar{h} = g$, e portanto, P é projetivo. □

Exemplo 1.35. Sejam $R = \mathbb{Z}_6$, $P = \{\bar{0}, \bar{2}, \bar{4}\}$ e $Q = \{\bar{0}, \bar{3}\}$. Assim, P e Q são R-módulos e $R = P \oplus Q$, ou seja, P e Q são projetivos, pois são somandos diretos de R que é livre.

Exemplo 1.36. Sejam K um corpo, $R = M_2(K)$ e

$$P = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in K \right\} \text{ e } Q = \left\{ \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} : c, d \in K \right\}.$$

Assim, P e Q são submódulos de R, onde $R = P \oplus Q$. Logo, P e Q são projetivos visto que R é livre.

Utilizando a condição iii) da Proposição 1.34, veremos na próxima proposição uma outra definição equivalente, que usamos em determinados momentos no decorrer do texto.

Observação 1.37. Seja P um R-módulo projetivo. Como P é projetivo, segue que toda sequência exata de R-módulos do tipo $M \xrightarrow{\phi} P \to 0$ cinde. De fato, suponhamos que $M \xrightarrow{\phi} P \to 0$ é exata. Essa sequência se estende a uma outra sequência exata $0 \to N \to M \xrightarrow{\phi} P \to 0$, onde $N = \mathrm{Ker}(\phi)$. Pela Proposição 1.29 e pela definição de módulo projetivo, segue que $0 \to \mathrm{Hom}_R(P, N) \to \mathrm{Hom}_R(P, M) \xrightarrow{\phi^*} \mathrm{Hom}_R(P, P) \to 0$ é exata. Logo, dado $id_P \in \mathrm{Hom}_R(P, P)$, segue que existe $\psi \in \mathrm{Hom}_R(P, M)$ tal que $\phi^*(\psi) = id_P$, o que mostra que toda sequência $M \xrightarrow{\phi} P \to 0$ cinde.

Proposição 1.38. *Um R-módulo P é projetivo se, e somente se, existem elementos $p_i \in P$ e $f_i \in P^* = Hom_R(P, A)$, em que $i \in I$, tal que para todo $p \in P$, $p = \sum_i f_i(p)p_i$, onde $f_i(p) = 0$ exceto para um número finito de índices.*

Demonstração. Suponhamos que P é gerado por $\{p_i | i \in I\}$ como um R-módulo e seja L um R-módulo livre com base $\{e_i | i \in I\}$. Definimos o homomorfismo de R-módulos $\varphi : L \to P$ dado por $\varphi(e_i) = p_i$, para todo $i \in I$. Como a sequência $L \xrightarrow{\varphi} P \to 0$ é exata, segue pela Observação 1.37 que essa sequência cinde. Logo, existe $\delta : P \to L$ tal que $\varphi \circ \delta = id_P$. Seja $\pi_i : L \to R$ a projeção da i-ésima coordenada, isto é, $\pi\left(\sum_j \lambda_j e_j\right) = \lambda_i$, para todo $i \in I$. Definimos o homomorfismo $f_i : P \to R$ por $f_i = \pi_i \circ \delta$, para todo $i \in I$. Assim, dado $p \in P$, segue que

$$\delta(p) = \sum_{i \in I} \lambda_i e_i = \sum_{i \in I} f_i(p) e_i,$$

com $\lambda_i = f_i(p) = 0$ exceto para um número finito de índices, e portanto,

$$p = (\varphi \circ \delta)(p) = \varphi\left(\sum_{i \in I} f_i(p) e_i\right) = \sum_{i \in I} f_i(p)\varphi(e_i) = \sum_{i \in I} f_i(p) p_i.$$

Reciprocamente, sejam P um R-módulo e $p_i \in P$, $f_i \in P^*$ elementos que satisfazem a hipótese. Considere o R-módulo livre L gerado pela base $\{e_i : i \in I\}$ e $\varphi : L \to P$

o homomorfismo sobrejetor de R-módulos dado por $\varphi(e_i) = p_i$, para todo $i \in I$. Considere também o homomorfismo de R-módulos $\delta : P \to L$, onde $\delta(p) = \sum_{i\in I} f_i(p)e_i$. Observemos que $\varphi \circ \delta$ é um isomorfismo, uma vez que dado $p \in P$, segue que

$$(\varphi \circ \delta)(p) = \varphi\left(\sum_{i\in I} f_i(p)e_i\right) = \sum_{i\in I} f_i(p)\varphi(e_i) = \sum_{i\in I} f_i(p)p_i = p,$$

ou seja, $\varphi\circ\delta = id_P$ que é um isomorfismo. Logo, $L = \mathrm{Im}(\delta)\oplus\mathrm{Ker}(\varphi) = \delta(P)\oplus\mathrm{Ker}(\varphi)$. Mostramos, agora, que δ é injetiva. Seja $p = \sum_{i\in I} f_i(p)p_i$, com $f_i(p) = 0$ exceto para um número finito de índices, tal que $\delta(p) = 0$. Assim, $\sum_{i\in I} f_i(p)e_i = 0$. Como $\{e_i\}$ é uma base de L, segue que $f_i(p) = 0$, para todo $i \in I$, e desse modo, $p = 0$. Assim, pelo Teorema 1.9, segue que $P \cong \delta(P)$, ou seja, P é isomorfo a um somando direto de um módulo livre, o que conclui a prova de que P é projetivo. □

Definição 1.39. *Seja P um R-módulo. Dizemos que P é **projetivo finitamente gerado** se P é um somando direto de um R-módulo livre finitamente gerado.*

A seguir veremos alguns resultados que nos auxiliarão na prova de um dos teoremas principais deste trabalho.

Sejam P um R-módulo, $P^* = \mathrm{Hom}_R(P, R)$ e o homomorfismo de R-módulos dado por

$$\begin{array}{rccc} \phi: & P \otimes_R P^* & \to & Hom_R(P,P) \\ & \phi\left(\sum_{i=1}^{n} p_i \otimes f_i\right)(p) & = & \sum_{i=1}^{n} f_i(p)p_i, \end{array}$$

para todo $p \in P$.

O próximo teorema fornece uma condição necessária e suficiente para que esse homomorfismo seja bijetivo.

Teorema 1.40. *Seja P um R-módulo. As seguintes condições são equivalentes:*

1. *P é projetivo finitamente gerado.*

2. *$\phi : P \otimes_R P^* \to Hom_R(P,P)$ é um isomorfismo de R-módulos.*

Demonstração. 1) $\Rightarrow$ 2) Seja P um R-módulo projetivo finitamente gerado. Assim, pela Proposição 1.38, segue que existem elementos $p_i \in P$ e $f_i \in P^*$, com $1 \leq i \leq n$, tal que para todo $p \in P$, $p = \sum_{i=1}^{n} f_i(p)p_i$. Como ϕ é homomorfismo, resta mostrar que ϕ é bijetivo. Para mostrar a sobrejetividade, tomamos $\sigma \in Hom_R(P,P)$. Como $f_i\sigma \in P^*$, segue que $\sum_{i=1}^{n} p_i \otimes f_i\sigma \in P \otimes P^*$. Mostramos que a imagem deste elemento

por ϕ é σ. Seja $p \in P$, logo

$$\phi\left(\sum_{i=1}^{n} p_i \otimes f_i\sigma\right)(p) = \sum_{i=1}^{n} f_i(\sigma(p))p_i = \sigma\left(\sum_{i=1}^{n} f_i(p)p_i\right) = \sigma(p),$$

e assim, $\phi\left(\sum_{i=1}^{n} p_i \otimes f_i\sigma\right) = \sigma$, o que mostra que ϕ é sobrejetora. Para mostrar a injetividade, suponhamos que $a = \sum_{j=1}^{n} q_j \otimes g_j \in \mathrm{Ker}(P \otimes P^*)$. Assim, $\phi(a) = 0$. Como $q_j \in P$, por hipótese, segue que $q_j = \sum_{i=1}^{n} f_i(q_j)p_i$. Utilizando essa igualdade e o fato de que o produto tensorial é bilinear, segue que

$$a = \sum_{j=1}^{n} q_j \otimes g_j = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} f_i(q_j)p_i\right) \otimes g_j = \sum_{j=1}^{m}\sum_{i=1}^{n} f_i(q_j)p_i \otimes g_j = \sum_{i=1}^{n} p_i \otimes \sum_{j=1}^{m} f_i(q_j)g_j.$$

Mas para todo $p \in P$,

$$\begin{aligned}\sum_{j=1}^{n} g_j(p)f_i(q_i) &= f_i\left(\sum_{j=1}^{n} g_j(p)q_j\right) = f_i\left(\phi\left(\sum_{j=1}^{n} q_j \otimes g_j\right)(p)\right)\\ &= f_i(\phi(a)(p)) = f_i(0) = 0.\end{aligned}$$

Logo, $\sum_{j=1}^{m} f_i(q_j)g_j = 0$, e consequentemente, $a = \sum_{j=1}^{m} q_j \otimes 0 = 0$, ou seja, ϕ é injetivo. Portanto, ϕ é um isomorfismo.

2) $\Rightarrow$ 1) Por hipótese, ϕ é um isomorfismo, e portanto, ϕ é sobrejetivo. Logo, considerando $id_P \in \mathrm{Hom}_R(P, P)$, segue que existem $p_1, \ldots, p_n \in P$ e $f_1, \ldots f_n \in P^*$ tal que $\phi\left(\sum_{i=1}^{n} p_i \otimes f_i\right) = id_P$. Logo, para todo $p \in P$, segue que

$$p = id_P(p) = \phi\left(\sum_{i=1}^{n} p_i \otimes f_i\right)(p) = \sum_{i=1}^{n} f_i(p)p_i,$$

o que mostra que P é projetivo finitamente gerado, de acordo com a Proposição 1.38, o que prova o resultado. □

Definição 1.41. *Seja P um R-módulo. O conjunto $an_R(P) = \{a \in R : ap = 0$, para todo $p \in P\}$ é um ideal de R, chamado* ***anulador de P em R****. Dizemos que P é um R-módulo* ***fiel*** *se $an_R(P) = 0$.*

Lema 1.42. *(Nakayama) Seja P um R-módulo finitamente gerado. Se I é um ideal de R, então $IP = \{xp : \ x \in I, p \in P\} = P$ se, e somente se, $I + an_R(P) = R$.*

Demonstração. Suponhamos que $P = IP$. Como por hipótese, P é finitamente gerado, segue que existem $p_1, \ldots, p_n \in P$ tal que $P = Rp_1 + \cdots + Rp_n$. Definimos $P_i = Rp_i + \cdots + Rp_n$, para $i = 1, \ldots, n$ e $P_{n+1} = 0$. Vamos mostrar que, para cada $i = 1, \ldots, n+1$, existe $x_i \in I$ tal que $(1-x_i)P \subset P_i$, pois se esta inclusão é verdadeira para $n+1$, segue que o elemento $(1 - x_{n+1})$ pertence ao conjunto $\mathrm{an}_R(P)$, e usando esse fato segue o resultado. Faremos a prova por indução sobre i. Para $i = 1$, a inclusão ocorre tomando $x_1 = 0$. Agora, suponhamos que a afirmação é verdadeira para algum $i > 0$, isto é, que para algum $i > 0$, existe $x_i \in I$ tal que $(1 - x_i)P \subset P_i$, e com essa hipótese de indução mostramos que vale para $i+1$, e assim, é verdadeira para todo n. Usando que $P = IP$, segue que $(1 - x_i)P = (1 - x_i)IP = I(1 - x_i)P \subset IP_i$, o que implica que $(1 - x_i)p_i = \sum_{j=i}^{n} \lambda_{ij} p_j$ onde $\lambda_{ij} \in I$, e assim, $(1 - x_i - \lambda_{ij})p_i = 0 \in P_{i+1}$. Além disso, $(1 - x_i)(1 - x_i - \lambda_{ij})P \subset (1 - x_i - \lambda_{ij})P_i \subset P_{i+1}$, e consequentemente, $[1 - (2x_i + \lambda_{ij} - x_i^2 - x_i\lambda_{ij})]P \subset P_{i+1}$. Assim, é suficiente tomar $x_{i+1} = 2x_i + \lambda_{ij} - x_i^2 - x_i\lambda_{ij} \in I$, para concluir que existe $x_{i+1} \in I$ tal que $(1 - x_{i+1})P \subset P_{i+1} = 0$. Considerando $i = n$, segue que existe x_{n+1} tal que $(1 - x_{n+1})P \subset P_{n+1}$ e assim, $1 - x_{n+1} \in \mathrm{an}_R(P)$. Como $1 = x_{n+1} + (1 - x_{n+1}) \in I + \mathrm{an}_R(P)$, segue que $I + \mathrm{an}_R(P) = R$. Reciprocamente, se $I + \mathrm{an}_R(P) = R$, então existem $y \in I$ e $z \in \mathrm{an}_R(P)$ tal que $1 = y + z$. Assim, para todo $p \in P$, segue que $p = 1p = yp + zp = yp \in IP$. Logo, $P \subset IP \subset P$, e portanto, $P = IP$. □

Teorema 1.43. *Se P um R-módulo projetivo finitamente gerado e $T_R(P)$ é o ideal gerado por $\{f(p) : \ p \in P, f \in P^*\}$, então $T_R(P) \oplus an_R(P) = R$.*

Demonstração. Como P é projetivo finitamente gerado, pela Proposição 1.38, segue que existem $p_1, \cdots, p_n \in P$ e $f_1, \ldots, f_n \in P^*$ tal que $p = \sum_{i=1}^{n} f_i(p)p_i$, para todo $p \in P$. Assim, $P \subset T_R(P)P \subset P$, que implica que $P = T_R(P)P$. Pelo Lema de Nakayama, segue que $R = T_R(P) + \mathrm{an}_R(P)$, e portanto, existem $y \in T_R(P)$ e $z \in \mathrm{an}_R(P)$ tal que $1 = y + z$. Para mostrar que a soma é direta, seja $x \in T_R(P) \cap \mathrm{an}_R(P)$. Assim, $x1 = xy + xz \in T_R(P)\mathrm{an}_R(P)$, e assim, $T_R(P) \cap \mathrm{an}_R(P) \subset T_R(P)\mathrm{an}_R(P)$. Mas, $T_R(P)\mathrm{an}_R(P) = 0$, pois dado $\lambda \in \mathrm{an}_R(P)$, $p \in P$ e $f \in P^*$, segue que $\lambda f(p) = f(\lambda p) = f(0) = 0$. Logo, $T_R(P) \cap \mathrm{an}_R(P) = 0$, e portanto, $R = T_R(P) \oplus \mathrm{an}_R(P)$. □

Corolário 1.44. *Se P é um R-módulo projetivo finitamente gerado e fiel, então $T_R(P) = R$.*

Demonstração. Segue diretamente do Teorema 1.43 e da definição de módulo fiel. □

Observemos que todo módulo projetivo é um módulo plano, e sendo assim, dado P um R-módulo projetivo e $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ uma sequência exata de R-módulos, segue que a sequência $0 \to M' \otimes_R P \xrightarrow{\alpha \otimes id_P} M \otimes_R P \xrightarrow{\beta \otimes id_P} M'' \otimes_R P \to 0$ é exata.

1.4 Módulo simples e semi-simples

O objetivo desta seção é apresentar os chamados módulos simples e semi-simples. Sabemos que todo módulo M tem no mínimo dois submódulos, M e $\langle 0 \rangle$, podendo inclusive ter apenas esses. Mas existem casos em que um módulo possui muitos submódulos e é útil quando podemos afirmar alguma coisa sobre esses módulos, que são chamados módulos semi-simples. Nesta seção, veremos que os módulos semi-simples preservam uma propriedade que é válida nos espaços vetoriais.

Definição 1.45. *Dizemos que um R-módulo M é **simples** se seus únicos submódulos são $\langle 0 \rangle$ e o próprio M.*

Proposição 1.46. *Um R-módulo simples é gerado por qualquer um de seus elementos não nulo.*

Demonstração. Sejam M um R-módulo simples e $x \in M$, com $x \neq 0$. Assim, $\langle x \rangle$ é um submódulo de M. Como os únicos submódulos de M são M e $\langle 0 \rangle$ e $x \neq 0$, segue que $\langle x \rangle = M$. □

Lema 1.47 (Lema de Schur)**.** *Todo homomorfismo não nulo de R-módulos simples é um isomorfismo.*

Demonstração. Sejam M, N dois R-módulos simples e $f : M \to N$ um homomorfismo não nulo. Como $\mathrm{Ker}(f) \leq M$, $\mathrm{Ker}(f) \neq M$, $f \neq 0$ e M é simples, segue que $\mathrm{Ker}(f) = 0$. Também, como $\mathrm{Im}(f) \leq N$, $\mathrm{Im}(f) \neq \{0\}$ e N é simples, segue que $\mathrm{Im}(f) = N$. Portanto, f é um homomorfismo bijetor, ou seja, um isomorfismo. □

Corolário 1.48. *Se M um R-módulo simples, então $End_R(M)$ é um anel de divisão, isto é, todos os elementos não nulo são invertíveis.*

Demonstração. Pelo Lema 1.47, como M é simples, segue que todo homomorfismo f não nulo que pertence a $\mathrm{End}(M)$ é um isomorfismo, e assim, possui inverso. Além disso, a função identidade $id : M \to M \in \mathrm{End}(M)$, já que é um homomorfismo. Portanto, $\mathrm{End}(M)$ é um anel de divisão. □

Vimos na Seção 1.1 que nem todo submódulo de M é um somando direto, sendo M um R-módulo qualquer, mas às vezes é interessante trabalhar com módulos dessa natureza, por isso essa classe de R-módulos recebe um nome especial.

Definição 1.49. *Seja M um R-módulo. Dizemos que M é* ***semi-simples*** *se todo submódulo de M é um somando direto.*

Exemplo 1.50. Se K for corpo, então todo K-espaço vetorial é um K-módulo semi-simples.

Exemplo 1.51. Todo módulo simples é semi-simples, pois $M = M + \langle 0 \rangle$, mas $\langle 0 \rangle$ é semi-simples e não é considerado simples, pois tem apenas um submódulo.

Exemplo 1.52. $\mathbb{Z}$ visto como um $\mathbb{Z}$-módulo não é semi-simples, pois não possui somandos diretos. De fato, se $N \leq \mathbb{Z}$, com $N \neq \langle 0 \rangle$, então $N = \langle n \rangle$, para algum $n \in \mathbb{Z}$. Suponhamos que N admite suplementar, isto é, existe S tal que $\mathbb{Z} = N \oplus S$. Como S é um $\mathbb{Z}$-submódulo de $\mathbb{Z}$ segue que $S = \langle s \rangle$, para algum $s \in \mathbb{Z}$. Tomando $x = ns \neq 0$, com $n \in N$ e $s \in S$, segue que $x \in N \cap S$ e $x \neq 0$, o que não ocorre.

Proposição 1.53. *Todo submódulo de um módulo semi-simples é semi-simples.*

Demonstração. Sejam M um R-módulo semi-simples e $N \leq M$. Para mostrar que N é semi-simples devemos mostrar que para todo $H \leq N$, H é um somando direto. Para isso, seja $H \leq N$. Como $H \leq M$, segue que existe $J \leq M$ tal que $M = J \oplus H$. Mostramos que $N = (J \cap N) \oplus H$. Como $J \cap N \cap H \subset J \cap H = \{0\}$, segue que $(J \cap N) \cap H = \{0\}$. Como $(J \cap N) \oplus H$ é um submódulo de N, é suficiente mostrar que $N \subset (J \cap N) \oplus H$. Se $n \in N \subset M$, então existem $u \in J$ e $v \in H \subset N$ tal que $n = u + v$, o que implica que $u = n - v \in N$. Logo, $n = u + v \in (J \cap N) \oplus H \Rightarrow N = (J \cap N) \oplus H$. Portanto, N é semi-simples. □

Proposição 1.54. *Todo R-módulo M semi-simples não nulo contém um submódulo simples.*

Demonstração. Seja M um R-módulo semi-simples não nulo. Se $0 \neq m \in M$, então $\langle m \rangle$ é um submódulo não nulo de M, que pela Proposição 1.53, é semi-simples. Mostramos que $\langle m \rangle$ contém um submódulo simples. Se $\Omega = \{H \leq \langle m \rangle : m \notin H\}$, então $\Omega \neq 0$, pois $\langle 0 \rangle \in \Omega$. Ordenando Ω por inclusão, pelo Lema de Zorn, segue que Ω possui elemento maximal, que chamamos de N. Como $\langle m \rangle$ é semi-simples, segue que existe $N' \leq \langle m \rangle$ tal que $\langle m \rangle = N \oplus N'$. Além disso, $N' \neq 0$, pois caso contrário teríamos $\langle m \rangle = N$, o que implica $m \notin \langle m \rangle$. Mostramos que N' é simples. Para isso, se $N'' \leq N$, então $N \oplus N''$ contém m devido à maximalidade de N. Logo, $\langle m \rangle = N \oplus N''$, o que implica que $N'' = N'$. Portanto, N' é um submódulo simples de M. □

A próxima proposição caracteriza os módulos semi-simples.

Proposição 1.55. *Seja M um R-módulo. As seguintes afirmações são equivalentes:*

i) *M é semi-simples;*

ii) *M é a soma de uma família de R-módulos simples;*

iii) *M é soma direta de R-módulos simples.*

Demonstração. Se $M = 0$, então não existem submódulos simples. Mas, por convenção, uma soma, direta ou não, de uma família vazia de submódulos, é igual ao módulo nulo. Logo, $M = 0$ satisfaz as condições da proposição, e assim, assumimos $M \neq 0$.

i) $\Rightarrow$ **ii)** Seja $N = \sum_{i \in I} S_i$, onde $\{S_i\}_{i \in I}$ é a família de todos os R-submódulos simples de M, que não é vazia, pela Proposição 1.55. Assim, $N \neq 0$, e logo, pela hipótese, existe $P \leq M$ tal que $M = N \oplus P$. Supondo que $P \neq 0$, pela Proposição 1.55, segue que P contém um submódulo simples, pois P é semi-simples pela proposição 1.53. Assim, $P \cap N \neq 0$ visto que N contém todos os submódulos simples, o que contraria o fato de a soma ser direta. Logo, só podemos ter $P = 0$, e consequentemente, $M = N$. Portanto, M é uma soma de submódulos simples.

ii) $\Rightarrow$ **iii)** Pela hipótese, segue que vale a parte da soma. Assim, falta mostrar que a mesma é direta. Suponhamos que $M = \sum_{i \in I} S_i$, onde $\{S_i\}_{i \in I}$ é uma família de submódulos simples de M e consideramos $\Omega = \left\{ J \subseteq I : \sum_{j \in J} S_j \text{ é soma direta } \right\}$, onde I é um conjunto de índices. Como toda cadeia em Ω tem cota superior (união dos elementos), pelo Lema de Zorn, segue que Ω tem um elemento maximal, e supomos que seja I'. Consideramos $M' = \bigoplus_{j \in I'} S_j$. Mostramos que $M' = M$. Para todo $i \in I$, segue que S_i é um módulo simples, e assim, $S_i \cap M' = S_i$ ou $S_i \cap M' = \{0\}$, pois essa interseção é um submódulo de S_i (interseção de dois submódulos e está contido em S_i). Se $S_i \cap M = \{0\}$, com $i \notin I'$, então $I' \cup \{i\} \supsetneq I'$, o que contradiz a maximalidade de I'. Logo, $S_i \subset M'$, para todo $i \in I$, ou seja, $M' = M$, e portanto, M é soma direta de submódulos simples.

iii) $\Rightarrow$ **i)** Por hipótese, M é uma soma direta de submódulos simples, isto é, $M = \bigoplus_{i \in i} M_i$. Seja N um submódulo de M. De modo análogo ao caso anterior, segue que $N \cap M_i = M_i$ ou $N \cap M_i = 0$, para todo $i \in I$. Claramente, $N = \bigoplus_{j \in J} M_j$, onde $J = \{i \in I : M_i \cap N = M_i\}$. Portanto, como $M = \bigoplus_{j \in J} M_j \oplus \left(\bigoplus_{j \in I/J} M_j \right) = N \oplus K$, onde $K = \bigoplus_{j \in I/J} M_j$, segue que M é semi-simples. $\square$

1.5 Radicais

Nesta seção, apresentamos alguns tipos de radicais conhecidos sobre anéis comutativos.

Definição 1.56. *Sejam R um anel e $x \in A$. Dizemos que x é **nilpotente** se existe um inteiro m positivo tal que $x^m = 0$.*

Definição 1.57. *Um ideal I de um anel R é chamado nilpotente se existe um inteiro m positivo tal que $I^m = 0$.*

Note que se todo elemento de um ideal I for nilpotente, então I é um ideal nilpotente.

Definição 1.58. *Seja R um anel comutativo. O **radical de Jacobson** de R, denotado por $J(A)$, é definido como sendo a interseção de todos os ideais maximais de R, ou seja, $J(A) = \cap M_i$, onde M_i são os ideais maximais de R.*

A próxima proposição caracteriza os radicais de Jacobson.

Proposição 1.59. *Sejam R um anel e $y \in A$. As seguintes condições são equivalentes:*

i) $y \in J(A)$;

ii) $1 - xy$ *é invertível para todo* $x \in A$;

iii) $yM = 0$ *para todo R-módulo simples M.*

Demonstração. **i)** $\Rightarrow$ **ii)** Suponhamos que exista $x \in A$ tal que $1 - xy$ não é invertível. Assim, $\langle 1 - xy \rangle$ é um ideal próprio de R. Portanto, existe um ideal maximal M de R tal que $1 - xy \in M$, pois todo ideal próprio está contido em um ideal maximal. Como $y \in J(A) \subseteq M$, segue que $1 \in M$, o que é uma contradição.

ii) $\Rightarrow$ **iii)** Seja M um R-módulo simples e suponhamos que existe $m \in M$ tal que $ym \neq 0$. Como M é simples, segue que $\langle ym \rangle = M$. Portanto, existe $x \in A$ tal que $xym = m$, ou seja, $(1 - xy)m = 0$. Como por hipótese $1 - xy$ é invertível, segue que $m = 0$, o que é uma contradição pois $ym \neq 0$.

iii) $\Rightarrow$ **i)** Suponhamos que $y \notin J(A)$. Assim, existe um ideal maximal M de R tal que $y \notin M$. Como $\frac{M}{A}$ é simples (porque é um corpo), segue por hipótese que $y\frac{A}{M} = 0$. Assim, $y \in M$, o que é uma contradição. □

Definição 1.60. *Seja I ideal de um anel R. O **radical** de I denotado por $\sqrt{I}$ ou $r(I)$ é definido como $\sqrt{I} = \{a \in A : a^n \in I \text{ para algum } n > 0\}$.*

Os elementos de $\sqrt{I}$ representam os elementos nilpotentes de R/I. De fato,

$$a \in \sqrt{I} \Leftrightarrow a^n \in I \Leftrightarrow \bar{a}^n = \bar{0} \text{ em } A/I, \text{ para algum } n. \tag{1.1}$$

Também, usando a Equação (1.1) e que os ideias de R/I são da forma J/I em que $I \subseteq J \trianglelefteq A$, segue que $\sqrt{I} = \cap P$, onde P é um ideal primo de R que contém I.

Definição 1.61. *O **nilradical** de R é a interseção de todos os ideais primos de R, isto é, $Nil(A) = \cap P_i$, onde P_i são os ideais primos de R.*

Proposição 1.62. *Se R é um anel comutativo, então o nilradical de R é o ideal formado pelos elementos nilpotentes de R, isto é, $Nil(A) = \{a \in A : a \text{ é nilpotente}\}$.*

Demonstração. Denotamos por Π a interseção de todos os ideias primos de R. Se $x \in Nil(A)$, então existe $n > 0$ tal que $x^n = 0$. Como $0 \in P$, para todo ideal primo P, segue que $x^n \in P$, e assim, $x \in P$ para todo ideal primo P (do fato de que $x^n \in P \Rightarrow x \in P$ ou $x^{n-1} \in P$; seguindo o raciocínio para x^{n-1}, e assim sucessivamente, segue que $x \in P$). Logo, $x \in \Pi$. Por outro lado, seja $x \in \Pi$ e suponhamos que $x \notin Nil(A)$, ou seja, $x^n \neq 0$ para algum n. Seja $\Sigma = \{I \trianglelefteq A : n > 0 \Rightarrow x^n \notin I\}$. Note que $\Sigma \neq \emptyset$ pois $\langle 0 \rangle \in \Sigma$. Sendo Σ um conjunto não vazio parcialmente ordenado por inclusão, onde toda cadeia de ideais $(I_i)_{i \in I}$ em Σ, possui cota superior $J = \cup I_i$ (observe que união de ideais não é necessariamente um ideal, mas nesse caso J é um ideal pois os ideais da união fazem parte de uma cadeia), podemos aplicar o Lema de Zorn e concluir que Σ possui um elemento maximal P. Mostramos que P é primo. Suponhamos que $xy \in P$ mas $x \notin P$ e $y \notin P$. Assim, $P \subsetneq \langle x \rangle + P$ e $P \subsetneq \langle y \rangle + P$. Como P é elemento maximal de Σ, segue que $\langle x \rangle + P, \langle y \rangle + P \notin \Sigma$. Mas isso significa que existem $m, n > 0$ tal que $x^m \in \langle x \rangle + P$ e $x^n \in \langle y \rangle + P$. Logo, $x^m x^n \in \langle xy \rangle + P = P$, pois $xy \in P$. Assim, $x^{m+n} \in P$, o que contradiz o fato de $P \in \Sigma$. O absurdo segue do fato de ter suposto que P não é primo, e portanto, concluímos que P é um ideal primo. □

1.6 Módulos noetherianos e artinianos

Iniciamos esta seção mostrando uma equivalência entre duas condições de cadeia necessárias para definirmos e explorarmos um pouco os módulos noetherianos e artinianos.

