LUANA DEMARCHI GRASSI

ANÉIS SEMISSIMPLES E REPRESENTAÇÕES DE GRUPO

TOLEDO

2021

LUANA DEMARCHI GRASSI

ANÉIS SEMISSIMPLES E REPRESENTAÇÕES DE GRUPO

SEMISIMPLE RINGS AND GROUP REPRESENTATIONS

Trabalho de Conclusão de Curso de graduação apresentado como requisito para obtenção do título de Licenciado em Matemática da Universidade Tecnológica Federal do Paraná (UTFPR).

Orientador: Robson Willians Vinciguerra

TOLEDO

2021

LUANA DEMARCHI GRASSI

ANÉIS SEMISSIMPLES E REPRESENTAÇÕES DE GRUPO

Trabalho de Conclusão de Curso de graduação apresentado como requisito para obtenção do título de Licenciado em Matemática da Universidade Tecnológica Federal do Paraná (UTFPR).

Data de aprovação: 20 de agosto de 2021.

Robson Willians Vinciguerra
Doutor
Universidade Tecnológica Federal do Paraná

Ricardo Leite dos Santos
Doutor
Universidade Federal do Rio Grande

Wilian Francisco de Araujo
Doutor
Universidade Tecnológica Federal do Paraná

TOLEDO
2021

Este trabalho é dedicado aos meus pais,
Carmen e Ari...

Agradecimentos

Agradeço a Deus pela vida, pelo amor e por minhas conquistas. Sem Ele, eu nada teria alcançado.

Aos meus pais por sonharem junto comigo, por serem minha base, minhas raízes, mas sempre que me deram asas.

Ao meu namorado pela paciência, por acreditar em mim e por me incentivar.

Aos meus colegas e amigos de graduação, não há palavras para descrever a importância de vocês. Obrigada pelo apoio, risadas, conversas e estudos.

Ao meu orientador professor Robson, pelo bom exemplo, paciência, dedicação e ensinamentos.

Aos demais professores da graduação, por todos os ensinamentos, correções e contribuições.

Ao PICME (Programa de Iniciação Científica e Mestrado – OBMEP – CNPq), pela bolsa de iniciação científica que culminou neste trabalho.

"Apenas lembre-se de uma coisa, sempre mantenha uma mente aberta,
e ainda mais importante, um coração aberto,
e nunca esqueça que sempre há mais de um significado para tudo
e mais de uma resposta para toda pergunta. [...]
Coisas que parecem totalmente ilógicas
têm bastante sentido se forem encaradas do jeito certo."
(Colin Thompson)

Resumo

O presente trabalho objetiva apresentar a teoria de anéis semissimples, anéis de grupo e representações de grupo, de forma a possibilitar o cálculo e a obtenção de representações matriciais de grupos. Este estudo se justifica pela ausência de detalhamento dos exemplos apresentados na literatura, especialmente em língua portuguesa. Dessa forma, foi feita uma pesquisa bibliográfica em obras que contemplam este tema e foram desenvolvidos alguns exemplos de representações de grupo. Espera-se que este trabalho contribua para o crescimento acadêmico da autora e possa vir a ser um subsidio de estudo para outros acadêmicos que se interessem pelo tema.

Palavras-chave: Representação de Grupo. Anel Semissimples. Anel de Grupo.

Abstract

The present work aims to present the theory of semisimple rings, group rings and group representations, in order to enable the calculation and to obtain the matrix representations of groups. This study is justified by the lack of detailing on the examples presented in the literature, especially in Portuguese. Thus, a bibliographical research was carried out in works that contemplate this theme and some examples of group representations were developed. It is hoped that this work will contribute to the author's academic growth and may become a study subsidy for other academics interested in the subject.

Keywords: Group Representation. semisimple Ring. Group Ring.

Sumário

1 Introdução

O estudo da álgebra abstrata nos cursos de Licenciatura em Matemática costuma ser restrito a uma ou duas disciplinas obrigatórias, fazendo com que o aluno que se interesse por este tema busque estudá-lo por conta própria ou em programas de Iniciação Científica. A autora deste trabalho encontra-se no segundo grupo. Durante o estudo de Anéis Semissimples, Anéis de Grupo e Representações de Grupo, notou-se a falta de materiais que detalhassem demonstrações e exemplos, tornando difícil o estudo para um aluno com conhecimentos básicos de álgebra abstrata.

Especialmente no caso de representações, podemos encontrar vários livros, monografias e artigos com exemplos e demonstrações da teoria, mas é raro obter trabalhos em que a obtenção das representações irredutíveis estejam explicadas com clareza e detalhes. Desta forma, o objetivo do Trabalho de Conclusão de Curso é desenvolver um texto que apresente com os detalhes e explicações necessárias a Teoria de Representações de Grupos, de forma que um aluno na graduação em Matemática seja capaz de compreender e estudar.

Para tanto, seguimos a estrutura de estudo do livro An Introduction to Group Rings (Milies e Sehgal, 2002, [3]), iniciando com o estudo de Anéis, Anéis de Grupo e então o estudo de Representações de Grupo. Outros autores como Steinberg (2011) adotam outras abordagens, igualmente válidas.

De acordo com Steinberg (2011, p. 22, [5]), se $\phi : G \to GL(V)$ é uma representação não nula de um grupo G finito, então ϕ é irredutível ou decomponível em representações irredutíveis. Assim, para conhecer qualquer representação de grupo, precisamos apenas determinar as representações irredutíveis deste grupo.

Obter representações irredutíveis de grau 1 é uma tarefa simples, mas a medida em que aumentamos o grau da representação, esta tarefa se torna cada vez mais complexa. Muitas vezes pode-se saber várias informações sobre uma representação, como seu traço, sem realmente determinar esta representação. Neste trabalho, usaremos o conceito de Carácter de uma representação e os Diagramas de Young para calcular as representações de alguns grupos.

Cabe ainda destacar que a escolha de desenvolver o Trabalho de Conclusão de Curso na área de Álgebra Abstrata se deve aos sentimentos de curiosidade e admiração que este estudo provoca na autora.

De acordo com Gil (2017, [1]), esta pesquisa se classifica como básica pura, exploratória, quantitativa e emprega pesquisa bibliográfica como procedimento técnico.

O Capítulo 2 dedica-se a apresentação de definições e resultados básicos sobre anéis e módulos, é o capítulo dos pré-requisitos. O capítulo 3 trará o estudo dos anéis semissimples, destacando o Teorema de Wedderburn-Artin, que apresenta uma decomposição destes anéis. Já o capítulo 4 apresentará os anéis de grupo e as condições para que sejam semissimples, por meior do Teorema de Maschke. No capítulo 5 teremos o primeiro contato com as representações de grupo e alguns resultados que as relacionam aos anéis de grupo. Por fim, os capítulos 6 e 7 trazem os caracteres de grupo e os diagramas de Young como ferramentas para refinar a busca por representações irredutíveis.

2 ANÉIS, MÓDULOS E ÁLGEBRAS

Este primeiro capítulo busca estabelecer as definições básicas que serão utilizadas ao longo de todo o texto. Traremos também, alguns exemplos de forma a ilustrar esses resultados. Mais detalhes podem ser obtidos em (Milies e Sehgal, 2002, [3]) e (Steinberg, 2011, [5]).

2.1 Anéis

Definição 2.1.1 *Um conjunto não vazio R com operações*

$$\begin{array}{rccc} + : & R \times R & \longrightarrow & R \\ & (x, y) & \longmapsto & x + y \end{array} \qquad \begin{array}{rccc} \cdot : & R \times R & \longrightarrow & R \\ & (x, y) & \longmapsto & x \cdot y \end{array}$$

é um ***anel*** *se, para todo $x, y, z \in R$, satisfaz as seguintes propriedades:*

i. $x + (y + z) = (x + y) + z$;

ii. $x + y = y + x$;

iii. $\exists\, 0 \in R$ *tal que* $x + 0 = x = 0 + x$

iv. $\forall\, x \in R, \exists - x \in R$ *tal que* $x + (-x) = 0 = -x + x$;

v. $x(yz) = (xy)z$;

vi. $x(y + z) = xy + xz$;

vii. $(x + y)z = xz + yz$.

Se, além disso, em R ocorre que $xy = yx$, para todo $x, y \in R$, dizemos que R é um **anel comutativo**. Quando existir $1 \in R$ tal que $x1 = 1x = x$, para todo $x \in R$, dizemos que R é um **anel com identidade**. Os conjuntos numéricos $\mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$ são exemplos de anéis comutativos com identidade.

Definição 2.1.2 *Um elemento $a \in R$ é dito* ***inversível*** *ou uma* ***unidade*** *se existe $a^{-1} \in R$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. O conjunto $\mathbb{U}(R) = \{a \in R | a \text{ é inversível}\}$ é chamado de conjunto das unidades de R.*

Tomando o anel $GL(n, \mathbb{R})$ da matrizes inversíveis $n \times n$ com entradas em $\mathbb{R}$ e determinante não nulo, temos que todos os elementos não nulos são unidades. De fato,

$\mathbb{U}(M_n(R)) = GL(n, R)$. Anéis como $GL(n, \mathbb{R})$ recebem uma denominação especial, como vemos a seguir.

Definição 2.1.3 *Um anel em que todos os seus elementos não nulos são inversíveis é chamado de* ***anel de divisão****.*

Um anel de divisão que é comutativo é chamado de **corpo**. Alguns exemplos de corpos são: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ com as operações de adição e multiplicação usuais.

Definição 2.1.4 *A* ***característica*** *de um corpo K é o menor inteiro positivo m tal que $ma = \underbrace{a + \cdots + a}_{m \text{ vezes}} = 0$. Quando tal m não existe, dizemos que K tem característica 0.*

Os corpos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ têm característica 0. Já o conjunto $\mathbb{Z}_p$ dos inteiros módulo p, com p primo, possui característica p.

Veremos agora um tipo de subconjunto importante dos anéis: os ideais.

Definição 2.1.5 *Um subconjunto não vazio I de um anel R, é um* ***ideal*** *à esquerda se:*

(*i.*) $0 \in I$

(*ii.*) $\forall\, a, b \in I \Rightarrow a - b \in I$

(*iii.*) $\forall\, x \in R$ *e* $\forall\, a \in I \Rightarrow xa \in I$

A definição de ideal à direita é análoga. Um conjunto I é ideal bilateral, ou simplesmente ideal, quando I é ideal à esquerda e direita simultaneamente.

Dizemos que um ideal I de R é principal se $I = \{xa | x \in R\}$, para algum $a \in I$. Neste caso, denotamos $I = Ra$ ou $I = (a)$. Por exemplo, todos os ideais de $\mathbb{Z}$ são principais da forma $n\mathbb{Z} = \{nk \,|\, k \in \mathbb{Z}\}$, para algum $n \in \mathbb{Z}$.

Os conjunto $\{0\}$ e R são exemplos de ideais de R chamados de triviais. Dizemos que um ideal I é próprio quando I não é trivial.

Definição 2.1.6 *Anéis em que os únicos ideais são os triviais são chamados de* ***anéis simples****.*

Definição 2.1.7 *Um ideal $I \neq 0$ de R é chamado de* ***minimal****, quando dado um ideal J de R com $0 \subset J \subset I$ então $J = 0$ ou $J = I$.*

Claramente em um corpo K, K é um ideal minimal trivial.

Proposição 2.1.8 *Sejam I, J ideais de um anel R. Então $I + J = \{x + y | x \in I, y \in J\}$ é um ideal de R.*

Demonstração: Verificaremos as 3 condições para que $I + J$ seja ideal:

$(i.)$ $0 \in I + J$, pois $0 = 0 + 0 \in I + J$;

$(ii.)$ $\forall\, x_1 + y_1, x_2 + y_2 \in I + J \Rightarrow (x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) - (y_1 - y_2) \in I + J$;

$(iii.)$ $\forall\, r \in R$ e $\forall\, x + y \in I + j \Rightarrow r(x + y) = rx + ry \in I + J$.

O lado direito é análogo. Portanto, $I + J$ é um ideal. ■

Seja I um ideal do anel R. Definimos a seguinte relação

$$x, y \in R, \quad x \sim y(mod\ I) \Leftrightarrow x - y \in I.$$

Pode-se provar que esta é uma relação de equivalência, e portanto, reorganiza os elementos de R em classes da forma $\overline{x} = \{x + y | y \in I\} = x + I$. Além disso, ao definirmos as operações $\overline{x} + \overline{y} = \overline{x + y}$ e $\overline{x} \cdot \overline{y} = \overline{xy}$ para todo $x, y \in R$, temos que o conjunto quociente $\dfrac{R}{I} = \{\overline{x} | \overline{x} = x + I\}$ é um anel.

Por fim, quando R é comutativo, $\frac{R}{I}$ também é comutativo e se 1 é a identidade de R, então $\overline{1}$ é a identidade de $\frac{R}{I}$.

Definição 2.1.9 *O **centro** de um anel R é o subconjunto*

$$\mathcal{Z}(R) = \{a \in R | ax = xa \forall\, x \in R\}$$

Observe que, apesar de ser um subconjunto, o centro de um anel não é obrigatoriamente um ideal.

Veremos agora a definição e alguns resultados sobre homomorfismos, um tipo especial de funções entre anéis que preservam as operações dos anéis.

Definição 2.1.10 *Sejam R e S anéis. Uma relação $f : R \to S$ é chamada de **homomorfismo de anel**, se para todo $a, b \in R$ temos:*

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

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

Quando $f : R \to S$ é um homomorfismo de anéis, temos que $f(0) = 0$ e $f(-a) = -f(a)$. De fato,

$$0 = 0 + 0 \Rightarrow f(0) = f(0 + 0) = f(0) + f(0) \Rightarrow 0 + f(0) = f(0) + f(0) \Rightarrow f(0) = 0$$

e

$$a + (-a) = 0 \Rightarrow 0 = f(0) = f(a + (-a)) = f(a) + f(-a) \Rightarrow -f(a) = f(-a).$$

Definição 2.1.11 *Um homomorfismo de anéis $f : R \to S$ é chamado de:*

(*i*) *Epimorfismo, quando f é sobrejetor;*

(*ii*) *Monomorfismo, quando f é injetor;*

(*iii*) *Isomorfismo, quando f é bijetor;*

(*iv*) *Endomorfismo, quando $S = R$;*

(*v*) *Automorfismo, quando f é isomorfismo e endomorfismo ao mesmo tempo.*

Um exemplo clássico de homomorfismo de anéis é o Homomorfismo canônico $\omega : R \to \dfrac{R}{I}$, dado por

$$R \ni a \mapsto \omega(a) = \overline{a} = a + I$$

Este homomorfismo é claramente sobrejetivo, pois dado $\overline{x} \in \dfrac{R}{I}$ sempre existe $x \in R$ tal que $\omega(x) = \overline{x}$.

Apresentaremos agora um importante resultado sobre homomorfismos de anéis: o Teorema do Homomorfismo. Por meio deste teorema, conseguimos criar isomorfismos a partir de um homomorfismo qualquer.

Teorema 2.1.12 *Sejam $f : R \to S$ um homomorfismo de anéis. Então,*

$$\frac{R}{Ker(f)} \simeq Im(f)$$

Demonstração: A demonstração pode ser vista em (Gonçalves, 2017, p. 55, [2]). ■

2.2 Módulos

Falaremos agora de uma estrutura que pode ser vista como um generalização dos espaços vetoriais: os módulos. Enquanto os espaços vetoriais possuem operação produto por escalar definida sobre um corpo, nos módulos esta operação pode estar definida apenas sobre um anel.

Definição 2.2.1 *Chamamos de R-**módulo** a esquerda um grupo abeliano $(M, +)$ que possui a operação de multiplicação por escalar*

$$\begin{array}{rccc} \cdot : & R \times M & \longrightarrow & M \\ & (a, m) & \longmapsto & a \cdot m \end{array}$$

de forma que, para todo $a, b \in R$ e $m, n \in M$, satisfazem:

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

(*ii.*) $a(m+n) = am + an$

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

(*iv.*) $1m = m$.

Analogamente, podemos definir um R-módulo a direita. Veremos agora alguns subconjuntos importantes dos módulos.

Definição 2.2.2 *Chamamos de* ***submódulo*** *um subconjunto $N \subseteq M$ se N é um subgrupo aditivo de M e se, para todo $a \in R$ e $n \in N$, temos $an \in N$.*

Por exemplo, os subconjuntos $\{0\}$ e M são claramente submódulos de M, conhecidos como submódulos triviais. Um módulo em que os únicos submódulos são os triviais chamado de módulo simples.

Exemplo 2.2.3 *Seja R um anel. Podemos ver R como um R-módulo quando definimos a multiplicação por escalar como a própria multiplicação do anel. Neste caso, os submódulos são os ideais a esquerda.*

A primeira diferença entre módulos e espaços vetoriais diz respeito a base. Enquanto todos os espaços vetoriais possuem base, isso nem sempre ocorre com os módulos. Quando um R-módulo possui base dizemos que ele é um **R-módulo livre**.

Definição 2.2.4 *O conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é chamado de* ***conjunto de geradores*** *de M se $M = RS = \{m \in M | m = r_1s_1 + \cdots + r_ns_n$ onde $r_i \in R$ e $s_i \in S\}$. Ou seja, todo elemento de M pode ser escrito como combinação linear finita de elementos de S com coeficientes em R.*

Definição 2.2.5 *O conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é chamado de* ***linearmente independente*** *se, qualquer combinação linear finita de elementos de S com coeficientes em R tem apenas solução trivial, ou seja,*

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

Definição 2.2.6 *O conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é chamado de* ***base*** *de M sobre R se ele é linearmente independente e é um conjunto de geradores.*

O conjunto $\mathcal{B} = \{1\}$ é uma base para $\mathbb{Z}$ visto como módulo sobre ele mesmo. Porém o conjunto $\mathcal{B}' = \{2, 3\}$, apesar de ser um conjunto gerador de $\mathbb{Z}$, não é uma base pois é linearmente dependente. De fato, a combinação linear $x2 + y3 = 0$ possui solução $x = -3 \neq 0$, $y = 2 \neq 0$. Por este motivo, $\mathbb{Z}$ é um $\mathbb{Z}$ módulo livre com relação à base $\mathcal{B}$, porém não o é em relação a base $\mathcal{B}'$.

Definição 2.2.7 *Seja $\{M_i\}_{i\in I}$ uma família de submódulos de um R-módulo M. Dizemos que M é a* ***soma direta interna*** *dos submódulos desta família, e escrevemos $M = \oplus_{i\in I} M_i$, se a família é base de M, ou seja:*

(*i*) *Para todo $i \in I$, temos que $M_i \cap (\sum_{j\neq i} M_j) = 0$;*

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

Definição 2.2.8 *Seja $\{M_i\}_{i\in I}$ uma família de R-módulos. A* ***soma direta externa*** *de módulos desta família, que denotamos por $\oplus_{i\in I} M_i$ é o conjunto de elementos da forma $\{m_i\}_{i\in I}$, onde $m_i \in M_i$ e $m_i = 0$, exceto para um número finito de índices $i \in I$.*

Definição 2.2.9 *Seja R um anel comutativo. Um R-módulo A é chamado de* ***R-álgebra*** *se existe uma multiplicação, definida em A, tal que, com a adição dada de A e esta multiplicação, A seja um anel e que, para todo $r \in R$ e todo $a, b \in A$, tenhamos*

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

Assim, como com anéis, podemos definir homomorfismos entre módulos:

Definição 2.2.10 *Sejam M e N dois R-módulos. Uma aplicação $f : M \to N$ é um* ***homomorfismo*** *se para todo $m_1, m_2 \in M$ tivermos $f(m_1 + m_2) = f(m_1) + f(m_2)$ e para todo $a \in R$ e todo $m \in M$ tivermos $f(am) = af(m)$.*

Se M é um R-módulo qualquer, a função nula $m \mapsto 0$ e a função identidade $m \mapsto m$ são exemplos triviais de homomorfismos. As denominações dadas para os homomorfismos na Definição 2.1.11 também valem para homomorfismos de módulos.

