Trabalho de Conclusão de Curso - Bacharelado em Matemática

O Teorema de Wedderburn-Artin

Michael da Silva Bressiani

Universidade Federal do ABC

Título: O Teorema de Wedderburn-Artin

Autor: Michael da Silva Bressiani
Orientador: Prof. Dr. Edson Ryoji Okamoto Iwaki

Trabalho de conclusão de curso apresentado como requisito parcial para obtenção do título de Bacharel em Matemática pela Universidade Federal do ABC.

Banca Examinadora:

Prof. Dr. Ercílio Carvalho da Silva
Universidade Federal do ABC

Prof. Dr. Roldão da Rocha Junior
Universidade Federal do ABC

Santo André, 31 de outubro de 2017.

Sumário

Agradecimento

Agradeço a todos aqueles que me auxiliaram na elaboração deste trabalho. Em particular ao professor Edson, pelas reuniões e sugestões para o desenvolvimento do projeto. Faço um agradecimento também aos familiares, amigos, por incentivarem e estarem sempre presentes nos momentos importantes. Agradeço especialmente à Raiane, pessoa que esteve sempre ao meu lado, dando apoio e incentivo.

1 Resumo

Este trabalho contém uma demonstração do Teorema de Wedderburn-Artin baseada no artigo [4]. Tal teorema caracteriza a estrutura de anéis semissimples, os identificando com um produto finito de matrizes sobre anéis de divisão.

Além disso, há uma breve introdução aos anéis de grupo, onde é provado o Teorema de Maschke, que caracteriza quando anéis de grupo RG é semissimples. Essa última parte é baseada na referência [3].

Palavras Chaves: Teorema de Wedderbrun-Artin, semissimples, anéis de grupo, Teorema de Maschke

Abstract

This work contains a demonstration of the Wedderburn-Artin Theorem, this part is based on the reference [4]. Such a theorem characterizes the structure of semisimple rings, identifying them with a finite matrix product on division rings.

In addition, there is a brief introduction to the group rings, where Maschke's theorem is proved, characterizing when a RG group rings is semisimple. This last part is based on the reference [3].

Keywords: Wedderbun-Artin Theorem, semisimple, group rings, Maschke's Theorem

Introdução

Neste trabalho pretendemos mostrar o Teorema de Wedderburn-Artin fazendo uso apenas de conceitos elementares da teoria de anéis, tendo como referência [4]. Além disso, apresentamos algumas definições e resultados necessários para que o leitor, que não esteja familiarizado com a teoria de anéis, tenha condições de entender o conteúdo explicitado. Outras definições e teoremas, menos comuns em cursos de graduação, também foram enunciadas, com o propósito de introduzir a teoria de anéis de grupo.

Este trabalho está estruturado em quatro partes. Na primeira, temos as definições básicas, como a definição de anel e exemplos relevantes, como o anel de matrizes, essencial no contexto deste trabalho. Já na segunda parte, se baseando em [2] e [3], apresentamos as condições de finitude e o conceito de anel semiprimo, que adotaremos como hipóteses no Teorema de Wedderburn-Artin. Ainda nessa parte, mostraremos algumas aplicações do Lema de Zorn e também como as condições de finitude sobre um anel, se relacionam com os elementos idempotentes dele. Na terceira parte, tendo como base [1] e [3], definimos módulo, anel de endomorfismos e finalmente o conceito de semissimplicidade. Nessa parte, retomamos alguns resultados vistos na terceira, terminando por mostrar que um anel é semissimples se, e somente se é simultaneamente semiprimo e artiniano a esquerda. Finalmente, na quarta parte, há a prova do Teorema de Wedderburn e Teorema de Wederburn-Artin. Por fim, como aplicação de todos os conceitos vistos no decorrer do trabalho, apresentamos uma demonstração do Teorema de Maschke tendo como referência [3].

Em termos de aplicações, o Teorema de Wedderbrun-Artin é importante, por exemplo, na teoria de anéis de grupo, pois é relativamente fácil encontrar anéis de grupo semissimples, dessa forma, um teorema que caracteriza anéis semissimples é fundamental para o desenvolvimento dessa teoria.

2.1 Definições básicas

Definição 2.1 *Dizemos que um conjunto G não vazio, munido de uma operação binária, que denotamos por $\cdot$, é um grupo, se as seguintes condições são satisfeitas:*
i. *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$, sejam quais forem $a, b, c \in G$ tomados;*
ii. *Existe $e \in G$ tal que $g \cdot e = e \cdot g = g$ seja qual for $g \in G$, chamado elemento neutro;*
iii. *Dado $g \in G$, existe $g^{-1} \in G$, tal que $g \cdot g^{-1} = g^{-1} \cdot g = e$, chamado de inverso de g.*

Nesse caso dizemos que $(G, \cdot)$ é um grupo.

Também é comum se usar a notação "$+$" no lugar de "$\cdot$", e nesse caso, por convenção, trocamos e por 0 e "g^{-1}" por "$-g$" na definição acima, e dizemos que $(G, +)$ é um grupo.

Definição 2.2 *Um anel é um conjunto R não vazio munido de duas operações binárias, $+$ e $\cdot$, chamadas adição e multiplicação respectivamente, que satisfazem as seguintes condições:*
Dados $a, b, c \in R$, tem-se que:
i. *$(R, +)$ é um grupo;*
ii. *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$, associatividade;*
iii. *$(a + b) \cdot c = a \cdot c + b \cdot c$, distributividade à direita;*
iv. *$c \cdot (a + b) = c \cdot a + c \cdot b$, distributividade à esquerda.*
Se além dessas propriedades também for satisfeito:
v. *Existe $1 \in R$ tal que $1 \cdot r = r \cdot 1 = r$ para todo $r \in R$,*
então dizemos que R é um anel com unidade e chamamos 1 de identidade.

Observação 2.3 *Note que, se um anel R tem identidade, então ela é única. De fato, se 1 e $1'$ são identidades em R, então $1 = 1 \cdot 1' = 1'$.*

Outra propriedade que um anel R pode satisfazer é a comutatividade, que corresponde a dizer que $a \cdot b = b \cdot a$, para todo $a, b \in R$. Nesse caso dizemos que o anel é comutativo.

Observação 2.4 *Afim de simplificar a notação, definimos* $a - b = a + (-b)$ *e* $a \cdot b = ab$.

Definição 2.5 *Seja R um anel. Dizemos que um subconjunto não vazio S de R é subanel de R se for um anel com as operações de R.*

Proposição 2.6 *Seja subconjunto não vazio S de R. Se* $ab \in S$ *e* $a - b \in S$ *para todo* $a, b \in S$, *então S é subanel de R.*

Demonstração: De fato, por hipótese, $ab \in S$ para todo $a, b \in S$, note também que $a - a = 0 \in S$, logo dado $a \in S$, temos $0 - a = -a \in S$, assim $a + b = a - (-b) \in S$. As propriedades restantes da definição de anel seguem do fato de que S é subconjunto de R. □

Observação 2.7 *(**Importante**) Neste trabalho lidaremos apenas com anéis que possuem identidade* $1 \neq 0$. *Dessa forma, de agora em diante, quando nos referirmos a um anel R, estará implícito que estamos considerando um anel com unidade. Se não for feito menção do contrário, denotaremos a identidade do anel por* 1.

Definição 2.8 *Seja R um anel. Dizemos que um subconjunto não vazio I de R é um ideal à esquerda de R se dados* $a, b \in I$ *temos que:*
i. $a - b \in I$;
ii. $rx \in I$, *para todo* $r \in R$ *e todo* $x \in I$.
*Se no lugar do item **ii.** for satisfeito:*
ii'. $xr \in I$, *para todo* $r \in R$ *e todo* $x \in I$,
então dizemos que I é um ideal à direita de R.
*Se tanto **ii.** quanto **ii'.** são satisfeitos, então dizemos que I é um ideal bilateral de R, ou mais sucintamente, ideal de R.*

Dado um anel R, então R e $\{0\}$, são ideais de R, como é fácil de verificar. Tais ideais são chamados de ideais triviais de R. Note também que dados dois ideais à esquerda I e J de um anel R, então $I \cap J$ também é ideal à esquerda de R, pois $a, b \in I \cap J$ implica que $a, b \in I$ e $a, b \in J$, logo $a - b,\ ra \in I$ e $a - b,\ ra \in J$, assim $a - b,\ ra \in I \cap J$ sejam quais forem $a, b \in I \cap J$ e $r \in R$.

De forma análoga, prova-se que $I \cap J$ é ideal à direita de R sempre que I e J são ideais à direita de R.

2.2 O anel das matrizes

Seja R um anel e $n \geq 1$ um número inteiro, um elemento da forma:

$$X = \begin{bmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{bmatrix},$$

onde $x_{ij} \in R$ para todo $i, j = 1, ..., n$, representa a forma geral de uma matriz de n linhas por n colunas com coeficientes sobre R. O conjunto de todas as matrizes sobre R com n linhas e n colunas será denotado por $M_n(R)$. Afim de simplificar a notação, podemos representar um elemento arbitrário $X \in M_n(R)$ simplesmente por $X = (x_{ij})_{nxn}$. Também é comum representar por $(X)_{ij}$ o elemento correspondente a linha i e coluna j de uma matriz X.

Assim, dados $A = (a_{ij})_{nxn}$ e $B = (b_{ij})_{nxn}$ matrizes em $M_n(R)$, definimos a soma de A com B como sendo $(A + B)_{ij} = a_{ij} + b_{ij}$, onde a operação "+", representa a adição definida no anel R, dessa forma a componente correspondente a linha i e coluna j da matriz $A + B$ é a soma de a_{ij} e b_{ij}. Observe que $A + B$ também tem n linhas e n colunas, logo $A + B \in M_n(R)$.

Naturalmente a operação de adição que definimos em $M_n(R)$ herda todas as propriedades de adição de R, onde o elemento neutro do conjunto das matrizes, $N \in M_n(R)$, é aquela tal que $(N)_{ij} = 0$, para todo $1 \leq i, j \leq n$. Para obter o inverso aditivo de uma matriz $A \in M_n(R)$, basta substituir cada elemento $(A)_{ij}$, $1 \leq i, j \leq n$ de A por seu respectivo inverso aditivo em R.

Dessa forma M_n é grupo com respeito a operação de adição definida acima.

Agora, defina a multiplicação de A por B, como sendo $(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$, onde a soma e a multiplicação são as do anel R e novamente i e j variam de 1 a n. Assim, o elemento correspondendo a uma linha i e coluna j de AB é definido por $\sum_{k=1}^{n} a_{ik} b_{kj}$. Note ainda que $AB \in M_n(R)$.

Vamos mostrar que a operação de multiplicação entre elementos de $M_n(R)$ definida acima é associativa.

Dados $A, B, C \in M_n(R)$ e denotando $A = (a_{ij})_{nxn}$, $B = (b_{ij})_{nxn}$ e $C = (c_{ij})_{nxn}$, temos

que

$$\begin{aligned}((AB)C)_{ij} &= \sum_{l=1}^{n}\Big(\sum_{k=1}^{n} a_{ik}b_{kl}\Big)c_{lj} = \sum_{l=1}^{n}\sum_{k=1}^{n} a_{ik}\Big(b_{kl}c_{lj}\Big)\\ &= \sum_{k=1}^{n}\sum_{l=1}^{n} a_{ik}\Big(b_{kl}c_{lj}\Big) = \sum_{l=1}^{n} a_{ik}\Big(\sum_{k=1}^{n} b_{kl}c_{lj}\Big)\\ &= (A(BC))_{ij},\end{aligned}$$

onde usamos o fato de que a multiplicação de R é associativa e distributiva com respeito a soma.

Temos também que tal multiplicação é distributiva com respeito a soma. De fato,

$$\begin{aligned}(C(A+B))_{ij} &= \sum_{k=1}^{n} c_{ik}\Big(a_{kj}+b_{kj}\Big)\\ &= \sum_{k=1}^{n}\Big(c_{ik}a_{kj}+c_{ik}b_{kj}\Big)\\ &= \sum_{k=1}^{n} c_{ik}a_{kj} + \sum_{k=1}^{n} c_{ik}b_{kj} = (CA+CB)_{ij},\end{aligned}$$

onde usamos o fato de que a multiplicação em R é distributiva.

O caso $(A+B)C = AC+BC$ prova-se de maneira análoga.

Portanto o conjunto $M_n(R)$ munido das operações de soma e multiplicação definidos acima é um anel.

Note que, como R é um anel com unidade, é fácil ver que a matriz $I_n \in M_n(R)$ onde as entradas correspondendo a $i = j$ valem 1 e o restante vale 0, é a identidade de $M_n(R)$ (chamada de matriz identidade).

Definição 2.9 *Seja R um anel. Dizemos que R é anel de divisão, se todo elemento não nulo de R é inversível, isto é, dado $x \in R$ com $x \neq 0$, então existe $y \in R$ tal que $xy = yx = 1$.*

Definição 2.10 *Um anel R é simples se os únicos ideais bilaterais são os triviais.*

Note que de acordo com essa definição um anel de divisão é simples.

Proposição 2.11 *Seja D um anel de divisão. Então o anel $M_n(D)$ é simples.*

Demonstração: Seja $\mathcal{M}$ um ideal de $M_n(D)$, logo

$$\mathcal{M} = \begin{bmatrix} D_{11} & \cdots & D_{1n} \\ \vdots & \ddots & \vdots \\ D_{n1} & \cdots & D_{nn} \end{bmatrix}$$

onde $D_{ij} = \{0\}$ ou $D_{ij} = D$. Supondo que $\mathcal{M}$ seja diferente de $M_n(D)$, então existe l e m tais que $D_{lm} = \{0\}$. Tome a matriz M^{ϕ}, cujo as entradas são dadas por

$$(M^{\phi})_{ij} = \begin{cases} 1, & \text{se } i = \phi, j = m \\ 1, & \text{se } i = l, j = \phi \\ 0, & \text{caso contrário} \end{cases}$$

onde ϕ é um inteiro entre 1 e n.