Proposição 1.63. *Seja Σ um conjunto parcialmente ordenado pela relação $\leq$. As seguintes condições em Σ são equivalentes:*

i) *Toda cadeia crescente de elementos de Σ é estacionária;*

ii) *Todo subconjunto não vazio de Σ possui um elemento maximal.*

Demonstração. **i)** $\Rightarrow$ **ii)** Seja $\emptyset \neq S \subseteq \Sigma$ e tome $x_1 \in S$. Se x_1 for um elemento maximal de S, está provado. Caso contrário, existe $x_2 \in S$ tal que $x_1 < x_2$. Se x_2 for maximal, o resultado segue, caso contrário repetimos o argumento. Repetindo sucessivamente o mesmo argumento, obtemos uma cadeia crescente $x_1 \leq x_2 \leq ...$ que por hipótese é estacionária. Logo, existe k tal que x_k é maximal em S.

ii) $\Rightarrow$ **i)** Dada a cadeia $x_1 \leq x_2 \leq ... \leq x_n \leq ...$, segue por hipótese que o conjunto $S = \{x_1, x_2, ...\}$ tem um elemento maximal, digamos x_l. Assim, $x_l = x_{l+1} = ...$, e portanto, essa cadeia é estacionária. □

Definição 1.64. *Sejam M um R-módulo e Σ um conjunto de submódulos de M. Consideremos $(\Sigma, \subseteq)$ com a relação de ordem. Se $(\Sigma, \subseteq)$ satisfaz uma das condições da Proposição 1.63, M é dito um R-módulo* ***noetheriano****.*

O resultado da Proposição 1.63 ainda vale se trocarmos "cadeia crescente" por "cadeia decrescente" e "elemento maximal" por "elemento minimal". O módulo que satisfizer uma das duas condições nesses termos é chamado de módulo **artiniano**. Observamos que todo anel R é um R-módulo e seus ideais são exatamente os submódulos. Assim, um anel é noetheriano (artiniano) se os seus ideais satisfizem as condições da Proposição 1.63, considerando a condição crescente (decrescente).

Exemplo 1.65. O anel $\mathbb{Z}$ é noetheriano mas não é artiniano. Para ver isso, seja $\Sigma = \{(n) : n \in \mathbb{Z}\}$. Assim, $(n) \subseteq (m) \Leftrightarrow m|n$. Logo, essa cadeia é estacionária, uma vez que n tem um número finito de divisores. Agora, se tomarmos a cadeia decrescente $(n) \supsetneq (n^2) \supsetneq (n^3) \supsetneq ... \supsetneq (n^k) \ldots$, segue que essa não estaciona, pois n possui infinitos múltiplos.

Exemplo 1.66. Seja K um corpo. Um K-espaço vetorial de dimensão finita é ambos noehteriano e artiniano. Seus subespaços satisfazem a condição de cadeia crescente porque a dimensão é finita (espaços vetoriais de dimensão infinita não são noetherianos) e também satisfaz a condição de cadeia decrescente pois sempre terminará no máximo com o espaço nulo.

Exemplo 1.67. O anel dos polinômios $K[x_1, x_2, x_3, \ldots]$ em infinitas variáveis não é noetheriano, uma vez que $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq ...$ não é estacionária pois como existem infinitas variáveis, sempre podemos acrescentar mais uma. Também não é artiniano, uma vez que $(x_1) \supsetneq ({x_1}^2) \supsetneq ({x_1}^3) \supsetneq ...$ claramente também não é estacionária.

Proposição 1.68. *Seja M um R-módulo. Assim, M é noetheriano se, e somente se, todo submódulo de M é finitamente gerado.*

Demonstração. Suponhamos que M é noetheriano. Seja $N \leq M$. Se $N = \{0\}$, então N é finitamente gerado. Caso contrário, existe $n_1 \in N\backslash\{0\}$. Se $(n_1) = N$, então N é finitamente gerado. Caso contrário, existe $x_2 \in N\backslash(n_1)$ tal que $(n_1) \subsetneq (n_1, n_2) \leq N$. Se $N = (n_1, n_2)$, então N é finitamente gerado. Caso contrário, prosseguimos com o mesmo raciocínio de modo que obteremos $(n_1) \subsetneq (n_1, n_2) \subsetneq \cdots \subsetneq (n_1, \ldots, n_k) \subsetneq \cdots \subsetneq N$ uma cadeia crescente de submódulos de N, e também de M, que por hipótese é estacionária. Logo, existe l tal que $(n_1, \ldots, n_l) = (n_1, \ldots, n_l, n_{l+1}) = \cdots = N$, ou seja, N é finitamente gerado. Reciprocamente, seja $M_1 \subseteq M_2 \subseteq \cdots \subseteq \ldots$ uma cadeia crescente de submódulos de M. Assim, $N = \cup_{n=1}^{\infty} M_n$ é um submódulo de M (por formarem uma cadeia em M), e logo, é finitamente gerado, por hipótese, isto é, $N = (x_1, \ldots, x_r)$ onde $x_i \in M_{n_i}$. Se $n = \max\{n_1, \ldots, n_r\}$, então $x_i \in M_{n_i} \subset M_n$ para todo i. Logo, $N = M_n$, e portanto, a cadeia é estacionária. □

Proposição 1.69. *Seja $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ uma sequência exata de R-módulos.*

i) *M é noetheriano $\Leftrightarrow$ M' e M'' são noetherianos;*

ii) *M é artiniano $\Leftrightarrow$ M' e M'' são artinianos;*

Demonstração. **i)** Sejam $M'_1 \subseteq M'_2 \subseteq \cdots \subseteq \cdots$ uma cadeia crescente de submódulos de M' e $M''_1 \subseteq M''_2 \subseteq \cdots \subseteq \cdots$ uma cadeia de submódulos de M''. Assim, $f(M'_1) \subseteq f(M'_2) \subseteq \cdots$ e $g^{-1}(M''_1) \subseteq g^{-1}(M''_2) \subseteq \cdots$ são cadeias crescentes de submódulos de M, que por hipótese é noetheriano. Logo, existem k e n tal que $f(M'_k) = f(M'_{k+1}) = \cdots$ e $g^{-1}(M''_n) = g^{-1}(M''_{n+1}) = \cdots$. Como f é injetora, segue que $f^{-1}f(M'_k) = M'_k$, para todo k. Logo, $M'_k = M'_{k+1}$, o que implica que M' é noetheriano. Analogamente, como g é sobrejetora, segue que $g(g^{-1}(M''_n)) = M''_n$ para todo n, assim $M''_n = M''_{n+1}$, o que implica que M'' é noetheriano. Reciprocamente, se $M_1 \subseteq M_2 \subset \cdots$ é uma cadeia de submódulos de M, então $f^{-1}(M_1) \subseteq f^{-1}(M_2) \subseteq \cdots$ é uma cadeia de submódulos de M', que por hipótese, é estacionária, isto é, existe k tal que $f^{-1}(M_k) = f^{-1}(M_{k+1}) = \ldots$ Também, $g(M_1) \subseteq g(M_2) \subseteq \cdots$ é uma cadeia de submódulos de M''. Logo, existe l tal que $g(M_l) = g(M_{l+1}) = \cdots$. Seja $r = max\{k, l\}$. Como $M_r \subset M_{r+1}$ para todo r, é suficiente mostrar a inclusão contrária. Seja $x \in M_{r+1} \subseteq M$. Como $g(M_r) = g(M_{r+1})$ para todo $r \geq l$, segue que existe $y \in M_r$ tal que $g(x) = g(y)$. Assim, $g(x - y) = 0 \Rightarrow x - y \in \mathrm{Ker}(g) = Im(f)$, e então, existe $z \in M'$ tal que $f(z) = x - y \in M_{r+1}$. Logo, $z \in f^{-1}(M_{r+1}) = f^{-1}(M_r)$, e isto implica que, $f(z) = x - y \in M_r$. Como $y \in M_r$, segue que $x \in M_r$, e assim,

$M_{r+1} \subseteq M_r$. Portanto, a cadeia em M é estacionária e M é noetheriano.

ii) A prova é feita de modo análogo ao item **i**) utilizando cadeias decrescentes. □

Corolário 1.70. *Sejam M um R-módulo e $N \leq M$. Assim, M é noetheriano se, e somente se, N e $\frac{M}{N}$ são noetherianos.*

Demonstração. Pela Proposição 1.69, é suficiente considerar a sequência exata $0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} \frac{M}{N} \longrightarrow 0$. □

Corolário 1.71. *Se $M_1, \ldots, M_n$ são R-módulos noetherianos, então $\bigoplus_{i=1}^{n} M_i$ é noetheriano.*

Demonstração. Como $\bigoplus_{i=1}^{n} M_i = \left(\bigoplus_{i=1}^{n-1} M_i\right) \bigoplus M_n$, para $n > 1$, é suficiente motrar para $n = 2$, e o caso geral, segue por indução. Considere a sequência $0 \longrightarrow M_2 \xrightarrow{i} M_1 \oplus M_2 \xrightarrow{p} M_1 \longrightarrow 0$, onde $i(m_2) = (0, m_2)$ e $p(m_1, m_2) = m_1$. Esta sequência é exata, pois i é injetora, visto que $i(m_2) = (0,0) \Rightarrow (0, m_2) = (0,0) \Rightarrow m_2 = 0$, e p é sobrejetora, pois dado $m_1 \in M_1$, existe $(m_1, m_2) \in M_1 \oplus M_2$, tal que $p(m_1, m_2) = m_1$. Além disso, $\mathrm{Im}(i) = (0, m_2) = M_2 = \mathrm{Ker}(g)$. Logo, o resultado segue pela Proposição 1.69. □

Proposição 1.72. *Se R é noetheriano e M é um R-módulo finitamente gerado, então M é noetheriano.*

Demonstração. Pelo Corolário 1.71, segue que se M é noetheriano, e portanto, M^n também é noetheriano. Logo, como R é noetheriano, segue que R^n também é noetheriano. Como M é finitamente gerado, seja $\{m_1, ..., m_k\}$ um conjunto de geradores. A aplicação

$$\begin{array}{rccc} f: & R^k & \to & M \\ & (a_1, ..., a_k) & \mapsto & \displaystyle\sum_{i=1}^{k} a_i m_i \end{array}$$

é um epimorfismo, e assim, $\frac{R^k}{\mathrm{Ker}(f)} \cong M$. Portanto, pelo Corolário 1.70, segue que M é noetheriano. □

Note que os resultados anteriores também são válidos substituindo-se noetheriano por artiniano, conforme a Proposição 1.69.

Vejamos alguns resultados que relacionam anel artiniano e radicais.

Proposição 1.73. *Se R é artiniano então todo ideal primo é maximal.*

Demonstração. Se P um ideal primo de R, então R/P é um domínio e como R é artiniano, pelo Corolário 1.70, segue que R/P também é artiniano. Assim, dado $x \in (R/P)\backslash\{0\}$, considerando a cadeia $(x) \supseteq (x^2) \supseteq (x^3) \ldots$, segue que existe n tal que $(x^n) = (x^{n+1}) = \ldots$. Assim, existe $b \in R/P$ tal que $x^n = bx^{n+1} \Rightarrow x^n(1 - bx) = 0$. Como $x \neq 0$ e R/P é um domínio, segue que $bx = 1$, ou seja, $x \neq 0$ possui inverso. Portanto, R/P é um corpo, e assim, P é um ideal maximal. □

Corolário 1.74. *Se R é artiniano, então $nil(R) = Jac(R)$.*

Demonstração. Segue diretamente da Proposição 1.73. □

1.7 Considerações finais

Neste capítulo, apresentamos os conceitos iniciais sobre módulos necessários para entender o restante do texto, e que também pode ser utilizado como um texto à parte para quem deseja estudar um pouco sobre os módulos. Por esta razão, apresentamos conceitos como, por exemplo, de módulo noetheriano e artiniano, que não são propriamente utilizados aqui. Os conceitos de produto tensorial, módulos simples e módulo semi-simples recebem uma generalização para o caso das álgebras no Capítulo 2. Os módulos projetivos serão utilizados no Capítulo 3 para o desenvolvimento da teoria de Galois para anéis comutativos.

2 Álgebras

Neste capítulo, apresentamos as definições e propriedades básicas sobre as álgebras definidas sobre um anel R, dedicando uma atenção especial às álgebras semi-simples e às álgebras separáveis, conceitos que serão de suma importância para a realização dos próximos capítulos. Para a realização deste capítulo, nos baseamos nas definições e demonstrações apresentadas em [1], [4], [15] e [16].

2.1 Noções básicas

Nesta seção, apresentamos o conceito de álgebra e suas principais propriedades, onde veremos que uma álgebra possui três operações sendo duas internas e uma externa.

Definição 2.1. *Sejam R um anel e A um conjunto não vazio. Dizemos que A é uma R-**álgebra** se satisfizer:*

1. *A é um R-módulo;*
2. *existe uma aplicação bilinear $f : A \times A \to A$, denotada por $f(x, y) = xy$, que satisfaz: $x(y + z) = xy + xz, (x + y)z = xz + yz$ e $(xy)z = x(yz)$, para todo $x, y, z \in A$.*

Com menos rigor, uma R-álgebra A é um conjunto A que é ao mesmo tempo um R-módulo e um anel. Quando se define uma K-álgebra A sobre um corpo K, então A tem estrutura de anel e de K-espaço vetorial.

Observe que dados dois anéis quaisquer R e S tal que exista um homomorfismo $f : R \to S$, podemos definir o produto $ab = f(a)b$, e com essa operação, S também tem estrutura de R-módulo. Logo, S tem uma estrutura de um R-módulo além da estrutura de anel, ou seja, S é uma R-álgebra. Assim, podemos ver S como uma R-álgebra considerando quaisquer anéis R e S tal que que exista um homomorfismo entre eles. Nesse caso, uma R-álgebra pode ser definida como uma estrutura formada por

um anel S munido de um homomorfismo de anéis $f : R \to S$ com a operação definida por $ab = f(a)b$.

Definição 2.2. *Sejam R um anel, A e B duas R-álgebras. Uma aplicação $h : A \to B$, é chamada um* ***homomorfismo de álgebras*** *se, além de homomorfismo de anéis, h for também um homomorfismo de R-módulos.*

Definição 2.3. *Uma R-álgebra A é dita* ***finita*** *se A é finitamente gerada como um R-módulo.*

Exemplo 2.4. $\mathbb{R}$ e $\mathbb{C}$ com suas operações usuais são $\mathbb{R}$-álgebras.

Exemplo 2.5. O espaço dos polinômios $R[x_1, \ldots, x_n]$, em n variáveis com coeficientes em R munido da multiplicação usual de polinômios, é uma álgebra sobre R, ou seja, é uma R-álgebra.

Definição 2.6. *Seja A uma R-álgebra. Uma* ***subálgebra*** *de A é um subconjunto N de A que também é uma álgebra com as operações de A restritas a N, ou seja, que é tanto um subanel como um submódulo de A.*

Dadas duas R-álgebras A e B, que também são R-módulos, podemos definir seu produto tensorial $D = A \otimes B$ sobre R. Definindo a soma e a multiplicação por escalar como $(b \otimes c) + (b' \otimes c') = (b + b') \otimes (c + c')$ e $a(b \otimes c) = ab \otimes c$, respectivamente, segue que D é um R-módulo. Assim, para mostrar que D é uma R-álgebra, precisamos definir uma multiplicação entre os elementos de D. Para isso, considere a aplicação

$$\begin{array}{rccc} f: & A \times B \times A \times B & \to & D \\ & (b, c, b', c') & \mapsto & bb' \otimes cc'. \end{array}$$

Observando que f é linear em cada coordenada, segue da Proposição 1.28, que f induz o homomorfismo de R-módulos $f' : A \otimes B \otimes A \otimes B \to D$. Como o produto tensorial é associativo, segue que f induz um homomorfismo de $D \otimes D$ em D que corresponde à aplicação bilinear $g : D \times D \to D$ dada por $u(b \otimes c, b' \otimes c') = bb' \otimes cc'$. Assim, a multiplicação $(a \otimes b)(a' \otimes b') = (aa' \otimes bb')$ está bem definida. Poderíamos ter apresentado essa fórmula diretamente, mas desta forma não poderíamos garantir que a mesma está bem definida. Com essa multiplicação, essa soma e esse produto por escalar, segue que o produto tensorial $D = A \otimes B$ é uma R-álgebra com unidade $1 \otimes 1$.

Vejamos, agora, duas definições que utilizaremos nas seções seguintes.

Definição 2.7. *Seja A uma R-álgebra. Dizemos que A é* ***central*** *se $Z(A) \cong R$, onde $Z(A) = \{a \in A |\ ab = ba, \text{para todo } b \in A\}$ indica o centro da álgebra A. Os elementos $x \in A$ tal que $xa = ax$, para todo $a \in A$, isto é, tal que $x \in Z(A)$, são chamados de* ***elementos centrais de*** *A.*

Definição 2.8. *Sejam A uma K-álgebra e $N(A)$ a soma de todos os ideais (bilaterais) nilpotentes de A. O ideal $N(A)$ é chamado* ***radical de*** *A.*

2.2 Álgebras simples e semi-simples

Nosso principal objetivo nesta seção, é definir e caracterizar as álgebras simples e semi-simples através do Teorema de Wedderburn. As álgebras aqui consideradas são definidas sobre um corpo K, de dimensão finita, associativas, com elemento identidade e não necessariamente comutativas.

Definição 2.9. *Seja A uma K-álgebra. Dizemos que A é uma álgebra* ***simples*** *se A não possui ideal além dos triviais $\{0\}$ e A.*

Definição 2.10. *Seja A uma K-álgebra de dimensão finita. Dizemos que A é* ***semi-simples*** *se $N(A) = 0$, ou seja, se A não possui ideais laterais nilpotentes.*

Notemos que toda K-álgebra de dimensão finita sem elementos nilpotentes não nulos, é semi-simples. Se a álgebra for comutativa, a recíproca também vale.

Veremos a seguir uma sequência de resultados que serão auxiliares à prova do teorema principal.

Lema 2.11. *Seja A uma K-álgebra de dimensão finita. Se I é um ideal não nulo de A que não é nilpotente, então I possui um elemento idempotente não nulo, isto é, existe $0 \neq e \in I$ tal que $e^2 = e$.*

Demonstração. Como I não é nilpotente, segue que existe $a \in I$ que não é nilpotente. Consideremos a sequência $I \supset Ia \supset Ia^2 \supset \cdots \supset Ia^n \cdots$. Pelo fato de que a dimensão de A é finita, segue que essa sequência é estacionária, e logo, existe um inteiro m positivo tal que $Ia^m = Ia^{m+1} = \cdots$. Chamando $B = Ia^m$ e $b = a^{m+1}$, segue que $Bb = Ia^m a^{m+1} = Ia^{2m+1} = Ia^m = B$, e desta forma, como $b \in B$, segue que existe $e \in B$ tal que $eb = b$, e logo, $(e^2 - e)b = 0$. Usaremos esta igualdade e a função dada a seguir para mostrar que e é um idempotente não nulo. Definindo $\phi : B \to B$ por $\phi(x) = xb$, segue que ϕ é linear e claramente sobrejetora. Pelo fato de que B tem dimensão finita, segue que ϕ é também injetora, e assim, $0 = (e^2 - e)b = \phi(e^2 - e) \Rightarrow e^2 - e = 0$, donde segue que $e^2 = e$. Além disso, supondo que $e = 0$, segue que $a^{m+1} = b = eb = 0$, o que contradiz o fato de que a não é nilpotente. Logo, $e \neq 0$. □

Teorema 2.12. *Seja A uma K-álgebra semi-simples. Se I é um ideal à esquerda não nulo de A, então $I = Ae$ para algum elemento idempotente não nulo $e \in I$.*

Demonstração. Seja I um ideal não nulo de A. Como A é semi-simples, segue que I não é nilpotente, e então, pelo Lema 2.11, segue que existe um elemento idempotente não nulo e_o em I. Consideremos o conjunto anulador $\mathrm{an}_I(e_o) = \{b \in I : be_o = 0\}$, que é um ideal de A e, portanto, não pode ser nilpotente. Suponhamos que $\mathrm{an}_I(e_o) \neq \{0\}$. Usando novamente o Lema 2.11, segue que existe um idempotente não nulo $e_1 \in \mathrm{an}_I(e_o)$. Seja $f_o = e_0 + e_1 - e_0e_1 \in I$. Claramente $f_o^2 = (e_0 + e_1 - e_oe_1)^2 = f_0$ já que $e_1e_o = 0$. Também, $f_o \neq 0$, pois caso contrário teríamos $0 = f_oe_o = e_o^2 + e_1e_0 - e_0e_1e_0 = e_o^2 = e_o$, que é um absurdo. Além disso, dado $b \in \mathrm{an}_I(f_o)$, segue que $0 = (bf_oe_o)e_o = b(f_oe_o) = be_o$, donde concluímos que $b \in \mathrm{an}_I(e_o)$, e logo, $\mathrm{an}_I(f_o) \subset \mathrm{an}_I(e_o)$. Note que esta inclusão é própria, visto que $e_1 \in \mathrm{an}_I(e_o)$ mas $e_1f_o = e_1 \neq 0$. Supondo que $\mathrm{an}_I(f_o) \neq 0$, continuamos o processo obtendo a cadeia de ideais $\mathrm{an}(e_o) \supset \mathrm{an}(f_o) \supset \mathrm{an}(g_o) \supset \cdots$. Mas, pelo fato de a dimensão de A ser finita, segue que esse processo para após algumas repetições finitas, de modo que podemos concluir que existe um elemento idempotente $e \neq 0$ em I tal que $\mathrm{an}(e) = 0$. Mas dado $b \in B$, segue que $(be - b)e = 0$, e logo, $be - b \in \mathrm{an}(e) = 0$, e consequentemente, $be = b$. Portanto, $Ae \subset I \subset Ae$, ou seja, $Ae = I$. □

Corolário 2.13. *Seja A uma K-álgebra semi-simples. Se I é um ideal não nulo de A, então $I = Ae = eA$, para algum elemento idempotente central não nulo $e \in I$ em A. Em particular, I é uma K-álgebra com elemento idempotente e.*

Demonstração. Pelo Teorema 2.12, sabemos que existem elementos idempotentes $e_1, e_2 \in I$ não nulos tal que $e_1b = b = be_2$, para todo $b \in I$. Assim, em particular, vale que $e_1 = e_1e_2 = e_2$. Logo, $e_1 = e_2 = e$ é o elemento identidade da multiplicação de I, e portanto, $I = Ae = eA$. Agora, mostramos que e é central em A, isto é, que $ae = ea$, para todo $a \in A$. Notemos que $ea, ae \in I$ para todo $a \in A$. Logo, $ae = e(ae) = (ea)e = ea$, para todo $a \in A$, o que conclui a prova. □

Lema 2.14. *Seja A uma K álgebra semi-simples. Se $I_1, \ldots, I_n$ são ideais minimais distintos de A, então $I_1 + \cdots + I_n = I_1 \oplus \cdots \oplus I_n$. Em particular, A possui um número finito de ideais minimais.*

Demonstração. Vimos no Teorema 2.12 que para cada ideal minimal I_i, existe um elemento idempotente $e_i \neq 0$ tal que $I_i = Ae_i$, para todo $i = 1, \ldots, n$. Suponhamos que $e_ie_j \neq 0$, para algum i e algum j. Assim, $I_i \cap I_j \neq 0$. Mas como $I_i \cap I_j$ é um ideal de A contido em I_i e em I_j, pela minimalidade de ambos, segue que $I_i = I_i \cap I_j = I_j$, e pelo fato de os ideais serem distintos, devemos ter necessariamente que $I_i = I_j$. Logo, $e_ie_j = 0$ sempre que $i \neq j$. Agora, suponhamos que existam $a_i \in A$ tal que $a_1e_1 + \cdots + a_ne_n = 0$. Multiplicando por e_i, obtemos $ae_i^2 = ae_i = 0$, para todo $i = 1, \ldots, n$, o que mostra que

a soma é direta. Para ver que o número de ideais minimais de A é finito, é suficiente observar que $\dim_K A$ é finita e $\dim_K(I_1 + \cdots + I_n) = \sum_{i=1}^{n} \dim_K I_i$. □

Teorema 2.15. *Seja A uma K-álgebra semi-simples. Se $I_1, \ldots, I_n$ são todos os ideais minimais de A, então $A = I_1 \oplus \cdots \oplus I_n$.*

Demonstração. Usando o Lema 2.14, só falta mostrar que $A \subset I_1 + \cdots + I_n$. Já vimos que para cada I_i, existem elementos idempotentes e_i tal que $I_i = Ae_i$ e $e_i e_j = 0$, para $i \neq j$. Seja $e = e_1 + \cdots + e_n$, que é também um idempotente central não nulo satisfazendo $ee_i = e_i$, para todo $i = 1, \ldots, n$. Suponhamos que $e \neq 1$. Assim, $J = A(e-1)$ é um ideal não nulo de A, e desse modo, J contém algum dos ideais minimais I_i de A, digamos I_k. Logo, para algum $a \in A$, podemos escrever $e_k = a(e-1)$, e consequentemente, $e_k = e_k^2 = e_k a(e-1) = e_k ea - e_k a = 0$, já que $e_k e = e_k$, o que é um absurdo. Assim, $e_1 + \cdots + e_n = 1$, e dado $a \in A$, segue que $a = ae_1 + \cdots + ae_n \in I_1 + \cdots + I_n$. Portanto, $A = I_1 \oplus \cdots \oplus I_n$. □

A partir do Teorema 2.15 podemos concluir que uma K-álgebra semi-simples é a soma direta de todos os seus ideais minimais, fato que será utilizado recorrentemente na aplicação em códigos feita no último capítulo. A partir disso, para provar que uma álgebra semi-simples é a soma direta de álgebras simples, basta provar que todo ideal minimal é uma álgebra simples, como faremos no próximo lema.

Lema 2.16. *Sejam A uma K-álgebra semi-simples e I um ideal não nulo de A. Se I é minimal, então I é uma K-álgebra simples.*

Demonstração. Como I é uma K-álgebra, segue que somente precisamos mostrar que os únicos ideais de I são os triviais. Seja J um ideal não nulo de I e consideremos o ideal IJI de A, que também está contido em I. Suponhamos que $IJI = 0$. Assim, $J^3 \subset IJI = 0$, e logo, $J^3 = 0$. Assim, J é um ideal nilpotente de I, o que contradiz o fato de que I é semi-simples. Logo, $IJI \neq 0$, e então, pela minimalidade de I, segue que $I = IJI \subset J \subset I$, ou seja, $J = I$. Portanto, I é uma K-álgebra simples. □

Dos dois últimos resultados concluímos o seguinte teorema.

Teorema 2.17. *Toda álgebra semi-simples é uma soma direta de álgebras simples.*

O Teorema de Wedderburn, objetivo dessa seção, fornece ainda mais informações sobre as álgebras semi-simples, pois nos mostra exatamente a "cara" que essas álgebras simples da decomposição possuem. Para prová-lo vamos precisar de algumas definições e observações, que faremos a seguir.

Dados um corpo K e D uma K-álgebra, o conjunto $M_n(D)$ das matrizes $n \times n$ com entradas em D é uma K-álgebra chamada de álgebra de matrizes. Dizemos que D é uma álgebra de divisão, se D for um anel de divisão. Aqui estamos interessados nas matrizes $M_n(D)$, especialmente quando D for álgebra de divisão.

Seja $C_j \subseteq M_n(D)$ conjunto das matrizes cujos elementos que não estão na coluna j são zero:

$$\begin{bmatrix} 0 & \dots & c_1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & c_i & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & c_n & \dots & 0 \end{bmatrix}.$$

Cada conjunto C_j é um submódulo de $M_n(D)$. Mostramos que C_j é um $M_n(D)$-módulo simples. Seja $N \neq 0$ um submódulo de C_j. Como N não é 0, segue que N contém um vetor $v \neq 0$. Este vetor visto como uma matriz de $M_n(D)$ é da forma $v = \sum_{l=1}^{n} c_l E_{l,j}$, onde $E_{i,j}$ são as chamadas matrizes elementares, que são as matrizes que possuem o número 1 na posição (i, j) e têm as outras posições preenchidas com zeros. Como $v \neq 0$, segue que existe $1 \leq k \leq n$ tal que $c_k \neq 0$. Como D é um anel de divisão, segue que todo elemento não nulo possui inverso. Assim, temos que ${c_k}^{-1} E_{i,k} v = E_{i,j} \in N$ (pois $E_{i,j} E_{l,j} = 0$ para todo $i \neq j$) para todo i. Do fato de que $E_{i,j}$ gera C_j, concluímos que $N = C_j$, ou seja, C_j é simples, como queríamos mostrar. Além disso, nota-se claramente que $M_n(D) = \bigoplus_{j=1}^{n} C_j$ e que todos os $C_j's$ são isomorfos como $M_n(D)$-módulos a D^n, conjunto de vetores colunas com entrada em D. Aliás, vale mais do que isso, todos os $M_n(D)$-módulos simples são isomorfos, como afirma o próximo lema.