Proposição 2.2.11 *Todo R-módulo M é imagem epimórfica de um R-módulo livre.*

Demonstração: Seja X um conjunto de geradores de M e F o R-módulo livre no conjunto X. A inclusão $f : X \to M$ induz um homomorfismo de R-módulos $\overline{f} : F \to M$ tal que $X \subset Im(\overline{f})$. Como X gera M, devemos ter $Im(\overline{f}) = M$. ■

O Lema a seguir é chamado de **Lema de Zorn** e será utilizado na demonstração de alguns resultados deste trabalho.

Lema 2.2.12 *Seja $\mathcal{F}$ uma coleção não vazia de subconjuntos de um conjunto dado, tal que toda família totalmente ordenada de elementos de $\mathcal{F}$ tenha um limitante superior em $\mathcal{F}$. Então $\mathcal{F}$ contém um elemento maximal.*

3 SEMISSIMPLICIDADE

Algumas vezes, ao trabalharmos com anéis e módulos, é conveniente conhecer sua decomposição, de forma a facilitar cálculos. Devido a isto, estamos interessados em anéis e módulos que possam ser decompostos em forma de soma direta. Nesta seção, R denotará um anel com identidade.

3.1 Anéis e módulos semissimples

Definição 3.1.1 *Um R-módulo M é chamado de* ***semissimples*** *quando todos os seus submódulos são somandos diretos.*

Proposição 3.1.2 *Seja $N \neq (0)$ um submódulo de um módulo semissimples M. Então N é semissimples e contém um submódulo simples.*

Demonstração: Seja L um submódulo qualquer de N. Então L é um submódulo de M, e como M é semissimples, existe L' tal que $M = L \oplus L'$. Afirmamos que $N = L \oplus (N \cap L')$. De fato, dado um elemento $n \in N \subset M$, podemos escrever $n = l + x$, com $l \in L$ e $x \in L'$, pois todo elemento de M pode ser escrito como soma de elementos de L e de L'. Mas, $x = n - l \in N$ pois N é submódulo e $n \in N$ e $l \in L \subset N$. Assim, $x \in L' \cap N$. Por outro lado, temos $L \cap (N \cap L') \subset L \cap L' = (0)$, pois $M = L \oplus L'$.

Com isto, provamos que N é semissimples, restando provar que N contém um submódulo simples. Assim, como N $\neq (0)$, podemos escolher $x \in N$ com $x \neq 0$. Consideremos $\mathbb{F} = \{L \subseteq N | L$ é submódulo e $x \notin L\}$ e notemos que $\mathbb{F} \neq \emptyset$, visto que $(0) \in \mathbb{F}$. Além disso, escolhamos $x \in N$ com $x \neq 0$. Podemos verificar que a família de todos os submódulos de N que não contém x é não vazia, pois $x \neq (0)$, e toda família ordenada tem um limitante superior, pois dada $\mathbb{F}' = \{N_\alpha\}_{\alpha \in I}$ uma subfamília de $\mathbb{F}$ totalmente ordenada, temos que $N^* = \bigcup_{\alpha \in I} N_\alpha$ é um limitante superior de $\mathbb{F}$. Primeiramente,observamos que $N^* \in \mathbb{F}'$ contém todos os demais conjuntos dessa família e pertence a ela, pois dados $x, y \in N^*$, temos que $x \in N_\alpha,\ y \in N_\beta$ para $\alpha, \beta \in I$. Como $\mathbb{F}$ é totalmente ordenada, podemos supor $N_\alpha \subset N_\beta$, assim, $x \in N_\alpha \subset N_\beta$ e $x - y \in N_\beta$. Da mesma forma, fazendo $a \cdot \alpha$ com $a \in R$ e $\alpha \in N^*$ teremos que $\alpha \in N_\alpha$ para algum $\alpha \in I$, assim, como N_β é submódulo, $a \cdot \alpha \in N_\beta \subset N^*$, assim N^* é um submódulo de N. Também podemos ver que $x \notin N^*$, pois $x \notin N_\alpha$ para todos os $\alpha \in I$.

Então, claramente N^* é um limitante superior de $\mathbb{F}'$, pois $N^* \supseteq N_\alpha, \forall\, \alpha \in I$. Pelo Lema de Zorn (2.2.12), existe um elemento maximal N_1 em $\mathbb{F}$. Como N é semissimples, existe um submódulo N_2 tal que $N = N_1 \oplus N_2$. Mostraremos que N_2 é simples.

De fato, se N_2 não for simples, ele contém um submódulo não trivial W e então existe W', tal que $N_2 = W \oplus W'$. Mas desta forma, $N = N_1 \oplus N_2 = N_1 \oplus W \oplus W'$ e afirmamos que $N_1 = (N_1 + W) \cap (N_1 + W')$. Isso ocorre pois, dado $n \in N_1$, podemos escrever $n = n + 0$ com $0 \in W$ e $0 \in W'$, assim, $n + 0 \in (N_1 + W) \cap (N_1 + W')$. Por outro lado, dado $y \in (N_1+W)\cap(N_1+W')$ teremos $y = n_1+w \in N_1+W$ e $y = n_1'+w' \in N_1+W'$, logo, $n_1 + w = n_1' + w' \Rightarrow n_1 - n_1' = w - w'$, como $n_1, n_1' \in N_1$ teremos $n_1 - n_1' \in N_1$ e portanto, $w - w' \in N_1$, mas $w \in W \subset N_2$ e $w' \in W' \subset N_2$, então $w - w' \in N_2$. Como $N_1 \cap N_2 = (0)$, teremos $w - w' = 0 \Rightarrow w = w' \in W \cap W' = (0)$ e consequentemente, $n_1 = n_1'$ e $w = w' = 0$, assim, $y = n_1 \in N_1$.

Como $x \notin N_1 = (N_1 + W) \cap (N1 + W')$, teremos que $x \notin N_1 + W$ ou $x \notin N_1 + W'$, o que contradiz a maximalidade de N_1. Portanto, concluímos que $N_2 \subset N$ é simples.

■

A partir desta proposição, podemos obter caracterizações melhores para um módulo semissimples, como nos mostra o próximo teorema:

Teorema 3.1.3 *Seja M um R-módulo. São equivalentes:*

i) M é semissimples.

ii) M é soma direta de submódulos simples.

iii) M é a soma (não necessariamente direta) de submódulos simples.

Demonstração:

$(i) \Rightarrow ii)$) Seja $\mathcal{F}$ uma família de submódulos de M que podem ser escritos como uma soma direta de módulos simples. Pela Proposição 3.1.2, todo módulo semisimples contém um módulo simples, assim $\mathcal{F}$ é não vazia, pois podemos obter ao menos uma soma de um único termo. Assim, podemos definir uma relação de ordem em $\mathcal{F}$, onde dados $\oplus_{i\in I} M_i, \oplus_{j\in J} M_j \in \mathcal{F}$, escrevemos $\oplus_{i\in I} M_i \prec \oplus_{j\in J} M_j \Leftrightarrow I \subset J$.

Como $\mathcal{F}$ não é vazia, e toda subfamília $\mathcal{F}' = \{\bigoplus_{i\in I_\alpha} M_i\}_\alpha$ totalmente ordenada de $\mathcal{F}$ possui um limitante superior (basta tomar $\oplus_{i\in \cup I_\alpha} M_i$, que pertence a $\mathcal{F}$ pois é um submódulo de M), podemos aplicar o Lema de Zorn (2.2.12) para concluir que existe um elemento maximal $M_0 = \oplus_{i\in I} M_i \in \mathcal{F}$ com $M_i, i \in I$ simples.

Queremos provar que $M_0 = M$. Suponhamos assim, por absurdo, que $M_0 \neq M$. Por hipótese, existe um submódulo $N \neq (0)$ com $N \subset M$ tal que $M = M_0 \oplus N$. Como N é somando direto, pela Proposição 3.1.2, N contém um submódulo simples S. Assim, $M_0 \oplus S = \oplus_{i\in I} M_i \oplus S \supset M_0$. Ou seja, M_0 estaria contido em uma soma direta de submódulos simples de M, mas isto contraria o fato de M_0 ser maximal de $\mathcal{F}$, portanto, $M = M_0 = \oplus_{i\in I} M_i$.

$(ii) \Rightarrow iii))$ É trivial: se M é uma soma direta de submódulos simples, M é soma de submódulos simples.

$(iii) \Rightarrow i))$ Por hipótese, temos que $M = \sum_{i \in I} M_i$ é soma de submódulos simples. Assim, dado um submódulo próprio $N \subset M$, queremos mostrar que N é somando direto.

Dessa forma, consideremos $\mathcal{I} = \{\sum_{i \in J} M_i : J \subset I, (\sum_{i \in J} M_i) \cap N = (0)\}$, ou seja, $\mathcal{I}$ é a família das somas de submódulos simples, tais que a interseção destas somas com N é igual a (0). Como cada M_i é simples, temos que $N \cap M_i \neq (0)$ implica que $M_i \subset N$. E como $N \neq M$, segue que existe pelo menos um submódulo M_i tal que $N \cap M_i = (0)$ e assim $\mathcal{I}$ é não vazia. Pelo Lema de Zorn 2.2.12, podemos encontrar um submódulo maximal $M_0 = \sum_{i \in J_0} M_i$ em $\mathcal{I}$. Como $(\sum_{i \in J_0} M_i) \cap N = (0)$, a demonstração estará completa se mostrarmos que $M = M_0 + N$.

Se, para todo $i \in I$, tivermos $M_i \subset M_0 + N$, então $M = M_0 + N$ e a prova está concluída. Assumamos, por absurdo, que existe um índice $i_0 \in I$ tal que $M_{i_0} \not\subset M_0 + N$. Como M_{i_0} é simples, temos que $M_{i_0} \cap (M_0 + N) = (0)$. Então também temos que $(M_{i_0 + M_0}) \cap N = (0)$. Isso significa que $M_{i_0} + M_0 \in \mathcal{I}$, contradizendo a maximalidade de M_0. ■

Exemplo 3.1.4 *Alguns exemplos de módulos semissimples:*

a) Seja $\mathbb{K}$ um corpo. Então todo $\mathbb{K}$-espaço vetorial V de dimensão finita n é um módulo semissimples. De fato, seja W um subespaço de V com base $\mathcal{B}' = \{v_1, \ldots, v_r\}$, podemos estender $\mathcal{B}'$ até uma base $\mathcal{B} = \{v_1, \ldots, v_r, v_{r+1}, \ldots, v_n\}$ de V. Assim, $V = W \oplus \langle v_{r+1}, \ldots, v_n \rangle$, ou seja, W é um somando direto de V.

b) O $\mathbb{Z}$-módulo $\mathbb{Z}$ não é semissimples. De fato, se $\mathbb{Z}$ fosse semissimples, dado o submódulo $2\mathbb{Z}$, poderíamos encontrar um submódulo $n\mathbb{Z}$, tal que $\mathbb{Z} = 2\mathbb{Z} \oplus n\mathbb{Z}$. Dessa forma, $2\mathbb{Z} \cap n\mathbb{Z} = (0)$, mas $2n \in 2\mathbb{Z} \cap n\mathbb{Z}$ e, portanto, $2n = 0 \Rightarrow n = 0$. Mas assim, $\mathbb{Z} = 2\mathbb{Z} \oplus 0\mathbb{Z} \Rightarrow \mathbb{Z} = 2\mathbb{Z}$, o que é absurdo. Portanto, $\mathbb{Z}$ não é semissimples como módulo sobre ele mesmo.

Corolário 3.1.5 *Seja M um módulo semissimples de forma que $M = \bigoplus_{i \in I} M_i$, onde cada M_i é um submódulo simples e seja N um submódulo de M. Então, existe $J \subset I$, tal que $N \simeq \bigoplus_{i \in J} M_i$.*

Demonstração: Conforme os argumentos utilizados na demonstração da implicação $iii) \Rightarrow i)$ do Teorema (3.1.3), teremos que, dado um submódulo N de M, podemos encontrar um subconjunto de índices $J_0 \subset I$ tal que $M = N \oplus N_0$, onde $N_0 = \bigoplus_{i \in I \setminus J_0} M_i$. Consideremos o homomorfismo:

$$M = N \oplus N_0 \to N$$

$$n + n' \mapsto n$$

Assim, pelo Teorema do Homomorfismo (2.1.12),

$$N \simeq \frac{M}{N_0} = \frac{\bigoplus_{i \in I} M_i}{\bigoplus_{i \in J_0} M_i} \simeq \bigoplus_{i \in I \setminus J_0} M_i$$

e o resultado segue com $J = I \setminus J_0$. ■

Corolário 3.1.6 *Seja L um módulo quociente de um módulo semissimples M. Então L é isomorfo a um submódulo de M e portanto também é semissimples.*

Demonstração: Sejam L um módulo quociente de M, $\pi : M \to L$ o homomorfismo canônico ($\pi(m) = \overline{m}$), e $N = Ker(\pi)$. Assim, $L \simeq \dfrac{M}{Ker(\pi)}$ pelo Teorema do Homomorfismo (2.1.12). Por outro lado, como M é semissimples e $Ker(\pi)$ é um submódulo de M, existe um submódulo $N' \subset M$, tal que $M = N \oplus N'$. Pelo corolário anterior, temos que $L \simeq \dfrac{M}{Ker(\pi)} \simeq N'$. Assim, $L \simeq N'$ e, portanto, é semissimples. ■

Definição 3.1.7 *Um anel R é chamado de* ***semissimples*** *quando R visto como R-módulo é semissimples.*

É importante observar que os submódulos do R-módulo R são os ideais a esquerda do anel R. Assim, o anel R é semissimples, se e somente se, todo ideal a esquerda é um somando direto.

Teorema 3.1.8 *Seja R um anel. São equivalentes:*

i) *Todo R-módulo é semissimples;*

ii) *R é um anel semissimples;*

iii) *R é soma direta de um número finito de ideais minimais a esquerda.*

Demonstração: ($i) \Rightarrow ii)$) Suponha que todo R-módulo é semisimples, em particular, obtemos que o R-módulo R é semisimples. Portanto, R é um anel semisimples.

($ii) \Rightarrow i)$) Suponhamos que R seja um anel semissimples e M um R-módulo qualquer. Sabemos pela Proposição 2.2.11 que M é a imagem epimórfica de um R-módulo livre F. Podemos escrever $F = \bigoplus_{i \in I} Ra_i$ onde $Ra_i \simeq R$ via o isomorfismo $x \mapsto xai$, para todo $x \in R$. Agora, como R é semisimples, segue que o R-módulo R é uma soma direta de módulos simples. Do isomorfismo acima, obtemos que F também é uma soma direta de módulos simples e, por 3.1.3, segue que F é semisimples. Sendo M um quociente de F e F semisimples, concluímos que M é semisimples.

$(ii) \Rightarrow iii))$ Como R é um anel semissimples, R como R-módulo é semissimples. O Teorema 3.1.3 nos mostra que R é soma direta de submódulos simples. Mas, como os submódulos simples de R como R-módulo são os ideais minimais a esquerda de R, temos que R é soma de ideais minimais a esquerda, restando provar que esta soma é finita.

Considere então $R = \bigoplus_{i \in I} L_i$ uma decomposição de R em soma de ideais minimais a esquerda. Assim, temos que $1 = x_{i_1} + \cdots + x_{i_n}$ é uma soma finita em que cada $x_{i_j} \in L_{i_j}$. Vamos mostrar que $R = L_{i_1} \oplus \cdots \oplus L_{i_n}$. De fato, para um elemento arbitrário $r \in R$, temos que $r = r \cdot 1 = rx_{i_1} + \cdots + rx_{i_n}$, onde $rx_{i_j} \in L_{i_j}$. Isso nos mostra que $R \subset L_{i_1} \oplus \cdots \oplus L_{i_n}$, e como a soma de ideais de R está sempre contida em R, temos que $R = \bigoplus_{j=1}^{n} L_{i_j}$.

$(iii) \Rightarrow ii))$ Se R é uma soma direta finita de ideais minimais a esquerda, então o R-módulo R é a soma direta de submódulos simples. Pelo Teorema 3.1.3, R é um R-módulo semissimples, e portanto, R é anel semissimples. ■

Definição 3.1.9 *Uma cadeia de submódulos de um R-módulo M:*

$$(0) = M_n \subset \cdots \subset M_1 \subset M_0 = M$$

*é chamada de **série de composição** de M se todo submódulo M_i/M_{i+1} é simples. Um módulo que possui uma série de composição é dito de **comprimento finito**.*

Corolário 3.1.10 *Se R é um anel simples, então o R-módulo R tem comprimento finito.*

Demonstração: Se R é simples, ele também será um anel semissimples, e assim podemos escrever $R = L_1 \oplus \cdots \oplus L_t$, onde L_i é um ideal minimal a esquerda, $1 \leq i \leq t$. Então

$$(0) \subset L_t \subset (L_{t-1} \oplus L_t) \subset \cdots \subset (L_1 \oplus \cdots \oplus L_t) = R$$

é uma série de composição de comprimento finito de R como R-módulo. ■

Exemplo 3.1.11 *Seja $M_n(D)$ o anel da matrizes de ordem $n \times n$ com entradas em um anel de divisão D. Afirmamos que $M_n(D)$ é um anel semissimples. De fato, considere:*

$$L_1 = \begin{bmatrix} D & 0 & \cdots & 0 \\ D & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ D & 0 & \ldots & 0 \end{bmatrix}, \ldots, L_n = \begin{bmatrix} 0 & 0 & \cdots & D \\ 0 & 0 & \cdots & D \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & D \end{bmatrix}.$$

Vamos provar que cada $L_i, 1 \leq i \leq n$, é um ideal minimal a esquerda de $M_n(D)$.

Assim, sejam $X \in M_n(D)$ e $A, B \in L_i$, tais que:

$$X = \begin{bmatrix} x_{11} & \cdots & x_{1i} & \cdots & x_{1n} \\ x_{21} & \cdots & x_{2i} & \cdots & x_{2n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{ni} & \cdots & x_{nn} \end{bmatrix}, A = \begin{bmatrix} 0 & \cdots & a_{1i} & \cdots & 0 \\ 0 & \cdots & a_{2i} & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & a_{ni} & \cdots & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & \cdots & b_{1i} & \cdots & 0 \\ 0 & \cdots & b_{2i} & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & b_{ni} & \cdots & 0 \end{bmatrix}$$

Temos que

$$A - B = \begin{bmatrix} 0 & \cdots & a_{1i} - b_{1i} & \cdots & 0 \\ 0 & \cdots & a_{2i} - b_{2i} & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & a_{ni} - b_{ni} & \cdots & 0 \end{bmatrix} \in L_i$$

$$XA = \begin{bmatrix} 0 & \cdots & \sum_{j=1}^{n} a_{ji}x_{1j} & \cdots & 0 \\ 0 & \cdots & \sum_{j=1}^{n} a_{ji}x_{2j} & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & \sum_{j=1}^{n} a_{ji}x_{nj} & \cdots & 0 \end{bmatrix} \in L_i$$

Logo, L_i é ideal a esquerda de $M_n(D)$.

Suponhamos agora que exista I ideal de $M_n(D)$ tal que $(0) \subset I \subset L_i$. Queremos mostrar que se $I \neq (0)$ então $I = L_i$. Tomemos então $I \neq (0)$ tal que $I \subset L_i$. Assim, existe $Y = (y_{kj}) \in I \subset L_i$ com $Y \neq 0$, e portanto, existe $y_{qi} \neq 0$ para algum $1 \leq q \leq n$. Da mesma forma, $y_{kj} = 0$ se $j \neq i$, pois $Y \in L_i$. Assim,

$$I \ni E_{qq}Y = E_{qq}\sum_{i=1}^{n} y_{ki}E_{ki} = y_{qi}E_{qi} \in I$$

onde E_{kj} é a matriz elementar que possui 1 na entrada (kj) e 0 nas demais entradas. Considere uma matriz $Z = (z_{kj}) \in L_i$ e observe que

$$\sum_{k=1}^{n}(z_{ki}y_{qi}^{-1}E_{kk})\underbrace{y_{qi}E_{qi}}_{\in I} \overset{k=q}{=} z_{qi}E_{qi}$$

Assim,

$$Z = \sum_{q=1}^{n} z_{qi}E_{qi} = \sum_{q=1}^{n}\left(\sum_{k=1}^{n}(z_{ki}y_{qi}^{-1}E_{kk})\underbrace{y_{qi}E_{qi}}_{\in I}\right) \in I$$

Portanto, $I = L_i$, o que conclui que cada L_i é um ideal minimal a esquerda de $M_n(D)$.