Seja $N \in \mathcal{M}$ um elemento arbitrário que denotaremos por

$$N = \begin{bmatrix} d_{11} & \cdots & d_{1n} \\ \vdots & \ddots & \vdots \\ d_{n1} & \cdots & d_{nn} \end{bmatrix}.$$

Como $\mathcal{M}$ é um ideal de $M_n(D)$, então $NM^{\phi} \in \mathcal{M}$ para todo $\phi = 1, ..., n$. Mas note que isso implica em $d_{l\phi} = \sum_{k=1}^{n} d_{lk}(M^{\phi})_{km} \in D_{lm} = \{0\}$, para todo $\phi = 1, ..., n$. Por outro lado, temos também que $M^{\phi}N \in \mathcal{M}$ para todo $\phi = 1, ..., n$, logo $d_{\phi m} = \sum_{k=1}^{n} (M^{\phi})_{lk} d_{km} \in D_{lm} = \{0\}$ para todo $\phi = 1, ..., n$.

Assim o fato de $D_{lm} = \{0\}$ implica $D_{l\phi} = \{0\}$ e $D_{\phi m} = \{0\}$ para todo $\phi = 1, ..., n$.

Aplicando o raciocínio acima para $D_{l\phi} = \{0\}$ e $D_{\phi m} = \{0\}$ para cada $\phi = 1, ..., n$, concluímos que $D_{ij} = \{0\}$ para todo i e j.

Dessa forma $\mathcal{M} = \{0\}$, e portanto $M_n(D)$ é simples. □

Definição 2.12 *Dizemos que um anel R é semiprimo se dado um ideal $I \subseteq R$, com $I \neq \{0\}$, então $I^2 \neq \{0\}$.*

Sabemos que um anel R simples admite apenas R e $\{0\}$ como ideais. Além disso, $\{0\} \neq R \subseteq R^2$, pois $r = 1 \cdot r \in R^2$ para todo $r \in R$, dessa forma todo $R^2 \neq \{0\}$. Portanto todo anel simples é semiprimo. Em particular, $M_n(D)$ dado acima é semiprimo.

Definição 2.13 *Sejam $R_1, R_2, \ldots, R_n$, anéis. Defina o produto cartesiano $R_1 \times R_2 \times \ldots \times R_n$ como sendo o conjunto consistindo de todos os elementos da forma $(r_1, r_2, \ldots, r_n)$, onde para cada $1 \leq i \leq n$ temos $r_i \in R_i$.*

Dados $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$ elementos de $R_1 \times R_2 \times \ldots \times R_n$. Podemos definir a soma de x por y como sendo $x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ e o produto $xy = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$.

Sendo $R_1, R_2, \ldots, R_n$ anéis, então $R_1 \times R_2 \times \ldots \times R_n$ também é anel quando munido das operações definidas acima.

Proposição 2.14 *Sejam $R_1, R_2, \ldots, R_n$, anéis simples, então o anel $R = R_1 \times R_2 \times \ldots \times R_n$ é semiprimo.*

Demonstração: Seja I um ideal não nulo de R, logo existem I_i ideal de R_i tais que $I = (I_1, I_2, \ldots, I_n)$, como cada R_i é simples, então $I_i = \{0\}$ ou $I_i = R_i$ para cada $1 \leq i \leq n$. Como I é não nulo, então existe $I_k \neq \{0\}$ e nesse caso $I_k = R_k \neq \{0\}$, donde $I_k^2 = R_k^2 = R_k$. Assim $I^2 = (I_1^2, I_2^2, \ldots, R_k, \ldots, I_n^2) \neq \{0\}$. □

Em particular

$$R = M_{n_1}(D_1) \times M_{n_2}(D_2) \times \ldots \times M_{n_m}(D_m)$$

é semiprimo, onde cada D_i é um anel de divisão.

2.3 Isomorfismo de anéis

Definição 2.15 *Seja R e S anéis. Uma aplicação $\psi : R \longrightarrow S$ é dito um homomorfismo de anéis, se $\psi(a+b) = \psi(a) + \psi(b)$ e $\psi(ab) = \psi(a)\psi(b)$, sejam quais forem $a, b \in R$.*

Sejam R e S anéis e $\psi : R \longrightarrow S$ um homomorfismo de anéis. Dado $r \in R$, então $\psi(r) = \psi(r+0) = \psi(r) + \psi(0)$, logo $\psi(0) = 0$. Note também que $0 = \psi(0) = \psi(r + (-r)) = \psi(r) + \psi(-r)$, logo $\psi(-r) = -\psi(r)$.

Dessa forma temos que $Ker(\psi) = \{r \in R : \psi(r) = 0\}$ é ideal à esquerda de R, pois $\psi(a-b) = \psi(a) - \psi(b) = 0$ e $\psi(ra) = r\psi(a) = 0$, sejam quais forem $a, b \in Ker(\psi)$ e $r \in R$.

Temos também que $Im(\psi) = \{s \in S : \psi(r) = s,$ para algum $r \in R\}$ é ideal à esquerda de S, pois dados $a, b \in Im(\psi)$ e $r \in R$, então existem $r_1, r_2 \in R$ tais que $\psi(r_1) = a$ e $\psi(r_2) = b$, assim $a - b = \psi(r_1) - \psi(r_2) = \psi(r_1 - r_2)$ e $ra = r\psi(r_1) = \psi(rr_1)$.

Definição 2.16 *Dizemos que dois anéis R e S são isomorfos se existe um homomorfismo $\psi : R \longrightarrow S$ que é injetor e sobrejetor. Nesse caso dizemos que ψ é um isomorfismo de R em S e escrevemos $R \simeq S$.*

Proposição 2.17 *Sejam R e S anéis. Um homomorfismo $\psi : R \longrightarrow S$ é injetor se, e somente se $Ker(\psi) = \{0\}$.*

Demonstração: Assuma que ψ é injetora. Como ψ é homomorfismo, então $\psi(0) = 0$, seja então $r \in R$ tal que $\psi(r) = 0$, logo $\psi(0) = \psi(r)$, como ψ é injetora, então $r = 0$.

Reciprocamente, suponha que $Ker(\psi) = \{0\}$. Sejam $r_1, r_2 \in R$ tais que $\psi(r_1) = \psi(r_2)$, como ψ é homomorfismo, temos que $\psi(r_1 - r_2) = 0$, pela hipótese, $r_1 - r_2 = 0$. □

Para entender o próximo teorema é preciso conhecer o conceito de anel quociente, para isso consulte [3], ou veja o apêndice desse trabalho.

Teorema 2.18 *(**Teorema do homomorfismo para anéis**) Seja R e S anéis e ϕ um homomorfismo de R em S. Então $R/Ker(\phi) \simeq Im(\phi)$.*

Demonstração: Defina $\psi : R/Ker(\phi) \longrightarrow Im(\phi)$ dada por $\psi(r + Ker(\phi)) = \phi(r)$, qualquer que seja $r \in R$.

i. ψ está bem definida: De fato, sejam $r_1, r_2 \in R$ tais que $r_1 + Ker(\phi) = r_2 + Ker(\phi)$, então $r_1 - r_2 \in Ker(\phi)$, assim $\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = 0$, portanto $\phi(r_1) = \phi(r_2)$.

ii. A aplicação ψ é um homomorfismo de anéis: Sejam $r_1 + Ker(\phi), r_2 + Ker(\phi) \in R/Ker(\phi)$, logo $\psi((r_1 + Ker(\phi)) + (r_2 + Ker(\phi))) = \psi((r_1 + r_2) + Ker(\phi)) = \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) = \psi(r_1 + Ker(\phi)) + \phi(r_2 + Ker(\phi))$.

Também temos $\psi((r_1+Ker(\phi))(r_2+Ker(\phi))) = \psi((r_1r_2)+Ker(\phi)) = \phi(r_1r_2) = \phi(r_1)\phi(r_2) = \psi(r_1 + Ker(\phi))\phi(r_2 + Ker(\phi))$.

iii. A aplicação ψ é injetora: Seja $r \in R$ tal que $\psi(r + Ker(\phi)) = \phi(r) = 0$, logo $r \in Ker(\phi)$, assim $r + Ker(\phi) = Ker(\phi)$.

iv. A aplicação ψ é sobrejetora: Segue da própria definição de ψ.

Portanto $R/Ker(\phi) \simeq Im(\phi)$. □

3 Condições de Finitude

3.1 Condições de Cadeia

Definição 3.1 *Dizemos que um anel R satisfaz a condição de cadeia descendente (respectivamente ascendente) sobre ideais à esquerda de R se, toda cadeia $I_1 \supseteq I_2 \supseteq \dots$ (respectivamente $I_1 \subseteq I_2 \subseteq \dots$) de ideais à esquerda de R é finita, isto é, existe um inteiro positivo n tal que $I_i = I_n$ para todo $i \geq n$. Satisfeito isso, dizemos que o anel R é artiniano (respectivamente noetheriano) à esquerda.*

De forma análoga podemos definir anel artiniano (respectivamente noetheriano) à direita, bastando substituir "esquerda"por "direita"na definição acima.

Proposição 3.2 *Seja D um anel de divisão, então D é artiniano à esquerda e à direita.*

Demonstração: Segue do fato de que os únicos ideais à esquerda de D são os triviais. O mesmo vale para os ideais à direita. □

Proposição 3.3 *Seja D um anel de divisão. Então o anel $M_n(D)$ é artiniano à esquerda e à direita.*

Demonstração: Seja $\mathcal{M}_1 \supseteq \mathcal{M}_2 \supseteq \dots$ uma cadeia descendente de ideias à esquerda de $M_n(D)$. Denotando

$$\mathcal{M}_k = \begin{bmatrix} D_{11}^k & \cdots & D_{1n}^k \\ \vdots & \ddots & \vdots \\ D_{n1}^k & \cdots & D_{nn}^k \end{bmatrix},$$

onde D_{lm}^k são ideais à esquerda de D para cada $k \geq 1$ inteiro e $l, m = 1, ..., n$. Como D é anel de divisão, então D_{lm}^k é ideal para cada $k \geq 1$ inteiro e $l, m = 1, ..., n$. Além disso D é simples, pois é anel de divisão, logo $D_{lm}^k = \{0\}$ ou $D_{lm}^k = D$ para cada $k \geq 1$ inteiro e $l, m = 1, ..., n$.

Como $\mathcal{M}_i \supseteq \mathcal{M}_j$ sempre que $j \geq i$, então $D_{lm}^i \supseteq D_{lm}^j$ para todos $l, m = 1, ..., n$, assim nosso problema se resume a estudar as cadeias $D_{lm}^1 \supseteq D_{lm}^2 \supseteq \dots$ para cada $l, m = 1, ..., n$. Como D é artiniano à esquerda, então tais cadeia são finitas, o que implica que a cadeia considerada inicialmente também é finita.

Portanto $M_n(D)$ é artiniano à esquerda. Para mostrar que $M_n(D)$ é artiniano à direita o raciocínio é análogo, bastando apenas trocar "esquerda"por "direita". □

Proposição 3.4 *Sejam $R_1, R_2, \ldots, R_n$, anéis artinianos à esquerda (respectivamente à direita), então o anel $R = R_1 \times R_2 \times \ldots \times R_n$ é artiniano à esquerda (respectivamente à direita).*

Demonstração: Seja uma cadeia $I_1 \supseteq I_2 \supseteq \ldots$ de ideais à esquerda de R. Como para cada j podemos escrever $I_j = (I_{j1}, I_{j2}, \ldots, I_{jn})$, onde para cada i, I_{ji} é ideal à esquerda de R_i para todo j. É claro que, $I_j \supseteq I_k$ implica $I_{ji} \supseteq I_{ki}$ para todo i. Dessa forma a cadeia inicial de ideais à esquerda nos dá $I_{1i} \supseteq I_{2i} \supseteq \ldots$ para todo i, como R_i é artiniano à esquerda para cada i, então tais cadeias são finitas. Logo a cadeia $I_1 \supseteq I_2 \supseteq \ldots$ também é finita.

O caso artinino à direita se prova de mandeira similar. □

Em particular o anel

$$R = M_{n_1}(D_1) \times M_{n_2}(D_2) \times \ldots \times M_{n_m}(D_m)$$

é artiniano tanto à esquerda quanto à direita, onde cada D_i é um anel de divisão.

Observação 3.5 *(**Importante**) De agora em diante, a menos que seja indicado, vamos considerar apenas o caso artinaino à esquerda, dessa forma, afim de abreviar a notação, sempre que escrevermos anel artiniano, estaremos nos referindo ao caso artiniano à esquerda. Também vamos abreviar noetheriano à esquerda por noetheriano.*

Isso não implica em perda de generalidade, pois todos os resultados vistos neste trabalho podem ser naturalmente estendidos pra o caso "à direita".

3.2 Algumas aplicações do Lema de Zorn

Definição 3.6 *Seja R um anel. Dizemos que um ideal I à esquerda (respectivamente a direita) de R é maximal, se $I \neq R$ e dado um ideal à esquerda (respectivamente à direita) J, com $I \subseteq J$, então $J = R$.*

Dizemos que um ideal I de R é maximal se $I \neq R$ e dado um ideal J, com $I \subseteq J$, então $J = R$.

Definição 3.7 *Seja R um anel. Dizemos que um ideal I à esquerda (respectivamente à direita) de R é minimal, se $I \neq \{0\}$ e dado um ideal à esquerda (respectivamente à direita) J, com $J \subseteq I$, então $J = \{0\}$.*

Dizemos que um ideal I de R é minimal se $I \neq \{0\}$ e dado um ideal J, com $J \subseteq I$, então $J = \{0\}$.

Definição 3.8 *Seja $\mathcal{F}$ um conjunto de subconjuntos de um conjunto dado. Dizemos que um elemento $A \in \mathcal{F}$ é Maximal em $\mathcal{F}$, se $A \nsubseteq F$ para todo $F \in \mathcal{F}$.*

Por outro lado um elemento $B \in \mathcal{F}$ é minimal em $\mathcal{F}$, se $F \nsubseteq B$ para todo $F \in \mathcal{F}$.