Lema 2.18. *Se S é um $M_n(D)$-módulo simples, então $S \cong D^n$.*

Demonstração. Seja S um $M_n(D)$-módulo simples. Pela Proposição 1.46, segue que $S = M_n(D)v$, para qualquer $v \in S \backslash \{0\}$. Como $D^n \cong C_j$, segue que D^n também é simples, e logo, $D^n = M_n(D)e_1$ (porque um módulo simples é gerado por qualquer um de seus elementos), onde e_1 é o primeiro vetor da base canônica ordenada. Assim, podemos definir o seguinte homomorfismo

$$\begin{aligned} f: \ S &\to D^n \\ v &\mapsto e_1. \end{aligned}$$

Essa definição de f dada a partir dos geradores, estende-se para todo o conjunto S. Como $f \neq 0$, pelo Lema 1.47, segue que f é um isomorfismo, e portanto, $S \cong D^n$, ou

seja, todo $M_n(D)$-módulo simples é isomorfo a D^n. □

Teorema 2.19. *(Teorema de Wedderburn para álgebras simples) Se A é uma K-álgebra simples, então A é isomorfo à álgebra $D_n = M_n(D)$ das matrizes $n \times n$ para algum inteiro $n > 1$ com coeficientes em uma K-álgebra de divisão D.*

Demonstração. Seja M um ideal minimal à esquerda de A. O ideal M existe visto que A é um K-espaço vetorial de dimensão finita. Pelo Lema 2.16, segue que M é simples, e como provamos no Corolário 1.48, segue que $D = \mathrm{End}_R(M)$ é uma álgebra de divisão. Podemos ver M como um D-módulo à esquerda via a ação $dm = d(m)$, para todo $m \in M$ e para todo $d \in D$. Desta forma, podemos definir a aplicação de D-módulos $g_a : M \to M$ por $g_a(x) = ax$. Claramente, $g_a \in \mathrm{End}_D(M)$, para todo $a \in A$. Consideremos, então, o homomorfismo de K-álgebras

$$\begin{array}{rccc} i: & A & \to & \mathrm{End}_D(M) \\ & a & \mapsto & g_a \end{array}.$$

Mostramos que i é bijetivo. Por A ser simples, segue que i é injetivo. Para verificar a sobrejetividade, consideramos a aplicação $h_y : M \to M$ dada por $h_y(x) = xy$, que obviamente pertence a D. Assim, $f(xy) = f(h_y(x)) = f(h_y \cdot x) = h_y \cdot (f(x)) = h_y(f(x)) = f(x)y$, para todo $x, y \in M$ e para todo $f \in \mathrm{End}_D(M)$. Usando este fato, vamos mostrar que $i(M)$ é um ideal à esquerda de $\mathrm{End}_D(M)$. De fato, dados $f \in \mathrm{End}_D(M)$ e $x, y \in M$, segue que $f.i(x)y = f(i(x)y) = f(xy) = f(x)y = i(f(x))(y)$, e consequentemente, $f.i(x) = i(f(x)) \in i(M)$, para todo $f \in \mathrm{End}_D(M)$, ou seja, $i(M)$ é ideal de $\mathrm{End}_D(M)$. Usando novamente o fato de A ser simples, segue que $A = MA$, e assim, $i(A) = i(MA) = i(M)i(A)$ é ideal à esquerda de $\mathrm{End}_D(M)$. Como $id_M = i(1_R) \in i(A)$, segue que $i(A) = \mathrm{End}_D(M)$, ou seja, i é sobrejetora, e logo, $A \cong \mathrm{End}_D(M)$. Além disso, pelo fato de A ser uma álgebra de dimensão finita sobre K, segue que a dimensão de M como D-espaço vetorial é finita, digamos n, e desse modo, $\mathrm{End}_D(M) \cong M_n(D)$. Assim, concluímos que $A \cong M_n(D)$. Para concluir a demonstração do teorema resta provar que a álgebra D e o inteiro n são unicamente determinados por A. Para mostrar isso, suponhamos que D e D' são K-álgebras de divisão tal que as correspondentes álgebras de matrizes, D_n e D'_n, são isomorfas. Devemos mostrar que $D \cong D'$ e $n = n'$. Para mostrar que $D \cong D'$, é suficiente mostrar que, para todo D_n-módulo simples N, existe um isomorfismo de K-álgebras em que $D \cong \mathrm{End}_{D_n}(N)$. Pelo Lema 2.18, segue que quaisquer dois D_n-módulos à esquerda são isomorfos a D^n, e assim, podemos tomar $N = D^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in D \right\}$. Além disso,

$N = D^n$ é também um D-módulo à direita, o que nos permite considerar a aplicação $\phi : D \to \mathrm{End}_{D_n}(D^n)$ dada por $\phi(d)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 d \\ \vdots \\ x_n d \end{pmatrix}$, para todo $d, x_1, \ldots, x_n \in D$. Claramente, ϕ é um homomorfismo injetor, visto que D é um anel de divisão. Para ver a sobrejetividade, tomamos $f \in \mathrm{End}_{D_n}(D^n)$ e escrevemos $f(e_1) = e_1\lambda_1 + \cdots + e_n\lambda_n$, onde $\lambda_i \in D$ e $\{e_1, \ldots, e_n\}$ é a base canônica de D. Das equações $f(e_1) = f(E_{11}e_1) = E_{11}f(e_1) = E_{11}\lambda_1$ e $f(e_j) = f(E_{j1}e_1) = E_{j1}\lambda_1$, para $2 \leq j \leq n$, segue que $\phi(e_j) = f$, e portanto, ϕ é sobrejetor. Por fim, pelo fato que $D \cong D'$, segue que $n^2 = \dim_D D^n = \dim_{D'} D'_{n'} = n'^2$, que implica que $n = n'$. Com isso, o teorema está demonstrado. □

Teorema 2.20 (Teorema de Wedderburn para álgebras semi-simples)**.** *Uma K-álgebra A é semi-simples se, e somente se, existem inteiros n_i e álgebras de divisão D_i tal que*

$$A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r).$$

Demonstração. Pelo Teorema 2.17, segue que A é soma direta de álgebras simples, e pelo Teorema de Wedderburn para álgebras simples, segue que toda ágebra simples é isomorfa a $M_n(D)$, onde D é uma álgebra de divisão. Assim, a demonstração desse teorema sai diretamente da aplicação desses dois resultados. □

A próxima proposição nos dá algumas definições equivalentes para álgebras semi-simples, que utilizamos na próxima seção.

Proposição 2.21. *Seja A uma K-álgebra de dimensão finita não necessariamente comutativa. As seguintes afirmações são equivalentes (os módulos e submódulos referidos são sempre à esquerda):*

1. *A é semi-simples.*
2. *A é uma soma direta finita de ideais minimais.*
3. *Todo A-módulo é uma soma de submódulos simples.*
4. *Todo submódulo de um A-módulo M é somando direto de M.*
5. *Toda sequência exata de A-módulos*

$$0 \to M' \to M \to M'' \to 0$$

cinde.

6. *Todo ideal à esquerda de A é um somando direto de A como um A-módulo.*

7. A não contém ideais laterais nilpotentes.

Demonstração. $(1 \Rightarrow 2)$ decorre do Teorema 2.15.

$(2 \Rightarrow 3)$ Por hipótese e pelo Teorema 2.12, segue que $A = Ae_1 \oplus \cdots \oplus Ae_r$, onde os e_i são idempotentes não nulos tal que $e_i e_j = 0$ para $i \neq j$. Assim, dado um A-módulo M, segue que $M = \sum_{x \in M} \sum_{i=1}^{r} Ae_i x$. Além disso, a aplicação

$$\begin{array}{rccc} \varphi: & Ae_i & \to & Ae_i x \\ & ae_i & \mapsto & ae_i x \end{array}$$

é um homomorfismo sobrejetivo de A-módulos. Como $\mathrm{Ker}(\varphi) \subset Ae_i$ é um ideal de A e Ae_i são ideais minimais, segue que $\mathrm{Ker}(\varphi) = 0$ ou $\mathrm{Ker}(\varphi) = Ae_i$. Supondo que $\mathrm{Ker}(\varphi) = 0$, segue que φ é um isomorfismo e então, pelo fato de Ae_i ser semi-simples, segue que $Ae_i x$ também é. Supondo que $\mathrm{Ker}(\varphi) = Ae_i$, segue que $Ae_i x = 0$, ou seja, em ambos os casos $Ae_i x$ é simples, de onde concluímos que M, e logo, todo A-módulo é uma soma de submódulos simples.

$(3 \Rightarrow 4)$ Segue da Proposição 1.55.

$(4 \Rightarrow 5)$ Se $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ é uma sequência exata de A-módulos, então $f(M')$ é um submódulo de M e logo, por hipótese, segue que existe $H \subset M$ tal que $M = f(M') \oplus H$. Como g é sobrejetora, dado $x'' \in M''$ existe $x \in M$ tal que $g(x) = x''$. Por outro lado, da igualdade $M = f(M') \oplus H$, segue que existem $y \in f(M') = \mathrm{Ker}(g)$ e $z \in H$ tal que $x = y + z$. Logo, $x'' = g(x) = g(y + z) = g(y) + g(z) = g(z)$, sendo este z único. Para concluir a prova, consideremos o seguinte A-homomorfismo

$$\begin{array}{rccc} h: & M'' & \to & M \\ & x'' & \mapsto & z. \end{array}$$

Observamos que $g \circ h(x'') = g(z) = x''$, ou seja, $g \circ h = id_{M''}$, e portanto, a sequência cinde.

$(5 \Rightarrow 6)$ Seja I um ideal à esquerda de A e consideremos a sequência exata de A-módulos

$$0 \to I \to A \xrightarrow{\pi} A/I \to 0.$$

Por hipótese, esta sequência cinde, ou seja, existe $h : A/I \to A$ tal que $\pi \circ h = id_{A/I}$.

Logo, $A = I \oplus h(A/I)$, o que mostra que I é somando direto de A.

$(6 \Rightarrow 7)$ Sabemos que $N(A)$ é um ideal à esquerda de A, e assim, por hipótese, segue que existe um ideal N' de A tal que $A = N(A) \oplus N'$. Assim, existem $x \in N(A)$ e $x' \in N'$ tal que $1 = x + x'$, e então, $x = x^2 + xx'$. Desta igualdade, segue que $x - x^2 = xx' \in N(A) \cap N' = 0$, donde segue que $x^2 = x$. Mas, como $x \in N(A)$, x é nilpotente, e então existe um inteiro $n > 1$ tal que $x^n = 0$, e logo, $x = x^2 = \cdots = x^n = 0$. Desta forma, da igualdade $1 = x + x'$, segue que $x' = 1$, e consequentemente, $N' = A$. Sendo assim, só podemos ter $N(A) = 0$, ou seja, A não tem ideais laterais nilpotentes.

$(7 \Rightarrow 1)$ Sai diretamente da definição de álgebra semi-simples. □

Observação 2.22. Existe também uma teoria de álgebras semi-simples sobre anéis comutativos, que encontra-se em [8], onde é dada uma caracterização das álgebras semi-simples sobre anéis noetherianos. Não exploramos esta parte neste trabalho pois esta teoria exige conhecimentos prévios que fogem ao nosso objetivo.

2.3 Álgebras separáveis

Nesta seção, apesentamos as álgebras separáveis, que são um tipo de álgebra semi-simples. Inicialmente, apresentamos uma definição para álgebras separáveis sobre um corpo K, que podem ser interpretadas como sendo as K-álgebras semi-simples sobre K que permanecem semi-simples sobre um corpo $L \supset K$. Em seguida, apresentamos outras versões de definições e propriedades que valem para álgebras sobre corpos e se estendem naturalmente para o caso geral das álgebras sobre um anel comutativo.

Definição 2.23. *Seja A uma K-álgebra de dimensão finita. Dizemos que A é **separável** sobre K, se $A \otimes_K E$ é uma E-álgebra semi-simples, para todo corpo E contendo K. Em particular, $A = A \otimes_K K$ deve ser semi-simples se A for separável.*

Pelo fato de as álgebras separáveis serem semi-simples, segue o seguinte teorema.

Teorema 2.24. *(Teorema de Wedderburn para álgebras separáveis) Seja A uma K-álgebra de dimensão finita. Assim, A é separável sobre K se, e somente se, $A \cong M_{n_1}(D_1) \otimes \cdots \otimes M_{n_r}(D_r)$, sendo D_i K-álgebras de divisão de dimensão finita.*

Exemplo 2.25. Se $F_1, \ldots, F_r$ são extensões finitas separáveis de um corpo K, então a álgebra $A = F_1 \oplus \cdots \oplus F_r$ é separável. De fato, se $L \supseteq K$ é uma extensão de K, então $A \otimes_K L = (\bigoplus_{i=1}^{r} F_i) \otimes_K L = \bigoplus_{i=1}^{r} (F_i \otimes_K L)$. Como cada somando não possui nilpotentes

não-nulos, $A \otimes_K L$ também não os possui, ou seja, $A \otimes_K L$ é uma álgebra semi-simples. Portanto, pela Definição 2.23, segue que A é uma álgebra separável.

O Exemplo 2.25, representa todos as K-álgebras A comutativas que são separáveis sobre um corpo K, pois dada qualquer K-álgebra separável podemos representá-la da mesma forma como uma soma direta. Este fato segue do próximo corolário.

Corolário 2.26. *Seja A uma K-álgebra comutativa de dimensão finita. Assim, A é separável sobre K se, e somente se, $A \cong F_1 \oplus \cdots \oplus F_n$, onde os F_i são extensões finitas separáveis de K.*

Demonstração. A condição "somente se" foi demonstrada no Exemplo 2.25. Mostremos que vale a condição "se". Pelos resultados Lema 2.11, Teorema 2.12, Lema 2.14 e Teorema 2.15, temos que $A = F_1 \oplus \cdots \oplus F_n$ e pelo Lema 2.16, segue que os únicos ideais de F_i são os triviais, logo, cada F_i é corpo. Para mostrar que cada F_i é extensão de K, considere a aplicação $i : K \to F_i$ definida por $i(\lambda) = \lambda e$ para todo $\lambda \in K$. A função i é um monomorfismo, e portanto, F_i é uma extensão de K. Supondo que F_i não é separável sobre K então existe uma extensão L de K tal que $F_i \otimes_K L$ tem pelo menos um elemento idempotente $x \neq 0$. Portanto, $(0, \ldots, 0, x, 0, \ldots, 0) \in F_1 \otimes_K L \oplus \cdots \oplus F_n \otimes_K L = A \otimes_K L$ é um elemento idempotente não nulo, o que contradiz o fato de que A é separável. Logo todos os F_i são separáveis. □

Corolário 2.27. *Seja A uma K-álgebra comutativa com elemento identidade 1 e dimensão finita. Assim, A é separável se, e somente se, existe um corpo de extensão E de K tal que $A \otimes_K E \cong E \oplus \cdots \oplus E$, para um número finito de somandos.*

Este corolário é um caso particular do seguinte lema:

Lema 2.28. *Seja A uma K-álgebra de dimensão finita. Assim, A é separável sobre K se, e somente se, existe um corpo E extensão de K tal que $A \otimes_K E = E_{n_1} \oplus \cdots \oplus E_{n_r}$ onde $E_{n_i} = M_{n_i}(E)$.*

Demonstração. Sejam A uma álgebra separável de dimensão finita sobre K e E um corpo algebricamente fechado contendo K. Assim, $A \otimes_K E$ é semi-simples, e portanto, pelo Teorema de Wedderburn, segue que $A \otimes_K E \cong D_{n_1}^{(1)} \oplus \cdots \oplus D_{n_r}^{(r)}$, onde $D^{(i)}$ são álgebras de divisão de dimensão finita sobre E. Suponhamos que $\dim_K D^{(i)} = m_i$ para $i = 1, \ldots, r$. Assim, para todo $x \in D^{(i)}$, o conjunto $\{1, x, x^2, \ldots, x^{m_i}\}$ é linearmente dependente, pois tem $m_i + 1$ elementos, e logo, existem $a_0, a_1, \ldots, a_{m_i} \in E$, não todos nulos, tal que $a_0 + a_1 x + \cdots + a_{m_i} x^{m_i} = 0$, de onde concluímos que x é algébrico sobre E, e portanto, $x \in E$. Com isso $D^{(i)} \subset E \subset D^{(i)}$, e logo, $D^{(i)} = E$, para todo $i = 1, \ldots, r$, donde segue que $A \otimes_K E \cong E_{n_1} \oplus \cdots \oplus E_{n_r}$. Reciprocamente, seja E um

corpo que é extensão de K tal que $A \otimes_K E \cong E_{n_1} \oplus \ldots, \oplus E_{n_r}$. Queremos mostrar que A é separável, isto é, que dado F um corpo arbitrário extensão de K, a álgebra $A \otimes_K F$ é semi-simples. Para isso, consideramos o corpo $EF = (E \otimes_K F)_M$ para algum ideal maximal M de $E \otimes_K F$. Pelo fato de que $E \cong E \otimes_K K \subset E \otimes_K F$ e a aplicação canônica $f : E \otimes_K F \to EF$ restrita a E é injetiva (pois se não fosse, existiria $0 \neq x \in F$ tal que $x \otimes 1 \in M$ e então $1 \otimes 1 = (x^{-1} \otimes 1)(x \otimes 1) \in M$, o que seria uma contradição), segue que $EF \supset E$. De modo análogo, segue que $EF \supset F$. Agora,

$$\begin{aligned} A \otimes_K EF &\cong (A \otimes_K E) \otimes_E EF \cong (E_{n_1} \oplus \cdots \oplus E_{n_r}) \otimes_E EF \\ &\cong E_{n_1} \otimes_E EF \oplus \cdots \oplus E_{nr} \otimes_E EF \cong (EF)_{n_1} \oplus \cdots \oplus (EF)_{nr}, \end{aligned}$$

ou seja, $A \otimes_K EF$ é semi-simples. Por outro lado, $A \otimes_K EF \cong (A \otimes_K F) \otimes_F EF$ e se $A \otimes_K F$ tivesse algum ideal nilpotente não nulo I, então $I \otimes_F EF$ seria um ideal nilpotente não nulo de $A \otimes_K EF$, o que contradiz o fato de ser semi-simples. Portanto, $A \otimes_K F$ é semi-simples. □

Agora, apresentamos uma teoria para álgebras separáveis sobre um corpo que pode ser estendida naturalmente ao caso de anéis comutativos. Antes, definimos a chamada álgebra envolvente, que será utilizada nesta caracterização das álgebras separáveis.

Seja A uma K-álgebra. Chamamos de **álgebra oposta** de A e denotamos por A^o ao conjunto A com a adição e multiplicação por escalar originais mas com a multiplicação entre elementos de A dada por $a * b = ba$, para todo $a, b \in A$. Seja $A^e = A \otimes_k A^o$ a denominada **álgebra envolvente**.

Podemos ver A como um A^e-módulo à esquerda com a multiplicação por escalar $(x \otimes y^o)a = xay$, para todo $a, x, y \in A$. A aplicação $f : A \times A^o \to A$ definida por $f(x, y^o) = xy$ é K-bilinear, e portanto, induz a aplicação K-linear

$$\begin{aligned} \psi : \quad A \otimes A^o &\to A \\ \sum x_i \otimes {y_i}^o &\mapsto \sum_{i=1}^{n} x_i y_i. \end{aligned}$$

A aplicação ψ é sobrejetora, pois dado $x \in A$, segue que $\psi(x \otimes 1^o) = x$. Além disso, para qualquer $a, b, x, y \in A$, segue que $\psi((a \otimes b^o)(x \otimes y^o)) = \psi(ax \otimes (yb)^o) = (ax)(yb) = a(xy)b = (a \otimes b^o)(xy) = (a \otimes b^o)\psi(x \otimes y^o)$, o que mostra que ψ é A^e-linear. Portanto, obtemos a seguinte sequência exata deA^e-módulos à esquerda

$$0 \to \mathrm{Ker}(\psi) \to A^e \xrightarrow{\psi} A \to 0.$$

Definição 2.29. *Seja A uma K-álgebra. Dizemos que A é uma álgebra separável, se A é um módulo projetivo quando visto como um A^e-módulo à esquerda.*

Diretamente da definição de módulo projetivo, segue que a Definição 2.29 é equivalente à seguinte: A é uma K-álgebra separável se, e somente se, a sequência exata de A^e-módulos à esquerda $0 \to \mathrm{Ker}(\psi) \to A^e \xrightarrow{\psi} A \to 0$ cinde.

A próxima proposição, além de fornecer uma outra definição para álgebras separáveis, introduzirá um elemento muito importante, chamado idempotente de separabilidade de A.

Proposição 2.30. *Uma K-álgebra A é separável se, e somente se, existe $e \in A^e$ tal que $\psi(e) = 1$ e $Ker(\psi)e = 0$.*

Demonstração. Por definição, segue que A é separável se, e somente se, a sequência exata de A^e-módulos à esquerda $0 \to \mathrm{Ker}(\psi) \to A^e \xrightarrow{\psi} A \to 0$ cinde. Assim, por hipótese, segue que existe um A^e-homomorfismo $h : A \to A^e$ tal que $\psi \circ h = id$. Seja $e = h(1) \in A^e$. Logo, $\psi(e) = 1$. Resta mostrar que $\mathrm{Ker}(\psi)e = 0$. Para isso observamos que $\mathrm{Ker}(\psi)$ é um ideal de A^e gerado por elementos da forma $a \otimes 1^o - 1 \otimes a^o$, para todo $a \in A$. De fato: $a \otimes 1^o - 1 \otimes a^o \in \mathrm{Ker}(\psi)$, pois $\psi(a \otimes 1^o - 1 \otimes a^o) = a1 - 1a = 0$. Por outro lado, se $\sum_{i=1}^{n} a_i \otimes {b_i}^o \in \mathrm{Ker}(\psi)$, então $\sum_{i=1}^{n} a_i b_i = 0$, e logo, $\sum_{i=1}^{n} a_i \otimes {b_i}^o = \sum_{i=1}^{n} (a_i \otimes 1^o)(1 \otimes {b_i}^o - b_i \otimes 1^o)$, ou seja, $\mathrm{Ker}(\psi)$ é gerado por elementos da forma $a \otimes 1^o - 1 \otimes a^o$. Assim, para mostrar que $(\psi)e = 0$, é suficiente mostrar que $(a \otimes 1^o - 1 \otimes a^o)e = 0$. Para isso, se $a \in A$, então

$$\begin{aligned} (a \otimes 1^o)e &= (a \otimes 1^o)h(1) = h((a \otimes 1^o)1) = h(a) \\ &= h((1 \otimes a^o)1) = (1 \otimes a^o)h(1) = (1 \otimes a^o)e. \end{aligned}$$

Consequentemente, $(a \otimes 1^o - 1 \otimes a^o)e = 0$, e portanto, $(\psi)e = 0$. Reciprocamente, por hipótese, segue que existe $e \in A^e$ tal que $\psi(e) = 1$ e $(\psi)e = 0$. Consideremos a aplicação $h : A \to A^e$ definida por $h(a) = (a \otimes 1^o)e = (1 \otimes a^o)e$. Assim, $h(a + b) = h(a) + h(b)$, para todo $a, b \in A$ e $\psi \circ h = id$. Além disso, dados $a, b, c \in A$ segue que $h((a \otimes b^o)c) = h(acb) = (acb \otimes 1^o)e = (ac \otimes 1^o)(b \otimes 1^o)e = (ac \otimes b^o)e = (a \otimes b^o)(c \otimes 1^o)e = (a \otimes b^o)h(c)$, ou seja, h é um A^e-homomorfismo, e portanto, a sequência $0 \to \mathrm{Ker}(\psi) \to A^e \xrightarrow{\psi} A \to 0$ cinde, e portanto, A é separável. □

O elemento $e \in A^e$ da Proposição 2.30 é elemento idempotente, uma vez que $e^2 - e = (e - 1)e \in \mathrm{Ker}(\psi)e = 0$. Por isso, o elemento é chamado **idempotente de separabilidade de A**. Portanto, podemos concluir que A é separável se, e somente se, possui um idempotente de separabilidade. Encontrar o elemento de separabilidade é, em muitos casos, uma maneira mais prática de mostrar que a álgebra é separável.

Agora, vamos verificar que a Definição 2.23 é equivalente à Definição 2.29.

Teorema 2.31. *Seja A uma K-álgebra. Assim, A é separável ($A \otimes_K L$ é semi-simples) se, e somente se, a sequência exata curta de A^e-módulos $0 \to Ker(\psi) \to A^e \xrightarrow{\psi} A \to 0$ cinde.*

Demonstração. Suponhamos que A é separável sobre K. Consequentemente, A^o também é separável sobre K. Assim, pelo Lema 2.28, segue que existem corpos E e E' contendo K tal que $A \otimes_K E \cong E_{n_1} \oplus \cdots \oplus E_{n_r}$ e $A^o \otimes_K E' \cong E'_{m_1} \oplus \cdots \oplus E_{m_s}$. Consideremos o corpo $EE' \cong (E \otimes_K E')_M$, para algum ideal maximal M de $E \otimes_K E'$. Como EE' contém E e E', segue que

$$\begin{aligned} A \otimes_K EE' &\cong (A \otimes_K E) \otimes_E EE' \cong (EE')_{n_1} \oplus \cdots \oplus (EE')_{n_r} \quad \text{e} \\ A^o \otimes_K EE' &\cong (A \otimes_K E') \otimes_{E'} EE' \cong (EE')_{m_1} \oplus \cdots \oplus (EE')_{m_s}, \end{aligned}$$

e consequentemente,

$$\begin{aligned} A \otimes_K A^o \otimes_K EE' &\cong (A \otimes_K EE') \otimes_{EE'} (A^o \otimes_K EE') \\ &\cong ((EE')_{n_1} \oplus \cdots \oplus (EE')_{n_r}) \otimes_{EE'} ((EE')_{m_1} \oplus \cdots \oplus (EE')_{m_s}) \\ &\cong (EE')_{n_1 m_1} \oplus \cdots \oplus (EE')_{n_1 m_s} \oplus \\ &\quad \cdots \oplus (EE')_{n_r m_1} \oplus \cdots \oplus (EE')_{n_r m_s}, \end{aligned}$$

e portanto, $A^e \cong A \otimes_K A^o$ é uma K-álgebra separável, e consequentemente, semi-simples. Logo, pela Proposição 2.21, segue que toda sequência exata de A^e-módulos cinde, em particular, a sequência exata de A^e-módulos $0 \to \mathrm{Ker}(\psi) \to A^e \xrightarrow{\psi} A \to 0$ cinde. Reciprocamente, para mostrar que A é separável, de acordo com a Definição 2.23, devemos mostrar que $A \otimes_K F$ é semi-simples, para todo corpo F contendo K. Sendo assim, seja F uma extensão de K e $B = A \otimes_K F$ uma F-álgebra. Nosso objetivo é provar que B é semi-simples, e para isso vamos mostrar que todo submódulo de um B-módulo é um somando direto. Primeiramente, observamos que como $B^e = B \otimes_F B = (A \otimes_K F) \otimes_F (A \otimes_K F) = (A \otimes_K A) \otimes_F F = A^e \otimes_F F$, podemos definir um isomorfismo $\theta : B^e \to A^e \otimes_K F$. Além disso, como por hipótese a sequência $0 \to \mathrm{Ker}(\psi) \to A^e \xrightarrow{\psi} A \to 0$ cinde, segue que existe um homomorfismo $\nu : A \to A^e$ tal que $\psi \circ \nu = 1_R$. Sejam

$$\psi' = (\psi \otimes 1) \circ \theta : B^e \to A^e \otimes_K F \to B \qquad \text{e}$$

$$\nu' = \theta^{-1} \circ (\nu \otimes 1) : B \to A^e \otimes_K F \to B^e,$$

onde $\psi' \circ \nu' = 1_B$. Sejam M um B-módulo e N um B-submódulo de M. Como ambos são B-módulos, consequentemente são também K-espaço vetoriais. Portanto, podemos

definir a projeção K-linear $\pi : M \to N$ tal que $\pi|_N = id_N$. Seja $\nu'(1) = \sum_{i=1}^{r} x_i \otimes y_i$. Aplicando ψ' em ambos os lados, segue que

$$1 \overset{\psi' \circ \nu' = 1_B}{=} \psi'(\nu'(1)) = \sum_{i=1}^{r} \psi'(x_i \otimes y_i) = \sum_{i=1}^{r} x_i y_i.$$

Dados uma aplicação K-linear $f : M \to M$ e $a \otimes b \in B^e$, definimos $(a \otimes b)f(m) = af(bm)$. Como π é K-linear, π satisfaz $(a \otimes b)\pi(m) = a\pi(bm)$. Seja $\pi' = \nu'(1)\pi : M \to M$. Se π' for um projetor, isto é, se $(\pi')^2 = \pi'$, segue que é B-linear com imagem N, e o teorema está provado (usando o seguinte resultado: $p : M \to M$ projetor $\Rightarrow M = \mathrm{Ker}(p) \oplus \mathrm{Im}(p)$). Mostramos, então, que isso vale.