Além disso, temos que $L_1 + \cdots + L_n \subset M_n(D)$ e dada

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{bmatrix} \in M_n(D)$$

temos que

$$X = \begin{bmatrix} x_{11} & 0 & \cdots & 0 \\ x_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & 0 & \cdots & 0 \end{bmatrix} + \begin{bmatrix} 0 & x_{12} & \cdots & 0 \\ 0 & x_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & x_{n2} & \cdots & 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 & 0 & \cdots & x_{1n} \\ 0 & 0 & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x_{nn} \end{bmatrix} \in L_1 + \cdots + L_n$$

E por fim, se $Y \in L_i \cap L_j$, com $i \neq j$, claramente Y é a matriz nula. Portanto, $M_n(D) = L_1 \oplus \cdots \oplus L_n$ é um anel semissimples.

Definição 3.1.12 *Um elemento $e \in R$ é chamado de* ***idempotente*** *se $e^2 = e$.*

Dois exemplos bastante triviais são o elemento identidade 1 e o elemento nulo 0 de qualquer anel. Outro exemplo é a matriz $E_{11} \in M_3(D)$:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Teorema 3.1.13 *Seja R um anel. Então, R é semissimples se, e somente se, todo ideal a esquerda L de R é da forma $L = Re$, onde $e \in R$ é um elemento idempotente.*

Demonstração:

($\Rightarrow$) Suponhamos que R é um anel semissimples e L é um ideal a esquerda de R. Logo, $R = L \oplus N$, para algum ideal a esquerda N de R. Assim, como $1 \in R$, podemos escrever $1 = e + n$, onde $e \in L$ e $n \in N$. Vamos mostrar que e é idempotente e que $L = Re$. De fato, temos que

$$e = e \cdot 1 = e(e+n) = e^2 + en \Rightarrow en = e - e^2.$$

Mas $en \in N$, pois N é ideal a esquerda e $e - e^2 \in L$, logo, $en = e - e^2 \in L \cap N = (0) \Rightarrow e - e^2 = 0$ e assim, $e = e^2$. Isso nos mostra que e é um elemento idempotente. Resta mostrar que $L = Re$. Com efeito, L é um ideal a esquerda e $e \in L$, temos que $Re \subseteq L$. Por outro lado, dado $x \in L$, temos que $x = x \cdot 1 = x(e+n) = xe + xn$. Disso, temos que $x - xe = xn \in L \cap N = 0$ e, assim $x - xe = 0 \Rightarrow x = xe \in Re$. Portanto, $L = Re$.

($\Leftarrow$) Agora, suponhamos que todo ideal a esquerda L de R é da forma $L = Re$, onde e é um elemento idempotente. Queremos mostrar que existe um ideal a esquerda N de R, tal que $R = L \oplus N$. Consideremos então $N = R(1-e)$. Afirmamos que *i)* $1-e$ é idempotente;

ii) $R = L \oplus N$.

Para o item *i)*, temos que $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$. Logo $1-e$ é idempotente.

Já para o item *ii)*, temos que L e N são ideias de R, portanto $L + N \subseteq R$ e dado $r \in R$, podemos escrever $r = re + r(1-e)$ e assim, $R \subseteq L + N$. Além disso, se $r \in L \cap N$, então por um lado temos que $r = xe$,para algum $x \in R$, que nos dá

$$re = xe \cdot e = xe^2 = xe = r \tag{3.1}$$

Por outro lado, $r = y(1-e)$ para algum $y \in R$. Assi temos que

$$re = y(1-e) \cdot e = (y - ye) \cdot e = ye - ye^2 = ye - ye = 0 \tag{3.2}$$

De 3.1 e 3.2, segue que $r = re = 0$ e, assim, $L \cap N = (0)$. Portanto $R = L \oplus N$.

■

Teorema 3.1.14 *$R = \bigoplus_{i=1}^{t} L_i$ é a decomposição de um anel semissimples em ideais minimais a esquerda se, e somente se, existe uma família de elementos de R, a saber, $\{e_1, \ldots, e_t\}$ tais que*

i) *$e_i \neq 0$ é um elemento idempotente, $1 \leq i \leq t$;*

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 $e_i = e'_i + e''_i$ onde e'_i e e''_i são idempotentes tais que $e'_i, e''_i \neq 0$ e $e'_i e''_i = 0$, $1 \leq i \leq t$.*

Demonstração:

($\Rightarrow$) Suponhamos que $R = \bigoplus_{i=1}^{t} L_i$ é a decomposição de um anel semissimples em ideais minimais a esquerda e $1 = e_1 + \cdots + e_t$, com $e_i \in L_i, 1 \leq i \leq t$. Pelo Teorema 3.1.13, temos que $L_i = Re_i$, e_i é um idempotente e $e_i e_j = 0$ se $i \neq j$. Para a condição *iv)*, suponhamos que para algum i, possamos escrever $e_i = e'_i + e''_i$ onde e'_i e e''_i são idempotentes tais que $e'_i, e''_i \neq 0$ e $e'_i e''_i = 0$, então pelo Teorema 3.1.13, teríamos $L_i = Re'_i \oplus Re''_i$, o que contradiz a minimalidade de L_i.

($\Leftarrow$) Assumiremos agora que existe uma família de idempotentes que satisfazem as condições dadas no teorema. Veremos que os ideais $L_i = Re_i$ são minimais, $1 \leq i \leq t$. De fato, suponha que L_i não seja minimal, então L_i contém um ideal J e como R é semissimples, L_i também é semissimples. Logo existe J' tal que $L_i = J \oplus J'$, o que implicaria que podemos escrever $e_i = e_i' + e_i''$ onde e_i' e e_i'' são idempotentes tais que $e_i', e_i'' \neq 0$ e $e_i'e_i'' = 0$, uma contradição ao item iv) da hipótese. Logo, L_i é minimal.

Já a condição iii), nos dá que para qualquer $r \in R$, temos $r = r \cdot 1 = r(e_1 + \cdots + e_t) = re_1 + \cdots + re_t \in L_1 + \cdots + L_t$. Mais ainda, seja $x \in L_i \cap (L_1 + \cdots + L_{i-1} + L_{i+1} + \cdots + L_t)$, então por um lado, $x = r_i e_i$ e por outro, $x = r_j e_j$. Assim,

$$x = r_j e_j = r_j e_j^2 = (r_j e_j) e_j = x e_j = (r_i e_i) e_j = r_i (e_i e_j) = r_i \cdot 0 = 0.$$

Portanto, $R = L_1 \oplus \cdots \oplus L_t$.

■

A definição a seguir nos traz uma denominação para a família de idempotentes apresentada no Teorema 3.1.14.

Definição 3.1.15 *A família de idempotentes $\{e_1, \ldots, e_t\}$ que satisfaz as condições $i), ii), iii)$ do Teorema 3.1.14 é chamada de **família completa de idempotentes ortogonais**. Um idempotente que satisfaz a condição $iv)$ do mesmo teorema é chamado de primitivo.*

Com os resultados apresentados até este momento, sabemos que se R é um anel semissimples, então todo R-módulo é semissimples e pode ser decomposto como soma direta de R-módulos simples. Com os próximos resultados veremos que a decomposição de R como soma direta de ideais minimais a esquerda está relacionada via isomorfismo com a decomposição dos R-módulos em submódulos simples.

Lema 3.1.16 *Sejam L um ideal minimal a esquerda de um anel semissimples R e M um R-módulo simples. Então $LM = \{lm | l \in L \text{ e } m \in M\} \neq (0)$ se, e somente se, $L \simeq M$ como R-módulos. Neste caso, $LM = M$.*

Demonstração:

($\Rightarrow$) Suponhamos que $LM \neq (0)$, então existem $l \in L$ e $m \in M$ tais que $lm \neq 0$. Dessa forma, o submódulo $0 \neq Lm \subset M$ é diferente do submódulo (0) e como M é simples, $Lm = M = LM$. Observe que a igualdade $Lm = M$ nos mostra que M é gerado por um único elemento $m \in M$.

Consideremos agora o homomorfismo $f : L \to M$, tal que $f(x) = xm$. Como $M = Lm$, temos que para todo $lm \in M$, existe $l \in L$ tal que $lm = f(l)$, portanto f é sobrejetor. E ainda, como $Ker(f)$ é um submódulo de M que é um módulo simples, $Ker(f) = (0)$ ou $Ker(f) = L$. Mas se $Ker(f) = L$ teríamos $Im(f) = M = LM = (0)$ o que contraria nossa hipótese. Logo, $Ker(f) = (0)$, ou seja, f é injetora e portanto um isomorfismo.

($\Leftarrow$) Suponhamos agora que $L \simeq M$ e $f : L \to M$ é um isomorfismo de R-módulos. Como R é semissimples, $L = Re$, para algum $e \in R$ idempotente. Definamos $m_0 = f(e)$. Como f é um homomorfismo, $f(re) = rf(e) = rm_0$, para todo $r \in R$. Afirmamos que $m_0 \neq 0$. De fato, se $m_0 = 0$, então $0 = m_0 = f(e)$, e como e é o gerador de L, teríamos que f seria o homomorfismo nulo, absurdo, pois f é isomorfismo. E como $m_0 = f(e) = f(e^2) = ef(e) = em_0$ temos que $em_0 \neq 0$ com $e \in L$ e $m_0 \in M$, portanto $LM \neq (0)$. Por fim, como $(0) \neq LM \subset M$ e M é simples, temos que $LM = M$.

■

Proposição 3.1.17 *Seja $R = \bigoplus_{i=1}^{t} L_i$ a decomposição de um anel semissimples em ideais minimais a esquerda. Então todo R-módulo simples é isomorfo a um dos ideais L_i da decomposição de R.*

Demonstração: Seja $R = \bigoplus_{i=1}^{t} L_i$ a decomposição de um anel semissimples em ideais minimais a esquerda e M um R-módulo simples. Como RM é um submódulo de M diferente de (0), portanto $RM = M$. Mas $RM = \bigoplus_{i=1}^{t} L_iM \neq (0)$, então existe $1 \leq j \leq t$ tal que $L_jM \neq (0)$ e, pelo Lema 3.1.16, temos que $L_j \simeq M$. ■

3.2 O Teorema de Wedderburn-Artin

Nesta seção, veremos com mais detalhes a estrutura de anéis semissimples. O lema a seguir nos traz informações sobre os ideais bilaterais de um anel semissimples.

Lema 3.2.1 *Seja L um ideal minimal a esquerda de um anel semissimples R. Então a soma $\sum_{J \simeq L} J$ de todos os ideais a esquerda de R que são isomorfos a L é um ideal bilateral de R.*

Demonstração: Precisamos mostrar que $\sum_{J \simeq L} J$ é ideal a esquerda e a direita. Como $\sum_{J \simeq L} J$ é soma de ideais a esquerda pela Proposição 2.1.8 temos que também é um ideal a esquerda. Agora, como R é semissimples, podemos escrever $R = \bigoplus_{i=1}^{t} L_i$, onde L_i é ideal minimal a esquerda. Assim,

$$\left(\sum_{J \simeq L} J\right) R = \sum_{J \simeq L} JR = \sum_{J \simeq L} J \left(\sum_{i=1}^{t} L_i\right) = \sum_{J \simeq L} \sum_{i=1}^{t} JL_i$$

Como L_i é ideal a esquerda para todo $i = 1, \ldots, t$ e $J \subset R$ temos que JL_i é um ideal. Assim, $JL_i = (0)$ ou $JL_i = L_i$. Mas o Lema 3.1.16 nos mostra que $JL_i = L_i$ apenas se $J \simeq L_i$ e como $J \simeq L$, teríamos $L_i \simeq L$, implicando em $L_i \subset \sum_{J \simeq L} J$. Assim, $\left(\sum_{J \simeq L} J\right) R$ é uma soma de ideais nulos (quando $L_i \not\simeq J$) com ideais isomorfos a L (quando $L_i \simeq J$). Assim, $\left(\sum_{J \simeq L} J\right) R \subseteq \left(\sum_{J \simeq L} J\right)$ e assim provamos que é um ideal a direita também. ■

Lema 3.2.2 *Seja I um ideal bilateral de um anel semissimples R, tal que I contém um ideal minimal a esquerda L. Então I contém todos os ideais a esquerda isomorfos a L.*

Demonstração: Seja J um ideal a esquerda de R tal que $J \simeq L$. Assim, pelo Lema 3.1.16, $LJ = J$. Como $L \subset I$ e I é ideal bilateral, então $J = LJ \subset I$. Assim, todos os ideais a esquerda isomorfos a L estão contidos em I. ■

Proposição 3.2.3 *Seja L um ideal minimal a esquerda de um anel semissimples R e seja B a soma de todos os ideais a esquerda de R que são isomorfos a L. Então B é um ideal minimal bilateral de R.*

Demonstração: Pelo Lema 3.2.1, temos que B é um ideal bilateral de R. Resta mostrar que B também é minimal. Assim, seja $C \subset B$ um ideal bilateral e $L_1 \subset C$ um ideal minimal a esquerda contido em C. Note que L_1 existe, pois poderia ser igual a C. Suponhamos que $L_1 \not\simeq L$, então temos que $L_1 J = (0)$, para todo $J \simeq L$ (pelo Teorema 3.1.16). Assim, $L_1 B = (0)$ pois B é a soma de todos os ideais isomorfos a L. Mas como $L_1 \subset C \subset B$, temos que em particular, $L_1 L_1 = (0)$, o que é absurdo, pois de acordo com o Teorema 3.1.13, L_1 contém um idempotente. Logo, $L_1 \simeq L$ e por consequência do Lema 3.2.2, C contém todos os ideais a esquerda isomorfos a L e portanto também contém a soma de todos estes ideais. Assim, $B \subset C \Rightarrow B = C$, ou seja, B é minimal. ■

Considere uma decomposição de um anel semissimples em soma direta de ideais simples a esquerda. Podemos reordená-los e agrupar os ideais que são isomorfos:

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

onde $L_{ij} \simeq L_{ik}$ e $L_{ij} L_{kh} = (0)$ quando $i \neq k$ (de acordo com o Lema 3.1.16). Além disso, pela Proposição 3.1.17, todo ideal minimal a esquerda de R é isomorfo a algum L_{ij} da decomposição acima.

Esta decomposição, combinada com os lemas e proposições anteriores nos dá o seguinte teorema:

Teorema 3.2.4 *Seja $R = A_1 \oplus \cdots \oplus A_s$ um anel semissimples onde $A_i = L_{i1} \oplus \cdots \oplus L_{ir_i}$, $1 \leq i \leq s$ onde $L_{ij} \simeq L_{ik}$. Então:*

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

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

iii) *$R = \bigoplus_{i=1}^{s} A_i$ como anéis, onde s é o número de classes isomorfas de ideais minimais a esquerda de R.*

Demonstração:

i) A Proposição 3.2.3 nos mostra que a soma de ideais minimais a esquerda é um ideal minimal bilateral, ou seja, $A_i = L_{i1} \oplus \cdots \oplus L_{ir_i}$, $1 \leq i \leq s$ é um ideal minimal a esquerda.

ii) Por construção temos que se $i \neq j$, então $A_i \not\simeq A_j$, então pela contrapositiva do Lema 3.1.16, temos que $A_iA_j = (0)$.

iii) Imediata pela construção dos A_i's.

■

Corolário 3.2.5 *Os ideais A_i, $1 \leq i \leq s$, definidos no Teorema 3.2.4 são anéis simples.*

Demonstração: Como visto no Teorema 3.2.4, cada A_i é um ideal minimal bilateral de R. Assim, é suficiente mostrar que dado um B_i ideal bilateral de A_i, então B_i também é ideal de R. Pois se $B_i \subset A_i$ e A_i é minimal, então $B_i = (0)$ ou $B_i = A_i$, o que prova que A_i é anel simples.

Assim, sejam $b \in B_i$ e $r \in R$. Podemos escrever $r = x_1 + \cdots + x_s$, onde $x_j \in A_j$, $1 \leq j \leq s$. Assim, $rb = \sum_{j=1}^{s} x_jb = x_ib$, pois $x_jb = 0$ se $j \neq i$ e $rb = x_ib \in B_i$, pois B_i é ideal de A_i. Da mesma forma, $br = b\left(\sum_{j=1}^{s} x_j\right) = \sum_{j=1}^{s} x_jb = x_ib$ e assim, $br = x_ib \in B_i$.

Portanto, B_i é um ideal de R, como queríamos demonstrar. ■

Vejamos um exemplo de anéis simples que, como veremos adiante, tem a mesma estrutura dos A_i's.

Exemplo 3.2.6 *Seja D um anel de divisão, então $M_n(D)$ é um anel simples. De fato, seja I um ideal bilateral de $M_n(D)$. Temos que provar que se $I \neq (0)$, então $I = M_n(D)$.*

Assim, suponhamos que $I \neq (0)$, então existe uma matriz $A = (a_{ij}) \in I$ tal que pelo menos uma entrada de A é diferente de 0, digamos que seja a entrada a_{hk}. Seja

$B_i = E_{ih}AE_{ki}$, podemos ver que a matriz B_i tem todas as entradas iguais a 0, exceto a entrada i, i que é igual a a_{hk}.

Além disso, como B_i é resultado de uma multiplicação de A a direita e a esquerda por elementos de $M_n(D)$ e $A \in I$ que é ideal bilateral, então $B_i \in I$. Assim, quando consideramos $B = B_1 + \ldots + B_n$ temos que $B \in I$ e B é invertível, pois é uma matriz diagonal com entradas diferentes de 0 na diagonal principal. Logo, $I = M_n(D)$. E assim concluímos que $M_n(D)$ é um anel simples.

Proposição 3.2.7 *Seja $R = \bigoplus_{i=1}^{s} A_i$ a decomposição de um anel semissimples em soma direta de ideais minimais bilaterais. Então:*

i) Todo ideal bilateral I de R pode ser escrito da forma $I = A_{i_1} \oplus \cdots \oplus A_{i_t}$, onde $1 \leq i_1 < \cdots < i_t \leq s$.

ii) Se $R = \bigoplus_{i=1}^{r} B_i$ é outra decomposição de R em soma direta de ideais minimais bilaterais, então $s = r$ e após possível reordenação, $A_i = B_i$ para todo i.

Demonstração: Seja $I \subset R$ um ideal bilateral, então $I = R \cap I = \bigoplus_{i=1}^{s} A_i \cap I = \bigoplus_{i=1}^{s}(A_i \cap I)$. Como cada A_i é um ideal minimal bilateral e $A_i \cap I$ é um ideal bilateral de A_i, segue que $A_i \cap I = (0)$ ou $A_i \cap I = A_i$.

Esta mesma construção pode ser feita para cada B_j, pois são ideais minimais bilaterais. Como cada B_j é um ideal bilateral de R, temos que $B_j = A_{i_1} \oplus \cdots \oplus A_{i_t}$, com $1 \leq i_1 < \ldots < i_t \leq s$. Além disso, temos que B_j é minimal, e portanto, devemos ter apenas um A_i na decomposição de B_j, o que implica em $A_i = B_j$. Com uma possível reordenação, podemos concluir que $A_i = B_i$, para todo $1 \leq i \leq s$. ■

Definição 3.2.8 *Os únicos ideais minimais bilaterais de um anel semissimples R são chamados de* ***componentes simples de*** *R.*

Teorema 3.2.9 *Seja $R = \bigoplus_{i=1}^{s} A_i$ a decomposição de um anel semissimples em soma direta de ideais minimais bilaterais. Então, existe uma família $\{e_1, \ldots, e_s\}$ de elementos de R tais que:*

i) $e_i \neq 0$ é um idempotente central, $1 \leq i \leq s$.

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

iii) $1 = e_1 + \ldots + e_s$.

iv) e_i não pode ser escrito como $e_i = e_i' + e_i''$ onde e_i' e e_i'' são idempotentes centrais tais que $e_i', e_i'' \neq 0$, $1 \leq i \leq s$.

