Mariana Macedo dos Santos

Uma Introdução ao Estudo dos Anéis de Grupo via Semissimplicidade

Volta Redonda, RJ

2021

Mariana Macedo dos Santos

Uma Introdução ao Estudo dos Anéis de Grupo via Semissimplicidade

Trabalho de Conclusão de Curso submetido ao Curso de Matemática com ênfase em Matemática Computacional da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Matemática.

Universidade Federal Fluminense

Instituto de Ciências Exatas

Curso de Matemática

Orientador: Rosemary Miguel Pires

Volta Redonda, RJ

2021

Ficha catalográfica automática - SDC/BAVR
Gerada com informações fornecidas pelo autor

S237i Santos, Mariana Macedo dos
Uma Introdução ao Estudo dos Anéis de Grupo via Semissimplicidade / Mariana Macedo dos Santos, < ; Rosemary Miguel Pires, orientadora. Volta Redonda, 2021.
80 f.

Trabalho de Conclusão de Curso (Graduação em Matemática)- Universidade Federal Fluminense, Instituto de Ciências Exatas, Volta Redonda, 2021.

1. Anéis de Grupo. 2. Semissimplicidade. 3. Teorema de Wedderburn-Artin. 4. Teorema de Maschke. 5. Produção intelectual. I. , <. II. Pires, Rosemary Miguel, orientadora. III. Universidade Federal Fluminense. Instituto de Ciências Exatas. IV. Título.

CDD -

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

Mariana Macedo dos Santos

Uma Introdução ao Estudo dos Anéis de Grupo via Semissimplicidade

Trabalho de Conclusão de Curso submetido ao Curso de Matemática com ênfase em Matemática Computacional da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Matemática.

Trabalho aprovado. Volta Redonda, RJ, 04 de maio de 2021:

Prof. Dra. Rosemary Miguel Pires – UFF
Orientadora

Carlos Henrique P. do Nascimento

Prof. Dr. Carlos Henrique Pereira do Nascimento – UFF

Rodrigo Lucas Rodrigues

Prof. Dr. Rodrigo Lucas Rodrigues – UFC

Volta Redonda, RJ
2021

Dedico este trabalho a todos que sempre estiveram ao meu lado
e que tornaram esse sonho possível.

Agradecimentos

Agradeço, em primeiro lugar, a Deus por todo direcionamento e sustento, em tempos de alegria e tristeza.

À minha mãe Denise por sempre ter me dado suporte e inspiração e aos meus irmãos Juliana e Junior por sempre me lembrarem das doçuras da vida mesmo em tempos difíceis. A eles todo meu amor e agradecimento.

À minha orientadora Rosemary, que me ajudou de diversas formas e inúmeras vezes, me orientando e auxiliando neste trabalho, na graduação e na vida. À professora Marina Ribeiro, que desde meu primeiro período me acolheu e me guiou, me ajudando a crescer como matemática e como pessoa também. Sou imensamente grata as duas por onde cheguei e por todo amor e carinho que recebi.

Aos meus amigos João Pedro, Guylherme, Joel, Tais, Rayan, Nelson e Patrick, que iniciaram comigo essa jornada, a qual finalizaremos juntos, sempre alegrando meus dias com brincadeiras e conselhos. Aos meus amigos Guilherme, Victor, Beatriz, Carolini, Mateus, João Victor, Elis e Otaviano pela companhia, conselhos e por sempre estarem ao meu lado nos estudos, sendo na biblioteca e salinha da UFF de manhã cedinho até altas horas, no discord fofocando e estudando, em casa fazendo receitas mirabolantes e depois resolvendo listas imensas, ou mesmo no bar, jantando litrão depois de um dia exaustivo na faculdade. E a todos aqueles que participaram da minha formação, meus sinceros agradecimentos.

Aos meus amigos Matheus, Beatriz, Diana, Tamires, Ana Julia, Jhulia e Felipe, por estarem comigo, alegrando meus dias e principalmente meus finais de semana com sua companhia, sempre me lembrando que os períodos de lazer e autocuidado são tão importantes quanto os de estudos.

Ao corpo docente da UFF por todo conhecimento acadêmico que me proporcionaram, em especial aos professores Carlos Henrique, Ivan Aguilar, Alessandro Gaio e Alan Prata, por, além de me auxiliarem na graduação, sempre me lembrarem que não estou sozinha nessa jornada. E a todos que trabalharam na UFF, em todos os setores, que tornaram o ambiente agradável e propício para estudo.

"Nós nunca descobriremos o que vem depois da escolha, se não tomarmos uma decisão. Por isso, entenda os seus medos, mas jamais deixe que eles sufoquem os seus sonhos."

(Alice no País das Maravilhas)

Resumo

A teoria de anéis de grupo traz uma comunicação entre a área de álgebra e álgebra linear, abordando novas estruturas algébricas e suas propriedades. A fim de introduzir e explorar essa área da matemática, foram apresentadas novas estruturas e suas propriedades, focando na ideia de semissimplicidade de módulos e anéis de grupo, além de analisar esse conceito em estruturas já conhecidas, como os anéis. Ademais, foi feita uma aplicação em conjunto com a teoria de grupos, na parte de representações e ações de grupo, com a ideia de apresentar uma aplicação do conceito de semissimplicidade nos anéis de grupo. O objetivo do trabalho é ser um material introdutório à teoria de módulos e anéis de grupo, além de estudar a caracterização dos anéis, através da noção de semissimplicidade, e dos grupos, a partir da teoria das representações.

Palavras-chave: Anéis de Grupo. Teorema de Wedderburn-Artin. Teorema de Maschke. Semissimplicidade.

Abstract

The group rings theory shows a connection between both areas of abstract and liner algebra, introducing new algebraic structures and their properties. In order to introduce and explore this area of mathematics, new structures and their properties were presented, focusing on the idea of semisimplicity of modules and group rings, in addition to analyzing this concept in already known structures, such as rings. Furthermore, an application was made in conjunction with group theory, in terms of representation and group actions theory, with the purpose of presenting an application of the concept of semisimplicity in group rings. The aim of this paper is to introduce group rings and modules theory, by studying the characterization of rings through the notion of semisimplicity, as well as the characterization of groups using the representation theory.

Keywords: Group Rings. Wedderburn-Artin Theorem. Maschke's Theorem. Semisimplicity.

Sumário

1 Introdução

Dado um grupo G e um anel com unidade R, construímos o *Anel de Grupo RG* como um R-módulo livre com base formada pelos elementos de G, cuja multiplicação é induzida pela multiplicação de G. A Teoria dos Anéis de Grupo, a qual teve seus primórdios por volta de 1890 ([1]), ganhando espaço como uma área de estudo própria apenas recentemente. Começando com o desenvolvimento da teoria de representação de grupos finitos sobre os complexos, que teve seu alicerce firmado por T. Molien, que desenvolveu a teoria de álgebras sobre o corpo dos complexos (a qual foi mais tarde generalizada por Wedderburn). Molien aplicou sua teoria em conjunto com a ideia de Cayley de representação de grupos finitos como grupos de permutação sobre eles mesmos, os quais podem ser "linearizados" para obter uma representação fiel de um grupo G em $GL(n, \mathbb{C})$, o grupo de matrizes invertíveis n×n com coeficientes em $\mathbb{C}$. Dessa forma, o conceito de anel de grupo veio a adquirir grande importância por causa de suas aplicações na teoria de representações de grupos, a partir dos trabalhos de E. Noether, R. Brauer e I. Schur ([2]).

Sabemos da Álgebra Linear que todo subespaço de um espaço vetorial é um somando direto. Isto não é verdadeiro no caso mais geral de módulos sobre um anel arbitrário. Por exemplo, o anel do inteiros $\mathbb{Z}$ não é um somando direto de $\mathbb{Q}$, o corpo dos números racionais, como um $\mathbb{Z}$-módulo. Focaremos parte do trabalho no estudo de módulos que tem particularmente esta propriedade. Dizemos que um R-módulo M é *semissimples* se todo submódulo de M é um somando direto. Assim como os teoremas de decomposição possuem um lugar muito importante na teoria de Álgebra Linear, pois facilitam o estudo de estruturas mais abstratas e suas propriedades, estes teoremas possuem extrema importância na teoria de módulos e anéis de grupo, pois os mesmos transformam problemas de análise em uma estrutura não muito conhecida, bem como suas propriedades, na análise do mesmo problema em estruturas mais conhecidas e exploradas, tais quais o conjunto das matrizes.

Neste trabalho, propomos que seja feito um estudo da estrutura dos anéis e módulos semissimples, trazendo uma caracterização dessas estruturas baseada em suas decomposições em somas diretas de matrizes através do Teorema de Wedderburn-Artin. Depois, estenderemos o conceito de semissimplicidade para os anéis e álgebras de grupo, a partir do Teorema de Maschke, a fim, também, de obter uma descrição a partir de somas diretas. Ademais a isso, apresentaremos o conceito de representação de grupos, com definições e exemplos, além de corresponder esse conceito com a teoria de módulos. Por fim, finalizaremos com uma aplicação bastante útil e interessante do Teorema de Maschke ao estudo da semissimplicidade em conjunto com a teoria de representação de grupos.

2 Conceitos Básicos

Os resultados apresentados neste capítulo, bem como suas respectivas demonstrações, podem ser encontrados nas referências: [2], [3], [4], [5], [6].

2.1 Grupos

Definição 2.1. Um conjunto não vazio G com uma operação

$$\begin{aligned} G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

é um grupo se as condições seguintes são satisfeitas:

i. Associativa:
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad \forall a, b, c \in G.$$

ii. Existência do neutro:
$$\exists e \in G \quad \text{tal que } e \cdot a = a \cdot e = a, \quad \forall a \in G.$$

iii. Existência do elemento inverso:
$$\forall a \in G, \quad \exists b \in G \quad \text{tal que } a \cdot b = b \cdot a = e.$$

Além disso, o grupo é abeliano ou comutativo se vale a seguinte condição:

iv. Comutativa:
$$a \cdot b = b \cdot a, \quad \forall a, b \in G.$$

Observação 2.2. *i. O elemento neutro é único, pois se $e, e' \in G$ são elementos neutros de G então:*
$$e = e \cdot e' = e'.$$

ii. O elemento inverso é único, já que sendo $a \in G$ e $b, b' \in G$ elementos inversos de a, assim:
$$b = b \cdot e = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = e \cdot b' = b'.$$

Exemplo 2.3. *O conjunto $\mathbb{Z}$ de inteiros racionais; o conjunto $\mathbb{Q}$ de números racionais, o conjunto $\mathbb{R}$ de números reais e o conjunto $\mathbb{C}$ de números complexos, com a operação adição, são exemplos de grupos, os quais também são comutativos. Além disso, se denotarmos por $\mathbb{Q}^*, \mathbb{R}^*$ e $\mathbb{C}^*$ os conjuntos obtidos dos anteriores excluindo o elemento 0, então esses conjuntos, com a*

operação multiplicação, também são grupos abelianos. O conjunto $\mathbb{Z}^*$ *de inteiros sem* 0 *não é um grupo sob multiplicação já que nenhum inteiro, exceto 1 e -1, tem um inverso multiplicativo.*

O conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ *de inteiros módulo* m*, com adição definida por* $\overline{a+b} = \bar{a} + \bar{b}$ *é um grupo abeliano.*

Também, definindo a multiplicação por $\overline{a \cdot b} = \bar{a} \cdot \bar{b}$ *segue que* $\mathbb{Z}_m^*$ *(que é o conjunto* $\mathbb{Z}_m$ *se o elemento* $\overline{0}$*) é um grupo sob multiplicação se e somente se o módulo* m *é um número primo.*

Exemplo 2.4. *Seja* S *um conjunto não vazio e seja*

$$G = \{f : S \to S : f \text{ bijetiva } \}$$

Se $\circ$ *é a operação composição de funções, isto é,*

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, f) &\longmapsto g \circ f \end{aligned}$$

então $(G, \circ)$ *é um grupo tendo*

como identidade.

$$\begin{aligned} I_S : S &\to S \\ x &\longmapsto x \end{aligned}$$

Esse grupo é chamado de grupo das permutações do conjunto S*. Se* $S = \{1, 2, \ldots, n\}$ *denotaremos esse grupo por* S_n*, e temos que o número de elementos de* S_n *é exatamente* $n!$*.*

Por exemplo, o grupo S_3 *é composto dos seguintes 6 elementos:*

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad ; \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_1^{-1}$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2^{-1}; \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_3^{-1}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5^{-1}; \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_4^{-1}$$

Observação 2.5. *Mostraremos agora que os grupos* S_n*,* $n \geq 3$*, são exemplos de grupos não abelianos. De fato, sejam* $f, g \in S_n$ *definidas como segue:*

$$f : \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\}$$

$$f(1) = 2, \quad f(2) = 1, \quad f(x) = x \quad \forall x, \quad 3 \leq x \leq n$$

$$g : \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\}$$

$$g(1) = 2, \quad g(2) = 3, \quad g(3) = 1 \text{ e se } n \geq 4 \quad g(x) = x \quad \forall x, \quad 4 \leq x \leq n$$

Ora, como

$$(g \circ f)(1) = g(f(1)) = g(2) = 3$$
$$(f \circ g)(1) = f(g(1)) = f(2) = 1$$

teremos $g \circ f \neq f \circ g$.

Exemplo 2.6. *Seja K um corpo. Então, o conjunto $GL(n, K)$ de todas $n \times n$ matrizes invertíveis com entradas em K, com a multiplicação de matrizes, é um grupo, que não é comutativo se $n > 1$.*

Exemplo 2.7. *Seja G o conjunto de retas no plano $\mathbb{R}^2$ com coeficiente angular não nulo, isto é*

$$G = \{f : \mathbb{R} \to \mathbb{R} : f(x) = ax + b, 0 \neq a, b \in \mathbb{R}\}$$

Se $f(x) = ax + b, a \neq 0$ e $g(x) = cx + d, c \neq 0$ então:

$$(g \circ f)(x) = g(f(x)) = acx + (bc + d), ac \neq 0$$

ou seja a composição de funções o define uma operação em G que é associativa.

Agora, se $e = I_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ é um elemento de G e se $f^{-1}(x) = x \mapsto x = \frac{1}{a}x - \frac{b}{a}, a \neq 0$, temos:

$$f^{-1} \circ f = f \circ f^{-1} = I_{\mathbb{R}} \text{ onde } f(x) = ax + b, a \neq 0.$$

Assim, $(G, \circ)$ é um grupo onde $\circ$ é a operação composição de funções.

$$\text{Se } f(x) = 2x + 4 \text{ e } g(x) = 3x + 2 \text{ temos,}$$
$$(g \circ f)(x) = g(f(x)) = g(2x + 4) = 6x + 14$$
$$(f \circ g)(x) = f(3x + 2) = 6x + 8$$

Portanto $(G, \circ)$ é um grupo não abeliano contendo um número infinito de elementos.

Exemplo 2.8. *Seja a um elemento de um grupo G. Definimos as potências de a como:*

$$a^n = \begin{cases} \underbrace{a \cdot a \cdots a}_{n \text{ vezes}} & \text{se } n > 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{|n| \text{ vezes}} & \text{se } n < 0 \\ e & \text{se } n = 0. \end{cases}$$

Já que $a^m \cdot a^n = a^{m+n}$, segue imediatamente que o conjunto

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

é um subgrupo de G, que é chamado de subgrupo cíclico de G gerado por a.

Definição 2.9. Se o grupo definido acima é finito, então existem inteiros distintos n, m tais que $a^n = a^m$. Sendo assim $a^{n-m} = a^{-(m-n)} = e$. O maior inteiro positivo n tal que $a^n = e$ é chamado de **ordem** de a e é denotado por $o(a)$. Se $\langle a \rangle$ é infinito, então dizemos que a é um elemento de ordem infinita.

Observação 2.10. *Se existe um elemento a em G tal que $G = \langle a \rangle$, então dizemos que G é um grupo cíclico e que a é seu gerador. Note que $o(a) = |\langle a \rangle|$.*

Definição 2.11. Seja $(G, \cdot)$ um grupo. Um subconjunto não vazio H de G é um subgrupo de G (denotamos $H \leq G$) quando, com a operação de G, o conjunto H é um grupo, isto é, quando as condições seguintes são satisfeitas:

i. $h_1 \cdot h_2 \in H, \quad \forall h_1, h_2 \in H.$

ii. $h_1 \cdot (h_2 \cdot h_3) = (h_1 \cdot h_2) \cdot h_3, \quad \forall h_1, h_2, h_3 \in H.$

iii. $\exists\ e_H \in H$ tal que $e_H \cdot h = h \cdot e_H = h, \forall h \in H.$

iv. Para cada $h \in H$, existe $k \in H$ tal que $h \cdot k = k \cdot h = e_H$.

Exemplo 2.12. *Se G é grupo, então $\{e\}$ e G são subgrupos (triviais) de G.*

Exemplo 2.13. *$(2\mathbb{Z}, +)$ é subgrupo de $(\mathbb{Z}, +)$. De maneira geral, se $n \in \mathbb{N}$, então $(n\mathbb{Z}, +)$ é subgrupo de $(\mathbb{Z}, +)$.*

Definição 2.14. Seja G um grupo e seja H um subgrupo de G. Definimos sobre G, a relação de equivalência $\sim$ da maneira seguinte:

$$y \sim x \Leftrightarrow \exists h \in H \text{ tal que } y = xh.$$

Definimos o conjunto $xH = \{y \in G \mid y \sim x\} = \{xh \mid h \in H\}$ por classe lateral de x à esquerda. Em particular, H é a classe lateral do elemento neutro e à esquerda. Observe que $y \in xH \Leftrightarrow yH = xH$. Analogamente, poderíamos definir a relação de equivalência seguinte:

$$y \sim x \Leftrightarrow \exists h \in H \text{ tal que } y = hx.$$

Obteríamos então as classes laterais à direita de H em G; a classe lateral de x à direita seria $Hx = \{hx \mid h \in H\}$.

Definição 2.15. Dado um grupo G, o **centro de** G é o conjunto dos elementos que comutam com todos elementos de G, ou seja:

$$Z(G) = \{z \in G \mid gz = zg,\ \forall g \in G\}.$$

Observação 2.16. *É fácil verificar que $Z(G)$ é subgrupo de G.*

Definição 2.17. A cardinalidade do conjunto das classes laterais à esquerda é o índice de H em G; ele será denotado por $(G : H)$.

Observação 2.18. *O índice de H em G também é a cardinalidade do conjunto das classes laterais à direita de H em G, pois a aplicação φ abaixo é uma bijeção bem definida:*

$$\varphi : \{ \text{ classes laterais à esquerda } \} \longrightarrow \{ \text{ classes laterais à direita } \}$$

$$xH \longmapsto Hx^{-1}.$$

Teorema 2.19 (Lagrange)**.** *Se G é grupo finito e H é tal que $H \leq G$, então $|G| = |H|(G : H)$.*

Definição 2.20. Seja G um grupo e $H \leq G$. Se $g \in G$, definimos a função ψ_g da seguinte forma:

$$\begin{aligned} \psi_g : G &\to G \\ x &\mapsto \psi_g(x) = x^g = g^{-1}xg \end{aligned}$$

Notemos que $\psi_g(H) = \{\psi_g(h) : h \in H\} = \{h^g = g^{-1}hg : h \in H\}$ o qual denotaremos por H^g ou $g^{-1}Hg$. Observe que H^g é também um subgrupo de G pois:

i. $e = e^g \in H^g$

ii. $h_1^g, h_2^g \in H^a \Rightarrow h_1^g \cdot h_2^g = (h_1h_2)^a \in H^y$

iii. $h^g \in H^g \Rightarrow (h^g)^{-1} = (h^{-1})^g \in H^g$.

Dessa forma, dizemos que $H \leq G$ é **normal** em G, e denotaremos por $H \triangleleft G$, se $\psi_g(H) = H^g \subset H, \ \forall \ g \in G$.

Observação 2.21. $H^g \subset H, \ \forall \ g \in G \Rightarrow H^g = H \ \forall, \ g \in G$.