- $(\pi')^2 = \pi'$, o que mostra que π' é projetor.
- Se $n \in N$, então

  $$\pi'(n) = \nu'(1)\pi(n) = \sum_{i=1}^{r} x_i \otimes y_i \pi(n) = \sum_{i=1}^{r} x_i \pi(y_i n) = \sum_{i=1}^{r} x_i y_i n = n.$$

  Logo, $N \subset \mathrm{Im}(\pi')$. Como a outra inclusão é óbvia, segue que $N = \mathrm{Im}(\pi')$.
- Se $b \in B$ e $m \in M$, então

  $$\begin{aligned} \pi'(bm) &= (1 \otimes b)\pi'(m) = (1 \otimes b)\nu'(1)\pi(m) = \nu'(1 \otimes b)\pi(m) = \nu'(b \otimes 1)\pi(m) \\ &= (b \otimes 1)\nu'(1)\pi(m) = (b \otimes 1)\pi'(m) = b\pi'(m), \end{aligned}$$

  ou seja, π' é B-linear.

Assim, mostramos que $M = N \oplus \mathrm{Im}(\pi')$, ou seja, que N é um somando direto de M. Portanto, B é uma álgebra semi-simples, como queríamos mostrar, e disto segue que A é separável. □

Exemplo 2.32. $\mathbb{R}$ é separável sobre $\mathbb{R}$, cujo idempotente de separabilidade é $1 \otimes 1$.

Exemplo 2.33. A álgebra das matrizes $n \times n$, $M_n(R)$, é separável. De fato, sejam e_{ij} as matrizes elementares. Mostramos que $e = \sum_{i=1}^{n} e_{ij} \otimes e_{ji}$ onde j é um inteiro fixo entre 1 e n, é um idempotente de separabilidade de $M_n(R)$. Assim,

$$\psi(e) = \sum_{i=1}^{n} e_{ij} e_{ji} = \sum_{i=1}^{n} e_{ii} = 1 \ (e_{ii} = 1 \ \text{ para } \ i = j \ \text{ e } \ e_{ii} = 0 \ \text{ para } \ i \neq j).$$

Além disso, para todo k, l, segue que

$$\begin{aligned}(e_{kl}\otimes 1 - 1\otimes e_{kl})e &= (e_{kl}\otimes 1 - 1\otimes e_{kl})(\sum_{i=1}^{n} e_{ij}\otimes e_{ji}) \\ &= \sum_{i=1}^{n}(e_{kl}e_{ij}\otimes e_{ji} - e_{ij}\otimes e_{ji}e_{kl}) \\ &= e_{kj}\otimes e_{jl} - e_{kj}\otimes e_{jl} = 0.\end{aligned}$$

Como $e_{kl}\otimes 1 - 1\otimes e_{kl}$ gera $\mathrm{Ker}(\psi)$, segue que $\mathrm{Ker}(\psi)e = 0$. Portanto, $M_n(R)$ é uma R-álgebra separável e e é o idempotente de separabilidade.

Exemplo 2.34. Agora, veremos um exemplo de uma álgebra sobre um anel que não é separável. Considere $A = \mathbb{Z}[\sqrt{2}]$ e $R = \mathbb{Z}$. Suponhamos que A é uma álgebra separável com idempotente de separabilidade $x \in A^e$. Do fato que A tem $\{1, \sqrt{2}\}$ como base, segue que $\{1\otimes 1, 1\otimes\sqrt{2}, \sqrt{2}\otimes 1, \sqrt{2}\otimes\sqrt{2}\}$ é uma base para A^e. Logo, existem $a, b, c, d \in R$ tal que $x = a(1\otimes 1) + b(1\otimes\sqrt{2}) + c(\sqrt{2}\otimes 1) + d(\sqrt{2}\otimes\sqrt{2})$. Como x é idempotente de separabilidade, segue que $1 = \psi(x) = (a+2d) + (b+c)\sqrt{2}$, que nos dá o sistema

$$\begin{cases} a + 2d = 1 \\ b + c = 0. \end{cases}$$

Além disso, x deve satisfazer a igualdade $\mathrm{Ker}(\psi)x = 0$, isto é, $ax = 0$, para todo $a \in \mathrm{Ker}(\psi)$. Como $1\otimes\sqrt{2} - \sqrt{2}\otimes 1 \in \mathrm{Ker}(\psi)$, segue que $(1\otimes\sqrt{2} - \sqrt{2}\otimes 1)x = 0$, e logo, $(1\otimes\sqrt{2})x = (\sqrt{2}\otimes 1)x$. Assim,

- $(1\otimes\sqrt{2})x = (1\otimes\sqrt{2})[a(1\otimes 1) + b(1\otimes\sqrt{2}) + c(\sqrt{2}\otimes 1) + d(\sqrt{2}\otimes\sqrt{2})] = a(1\otimes\sqrt{2}) + b(1\otimes 2) + c(\sqrt{2}\otimes\sqrt{2}) + 2d(1\otimes\sqrt{2})$
- $(\sqrt{2}\otimes 1)x = (\sqrt{2}\otimes 1)[a(1\otimes 1) + b(1\otimes\sqrt{2}) + c(\sqrt{2}\otimes 1) + d(\sqrt{2}\otimes\sqrt{2})] = a(\sqrt{2}\otimes 1) + b(\sqrt{2}\otimes\sqrt{2}) + c(2\otimes 1) + 2d(1\otimes\sqrt{2})$.

Portanto, a, b, c e d devem satisfazer também o sistema

$$\begin{cases} a = 2d \\ b = c. \end{cases}$$

Assim, devemos ter $b = c = 0$, $d = \frac{1}{4}$ e $a = \frac{1}{2}$, o que é uma contradição, visto que, por hipótese, a, b, c e d são todos números inteiros. A contradição segue do fato de supormos que x é idempotente de separabilidade de A, logo, A não pode possuir elemento de separabilidade, e portanto, A não é separável.

Vejamos, agora, um teorema que será utilizado no próximo capítulo.

Teorema 2.35. *Se R é um anel e P um R-módulo projetivo finitamente gerado, então $A = Hom_R(P,P)$ é uma R-álgebra separável e central.*

Demonstração. Para mostrar que A é separável, vamos exibir seu idempotente de separabilidade. Como P é projetivo finitamente gerado e fiel, pelo Corolário 1.44 segue que $R = T_R(P)$, e com isso, existem elementos $x_1, \ldots, x_n \in P$ e $g_1, \ldots, g_m \in P^*$ tal que $\sum_{j=1}^{n} g_j(x_i) = 1$. Também, pela hipótese de que P é projetivo finitamente gerado, sabemos que existem elementos $p_1, \ldots, p_n \in P$ e $f_1, \ldots f_n \in P^*$ tal que $\sum_{i=1}^{n} f_i(p)p_i = p$, para todo $p \in P$. A partir destes elementos, definimos $E_{ij}, F_{ji} \in A$ por $E_{ij}(p) = g_j(p)p_i$ e $F_{ji}(p) = f_i(p)x_j$, para todo $p \in P$, $1 \leq i \leq n$ e $1 \leq j \leq m$. Mostramos que $e = \sum_{i,j} E_{ij} \otimes F_{ji}^o \in A \otimes_R A^o$ é idempotente de separabilidade de A. De fato,

$$\begin{aligned}
\mu(e)(p) &= \sum_{i,j} E_{ij}F_{ji}(p) = \sum_{i,j} E_{ij}(f_i(p)x_j) = \sum_{i,j} f_i(p)E_{ij}(x_j) \\
&= \sum_{i,j} f_i(p)g_j(x_j)p_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} g_j(x_j)\right) f_i(p)p_i \\
&= \sum_{i=1}^{n} f_i(p)p_i = p,
\end{aligned}$$

para todo $p \in P$. Logo, $\mu(e) = id_P = 1_R$. Para mostrar que $(f \otimes 1^o)e = (1 \otimes f)e$, para todo $f \in A$, observamos, primeiramente, que o conjunto $\{D_{kl} | 1 \leq k, l \leq n\}$, onde $D_{kl}(p) = f_l(p)p_k$ para todo $p \in P$, gera A. De fato, seja $f \in A$ e $f(p_k) = \sum_{l=1}^{n} c_{kl}p_l$, então

$$f(p) = f\left(\sum_{k=1}^{n} f_k(p)p_k\right) = \sum_{k=1}^{n} f_k(p)f(p_k) = \sum_{k,l} c_{kl}f_k(p)p_l = \sum_{k,l} c_{kl}D_{kl},$$

para todo $p \in P$, ou seja, $f = \sum_{k,l} c_{kl}D_{lk}$, para todo f. Desta forma, é suficiente verificar que $(f \otimes 1^o)e = (1 \otimes f^o)e$ para o conjunto de geradores D_{kl}, isto é, que $(D_{kl} \otimes 1^o)e = (1 \otimes D_{kl}^o)e$. Antes, observamos que

$$(D_{kl} \otimes 1^o)e = (D_{kl} \otimes 1^o)\left(\sum_{i,j} E_{ij} \otimes F_{j,i}^o\right) = \sum_{i,j} DklE_{ij} \otimes F_{ji}^o$$

e

$$\begin{aligned}
D_{kl}E_{ij}(p) &= D_{kl}(g_j(p)p_i) = f_l(g_j(p)p_i)p_k \\
&= g_j(p)f_l(p_i)p_k = f_l(p_i)g_j(p)p_k = f_l(p_i)E_{kj}(p) = r_{il}E_{kj}(p),
\end{aligned}$$

onde $r_{il} = f_l(p_i) \in R$, para todo $p \in P$, e assim, $D_{kl}E_{ij} = r_{il}E_{kj}$. Logo, $(D_{kl} \otimes 1^o)e = \sum_{i,j} r_{il}E_{kl} \otimes F^o_{ji} = \sum_{i,j} E_{kj} \otimes r_{ij}F^o_{ji}$. Mas,

$$\sum_i r_{il}F_{ji}(p) = \sum_i f_l(p_i)f_i(p)x_j = f_l\left(\sum_i f_i(p)p_i\right)x_j = f_l(p)x_j = F_{jl}(p),$$

para todo $p \in P$, ou seja, $\sum_i r_{il}F_{ji} = F_{jl}$. Consequentemente, $(D_{kl} \otimes 1^o)e = \sum_j E_{kj}F^o_{jl}$. Por outro lado, $(1 \otimes D^o_{kl})e = \sum_{i,j} E_{ij} \otimes D^o_{kl}F^o_{ji} = \sum_{i,j} E_{ij} \otimes (F_{ji}D_{kl})^o$. De modo análogo segue que $F_{ji}D_{kl} = r_{ki}F_{jl}$, com $r_{ki} = f_i(p_k) \in R$. Assim,

$$(1 \otimes D^o_{kl})e = \sum_{i,j} E_{ij} \otimes r_{ki}F^o_{jl} = \sum_{i,j} r_{ki}E_{ij} \otimes F^o_{jl} = \sum_i \left(\sum_j r_{ki}E_{ij}\right) \otimes F^o_{jl}.$$

Usando novamente o mesmo raciocínio, segue que $\sum_i r_{ki}E_{ij} = E_{kj}$, e logo, $(1 \otimes D^o_{kl})e = \sum_i E_{kj} \otimes F^o_{jl} = (D_{kl} \otimes 1^o)e$. Portanto, A é uma R-álgebra separável. Mostramos, agora, que A é central, isto é, que $Z(A) \cong R$. Vamos verificar essa equivalência em duas etapas, primeiro mostramos que $Z(A) = eA$, e em seguida, que $eA = R$. Dados $f, g \in A$, segue que

$$(ef)g = (1 \otimes g^o)(ef) = [(1 \otimes g^o)e]f = [(g \otimes 1^o)e]f = (g \otimes 1^o)(ef) = g(ef),$$

o que mostra que $ef \in Z(A)$, e consequentemente, $eA \subset Z(A)$. Agora, consideramos $f \in Z(A)$. Assim,

$$ef = \left(\sum_{i,j} E_{ij} \otimes F^o_{ji}\right)f = \sum_{i,j} E_{ij}fF_{ji} = \left(\sum_{i,j} E_{ij}F_{ji}\right)f = \mu(e)f = 1f = f,$$

de onde segue que $Z(A) \subset eA$, e portanto, $Z(A) = eA$. No que se segue mostramos que $eA = R$. Dado $f \in Z(A)$, segue f é um R-homomorfismo, e assim, para todo $r \in R, x \in S$, segue que $rf(x) = f(rx) = fr(x)$, o que mostra que $R \subset Z(A) = eA$. Para a inclusão contrária, considere $D_{kl} \in A$. Assim,

$$eD_{kl} = \left(\sum_{i,j} E_{ij} \otimes F^o_{ji}\right)D_{kl} = \sum_{i,j} E_{ij}D_{kl}F_{ji}$$

e

$$\begin{aligned} E_{ij}D_{kl}F_{ji}(p) &= E_{ij}D_{kl}(f_i(p)x_j) = f_i(p)E_{ij}(D_{kl}(x_j)) \\ &= f_i(p)E_{ij}(f_l(x_j)p_k) = f_i(p)f_l(x_j)E_{ij}(p_k) = f_i(p)f_l(x_j)g_j(p_k)p_i, \end{aligned}$$

de onde segue que

$$\begin{aligned} eD_{kl}(p) &= \sum_{i,j} f_i(p)f_l(x_j)g_j(p_k)p_i = \sum_j f_l(x_j)g_j(p_k)\sum_i f_i(p)p_i \\ &= \sum_j f_l(x_j)g_j(p_k)p = \lambda_{kl}1(p), \end{aligned}$$

para todo $p \in P$, onde $\lambda_{kl} = \sum_j f_l(x_j)g_j(p_k) \in R$. Portanto, $eD_{kl} \in R1$, e logo, $Z(A) = eA = R1$. Portanto, A é central. □

2.4 Considerações finais

Neste capítulo, apresentamos a definição de uma R-álgebra, onde R é um anel, além de apresentar algumas propriedades importantes. Duas álgebras particulares que são fundamentais para o desenvolvimento deste trabalho, são as álgebras semi-simples e as álgebras separáveis, apresentadas detalhadamente neste capítulo. As álgebras separáveis serão utilizadas no Capítulo 3, onde são imprescindíveis. As álgebras semi-simples possuem uma aplicação na teoria dos códigos sobre anéis. A construção dos códigos sobre $\mathbb{Z}_m$ é feita no Capítulo 4.

3 Teoria de Galois

A teoria de Galois sobre corpos mostrou-se muito útil em várias áreas da matemática, e por esta razão, alguns matemáticos se interessaram em estudar variações da mesma. Entre estes estudos, estão: teoria de Galois sobre anéis de divisão, em particular, sobre anéis não comutativos, teoria de Galois sobre equações diferenciais e teoria de Galois sobre anéis comutativos. Neste trabalho, apresentamos a Teoria de Galois sobre anéis comutativos.

O objetivo, deste capítulo, é generalizar a Teoria de Galois finita conhecida sobre corpos para anéis comutativos. Analisamos algumas das definições equivalentes de extensão galoisiana de um corpo com o intuito de encontrar qual a mais adequada a uma generalização para o caso dos anéis comutativos. As álgebras separáveis são elementos fundamentais para o desenvolvimento desta teoria. As definições, os resultados e as demonstrações aqui apresentados tiveram [5], [13], [16], [18], [19] e [22] como referência.

3.1 Alguns fatos sobre a teoria de Galois sobre corpos

Nesta seção, apresentamos alguns fatos da teoria de Galois sobre corpos e apresentamos outras versões para conceitos já conhecidos sobre polinômios e extensões de corpos separáveis, utilizando os fatos vistos nos Capítulos 1 e 2, em especial o conceito de álgebra separável. Para isso, vamos começar explorando um pouco as definições de polinômio e extensão separável, a fim de dar uma caracterização a elas. Lembramos que um polinômio é separável sobre um corpo K, se possui somente raízes simples no seu corpo de raízes. Isso equivale a dizer que para qualquer extensão L de K, f não possui fatores repetidos em L. Uma extensão $L \supseteq K$ é separável, se todo elemento de L é separável sobre K, isto é, se seu polinômio minimal sobre K é separável.

Proposição 3.1. *Seja K um corpo e $f \in K[x]$ um polinômio irredutível. Assim, f é separável se, e somente se, $\frac{K[x]}{\langle f \rangle} \otimes_K L$ não tem elementos nilpotentes, ou seja, se $\frac{K[x]}{\langle f \rangle} \otimes_K L$ é semi-simples.*

Demonstração. Sejam $f \in K[x]$ um polinômio irredutível e separável em $K[x]$ e L uma extensão de K. Em $L[x]$, segue que f pode não ser irredutível, mas sabemos que é da forma $f = {p_1}^{n_1} \dots {p_r}^{n_r}$, onde cada p_i é irredutível. Como f é separável, segue que f não possui raízes repetidas em qualquer extensão de K. Assim, devemos ter $n_i = 1$, para $i = 1, \dots, r$. Passando o quociente e aplicando o Teorema Chinês do Resto, segue que

$$\frac{L[x]}{\langle f \rangle} \cong \frac{L[x]}{\langle p_1 \rangle} \oplus \dots \oplus \frac{L[x]}{\langle p_r \rangle}.$$

Como cada p_i é irredutível, segue que $\langle p_i \rangle$ é um ideal primo, e desse modo, $\frac{L[x]}{\langle p_i \rangle}$ é um domínio, que não tem elementos nilpotentes. Como $\frac{L[x]}{\langle f \rangle}$ é a soma direta dos $\frac{L[x]}{\langle p_i \rangle}$, segue que o conjunto $\frac{L[x]}{\langle f \rangle}$ também não possui elementos nilpotentes. Além disso, vimos no Capítulo 2 que $L[x] \cong K[x] \otimes_K L$, de onde concluímos que $\frac{K[x]}{\langle f \rangle} \otimes_K L$ não tem elementos nilpotentes, ou seja, é semi-simples. Reciprocamente, sejam $f \in K[x]$ irredutível e $L = K(\alpha)$. Se f possui uma raiz múltipla, α, em $L[x]$, então $(x - \alpha)^m = p_1(x)^m \in L[x]$. Assim, f escreve-se como $f(x) = p_1(x)^m g(x)$, onde $g(x) = p_2(x) \dots p_r(x)$, tal que $p_i(x) \in L[x]$ são irredutíveis. Em $\frac{L[x]}{\langle f \rangle}$, segue que $\overline{f(x)} = \overline{0}$, o que implica que $\overline{p_1(x)^m g(x)} = \overline{0}$. Como a soma é direta, segue que $\overline{0}$ se escreve de maneira única, e assim, $\overline{p_1(x)^m} = \overline{0}$ em $\frac{L[x]}{\langle p_1(x)^m \rangle}$ e $\overline{p_i(x)} = \overline{0}$, para todo $i = 2 \dots r$ em $\frac{L[x]}{\langle p_i(x) \rangle}$. Considere

$$\overline{h(x)} = (\overline{p_1(x)}, \overline{0}, \dots, \overline{0}) \in \frac{L[x]}{\langle f \rangle} = \frac{L[x]}{\langle p_1^m \rangle} \oplus \frac{L[x]}{\langle p_2 \rangle} \oplus \dots \oplus \frac{L[x]}{\langle p_r \rangle}.$$

Assim, $\overline{h(x)}^m = (\overline{p_1(x)}^m, \overline{0}^m, \dots, \overline{0}^m)$. Como $\overline{p_1(x)}^m = \overline{0}$, segue que $\overline{h(x)}^m = \overline{0}$, ou seja, $h(x)$ é um elemento nilpotente de $\frac{L[x]}{\langle f \rangle} \cong \frac{K[x]}{\langle f \rangle} \otimes_K L$, o que contradiz a hipótese do mesmo ser semi-simples. Desta forma, f não pode ter raízes múltiplas em L, de onde concluímos que f é separável. □

Corolário 3.2. *Seja $L \supseteq K$ uma extensão finita. Assim, L é uma extensão separável se, e somente se, $L \otimes_K F$ não tem elementos nilpotentes para toda extensão F de K.*

Demonstração. Seja $L \supseteq K$ uma extensão finita separável. Pelo Teorema do Elemento Primitivo, segue que existe $\alpha \in L$ algébrico com polinômio minimal $f \in K[x]$ separável tal que $L = K(\alpha)$. Assim, pela Proposição 3.1, segue que $\frac{K[x]}{\langle f \rangle} \otimes_K F$ não tem elementos nilpotentes, para toda extensão F de K. Mas $\frac{K[x]}{\langle f \rangle} = K(\alpha) = L$, e assim, $L \otimes_K F$ não tem elementos nilpotentes, para toda extensão F de K. Reciprocamente, suponhamos

que $L \otimes_K F$ não tem elementos nilpotentes para toda extensão F de K. Sejam $\alpha \in L$ e f seu polinômio minimal. O corpo $K(\alpha)$ é uma extensão de K, e assim, por hipótese, segue que $L \otimes_K K(\alpha)$ não tem elementos nilpotentes. Como $K(\alpha) = \frac{K[x]}{\langle f \rangle}$, segue que $L \otimes_K \frac{K[x]}{\langle f \rangle}$ não tem elementos nilpotentes, e assim, pela Proposição 3.1, segue que f é separável. Como tomamos $\alpha \in L$ qualquer, concluímos que L é separável. □

Analisando o Corolário (3.2) e a Definição 2.23 percebemos que o conceito de álgebra separável sobre um corpo é uma generalização do conceito de extensão separável de corpos. De fato, se $L \supseteq K$ é uma extensão de corpos, então L é um anel e, além disso, L pode ser visto como um K-espaço vetorial, ou seja, o corpo L pode ser visto como uma K-álgebra. Desta forma, toda extensão de um corpo K que é separável, é uma álgebra separável sobre K. Esta observação será fundamental no decorrer da próxima seção, cujo objetivo é encontrar condições para uma extensão de anéis ser galoisiana, de modo que generalize naturalmente o conceito de extensão galoisiana sobre corpos.

3.2 Teoria de Galois sobre anéis comutativos

Nesta seção, apresentamos uma generalização adequada da Teoria de Galois sobre corpos para a Teoria de Galois sobre anéis comutativos, readaptando as definições e resultados, inclusive o Teorema Fundamental da Teoria de Galois.

Vamos começar definindo extensão de anéis.

Definição 3.3. *Seja R um anel. Dizemos que um anel S é uma extensão de R se S é uma R-álgebra fiel, ou seja, se $r \in R\backslash\{0\}$, então $r \cdot 1 \neq 0$.*

A condição "se $r \in R\backslash\{0\}$, então $r \cdot 1 \neq 0$" quer dizer que o homomorfismo canônico $f : R \to S$ onde $f(r) = r \cdot 1$, é injetor, de modo que podemos identificar R com sua imagem $R \cdot 1$, e a partir disso, podemos pensar em R como um subanel de S. Assim, de um modo geral, uma extensão de R é qualquer anel S que tenha R como subanel ou um anel S tal que R esteja naturalmente imerso através desse homomorfismo.

Com essa identificação, um R-automorfismo de S deve deixar os elementos de R fixos, e qualquer automorfismo de S que fixa R, é um R-automorfismo. O conjunto de todos os R-automorfismos de S formam um grupo cuja operação é a composição. Assim, o grupo de R-automorfismos $\mathrm{Aut}_R(S)$ de uma extensão de anéis é definido de maneira análoga ao que fazemos para extensão de corpos: $\mathrm{Aut}_R(S) = \{\sigma : S \to S : \sigma|_R = id_R\}$.

Agora, vamos trabalhar para encontrar uma definição para extensão galoisiana sobre anéis. Para isso, precisamos definir duas álgebras.

Sejam G um subgrupo finito de $\mathrm{Aut}_R(S)$ e F o S-módulo gerado pela base $\{\sigma : \sigma \in G\}$. A soma e a multiplicação por escalar são as usuais e iremos definir duas multiplicações distintas em F, que originará duas álgebras diferentes. São elas:

1. $\left(\sum_{\sigma\in G} a_\sigma\sigma\right)\left(\sum_{\tau\in G} b_\tau\tau\right) = \sum_{\sigma,\tau\in G} a_\sigma\sigma(b_\tau)(\sigma\tau)$.

   Essa R-álgebra é denotada por $\triangle(S:G)$.

2. $\left(\sum_{\sigma\in G} a_\sigma\sigma\right)\left(\sum_{\tau\in G} b_\tau\tau\right) = \sum_{\sigma,\tau\in G} (a_\sigma b_\tau)\delta_{\sigma,\tau}\sigma$, onde $\delta_{i,j}$ é o delta de Kronecker.

   Essa S-álgebra (em particular R-álgebra) é denotada por $\bigtriangledown(S:G)$.

Vejamos alguns fatos importantes sobre essas álgebras que serão úteis no decorrer do texto.

- Podemos definir o homomorfismo de R-álgebras:

$$\begin{array}{rccc} \phi: & \triangle(S:G) & \to & Hom_R(S,S) \\ & \phi\left(\sum_{\sigma\in G} a_\sigma\sigma\right)(x) & \mapsto & \sum_{\sigma\in G} a_\sigma\sigma(x), \end{array}$$

  para todo $x \in S$.

- Podemos definir também o homomorfismo de S-álgebras (em particular de R-álgebras):

$$\begin{array}{rccc} \psi: & S\otimes_S S & \to & \bigtriangledown(S:G) \\ & \left(\sum_{i=1}^{n} a_i\otimes b_i\right) & \mapsto & \sum_{i=1}^{n}\sum_{\sigma\in G} a_i\sigma(b_i)\sigma. \end{array}$$

- Note que $\bigtriangledown(S:G)$ é isomorfo a $|G|$ cópias de S, através do isomorfismo

$$\begin{array}{rccc} f: & \bigtriangledown(S:G) & \to & S^{\oplus|G|} \\ & \sum_{\sigma\in G} a_\sigma\sigma & \mapsto & \sum_{\sigma\in G} a_\sigma. \end{array}$$

De fato, f é sobrejetora, e a injetividade segue do fato de a soma ser direta, pois se $f(\sum a_\sigma\sigma) = 0$, então $\sum a_\sigma = 0$, e assim, $a_\sigma = 0$, para todo $\sigma \in G$, visto que 0 escreve-se de maneira única por essa soma. Além disso, f é S-homomorfismo devido às propriedades de soma e multiplicação por escalar do operador somatório. Portanto, f é um isomorfismo.

Antes de prosseguir, relembramos da Teoria de Galois sobre corpos, que uma extensão $L \supseteq K$ é dita galoisiana com grupo de Galois $G = \mathrm{Aut}_K L$ se é uma extensão normal e separável. Outras definições equivalentes são bem conhecidas que listamos no seguinte resultado.

Teorema 3.4. *Sejam $L \supseteq K$ uma extensão de corpos e $G \subset Aut_K(L)$ um subgrupo finito. São equivalentes:*

1. *L é uma extensão galoisiana de K e $G = Aut_K(L)$.*
2. *$L^G = K$.*
3. *$G \subset Aut_K(L)$ e $|G| = dim_K L$.*

Nosso objetivo, agora, é buscar entre as definições de extensão de Galois para corpos, alguma que permita uma generalização natural para o caso de anéis. Observamos que, sobre um anel, as três condições equivalentes do Teorema 3.4 não são adequadas. A primeira não é conveniente porque os conceitos de raízes de polinômios necessários para definição de extensão normal, não se aplicam ao contexto de anéis; a terceira não é adequada porque em uma extensão de anéis $L \supset K$, tem-se que L não é necessariamente um K-módulo livre, e assim, nem sempre podemos falar em dimensão. A segunda definição também não permite uma generalização, de acordo com o próximo exemplo. Como para a extensão ser de Galois, esta deve ser separável, se exibirmos uma extensão de anéis e um subgrupo finito G de $\mathrm{Aut}_R(S)$ em que vale $S^G = R$ mas a mesma não é separável, é suficiente para concluir que essa generalização não é adequada, pois a definição que apresentarmos para a extensão ser de Galois deve implicar na separabilidade.

Exemplo 3.5. Sejam $R = \mathbb{Z}$ e $S = \mathbb{Z}[\sqrt{2}]$. Assim, $S \supseteq R$ é uma extensão de anéis e S pode ser visto como R-módulo livre com base $\{1, \sqrt{2}\}$, sendo assim, uma R-álgebra. Seja $\sigma \in \mathrm{Aut}(S)$ tal que $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$, para $a, b \in R$, e considere $G = \langle\sigma\rangle$. Pela definição de σ, fica claro que R é fixo por G, isto é, $G \subseteq \mathrm{Aut}_R(S)$, e como $\sigma^2 = id$, temos que $|G| = 2 = \dim_R S$. Também é imediato que $S^G = R$, de modo que as condições 2 e 3 do Teorema 3.4 são satisfeitas, mas R não é separável sobre K, como vimos no Exemplo 2.34. Assim, apenas a condição $S^G = R$ também não é suficiente para a generalização, já que não garante a separabilidade.

Mas, existe uma outra definição equivalente de extensão de Galois para corpos que normalmente não é encontrada em livros básicos, e que permite uma generalização para anéis. Essa generalização é dada através do próximo resultado, que encontra-se em [16].