Definição 3.9 *Seja $\mathcal{I}$ uma subfamília de $\mathcal{F}$. Dizemos que um elemento $A \in \mathcal{F}$ é uma cota superior de $\mathcal{I}$, se $I \subseteq A$ para todo $I \in \mathcal{I}$.*

Por outro lado um elemento $B \in \mathcal{F}$ é uma cota inferior de $\mathcal{I}$, se $B \subseteq I$ para todo $I \in \mathcal{I}$.

Lema 3.10 ***(Lema de Zorn)*** *Seja $\mathcal{F} \neq \varnothing$ uma família parcialmente ordenada de subconjuntos de um conjunto dado, com a propriedade de que toda subfamília totalmente ordenada admite uma cota superior em $\mathcal{F}$, então $\mathcal{F}$ contém um elemento maximal.*

É possível enunciar o lema de Zorn de forma equivalente trocando "cota superior"por "cota inferior", e nesse caso trocamos "maximal"por "minimal", como podemos ver no corolário a seguir:

Corolário 3.11 *Seja $\mathcal{F} \neq \varnothing$ uma família parcialmente ordenada de subconjuntos de um conjunto dado, com a propriedade de que toda subfamília totalmente ordenada admite uma cota inferior em $\mathcal{F}$, então $\mathcal{F}$ contém um elemento minimal.*

Demonstração: De fato, denote por $\geq$ a ordem parcial de $\mathcal{F}$ e defina a ordem parcial $\geq^*$ em $\mathcal{F}$ como $b \geq^* a$ se, e somente se $a \geq b$, para todo $a, b \in \mathcal{F}$.

Dessa forma $\mathcal{F}$ munido com $\geq^*$ satisfaz a condição do lema de Zorn, então, com respeito a $\geq^*$, existe um elemento maximal c em $\mathcal{F}$, ou seja, $d \ngeq^* c$ para todo $d \in \mathcal{F}$, logo $c \ngeq d$ para todo $d \in \mathcal{F}$. Dessa forma c é um elemento minimal em $\mathcal{F}$ com respeito a $\geq$. □

Proposição 3.12 *Seja R um anel artiniano, então R contém um ideal minimal à esquerda.*

Demonstração: Seja $\mathcal{J}$ a família de todos os ideais à esquerda não nulos de R. Como R está em $\mathcal{J}$, então $\mathcal{J} \neq \varnothing$. Tal família é parcialmente ordenada pela relação de inclusão. Como R é artiniano, então toda subfamília totalmente ordenada de $\mathcal{J}$ tem uma cota inferior em $\mathcal{J}$.

Portanto, pelo corolário do lema de Zorn, $\mathcal{J}$ contém um elemento minimal, isto é, um ideal à esquerda minimal. □

Proposição 3.13 *Seja R um anel e $L \neq \{0\}$ um ideal à esquerda de R. Se R é artiniano, então existe um ideal minimal à esquerda de R contido em L.*

Demonstração: Considere a família $\mathcal{L}$ de todos os ideais à esquerda não nulos de R que estão contidos em L, tal família é não vazia, pois $L \in \mathcal{L}$. Como R é artiniano, então toda subfamília totalmente ordenada de $\mathcal{L}$ tem uma cota inferior em $\mathcal{L}$.

Portanto, pelo corolário lema de Zorn, existe em $\mathcal{L}$ um elemento minimal, ou seja, existe um ideal minimal à esquerda de R que está contido em L. □

3.3 Idempotentes e Anuladores

Definição 3.14 *Seja R um anel. Se X e Y são subconjuntos não vazios de R, nós definimos o produto se X por Y como:*

$$XY = \left\{ \sum_{i=1}^{n} x_i y_i : \ x_i \in X, \ y_i \in Y \ e \ n \geq 1 \ inteiro \right\}.$$

Afim de simplificação, dado um conjunto X, não vazio, definimos $X^2 = XX$.

Proposição 3.15 *Seja R um anel, então I é ideal à esquerda (respectivamente à direita) de R se, e somente se $RI \subseteq I$ (respectivamente $IR \subseteq I$).*

Demonstração: Assuma que I é ideal à esquerda, pela definição 2.8, naturalmente temos que $RI \subseteq I$. Reciprocamente, dados $x, y \in I$, como R é anel com unidade, temos que $x - y = 1x + (-1)y \in RI \subseteq I$. Agora dados $r \in R$ e $x \in I$, é claro que $rx \in RI \subseteq I$. Portanto I é ideal à esquerda de R.

O caso em que I é ideal à direita de R, prova-se de maneira análoga. □

Note que dado um subconjunto S não vazio de R, então $R^2S \subseteq RS$ (respectivamente $SR^2 \subseteq SR$), logo RS (respectivamente SR) é ideal à esquerda (respectivamente à direita) de R. No caso em que S é um conjunto unitário, digamos $S = \{x\}$, costuma-se representar o ideal à esquerda $R\{x\}$ (respectivamente $\{x\}R$) simplesmente como Rx (respectivamente xR).

Definição 3.16 *Seja R um anel e seja S um subconjunto não vazio de R. Defina o con-*

junto $Ann_l(S)$, chamado o anulador à esquerda de S em R como sendo :

$$Ann_l(S) = \{r \in R : rs = 0, \forall s \in S\}$$

Analogamente defina

$$Ann_r(S) = \{r \in R : sr = 0, \forall s \in S\}$$

o anulador à direita de S em R.

Quando S for um conjunto unitário, digamos $S = \{s\}$, vamos denotar $Ann_l(S)$, simplesmente por $Ann_l(s)$, analogamente $Ann_r(s)$.

Definição 3.17 *Seja R um anel, um elemento $e \in R$ é dito idempotente, se $e^2 = e$.*

Observe que em um anel com unidade $1^2 = 1$ e $0^2 = 0$ são elementos idempotentes triviais. Note também que $e(1-e) = (1-e)e = e - e^2 = 0$, assim, caso $e \neq 1$ e $e \neq 0$, então teremos dois elementos e e $(1-e)$ não nulos cujo o produto é nulo.

Proposição 3.18 *Seja R um anel, então segue que:*
i. *Se S é um subconjunto de R, então $Ann_l(S)$ (resp. $Ann_r(S)$) é um ideal à esquerda (resp. direita) de R.*
ii. *Seja $eR \subsetneq fR$, onde $e^2 = e$, $f^2 = f$, então $Ann_l(f) \subsetneq Ann_l(e)$.*
iii. *Seja $Re \subsetneq Rf$, onde $e^2 = e$, $f^2 = f$, então $Ann_r(f) \subsetneq Ann_r(e)$.*

Demonstração: Vamos começar por **i.** Tome $x, y \in Ann_l(S)$, logo $(x-y)s = xs - ys = 0 - 0 = 0$ para todo $s \in S$, dessa forma $x - y \in Ann_l(S)$. Agora dados $r \in R$ e $x \in Ann_l(S)$, então $(rx)s = r(xs) = r0 = 0$, seja qual for s em S, portanto $rx \in Ann_l(S)$, quaisquer que sejam $r \in R$ e $x \in Ann_l(S)$ tomados. O caso de $Ann_r(S)$ é análogo.

ii. Seja $x \in Ann_l(f)$. Por hipótese temos que $e = fr$ para algum $r \in R$, logo $xe = x(fr) = (xf)r = 0$, assim $x \in Ann_l(e)$. Portanto $Ann_l(f) \subseteq Ann_l(e)$.

Agora note que $(1-e)e = e - e^2 = e - e = 0$, logo $1 - e \in Ann_l(e)$. Por outro lado $(1-e)f = f - ef \neq 0$, pois se $f = ef$ então $f \in eR$, ou seja $fR \subseteq eR$, mas por hipótese temos que eR está contido propriamente em fR. Portanto $Ann_l(f) \neq Ann_l(e)$.

A prova de **iii.** é similar a prova de **ii.** □

Definição 3.19 *Seja R um anel. Dizemos que $x, y \in R$ são ortogonais se $xy = yx = 0$. O conjunto dos elementos idempotentes ortogonais de R é aquele consistindo apenas de elementos idempotentes que são ortogonais entre si, dois a dois.*

Proposição 3.20 *Se um anel R é artiniano, então R satisfaz a condição de cadeia ascendente para ideais da forma eR, onde $e^2 = e$.*

Demonstração: Seja $e_1R \subseteq e_2R \subseteq e_3R \subseteq \ldots$ uma cadeia ascendente de ideais à direita da forma e_iR, com $e_i^2 = e_i$ para cada $i \geq 1$ inteiro. Redefinindo a cadeia, se necessário, podemos assumir que e_iR está contido propriamente em e_jR para todo $j \geq i$.

Suponha por absurdo que a cadeia é infinita. Pela proposição anterior temos que $Ann_l(e_1R) \supsetneq Ann_l(e_2R) \supsetneq Ann_l(e_3R) \supsetneq \ldots$ é uma cadeia infinita de ideais à esquerda com $Ann_l(e_iR)$ contido propriamente em $Ann_l(e_jR)$ sempre que $j \geq i$, mas isso é absurdo, pois por hipótese R é artiniano. □

Proposição 3.21 *Se um anel R satisfaz a condição de cadeia ascendente para ideais da forma eR, onde $e^2 = e$ (ideais da forma Re, onde $e^2 = e$), então o conjunto dos idempotentes ortogonais de R é finito.*

Demonstração: Seja $E = \{e_1, e_2, e_3, \ldots\}$ o conjunto dos idempotentes ortogonais de R tais que $e_k \neq 0$, para todo $k \geq 1$ inteiro. Suponha por absurdo que E seja infinito. Note que $(\sum_{i=1}^{n} e_i)^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} e_ie_j = \sum_{i=1}^{n} e_i$, pois $e_i^2 = e_i$ para cada $1 \leq i \leq n$ e $e_ie_j = e_je_i = 0$ sempre que $i \neq j$, $1 \leq i, j \leq n$.

Observe também que

$$\sum_{i=1}^{n+1} e_i \sum_{j=1}^{n} e_j = \sum_{i=1}^{n+1}\sum_{j=1}^{n} e_ie_j = \sum_{i=1}^{n} e_i \sum_{j=1}^{n} e_j + e_{n+1}\sum_{j=1}^{n} e_j = \sum_{i=1}^{n} e_i,$$

logo $(e_1 + e_2 + \ldots + e_n)R \subseteq (e_1 + e_2 + \ldots + e_{n+1})R$.

Por fim, se existir $r \in R$ tal que $(e_1 + e_2 + \ldots + e_{n+1}) = (e_1 + e_2 + \ldots + e_n)r$, então $e_{n+1} = e_{n+1}(e_1+e_2+\ldots+e_{n+1}) = e_{n+1}(e_1+e_2+\ldots+e_n)r = 0$, que é uma contradição, pois estamos supondo que $e_i \neq 0$ para todo i. Dessa forma temos que $(e_1 + e_2 + \ldots + e_n)R$ está contido propriamente em $(e_1 + e_2 + \ldots + e_{n+1})R$.

Agora, considere a cadeia $e_1R \subsetneq (e_1 + e_2)R \subsetneq (e_1 + e_2 + e_3)R \subsetneq \ldots$ como E é infinito então tal cadeia nunca termina, o que é absurdo. Portanto o conjunto E é finito.

Agora, se assumirmos que R satisfaz a condição de cadeia ascendente para ideais da forma Re, $e^2 = e$, então procedendo de forma análogo ao caso acima, temos que a cadeia $Re_1 \subsetneq R(e_1 + e_2) \subsetneq R(e_1 + e_2 + e_3) \subsetneq \ldots$ nunca termina, uma contradição. Portando E é finito. □

Proposição 3.22 *Se o conjunto dos idempotentes ortogonais de R é finito, então R satisfaz a condição de cadeia ascendente e descendente para ideais da forma Re, onde $e^2 = e$.*

Demonstração: Suponha que R possua apenas o elemento 1 como idempotente não nulo. Nesse caso, só existem dois ideais da forma Re, com $e^2 = e$, que são R e $\{0\}$, assim é claro que a proposição vale para R.

Agora suponha que a quantidade de idempotentes não nulos de R seja maior ou igual a 2.

Considere uma cadeia finita $Re_1 \subsetneq Re_2 \subsetneq Re_3 \subsetneq \ldots \subsetneq Re_n$ onde cada e_i é um elemento idempotente não nulo e $n \geq 2$.

Note que $e_i \neq e_j$ sempre que $i \neq j$ e que dados $j \geq i$, então existe $r_i \in R$ tal que $e_i = r_i e_j$, donde concluimos que $e_i e_j = r_i e_j e_j = r_i e_j = e_i$.

Considere o conjunto $E_n = \{e_n - e_n e_{n-1}, e_n e_{n-1} - e_n e_{n-1} e_{n-2}, \cdots, e_n \cdots e_2 - e_n \cdots e_1, e_n \cdots e_1\}$.

Vamos usar indução sobre n para mostrar que os elementos de tal conjunto são idempotentes, ortogonais dois a dois, distintos e não nulos.

Base: Para $n = 2$ temos $E_1 = \{e_2 - e_2e_1, e_2e_1\}$. São não nulos, pois caso $e_2 = e_2e_1$, então $e_2 \in Re_1$, mas estamos supondo que isso não ocorre. Agora se $e_2e_1 = 0$ então $e_1e_2e_1 = e_1e_1 = e_1 = 0$, que não é o caso. São distintos, pois $e_1(e_2 - e_2e_1) = e_1e_2 - e_1e_2e_1 = e_1 - e_1 = 0$, enquanto que $e_1e_2e_1 = e_1 \neq 0$. São idempotentes, pois $(e_2 - e_2e_1)^2 = e_2^2 - e_2^2e_1 - e_2e_1e_2 + e_2e_1e_2e_1 = e_2 - e_2e_1 - e_2e_1 + e_2e_1 = e_2 - e_2e_1$, e no outro caso $(e_2e_1)^2 = e_2e_1e_2e_1 = e_2e_1$.