Exemplo 2.22. *Se G é o grupo das retas no $\mathbb{R}^2$ com coeficientes angulares não nulos e H é o subgrupo de G das retas de $\mathbb{R}^2$ com coeficientes angulares iguais a 1, então $H \triangleleft G$. De fato:*

$$g(x) = ax + b, \ a \neq 0 \ e \ h(x) = x + c \ então \ (g^{-1} \cdot h \cdot g)(x) = x + \frac{c}{a}.$$

Definição 2.23. Sejam $(G, *)$ e $(H, \circ)$ grupos. A aplicação $f : G \to H$ é chamada **homomorfismo de grupos** se $\forall x, y \in G$, temos:

$$f(x * y) = f(x) \circ f(y).$$

Definição 2.24. Seja $f : G \to H$ um homomorfismo de grupos. Então a **imagem** de f é o conjunto

$$Im(f) = \{y \in H \mid f(x) = y, \ x \in G\}.$$

O **núcleo** de f é o conjunto

$$Ker(f) = \{x \in G \mid f(x) = e\}.$$

Teorema 2.25. *Seja $f : G \to H$ homomorfismo de grupos. Então*

$$G/Ker(f) \simeq Im(f).$$

Definição 2.26. Seja G grupo, definimos a **classe de conjugação** de um elemento x por $C(x) = \{x^g \mid g \in G\}$.

Teorema 2.27 (Equação de Classes)**.** *Dado um grupo G:*

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} (G : C(x_i)).$$

2.2 Ações de Grupos

Definição 2.28. Sejam G um grupo e X um conjunto. Dizemos que G age em X se existir uma aplicação

$$\begin{aligned} \alpha : G \times X &\to X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

satisfazendo as seguintes condições:

i. $e \cdot x = x, \forall x \in X$;

ii. $g \cdot (h \cdot x) = gh \cdot x, \forall g, h \in G, x \in X$.

Observação 2.29. *Note que na definição acima, escrevemos $g \cdot x$ para indicar a imagem do par ordenado $(g, x) \in G \times X$ pela ação α, para simplificar a notação.*

Exemplo 2.30. *Seja G um grupo e X um conjunto. Então a ação trivial de G em X é definida por $g \cdot x = x, \forall x \in X$.*

Exemplo 2.31. *Sejam K um corpo e V um espaço vetorial. Então definimos o grupo multiplicativo $K^* := K \backslash \{0\}$. Dessa forma, K^* age no conjunto V de maneira natural, a saber:*

$$\alpha(g, v) = gv, \ g \in K^* \ e \ v \in V.$$

Exemplo 2.32. *Seja X um conjunto. Então o grupo $(\mathscr{B}ij(X), \circ)$, das permutações de elementos de X, age em X de maneira natural, via $\sigma \cdot x = \sigma(x)$, para* todos *$\sigma \in \mathscr{B}ij(X)$ e $x \in X$.*

Exemplo 2.33. *Todo grupo G age em si mesmo via multiplicação, isto é, a aplicação $\alpha : G \times G \to G$, dada por $\alpha(g, h) = g \cdot h = gh$ define uma ação de G em G, chamada de ação regular.*

2.3 Anéis

Definição 2.34. Dado R um conjunto não vazio com duas operações binárias:

$$+: \begin{array}{l} R \times R \longrightarrow R \\ (a,b) \longmapsto a+b \end{array} \quad \text{e} \quad \cdot: \begin{array}{l} R \times R \longrightarrow R \\ (a,b) \longmapsto a \cdot b \end{array}$$

tais que, $\forall a, b, c \in R$ valem as seguintes propriedades:

i. $(a+b)+c = a+(b+c)$.

ii. $\exists\ 0 \in G$, tal que $a+0 = 0+a = a$.

iii. $\exists\ -a \in G$, tal que $a+(-a) = (-a)+a = 0$.

iv. $a+b = b+a$.

v. $a \cdot (b+c) = a \cdot b + a \cdot c$.

vi. $(a+b) \cdot c = a \cdot c + a \cdot c$.

O conjunto $(R, +, \cdot)$ acima definido é denominado **anel**.

Observação 2.35. *i. Se $a \cdot b = b \cdot a$, dizemos que o anel é comutativo*

ii. Se o anel R contém um elemento $1 \neq 0$, tal que $1 \cdot a = a \cdot 1 = a, \forall\ a \in R$, dizemos que R é anel com unidade.

Observação 2.36. *Ao longo deste trabalho, consideraremos que todo anel abordado possui unidade.*

Exemplo 2.37. *Sendo $R = \mathscr{F}(\mathbb{R})$ o conjunto de todas as funções $f : \mathbb{R} \to R$, definimos duas operações no conjunto R, a saber:*

$$+: \begin{array}{l} R \times R \longrightarrow R, \text{ onde } (f+g)(x) = f(x) + g(x)\ \forall x \in \mathbb{R} \\ (f,g) \longmapsto f+g \end{array}$$

$$\cdot: \begin{array}{l} R \times R \longrightarrow R, \text{ onde } (f \cdot g)(x) = f(x) \cdot g(x)\ \forall x \in \mathbb{R} \\ (f,g) \longmapsto f \cdot g \end{array}$$

Note que a função constante igual a zero é o elemento neutro em relação à adição de R, e a função constante igual a 1 é o elemento neutro em relação à multiplicação.

As demais propriedades que definem um anel comutativo são facilmente verificadas. Porém se $f : \mathbb{R} \to \mathbb{R}$ é definida por:

$$f(x) = \begin{cases} 0, & x < 0 \\ x, & x \geq 0 \end{cases}$$

e se $g : \mathbb{R} \to \mathbb{R}$ *é dada por:*

$$g(x) = \begin{cases} x^2, & x < 0 \\ 0, & x \geq 0. \end{cases}$$

teremos $f \neq 0$, $g \neq 0$ *e* $f \cdot g = 0$, *logo* $\mathscr{F}(\mathbb{R})$ *possui divisores de zero, ou seja, elementos diferentes de 0 que quando multiplicados levam em 0.*

Definição 2.38. Sendo $(R, +, \cdot)$ anel e $\emptyset \neq A \subset R$. Se A for for fechado para as operações $+$ e $\cdot$ de R, ou seja:

i. $x, y \in A \Rightarrow x + y \in A$

ii. $x, y \in A \Rightarrow x \cdot y \in A$

e assim, se com as operações de R, A é anel, dizemos que A é **subanel** de R e denotamos por $A \leq R$.

Definição 2.39. Sendo R anel e $I \leq R$. Dizemos que I é **ideal à esquerda** de R, se:

i. $a \cdot x \in I, \ \forall a \in R, \ \forall x \in I \quad (R \cdot I \subset I)$.

Analogamente, definimos $J \leq R$ um **ideal à direita** se:

ii. $x \cdot a \in J, \ \forall a \in R, \ \forall x \in I \quad (R \cdot J \subset J)$.

Dessa forma, se I é simultaneamente ideal à esquerda e à direita, dizemos que I é **ideal bilateral** de R, isto é:

iii. $A \cdot I \subset I$ e $I \cdot A \subset I$.

Exemplo 2.40. *Seja* $n \geq 0$ *um inteiro. Claramente, o subconjunto* $n\mathbb{Z} := \{zn \mid z \in \mathbb{Z}\}$ *é um ideal do anel dos inteiros.*

Mais geralmente, seja $(R, +, \cdot)$ *um anel e sejam* $\alpha_1, \ldots, \alpha_t$ *elementos do anel* R. *Então, claramente, o subconjunto* $R\alpha_1 + \cdots + R\alpha_t := \{a_1\alpha_1 + \cdots + a_t\alpha_t \mid a_1, \ldots, a_t \in R\}$ *é um ideal de* $(R, +, \cdot)$ *que será denotado por* $(\alpha_1, \ldots, \alpha_t)$.

Exemplo 2.41. *Sejam* $(R, +, \cdot)$ *um anel e* I *um ideal de* R. *Sobre* R, *definimos a relação de congruência* $(\mathrm{mod} I)$: *para* $a, b \in R$.

$$a \equiv b \ (\mathrm{mod} \ I) \quad \Leftrightarrow \quad a - b \in I.$$

É imediato verificar que esta relação é uma relação de equivalência. Se $a \in R$, então por definição, sua classe de equivalência módulo I é o subconjunto

$$\{b \in R \mid b \equiv a \pmod{I}\} = \{a + c \mid c \in I\},$$

o qual será denotado por $\bar{a}$ ou $a + I$. Além disso, denotaremos por R/I o conjunto das classes de equivalência módulo I. Sobre este conjunto, definimos duas operações $\oplus$ e $\odot$ da maneira seguinte:

$$\bar{x} \oplus \bar{y} := \overline{x + y} \quad e \quad \bar{x} \odot \bar{y} := \overline{x \cdot y} \quad para \quad \bar{x}, \bar{y} \in R/I,$$

de forma que tais operações estão bem definidas e que $(R/I, \oplus, \odot)$ é um anel, chamado de anel quociente de R módulo I.

Proposição 2.42. *Seja D um anel de divisão e seja n um inteiro positivo. Então, o anel $M_n(D)$ das matrizes $n \times n$ sobre D, não contém ideais bilaterais próprios.*

Demonstração. Ver ([2], p. 70). □

Definição 2.43. Sejam R, S anéis. A aplicação $f : R \to S$ é chamada **homomorfismo de anéis** se $\forall a, b \in R$, temos:

i. $f(a + b) = f(a) + f(b)$.

ii. $f(ab) = f(a)f(b)$.

Definição 2.44. Seja $f : R \to A$ um homomorfismo de anéis. Então a **imagem** de f é o subanel

$$Im(f) = \{y \in A \mid f(x) = y,\ x \in R\}.$$

O **núcleo** de f é o ideal

$$Ker(f) = \{x \in R \mid f(x) = 0\}.$$

Definição 2.45. Um anel R é chamado **simples** se os seus únicos ideais bilaterais são (0) e R.

2.4 Módulos e Álgebras

Nesta sessão introduziremos conceitos básicos de módulos, os quais aparecem implicitamente no trabalho de Dedekind sobre teoria dos números [2]. Apresentaremos algumas de suas propriedades e resultados, a fim de criar preliminares para o conceito de um anel de grupo.

Definição 2.46. Considere um anel R. Um grupo abeliano aditivo M é chamado **R-módulo** (à esquerda) sobre R se, para cada elemento $a \in R$ e $m \in M$, temos $am \in M$ tais que:

i. $(a+b)m = am + bm$;

ii. $a(m_1 + m_2) = am_1 + am_2$;

iii. $a(bm) = (ab)m$;

iv. $1m = m$.

$\forall\ a, b \in R$ e $m, m_1, m_2 \in M$.

De forma análoga, podemos definir módulo à direita considerando a multiplicação por elementos de R sendo feita pela direita. Note que podemos também definir módulo a partir da seguinte função:

$$\begin{array}{rccc} \cdot\ : & R \times M & \to & M, \\ & (r, m) & \mapsto & r \cdot m \end{array}$$

e que cumpre as quatro propriedades citadas na definição.

Segue da definição, que se K é um corpo, então o conceito de K-módulo coincide com a noção de espaço vetorial sobre K. Dessa forma podemos dizer, a grosso modo, que um módulo é um "espaço vetorial" sobre um anel. Essa visão nos permite justificar os estudos sobre módulos a partir de alguns resultados análogos da teoria de espaços vetoriais.

Exemplo 2.47. *Seja I um ideal à esquerda de um anel R e seja R/I o grupo quociente com operação aditiva. Então R/I possui estrutura de R-módulo com o produto*

$$r(a + I) = ra + I,\ \forall\ r, a \in R.$$

Exemplo 2.48. *Consideremos S o anel de matrizes $n \times n$ com entradas num anel R. Seja N o conjunto de todas as matrizes $n \times 1$ com entradas em R. Então N é um grupo abeliano aditivo com a soma de matrizes. Assim, N torna-se um S-módulo à esquerda via multiplicação usual de matrizes. De modo análogo se mostra que o conjunto L das matrizes $1 \times n$, com entradas em R, é um S-módulo à direita.*

Exemplo 2.49. *(a) Todo espaço vetorial sobre um corpo K é um K-módulo.*
(b) Todo anel pode ser considerado como um módulo sobre si mesmo.
(c) Todo grupo abeliano G pode ser considerado como um módulo sobre o anel $\mathbb{Z}$ dos números inteiros, definindo o produto de um inteiro n por um elemento $g \in G$ do seguinte modo:

$$ng = \begin{cases} g + \cdots + g\ (n\ vezes), & se\ \ n > 0 \\ (-g) + \cdots + (-g)\ (|n| vezes), & se\ \ n < 0 \\ 0, & se\ \ n = 0 \end{cases}.$$

Exemplo 2.50. *Seja L um ideal à esquerda de um anel R. Como o produto de elementos de R por elementos de L permanecem em L, segue que L pode ser considerado com um R-módulo à esquerda. Analogamente, um ideal à direita pode ser considerado um R-módulo à direita, em particular, um anel R é sempre um módulo sobre si mesmo.*

Definição 2.51. Seja R um anel comutativo. Um R-módulo A é dito **R-Álgebra** se existe uma multiplicação, definida em A, tal que, com a adição dada em A e esta multiplicação, A é um anel tal que a seguinte condição segue:

$$r(ab) = (ra)b = a(rb),$$

$\forall r \in R$ e $a, b \in A$.

Definição 2.52. Seja M um módulo sobre um anel R. Um subconjunto não nulo $N \subset M$ é dito R-submódulo de M se as seguintes condições são satisfeitas:

i. $0 \in N$.

ii. $\forall x, y \in N$, temos que $x + y \in N$.

iii. $\forall r \in R \in \forall n \in N$, temos que $rn \in N$.

Observação 2.53. *Segue da definição acima que se V é um espaço vetorial sobre um corpo K, então os K-submódulos de V são exatamente os seus subespaços vetoriais. Similarmente os A-submódulos de um grupo abeliano A são os seus subgrupos.*

Exemplo 2.54. *Seja V um espaço vetorial sobre um corpo K e seja $T : V \to V$ uma aplicação linear. Considere V um $K[X]$-módulo com a estrutura de módulo definida por*

$$f(X)v = f(T)(v),$$

para $v \in V$ e $f(X) \in K|X|$. Então os $K[X]$-submódulos de V são os subespaços de V que são invariantes por T, isto é, os subespaços S tais que $T(S) \subset S$. Pela observação acima, basta notar que se S é um $K[X]$-submódulo de V e $s \in S$, então para $f(x) = x \in K[x]$ temos que $f(x)s \in S$, mas

$$f(x)s = f(T)(s) = T(s),$$

o que mostra que $T(s) \in S$, logo $T(S) \subset S$. Portanto, os $K[X]$-submódulos são invariantes por T.

Agora, dados um subespaço S de V invariante por T, $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ e $s \in S$, temos que

$$f(T)(s) = a_0 + a_1T(s) + \cdots + a_nT^n(s) \in S$$

pois como S é subespaço invariante por T temos que $T^n(s) \in S, \forall n \geq 1$ ou seja, combinações lineares de vetores em S continuam em S. A condição (i) segue do fato de S ser subespaço vetorial.

Portanto, S é um $K[X]$ -submódulo de V. Cada módulo $M \neq (0)$ contém pelo menos dois submódulos; a saber, M e (0), chamados submódulos triviais. Todo módulo $M \neq (0)$ contém (0) como submódulo próprio.

Definição 2.55. Um módulo M é simples se possui apenas submódulos triviais.

Exemplo 2.56. *Sejam K um corpo e $i \in \{1, \ldots, n\}$. O ideal à esquerda*

$$L_i = \left\{ \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix}, a_{ji} \in K, \forall j = 1, \ldots, n \right\}$$

é um $M_n(K)$-módulo simples com a operação usual.

Exemplo 2.57. *Os submódulos de um espaço vetorial são exatamente seus subespaços vetoriais.*

2.5 Módulos Livres e Soma Direta

Nessa seção, abordaremos a noção de base em um espaço vetorial para o caso de um módulo sobre um dado anel.

Sendo S um subconjunto de um R-módulo M, denotaremos por RS o conjunto de todas as somas finitas da forma

$$\sum_{i=1}^{n} x_i s_i,$$

em que n é qualquer inteiro positivo e $x_i \in R, s_i \in S$ para $1 \leq i \leq n$, ou seja, o conjunto de todas as combinações lineares dos elementos de S.

Definição 2.58. Um conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é chamado de **conjunto de geradores** de M se $M = RS$, ou seja, se todo elemento de M puder se escrito como uma combinação linear (finita) de elementos de S com coeficientes em R.

Definição 2.59. Um conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é chamado de **linearmente independente** se, para toda combinação linear (finita) de elementos de S com coeficientes em R :

$$r_{i_1} s_{i_1} + r_{i_2} s_{i_2} + \cdots + r_{i_t} s_{i_t} = 0$$

implica que $r_{i_1} = r_{i_2} = \cdots = r_{i_t} = 0$.

Definição 2.60. O conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é dito **base** de M sobre R, se ele for um conjunto de geradores linearmente independentes.

Proposição 2.61. *Um conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é base se, e somente se, todo elemento $m \in M$ puder ser expresso unicamente como uma combinação linear finita na forma:*

$$m = r_{i_1} s_{i_1} + r_{i_2} s_{i_2} + \cdots + r_{i_t} s_{i_t},$$

com $r_{i_j} \in R, s_{i_j} \in S_{i_j}, 1 \leq j \leq t$.

Observação 2.62. *Nem todo R-módulo M tem uma base. Considere, por exemplo, o conjunto $\mathbb{Z}_6$ como um $\mathbb{Z}$-módulo. Para todo elemento $\bar{a} \in \mathbb{Z}_6$ temos $6\bar{a} = \overline{0}$ e $6 \neq 0 \in \mathbb{Z}$. Isso mostra que não existe subconjunto de $\mathbb{Z}_6$ que é linearmente independente sobre $\mathbb{Z}$, então esse módulo não pode ter uma base.*

Definição 2.63. Um R-módulo M é dito **livre** se ele tem uma base.

Definição 2.64. Uma família $\{M_i\}_{i\in I}$ de submódulos de um R-módulo M é chamada de independente se, para todo índice $i \in I$, temos que

$$M_i \cap \left(\sum_{j \neq i} M_j \right) = (0)$$

Definição 2.65. Sendo $\{M_i\}_{i\in I}$ uma família de submódulos de um R-módulo M. Dizemos que M é a **soma direta** (interna) dos submódulos dessa família, e dizemos que $M = \oplus_{i\in I} M_i$ se a família é independente e gera M; ou seja, se as seguintes condições forem verdadeiras:

i. $\forall\ i \in I$, temos que $M_i \cap \left(\sum_{j\neq i} M_j \right) = 0$.

ii. $M = \sum_{i\in I} M_i$.

As duas condições da definição são equivalentes a:

iii. Se todo elemento $m \in M$ puder ser escrito unicamente como $m = m_{i_1} + m_{i_2} + \cdots + m_{i_t}$ com $m_{i_j} \in M_{i_j}, 1 \leq j \leq t$.

Particularmente, se $\{m_i\}_{i\in I}$ é uma base de M, então M é a soma direta $M = \oplus_{i\in I} Rm_i$.

Definição 2.66. Um submódulo N de um R-módulo M é chamado de um **somando direto** se existir outro módulo N' tal que $M = N \oplus N'$.

Observação 2.67. *Diferente dos espaços vetoriais, nem todos os submódulos de um dado módulo são somandos diretos. A seguinte caracterização de somando direto é bem útil.*

Lema 2.68. *Seja N um submódulo de um R-módulo M. Então N é um somando direto de M se, e somente se, existir um endomorfismo $f : M \to M$ tal que $f \circ f = f$ e $Im(f) = N$.*

Observação 2.69. *O homomorfismo $f : M \to M$ do lema acima é chamado de projeção de M em N. Note também que se N é um R subálgebra de M, então f é um homomorfismo de R-álgebras.*

Proposição 2.70. *Sendo R um anel. Todo R-módulo M é uma imagem epimórfica de um R-módulo livre.*

3 Teoremas de Decomposição de Anéis

Neste capítulo, introduziremos o conceito de *Semissimplicidade* e enunciaremos e demonstraremos alguns teoremas de decomposição. Para isto, foram-se utilizadas as referências: [2], [7], [8], [9].

