Uma introdução ao estudo dos anéis semissimples

ALVERI A. SANT'ANA[1]

13 de março de 2016

[1] alveri@mat.ufrgs.br

À Marília, pelo carinho, apoio e cumplicidade.

Ao Filipe, por estar sempre tentando me mostrar a (semi) simplicidade da vida.

Sumário

Prefácio

Estas notas foram escritas para servir de apoio a um minicurso de mesmo título, oferecido no IV Colóquio de Matemática da Região Sul, realizado de 02 a 06 de maio de 2016, na Universidade Federal de Rio Grande, em Rio Grande, RS. Como anunciado na divulgação do mesmo, o estudo dos anéis semissimples tem se mostrado bastante adequado para introduzirmos os estudantes no mundo dos anéis não comutativos. O objetivo deste texto, conforme sua concepção inicial, era o de apresentar uma demonstração do Teorema de Wedderburn-Artin. Durante o processo de escrita das notas, se pensou em escrever um texto um pouco mais completo, acrescentando uma aplicação interessante da semissimplicidade na classificação das representações irredutíveis de grupos finitos (Capítulo 4) e a J-semissimplicidade (capítulo 5), que é uma generalização natural do conteúdo estudado nos três primeiros capítulos. Esta ideia se justifica, pois acreditamos que desta forma estas notas serviriam também para nortear um estudo ao nível de iniciação científica, ou mesmo como um texto para ser aprofundado em uma disciplina eletiva de graduação nos cursos de matemática, posto que não existem muitos textos escritos em português, tratando do estudo de anéis não comutativos, pelo menos do conhecimento do autor. Assim, o presente texto se propõe a ser mais uma alternativa nesta direção.

Para muitos autores, a álgebra moderna, como a conhecemos hoje, tem seu nascimento quando Wedderburn apresentou seu trabalho de classificação das álgebras semissimples sobre um corpo qualquer. Antes dele, muitos autores trabalhavam na classificação destas álgebras, mas sobre determinados corpos específicos. Por exemplo, T. Molien e E. Cartan, antes de Wedderburn, descreveram a completamente as álgebras semissimples finito-dimensionais sobre os corpos dos complexos e dos reais e deram os primeiros passos na direção de estudar as álgebras não semissimples sobre estes mesmos corpos.

A ideia de semissimplicidade está associada a um certo radical, e já aparece nos trabalhos de Cartan, quando este classifica as álgebras de Lie finito-dimensionais sobre os complexos. Cartan chamou de radical de uma tal álgebra, o maior ideal solúvel e este é igual a soma dos ideais solúveis desta álgebra. Assim, uma álgebra de Lie é semissimples, se seu radical é nulo, ou ainda, se não existem ideais solúveis não nulos. Wedderburn trabalhou com um “radical" definido como sendo o maior ideal nilpotente, o qual coincide com a soma dos ideais nilpotentes de uma álgebra finito-dimensional, embora este ideal de Wedderburn não seja de fato um

radical como se conhece hoje. Por exemplo, este “radical de Wedderburn"não está definido para uma grande classe de anéis. Atualmente se estuda a semissimplicidade associada a diversos radicais, ou seja, se β é um dado radical de um anel, então podemos estudar aqueles anéis que são β-semissimples, isto é, aqueles anéis para os quais o radical β é nulo. No caso da semissimplicidade estudada por Wedderburn, o radical apropriado é o chamado radical de Jacobson, introduzido por N. Jacobson nos anos 40, dando origem aos anéis J-semissimples, na linguagem de hoje.

Em 1907 J. H. M. Wedderburn apresentou seu resultado fundamental no estudo das álgebras sobre corpos quaisquer, o qual dá uma classificação das álgebras finito-dimensionais, mostrando que estas são um produto direto de álgebras de matrizes sobre anéis de divisão. Desta forma, o estudo destas álgebras fica restrito ao estudo dos anéis de matrizes sobre anéis de divisão, e estes são relativamente mais elementares e mais fáceis de serem entendidos. Daí a importância do resultado de Wedderburn.

Em torno dos anos 20, E. Noether e E. Artin introduziram as condições de cadeia ascendente e descendente, respectivamente. Um módulo que satisfaz ambas as condições de cadeia é um módulo que possui comprimento finito. O comprimento de um módulo é, de certa forma, o análogo a dimensão de um espaço vetorial. Usando estas ideias, em 1927 Artin estendeu o teorema de Wedderburn para anéis satisfazendo ambas as condições de cadeia. Este resultado é conhecido hoje como o Teorema de Wedderburn-Artin, e é o tema central do capítulo três destas notas, onde apresentamos uma demonstração usando uma linguagem mais moderna que aquela usada nos trabalhos originais, independente do conceito de radical, razão pela qual não vamos apresentar uma definição formal de radical de um anel. Curiosamente, Artin parece não ter percebido que para anéis com unidade, a condição de cadeia descendente implica a condição de cadeia ascendente, fato este que só foi tornado público por C. Hopkins e J. Levitzki, em 1939, em trabalhos independentes. Vale lembrar que esta mesma implicação não vale para módulos em geral.

Mais tarde, N. Jacobson introduziu a noção de radical de um anel, hoje conhecido como o radical de Jacobson, o que permitiu estender a teoria de Wedderburn para anéis quaisquer. Por exemplo, Jacobson mostrou que um anel é semissimples se, e somente se, este anel satisfaz a condição de cadeia descendente e seu radical é nulo. Denotando por $J(R)$ o radical de Jacobson de um anel R, o resultado de Jacobson nos permite estudar anéis que não são semissimples, estudando o anel fator $R/J(R)$ e depois “levantando" sua estrutura para o anel R. Aliás, grosso modo, esta é a ideia de um radical β de um anel R. Ele captura todos os elementos indesejáveis para o estudo de uma certa propriedade e o anel fator R/β possui este radical nulo, isto é, $\beta(R/\beta) = 0$. Com isto, o anel fator R/β não contém nenhum destes elementos indesejáveis. Depois, levantamos (se possível) esta propriedade ao anel R inicial.

Este histórico simplificado dá uma ideia da evolução do estudo dos anéis, via semissimplicidade, e serviu de fio condutor para a escrita destas notas. Para esta tarefa, vários livros clássicos da literatura foram consultados, e em certas partes, é

inegável suas respectivas influências.

No capítulo 1, decidimos incluir uma série de resultados básicos da teoria de anéis e módulos, principalmente para auxiliar aqueles leitores menos familiarizados com estes tópicos. O capítulo 2 foi dedicado ao estudo das condições de cadeia para anéis e módulos. Nele se procura mostrar que o comprimento de um módulo é um análogo da dimensão de um espaço vetorial e, portanto, se trona um substituto natural para a finito-dimensionalidade. No capitulo 3 apresentamos uma demonstração completa do Teorema de Wedderburn-Artin, primeiro objetivo destas notas. Feito isto, decidimos apresentar uma aplicação interessante da semissimplicidade, e fazemos isto no capítulo 4, onde discutimos, sem muita profundidade, as representações lineares de um grupo finito. Finalmente, no capítulo 5, definimos o radical de Jacobson e discutimos aspectos básicos da J-semissimplicidade de um anel, culminando no Teorema de Hopkins-Levitzki.

Alveri A. Sant'Ana

Março de 2016

Agradecimentos

Agradeço às comissões científica e organizadora do IV Colóquio de Matemática da Região Sul, da Sociedade Brasileira de Matemática, por permitirem a realização do minicurso "Uma introdução ao estudo dos anéis semissimples", dando a mim a oportunidade de discutir com a platéia, os temas abordados neste texto. É sempre bom lembrar que as grades curricilares dos cursos de graduação em matemática tem reservado pequenos espaços para o tratamento de anéis não comutativos e, portanto, oportunidades como esta ganham importância, na medida que se tornam espaços adequados para mostrarmos aos ouvintes um pouco do sabor da álgebra não comutativa.

Agradeço também à minha esposa Marília e ao meu aluno John Freddy Lozada, por encontrarem vários erros de digitação (e alguns mais graves) cometidos no processo de escrita destas notas. Porém, outros tantos podem ainda existirem, inclusive porque ocorreram alterações de última hora em alguns trechos do texto. Assim, agradeço antecipadamente aos leitores que me apontarem qualquer tipo de erro, omissão ou imprecisão.

Capítulo 1

Pré-requisitos

Desde o começo, a ideia sempre foi a de apresentar um texto o mais auto suficiente possível, decidimos incluir um capítulo prévio contendo os principais tópicos que serão necessários para o bom aproveitamento do mesmo. Este capítulo pode ser dispensável para aqueles leitores com uma certa familiaridade com os conceitos básicos da teoria de anéis e módulos, mas, porém, ele será usado para fixarmos algumas notações.

1.1 Anéis

Definição 1.1.1. Dizemos que um conjunto R, munido de duas operações binárias, chamadas soma (+) e multiplicação ($\cdot$), é um anel, se valem as seguintes propriedades:

(i) $(R, +)$ é um grupo abeliano, isto é, $+$ é associativa, possui elemento neutro, possui elemento simétrico e é comutativa,

(ii) $\cdot$ é associativa,

(iii) $+$ e $\cdot$ são compatíveis, isto é, para todos $a, b, c \in R$ vale que

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{e} \quad (a + b) \cdot c = a \cdot c + b \cdot c,$$

Lembramos que uma operação $\star$ definida em um conjunto A nada mais é do que uma função $\star : A \times A \to A$. Além disso, dizemos que:

- $\star$ é *associativa*, se $a \star (b \star c) = (a \star b) \star c$, $\forall a, b, c \in A$;
- $\star$ *possui elemento neutro*, se existir um elemento $e \in A$ tal que $e \star a = a = a \star e$, $\forall a \in A$;
- $\star$ *possui elemento simétrico*, se $\forall a \in A$, $\exists a' \in A$ tal que $a \star a' = e = a' \star a$, onde e é um elemento neutro de $\star$.

- $\star$ é *comutativa*, se $a \star b = b \star a$, $\forall a, b \in A$.

É possível mostrar que elementos neutros e simétricos, quando existem, são unicamente determinados (faremos isto mais adiante para anéis). Assim, estes elementos podem ser denotados por algum símbolo especial. No caso de anéis, denotaremos o elemento neutro da soma sempre por 0, e o chamaremos de *elemento zero* do anel. Também, denotaremos por $-a$ o simétrico aditivo do elemento a.

Notaremos um anel por $(R, +, \cdot)$, mas quando não houver possibilidade de confusão, escreveremos apenas R em lugar de $(R, +, \cdot)$, sem especificar as operações consideradas. Também, vamos escrever ab em lugar de $a \cdot b$, quando estivermos nos referindo ao elemento dado pela multiplicação de a por b.

Exemplo 1.1.2. Os conjuntos $\mathbb{Z}$ (dos números inteiros), $\mathbb{Q}$ (dos números racionais), $\mathbb{R}$ (dos números reais) e $\mathbb{C}$ (dos números complexos), com as operações usuais de soma e multiplicação, são exemplos de anéis.

Exemplo 1.1.3. Se R é um anel, então o conjunto $\mathcal{M}_n(R)$, das matrizes $n \times n$ com entradas em R, com as operações usuais de soma e multiplicação de matrizes, é um anel.

A partir destes exemplos podemos construir novos, através das seguintes técnicas: Se $R_1, R_2, ..., R_n$ são anéis, então o produto cartesiano $\mathcal{R} = R_1 \times R_2 \times \cdots \times R_n$ é um anel, onde as operações são definidas componente a componente. Se $(R, +, \cdot)$ é um anel, então pode-se mostrar que $R^{op} = (R, +, \bullet)$ também é um anel, onde $\bullet$ é definida por: $a \bullet b = b \cdot a, \forall a, b \in R$. R^{op} é chamado de *anel oposto de* R.

Seja $(R, +, \cdot)$ um anel. Se a multiplicação possui elemento neutro, denotado por 1_R (ou simplesmente por 1), então dizemos que R é um *anel com unidade*. Nossos exemplos acima são todos exemplos de anéis com unidade. Se considerarmos $R = n\mathbb{Z} := \{na : a \in \mathbb{Z}\}$, o conjunto de todos os múltiplos inteiros de um certo n fixo, com as operações usuais de soma e multiplicação dos inteiros, então temos um exemplo de um anel sem unidade.

O exemplo acima foi obtido fazendo a restrição das operações do anel $\mathbb{Z}$ ao subconjunto $n\mathbb{Z}$. Isto sugere uma nova definição.

Definição 1.1.4. Sejam $(R, +, \cdot)$ um anel e $\emptyset \neq S \subseteq R$. Então dizemos que S é um subanel de R, se as restrições das operações de R em S estão bem definidas e $(S, +_{|S}, \cdot_{|S})$ é um anel.

Se consideramos as imersões canônicas $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, então podemos ver $\mathbb{Q}$ como um subanel de $\mathbb{R}$ e de $\mathbb{C}$, assim como $\mathbb{R}$ se torna um subanel de $\mathbb{C}$. Se S é um subanel de R, então é fácil verificar que $\mathcal{M}_n(S)$ é um subanel de $\mathcal{M}_n(R)$

Os próximos exercícios nos fornecem propriedades básicas das operações de um anel, que serão usadas livremente no texto.

Exercício 1.1.5. Seja $(A, \star)$ um cojunto A munido de uma operação $\star$. Mostre que se $\star$ é associativa, possui neutro e possui simétrico, então as equações de primeiro grau

$$a \star X = b\,, \text{ e } \; X \star a = b$$

possuem solução única, para quaisquer escolhas de a e b em A.

Exercício 1.1.6. Seja $(R, +, \cdot)$ um anel. Deduza do exercício acima que o elemento neutro da soma é unicamente determinado. Além disso, se R é um anel com unidade, então a unidade de R é unicamente determinada também.

Exercício 1.1.7. Sejam R um anel e $a, b, c \in R$. Mostre que:

(i) $0 \cdot a = a \cdot 0 = 0$,

(ii) $-(ab) = (-a)b = a(-b)$,

(iii) $(-a)(-b) = ab$.

- Se R é um anel com unidade, então mostre que:

(iv) $(-1)a = a(-1) = -a$,

(v) $(-1)(-1) = 1$,

(vi) $(-1)(-a) = a$.

Também é um exercício de fácil verificação o seguinte resultado, o qual nos dá uma caracterizaçao dos subconjuntos de um anel que são seus subanéis.

Proposição 1.1.8. *Sejam R um anel e S um subconjunto de R. Então S é um subanel de R se, e somente se, as seguintes condições se verificam:*

(i) $0 \in S$;

(ii) $x, y \in S \Rightarrow x - y \in S$;

(iii) $x, y \in S \Rightarrow xy \in S$.

Observamos que se R tem unidade, então a condição (ii) da Proposição acima pode ser substituida por $(ii)' x, y \in S \Rightarrow x + y \in S$. Além disso, se R é um anel com unidade e S é um subanel de R, então S não possui necessariamente a mesma unidade de R. Aliás, a este respeito, tudo pode acontecer, como os exemplos abaixo mostram:

Observação 1.1.9. Sejam R um anel e S um subanel de R. Os seguintes casos podem ocorrer:

- R tem unidade e S não tem: $R = \mathbb{Z}$ e $S = 2\mathbb{Z}$.