Lema 3.6. *Sejam L uma extensão de K e G um subgrupo finito de $Aut_R(S)$. As seguintes afirmações são equivalentes:*

1. *$L^G = K$.*
2. *$dim_K L$ é finita e $\phi : \triangle(L : G) \to Hom_K(L, L)$ é um isomorfismo de K-álgebras.*

Demonstração. $(1 \Rightarrow 2)$ Pela hipótese que $L^G = K$ e G é finito, pelo Teorema 3.4, segue que $\dim_K L = [L : K] = |G| < \infty$. Diretamente do fato de que $G \subset \mathrm{Aut}_K(L)$, segue que ϕ é um homomorfismo. Para mostrar que ϕ é injetora, considere $\alpha = \sum_{\sigma \in G} a_\sigma \sigma \in \mathrm{Ker}(\phi)$. Assim, $\phi\left(\sum_{\sigma \in G} a_\sigma \sigma\right)(x) = 0$, e assim, $\sum_{\sigma \in G} a_\sigma \sigma(x) = 0$, para todo $x \in L$, isto é, $\sum_{\sigma \in G} a_\sigma \sigma \equiv 0$ (função nula). Mas pelo Lema de Dedekind, segue que os automorfismos de G formam um conjunto linearmente independente, donde segue que $a_\sigma = 0$, para todo $\sigma \in G$, ou seja, $\alpha = 0$, e desse modo, ϕ é injetora. Além disso, ϕ é sobrejetora, pois $\dim_K \triangle (L : G) = \dim_K L|G| = (\dim_K L)^2 = \dim_K \mathrm{Hom}_K(L, L)$. Portanto, ϕ é um isomorfismo de K-álgebras.

$(2 \Rightarrow 1)$ Como ϕ é um isomorfismo de K-álgebras, segue que $\triangle(L : G)$ é uma K-álgebra, e com isso, G é um K-automorfismo, ou seja, $G \subset \mathrm{Aut}_K(L)$. Pela bijetividade de ϕ, segue que $\dim_K \triangle (L : G) = \dim_K \mathrm{Hom}_K(L, L)$, e assim, usando a hipótese que $\dim_K L < \infty$, concluímos que $\dim_K \triangle (L : G) = \dim_K L|G| = \dim_k(\mathrm{Hom}_K(L, L)) = (\dim_K L)^2$, que implica $|G| = \dim_K L = [L : K]$. Logo, pelo Teorema 3.4, segue que $L \supseteq K$ é uma extensão de Galois, e portanto, $L^G = K$. □

O próximo teorema é um dos mais importantes deste trabalho, pois ele estabelece a definição de extensão galoisiana de anéis. Sua demonstração encontra-se em [16] e será feita aqui cuidadosa e detalhadamente, de modo que esta demonstração seja uma das principais contribuições deste trabalho.

Teorema 3.7. *Sejam S uma extensão do anel R e G um subgrupo finito de $Aut(S)$. As seguintes condições são equivalentes:*

1. **i)** *S é um R-módulo projetivo finitamente gerado;*

   ii) *$\phi : \triangle(S : G) \to Hom_R(S, S)$ é um isomorfismo de R-álgebras.*

2. **i)** *$S^G = R$;*

   ii) *$\psi : S \otimes S \to \nabla(S : G)$ é um isomorfismo de S-álgebras.*

3. **i)** *$S^G = R$;*

   ii) *existem elementos $x_1, \ldots, x_n, y_1, \ldots, y_n$ em S tal que $\sum_{j=1}^{n} x_j \sigma(y_j) = \delta_{1,\sigma}$, para todo $\sigma \in G$.*

4. **i)** *$S^G = R$;*

   ii) *para cada $\sigma \neq 1$ em G e para cada ideal maximal M de S, existe $x \in S$ tal que $\sigma(x) - x \notin M$.*

5. **i)** $S^G = R$;

   ii) *para cada idempotente não nulo* $e \in S$ *e para cada par* $\sigma \neq \tau$ *em* G, *existe* $x \in S$ *tal que* $\sigma(x)e \neq \tau(x)e$;

   iii) S *é separável sobre* R.

Demonstração. $(1 \Rightarrow 2)$ Primeiro vamos mostrar que $S^G = R$. Como ϕ é um isomorfismo de R-álgebras, segue que $\triangle(S:G)$ é uma R-álgebra (ou seja, é definida a multiplicação por elementos de R, e sendo G um grupo de automorfismos, todo elemento de R deve ficar fixo para automorfismos em G) e assim, $G \subset \mathrm{Aut}_R(S)$, ou seja, $R \subset S^G$. Para mostrar a inclusão contrária, consideremos $x \in S^G$. Identificando x com $x.id \in \triangle(S:G)$, segue que x pertence ao centro de $\triangle(S:G)$, isto é, para todo $y \in \triangle(S:G)$, $xy = yx$, ou seja, para todo $b \in S$, segue que $(x \circ y)(b) = (y \circ x)(b)$. Vejamos que de fato a igualdade é válida. Sejam $y = \sum_{\sigma \in G} a_\sigma \sigma \in \triangle(S:G)$ e $b \in S$. Assim,

$$\left(x \circ \sum_{\sigma \in G} a_\sigma \sigma\right)(b) = x\left(\sum_{\sigma \in G} a_\sigma \sigma(b)\right) = x \sum_{\sigma \in G} a_\sigma \sigma(b).$$

Por outro lado,

$$\left(\sum_{\sigma \in G} a_\sigma \sigma \circ x\right)(b) = \sum_{\sigma \in G} a_\sigma \sigma(xb) = \sum_{\sigma \in G} a_\sigma \sigma(x)\sigma(b) = \sum_{\sigma \in G} a_\sigma x \sigma(b) = x \sum_{\sigma \in G} a_\sigma \sigma(b).$$

Logo, $\phi(x)$ está no centro de $\mathrm{Hom}_R(S,S)$, por ϕ ser um isomorfismo. Pelo Teorema 2.35, segue que $Z(\mathrm{Hom}_R(S,S)) \cong R$. Consequentemente, $Z(\triangle(S:G)) = R$, e assim, $x \in R$, o que mostra que $S^G = R$. Para mostrar que vale o item ii), observemos que $\phi(t \cdot S) = \mathrm{Hom}_R(S,S)$ para $t = \sum_{\sigma \in G} \sigma \in \triangle(S:G)$. De fato, dados $a, x \in S$, então

$$\phi(ta) = \phi\left(\sum_{\sigma \in G} \sigma a \cdot id\right) = \phi\left(\left(\sum_{\sigma \in G} 1\sigma\right)\left(\sum_{\sigma \in G} a \cdot id\right)\right) = \phi\left(\sum_{\sigma \in G} \sigma(a)\sigma\right),$$

e assim,

$$\phi(ta)(x) = \sum_{\sigma \in G} \sigma(a)\sigma(x) = \sum_{\sigma \in G} \sigma(ax) \in S^G = R,$$

o que mostra que $\phi(t \cdot S) \subset \mathrm{Hom}_R(S,R)$. Para mostrar que vale a inclusão contrária, sejam $f \in \mathrm{Hom}_R(S,R) \subset \mathrm{Hom}_R(S,S)$ e $w = \sum_{\sigma \in G} a_\sigma \sigma \in \triangle(S:G)$ tal que $\phi(w) = f$. Como $f \in \mathrm{Hom}_R(S,R)$, para todo $x \in S$, segue que $\phi(w)(x) = f(x) \in R$, ou seja,

$\sum_{\sigma\in G} a_\sigma\sigma(x) \in R$. Assim, para todo $\rho \in G$, segue que $\rho\left(\sum_{\sigma\in G} a_\sigma\sigma(x)\right) = \sum_{\sigma\in G} a_\sigma\sigma(x)$, e logo,

$$\sum_{\sigma\in G} \rho(a_\sigma)\rho\sigma(x)) = \sum_{\sigma\in G} a_\sigma\sigma(x) = \sum_{\sigma\in G} a_{\rho\sigma}\rho\sigma(x).$$

Consequentemente, devemos ter $\rho(a_\sigma) = a_{\rho\sigma}$, para todo $\rho, \sigma \in G$, e desse modo, $\rho(a_1) = a_\rho$, para todo $\rho \in G$. Desta forma,

$$w = \sum_{\sigma\in G} \sigma(a_1)\sigma = \left(\sum_{\sigma\in G} \sigma\right) a_1 = ta_1.$$

Portanto, $f = \phi(w) = \phi(a_1) \in \phi(t \cdot S)$, e assim, $\phi(t \cdot S) = \mathrm{Hom}_R(S, R)$. Agora, consideramos a seguinte sequência de isomorfismos de R-módulos

$$S \otimes S \overset{\phi_1}{\to} S \otimes t \cdot S \overset{\phi_2}{\to} S \otimes \mathrm{Hom}_R(S, R) \overset{\phi_3}{\to} \mathrm{Hom}_R(S, S) \overset{\phi_4}{\to} \triangle(S : G) \overset{\phi_5}{\to} \bigtriangledown(S : G),$$

onde

- $\phi_1(a \otimes b) = a \otimes tb$, está bem definida, pois é induzida pela aplicação R-bilinear

  $$\begin{array}{rcl} S \times S & \to & S \otimes t \cdot S \\ (a, b) & \mapsto & a \otimes tb, \end{array}$$

  cuja função inversa é induzida pela aplicação

  $$\begin{array}{rcl} S \times t \cdot S & \to & S \otimes S \\ (a, tb) & \mapsto & a \otimes b, \end{array}$$

  que também é R-bilinear.

- $\phi_2(a \otimes tb) = a \otimes \phi(tb)$.

- $\phi_3(a \otimes f(x)) = f(x)a$. A bijetividade é assegurada pelo fato de S ser um R-módulo projetivo finitamente gerado.

- $\phi_4 = \phi^{-1}$.

- $\phi_5\left(\sum_{\sigma\in G} a_\sigma\sigma\right) = \sum_{\sigma\in G} a_\sigma\sigma$, ou seja, $\phi_5 = id$ (lembre-se que estamos olhando para esses conjuntos como R-módulos).

Agora, fazendo alguns cálculos, segue que $\psi = \phi_5 \circ \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1$. Como cada ϕ_i é um isomorfismo de R-módulos, segue que ψ também é um isomorfismo de R-módulos.

Como ψ é um homomorfismo de S-álgebras, segue que ψ é um isomorfismo de S-álgebras.

(2 $\Rightarrow$ 3) Suponhamos que $\psi^{-1}(1 \cdot id) = \sum_{i=1}^{n} x_i \otimes y_i \in S \otimes S$. Assim,

$$1 \cdot id = \psi\left(\sum_{i=1}^{n} x_i \otimes y_i\right) = \sum_{\sigma \in G}\left(\sum_{i=1}^{n} x_i \sigma(y_i)\right)\sigma,$$

pela definição de ψ. Mas, para essa soma resultar em $1 \cdot id$, para todo $\sigma \in G\backslash\{id\}$, segue que o escalar deve ser 0, e quando $\sigma = id$, segue que o escalar deve ser 1, ou seja, $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{1,\sigma}$.

(3 $\Rightarrow$ 1) Primeiramente, vamos mostrar que vale 1.i). Sejam $x_1, \ldots, x_n, y_1, \ldots, y_n$ elementos de S que satisfazem 3.ii), isto é, tal que $\sum_{j=1}^{n} x_j\sigma(y_j) = \delta_{1,\sigma}$, para todo $\sigma \in G$. Dado $x \in S$ podemos definir $f_i(x) = \sum_{\sigma \in G} \sigma(xy_i)$, que é um R-homomorfismo de S em R, isto é, $f_i \in \mathrm{Hom}_R(S, R)$. Além disso, tomando $x \in S$, segue que

$$\sum_{j=1}^{n} f_j(x)x_j = \sum_{j=1}^{n}\sum_{\sigma \in G}\sigma(xy_j)x_j = \sum_{\sigma \in G}\sigma(x)\sum_{j=1}^{n}\sigma(y_j)x_j = \sum_{\sigma \in G}\sigma(x)\delta_{1,\sigma} = x.$$

Logo, existem $x_i \in S$ e $f_i \in \mathrm{Hom}_R(S, R)$, tal que para todo $x \in S$, segue que $x = \sum_{j=1}^{n} f_i(x)x_i$, ou seja, S é um R-módulo projetivo finitamente gerado, de acordo com a Proposição 1.38. Mostramos agora que $\phi : \triangle(S : G) \to \mathrm{Hom}_R(S, S)$ é um isomorfismo. Como já vimos que ϕ é um homomorfismo, falta mostrar que ϕ é bijetora. Para mostrar a sobrejetividade, seja $h \in \mathrm{Hom}_R(S, S)$ e consideremos $w = \sum_{\sigma \in G}\sum_{j=1}^{n} h(x_j)\sigma(y_j)\sigma \in \triangle(S : G)$. Provemos que $\phi(w) = h$, isto é, que para todo $x \in S$, tem-se $\phi(w)(x) = h(x)$. Dado $x \in S$, segue que

$$\begin{aligned}
\phi(w)(x) &= \phi\left(\sum_{\sigma \in G}\sum_{j=1}^{n} h(x_j)\sigma(y_j)\sigma\right)(x) = \sum_{\sigma \in G}\sum_{j=1}^{n} h(x_j)\sigma(y_j)\sigma(x) \\
&= \sum_{j=1}^{n} h(x_j)\sum_{\sigma \in G}\sigma(y_j x) = h\left(\sum_{j=1}^{n} x_j \sum_{\sigma \in G}\sigma(y_j x)\right) \\
&= h\left(\sum_{\sigma \in G}\left(\sum_{j=1}^{n} x_j\sigma(y_j)\right)\sigma(x)\right) = h\left(\sum_{\sigma \in G}\delta_{1,\sigma}\sigma(x)\right) = h(x).
\end{aligned}$$

Agora, provemos que ϕ é injetora. Se $w = \sum_{\sigma\in G} a_\sigma\sigma \in \mathrm{Ker}(\phi)$, então $\phi(w) = 0$, isto é, $\phi(w)(x) = 0$, para todo $x \in S$, em particular, para todo x_i da hipótese. Logo,

$$\begin{aligned} 0 &= \sum_{\tau\in G}\sum_{j=1}^{n} \phi(w)(x_j)\tau(y_j)\tau = \sum_{\tau\in G}\sum_{j=1}^{n}\sum_{\sigma\in G} a_\sigma\sigma(x_j)\tau(y_j)\tau \\ &= \sum_{\tau\in G}\sum_{\sigma\in G} a_\sigma\sigma\left(\sum_{j=1}^{n} x_j\sigma^{-1}\tau(y_j)\right)\tau = \sum_{\tau\in G}\sum_{\sigma\in G} a_\sigma\delta_{1,\sigma^{-1}\tau}\tau \\ &= \sum_{\sigma\in G} a_\sigma\sigma = w. \end{aligned}$$

Logo, ϕ é injetora e, portanto, um isomorfismo.

(3 $\Rightarrow$ 4) Suponhamos que existem $\sigma \neq id$ em G e algum ideal maximal M de S tal que $x - \sigma(x) \in M$, para todo $x \in S$. Assim, tomando x_i e y_i como na hipótese ii), segue que

$$\sum_{j=1}^{n} x_j(y_j - \sigma(y_j)) = \sum_{j=1}^{n} x_jy_j - \sum_{j=1}^{n} x_j\sigma(y_j) = \delta_{1,1} - \delta_{1,\sigma}\ (\sigma \neq 1) = 1 - 0 = 1$$

é um elemento de M, o que contradiz o fato de M ser maximal. Logo, para cada $\sigma \neq 1$ em G e para cada ideal maximal M de S, segue que existe $x \in S$ tal que $\sigma(x) - x \notin M$.

(4 $\Rightarrow$ 3) Sejam $1 \neq \sigma \in G$ e I o ideal de S gerado por $\{x - \sigma(x) | x \in S\}$. Como $x - \sigma(x) \in I$, para todo $x \in S$, pela hipótese 4.ii), segue que $I = S$, e logo, $1 \in I$. Assim, existem elementos $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ tal que $\sum_{j=1}^{n} x_j(y_j - \sigma(y_j)) = 1$, e portanto, $\sum_{j=1}^{n} x_jy_j = 1 + \sum_{j=1}^{n} x_j\sigma(y_j)$. Se $x_{n+1} = -\sum_{j=1}^{n} x_j\sigma(y_j)$ e $y_{n+1} = 1$, então

$$\sum_{j=1}^{n+1} x_jy_j = \sum_{j=1}^{n} x_jy_j + x_{n+1}y_{n+1} = 1 + \sum_{j=1}^{n} x_j\sigma(y_j) - \sum_{j=1}^{n} x_j\sigma(y_j) = 1$$

e

$$\sum_{j=1}^{n+1} x_j\sigma(y_j) = \sum_{j=1}^{n} x_j\sigma(y_j) + x_{n+1}\sigma(y_{n+1}) = \sum_{j=1}^{n} x_j\sigma(y_j) - \sum_{j=1}^{n} x_j\sigma(y_j) = 0.$$

Portanto, $\sum_{j=1}^{n+1} x_j\sigma(y_j) = \delta_{1,\sigma}$. Acabamos de mostrar que para cada $\sigma \in G$ fixado, existe um conjunto de elementos satisfazendo 3.ii), onde estes elementos são determi-

nados a partir de σ. Usaremos isso para mostrar que existe um conjunto de elementos satisfazendo essa condição que independe da escolha de σ.

Sejam V e V' dois subconjuntos quaisquer de G que contém a identidade e para os quais existem elementos

$$x_1, \ldots, x_n, y_1, \ldots, y_n, x'_1, \ldots, x'_m, y'_1, \ldots, y'_m$$

em S tal que para todo $\sigma \in V$, tem-se $\sum_{j=1}^{n} x_j \sigma(y_j) = \delta_{1,\sigma}$ e para todo $\sigma' \in V'$, tem-se $\sum_{k=1}^{m} x'_k \sigma'(y'_k) = \delta_{1,\sigma'}$. Tomando $a_j = \sum_{k=1}^{m} x_j x'_k$ e $b_j = y_j y'_k$, com $j = 1, \ldots, n$ e $\tau \in V \cup V'$, segue que

$$\sum_{j=1}^{n} a_j \tau(b_j) = \sum_{j=1}^{n} \sum_{k=1}^{m} x_j x'_k \tau(y_j y'_k) = \sum_{j=1}^{n} \left(\sum_{k=1}^{m} x'_k \tau(y'_k) \right) x_j \tau(y_j) = \delta_{1,\tau}.$$

Como $G = \bigcup_{\sigma \neq 1} \{1, \sigma\}$, segue que existem elementos $a_1, \ldots, a_n, b_1, \ldots, b_n$ em S tal que $\sum_{j=1}^{n} a_j \tau(b_j) = \delta_{1,\sigma}$, para todo $\sigma \in G$.

$(3 \Rightarrow 5)$ Consideramos, primeiramente, que $g \in \mathrm{Hom}_R(S, R)$ e é definido por $g(x) = \sum_{\sigma \in G} \sigma(x)$. Mostramos que, de fato, $g(x) \in R$, para todo $x \in S$. Dado $\tau \in G$, tem-se

$$\tau(g(x)) = \sum_{\sigma \in G} \tau(\sigma(x)) = \sum_{\tau\sigma \in G} (\tau\sigma)(x) = g(x),$$

ou seja, $g(x)$ é invariante pela ação de G, logo, $g(x) \in S^G = R$. Agora, podemos mostrar que S é separável sobre R. Seja $e = \sum_{j=1}^{n} x_j \otimes y_j \in S \otimes_R S$, onde x_i, y_i satisfazem a condição 3.ii). Mostramos que e é um idempotente de separabilidade de S, isto é, que $\mu(e) = 1$ e $(\mu)e = 0$, sendo $\mu : S \otimes_R S \to S$ o homomorfismo dado por $\mu(a \otimes b) = ab$, como definido no Capítulo 2. A primeira afirmação ocorre, pois $\mu(e) = \sum_{j=1}^{n} x_j y_j = \delta_{1,1} = 1$. Para mostrar que vale a segunda afirmação, lembramos que os elementos da forma $1 \otimes x - x \otimes 1$, onde $x \in S$, formam uma base para $\mathrm{Ker}(\mu)$, e sendo assim, para provar que $\mathrm{Ker}(\mu)e = 0$, é suficiente mostrar que $(x \otimes 1)e = (1 \otimes x)e$, que é o que faremos a seguir. Se $x \in S$, então

$$\begin{aligned}
(x\otimes 1)e &= \sum_{j=1}^{n} xx_y\otimes y_j = \sum_{j=1}^{n}\left(\sum_{\sigma\in G}\sigma(xx_j)\delta_{1,\sigma}\right)\otimes y_j \\
&= \sum_{j=1}^{n}\left(\sum_{\sigma\in G}\sigma(xx_j)\sum_{k=1}^{n}\sigma(y_k)x_k\right)\otimes y_j = \sum_{j=1}^{n}\sum_{k=1}^{n}\left(\sum_{\sigma\in G}\sigma(xx_jy_k)\right)x_k\otimes y_j \\
&= \sum_{j=1}^{n}\sum_{k=1}^{n} g(xx_jy_k)x_k\otimes y_j = \sum_{k=1}^{n} x_k\otimes\sum_{j=1}^{n} g(xx_jy_k)y_j \\
&= \sum_{k=1}^{n} x_k\otimes\sum_{j=1}^{n}\left(\sum_{\sigma\in G}\sigma(xx_jy_k)\right)y_j = \sum_{k=1}^{n} x_k\otimes\sum_{\sigma\in G}\left(\sum_{j=1}^{n}\sigma(x_j)y_j)\right)\sigma(xy_k) \\
&= \sum_{k=1}^{n} x_k\otimes\sum_{\sigma\in G}\delta_{1,\sigma}\sigma(xy_k) = \sum_{k=1}^{n} x_k\otimes xy_k = (1\otimes x)e.
\end{aligned}$$

Logo, e é um idempotente de separabilidade e S é separável sobre R. Agora, mostramos que a condição 5.ii) é satisfeita. Sejam $\sigma,\tau\in G$ e $e\in S$ um idempotente não nulo. Suponhamos que $\sigma(x)e=\tau(x)e$, para todo $x\in S$. Como $\sigma,\tau\in G$, segue que eles possuem inverso pois são automorfismos, e assim, podemos aplicar σ^{-1} à igualdade $\sigma(x)e=\tau(x)e$, obtendo que $x\sigma^{-1}(e)=\sigma^{-1}\tau(x)\sigma^{-1}e$ para todo $x\in S$. Com isso,

$$\sigma^{-1}(e)=1\sigma^{-1}(e)=\sum_{j=1}^{n}x_jy_j\sigma^{-1}(e)=\sum_{j=1}^{n}x_j\sigma^{-1}\tau(y_j)\sigma^{-1}(e)=\sigma^{-1}(e)\delta_{\sigma^{-1}\circ\tau,1}.$$

Como $e\neq 0$, segue que $\sigma^{-1}(e)\neq 0$, e assim, $\delta_{\sigma^{-1}\circ\tau,1}=1$, ou seja, $\sigma=\tau$. Portanto, para $\sigma\neq\tau$, sempre existe algum $x\in S$ tal que $\sigma(x)e\neq\tau(x)e$.

(5 $\Rightarrow$ 3) Como por 5.iii), S é separável sobre R, segue que existe um idempotente de separabilidade $e\in S\otimes_R S$. Se $e=\sum_{j=1}^{n}x_j\otimes y_j$ é um idempotente de separabilidade, então $\mu(e)=\sum_{j=1}^{n}x_jy_j=1$ e $(x\otimes 1-1\otimes x)e=0$, para todo $x\in S$. Os elementos x_i,y_i constituirão o elemento que satisfaz 3.ii). Para cada $\sigma\in G$, definimos $e_\sigma=\mu((1\otimes\sigma)(e))\in S$. Esta expressão está bem definida, pois como σ é um automorfismo de S, segue que $1\otimes\sigma$ é um automorfismo de $S\otimes S$ e além disso, $\mu: S\otimes S\to S$ é um homomorfismo de anéis. Se $\sigma\in G$, então

$$\begin{aligned}
e_\sigma^2 &= \mu((1\otimes\sigma)(e))\cdot\mu((1\otimes\sigma)(e)) = \mu((1\otimes\sigma)(e)\cdot(1\otimes\sigma)(e)) \\
&= \mu((e\otimes\sigma(e))(e\otimes\sigma(e)) = \mu(e^2\otimes\sigma(e^2)) = \mu((1\otimes\sigma)(e^2)) \\
&= \mu((1\otimes\sigma)(e)) = e_\sigma,
\end{aligned}$$

ou seja, e_σ é idempotente. Além disso, dado $x\in S$, segue que

$$\begin{aligned} xe_\sigma &= x\mu((1\otimes\sigma)(e)) = \mu(x\otimes 1)\cdot\mu((1\otimes\sigma)(e)) = \mu((x\otimes 1)\cdot(1\otimes\sigma)(e)) \\ &= \mu((1\otimes\sigma)(x\otimes 1)\cdot(1\otimes\sigma)(e)) = \mu((1\otimes\sigma)(x\otimes 1)e) \\ &= \mu((1\otimes\sigma)(1\otimes x)\cdot(1\otimes\sigma)(e)) = \mu(1\otimes\sigma(x)\cdot(1\otimes\sigma)(e)) \\ &= 1\otimes\sigma(x)\cdot\mu((1\otimes\sigma)(e)) = 1\otimes\sigma(x)\cdot e_\sigma = e_\sigma\sigma(x) = \sigma(x)e_\sigma. \end{aligned}$$

Assim, pela condição 5.ii), segue que $e_\sigma = 0$ ou $\sigma = 1$, isto é, se $\sigma \neq 1$, necessariamente $e_\sigma = 0$, e pela definição de e_σ, se $\sigma = 1$, então $e_\sigma = \sum_{j=1}^{n} x_j y_j = 1$, pois x_i, y_i são os mesmos que compõem e. Portanto, $e_\sigma = \sum_{j=1}^{n} x_j\sigma(y_j) = \delta_{1,\sigma}$. □

Definição 3.8. *Seja S uma extensão do anel R e G um subgrupo finito de Aut(S). Dizemos que S é uma* ***extensão galoisiana*** *de R com grupo de Galois G, se S satisfaz uma, e portanto todas, as condições equivalentes do Teorema 3.7.*

A definição dada no item *1.* foi a primeira definição de extensão galoisiana de anéis que apareceu na literatura, em 1960, em [5]. As outras definições equivalentes foram apresentadas posteriormente, em 1995, no trabalho "Galois Theory and Cohomology of Commutative Rings" de Chase, Harison e Rosenberg. Os exemplos 3.9, 3.10, 3.11 e 3.12 encontram-se em [16] e aqui foram descritos mais detalhadamente. Os demais encontram-se em [19].

Exemplo 3.9. Sejam S uma extensão de R e $G \subseteq \mathrm{Aut}(S)$ um grupo finito tal que $S^G = R$. Se S é um corpo, então o único ideal maximal de S é $\langle 0\rangle$, de modo que o item 4 do Teorema 3.7 é satisfeito, e logo, S é uma extensão galoisiana de R.

Exemplo 3.10. Seja $L \supseteq K$ uma extensão galoisiana de corpos com grupo de Galois G. Assim, $L^G = K$ e a extensão é separável, de modo que, L é separável sobre K (como K-álgebra). Como 1 é o único idempotente não nulo de L, a condição *5.*ii) é satisfeita, porque sempre que $\sigma \neq \tau$, segue que existe $x \in L$ tal que $\sigma(x) \neq \tau(x)$, pois caso contrário seriam iguais. Assim, $L \supseteq K$ satisfaz o Teorema 3.7, e portanto, é uma extensão galoisiana de anéis com o mesmo grupo de Galois da extensão galoisiana de corpos. Com este exemplo, percebemos que toda extensão galoisiana de corpos é uma extensão galoisiana de anéis, ou seja, de fato a Definição 3.8 é uma generalização da definição de extensão galoisiana para corpos.

Exemplo 3.11. Considerando a extensão $R \subseteq R$ e $G = \{id_R\}$, onde R é um anel comutativo com identidade, o item *4.* do Teorema 3.7 é satisfeito, já que não existe $\sigma \neq 1$ em G, e também, $R^G = R$. Assim, a extensão $R \subseteq R$ é galoisiana com grupo de Galois G. Com este exemplo fica explícito que diferente da teoria de Galois sobre corpos, neste caso nem sempre teremos $G = \mathrm{Aut}_R(S)$.