Por fim são ortogonais dois a dois, pois $(e_2 - e_2e_1)e_2e_1 = e_2^2e_1 - e_2e_1e_2e_1 = 0$, por outro lado, $e_2e_1(e_2 - e_2e_1) = e_2e_1e_2 - e_2e_1e_2e_1 = e_2e_1 - e_2e_1 = 0$.

Hipótese: Suponha que para algum $n \geq 2$, o resultado vale para E_n. Dado $x \in E_{n+1}$, então existe $f \in E_n$ tal que $x = e_{n+1}f$, logo $e_n x = e_n(e_{n+1}f) = (e_ne_{n+1})f = e_nf = f$, mas por hipótese de indução, $f \neq 0$, logo $x \neq 0$.

Por hipote de indução, podemos tomar $f, f' \in E_n$ distintos, observe que isso implica em $e_{n+1}f, e_{n+1}f' \in E_{n+1}$. Dessa forma $e_{n+1}f$ e $e_{n+1}f'$ são distintos pois, $e_{n+1}ff = e_{n+1}f^2 = e_{n+1}f$ enquanto que $e_{n+1}f'f = e_{n+1}f'f = 0$, mas pelo que acabamos de ver acima, $e_{n+1}f \neq 0$. Como qualquer elemento de E_{n+1} tem a forma $e_{n+1}f$ para algum $f \in E_n$, então os elemento de E_{n+1} são todos distintos.

Note agora que $(e_{n+1}f)^2 = e_{n+1}fe_{n+1}f = e_{n+1}e_{n+1}f = e_{n+1}f$, logo são idempotentes.

Por último, são ortogonais dois a dois, pois $e_{n+1}fe_{n+1}f' = e_{n+1}ff' = 0 = e_{n+1}f'e_{n+1}f = e_{n+1}f'f$, pois por hipótese de indução f e f' são ortogonais.

Agora suponha que exista uma cadeia infinita $Re_1 \subseteq Re_2 \subseteq Re_3 \subseteq \ldots$ onde $e_i^2 = e_i$ para todo i. Sem perda de generalidade podemos supor que as continências sejam estritas. Como o conjunto de elementos idempotente E é finito, então existe um inteiro positivo m correspondendo a cardinalidade de E. Sendo a cadeia acima infinita, então cosidere o truncamento $Re_1 \subsetneq Re_2 \subsetneq Re_3 \subsetneq \ldots \subsetneq Re_{m+1}$, mas mostramos que a partir de uma cadeia desse tipo podemos construir um subconjunto E_{m+1} de E cujo a cardinalidade é $m+1$, uma contradição.

Para mostrar que R satisfaz a condição de cadeia descendente para ideais da forma

$Re,\ ^2 = e$, basta redefinir a cadeia $Re_1 \subsetneq Re_2 \subsetneq Re_3 \subsetneq \ \ldots \ \subsetneq Re_n$ acima, fazendo $f_1 = e_n, \ldots, f_n = e_1$, assim teremos que $Rf_1 \supsetneq Rf_2 \supsetneq Rf_3 \supsetneq \ \ldots \ \supsetneq Rf_n$ onde cada $f_i^2 = f_i$, $i \geq 1$ inteiro. Proceda da mesma maneira que feito para o caso de cadeia ascendente. □

Corolário 3.23 *Seja R um anel artiniano, então R satisfaz a condição de cadeia ascendente para ideais da forma Re, onde $e^2 = e$.*

Demonstração: Sendo R artiniano, então pela proposição 3.20, temos que R satisfaz a condição de cadeia ascendente para ideais da forma eR, mas isso por sua vez implica, pela proposição 3.21, que o conjunto de idempotentes ortogonais é finito, e como consequência, pela proposição 3.22, segue o resultado desejado. □

Corolário 3.24 *Seja R um anel artiniano e seja $S \subseteq R$ um subconjunto não vazio de R, então a família $I = \{Re \subseteq R : e^2 = e,\ e \in S\}$ admite um elemento maximal.*

Demonstração: Note que os elementos da família $\mathcal{I}$ são da forma Re, onde $e \in S \subseteq R$ é elemento idempotente. Como R é artiniano, então pelo corolário anterior temos que toda cadeia ascendente de elementos de $\mathcal{I}$ admite uma cota superior, dessa forma estamos nas condições das hipóteses do Lema de Zorn, portanto $\mathcal{I}$ possuí elemento maximal. □

4 Módulos

4.1 Módulos e Endomorfismo

Definição 4.1 *Seja R um anel. Um grupo $(M,+)$ abeliano é chamado R-módulo à esquerda se para cada elemento $r \in R$ e cada elemento $m \in M$, existe um produto $rm \in M$ tal que:*
i. $(a+b)m = am + bm$;
ii. $a(m_1 + m_2) = am_1 + am_2$;
iii. $a(bm) = (ab)m$;
iv. $1m = m$.
Para todo $a, b \in R$ e todo $m, m_1, m_2 \in M$.
De forma análoga defini-se R-módulo à direita.

Observação 4.2 *(**Importante**) De agora em diante, quando não for indicado, vamos lidar apenas com R-módulos à esquerda, dessa forma, afim de abreviar a nomenclatura, usaremos R-módulo no lugar de R-módulo à esquerda.*
Isso não implica em perda de generalidade, pois todos os resultados vistos neste trabalho podem ser naturalmente estendidos pra o caso "à direita".

Definição 4.3 *Seja M um R-módulo. Dado um subconjunto não vazio N de M, dizemos que N é um R-submódulo de M, se $n_1 + n_2 \in N$ quaisquer que sejam $n_1, n_2 \in N$ e $rn \in N$ para todo $r \in R$ e todo $n \in N$.*

Exemplo 4.4 Dado um R-módulo M, então $\{0\}$ e M são submódulos de M, chamados submódulos triviais, qualquer submódulo diferente dos triviais é chamado de submódulo próprio.

Definição 4.5 *Um modulo que não contém submódulos próprios é chamado de simples.*

Note que A interseção de dois submódulos é sempre submódulo. Além disso, para toda cadeia $M_1 \subseteq M_2 \subseteq \ldots$ de submódulos de M tem-se que $M' = \cup_{i=1}^{\infty} M_i$ também submódulo de M.

De fato, dados $a, b \in M'$, então existem k e j inteiros positivos tais que $a \in M_k$ e $b \in M_j$, assim $a, b \in M_n$, onde n é o máximo de k e j. Como M_n é submódulo, então $a+b$, $ra \in M_n \subseteq M'$ para todo $r \in R$.

Definição 4.6 *Sejam M e N módulos sobre um anel R. Uma aplicação $T : M \longrightarrow N$ é dita R-linear (ou R-homomorfismo) se satisfaz a condição $T(rm_1+m_2) = rT(m_1)+T(m_2)$, para todo $r \in R$ e $m_1, m_2 \in M$.*

Com a notação da definição acima, definimos o conjunto de todos elementos $m \in M$ tais que $T(m) = 0$, denotado por $Ker(T)$, é chamado núcleo (ou kernel) de T.

Definimos o subconjunto $Im(T)$ de N, como aquele consistindo de todos os elementos n de N para os quais existe algum outro elemento m em M tal que $T(m) = n$.

É fácil ver que tanto $Ker(T)$ quanto $Im(T)$ são R-submódulos.

Definição 4.7 *Dado um anel R e um R-módulo M, definimos o conjunto de Endomorfismos de M sobre R, como sendo o conjunto das transformações R-lineares de M em M.*

Denotaremos tal conjunto pelo simbolo $End_R M$.

Dados $T, S \in End_R M$, podemos definir a soma $T+S$ como sendo $(T+S)v = Tv + Sv$ para todo $v \in M$. Também podemos definir a multiplicação de T por S, como sendo $(T \circ S)v = T(Sv)$ para todo $v \in M$.

É fácil ver que $T+S, T \circ S \in End_R M$ para todo $T, S \in End_R M$. Além disso $End_R M$, munido com essas operações é um anel, chamado de anel de endomorfismo de M sobre R.

Definição 4.8 *Um R-homomorfismo que é bijeção, é chamado de R-isomorfismo. Sejam M e N R-módulos e suponha que exita uma aplicação $f : M \longrightarrow N$ que é um R-isomorfismo, então escrevemos que $M \simeq N$ e dizemos que M e N são isomorfos como módulos.*

Para entender o próximo teorema é preciso conhecer o conceito de módulo quociente, para isso consulte [3], ou veja o apêndice desse trabalho.

Teorema 4.9 *(**Teorema do Homomorfismo para módulos**) Sejam R um anel e M, N R-módulos. Considere T um R-homomorfismo de M em N. Então $M/Ker(T) \simeq Im(T)$.*

Demonstração: Defina $\phi : M/Ker(T) \longrightarrow Im(T)$, dada por $\phi(\overline{m}) = T(m)$, onde $\overline{m} = m + Ker(T)$. Vamos mostrar que ϕ é um R-isomorfismo:

i. ϕ está bem definida. De fato, sejam $n, m \in M$ tais que $\overline{n} = \overline{m}$, logo $n - m \in Ker(T)$, como T é R-homomorfismo, então $T(n-m) = T(n) - T(m) = 0$, assim $T(n) = T(m)$. Portanto $\phi(\overline{n}) = \phi(\overline{m})$.

ii. ϕ é R-homomorfismo. De fato, sejam $\overline{m_1}, \overline{m_2} \in M/Ker(T)$ e $r \in R$, então $\phi(\overline{rm_1} + \overline{m_2}) = \phi(\overline{rm_1 + m_2}) = T(rm_1 + m_2) = rT(m_1) + T(m_2) = r\phi(\overline{m_1}) + \phi(\overline{m_2})$.

iii. ϕ é injetora. De fato, sejam $n, m \in M$ tais que $\phi(\overline{n}) = \phi(\overline{m})$, logo $T(n) = T(m)$, que implica em $T(n-m) = 0$, donde concluímos que $n - m \in Ker(T)$, logo $n, m \in M$ tais que $\overline{n} = \overline{m}$.

Como o contradomínio é $Im(T)$, então naturalmente ϕ é sobrejetora. Portanto $M/Ker(T) \simeq Im(T)$. □

Observe que se, no teorema acima, T for sobrejetiva, então teremos $Im(M) = N$ e como consequência, $M/Ker(T) \simeq N$.

4.2 Base e Dimensão em Módulos

Definição 4.10 *Seja M, um R-módulo, e seja $S \subseteq M$, um subconjunto não vazio. Dizemos que o conjunto S é linearmente independentes sobre R se, para todo subconjunto $\{s_1, s_2, \ldots, s_n\}$ finito de S e $r_1, r_2, \ldots r_n \in R$ tem-se que:*

$$r_1 s_1 + r_2 s_2 + \ldots r_n s_n = 0 \Rightarrow r_1 = r_2 = \ldots = r_n = 0.$$

Definição 4.11 *Seja M, um R-módulo, e seja $S \subseteq M$, um subconjunto não vazio. Dizemos que S é gerador de M sobre R, se dado $m \in M$, então existem $s_1, s_2, \ldots, s_n \in S$ e $r_1, r_2, \ldots r_n \in R$, tais que:*

$$m = \sum_{i=1}^{n} r_i s_i.$$

Se além de S ser gerador M sobre R, tem-se também que seus elementos são linearmente independentes sobre R, então dizemos que S é uma base de M sobre R.

Definição 4.12 *Seja M um R-módulo. Defina $\langle S \rangle$ como sendo*

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} r_i s_i : \ r_i \in D, \ s_i \in M \text{ e } n \geq 1 \text{ inteiro} \right\}.$$

É fácil verificar que tal conjunto é um R-submódulo de M. Chamamos $\langle S \rangle$ de R-submódulo gerado por S.

Proposição 4.13 *Seja M um R-módulo. Suponha que $\{m_1, \ldots, m_k\}$ é um subconjunto de M, linearmente independente sobre R. Agora seja $x \in M$ dado por $x = r_1 m_1 + \ldots + r_k m_k$, onde $r_i \in R$ para todo $1 \leq i \leq n$ e suponha que existam $r_i \in R$, onde $1 \leq i \leq n$ tais que $x = r_1' m_1 + \ldots + r_k' m_k$. Então $r_i = r_i'$ para todo $1 \leq i \leq k$.*

Demonstração: De fato, temos que $r_1 m_1 + \ldots + r_k m_k = r_1' m_1 + \ldots + r_k' m_k$, logo $(r_1 - r_1')m_1 + \ldots + (r_k - r_k')m_k = 0$, como $\{m_1, \ldots, m_k\}$ é um subconjunto de M, linearmente independente sobre R, então $r_i = r_i'$ para todo $1 \leq i \leq k$. □

Observação 4.14 *Como veremos mais para frente, o conceito de dimensão para módulos será essencial na prova do Teorema de Wedderburn, assim os teorema a seguir são essenciais para se definir tal conceito.*

Definição 4.15 *Seja M um R-módulo e considere $S \subseteq M$, $S \neq \varnothing$. Dizemos que S é um conjunto linearmente independente maximal de M sobre R se, S é linearmente independente sobre R e, para qualquer subconjunto S' de M que também é linearmente independente sobre R, tem-se que $S \nsubseteq S'$.*

Lema 4.16 *Seja M um D-módulo, onde D é um anel de divisão. Seja $S \subseteq M$, $S \neq \varnothing$, um conjunto linearmente independente maximal de M sobre D. Então S é uma base de M sobre D.*

Demonstração: Considere o D-submódulo $\langle S \rangle$, como S é linearmente independente sobre D, então S é base de $\langle S \rangle$ sobre D. Se $\langle S \rangle = D$, então nada há para se fazer. Se não, então existe $a \in D$ tal que $a \notin \langle S \rangle$. Assim, considere o conjunto $S \cup \{a\}$. Sejam $r, r_1, ..., r_n \in D$ e $s_1, ..., s_2 \in S$ tais que $ra + r_1 s_1 + ... + r_n s_n = 0$. Se $r \neq 0$, então r é inversível, pois D é anel de divisão, logo $a = r^{-1}(ra) = -r^{-1} r_1 s_1 - ... - r^{-1} r_n s_n \in \langle S \rangle$, mas isso é contraditório com nossa escolha de a.