- R tem unidade 1_R e S possui uma unidade 1_S, mas $1_R \neq 1_S$: $R = \mathcal{M}_2(\mathbb{Z})$ e $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{Z} \right\}$.
- R não tem unidade e S tem:

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Z} \right\} \text{ e } S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{Z} \right\}$$

  .
- R e S não possuem unidade: $R = 2\mathbb{Z}$ e $S = 4\mathbb{Z}$.
- R e S possuem a mesma unidade: $R = \mathbb{Q}$ e $S = \mathbb{Z}$.

O próximo exercício apresenta um subanel importante, chamado centro do anel, e será usado no capítulo 4.

Exercício 1.1.10. Seja R um anel. Mostre que o subconjuto $\mathcal{Z}(R) := \{a \in R : ax = xa, \forall x \in R\}$ é um subanel de R, chamado *centro de* R. Se n é um inteiro positivo, então mostre que o centro do anel de matrizes $n \times n$ sobre um corpo $\Bbbk$ é o conjunto das matrizes escalares (matrizes da forma aI_n, onde $a \in \Bbbk$ e I_n denota a matriz identidade de ordem n), isto é, mostre que

$$\mathcal{Z}(\mathcal{M}_n(\Bbbk)) = \{aI_n : a \in \Bbbk\}$$

Portanto, $dim_{\Bbbk}\mathcal{Z}(\mathcal{M}_n(\Bbbk)) = 1$ e, consequentemente, $\Bbbk \simeq \mathcal{Z}(\mathcal{M}_n(\Bbbk))$.

Dado um anel R, dizemos que R é um *anel comutativo* se a multiplicação de R é uma operação comutativa, isto é, se $xy = yx$, para todos elementos $x, y \in R$. Os anéis $\mathbb{Z}, n\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos de anéis comutativos. Os anéis de matrizes em geral são não comutativos. É fácil verificar que R é um anel comutativo se, e somente se, $R = R^{op}$.

Um elemento a em um anel R é chamado de *divisor de zero* se existir $0 \neq b \in R$ tal que $ab = 0 = ba$. Já um elemento u em um anel com unidade R é dito um *elemento invertível* se existir $v \in R$ tal que $uv = 1 = vu$.

Um anel comutativo com unidade e sem divisores de zero, além do próprio elemento 0, é dito um *domínio de integridade* (ou simplesmente um domínio). Um anel com unidade em que todo elemento não nulo é invertível é chamado de um *anel de divisão*. Por fim, um anel de divisão comutativo é chamado um *corpo*.

É fácil ver que $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos de corpos, que $\mathbb{Z}$ é um domínio (que não é um corpo). Também é fácil obter exemplos de divisores de zero em anéis de matrizes.

Vamos agora apresentar um exemplo de um anel de divisão que não é um corpo. Lembramos que o *anel dos quatérnios* $\mathbb{H}$ sobre os reais está definido como sendo o espaço vetorial 4-dimensional sobre $\mathbb{R}$ gerado pelos elementos $1, i, j, k \in \mathbb{H}$, com a multiplicação dada pelas seguintes relações: $i^2 = j^2 = k^2 = 1, ij = k, jk = i, ki = j, ji = -k, kj = -i$ e $ik = -j$.

Quando se estuda uma certa estrutura algébrica, precisamos considerar as funções entre elas, que tem a propriedade de preservar a dada estrutura. Como as estruturas algébricas estão definidas em função de certas operações, precisamos então considerar as funções que preservam estas operações. Estas funções levam o nome de *homomorfismos*. Vamos apresentar uma definição mais precisa, para o caso de anéis.

Definição 1.1.11. Sejam $R = (R, +_R, \cdot_R)$ e $S = (S, +_S, \cdot_S)$ dois anéis. Uma função $f : R \to S$ é dita um homomorfismo de anéis, se:

- $f(a +_R b) = f(a) +_S f(b), \forall a, b \in R$,
- $f(a \cdot_R b) = f(a) \cdot_S f(b), \forall a, b \in R$.

Antes de apresentarmos alguns exemplos de homomorfismos de anéis, vejamos algumas propriedades que decorrem diretamente da definição.

Proposição 1.1.12. *Sejam R e S anéis e $f : R \to S$ um homomorfismo de anéis. Então valem as seguintes propriedades:*

(i) $f(0_R) = 0_S$,

(ii) $f(-a) = -f(a), \forall a \in R$,

(iii) $f(R)$ *é um subanel de* S.

Demonstração. (i) Basta observar que $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$, de onde segue que $f(0_R) = 0_S$, pois $f(0_R)$ e 0_S são ambas soluções da equação $f(0_R) + X = f(0_R)$ em S.

(ii) Temos que mostrar que $f(-a) + f(a) = 0_S$. Mas isto segue diretamente do item anterior, pois $f(-a) + f(a) = f(-a + a) = f(0_R) \overset{(i)}{=} 0_S$. Logo, $f(-a)$ é o simétrico de $f(a)$ em S.

(iii) Por (i), temos que $0_S \in \mathcal{I}m\, f$. Dados $x, y \in \mathcal{I}m\, f$, segue que existem $a, b \in R$ tais que $f(a) = x$ e $f(b) = y$. Assim, $x - y = f(a) - f(b) = f(a - b)$ e $xy = f(a)f(b) = f(ab)$ e, consequentemente, $x - y, xy \in \mathcal{I}m\, f$. Segue então da Proposição 1.1.8 que $\mathcal{I}m\, f$ é um subanel de S. □

Seja $f : R \to S$ um homomorfismo de anéis. Dizemos que f é um *monomorfismo* se f for injetor. Neste caso, S é dito uma *extensão* de R. Dizemos que f é um *epimorfismo* se f for sobrejetor. No caso em que f é bijetor, então dizemos que f é um *isomorfismo*. Neste último caso, R e S são cópias um do outro, como anéis, e dizemos que eles são anéis isomorfos, notando por $R \simeq S$. Cabe observar que se $f : R \to S$ é um monomorfismo de anéis, então f é um isomorfismo sobre sua imagem e, neste caso, S contém um subanel que é uma cópia de R. Identificando estes anéis, podemos então dizer que R é um subanel de S. Isto é o que se faz, por exemplo, quando se diz que $\mathbb{Z}$ é um subanel de $\mathbb{Q}$, pois neste caso, estamos considerando o homomorfismo $f : \mathbb{Z} \to \mathbb{Q}$ definido por $f(a) = \frac{a}{1} \in \mathbb{Q}$, para todo $a \in \mathbb{Z}$.

Exemplo 1.1.13. Sejam R e S dois anéis quaisquer. A função $f : R \to S$ definida por $f(a) = 0$, para todo elemento $a \in R$, é um homomofismo de anéis, chamado *homomorfismo nulo*. A função $id_R : R \to R$, dada por $id_R(a) = a$, é um homomorfismo de anéis, chamado *homomorfismo identidade*.

O próximo exemplo mostra que podem não existir muitos homomorfismos entre dois anéis.

Exemplo 1.1.14. Se $f : \mathbb{Z} \to \mathbb{Z}$ é um homomorfismo de anéis, então f é o homomorfismo nulo ou f é o homomorfismo identidade.

De fato, pois se $n \in \mathbb{Z} \setminus \{0\}$, então $n = 1 + 1 + \cdots + 1$ (n vezes, se $n > 0$) ou $n = -1 + (-1) + \cdots + (-1)$ ($-n$ vezes, se $n < 0$). Suponhamos, sem perda de generalidade, que $n > 0$. Então, $f(n) = f(1) + f(1) + \cdots + f(1)$ (n vezes). Portanto, para se definir um homomorfismo cujo domínio é $\mathbb{Z}$, basta definir $f(1)$. Claramente, se $f(1) = 0$ então f é o homomorfiso nulo. Por outro lado, observamos que $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$, ou seja, $f(1)(1 - f(1)) = 0$, de onde segue que $f(1) = 0$ ou $f(1) = 1$. Consequentemente, devemos ter que f é o homomorfismo nulo ou f é o homomorfismo identidade. Este resultado pode ser generalizado para domínios de integridade quaisquer, como mostra o próximo exercício.

Exercício 1.1.15. Sejam D e D' dois domínios de integridade. Mostre que se $f : D \to D'$ é um homomorfismo de anéis, então devemos ter $f(1_D) = 0$ ou $f(1_D) = 1_{D'}$.

Exercício 1.1.16. Mostre que $f : \mathbb{R} \to \mathcal{M}_2(\mathbb{R})$, dada por $f(x) = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$, $\forall x \in \mathbb{R}$ é um homomorfismo de anéis e que $f(1) \neq 0$ e $f(1) \neq 1_{\mathcal{M}_2(\mathbb{R})}$. Conclua daí que a hipótese de D' ser um domínio de integridade é essencial no exercício anterior.

Exercício 1.1.17. Sejam R e S dois anéis. Se R tem unidade e $f : R \to S$ não é o homomorfismo nulo, então mostre que $f(1_R)$ é a unidade do anel $\mathcal{I}m\, f$.

Definição 1.1.18. Seja $f : R \to S$ um homomorfismo de anéis. Chamamos de núcleo de f ao conjunto $\mathcal{N}uc\, f = \{a \in R : f(a) = 0\}$.

O núcleo de um homomorfismo tem propriedades bastante interessantes. Começamos por observar que se $f : R \to S$ é um homomorfismo de anéis e $f(a) = f(b)$, para certos elementos $a, b \in R$, então devemos ter $f(a-b) = f(a) - f(b) = 0$ em S, ou seja, $a - b \in \mathcal{N}uc\, f$. Isto nos diz que se dois elementos de R têm a mesma imagem por um homomorfismo, então a diferença deles deve estar no seu núcleo. Assim, homomorfismos com núcleo nulo devem ser injetores. A recíproca deste fato é claramente verdadeira, de modo que temos o seguinte resultado.

Proposição 1.1.19. *Um homomorfismo de anéis $f : R \to S$ é injetor se, e somente se, $\mathcal{N}uc\, f = \{0\}$.*

Assim, o núcleo de um homomorfismo nos dá uma medida de quão longe de ser injetor este homomorfismo está. Mais ainda, o núcleo de um homomorfismo é um subanel. De fato, pois se $f : R \to S$ é um homomorfismo de anéis, então $f(0_R) = 0_S$, ou seja, $0_R \in \mathcal{N}uc\, f$. Tomando-se $x, y \in \mathcal{N}uc\, f$, temos claramente que $f(x-y) = 0$ e $f(xy) = 0$, de onde segue que $x - y, xy \in \mathcal{N}uc\, f$. Segue então da Proposição 1.1.8 que $\mathcal{N}uc\, f$ é um subanel de R. Este subanel tem uma propriedade especial, a saber, a absorção da multiplicação tanto pela esquerda como pela direita. Mais precisamente, se $f : R \to S$ é um homomorfismo de anéis, $x \in \mathcal{N}uc\, f$ e $a \in R$, então $ax, xa \in \mathcal{N}uc\, f$. De fato, pois $f(ax) = f(a)f(x) = f(a)0 = 0$. Analogamente, $f(xa) = 0$. Isto induz a seguinte definição.

Definição 1.1.20. Dado um anel R, dizemos que um subanel I de R é um:

(i) ideal à esquerda de R, se $xa \in I$, sempre que $x \in R$ e $a \in I$,

(ii) ideal à direita de R, se $ax \in I$, sempre que $x \in R$ e $a \in I$,

(iii) ideal de R, se I é um ideal à esquerda e à direita de R.

Vamos usar as seguintes notações para representar estes tipos de ideais: escreveremos $I \lhd R$, para dizer que I é um ideal de R; notaremos por $I \lhd_r R$ os ideais à direita e por $I \lhd_l R$ os ideais à esquerda de R.

Como vimos acima, núcleos de homomorfismos são exemplos de ideais, mas nem todo subanel é um ideal, pois é fácil ver que $\mathbb{Z}$ é um subanel de $\mathbb{Q}$ que não é um ideal de $\mathbb{Q}$. Também é fácil ver que se I é um ideal à esquerda de R, então I é um ideal à direita de R^{op}. Assim, os três conceitos acima coincidem num anel comutativo. Veremos exemplos destas estruturas em anéis não comutativos, onde elas diferem. Antes porém, vamos classificar os ideais de $\mathbb{Z}$ usando conhecimentos da aritmética dos números inteiros.

Já sabemos que para cada $n \in \mathbb{Z}$, o conjunto $I = n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ é um subanel de $\mathbb{Z}$. Vamos ver que estes conjuntos são na verdade, ideais de $\mathbb{Z}$. De fato, pois se $x \in \mathbb{Z}$, então $x(na) = (na)x = n(xa) \in n\mathbb{Z}$. Reciprocamente, se I é um ideal de $\mathbb{Z}$ e $a \in I$ é o menor inteiro positivo em I, então $I = a\mathbb{Z}$. Isto decorre da divisão euclidiana, já que se $x \in I$, então existem elementos unicamente determinados $q, r \in \mathbb{Z}$ tais que $x = aq + r$, com $0 \leq r < a$. Mas então, devemos ter $r = x - aq \in I$, de onde segue que $r = 0$, pela minimalidade de a em I. Logo, $x = aq \in a\mathbb{Z}$, o que conclui nosso raciocínio.

Os próximos exemplos mostram a existência de ideais unilaterais em anéis de matrizes. Estes exemplos serão importantes no decorrer do texto. Os cálculos serão deixados ao leitor interessado.

Exemplo 1.1.21. Seja R um anel e consideremos $S = \mathcal{M}_n(R)$ o anel de matrizes $n \times n$ com entradas em R. Então, fixando-se $k \in \{1, 2, ..., n\}$, temos que:

- $\mathcal{I}_k := \{(a_{ij}) \in S : a_{ij} = 0, \text{ se } j \neq k\}$ é um ideal à esquerda de S, que não é um ideal à direita de S.

- $\mathcal{J}_k := \{(a_{ij}) \in S : a_{ij} = 0, \text{ se } i \neq k\}$ é um ideal à direita de S, que não é um ideal à esquerda de S.

Além destes, existem outros ideais, tanto à esquerda quanto à direita, em um anel de matrizes, mas não pretendemos classificá-los neste texto. Entretanto, uma tarefa bem mais simples é a classificação dos ideais (bilaterais) dos anéis de matrizes. Passaremos a fazer isto agora, pois esta classificação será importante para nossos propósitos. Começaremos por apresentar certos cálculos matriciais que serão importantes para a nossa tarefa.

Seja R um anel e consideremos $S = \mathcal{M}_n(R)$ o anel de matrizes $n \times n$ com entradas em R. Para $k, l \in \{1, 2, ..., n\}$ fixos, consideremos a matriz elementar $E_{kl} = (e_{ij}) \in S$, onde $e_{ij} = 1$, se $i = k$ e $j = l$ e $e_{ij} = 0$ nas demais entradas. Consideremos $A = (a_{ij})_{n\times n} \in S$, e calculemos AE_{rs} e $E_{pq}A$, onde $1 \leq r, s, p, q \leq n$.