3.1 Semissimplicidade de Anéis

Definição 3.1. Sejam R anel e M um R-módulo à esquerda. Dizemos que M é um módulo:

i. **Simples**, se $M \neq (0)$ e seus únicos submódulos são os triviais, ou seja, (0) e M.

ii. **Semissimples**, se todo R-submódulo de M é somando direto.

Exemplo 3.2. *Todo ideal minimal de um anel R é módulo simples.*

Exemplo 3.3. *Todo módulo simples é semissimples. A volta não vale, pois temos que o módulo nulo é semissimples, mas não é simples.*

Exemplo 3.4. *Se K é um corpo ou um anel de divisão, então todo K-espaço vetorial é um módulo semissimples. De fato, pois se W é um subespaço de V, então, tomando uma base de W e completando a uma base de V, podemos verificar facilmente que W é um somando direto de V.*

Lema 3.5. ***(Lema de Zorn)*** *Seja $(\mathscr{F}, \preceq)$ uma família não vazia e parcialmente ordenada. Se toda cadeia em $\mathscr{F}$ possui uma cota superior (respectivamente, cota inferior) em $\mathscr{F}$, então $\mathscr{F}$ possui elemento maximal (respectivamente, elemento minimal).*

Lema 3.6. *Seja $N \neq (0)$ um submódulo de um módulo semissimples M. Então:*

i. N é semissimples.

ii. N contém um submódulo simples.

Demonstração.

(i) N é semissimples

Seja $L \leq N$, assim $L \leq M$ também, ou seja, existe K submódulo tal que $M = L \oplus K$. Dessa forma:

$$N = M \cap N = (L \oplus K) \cap N = (L \cap N) + (K \cap N) = L + (K \cap N) = L \oplus (K \cap N)$$

Como L é arbitrário, segue que todo submódulo de N é somando direto, ou seja, N é semissimples.

(ii) N contém um submódulo simples

Como $N \leq M$ é semissimples ($N \neq 0$), seja $x \in N$, $x \neq 0$. Já que $Rx \leq N$, basta mostrar que Rx contém um submódulo simples.

Para isso, considere a família F de todos os submódulos de Rx que não contém x. $F \neq 0$, pois $0 \in F$. Note que F é parcialmente ordenada e possui cota superior, dessa forma, pelo lema de Zorn, existe elemento maximal em F, digamos N_1. Mas do que provamos em (i), segue que $Rx = N_1 \oplus N_2$.

Mostraremos que N_2 é simples.

Inicialmente, note que $N_2 \neq (0)$, pois $x = n_1 + n_2$, $n_1 \in N_1$ e $n_2 \in N_2$, e já que $m \notin N_1$, $n_2 \neq 0$.

Além disso, se $(0) \neq N_3 \leq N_2$, então devemos ter $N_2 = N_3 \oplus W$ para algum submódulo W de N_2.

Agora, pela maximalidade de N_1, devemos ter $x \in N_1 \oplus N_3$ de forma que $N_1 \oplus N_3 = Rx$.

Mas daí $N_1 \oplus N_3 = Rx = N_1 \oplus N_2 = N_1 \oplus (N_3 \oplus W)$, da onde segue que $W = 0$, ou seja, $N_3 = N_2$ e assim segue que N_2 é simples.

□

Teorema 3.7. *Seja M um R-módulo. Então as seguintes condições são equivalentes*

i. M é semissimples.

ii. M é uma soma de submódulos simples.

iii. M é uma soma direta de submódulos simples.

Demonstração.

Se $M = (0)$ não há nada para mostrar, então, em toda demonstração, suponhamos que $M \neq (0)$.

(i) ⇒ (ii)

Seja $N = \sum_{i \in I} Si$, em que $\{Si\}_i \in x$ é a família de todos R-submódulos simples de M, a qual não é vazia pelo lema anterior.

Dessa forma, $\exists P \leq M$ tal que $M = N \oplus P$. Caso $P \neq (0)$, novamente pelo lema anterior, $\exists T$ submódulo simples de P, já que P deve ser semissimples por ser submódulo de um módulo semissimples.

Mas daí $P \cap N \neq (0)$, contradição. Ou seja, $M = N = \sum_{i \in I} Si$.

(ii) ⇒ (iii)

Suponhamos $M = \sum_{i \in I} Si$, em que $\{Si\}_{i \in I}$ é uma família de submódulos simples de M.

Considere a família $F = \{J \subset I \mid \sum_{j\in J} M_j \text{ é uma soma direta}\}$.

Como todo módulo simples é semissimples, segue que $F \neq \emptyset$. Além disso, como toda cadeia em F possui cota superior (a união de seus membros) segue do lema de Zorn que existe $I \in F$ elemento.

Seja $M' = \oplus_{j\in S} Mj$, afirmamos que $M' = M$.

De fato, pois para cada $i \in I$, M_i é simples, da onde decorre que $M_i \cap M' = M_i$ ou $M_i \cap M' = (0)$.

Se ocorrer $M_i \cap M' = (0)$, então $I \subseteq I \cup \{i\}$, o que contradiz a maximalidade de I.

Portanto $M_i \subseteq M' \ \forall\ i{\in}I \Rightarrow M = M'$.

(iii) ⇒ (i)

Suponha que M seja soma direta de submódulos simples $M = \oplus_{i\in I} M_i$, em que M_i é simples para todo $i \in I$.

Seja $N \neq M$, dessa forma, pelo mesmo raciocínio usado no item anterior, $N \cap M_i = M_i$ ou $N \cap M_i = (0)$. Como vimos anteriormente, o segundo caso não ocorre e daí $N = \oplus_{j\in J} M_j$, em que $J = \{i \in I \mid M_i \cap N = M_i\}$. Dessa forma, segue que M é semissimples pois dado $N \leq M$, temos que $M = N \oplus K$, em que $K = \oplus_{j\in I\setminus J} M_j$. □

Corolário 3.8. *Se um módulo quociente L de um módulo M semissimples é isomorfo a um submódulo de M então também é semissimples.*

Definição 3.9. Um anel R é chamado **semissimples** se o módulo de R sobre R é semissimples.

Exemplo 3.10. *Suponhamos que $R_1, R_2, \ldots, R_t$ são anéis semissimples. Então $R = R_1 \times R_2 \times \cdots \times R_t$ é um anel semissimples.*

Para vermos isto, observamos que, sendo R_i módulo sobre ele mesmo, $R_i = I_1 \oplus I_2 \oplus \cdots \oplus I_{n_i}$, para cada $i = 1, 2, \ldots, t$, onde I_j é um ideal à esquerda minimal de $R_i, 1 \leq j \leq n_i$. Assim, sendo R módulo sobre ele mesmo, temos:

$$R = \oplus_{i=1}^{t} R_i = \oplus_{i=1}^{t} (\oplus_{J=1}^{n_i} I_J)$$

e daí, segue que R é um módulo semissimples, ou seja, R é um anel semissimples, como queríamos mostrar.

Teorema 3.11. *Seja R anel. Então, as seguintes condições são equivalentes:*

i. Todo R-módulo é semissimples.

ii. R é um anel semissimples.

iii. R é uma soma direta de um número finito de ideais minimais (à esquerda).

Demonstração. $(i) \Rightarrow (ii)$ Por definição.

$(ii) \Rightarrow (iii)$ Já que os submódulos simples do R-módulo R são exatamente os ideais minimais à esquerda de R, segue do Teorema 3.7 que R pode ser escrito como $R = \oplus_{i\in I} L_i$ em que cada L_i é ideal minimal à esquerda, para cada $i \in I$. Agora, em particular, $1 \in R$ pode ser escrito como a soma finita $1 = x_{i_1} + \cdots + x_{i_n}$ com $x_{i_j} \in L_{ij}$. Então, para um elemento arbitrário r, temos que $r \cdot 1 = rx_{i_1} + \cdots + rx_{i_n}$ com $rx_{i_j} \in L_{i_j},\ 1 \leq j \leq n$. O que nos mostra que $R \subset L_{i_1} \oplus \cdots \oplus L_{i_n}$, porém, como a inclusão contrária é claramente $R = L_{i_1} \oplus \cdots \oplus L_{i_n}$.

$(iii) \Rightarrow (ii)$ Consequência direta do Teorema 3.7.

$(ii) \Rightarrow (i)$ Agora, assumindo que R é semissimples, seja M um R-módulo. Sabemos da Proposição 2.70 que M é a imagem epimórfica de um R-módulo livre F, assim, podemos escrever $F = \oplus_i Ra_i$ em que $Ra_i \simeq R$, o qual é semissimples. Dessa forma F é semissimples e o resultado segue do Corolário 3.8

□

Corolário 3.12. *Um anel semissimples, quando considerado como um módulo sobre si mesmo, tem comprimento finito.*

Demonstração. Como visto acima, se R é semissimples, pode ser escrito como uma soma direta finita:

$$R = L_1 \oplus L_2 \oplus \cdots \oplus L_t,$$

em que L_i é ideal minimal à esquerda, $1 \leq i \leq t$. Assim,

$$R = (L_1 \oplus L_2 \oplus \cdots \oplus L_t) \supset (L_2 \oplus \cdots \oplus L_t) \supset \cdots \supset L_t \supset (0),$$

e o resultado segue. □

Exemplo 3.13. *Seja $M_n(D)$ o anel de todas matrizes $n \times n$ sobre o anel de divisão D. Mostraremos que é um anel semissimples:*

$$L_1 = \begin{bmatrix} D & 0 & \cdots & 0 \\ D & 0 & \cdots & 0 \\ & & \cdots & \\ D & 0 & \cdots & 0 \end{bmatrix}, \ \cdots, \ L_n = \begin{bmatrix} 0 & 0 & \cdots & D \\ 0 & 0 & \cdots & D \\ & & \cdots & \\ 0 & 0 & \cdots & D \end{bmatrix}$$

Sendo $L_i, 1 \leq i \leq n$, ideais minimais à esquerda de $M_n(D)$ de forma que

$$M_n(D) = L_1 \oplus L_2 \oplus \cdots \oplus L_n.$$

Então, $M_n(D)$ é semissimples.

Teorema 3.14. *Seja R anel. Então R é semissimples se, e somente se, todo ideal à esquerda L é na forma $L = Re$, onde $e \in R$ é um idempotente.*

Demonstração. Ver ([2], p. 95). □

Teorema 3.15. *Seja $R = \oplus_{i=1}^{s} L_i$ a decomposição de um anel semissimples como soma direta de ideais minimais à esquerda. Então, existe uma família $\{e_1, \ldots, e_s\}$ de elementos de R tais que:*

i. $e_i \neq 0$ *é um idempotente central,* $1 \leq i \leq t$.

ii. Se $i \neq j$ *então* $e_i e_j = 0$.

iii. $1 = e_1 + \cdots + e_t$.

iv. e_i *não pode ser escrito como* $e_i = e_i' + e_i''$ *em que* e_i', e_i'' *são idempotentes tais que* $e_i' e_i'' = 0, 1 \leq i \leq t$.

Reciprocamente, se existe uma família de idempotentes $\{e_1, \ldots, e_s\}$ satisfazendo as condições acima, então os ideais à esquerda $L_i = Re_i$ são minimais e $R = \oplus_{i=1}^{t} L_i$.

Demonstração. Ver ([2], pg 96). □

Lema 3.16. *Sejam L ideal minimal de um anel semissimples R e M um R-módulo simples. Então*

$$LM \neq (0) \Longleftrightarrow L \simeq M$$

como R-módulos. Nesse caso, $LM = M$.

Demonstração.

($\Rightarrow$) Seja $LM \neq (0)$, então $\exists x \in L$, e $m \in M$ tais que $xm \neq 0 \Rightarrow Lm \neq (0)$. Já que $Lm \leq M$, que é simples, temos que $Lm = LM = M$.

Agora considere

$$f : L \to M$$
$$x \mapsto xm$$

f é homomorfismo: $f(x+y) = (x+y)m = xm + ym = f(x) + f(y)$

f é sobrejetora: como $M = LM$, o resultado segue.

f é injetora: $Kerf \subseteq L$ é ideal a esquerda de R e L é minimal $\Rightarrow Kerf = (0)$

$\therefore L \simeq M$.

($\Leftarrow$) Assuma que $L \simeq M$ como R-módulos e $f : L \to M$ um isomorfismo. Como R é semissimples, existe um elemento idempotente $e \in R$ tal que $L = Re$.

Faça $m_0 = f(e)$. Como $f(re) = rf(e)\ \forall\ v \in R$, segue que $m_o \neq 0$. Já que $m_0 = f(e) = f(e^2) = ef(e) = em$. Segue que $LM \neq (0)$.

□

Proposição 3.17. *Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de um anel semissimples R como soma direta de ideais minimais à esquerda. Então todo R-módulo simples é isomorfo a um dos ideais L_i na decomposição inicial.*

Demonstração. Dada a decomposição do anel semissimples $R = \oplus_{i=1}^{t} L_i$, considere M um R-módulo simples. Assim, como RM é submódulo não nulo de M e M é simples, temos, pelo lema acima que que $RM = M$. Dessa forma, temos que $RM = \oplus_{i=1}^{t} L_i M$, então, pela não nulidade de RM, existe um índice j tal que $L_j M \neq (0)$ e, novamente pelo lema anterior, obtemos que $L_j \simeq M$. □

3.2 Teorema de Wedderburn-Artin

Nesta seção, temos como objetivo principal a demonstração de um dos teoremas mais importantes deste trabalho: o *Teorema de Wedderburn-Artin*.

A importância deste resultado vem do fato de que ele nos oferece a possibilidade de decompor anéis semissimples em somas diretas de álgebras de matrizes sobre anéis de divisão, além de possibilitar uma outra caracterização de anéis semissimples.

Antes de iniciarmos os resultados necessários, mostraremos um exemplo de decomposição de um anel em soma direta de álgebras de matrizes.

Exemplo 3.18. *Considere o conjunto das matrizes 2×2 sobre o corpo $\mathbb{Z}_2$:*

$$M_2(\mathbb{Z}_2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \ a, b, c, d \in \mathbb{Z}_2 \right\} = R$$

A partir da Observação 3.24, temos que o anel $M_2(\mathbb{Z}_2)$ é simples, e por consequência, semissimples.

Além disso, pelo Exemplo 3.13, sabemos que os ideais minimais à esquerda de R são da forma:

$$\begin{bmatrix} \mathbb{Z}_2 & 0 \\ \mathbb{Z}_2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \mathbb{Z}_2 \\ 0 & \mathbb{Z}_2 \end{bmatrix}.$$

E daí, segue que:

$$R = L_1 \oplus L_2$$

em que

$$L_1 = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} : \ a, c, \in \mathbb{Z}_2 \right\} \ \ e \ \ L_2 = \left\{ \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} : \ b, d \in \mathbb{Z}_2 \right\}$$

Lema 3.19. *Seja L um ideal minimal a esquerda de um anel semissimples R. Então a soma de todos os ideais à esquerda de R isomorfos a L é um ideal bilateral de R.*

Demonstração. Seja $A = \sum_{J \simeq L} J$. Temos que A é um ideal a esquerda, pois o somatório de ideais também é ideal. Agora, provaremos que ele também é um ideal à direita.

Como R é semissimples, podemos escrevê-lo na forma de uma soma direta de ideais minimais à esquerda: $R = \oplus_{i=1}^{t} L_i$, então

$$AR = \sum_{J \simeq L} JR = \sum_{J \simeq L} \sum_{i=1}^{t} JL_i.$$

Porém, como sabemos, ou $JL_i = (0)$ ou $JL_i = L_i$, pois L_i é minimal. Pelo Lema 3.16, $JL_i = L_i$ apenas se $J \simeq L_i$, ou seja, quando $J \simeq L$. O que nos diz que os elementos de L_i também são elementos de A, e assim $L_i \subset A$.

Mas como os elementos em AR são somas de elementos de $J \subset A$ e de $L_i \subset A$, concluímos que $AR \subset A$.

□

Lema 3.20. *Seja I um ideal bilateral de um anel semissimples, que contém um ideal minimal L. Então I contém todos os ideais à esquerda isomorfos a L.*

Demonstração. Seja $L \subset I$ um ideal minimal a esquerda e seja J um ideal a esquerda isomorfo a L. Se olharmos J e L como R-módulos, do Lema 3.16, segue que $J = LJ$. Mas daí, sendo $j \in J,\ j = l + j_1,\ l \in L,\ j_1 \in J \subset R \Rightarrow j \in L$, pois L é ideal. Portanto, $J = LJ \subset I$.

□

Proposição 3.21. *Seja L, um ideal minimal a esquerda de um anel semissimples R e seja B a soma de todos os ideais à esquerda de R que são isomorfos a L. Então, B é um ideal minimal bilateral de R.*

Demonstração. Seja B_1 um ideal bilateral de R tal que $B_1 \subset B$ e seja L_1 um ideal minimal a esquerda de R contido em B_1. Se $L_1 \not\simeq L$, utilizando o Lema 3.16 temos que $L_1 J = (0)$, para todo $J \simeq L$. Daí, $L_1 B = (0)$, o que, em particular, implica que $L_1 L_1 = (0)$. Porém isso não pode acontecer, visto que L_1 contém um elemento idempotente, como visto no Teorema 3.14.

Dessa forma, temos que $L_1 \simeq L$, ou seja, $L \subset B_1$ daí, do Lema 3.20, B_1 contém todos os ideais à esquerda isomorfos a L. Assim, $B \subset B_1$ e portanto $B_1 = B$.

□

Observação 3.22. *Dada a decomposição de um anel semissimples R como soma direta de ideais minimais à esquerda, reordenando se necessário, nós podemos agrupar ideais à esquerda isomorfos juntos:*

$$R = L_{11} \oplus \cdots \oplus L_{1r_1} \oplus L_{21} \oplus \cdots \oplus L_{2r_2} \oplus \cdots \oplus L_{s1} \oplus \cdots \oplus L_{sr_s}$$

Com a notação dada acima, temos $L_{ij} \simeq L_{ik}$ *e* $L_{ij}L_{kh} = (0)$ *se* $i \neq k$ *pelo Lema 3.16.*

Além disso, da Proposição 3.17, segue que todos os ideais minimais à esquerda são isomorfos a um dos ideais na decomposição de R *dada acima.*

Teorema 3.23. *Com a notação acima, seja* A_i *a soma de todos os ideais à esquerda isomorfos a* $L_{i1},\ 1 \leq i \leq s$. *Então:*

i. Cada A_i *é um ideal minimal bilateral de* R.

ii. $A_iA_j = (0)$ *se* $i \neq j$.

iii. $R = \oplus_{i=1}^{s} A_i$ *como anéis, onde* s *é o número de classes isomórficas de ideais minimais à esquerda de* R.

Demonstração. i. segue da Proposição 3.21 em vista da observação acima.

ii. para provar este item, escrevemos

$$R = (L_{11} \oplus \cdots \oplus L_{1r_1}) \oplus (L_{21} \oplus \cdots \oplus L_{2r_2}) \oplus \cdots \oplus (L_{s1} \oplus \cdots \oplus L_{sr_s})$$

como acima. Então, todo elemento $x \in R$ pode ser escrito na forma $x = x_{11} + \cdots + x_{s1} + \cdots + x_{sr_s}$,com $x_{ij} \in L_{ij}$. Defina $y_i = x_{i1} + \cdots + x_{ir},\ 1 \leq i \leq s$. Então, $y_i \in A_i,\ 1 \leq i \leq s$ e $x = y_1 + \cdots + y_s$. Isso mostra que $R = A_1 + \cdots + A_s$.

Note que, dada essa apresentação dos A_i, o resultado segue do Lema 3.16, pois $L_{ij} \simeq L_{ik}$ e $L_{ij}L_{kh} = (0)$ se $i \neq k$.

iii. Como $A_i = \oplus_{i=1}^{s} = L_{i1}$, o resultado segue diretamente da decomposição de R dada acima.

□

Observação 3.24. *A partir da Definição 2.45, podemos notar que se* D *é um anel de divisão e* n *é um inteiro positivo, a Proposição 2.42 mostra que* $M_n(D)$ *é um* ***anel simples****.*

Corolário 3.25. *Os ideais* $A_i,\ 1 \leq i \leq s$, *definidos acima, são anéis simples.*

Demonstração. Já que $A_i,\ 1 \leq i \leq s$, é um ideal minimal bilateral de R, é suficiente mostrar que qualquer ideal bilateral B_i de A_i é também um ideal de R. Isso implicará imediatamente que ou $B_i = (0)$ ou $B_i = A_i$.