Demonstração: Como todo ideal minimal bilateral também é um ideal minimal a esquerda, a prova deste teorema é idêntica a do Teorema 3.1.14, restando provar que os elementos idempotentes são centrais, ou seja, que comutam com qualquer elemento $x \in R$. Assim, utilizando o item *iii*), temos que

$$x = x \cdot 1 = x(e_1 + \cdots + e_s) = xe_1 + \cdots + xe_s$$

$$x = 1 \cdot x = (e_1 + \cdots + e_s)x = e_1x + \cdots + e_sx$$

Como $e_i \in A_i$ e A_i é ideal bilateral, temos que $xe_i, e_ix \in A_i$. Além disso, o fato de R ser soma direta de ideais A_i nos garante a unicidade na escrita de qualquer elemento de R como soma de elementos de $A_1 \oplus \cdots \oplus A_s$, assim, temos que $xe_i = e_ix$, portanto os idempotentes são centrais.

■

Definição 3.2.10 *Os elementos definidos no Teorema 3.2.9 acima são chamados de* ***idempotentes centrais primitivos*** *de R.*

Lema 3.2.11 *Sejam R um anel, $M = M_1 \oplus \cdots \oplus M_r$ e $N = N_1 \oplus \cdots \oplus N_s$ R-módulos escritos como soma direta de submódulos. Seja $\epsilon_j : M_j \to M$ as inclusões de cada M_j em M e $\pi_i : N \to N_i$ os homomorfismos naturais de N em seus componentes.*

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

$$\begin{aligned}\phi(m_1 + \cdots + m_r) &= \begin{bmatrix} \phi_{11} & \cdots & \phi_{1r} \\ \vdots & \ddots & \vdots \\ \phi_{s1} & \cdots & \phi_{sr} \end{bmatrix} \begin{bmatrix} m_1 \\ \vdots \\ m_r \end{bmatrix} \\ &= \phi_{11}(m_1) + \cdots + \phi_{1r}(m_r) + \cdots + \phi_{s1}(m1) + \cdots + \phi_{sr}(m_r)\end{aligned}$$

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

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

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

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

Demonstração:

i) Suponha que $\phi_{ij} \in Hom_R(M_j, N_i)$. Sejam $a, a' \in M$, assim $a = m_1 + \cdots + m_r$ e $a' = m'_1 + \cdots + m'_r$, onde $m_i, m'_i \in M_i$, $1 \leq i \leq r$. Vamos mostrar que $\phi(a + a') = \phi(a) + \phi(a')$ e $\phi(\lambda a) = \lambda\phi(a)$. De fato,

$$\begin{aligned}
\phi(a+a') = \;& ((m_1 + m'_1) + (m_2 + m'_2) + \cdots + (m_r + m'_r)) \\
= \;& \begin{bmatrix} \phi_{11} & \cdots & \phi_{1r} \\ \phi_{21} & \cdots & \phi_{2r} \\ \vdots & \ddots & \vdots \\ \phi_{s1} & \cdots & \phi_{sr} \end{bmatrix} \begin{bmatrix} m_1 + m'_1 \\ m_2 + m'_2 \\ \vdots \\ m_r + m'_r \end{bmatrix} \\
= \;& \phi_{11}(m_1 + m'_1) + \cdots + \phi_{1r}(m_r + m'_r) + \\
& \phi_{21}(m_1 + m'_1) + \cdots + \phi_{2r}(m_r + m'_r) + \\
& \qquad \vdots \\
& \phi_{s1}(m_1 + m'_1) + \cdots + \phi_{sr}(m_r + m'_r) \\
= \;& \underbrace{\phi_{11}(m_1) + \cdots + \phi_{1r}(m_r) + \cdots + \phi_{s1}(m_1) + \cdots + \phi_{sr}(m_r)}_{\phi(a)} + \\
& \underbrace{\phi_{11}(m'_1) + \cdots + \phi_{1r}(m'_r) + \cdots + \phi_{s1}(m'_1) + \cdots + \phi_{sr}(m'_r)}_{\phi(a')} \\
= \;& \phi(a) + \phi(a')
\end{aligned}$$

$$\begin{aligned}
\phi(\lambda a) = \;& \phi(\lambda m_1 + \cdots + \lambda m_r) \\
= \;& \phi_{11}(\lambda m_1) + \cdots + \phi_{1r}(\lambda m_r) + \cdots + \phi_{s1}(\lambda m_1) + \cdots + \phi_{sr}(\lambda m_r) \\
= \;& \lambda\phi_{11}(m_1) + \cdots + \lambda\phi_{1r}(m_r) + \cdots + \lambda\phi_{s1}(m_1) + \cdots + \lambda\phi_{sr}(m_r) \\
= \;& \lambda\phi(a)
\end{aligned}$$

ii) Suponha que $\phi \in Hom(M, N)$, de forma que

$$\begin{aligned}
\phi: \quad M_1 \oplus \cdots \oplus M_r &\to N_1 \oplus \cdots \oplus N_s \\
m_1 + \cdots + m_r &\mapsto n_1 + \cdots + n_s
\end{aligned}$$

e defina

$$\phi(0 + \cdots + m_j + \cdots + 0) = \phi_{1j}(m_j) + \cdots + \phi_{sj}(m_j) \in N_1 \oplus \cdots \oplus N_s$$

onde $\phi_{ij} : M_j \to N_i$ são aplicações que dependem de m_j. Dessa forma,

$$\begin{aligned}
(\pi_i \circ \phi \circ \epsilon_j)(m_j) &= (\pi_i \circ \phi)(0 + \cdots + m_j + \cdots + 0) \\
&= \pi_i(\phi_{1j}(m_j) + \cdots + \phi_{sj}(m_j)) \\
&= \phi_{ij}(m_j) \in N_i
\end{aligned}$$

é homomorfismo. Logo, $\phi_{ij} \in Hom_R(M_j, N_i)$.

iii) Seja $\phi = (\phi_{ij})$ e $\psi = (\psi_{ij})$, dado um $m \in M$, vamos mostrar que $(\phi+\psi)(m) = (\phi_{ij}+\psi_{ij})(m)$. De fato, como $m = m_1 + \cdots + m_r \in M = M_1 \oplus \cdots \oplus M_r$.

$$\begin{aligned}
(\phi_{ij}+\psi_{ij})(m) = & \begin{bmatrix} \phi_{11}+\psi_{11} & \cdots & \phi_{1r}+\psi_{1r} \\ \vdots & \ddots & \vdots \\ \phi_{s1}+\psi_{s1} & \cdots & \phi_{sr}+\psi_{sr} \end{bmatrix} \begin{bmatrix} m_1 \\ \vdots \\ m_r \end{bmatrix} \\
= & (\phi_{11}+\psi_{11})(m_1) + \cdots + (\phi_{1r}+\psi_{1r})(m_r) + \\
& \vdots \\
& (\phi_{s1}+\psi_{s1})(m_1) + \cdots + (\phi_{sr}+\psi_{sr})(m_r) \\
= & \underbrace{\phi_{11}(m_1) + \cdots + \phi_{1r}(m_r) + \cdots + \phi_{s1}(m_1) + \cdots + \phi_{sr}(m_r)}_{\phi(m)} + \\
& \underbrace{\psi_{11}(m_1) + \cdots + \psi_{1r}(m_r) + \cdots + \psi_{s1}(m_1) + \cdots + \psi_{sr}(m_r)}_{\psi(m)} \\
= & \quad \phi(m) + \psi(m) = (\phi+\psi)(m)
\end{aligned}$$

iv) Consideremos o homomorfismo

$$\begin{aligned}
\varphi : \quad & M_n(Hom_R(M,M)) & \to \quad & Hom_R(M^n, M^n) \\
A = & \begin{bmatrix} \phi_{11} & \cdots & \phi_{1n} \\ \vdots & \ddots & \vdots \\ \phi_{n1} & \cdots & \phi_{nn} \end{bmatrix} & \mapsto \quad & \varphi(A)
\end{aligned}$$

onde

$$\begin{aligned}
\varphi(A) = \phi : \quad & M^n & \to \quad & M^n \\
& (m_1 + \cdots + m_n) & \mapsto \quad & \underbrace{\phi_{11}(m_1) + \cdots + \phi_{1n}(m_n)} + \\
& & & \vdots \\
& & & \underbrace{\phi_{n1}(m_1) + \cdots + \phi_{nn}(m_n)}
\end{aligned}$$

Este homomorfismo é injetor e sobrejetor, portanto é um isomorfismo.

■

Lema 3.2.12 *Seja R um anel, M um R-módulo semissimples e $B = Hom_R(M,M)$. Então M admite uma estrutura de B-módulo, com ação dada por $\phi \cdot m = \phi(m)$, $\forall\, \phi \in B$, $\forall\, m \in M$. Mais ainda, para cada $m \in M$ e cada $f \in Hom_R(M,M)$, existe um elemento $a \in R$ tal que $f(m) = am$.*

Demonstração: Primeiramente iremos mostrar que M tem uma estrutura de B-módulo com a ação dada pelo lema enunciado. De fato, M é um anel comutativo pois é R-módulo e B é um anel com identidade. Assim, basta verificar as condições da Definição 2.2.1: Sejam $f, g \in B$ e $m, n \in M$, temos

$$(f+g)\cdot m = (f+g)(m) = f(m)+g(m) = f\cdot m + g\cdot m$$

$$f\cdot(m+n) = f(m+n) = f(m)+f(n) = f\cdot m + f\cdot n$$

$$(fg)\cdot m = (fg)(m) = f(g(m)) = f\cdot(g(m)) = f\cdot(g\cdot m)$$

$$1\cdot m = 1(m) = m.$$

Veremos agora a segunda afirmação. Tomemos $m \in M$ e consideremos o submódulo Rm. Como M é semissimples, existe um submódulo N tal que $M = Rm \oplus N$, e assim podemos definir $\pi : M \to M$ a projeção de M em Rm, dada por $\pi(rm+n) = rm$, onde $rm \in Rm$ e $n \in N$. Assim, sabemos que $\pi \in Hom_R(M,M) = B$. Tomando $f \in Hom_B(M,M)$, temos $f(m) = f(\pi(m))$ já que $\pi(m) = m$, pois π é projeção. Por outro lado, $\pi \in B$ pode ser visto como um escalar quando vemos M como B-módulo e como f é um homomorfismo em B-módulo, temos que $f(\pi(m)) = \pi(f(m))$. Novamente, como π é projeção, temos que $\pi(f(m)) \in Rm$ e usando a transitividade, $f(m) \in Rm$, portanto, $f(m) = am$ para algum $a \in R$. ■

Teorema 3.2.13 (Teorema da Densidade de Jacobson) *Sejam M um R-módulo semissimples e $B = Hom_R(M,M)$, $f \in Hom_B(M,M)$. Se $\{m_1,\ldots,m_n\}$ é um conjunto arbitrário de elementos de M, então existe um elemento $a \in R$ tal que $f(m_i) = am_i$, para todo $1 \leq i \leq n$.*

Demonstração: Seja $M^{(n)} = M\oplus M\oplus\cdots\oplus M$ (somado n vezes). Dado $f \in Hom_B(M,M)$, definimos $f^{(n)} : M^{(n)} \to M^{(n)}$ por $f^{(n)}(x_1+\cdots+x_n) = f(x_1)+\cdots+f(x_n)$, onde $x_i \in M, i = 1,\ldots,n$.

Seja $B' = Hom_R(M^{(n)}, M^{(n)})$. Afirmamos que $f^{(n)} \in Hom_{B'}(M^{(n)}, M^{(n)})$. De fato, dado $\phi \in B'$, pelo Lema 3.2.11, podemos escrever $\phi = (\phi_{ij})$, com $\phi_{ij} \in Hom_R(M,M)$. Assim, temos:

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

Agora, pelo Lema 3.2.12, existe um elemento $a \in R$ tal que

$$f^{(n)}(m_1+\cdots+m_n) = a(m_1+\cdots+m_n) = am_1+\cdots+am_n.$$

Portanto, pela definição de $f^{(n)}$, temos $f(m_i) = am_i, i = 1,\cdots,n$. ■

Lema 3.2.14 (Lema de Schur) *Sejam R um anel e M, N R-módulos simples. Considere $f : M \to N$ um homomorfismo não nulo. Então f é um isomorfismo.*

Demonstração: Como $Im(f)$ é um submódulo de N que é um módulo simples, temos que $Im(f) = 0$ ou $Im(f) = N$. Como f é não nulo, então $Im(f) = N$ e portanto, f é sobrejetor. Da mesma forma, $Ker(f)$ é um submódulo de M que é um módulo simples. Assim, $Ker(f) = 0$ ou $Ker(f) = M$, mas como f é não nulo, a segunda opção não ocorre. Logo, $Ker(f) = 0$, o que implica em f ser injetor. Portanto, f é um isomorfismo. ■

Corolário 3.2.15 *Sejam R um anel e M, N R-módulos simples. Então:*

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

ii) *$Hom_R(M, M)$ é um anel de divisão.*

Demonstração:

i) Usando a contra-positiva, se $Hom_R(M, N) \neq (0)$ então existe um homomorfismo não nulo $f : M \to N$. De acordo com o Lema 3.2.14, f é um isomorfismo, logo $M \simeq N$.

ii) Não é difícil ver que $Hom_R(M, M) \subset \mathcal{F}(M, M)$ é um anel com as operações de soma e multiplicação de $\mathcal{F}(M, M)$. Além disso, pelo Lema 3.2.14, temos que todo homomorfismo $f : M \to M$ não nulo é um isomorfismo e portanto tem inverso.

■

Definição 3.2.16 *Um anel R é dito* ***artiniano*** *a esquerda se qualquer cadeia decrescente de ideais a esquerda*

$$I_1 \supset I_2 \supset \cdots \supset I_i \supset \cdots$$

estaciona, ou seja, existe um índice t tal que $I_t = I_{t+i}$, para $i \geq 1$.

A próxima observação utilizará esta definição.

Observação 3.2.17 *Se R é um anel Artiniano semissimples e M é um R-módulo simples, então $D = Hom_R(M, M)$ é um anel de divisão. Como M é também um D-módulo, M é um espaço vetorial sobre D. Afirmamos que M é um D-espaço vetorial de dimensão finita. De fato, seja $\{m_1, \ldots, m_n, \ldots\}$ um conjunto linearmente independente de M sobre D. Para cada índice t definimos:*

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

A_t é um ideal a esquerda de R e $A_i \supset A_{i+1}$, $i = 1, 2, \ldots$. Além disso, essa união é estrita. De fato, como M é um R-módulo simples, $M \neq 0$ e assim podemos tomar $0 \neq m \in M$. Definimos assim, um homomorfismo de D-módulos:

$$f(m_i) = \begin{cases} 0, & se\ i \neq t+1 \\ m, & se\ i = t+1 \end{cases}$$

Sendo $\{m_1, \ldots, m_{t+1}\} \subset M$ e $f \in Hom_D(M, M)$, o Teorema 3.2.13 implica que existe $a \in R$ tal que

$$f(m_i) = am_i = \begin{cases} 0, & se\ 1 \leq i \leq t \\ m, & se\ i = t+1 \end{cases}$$

E assim, $a \in A_t$, mas $a \notin A_{t+1}$ e esta inclusão é estrita. Então como o conjunto linearmente independente é infinito, podemos criar uma cadeia descendente de ideais:

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

o que contraria a hipótese de R ser Artiniano.

Definição 3.2.18 *Dado um anel de divisão D, chamamos de* ***anel oposto*** *D^{op} o anel definido sobre o mesmo conjunto e multiplicação dada por $x \cdot y = yx$, onde yx é a multiplicação de y por x em D.*

Lema 3.2.19 *Sejam R um anel artiniano simples, M um R-módulo simples e $D = Hom_R(M, M)$. Então,*

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

onde n é a dimensão de M como D-módulo.

Demonstração: Primeiramente veremos que $R \simeq Hom_D(M, M)$. Para isto, considere o homomorfismo $\Phi : R \to Hom_D(M, M)$ que associa a cada elemento $a \in R$ o homomorfismo $f_a \in Hom_D(M, M)$, dado por $f_a(x) = ax$ para todo $x \in M$.

Podemos notar que o conjunto $Ker\ \Phi = \{a \in R | f_a = 0\} = \{a \in R | ax = 0, \forall\, x \in M\}$ é um ideal bilateral de R. Como R é simples e $1 \notin Ker\ \Phi$, segue que $Ker\ \Phi = 0$, logo Φ é injetor. Seja agora $\{m_1, \ldots, m_n\}$ uma base de M sobre D. Segue do Teorema 3.2.13, que existe um elemento $a \in R$ tal que $f(m_i) = am_i, 1 \leq i \leq n$, e por linearidade, $f(m) = am, \forall\, m \in M$. Logo, para cada $f \in Hom_D(M, M)$, existe $a \in R$ tal que $\Phi(a) = f$ e $f(x) = ax, \forall\, x \in M$, logo Φ é sobrejetora e portanto um isomorfismo.

Agora se n é a dimensão de M como D-módulo, sabemos que $M \simeq D^{(n)}$ como D-módulos. Assim, pelo item $iv)$ do Lema 3.2.11, $Hom_D(M, M) \simeq Hom_D(D^{(n)}, D^{(n)}) \simeq M_n(Hom_D(D, D))$, restando mostrar que $Hom_D(D, D) \simeq D^{op}$.

Definimos agora $\Psi : D \to Hom_D(D, D)$ dada por $\Psi(a) = f_a$, onde $f_a(x) = xa, \forall\, x \in D$. Usando o mesmo argumento da função Φ, podemos ver que $Ker\Psi = (0)$ e portanto, Ψ é injetora. Dado $f \in Hom_D(D, D)$, temos que $f(x) = f(x1) = xf(1)$, pois x é escalar em D. Então se fixarmos $f(1) = a$ teremos que $f = \Psi(a)$ e portanto Ψ é sobrejetora. Como ainda $\Psi(ab) = f_{ab} = f_b \circ f_a = \Psi(b)\Psi(a)$, temos que $Hom_D(D, D) \simeq D^{op}$. ■

Corolário 3.2.20 *Um anel artiniano simples é semissimples.*

Demonstração: De acordo como Lema 3.2.19, temos que se R é um anel artiniano simples, então $R \simeq M_n(D^{op})$, onde D^{op} é o anel oposto de $D = Hom_R(M, M)$ e M é um R-módulo simples. Mas como vimos no Exemplo 3.1.11, $M_n(D^{op})$ é um anel semissimples. Logo, R também é semissimples. ■

Teorema 3.2.21 (Wedderburn-Artin) *Um anel R é semissimples se, e somente se, ele é uma 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:

($\Rightarrow$) Se R é um anel semissimples, então R é a soma de ideais minimais a esquerda. Pelo Teorema 3.2.4, podemos reagrupar estes ideais a esquerda, unindo os que são isomorfos e obtendo a seguinte decomposição para R:

$$R = A_1 \oplus \cdots \oplus A_s,$$

onde cada A_i é um ideal minimal bilateral de R, e é também um anel simples, pelo Corolário 3.2.5. Já pelo Lema 3.2.19, temos que $A_i \simeq Hom_{D_i}(L_{i1}, L_{i1})$, onde $D_i = Hom_R(L_{i1}, L_{i1})$ é um anel de divisão de acordo com o Corolário 3.2.15. Novamente pelo Lema 3.2.19, temos que $A_i \simeq M_{n_i}(D_i)$ para $1 \leq i \leq s$. Portanto,

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

.

($\Leftarrow$) Suponhamos que $R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s)$. Como visto no Exemplo 3.2.6, o anel de matrizes com entradas em um anel de divisão é um anel simples, logo não possui ideais minimais bilaterais. Assim, para cada $i = 1, \ldots, s$, temos a seguinte decomposição para $M_{n_i}(D_i)$:

$$M_{n_i}(D_i) = \begin{bmatrix} D_i & \cdots & 0 \\ \vdots & \cdots & \vdots \\ D_i & \cdots & 0 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} 0 & \cdots & D_i & \cdots & 0 \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ 0 & \cdots & D_i & \cdots & 0 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} 0 & \cdots & D_i \\ \vdots & \cdots & \vdots \\ 0 & \cdots & D_i \end{bmatrix}$$

Como cada um destes ideais $L_i = \begin{bmatrix} 0 & \cdots & D_i & \cdots & 0 \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ 0 & \cdots & D_i & \cdots & 0 \end{bmatrix}$ é minimal a esquerda, temos que R é um anel semissimples.