Exemplo 3.12. Sejam R um anel comutativo com identidade e G um grupo finito. Consideramos $S = \sum_{\sigma\in G} \oplus Re_\sigma$, onde $e_\sigma e_\tau = \delta_{\sigma\tau} e_\sigma$, para todo $\sigma, \tau \in G$ e $\sum_{\sigma\in G} e_\sigma = 1$. A ação de G sobre S é dada por $\sigma(e_\tau) = e_{\sigma\tau}$ para todo $\sigma, \tau \in G$. Mostremos que a extensão $S \supset R$ munida do grupo G satisfaz o item *3.* do Teorema 3.7.

i) Se $r \in R$, então $\sigma(r) = \sigma(r.1) = \sigma\left(r.\sum_{\tau\in G} e_\tau\right) = \sum_{\tau\in G} r\sigma(e_\tau) = r\left(\sum_{\tau,\sigma\in G} e_{\sigma\tau}\right) = r.1 = r$, para todo $\sigma \in G$, ou seja, $R \subset S^G$. Por outro lado, se $x \in S$ é tal que $\sigma(x) = x$, para todo $\sigma \in G$ então $x = r_1e_{\sigma 1} + r_2e_{\sigma 2} + \cdots + r_ne_{\sigma n}$, onde $r_i \in R$, para todo i, e da igualdade $\sigma(x) = x$, segue que $\sigma(r_1e_{\sigma 1} + r_2e_{\sigma 2} + \cdots + r_ne_{\sigma n}) = r_1\sigma(e_{\sigma 1}) + r_2\sigma(e_{\sigma 2}) + \cdots + r_n\sigma(e_{\sigma n}) = r_1e_{\sigma\sigma 1} + r_2e_{\sigma\sigma 2} + \cdots + r_ne_{\sigma\sigma n} = r_1e_{\sigma 1} + r_2e_{\sigma 2} + \cdots + r_ne_{\sigma n}$, e logo, devemos ter $\sigma(e_{\sigma_i}) = e_{\sigma_i}$, para todo i. Mas, como σ é qualquer, esta igualdade é válida se, e somente se, $e_{\sigma_i} = 1$, para todo i. Assim, $x = r_1 + \cdots + r_n \in R$, ou seja, $S^G \subset R$.

ii) Tomando $x_i = e_\sigma$, com $\sigma \in G$ e $y_i = e_\tau$, com $\tau \in G$, segue que

$$\sum_{i=1}^{n} x_i\sigma(y_i) = \sum_{\sigma,\tau\in G} e_\sigma\sigma(e_\tau) = \sum_{\sigma,\tau\in G} e_\sigma e_{\sigma\tau} = \sum_{\sigma,\tau\in G} \delta_{\sigma,\sigma\tau}e_\sigma.$$

Assim, se $\sigma = \sigma\tau$, segue que $\sum_{i=1}^{n} x_i\sigma(y_i) = \sum_{\sigma\in G} e_\sigma = 1$ e se $\sigma \neq \sigma\tau$, segue que $\sum_{i=1}^{n} x_i\sigma(y_i) = 0$. Mas $\sigma = \sigma\tau$ implica que $\sigma = 1$, ou seja, se $\sigma = 1$ temos $\sum_{i=1}^{n} x_i\sigma(y_i) = 1$. Além disso, se $\sigma \neq \sigma\tau$, segue que $\sigma \neq 1$, isto é, se $\sigma \neq 1$ temos $\sum_{i=1}^{n} x_i\sigma(y_i) = 0$. Assim, $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{1,\sigma}$.

Exemplo 3.13. Seja R um anel comutativo de característica prima p. Suponhamos que R possui elemento identidade e tomamos $r \in R$. Considerando $S = \frac{R[X]}{(X^p - X - r)} = R[\alpha]$, onde $\alpha = X + (X^p - X - r)$ e $G = \langle\sigma\rangle$ um grupo cíclico de ordem p definido por $\sigma|_R = R$ e $\sigma(\alpha) = \alpha + 1$, segue que S é uma extensão galoisiana de R com grupo de Galois G. Vamos fazer esta prova mostrando que $(R[\alpha], \sigma)$ satisfaz o item *4.* do Teorema 3.7.

i) Observamos que $R[\alpha] = \{r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{p-1}\alpha^{p-1} : r_i \in R\}$ e $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ é um conjunto linearmente independente. Da definição de σ, segue naturalmente que $R \subset S^G$. Por outro lado, se $f(\alpha) \in S^G$, então $f(\alpha) = r_0 + r_1\alpha + \cdots + r_{p-1}\alpha^{p-1}$, e supondo que $\sigma(f(\alpha)) = f(\alpha)$, devemos ter $\sum_{i=1}^{p-1} r_i(\alpha + 1)^i = \sum_{i=1}^{p-1} r_i\alpha^i$, donde segue que $f(\alpha) = r_0$, uma vez que $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ é linearmente independente. Logo, $S^G \subset R$, e portanto, $S^G = R$.

ii) Primeiro mostremos que G tem ordem p. De fato, para $1 \leq i \leq p$, segue que $\sigma^i(x) = x + i.1$. Assim, pelo fato de que R tem característica p, segue que $\sigma^p(x) = x$, isto é, $\sigma^p = id$ e $\sigma^i(x) \neq x$, para todo $1 \leq i \leq p-1$, isto é, $\sigma^i \neq id$, para todo $1 \leq i \leq p-1$. Agora, observamos que se $id \neq \tau \in G$, então existe $1 \leq j \leq p-1$ tal que $\tau = \sigma^j$. Assim, se M é um ideal maximal de S e x um elemento arbitrário de S, então $\tau(x) - x = \sigma^j(x) - x = x + j.1 - x = j \notin M$, para todo $\tau \in G$, uma vez que M é um ideal maximal e j é inversível em R.

Exemplo 3.14. Sejam R um anel comutativo com elemento identidade e n um número inteiro maior ou igual a 2 tal que $\frac{1}{n} \in R$. Suponhamos também que existe $\zeta \in R$, uma raiz n-ésima da unidade, isto é, tal que $\zeta^n = 1$, satisfazendo que $(1-\zeta^i)$ é uma unidade de R, para todo inteiro $1 \leq i \leq n-1$. Além disso, sejam $r \in R$ uma unidade de R, $S = \frac{R[X]}{X^p - X - r} = R[\alpha]$ e G um grupo cíclico de ordem n gerado por σ, definido por $\sigma(x) = \zeta x$, para todo $x \in S$. Então S é uma extensão galoisiana de R com grupo de Galois G.

Para ver isso, vamos mostrar que o item *4.* do Teorema 3.7 é satisfeito. A prova de que $S^G = R$ é análoga à que fizemos no item i) do Exemplo 3.13. Assim, para mostrar que a extensão é galoisiana, dada $id \neq \tau \in G$, basta exibir $\lambda \in S$ tal que $\tau(\lambda) - \lambda \notin M$, para todo ideal maximal M de S. Seja então $\tau = \sigma^j$, com $1 \leq j \leq n-1$. Tomando $\lambda = \alpha = X + (X^n - r)$, temos

$$\tau(\lambda) - \lambda = \tau(\alpha) - \alpha = \sigma^j(\alpha) - \alpha = \zeta^j \alpha - \alpha = (\zeta^j - 1)\alpha.$$

Note que $(\zeta^j - 1)$ e α são ambos inversíveis em S, desta forma, $(\zeta^j - 1)\alpha \notin M$, para todo ideal maximal M de S. Portanto, S é uma extensão galoisiana de R com grupo de Galois G.

A seguir, vejamos alguns resultados e definições necessários para chegarmos ao teorema fundamental.

Lema 3.15. *Seja S uma extensão galoisiana de R com grupo de Galois G.*

1. *Existe um elemento $c \in S$ tal que para $g \in Hom_R(S, R)$ dada por $g(x) = \sum_{\sigma \in G} \sigma(x)$, tem-se $g(c) = \sum_{\sigma \in G} \sigma(c) = 1$.*

2. *R é um somando direto de S como R-módulo.*

3. *Se T é uma R-álgebra comutativa com elemento identidade 1 e G atua sobre $T \otimes S$ via $\sigma(t \otimes s) = t \otimes \sigma(s)$, para todo $s \in S$, $t \in T$ e $\sigma \in G$, então $T \otimes S$ é uma extensão galoisiana de T com grupo de Galois G.*

Demonstração. 1. No Teorema 3.7, da prova de $(1 \Rightarrow 2)$, segue que $\mathrm{Hom}_R(S,R) = \phi(t \cdot S)$. Assim, dado $f \in \mathrm{Hom}_R(S,R)$, segue que existe $s \in S$ tal que $f = \phi(t \cdot s) = \phi\left(\sum_{\sigma \in G} \sigma(s)\sigma\right)$. Então, para todo $x \in S$, segue que

$$f(x) = \phi\left(\sum_{\sigma \in G} \sigma(s)\sigma\right)(x) = \sum_{\sigma \in G} \sigma(s)\sigma(x) = \sum_{\sigma \in G} \sigma(sx) = g(sx).$$

Logo, para todo $f \in \mathrm{Hom}_R(S,R)$, segue que $f(x) = g(sx)$, para algum $s \in S$. Por outro lado, como $S \supset R$ é de Galois, pelo item 1 do Teorema 3.7, segue que S é um R-módulo projetivo finitamente gerado, e desse modo, existem $x_1, \ldots, x_n \in S$ e $f_1, \ldots, f_n \in \mathrm{Hom}_R(S,R)$ tal que $\sum_{i=1}^{n} f_i(x_i) = 1$, e assim, existem $s_1 \ldots, s_n \in S$ tal que $f_i = g(s_i x)$. Consequentemente,

$$1 = \sum_{i=1}^{n} f_i(x_i) = \sum_{i=1}^{n} g(s_i x_i) = g\left(\sum_{i=1}^{n} s_i x_i\right).$$

Tomando $c = \sum_{i=1}^{n} s_i x_i \in S$, segue $g(c) = 1$ e a afirmação está provada.

2. Pelo item *1.*, segue que existe $c \in S$ tal que $g(c) = 1$, de modo que a imagem de g é R. Isso implica que a sequência $S \xrightarrow{g} R \to 0$ é exata. Definindo $\theta : R \to S$ por $\theta(r) = rc$, segue que θ é um homomorfismo de R-módulos e $g \circ \theta = 1_R$, ou seja, a sequência cinde, e logo, R é um somando direto de S.

3. Vamos mostrar que o item *3.* do Teorema 3.7 é satisfeito. Sejam $x_1, \ldots, x_n, y_1, \ldots, y_n$ os elementos de S tal que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{i,j}$. Assim, $1 \otimes x_1, \ldots, 1 \otimes x_n, 1 \otimes y_1, \ldots, 1 \otimes y_n$ são elementos de $T \otimes S$ e vale

$$\sum_{i=1}^{n} (1 \otimes x_i)(1 \otimes \sigma)(1 \otimes y_i) = 1 \otimes \sum_{i=1}^{n} x_i \sigma(y_i) = 1 \otimes \delta_{1,\sigma} = \delta_{1,\sigma}.$$

Também devemos mostrar que $(T \otimes S)^G = T$. Para ver que $T \subseteq (T \otimes S)^G$, é suficiente observar que $t \otimes 1$, que é a identificação de T em $T \otimes S$, fica fixo para todo $\sigma \in G$. De fato, $(1 \otimes \sigma)(t \otimes 1) = t \otimes \sigma(1) = t \otimes 1$. Agora, seja $w \in (T \otimes S)^G$. Pelo item *1.*, segue que existe $c \in S$ tal que $g(c) = 1$, então $\sum_{\sigma \in G} (1 \otimes \sigma)(1 \otimes c) = 1 \otimes 1$. Suponhamos que $w \cdot 1 \otimes c = \sum_{i=1}^{m} t_i \otimes s_i \in T \otimes S$. Assim,

$$\begin{aligned} w &= w\cdot 1\otimes 1 = w\sum_{\sigma\in G}(1\otimes\sigma)(1\otimes c) = \sum_{\sigma\in G}(1\otimes\sigma)(w\cdot 1\otimes c) \\ &= \sum_{\sigma\in G}(1\otimes\sigma)\left(\sum_{i=1}^{n} t_i\otimes s_i\right) = \sum_{i=1}^{m} t_i\otimes\sum_{\sigma\in G}\sigma(s_i) = \sum_{i=1}^{m} t_i t_r(s_i)\otimes 1 \in T\otimes 1 = T. \end{aligned}$$

Logo $(T\otimes S)^G = T$, e portanto, $T\otimes S$ é uma extensão galoisiana de T com grupo de Galois G. □

Definição 3.16. *Sejam $f, g : S \to T$ homomorfismo de anéis. Dizemos que f e g são* ***fortemente distintos*** *se, para todo idempotente não nulo e de T, existe $s \in S$ tal que $f(s)e \neq g(s)e$.*

Note que a condição 5.ii) do Teorema 3.7 significa que os automorfismos de G são 2 a 2 fortemente distintos. Levando em consideração apenas os anéis que não possuem elementos idempotentes não nulos, como é o caso dos corpos, essa condição não seria necessária, e teríamos que uma extensão de anéis é galoisiana se, e somente se, $S^G = R$ e S é separável sobre R. Mas como queremos incluir neste estudo também os anéis que possuem elementos idempotentes não triviais, é necessário introduzir este conceito para que o Teorema Fundamental seja válido neste caso. Em [13], de Mayer define que uma extensão $S \supset R$ de anéis é normal se satisfaz $S^G = R$. Neste sentido, a definição do item 5. do Teorema 3.7 pode ser vista como uma generalização do conceito de extensão normal e separável utilizada para corpos.

Lema 3.17. *Se S é uma R-álgebra comutativa separável com elemento identidade 1 e $f : S \to R$ é um homomorfismo de R-álgebras, então existe um único idempotente $e \in S$ tal que $f(e) = 1$ e $xe = f(x)e$, para todo $x \in S$. Além disso, se $f_1, \ldots, f_n : S \to R$ são homomorfismos de R-álgebras fortemente distintos dois a dois e $e_1, \ldots, e_n \in S$ são os idempotentes correspondentes, então $e_i e_j = 0$, se $i \neq j$ e $f_i(e_j) = \delta_{i,j}$, para $i, j = 1, \ldots, n$.*

Demonstração. Seja $f : S \to R$ um homomorfismo de R-álgebras onde S é uma R-álgebra separável. Assim, S admite um elemento idempotente de separabilidade $e \in S\otimes S$ e existem elementos $x_1, \ldots, x_n, y_1, \ldots, y_n$ em S tais que $\sum_{i=1}^{n} x_i y_i = 1$ e $\sum_{i=1}^{n} x x_i \otimes y_i = \sum_{i=1}^{n} x_i \otimes y_i x$, para todo $x \in S$. Seja $e = \sum_{j=1}^{n} f(x_i) y_i \in S$. Mostramos que esse elemento é o idempotente que procuramos, isto é, que $f(e) = 1$ e $f(x)e = xe$, para todo $x \in S$, ou seja,

- $f(e) = f\left(\sum_{i=1}^{n} f(x_i)y_i\right) = \sum_{i=1}^{n} f(x_i)f(y_i) = f\left(\sum_{i=1}^{n} x_i y_i\right) = f(1) = 1.$

- $(f \otimes 1)\left(\sum_{i=1}^{n} xx_i \otimes y_i\right) = (f \otimes 1)\left(\sum_{i=1}^{n} x_i \otimes y_i x\right) \Rightarrow \sum_{i=1}^{n} f(xx_i) \otimes y_i = \sum_{i=1}^{n} f(x_i) \otimes y_i s \Rightarrow \sum_{i=1}^{n} 1 \otimes f(xx_i)y_i = \sum_{i=1}^{n} 1 \otimes f(x_i)y_i x \Rightarrow 1 \otimes f(x)e = 1 \otimes xe.$ Aplicando $\mu : S \otimes S \to S$ onde $\mu\left(\sum_{i=1}^{n} x_i \otimes y_i\right) = \sum_{i=1}^{n} x_i y_i$, em ambos os lados da igualdade $1 \otimes f(x)e = 1 \otimes xe$, segue que $f(x)e = xe$, para todo $x \in S$.

- Fazendo $x = e$, dos itens anteriores, segue que $e = 1e = f(e)e = e^2$, ou seja, e é de fato idempotente.

Falta mostrar a unicidade de e. Suponhamos que e' é outro idempotente de S que satisfaz $f(e') = 1$ e $f(x)e' = xe'$, para todo $x \in S$. Assim, $e' = 1e' = f(e)e' = ee' = e'e = f(e')e = 1e = e$, o que mostra que e é único. Agora, vamos provar a segunda parte do lema. Sejam $f_1, \ldots, f_n : S \to R$ homomorfismos de R-álgebras fortemente distintos dois a dois e $e_1, \ldots, e_n \in S$ os idempotentes correspondentes que satisfazem $f_i(e_i) = 1$ e $f_i(x)e_i = xe_i$, para todo $x \in S$. Assim, $e_{ij} = f_i(e_j)$ é um idempotente de R (pois é a imagem de um elemento idempotente) para $i, j = 1, \ldots, n$. Além disso,

$$f_i(x)e_{ij} = f_i(x)f_i(e_j) = f_i(xe_j) = f_i(f_j(x)e_j) = f_j(x)f_i(e_j) = f_j(x)e_{ij},$$

para todo $x \in S$. Supondo $i \neq j$, por hipótese, segue que f_i e f_j são fortemente distintos, e então, para cada idempotente e não nulo de S, existe $x \in S$ tal que $f_i(x)e \neq f_j(x)e$, o que não ocorre com e_{ij}. Logo, se $i \neq j$, então $e_{ij} = f_i(e_j) = 0$. Se $i = j$, então caímos no caso que já foi provado na primeira parte, onde $f_i(e_i) = 1$. Portanto, $f_i(e_j) = \delta_{i,j}$, para $i, j = 1, \ldots n$. Finalmente, $e_{ij} = f_j(1)e_i e_j = f_j(e_i)e_j = \delta_{ij}e_j = 0$, se $i \neq j$, o que conclui a demonstração do lema. □

A próxima definição também é crucial para que consigamos determinar uma correspondência entre os subanéis de S que contém R e os subgrupos do grupo de Galois G.

Definição 3.18. *Sejam S uma extensão galoisiana de R com grupo de Galois G e T um subanel de S. Dizemos que T é* ***G-forte*** *se para todo $\sigma, \tau \in G$, tem-se que $\sigma|_T = \tau|_T$ ou $\sigma|_T$ e $\tau|_T$ são fortemente distintos.*

Na teoria de Galois sobre corpos, considerando uma extensão galoisiana de corpos $L \supset K$ com grupo de Galois G, o Teorema Fundamental estabelece uma correspondência biunívoca entre os corpos intermediários M e os subgrupos de G. O nosso próximo passo é determinar um teorema similar para a teoria de Galois sobre anéis, apresentando as especificidades que os subanéis devem possuir para que haja uma correspondência.

Definindo os conjuntos $\mathcal{F} = \{T \text{ anel} \mid R \subseteq T \subseteq S \text{ e } T \text{ é uma } R-\text{álgebra separavél e } G-\text{forte de } S\}$, $\mathcal{G} = \{H \subset G \mid H \text{ é subgrupo de } G\}$, $S^H = \{x \in S : \sigma(x) = x, \text{ para todo } \sigma \in H\}$ e $H_T = \{\sigma \in H : \sigma(x) = x, \text{ para todo } x \in T\}$, consideramos as aplicações

$$\begin{array}{rccc} \varphi: & \mathcal{F} & \to & \mathcal{G} \\ & T & \mapsto & H_T \end{array}$$

$$\begin{array}{rccc} \psi: & \mathcal{G} & \to & \mathcal{F} \\ & H & \mapsto & S^H. \end{array}$$

Veremos, entre outros fatos relevantes, que estas aplicações estão bem definidas e são inversas uma da outra, através do teorema a seguir, o principal deste trabalho.

Teorema 3.19. *(Teorema Fundamental da Teoria de Galois) Seja S uma extensão galoisiana de R com grupo de Galois G.*

1. *Se H é um subgrupo de G onde $S^H = T$, então*
   - *S é uma extensão galoisiana de T com grupo de Galois H.*
   - *T é uma R-álgebra separável.*
   - *T é G-forte como subálgebra de S.*
   - *$H = H_T$.*
2. *Se T é uma R-subálgebra separável e G-forte de S onde $H = H_T$, então $T = S^H$.*
3. *Seja T uma R-subálgebra separável e G-forte de S. Assim, T é uma extensão galoisiana de R se, e somente se, o subgrupo correspondente H é um subgrupo normal de G.*

Demonstração. 1.

- S é uma extensão galoisiana de T com grupo de Galois H: como S é uma extensão galoisiana de R, segue que existem $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ tal que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma}$ para todo $\sigma \in G$. Como $H \subseteq G$, segue que esta igualdade vale para todo $\sigma \in H$. Ademais, por hipótese, segue que $S^H = T$. Portanto, S é uma extensão galoisiana de T com grupo de Galois H.

- $S^H = T$ é uma R-álgebra separável: seja $g \in \text{Hom}_{S^H}(S, S^H)$ a função traço definida por $g(s) = \sum_{\sigma \in H} \sigma(s)$, para todo $s \in S$. Vamos mostrar que S é uma extensão galoisiana de T com grupo de Galois H. Pelo Lema 3.15, segue que

existe $c \in S$ tal que $g(c) = 1$. Definimos $a_j = g(x_j)$ e $b_j = g(y_j c)$, e consideramos, $e = \sum_{j=1}^{n} a_j \otimes b_j \in S^H \otimes S^H$. Mostramos que e é um idempotente de separabilidade de S^H, isto é, que $\mu(e) = 1$ e $(\mu)e = 0$.

$$\begin{aligned}\mu(e) &= \sum_{j=1}^{n} a_j b_j = \sum_{j=1}^{n} g(x_j)g(y_j c) = \sum_{j=1}^{n}\sum_{\sigma\in H}\sum_{\tau\in H}\sigma(x_j)\tau(y_j c)\\ &= \sum_{\sigma\in H}\sum_{\tau\in H}\sigma\left(\sum_{j=1}^{n} x_j\sigma^{-1}\tau(y_j)\right)\tau(c) = 1.\end{aligned}$$

e

$$\begin{aligned}(x\otimes 1)e &= \sum_{j=1}^{n} xa_j \otimes b_j = \sum_{j=1}^{n}\sum_{\sigma\in H}\sum_{\tau\in H} x\sigma(x_j)\otimes\tau(y_j c)\\ &= \sum_{\sigma\in H}\sum_{\tau\in H}\sigma\otimes\tau\left(\sum_{j=1}^{n} xx_j\otimes y_j c\right)\\ &= \sum_{j=1}^{n}\left(\sum_{\sigma\in H}\sigma(x_j)\right)\otimes\left(\sum_{\tau\in H}\tau(y_j c)\right)1\otimes x\\ &= (1\otimes x)\sum_{j=1}^{n} a_j\otimes b_j = (1\otimes x)e.\end{aligned}$$

Assim, $S^H = T$ é separável sobre R.

- T é G-forte: como S é uma extensão galoisiana de T com grupo de Galois H, segue que existe $c \in S$ tal que $g(c) = \sum_{\rho\in H}\rho(c) = 1$. Além disso, como $S \supset R$ é galoisiana, segue que existem $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ tal que $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{1,\sigma}$, para todo $\sigma \in G$. Sejam $x_1' = \sum_{\rho\in H}\rho(x_i c) = g(x_i c)$ e $y_i' = \sum_{\rho\in H}\rho(y_i) = g(y_i)$, para $i = 1, \ldots, n$. Como $g \in \mathrm{Hom}_T(S, T)$, segue que $x_i', y_i' \in S^H = T$, e assim,

$$\begin{aligned}\sum_{i=1}^{n} x_i'\sigma(y_i') &= \sum_{i=1}^{n}\left(\sum_{\rho\in H}(x_i c)\right)\sigma\left(\sum_{\tau\in H}\tau(y_i)\right)\\ &= \sum_{\rho,\tau\in H}\rho(c)\sum_{i=1}^{n}\rho(x_i)\sigma\tau(y_i)\\ &= \sum_{i=1}^{n}\rho(c)\rho\left(\sum_{i=1}^{n} x_i\rho^{-1}\sigma\tau(y_i)\right) = \sum_{\rho,\tau\in H}\delta_{1,\rho^{-1}\sigma\tau}\rho(c)\\ &= \begin{cases} 1 & se \quad \sigma\in H\\ 0 & se \quad \sigma\notin H,\end{cases}\end{aligned}$$

para todo $\sigma \in G$. Logo,

$$\sum_{i=1}^{n} x_i' \sigma(y_i') = \begin{cases} 1 & se \quad \sigma \in H \\ 0 & se \quad \sigma \notin H, \end{cases}$$

para todo $\sigma \in G$. Agora, sejam $\sigma, \tau \in G$ tal que $\sigma|_T \neq \tau|_T$. Assim, $\tau\sigma^{-1} \notin H$. Consideramos, agora, $e \in S$ um idempotente não nulo tal que $\sigma(t)e = \tau(t)e$, para todo $t \in T$. Assim, $te = \tau\sigma^{-1}(t)e$, para todo $t \in T$, e logo,

$$e = \left(\sum_{i=1}^{n} x_i' y_i'\right) e = \sum_{i=1}^{n} x_i'(y_i' e) = \sum_{i=1}^{n} x_i' \tau\sigma^{-1}(y_i') e \overset{\tau\sigma^{-1} \notin H}{=} 0e = 0.$$

Portanto, T é G-forte.

- $H = H_T$: como $S^H = T$, segue que $H \subset H_T$ e $S^{H_T} = S^H = T$. Pelo fato que $H_T \subset G$ e usando o mesmo raciocínio utilizado para mostrar que S é extensão galoisiana de T com grupo de Galois H, segue que S também é uma extensão de Galois com grupo de Galois H_T, e assim, pelo item *2.* do Teorema 3.7 segue que $\psi : S \otimes_T S \to \bigtriangledown(S : H_T)$ é um isomorfismo de S-álgebras e $\psi : S \otimes_T S \to \bigtriangledown(S : H)$ também é um isomorfismo de S-álgebras. Logo, $\dim_T S \cdot |H| = \dim_S S \otimes_T S = \dim_T S \cdot |H_T|$, e consequentemente, $|H| = |H_T|$. Desta igualdade e do fato que $H \subset H_T$, segue que $H = H_T$.