Então, dado $b \in B_i$ e $r \in R$. Nós podemos escrever $r = x_1 + \cdots + x_s$, em que $x_j \in A_j,\ 1 \leq j \leq s$.

Dessa forma, $rb = \sum_{j=1}^{s} x_j b$ e, já que $x_j b = 0$ se $j \neq i$, nós temos que $rb = x_j b \in B_i$, já que B_i é um ideal de A_i.

Analogamente, $br = \sum_{j=1}^{s} b x_j$, mas como $b x_j = 0$ se $j \neq i$, segue que $br = b x_j \in B_i$, pois B_i é ideal bilateral de A_i.

Ou seja, temos que qualquer ideal bilateral B_i de A_i é também ideal de R. Mas daí, segue da definição de ideal minimal que $B_i = (0)$ ou $B_i = A_i$, e por consequência, concluímos que $A_i,\ 1 \leq i \leq s$, é simples.

□

Proposição 3.26. *Seja $R = \oplus_{i=1}^{s} A_i$ a decomposição de um anel semissimples R como soma direta de ideais minimais bilaterais. Então*

i. Todo ideal bilateral I de R pode ser escrito como $I = A_{i_1} \oplus \cdots A_{i_t}$, em que $1 \leq i_1 < \cdots < i_t \leq s$.

ii. Se $R = \oplus_{j=1}^{r} B_i$ é outra decomposição de R em uma soma direta de ideais minimais bilaterais, então $s = r$ e, com uma possível reenumeração de índices, $A_i = B_i\ \forall i$.

Demonstração. i. Seja I um ideal bilateral em R. Então $I = \oplus_{i=1}^{s}(A_i \cap I)$. Como os A_i's são minimais, $A_i \cap I = (0)$ ou $A_i \cap I = A_i$ para todo $i \in \{1, \cdots, s\}$ e o resultado segue.

ii. Novamente pela minimalidade dos A_i's, $A_i \cap B_j = (0)$ ou $A_i \cap B_j = A_i$, $\forall j \in \{1, \cdots, r\}$, e portanto $r = s$.

□

Definição 3.27. Os únicos ideais minimais bilaterais de um anel semissimples R são chamados de **componentes simples** de R.

Lema 3.28. *Seja R um anel e sejam $M = M_1 \oplus \cdots \oplus M_r$ e $N = N_1 \oplus \cdots N_s$ dois R-módulos escritos como soma direta de submódulos. Além disso, seja $\varepsilon_j : M_j \to M$ as inclusões de cada M_j em M e $\pi_i : N \to N_i$ o homomorfismo natural de N em suas componentes. Daí:*

i. Suponha que, para cada par de índices i, j, temos um homomorfismo $\phi_{ij} \in \mathrm{Hom}_R(M_j, N_i)$. Então, a aplicação $\phi : M \to N$ definida por:

$$\phi(m_1 + \cdots + m_r) = \begin{bmatrix} \phi_{11} & \cdots & \phi_{1r} \\ \cdots & \cdots & \cdots \\ \phi_{s1} & \cdots & \phi_{sr} \end{bmatrix} \begin{bmatrix} m_1 \\ \cdots \\ m_r \end{bmatrix} =$$
$$= \underbrace{\phi_{11}(m_1) + \cdots + \phi_{1r}(m_r)}_{\in N_1} + \cdots + \underbrace{\phi_{s1}(m_1) + \cdots + \phi_{sr}(m_r)}_{\in N_s},$$

é um homomorfismo. Para indicar que ϕ é dado da forma acima, por notação, escreveremos $\phi = (\phi_{ij})$.

ii. Reciprocamente, se $\phi \in Hom_R(M,N)$*, então* $\phi_{ij} = \pi_i \circ \phi \circ \varepsilon_j \in Hom_R(M_j, N_i)$ *e* $\phi = (\phi_{ij})$.

iii. Para $\phi = (\phi_{ij})$ *e* $\phi = (\psi_{ij})$*, temos* $\phi + \psi = (\phi_{ij} + \psi_{ij})$.

iv. $Hom_R(M^{(n)}, M^{(n)}) \simeq M_n(Hom_R(M,M))$*, como anéis.*

Demonstração. Ver ([2], p. 101). □

Lema 3.29. *Seja* R *um anel,* M *um* R*-módulo semissimples e* $B = Hom_r(M,M)$*. Então,* M *admite uma estrutura de* B*-módulo dada por* $\phi \cdot m = \phi(m)$, $\forall \phi \in B$, $\forall m \in M$*. Mais ainda, para cada* $m \in M$ *e cada* $f \in Hom_B(M,M)$*, existe um elemento* $a \in R$ *tal que* $f(m) = am$.

Demonstração. A primeira afirmação segue da definição de módulo a partir da definição da operação de um elemento de B por um elemento de M. Para provar a segunda, pegue $m \in M$ e considere o submódulo Rm. Como M é semissimples, existe um submódulo W tal que $M = Rm \oplus W$ e, se denotarmos por $\pi : M \to M$ a projeção em Rm, temos que $\pi \in Hom_R(M,M) = B$, pois sabemos que a função projeção é um homomorfismo. Dado um elemento de $f \in Hom_B(M,M)$, temos

$$f(m) = f(\pi(m)) = \pi(f(m)) \in Rm.$$

pois M é B-módulo e $\pi \in B$. Dessa forma, como $f(m) \in Rm$ existe um elemento $a \in R$ tal que $f(m) = am$. □

Teorema 3.30. ***(Teorema da Densidade de Jacobson)*** *Seja* M R*-módulo semissimples e* $B = Hom_R(M,M)$, $f \in Hom_R(M,M)$*. Se* $m_1, \cdots, m_n$ *é um conjunto de elementos arbitráros de* M*, existe um elemento* $a \in R$ *tal que* $f(m_i) = am_i, \forall 1 \leq i \leq n$.

Demonstração. Dado $f \in Hom_B(M,M)$ definimos $f^{(n)} : M^{(n)} \to M^{(n)}$ dado por

$$f^{(n)}(x_1 + \cdots + x_n) = f(x_1) + \cdots + f(x_n), \quad x_1, \ldots, x_n \in M$$

Seja $B' = Hom_R(M^{(n)}, M^{(n)})$. Queremos que $f^{(n)} \in Hom_{B'}(M^{(n)}, M^{(n)})$. De fato, dado $\phi \in B'$, pelo Lema 3.28 podemos escrever $\phi = (\phi_{ij})$ com $\phi_{ij} \in Hom_r(M_j, M_i)$. Daí temos:

$$\begin{aligned}
&f^{(n)} \circ \phi(m_1 + \cdots + m_n) \\
&= f^{(n)}(\phi_{11}(m_1) + \cdots + \phi_{1n}(m_n) + \cdots + \phi_{n1}(m_1) + \cdots + \phi_{nn}(m_n)) \\
&= \phi_{11}(f(m_1)) + \cdots + \phi_{1n}(f(m_1)) + \cdots + \phi_{n1}(f(m_1)) + \cdots + \phi_{nn}(f(m_n)) \\
&= \phi(f(m_1) + \cdots + f(m_n)) \\
&= \phi \circ f^{(n)}(m_1 + \cdots + m_n)
\end{aligned}$$

Pelo lema anterior, segue que existe um elemento $a \in R$ tal que $f^{(n)}(m_1 + \cdots + m_n) = a(m_1 + \cdots + m_n)$. Temos assim, $f(m_i) = am_i$, $1 \leq i \leq n$.

□

Lema 3.31. ***(Lema de Schur)*** *Seja R anel e sejam M, N R-módulos simples. Seja $f : M \to N$ um homomorfismo não nulo. Então, f é isomorfismo.*

Demonstração. Como sabemos que $Im(f)$ é submódulo do módulos simples N e não é igual a (0), pois f é um homomorfismo não nulo, segue que $Im(f) = N$, pela definição de simplicidade. Assim, concluímos que f é epimorfismo.

De forma similar, já que $Ker(f)$ é submódulo do módulos simples M e não é igual a M, novamente porque o homomorfismo é não nulo, segue que $Ker(f) = (0)$. Ou seja, f também é monomorfismo, e, portanto, isomorfismo.

□

Corolário 3.32. *Seja R anel e M, N R-módulos simples. Então, temos:*

i. Se $M \not\cong N$, então $Hom_R(M, N) = (0)$.

ii. $Hom_R(M, M)$ é anel de divisão.

Demonstração. i. Supondo que $M \not\cong N$, pela contrapositiva do lema anterior, sendo $f : N \to M$ homomorfismo, o mesmo será nulo.

ii. Como já sabemos, $Hom_R(M, M)$ é o anel dos homomorfismos de M em M, como R-módulos. Dessa forma, novamente pelo lema anterior, temos que os homomorfismos em $Hom_R(M, M)$, são na verdade, isomorfismos, ou seja, todo elemento no anel é inversível. Assim, concluímos que $Hom_R(M, M)$ é anel de divisão.

□

Observação 3.33. *Note que se R é anel artiniano semissimples e M é R-módulo simples, pelo Lema de Schur, $D = Hom_R(M, M)$ é anel de divisão. Mas se R já que, pelo Lema 3.29, M também é D-módulo, é na verdade espaço vetorial sobre D. Queremos que este espaço vetorial possua dimensão finita. De fato, se $\{m_1, \cdots, m_n, \cdots\}$ é um conjunto linearmente independente de elementos de M sobre D, podemos definir para cada índice t o seguinte conjunto:*

$$A_t = \{a \in R \mid am_i = 0, 1 \leq i \leq t\}.$$

Vamos provar que A_t é ideal à esquerda:

i. Note que $A_t \neq \emptyset$ pois existe $0 \in R$ tal que $0m_i = 0, \forall i \in \{1, \cdots, t\}$, logo $0 \in A_t$.

ii. Dados $a, b \in A_t$, temos que $am_i = 0 = bm_i \Rightarrow am_i - bm_i = 0 \Rightarrow (a-b)m_i = 0 \Rightarrow a-b \in A_t$.

iii. Por fim, sendo $r \in R$ e $a \in A_t \Rightarrow am_i = 0 \Rightarrow r(am_i) = 0 \Rightarrow (ra)m_i = 0 \Rightarrow ra \in A_t$

Além disso, perceba que $A_{i+1} \subset A_i,\ i \in \{1, 2, \cdots\}$ e que, pelo Teorema da Densidade de Jacobson essa inclusão é estrita, então, se o conjunto linearmente independente dado for inifito, teríamos uma cadeia decrescente de inclusões estritas de ideais:

$$A_1 \supset A_2 \supset \cdots \supset A_t \supset \cdots$$

contradizendo o fato de que R é artiniano.

Observação 3.34. *Para o próximo lema, precisaremos definir uma notação: dado um anel de divisão D, denotaremos por D^{op} o* ***anel oposto*** *a D, ou seja, o anel definido pelo mesmo conjunto, usando a mesma adição que em D e com a multiplicação dada por $x \cdot y = yx$, em que yx denota a multiplicação de y e x em D.*

Lema 3.35. *Seja R anel artiniano simples, M R-módulo simples e $D = Hom_R(M, M)$. Então,*

$$R \simeq Hom_D(M, M) \simeq M_n(D^{op})$$

em que n é a dimensão de M como D-módulo.

Demonstração. Considere a aplicação $\Phi : R \to Hom_D(M, M)$

$$a \mapsto f_a : M \to M$$
$$x \mapsto f_a(x) = ax,\ \forall x \in M.$$

Provaremos que Φ é bijeção. Considere o seguinte conjunto:

$$I = \{a \in R \mid am = 0,\ \forall m \in M\},$$

queremos ver que I é ideal (bilateral) de R:

i. $I \neq \emptyset$, pois $0 = 0 \cdot m \in I \Rightarrow 0 \in I$.

ii. $a, b \in I \Rightarrow am = 0 = bm \Rightarrow am - bm = 0 \Rightarrow (a - b)m = 0 \Rightarrow a - b \in I$.

iii. Sendo $r \in R$ e $a \in I \Rightarrow am = 0 \Rightarrow a(bm) = 0 \Rightarrow (ab)m = 0 \Rightarrow ab \in I$;

Da mesma forma: $a(rm),\ rm \in M$, pois M é módulo. Mas como $a \in I$, temos que $bx = 0\ \forall x \in M \Rightarrow b(am) = 0$.

Dessa forma, como R é simples, $I = R$ ou $I = (0)$. Mas como $1 \notin I$, segue que $I = Ker\Phi = (0)$, ou seja, Φ é injetora.

Agora, considere $\{m_1, \cdots, m_n\}$ base de M sobre D, que é finita, pelo **Corolário 21**. Segue do Teorema da Densidade de Jacobson que $\exists\ a \in R$ tal que $f(m_i) = am_i,\ \forall i \in \{1, \cdots, n\}$, ou seja para todo $f \in Hom_D(M, M)$, existe $a \in R$ tal que $f = f_a$ e Φ é sobrejetora.

Por fim, sendo $a, b \in R$ vemos que:

$$(\Phi(a) \circ \Phi(b))(x) = (f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(bx) = (ab)x = f_{ab}(x) = (\Phi(a \cdot b))(x).$$

$\therefore \Phi$ é isomorfismo.

Finalmente, se n é a dimensão de M como D-módulo, $M \simeq D^{(n)}$ como D-módulos ([10]).

Assim, pelo Lema 3.28, temos que $Hom_D(M, M) \simeq M_n(Hom_D(D, D))$ e basta mostrar que $Hom_D(D, D) \simeq D^{op}$.

Defina a aplicação $\Psi : D \to Hom_D(M, M)$

$$a \mapsto f_a : D \to D$$

$$x \mapsto f_a(x) = xa, \ \forall x \in D.$$

Provaremos que Ψ é bijeção.

Pelo mesmo raciocínio usado anteriormente, definindo $J = Ker\Psi$ que será ideal à direita, concluímos que Ψ é injetora.

Além disso, dada $f \in Hom_D(D, D)$, temos que $f(x) = f(x1) = xf(1)$, então, se definirmos $a = f(1)$, teremos que $f = \Psi(a)$ e assim, Ψ é sobrejetora.

Agora, note que

$$(\Psi(a) \circ \Psi(b))(x) = (f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(xb) = x(ba) = f_{ba}(x) = (\Psi(b \cdot a))(x),$$

e daí, segue que $Hom_D(D, D) \simeq D^{op}$, como queríamos. □

Corolário 3.36. *Um anel artiniano simples é semissimples.*

Demonstração. Pelo Lema 3.35, temos que todo anel artiniano simples é isomorfo a uma soma direta de matrizes sobre anéis de divisão. Mas, do Exemplo 3.13, temos que as matrizes sobre anéis de divisão são semissimples. □

Teorema 3.37. ***(Wedderburn-Artin)*** *Um anel R é semissimples se, e somente se, é soma direta de álgebras de matrizes sobre anéis de divisão:*

$$R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s).$$

Demonstração. Seja R semissimples e suponha a seguinte decomposição em ideais minimais à esquerda, que será agrupada em ideais à esquerda isomorfos entre si:

$$R = \underbrace{L_{11} \oplus \cdots \oplus L_{1r_1}}_{A_1} \oplus \cdots \oplus \underbrace{L_{s1} \oplus \cdots \oplus L_{sr_s}}_{A_s}$$

Então, pelo Teorema 3.23, a decomposição $R = \oplus_{i=1}^{s} A_i$ é formada por ideais minimais bilaterais. Além disso, pelo Lema 3.35, $A_i \simeq Hom_{D_i}(L_{i1}, L_{i1})$. Já $D_i = Hom_R(L_{i1}, L_{i1})$ é, por sua vez, anel de divisão pelo Corolário 3.32. Novamente pelo Lema 3.35, temos que $A_i \simeq M_{n_i}(D_i)$, em que n_i é a dimensão de L_{i1} com D_i-módulo.

Reciprocamente, tendo como hipótese o isomorfismo de R como soma direta de álgebras de matrizes sobre anéis de divisão, temos que cada componente da decomposição é simples, pela Proposição 2.42. Assim temos pela Proposição 3.21 que A_i é ideal minimal bilateral de R, e daí, do Teorema 3.7, R é semissimples.

□

Corolário 3.38. *Um anel artiniano é simples se, e somente se, é isomorfo a um anel de matrizes sobre um anel de divisão.*

Demonstração. Seja R um anel artiniano e simples. Como R tem unidade, segue que todo ideal à esquerda é um R-módulo. Além disso, como R é artiniano, todo R-módulo à esquerda possui um R-submódulo simples. Portanto, nas condições acima, ou R é um anel de divisão ou R é um anel simples que possui um ideal à esquerda minimal. Portanto, $R \simeq M_n(D)$, para algum $n \geq 1$ e D um anel de divisão.

A recíproca se dá do fato de que, se R é isomorfo a um anel de matrizes sobre um anel de divisão que é simples como visto na Observação 3.24.

□

Com o próximo teorema, estabelerecemos a unicidade da decomposição de Wedderburn-Artin para um anel semissimples.

Teorema 3.39. *Seja R anel semissimples e assuma que*

$$R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s) \simeq M_{m_1}(D'_1) \oplus \cdots \oplus M_{m_r}(D'_r),$$

em que $D_i, D'_j, 1 \leq i \leq s, 1 \leq j \leq r$ são anéis de divisão. Então $s = r$ e, depois de uma possível permutação de índices, temos que $n_i = m_i$ e $D_i \simeq D'_i$.

Demonstração. Já que anéis de matrizes sobre anéis de divisão são simples, segue da Proposição 3.26 que $s = r$ e que existe uma bijeção entre os dois conjuntos de ideais, tal que os ideais correspondentes no isomorfismo são iguais.

Dessa forma, resta apenas provar que $M_n(D) \simeq M_m(D')$, e então $n = m$ e $D \simeq D'$ como anéis de divisão.

Denote por $E = M_n(D)$ e $E' = M_m(D')$ e defina:

$$L = \begin{bmatrix} D & 0 & \cdots & 0 \\ D & 0 & \cdots & 0 \\ & & \cdots & \\ D & 0 & \cdots & 0 \end{bmatrix}, \quad L' = \begin{bmatrix} D' & 0 & \cdots & 0 \\ D' & 0 & \cdots & 0 \\ & & \cdots & \\ D' & 0 & \cdots & 0 \end{bmatrix}$$

Então $L = eE,\ L' = fE'$, em que e e f são as correspondentes matrizes de idempotentes com 1 na entrada (1,1) e zeros nas outras. Sobre o isomorfismo $E \to E'$, e é aplicado em um idempotente e', então $e'L'$ é ideal minimal à esquerda. Trocando as bases de E' temos um novo isomorfismo $E \to E'$ de forma que $e \to f$ e tal que $L \to L'$. Então

$$D \simeq eEe \to fE'f \simeq D'$$

e como $s = r$, segue também que $n = m$. □

4 Anéis de Grupo

As referências principais do capítulo a seguir são: [2], [11], [12], [13].

4.1 Conceitos Essenciais

Sejam G um grupo (não necessariamente finito) e R um anel com unidade.

Construiremos um *R-módulo* com os elementos de G como base e usaremos as operações de G e R para definir estrutura de anel nele.

Denotaremos por RG o conjunto de todas as combinações lineares da forma

$$\alpha = \sum_{g \in G} a_g \cdot g,$$

em que $a_g \in R$ e $a_g \neq 0$ para quantidades finitas de elementos $g \in G$.

Definição 4.1. Definimos o conjunto suporte de um elemento α como

$$supp(\alpha) = \{g \in G \mid a_g \neq 0\}.$$

Dados $\alpha, \beta \in RG$ tais que:

$$\alpha = \sum_g a_g g \text{ e } \beta = \sum_g b_g g$$

definimos as seguintes propriedades:

i. Igualdade:

$$\alpha = \beta \Leftrightarrow a_g = b_g \forall g$$

ii. Soma de elementos:

$$\left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g$$

iii. Multiplicação de elementos:

$$\left(\sum_{g \in G} a_g g\right) \cdot \left(\sum_{h \in G} b_h h\right) = \sum_{g,h} a_g b_h g \cdot h$$

iv. Multiplicação de elementos por escalar:

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

Note que as operações acima estão bem definidas pois:

$$supp(\lambda + \mu) \subset supp(\lambda) \cup supp(\mu) \text{ e } supp(\lambda\mu) \subset supp(\lambda) \cdot supp(\mu).$$

Definição 4.2. O conjunto RG definido acima é chamado de Anel de Grupo de G sobre R.