Assim, $AE_{rs} = \left((\sum_{k=1}^{n} a_{ik}e_{kj})_{ij}\right)_{n\times n}$, onde temos:

$$\begin{array}{rcl} j \neq s \;\Rightarrow\; \sum_{k=1}^{n} a_{ik}e_{kj} &=& 0 \\ j = s \;\Rightarrow\; \sum_{k=1}^{n} a_{ik}e_{ks} &=& \sum_{k\neq r} a_{ik}e_{ks} + a_{ir}e_{rs} = a_{ir} \end{array}$$

Logo,

$$AE_{rs} = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_{1r} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & a_{2r} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{nr} & 0 & \cdots & 0 \end{pmatrix}_{n\times n} \quad \begin{matrix} \\ \\ \\ \\ \downarrow \\ s \end{matrix}$$

Portanto, a ação da multiplicação de E_{rs} à direita de A equivale a transportar a coluna r de A para a posição da coluna s, anulando as demais colunas de A.

Calculemos agora o produto $E_{pq}A$. Assim, temos

$$E_{pq}A = \left(\left(\sum_{k=1}^{n} e_{ik}a_{kj}\right)_{ij}\right)_{n\times n},$$

onde

- $i \neq p \Rightarrow \sum_{k=1}^{n} e_{ik}a_{kj} = 0$;
- $i = p \Rightarrow \sum_{k=1}^{n} e_{ik}a_{kj} = \sum_{k\neq q} e_{pk}a_{kj} + e_{pq}a_{qj} = a_{qj}$

ou seja, temos

$$E_{pq}A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ a_{q1} & a_{q2} & \cdots & a_{qn-1} & a_{qn} \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \longleftarrow p$$

Logo, a ação da multiplicação de E_{pq} à esquerda de A equivale a transportar a linha q de A para a posição da linha p, anulando as demais linhas de A.

Portanto, dado $A \in S$, obtemos que $E_{pq}AE_{rs}$ será a matriz cujas entradas são todas nulas, exceto a da posição ps, cuja entrada será dada pelo elemento a_{qr} de A.

Os cálculos acima mostram que se $A \in \mathcal{I} \lhd S$, então existe uma matriz $B = (b_{ij}) \in \mathcal{I}$ tal que o elemento b_{11} é igual a qualquer uma das entradas de A, sendo as demais entradas de B nulas. Basta para tal, escolhermos apropriadamente as matrizes elementares $E_{kl} \in S$ para multiplicarmos à esquerda e à direita de A. Com esta argumentação, pode-se mostrar o seguinte resultado.

Proposição 1.1.22. *Sejam R um anel e $S = \mathcal{M}_n(R)$ o anel das matrizes $n \times n$ com entradas em R. Então, $\mathcal{I}$ é um ideal de S se, e somente se, existe um ideal I de R tal que $\mathcal{I} = \mathcal{M}_n(I)$.*

Ideia da demonstração. De fato, é fácil verificar que se $I \lhd R$, então $\mathcal{M}_n(I)$, o anel das matrizes com entradas em I, é um ideal de S. Para a recíproca, usamos os cálculos acima para mostrar que se $\mathcal{I} \lhd S$, então o conjunto

$$I = \{a \in R : \text{ existe } A = (a_{ij}) \in \mathcal{I} : a_{11} = a\}$$

é um ideal de R tal que $\mathcal{I} = \mathcal{M}_n(I)$. □

Observamos agora que se D é um anel de divisão, então D não possui ideais (bilaterais, unilaterais) não triviais (i. e, além de $\{0\}$ e D). De fato, pois se $I \lhd D$ é não nulo, então tomando $0 \neq x \in I$, teremos que $1 = x^{-1}x \in I$, de onde decorre que $D \subseteq I \subseteq D$, ou seja, $I = D$. Assim, segue então da Proposição 1.1.22 que o anel $\mathcal{M}_n(D)$ não possui ideais (bilaterais). Anéis que não possuem ideais não triviais são chamados de *anéis simples*. Formulemos isto precisamente numa definição.

Definição 1.1.23. Dizemos que um anel $R \neq 0$ é simples se R não possui nenhum ideal além dos triviais, i. é, além de $\{0\}$ e R.

Pela nossa discussão anterior, corpos, anéis de divisão e anéis de matrizes sobre anéis de divisão são exemplos de anéis simples. Mais a frente exibiremos outro exemplo que difere destes.

Uma outra aplicação dos ideais na teoria de anéis são os anéis quocientes. Veremos abaixo que os ideais são exatamente os subaneis para os quais podemos induzir uma estrutura de anel no conjunto quociente, tal como se faz com a aritmética modular dos inteiros. Se $n \in \mathbb{Z}$, então a relação dada por:

$$x, y \in \mathbb{Z},\ x \equiv y \overset{def}{\Leftrightarrow} x - y \in n\mathbb{Z}$$

é uma relação de equivalência e o conjunto quociente $\mathbb{Z}/n\mathbb{Z} = \{\overline{1}, \overline{2}, ..., \overline{n-1}\}$ tem uma estrutura de anel $(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\cdot})$, dada por:

- $\overline{a} \ \overline{+} \ \overline{b} := \overline{a + b}, \forall a, b \in \mathbb{Z}$,
- $\overline{a} \ \overline{\cdot} \ \overline{b} := \overline{a \cdot b}, \forall a, b \in \mathbb{Z}$

As igualdades acima podem ser facilmente verificadas, usando propriedades dos restos da divisão euclidiana em $\mathbb{Z}$, pois se $x - y \in n\mathbb{Z}$, então existe $q \in \mathbb{Z}$ tal que $x - y = nq$, ou seja, $x = nq + y$. Agora é só observar que se x e y estão relacionados pela equação acima, então ambos deixam o mesmo resto na divisão euclidiana por n.

Vamos generalizar estas ideias para anéis quaisquer. Sejam R um anel e I um subanel de R. Não é difícil verificar que a relação definida em r por:

$$x, y \in R, x \equiv_I y \overset{def}{\Leftrightarrow} x - y \in I$$

é uma relação de equivalência em R. O que não se consegue mostrar é que a aplicação $\overline{\cdot} : R/I \times R/I \to R/I$ definida por

$$\overline{x \cdot y} := \overline{x \cdot y}, \forall x, y \in R$$

está bem definida. Para que esta aplicação esteja bem definida, e portanto ser uma operação em R/I, é necessário exigir que o subanel I seja de fato um ideal de R. Deixamos este fato para ser mostrado no seguinte exercício.

Exercício 1.1.24. Sejam R um anel, I um subanel de R e $\equiv_I$ a relação de equivalência dada por: $x, y \in R$; $x \equiv_I y \Leftrightarrow x - y \in I$. Mostre que

$$\overline{\cdot} : R/I \times R/I \to R/I,$$

definida por $\overline{\cdot}(\overline{a}, \overline{b}) := \overline{a \cdot b}$, é uma função se, e somente se, I é um ideal de R.

Além disso, precisamos ver que as propriedades de associatividade, comutatividade, existência de neutro e de simétrico são herdadas por operações induzidas em conjuntos quocientes, mas isto também é de fácil verificação e será deixada ao encargo do leitor.

Portanto, se I é um ideal de R, então podemos considerar o anel quociente R/I. Assim, fica definido um homomorfismo de anéis $\pi : R \to R/I$, por $\pi(a) = \overline{a} := a + I = \{a + x : x \in I\}$. É facil ver que este homomorfismo é sobrejetor

e que seu núcleo é exatamente o ideal I. Isto mostra que todo ideal é o núcleo de algum homomorfismo de anéis. Assim, podemos caracterizar os ideais como sendo aqueles subanéis que são núcleos de homomorfismos.

Outra observação pertinente é que se $f : R \to S$ é um homomorfismo de anéis, então os elementos de R que tem mesma imagem por f são identificados no anel quociente $R/\mathcal{N}uc\, f$. Assim, deveríamos poder mergulhar este anel quociente em S. De fato, isto é possível, como mostra o próximo resultado.

Teorema 1.1.25. (Teorema dos Homomorfismos para anéis) *Sejam R, S anéis e $f : R \to S$ um homomorfismo de anéis. Então existe um único monomorfismo de anéis $\overline{f} : R/\mathcal{N}uc\, f \to S$ tal que $\overline{f} \circ \pi = f$*

Demonstração. Basta definir $\overline{f}(\overline{a}) = f(a)$, para todo $\overline{a} \in R/\mathcal{N}uc\, f$. Vejamos que assim $\overline{f}$ está bem definida. De fato, pois se $\overline{a} = \overline{b}$ em $R/\mathcal{N}uc\, f$, então $a - b \in \mathcal{N}uc\, f$, ou seja, $f(a - b) = 0$, de modo que $f(a) = f(b)$, pois f é um homomorfismo de anéis. Assim temos $\overline{f}(\overline{a}) = \overline{f}(\overline{b})$. Além disso, por definição, temos que $f(a) = \overline{f}(\overline{a}) = \overline{f}(\pi(a)) = \overline{f} \circ \pi(a)$, para todo $a \in R$, ou seja, $\overline{f} \circ \pi = f$.

Afirmamos que $\overline{f}$ é injetora. De fato, pois se $\overline{a} \in \mathcal{N}uc\, \overline{f}$, então $\overline{f}(\overline{a}) = 0$, ou seja, $0 = \overline{f}(\overline{a}) = f(a)$, de onde segue que $a \in \mathcal{N}uc\, f$, o que nos diz que $\overline{a} = \overline{0}$. Resta mostrar a unicidade de $\overline{f}$. Para tal, suponhamos que $g : R/\mathcal{N}uc\, f \to S$ é tal que $g \circ \pi = f$. Mas então, para cada $\overline{a} \in R/\mathcal{N}uc\, f$, temos $g(\overline{a}) = g \circ \pi(a) = f(a) = \overline{f}(\overline{a})$, e segue que $g = \overline{f}$. □

A seguinte consequência do resultado acima é imediata.

Corolário 1.1.26. *Com as notações do Teorema anterior, se f é um epimorfismo, então $R/\mathcal{N}uc\, f \simeq S$ como anéis.*

Vamos discutir o próximo exemplo a luz dos nossos resultados. Consideremos $R = \left\{ \begin{bmatrix} a & x \\ 0 & a \end{bmatrix} : a \in \mathbb{Z}, x \in \mathbb{Q} \right\}$. É fácil verificar que R, com as operações usuais de matrizes, é um anel comutativo com unidade (verifique isto!). Afirmamos que $J := \left\{ \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} : x \in \mathbb{Q} \right\}$ é um ideal de R. Faremos isto mostrando que J é o núcleo de um homomorfismo de anéis (mostre isto diretamente). De fato, basta definir o homomorfismo $\varphi : R \to \mathbb{Z}$, por $\varphi \begin{pmatrix} a & x \\ 0 & a \end{pmatrix} = a$. É fácil ver que φ é um homomorfismo de anéis e que $J = \mathcal{N}uc\, \varphi$, de onde segue que J é um ideal de R. Mais ainda, como φ é sobrejetor, segue que $R/J \simeq \mathbb{Z}$.

1.2 Módulos.

Nesta seção apresentaremos algumas propriedades básicas da teoria dos módulos. Para simplificar nossos resultados, vamos supor no restante do texto que todos os nossos anéis possuem unidade.

Grosso modo, um módulo é um “espaço vetorial"sobre um anel. Isto justifica estudarmos módulos, estudando certos análogos da teoria dos espaços vetoriais. Num certo sentido, é aproximadamente isto o que faremos neste texto.

Mais precismente, temos a seguinte definição.

Definição 1.2.1. Seja R um anel (com unidade). Dizemos que $(M, +_M)$ é um R-módulo à esquerda, se $(M, +_M)$ for um grupo abeliano (i. é, $+_M$ é associativa, possui neutro, possui simétrico e é comutativa) e, além disso, existir uma aplicação $\bullet : R \times M \to M$ (chamada de ação de R em M), satisfazendo as seguintes propriedades:

(i) $1_R \bullet m = m, \forall m \in M$,

(ii) $r \bullet (m_1 +_M m_2) = r \bullet m_1 +_M r \bullet m_2; \forall r \in R, \forall m_1, m_2 \in M$,

(iii) $r_1 \bullet (r_2 \bullet m) = (r_1 \cdot r_2) \bullet m; \forall r_1, r_2 \in R, \forall m \in M$,

(iv) $(r_1 + r_2) \bullet m = (r_1 \bullet m) +_M (r_2 \bullet m); \forall r_1, r_2 \in R, \forall m \in M$.

Analogamente, podemos definir um R-módulo à direita, bastando coniderar uma ação de R em M pela direita, ou seja, uma aplicação $\bullet : M \times R \to M$, satisfazendo os mesmos axiomas acima, devidamente adaptados. Notaremos um R-módulo à esquerda por ${}_RM$ e por M_R, um R-módulo à direita. Na definição acima, escrevemos $+_M$ para denotar a soma de M, e não confundir com a soma $+$ de R. O mesmo foi feito em relação as notações da ação de R em M, denotada por $\bullet$ e a multiplicação de R. Mas no que segue, vamos denotar tanto a soma de R quanto a soma de M por $+$, e a multiplicação de R bem como a ação de R em M, por justaposição dos elementos, ou seja, se $r_1, r_2 \in R$ e $m \in M$, escreveremos $r_1 r_2$ para denotar a multiplicação de r_1 por r_2 em R e também, $r_1 m$ para denotar a ação de r_1 em m, pois não haverá perigo de confusão.

Antes de apresentar exemplos, gostaríamos de observar que se M é um R-módulo à esquerda, então M é um R^{op}-módulo à direita, e vice-versa, como é fácil verificar. Assim, a teoria de módulos é completamente simétrica e todo resultado que vale para módulos à esquerda também vale para módulos à direita, de modo que podemos fixar os adjetivos “à esquerda"ou “à direita" para desenvolvermos nossa teoria. Além disso, se R é um anel comutativo, então os conceitos de módulos à direita e de módulos à esquerda coincidem e, neste caso, escreveremos apenas R-módulo.

Exemplo 1.2.2. Seja $\Bbbk$ um corpo. Então um $\Bbbk$-módulo nada mais é do que um $\Bbbk$-espaço vetorial.

Exemplo 1.2.3. Todo grupo abeliano é um $\mathbb{Z}$-módulo.

De fato, se $(G, +)$ é um grupo abeliano (aditivo), então basta considerar a ação dada por:

- $0_{\mathbb{Z}} g = 0_G$

- $ng = g + g + \cdots + g (n \text{ vezes })$, se $n > 0$
- $ng = (-g) + (-g) + \cdots + (-g) (-n \text{ vezes })$, se $n < 0$.

Exemplo 1.2.4. Todo anel é um módulo sobre si mesmo, tanto à esquerda quanto à direita, com a ação dada pela própria multiplicação.

Com relação ao exemplo acima, o R-módulo à esquerda ${}_RR$ é chamado de *módulo regular à esquerda*, e o R-módulo à direita R_R é chamado de *módulo regular à direita*. Observamos neste momento que se R não for comutativo, então a estrutura destes dois módulos regulares não precisam necessariamente coincidirem, de modo que muitas vezes o módulo regular à esquerda possui uma propriedade que o módulo regular à direita não possui e vice-versa. Vamos ver exemplos deste fato mais adiante.