2. Seja T uma R-álgebra separável e G-forte de S em que $H = H_T$. Como $H = H_T$, segue que $T \subset S^H$, de modo que resta provar a inclusão $S^H \subset T$. Nosso trabalho inicial nessa longa demonstração é mostrar que $\bigtriangledown(S : G)^H = \psi(S \otimes T)$, pois a partir dessa igualdade chegamos na inclusão desejada. Pelo item *3.* do Lema 3.15, segue que $S \otimes S$ é uma extensão galoisiana de $S = S \otimes R$ com grupo de Galois G, onde $\sigma(a \otimes b) = a \otimes \sigma(b)$, para todo $a, b \in S$ e $\sigma \in G$. Como pelo item *2.* do Teorema 3.7 a aplicação $\psi : S \otimes S \to \bigtriangledown(S : G)$ é um isomorfismo, podemos definir uma ação de G sobre $\bigtriangledown(S : G)$, dada por $\rho(\sigma) = \sigma\rho^{-1}$, para todo $\rho \in G$. Observamos que vale a

igualdade $\psi(\sigma(a\otimes b))=\sigma(\psi(a\otimes b))$, para todo $a\otimes b\in S\otimes S$ e $\sigma\in G$. De fato,

$$\psi(\sigma(a\otimes b))=\psi(a\otimes\sigma(b))=\sum_{\rho\in G}a\rho(\sigma(b))\rho;$$
$$\sigma(\psi(a\otimes b))=\sigma\left(\sum_{\rho\in G}a\rho(b)\rho\right)=\sum_{\rho\in G}a\rho(b)\rho\sigma^{-1}=\sum_{\tau\in G}a\tau(\sigma(b))\tau.$$

Além disso, ψ é um isomorfismo, e assim, concluímos que $\bigtriangledown(S:G)$ também é uma extensão galoisiana de S com grupo de Galois G. Ademais, como $T\subset S^H\subset S$, podemos considerar as sequências $0\xrightarrow{f}T\xrightarrow{i}S^H$ e $0\xrightarrow{f}S^H\xrightarrow{i}S$, onde i são inclusões, que são injetoras, de modo que as sequências são exatas. Como S é um R-módulo projetivo, ao tensorizar uma sequência exata por S, a mesma continua exata. Assim, as sequências $0\xrightarrow{id\otimes f}S\otimes T\xrightarrow{id\otimes i}S\otimes S^H$ e $0\xrightarrow{id\otimes f}S\otimes S^H\xrightarrow{id\otimes i}S\otimes S$ são exatas, de modo que podemos identificar $S\otimes T$ com sua imagem em $S\otimes S^H$ (isto é, vê-lo como subconjunto) e $S\otimes S^H$ com sua imagem em $S\otimes S$. Dessa forma, seguem as inclusões $S\otimes T\subset S\otimes S^H\subset(S\otimes S)^H$. Aplicando ψ, segue que

$$\psi(S\otimes T)\subset\psi((S\otimes S)^H)=(\psi(S\otimes S))^H=\bigtriangledown(S:G)^H.$$

Portanto, para concluir esta primeira etapa da demonstração, falta apenas mostrar que $\bigtriangledown(S:G)^H\subset\psi(S\otimes T)$. Para tal, consideramos $\sigma_1,\ldots,\sigma_r\in G$ os representantes das classes laterais distintas de H em G. Para cada $1\leq i\leq r$, definimos o homomorfismo de S-álgebras

$$\begin{array}{rccc} f_i: & \bigtriangledown(S:G) & \to & S \\ & \displaystyle\sum_{\sigma\in G}a_\sigma\sigma & \mapsto & a_{\sigma_i}. \end{array}$$

Mostramos que $f_i=f_i|_{\psi(S\otimes T)}:\psi(S\otimes T)\to S$ são homomorfismos fortemente distintos dois a dois. Supondo que $\sigma_i|_T=\sigma_j|_T$, para $i\neq j$, como $H=H_T$, segue que $\sigma_i,\sigma_j\in H$, e assim, $\bar{\sigma}_i=\bar{\sigma}_j=H$, o que contradiz o fato de que os $\sigma_i's$ são representantes de classes laterais distintas. Logo, se $i\neq j$, segue que $\sigma_i|_T\neq\sigma_j|T$, e então, por T ser G forte, dado um idempotente $e\in S$ não nulo, existe $t\in T$ tal que $\sigma_i(t)e\neq\sigma_j(t)e$, e a partir disso, segue que

$$f_i(\psi(1\otimes t))e=f_i\left(\sum_{\sigma\in G}\sigma(t)\sigma\right)e=\sigma_i(t)e\neq\sigma_j(t)e=f_j(\psi(1\otimes t))e,$$

ou seja, f_i,f_j, com $i\neq j$ são fortemente distintos. Além disso, como T é uma R-álgebra separável, segue que $S\otimes T$ é uma S-álgebra separável, pois se $e\in T\otimes T$ é o idempotente de separabilidade de T sobre R, então $1\otimes e\in S\otimes(T\otimes T)=(S\otimes T)\otimes(S\otimes T)$ é o idempotente de separabilidade se $S\otimes T$ sobre S. Como ψ é um isomorfismo de S-álgebras, segue que $\psi(S\otimes T)$ também é uma S- álgebra separável. Assim, podemos usar

o Lema 3.17 para concluir que existem elementos idempotentes $w_i, \ldots, w_r \in \psi(S \otimes T)$ tal que $f_i(x)w_i = xw_i$, para todo $x \in \psi(S \otimes T)$ e $f_i(w_j) = \delta_{ij}$, para $i, j = 1, \ldots, r$. Como $\psi(S \otimes T) \subset \bigtriangledown(S : G)^H$, segue que $w_i \in \bigtriangledown(S : G)^H$, para todo i. Dessa forma, se mostrarmos que $\{w_1, \ldots, w_r\}$ gera $\bigtriangledown(S : G)^H$, todo elemento de $\bigtriangledown(S : G)^H$ também pertence a $\psi(S \otimes T)$, de modo que a inclusão contrária estaria satisfeita. Para isso, vamos tomar um elemento qualquer em $\bigtriangledown(S : G)^H$ e mostrar que ele é uma combinação linear dos $w_i's$. Seja $z = \sum_{\sigma \in G} a_\sigma \sigma \in \bigtriangledown(S : G)^H$. Pela definição de $\bigtriangledown(S : G)^H$, segue que H deixa z fixo, e logo, $\rho(z) = z$, para todo $\rho \in H$. Mas usando a definição da atuação de G em $\bigtriangledown(S : G)$, segue que $\rho(z) = \sum_{\sigma \in G} a_\sigma \sigma \rho^{-1}$. Logo, $\sum_{\sigma \in G} a_\sigma \sigma = \sum_{\sigma \in G} a_\sigma \sigma \rho^{-1}$, ou seja, $\sum_{\sigma \in G} a_{\sigma\rho} \sigma = \sum_{\sigma \in G} a_\sigma \sigma$, de onde segue que $a_\sigma = a_{\sigma\rho}$, para todo $\sigma \in G$, $\rho \in H$. Assim, em particular, tem-se $a_{\sigma_i} = a_{\sigma_i \rho}$, para todo $\rho \in H$ e $i = 1, \ldots, r$. Levando em consideração que $G = \bigcup_{i=1}^{r} \sigma_i H$, isto é, que G é a união de todas as classes laterais de H em G, segue que

$$z = \sum_{\sigma \in G} a_\sigma \sigma = \sum_{i=1}^{r} \sum_{\rho \in H} a_{\sigma_i \rho^{-1} \sigma_i \rho^{-1}} = \sum_{i=1}^{r} a_{\sigma_i} \left(\sum_{\rho \in H} \rho(\sigma_i) \right).$$

Podemos tomar $w_i = \sum_{\rho \in H} \rho(\sigma_i)$, pois satisfaz $f_i(w_j) = \delta_{ij}$ e $f_i(x)w_i = xw_i$, de modo que obtemos $z = \sum_{i=1}^{r} a_\sigma w_i$, para todo $z \in \bigtriangledown(S : G)^H$, ou seja, o conjunto dos $w_i's$ gera $\bigtriangledown(S : G)^H$, e daí segue que $\bigtriangledown(S : G)^H = \psi(S \otimes T)$. Agora, vamos mostrar que a partir dessa igualdade a inclusão $S^H \subset T$ se verifica. Se $\bigtriangledown(S : G)^H = \psi(S \otimes T)$, então

$$S \otimes S^H \subset (S \otimes S^H) = \psi^{-1}(\bigtriangledown(S : G)^H) = S \otimes T.$$

Aplicando $g \otimes 1$, onde g é a função traço, a essa inclusão, obtemos $g(S) \otimes S^H \subset g(S) \otimes T$. Pelo Lema 3.15, existe $c \in S$ tal que $g(c) = 1$, de onde $g(S) = R$, e logo, $S^H = R \otimes S^H \subset R \otimes T = T$. Portanto, $S^H = T$.

3. Pelo item *1.*, segue que se $S \supset R$ é Galois, então S é sempre Galois sobre T. Mas será que para a extensão $T \supset R$ podemos fazer a mesma afirmação? Vamos mostrar que não, que isso vale se, e somente se, H é um subgrupo normal de G. Primeiramente, mostramos que vale $H_{\sigma(T)} = \sigma H_T \sigma^{-1}$. Se $\rho \in H_{\sigma(T)}$, então $\rho(\sigma(T)) = \sigma(T)$, para todo $\sigma \in G$, e consequentemente, $\sigma^{-1}\rho\sigma(T) = T$, para todo $\sigma \in G$. Logo, $\sigma^{-1}\rho\sigma$ fixa T, e portanto, $\sigma^{-1}\rho\sigma \in H_T$. Mas $\rho = \sigma(\sigma^{-1}\rho\sigma)\sigma^{-1} \in \sigma H_T \sigma^{-1}$, ou seja, $H_{\sigma(T)} \subseteq \sigma H_T \sigma^{-1}$. Para ver a inclusão contrária, consideramos $\psi \in \sigma H_T \sigma^{-1}$. Assim, $\psi = \sigma\rho\sigma^{-1}$ onde $\rho \in H_T$. Afirmamos que $\psi \in H_{\sigma(T)}$, isto é, que ψ fixa $\sigma(T)$ para todo $\sigma \in G$. De fato, $\psi(\sigma(t)) = \sigma \circ \rho \circ \sigma^{-1} \circ (\sigma(t)) = \sigma \circ \rho(t) = \sigma(t)$ pois $\rho \in H_T$. Portanto,

$H_{\sigma(T)} = \sigma H_T \sigma^{-1}$, como queríamos mostrar. Por definição, H é um subgrupo normal de G se $H = \sigma H \sigma^{-1}$, para todo $\sigma \in G$, de onde concluímos que um subgrupo H de G é normal se, e só se, $\sigma(T) = T$, para todo $\sigma \in G$. Resta mostrar que $T \subseteq R$ é galoisiana com grupo G/H. Pelo item *3.* do Teorema 3.7, devemos mostrar que $T^{G/H} = R$ e que existem $x'_1, \ldots, x'_n, y'_1, \ldots, y'_n \in T$ satisfazendo a igualdade do item ii) para todo $\sigma \in G/H$. Seja H um subgrupo normal de G e $T = S^H$. Assim, $\sigma(T) = T$, para todo $\sigma \in H$. Considerando novamente $\bar{\sigma}_1, \ldots, \bar{\sigma}_r$ os representantes das classes laterais distintas de H em G, segue que $G/H = \{\bar{\sigma}_i = \sigma_i H | 1 \leq i \leq r\}$ é o conjunto de todas essas classes (observe que precisamos da condição de H ser normal em G para definir esse quociente). Definimos essas funções $\bar{\sigma}_i : T \to T$ por $\bar{\sigma}_i(t) = \sigma_i(t)$, para todo $t \in T$ e $i = 1, \ldots, r$, que está bem definida pois independe do representante. Além disso, $\bar{\sigma}_i(t) = t \Leftrightarrow \sigma_i(t) = t$, o que implica que $T^{G/H} = S^G = R$. Tomando os $x'_i, y'_i \in T$ definidos na prova de que T é G-forte, segue que

$$\sum_{i=1}^{n} x'_i \sigma(y'_i) = \begin{cases} 1 & se \quad \sigma \in H \\ 0 & se \quad \sigma \notin H, \end{cases}$$

para todo $\sigma \in G$. Mas observamos que, se $\sigma \in H$, então $\sigma(t) = \bar{\sigma}_i(t) = t$, para todo $t \in T$, ou seja, $\bar{\sigma}_i = id$, e se $\sigma \notin H$, existe $t \in T$ tal que $\sigma(t) = \bar{\sigma}_i(t) \neq t$ (pois $H_T = H$), e então, $\sigma \neq id$. Dessa forma

$$\sum_{i=1}^{n} x'_i \bar{\sigma}_i(y'_i) = \begin{cases} 1 & se \quad \bar{\sigma}_i = 1 \\ 0 & se \quad \bar{\sigma}_i \neq 1, \end{cases}$$

para todo $\bar{\sigma}_i \in G/H$. Portanto, T é uma extensão galoisiana de R com grupo de Galois G/H. □

A partir dos itens *1.* e *2.* concluímos que as funções φ e ψ estão bem definidas e são inversas uma da outra e, dessa forma, existe uma correspondência biunívoca entre os subgrupos de G e os subanéis de S que contém R e são R-álgebra separável e G-forte, isto é, a cada subgrupo H de G existe uma R-álgebra associada e a cada R-álgebra existe um subgrupo correspondente. Essa correspondência é chamada **correspondência de Galois**. Já o item *3.* estabelece uma condição para que a extensão $T \supset R$ seja galoisiana.

Observe que a hipótese de que T é G-forte no Teorema 3.19 é necessária e não pode ser descartada. Exemplificamos este fato no exemplo a seguir.

Exemplo 3.20. Seja S uma R-álgebra separável dada por $S = Re_0 \oplus Re_1 \oplus Re_2 \oplus Re_3$, onde $e_i e_j = \delta_{ij} e_i$ e $\sum_{i=0}^{3} e_i = 1$. Sejam $G = \langle \sigma \rangle$ um grupo cíclico de ordem 4 tal que

$\sigma(e_i) = e_{i+1(mod4)}$ e $T = R(e_o + e_1) \oplus R(e_2 + e_3)$ um subanel de S. Mostramos que satisfazem:

1. T não é G-forte.
2. $H_T = 1 = H$.
3. T é R-separável.
4. $S^H \neq T$.

Em outras palavras, se no item 2, apenas a condição G-forte for omitida, não podemos concluir a igualdade $S = T^H$, que é fundamental para que as funções sejam inversas uma da outra. Para mostrar que T não é G-forte, é suficiente exibir um par $\sigma, \tau \in G$, onde $\sigma|_T \neq \tau|_T$ e $\sigma|_T$ e $\tau|_T$ não são fortemente distintos, isto é, que existe $e \neq 0$ idempotente de S tal que para todo $s \in S$, tem-se $\sigma|_T(s)e = \sigma|_T(s)e$. Todos os $e_i's$ são idempotentes de S pela maneira que a multiplicação foi definida, então tomando $e_0 \in S$, segue que o par $\sigma, \sigma^2 \in G$, e considerando $t \in T$, dada por $t = a(e_0 + e_1) + b(e_2 + e_3)$ onde $a, b \in R$, segue que $\sigma|_T \neq \sigma^2|_T$. Além disso,

$$\sigma|_T(t)e_o = (a(e_1 + e_2) + b(e_3 + e_0))e_0 = be_o$$

e

$$\sigma^2|_T(t)e_o = (a(e_2 + e_3) + b(e_0 + e_1))e_0 = be_o,$$

o que mostra que T não é G-forte. Agora, vamos mostrar que $H_T = \{1\}$. Tem-se que $1 \in H_T$. Mostramos que os outros elementos de G não fixam T:

- $\sigma(t) = \sigma(a(e_0 + e_1) + b(e_2 + e_3)) = a(e_1 + e_2) + b(e_3 + e_0) \neq t$, e assim, $\sigma \notin H_T$.
- $\sigma^2(t) = \sigma^2(a(e_0 + e_1) + b(e_2 + e_3)) = a(e_2 + e_3) + b(e_0 + e_1) \neq t$, e assim, $\sigma^2 \notin H_T$.
- $\sigma^3(t) = \sigma^3(a(e_0 + e_1) + b(e_2 + e_3)) = a(e_3 + e_0) + b(e_1 + e_2) \neq t$, e assim,, $\sigma^3 \notin H_T$.

Logo, $H_T = \{1\}$. Para ver que T é R-separável devemos tomar $e = 1 \otimes 1 \in T \otimes T^o$ (fazendo $a = b = 1$ em $t = a(e_0 + e_1) + b(e_2 + e_3) \in T$, pois $e_0 + e_1 + e_2 + e_3 = 1$) e mostrar que e é um idempotente de separabilidade de T, ou seja,

- $\mu(e) = 1$.

- $\mathrm{Ker}(\mu)e = 0$. De fato,

$$\begin{aligned}
(a(e_0+e_1)+b(e_2+e_3)\otimes 1)e &= (a(e_0+e_1)+b(e_2+e_3)\otimes 1)(1\otimes 1)\\
&= ae_0+ae_1+be_2+be_3\otimes e_0+e_1+e_2+e_3\\
&= ae_0\otimes e_0+ae_1\otimes e_1+be_2\otimes e_2+be_3\otimes e_3\\
&\overset{a,b\in R}{=} e_0\otimes ae_0+e_1\otimes ae_1+e_2\otimes be_2+e_3\otimes be_3\\
&= e_0+e_1+e_2+e_3\otimes ae_0+ae_1+be_2+be_3\\
&= 1\otimes(a(e_0+e_1)+b(e_2+e_3))\\
&= 1\otimes(a(e_0+e_1)+b(e_2+e_3))(1\otimes 1)\\
&= (1\otimes a(e_0+e_1)+b(e_2+e_3))e.
\end{aligned}$$

Finalmente, para mostrar que $S^H \neq T$, consideramos $x \in S^H$. Assim, $x \in S$ e $\tau(x) = x$, para todo $\tau \in H$. Logo, $S^H = S \neq T$, pois por exemplo $x = ae_o + be_1 + ce_2 + de_3$ com $a \neq b$ e $c \neq d$ pertence a S, mas $x \notin T$.

3.3 Considerações finais

Neste capítulo, analisamos as três definições equivalentes conhecidas de extensão galoisiana de corpos, evidenciando o porquê de não poderem ser estendidas naturalmente para anéis. Em seguida, apresentamos uma outra definição que permite a generalização que buscamos. Com base nesta definição, apresentamos um teorema contendo cinco definições equivalentes para que uma extensão de anéis seja galoisiana. Com um exemplo, mostramos que a definição apresentada para extensão de anéis de Galois é de fato uma generalização da extensão de corpos de Galois, ou seja, o objetivo de apresentar uma definição para que extensão de anéis seja galoisiana, foi cumprido. Feito isso, partimos para o próximo passo, o de encontrar um Teorema Fundamental para essa teoria. Após algumas observações e considerações, concluímos que dada uma extensão galoisiana de anéis $S \supset R$, existe sim uma correspondência entre os subgrupos de $\mathrm{Aut}_R(S) = G$ e os subanéis de S contendo R, mas estes subanéis devem possuir algumas propriedades extras. O anel S deve ser uma R-álgebra separável e G-forte. Desta forma, apresentamos uma teoria de Galois sobre anéis comutativos, objetivo deste trabalho.

Este estudo é passível de continuação, pois existem alguns caminhos que podem ser tomados. É possível utilizar esta teoria para estudar o grupo de Brauer de um anel comutativo, ou até mesmo, generalizar ainda mais o que fizemos aqui, apresentando uma teoria de Galois sobre anéis não comutativos.

4 Aplicações em códigos

A maioria dos trabalhos sobre códigos fazem o estudo deste sobre corpos, mas códigos sobre anéis podem ser apropriados em alguns contextos. Descobertas recentes de que bons códigos binários não lineares estão relacionados com códigos lineares sobre $\mathbb{Z}_4$, tem motivado os estudo dos códigos sobre anéis em gerais. Uma das vantagens de estudar os códigos sobre anéis é que eles servem de base para a construção de códigos definidos sobre grupos abelianos. O objetivo, deste capítulo, é apresentar códigos sobre o anel $\mathbb{Z}_m$ a partir da álgebra de grupo $\mathbb{Z}_m G$. Na primeira seção, apresentamos a definição de anel e álgebra de grupo e alguns resultados que determinam quando $\mathbb{Z}_m G$ é semi-simples, e em seguida, na segunda seção, trabalhamos para encontrar as estruturas dos códigos. Neste capítulo nos baseamos nas definições e nos resultados apresentados em [2], [3], [6], [9], [11], [17], [20] e [21].

Algumas demonstrações deste capítulo serão omitidas, pois fogem ao objetivo do nosso estudo.

4.1 Anel de grupo

Dados um grupo G e um anel R podemos construir um novo anel, o chamado anel de grupo. Além disso, quando R é comutativo, este anel pode ser visto como uma R-álgebra. É por meio desta estrutura que investigaremos os códigos sobre $\mathbb{Z}_m$.

Definição 4.1. *Sejam G um grupo e R um anel com unidade. Considere o conjunto*

$$RG = \left\{ \sum_{g \in G} a_g g \ | a_g \in R, \ g \in G \text{ e } a_g = 0 \quad \textit{exceto para um número finito de termos} \right\}$$

e para $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g$ pertencentes a RG, considere as operações:

- $\alpha + \beta = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$;
- $\alpha\beta = \sum_{g,h \in G} (a_g b_h) gh$.

*O conjunto RG munido destas operações é chamado **anel de grupo** de G sobre R.*

O elemento neutro de RG é dado por $1_{RG} = 1_R 1_G$ e o inverso aditivo por $-\alpha = \sum_{g\in G}(-a_g)g$. Para que dois elementos α, β de RG sejam iguais, devemos ter $a_g = b_g$, para todo $g \in G$. Sejam $\lambda \in R$ e $\alpha = \sum_{g\in G} a_g g \in RG$. Assim, podemos definir o produto escalar como

$$\lambda\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G}(\lambda a_g)g.$$

Com essa operação e a operação soma, segue que RG tem estrutura de R-módulo, e consequentemente, considerando as três operações e sendo R um anel comutativo, RG pode ser visto como uma R-álgebra, chamada de **álgebra de grupo** de G sobre R. Na próxima seção, estamos interessados nas álgebras de grupo que são semi-simples. Os próximos teoremas dão algumas condições para que isso ocorra.

Teorema 4.2. *[15] (Teorema de Maschke) Sejam G um grupo e R um anel com identidade. A álgebra de grupo RG é semi-simples se, e somente se, R é um anel semi-simples, a ordem n de G é finita e n é uma unidade em R.*

Corolário 4.3. *Se G é um grupo e K é um corpo de característica 0 ou p primo que não divide a ordem de G, então a álgebra de grupo KG é semi-simples.*

Desta forma, a álgebra de grupo $\mathbb{Z}_m C_n$ onde C_n é um grupo cíclico de ordem n, é semi-simples se, e somente se, $\mathbb{Z}_m$ é semi-simples e n é uma unidade de $\mathbb{Z}_m$. Mas $\mathbb{Z}_m$ é semi-simples se, e somente se, m é o produto de primos distintos. De fato, supondo que existe um primo p repetido na decomposição de m, podemos escrever $m = kp^2$, e assim, kp seria um elemento nilpotente de $\mathbb{Z}_m$, pois $(kp)^2 = km = 0$, mas isso contradiz o fato de que $\mathbb{Z}_m$ é semi-simples (lembre-se que para anéis comutativos, que é o caso de $\mathbb{Z}_m$, não ter ideais nilpotentes equivale a não ter elementos nilpotentes). A recíproca é claramente verdadeira, visto que se m é o produto de primos distintos, segue que $\mathbb{Z}_m$ se decompõe como o produto de corpos (que são semi-simples). Além disso, n é uma unidade de $\mathbb{Z}_m$ se, e somente se, $\text{mdc}(m, n) = 1$. Com essa discussão, acabamos de provar o próximo resultado.

Proposição 4.4. *$\mathbb{Z}_m C_n$ é semi-simples se, e somente se,*

- *$m = \prod_{i=1}^{t} p_i$, onde cada p_i é primo e $p_i \neq p_j$, para todo $i \neq j$.*
- *$mdc(m, n) = 1$.*

Agora, consideremos a aplicação

$$\begin{array}{rccc} \phi: & \mathbb{Z}_m & \to & \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_t} \\ & i & \mapsto & (a_i(1), a_i(2), \ldots, a_i(t)), \end{array}$$

onde $i \in \mathbb{Z}_m$ e $i \equiv a(j)\text{mod}(p_j)$. A função ϕ é um isomorfismo de anéis conhecido da teoria dos números. Assim, a partir de ϕ, podemos definir

$$\psi : \mathbb{Z}_m G \longrightarrow \mathbb{Z}_{p_1} G \times \mathbb{Z}_{p_2} G \times \cdots \times \mathbb{Z}_{p_t} G$$

dada por

$$\psi\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} \phi(r_i) g_i = \left(\sum_{i=1}^{n} a_i(1) g_i, \sum_{i=1}^{n} a_i(2) g_i, \ldots, \sum_{i=1}^{n} a_i(t) g_i\right),$$

com $r_i \in \mathbb{Z}_m$ e $g_i \in G$, que é também um isomorfismo, por consequência de ϕ ser um isomorfismo. Este isomorfismo de álgebras será o ponto chave da investigação dos códigos sobre $\mathbb{Z}_m$, e a partir dele, demonstramos o próximo teorema.

Teorema 4.5. *Sejam G um grupo finito de ordem n e $m = \prod_{i=1}^{t} p_i$, onde p_i são primos distintos. Se $mdc(m, n) = 1$, então $\mathbb{Z}_m G \cong \mathbb{Z}_{p_1} G \times \cdots \times \mathbb{Z}_{p_t} G$.*

Observação 4.6. O isomorfismo $\mathbb{Z}_m G \cong \prod_{i=1}^{t} \mathbb{Z}_{p_i}^{e_i} G$ é válido para todo $e_i \geq 1$, mas para $e_i > 1$, as parcelas $\mathbb{Z}_{p_i}^{e_i} G$ e a álgebra $\mathbb{Z}_m G$ não são semi-simples.

A adição e a multiplicação em $\prod_{i=1}^{t} \mathbb{Z}_{p_i} C_n$ são inerentes de $\mathbb{Z}_m C_n$ e são definidas como segue. Sejam $a = \sum_{i=1}^{n} (a_i(1), \ldots, a_i(t)) g^i$ e $b = \sum_{j=1}^{n} (b_j(1), \ldots, b_j(t)) g^j$ elementos de $\prod_{i=1}^{t} \mathbb{Z}_{p_i} C_n$. Assim,

- $a + b = \sum_{i=1}^{n} (a_i(1) + b_i(1), \ldots, a_i(t) + b_i(t)) g^i$;
- $ab = \sum_{i=1}^{n} \sum_{j=1}^{n} (a_i(1) b_j(1), \ldots, a_i(t) b_j(t)) g^i g^j$.

4.2 Códigos

Nesta seção, apresentamos um método para construir códigos sobre os anéis $\mathbb{Z}_m$, onde m é um inteiro qualquer. Dado o número inteiro m, ele pode ser decomposto como $m = p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}$, onde p_i são primos e e_i inteiros positivos. Quando $e_i = 1$ para todo i, ou seja, quando m é o produto de primos distintos, o trabalho de encontrar os códigos sobre $\mathbb{Z}_m$ resume-se em encontrar os códigos sobre os corpos $\mathbb{Z}_{p_i} = GF(p_i)$, o que facilita o nosso trabalho. Já quando m possui uma potência de um primo, isto

é, quando existe $e_i > 1$, devemos usar outras ferramentas para resolver o problema, já que $\mathbb{Z}_{p_i}^{e_i}$ não é corpo e $\mathbb{Z}_m G$ não é semi-simples neste caso, e por isso, o estudo dos códigos sobre $\mathbb{Z}_m$ é dividido nestes dois casos, que aqui representarão duas subseções. Em resumo, nesta seção faremos a construção de códigos cíclicos sobre o anel $\mathbb{Z}_m$ a partir dos códigos cíclicos sobre os corpos $GF(p_i)$.

Antes de iniciar as construções dos códigos $\mathbb{Z}_m$, vejamos algumas definições básicas da teoria de códigos.

Definição 4.7. *Dado um anel R comutativo com unidade, um subconjunto C de R^n é chamado de* ***código linear*** *de comprimento n sobre R, se C é um R-submódulo próprio de R^n. Os elementos do código C são chamados de* ***palavras****.*

Definição 4.8. *Dados $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ palavras do código C, chamamos de* ***distância de Hamming*** *entre u e v ao valor*

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|,$$

ou seja, é o número de coordenadas distintas entre duas palavras.

Definição 4.9. *A* ***distância de um código*** *C é definida como:*

$$d(C) = min\{d(u, v) : u, v \in C \backslash \{0\}\},$$

onde $d(x, y)$ é a distância de Hamming. Como o código é linear, segue que $d(u, v) = d(u - v, 0)$, e assim, a distância de um código pode ser definida como o menor valor de coordenadas não nulas considerando todas as palavras de C.

Definição 4.10. *Dado $u = (u_1, \ldots, u_n) \in C$, define-se o* ***peso*** *de u como*

$$\omega(u) = |\{i : u_i \neq 0\}|.$$

Observamos que o peso de um elemento u é a distância de Hamming entre u e 0.

Definição 4.11. *O peso de um código C é dado por*

$$\omega(C) = min\{\omega(u) : u \in C \backslash \{0\}\}.$$

Das Definições 4.9, 4.10 e 4.11, segue que $d(C) = \omega(C)$.

Uma classe importante dos códigos lineares, são os chamados códigos cíclicos, que definimos a seguir.

Definição 4.12. *Um código linear C sobre R é cíclico se sempre que $v = (v_0, v_1, \ldots, v_{n-1}) \in C$, a palavra $v' = (v_{n-1}, v_0, \ldots, v_{n-2}) \in C$.*

Note que o conjunto de todas as palavras pertencentes a um código cíclico C, formam um subconjunto do anel $R_n = R[x]/\langle x^n - 1\rangle$, isto é, do conjunto de todos os polinômios cujo grau é menor do que n. Olhando para $R = \mathbb{Z}_m$, isto quer dizer que cada palavra código c de C é associada a um polinômio $c(x)$ via o isomorfismo

$$\begin{array}{rccc} \nu: & \mathbb{Z}_m^n & \to & \frac{\mathbb{Z}_m[x]}{\langle x^n-1\rangle} \\ & (c_0,\ldots,c_{n-1}) & \mapsto & c_o + c_1x + \cdots + c_{n-1}x^{n-1}. \end{array}$$

Observe que, se $\mathbb{Z}_m$ é um corpo, então C é um subespaço de $\mathbb{Z}_m^n$. Assim, se m e n são relativamente primos e m é primo, os códigos cíclicos de comprimento n sobre $\mathbb{Z}_m$ são associados com os ideais principais cujos geradores são fatores de $\langle x^n - 1\rangle$. Mas, se $\mathbb{Z}_m$ é um anel que não é corpo, então o ideal R_n não é necessariamente principal, além de a fatoração de $\langle x^n - 1\rangle$ não ser única, o que torna mais difícil a classificação dos códigos cíclicos sobre $\mathbb{Z}_m$. Para contornar esse problema, vamos considerar os anéis de grupo $\mathbb{Z}_mC_n$, onde C_n é um grupo cíclico de ordem n gerado por g, e então, vamos associar os códigos de $\mathbb{Z}_m$ aos coeficientes dos polinômios de $\mathbb{Z}_mC_n$.

O próximo resultado, que vale para anéis gerais, garante que C não é apenas um subconjunto de R_n, mas sim um ideal, fato que será muito útil a esse estudo, pois assim podemos associar os códigos cíclicos de RG aos ideais de R_n, ideia central utilizada nesta seção.

Teorema 4.13. *Um código C de comprimento n sobre R é cíclico se, e somente se, C é um ideal de R_n.*

Demonstração. Seja C um código cíclico de comprimento n sobre R. Então, de acordo com o isomorfismo ν, segue que $xc(x) \in C$, para todo polinômio $c(x) \in R[x]$. Logo, $x^ic(x) \in C$, para todo i. Como C é linear, segue que $a(x)c(x) \in C$ para todo $a(x) \in R_n$. Portanto, C é ideal em R_n. Reciprocamente, seja $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ um elemento de R_n. Então $xc(x) \in C$, já que C é um ideal em R_n. Portanto, C é um código cíclico sobre R. □

A partir do Teorema 4.13, obtemos a seguinte definição.

Definição 4.14. *Um **código cíclico linear** de comprimento n sobre $\mathbb{Z}_m$ é o conjunto das n-uplas associadas com os elementos de um ideal de $\mathbb{Z}_mC_n$.*

Assim, a quantidade de códigos para cada $\mathbb{Z}_m$ é a quantidade de ideais que $\mathbb{Z}_mC_n$ possui. Supondo que G é finito de ordem n e que seus elementos estão escritos na ordem $g_1, g_2, \ldots, g_n$, segue que a cada elemento $\sum_{i=1}^{n} a_ig_i$, podemos associar a n-upla $(a_1, \ldots, a_n)$, que representa uma palavra do código.

Quando mencionarmos um (n, k) código sobre $GF(q)$, estamos referindo a um código de comprimento n, isto é, cada palavra tem n dígitos, é uma n-upla, e este código tem q^k palavras.