Caso R seja comutativo, RG também pode ser chamado de Álgebra de Grupo de G sobre R.

Caso $R = \mathbb{Z}$, podemos chamar o anel de grupo $\mathbb{Z}G$ de Anel de Grupo Integral.

Exemplo 4.3. *Dado $G = \{1, a, a^2\}$ o grupo cíclico de ordem 3 com gerador a e $\mathbb{K} = \mathbb{C}$, teremos que $r \in \mathbb{C}G$ é dado da forma:*

$$r = z_0 + z_1 a + z_2 a^2.$$

Note que é a mesma descrição de um anel de polinômio na variável a tal que $a^3 = a^0$, ou seja,

$$r = ax^2 + bx + c$$

com $a, b, c \in \mathbb{C}$ e x o gerador do grupo cíclico.

Se $s = \omega_0 + \omega_1 a + \omega_2 a^2$, a soma é:

$$r + s = (z_0 + \omega_0) + (z_1 + \omega_2)a + (z_2 + \omega_2)a^2$$

e o produto:

$$rs = (z_0\omega_0 + z_1\omega_2 + z_2\omega_1) + (z_0\omega_1 + z_1\omega_0 + z_2\omega_2)a + (z_0\omega_2 + z_2\omega_0 + z_1\omega_1)a^2.$$

Observação 4.4. *De acordo com a definição de produto no anel de grupo, caso R seja comutativo e G seja abeliano, o anel de grupo RG é comutativo.*

Definição 4.5. É chamada de **imersão** de G em RG a aplicação

$$i : G \to RG,$$

definida por

$$i(x) \mapsto \sum_{g \in G} a_g g,$$

em que $a_x = 1$ e $a_g = 0$ se $g \neq x$. Assim, podemos considerar G como um subconjunto de RG.

Também podemos definir a aplicação

$$v : R \to RG$$

dada por

$$v(r) = \sum_{g \in G} a_g g,$$

em que $a_e = r$ e $a_g = 0$ se $g \neq e$. A aplicação v é um monomorfismo de anéis e, portanto, podemos considerar R como um subanel de RG.

Teorema 4.6 (Propriedade Universal de Anéis de Grupos)**.** *Sejam G um grupo, R e A anéis comutativos com unidade,*

$$f : G \to A^*,$$

onde A^* representa o grupo multiplicativo de A, e

$$\phi : R \to A$$

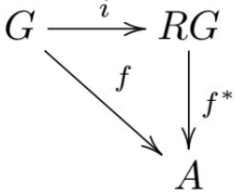
denota um homomorfismo de anéis tal que

$$f(g)\phi(r) = \phi(r)f(g),$$

então existe um único homomorfismo

$$f^* : RG \to A$$

que estende f e ϕ tal que o seguinte diagrama é comutativo



Demonstração. Seja $f : G \to A$, considere $f^* : RG \to A$ definida por

$$\sum_{g \in G} a_g g \mapsto \sum_{g \in G} \phi(a_g) f(g)$$

.

$\vdash$: f^* é um homomorfismo de anéis.

Dados $\alpha = \sum_{g\in G} a_g g$, $\beta = \sum_{g\in G} b_g g$ e $r \in R$ em RG, temos que:

$$\begin{aligned} f^*(\alpha+\beta) &= f^*\left(\sum_{g\in G}(a_g+b_g)g\right) \\ &= \sum_{g\in G}\phi(a_g+b_g)f(g) \\ &= \sum_{g\in G}\phi(a_g)f(g) + \sum_{g\in G}\phi(b_g)f(g) \\ &= f^*(\alpha)+f^*(\beta) \end{aligned}$$

$$\begin{aligned} f^*(\alpha\beta) = f^*\left(\sum_{h,g\in G}\phi(a_g b_h)f(gh)\right) &= \sum_{g,h}\phi(a_g)\phi(b_h)f(g)f(h) \\ &= \sum_{g\in G}\phi(a_g)f(g)\sum_{h\in H}\phi(b_h)f(h) \\ &= f^*(\alpha)f^*(\beta) \end{aligned}$$

$\vdash$: Unicidade de f^*

Suponha que exista outra função π, nas condições pedidas, tal que $\pi \circ i = f$ para $\alpha = \sum_{g\in G} a_g g \in RG$. Assim, temos que

$$\begin{aligned} \pi(\alpha) &= \pi\left(\sum_{g\in G} a_g g\right) \\ &= \sum_{g\in G}\pi(a_g)\pi(g) \\ &= \sum_{g\in G}\phi(a_g)\pi(i(g)) \\ &= \sum_{g\in G}\phi(a_g)f(g) \\ &= f^*(\alpha) \end{aligned}$$

□

Observação 4.7. *Note que se A for uma R-álgebra, então o homomorfismo f^* é de R-álgebras. De fato, sendo A uma R-álgebra, basta tomarmos ϕ definida por:*

$$\begin{aligned} \phi : R &\to A \\ r &\mapsto r \cdot 1_A. \end{aligned}$$

Assim se $r \in R$:

$$\begin{aligned} f^*\left(\sum_{g\in G} ra_g g\right) &= \sum_{g\in G} \phi\left(ra_g\right) f(g) \\ &= \sum_{g\in G} \left(ra_g\right) \cdot 1_A f(g) \\ &= \sum_{g\in G} r\left(a_g \cdot 1_A\right) f(g) \\ &= r\sum_{g\in G} \left(a_g \cdot 1_A\right) f(g) \\ &= r\sum_{g\in G} \phi\left(a_g\right) f(g) \\ &= r f^*\left(\sum_{g\in G} a_g g\right) \end{aligned}$$

Proposição 4.8. *Seja $\pi : G \to H$ um isomorfismo entre os grupos G e H. Então, existe um isomorfismo entre RG e RH.*

Demonstração. Seja $\pi^* : RG \to RH$ definida por

$$\pi^*\left(\sum_{g\in G} a_g g\right) = \sum a_g \pi(g)$$

.

$\vdash$: π^* é um homomorfismo de anéis

Sejam $\alpha = \sum_{g\in G} a_g g$, $\beta = \sum_{g\in G} b_g g \in RG$, $r \in R$, teremos que:

$$\begin{aligned} \pi^*(\alpha+\beta) &= \pi^*\left(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\right) \\ &= \pi^*\left(\sum_{g\in G} (a_g + b_g) g\right) \\ &= \sum_{g\in G} (a_g + b_g)\pi(g) \\ &= \sum_{g\in G} a_g \pi(g) + \sum_{g\in G} b_g \pi(g) \\ &= \pi^*(\alpha) + \pi^*(\beta) \end{aligned}$$

$$\begin{aligned}
\pi^*(\alpha\beta) &= \pi^*\left(\sum_{g,h} a_g b_h gh\right) \\
&= \sum_{g,h} a_g b_h \pi(gh) \\
&= \sum_{g,h} a_g b_h \pi(g)\pi(h) \\
&= \left(\sum_{g\in G} a_g \pi(g)\right)\left(\sum_{h\in H} b_h \pi(h)\right) \\
&= \pi^*(\alpha)\pi^*(\beta)
\end{aligned}$$

$$\begin{aligned}
\pi^*(r\alpha) &= \pi^*\left(\sum_{g\in G}(ra_g)g\right) \\
&= \sum_{g\in G}(ra_g)\pi(g) \\
&= r\sum_{g\in G} a_g\pi(g)
\end{aligned}$$

$\vdash$: π^* é injetivo

Seja $\sum\limits_{g\in G} a_g \in \ker\pi^* \Rightarrow \sum\limits_{g\in G} a_g\pi^*(g) = 0 \Rightarrow a_g = 0 \ \ \forall g.$

$\vdash$: π^* é sobrejetivo

Seja $\sum\limits_{h\in H} a_h h \in RH$. Tome $\sum\limits_{h\in H} a_h\pi^{-1}(h) \in RG$, então

$$\begin{aligned}
\pi^*\left(\sum_{h\in H} a_h\pi^{-1}(h)\right) &= \sum_{h\in H} a_h(\pi\circ\pi^{-1})(h) \\
&= \sum_{h\in H} a_h h
\end{aligned}$$

□

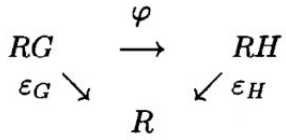
Observação 4.9. *A proposição anterior mostra que é sempre verdade que os grupos isomorfos induzem anéis de grupo isomorfos. A recíproca, por outro lado, nem sempre é verdadeira. A análise dessa recíproca é conhecida como o Problema do Isomorfismo.*

Definição 4.10. Sejam G e H grupos finitos.

Um isomorfismo $\varphi : RG \to RH$ é chamado isomorfismo **normalizado** se preserva a aplicação do aumento, ou seja, se

$$\varepsilon_H \circ \varphi = \varepsilon_G,$$

o que é o mesmo que dizer que o seguinte diagrama comuta



Teorema 4.11. *Seja R um anel comutativo com unidade, e sejam grupos. Então,*

$$R(G \times H) \simeq (RG)H.$$

Demonstração. Considere $f : R(G \times H) \to (RG)H$, dada por

$$\sum_{g,h} a_{gh}(g,h) \mapsto \sum_{h \in H} \left(\sum_{g \in G} a_{gh} g \right) h$$

.

$\vdash$: f é um homomorfismo de R-álgebras

Sendo $\alpha = \sum\limits_{g,h} a_{gh}(g,h)$, $\beta = \sum\limits_{g',h'} b_{g'h'}(g'h')$ e $r \in R$, temos que

$$\begin{aligned}
f(\alpha\beta) &= f\left(\sum_{g,g',h,h'} a_{gh} b_{g'h'} (gg', hh') \right) \\
&= \sum_{h,h'} \left(\sum_{g,g'} a_{gh} b_{g'h'} gg' \right) hh' \\
&= \sum_{h,h'} \left(\left(\sum_{g \in G} a_{gh} g \right) \left(\sum_{g'} b_{g'h'} g' \right) \right) hh' \\
&= \left[\sum_{h \in H} \left(\sum_{g \in G} a_{gh} g \right) h \right] \left[\sum_{h'} \left(\sum_{g'} b_{g'h'} g' \right) h' \right] \\
&= f\left(\sum_{g,h} a_{gh}(g,h) \right) f\left(\sum_{g'h'} b_{g'h'}(g',h') \right) \\
&= f(\alpha) f(\beta).
\end{aligned}$$

$$\begin{aligned} f(r\alpha+\beta) &= f\left(\sum_{g,h}(ra_{gh}+b_{gh})(g,h)\right) \\ &= \sum_{h\in H}\left(\sum_{g\in G}(ra_{gh}+b_{gh})g\right)h \\ &= \sum_{h\in H}\left(\sum_{g\in G}ra_{gh}g+\sum_{g\in G}b_{gh}g\right)h \\ &= \sum_{h\in H}\left(r\sum_{g\in G}a_{gh}g\right)h+\sum_{h\in H}\left(\sum_{g\in G}b_{gh}g\right)h \\ &= r\sum_{h\in H}\left(\sum_{g\in G}a_{gh}g\right)h+\sum_{h\in H}\left(\sum_{g\in G}b_{gh}g\right)h \\ &= rf(\alpha)+f(\beta). \end{aligned}$$

Definindo $g : (RG)H \to R(G \times H)$, por

$$\sum_{h\in H}\left(\sum_{g\in G}a_{gh}gh\right) \mapsto \sum_{g,h}a_{gh}(g,h)$$

de modo similar ao que foi feito acima, provamos que g é um homomorfismo de R-álgebras e é a inversa de f. □

4.2 Ideais de Aumento

Definição 4.12. A aplicação

$$\varepsilon : RG \to R$$

definida por

$$\varepsilon(\alpha) = \varepsilon\left(\sum_{g\in G}a_g g\right) = \sum_{g\in G}a_g$$

é denominada **aplicação de aumento** de RG.

Além disso, o conjunto:

$$\Delta_R(G) = Ker(\varepsilon) = \left\{\alpha = \sum_{g\in G}a_g g \in RG \mid \sum_{g\in G}a_g = 0\right\}$$

é chamado **ideal de aumento** de RG.

Assim, para $H \leq G$, denotamos por $\Delta_R(G,H)$ o ideal à direita de RG gerado pelo conjunto $\{h-1 \mid h \in H\}$, ou seja

$$\Delta_R(G,H) = \left\{ \sum_{h\in H} a_h(h-1) \mid a_h \in RG \right\}.$$

Como trabalhamos com um anel R fixo, denotaremos, por fins de notação, esse ideal simplesmente por $\Delta(G,H)$.

Observação 4.13. *Note que o ideal $\Delta(G,G)$ coincide com o ideal de aumento $\Delta(G)$ definido acima.*

Proposição 4.14. *A aplicação de aumento $\varepsilon : RG \to R$ definida acima é um homomorfismo de anéis.*

Demonstração. Sejam $\alpha = \sum_{g\in G} a_g g,\ \beta = \sum_{g\in G} b_g g \in RG$ e $r \in R$. Assim, temos que:

$$\begin{aligned}
\varepsilon(\alpha+\beta) &= \varepsilon\left(\sum_{g\in G}(a_g+b_g)g\right) \\
&= \sum_{g\in G} a_g + b_g \\
&= \sum_{g\in G} a_g + \sum_{g\in G} b_g \\
&= \varepsilon(\alpha)\varepsilon(\beta)
\end{aligned}$$

$$\begin{aligned}
\varepsilon(\alpha\beta) &= \varepsilon\left(\sum_{g,h} a_g b_h gh\right) \\
&= \sum_{g,h} a_g b_h \\
&= \left(\sum_{g\in G} a_g\right)\left(\sum_{h\in H} b_h\right) \\
&= \varepsilon(\alpha)\varepsilon(\beta)
\end{aligned}$$

$$\begin{aligned}
\varepsilon(r\alpha) &= \varepsilon\left(\sum_{g\in G}(ra_g)g\right) \\
&= \sum_{g\in G} ra_g \qquad =
\end{aligned}$$

$$r\varepsilon(\alpha)$$

□

Proposição 4.15. *O conjunto* $\{g-1 \mid g \in G, g \neq e\}$ *é uma base de* $\Delta(G)$ *sobre* R.

Demonstração. Dado $\alpha \in Ker(\varepsilon)$, então $\sum_{g\in G} a_g = 0$. Dessa forma, podemos escrever:

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1).$$

Como todo elemento da forma $g-1$ pertence a $\Delta(G)$, o que nos mostra que o conjunto $\{g-1 \mid g \in G, g \neq e\}$ é um conjunto de geradores de $\Delta(G)$.

A independência linear segue por argumentos usuais. □

Agora, daremos uma melhor descrição de $\Delta(G,H)$, em especial, quando $H \triangleleft G$:

Definição 4.16. Seja $\Gamma = \{q_i\}_{i\in I}$ um conjunto completo de representantes das classes laterais à esquerda de H em G. Então, cada elemento $g \in G$ pode ser escrito de forma única como

$$g = q_i h_j,$$

onde $q_i \in \Gamma$ e $h_j \in H$.

Proposição 4.17. *O conjunto* $B_H = \{q(h-1) \mid q \in \Gamma,\ 1 \neq h \in H\}$ *é uma base para* $\Delta(G,H)$ *sobre* R.

Demonstração. Para isso verificaremos que B_H é linearmente independente e gera $\Delta(G,H)$.

$\vdash B_H$ é linearmente independente:

Suponha que

$$\sum_{i,j} r_{ij} q_i (h_j - 1) = 0,\ r_{ij} \in R.$$

Assim:

$$\sum_{i,j} r_{ij} q_i h_j - \sum_{i,j} r_{ij} q_i \ \Rightarrow\ \sum_{i,j} r_{ij} q_i h_j = \sum_i \left(\sum_j r_{ij} \right) q_i.$$

Como sabemos que $h_j \neq 1\ \forall j$ e os elementos de G são linearmente independentes sobre R, a equação acima só é possível se $r_{ij} = 0$ para todos valores de i e j.

$\vdash B_H$ gera $\Delta(G,H)$:

Para verificarmos essa propriedade, basta ver que todo elemento na forma $g(h-1),\ g \in G,\ h \in H$, pode ser escrito como combinação linear dos elementos de B_H. De fato, dado $g = q_i h_j$, para algum $q_i \in \Gamma$ e $h_j \in H$, então:

$$g(h-1) = q_i h_j (h-1) = q_i(h_j h - 1) - q_i(h_j - 1).$$

Dessa forma, concluímos o resultado. □

Observação 4.18. *No caso em que $H \triangleleft G$, o homomorfismo canônico $\omega : G \to G/H$ pode ser estendido para um epimorfismo $\omega^* : RG \to R(G/H)$ tal que*

$$\omega^* \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g \omega(g).$$

Proposição 4.19. *Se $H \triangleleft G$, então $Ker(\omega^*) = \Delta(G, H)$.*

Demonstração. Dado um elemento $\alpha \in RG$, o mesmo pode ser reescrito como uma soma finita

$$\alpha = \sum_{i,j} r_{ij} q_i h_j$$

em que $r_{ij} \in R, q_i \in \Gamma$ e $h_j \in H$.

Dessa forma, se denotarmos por $\overline{q_i}$ a imagem de q_i no grupo quociente G/H então temos

$$\omega^*(\alpha) = \sum_i \left(\sum_j r_{ij} \right) \overline{q_i}.$$

Como consequência, $\alpha \in Ker(\omega^*) \Leftrightarrow \sum_j r_{ij} = 0\ \forall i$.

Assim, se $\alpha \in Ker(\omega^*)$:

$$\begin{aligned} \alpha &= \sum_{i,j} r_{ij} q_i h_j \\ &= \sum_{i,j} r_{ij} q_i h_j - \sum_i \left(\sum_j r_{ij} \right) q_i \\ &= \sum_{i,j} r_{ij} q_i \left(h_j - 1 \right) \in \Delta(G, H) \end{aligned}$$

Portanto, $\mathrm{Ker}\,(\omega^*) \subset \Delta(G, H)$.

Para a outra inclusão basta observar que

$$\omega^*(h-1) = \omega(h) - \omega(1) = H - H = 0,\ \forall h \in H.$$

□

Corolário 4.20. *Seja $H \triangleleft G$. Então, $\Delta(G,H)$ é um ideal bilateral de RG e*

$$\frac{RG}{\Delta(G,H)} \simeq R(G/H).$$

Demonstração. A demonstração segue da proposição anterior em conjunto com o Teorema do Isomorfismo. □

4.3 Semissimplicidade e o Teorema de Maschke

Definição 4.21. Seja X um subconjunto do anel de grupo RG. O anulador à esquerda de X é o conjunto

$$Ann_l(x) = \{\alpha \in RG \mid \alpha x = 0, \forall x \in X\}$$

similarmente definimos:

$$Ann_r(x) = \{\alpha \in RG \mid x\alpha = 0, \forall x \in X\}$$

Definição 4.22. Dado RG em um subconjunto finito X do grupo G, denotamos por $\hat{X}$ o elemento de RG:

$$\hat{X} = \sum_{x \in X} x.$$

Lema 4.23. *Seja H um subgrupo de um grupo G e R anel. Então, $Ann_r(\Delta(G,H)) \neq 0$ se, e somente se, H é finito. Nesse caso, teremos*

$$Ann_r(\Delta(G,H)) = \widehat{H} \cdot RG$$

Ademais, se $H \triangleleft G$, então o elemento $\widehat{H}$ é central em RG, ou seja

$$Ann_r(\Delta(G,H)) = Ann_l(\Delta(G,H)) = RG \cdot \widehat{H}$$

Demonstração. ($\Rightarrow$) Assuma que $Ann_r(\Delta(G,H)) \neq 0$ e escolha $\alpha = \sum_{g \in G} a_g g \neq 0$ em $Ann_r(\Delta(G,H))$.