Exemplo 1.2.5. Consideremos S o anel de matrizes $n \times n$ com entradas num anel R. Seja N o conjunto de todas as matrizes $n \times 1$ com entradas em R. Então N é um grupo abeliano aditivo com a soma de matrizes. Assim, N torna-se um S-módulo à esquerda via a multiplicação usual de matrizes. De modo análogo se mostra que o conjunto L das matrizes $1 \times n$, com entradas em R, é um S-módulo à direita.

Como dito antes, uma vez que estamos estudando módulos, queremos estudar as funções que preservam esta estrutura e também estudar as subestruturas dos módulos. Passaremos a definir estes objetos mais precisamente.

Definição 1.2.6. Sejam R um anel e M um R-módulo à esquerda. Dizemos que um subconjunto não vazio N de M é um submódulo de M (ou um R-submódulo de M), se $(N, +)$ é um subgrupo de $(M, +)$ e a restrição da ação de R em N induz uma estrutura de R-módulo em N.

Vamos escrever $N \leq M$ para dizer que N é um submódulo de M. O próximo resultado caracteriza os subconjuntos de um módulo que são submódulos deste.

Proposição 1.2.7. *Sejam R um anel, M um R-módulo à esquerda e $N \subseteq M$. Então N é um submódulo de M se, e somente se:*

(i) $0 \in N$,

(ii) $\forall n_1, n_2 \in N \Rightarrow n_1 + n_2 \in N$,

(iii) $\forall r \in R, n \in N \Rightarrow rn \in N$.

A demonstração da proposição acima será deixada como um exercício. Vejamos alguns exemplos.

Exemplo 1.2.8. Os submódulos de um módulo regular à esquerda (resp. à direita) são exatamente os ideais à esquerda (resp. à direita) do anel base.

O exemplo acima nos diz que podemos estudar a estrutura dos ideais de um anel, estudando a estrutura de submódulos de um módulo. Assim, toda propriedade válida para módulos pode ser traduzida para a linguagem de anéis, via ideais à esquerda (ou à direita).

Exemplo 1.2.9. Os submódulos de um espaço vetorial são exatamente os seus subespaços vetoriais.

Exemplo 1.2.10. Os subgrupos de um grupo abeliano G são os $\mathbb{Z}$-submódulos de G.

O próximo exemplo nos dá uma receita de como obtermos novos submódulos a partir de outros já conhecidos.

Exemplo 1.2.11. Sejam M um R-módulo à esquerda e $\mathcal{F} = \{N_i\}_{i\in I}$ uma família de R-submódulos de M. é fácil verificar que $N = \cap_{i\in I} N_i$ é um submóduo de M.

O próximo exercício mostra que o produto de ideais é também um ideal, e será usado mais adiante.

Exercício 1.2.12. Sejam R um anel e I, J ideais (bilaterais) de R. Mostre que o conjunto $IJ := \{\sum_{i=1}^{n} a_i b_i : n \in \mathbb{N}, a_i \in I, b_i \in J\}$ é um ideal de R tal que $IJ \subseteq I \cap J$.

Num primeiro curso de álgebra linear vemos que a união de subespaços não é, em geral, um espaço vetorial, pois esta não é fachada para a soma. O mesmo fenômeno ocorre no contexto de módulos. Assim, tal como no caso dos espaços vetoriais, nasce o conceito de submódulo gerado por um conjunto, para contornar este problema.

Definição 1.2.13. Sejam R um anel, M um R-módulo à esquerda e $K \subseteq M$. Chamamos de submódulo de M gerado por K, e denotamos por $< K >$, ao menor submódulo de M que contém K.

Do exemplo anterior, se $K \subseteq {}_RM$, então $< K >= \cap\{N \leq M : N \supseteq K\}$. Afirmamos que este último conjunto é igual ao conjunto $\mathcal{K} = \{\sum_{i=1}^{n} r_i x_i : n \in \mathbb{N}, r_i \in R \text{ e } x_i \in K, 1 \leq i \leq n\}$. De fato, pois como estamos assumindo que R tem unidade, segue facilmente que $\mathcal{K}$ é um R-submódulo de M que contém K, de onde decorre que $< K > \subseteq \mathcal{K}$. Por outro lado, todo submódulo de M que contém K deve conter todas as somas finitas de múltiplos escalares de elementos de K, de onde segue que $\mathcal{K} \subseteq < K >$.

Quando K é um subconjunto finito de M, digamos $K = \{x_1, x_2, ..., x_n\}$, vamos escrever $< x_1, x_2, ..., x_n >$, em lugar de $< \{x_1, x_2, ..., x_n\} >$, para denotar o submódulo de M gerado pelo conjunto $\{x_1, x_2, ..., x_n\}$. Os elementos $x_1, x_2, ..., x_n$ serão chamados de *geradores* do submódulo $< K >$. Quando $K = \{y\}$ é um conjunto unitário, então diremos que $< y >$ é um *módulo cíclico*.

Mais ainda, dizemos que um módulo M é *finitamente gerado*, se existir um conjunto finito $\{m_1, m_2, ..., m_t\} \subseteq M$ tal que $M =< m_1, m_2, ..., m_t >$. Pela

argumentação acima, se M é um R-módulo à esquerda e $m_1, m_2, ..., m_t \in M$, então segue que $< m_1, m_2, ..., m_t >= \{\sum_{i=1}^{t} r_i m_i : r_i \in R, 1 \leq i \leq t\}$, e neste caso, o módulo $< m_1, m_2, ..., m_t >$ será denotado por $\sum_{i=1}^{t} Rm_i$. Assim, o R-módulo à esquerda cíclico gerado por um elemento x será denotado por Rx. Vamos observar neste momento que se R é um anel e $x \in R$, então o submódulo cíclico do módulo regular à esquerda (resp. à direita) Rx (resp. xR) é chamado de *ideal principal à esquerda (resp. à direita) de* R.

Analogamente, se $\{N_i\}_{i\in I}$ é uma família de R-submódulos de um R-módulo à esquerda M, então o R-submódulo de M gerado por $\cup_{i\in I} N_i$ será denotado por $\sum_{i\in I} N_i$ e seus elementos serão somas finitas de elementos de N_i, quando i percorre o conjunto de índices I. Quando a família de submódulos for finita, escreveremos $N_1 + N_2 + \cdots + N_t$ em lugar daquela notação de somatório. Assim, se N e L são dois módulos, teremos que $N + L = \{x + y : x \in N, y \in L\}$ também é um módulo. Quando ocorrer que $N \cap L = 0$, diremos que o módulo soma $N + L$ é uma *soma direta* de N e L, e escreveremos $N \oplus L$. Mais geralmente, temos a seguinte definição.

Definição 1.2.14. Seja M um R-módulo à esquerda e $\{M_i\}_{i\in I}$ uma família de submódulos de M. Então dizemos que M é a soma direta da família $\{M_i\}_{i\in I}$, e notamos por $M = \oplus_{i\in I} M_i$, se:

(i) Todo elemento $m \in M$ pode ser escrito como uma soma $m = \sum_{i\in I} m_i$, com $m_i \in M_i$ e $m_i = 0$, exceto para um número finito de índices.

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

Observamos que se $\Bbbk$ é um corpo (ou um anel de divisão) e V é um $\Bbbk$-espaço vetorial de dimensão finita, então existe uma base $\mathcal{B} = \{v_1, v_2, ..., v_n\}$ de V, onde $n = dim_{\Bbbk} V$, e segue que $V = \Bbbk v_1 \oplus \Bbbk v_2 \oplus \cdots \oplus \Bbbk v_n$. Se R é um anel, então $M = R \times R \times R \cdots \times R$ (n cópias de R) tem uma estrutura natural de R-módulo e, neste caso, $M = \oplus_{i=1}^{n} R_i$, onde $R_i = R$, $1 \leq i \leq n$. Note que , em geral, $\Pi_{i\in I} M_i \neq \oplus M_i$, pois se I for um conjunto infinito, então $\Pi_{i\in I} M_i$ é o conjunto de todas as sequências infinitas com entradas em M_i, $i \in I$, enquanto que os elementos de $\oplus_{i\in I} M_i$ são somas (ou n-uplas) finitas.

Uma outra caracterização de uma soma direta que pode ser bastante conveniente é dada no próximo exercício.

Exercício 1.2.15. Sejam R um anel e M um R-módulo à esquerda. Mostre que $M = \oplus_{i\in I} M_i$ se, e somente se, todo elemento $m \in M$ pode ser escrito de modo único como uma soma finita $m = \sum_{i\in I} m_i$, com $m_i \in M_i$, onde $m_i = 0$, exceto para um número finito de índices.

Vamos considerar agora as aplicações entre módulos que preservam esta estrutura.

Definição 1.2.16. Sejam R um anel e M, N dois R-módulos à esquerda. Dizemos que uma função $f : M \to N$ é um homomorfismo de R-módulos (ou um R-homomorfismo), se:

(i) $f(m_1 + m_2) = f(m_1) + f(m_2), \forall m_1, m_2 \in M$,

(ii) $f(rm) = rf(m), \forall r \in R, m \in M$.

Um R-homomorfismo $f : M \to M$ é dito um R-endomorfismo.

Decorre imediatamente da definição acima que se $\Bbbk$ é um anel de divisão, então os $\Bbbk$-homomorfismos são exatamente as transformações $\Bbbk$-lineares. Por conta disso, muitas vezes nos referimos a um R-homomorfismo como uma *aplicação R-linear*.

Exemplo 1.2.17. Sejam R um anel e M, N dois R-módulos à esquerda. Claramente a aplicação nula $0 : M \to N$ dada por $0(m) = 0_N$ é um R-homomorfismo. Além disso, a aplicação identidade $id_M : M \to M$ também é um R-homomorfismo, como é facil verificar.

Como no caso de anéis, se $f : M \to N$ é um homomorfismo de R-módulos à esquerda, então dizemos que f é um *monomorfismo* se f é injetor; dizemos que f é um *epimorfismo* se f é sobrejetor. Por fim, dizemos que f é um *isomorfismo* se f for bijetor. Podemos também considerar o núcleo de um R-homomorfismo $f : M \to N$ como sendo o conjunto

$$\mathcal{N}uc\, f := \{m \in M : f(m) = 0_N\}.$$

Como no caso de anéis, podemos enunciar os seguintes resultados. A demonstração será deixada como exercício ao leitor, por ser completamente análoga àquela feita antes.

Proposição 1.2.18. *Sejam R um anel, M e N dois R-módulos à esquerda e $f : M \to N$ um R-módulo. Então:*

(i) $f(0_M) = 0_N$,

(ii) $\mathcal{N}uc\, f$ *é um R-submódulo de M,*

(iii) f *é um monomorfismo se, e somente se,* $\mathcal{N}uc\, f = \{0\}$,

(iv) Se $M' \leq M$, então $f(M')$ é um R-submódulo de N,

(v) Se N' é um R-submódulo de N, então $f^{-1}(N')$ é um R-submódulo de M.

Sejam R um anel, M um R-módulo à esquerda e N um R-submódulo de M. É fácil verificar que a relação *"congruência módulo N"* define em M uma relação de equivalência, isto é, a relação definida por

$$\forall x, y \in M, x \equiv_N y \Leftrightarrow x - y \in N$$

é reflexiva, simétrica e transitiva. Vamos denotar a classe de equivalência de um elemento $m \in M$ por $\overline{m}$. Assim, $\overline{m} = m + N = \{m + x : x \in N\} \subseteq M$.

Podemos então induzir, de modo natural, uma estrutura de R-módulo no conjunto quociente M/N, da seguinte forma:

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

Exemplo 1.2.19. Sejam R um anel, M um R-módulo à esquerda e N um R-submódulo de M. Então a aplicação $\pi : M \to M/N$, dada por $\pi(m) = \overline{m}$ é um R-homomorfismo cujo núcleo é precisamente N.

Neste contexto, podemos também enunciar um teorema de homomorfismos. Note que só foi usada a estrutura aditiva de um anel para mostrarmos o teorema dos homomorfismos para anéis. Isto permite usarmos a mesma argumentação de antes para mostrar o seguinte resultado.

Teorema 1.2.20. (Teorema dos homomorfismos) *Sejam R um anel e $f : M \to N$ um homomorfismo de R-módulos à esquerda. Então existe um R-monomorfismo $\overline{f} : M/\mathcal{N}uc\, f \to N$, únicamente determinado, tal que $f = \overline{f} \circ \pi$.*

O seguinte corolário muitas vezes é enunciado como um segundo teorema de homomorfismos.

Corolário 1.2.21. *Sejam R um anel e M um R-módulo à esquerda. Se L e N são dois submódulos de M, então*

$$\frac{L}{L \cap N} \simeq \frac{L+N}{N}$$

Demonstração. Basta observar que a composição de homomorfismos $L \hookrightarrow L + N \twoheadrightarrow (L+N)/N$ é sobrejetor e seu núcleo é dado exatamente por $L \cap N$. O resultado então segue pelo Teorema dos Homomorfismos. □

Um fato importante que será usado mais a frente, é a existência de uma correspondência biunívoca entre os submódulos de um módulo quociente M/N e os submódulos de M que contém N, dadas por

$$\{K \leq M : K \supseteq N\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{X : X \leq M/N\},$$

onde $\Phi(K) = \pi(K)$ e $\Psi(X) = \pi^{-1}(X)$, sendo $\pi : M \to M/N$ a projeção canônica.

A seguinte definição e suas consequências serão úteis mais adiante.

Definição 1.2.22. Sejam R um anel, M um R-módulo à esquerda e K, L dois R-submódulos de M. Então definimos o condutor (à esquerda) de K em L como sendo o conjunto $(L : K) = \{r \in R : rK \subseteq L\}$.

Observamos que o condutor de K em L é um ideal (bilateral) de R. Quando $L = 0$, então chamamos o condutor $(0 : K)$ de *anulador de K em R*, e denotamos por $An_R(K)$. Assim, $An_R(K) = (0 : K) = \{r \in R : rK = 0\}$. Podemos também definir os condutores de elementos em submódulos da seguinte forma: se M é um R-módulo à esquerda, N é um submódulo de M e $m \in M$, então $(N : m) = \{r \in R : rm \in N\}$. Note que $An_R(m)$ é um ideal à esquerda de R. Como antes, se $N = 0$, então o condutor $(0 : m)$ será chamado de *anulador de m em R* e será denotado por $An_R(m)$. Assim, $An_R(m) = (0 : m) = \{r \in R : rm = 0\}$.

Definição 1.2.23. Sejam R um anel e M um R-módulo à esquerda. Dizemos que M é fiel (ou que R age fielmente em M), se $An_R(M) = 0$.

Podemos traduzir a definição acima, dizendo que M é um R-módulo à esquerda fiel se, e somente se, para todo elemento $r \in R$, $rM = 0$ implica que $r = 0$.

Para vermos exemplos de tais módulos, basta observar que se R é um domínio de integridade, então todo ideal de R é um R-módulo fiel. Além disso, se M é um R-módulo à esquerda, então as ações de R e $R/An_R(M)$ coincidem e, portanto, todo R-módulo é um $R/An_R(M)$-módulo fiel. Note que estamos usando a ação induzida $(r + An_R(M))m = rm + An_R(M)$, no caso do anel $R/AN_R(M)$.