4.2.1 Códigos sobre $\mathbb{Z}_m$ onde m é o produto de primos distintos

Nesta subseção, dedicaremos nosso trabalho para a construção dos códigos sobre $\mathbb{Z}_m$, onde m é o produto de primos distintos, pois, neste caso, a álgebra de grupo $\mathbb{Z}_m G$ é semi-simples, o que nos trás algumas facilidades. Uma das vantagens de se trabalhar com álgebra semi-simples, é que neste caso todo ideal é um produto de ideais minimais, e assim o nosso trabalho de encontrar os códigos sobre $\mathbb{Z}_m$ resume-se ao trabalho de encontrar os ideais minimais de $\mathbb{Z}_m C_n$, com $(m, n) = 1$.

Da teoria de códigos, segue que todo código cíclico linear de comprimento n pode ser visto como um ideal na álgebra de grupo RC_n, onde $C_n = \langle g \rangle$ é um grupo cíclico de ordem n gerado por g. Esta interpretação dos códigos cíclicos é de extrema importância para conseguirmos determinar suas estruturas, pois veremos que os ideias de $\mathbb{Z}_m G$ e o produto dos ideais de $\mathbb{Z}_{p_i} G$ estão em correspondência.

Neste momento, estamos preocupados com esta associação entre os ideais e em como podemos encontrar códigos de $\mathbb{Z}_m$ a partir deles, mas a estrutura dos ideais minimais e seus geradores idempotentes não serão considerados.

Nosso objetivo, agora, é mostrar que existe uma correspondência entre os ideais de $\mathbb{Z}_m C_n$ e o produto direto de ideais de $\prod_{i=1}^{t} \mathbb{Z}_{p_i} C_n$. Para isso, apresentamos uma definição para o produto direto de ideais.

Definição 4.15. *Seja B_l um ideal em $\mathbb{Z}_{p_l} C_n$. O produto direto de ideais $\prod_{i=1}^{t} B_i$ em $\prod_{i=1}^{t} \mathbb{Z}_{p_i} C_n$ é definido como o conjunto*

$$\{(b(1), \ldots, b(t)) : b(i) \in B_i\},$$

onde todas as combinações possíveis são consideradas.

Como o produto direto de ideais é um ideal, segue que o produto direto de ideais em $\prod_{i=1}^{t} \mathbb{Z}_{p_i} C_n$ corresponde a um ideal em $\mathbb{Z}_m C_n$. Agora, falta mostrar a recíproca. Seja A um ideal em $\mathbb{Z}_m C_n$ formado pelos elementos $\left\{ \sum_{i=1}^{n} r_i^{(j)} g^i \right\}$, onde j varia em algum conjunto de índices K para dar cada elemento de A (ou seja, A tem a quantidade de elementos que K possui). Assim,

$$\psi\left(\sum_{i=1}^{n} r_i^{(j)} g^i\right) = \left\{\left(\sum_{i=1}^{n} a_i(1)g^i, \ldots, \sum_{i=1}^{n} a_i(t)g^i\right)^{(j)}\right\}$$

$$= \left(\sum_{i=1}^{n} a_i^{(1)} g^i\right)^{(j)}, \ldots, \left(\sum_{i=1}^{n} a_i^{(t)} g^i\right)^{(j)},$$

onde $j \in K$. Seja A_l o conjunto formado pelos elementos $\left\{\left(\sum_{i=1}^{n} a_i^{(l)} g^i\right)^{(j)}\right\}$ para $l = 1, \ldots, t$, onde a função do j é indicar que este elemento refere-se ao elemento $\sum_{i=1}^{n} r_i^{(j)} g^i$ de A. Como A é ideal em $\mathbb{Z}_m C_n$, segue que A_l é ideal em $\mathbb{Z}_{p_l} C_n$. Assim, para mostrar que existe uma correspondência entre os ideais, resta mostrar que a imagem de um ideal A em $\mathbb{Z}_m C_n$ é o produto de ideais em $\prod_{i=1}^{t} \mathbb{Z}_{p_i} C_n$. Para isso, vamos considerar os ideais A_l, e mostrar que dado um ideal A, ele pode ser escrito como um produto desses ideais. Mas, para ver que isso ocorre, é suficiente mostrar que para todo $a = \sum_{i=1}^{n} a_i g^i \in A$ tal que $\psi(a) = \sum_{i=1}^{n} (a_i(1), \ldots a_i(t)) g^i$, considerando $\psi : \mathbb{Z}_m G \to \mathbb{Z}_{p_1} G \times \mathbb{Z}_{p_2} G \times \cdots \times \mathbb{Z}_{p_t} G$ definida como na Seção 4.1, a imagem inversa $\psi^{-1}\left(\sum_{i=1}^{n} (0, \ldots a_i(l), \ldots 0) g^i\right) \in A$. Isso segue do fato que tomando $r \in R$ tal que $\phi(r) = (0, \ldots, 0, 1, 0, \ldots, 0)$, onde 1 está na l-ésima coordenada, utilizando a aplicação $\phi : \mathbb{Z}_m \to \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_t}$ definida na Seção 4.1, obtemos

$$\psi(ra) = \sum_{i=1}^{n} (0, \ldots a_i(l) \ldots, 0) g^i.$$

Assim, todo ideal em $\mathbb{Z}_m C_n$ é um produto de ideais A_l em $\prod_{i=1}^{t} Z_{p_i} C_n$, e vice-versa, de modo que existe uma bijeção entre estes ideais.

Como os elementos dos ideais são associados a uma n-upla que é uma palavra do código, para determinar os códigos sobre $\mathbb{Z}_m$, é suficiente encontrar os ideais de $\mathbb{Z}_{p_i} C_n$, pois a partir da correspondência dada por ψ obtemos os ideais de $\mathbb{Z}_m C_n$, e a partir de cada ideal construímos um código cujas palavras correspondem aos seus elementos. Encontrar explicitamente estes ideais não é o nosso objetivo, mas sim construir um código sobre $\mathbb{Z}_m$ a partir de códigos dados sobre $\mathbb{Z}_{p_i} = GF(p_i)$.

Consideremos um conjunto de (n, k_i) códigos (ideais) A_i sobre $GF(p_i)$ com distâncias mínimas d_i, para $i = 1, \ldots, t$. Pela correspondência entre os ideais, segue que o produto direto desses códigos é isomorfo a um código A sobre $\mathbb{Z}_m$. Também, de acordo com a definição dada para o produto direto de ideais, concluímos que o código A tem

$\prod_{i=1}^{t} p_i^{k^i}$ palavras de comprimento n (cada código tem $p_i^{k^i}$ palavras) e a distância mínima é dada por $\min_i d_i$, como veremos adiante.

Agora, vamos mostrar explicitamente a construção do código A em $\mathbb{Z}_m$ a partir dos códigos dados em $GF(p_i)$. Seja $a_j = \sum_{i=1}^{n} a_i g^i$ um elemento do ideal A_j que é associado à palavra $(a_1(j), \ldots, a_n(j))$, para $j = 1, \ldots, t$. Assim, $\left(\sum_{i=1}^{n} a_i(1)g^i, \ldots, \sum_{i=1}^{n} a_i(t)g^i\right)$ é um elemento de $\prod_{i=1}^{t} A_i$ que pode ser identificada sob a inversa ψ^{-1} com o elemento $\sum_{i=1}^{n} \alpha_i g^i \in \mathbb{Z}_m C_n$, onde $\alpha_i = \psi^{-1}(a_i(1), \ldots, a_i(t)) \in \mathbb{Z}_m$ e a este elemento é associada a n-upla $w = (\alpha_1, \ldots, \alpha_n)$, que representa uma palavra do código A em $\mathbb{Z}_m$. Fazendo essa correspondência para cada elemento do ideal $\prod_{i=1}^{t} A_i$ encontramos todos os elementos do ideal A, e consequentemente, todas as palavras do código A. Para facilitar a compreensão e a explicação do próximo fato, vamos explicitar os elementos a_j. Se

$$a_1 = (a_1(1), \ldots, a_n(1)) \in \mathbb{Z}_{p_i} C_n$$

$$\vdots$$

$$a_t = (a_1(t), \ldots, a_n(t)) \in \mathbb{Z}_{pi} C_n,$$

então a primeira coordenada de w é obtida a partir da primeira coordenada das n-uplas a_j, e assim sucessivamente, para todas as coordenadas. Usando este fato, vejamos que realmente a distância mínima do código A é dada por $\min_i d_i$. Suponhamos que $(t-1)$ das n-uplas a_i são nulas e a outra tem peso $\min_i d_i$. Assim, a partir dessas n-uplas, obtemos uma palavra de peso $\min_i d_i$, e toda palavra sobre $\mathbb{Z}_m$ terá no mínimo peso $\min_i d_i$, pois como ψ é um isomorfismo, segue que uma palavra de um código em $\mathbb{Z}_m$ só terá um dígito zero em uma determinada posição se esta coordenada é nula em todas as n-uplas a_j. Resumindo, dada uma coleção de (n, k_i) códigos sobre $GF(p_i)$ com distâncias mínimas d_i, construímos um código de comprimento n sobre $\mathbb{Z}_m$ com $\prod_{i=1}^{t} p_i^{k_i}$ palavras e distância mínima $\min_i d_i$.

Exemplo 4.16. Consideremos a álgebra de grupo $\mathbb{Z}_{15}C_8 \cong \mathbb{Z}_3C_8 \times \mathbb{Z}_5C_8$. Sejam o $(8, 3)$ código sobre $\mathbb{Z}_3$ gerado pelo polinômio $g_1(x) = 1 + x + x^2 + 2x^3 + x^5$ que pode ser visto como um ideal A_1 de $\mathbb{Z}_3C_8$ e o $(8, 2)$ código sobre $\mathbb{Z}_5$ gerado por $g_2(x) = 2 + 2x + x^2 + x^4 + 2x^5 + x^6$ visto como o ideal A_2 em $\mathbb{Z}_5C_8$. Assim $A_1 \times A_2$ é um ideal em $\mathbb{Z}_{15}$, e logo, seus elementos podem ser identificados como palavras do código

A. Pela forma como definimos o produto, A tem $3^3 \times 5^2$ palavras e distância mínima 5. Tomando os elementos $a_1 = (11120100) \in A_1$ e $a_2 = (22101210) \in A_2$ correspondentes a $g_1 \in A_1$ e $g_2 \in A_2$, respectivamente, vamos determinar o elemento correspondente $(a_1, a_2) \in A_1 \times A_2 \cong A$ em $\mathbb{Z}_{15}C_8$. Usando o processo descrito nesta seção, encontramos cada coordenada da n-upla com as respectivas coordenadas de a_1 e a_2. Assim, a primeira e a segunda coordenadas são obtidas fazendo $\psi^{-1}(1,2) = a$, onde a satisfaz as congruências $a \equiv 1 \bmod(3)$ e $a \equiv 2 \bmod(7)$. Facilmente se vê que $\psi^{-1}(1,2) = 7$. Fazendo esse processo para as 8 coordenadas, obtemos que $a_1 \times a_2 = (77156760) \in A_1 \times A_2$ é um elemento do código A. É possível encontrar todos os $3^3 \times 5^2$ elementos de A a partir dos elementos de A_1 e A_2 prosseguindo desta maneira.

4.2.2 Códigos sobre $\mathbb{Z}_m$, onde m é uma potência de um primo

Agora, vamos analisar os códigos sobre $\mathbb{Z}_m$, onde $m = p^n$ com p primo. A álgebra $\mathbb{Z}_{p^n}G$ não é semi-simples, e assim, nada podemos afirmar sobre sua decomposição e seus ideais diretamente, por isso partimos da álgebra $\mathbb{Z}_pG$ que é semi-simples, fato que nos permite usar o Teorema de Wedderburn, e então, com o auxílio de outros resultados, conseguimos determinar os ideais de $\mathbb{Z}_{p^n}C_n$ a partir dos ideais de $\mathbb{Z}_pC_n$.

Antes de iniciar a construção dos códigos sobre $\mathbb{Z}_{p^n}$, faremos uma análise mais aprofundada sobre os ideais minimais da decomposição de $\mathbb{Z}_mC_n$ dada na Seção 4.2.1. A análise que faremos agora será fundamental para a investigação do caso $\mathbb{Z}_{p^n}$.

Como $\mathbb{Z}_pG$ é semi-simples, pelo Corolário 2.26, segue que existem corpos $F_1, \ldots, F_t$ que são extensões do corpo $\mathbb{Z}_p$ tal que $Z_pG \cong F_1 \times \cdots \times F_t$. Como $\mathbb{Z}_pG$ tem característica p, segue que os corpos F_i também terão, e logo, da teoria de corpos finitos, segue que F_i terá p^{n_i} elementos para algum inteiro positivo n_i. Também, da teoria de corpos finitos, segue que todo subgrupo finito de um corpo é cíclico, e assim, o subgrupo multiplicativo $F_i^* = F_i \backslash \{0\}$ é cíclico de ordem $p^{n_i} - 1$, de modo que existe $a_i \in F_i^*$ tal que $a_i^{p^{n_i}-1} = 1$, e para todo $m < p^{n_1} - 1$, segue que $a_i^m \neq 1$, ou seja, a_i é uma raiz $p^{n_i} - 1$-ésima da unidade, e assim, $F_i \cong \mathbb{Z}_p(a_i)$. Logo,

$$\mathbb{Z}_pG \cong \prod_{i=1}^{t} \mathbb{Z}_p(a_i). \tag{4.1}$$

Da teoria de álgebras semi-simples, segue que toda álgebra semi-simples é uma soma direta de ideais minimais e essa decomposição é única, de onde vem que os corpos F_i também podem ser interpretados como ideais minimais (em um corpo os únicos ideais são (0) e o próprio corpo, e como por definição o ideal minimal é não nulo, só pode ser o próprio corpo o seu único ideal minimal). Como em cada parcela os únicos ideais são (0) e F_i, existem t parcelas, e vimos que todo produto direto de ideais é um ideal e vice-versa, $\mathbb{Z}_pG$ possui 2^t ideais.

Este método não se aplica a $\mathbb{Z}_{p^n}G$, pois o mesmo não é semi-simples, por isso usamos outra estratégia, mas que não foge a esta ideia. Nosso objetivo, agora, é tentar descrever $\mathbb{Z}_{p^n}G$ de maneira similar à Equação (4.1).

Sejam r tal que $(r,p) = 1$ e $F = \mathbb{Z}_p(\zeta_r)$, onde ζ_r é a raiz r-ésima da unidade. Suponhamos que r é um divisor de $p^n - 1$ e que r não divide $p^k - 1$, para $k < n$. Com essa notação em mente, enunciamos o próximo resultado que encontra-se em [20], cuja prova será omitida por fugir ao nosso intuito.

Teorema 4.17. *Considerando o anel $R = \mathbb{Z}_{p^k}(\zeta_r)$, para algum inteiro k positivo, então*

$$RG \cong \bigoplus_{i=1}^{t} [R(\zeta_{m_i})]_{n_i}.$$

Utilizando o Teorema 4.17 para $R = \mathbb{Z}_{p^n}$, segue que

$$\mathbb{Z}_{p^n}G \cong \prod_{i=1}^{t} [Z_{p^n}(\zeta_{k_i})]_{n_i},$$

ou seja, escrevemos $\mathbb{Z}_{p^n}G$ como o produto direto de matrizes sobre os corpos $\mathbb{Z}_{p^n}(\delta_{k_i})$ que possuem um número finito de ideais, e logo, as matrizes também possuem, de acordo com o resultado a seguir que nos mostrará como são os ideais dessas matrizes.

Teorema 4.18. *Sejam R um anel comutativo com unidade e $S = [R]_n$, isto é, o anel das matrizes $n \times n$ sobre R. Se I é um ideal de S, então existe um ideal J de R tal que $I = [J]_n$.*

Demonstração. Sejam E_{ij} as matrizes $n \times n$ tal que o coeficiente da i-ésima linha e j-ésima coluna é 1 e todas as outras posições são preenchidas com zero. Chamamos C_{ij} às matrizes obtidas da identidade permutando a i-ésima e a j-ésima coluna. Para $i, j \in \mathbb{Z}$ tal que $1 \leq i, j \leq n$, considere as aplicações

$$\begin{array}{rccc} T_{ij}: & I & \to & R \\ & A & \mapsto & a_{ij}, \end{array}$$

onde $A = (a_{ij})$, isto é, a matriz formada pelos coeficientes a_{ij}. Usando o fato que $T_{ij}(A+B) = T_{ij}(A)+T_{ij}(B)$ e $T_{ij}(rA) = rT_{ij}(A)$, para todo $A, B \in I$ e $r \in R$, podemos afirmar que $J_{ij} = \{T_{ij}(A) : A \in I\}$ é um ideal de R. Mas considerando i, j, k, l tal que $1 \leq i, j, k, l \leq n$ e $A \in I$, segue que $C_{ik}AC_{jl} \in I$ e $T_{ij}(A) = T_{kl}(C_{ik}AC_{jl})$, de modo que $J_{ij} = J_{kl}$, pois para cada A que resulta um valor em J_{ij}, existe $C_{ik}AC_{jl}$ que resulta no mesmo valor em J_{kl}. Logo, J_{ij} independe de i, j, isto é, os J_{ij} são todos iguais. Assim, tomando $J = J_{11}$, segue que $I \subset [J]_n$, onde J possui todos os elementos da matriz A que esta em I. Para mostrar a inclusão contrária, é suficiente mostrar que para i, j tal

que $1 \leq i, j \leq n$ e $r \in R$, segue que $rE_{ij} \in I$ (assim I terá coeficientes em R). Seja $I_{ij} = \{A \in I : T_{kl}(A) = 0, \text{ se } (k,l) \neq (i,j)\}$, isto é, as matrizes preenchidas por 0 nas posições diferentes de ij. Assim, $J'_{ij} = \{T_{ij}(A) : A \in I_{ij}\} \subset J$ é um ideal de R, uma vez que contém todos os coeficientes da posição ij. Mas, como $A \in I$, segue que $E_{ii}AE_{jj} \in I_{ij}$ e $T_{ij}(A) = T_{ij}(E_{ii}AE_{jj})$, de modo que $J'_{ij} = J_{ij} = J$, e logo, $r \in J$, pois $r \in J'_{ij}$. Portanto, $rE_{ij} \in I_{ij} \subset I$, o que prova o teorema. □

Assim, os ideais de $[\mathbb{Z}_{p^n}(\zeta_{k_i})]_{n_i}$ são dados a partir dos ideais de $\mathbb{Z}_{p^n}(\zeta_{k_i})$, e logo, $[\mathbb{Z}_{p^n}(\zeta_{k_i})]_{n_i}$ tem $n+1$ ideais: $[\mathbb{Z}_{p^n}(\zeta_{k_i})]_{n_i}$, $[p\mathbb{Z}_{p^n}(\zeta_{k_i})]_{n_i} \ldots, [p^n\mathbb{Z}_{p^n}(\zeta_{k_i})]_{n_i} = 0$. Assim, cada ideal minimal de $\mathbb{Z}_pG$, induz $n+1$ ideais em $\mathbb{Z}_{p^n}G$, de modo que existem $(n+1)^t$ ideais em $\mathbb{Z}_{p^n}G$. Dessa forma, para determinar os ideais, e logo, os códigos de $\mathbb{Z}_{p^n}G$ é suficiente determinar os ideais de $[\mathbb{Z}_{p^n}(\zeta_{k_i})]_{n_i}$ e para isso é suficiente encontrar os ideais de $\mathbb{Z}_{p^n}(\zeta_{k_i})$.

Em suma, para encontrar os códigos sobre $\mathbb{Z}_{p^n}$ procedemos da seguinte maneira. Primeiramente, encontramos os ideais minimais de $\mathbb{Z}_pG$, que são os corpos F_i de ordem p^{n_i}, em seguida determinamos os elementos $a_i > 0$ tal que $p^{n_i} \equiv 1 (\text{mod } a_i)$ mas $p^i \neq 1 (\text{mod } a_i)$, para $i < n_i$, isto é, os elementos a_i que são uma raiz $p_{n_i} - 1$-ésima da unidade. Desta forma, F_i irá conter todas as raízes de $x^{p^{n_i}} - 1$ e logo, $F_i = \mathbb{Z}_p(a_i)$. Usando o Teorema 4.17, chegamos que $\mathbb{Z}_{p^n}G \cong \prod_{i=1}^{t}[\mathbb{Z}_{p^n}(a_i)]$. Assim, todos os ideais, e logo, todos os códigos de $\mathbb{Z}_{p^n}G$, podem ser obtidos.

Portanto, dados os códigos sobre $\mathbb{Z}_p = GF(p)$, encontramos os códigos sobre $\mathbb{Z}_{p^n}$ da maneira descrita nesta seção, e então, usando o isomorfismo descrito na Observação 4.6 considerando a função

$$\psi : \mathbb{Z}_mG \to \mathbb{Z}_{p_1}^{e_1}G \times \mathbb{Z}_{p_2}^{e_2}G \times \cdots \times \mathbb{Z}_{p_t}^{e_t}G$$

dada por

$$\psi\left(\sum_{i=1}^{n} r_ig_i\right) = \sum_{i=1}^{n}\phi(r_i)g_i = \left(\sum_{i=1}^{n} a_i(1)g_i, \sum_{i=1}^{n} a_i(2)g_i, \ldots, \sum_{i=1}^{n} a_i(t)g_i\right),$$

conseguimos obter os códigos sobre $\mathbb{Z}_m$ para m qualquer, do mesmo modo como foi feito na Subseção 4.2.1.

Não foi encontrado nenhum exemplo na literatura deste caso, quando m é a potência de um primo. A dificuldade está em encontrar os ideais minimais da decomposição da álgebra de grupo $\mathbb{Z}_pG$, para então obter os ideais de $\mathbb{Z}_{p^n}G$. Assim, determinar esses ideais pode ser um tema para um trabalho futuro.

4.3 Considerações finais

Neste capítulo, apresentamos algumas definições básicas sobre anel e álgebra de grupo e algumas noções relativas à teoria dos códigos. Com essa base, apresentamos um método para construir códigos sobre o anel $\mathbb{Z}_m$, onde m é um inteiro qualquer, a partir dos códigos sobre os corpos $GF(p)$, onde p é primo, utilizando conceitos apresentados no Capítulo 2, especialmente as álgebras semi-simples e o Teorema de Wedderburn.

Em trabalhos futuros este estudo dos códigos pode ser aprofundado e outros aspectos podem ser considerados. Também podem ser construídos códigos BCH, de Hamming e Reed-Solomon sobre anéis.

5 Conclusões e perspectivas futuras

Ao generalizar algum conceito, é comum que algumas propriedades válidas no caso específico sejam perdidas. Por esta razão, sempre procuramos quais características mínimas devemos adicionar ao caso mais geral de modo que a propriedade desejada continue válida. No trabalho de generalização da teoria de Galois sobre corpos para anéis comutativos, tivemos esta preocupação, visto que considerando anéis comutativos gerais não obtemos uma teoria de Galois consistente.

Ao desenvolver a teoria de Galois sobre anéis, a definição básica de extensão galoisiana, como sendo uma extensão normal e separável, não pode ser generalizada naturalmente, uma vez que estes conceitos não estão bem definidos no contexto dos anéis. Explorando outras definições equivalentes, conseguimos obter uma generalização e apresentar uma definição para extensão galoisiana de anéis provando cinco definições equivalentes que envolvem módulo projetivo, isomorfismos e álgebras separáveis.

Dada uma extensão de anéis $S \supset R$ e sendo G o grupo dos automorfismos de S, considerando simplesmente os subanéis de S e os subgrupos de G, não é possível estabelecer uma correspondência entre eles, mas considerando os subanéis de S que contém R, e são R-álgebras separáveis e G-forte, é possível estabelecer uma correspondência biunívoca entre estas e os subgrupos de G, que é dada pelo Teorema Fundamental da Teoria de Galois.

Aproveitando o estudo feito sobre as álgebras semi-simples, fizemos a análise dos códigos cíclicos sobre os anéis $\mathbb{Z}_m$. Podemos dizer que generalizamos o conceito de códigos sobre o corpo $\mathbb{Z}_p$, que é o mais comum na literatura, para anéis $\mathbb{Z}_m$ quaisquer, com o auxílio das álgebras semi-simples.

Há vários caminhos possíveis que este trabalho pode tomar no futuro. Podemos usar a teoria que exploramos aqui para estudar os grupos de Brauer de um anel comutativo, tomando como referência o artigo [5], o primeiro a apresentar a definição de extensão galoisiana de anéis, inclusive, generalizar o grupo de Brauer de corpos para anéis foi uma motivação para estender a teoria de Galois sobre corpos para anéis; também é possível continuar fazendo o uso das álgebras separáveis e semi-simples para fazer generalizações de outras teorias ou desenvolver outros estudos sobre elas, explorar mais os códigos sobre os anéis $\mathbb{Z}_m$ ou partir para outros casos da teoria de Galois,

considerando anéis não comutativos ou até mesmo estudar a teoria de Galois sobre equações diferenciais, se baseando em [10], onde é provado que equações diferenciais do tipo $u'(t) = t - [u(t)]^2$ não possui soluções que podem ser escritas usando funções elementares ou primitivas de funções elementares, exponenciais de tais primitivas ou primitivas das exponenciais, ou seja, o método de solução não é de natureza algébrica. Esta teoria é análoga à parte da teoria de Galois onde é provado que uma equação polinomial geral de grau maior ou igual a cinco não pode ser resolvida por radicais.

Referências

[1] de ANDRADE, A.A. *Separabilidade, Ramificação e Difierente*. Dissertação (Mestrado) - IMECC - Unicamp, Campinas - SP, 1988.

[2] de ANDRADE, A. A. Códigos sobre $\mathbb{Z}_m$. *Notas de Seminário*. Departamento de Matemática, Ibilce-UNESP. São José do Rio Preto, 1995.

[3] de ANDRADE, A. A.; ANDRADE, M. G. C. A note on principal ideal rings. Rev. Mat. Estat., n. 18, p. 207-212, 2000.

[4] ATIYAH, M.F.; MACDONALD, L.G. Introduction to Commutative Algebra. Addison-Wesley Publishing Company, 1969.

[5] AUSLANDER, M.; GOLDMAN, O. The Brauer group of a commutative ring. Transactions of the American Mathematical Society.Waltham, Massachusetts. vol. 97, n. 3, p. 367-409, 1960.

[6] BLAKE, I. F. Codes over certain rings. Information and Control. Waterloo, Ontario, Canada. n. 20, p. 396-404, 1972.

[7] CURY, A.J. *Revolucione sua qualidade de vida*: navegando nas águas da emoção. Rio de Janeiro. Sextante, 2002.

[8] HATTORI, A. Semisimple álgebras over a commutative ring. J. Math. Soc. Japan. vol. 15, n. 4, p.404-419, 1963.

[9] HEFEZ, A.; VILLELA, M.L.T. Códigos Corretores de Erros. Série de Computação e Matemática. Rio de Janeiro: Impa, 2002.

[10] HUBBARD, J.H.; LUNDELL, B.E. A first look at Differential Algebra. The American Mathematical Monthly. vol, 118, n. 3, p. 245-261, 2011.

[11] MACWILLIAMS, F.J.; SLOANE, N.J.A. The Theory of Error Correcting Codes. [S.l.]: North-Holland Publishing Company, 1977.

[12] MARTINS, M.E. *Álgebra Comutativa.* Notas de Aula. url: https://www.ime.usp.br/~eugenia/algebra-comutativa/algebra_comutativa.pdf. Acesso em: 10 de janeiro de 2020. São Paulo, 2014.

[13] de MEYER, F.; INGRAHAM, E. Separable algebras over commutative rings. [S.l.]: Springer, 2006.

[14] MILES, F.C.P. Anéis e Módulos. São Paulo, IME - USP, 1972.

[15] do NASCIMENTO, R.F.D. *Semissimplicidade de anéis de grupos e o teorema de Perlis-Walker.* Monografia (Especialização) - Universidade Federal de Minas Gerais, Belo Horizonte - MG, 2017.

[16] PAQUES, A. *Teoria de galois sobre anillos conmutativos.* Universidad Los Andes, 1999.

[17] PETERSON, W.W.; WELDON, E.J. Jr., Error Correcting Codes. 2nd. ed. Cambridge, Mass.: MIT Press, 1972.

[18] RUIZ, J.R.M. *Teoria de Galois para Anéis Comutativos.* url: http://www.mtm.ufsc.br/~ebatista/2018-1/Artigo_Joao.pdf. Acesso em: 15 de janeiro de 2020. [S.l.], 2018.

[19] SANTANA, A.A. *Extensões de Galois de Anéis Comutativos de Característica p.* Dissertação (Mestrado) - UFRGS, Porto Alegre, RG, 1991.

[20] SPIEGEL, E. Codes over $\mathbb{Z}_m$. Information and Control. University of Connecticut, Storrs, Connecticut, vol. 35, p. 48-51, 1977.

[21] SPIEGEL, E. Codes over $\mathbb{Z}_m$, Revisted. Information and Control. University of Connecticut, Storrs, Connecticut, vol. 37, p. 100-104, 1978.

[22] TAKEUCHI, Y. On Galois extensions over commutative rings. Osaka J. Math. Osaka, Japan, vol. 2, n.1, p.137-145, 1965.