Assim, para cada elemento $h \in H$ temos que $(h-1)\alpha = 0$, então $h\alpha = \alpha$. Isto é,

$$\alpha = \sum_{g \in G} a_g g = \sum_{g \in G} a_g (hg).$$

Considere $g_0 \in \text{supp}(\alpha)$. Então, $\alpha_{g_0} \neq 0$, e assim a equação acima mostra que $hg_0 \in \text{supp}(\alpha)$ para todo $h \in H$. Além disso, já que $\text{supp}(\alpha)$ é finito, por definição, temos que H tem que ser finito.

($\Leftarrow$) Supondo que H seja finito, digamos $|H| = n$.

Note que sempre que $g_0 \in \text{supp}(\alpha)$, então o coeficiente de todo elemento da forma hg_0 é igual ao coeficiente de g_0, ou seja:

$$\alpha h_1 = \alpha$$
$$\alpha h_2 = \alpha$$
$$\vdots$$
$$\alpha h_n = \alpha$$

Daí:

$$n\alpha(h_1 + h_2 + \cdots + h_n) = n\alpha \Rightarrow \alpha(h_1 + h_2 + \cdots + h_n) = \alpha \Rightarrow \alpha\widehat{H} = \alpha$$

então podemos escrever α na forma:

$$\alpha = a_{g_0}\widehat{H}g_0 + a_{g_1}\widehat{H}g_1 + \cdots + a_{g_t}\widehat{H}g_t = \widehat{H}\beta, \beta \in RG.$$

Isso mostra que, se H é finito, então $Ann_r\Delta(G, H)) \subset \widehat{H} \cdot RG$.

A inclusão reversa é trivial a partir disso, já que $h\widehat{H} = \widehat{H}$ implica que $(h-1)\widehat{H} = 0$ para todo $h \in H$.

Sendo assim, se $H \triangleleft G$, para qualquer $g \in G$ temos que $g^{-1}Hg = H$. Então

$$g^{-1}\widehat{H}g = \sum_{x\in H} g^{-1}xg = \sum_{x\in H} x = \widehat{H}$$

. Dessa forma, $\widehat{H}g = g\widehat{H}$, para todo $g \in G$, o que mostra que $\widehat{H}$ é central em G. Consequentemente, $RG \cdot \widehat{H} = \widehat{H} \cdot RG$. □

Corolário 4.24. *Seja G grupo finito, então:*

i. $Ann_r(\Delta(G)) = Ann_l(\Delta(G)) = R \cdot \widehat{G}$

ii. $Ann_r(\Delta(G)) \cap \Delta(G) = \{a\widehat{G} \mid a \in R,\ a|G| = 0\}$.

Demonstração. i. pra a primeira afirmação basta tomar $H = G$ e o resultado segue.

ii. Para a segunda, note que $\alpha = a\widehat{G} \in \Delta(G) \Leftrightarrow \varepsilon(\alpha) = a\varepsilon(\widehat{G}) = a|G| = 0$.

□

Lema 4.25. *Seja I um ideal bilateral do anel R. Supondo que exista um ideal à esquerda J tal que $R = I \oplus J$ (como R-módulos à esquerda). Então $J \subset Ann_r(I)$*

Demonstração. Sejam $x \in J$ e $y \in I$. Como I é um ideal bilateral, J um ideal à esquerda e $R = I \oplus J$, temos que

$$yx \in J \cap I = (0) \Rightarrow yx = 0 \Rightarrow x \in Ann_r(I).$$

□

Lema 4.26. *Se o ideal de aumento $\Delta(G)$ é um somando direto de RG, como RG-módulo, então G é finito e $|G|$ é invertível em R.*

Demonstração. Assumindo que $\Delta(G)$ é somando direto de RG, o lema anterior mostra que $Ann_r(\Delta(G)) \neq 0$, já que sendo J ideal à esquerda tal que $R = \Delta(G) \oplus J$, então teremos $J \subset \Delta(G)$.

Sendo $RG = \Delta(G) \oplus J$ e $1 = e_1 + e_2$ com $e_1 \in \Delta(G)$ e $e_2 \in J$, temos que $1 = \varepsilon(1) = \varepsilon(e_1) + \varepsilon(e_2)$. Já que $e_2 = a\widehat{G}$, para algum $a \in R$, temos que $a\varepsilon(\widehat{G}) = 1$; então, $a|G| = 1$. Isso mostra que $|G|$ é invertível em R e que $|G|^{-1} = a$.

□

Teorema 4.27 (Maschke)**.** *Seja G um grupo. Então o anel de grupo RG é semissimples se, e somente se, as seguintes condições forem satisfeitas:*

i. R é anel semissimples.

ii. G é finito.

iii. $|G|$ é invertível em R.

Demonstração. ($\Rightarrow$) Assumindo que RG seja semissimples, sabemos que $R \simeq RG/\Delta(G)$ (como R-módulos), e já que anéis quocientes de anéis semissimples são semissimples, a afirmação *i* segue.

Como a semissimplicidade de RG implica que $\Delta(G)$ é somando direto, *ii* e *iii* seguem do Lema 4.26.

($\Leftarrow$) Suponha *i*, *ii* e *iii*, e seja M um RG-submódulo de RG. Já que R é semissimples, segue que RG é semissimples como R-módulo.

Logo, existe um R-submódulo N de RG tal que

$$RG = M \oplus N,$$

como R-módulos.

Seja $\pi : RG \to M$ a projeção canônica associada a soma direta. Queremos definir uma aplicação a fim de termos um RG-homomorfismo de RG em RG com imagem M, para isso consideremos a seguinte função:

$$\pi^*(x) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gx),\ \forall x \in RG.$$

Provaremos que π^* é RG-homomorfismo. Tome $x, y \in RG$ e $a \in G$, daí:

$$\begin{aligned}\pi^*(x+y) &= \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(g(x+y)) \\ &= \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gx+gy) \\ &= \frac{1}{|G|}\sum_{g\in G} g^{-1}(\pi(gx)+\pi(gy)).\end{aligned}$$

$$\begin{aligned}\pi^*(x)+\pi^*(y) &= \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gx) + \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gy) \\ &= \frac{1}{|G|}\left(\sum_{g\in G} g^{-1}\pi(gx) + \sum_{g\in G} g^{-1}\pi(gy)\right) \\ &= \frac{1}{|G|}\sum_{g\in G} g^{-1}(\pi(gx)+\pi(gy)).\end{aligned}$$

Além disso,

$$\pi^*(ax) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gax) = \frac{1}{|G|}\sum_{g\in G}(aa^{-1})g^{-1}\pi(gax) = \frac{a}{|G|}\sum_{g\in G}(ga)^{-1}\pi((ga)x).$$

Quando g percorre os elementos em G, o produto ga também percorre os elementos de G, logo:

$$\pi^*(ax) = a\frac{1}{|G|}\sum_{t\in g} t^{-1}\pi(tx) = a\pi^*(x)$$

Portanto, π^* é RG-homomorfismo. Agora, provaremos que $(\pi^*)^2 = \pi^*$:

Já que π é uma projeção em M, então $\pi(m) = m,\ \forall m \in M$. De igual modo, já que M é um RG-módulo, temos que $gm \in M\ \forall g \in G$. Portanto:

$$\pi^*(m) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gm) = \frac{1}{|G|}\sum_{g\in G} g^{-1}gm = m,$$

ou seja, $\pi^*(\pi^*(m)) = \pi^*(m) \Rightarrow (\pi^*)^2 = \pi^*$, como queríamos.

Agora, temos que π^* é RG-homomorfismo e projeção, ou seja, é endomorfismo. Mais ainda, sendo $Ker\pi^* = W$, temos que W é RG-submódulo de RG e daí, $RG = M \oplus W$ e o resultado segue.

□

Exemplo 4.28. *Seja $G = S_3$ com $V = \langle v_1, v_2, v_3\rangle$ sendo o módulo de permutação para G sobre K. Defina*

$$u = v_1 + v_2 + v_3 \quad e \quad U = \langle u\rangle.$$

Então U é um KG-submódulo de V, já que $ug = u$ para todo $g \in G$.

Existem vários subespaços de V tais quais $V = U \oplus W$, por exemplo $\langle v_2, v_3\rangle$ e $\langle v_1, v_2 - 2v_3\rangle$. Mas existe, de fato, apenas um KG-submódulo W de V com $V = U \oplus W$. Utilizaremos o Teorema de Maschke para encontrar esse W.

Primeiramente, considere $W_0 = span\{v_1, v_2\}$. Então $V = U \oplus W_0$ (porém, W_0 não é um FG-submódulo). A projeção ϕ em U é dada por

$$\phi : v_1 \to 0, v_2 \to 0, v_3 \to v_1 + v_2 + v_3$$

Agora, do Teorema de Maschke temos:

$$\pi^* : v_i \to \frac{1}{3}(v_1 + v_2 + v_3) \quad (i = 1, 2, 3)$$

Dessa forma, W será exatamente $Ker\pi^*$, ou seja

$$W = span\{v_1 - v_2, v_2 - v_3\}.$$

Corolário 4.29. *Seja G um grupo finito e seja K um corpo. Então, KG é semissimples se, e somente se, $char(K) \nmid |G|$.*

Demonstração. Como K é corpo, temos que K é sempre semissimples e $|G|$ é invertível em K se, e somente se, $|G| \neq 0$ em K, isto é, se, e somente se, $char(K) \nmid |G|$. □

Teorema 4.30 (Wedderburn-Artin Generalizado)**.** *Seja G um grupo finito e seja K um corpo tal que $char\ (K) \nmid |G|$. Então:*

i. KG é uma soma direta de um número finito de ideais bilaterais $\{B_i\}_{1\leq i\leq r}$, as componentes simples de KG.

ii. Qualquer ideal bilateral de KG é soma direta de membros da família $\{B_i\}_{1\leq i\leq r}$.

iii. Cada componente simples B_i é isomorfa ao anel de matrizes completas da forma $M_{n_i}(D_i$, em que D_i é anel de divisão contendo uma cópia de K no seu centro, e o isomorfismo.

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$$

é isomorfismo de K-álgebras.

iv. Em cada anel de matrizes $M_{n_i}(D_i)$, o conjunto

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \dots & 0 \\ x_2 & 0 & \dots & 0 \\ & & \dots & \\ x_{n_i} & 0 & \dots & 0 \end{bmatrix} \;\middle|\; x_1, x_2, \dots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

é ideal minimal à esquerda.

Dado $x \in KG$, consideramos $\phi(x) = (\alpha_1, \dots, \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$ e definimos o produto de x por um elemento $m_i \in I_i$ por $xm_i = \alpha_i m_i$. A partir dessa definição, I_i se torna um KG -módulo simples.

v. $I_i \not\simeq I_j$ se $i \neq j$.

vi. Qualquer KG-módulo simples é isomorfo a algum $I_i, 1 \leq i \leq r$.

Corolário 4.31. *Sejam G um grupo finito de ordem n, K um corpo algebricamente fechado tal que $char(K) \nmid |G|$. Então*

$$KG \simeq M_{n_1}(K) \oplus M_{n_2}(K) \oplus \cdots \oplus M_{n_r}(K)$$

onde $n = n_1^2 + n_2^2 + \cdots + n_r^2$.

Demonstração. Pelo Teorema de Maschke, KG é anel semissimples. Do Teorema de Wedderburn-Artin, segue que

$$KG \simeq M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_r}(D_r)$$

sendo $D_i = End_{KG}(V_i)$ anel de divisão e V_i módulo simples sobre KG. Assim, D_i possui dimensão finita sobre K, e daí, temos que $D_i = K$, pois K é algebricamente fechado. Portanto,

$$KG \simeq M_{n_1}(K) \oplus M_{n_2}(K) \oplus \cdots \oplus M_{n_r}(K)$$

como queríamos. Além disso, computando dimensões sobre K, obtemos do isomorfismo acima que

$$|G| = \sum_{i=1}^{r} n_i^2 [K : K],$$

e assim:

$$n = n_1^2 + n_2^2 + \cdots + n_r^2.$$

□

Definição 4.32. Um KG-módulo V é dito **completamente redutível** (ou irredutível) se $V = U_1 \oplus \cdots \oplus U_r$, em que cada U_i é um KG-submódulo irredutível de V.

Teorema 4.33. *Se G é um grupo finito e K corpo tal que a ordem de G é invertível em K, então todo KG-módulo não nulo é completamente redutível.*

Demonstração. Seja V um KG-submódulo não nulo. A prova será feita por indução sobre a dimensão de V. Se $\dim V = 1$, o resultado vale, pois nesse caso, V já é irredutível.

Então, suponhamos que V seja redutível, ou seja, V possui um KG-submódulo não trivial U. Pelo Teorema de Maschke, existe um KG-submódulo W de forma que $V = U \oplus W$. Como $\dim U < \dim V$ e $\dim W < \dim V$, temos, por indução:

$$U = U_1 \oplus \cdots \oplus U_r \text{ e } W = W_1 \oplus \cdots \oplus W_s,$$

em que cada U_i e W_j são KG-submódulos irredutíveis, e assim:

$$V = U_1 \oplus \cdots \oplus U_r \oplus W_1 \oplus \cdots \oplus W_s.$$

□

Observação 4.34. *O teorema acima faz uma caracterização dos KG-módulos não nulos construídos a partir de um corpo K tal que a ordem de G é invertível em K, nos mostrando que sempre podemos escrevê-los como uma soma direta de submódulos irredutíveis.*

4.4 Álgebras de Grupo Abeliano

Nesta seção, abordaremos os anéis de grupo de um grupo abeliano finito G sobre um corpo K, tal que $char(K) \nmid |G|$, a fim de caracterizá-los por completo.

Primeiramente, tomaremos o caso em que G é cíclico, ou seja

$$G = \langle a \mid a^n = 1 \rangle,$$

e K é um corpo tal que $char(K) \nmid |G|$. Consideremos então

$$\begin{array}{rccc} \phi: & K[X] & \to & KG \\ & f & \mapsto & f(a) \end{array}$$

É fácil ver que ϕ é homomorfismo sobrejetor de anéis, daí

$$KG \simeq \frac{K[X]}{Ker\phi},$$

onde $Ker\phi = \{f \in K[X] \mid f(a) = 0\}$.

Como $K[x]$ é domínio de ideais principais, $Ker\phi$ é gerado por um polinômio mônico de menor grau f_0, tal que $f_0(a) = 0$. Note que o elemento a é levado em $X + (f_0) \in \dfrac{K[X]}{(f_0)}$.

Já que $a^n = 1$, $X^n - 1 \in Ker\phi$. Mais ainda, se $f = \sum_{i=0}^{r} k_i X^i$ é um polinômio de grau $r < n$, temos que $f(a) = \sum_{i=0}^{r} k_i a^i \neq 0$, pois os elementos $\{1, a, \ldots, a^r\}$ são linearmente independentes sobre K, ou seja, $Ker\phi = (X^n - 1)$ e assim

$$KG \simeq \frac{K[X]}{(X^n - 1)}.$$

Se escrevermos $X^n - 1 = f_1 f_2 \cdots f_t$ como sendo a decomposição de $X^n - 1$ como produto de polinômios irredutíveis em $K[X]$, este polinômio será separável (pois $char(K) \nmid n$), e assim $f_i \neq f_j$ se $i \neq j$. Usando o Teorema Chinês do Resto

$$KG \simeq \frac{K[X]}{(f_1)} \oplus \frac{K[X]}{(f_2)} \oplus \cdots \oplus \frac{K[X]}{(f_t)}.$$

E a partir desse isomorfismo,

$$a \mapsto (X + (f_1), \ldots, X + (f_t))$$

.

Agora, sendo ζ_i uma raiz de f_i, $1 \leq i \leq t$, temos

$$\frac{K[X]}{(f_i)} \simeq K(\zeta_i),$$

e, consequentemente,

$$KG \simeq K(\zeta_1) \oplus \cdots \oplus K(\zeta_t).$$

Já que todos elementos da forma ζ_i, com $1 \leq i \leq t$ são raízes de $X^n - 1$, acabamos de mostrar que KG é isomorfo a uma soma direta de extensões ciclotômicas de K e, de acordo com esse último isomorfismo:

$$a \mapsto (\zeta_1, \ldots, \zeta_t).$$

Exemplo 4.35. *Seja $G = \langle a \mid a^7 = 1 \rangle$ e $K = \mathbb{Q}$.*

Nesse caso, a decomposição de $X^7 - 1$ em $\mathbb{Q}[X]$ é

$$X^7 - 1 = (X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1).$$

Daí, sendo ζ uma raiz primitiva da unidade de ordem 7, temos:

$$\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta).$$

Teorema 4.36 (Perlis-Walker)**.** *Seja G grupo abeliano finito de ordem n, e seja K corpo tal que $char(K) \nmid n$. Então*

$$KG \simeq \oplus_{d|n} a_d K(\zeta_d),$$

onde ζ_d denota uma raiz primitiva da unidade de ordem d e

$$a_d = \frac{n_d}{(K(\zeta_d) : K)}.$$

Nessa fórmula, n_d denota o número de elementos de ordem d em G.

Demonstração. Ver ([2], p. 148). □

Corolário 4.37. *Seja G grupo abeliano de ordem n e K corpo tal que $char(K) \nmid n$. Se K contém uma raiz primitiva da unidade de ordem n, então*

$$KG \simeq \underbrace{K \oplus \cdots \oplus K}_{n}.$$

Demonstração. Se K contém uma raiz primitiva da unidade de ordem n, então $K(\zeta_d) = K \ \forall \ d|n$ e o corolário segue diretamente do teorema acima.

Para verificar que obtemos exatamente n somandos, basta computar as dimensões sobre K em ambos os lados da equação. □

Observação 4.38. *Se G e H são grupos isomorfos, como já vimos anteriormente, as álgebras de grupo KG e KH também são isomorfas, qualquer que seja K. Porém, a equivalência contrária nem sempre é verdade, pois como acabamos de ver, se G e H são grupos abelianos não isomorfos de ordem n e K é corpo tal que $char(K) \nmid n$, contendo uma raiz primitiva da unidade de ordem n do corolário acima segue que:*

$$KG \simeq \underbrace{K \oplus \cdots \oplus K}_{n} \simeq KH.$$

Finalizaremos o capítulo com um exemplo mais concreto sobre esta última afirmação.

Exemplo 4.39. *Sendo C_2 e C_4 os grupos cíclicos de ordem 2 e 4, respectivamente, então, para a álgebra de grupo complexa, teremos:*

$$\mathbb{C}(C_2 \times C_2) \simeq \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \simeq \mathbb{C}C_4.$$

Definição 4.40. Sejam G um grupo, R anel comutativo e $\{C_i\}_{i \in I}$ o conjunto de classes de conjugação de G. Para cada classe de conjugação C_i de G, definimos o elemento

$$\widehat{C_i} = \sum_{x \in C_i} x,$$

chamado **soma de classe** de G sobre R.

Teorema 4.41. *Seja G grupo e R anel comutativo. Então, o conjunto $\{C_i\}_{i \in I}$ de todas as somas de classe formam uma base para $Z(RG)$, o centro de RG sobre R.*

Demonstração. Seja

$$\widehat{C_i} = \sum_{x \in \mathscr{C}_i} x \in KG.$$

Assim, se $g \in G$, então $g^{-1}\widehat{C_i}g = \widehat{C_i}$, e disso segue que todos elementos $\widehat{C_i}$ estão no centro de KG. Mais ainda, como $\{\widehat{C_i}\} \in G$, segue que $\{\widehat{C_i}\}$ é um conjunto linearmente independente sobre K, já que é um subconjunto de uma base de KG. Finalmente, se $\sum_{g \in G} a_g g \in Z(KG)$, então para cada $h \in G$, temos

$$\sum_{g \in G} a_g g = h^{-1} \left(\sum_{g \in G} a_g g \right) h = \sum_{g \in G} a_g h^{-1} g h.$$

Ou seja, da unicidade da escrita dos elementos de KG, segue que $a_g = a_{h^{-1}gh}$, o que nos diz que $\sum_{g \in G} a_g$ é uma combinação linear dos elementos do conjunto $\{\widehat{C_i}\}$. Portanto, $\{\widehat{C_i}\}$ é uma base para $Z(KG)$. □

Proposição 4.42. *Seja G grupo finito e K corpo algebricamente fechado tal que $char(K) \nmid |G|$. Então, o número de componentes simples de KG é o número de classes de conjugação de G.*

Demonstração. Primeiramente, do Corolário 4.31, temos que

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(K) \quad \Rightarrow \quad Z(KG) \simeq \oplus_{i=1}^{r} Z(M_{n_i}(K)).$$

Além disso, em virtude do teorema acima, é suficiente mostrar que a dimensão de $Z(KG)$ sobre K é igual ao número de componentes simples de KG.