Se $r = 0$, então $r_1 = r_2 = ... = r_n = 0$, pois S é linearmente independente sobre D, logo $S \cup \{a\}$ é linearmente independente sobre D, contrariando a maximalidade de S. □

Teorema 4.17 *Seja M um D-módulo, então M admite base sobre D.*

Demonstração: Seja $S = \{a\}$, onde $a \in M$ e $a \neq 0$, então S é linearmente independente sobre D. De fato, seja $r \in D$, $r \neq 0$, e suponha que $ra = 0$. Como D é anel de divisão, então r é inversível, logo $r^{-1}(ra) = (r^{-1}r)a = 1a = a = r^{-1}0 = 0$, absurdo, logo $r = 0$.

Defina $\mathcal{I}$ como sendo o conjunto de todos os subconjunto de M que são linearmente independentes sobre D, como $S \in \mathcal{I}$, então $\mathcal{I} \neq \varnothing$. Munindo $\mathcal{I}$ com a relação de inclusão, temos um conjunto parcialmente ordenado. Considere uma cadeia $S_1 \subseteq$

$S_2 \subseteq \ldots$, de $\mathcal{I}$. Logo $S = \cup_{i=1}^{\infty} S_i$ é uma cota superior dessa cadeia e dados quaisquer $s_{i_1}, ..., s_{i_n} \in S$, onde $i_k \geq 1$ são inteiros, para todo $1 \leq k \leq n$, então $s_{i_1}, ..., s_{i_n} \in S_L$, onde $L = max\{i_1, ..., i_n\}$. Como S_L é linearmente independente sobre D, então qualquer combinação $r_1 s_{i_1} + ... + r_n s_{i_n} = 0$, com $r_1, ..., r_n \in D$, implica em $r_1 = ... = r_n = 0$. Assim S é linearmente independente obre D. Dessa forma $S \in \mathcal{I}$. Pelo Lema de Zorn, $\mathcal{I}$ contém um elemento maximal A. Portanto, pelo lema 4.16, A é base de M sobre D. □

Teorema 4.18 *Seja M um D-módulo, então toda base de M sobre D tem a mesma cardinalidade.*

Para uma demonstração desse resultado veja referência [1].

Definição 4.19 *Seja M módulo sobre um anel R e suponha que M admite base sobre R. Dizemos que R tem a propriedade da dimensão invariante, se toda base de M sobre R tem a mesma cardinalidade, assim o cardinal de qualquer uma dessas bases é chamada de dimensão de M sobre R e denotada por $dim_R M$.*

Exemplo 4.20 *Pelo teorema anterior, módulos sobre anéis de divisão possuem a propriedade da dimensão invariante e portanto o conceito de dimensão está bem definido.*

Observação 4.21 *Os resultados acima podem ser naturalmente estendidos para o caso de módulos à direita.*

A próxima proposição ilustra um exemplo de como o conceito de dimensão pode nos auxiliar a obter resultados importantes.

Além disso, o resultado abaixo é enunciada para módulos à direita, pois como veremos na demonstração do Teorema de Wedderburn, em um passo da prova, este fato nos será útil.

Proposição 4.22 *Seja D um anel de divisão e M um D-módulo à direita. Suponha que $dim_D M = n$, para algum inteiro positivo n, então $End_D M \simeq M_n(D)$, como anéis.*

Demonstração: Como $dim_D M = n$, então existe uma base de M sobre D, que denotaremos por $\mathcal{B} = \{e_1, ..., e_n\}$. Assim, dado $T \in End_D M$, temos que para cada $e_i \in \mathcal{B}$, $1 \leq i \leq n$, temos que existem $A_{1i}, ..., A_{ni} \in D$, únicos, tais que $Te_i = \sum_{k=1}^{n} e_k A_{ki}$. Dessa

forma, dado $T \in End_D M$, podemos associar um elemento $A \in M_n(D)$ dado por

$$A = \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{bmatrix}.$$

Afirmação: A aplicação $\psi : End_D M \longrightarrow M_n(D)$, dada por $\psi(T) = A$, é um isomorfismo de anéis.

i. Como os elemento de A são determinados univocamente pela transformação T, então ψ está bem definida.

ii. ψ é um homomorfismo de anéis: Dados $T, S \in End_D M$, tais que $\psi(T) = A$ e $\psi(S) = B$, logo $(T+S)e_i = Te_i + Se_i = \sum_{k=1}^n e_k A_{ki} + \sum_{j=1}^n e_j B_{ji} = \sum_{k=1}^n e_k(A_{ki} + B_{ki})$, para todo $i = 1, ..., n$, pela unicidade da representação na base, temos que $\psi(T+S) = A + B = \psi(T) + \psi(S)$.

Agora seja $(T \circ S)e_j = T(Se_j) = T(\sum_{k=1}^n e_k B_{kj}) = \sum_{k=1}^n (Te_k)B_{kj} = \sum_{k=1}^n \sum_{i=1}^n e_i A_{ik} B_{kj} = \sum_{i=1}^n e_i \Big(\sum_{k=1}^n A_{ik} B_{kj} \Big) = \sum_{i=1}^n e_i (AB)_{ij}$.

Portanto, pela unicidade da representação na base, temos que $\psi(T \circ S) = AB = \psi(T)\psi(S)$.

iii. ψ é injetora: seja $T \in End_D M$ tal que $\psi(T) = 0$, mas pela definição de ψ isso implica em $Te_i = 0$ para todo $i = 1, ..., n$, ou seja, $T = 0$. Assim, $Ker\psi = 0$.

iv. ψ é sobrejetora: seja $A \in M_n(D)$, defina $Te_i = \sum_{k=1}^n A_{ki} e_k$, para todo $i = 1, ..., n$.

Pela unicidade da representação na base, temos que $\psi(T) = A$.

Portanto $End_D M \simeq M_n(D)$. □

4.3 Soma Direta

Definição 4.23 *Seja M um R-módulo. Considere $\mathcal{M} = \{M_i\}_{i \in I}$, uma família de R-submódulos de M, onde I é um conjunto de índices. Dizemos que M é soma direta de R-submódulos da família $\mathcal{M}$ se:*

i. *Para todo $i \in I$, tem-se que $M_k \cap (\sum_{i \neq k} M_i) = \{0\}$.*

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

Nesse caso escrevemos $M = \oplus_{i \in I} M_i$.

*As condições **i.** e **ii.** acima, podem ser substituídas equivalentemente pela condição:*

iii. *Todo $m \in M$ pode ser escrito de forma única como $r = s_{i_1} + s_{i_2} + \ \ldots \ + s_{i_n}$, onde $s_{i_j} \in M_{i_j}$, $i_j \in I$ e $1 \leq j \leq n$.*

Dado um anel S, se trocarmos R-submódulos por subanéis de S na definição acima,

então dizemos que S é uma soma direta de subanéis.

Definição 4.24 *Dado um R-módulo M e seja N um R-submódulo. Dizemos que N é um somando direto de M, se existe um outro R-submódulo N' de M tal que* $R = N \oplus N'$.

Proposição 4.25 *Seja R um anel e suponha que existem* $S_1, S_2, \ldots, S_n$ *subanéis em R tais que* $R = \oplus_{i=1}^{n} S_i$. *Suponha também que para cada i tem-se que* $S_i \simeq M_i$, *onde* M_i *é anel para todo i, então* $R \simeq M_1 \times M_2 \times \ldots \times M_n$.

Demonstração: Sejam $\psi_i : S_i \longrightarrow M_i$ isomorfismos para cada i. Dado $r \in R$, então existem únicos $s_i \in S_i$ tais que $r = \sum_{i=1}^{n} s_i$. Assim defina $\Psi : R \longrightarrow M_1 \times M_2 \times \ldots \times M_n$, dada por $\Psi(r) = (\psi_1(s_1), \psi_2(s_2), \ldots, \psi_n(s_n))$. Como os elementos s_i são únicos, então Ψ está bem definida. É fácil ver que, o fato de que cada ψ_i ser isomorfismo, implica que Ψ é isomorfismo. □

4.4 Semissimplicidade

Definição 4.26 *Um R-módulo M é dito semissimples se todo R-submódulo é somando direto de M.*

Proposição 4.27 *Seja M um R-módulo semissimples. Então todo submódulo de M, não nulo, é semissimples e contém um submódulo simples.*

Demonstração: Seja N um R-submódulo não nulo de M, e considere L um R-submódulo de N. Note que L também é R-submódulo de M. Como M é semissimples, então existe um R-submódulo L' de M tal que $M = L \oplus L'$. Como tanto N quanto L' são R-submódulo de M, então $N \cap L'$ também é.

Vamos mostrar que $N = L \oplus (N \cap L')$. De fato, note que $L \cap (N \cap L') \subseteq L \cap L' = 0$. Agora, como $M = L \oplus L'$, então dado $x \in N$, existem $a \in L$ e $b \in L'$ tais que $x = a + b$, mas $b = x - a \in N$, logo $b \in N \cap L'$.

Para provar que N contém um submódulo simples. Escolha um elemento $x \in N$, $x \neq 0$. A família de todos os submódulos de N que não contém x é não vazio, pois o módulo nulo pertence a tal família. Note que essa família é parcialmente ordenada pela relação de inclusão $\subseteq$, além disso toda subfamília totalmente ordenada tem uma cota superior (basta tomar a união dos elementos dessa subfamília). Assim pelo lema de Zorn existe um elemento maximal N_1. Como N é semisimples, então existe um submódulo N_2 tal que $N = N_1 \oplus N_2$.

Vamos mostrar que N_2 é simples. Suponha por absurdo que N_2 não é simples, então existe um submódulo próprio Y de N_2. Como N_2 é semissimples então existe

um submódulo Y' tal que $N_2 = Y \oplus Y'$, assim $N = N_1 \oplus Y \oplus Y'$. Além disso, $N_1 \subseteq N_1 + Y$ e $N_1 \subseteq N_1 + Y'$, logo $N_1 \subseteq (N_1 + Y) \cap (N_1 + Y')$ e como $Y,\ Y' \subseteq N_1$, segue também a inclusão contraria. Assim, $N_1 = (N_1 + Y) \cap (N_1 + Y')$. Dessa forma, como $x \notin N_1$, então $x \notin (N_1 + Y)$ ou $x \notin (N_1 + Y')$ o que contrária a maximalidade de N_1. □

Teorema 4.28 *Seja M um R-módulo. Então as seguintes condições são equivalentes:*
i. *M é semissimples*
ii. *M é uma soma direta de R-submódulos simples*
iii. *M é uma soma, não necessariamente direta, de R-submódulos simples.*

Demonstração: i. ⇒ ii. Seja $\mathcal{F}$ a família de todos os submódulos de M que podem ser escritos como soma direta de submódulos simples. Note que pela proposição 4.13 todo submódulo de M contém um submódulo simples, assim $\mathcal{F}$ contém ao menos esses submódulos simples, assim $\mathcal{F} \neq \varnothing$. Vamos definir uma ordem parcial em nessa família. Dados $\oplus_{i\in I}$ e $\oplus_{i\in J} M_i$ elementos de $\mathcal{F}$ definimos $\oplus_{i\in I} M_i \preceq \oplus_{i\in J} M_i$ se, e somente se $I \subseteq J$.

Não é difícil ver que $\preceq$ determina uma relação de ordem parcial em $\mathcal{F}$. Além disso $(\mathcal{F}, \preceq)$ satisfaz as condições do lema de Zorn, de fato dado uma subfamília não vazia e totalmente ordenada $\mathcal{E} = \{\oplus_{k\in K_i} M_k\}_{i\in L}$, o elemento $\oplus_{k\in K} M_k$, onde $K = \cup_{i\in L} K_i$ é cota superior de $\mathcal{E}$.

Assim, existe um elemento $M' \in \mathcal{F}$ que é maximal. Dessa forma $M' = \oplus_{i\in I} M_i$, para algum conjunto de índices I, e M_i simples para todo $i \in I$.

Vamos mostrar que $M = M'$. Assuma que $M \neq M'$, então por semissimplicidade de M existe um submódulo não nulo N tal que $M = M' \oplus N$. Pela proposição 4.27, N contém um submódulo simples, digamos S. Note que $S \subseteq N \nsubseteq M'$, assim $M' \oplus S = \oplus_{i\in I} M_i \oplus S \supsetneq M'$, o que contraria a maximalidade de M'.

Por definição de soma direta temos que **i. ⇒ ii.**

iii. ⇒ i. Assuma que $M = \sum_{i\in I} M_i$ com cada submódulo M_i simples. Seja N um submódulo de M. Se $N = M$ ou $N = \{0\}$, então é claro que N é somando direto de M. Sendo assim assuma que N é submódulo próprio de M.

Considere a seguinte família:

$$\mathcal{J} = \left\{ \sum_{i\in J} M_i : J \subseteq I, \left(\sum_{i\in J} M_i \right) \cap N = \{0\} \right\}.$$

Note que, como M_i é simples para todo i, então $N \cap M_i \neq \{0\}$ implica em $M_i \subseteq N$, seja qual for o índice i, como $N \neq M$, então N não pode conter todos os M_i's, logo existe um submódulo M_k tal que $M_k \nsubseteq N$, assim por semissimplicidade de M_k, temos

$M_k \cap N = \{0\}$. Dessa forma $\mathcal{J} \neq \varnothing$. agora, defina a relação $\sum_{i\in J_1} M_i \preceq \sum_{i\in J_2} M_i$ se, e somente se $J_1 \subseteq J_2$. Não é difícil ver que $\preceq$ define uma relação de ordem parcial em $\mathcal{J}$. Além disso, argumentando de forma similar ao caso acima, mostra-se que $(\mathcal{J}, \preceq)$ satisfaz as condições do lema de Zorn. Seja então, $M' = \sum_{i\in J'} M_i$ o elemento maximal de $\mathcal{J}$. Vamos mostrar que $M = M' \oplus N$. Como $(\sum_{i\in J'}) \cap N = \{0\}$, então basta mostrar que $M = M' + N$.