■

Teorema 3.2.22 *Seja R um anel semissimples e assuma que*

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

onde $D_i, D'_j,\ 1 \leq i \leq s,\ 1 \leq j \leq r$ são anéis de divisão. Então, $s = r$ e, permutando os índices de forma conveniente, temos $n_i = m_j$ e $D_i = D'_j$.

Demonstração: Pode ser vista em (Milies e Sehgal, 2002, p. 105, [3]) ■

4 ANÉIS DE GRUPO

Nesta seção estudaremos sobre um tipo de anel muito importante: ele é o resultado da junção de um grupo e um anel, é o anel de grupo. Veremos como se dá sua construção, estudaremos os ideais de aumento e as condições de semissimplicidade nesta estrutura.

4.1 Anéis de Grupo e Semissimplicidade

Iniciaremos esta seção com a construção dos elementos de um anel de grupo RG e das operações de adição e multiplicação que tornam este conjunto um anel.

Dado um grupo G e um anel R, definimos o **anel de grupo** RG como o conjunto de todas as combinações lineares formais da forma $\alpha = \sum_{g \in G} a_g g$, onde $a_g \in R$ e $a_g = 0$, exceto para um número finito de $g \in G$.

Exemplo 4.1.1 *Consideremos o anel dos números inteiros* $\mathbb{Z}$ *e o grupo* $S_3 = \{e, f_1, f_2, f_3, f_4, f_5\}$ *das permutações de 3 elementos. O anel de grupo* $\mathbb{Z}S_3$ *é da forma:*

$$\mathbb{Z}S_3 = \{n_e e + n_{f_1} f_1 + n_{f_2} f_2 + n_{f_3} f_3 + n_{f_4} f_4 + n_{f_5} f_5 \mid n_e, n_{f_1}, n_{f_2}, n_{f_3}, n_{f_4}, n_{f_5} \in \mathbb{Z}\}.$$

Definição 4.1.2 *Dado um elemento* $\alpha = \sum_{g \in G} a_g g \in RG$*, definimos o* ***suporte*** *de* α*, denotado por* $supp(\alpha)$ *e definido como:*

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

Decorre diretamente da definição dos elementos de RG, que dados $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g \in RG$, $\alpha = \beta$ se, e somente se, $a_g = b_g, \forall\, g \in G$.

Temos agora, condições de definir a soma e a multiplicação em RG de forma bastante natural:

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

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

Vale notar que como R é um anel, $(a_g + b_g) = c_g, (a_g b_h) = d_j \in R$ e como G é um grupo $gh = j \in G$, desta forma, podemos concluir que

$$\alpha \cdot \beta = \sum_{j \in G} d_j j$$

Podemos ver com facilidade que, munido destas operações, RG é um anel com unidade, uma vez que, dados $\alpha = \sum_{g\in G} a_g g, \beta = \sum_{g\in G} b_g g, \gamma = \sum_{g\in G} c_g g \in RG$, temos

- $$\begin{aligned} \alpha + (\beta + \gamma) = & \sum_{g\in G} a_g g + (\sum_{g\in G} b_g g + \sum_{g\in G} c_g g) \\ = & \sum_{g\in G} a_g g + (\sum_{g\in G}(b_g + c_g)g) \\ = & \sum_{g\in G}(a_g + (b_g + c_g))g \\ = & \sum_{g\in G}((a_g + b_g) + c_g)g = (\sum_{g\in G}(a_g + b_g)g) + \sum_{g\in G} c_g g \\ = & (\sum_{g\in G} a_g g + \sum_{g\in G} b_g g) + \sum_{g\in G} c_g g \\ = & (\alpha + \beta) + \gamma \end{aligned}$$

- Existe $0 = \sum_{g\in G} 0g \in RG$ tal que

$$\begin{aligned} \alpha + 0 = & \sum_{g\in G} a_g g + \sum_{g\in G} 0g \\ = & \sum_{g\in G}(a_g + 0)g \\ = & \sum_{g\in G} a_g g \\ = & \alpha \end{aligned}$$

o outro lado é análogo.

- Existe $-\alpha = \sum_{g\in G}(-a_g)g \in RG$, tal que

$$\begin{aligned} -\alpha + \alpha = & \sum_{g\in G}(-a_g)g + \sum_{g\in G} a_g g \\ = & \sum_{g\in G}(-a_g + a_g)g \\ = & \sum_{g\in G} 0g \\ = & 0 \end{aligned}$$

o outro lado é análogo.

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

- $$\begin{aligned} \alpha \cdot (\beta \cdot \gamma) = & \sum_{g\in G} a_g g \cdot (\sum_{g\in G} b_g g \cdot \sum_{g\in G} c_g g) \\ = & \sum_{g\in G} a_g g \cdot (\sum_{g,h\in G}(b_g c_h)gh) \\ = & \sum_{g,h,j\in G}(a_g(b_h c_j))ghj \\ = & \sum_{g,h,j\in G}((a_g b_h)c_j)ghj \\ = & (\sum_{g,h\in G}(a_g b_h)gh) \cdot \sum_{g\in G} c_g g \\ = & (\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g) \cdot \sum_{g\in G} c_g g \\ = & (\alpha \cdot \beta) \cdot \gamma \end{aligned}$$

- $$\begin{aligned}\alpha \cdot (\beta + \gamma) = & \textstyle\sum_{g \in G} \cdot (\sum_{g \in G} b_g g + \sum_{g \in G} c_g g)\\ = & \textstyle\sum_{g \in G} a_g g \cdot (\sum_{g \in G} (b_g + c_g) g)\\ = & \textstyle\sum_{g,h \in G} (a_g (b_h + c_h)) gh\\ = & \textstyle\sum_{g,h \in G} (a_g b_h + a_g c_h) gh\\ = & \textstyle\sum_{g,h \in G} (a_g b_h) gh + \sum_{g,h \in G} (a_g c_h) gh\\ = & \textstyle(\sum_{g \in G} a_g g \cdot \sum_{g \in G} b_g g) + (\sum_{g \in G} a_g g \cdot \sum_{g \in G} c_g g)\\ = & \alpha \cdot \beta + \alpha \cdot \gamma\end{aligned}$$

- $$\begin{aligned}(\alpha + \beta) \cdot \gamma = & \textstyle(\sum_{g \in G} a_g g + \sum_{g \in G} b_g) \cdot \sum_{g \in G} c_g g\\ = & \textstyle(\sum_{g \in G} (a_g + b_g) g) \cdot \sum_{g \in G} c_g g\\ = & \textstyle\sum_{g,h \in G} ((a_g + b_g) c_h) gh\\ = & \textstyle\sum_{g,h \in G} (a_g c_h + b_g c_h) gh\\ = & \textstyle\sum_{g,h \in G} (a_g c_h) gh + \sum_{g,h \in G} (b_g c_h) gh\\ = & \textstyle(\sum_{g \in G} a_g g \cdot \sum_{g \in G} c_g g) + (\sum_{g \in G} b_g g \cdot \sum_{g \in G} c_g g)\\ = & \alpha \cdot \gamma + \beta \cdot \gamma\end{aligned}$$

- Existe $1 = \sum_{g \in G} x_g g \in RG$, onde $x_e = 1$, $x_g = 0, g \neq e$ tal que

$$\begin{aligned}1 \cdot \alpha = & \textstyle 1e \cdot \sum_{g \in G} a_g g\\ = & \textstyle\sum_{g \in G} (1 a_g) eg\\ = & \textstyle\sum_{g \in G} a_g g = \alpha\end{aligned}$$

o outro lado é análogo.

Além disso, podemos definir o produto de elementos $r \in R$ por elementos de RG como:

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

E com esta operação podemos verificar que RG é um R-módulo, pois dados $\alpha = \sum_{g \in G} a_g g, \beta = \sum_{g \in G} b_g g \in RG$ e $1, r, s \in R$, temos:

- $$\begin{aligned}(r + s)\alpha = & \textstyle(r + s) \sum_{g \in G} a_g g\\ = & \textstyle\sum_{g \in G} ((r + s) a_g) g\\ = & \textstyle\sum_{g \in G} (r a_g + s a_g) g\\ = & \textstyle\sum_{g \in G} r a_g g + \sum_{g \in G} s a_g g\\ = & \textstyle r(\sum_{g \in G} a_g g) + s(\sum_{g \in G} a_g g)\\ = & r\alpha + s\alpha\end{aligned}$$

- $$\begin{aligned} r(\alpha+\beta) = & \; r(\textstyle\sum_{g\in G} a_g g + \sum_{g\in G} b_g g) \\ = & \; r\textstyle\sum_{g\in G}(a_g+b_g)g \\ = & \; \textstyle\sum_{g\in G}(r(a_g+b_g))g \\ = & \; \textstyle\sum_{g\in G}(ra_g+rb_g)g \\ = & \; \textstyle\sum_{g\in G}(ra_g)g + \sum_{g\in G}(rb_g)g \\ = & \; r(\textstyle\sum_{g\in G} a_g g) + r(\sum_{g\in G} b_g g) \\ = & \; r\alpha + r\beta \end{aligned}$$

- $$\begin{aligned} r(s\alpha) = & \; r(s(\textstyle\sum_{g\in G} a_g g)) \\ = & \; r(\textstyle\sum_{g\in G}(sa_g)g) \\ = & \; \textstyle\sum_{g\in G}(r(sa_g))g \\ = & \; \textstyle\sum_{g\in G}((rs)a_g)g \\ = & \; (rs)(\textstyle\sum_{g\in G} a_g g) \\ = & \; (rs)\alpha \end{aligned}$$

- $$\begin{aligned} 1\alpha = & \; 1(\textstyle\sum_{g\in G}(1a_g)g) \\ = & \; \textstyle\sum_{g\in G} a_g g \\ = & \; \alpha \end{aligned}$$

Mais ainda, se R é comutativo, então RG é uma R-álgebra. De fato, para $r \in R$ e $\alpha, \beta \in RG$, temos:

$$\begin{aligned} r(\alpha\beta) = & \; r(\textstyle\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g) \\ = & \; r(\textstyle\sum_{g,h\in G}(a_g b_h)gh) \\ = & \; \textstyle\sum_{g,h\in G}(r(a_g b_h)gh) \\ = & \; \textstyle\sum_{g,h\in G}((ra_g)b_h)gh \\ = & \; \textstyle\sum_{g\in G}(ra_g)g \cdot \sum_{g\in G} b_g g \\ = & \; (r(\textstyle\sum_{g\in G} a_g g)) \cdot \sum_{g\in G} b_g g \\ = & \; (r\alpha)\beta \end{aligned}$$

Por outro lado,

$$\begin{aligned}
r(\alpha\beta) = & \; r(\textstyle\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g) \\
= & \; r(\textstyle\sum_{g,h\in G}(a_g b_h)gh) \\
= & \; \textstyle\sum_{g,h\in G}(r(a_g b_h)gh)gh \\
= & \; \textstyle\sum_{g,h\in G}(r a_g b_h)gh \\
= & \; \textstyle\sum_{g,h\in G}(a_g r b_g)gh \\
= & \; \textstyle\sum_{g,h\in G}(a_g(r b_h))gh \\
= & \; \textstyle\sum_{g\in G} a_g g \cdot \sum_{g\in G}(r b_g)g \\
= & \; \textstyle\sum_{g\in G} a_g g \cdot (r(\sum_{g\in G} b_g g)) \\
= & \; \alpha(r\beta)
\end{aligned}$$

Assim, RG é um anel, um R-módulo e quando R é comutativo, RG é uma R-álgebra. Veremos agora como G e R se relacionam com o anel RG.

Podemos definir uma inclusão $i : G \to RG$ dada por $i(x) = \sum_{g\in G} a_g g$, onde $a_x = 1$ e $a_g = 0$ quando $g \neq x$. Por esta identificação, podemos considerar G como um subconjunto de RG, mais ainda, podemos afirmar pela construção de RG, que G é uma base de RG sobre R. Logo, se G é finito, temos que o dim $(RG) = |G|$ sobre R.

Da mesma forma, considerando $\nu : R \to RG$ dada por $\nu(r) = \sum_{g\in G} a_g g$ onde $a_e = r$ e $a_g = 0$ quando $g \neq e$, temos que R pode ser considerado um subanel de RG, pois ν é injetivo.

Além estas identificações, dados $r \in R$ e $g \in G$, temos que $rg = gr$ e no caso em que R for comutativo, teremos $R \subset Z(RG)$.

Apresentaremos agora o Teorema de Maschke que nos dá uma caracterização dos anéis de grupo semissimples. Vale também a recíproca deste teorema e sua demonstração pode ser vista em (Milies e Sehgal, 2002, p. 141, [3]).

Teorema 4.1.3 ***Teorema de Maschke*** *Seja G um grupo. Então o anel de grupo RG é semissimples se as seguintes condições ocorrem:*

(i) *R é um anel semissimples.*

(ii) *G é finito.*

(iii) *$|G|$ é inversível em R.*

Demonstração: Assuma que R é anel semissimples, G é finito, $|G|$ é inversível em R e seja M um RG-submódulo de RG. Como R é semissimples, segue que RG é semissimples como R-módulo. Logo, existe N, R-submódulo de RG, tal que

$$RG = M \oplus N$$

Seja $\pi : RG \to M$ a projeção canônica associada a soma direta. Definimos $\pi^* : RG \to M$ pelo processo

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

Temos que π^* está bem definida, pois $\pi(gx) \in M$, para todo $x \in RG$ e todo $g \in G$. E assim, como M é um RG submódulo, $g^{-1}\pi(gx) \in M$, e portanto, $\pi^*(x) = \frac{1}{|G|}\sum_{g \in G} g^{-1}\pi(gx) \in M$.

Se provarmos que π^* é realmente um RG-homomorfismo tal que $(\pi^*)^2 = \pi^*$ e $Im(\pi^*) = M$, então $Ker(\pi^*)$ será um RG-submódulo tal que $RG = M \oplus Ker(\pi^*)$ e o teorema estará provado.

Como π^* é um R-homomorfismo, para mostrar que também é um RG-homomorfismo é suficiente mostrar que

$$\pi^*(ax) = a\pi^*(x), \quad \forall\, x \in G, \quad \forall\, a \in G$$

Temos que

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

Quando g percorre todos os elementos de G, o produto ga também percorre todos os elementos de G, e assim

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

Como π é uma projeção em M, sabemos que $\pi(m) = m$, para todo $m \in M$. Além disso, como M é um RG-módulo, temos que $gm \in M$, para todo $g \in G$. E assim,

$$\pi^*(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gm) = \frac{1}{|G|} \sum_{g \in G} g^{-1}gm = \frac{1}{|G|}(\underbrace{m + \cdots + m}_{|G| \text{ vezes}}) = m$$

e segue que $Im(\pi^*) = M$. Ainda temos que, para todo $x \in RG$,

$$\pi^*(\pi^*(x)) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi\,\underbrace{(g\pi^*(x))}_{\in M} = \frac{1}{|G|} \sum_{g \in G} g^{-1}(g\pi^*(x)) = \pi^*(x)$$

ou seja, $(\pi^*)^2 = \pi^*$.

Por fim, considerando a sequência exata

$$0 \to Ker(\pi^*) \xrightarrow{i} RG \xrightarrow{\pi^*} M \to 0$$

Tomemos $\varphi = \pi^*_{|M} : M \to RG$, e notemos que $Im(\pi^*) = M \subset RG$. Assim, φ é um homomorfismo de RG-módulos tal que $\pi^* \circ \varphi = Id_M$. De fato, como π^* é sobrejetor, dado $m \in M$, existe $x \in RG$ tal que $\pi^*(x) = m$ e assim,

$$(\pi^* \circ \varphi)(m) = (\pi^* \circ \varphi)(\pi^*(x)) = \pi{*}(\pi^*(\pi^*(x))) = \pi^*(x) = m$$

Portanto, a sequência se fatora e $RG = M \oplus Ker(\pi^*)$. ■

Corolário 4.1.4 *Seja G um grupo finito e K um corpo. Então, KG é semissimples se, e somente se, $char(K) \nmid |G|$.*

Demonstração: $|G|$ é inversível em K se, e somente se, $char(K) \nmid |G|$. Logo, pelo Teorema de Maschke 4.1.3, KG é semissimples se, e somente se, $char(K) \nmid |G|$. ■ Veremos agora a versão do Teorema de Wedderburn-Artin para anéis de grupo.

Teorema 4.1.5 *Seja G um grupo finito e seja K um corpo tal que $char(K) \nmid |G|$. Então:*

(i) KG é a soma direta de um número finito de ideais bilaterais $\{B_i\}_{1\leq i\leq r}$, chamados de componentes simples de KG. Cada B_i é um anel simples.

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

(iii) Cada componente simples B_i é isomorfo a um anel de matrizes da forma $M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia isomórfica de K em seu centro, e o isomorfismo

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

é um isomorfismo de K-álgebras.

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

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_{n_i} & 0 & \cdots & 0 \end{bmatrix} | x_1, x_2, \ldots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

é um ideal minimal a esquerda.

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

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

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

Demonstração: A demonstração deste teorema é análoga às apresentadas nos resultados na Seção 3.2. ■

Corolário 4.1.6 *Seja G um grupo finito e K um corpo algebricamente fechado, tal que $char(K) \nmid |G|$. Então:*

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

e $n_1^2 + n_2^2 + \ldots + n_r^2 = |G|$.

Demonstração: Como $char(K) \nmid |G|$, temos que

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

onde D_i é um anel de divisão que contém uma cópia de K em seu centro.

Se calcularmos as dimensões sobre K em ambos os lados da equação acima, teremos

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

onde $[D_i : K]$ é a dimensão de D_i sobre K. E assim, segue que cada anel de divisão é de dimensão finita sobre K. Como K é algebricamente fechado, temos que $D_i = K, 1 \leq i \leq r$ e o resultado segue. ■

4.2 Decomposição de Álgebras Semissimples

Nesta seção veremos com mais detalhes o processo de obtenção das componentes simples de um anel de grupo. Iremos focar no caso em que $K = \mathbb{C}$, mas resultados similares podem ser obtidos com outros corpos, como em (Milies e Sehgal, 2002, p. 144, [3]). Iniciaremos com as definições de classe de conjugação e de soma de classe. Seja G um grupo, definiremos uma relação de equivalência sobre G da seguinte forma:

$$\forall\, x, y \in G, x \text{ está relacionado com } y \Leftrightarrow \exists\, g \in G \text{ tal que } y = g^{-1}xg$$

Quando x está relacionado com y pela relação acima, dizemos que x e y são elementos **conjugados** em G.

Definição 4.2.1 *O conjunto $\overline{x} = \{y \in G | y = g^{-1}xg, \text{ para algum } g \in G\}$ é chamado de* ***classe de conjugação*** *em G do elemento x. Denotaremos as classes de conjugação de G por C_x.*

Exemplo 4.2.2 *Vamos calcular as classes de conjugação do grupo das permutações de 3 elementos, $S_3 = \{I, (12), (13), (23), (123), (132)\}$:*

$C_1 = \{I\}$, *pois* $y = g^{-1}Ig = g^{-1}g = I$;

$C_2 = \{(12), (13), (23)\}$, *pois* $(13) = (123)(12)(132)$ *e* $(23) = (132)(12)(123)$;

$C_3 = \{(123), (132)\}$, *pois* $(132) = (12)(123)(12)$.

Podemos perceber que existem 3 classes de conjugação do grupo S_3.

Definição 4.2.3 *Sejam G um grupo, R um anel comutativo, $\{C_i\}_{i \in I}$ o conjunto de classes de conjugação de G. Para cada índice $i \in I$, definimos $\gamma_i = \hat{C}_i = \sum_{x \in C_i} x$. Esses elementos são chamado de* ***somas de classe*** *de G sobre R.*

Teorema 4.2.4 *Seja G um grupo e R um anel comutativo. Então o conjunto $\{\hat{C}_i\}_{i\in I}$ de todas as classes de conjugação forma uma base de $\mathcal{Z}(RG)$, o centro de RG, sobre R.*

Demonstração: Dado $g \in G$, notemos que

$$\begin{aligned} g^{-1}\hat{C}_i g = & \ g^{-1}(\textstyle\sum_{x\in C_i} x)g \\ = & \ \textstyle\sum_{x\in C_i} g^{-1}xg \\ = & \ \textstyle\sum_{y\in C_i} y \\ = & \ \hat{C}_i \end{aligned}$$

Disso decorre que $\hat{C}_i g = g\hat{C}_i$ e, portanto, $\hat{C}_i \in \mathcal{Z}(RG)$.