Note que

$$Z(M_{n_i}(K)) = \{kI \mid k \in K\}.$$

Daí,

$$Z(KG) \simeq \underbrace{K \oplus \cdots \oplus K}_{r \text{ vezes}}.$$

Dessa forma, segue do isomorfismo acima que $\dim Z(KG) = [Z(KG) : K] = r$. □

No capítulo seguinte, apresentaremos uma aplicação dos resultados apresentados acima a fim de computar a decomposição da álgebra de grupo $\mathbb{C}S_3$.

5 Uma Aplicação da Semissimplicidade

Para o desenvolvimento deste capítulo foram utilizadas as referências: [2], [7], [11].

5.1 Representações de Grupos

O conceito de representação de grupo começou a criar forma em 1879, quando no Colóquio de Matemática em Evanston, Illinois, o matemático Christian Felix Klein chamou atenção para a possibilidade de representar grupos abstratos através de um grupo de transformações lineares, ([2]).

Dessa forma, uma representação de um certo grupo G nos dá formas de visualizá-lo como um grupo de matrizes. Mais especificamente, uma representação é um homomorfismo que vai de G a um grupo de matrizes invertíveis.

Neste capítulo iremos definir e exemplificar a ideia de representação de grupos, além de fazer uma aplicação em conjunto com a semissimplicidade.

Definição 5.1. Seja G um grupo, R anel comutativo e e V um R-módulo livre de dimensão finita. A **representação** de G sobre R, com espaço de representação V, é um homomorfismo de grupos $T : G \to GL(V)$, em que $GL(V)$ denota o grupo de R-automorfismos de V. A dimensão de V determina o **grau** da representação T e será denotado por $deg(T)$.

Observação 5.2. *Para um elemento $g \in G$, denotamos por $T_g : V \to V$ o automorfismo correspondente sobre T. Dessa forma, se $g, h \in G$, teremos que $T_{gh} = T_g \circ T_h$. Além disso, $T_1 = I$.*

Definição 5.3. Seja G um grupo e R anel comutativo. A **representação matricial** de G sobre R de grau n é um homomorfismo de grupos $T : G \to GL(n, R)$.

Observação 5.4. *Se $T : G \to GL(V)$ é uma representação de G sobre R com espaço de representação V e consideramos o isomorfismo $\phi : GL(V) \to GL(n, R)$ associado a mesma base, então $\phi \circ T : G \to GL(n, R)$ é a representação matricial de G.*

Da mesma forma, dada a representação matricial $T : G \to GL(n, R)$, vemos que $\phi^{-1} \circ T : G \to GL(V)$ é a representação de G sobre R.

Exemplo 5.5 (Representação Trivial)**.** *Dado um grupo G e um anel comutativo R, a aplicação $T : G \to GL(n, R)$ que associa a todo elemento de G a matriz identidade de $GL(n, R)$ é chamada representação trivial de G sobre R de grau n.*

Exemplo 5.6 (Representação do Grupo de Klein)**.** *Seja G o grupo de Klein de 4 elementos, $\{1, a, b, ab\}$ com 3 elementos de ordem 2. É fácil ver que a aplicação $T : G \to GL(2, \mathbb{Z})$ dada por*

$$T(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix};\ T(a) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix};$$

$$T(b) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}; T(ab) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix};$$

é uma representação de G.

Exemplo 5.7 (Representação de Permutações)**.** *Seja S_n o grupo de permutação de ordem $n!$ e seja R um anel comutativo. Seja V um R-módulo livre de dimensão n com base $\{v_1, \cdots, v_n\}$.*

Agora, definimos a aplicação $T : S_n \to GL(V)$ da seguinte forma: para cada $\sigma \in S_n$, associamos a aplicação $T_\sigma \in GL(V)$ que age na base dada da seguinte forma:

$$T_\sigma(v_i) = v_{\sigma(i)}.$$

Já que cada T_σ leva base em base, da teoria de álgebra linear, segue que T_{sigma} é isomorfismo de V. Em particular, também é homomorfismo, e assim, uma representação de S_n.

Agora, se denotarmos por $A(\sigma)$ a matriz de representação associada a T_σ, teremos que a j-ésima coluna de $A(\sigma)$ é composta por $T_\sigma(v_j)$ escrita como combinação linear da base. Mas como $T_\sigma(v_j) = v_{\sigma(j)}$, segue que cada coluna da matriz será composta por entradas nulas, exceto na entrada $(\sigma(j), j)$, que será igual a 1.

Esta matriz definida acima é chamada matriz de permutação.

Exemplo 5.8 (Representação Regular)**.** *Seja G grupo finito de ordem n e seja R anel comutativo. Tome como espaço de representação o anel de grupo RG de G sobre R.*

Definimos a aplicação $T : G \to GL(RG)$ da seguinte forma: para cada elemento $g \in G$ associamos a aplicação linear T_g, a qual age na base dada através da multiplicação pela esquerda, ou seja, $T_g(g_i) = gg_i$. Dessa forma:

$$T_{gh}(y) = (gh)y = g(h(y)) = T_g T_h(y).$$

*Lembrando que os elementos de G formam uma base para RG sobre R, note que na matriz de representação com respeito a base $G = \{1 = g_1, \cdots, g_n\}$, a imagem de cada elemento $g \in G$ é uma **matriz de permutação**, pois como a operação será feita entre elementos do mesmo grupo e a base do espaço de representação também é formada pelos elementos do grupo, quando formos representar a imagem (que é de um elemento de G) na base também formada*

pelos elementos de G, obteremos coeficientes binários (0 ou 1).

Para exemplificar de forma mais visual, tome o grupo cíclico de ordem 3, $G = \{1, a, a^2\}$, o qual enumeraremos os elementos da seguinte forma: $g_1 = 1,\ g_2 = a,\ g_3 = a^2$. Daí:

$$ag_1 = a = g_2, \quad ag_2 = a^2 = g_3, \quad ag_3 = 1 = g_1.$$

E dessa forma, temos que

$$T_a(g_1) = g_2, \quad T_a(g_2) = g_3, \quad T_a(g_3) = g_1.$$

Consequentemente, a matriz associada a T_a na base dada é

$$\rho(a) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Assim sendo, se considerarmos G como o grupo de Klein $\{1, a, b, ab\}$, o qual podemos enumerar na forma $g_1 = 1$, $g_2 = a$, $g_3 = b$ e $g_4 = ab$, podemos escrever as matrizes ρ de modo similar ao que foi feito acima, a saber:

$$\rho(a) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},\ \rho(b) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},\ \rho(ab) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},\ \rho(1) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Em particular, se pegarmos um elemento $1 \neq g \in G$, para qualquer outro elemento $g_i \in G$, temos que $gg_1 \neq g_i$. Isso nos diz que $T_g(g_i) \neq g_i$, ou seja, os elementos da diagonal da matriz $\rho(g)$ são todos zero. Logo, se computarmos o traço de T_g, para $g \in G$, obtemos que $tr(T_g) = 0$, se $g \neq 1$ e $tr(T_1) = n = |G|$.

Exemplo 5.9 (Representação Regular de Grupos Cíclicos)**.** *Seja $G = \{1, a, \cdots, a^{m-1}\}$ o grupo cíclico de ordem m e seja K um corpo. Note que a matriz de representação $A : G \to GL(n, K)$ é completamente determinada pela matriz $A(a)$, correspondente ao gerador a de G, já que, se A for homomorfismo, devemos ter que $A(a^r) = A(a)^r$. Além disso, para verificar que A é realmente um homomorfismo de grupos, e consequentemente uma representação, basta ver que $A(a)^r = I$.*

Note que, do exemplo anterior, temos que a representação regular de G é dada por

$$\rho(a) = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ & & \cdots & & \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

Exemplo 5.10 (Representação dE D_8)**.** *Seja G o grupo diedral dado por $D_8 = \langle a, b : a^4 = b^2 = 1, b^{-1}ab = a^{-1}\rangle$. Definimos as matrizes A e B por:*

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

Note que as matrizes definidas acima cumprem as seguintes propriedades:

$$A^4 = B^2 = I, B^{-1}AB = A^{-1}$$

Agora, definimos a função $\rho : G \to \mathrm{GL}(2, K)$ a qual é dada por:

$$\rho : a^i b^j \to A^i B^j \quad (0 \leq i \leq 3, \quad 0 \leq j \leq 1)$$

Verificando que ρ é homomorfismo:

Suponha que $0 \leq r \leq 3,\ 0 \leq s \leq 1,\ 0 \leq t \leq 3,\ 0 \leq u \leq 1$. Então:

$$a^r b^s a^t b^u = a^i b^j$$

para i, j com $0 \leq i \leq 3,\ 0 \leq j \leq 1$. Mais ainda, i e j são determinados utilizando a relação abaixo repetitivamente:

$$a^4 = b^2 = 1, b^{-1}ab = a^{-1}.$$

Já que $x^4 = y^2 = 1,\ y^{-1}xy = x^{-1}$, podemos deduzir que

$$x^r y^s x^t y^u = x^i y^j$$

Desse modo,

$$\begin{aligned} \rho\left(a^r b^s a^t b^u\right) = \rho\left(a^i b^j\right) = x^i y^j = x^r y^s x^t y^u \\ = \rho\left(a^r b^s\right) \cdot \rho\left(a^t b^u\right). \end{aligned}$$

e assim segue que ρ é homomorfismo, e, consequentemente, uma representação de grau 4 de D_8 sobre K.

As matrizes g para $g \in D_8$ são dadas na seguinte tabela:

g	1	a	a^2	a^3
$\rho(g)$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$	$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

g	b	ab	a^2b	a^3b
$\rho(g)$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Exemplo 5.11 (Soma Direta de Representações)**.** *Sejam $T : G \to GL(V)$ e $S : G \to GL(W)$ duas representações de um grupo G sobre um anel comutativo R. Podemos definir uma nova representação de G sobre R, com espaço de representação $V \oplus W$, a qual chamaremos de soma direta das representações dadas e denotaremos $T \oplus S$ por*

$$(T \oplus S)_g = T_g \oplus S_g, \ \forall g \in G.$$

Se tomarmos $\{v_1, \ldots, v_n\}$ e $\{w_1, \ldots, w_m\}$ bases de V e W, respectivamente, e denotarmos por $g \mapsto A(g)$ e $g \mapsto B(g)$ as representações matriciais correspondentes nas suas respectivas bases, então a matriz associada a $T \oplus S$ com respeito à base $\{(v_1, 0), \ldots, (v_n, 0), (0, w_1), \ldots, (0, w_m)\}$ de $V \oplus W$ é dada por

$$g \mapsto \begin{bmatrix} A(g) & 0 \\ 0 & B(g) \end{bmatrix}$$

5.2 Representações Equivalentes

Seja $\rho : G \to GL(n, K)$ uma representação e T uma matriz invertível de tamanho $n \times n$ sobre K. Da teoria de álgebra linear, temos que, para todas matrizes $n \times n$ A e B, temos que:

$$(T^{-1}AT)(T^{-1}BT) = T^{-1}(AB)T.$$

Dessa forma, podemos utilizar esta propriedade para produzir uma nova representação σ a partir de ρ da seguinte forma:

$$\sigma = T^{-1}(\rho(g))T \ \forall g \in G.$$

Dessa forma, para todos $g, h \in G$,

$$\begin{aligned}\sigma(gh) &= T^{-1}(\rho(gh))T \\ &= T^{-1}(\rho(g)\rho(h))T \\ &= T^{-1}(\rho(g))T \cdot T^{-1}(\rho(h))T \\ &= \sigma(g)\sigma(h),\end{aligned}$$

e assim, concluímos que, σ é de fato uma representação.

Definição 5.12. Duas representações $T : G \to GL(V)$ e $S : G \to GL(W)$ de um grupo G sobre o mesmo corpo K, são ditas **equivalentes** se existe um isomorfismo $\phi : V \to W$ tal que $S_g = \phi \circ T_g \circ \phi^{-1}$, para todo $g \in G$.

Observação 5.13. *Em particular, se considerarmos a representação $T : G \to GL(V)$ de G sobre K e pegarmos duas bases diferentes para o espaço de representação V, obteremos duas representações diferentes, porém equivalentes.*

Definição 5.14. Duas matrizes de representação $A : G \to GL(n, K)$ e $B : G \to GL(n, K)$ de um grupo G sobre K são ditas **equivalentes** se existe uma matriz invertível $U \in GL(n, K)$ tal que $A(g) = UB(g)U^{-1}, \ \forall g \in G$.

Definição 5.15. Uma representação $T : G \to GL(V)$ de um grupo G sobre o corpo K, é chamada **irredutível** se V é não nulo e os únicos subespaços invariantes de V sobre T são os triviais, ou seja, $\{0\}$ e V. E a representação é chamada **redutível** se V contém um subespaço não trivial W que seja invariante sobre T.

Definição 5.16. A matriz de representação $T : G \to GL(V)$ de um grupo G sobre o corpo K, é chamada **redutível** se existe uma matriz $U \in GL(n, K)$ tal que $\forall g \in G$ temos que a matriz $UM(g)U^{-1}$ é da forma

$$UM(g)U^{-1} = \begin{bmatrix} A(g) & B(g) \\ 0 & C(g) \end{bmatrix}.$$

Definição 5.17. Uma representação $T : G \to GL(V)$ de um grupo G sobre um corpo K é chamada **completamente redutível** se, para todo subespaço W que seja invariante sobre T, existe um subespaço invariante W' tal que $V = W \oplus W'$.

Definição 5.18. Uma matriz de representação $M : G \to GL(n, K)$ é chamada **completamente redutível** se, sempre que M é equivalente a uma matriz de representação na forma

$$\begin{bmatrix} A(g) & B(g) \\ 0 & C(g) \end{bmatrix}$$

é também equivalente a uma matriz de representação na forma

$$\begin{bmatrix} A(g) & 0 \\ 0 & D(g) \end{bmatrix}$$

Exemplo 5.19. *Tome $G = D_8 = \langle a, b : a^4 = b^2 = 1, b^{-1}ab = a^{-1}\rangle$, e consideremos a representação ρ do Exemplo 5.10. Então $\rho(a) = A$ e $\rho(b) = B$, sendo:*

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

Assuma $K = \mathbb{C}$ e defina:

$$T = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}$$

Então

$$T^{-1} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}$$

De fato, T foi construída de forma que $T^{-1}AT$ é diagonal. Assim, temos:

$$T^{-1}AT = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad T^{-1}BT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

e dessa forma, obtemos uma representação σ de D_8 tal que

$$\sigma(a) = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \sigma(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

E assim, as representações ρ e σ são equivalentes (por construção).

Exemplo 5.20. *Seja $G = C_2 = \langle a : a^2 = 1\rangle$ e*

$$A = \begin{bmatrix} -5 & 12 \\ -2 & 5 \end{bmatrix}$$

Note $A^2 = I$. *De fato:*

$$\begin{bmatrix} -5 & 12 \\ -2 & 5 \end{bmatrix} \cdot \begin{bmatrix} -5 & 12 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} (25-24) & (60-60) \\ (10-10) & (-24+25) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Daí $\rho : 1 \to I, a \to A$ *é uma representação de* G.

Mais ainda, se

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

então

$$T^{-1}AT = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

e assim, obtemos uma representação σ *de* G *para a qual*

$$\sigma(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma(a) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

ou seja, σ *é equivalente a* ρ.

5.3 Representações de Grupos e Módulos

Nesta seção faremos uma conexão entre a teoria de representações de grupos e a teoria de módulos, sendo essa ligação obtida usando o conceito de anéis de grupo. Uma breve descrição desse desenvolvimento será trabalhada ao longo desta seção.

Proposição 5.21. *Dado* G *um grupo e* R *anel comutativo com unidade, existe bijeção entre representações de* G *sobre* R *e* RG*-módulos livres com posto finito sobre* R.

Demonstração. Dada uma representação $T : G \to GL(V)$ de G sobre R, fazemos a associação de T RG-módulo construído a partir de V, utilizando a mesma estrutura aditiva e definindo o produto de um elemento $v \in V$ pelo escalar $\alpha = \sum_{g \in G} a_g g \in RG$ por:

$$\alpha v = \left(\sum_{g \in G} a_g g \right) v = \sum_{g \in G} a_g T_g(v).$$

De igual modo, se tomarmos M como um RG-módulo de dimensão finita sobre R, definimos a representação de G sobre R associando a cada elemento $g \in G$ o R-automorfismo $T_g : M \to M$ dado por $T_g(m) = gm \ \forall m \in M$. □

Exemplo 5.22. *Seja G grupo finito e considere RG um módulo sobre si mesmo. Então ele possui posto finito $|G|$ sobre R. Dado $x \in G$, a representação $T_x : RG \to RG$ é dada por:*

$$T_x \left(\sum_{g \in G} a_g g \right) = x \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g xg$$

Isso significa que $x \in G$ age nos elementos da base $G = \{g_1, \ldots, g_n\}$ por multiplicação à esquerda.

Em outras palavras, a representação associada ao RG-módulo RG é a representação regular de G.

Proposição 5.23. *Seja G um grupo e R um anel comutativo. Então:*

i. Duas representações T e T' de G sobre R são equivalentes se, e somente se, os RG-módulos correspondentes são isomorfos.

ii. Uma representação é irredutível (ou completamente redutível) se, e somente se, os correspondentes RG-módulos são irredutíveis (ou completamente redutíveis).

Demonstração. Ver ([2], p. 171). □

Vale ressaltar que se um RG-módulo M admite decomposição em soma direta de submódulos tais que $M = \oplus_{i=1}^{t} M_i$, e, além disso, T e T_i denotarem as representações correspondentes a esses módulos de 1 até t, então $T = \oplus_{i=1}^{t} T_i$.

Recapitulando, no Corolário 4.24, como consequência do Teorema de Maschke, obtemos que se G é grupo finito e K corpo, tais que $char(K) \nmid |G|$, então KG é anel semissimples. Também, do Teorema 3.11, temos que todos os KG-módulos obtidos são semissimples. A partir dessas informações, segue diretamente que *todo* KG-módulo que tem dimensão finita sobre K pode ser escrito como uma soma direta de módulos irredutíveis.

No âmbito das representações isso significa que, sobre as dadas hipóteses, toda representação de G sobre K é uma soma direta de representações irredutíveis. Dessa forma, para determinarmos todas representações de G sobre K, a menos de equivalência, é suficiente determinar todos os KG-módulos irredutíveis (a menos de isomorfismo).

Relembremos agora, que o Teorema 4.30 (generalização do teorema de Wedderburn-Artin para K-álgebras) nos diz que o número de KG-módulos irredutíveis não isomorfos é dado pelo

número de componentes simples de KG em sua decomposição e, mais ainda, que esse número é dado pela estrutura de KG. Ou seja, se escrevermos KG na forma

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$$

em que $D_i, 1 \leq i \leq r$ são anéis de divisão contendo K no centro. Computando as dimensões de ambas estruturas, teremos:

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : K]$$

Também sabemos que o módulo irredutível I_i, correspondente à componente simples $M_{n_i}(D_i)$, é isomorfo a $D_i^{n_i}$. Como sabemos, o grau de uma representação é dado pela dimensão do módulo correspondente sobre K, nós temos:

$$deg(T_i) = [D_i^{n_i} : K] = n_i [D_i : K]$$

e dessa forma:

$$|G| = \sum_{i=1}^{r} n_i deg(T_i).$$

A fim de ilustrar o desenvolvimento feito, fecharemos esta seção com alguns exemplos.

Exemplo 5.24 (Representação do Grupo Cíclico de Ordem 7)**.** *Mostramos, no Exemplo 4.35, que se $G = \langle a \rangle$ denota o grupo cíclico de ordem 7, então*

$$\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta)$$

onde ζ denota a sétima raiz primitiva da unidade, ou seja, a raiz da equação $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = 0$. Então, os componentes simples de $\mathbb{Q}G$ são anéis de matrizes 1×1 sobre os anéis $\mathbb{Q}$ e $\mathbb{Q}(\zeta)$, respectivamente. Então existem apenas duas representações irredutíveis não equivalentes S e T de G sobre $\mathbb{Q}$, de graus

$$deg(S) = [\mathbb{Q} : \mathbb{Q}] = 1, \quad deg(T) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 6.$$

Dado que representações unidimensionais são equivalentes se e somente se elas forem iguais e já que cada grupo admite a representação trivial $S : G \to GL(1, \mathbb{Q})$ dada por $S_g = 1, \forall g \in G$, tempos que essa é a única representação unidimensional de G sobre Q.