Um outro conceito importante na teoria de módulos, e que será usado mais adiante, é o conceito de bimódulo. Essencialmente, um bimódulo é um grupo abeliano que possui uma estrutura de módulo à esquerda sobre um anel e uma estrutura de módulo à direita sobre outro anel, de modo que estas estruturas respeitam uma certa condição natural de compatibilidade. Mais precisamente, temos o seguinte.

Definição 1.2.24. Sejam R e S dois anéis e M um grupo abeliano. Dizemos que M é um (R, S)-bimódulo, se:

(i) M é um R-módulo à esquerda e um S-módulo à direita.

(ii) Para todos $r \in R, s \in S$ e $m \in M$, vale que $(rm)s = r(ms)$.

Muitas vezes escrevemos ${}_RM_S$, para indicar que M é um (R, S)-bimódulo. Quando $R = S$, dizemos apenas que M é um R-bimódulo.

Exemplo 1.2.25. Seja R um anel. A associatividade da multiplicação garante que os ideais bilaterais de R são exemplos naturais de R-bimódulos.

Exemplo 1.2.26. Sejam R um anel e M um R-módulo à esquerda. Consideremos $S = End_R(M)$, o anel dos R-endomorfismos de M. Afirmams que M possui uma estrutura de (R, S)-bimódulo.

De fato, para ver isto, basta definir uma ação de S à direita de M, por

$$m \blacktriangleleft f := (m)f$$

onde $m \in M$, $f \in S$ e o argumento de um operador R-linear está escrito à esquerda do operador, para facilitar a regra da composição de funções. Note que

neste caso, se $m \in M$ e $f, g \in S$, então escrevemos $(m \blacktriangleleft f) \blacktriangleleft g = ((m)f)g = (m)f \circ g$, para indicar que aplicamos primeiro f e depois g, em analogia com o que se faz quando se escreve os argumentos à direita das funções: a primeira função a ser aplicada é aquela mais próxima do argumento.

Assim, é fácil verificar que M é de fato um S-módulo à direita. Além disso, temos

$$(r \cdot m) \blacktriangleleft f = (rm)f = r((mf) = r \cdot (m \blacktriangleleft f)$$

e temos que M é um (R, S)-bimódulo.

Como uma aplicação dos bimódulos, podemos construir exemplos de anéis cujo reticulado de ideais à direita é completamente diferente do reticulado dos ideais à esquerda. Sejam R e S dois anéis e consideremos M um (R, S)-bimódulo. Usando operações matriciais, podemos definir um anel da forma

$$T \overset{not}{=} \begin{pmatrix} R & M \\ 0 & S \end{pmatrix} := \left\{ \begin{pmatrix} r & m \\ 0 & s \end{pmatrix} : r \in R, m \in M, s \in S \right\}$$

que é um anel com unidade $1_T = \begin{pmatrix} 1_R & 0 \\ 0 & 1_S \end{pmatrix}$. Se tomamos $I \lhd_l R$ e $J \lhd_r S$, então se verifica que

$$\begin{pmatrix} I & M \\ 0 & S \end{pmatrix} \lhd_l T \text{ e } \begin{pmatrix} R & M \\ 0 & J \end{pmatrix} \lhd_r T.$$

Além destes, é possível encontrar outros ideais tanto à esquerda como à direita de T, mas isto foge um pouco dos nossos propósitos. Portanto, a família de ideais à esquerda de T pode ter propriedades que a família de ideais à direita de T não as têm. Vamos construir exemplos concretos neste sentido mais a frente.

1.3 Sequências exatas e somas diretas

Apesar de as sequências exatas serem uma ferramenta muito útil em várias aplicações, como por exemplo, teoria de categorias ou álgebra homológica, nesta breve seção vamos discutir apenas algumas propriedades básicas das sequências exatas de módulos e R-homomorfismos, que estão relacionadas com somas diretas de módulos, e que serão utilizadas mais adiante no texto.

Definição 1.3.1. Seja R um anel. Dados $\{M_i\}$ e $\{f_i : M_i \to M_{i+1}\}$, famílias de R-módulos à esquerda e R-homomorfismos, respectivamente, chamamos de uma *sequência* a todo diagrama do tipo

$$\cdots \overset{f_{i-1}}{\to} M_i \overset{f_i}{\to} M_{i+1} \overset{f_{i+1}}{\to} \cdots$$

tal que $\mathcal{I}m\, f_i \subseteq \mathcal{N}uc\, f_{i+1}$, para todo índice i. Uma sequência é dita *exata em* M_i, se ocorrer $\mathcal{I}m\, f_i = \mathcal{N}uc\, f_{i+1}$. Além disso, dizemos que uma sequência é exata, se ela é exata em todos os seus módulos. O número de R-homomorfismos no diagrama acima é dito o comprimento da sequência.

Vejamos alguns exemplos claros.

Exemplo 1.3.2. Sejam R um anel e $f : N \to M$ um homomorfismo de R-módulos à esquerda. Então:

(i) A sequência $0 \to N \xrightarrow{f} M$ é exata se, e somente se, f é um monomorfismo.

(ii) A sequência $N \xrightarrow{f} M \to 0$ é exata se, e somente se, f é um epimorfismo.

(iii) A sequência $0 \to N \xrightarrow{f} M \to 0$ é exata se, e somente se, f é um isomorfismo.

No presente texto, estamos mais interessados nas chamadas sequências exatas curtas, que serão definidas a seguir.

Definição 1.3.3. Uma sequência exata do tipo $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$, é dita uma *sequência exata curta*.

Exemplo 1.3.4. Sejam R um anel, M um R-módulo à esquerda e N um R-submódulo de M. Então a sequência

$$0 \to N \hookrightarrow M \xrightarrow{\pi} M/N \to 0,$$

onde π é a projeção canônica, é claramente uma sequência exata curta.

Num certo sentido, podemos pensar que toda sequência exata curta é desta forma. Mais precisamente, dada a sequência exata curta

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

segue que f é um monomorfismo e g é um epimorfismo. Assim, podemos pensar que A é um submódulo de B e que C é um módulo fator de B, a saber B/A, pois $\mathcal{I}m\, f = \mathcal{N}uc\, g$ e, consequentemente, temos $A \simeq \mathcal{I}m\, f \leq B$ e $B \simeq C/\mathcal{N}uc\, g = B/\mathcal{I}m\, f \simeq B/A$.

Vamos examinar agora a relação entre sequências exatas curtas e somas diretas. Começamos observando que se $M = N \oplus P$ como R-módulo à esquerda, então podemos definir as aplicações canônicas $\iota_N : N \to M$, dada por $\iota(n) = n + 0$ (inclusão canônica) e $\pi_P : M \to P$, dada por $\pi(n + p) = p$, para $n \in N$ e $p \in P$ (projeção canônica). Assim, vemos claramente que a sequência curta abaixo é exata:

$$0 \to N \xrightarrow{\iota} M \xrightarrow{\pi} P \to 0.$$

O próximo exemplo mostra que a recíproca deste fato não vale em geral.

Exemplo 1.3.5. A sequência de $\mathbb{Z}$-módulos abaixo é exata

$$0 \to 2\mathbb{Z} \hookrightarrow \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

mas, no entanto, $\mathbb{Z} \not\simeq 2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, como $\mathbb{Z}$-módulo.

Pode-se então questionar sob quais condições esta recíproca é verdadeira. O próximo resultado responde esta questão.

Proposição 1.3.6. *Sejam R um anel. Consideremos a sequência exata curta de R-módulos à esquerda*

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0.$$

Então as seguintes afirmações são equivalentes:

(i) $M \simeq N \oplus P$;

(ii) Existe um R-homomorfismo $\psi : M \to N$, tal que $\psi \circ f = id_N$;

(iii) Existe um R-homomorfismo $\varphi : P \to M$, tal que $g \circ \varphi = Id_P$.

Demonstração. Vamos mostrar a equivalência $(i) \Leftrightarrow (ii)$. A equivalência $(i) \Leftrightarrow (iii)$ pode ser mostrada com uma argumentação semelhante e será deixada ao leitor.

$(i) \Rightarrow (ii)$ Como f é injetora, segue que $N \simeq \mathcal{I}m\, f$ e assim, $M \simeq N \oplus P \simeq \mathcal{I}m\, f \oplus P$. Desta forma, dado $m \in M$, temos $m = m_1 + m_2$, com $m_1 \in \mathcal{I}m\, f$ e $m_2 \in P$. Da injetividade de f segue que existe único $n \in N$ tal que $f(n) = m_1$. Definimos então $\psi : M \to N$, por $\psi(m) = n$. É fácil ver que ψ está bem definida e é um R-homomorfismo. Mais ainda, para todo $n \in N$, temos que $f(n)$ se escreve unicamente como $f(n) + 0 \in \mathcal{I}m\, f \oplus P$, de onde segue que

$$\psi \circ f(n) = \psi(f(n)) = \psi(f(n) + 0) = n = id_N(n)$$

como queríamos mostrar.

$(ii) \Rightarrow (i)$ Suponhamos que exista $\psi : M \to N$ tal que $\psi \circ f = id_N$. Afirmamos que neste caso, $M = \mathcal{I}m\, f \ \oplus\ \mathcal{N}uc\, \psi$. De fato, pois se $m \in M$, tomamos $x = f(\psi(m)) \in M$ e consideramos $y = m - x \in M$. Segue então que

$$\psi(y) = \psi(m - x) = \psi(m) - \psi(f(\psi(m))) = \psi(m) - \psi(m) = 0$$

ou seja, $y \in \mathcal{N}uc\, \psi$. Logo, $m = x + y \in \mathcal{I}m\, f + \mathcal{N}uc\, \psi$. Além disso, se $z \in \mathcal{I}m\, f \cap \mathcal{N}uc\, \psi$, segue que existe $n \in N$ tal que $f(n) = z$ e, consequentemente, $n = \psi \circ f(n) = \psi(z) = 0$, de onde decorre que $z = 0$. Portanto, $M = \mathcal{I}m\, f \oplus \mathcal{N}uc\, \psi$.

Como f é injetiva, temos que $N \simeq \mathcal{I}m\, f$. Resta mostrar agora que $P \simeq \mathcal{N}uc\, \psi$. De fato, basta observar que

$$P \simeq \frac{M}{\mathcal{N}uc\, g} = \frac{\mathcal{I}m\, f \oplus \mathcal{N}uc\, \psi}{\mathcal{I}m\, f} \simeq \mathcal{N}uc\, \psi.$$

□

Uma sequência exata curta que satisfaz (ii) (equivalentemente, que satisfaz (iii)) na Proposição acima é dita uma *sequência exata curta que cinde*. As aplicações ψ e φ acima são muitas vezes chamadas de *cisão* da sequência. Com esta nova nomeclatura, segue que $M \simeq N \oplus P$ se, e somente se, a sequência

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$$

cinde. Como uma aplicação do resultado acima, temos o seguinte resultado.

Corolário 1.3.7. *Sejam R um anel, M e N dois R-módulos à esquerda. Se $g : M \to N$ e $h : N \to M$ são R-homomorfismos tais que $g \circ h = id_N$, então $M = \mathcal{N}uc\, g \oplus \mathcal{I}m\, h$.*

Demonstração. Como $g \circ h = id_N$, segue imediatamente que g é um epimorfismo e h é um monomorfismo. Aplicando-se a Proposição 1.3.6 para a sequência

$$0 \to \mathcal{N}uc\, g \hookrightarrow M \xrightarrow{g} N \to 0$$

obtemos que $M \simeq \mathcal{N}uc\, g \oplus N$. O resultado então segue, pois $N \simeq \mathcal{I}m\, h$. □

1.4 Lema de Zorn e ideais maximais

O propósito desta seção é mostrar que todo anel com unidade possui ideais (bilaterais ou unilaterais) maximais. Este fato é uma decorrência do chamado *Lema de Zorn*, o qual será apresentado adiante. Vamos começar relembrando a definição de elemento maximal (resp., elemento minimal.)

Consideremos $(X, \preceq)$ um conjunto munido de uma relação de ordem parcial. Dizemos que um elemento $m \in X$ é maximal (resp., minimal), se valer a seguinte propriedade:

$$\forall x \in X, m \preceq x \Rightarrow m = x \quad (resp., x \preceq m \Rightarrow m = x)$$

Por exemplo, se consideramos $X = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$ munido com a ordem “divide", isto é,

$$a, b \in X, a \preceq b \Leftrightarrow a|b$$

então os elementos $6, 7, 8, 9$ e 10 são elementos maximais em X e os elementos $2, 3, 5$ e 7 são elementos minimais em X.

Seja X um conjunto e $\mathcal{P}(X)$ o conjunto das partes de X. Então a relação

$$A, B \in \mathcal{P}(X), A \preceq B \Leftrightarrow A \subseteq B$$

é claramente uma relação de ordem parcial em $\mathcal{P}(X)$. Vamos trabalhar com esta relação de ordem na família de ideais (ideais à esquerda, ideais à direita) de um anel. Para mostrar a existência de ideais maximais, vamos precisar do chamado Lema de Zorn, o qual enunciamos abaixo.

Lema 1.4.1. (Lema de Zorn) *Seja $(\mathcal{F}, \preceq)$ uma família não vazia e parcialmente ordenada. Se toda cadeia em $\mathcal{F}$ possui uma cota superior (respectivamente, cota inferior) em $\mathcal{F}$, então $\mathcal{F}$ possui elemento maximal (resp., elemento minimal).*

Uma *cadeia* em $\mathcal{F}$ é uma subfamília de $\mathcal{F}$ que é totalmente ordenada. Assim, $\{1, 2, 4, 8\}$ é uma cadeia em X, onde X é o conjunto do exemplo anterior, pois

$$1 \preceq 2 \preceq 4 \preceq 8$$

Dados $\mathcal{F}$ uma família parcialmente ordenada e $\mathcal{F}' \subseteq \mathcal{F}$, chamamos de uma *cota superior* (resp. *cota inferior*) para $\mathcal{F}'$ a todo elemento $\alpha \in \mathcal{F}$ tal que $x \preceq \alpha$ (resp. $\alpha \preceq x$), para todo $x \in \mathcal{F}'$.

Muitas vezes chamamos de *sistema indutivo* a toda família parcialmente ordenada $\mathcal{F}$ em que toda cadeia possui cota superior (inferior) em $\mathcal{F}$. Nesta linguagem, o Lema de Zorn poderia ser escrito da forma: *Todo sistema indutivo possui elemento maximal (minimal).*

Os exemplos abaixo mostram algumas aplicações do Lema de Zorn.

Exemplo 1.4.2. Seja R um anel com unidade. Então R possui ideais (resp. ideais à esquerda, ideais à direita) maximais.

Vamos discutir a existência de ideais maximais em um anel R. A mesma discussão pode ser feita para os casos de ideais à esquerda ou à direita, escolhendo adequadamente a família $\mathcal{F}$ abaixo.