Se para todo $i \in I$ verificarmos que $M_i \subseteq M' + N$, então $\sum_{i\in I} M_i = M \subseteq M' + N$ e portanto $M = M' + N$. Assim, suponha por absurdo que exista um índice $l \in I$ tal que $M_l \nsubseteq M' + N$, logo $M_l + M' \nsubseteq N$, Como M_l é simples, então $(M_l + M') \cap N = \{0\}$. Dessa forma $M_l + M' \in \mathcal{J}$, mas isso contraria a maximalidade de M', pois $M' \subseteq M_l + M'$. Portanto $M = M' + N$. □

Seja R um anel e J um ideal à esquerda de R. Como $RJ \subseteq J$, então J é um R-módulo. Em particular R é um R-módulo. Note que todos os R-submódulos de R são justamente os ideais à esquerda de R.

Definição 4.29 *Dizemos que um anel R é semissimples se R visto como um R-módulo é semissimples.*

Corolário 4.30 *Seja R um anel semissimples, então todo R-módulo M é semissimples.*

Demonstração: Como R é semissimples, então pelo teorema acima, $R = \sum_{i\in I} R_i$ onde cada R_i é um ideal minimal à esquerda de R. Agora note que $M = \sum_{m\in M} Rm$, logo $M = \sum_{m\in M}(\sum_{i\in I} R_i)m = \sum_{m\in M}\sum_{i\in I} R_i m$. Vamos mostrar que para cada i em I, $R_i m$ é um R-submódulo simples de M. De fato, é claro que $R_i ms$ é um R-submódulo de M. Agora seja A um R-submódulo de $R_i m$, note que $A = \{rm : r \in L\}$, onde $r \in L$ se, e somente se $rm \in A$. Observe que $L \subseteq R_i$. Assim $A = Lm$. Como $(ra)m = r(am) \in A$ e $(a + b')m \in A$ para quaisquer $r \in R$ e $a, b \in L$, então ra, $a + b \in L$, e portanto L é um ideal à esquerda de R_i. como R_i é ideal minimal à esquerda de R, então $L = \{0\}$ ou $L = R_i$, isto é, $A = \{0\}$ ou $A = R_i m$. Portanto M é semissimples. □

Um exemplo de anel semissimples é o anel $M_n(D)$, onde n inteiro positivo e D anel de divisão. De fato, seja

$$\mathcal{M}_1 = \begin{bmatrix} D_{11} & \cdots & D_{1n} \\ \vdots & \ddots & \vdots \\ D_{n1} & \cdots & D_{nn} \end{bmatrix},$$

ideal à esquerda de $M_n(D)$, então para cada i e j, $D_{ij} = D$ ou $D_{ij} = \{0\}$. Dessa forma

seja

$$\mathcal{M}_2 = \begin{bmatrix} D'_{11} & \cdots & D'_{1n} \\ \vdots & \ddots & \vdots \\ D'_{n1} & \cdots & D'_{nn} \end{bmatrix},$$

onde $D'_{ij} = D$ se $D_{ij} = \{0\}$ e $D'_{ij} = \{0\}$ se $D_{ij} = D$, assim $M_n(D) = \mathcal{M}_1 \oplus \mathcal{M}_2$.

Proposição 4.31 *Sejam $R_1, R_2, \ldots, R_n$, anéis semissimples, então o anel $R = R_1 \times R_2 \times \ldots \times R_n$ é semissimples.*

Demonstração: Seja $\mathcal{J}_1 = (J_1, J_2, \ldots, J_n)$ ideal a esquerda de R, onde cada J_i é ideal à esquerda de R_i. Como cada R_i é semissimples, então para cada i existem J'_i ideias à esquerda de R_i, tal que $R_i = J_i \oplus J'_i$. Logo, seja $\mathcal{J}_2 = (J'_1, J'_2, \ldots, J'_n)$. Assim $R = \mathcal{J}_1 \oplus \mathcal{J}_2$. □

Como consequência o anel

$$R = M_{n_1}(D_1) \times M_{n_2}(D_2) \times \ldots \times M_{n_m}(D_m)$$

é semissimples, onde cada D_i é um anel de divisão.

Proposição 4.32 *Seja R um anel semissimples, então todo ideal à esquerda de R é da forma Re, onde $e^2 = e$.*

Demonstração: Assuma que R é semissimples. Dado I um ideal à esquerda de R, então existe outro ideal à esquerda J de R tal que $R = I \oplus J$. Sejam $a \in I$ e $b \in J$ tais que $a + b = 1$. Assim $a = a \cdot 1 = a(a + b) = a^2 + ab$, logo $ab = a - a^2 \in I$. Como J é ideal à esquerda, então $ab \in J$, mas $I \cap J = \{0\}$, dessa forma $ab = 0$, ou seja, $a = a^2$.

Agora dado $x \in I$, temos que $x = x \cdot 1 = x(a + b) = xa + xb$, logo $x - xa = xb \in I$, e por outro lado $xb \in J$, assim $x - xa = 0$, mas nesse caso temos que $x = xa$, logo $x \in Ra$, assim $I \subseteq Ra$. Como $Ra \subseteq I$, então $I = Ra$.

□

Proposição 4.33 *Seja R um anel semissimples, e seja S um ideal de R, então R/S é um R-módulo semissimples. Além disso R/S também é um anel semissimples.*

Demonstração: Como R é semissimples, então existem um ideal à esquerda L de R tal que $R = S \oplus L$. Agora notando que dado $r \in R$, existem únicos $s \in S$ e $l \in L$, tais que $r = s + l$, defina o R-homomorfismo sobrejetor $\pi : R \longrightarrow L$ dada por $\pi(r) = l$. Como $Ker(\pi) = S$, então pelo teorema do homomorfismo para módulos, temos que

$R/S \simeq L$, mas sabemos que L é um R-módulo semissimples, pois R é semissimples. Logo R/S é um R-módulo semissimples.

Para ver que R/S é um anel semissimples, tome $I \subseteq R$ ideal à esquerda de R/S. Note que dado $a+S \in I$, então $(r+S)(a+S) = ra+S = r(a+S) \in R/S$ para todo $r \in R$, logo I é um R-submódulo de R/S, como R/S é R-módulo semissimples, então existe um R-submódulo J de R/S tal que $R/S = I \oplus J$. Dessa forma, seja $r \in R$, logo $r(b+S) \in J$, seja qual for $b+S \in J$. Como $r(b+S) = rb+S = (r+S)(b+S)$, então J é um ideal à esquerda de R/S. Dessa forma R/S é anel semissimples. □

Proposição 4.34 *Todo anel semisimples é noetheriano.*

Demonstração: Seja R um anel semisimples. Dado um ideal à esquerda I de R, então pela proposição anterior existe $e \in R$, com $e^2 = e$, tal que $I = Re$, dessa forma podemos trabalhar apenas com cadeias da forma $Re_1 \subseteq Re_2 \subseteq Re_3 \subseteq \ldots$ onde para cada i, e_i é idempotente.

Vamos mostrar que a cadeia é finita e termina em $\cup_{i=1}^{\infty} Re_i$. De fato, como $\cup_{i=1}^{\infty} Re_i$ é ideal à esquerda de R, então existe $e \in R$, $e^2 = e$ tal que $\cup_{i=1}^{\infty} Re_i = Re$, assim existe um inteiro positivo n tal que $e \in Re_n$, mas nesse caso temos que $Re \subseteq Re_n$. Agora note que $e \in Re_n \subseteq Re_k$ para todo $k \geq n$, logo $Re \subseteq Re_k$ para todo $k \geq n$, como $Re_j \subseteq \cup_{i=1}^{\infty} Re_i = Re$ para todo j, então $Re_k = Re$ para todo $k \geq n$.

□

Proposição 4.35 *Seja R um anel semissimples, então as duas afirmações são verdadeiras:*
i. *R é artiniano.*
ii. *R é semiprimo.*

Demonstração: Pela proposição anterior, o fato de um anel ser semissimples implica que tal anel satisfaz a condição de cadeia ascendente para anéis da forma Re, com $e^2 = e$, mas pela proposição 3.21 isso implica que o conjunto de idempotente ortogonais é finito, o que por sua vez implica, pela proposição 3.22, que o anel satisfaz a condição de cadeia descendente para ideias da forma Re, $e^2 = e$, como todos os ideais de R são da forma Re, com $e^2 = e$, então R é artiniano.

Agora para mostrar que é semiprimo, considere $M \neq \{0\}$ um ideal de R. Como R é semissimples então existe um ideal N a esquerda de R tal que $R = M \oplus N$, agora suponha por contradição que $M^2 = \{0\}$, dessa forma temos que $MR = M(M \oplus N) \subseteq M^2 + MN = MN \subseteq N$, como M é um ideal de R, então $MR \subseteq M$, logo $MR \subseteq M \cap N = \{0\}$ e portanto teríamos que $MR = \{0\}$, mas nesse caso $M = \{0\}$, uma contradição. Assim $M^2 \neq \{0\}$. Portanto R é semiprimo. □

5 Teorema de Wedderburn-Artin

5.1 Teorema de Wedderburn

Nesta seção provaremos um teorema que nos será essencial na argumentação final do teorema de Wedderburn-Artin.

Lema 5.1 *(**Lema de Brauer**) Seja R um anel com K um ideal minimal à esquerda e assuma que $K^2 \neq \{0\}$. Então*
i. *$K = Re$, com $e^2 = e$.*
ii. *eRe é um anel de divisão onde a unidade é e.*

Demonstração: Vamos provar (i). Como $K^2 \neq \{0\}$, então existe $u \in K$ tal que $Ku \neq \{0\}$. Sendo Ku um ideal à esquerda de R não nulo tal que $Ku \subseteq K$ então, por minimalidade de K, tem-se que $Ku = K$, dessa forma existe $e \in K$ tal que $eu = u$.

Agora defina $L = \{a \in K : au = 0\}$, como $(re-r)u = (re)u - ru = r(eu) - ru = ru - ru = 0$ para todo $r \in K$, então $re - r \in L$ para todo $r \in K$.

Não é difícil ver que L é um ideal à esquerda de R com $L \subseteq K$, além disso $eu = u \neq 0$, assim $e \in K \setminus L$, logo $L \neq K$.

Dessa forma concluimos, pela minimalidade de K, que $L = \{0\}$. Como $re - r \in L$ para todo $r \in K$, então $re - r = 0$ para todo $r \in K$, em particular $e^2 = e$, além disso, $K = Ke \subseteq Re$. Por outro lado $Re \subseteq K$, pois $e \in K$, logo $K = Re$.

Agora vamos mostrar (ii). De fato, dados $a, b \in eRe$, então existem $r, r' \in R$ tais que $a = ere$, $b = er'e$, assim $a - b = ere - er'e = e(r - r')e \in eRe$ e temos também que $ab = ereer'e = erer'e \in eRe$, dessa forma eRe é subanel de R e portanto é anel. Além disso, como R tem unidade, digamos 1, então $e = e^2 = e1e \in eRe$, agora $ea = e^2re = ere^2 = ae = ere = a$, logo e é unidade de eRe.

Agora vamos mostrar que eRe é anel de divisão. De fato, seja $b \in eRe$ um elemento não nulo, logo existe $r' \in R$ tal que $b = er'e$, como $rb = rer'e \in ReRe \subseteq Re$ para todo $r \in R$, então $0 \neq Rb \subseteq Re$. Como Rb é ideal à esquerda de R, então por minimalidade de K, $Rb = Re$. Assim $e = r"b$ para algum $r" \in R$. Tomando $er"e \in eRe$ temos $(er"e)b = er"(eb) = er"b = ee = e$, ou seja, b tem inverso à esquerda em eRe. Por outro lado

$b(er"e)b = b(er"eb) = b(er"b) = be = eb$, logo $(b(er"e) - e)b = 0$, se $b(er"e) - e \neq 0$, então seja $c \in eRe$ seu inverso à esquerda, logo $c(b(er"e) - e) = e$, mas nesse caso temos que $b = 0$, que é absurdo, logo $b(er"e) = e$. Assim b tem inverso à direita em eRe. Portanto eRe é anel de divisão. □

Corolário 5.2 *Todo ideal à esquerda não nulo de um anel R semiprimo e artiniano, contém um elemento idempotente não nulo.*

Demonstração: Seja $L \neq \{0\}$ um ideal à esquerda de R. Como R é artiniano, então existe um ideal minimal à esquerda K de R tal que $K \subseteq L$. Sendo K um ideal à esquerda de R, então $RK \subseteq K$, o que implica $RKR \subseteq KR$. Dessa forma KR é ideal à esquerda de R. Por outro lado $R^2 \subseteq R$, logo $KR^2 \subseteq KR$, assim KR é um ideal à direita de R. Portanto KR é um ideal de R. Como R é semiprimo e $KR \neq \{0\}$, então $(KR)^2 \neq \{0\}$. De $RK \subseteq K$, tem-se que $KRKR \subseteq K^2R$, assim $\{0\} \neq (KR)^2 \subseteq K^2R$, mostrando que $K^2 \neq \{0\}$. Agora estamos na condição do Lema de Brauer, basta aplica-lo. □

Quando o anel é simples podemos enfraquecer a hipótese de anel artiniano supondo apenas a existência de um ideal minimal à esquerda, e nesse caso o teorema de Wedderburn-Artin se reduz a o teorema de Wedderburn que mostraremos a seguir.

Teorema 5.3 *(**Teorema de Wedderburn**) Se R é um anel simples com um ideal minimal à esquerda K, então $R \simeq M_n(D)$ como anéis, para algum $n \geq 1$ e algum anel de divisão D.*

Demonstração: Vimos na demonstração do corolário acima que KR é um ideal de R, como $K \neq \{0\}$ e R é anel com unidade então $KR \neq \{0\}$, assim $KR = R$, pois R é simples. $R = R^2 = (KR)^2 = KRKR \subseteq K^2R$, dessa forma $K^2 \neq \{0\}$, assim pelo Lema de Brauer, existe $e \in K$ tal que $K = Re$, $e^2 = e$ e $D = eRe$ é anel de divisão. O que será feito daqui para frente é construir um isomorfismo de R com $End_D K$.