Além disso, suponhamos que $\sum_{i\in I} r_i\hat{C}_i = 0$, então, $\sum_{i\in I} r_i \sum_{x\in C_i} x = 0$, pois as classes de equivalência são disjuntas. Como o conjunto G é LI, e acima temos uma combinação linear de elementos de G igual a 0, segue que $r_i = 0, \forall\, i \in I$ e portanto, o conjunto $\{\hat{C}_i\}_{i\in I}$ é linearmente independente.

Tomemos agora $\alpha = \sum a_g g \in \mathcal{Z}(RG)$. Então, para todos $x \in G$,

$$x^{-1}\alpha x = x^{-1}(\sum a_g g)x = \sum a_g x^{-1}gx = \sum a_g h$$

onde h está na mesma classe de conjugação de g. Por outro lado, como $\alpha \in \mathcal{Z}(RG)$, $x\alpha = \alpha x \Rightarrow \alpha = x^{-1}\alpha x$, e assim,

$$\alpha = \sum a_g h \Rightarrow a_g = a_h$$

Em outras palavras, para todo elemento do centro de RG, os coeficientes de elementos de uma mesma classe de conjugação são iguais, assim, podemos reescrever α agrupando os elementos de uma mesma classe: $\alpha = \sum a_i\hat{C}_i$. E portanto, $\{\hat{C}_i\}_{i\in I}$ é gerador de $\mathcal{Z}(RG)$. ■

Proposição 4.2.5 *Seja G um grupo finito e K um corpo algebricamente fechado, tal que $char(K) \nmid |G|$. Então, o número de componentes simples de KG é igual ao número de classes de conjugação de G.*

Demonstração: Pelo Teorema 4.2.4, dim $\mathcal{Z}(KG)$ é igual ao número de classes de conjugação de G. Veremos agora que dim $\mathcal{Z}(KG)$ é igual ao número de componentes simples de KG.

Sabemos que $KG \simeq \oplus_{i=1}^{r} M_{n_i}(K)$, então, $\mathcal{Z}(KG) \simeq \oplus_{i=1}^{r}\mathcal{Z}(M_{n_i}(K))$. Além disso, $\mathcal{Z}(M_n(K)) = \{aI | a \in K\}$, o que implica em $\mathcal{Z}(M_n(K)) \simeq K$. Logo, $\mathcal{Z}(KG) \simeq \oplus_{i=1}^{r} K$ e portanto, dim $\mathcal{Z}(KG) = r$ e r é o número de componentes simples de KG. ■

Exemplo 4.2.6 *Conforme vimos no Exemplo 4.2.2,* S_3 *tem* 3 *classes de conjugação, logo,* $\mathbb{C}S_3$ *tem* 3 *componentes simples:*

$$\mathbb{C}S_3 = A_1 \oplus A_2 \oplus A_3$$

Como $\mathbb{C}S_3$ *tem dimensão* 6 *sobre* $\mathbb{C}$*, sabemos que a soma das dimensões de* A_1, A_2, A_3 *também deve ser* 6*. Como estamos tratando de anéis de matrizes com entradas em* $\mathbb{C}$*, nossa única possibilidade é:*

$$\begin{aligned} \mathbb{C}S_3 = &\quad M_1(\mathbb{C}) \oplus M_1(\mathbb{C}) \oplus M_2(\mathbb{C}) \\ = &\quad \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}). \end{aligned}$$

5 REPRESENTAÇÕES DE GRUPO

Neste capítulo apresentaremos a definição e alguns exemplos das Representações de Grupo. Em seguida, veremos a relação próxima que podemos estabelecer entre as representações e os módulos de um grupo. Por fim, usaremos esta relação para determinar as representações irredutíveis de alguns grupos.

5.1 Definições e Exemplos

As representações de um grupo estão ligadas a um espaço vetorial de dimensão finita, desta forma, podem facilmente ser representadas também por matrizes. Assim, iniciamos a seção com algumas definições.

Definição 5.1.1 *Sejam G um grupo, R um anel comutativo e V um R-módulo de dimensão finita (ou espaço vetorial). Uma* ***representação*** *de G sobre R, com espaço representativo V, é um homomorfismo de grupo $T : G \to GL(V)$, onde $GL(V)$ denota o grupo de automorfismos (operadores lineares) de V. A dimensão de V é chamada de* ***grau da representação*** *T e é denotada por $deg(T)$.*

Como para todo $g \in G$, a imagem de g é um operador linear em V, denotaremos $T(g) = T_g : V \to V$. É importante notar que, como T é um homomorfismo de grupos, para $g, h \in G$, teremos $T_{gh} = T_g \circ T_h$ e $T_e = I$.

Conforme dito anteriormente, ao fixarmos uma base para V, podemos estabelecer um isomorfismo entre $GL(V)$ e $GL(n, R)$, ou seja, associamos cada operador T_g com sua matriz na base fixada. Desta forma, temos a definição a seguir:

Definição 5.1.2 *Seja G um grupo e R um anel comutativo. A* ***representação matricial*** *de G sobre R de grau n é o homomorfismo de grupos $T : G \to GL(n, R)$.*

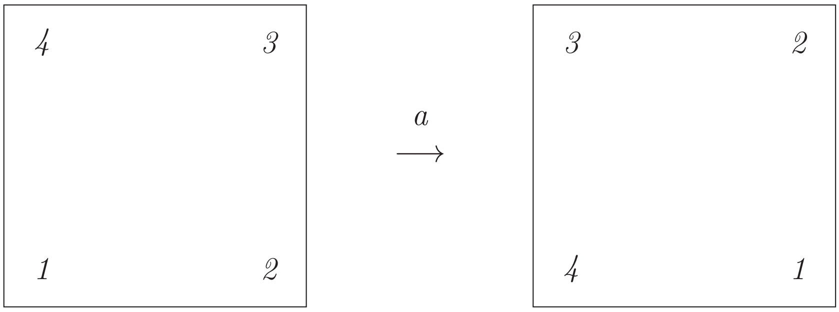
Veremos agora alguns exemplos de representações de grupos:

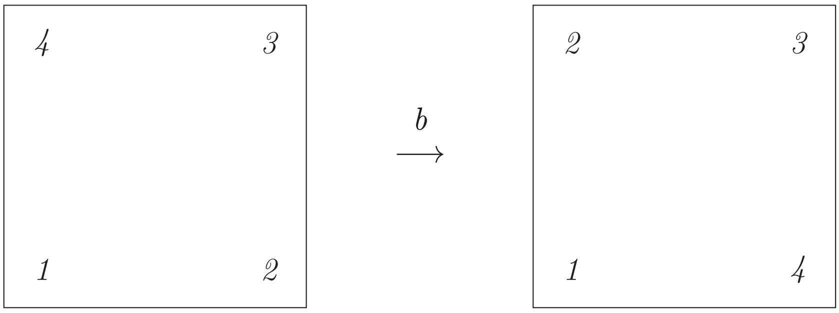
Exemplo 5.1.3 *Dado um grupo G e um anel R, a representação $T : G \to GL(n, R)$ que associa todos os elementos de G com o elemento identidade de $GL(n, R)$ é chamada de* ***representação trivial*** *de grau n.*

Exemplo 5.1.4 *Consideremos D_4 o grupo de todas as simetrias de um quadrado. Sendo a a rotação deste quadrado por um ângulo de $\frac{\pi}{2}$ e b a reflexão por uma diagonal, podemos descrever o conjunto da seguinte forma:*

$$D_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

onde a e b são os geradores do conjunto.





Se pensarmos no significado geométrico de a e b como duas transformações lineares do plano nele mesmo, podemos calcular suas matrizes sobre a base canônica de $\mathbb{R}^2$*, obtendo uma representação* W *de grau 2 para* D_4*:*

$$\begin{array}{cc} a(1,0) = (0,1) & a(0,1) = (-1,0) \\ b(1,0) = (0,1) & b(0,1) = (1,0) \end{array}$$

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

Exemplo 5.1.5 *Seja* S_n *o grupo das permutações de* n *elementos. Podemos definir uma representação* $S : S_n \to (R)$*, da seguinte forma:*

$$S(\sigma) = \begin{cases} 1, & se\ \sigma\ é\ permutação\ par \\ -1, & se\ \sigma\ é\ permutação\ ímpar \end{cases}$$

Esta é a chamada ***representação sinal****. Lembramos que uma permutação é par se o número de trocas que devemos realizar entre seus elementos para recuperar a ordem original da sequência for par. A permutação é ímpar se este número for ímpar.*

Exemplo 5.1.6 *Seja $\phi : S_n \to GL(n, \mathbb{C})$, dada por $\phi(\sigma)$ sendo a matriz identidade com as linhas permutadas de acordo com σ. Por exemplo, se $n = 3$, temos*

$$\phi(Id) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \phi((12)) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \phi((123)) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Esta é a chamada ***representação standard****.*

Exemplo 5.1.7 *Seja $G = \{1, a, a^2, \ldots, a^{m-1}\}$ um grupo cíclico de ordem m e K um corpo. Uma representação matricial $A : G \to GL(n, K)$ é totalmente determinada pela matriz $A(a)$, imagem do gerador do conjunto G, pois $A(a^r) = A(a)^r$.*

Consideremos o conjunto $G = \{1, a, a^2\}$ e sua representação em $GL(3, \mathbb{C})$:

$$A(a) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} + \frac{\sqrt{3}}{2}i & 0 \\ 0 & 0 & -\frac{1}{2} - \frac{\sqrt{3}}{2}i \end{bmatrix}$$

$$A(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, A(a^2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} - \frac{\sqrt{3}}{2}i & 0 \\ 0 & 0 & -\frac{1}{2} + \frac{\sqrt{3}}{2}i \end{bmatrix}$$

Podemos ver que a diagonal de $A(a)$ possui as raízes cúbicas da unidade em sua diagonal principal. Veremos em futuros exemplos que isso é comum em algumas representações.

Exemplo 5.1.8 *Seja $K = \{1, a, b, ab\}$ o grupo 4-Klein, que possui 3 elementos de ordem 2. Esta é sua tábua de operação:*

	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	a
b	b	ab	1	a
ab	ab	b	a	1

Iremos determinar uma representação $T : K \to GL(2, \mathbb{Z})$:

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

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

Repare que, como a, b, ab têm ordem 2, procuramos determinar esta representação utilizando matrizes que ao quadrado são iguais a matriz identidade.

Veremos agora, uma representação que está associada ao anel de grupo RG e tem grau igual a $|G|$:

Exemplo 5.1.9 *Definiremos a chamada* ***representação regular*** $\rho : G \to GL(RG)$ *por* $\rho_g(x) = gx$*, ou seja, associamos cada elemento de* G *ao operador linear que age pela multiplicação a esquerda em cada elemento da base de* RG*, que é precisamente o próprio* G*. Podemos ver que* ρ *é realmente uma representação, pois*

$$\rho_{gh}(y) = (gh)y = g(h(y)) = g(\rho_h(y)) = \rho_g(\rho_h(y)) = (\rho_g \circ \rho_h)(y)$$

Vejamos a representação regular do grupo 4*-Klein apresentado no Exemplo 5.1.8. Como* $a1 = a, aa = 1, ab = ab, aab = b$*, a representação matricial de* ρ_a *será:*

$$\rho_a = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Da mesma forma, podemos determinar as demais representações deste grupo:

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

Perceba que todas as matrizes apresentadas são a matriz identidade com suas linhas ou colunas permutadas. Esta é a principal característica da representação regular. Outra importante característica desta representação é que ela é fiel, ou seja, é uma representação injetiva.

De fato, sejam $g, h \in G$ *tais que* $\rho(g) = \rho(h)$*. Assim,*

$$\begin{array}{rl} \rho_g : & RG \to RG \\ & g_i \mapsto gg_i \end{array} \qquad \begin{array}{rl} \rho_h : & RG \to RG \\ & g_i \mapsto hg_i \end{array}$$

o que implica em $gg_i = hg_i \Rightarrow g = h$*. Logo,* ρ *é injetiva.*

Dadas duas representações $T : G \to GL(n, R)$ e $S : G \to GL(m, R)$, podemos definir uma representação $T \oplus S : G \to GL(n + m, R)$, dada por $(T \oplus S)_g = T_g \oplus S_g$, ou ainda,

$$(T \oplus S)_g = \begin{bmatrix} T_g & 0 \\ 0 & S_g \end{bmatrix}$$

Agora, apresentaremos algumas definições sobre representações.

Definição 5.1.10 *Duas representações $T : G \to GL(V)$ e $S : G \to GL(W)$ de um grupo G sobre um corpo K são chamadas de* ***equivalentes*** *se existir um isomorfismo $\phi : V \to W$ tal que $S_g = \phi \circ T_g \circ \phi^{-1}$, para todo $g \in G$.*

Definição 5.1.11 *Duas representações $T : G \to GL(n, K)$ e $S : G \to GL(n, K)$ de um grupo G em um corpo K são chamadas de* ***equivalentes*** *se existir uma matriz inversível $U \in GL(n, K)$ tal que $T_g = US_gU^{-1}$ para todo $g \in G$.*

Como exemplo, se tomarmos duas representações de G sobre um mesmo espaço vetorial, mas com bases diferentes, obteremos matrizes diferentes, porém equivalentes.

Para a próxima definição, precisamos lembrar da definição de subespaço invariante. Dado um operador linear $T : V \to V$, dizemos que um subespaço $W \subset V$ é T-invariante se, para todo $w \in W$, temos $T(w) \in W$.

Definição 5.1.12 *Uma representação $T : G \to GL(V)$ de um grupo G sobre um corpo K é chamada de* ***irredutível*** *se V é diferente de $\{0\}$ e os únicos subespaços T-invariantes de V são $\{0\}$ e V. Caso contrário, dizemos que T é* ***redutível****.*

Definição 5.1.13 *Uma representação $T : G \to GL(V)$ é chamada de* ***completamente redutível*** *se para todo subespaço T-invariante W, existe um subespaço T-invariante W', tal que $V = W \oplus W'$.*

Observe que um subespaço W de V é T-invariante, quando W é T_g-invariante para todo $g \in G$. Além disso, representações redutíveis tem matrizes triangulares superiores por blocos e representações completamente redutíveis tem matrizes diagonais por blocos. Vejamos alguns exemplos:

Exemplo 5.1.14 *A representação regular é sempre redutível. De fato, como na representação regular tomamos $V = RG$, o elemento $\hat{G} = \sum_{g \in G} g \in RG$ gera um subespaço ρ-invariante não trivial, pois para todo $h \in G$,*

$$\rho_h(\hat{G}) = h \cdot \hat{G} = \sum_{g \in G} hg = \sum_{x \in G} x = \hat{G}$$

Logo, $\hat{G}$ é invariante por ρ.

Exemplo 5.1.15 *Seja W a representação definida no Exemplo 5.1.4. Verificaremos que W é uma representação irredutível.*

De fato, considerando $\mathbb{R}^2$ como espaço vetorial, queremos encontrar um subespaço W-invariante S. Se $dim_{\mathbb{R}} S = 0$, $S = \{0\}$ que é W-invariante. Da mesma forma, se

$dim_{\mathbb{R}}S = 2$, $S = \mathbb{R}^2$ e também é W-invariante. Resta verificar o caso em que $dim_{\mathbb{R}}S = 1$. Neste caso, $S = [v]$ e assim, $W(v) = \lambda v$. Estamos procurando então um subespaço gerado por um autovetor v de $W(a)$ e $W(b)$ simultaneamente. Para isto, iremos calcular os autovalores de $W(a)$ e $W(b)$:

$$\begin{vmatrix} -x & -1 \\ 1 & -x \end{vmatrix} = x^2 + 1 \Rightarrow x^2 + 1 = 0 \Rightarrow x = \pm i$$

$$\begin{vmatrix} -x & 1 \\ 1 & -x \end{vmatrix} = x^2 - 1 \Rightarrow x^2 - 1 = 0 \Rightarrow x = \pm 1$$

Como x precisa ser autovalor de $W(a)$ e de $W(b)$ ao mesmo tempo, S não possui autovalores e consequentemente não possui autovetores. Portanto W é irredutível pois os únicos subespaços invariantes são $\{0\}$ e $\mathbb{R}^2$.

5.2 Módulos e Representações

Nesta seção, veremos que estabelecer uma relação biunívoca entre RG-módulos e as representações de G sobre R nos ajuda a determinar estas representações com mais facilidade.

Dados os conjuntos A das representações de um grupo G sobre um anel R e o conjunto B dos RG-módulos livres de dimensão finita sobre R, podemos estabelecer as seguintes bijeções:

$$\begin{array}{rccc} \phi : & A & \longrightarrow & B \\ & T : G \to GL(V) & \longmapsto & {}_{RG}V \end{array}$$

onde a ação de V é dada por $\alpha v = (\sum_{g\in G} a_g g)v = \sum_{g\in G} a_g T_g(v)$.

$$\begin{array}{rccccccccc} \psi : & B & \longrightarrow & A & & & & & & \\ & {}_{RG}M & \longmapsto & T : & G & \to & GL(M) & & & \\ & & & & g & \mapsto & Tg : & M & \to & M \\ & & & & & & & m & \mapsto & gm \end{array}$$

Afirmamos que $\phi = \psi^{-1}$. De fato, dada $T \in A$,

$$\begin{array}{rcccc} (\psi \circ \phi)(T) = \psi({}_{RG}V) = & L : & G & \to & GL(V) \\ & & g & \mapsto & L_g : \quad V \to V \end{array}$$

Mas como $L_g(v) = gv = 1 \cdot (gv) = 1 \cdot T_g(v) = T_g(v)$, teremos que $L = T$. Por outro lado, dado $M \in B$, temos

$$\begin{aligned}
(\phi \circ \psi)(M) = \quad & \phi \left(\begin{array}{cccccc} T: & G & \to & GL(M) & & \\ & g & \mapsto & T_g: & M & \to & M \\ & & & & m & \mapsto & gm \end{array} \right) \\
= \quad & {}_{RG}M
\end{aligned}$$

pois, $\left(\sum_{g \in G} a_g g\right) m = \sum_{g \in G} a_g T_g(m) = \sum_{g \in G} a_g g \cdot m$.

Portanto, $\phi \circ \psi = I = \psi \circ \phi$.

A proposição a seguir não será demonstrada por sua extensão, mas ela nos mostra a utilidade de estabelecer a associação acima:

Proposição 5.2.1 *Sejam 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 (respectivamente completamente redutível) se, e somente se, seu RG-módulo correspondente é simples (respectivamente semissimples).*

Esta proposição nos mostra que para determinar as representações irredutíveis de um grupo G sobre um anel R, podemos nos valer da decomposição de RG em componentes simples, que serão módulos simples ou semissimples. Assim, para cada componente da decomposição de RG associamos uma representação irredutível ou completamente redutível. Na próxima seção veremos isto em alguns exemplos.