Consideremos então a família

$$\mathcal{F} := \{I \subseteq A : I \text{ é um ideal de } A, I \neq A\}$$

Observamos que $\{0\} \in \mathcal{F}$ e, consequentemente, $\mathcal{F} \neq \emptyset$. Seja $\mathcal{F}'$ uma subfamília totalmente ordenada de $\mathcal{F}$. Então, $J = \cup_{I \in \mathcal{F}'} I$ é um ideal de A (mostre isto!). Agora, como $1 \notin J$, pois $1 \notin I, \forall I \in \mathcal{F}'$, segue que $J \in \mathcal{F}$. É fácil verificar que J é uma cota superior para $\mathcal{F}'$. Portanto, como toda cadeia de $\mathcal{F}$ possui uma cota superior em $\mathcal{F}$, segue pelo Lema de Zorn que $\mathcal{F}$ possui elemento maximal, ou seja, o anel R possui um ideal maximal.

Na literatura, muitas vezes encontramos o resultado de que um anel com unidade R possui ideais maximais, como uma consequência do fato que todo ideal I de R está contido em algum ideal maximal. Também é fato que muitas vezes este é o resultado que precisamos usar. Podemos mostrar isto, com uma leve modificação na argumentação acima, considerando a família dos ideais próprios de R, que contém o ideal I. Note que esta família é não vazia, por conter o próprio ideal I.

Exemplo 1.4.3. Todo espaço vetorial possui uma base.

Considere V um espaço vetorial sobre um corpo $\Bbbk$ qualquer (ou sobre um anel de divisão). Como uma base de V, é um conjunto linearmente independente maximal em V, podemos usar o Lema de Zorn para mostrar sua existência, independentemente da dimensão de V ser finita ou infinita. Basta mostrar que a família dos subconjuntos linearmente indepedente é um sistema indutivo. Os detalhes serão deixados como exercício ao leitor.

Questão. *Podemos usar o Lema de Zorn para provar que todo anel possui um ideal minimal?*

A resposta a esta questão é negativa. Para ver isto, precisamos de uma definição de ideal minimal. Dualizando a definição de ideal maximal, obtemos

Definição 1.4.4. Dados um anel (com unidade) R e um ideal I de R, dizemos que I é um ideal minimal de R, se $I \neq \{0\}$ e, se existir ideal J de R tal que $J \subseteq I$, então temos $J = \{0\}$ ou $J = I$.

É claro que podemos definir ideal à esquerda minimal e ideal à direita minimal de modo análogo.

Seja R um anel e consideremos a família $\mathcal{F}$ dos ideais de R não nulos. Assim, $R \in \mathcal{F}$ e $\mathcal{F} \neq \emptyset$. O candidato natural para uma cota inferior para uma subfamília totalmente ordenada $\mathcal{F}'$ de $\mathcal{F}$, seria $J = \cap_{I \in \mathcal{F}'} I$. Mas é claro que não podemos garantir que J seja não nulo, isto é, não podemos garantir que $J \in \mathcal{F}$, e o Lema de Zorn não pode ser usado.

De fato, existem exemplos de anéis que não possuem ideais minimais. Por exemplo, se tomamos $R = \mathbb{Z}$, então é fácil ver que a cadeia de ideais

$$n\mathbb{Z} \supset n^2\mathbb{Z} \supset \cdots \supset n^t\mathbb{Z} \supset \cdots$$

é uma cadeia estritamente decrescente e infinita. Como todos os ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z}$, isto mostra que $\mathbb{Z}$ não possui nenhum ideal minimal.

Exercícios

1. Use o Lema de Zorn para mostrar que todo espaço vetorial sobre um corpo (ou sobre um anel de divisão) possui uma base.

2. Sejam R um anel e M um R-módulo à esquerda. Mostre que se M é finitamente gerado, então M possui um submódulo maximal.

3. Seja D um anel de divisão. Considere $V = \oplus_{i=1}^{\infty} De_i$ e $E = End(V_D)$. Mostre que $I = \{f \in E : dim_D \mathcal{I}m\, f < \infty\}$ é um ideal de E.

4. Sejam $I_1, I_2, ..., I_n$ ideais bilaterais de um anel R tais que $I_i + I_j = R$, se $i \neq j$ (neste caso, dizemos que I_i e I_j são comaximais). Mostre as seguintes afirmações:

   (i) $I_i + \cap_{j \neq i} I_j = R$, para todo i.

   (ii) **(Teorema Chinês de Restos)** Dados $x_1, x_2, ..., x_n \in R$, existe $x \in R$, tal que $x \equiv x_i (mod\, I_i)$, para todo i.

   (iii) Use o anterior para mostrar que existe um isomorfismo de anéis

   $$\Phi : \frac{R}{I_1 \cap \cdots \cap I_n} \longrightarrow \frac{R}{I_1} \times \cdots \times \frac{R}{I_n},$$

   dado por $\Phi(x + (I_1 \cap \cdots \cap I_n) = (x + I_1, \ldots, x + I_n)$, para todo $x \in R$.

Capítulo 2

Condições de finitude para anéis e módulos

Como já dissemos na introdução, Wedderburn estudou a estrutura de álgebras finito-dimensionais. Em nossa abordagem necessitamos de algum conceito que substitua esta finitude. Isto será obtido com o conceito de comprimento de um módulo e as chamadas condições de cadeias ascendentes e descendentes que discutiremos nesta seção.

2.1 Módulos simples

Para o que segue, precisamos do conceito de simplicidade. A ideia de simplicidade está associada a ausência de subestruturas próprias com as quais podemos construir estruturas quocientes. Mais precisamente, temos a seguinte definição.

Definição 2.1.1. (i) Dizemos que um anel R é simples, se $R \neq 0$ e R não possui ideais além do ideal nulo e do próprio R.

(ii) Dizemos que um R-módulo à esquerda M é simples, se $M \neq 0$ e M não possui nenhum submódulo além do submódulo nulo e do próprio M.

Observamos que anéis de divisão bem como anéis de matrizes sobre anéis de divisão são exemplos de anéis simples. Um espaço vetorial unidimensional é um exemplo de um módulo simples. Se $\Bbbk$ é um anel de divisão e tomamos $S = \mathcal{M}_n(\Bbbk)$, então o conjunto M das matrizes $n \times 1$ com entradas em $\Bbbk$ é um exemplo de um S-módulo à esquerda simples, como é fácil verificar.

Se R é um anel e M é um R-módulo à esquerda simples, então tomando-se $0 \neq m \in M$, podemos considerar o R-homomorfismo $f : R \to M$ dado por $f(r) = rm$. Como M é simples, devemos ter $\mathcal{I}m\, f = 0$ ou $\mathcal{I}m\, f = M$. Como estamos assumindo que R tem unidade então f não pode ser o homomorfismo nulo, pois $0 \neq m = 1m = f(1)$. Logo, devemos ter $\mathcal{I}m\, f = M$ e, portanto, $M \simeq R/An_R(m)$. Assim, todo R-módulo simples é isomorfo a um módulo fator

do módulo regular. Mais ainda, como M é simples e $M \simeq R/An_R(m)$, segue da correspondência entre os submódulos de $R/An_R(m)$ e dos R-submódulos do módulo regular ${}_RR$, que $An_R(m)$ é um ideal à esquerda maximal de R. Portanto, podemos enunciar o seguinte resultado que nos dá uma classificação dos módulos simples.

Proposição 2.1.2. *Sejam R um anel e M um R-módulo à esquerda. Então M é simples se, e somente se, existe um ideal à esquerda maximal J de R tal que $M \simeq R/J$.*

2.2 Séries de composição e condições de cadeia

Sejam R um anel e M um R-módulo à esquerda. Consideremos

$$\mathcal{C} : M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_r = 0$$

e

$$\mathcal{C}' : M = M_0' \supset M_1' \supset M_2' \supset \cdots \supset M_t' = 0$$

duas cadeias estritamente decrescente de submódulos de M. Então dizemos que:

(i) $\mathcal{C}'$ é um *refinamento* de $\mathcal{C}$, se todo membro de $\mathcal{C}$ aparece em $\mathcal{C}'$ (notaremos este fato escrevendo $\mathcal{C} \subseteq \mathcal{C}'$);

(ii) A cadeia $\mathcal{C}$ é uma *serie de composição* de M, se cada módulo fator $\frac{M_i}{M_{i+1}}$ $(0 \leq i \leq r-1)$ é um módulo simples, isto é, $\mathcal{C}$ não pode ser propriamente refinada;

(iii) O módulo M tem um *comprimento* r, e denotamos por $\ell(M) = r$, se M possui uma série de composição com r inclusões estritas. Se M não possuir nenhuma série de composição, então dizemos que M tem comprimento infinito e escrevemos $\ell(M) = \infty$;

(iv) As cadeias $\mathcal{C}$ e $\mathcal{C}'$ são *equivalentes*, e denotamos por $\mathcal{C} \simeq \mathcal{C}'$, se $r = t$ e, após uma reordenação nos índices, se necessário, temos $\frac{M_i}{M_{i+1}} \simeq \frac{M_i'}{M_{i+1}'}$.

No que segue, vamos mostrar que o comprimento de um módulo é um invariante deste módulo, ou seja, se M possui uma série de composição com r inclusões, então qualquer outra série de composição também terá r inclusões, de modo que o comprimento de um módulo está bem definido. Vejamos primeiro um exemplo.

Exemplo 2.2.1. Se $\Bbbk$ é um corpo (ou um anel de divisão) e V é um $\Bbbk$-espaço vetorial de dimensão n com base $\mathcal{B} = \{v_1, v_2, ..., v_n\}$, então

$$V = V_0 = \sum_{i=1}^{n} \Bbbk v_i \supset V_1 = \sum_{i=2}^{n} \Bbbk v_i \supset \cdots \supset V_{n-1} = \Bbbk v_n \supset V_n = 0$$

é uma série de composição de V. Assim, um $\Bbbk$-espaço vetorial n-dimensional possui comprimento n.

O resultado a seguir vai nos garantir a boa definição do comprimento de um módulo.

Teorema 2.2.2. (Jordan-Holder) *Seja M um R-módulo à esquerda que possui uma série de composição (i. é, M tem comprimento finito). Então:*

(i) Toda a cadeia estritamente decrescente de submódulos de M é finita e admite um refinamento que é uma série de composição;

(ii) Duas séries de composição são equivalentes.

Antes de apresentar uma demonstração do Teorema de Jordan-Holder, apresentaremos dois resultados gerais que serão úteis.

Lema 2.2.3. (Lema de Zassenhaus) *Sejam R um anel e M um R-módulo à esquerda. Se $N \subseteq P$ e $N' \subseteq P'$ são submódulos de M, então:*

$$\frac{N + (P \cap P')}{N + (P \cap N')} \simeq \frac{P \cap P'}{(N \cap P') + (N' \cap P)} \simeq \frac{N' + (P' \cap P)}{N' + (P' \cap N)}$$

Demonstração. Vamos mostrar apenas o primeiro isomorfismo e o segundo pode ser mostrado por argumentos idênticos, tendo em vista a simetria entre o primeiro e o terceiro quocientes.

Consideremos a seguinte aplicação:

$$\begin{array}{rccc} \varphi: & N + (P \cap P') & \longrightarrow & \frac{P \cap P'}{(N \cap P') + (N' \cap P)} \\ & n + q & \mapsto & q + [(N \cap P') + (N' \cap P)] \end{array}$$

onde $n \in N$ e $q \in P \cap P'$.

É fácil verificar que φ é um R-homomorfismo. Além disso, dado $q + x$, com $q \in P \cap P'$ e $x = n + n' \in (N \cap P') + (N' \cap P)$, onde $n \in N \cap P'$ e $n' \in N' \cap P$, segue que $n + n' + q \in N + (P \cap P')$, pois $n' \in N' \cap P \subseteq P' \cap P$ (já que $N' \subseteq P'$). Assim, $\varphi(n + (n' + q)) = q + (n + n')$.

Vamos mostrar agora que $\mathcal{N}uc\,\varphi = N + (P \cap N')$. Observamos inicialmente que $N + (P \cap N') \subseteq \mathcal{N}uc\,\varphi$. Por outro lado, se $n \in N$ e $q \in P \cap P'$, são tais que $\varphi(n + q) \in (N \cap P') + (N' \cap P)$, então $q \in (N \cap P') + (N' \cap P)$, ou seja, $q = q_1 + q_2$, com $q_1 \in N \cap P'$ e $q_2 \in N' \cap P$. Assim, $n + q = n + q_1 + q_2$, com $n + q_1 \in N$ e $q_2 \in P \cap P'$, ou seja, $N + (P \cap N') \subseteq \mathcal{N}uc\,\varphi$. Isto mostra que φ é um isomorfismo como queríamos mostrar. □

Lema 2.2.4. (Lema do refinamento de Schreirer) *Sejam $\mathcal{C}$ e $\mathcal{C}'$ duas cadeias estritamente decrescentes de R-submódulos de M. Então existem refinamentos $\mathcal{C}_1$ de $\mathcal{C}$ e $\mathcal{C}'_1$ de $\mathcal{C}'$, os quais são equivalentes.*

Demonstração. Consideremos as seguintes cadeias estritamente decrescentes de R-submódulos de M:

$$\mathcal{C} : M = M_0 \supset M_1 \supset M_2 \cdots \supset M_r = 0$$

e

$$\mathcal{C}' : M = M'_0 \supset M'_1 \supset M'_2 \cdots \supset M'_s = 0.$$

Agora, para cada $i \in \{1, 2, ..., r\}$ e $j \in \{1, 2, ..., s\}$, definimos os R-módulos

$$M_{i,j} := M_i + (M_{i-1} \cap M'_j) \supseteq M_i \quad \text{e} \quad M'_{j,i} := M'_j + (M'_{j-1} \cap M_i) \supseteq M_j$$

e consideremos as seguintes cadeias decrescentes de R-submódulos de M (agora possivelmente não mais estritamente decrescentes):

$$\overline{\mathcal{C}_1} := M \supseteq M_{1,1} \supseteq \cdots \supseteq M_{1,s} = M_1 \supseteq M_{2,1} \supseteq \cdots \supseteq M_{2,s} = M_2 \supseteq \cdots \supseteq M_{r,s} = 0$$

e

$$\overline{\mathcal{C}'_1} := M \supseteq M'_{1,1} \supseteq \cdots \supseteq M'_{1,s} = M'_1 \supseteq M'_{2,1} \supseteq \cdots \supseteq M'_{2,r} = M'_2 \supseteq \cdots \supseteq M_{s,r} = 0.$$

Desta forma, temos $\mathcal{C} \subseteq \overline{\mathcal{C}_1}$ e $\mathcal{C}' \subseteq \overline{\mathcal{C}'_1}$. Segue então do Lema de Zassenhaus que

$$\frac{M_{i,j-1}}{M_{i,j}} = \frac{M_i + (M_{i-1} \cap M'_{j-1})}{M_i + (M_{i-1} \cap M'_j)} \simeq \frac{M'_j + (M'_{j-1} \cap M_{i-1})}{M'_j + (M'_{j-1} \cap M_i)} = \frac{M'_{j,i-1}}{M'_{j,i}}$$

de onde segue que

$$M_{i,j-1} = M_{i,j} \text{ se, e somente se, } M'_{j,i-1} = M'_{j,i}.$$

Portanto, a cadeia estritamente decrescente $\mathcal{C}_1$ obtida de $\overline{\mathcal{C}_1}$, eliminando-se todos os módulos que são iguais aos seus antecessores, é equivalente a cadeia $\mathcal{C}'_1$ obtida de $\overline{\mathcal{C}'_1}$ da mesma forma. Isto completa a demonstração do Lema. □

Estamos agora em condições de demonstrarmos o Teorema de Jordan-Holder.