Como K é um ideal à esquerda de R com $KeRe = ReeRe = Re^2Re = ReRe = K^2 \subseteq K$, então K pode ser visto como um D-módulo à direita com as operações de soma e produto induzida pelo anel R.

Agora, seja $r \in R$, a aplicação $\alpha_r : K \longrightarrow K$ dada por $\alpha_r(k) = rk$ com $k \in K$, é uma D-transformação linear, onde tal linearidade segue das propriedades associativas e distributivas do anel R.

Afirmação: A aplicação $\psi : R \longrightarrow End_D K$ definida por $\psi(r) = \alpha_r$ é um isomorfismo de anéis, e portanto $R \simeq End_D K$.

De fato,

i. A aplicação ψ é homomorfismo de anéis. De fato, dados $a, b \in R$ então, $\alpha_{a+b}(k) = (a+b)(k) = ak + bk = \alpha_a(k) + \alpha_b(k)$ para todo $k \in K$, e mais, $\alpha_{ab}(k) = (ab)k = a(bk) = \alpha_a(bk) = \alpha_a(\alpha_b(k)) = (\alpha_a \circ \alpha_b)(k)$ para todo $k \in K$.

ii. A aplicação ψ é injetora. Para ver isso vamos mostrar que $Ker(\psi) = \{0\}$. Seja $r \in R$ tal que $\alpha_r(k) = 0$ para todo $k \in K$, logo $\alpha_r(k) = ek = 0$ para todo $k \in K$, ou seja, $rK = \{0\}$, como $K = Re$, então $\{0\} = rRe = rReR = rR$ ($ReR = R$ pois, R é simples e tem $ReR \neq \{0\}$ como um ideal). Portanto, $1r = r = 0$.

iii. Aplicação ψ é sobrejetora. Como $1 \in ReR$ então, $1 = \sum_{i=1}^{n} r_i e s_i$ onde $r_i, s_i \in R$ para todo $i = 1, ..., n$. Dado $\alpha \in End_D K$, seja $a = \sum_{i=1}^{n} \alpha(r_i e) e s_i \in R$. Assim, usando a D-linearidade de α temos que

$$\alpha(re) = \alpha\left[\sum_{i=1}^{n}(r_i e s_i)re\right] = \sum_{i=1}^{n}\alpha(r_i e)(es_i re) = are = \alpha_a(re)$$

isso é verdade para todo r em R, logo $\alpha = \alpha_a$.

Portanto, temos que $R \simeq End_D K$.

Por fim, K tem dimensão finita sobre D, isto é, $dim_D K < \infty$. De fato, suponha por contradição que $dim_D K$ é infinito. Considere o conjunto

$$A = \{\alpha \in End_D K : dim_D \alpha(K) < \infty\}$$

tal conjunto é um ideal de $End_D K$, além disso A é ideal próprio pois, pela hipótese de absurdo, $\alpha_1 \notin A$. Pelo isomorfismo R em $End_D K$, isso implica que R possuí um ideal próprio não trivial, contrariando sua simplicidade.

Por fim, denotando por $End_D K$ o anel das D-transformações lineares de K em K, temos que se $n = dim_D K$, então $End_D K \simeq M_n(D)$ como anéis.

Portanto, concluímos que $R \simeq M_n(D)$ para algum n inteiro positivo.

□

Note que uma consequência do teorema acima é que todo anel simples e artiniano é semisimples, já que $M_n(D)$ é semisimples.

5.2 Teorema de Wedderburn-Artin

Nessa seção veremos um importante teorema que caracteriza os anéis semiprimos e artinianos, mais precisamente, vamos mostrar que todo anel semiprimo e artiniano tem a mesma estrutura algébrica (estrutura de anel) de algum produto finito de

anéis de matrizes sobre anéis de divisão.

A ideia por trás da demonstração do Teorema de Wedderburn-Artin que será apresentada, é decompor o anel R como soma direta de subanéis simples e "aplicar"teorema de Wedderburn em cada parcela dessa decomposição.

Teorema 5.4 *(**Teorema de Wedderburn-Artin**) Um anel R é semiprimo e artiniano se, e somente se*

$$R \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times \ldots \times M_{n_m}(D_m)$$

onde m é um número inteiro positivo, cada D_i é um anel de divisão e para cada n_i inteiro positivo, $M_{n_i}(D_i)$ denota o anel de matrizes $n_i \times n_i$ sobre D_i.

Demonstração: Já vimos que o fato de R ser artiniano implica na existência de um ideal minimal à esquerda K em R. Defina: $S = KR$ e $M = \{a \in R : Sa = \{0\}\}$. Já mostramos que S é um ideal de R, vamos mostrar que M também é. De fato, como $SR \subseteq S$ então, $SRM \subseteq SM = \{0\}$, logo $RM \subseteq M$. Por outro lado $SMR = \{0\}$, assim $MR \subseteq M$.

Afirmação: $R = S \oplus M$.

Primeiro vamos mostrar que $S \cap M = \{0\}$. De fato, $S \cap M \subseteq S$ e $S \cap M \subseteq M$, então $(S \cap M)^2 = (S \cap M)(S \cap M) \subseteq SM = \{0\}$, como R é semiprimo, então $S \cap M = \{0\}$.

Agora, considere a família

$$\mathcal{J} = \{Rf \subseteq R : f^2 = f,\ f \in S\}$$

note que $\mathcal{J}$ é subfamília da família de ideais à esquerda de R. Como R é artiniano então, pelo corolário 3.24, $\mathcal{J}$ admite um elemento maximal, isto é, existe $e \in S$ satisfazendo $e^2 = e$ tal que $Re \in \mathcal{J}$ com $Re \nsubseteq J$ para todo $J \neq Re$ em $\mathcal{J}$.

Para mostrar que $R = S + M$ é suficiente mostrar que $1 - e \in M$, pois caso isso seja verdade, então $\forall r \in R$ teremos que $r = re + r - re \in S + M$ com $re \in S$, $r - re \in M$.

Dessa forma, suponha por contradição que $1 - e \notin M$. Assim $S(1 - e) \neq \{0\}$. Pelo corolário do lema de Brauer existe $f \in S(1 - e)$ não nulo tal que $f^2 = f$. Então existe $r \in R$ tal que $f = r(1 - e) = r - re$, logo $fe = re - re^2 = re - re = 0$.

Agora defina $g = e + f - ef$, como $e, f \in S$ então $g \in S$, além disso

$$\begin{aligned} g^2 &= (e + f - ef)^2 = (e + f - ef)(e + f - ef) \\ &= e^2 + ef + ef + f^2 - e^2 f - fef - efe - ef^2 + efef \\ &= e + ef + f - ef - ef = e + f - ef = g \end{aligned}$$

note também que

$$eg = e(e + f - ef) = e^2 + ef - e^2 f = e^2 = e$$

ou seja, $e \in Rg$, logo $Re \subseteq Rg$. Como Re é maximal em $\mathcal{J}$, temos que $Re = Rg$. Assim existe $r \in R$ tal que $g = re$. Perceba que $ge = (e + f - ef)e = e^2 + fe - efe = e^2 = e$, portanto $eg = e = eg$. Assim $e = ge = g^2e = rege = re^2 = re = g$.

Sendo $e = g$, então $e = e + f - ef$, que implica em $f = ef$, portanto $f = f^2 = fef = 0$, uma contradição. Portanto $1 - e \in M$, provando que $R = S + M$.

S e M são subanéis de R com unidade e e $(1 - e)$ respectivamente.

O fato de $R = S \oplus M$ implica que todos os ideais à esquerda de S e M também são ideais à esquerda de R. Tal fato faz com que S e M herdem as propriedades de ser semiprimo e artiniano.

Agora vamos mostrar que S é simples. De fato, se $A \neq \{0\}$ é um ideal de S, então $A \cap K \neq \{0\}$ pois, caso contrário, $A^2 \subseteq AKR \subseteq (A \cap K)R = \{0\}$, mas $A^2 \neq \{0\}$, já que S é semiprimo. Sendo A um ideal de S, então em particular é um ideal à esquerda de R, logo $A \cap R$ é um ideal não nulo à esquerda de R contido em K, pela minimalidade de K temos que $K \subseteq A$, donde concluímos que $S = KR \subseteq A$.

Se $M = \{0\}$ então $R = S$ é anel simples e basta aplicar o teorema de Wedderburn. Caso $M \neq \{0\}$, como M é semiprimo e artiniano, podemos repetir o processo acima para M obtendo $M = S_1 \oplus M_1$, e portanto $R = S \oplus S_1 \oplus M_1$. Tal processo não pode continuar indefinidamente pois R é anel artiniano. Assim, $R = S \oplus S_1 \oplus \ldots \oplus S_m$ para algum m inteiro positivo, onde cada S_i é um anel simples. Como $S_i \simeq M_{n_i}(D_i)$, para todo $i = 1, ..., m$, então

$$R \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times \ldots \times M_{n_m}(D_m).$$

Reciprocamente, já mostramos todo produto cartesiano finito de anéis de matrizes sobre anéis de divisão é artiniano e semiprimo. Portanto R é semiprimo e artiniano. □

Corolário 5.5 *Um anel R é semissimples se, e somente se é artiniano e semiprimo.*

Demonstração: Assuma que R é semissimples, a proposição 4.35 mostra que R é artiniano e semiprimo. Reciprocamente, se R é artiniano e semiprimo, então pelo Teorema de Wedderburn-Artin, R é isomorfo a um produto cartesiano de matrizes sobre anéis de divisão, que como sabemos, é semissimples, logo R é semissimples. □

6 Aplicações

6.1 Anéis de Grupo

Definição 6.1 *Seja R um anel com unidade e G um grupo. Definimos RG como o conjunto de todas as combinações lineares da forma*

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

onde $a_g \in R$ e o número de elementos tais que $a_g \neq 0$, é finito.

Como consequência dessa definição tem-se que $\sum_{g\in G} a_g g = \sum_{g\in G} b_g g$ se, e somente se $a_g = b_g$ para todo $g \in G$.

Agora vamos introduzir uma operação de soma e uma de multiplicação entre os elementos de RG de forma a torna-lo um anel.

Usando a soma do anel R podemos introduzir de forma natural, uma operação de soma em RG da seguinte maneira:

Dados $\alpha = \sum_{g\in G} a_g g$, $\beta = \sum_{g\in G} b_g g \in RG$ defina

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

Agora, usando a definição de multiplicação de R, podemos definir uma multiplicação em RG como sendo

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

.

RG com as operações definidas acima fazem de RG um anel, chamado de anel de grupo de G sobre R. Note que o anel RG tem unidade dada por $1e$, onde 1 é a unidade de R e e é a unidade G.

Também podemos dar uma estrutura de R-módulo para RG. De fato, dado $\alpha = \sum_{g\in G} a_g g \in RG$ e $r \in R$, definia $r\alpha = \sum_{g\in G} r a_g g$. Para a soma entre elementos quais-

quer de RG, mantenha a definida acima. Sem muitas dificuldades é possível mostrar que RG com esse produto e soma consiste em um R-módulo.

Definição 6.2 *Seja $\alpha = \sum_{g\in G} a_g g \in RG$, então definimos $supp(\alpha) = \{g \in G : a_g \neq 0\}$.*

Definição 6.3 *Seja H um subgrupo de G, o denotamos por $\Delta_R(G,H)$ o ideal a esquerda de R gerado pelo conjunto $\{h-e : h \in H\}$, onde e é a unidade de G, ou seja*

$$\Delta_R(G,H) = \left\{ \sum_{h\in H} \alpha_h (h-e) : h \in H \right\}.$$

Afim de simplificar a notação vamos escrever $\Delta_R(G,H)$ simplesmente como $\Delta(G,H)$. Também vamos adotar a notação $\Delta(G)$ para representar $\Delta(G,G)$.

Definição 6.4 *Dado um anel de grupo RG e um subconjunto finito não vazio X de G, vamos denotar por $\widehat{X}$ o seguinte elemento de RG*

$$\widehat{X} = \sum_{x\in X} x$$

Lema 6.5 *Seja H um subgrupo de um grupo G e R um anel. Se $An_D(\Delta(G,H)) \neq \{0\}$, então H é finito. E nesse caso temos que*

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

Demonstração: Assuma que $An_D(\Delta(G,H)) \neq 0$, assim, existe $\alpha = \sum_{g\in G} a_g g \neq \{0\}$ pertencente a $An_D(\Delta(G,H))$. Como $(h-e) = 1\cdot(h-e)$, então $(h-e) \in \Delta(G,H)$, para todo $h \in H$, então $(h-e)\alpha = 0$, assim

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

Agora seja $g' \in supp(\alpha)$, logo $\alpha'_g \neq 0$, dessa forma, a igualdade acima nos diz que $hg' \in supp(\alpha)$, seja qual for o h tomado em H.

Note que dados $h_1, h_2 \in H$, distintos, então $h_1 g' \neq h_2 g'$, pois sendo $g' \neq 0$ e G grupo, então vale o cancelamento. Dessa forma, supondo que H seja infinito, teríamos que $supp(\alpha)$ também seria, mas isso não ocorre. Portanto H é finito.

Para a ultima parte, note que pelo que acabamos de mostrar faz sentido definir $\widehat{H}$, além disso, $\widehat{H} \in H$, pois H é subgrupo de G. Agora dado $\alpha \in Anl_D(\Delta(G,H))$, seja

$supp(\alpha) = \{g_1, g_2, \ldots, g_n\}$. Assim

$$\alpha = \sum_{i=1}^{n} a_{g_i} \widehat{H} g_i = \sum_{i=1}^{n} a_{g_i} (\sum_{j=1}^{m} h_j) g_i = \sum_{i=1}^{n} a_{g_i} (\sum_{j=1}^{m} h_j g_i) = \sum_{i=1}^{n} \sum_{j=1}^{m} (1 \cdot a_{g_i})(h_j g_i) = \widehat{H}\alpha$$

onde m é a cardinalidade do conjunto H. Observe que a relação acima vale para qualquer $\alpha \in An_D(\Delta(G,H))$, assim $An_D(\Delta(G,H)) \subseteq \widehat{H} \cdot RG$.