5.3 Mais exemplos

Exemplo 5.3.1 *Seja $K_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ o grupo das unidades básicas dos quatérnios com a operação de multiplicação. Podemos vê-lo como o gerado pelas unidades i e j, pois $1 = i^4, -1 = i^2, -i = i^3, -j = i^2 j, k = ij, -k = i^3 j$.*

Calculando as classes de conjugação, obtemos as 5 classes:

$$C_1 = \{1\},\ C_2 = \{-1\},\ C_3 = \{i, -i\},\ C_4 = \{j, -j\},\ C_5 = \{k, -k\}.$$

E portanto o número de componentes simples de $\mathbb{C}K_8$ é 5:

$$\mathbb{C}K_8 = A_1 \oplus A_2 \oplus A_3 \oplus A_4 \oplus A_5$$

Como a dimensão de $\mathbb{C}K_8$ sobre $\mathbb{C}$ é 8 e A_i são anéis de matrizes, temos que as dimensões serão: dim $A_1 =$ dim $A_2 =$ dim $A_3 =$ dim$A_4 = 1$ e dim $A_5 = 4$, ou seja,

$$\mathbb{C}K_8 = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$$

Seja T um representação de K_8 sobre $\mathbb{C}$, então $T = T_1 \oplus T_2 \oplus T_3 \oplus T_4 \oplus T_5$. Assim devemos determinar 4 representações não equivalentes de grau 1 e uma representação de grau 2.

$$\begin{array}{ll} T_1(i) = 1 & T_1(j) = 1 \\ T_2(i) = 1 & T_2(j) = -1 \\ T_3(i) = -1 & T_3(j) = 1 \\ T_4(i) = -1 & T_4(j) = -1 \end{array}$$

Nos resta ainda, determinar uma representação de grau 2. Podemos deduzi-la por tentativas, utilizando as identidades $i^2 = j^2 = -1$, $i^4 = 1$, $ij = k$, porém este é um método bastante trabalhoso e pouco metódico. Assim, utilizaremos resultados posteriores para determinar T_5 no Exemplo 6.2.2

Exemplo 5.3.2 *Conforme visto no Exemplo 4.2.6, o anel de grupo $\mathbb{C}S_3$ possui 3 componentes simples:*

$$\mathbb{C}S_3 = \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}).$$

Sabemos que devemos encontrar 3 representações irredutíveis, duas de grau 1 para as primeiras componentes do anel de grupo e uma de grau 2 para a última componente. Sejam então T_1, T_2, T_3 estas representações. Definiremos as representações apenas nos geradores, como representações são homomorfismos, precisamos definir matrizes de forma que $T(gh) = T(g)T(h)$. Podemos definir T_1 como a representação trivial e T_2 como a representação sinal:

$$\begin{array}{lcl} T_1((12)) = 1 & e & T_1((123)) = 1. \\ T_2((12)) = -1 & e & T_2((123)) = 1. \end{array}$$

Claramente estas duas transformações atendem a propriedade $T(gh) = T(g)T(h)$. Devemos definir agora uma representação T_3 de grau 2, de forma que:

$$T_3((12))^2 = T_3(I) = I_2 \text{ e } T_3((123))^3 = T_3(I) = I_2.$$

Com algumas tentativas, obtemos as seguintes matrizes:

$$T_3((12)) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ e } T_3((123)) = \begin{bmatrix} \dfrac{-1+\sqrt{3}i}{2} & 0 \\ 0 & \dfrac{-1-\sqrt{3}i}{2} \end{bmatrix}$$

Desta forma obtemos a matriz T para cada gerador, cuja diagonal são as matrizes T_1, T_2, T_3 em blocos:

$$T((12)) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$T((123)) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \dfrac{-1+\sqrt{3}i}{2} & 0 \\ 0 & 0 & 0 & \dfrac{-1-\sqrt{3}i}{2} \end{bmatrix}$$

No próximo capítulo veremos mais uma ferramenta que nos ajudará a determinar todas as representação de um grupo: os caracteres.

6 CARACTERES DE GRUPO

Neste capítulo veremos a definição de caracteres. Esta definição depende das representações de grupo, mas veremos que, com alguns resultados, podemos fazer o oposto, ou seja, conhecer o carácter de uma representação pode nos ajudar a determinar a matriz desta representação com mais facilidade.

6.1 Definição e exemplos

Iniciaremos com a definição e alguns exemplos de caracteres de grupos já apresentados anteriormente.

Definição 6.1.1 *Sejam G um grupo, V um espaço vetorial de dimensão finita sobre um corpo K e $T : G \to GL(V)$ a representação de G sobre K. Então o* ***carácter*** χ ***de*** G ***dado pela representação*** T*, é a associação $\chi : G \to K$ dada por $\chi(g) = tr(T_g)$, para todo $g \in G$.*

Denotamos o grau de um caracter χ por $gr(\chi)$ e o definimos como sendo igual ao grau da representação T.

Note que, se $char(K) = 0$, temos

$$\chi(1_G) = tr(T_{1_G}) = tr(I) = [V : K] = gr(\chi)$$

Em particular, se T é a representação regular, $\chi(1_G) = gr(\chi) = |G|$.

Em geral, χ não é um homomorfismo, porém quando $gr(\chi) = 1$, temos que $\chi = T$ e χ será um homomorfismo. Caracteres de grau 1 são chamados de caracteres lineares. O caso especial onde $\chi(g) = 1$, para todo $g \in G$ é chamado de carácter principal.

Ainda, se $T_1, \ldots, T_r$ são representações de G com caracteres $\chi_1, \ldots, \chi_r$, então $T = T_1 \oplus \cdots \oplus T_r$ gera o carácter $\chi = \chi_1 + \cdots + \chi_r$.

Veremos agora alguns resultados que nos ajudam a encontrar caracteres de representações.

Lema 6.1.2 *Se U é uma matriz inversível, então $tr(U^{-1}AU) = tr(A)$.*

Demonstração: Inicialmente, proveremos que $tr(AB) = tr(BA)$. Assim, sejam $A, B \in$

$M_n(K)$ tais que:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}, B = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{bmatrix}$$

Assim,

$$AB = \begin{bmatrix} a_{11}b_{11} + \cdots + a_{1n}b_{n1} & \cdots & a_{11}b_{1n} + \cdots + a_{1n}b_{nn} \\ \vdots & & \vdots \\ a_{n1}b_{11} + \cdots + a_{nn}b_{n1} & \cdots & a_{n1}b_{1n} + \cdots + a_{nn}b_{nn} \end{bmatrix}$$

Logo,

$$\begin{aligned} tr(AB) = & \ (a_{11}b_{11} + \cdots + a_{1n}b_{n1}) + \cdots + (a_{n1}b_{1n} + \cdots + a_{nn}b_{nn}) \\ = & \ a_{11}b_{11} + \cdots + a_{1n}b_{n1} + \cdots + a_{n1}b_{1n} + \cdots + a_{nn}b_{nn} \\ = & \ \sum a_{ij}b_{ji} \end{aligned}$$

Por outro lado,

$$BA = \begin{bmatrix} b_{11}a_{11} + \cdots + b_{1n}a_{n1} & \cdots & b_{11}a_{1n} + \cdots + b_{1n}a_{nn} \\ \vdots & & \vdots \\ b_{n1}a_{11} + \cdots + b_{nn}a_{n1} & \cdots & b_{n1}a_{1n} + \cdots + b_{nn}a_{nn} \end{bmatrix}$$

Logo,

$$\begin{aligned} tr(BA) = & \ (b_{11}a_{11} + \cdots + b_{1n}a_{n1}) + \cdots + (b_{n1}a_{1n} + \cdots + b_{nn}a_{nn}) \\ = & \ b_{11}a_{11} + \cdots + b_{1n}a_{n1} + \cdots + b_{n1}a_{1n} + \cdots + b_{nn}a_{nn} \\ = & \ \sum b_{ij}a_{ji} \end{aligned}$$

Como K é comutativo, para todo $1 \leq i \leq n$, e para todo $1 \leq j \leq n$, teremos que $\sum a_{ij}b_{ji} = \sum b_{ij}a_{ji}$ e portanto $tr(AB) = tr(BA)$.

Desta forma,

$$tr(U^{-1}AU) = tr(U^{-1}(AU)) = tr((AU)U^{-1}) = tr(A)$$

■

O resultado acima será útil para provarmos duas propriedades importantes dos caracteres.

Lema 6.1.3 *(i) Se T e T' são representações equivalentes, então elas geram o mesmo carácter.*

(ii) Caracteres são constantes nas classes de conjugação de G.

Demonstração:

(i) Se T e T' são equivalentes, então existe uma matriz inversível U tal que $T = U^{-1}T'U$, logo

$$\chi = tr(T) = tr(U^{-1}T'U) = tr(T') = \chi'$$

(ii) Se $g, h \in G$ pertencem a mesma classe de conjugação, existe $x \in G$ tal que $g = x^{-1}hx$, logo

$$\chi(g) = tr(T_g) = tr(T_{x^{-1}hx}) = tr(T_{x^{-1}}T_hT_x) = tr(T_h) = \chi(h)$$

■

Proposição 6.1.4 *Seja G um grupo finito e K um corpo tal que $char(K) \nmid |G|$. Se $\chi_1, \ldots, \chi_r$ denotam os caracteres dados por um conjunto completo de representações irredutíveis e não equivalentes de G sobre K, então o conjunto de todos os caracteres de G sobre K é o conjunto das combinações lineares não nulas da forma $\chi = \sum_{i=1}^{r} n_i\chi_i$, onde cada n_i é um inteiro não negativo.*

Demonstração: Sejam $\{T_1, \ldots, T_r\}$ o conjunto completo de todos as representações não equivalentes e irredutíveis de G sobre K, então qualquer outra representação T de G sobre K pode ser escrita na forma $T = \oplus_{i=1}^{r} n_iT_i$, com $n_i \leq 0$, $1 \leq i \leq r$. Assim, se χ é o carácter dado por T, temos que $\chi = \sum_{i=1}^{r} n_i\chi_i$. ■

Exemplo 6.1.5 *Seja $A : G \to GL(3, \mathbb{C})$ onde $G = \{1, a, a^2\}$, conforme visto no Exemplo 5.1.7. Temos que*

$$\begin{aligned}
\chi(1) &= tr(A(1)) = 1 + 1 + 1 = 3 \\
\chi(a) &= tr(A(a)) = 1 + \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) + \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = 0 \\
\chi(a^2) &= tr(A(a^2)) = 1 + \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) + \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = 0
\end{aligned}$$

Exemplo 6.1.6 *Seja G um grupo finito de ordem n. Denotaremos por $\rho : G \to \mathbb{C}$ o carácter regular, dado pela representação regular de G sobre $\mathbb{C}$. Seja $\mathbb{C}G \simeq \oplus_{i=1}^{r} M_{n_i}(\mathbb{C})$ a decomposição de $\mathbb{C}G$ como soma direta de componentes simples.*

Se $I_i \simeq \mathbb{C}^{n_i}$ (lembrando que $I_i \subset M_{n_i}(\mathbb{C})$ é o conjunto das matrizes que são nulas com exceção da coluna i) é o $\mathbb{C}G$-módulo irredutível correspondente à i-ésima componente simples, é fácil ver que, como $\mathbb{C}G$-módulos, temos

$$M_{n_i}(\mathbb{C}) \simeq \underbrace{I_i \oplus \cdots \oplus I_i}_{n_i \ vezes}$$

e assim,

$$\mathbb{C}G \simeq \underbrace{I_1 \oplus \cdots \oplus I_1}_{n_1 \ vezes} \oplus \cdots \oplus \underbrace{I_r \oplus \cdots \oplus I_r}_{n_r \ vezes}$$

Se T_i denota a representação irredutível de G sobre $\mathbb{C}$ correspondente a I_i, e χ_i seu carácter, para todo $1 \leq i \leq r$, então podemos escrever a representação T de G sobre $\mathbb{C}$ como:

$$T = \oplus_{i=1}^{r} n_iT_i$$

e calculando os traços, obtemos:

$$\rho = \sum_{i=1}^{r} n_i \chi_i$$

Como $n_i = gr(T_i) = \chi(1)$*, podemos reescrever a fórmula acima como*

$$\rho(g) = \sum_{i=1}^{r} \chi_i(1)\chi_i(g) \tag{6.1}$$

Lembrando que $\rho(1) = |G|$ *e* $\rho(g) = 0$ *quando* $g \neq 1$.

A partir de agora, iremos focar o estudo em caracteres complexos, ou seja, caracteres de um grupo G sobre o corpo $\mathbb{C}$. Consideremos então a decomposição de $\mathbb{C}G$:

$$\mathbb{C}G = \oplus_{i=1}^{r}(\mathbb{C}G)e_i \simeq \oplus_{i=1}^{r} M_{n_i}(\mathbb{C})$$

onde $\{e_1, \ldots, e_r\}$ é o conjunto de idempotentes primitivos centrais de $\mathbb{C}G$. Pode-se observar que cada idempotente e_i corresponde, por isomorfismo, ao elemento $(0, \ldots, o, Id_{n_i}, 0, \ldots, 0)$, onde Id_{n_i} denota a matriz identidade do anel $M_{n_i}(\mathbb{C})$, $1 \leq i \leq r$.

Seja $T : \mathbb{C}G \to \mathbb{C}$, dada por $T(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g T(g)$, assim, $T_i(e_i)$ é a função linear definida em $(\mathbb{C}G)e_i$ dada pela multiplicação pelo elemento identidade. Ou seja, T_i é a função identidade no componente simples $(\mathbb{C}G)e_i$. Além disso, como $e_i e_j = 0$ se $i \neq j$, segue que $T_i(e_j)$ é a função nula em toda componente simples $(\mathbb{C}G)e_j$, $j \neq i$. Portanto:

$$\begin{cases} \chi_i(e_i) = tr(Id_{n_i}) = gr(T_i) \\ \chi_i(e_j) = 0, \text{ se } i \neq j \end{cases}$$

O teorema a seguir nos ajudará a calcular os elementos idempotentes a partir dos caracteres. isto nos é útil pois as representações podem ser obtidas através de uma base de idempotentes.

Teorema 6.1.7 *Seja* $\{e_1, \ldots, e_r\}$ *o conjunto de idempotentes centrais de* $\mathbb{C}G$*. Temos que*

$$e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g$$

Demonstração: Cada idempotente e_i pode ser escrito na forma $e_i = \sum_{g \in G} a_i(g)g$, $1 \leq i \leq r$, pois $e_i \in \mathbb{C}G$. Avaliando o carácter regular em e_i, obtemos:

$$\rho(e_i) = \sum_{g \in G} a_i(g)\rho(g) = a_i(1)|G|$$

Assim, para um elemento $x \in G$ temos

$$\rho(x^{-1}e_i) = \sum_{g \in G} a_{ixg}\rho(g) = a_{ix}|G|$$

Usando a equação 6.1,

$$a_{ix}|G| = \rho(x^{-1}e_i) = \sum_{j=1}^{r} \chi_j(1)\chi_j(x^{-1}e_i)$$

Como já vimos que $T_i(e_i) = Id_{n_i}$ e $T_i(e_j) = 0$ se $i \neq j$, teremos

$$\begin{aligned} T_j(x^{-1}e_i) &= T_j(e_i)T_j(x^{-1}) = 0 \\ T_i(x^{-1}e_i) &= T_i(e_i)T_i(x^{-1}) = T_i(x^{-1}) \end{aligned}$$

assim,

$$\chi_j(x^{-1}e_i) = 0 \text{ se } i \neq j \text{ e } \chi_i(x^{-1}e_i) = \chi_i(x^{-1})$$

Consequentemente, teremos

$$a_{ix} = \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(x^{-1}), \forall\, x \in G$$

E substituindo em e_i, temos finalmente que

$$e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g.$$

■

Exemplo 6.1.8 *Vamos aplicar a fórmula obtida acima para calcular os idempotentes de* $\mathbb{C}K_8$*:*

$$\begin{aligned} e_1 = &\ \frac{1}{8}(1 + i + i^2 + i^3 + j + ij + i^2j + i^3j) \\ e_2 = &\ \frac{1}{8}(1 + i + i^2 + i^3 - j - ij - i^2j - i^3j) \\ e_3 = &\ \frac{1}{8}(1 - i + i^2 - i^3 + j - ij + i^2j - i^3j) \\ e_4 = &\ \frac{1}{8}(1 - i + i^2 - i^3 - j - ij - i^2j + i^3j) \\ e_5 = &\ \frac{1}{8}(1 - i^2) \end{aligned}$$

6.2 Tábua de Caracteres

Como os caracteres são constantes nas classes de conjugação $C_1, \ldots, C_r$ de G, podemos escolher um elemento x_i em cada classe e calcular cada carácter χ nestes elementos. Assim, determinamos completamente os caracteres de G sobre $\mathbb{C}$. Organizando estes dados em uma tabela, temos a chamada **Tábua de Caracteres**:

	C_1	C_2	$\cdots$	C_r
χ_1	$\chi_1(x_1)$	$\chi_1(x_2)$	$\cdots$	$\chi_1(x_r)$
χ_2	$\chi_2(x_1)$	$\chi_2(x_2)$	$\cdots$	$\chi_2(x_r)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
χ_r	$\chi_r(x_1)$	$\chi_r(x_2)$	$\cdots$	$\chi_r(x_r)$

A seguir, veremos um exemplo de uma tábua de caracteres, e como podemos utilizar o carácter regular para determinar os caracteres irredutíveis.

Exemplo 6.2.1 *Considere o Exemplo 5.3.2. Calculando o traço dos blocos das matrizes de T, obtemos a tábua dos caracteres:*

	C_1	C_2	C_3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Exemplo 6.2.2 *Concluiremos agora, o Exemplo 5.3.1 iniciado anteriormente. Como se trata de um grupo maior e com mais elementos para verificar, construiremos a tábua de caracteres para depois encontrar a T_5. Veremos que o traço nos ajudará a determinar com mais facilidade estas matrizes.*

	C_1	C_2	C_3	C_4	C_5
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	?	?	?	?	?

Como sabemos, pelo Exemplo 6.1.6, podemos aplicar os caracteres que conhecemos na fórmula 6.1 para obter os caracteres faltantes:

$$\rho(g) = \sum_{i=1}^{r} \chi_i(1)\chi_i(g)$$

Com $\rho(1) = |G|$ e $\rho(g) = 0$ quando $g \neq 1$. Assim,

$$\begin{aligned}
\rho(1) = {} & 8 = & 1\cdot 1 + 1\cdot 1 + 1\cdot 1 + 1\cdot 1 + 2\cdot 2 \\
\rho(-1) = {} & 0 = & 1\cdot 1 + 1\cdot 1 + 1\cdot 1 + 1\cdot 1 + 2\cdot(-2) \\
\rho(i) = {} & 0 = & 1\cdot 1 + 1\cdot 1 + 1\cdot(-1) + 1\cdot(-1) + 2\cdot 0 \\
\rho(j) = {} & 0 = & 1\cdot 1 + 1\cdot(-1) + 1\cdot 1 + 1\cdot(-1) + 2\cdot 0 \\
\rho(k) = {} & 0 = & 1\cdot 1 + 1\cdot(-1) + 1\cdot(-1) + 1\cdot 1 + 2\cdot 0
\end{aligned}$$

Portanto,

	C_1	C_2	C_3	C_4	C_5
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Agora sabemos que $tr(T_5(i)) = tr(T_5(j)) = tr(T_5(k)) = 0$, *além das igualdades dadas anteriormente no Exemplo 5.3.1. Com algumas tentativas, podemos obter as seguintes matrizes:*

$$T_5(i) = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \ e\ T_5(j) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Desta forma obtemos a matriz T *para cada classe de conjugação, cuja diagonal são as matrizes* T_1, T_2, T_3, T_4, T_5 *em blocos:*

$$T(i) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & 0 & -i \end{bmatrix}, \quad T(j) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$T(1) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad T(-1) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

$$T(k) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -i \\ 0 & 0 & 0 & 0 & -i & 0 \end{bmatrix}$$

Ou seja, ao mesmo tempo em que as representações nos mostram quais são os caracteres do grupo, os caracteres também nos auxiliam a obter as representações.

7 DIAGRAMAS DE YOUNG

Neste capítulo iremos apresentar a teoria dos diagramas de Young e estabelecer uma relação entre estes diagramas e os grupos simétricos. Desta forma, obteremos informações que poderão nos auxiliar a calcular as representações de qualquer grupo simétrico. Em especial, nosso objetivo é apresentar explicitamente as representações do grupo S_3. Devido ao tempo reduzido, nos ateremos apenas em aplicar os resultados, omitindo assim as suas respectivas demonstrações. Caso o leitor tenha interesse em saber mais sobre os diagramas de Young, indicamos (Silva, 2014, [4]).

7.1 Diagramas e quadros de Young

Iniciaremos com as definições e exemplos de partição de um número inteiro e dos diagramas de Young.