Para determinar T_a, de acordo com as considerações acima, devemos considerar o $\mathbb{Q}G$-módulo irredutível $I_2 = D_2^{n_2}$ correspondente à segunda componente simples de $\mathbb{Q}G$. Então, a representação $T : G \to GL(I_2)$ será dada por $T_a(v) = av, \forall v \in I_2$. Nesse caso, temos que $n_2 = 1$ e $D_2 = \mathbb{Q}(\zeta)$; portanto, podemos tomar $I_2 = \mathbb{Q}(\zeta)$, onde a multiplicação por um elemento $\alpha = (\alpha_1, \alpha_2) \in \mathbb{Q}G$ é dada por $\alpha v = \alpha_2 v, \forall v \in \mathbb{Q}(\zeta)$.

Agora, lembrando que o elemento $a \in \mathbb{Q}G$ corresponde, por isomorfismo, ao elemento $(1, \zeta) \in \mathbb{Q} \oplus \mathbb{Q}(\zeta)$, temos que

$$T_a(v) = av = \zeta v, \forall v \in \mathbb{Q}(\zeta)$$

Sendo assim, se tomarmos $\{1, \zeta, \zeta^2, \ldots, \zeta^5\}$ como uma base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$, então a matriz correspondente é dada por

$$A(a) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

Por outro lado, se usarmos o corpo dos complexos, de acordo com o Corolário 4.37, temos

$$\mathbb{C}G \cong \underbrace{\mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{\mathbf{7}\ \textit{vezes}},$$

então vemos que G admite sete representações não equivalentes de grau 1 sobre $\mathbb{C}$. Esses são os homomorfismos definidos enviando o gerador a em cada uma das sete raízes da unidade de ordem 7.

Exemplo 5.25 (Representações do Grupo Diedral de Ordem 8)**.** *Mostramos no Exemplo 5.10 que o grupo D_8 admite quatro representações diferentes de grau 1 e uma representação W de grau 2 sobre $\mathbb{Q}$. Então existem quatro componentes isomórficas simples para $\mathbb{Q}$. Seja $M_n(D)$ o componente simples correspondente à representação de grau 2. Já que $2 = deg(W) = n[D : \mathbb{Q}]$ devemos ter que ou $n = 1$ e $[D : \mathbb{Q}] = 2$ ou $n = 2$ e $[D : \mathbb{Q}] = 1$.*

No primeiro caso, vemos que $\mathbb{Q}D_8$ deve ser da forma

$$\mathbb{Q}D_8 \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus D \oplus D'.$$

onde D' também precisa ser o anel de divisão, com $[D' : \mathbb{Q}] = 2$. Assim, vemos que o anel de divisão de dimensão 2 sobre o corpo tem que ser comutativo, o que implica que $\mathbb{Q}D_8$ é comutativo; uma contradição, dado que D_8 é não abeliano. Consequentemente, devemos ter que $n = 2$ e $D = \mathbb{Q}$. Portanto,

$$\mathbb{Q}D_8 \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}).$$

Dado que as representações mencionadas também são representações irredutíveis de D_8 sobre $\mathbb{C}$, o mesmo argumento mostra que

$$\mathbb{C}D_8 \simeq \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}).$$

Exemplo 5.26 (Representações do Grupo dos Quatérnios de Ordem 8)**.** *Seja $\{1, i, j, k\}$ denotar as unidades básicas dos quatérnios sobre o corpo dos números reais, que consideramos no capítulo anterior. É fácil de notar que o conjunto $\{\pm 1, \pm i, \pm j, \pm k\}$ forma um grupo não abeliano sobre*

multiplicação, que será denotado por K_8. Esse grupo também pode ser definido pelo grupo gerado por dois elementos a e b que satisfazendo as seguintes relações:

$$a^4 = 1, \quad a^2 = b^2, \quad bab^3 = a^3$$

(para verificar, tome $a = i$ e $b = j$). Podemos facilmente exibir novamente quatro representações diferentes de grau 1 de K_8, dados por

$$\begin{aligned} A(a) &= 1, & A(b) &= 1. \\ B(a) &= 1, & B(b) &= -1. \\ C(a) &= -1, & C(b) &= 1. \\ D(a) &= -1, & D(b) &= -1. \end{aligned}$$

Porém, não parece ser fácil determinar diretamente outra representação de K_8 sobre $\mathbb{Q}$, então temos que tomar uma abordagem diferente. Teremos que determinar primeiro a estrutura de $\mathbb{Q}K_8$ e então deduzir a partir de sua representação correspondente.

Note que o subgrupo dos comutadores de $G = K_8$ é $G' = \{1, a^2\}$ e que podemos escrever (vide Proposição 3.6.11, [2], p. 154):

$$\mathbb{Q}G \simeq \mathbb{Q}\left(G/G'\right) \oplus \Delta\left(G, G'\right).$$

Já que todo elemento em G/G' é da ordem 2, podemos verificar que:

$$\mathbb{Q}\left(G/G'\right) \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}.$$

Além disso, dado que $\{1, a, b, ab\}$ é a transversal de G' em G, a Proposição 4.17 mostra que $\{a^2 - 1, a\left(a^2 - 1\right), b\left(a^2 - 1\right), ab\left(a^2 - 1\right)\}$ é a base de $\Delta\left(G, G'\right)$ sobre $\mathbb{Q}$. Queremos mostrar que $\Delta\left(G, G'\right)$ é isomorfo ao anel $\mathbf{H}_{\mathbb{Q}}$ dos quatérnios sobre o corpo dos números racionais:

$$\mathbf{H}_{\mathbb{Q}} = \left\{x_0 + x_1 i + x_2 j + x_3 k \mid x_0, x_1, x_2, x_3 \in \mathbb{Q}\right\}.$$

com as operações definidas na Seção 4.1. Para fazermos isso, considere os elementos $e_0 = \frac{1}{2}\left(1 - a^2\right), \quad e_1 = \frac{a}{2}\left(1 - a^2\right), e_2 = \frac{b}{2}\left(1 - a^2\right), e_3 = \frac{ab}{2}\left(1 - a^2\right)$. Uma conta direta mostra que $\{e_0, e_1, e_2, e_3\}$ também é a base de $\Delta\left(G, G'\right)$ sobre Q e que esses elementos satisfazem as mesmas relações que o conjunto $\{1, i, j, k\}$. Sendo assim, a aplicação linear $\phi : \Delta\left(G, G'\right) \to \mathbf{H}_{\mathbb{Q}}$ definido nessa base por $\phi\left(e_o\right) = 1, \phi\left(e_1\right) = i, \phi\left(e_2\right) = j, \phi\left(e_3\right) = k$ é um isomorfismo de $\mathbb{Q}$-álgebras. Então, mostramos que

$$\mathbb{Q}K_{\mathbf{8}} \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbf{H}_{\mathbb{Q}}.$$

As primeiros quatro componentes simples nos mostram que K_8 tem quatro representações não-equivalentes 1-dimensional; essas são, precisamente, as representações dadas no início desse exemplo. Para determinar a representação correspondente à quinta componente simples, notamos que $n_5 = 1$ e $D_5 = \mathbf{H}_{\mathbb{Q}}$ e assim podemos tomar $D_5 = \mathbf{H}_{\mathbb{Q}}$ como um $\mathbb{Q}K_8$-módulo irredutível. A ação da representação de a e b com respeito à base $\{e_0, e_1, e_2, e_3\}$ então é dada por:

$$ae_0 = e_1, \quad ae_1 = -e_0, \quad ae_2 = e_3, \quad ae_3 = -e_2$$
$$be_0 = e_2, \quad be_1 = -e_3, \quad be_2 = -e_0, \quad be_3 = e_1$$

Então, as representações matriciais são:

$$a \mapsto \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}$$

Agora precisamos determinar a estrutura de $\mathbb{C}K_8$. Para fazermos isso, precisamos notar que, já que quatro representações de dimensão 1 que demos também são representações de K_8 sobre $\mathbb{C}$, então $\mathbb{C}K_8$ contém pelo menos quatro componentes simples que são isomorfas a $\mathbb{C}$. Mostramos, durante a prova da Proposição 4.42 que, já que $\mathbb{C}$ é algebricamente fechado, todos os componentes simples devem ser anéis de matrizes com entradas no próprio corpo $\mathbb{C}$. Relembrando que $[\mathbb{C}K_8 : \mathbb{C}] = 8$, vemos que as únicas possibilidades são

$$\mathbb{C}K_8 \simeq \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$$

e

$$\mathbb{C}K_8 \simeq \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}).$$

Dado que a primeira possibilidade implicaria que $\mathbb{C}K_8$ é comutativo, segue-se que a segunda possibilidade é a correta. Também era possível chegar nessa conclusão se observássemos que K_8 contém cinco classes de conjugação e portanto $\mathbb{C}K_8$ obrigatoriamente terá exatamente cinco componentes simples.

É interessante notar que, apesar de $\mathbb{Q}D_4 \not\simeq \mathbb{Q}K_8$, obtivemos que $\mathbb{C}D_4 \simeq \mathbb{C}K_8$.

5.4 Representações Irredutíveis de S_3 sobre $\mathbb{C}$

Nesta seção apresentaremos um exemplo de aplicação da semissimplicidade juntamente com o Teorema de Maschke, classificando as representações irredutíveis de S_3, o grupo das permutações de três elementos, sobre o corpo $\mathbb{C}$.

Como visto previamente, $|S_3| = 6$, sendo

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}.$$

Porém, também podemos identificar o S_3 por seus geradores, isto é,

$$S_3 = \langle \sigma, \tau \mid \sigma^3 = (1),\ \tau^2 = (1),\ \sigma\tau = \tau\sigma^2 \rangle,$$

ou seja:

$$S_3 = \{I,\ \sigma,\ \sigma^2,\ \tau,\ \sigma\tau,\ \sigma^2\tau\}.$$

Lembramos ainda da teoria de grupos que S_3 possui um subgrupo normal $N = \langle\sigma\rangle$. Além disso, como elementos conjugados em S_n possuem a mesma estrutura de ciclos, segue que existem 3 classes de conjugação em S_3, a saber,

$$\begin{aligned} C_1 &= \{I\}; \\ C_2 &= \{(12), (13), (23)\}; \\ C_3 &= \{(123), (132)\}. \end{aligned}$$

Do Corolário 4.31 e da Proposição 4.42 obtemos que

$$\mathbb{C}S_3 \simeq M_{n_1}(\mathbb{C}) \oplus M_{n_2}(\mathbb{C}) \oplus M_{n_3}(\mathbb{C})$$

com $6 = n_1^2 + n_2^2 + n_3^2$. Como $\mathbb{C}S_3$ não é comutativo, não poderíamos ter um isomorfismo com uma soma direta de componentes comutativos. Daí, segue que pelo menos um dos índices n_i deve ser diferente de 1. Portanto, $n_1 = n_2 = 1$ e $n_3 = 2$, o que nos diz que S_3 possui duas representações irredutíveis unidimensionais e uma bidimensional. Assim, podemos melhor escrever a decomposição de $\mathbb{C}S_3$ na forma

$$\mathbb{C}S_3 \simeq \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}).$$

Representações de Grau 1 de S_3 sobre $\mathbb{C}$

- **Primeira representação:**

  Para encontrarmos as representações de grau 1 de S_3 sobre $\mathbb{C}$, tomamos V um $\mathbb{C}$-espaço vetorial unidimensional, digamos $V = \mathbb{C}v$.

  Note que a ação trivial $\rho : G \to GL_1(V)$, dada por $\rho_g = id_V,\ \forall g \in S_3$ é uma representação linear natural de S_3 sobre $\mathbb{C}$.

- **Segunda Representação:**

  Agora, sendo $N = \langle\sigma\rangle$ o subgrupo normal de índice 2, definimos então $\rho : S_3 \to GL_1(V)$, por

$$\rho_g = \begin{cases} id_V, & g \in N \\ -id_V, & g \notin N \end{cases}$$

  Assim, se $g, h \in S_3$, com $gh \in N$ então:

$$\begin{cases} g, h \in N \Rightarrow \rho_{gh} = id_V = \rho_g \circ \rho_h \\ g, h \notin N \Rightarrow \rho_{gh} = id_V = \rho_g \circ \rho_h \end{cases}$$

Deste modo, ρ é uma representação linear de S_3 sobre $\mathbb{C}$

Representações de Grau 2 de S_3 sobre $\mathbb{C}$

Sendo $\omega \in \mathbb{C}$ uma raiz cúbica primitiva da unidade, então

$$x^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad y^3 = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Mais ainda, temos que:

$$\begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}.$$

Logo, a aplicação $\varphi : S_3 \to GL_2(\mathbb{C})$, induzida por

$$\tau \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ e } \sigma \mapsto \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$$

é homomorfismo de grupos.

Assim, tomando V um $\mathbb{C}$-espaço vetorial de dimensão 2, com base $\mathscr{B} = \{e_1, e_2\}$, podemos definir $\rho : S_3 \to GL_2(V)$, induzida por

$$\rho_x : e_1 \mapsto e_2, \quad \rho_x : e_2 \mapsto e_1, \quad \rho_y : e_1 \mapsto \omega e_1 \quad \text{e} \quad \rho_y : e_2 \mapsto \omega^2 e_2$$

Verificaremos agora que a representação acima é de fato irredutível. Para tanto, precisamos mostrar que não existe nenhum subespaço unidimensional de V que seja invariante pela ação linear de S_3 dada por:

$$\begin{cases} x \cdot e_1 = e_2 \star \\ x \cdot e_2 = e_1 \\ y \cdot e_1 = \omega e_1 \\ y \cdot e_2 = \omega^2 e_2 \end{cases}$$

Note que $\mathbb{C}e_1$ não é fixo por x $(\star)$, ou seja, dado $W \subset V$ subespaço unidimensional de V, existe $\lambda \in \mathbb{C}$ tal que $W = \mathbb{C}(e_1 + \lambda e_2)$

Se W fosse invariante, teríamos:

$$x \cdot (e_1 + \lambda e_2) = e_1 + \lambda e_2 \in \mathbb{C}(e_1 + \lambda e_2).$$

Segue que existe $\alpha \in \mathbb{C}$ tal que $e_1 + \lambda e_2 = \alpha(e_1 + \lambda e_2) \Rightarrow \alpha = \lambda = 1$ ou $\alpha = \lambda = -1$.

Por outro lado, temos

$$y \cdot (e_1 + e_2) = \omega e_1 + \omega^2 e_2 \notin \mathbb{C}\,(e_1 + e_2)$$

e

$$y \cdot (e_1 - e_2) = \omega e_1 - \omega^2 e_2 \notin \mathbb{C}\,(e_1 + e_2)$$

o que é uma contradição. Ou seja, não existe nenhum subespaço unidimensional de V que seja fixo pela ação de S_3, isto é, V não possui nenhum $\mathbb{C}S_3$-submódulo próprio, o que implica em V ser um $\mathbb{C}S_3$-módulo simples e, por consequência, segue V é uma representação irredutível de grau 2 de S_3 sobre $\mathbb{C}$.

Dessa forma, concluímos a classificação das representações lineares irredutíveis de S_3 sobre $\mathbb{C}$.

6 Considerações finais

Neste trabalho, foi apresentada a teoria de semissimplicidade desde anéis e módulos até anéis e álgebras de grupo, com uma aplicação na teoria de representação de grupos, como proposto. Além disso, foi possível estabelecer uma conexão entre as áreas de Álgebra Abstrata e Álgebra Linear, fazendo correspondências entre a teoria de módulos e anéis de grupo com a teoria sobre espaços vetoriais. Mais especificamente, ao término deste trabalho, foi possível caracterizar anéis semissimples e suas diversas propriedades, decompondo-os em somas diretas de álgebras de matrizes sobre anéis de divisão, com base no Teorema de Wedderburn-Artin; caracterizar um anel de grupo RG, com relação à sua semissimplicidade, apenas tendo como informação a semissimplicidade de R e informações sobre a ordem de G, através do Teorema de Maschke e suas consequências, além de, por uma dessas consequências, descrever álgebras de grupo KG pela generalização do Teorema de Wedderburn-Artin; e, por fim, em conjunto com a teoria de representações, foram classificadas todas as representações irredutíveis da álgebra de grupo $\mathbb{C}S_3$.

Com relação a trabalhos futuros, uma questão muito interessante que este trabalho motiva, é o *Problema do Isomorfismo*. Vários pesquisadores como W. Burnside, G. Frobenius e I. Schur [2], estudaram sobre quais propriedades de um grupo finito G se refletem sobre o anel de grupo RG. Se dois grupos finitos são isomorfos, os seus anéis de grupo, determinados a partir de um mesmo anel de coeficientes, também o serão. Agora, o que os pesquisadores da área passaram a se questionar foi o seguinte: Se G é um grupo finito, H um outro grupo qualquer e R um anel com unidade tais que RG e RH são isomorfos, será que G e H também são isomorfos? Em 1940, G. Higman publicou o primeiro trabalho diretamente relacionado com este problema. Ele mostrou que se G é um grupo abeliano finito e $\mathbb{Z}G$ é isomorfo a $\mathbb{Z}H$, então G e H são isomorfos. Por outro lado, se G e H são grupos abelianos finitos de mesma ordem, mesmo não sendo isomorfos, suas álgebras de grupo são isomorfas sobre o corpo C dos números complexos. Este resultado mostra que o problema do isomorfismo, em

sua generalidade, tem resposta negativa ([12]), mas existem casos em que essa recíproca vale, e são para esses casos que o estudo do Problema do Isomorfismo é voltado.

Referências

1 SEHGAL, S. K. *Topics in Group Rings*. New York: Marcel Dekker Inc, 1978. Citado na página 1.

2 MILIES, C. P.; SEHGAL, S. K. *An Introduction to Group Rings*. Netherlands: Kluwer Academic Publishers, 2002. Citado 12 vezes nas páginas 1, 2, 10, 15, 19, 24, 30, 49, 52, 60, 63 e 68.

3 GONÇALVES, A. *Introdução à Álgebra*. Rio de Janeiro: IMPA, 2017. Citado na página 2.

4 ARNALDO, G.; YVES, L. *Elementos de Álgebra*. Rio de Janeiro: IMPA, 2001. Citado na página 2.

5 LANG, S. *Algebra, Graduate Texts in Mathematics, 211 (Revised third ed.)*. New York: Springer-Verlag, 2002. Citado na página 2.

6 ROTMAN, J. J. *An Introduction to the Theory of Groups*. New York: Wiley-Interscience, 2000. Citado na página 2.

7 SANT'ANA, A. *Uma Introdução ao Estudo dos Anéis Semissimples*. Rio de Janeiro: SBM, 2016. Citado 2 vezes nas páginas 15 e 52.

8 HUNGERFORD, T. W. *Algebra*. New York: Springer-Verlag, 1974. Citado na página 15.

9 SULEIMAN, F.; ABDULLAHI, S. *A STUDY ON WEDDERNBURN-ARTIN THEOREM FOR RINGS*. 2019. Citado na página 15.

10 HOFFMAN, K.; KUNZE, R.; WATANABE, R. *Álgebra Linear*. Rio de Janeiro: Livros Técnicos e Científicos, 1979. Citado na página 27.

11 GORDON, J.; MARTIN, L. *Representations and Characters of Groups*. London: Cambridge University Press, 2001. Citado 2 vezes nas páginas 30 e 52.

12 COSTA, V. P. *Conjecturas em Anéis de Grupo*. Tese (Mestrado) — UFES, Vitória, ES, Brasil, 2018. Citado 2 vezes nas páginas 30 e 69.

13 SANTOS, D. B. *O Problema de Isomorfismos em Anéis de Grupos sobre os Inteiros*. Tese (Mestrado) — UFPB, João Pessoa, PB, Brasil, 2003. Citado na página 30.