Demonstração do teorema de Jordan-Holder. Seja M um R-módulo à esquerda que possui uma série de composição.

(i) Sejam $\mathcal{C}$ uma série de composição de M e $\mathcal{C}'$ uma cadeia estritamente decrescente de R-submódulos de M. Então, pelo Lema do refinamento, para toda subcadeia finita $\mathcal{C}'_0$ de $\mathcal{C}'$, existem refinamentos $\mathcal{C}'_1$ de $\mathcal{C}'_0$ e $\mathcal{C}_1$ de $\mathcal{C}$ (i. é, tais que $\mathcal{C}'_0 \subseteq \mathcal{C}'_1$ e $\mathcal{C} \subseteq \mathcal{C}_1$) de modo que $\mathcal{C}'_1$ e $\mathcal{C}_1$ são equivalentes. Visto que $\mathcal{C}$ é uma série de composição, segue que $\mathcal{C}_1 = \mathcal{C}$, ou seja, $\mathcal{C}'_0$ pode ser refinada até $\mathcal{C}$. Portanto, $\mathcal{C}'$ é uma cadeia estritamente decrescente tal que toda subcadeia finita pode ser refinada até $\mathcal{C}$. Logo, $\mathcal{C}'$ deve ser finita.

(ii) Segue diretamente do Lema do refinamento. □

Os resultados acima nos dizem então que o comprimento de um módulo está bem definido, e os próximos vão nos mostrar uma certa analogia entre o comprimento de um módulo e a dimensão de um espaço vetorial.

Proposição 2.2.5. *Sejam R um anel, M um R-módulo à esquerda e N um R-submódulo de M. Então, $\ell(M) < \infty$ se, e somente se, $\ell(N), \ell(M/N) < \infty$. Neste caso, temos $\ell(M) = \ell(N) + \ell(M/N)$.*

Demonstração. ($\Rightarrow$) Se $N = 0$ ou $N = M$, não há nada a mostrar. Suponhamos então que N é um submódulo próprio de M. Consideremos a cadeia $0 \subset N \subset M$. Pelos resultados anteriores, esta cadeia pode ser refinada a uma série de composição, digamos

$$0 = N_0 \subset \cdots \subset N_n = N = M_0 \subset \cdots \subset M_m = M,$$

de onde segue que $\ell(N) = n < \infty$. Tomando $P_i = M_i/N$ $(1 \leq i \leq m)$, obtemos uma cadeia

$$0 = P_0 \subset \cdots \subset P_m = M/N$$

de modo que

$$\frac{P_i}{P_{i-1}} = \frac{M_i/N}{M_{i-1}/N} \simeq \frac{M_i}{M_{i-1}}$$

os quais são módulos simples. Portanto, $\ell(M/N) = m < \infty$ e, consequentemente, $\ell(M) = n + m = \ell(N) + \ell(M/N)$.

($\Leftarrow$) Suponhamos $\ell(N) = n$ e $\ell(M/N) = m$ e consideremos as respectivas séries de composição

$$0 = N_0 \subset N_1 \subset \cdots \subset N_n = N$$

e

$$0 = P_0 \subset P_1 \subset \cdots \subset P_m = M/N.$$

Tomando $M_i = \pi^{-1}(P_i)$, onde $\pi : M \to M/N, (1 \leq i \leq m)$ é a projeção canônica, segue que $P_i = M_i/N$ e

$$\frac{M_i}{M_{i-1}} \simeq \frac{P_i}{P_{i-1}}, \, 1 \leq i \leq m$$

os quais são módulos simples. Portanto,

$$0 = N_0 \subset \cdots \subset N_n = N = M_0 \subset \cdots \subset M_m = M$$

é uma série de composição para M, de onde segue que $\ell(M) = \ell(N) + \ell(M/N) < \infty$. □

Este resultado tem as seguintes consequências interessantes.

Corolário 2.2.6. *Sejam R um anel e M um R-módulo à esquerda com comprimento finito. Então:*

(i) Se M_1, M_2 são submódulos de M, temos

$$\ell(M_1 + M_2) = \ell(M_1) + \ell(M_2) - \ell(M_1 \cap M_2),$$

(ii) Se $\varphi : M \to N$ é um R-homomorfismo, temos

$$\ell(\mathcal{N}uc(\varphi)) + \ell(\mathcal{I}m(\varphi)) = \ell(M),$$

(iii) Se $\varphi : M \to M$ é um R-endomorfismo, temos

$$\varphi \text{ injetora} \iff \varphi \text{ sobrejetora}.$$

Demonstração. (i) Basta observar que $\frac{M_1+M_2}{M_2} \simeq \frac{M_1}{M_1 \cap M_2}$, para obter da Proposição 2.2.6 que

$$\ell(M_1+M_2) = \ell(M_2)+\ell\left(\frac{M_1+M_2}{M_2}\right) \text{ e } \ell(M_1) = \ell(M_1 \cap M_2)+\ell\left(\frac{M_1}{M_1 \cap M_2}\right)$$

de onde segue o resultado.

(ii) Como $\mathcal{I}m(\varphi) \simeq M/\mathcal{N}uc(\varphi)$, segue que $\ell(\mathcal{I}m(\varphi)) < \infty$. Então temos

$$\ell(M) = \ell(\mathcal{N}uc(\varphi)) + \ell(M/\mathcal{N}uc(\varphi)) = \ell(\mathcal{N}uc(\varphi)) + \ell(\mathcal{I}m(\varphi)).$$

(iii) Segue imediatamente dos anteriores. □

Gostaríamos de registrar neste momento, que o comprimento de um módulo não se comporta exatamente igual a dimensão de um espaço vetorial, pois dois $\mathbb{k}$-espaços vetoriais de mesma dimensão são sempre isomorfos, o que nem sempre acontece com módulos de comprimento finito, como mostra o próximo exemplo.

Exemplo 2.2.7. Sejam M um grupo cíclico de quatro elementos e K o grupo de Klein. Então, $\ell(_{\mathbb{Z}}M) = \ell(_{\mathbb{Z}}K)$ (encontre uma série de composição para cada um deles!), mas M e K não são isomorfos como $\mathbb{Z}$-módulos.

Nosso próximo resultado dá uma caracterização para os módulos que possuem uma série de composição.

Teorema 2.2.8. *Sejam R um anel e M um R-módulo à esquerda. Então M tem comprimento finito se, e somente se, toda cadeia estritamente decrescente e toda cadeia estritamente crescente de R-submódulos de M é finita. Em particular, todo R-módulo finito possui comprimento finito.*

Demonstração. $(\Rightarrow)$ Suponhamos $\ell(M) = r$. Se $\mathcal{C} := M = M_0 \supset M_1 \supset \cdots \supset M_k \supset \cdots$ é uma cadeia estritamente decrescente de submódulos de M, segue do Teorema de Jordan-Holder que $\mathcal{C}$ é finita. Suponhamos agora que $0 = N_0 \subset N_1 \subset \cdots \subset N_k \subset \cdots$ é uma cadeia estritamente crescente de submódulos de M. Daí, para cada $t \in \mathbb{N}$, podemos considerar cadeia finita $\mathcal{C}' := M = N_t \supset N_{t-1} \supset \cdots \supset N_0 = 0$, e segue do Teorema de Jordan-Holder que esta cadeia pode ser refinada até uma série de composição que tem comprimento r. Assim, $t \leq r = \ell(M)$, e como t foi tomado arbitrário, devemos ter $\mathcal{C}'$ uma cadeia finita.

$(\Leftarrow)$ Se $M = 0$ não há nada a mostrar. Suponhamos então $M \neq 0$. Escolhemos entre todos os submódulos de M, um submódulo maximal M_1, o qual existe pela hipótese de que todas as cadeias estritamente crescente são finitas. Se $M_1 = 0$, então $M \supset M_1 = 0$ é uma série de composição de M. Se $M_1 \neq 0$, escolhemos um submódulo maximal de M_1, digamos M_2. Se $M_2 = 0$, então $M = M_0 \supset$

$M_1 \supset M_2 = 0$ é uma série de composição de M. Se $M_2 \neq 0$, então continuamos este processo, obtendo a cadeia $M = M_0 \supset M_1 \supset \cdots \supset M_k = 0$, pois toda cadeia estritamente decrescente é finita. Como, para todo $0 \leq j \leq k-1$, o módulo M_j/M_{j+1} é um módulo simples, pela escolha de M_{j+1}, segue que a cadeia acima é uma série de composição de M. □

2.3 Artinianidade e Noetherianidade em anéis e módulos

Começamos esta seção observando que a argumentação usada na demonstração do Teorema 2.2.8 foi a seguinte: Seja X um conjunto parcialmente ordenado por $\preccurlyeq$. Então as seguintes afirmações são equivalentes:

(i) Toda cadeia estritamente crescente (resp. decrescente) em X é finita;

(ii) Toda família não vazia de subconjuntos de X possui um elemento maximal (resp. minimal).

Esta equivalência é uma consequência direta do Lema de Zorn. Estas condições sobre cadeias crescentes e decrescentes em um módulo induzem as seguintes definições.

Definição 2.3.1. Sejam R um anel e M um R-módulo à esquerda. Então, dizemos que:

(i) M é um módulo *artiniano*, se toda cadeia estritamente decrescente de submódulos de M é finita;

(ii) M é um módulo *noetheriano*, se toda cadeia estritamente crescente de submódulos de M é finita.

Também dizemos que um módulo M satisfaz a *condição de cadeia descendente* (do inglês, *DCC*), se toda cadeia decrescente de submódulos de M é estacionária, isto é, se $N_1 \supseteq N_2 \supseteq \cdots \supseteq N_k \supseteq \cdots$ é uma cadeia descendente, então existe $n \in \mathbb{N}$ tal que $N_{n+t} = N_n$, para todo $t \geq 1$. Note que cadeias estritamente decrescentes estacionárias são finitas, de modo que M satisfaz *DCC* se, e somente se, M é artiniano.

Analogamente, dizemos que um módulo M satisfaz a *condição de cadeia ascendente* (do inglês, *ACC*), se toda cadeia crescente de submódulos de M é estacionária, isto é, se $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq \cdots$ é uma cadeia ascendente, então existe $m \in \mathbb{N}$ tal que $N_{m+t} = N_m$, para todo $t \geq 1$. Note que cadeias estritamente crescentes estacionárias são finitas, de modo que M satisfaz *ACC* se, e somente se, M é noetheriano.

Sob a luz destas novas definições, o seguinte resultado é claro.

Corolário 2.3.2. *Seja M um R-módulo à esquerda. Então $\ell(M) < \infty$ se, e somente se, M é artiniano e noetheriano simultaneamente.*

Exemplo 2.3.3. (i) Todo espaço vetorial de dimensão finita sobre um corpo é um módulo artiniano e noetheriano, visto que possuem comprimento finito, como já observamos anteriormente.

(ii) $\mathbb{Z}$, como um $\mathbb{Z}$-módulo, é noetheriano mas não é artiniano.

Observe que os $\mathbb{Z}$-submódulos de $\mathbb{Z}$ são os seus ideais, os quais tem a forma $n\mathbb{Z}$, como vimos antes. Assim, a cadeia estritamente decrescente $2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots \supset 2^n\mathbb{Z} \supset \cdots$ não é finita. Por outro lado, $n\mathbb{Z} \subseteq m\mathbb{Z}$ se, e somente se, m divide n. Assim, como o conjunto de divisores de um inteiro é finito, segue que toda cadeia ascendente de submódulos de $\mathbb{Z}$ é estacionária.

Com o objetivo de poder apresentar novos exemplos, vamos discutir um pouco mais estas condições de cadeia. Começamos com o seguinte resultado.

Proposição 2.3.4. *Um R-módulo à esquerda M é noetheriano se, e somente se, todo submódulo de M é finitamente gerado. Em particular, todo módulo noetheriano é finitamente gerado.*

Demonstração. ($\Rightarrow$) Suponhamos M noetheriano e seja N um submódulo de M. Consideremos a família $\mathcal{F}$ de todos os submódulos finitamente gerados de N. Assim, $\mathcal{F} \neq \emptyset$, pois $0 \in \mathcal{F}$. Como M é noetheriano, segue que $\mathcal{F}$ tem elemento maximal, digamos L. Se $L \neq N$, então existe um elemento $x \in N \setminus L$, e podemos então considerar o R-submódulo $L + Rx$, o qual é finitamente gerado, de onde segue que $L + Rx \in \mathcal{F}$, o que contradiz a maximalidade de L, pois claramente $L \subsetneq L + Rx$. Portanto, $L = N$ e segue que N é finitamente gerado, como queríamos mostrar.

($\Leftarrow$) Seja $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq \cdots$ uma cadeia crescente de submódulos de M. Consideremos $N = \cup_{i\in\mathbb{N}} N_i$. Como N é um submódulo de M, segue que N é finitamente gerado por hipótese, digamos $N = Rx_1 + Rx_2 + \cdots + Rx_t$. Mas então, existe um índice $j \in \mathbb{N}$ tal que $x_1, x_2, ..., x_t \in N_j$ e, consequentemente, $N_j = N_{j+1} = \cdots = N_{j+k} = \cdots$ e, portanto, M é noetheriano. □

Segue então do resultado acima que o módulo regular de todo domínio de ideais principais é noetheriano.

Exemplo 2.3.5. Seja p um número primo (positivo) e consideremos $\mathbb{Z}_{(p)} := \{\frac{a}{p^m} : a \in \mathbb{Z} \text{ e } m \in \mathbb{N}\}$. Então $\mathbb{Z}_{(p)}$ é um grupo abeliano aditivo e, portanto, um $\mathbb{Z}$-módulo. Consideremos agora o $\mathbb{Z}$-módulo $M = \mathbb{Z}_{(p)}/\mathbb{Z}$. Afirmamos que M é artiniano e não é noetheriano.

Para ver que M não é noetheriano, primeiro consideramos a cadeia estritamente crescente

$$\mathbb{Z} \subsetneq \frac{1}{p}\mathbb{Z} \subsetneq \frac{1}{p^2}\mathbb{Z} \subsetneq \cdots$$

que não é estacionária, como é fácil ver. Então, a cadeia induzida no módulo quociente $M = \mathbb{Z}_{(p)}/\mathbb{Z}$ também não será estacionária.