Por outro lado, veja que $h\widehat{H} = \widehat{H}$, pois H é grupo finito, assim dado $\widehat{H}\alpha \in \widehat{H} \cdot RG$, temos que $(h-e)(\widehat{H}\alpha) = ((h-e)\widehat{H})\alpha = 0$, assim $\widehat{H}\alpha \in An_D(\Delta(G,H))$. □

Lema 6.6 *Seja I um ideal de R e suponha que exista um ideal a esquerda J de R tal que $R = I \oplus J$, então $J \subseteq An_D(I)$.*

Demonstração: Sejam $x \in J$ e $y \in I$ elementos quaisquer, como J é ideal a esquerda e I é ideal, então $yx \in J \cap I$, como por hipótese temos que $J \cap I = \{0\}$ então $yx = 0$, logo $x \in An_D(I)$. □

Definição 6.7 *O homomorfismo $\varepsilon : RG \longrightarrow R$ dado por*

$$\varepsilon\Big(\sum_{g\in G} \alpha_g g\Big) = \sum_{g\in G} \alpha_g$$

é chamado de homomorfismo de aumento.

Note que $Ker(\varepsilon) = \Delta(G)$, pois dado $\alpha \in \Delta(G)$, então

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

assim $\varepsilon(\alpha) = 0$, logo $\alpha \in Ker(\varepsilon)$.

Por outro lado, se $\varepsilon(\alpha) = 0$, então $\sum_{g\in G} a_g = 0$, logo

$$\alpha = \alpha - 0 = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-e) \in \Delta(G).$$

Observe que como $\Delta(G)$ é o núcleo de um R-homomorfismo, então $\Delta(G)$ é um ideal de RG.

Proposição 6.8 *Seja R um anel, G um grupo, então $R \simeq RG/\Delta(G)$, como anéis.*

Demonstração: Considere o homomorfismo ε, como vimos acima $Ker(\varepsilon) = \Delta(G)$, e também temos que ε é sobrejetivo (de fato, dado $r \in R$, note que $re \in RG$ e $\varepsilon(re) = r$).

Assim, pelo teorema do homomorfismo para anéis, temos que $R \simeq RG/\Delta(G)$ como anéis. □

Definição 6.9 *Seja R um anel e G um grupo finito, definimos* $|G| = \sum_{g \in G} 1$.

Lema 6.10 *Seja G um grupo e R um anel. Se o ideal de aumento* $\Delta(G)$ *é um somando direto de RG, então G é finito e* $|G|$ *é inversível em R.*

Demonstração: Suponha que $\Delta(G)$ é um somando direto de RG. Pelo lema 6.6, temos que $An_D(\Delta(G)) \neq \{0\}$, logo G é finito e $An_D(\Delta(G)) = \widehat{G} \cdot RG = \widehat{G} \cdot R$.

Seja J ideal à esquerda de RG tal que $RG = \Delta(G) \oplus J$. Logo $1 = x_1 + x_2$, onde $x_1 \in \Delta(G)$ e $x_2 \in J$. Assim $1 = \varepsilon(1) = \varepsilon(x_1) + \varepsilon(x_2)$. Como $ker(\varepsilon) = \Delta(G)$, então $\varepsilon(x_1) = 0$. Como pelo lema acima $J \subseteq An_D(\Delta(G))$, logo $x_2 = \widehat{G}a$, para algum $a \in R$, nós temos que $\varepsilon(\widehat{G})a = 1$, assim $|G|a = 1$, portanto $|G|$ é inversível em R. □

Lema 6.11 *Seja M um R-módulo e N um R-submódulo de M. Suponha que exista um endomorfismo* $T : M \longrightarrow M$ *tal que* $T^2 = T \circ T = T$ *e* $Im(T) = N$*, então N é um somando direto de M.*

Demonstração: Afirmamos que $M = N \oplus Ker(T)$. De fato, dado $m \in M$, então $T(m) \in N$ e $T(m - T(m)) = T(m) - T^2(m) = T(m) - T(m) = 0$, isto é, $m - T(m) \in Ker(T)$. Dessa forma $m = T(m) + (m - T(m))$, logo $M \subseteq N + Ker(T)$. Por outro lado é claro que $N + Ker(T) \subseteq M$. Assim segue que $M = N + Ker(T)$.

Agora vamos mostrar que $N \cap Ker(T) = \{0\}$. Seja $d \in N \cap Ker(T) \subseteq N$, logo existe $m \in M$ tal que $T(m) = d$ e portanto $T(T(m)) = T(d)$. Por outro lado $d \in Ker(T)$, então $T(d) = 0$, assim $T(T(m)) = 0$, mas como $T(T(m)) = T(m)$, então $d = 0$. Portanto $N \cap Ker(T) = \{0\}$. □

6.2 Teorema de Maschke

Teorema 6.12 ***(Teorema de Maschke)*** *Seja G um grupo e R um anel. O anel de grupo RG é semissimples se, e somente se todas as condições abaixo são satisfeitas*

i. *R é um anel semissimples.*

ii. *G é um grupo finito.*

iii. $|G|$ *é inversível no anel R.*

Demonstração: Assuma que RG é semissimples. Já vimos que $R \simeq RG/\Delta(G)$ como anéis, além disso, pela proposição 4.33, $RG/\Delta(G)$ é anel semissimples, logo **i.** segue.

Agora para mostrar **ii.** e **ii.**, basta observar que o fato de RG ser semissimples implica $\Delta(G)$ é somando direto de RG, assim, aplicando o lema 6.10, segue o resultado desejado.

Reciprocamente, assuma que **i.**, **ii.** e **iii.** ocorrem. Como R é semissimples, então RG visto como um R-módulo é semissimples. Agora seja M, um ideal à esquerda de RG, logo também é R-submódulo de RG, como RG é R-módulo semissimples, então existe N um R-submódulo, tal que $RG = M \oplus N$, dessa forma, dado $x \in RG$, existe $m \in M$ e $n \in N$ únicos tais que $x = m + n$, com isso defina a projeção canônica $\pi : RG \longrightarrow M$, dada por $\pi(x) = m$.

Agora defina $\pi^* : RG \longrightarrow M$ dada por

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

Agora vamos mostrar que π^* é um RG-homomorfismo com $(\pi^*)^2 = \pi^* \circ \pi^* = \pi^*$ e $Im(\pi^*) = M$, pois caso isso seja verdade então teremos que $RG = M \oplus Ker(\pi^*)$, com $Ker(\pi^*)$ é ideal à esquerda de RG, donde então segue o teorema.

De fato, como π é um R-homomorfismo, então π^* também é, dessa forma basta, para concluir que π^* é RG-homomorfismo, basta mostrarmos que $\pi^*(ax) = a\pi^*(x)$ para todo $x \in G$ e $a \in G$.

Basta ver que

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

Como g percorre todos os elementos do grupo G e, além disso, G é finito, então ga também percorre todos os elementos de G, logo

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

Agora, note $\pi(m) = m$ para todo $m \in M$, além disso, sendo M um ideal à esquerda de RG, então $gm \in M$ para todo $g \in G$, assim $\pi(gm) = gm$ para todo $g \in G$ e todo $m \in M$. Logo

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

Agora, dado um elemento qualquer $x \in RG$, então $\pi(gx) \in M$ para todo $g \in G$, logo

$\pi^*(x) \in M$, assim $Im(\pi^*) \subseteq M$, donde segue também que $(\pi^*(x))^2 = \pi^*(x)$ seja qual for x tomado em RG.

Por fim, dado $m \in M$, veja que $\pi^*(m) = m \in Im(\pi^*)$, logo $M \subseteq Im(\pi^*)$. □

Antes de apresentar um dos corolários do teorema de machske, precisamos de duas definições:

Definição 6.13 *Seja R um anel. Se R é anel de divisão e além disso também é comutativo, então dizemos que R é um corpo.*

Definição 6.14 *Seja R um corpo. O menor número inteiro positivo n, caso exista, tal que* 1 *somado n-vezes é igual a zero, é chamado de característica de R e denotada por* $char(R)$*, se tal número n não existe, então definimos* $char(R) = 0$.

Corolário 6.15 *Seja G um grupo finito e K um corpo, então o anel de grupo KG é semissimples se, e somente se* $char(K) \nmid |G|$.

Demonstração: Basta notar que $|G|$ é inversível em K se, e somente se $|G| \neq 0$, ou seja, se, e somente se $char(K)$ não divide a ordem do G, isto é, $char(K) \nmid |G|$. □

Usando o Teorema de Maschke juntamente com Teorema de Wedderburn-Artin, somos capazes de caracterizar completamente os anéis de grupo KG, onde G é um grupo finito e K um corpo tal que $char(K) \nmid |G|$. De fato, pelo corolário acima KG é semissimples, logo pelo teorema de Wedderburn-Artin

$$KG \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times \ldots \times M_{n_m}(D_m)$$

onde m é um número inteiro positivo, cada D_i é um anel de divisão e para cada n_i inteiro positivo, $M_{n_i}(D_i)$ denota o anel de matrizes $n_i \times n_i$ sobre D_i.

7 Apêndice

7.1 Anéis Quociente

Seja R uma anel e I um ideal bilateral de R. Para cada $r \in R$ defina $\overline{r} = \{r + a : a \in T\}$ e considere o conjunto $A/I = \cup_{r \in R}\{\overline{r}\}$. Defina as seguintes operações em A/I:
i. Adição: $\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$, quaisquer que sejam $r_1, r_2 \in R$.
ii. Multiplicação: $\overline{r_1} \cdot \overline{r_2} = \overline{r_1 r_2}$, quaisquer que sejam $r_1, r_2 \in R$.
É possível mostrar que as operações **i.** e **ii.** estão bem definidas e que A/I munido com essas operações forma uma anel. Veja referência [3].

Observação 7.1 *Também é comum usar a notação $\overline{r} = r+I$.*

Proposição 7.2 *Nas condições da definição acima, dados $r_1, r_2 \in R$, então $r_1 - r_2 \in I$ se, e somente se $\overline{r_1} = \overline{r_2}$.*

Demonstração: De fato, assuma que $r_1 - r_2 \in I$, logo existe $r' \in I$ tal que $r_1 - r_2 = r'$, assim $r_1 = r_2 + r'$, dessa forma $r_1 + x = r_2 + (r' + x) \in \overline{r_2}$, $\forall x \in I$, logo $\overline{r_1} \subseteq \overline{r_2}$. Por outro lado, $r_2 = r_1 - r'$, logo $r_2 + x = r_1 + (x - r') \in \overline{r_1}$, $\forall x \in I$, logo $\overline{r_2} \subseteq \overline{r_1}$. Portanto $\overline{r_1} = \overline{r_2}$.
Reciprocamente, se $\overline{r_1} = \overline{r_2}$, como $r_1 \in \overline{r_1}$, pois $r_1 = r_1 + 0$, então existe $x \in I$ tal que $r_1 = r_2 + x$, pois $\overline{r_1} \subseteq \overline{r_2}$, logo $r_1 - r_2 = x \in I$. □

7.2 Módulos Quociente

Seja R anel e M um R-módulo. Seja N um R-submódulo de M. Para cada $m \in M$, defina $\overline{m} = \{m + n : n \in N\}$ e considere $M/N = \cup_{m \in M}\{\overline{m}\}$. Defina as seguintes operações em M/N:
i. Adição: $\overline{m_1} + \overline{m_2} = \overline{m_1 + m_2}$, quaisquer que sejam $m_1, m_2 \in M$.
ii. Multiplicação: $r \cdot \overline{m} = \overline{rm}$, quaisquer que sejam $r \in R$ e $m \in M$.
É possível mostrar que as operações **i.** e **ii.** estão bem definidas e que M/N munido com essas operações forma uma R-módulo. Veja referência [3].

Observação 7.3 *Também é comum usar notação $\overline{m} = m + N$.*

Proposição 7.4 *Nas condições da definição acima, dados $m_1, m_2 \in M$, então $m_1 - m_2 \in N$ se, e somente se $\overline{m_1} = \overline{m_2}$.*

Demonstração: De fato, assuma que $m_1 - m_2 \in N$, logo existe $n' \in N$ tal que $m_1 - m_2 = n'$, assim $m_1 = m_2 + n'$, dessa forma $m_1 + x = m_2 + (n' + x) \in \overline{m_2}$, $\forall x \in N$, logo $\overline{m_1} \subseteq \overline{m_2}$. Por outro lado, $m_2 = m_1 - n'$, logo $m_2 + x = m_1 + (x - n') \in \overline{m_1}$, $\forall x \in N$, logo $\overline{m_2} \subseteq \overline{m_1}$. Portanto $\overline{m_1} = \overline{m_2}$.

Reciprocamente, se $\overline{m_1} = \overline{m_2}$, como $m_1 \in \overline{m_1}$, pois $m_1 = m_1 + 0$, então existe $x \in N$ tal que $m_1 = m_2 + x$, pois $\overline{m_1} \subseteq \overline{m_2}$, logo $m_1 - m_2 = x \in N$. □

Referências Bibliográficas

[1] Hungerford, T.W. *Algebra*. Springer, 1980, Graduate Texts in Mathematics, volume 73;

[2] Marubayashi H.; Miyamoto H.; Ueda A. *Non-Commutative Valuation Rings and Semi-Hereditary Orders*. Springer, 1997, volume 3;

[3] Milies, P.C.; Sehgal, K.S. *An Introduction to Group Rings*. Springer, 2002, volume 1;

[4] Nicholson, W.K. *A Short Proof of the Wedderburn-Artin Theorem*. New Zealand Journal of Mathematics, 1993, pag. 83-86, volume 22;

[5] Rotman, J.J. *An Introduction Homological to Algebra*. Academic Press, 1979, volume 3.