Definição 7.1.1 *Seja $n \in \mathbb{Z}$. Dizemos que $\lambda = (\lambda_1, \dots, \lambda_k)$ é uma* ***partição*** *de n, e denotamos $\lambda \vdash n$, se $\lambda_1 + \cdots + \lambda_k = n$ e $\lambda_1 \geq \cdots \geq \lambda_k$.*

Exemplo 7.1.2 *Vejamos alguns exemplos:*

a) Consideremos $n = 4$, há então cinco partições possíveis:

$$\begin{aligned}
4 = 1+1+1+1 &\Rightarrow (1,1,1,1)\\
4 = 2+2 &\Rightarrow (2,2)\\
4 = 2+1+1 &\Rightarrow (2,1,1)\\
4 = 3+1 &\Rightarrow (3,1)\\
4 = 4 &\Rightarrow (4)
\end{aligned}$$

b) Quando $n = 5$, temos que $1 + 2 + 2 = 5$, mas $(1, 2, 2)$ não é uma partição de 5, pois $1 < 2$. Entretanto, $(2, 2, 1)$ é partição de 5.

c) Consideremos a escrita dos elementos de S_3 em ciclos:

$$S_3 = \{I, (12), (13), (23), (123), (132)\}$$

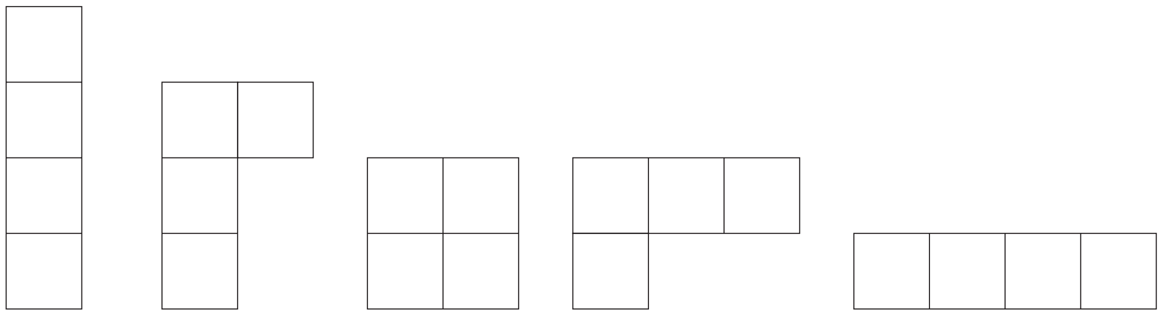
Nessa notação estamos omitindo os ciclos de tamanho 1, mas ao considerá-los, podemos associar cada elemento de S_3 com uma partição de 3, obtida pelo tamanho *dos ciclos:*

Elemento	*Elemento com ciclos de tamanho* 1	*Partição associada*
I	$(1)(2)(3)$	$(1,1,1)$
(12)	$(12)(3)$	$(2,1)$
(13)	$(13)(2)$	$(2,1)$
(23)	$(23)(1)$	$(2,1)$
(123)	(123)	(3)
(132)	(132)	(3)

é importante notar que ciclos do mesmo tamanho estão associados a mesma partição.

Definição 7.1.3 *Um* ***diagrama de Young*** *associado a uma partição* $\lambda = (\lambda_1, \ldots, \lambda_k)$ *é um conjunto de caixas organizadas em* k *linhas, com* λ_i *caixas na* i*-ésima linha.*

Exemplo 7.1.4 *Mostraremos os diagramas de Young associados a cada partição de* 4*:*



$(1,1,1,1)$ $(2,1,1)$ $(2,2)$ $(3,1)$ (4)

Definição 7.1.5 *Suponha que* $\lambda = (\lambda_1, \ldots, \lambda_l)$ *e* $\mu = (\mu_1, \ldots, \mu_m)$ *são partições de um inteiro* n*. Então,* λ ***domina*** μ *e escrevemos* $\lambda \trianglerighteq \mu$*, se*

$$\lambda_1 + \cdots + \lambda_i \geq \mu_1 + \cdots + \mu_i$$

para todo $i \geq 1$*. Onde se* $i > l$*, tomamos* $\lambda_i = 0$ *e se* $i > m$ *tomamos* $\mu_i = 0$*.*

Exemplo 7.1.6 *Considere as partições* $\lambda = (5,1)$ *e* $\mu = (3,3)$ *de* 6*. Temos que para*

$$\begin{aligned} i = 1 &\Rightarrow 5 > 3 \\ i = 2 &\Rightarrow 5 + 1 \geq 3 + 3 \end{aligned}$$

portanto, $\lambda \trianglerighteq \mu$*.*

Por outro lado, quando consideramos as partições $(3,3,1)$ *e* $(4,1,1,1)$ *de* 7*, temos que*

$$\begin{aligned} i = 1 &\Rightarrow 4 > 3 \\ i = 2 &\Rightarrow 4 + 1 < 3 + 3 \\ i = 3 &\Rightarrow 4 + 1 + 1 < 3 + 3 + 1 \\ i = 4 &\Rightarrow 4 + 1 + 1 + 1 = 3 + 3 + 1 + 0 \end{aligned}$$

e assim, não temos nem que $(3,3,1) \trianglerighteq (4,1,1,1)$ *e nem* $(4,1,1,1) \trianglerighteq (3,3,1)$*.*

Pode-se demonstrar que a relação $\trianglerighteq$ é reflexiva, antissimétrica e transitiva, portanto é uma relação de ordem. Mas como vimos no Exemplo 7.1.6, é uma relação de ordem parcial.

Definição 7.1.7 *Seja λ uma partição de um inteiro n e t o diagrama de Young associado a λ. Um* **quadro de Young** *associado a λ é o diagrama t preenchido com os inteiros de* 1 *a n sem repetições.*

Exemplo 7.1.8 *Alguns quadros de Young associados a partição $\lambda = (2,2)$ de 4 são:*

$$t^\lambda = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline\end{array}, \quad q^\lambda = \begin{array}{|c|c|}\hline 4 & 1 \\ \hline 2 & 3 \\ \hline\end{array}, \quad r^\lambda = \begin{array}{|c|c|}\hline 2 & 4 \\ \hline 1 & 3 \\ \hline\end{array}, \quad s^\lambda = \begin{array}{|c|c|}\hline 4 & 3 \\ \hline 1 & 2 \\ \hline\end{array}.$$

Um quadro de Young é dito **standard** se suas entradas crescem ao longo de cada linha e ao longo de cada coluna.

Assim, com $n = 5$ e $\lambda = (3,2)$ e dados

$$t^\lambda = \begin{array}{|c|c|c|}\hline 1 & 3 & 5 \\ \hline 2 & 4 \\ \cline{1-2}\end{array} \quad \text{e} \quad q^\lambda = \begin{array}{|c|c|c|}\hline 1 & 3 & 5 \\ \hline 4 & 2 \\ \cline{1-2}\end{array}$$

temos que t^λ é um quadro standard, enquanto q^λ não é standard.

Vejamos agora como um elemento de S_n age sobre um quadro de Young associado a uma permutação λ de n:

Seja $\sigma \in S_n$. Ao fazermos $\sigma(t^\lambda)$, teremos que se a é a entrada (i,j) de t^λ, então $\sigma(a)$ estará na posição (i,j) de $\sigma(t^\lambda)$.

Exemplo 7.1.9 *Sejam $n = 6$, $\lambda = (3,2,1)$,*

$$t^\lambda = \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 & 5 \\ \cline{1-2} 6 \\ \cline{1-1}\end{array}$$

e $\sigma = (243)$. Assim, teremos que

$$\sigma(t^\lambda) = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2} 6 \\ \cline{1-1}\end{array}$$

Veremos agora a definição de um subgrupo de S_n fundamental na obtenção das representações irredutíveis.

Definição 7.1.10 *Seja t um quadro de Young. Chamamos de **estabilizador de coluna** de t, o subgrupo de S_n que preserva as colunas de t. Ou seja, $\sigma \in C_t$ se, e somente se, $\sigma(i)$ está na mesma coluna que i, para cada $i \in \{1, \ldots, n\}$.*

Exemplo 7.1.11 *Dados $n = 7$ e $\lambda = (3, 2, 2)$, considere o seguinte quadro:*

$$t = \begin{array}{|c|c|c|} \hline 1 & 3 & 7 \\ \hline 4 & 5 & \multicolumn{1}{c}{} \\ \cline{1-2} 2 & 6 & \multicolumn{1}{c}{} \\ \cline{1-2} \end{array}$$

Queremos obter um subconjunto de S_7 que não altere a coluna em que cada elemento está. Desta forma, estamos procurando permutações entre os elementos $1, 2$ e 4, entre os elementos $3, 5$ e 6 e entre o 7. Chamando de $S_{\{i,j,k\}}$ o subgrupo de S_n que permuta os elementos i, j e k, mas mantém os outros, temos que

$$C_t = S_{\{1,2,4\}} S_{\{3,5,6\}} S_{\{7\}} \simeq S_{\{1,2,4\}} \times S_{\{3,5,6\}} \times S_{\{7\}}.$$

Alguns elementos de S_7 que pertencem a C_t são:

- (14);
- $(124)(35)$;
- Id;
- $(24)(35)$;
- $(124)(356)$.

Observe que $|S_{\{1,2,4\}}| = |S_{\{3,5,6\}}| = 3!$ e $|S_{\{7\}}| = 1$. Portanto, $|C_t| = 3! \cdot 3! \cdot 1 = 36$.

Iremos definir agora uma relação de equivalência entre os quadros associados a uma mesma partição. As classes de equivalência que provém desta relação nos ajudarão na construção das representações irredutíveis.

Sejam t_1 e t_2 dois λ-quadros. Dizemos que $t_1 \sim t_2$ se eles possuem as mesmas entradas em cada linha.

Definição 7.1.12 *Cada classe de equivalência dada pela relação $\sim$ é chamada de λ-* ***tabloid*** *e é representada por $[t]$, onde t é um λ-quadro que pertence a esta classe. O conjunto de todas as classes de equivalência de uma partição λ será denotado por T^λ.*

Em especial, dado $\lambda = (\lambda_1, \ldots, \lambda_l)$, o *tabloid* dos quadros que possuem as entradas $1, 2, \ldots, \lambda_1$ na primeira linha, $\lambda_1 + 1, \ldots, \lambda_1 + \lambda_2$ na segunda e assim por diante até $(\lambda_1 + \cdots + \lambda_{l-1} + 1), \ldots, (\lambda_1 + \cdots + \lambda_l)$ na última linha é chamada de T_λ. Vejamos estas definições com um exemplo.

Exemplo 7.1.13 *Analisemos esta relação com os quadros da partição $\lambda = (2, 1)$ de 3:*

$$t_1 = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} \quad \sim \quad t_2 = \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}$$

$$q_1 = \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} \quad \sim \quad q_2 = \begin{array}{|c|c|}\hline 3 & 1 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}$$

$$r_1 = \begin{array}{|c|c|}\hline 3 & 2 \\ \hline 1 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} \quad \sim \quad r_2 = \begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}$$

Assim, $[t_1] = \{t_1, t_2\}$, $[q_1] = \{q_1, q_2\}$, $[r_1] = \{r_1, r_2\}$, $T^\lambda = \{[t_1], [q_1], [r_1]\}$ e $T_\lambda = [t_1]$.

Proposição 7.1.14 *Suponha que $t_1 \sim t_2$ e que $\sigma \in S_n$. Então $\sigma t_1 \sim \sigma t_2$. Portanto, existe uma ação bem definida de S_n em T^λ dada por $\sigma[t] = [\sigma t]$, para t um λ-quadro.*

Demonstração: Pode ser vista em (Steinberg, 2011, p. 123, [5]). ■

Exemplo 7.1.15 *Suponha $\lambda = (n-1, 1)$. Então dois λ-quadros serão equivalentes se, e somente se, eles tiverem a mesma entrada na segunda linha. Por outro lado, se $\lambda = (n)$, então há apenas um λ-tabloid.*

7.2 Construção das Representações Irredutíveis de S_n

No início da Seção 5.2, estabelecemos uma relação biunívoca entre as representações irredutíveis e os KG submódulos simples (Proposição 5.2.1). Agora iremos estabelecer esta mesma relação. Assim, dada uma partição λ, definamos $M^\lambda = \mathbb{C}T^\lambda$ e $\varphi^\lambda : S_n \to GL(M^\lambda)$ a representação associada. Ou seja, como cada elemento de S_n está relacionado a uma partição de n, e cada partição λ está associada a T^λ, temos um $M^\lambda = \mathbb{C}T^\lambda$ para cada classe de S_n.

Nossa próxima definição é a de λ-polytabloid. Estes elementos tem o mesmo papel que os elementos idempotentes de KG definidos no Teorema 6.1.7.

Definição 7.2.1 *Sejam $\lambda, \mu \vdash n$. Seja t^λ um quadro de Young. O elemento*

$$e_t = \sum_{\pi \in C_t} sgn(\pi)\pi[t]$$

de M^μ é chamado de ***polytabloid*** *associado a t.*

Exemplo 7.2.2 *Sejam $\lambda = (3,2)$ uma partição de 5 e*

$$t = \begin{array}{|c|c|c|}\hline 4 & 1 & 2 \\ \hline 3 & 5 & \multicolumn{1}{c}{} \\ \cline{1-2}\end{array}$$

Sabemos que $C_t = S_{\{3,4\}} \times S_{\{1,5\}} \times S_{\{2\}}$, então $C_t = \{Id, (34), (34)(15), (15)\}$ e, assim

$$e_t = Id[t] - (34)[t] + (34)(15)[t] - (15)[t]$$

$$e_t = \begin{array}{|c|c|c|}\hline 4 & 1 & 2 \\ \hline 3 & 5 & \multicolumn{1}{c}{} \\ \cline{1-2}\end{array} - \begin{array}{|c|c|c|}\hline 3 & 1 & 2 \\ \hline 4 & 5 & \multicolumn{1}{c}{} \\ \cline{1-2}\end{array} + \begin{array}{|c|c|c|}\hline 3 & 5 & 2 \\ \hline 4 & 1 & \multicolumn{1}{c}{} \\ \cline{1-2}\end{array} - \begin{array}{|c|c|c|}\hline 4 & 5 & 2 \\ \hline 3 & 1 & \multicolumn{1}{c}{} \\ \cline{1-2}\end{array}$$

A próxima proposição nos auxilia a ver que a ação de S_n em um λ-quadro é compatível com a definição de um λ-tabloid.

Proposição 7.2.3 *Se $\pi \in S_n$ e t é um λ-quadro, então $e_{\pi[t]} = \pi e_t$.*

Demonstração: Pode ser vista em (Steinberg, 2011, p. 124, [5]). ■

Estamos buscando representações irredutíveis e, para tanto, precisamos trabalhar com módulos irredutíveis. Porém, em geral, o módulo M^λ não é irredutível, mas contém um submódulo irredutível que denotaremos por S^λ. Este submódulo é obtido através do seguinte processo:

- Para cada $\lambda \vdash n$, considere $[t]$ um λ-*tabloid*.
- Para cada $s \in [t]$, com s um quadro standard, calcule o estabilizador de coluna C_s e os elementos e_s.
- O conjunto $\{e_s\}_{s \in [t]}$ é uma base de S^λ.

Definição 7.2.4 *Os submódulos S^λ obtidos acima, são chamados de **Submódulos Specht** e as representações $\psi^\lambda : S_n \to GL(S^\lambda)$ são chamadas de **Representações Specht** (ou Sprecht).*

Teorema 7.2.5 *As representações Specht ψ^λ, com $\lambda \vdash n$, formam um conjunto completo de representações irredutíveis e não equivalentes de S_n.*

Demonstração: Pode ser vista em (Steinberg, 2011, p. 128, [5]). ■

Finalizamos este trabalho com um exemplo aplicando os resultados deste capítulo para obter as representações irredutíveis de S_3 por meio dos diagramas de Young.

Exemplo 7.2.6 *Consideremos $n = 3$ e suas partições $\lambda = (3), \mu = (2,1), \eta = (1,1,1)$.*

(λ) *Para a partição λ, existem 6 quadros diferentes, porém todos são da mesma classe de equivalência de*

$$t = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline\end{array}$$

Assim, $C_t = Id$ para todo λ-quadro t. Logo, $e_t = Id(t) = t$, ou seja, S^λ é unidimensional. Assim, a representação associada a partição λ é a representação trivial.

(η) *Para a partição η, existem 6 quadros diferentes e não equivalentes:*

$$q_1 = \begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline 3 \\ \hline\end{array}, \quad q_2 = \begin{array}{|c|}\hline 1 \\ \hline 3 \\ \hline 2 \\ \hline\end{array}, \quad q_3 = \begin{array}{|c|}\hline 2 \\ \hline 3 \\ \hline 1 \\ \hline\end{array}, \quad q_4 = \begin{array}{|c|}\hline 2 \\ \hline 1 \\ \hline 3 \\ \hline\end{array}, \quad q_5 = \begin{array}{|c|}\hline 3 \\ \hline 2 \\ \hline 1 \\ \hline\end{array}, \quad q_6 = \begin{array}{|c|}\hline 3 \\ \hline 1 \\ \hline 2 \\ \hline\end{array}$$

Porém, apenas q_1 é standard, assim,

$$e_{q_1} = Id[q_1] - (12)[q_1] - (13)[q_1] - (23)[q_1] + (123)[q_1] + (132)[q_1]$$

Assim, cada elemento fica associado ao sinal de uma das permutações de S_3, e portanto, a representação associada a S^η é a representação sinal.

(μ) *Para a partição μ, temos 3 tabloids $[r_1], [r_2]$ e $[r_3]$, onde*

$$\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} \quad e \quad \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}$$

estão em $[r_1]$,

$$\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \quad e \quad \begin{array}{|c|c|}\hline 3 & 1 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array}$$

estão em $[r_2]$ *e*

$$\begin{array}{|c|c|}\hline 3 & 2 \\ \hline 1 & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \quad e \quad \begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array}$$

estão em $[r_3]$.

Claramente, os estabilizadores de coluna são os elementos de S_3 *de ciclo tamanho* 2 *e a identidade. Além disso, os elementos de* $[r_3]$ *não são standard. Calculando os polytabloids, temos que*

$$\begin{aligned} e_{r_1} &= Id[r_1] - (13)[r_1] \\ e_{r_2} &= Id[r_2] - (12)[r_2] \end{aligned}$$

ou seja, S^μ *tem dimensão* 2*. Podemos obter as matrizes desta representação através de um processo de diminuição do grau da representação standard, porém isto requer outros resultados não abordados neste trabalho.*

O exemplo acima nos confirma que as representações de S_3 obtidas no Exemplo 5.3.2 são as representações irredutíveis procuradas.

8 Conclusão

Com este trabalho foi possível apresentar uma introdução ao estudo de representações de grupos. A teoria de anéis semissimples deu o suporte necessário para a decomposição dos anéis de grupo. Já os anéis de grupo foram especialmente fundamentais pois aliam os elementos de um grupo à estrutura de um anel ou corpo. Pelo Teorema de Maschke 4.1.3, conseguimos condições para decompor um anel de grupo em componentes simples.

Estas componentes simples estão biunivocamente associadas às representações irredutíveis do grupo. Desta forma, conseguimos calcular as dimensões e quantidades das representações irredutíveis. Já com o estudo dos caracteres, conhecemos os traços das matrizes das representações, o que nos auxiliou a refinar nossa busca.

Por fim, o estudo dos diagramas de Young deu luz a outra forma de obter representações irredutíveis, porém ainda manteve a relação com o anel de grupo. Devido ao tempo limitado para produção deste trabalho e as complicações causadas pela pandemia de Covid-19, não pudemos aprofundar o estudo destes diagramas. Todavia, este pode vir a ser o propósito de trabalhos futuros.

Referências

1 Gil, C. *Como Elaborar Projetos de Pesquisa*. Grupo GEN, 2017. Citado na página 9.

2 Gonçalves, A. *Introdução à Álgebra*. IMPA, 2017. Citado na página 14.

3 Milies, C. P., Sehgal, S. K., *An Introduction to Group Rings*. Kluwer Academic Publishers, 2002. Citado 5 vezes nas páginas 9, 11, 38, 43 e 46.

4 Silva, T. S. Z. C. *Grafo da Ramificação para Representações Irredutíveis de Grupos Simétricos*. 2014. Dissertação de Mestrado. Universidade de Lisboa. Disponível em: <https://repositorio.ul.pt/bitstream/10451/10968/1/ulfc106470_tm_Tania_Silva.pdf>. Acesso em: 15 out 2020. Citado na página 66.

5 Steinberg, B. *Representation Theory of Finite Groups: An Introductory Approach*. Springer Science & Business Media, 2011. Citado 5 vezes nas páginas 9, 11, 70, 71 e 72.