Agora vamos mostrar que M é artiniano. Para tanto, vamos mostrar que todo submódulo próprio de M é finito. Começamos por observar que se N é um submódulo próprio de M e $\frac{a}{p^m} + \mathbb{Z} \in N$, com $mdc(a, p) = 1$, então $\frac{b}{p^n} + \mathbb{Z} \in N$, para todo $b \in \mathbb{Z}$ e todo $n \leq m$. De fato, pois neste caso, existem $r, s \in \mathbb{Z}$ tais que $ra + sp^m = 1$, de onde segue que

$$b = b1 = b(ra + sp^m) = bra + bsp^m, \forall b \in \mathbb{Z}$$

e, se $n \leq m$, então segue que

$$\frac{b}{p^n} = \frac{bra}{p^n} + \frac{bsp^m}{p^n} = (p^{m-n})\frac{bra}{p^m} + p^{m-n}bs$$

e como esta última parcela está em $\mathbb{Z}$, quando passamos ao quociente, obtemos

$$\frac{b}{p^n} + \mathbb{Z} = (p^{m-n})br\left(\frac{a}{p^m} + \mathbb{Z}\right) \in N.$$

Agora, como N é um submódulo próprio de M, deve existir um número natural t_N tal que

$$N = \left\{\frac{a}{p^m} + \mathbb{Z} : a \in \mathbb{Z} \text{ e } m \leq t_N\right\}.$$

Assim, como existem apenas um número finito de classes de equivalência da forma $\frac{a}{p^m} + \mathbb{Z}$, com $m \leq t_N$, segue que N é finito, como queríamos mostrar.

O próximo exemplo mostra que um módulo pode não ser artiniano e nem noetheriano.

Exemplo 2.3.6. Sejam R um anel e $\{M_i\}_{i\in I}$ uma família de R-módulos à esquerda não nulos, onde I é um conjunto infinito. Então $M = \oplus_{i\in I} M_i$ não é nem artiniano e nem noetheriano.

Para ver que M não é noetheriano, basta considerar a família $\{J_n\}_{n\in\mathbb{N}}$ de subconjuntos de I, tais que $J_n \subsetneq J_m$, sempre que $n < m$. Assim, podemos construir a cadeia estritamente crescente $P_1 \subset P_2 \subset \cdots \subset P_k \subset \cdots$, onde $P_k = \oplus_{i\in J_k} M_i$, a qual é infinita.

Para o caso da artianidade de M, basta construir a família $\{K_n\}_{n\in\mathbb{N}}$, definida por:

- $K_0 = I$;
- $K_1 = I \setminus \{i_1\}$, onde $i_1 \in I$;
- $K_2 = I \setminus \{i_1, i_2\}$, onde $i_2 \in I \setminus \{i_1\}$;
- e assim sucessivamente.

Então é fácil verificar que a cadeia $Q_0 \supset Q_1 \supset \cdots \supset Q_k \supset \cdots$, onde $Q_t = \oplus_{i\in K_t} M_i$, é infinita. Portanto, M também não é artiniano.

O próximo resultado é útil quando se quer mostrar a artinianidade ou a noetherianidade de um módulo.

Proposição 2.3.7. *Seja* $0 \to M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \to 0$ *uma sequência exata curta de* R*-módulos à esquerda. Então,* M *é noetheriano (resp. artiniano) se, e somente se,* M_1 *e* M_2 *são noetherianos (resp. artinianos).*

Demonstração. Vamos apresentar uma demostração para o caso noetheriano. O caso artiniano pode ser demonstrado de forma completamente análoga. Suponhamos então que M seja noetheriano e consideremos as cadeias $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq \cdots$ e $L_1 \subseteq L_2 \subseteq \cdots \subseteq L_k \subseteq \cdots$ de R-submódulos de M_1 e M_2, respectivamente. Desta forma, $f(N_1) \subseteq f(N_2) \subseteq \cdots \subseteq f(N_k) \subseteq \cdots$ e $g^{-1}(L_1) \subseteq g^{-1}(L_2) \subseteq \cdots \subseteq g^{-1}(L_k) \subseteq \cdots$ são cadeias crescentes de R-submódulos de M. Da noetherianidade de M segue que existe um índice $n \in \mathbb{N}$ talque $f(N_n) = f(N_{n+j})$ e $g^{-1}(L_n) = g^1(L_{n+j})$, para todo $j \geq 1$. Do fato que f é injetora, segue que $N_n = N_{n+j}$, para todo $j \geq 1$. Do fato que g é sobrejetora, segue que $L_n = L_{n+j}$, para todo $j \geq 1$. Portanto, M_1 e M_2 são noetherianos.

Reciprocamente, suponhamos que ambos M_1 e M_2 sejam noetherianos. Consideremos uma cadeia $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_k \subseteq \cdots$ de R-submódulos de M. Esta cadeia induz as seguintes cadeias

$$f^{-1}(P_1) \subseteq f^{-1}(P_2) \subseteq \cdots \subseteq f^{-1}(P_k) \subseteq \cdots, \text{ em } M_1$$

e

$$g(P_1) \subseteq g(P_2) \subseteq \cdots \subseteq g(P_k) \subseteq \cdots, \text{ em } M_2$$

Assim, da noetherianidade de M_1 e de M_2, segue que existem índices n_1 e n_2 tais que $f^{-1}(P_{n_1}) = f^{-1}(P_{n_1+j})$ e $g(P_{n_2}) = g(P_{n_2+j})$, para todo $j > 0$. Tomando $n = max\{n_1, n_2\}$, obtemos que $f^{-1}(P_n) = f^{-1}(P_{n+j})$ e $g(P_n) = g(P_{n+j})$, para todo $j > 0$.

Agora, dado $j > 0$, escolhemos $x \in P_{n+j}$. Assim, $g(x) \in g(P_n)$, isto é, existe $y \in P_n$ talque $g(x) = g(y)$, de modo que $y - x \in \mathcal{N}uc\, g = \mathcal{I}m\, f$. Logo, existe $z \in f^{-1}(P_{n+j})$ tal que $f(z) = y - x$. Como f é injetora e $f^{-1}(P_n) = f^{-1}(P_{n+j})$, segue que $f(z) = y - x \in P_n$, de onde segue que $x = y - f(z) \in P_n$, ou seja, $P_{n+j} = P_n$, para todo $j > 0$. Isto mostra que M é noetheriano. □

Este resultado tem as seguintes consequências importantes.

Corolário 2.3.8. *Sejam* R *um anel,* M *um* R*-módulo à esquerda e* N *um* R*-submódulo de* M*. Então* M *é noetheriano (resp. artiniano) se, e somente se,* N *e* M/N *são noetherianos (resp. artinianos).*

Para a demonstração deste corolário, basta considerar a sequência exata curta $0 \to N \hookrightarrow M \to M/N \to 0$ e aplicar o resultado acima.

O próximo resultado é uma consequência direta dos anteriores, e mostra que uma soma direta finita de módulos noetherianos (resp., artinianos) é um módulo noetherianos (resp., artiniano).

Corolário 2.3.9. *Sejam* R *um anel e* $M_1, M_2, ..., M_r$ R*-módulos à esquerda noetherianos (resp. artinianos). Então* $M = \oplus_{i=1}^{r} M_i$ *é noetheriano (resp. artiniano).*

Estas propriedades de artinianidade e noetherianidade podem ser transferidas para anéis, de modo natural, bastando considerar os módulos regulares ${}_RR$ e R_R. Desta forma, temos o seguinte.

Definição 2.3.10. Seja R um anel. Então dizemos que R é um:

- *anel artiniano à esquerda* (resp. à direita), se o módulo regular ${}_RR$ (resp. R_R) é artiniano;
- *anel noetheriano à esquerda* (resp. à direita), se o módulo regular ${}_RR$ (resp. R_R) é noetheriano;
- *anel artiniano* (resp. noetheriano) se R é artiniano (resp. noetheriano) à esquerda e à direita, simultaneamente.

Finalizaremos esta seção apresentando alguns exemplos de tais anéis. Estes exemplos também mostram que a estrutura dos módulos regulares de um anel podem ser muito distintas.

Exemplo 2.3.11. Considere $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a \in \mathbb{Z}, b, c \in \mathbb{Q} \right\}$. Então R é um anel noetheriano à direita que não é noetheriano à esquerda.

Começamos observando que se $n \in \mathbb{Z}$ e $I_n = \left\{ \begin{bmatrix} 0 & \frac{m}{2^n} \\ 0 & 0 \end{bmatrix} : m \in \mathbb{Z} \right\}$, então $I_n \lhd_l R$ (verifique!). Portanto, a cadeia

$$I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

não é estacionária, ou seja, R não é noetheriano à esquerda.

Vamos verificar agora que R é noetherano à direita, mostrando que todo ideal à direita de R é finitamente gerado. Consideremos então $I \lhd_r R$. Vamos dividir nossa argumentação em casos.

Caso 1. $\forall X = (a_{ij}) \in I$, *temos* $a_{11} = 0$.

Dado $X = \begin{bmatrix} 0 & y \\ 0 & z \end{bmatrix}$, segue que para todo $c \in \mathbb{Q}$, $\begin{bmatrix} 0 & cy \\ 0 & cz \end{bmatrix} \in I$, pois

$$\begin{bmatrix} 0 & y \\ 0 & z \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & c \end{bmatrix} = \begin{bmatrix} 0 & cy \\ 0 & cz \end{bmatrix},$$

de onde obtemos que I é isomorfo a um $\mathbb{Q}$-espaço vetorial.

Mas agora, se $V = \left\{ (y, z) \in \mathbb{Q}^2 : \begin{bmatrix} 0 & y \\ 0 & z \end{bmatrix} \in I \right\}$ é um subespaço de $\mathbb{Q}^2$ sobre $\mathbb{Q}$, então existem vetores $v_1 = (y_1, z_1)$ e $v_2 = (y_2, z_2)$ em V (não necessariamente L. I.), tais que $V =< v_1, v_2 >$. Assim, $(y, z) = \alpha_1(y_1, z_1) + \alpha_2(y_2, z_2) = (\alpha_1 y_1 + \alpha_2 y_2, \alpha_1 z_1 + \alpha_2 z_2)$, para certos elementos $\alpha_1, \alpha_2 \in \mathbb{Q}$. Portanto,

$$\begin{bmatrix} 0 & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} 0 & y_1 \\ 0 & z_1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & \alpha_1 \end{bmatrix} + \begin{bmatrix} 0 & y_2 \\ 0 & z_2 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & \alpha_2 \end{bmatrix}$$

e segue que I é finitamente gerado neste caso.

Caso 2. $\exists X = (a_{ij}) \in I$, *com* $a_{11} \neq 0$.

Seja n o menor inteiro positivo que aparece na primeira entrada de alguma matriz em I. Assim, todo elemento de I pode ser escrito da forma

$$\begin{bmatrix} nk & y \\ 0 & z \end{bmatrix}, \text{ com } k \in \mathbb{Z} \text{ e } y, z \in \mathbb{Q}$$

Pela definição de n, existem $b, c \in \mathbb{Q}$ tais que $\begin{bmatrix} n & b \\ 0 & c \end{bmatrix} \in I$, de onde segue que

$$\begin{bmatrix} n & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} n & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I.$$

Vamos dividir nossa argumentação em outros dois subcasos.

subcaso 2.1 *Para toda matriz* $X = (a_{ij}) \in I$ *temos* $a_{22} = 0$.

Neste caso, se $X \in I$, segue que $X = \begin{bmatrix} kn & y \\ 0 & 0 \end{bmatrix}$, para algum $k \in \mathbb{Z}$ e $y \in \mathbb{Q}$. Mas então, temos

$$\begin{bmatrix} kn & y \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} n & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} k & \frac{y}{n} \\ 0 & 0 \end{bmatrix}$$

e segue que $\begin{bmatrix} n & 0 \\ 0 & 0 \end{bmatrix}$ gera I como ideal à direita de R.

Subcaso 2.2 *Existe uma matriz* $X = (a_{ij}) \in I$ *com* $a_{22} \neq 0$.

Neste caso, consideremos $X = \begin{bmatrix} kn & y_1 \\ 0 & z_1 \end{bmatrix} \in I$, onde $k \in \mathbb{Z}, y_1, z_1 \in \mathbb{Q}$ e $z_1 \neq 0$. Como $\begin{bmatrix} n & 0 \\ 0 & 0 \end{bmatrix} \in I$, segue que

$$\begin{bmatrix} kn & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} n & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} k & 0 \\ 0 & 0 \end{bmatrix} \in I$$

e também que

$$\begin{bmatrix} 0 & y_1 \\ 0 & z_1 \end{bmatrix} = \begin{bmatrix} kn & y_1 \\ 0 & z_1 \end{bmatrix} - \begin{bmatrix} kn & 0 \\ 0 & 0 \end{bmatrix} \in I$$

e, assim, temos

$$\begin{bmatrix} n & y_1 \\ 0 & z_1 \end{bmatrix} = \begin{bmatrix} kn & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & y_1 \\ 0 & z_1 \end{bmatrix} \in I.$$

Tomando então um elemento qualquer $\begin{bmatrix} rn & y \\ 0 & z \end{bmatrix} \in I$, segue que

$$\begin{bmatrix} rn & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} n & y_1 \\ 0 & z_1 \end{bmatrix} \begin{bmatrix} r & \frac{1}{n}\left(y - \frac{y_1 z}{z_1}\right) \\ 0 & \frac{z}{z_1} \end{bmatrix}$$

de onde segue que I é gerado por $\begin{bmatrix} n & y_1 \\ 0 & z_1 \end{bmatrix}$, como ideal à direita de R.

Portanto, em qualquer caso, todo ideal à direita de R é finitamente gerado, o que mostra que R é noetheriano à direita.

Modificando um pouco o exemplo anterior, podemos construir um anel artiniano à direita que não é artiniano à esquerda. Os cálculos serão deixados ao leitor.

Exemplo 2.3.12. Seja $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a \in \mathbb{Q}; b, c \in \mathbb{R} \right\}$. Então R é artiniano à direita mas não é artiniano à esquerda.

Exercícios

1. Seja R um anel que satisfaz a condição descendente de cadeia para ideais à esquerda principais. Mostre que R possui um ideal à esquerda minimal.

2. Sejam R um domínio de integridade e $a \in R$. Mostre que se

   $$< a^t > = < a^{t+1} >,$$

   para algum inteiro positivo t, então a é invertível. Conclua daí que todo domínio de integridade artiniano é um corpo.

3. Mostre que se M é um R-módulo à esquerda noetheriano, então todo R-epimorfismo de M é na verdade um R-isomorfismo.

4. Mostre que $A \supset < x > \supset < x^2 > \supset 0$ é uma série de composição para o A-módulo regular $A = \frac{\mathbb{k}[x]}{<x^3>}$.

5. Sejam R um anel e $M_1, M_2, ..., M_n$ R-módulos à esquerda. Mostre que

   $$\ell(M) = \sum_{i=1}^{n} \ell(M_i).$$

Capítulo 3

Semissimplicidade

Começamos este capítulo apresentando noções gerais sobre a semissimplicidade em anéis e módulos, para então apresentar o chamado Teorema de Wedderburn-Artin, o qual classifica os anéis artinianos semissimples. Alguns exemplos são dados no decorrer do texto e finalizamos com um exemplo clássico de um anel semissimples que não é artiniano.

Como dito no início destas notas, os módulos são uma generalização de espaços vetoriais. Então nada mais natural do que estudar os análogos a certos invariantes ou de certas propriedades importantes dos espaços vetoriais, na teoria dos módulos. Fizemos isto na seção anterior, estudando o conceito de comprimento de um módulo, que vem a ser um análogo a dimensão de um espaço vetorial. Uma propriedade fundamental dos espaços vetoriais é o fato que todo subespaço é um somando direto do espaço que o contém. Neste capítulo pretendemos estudar os módulos que possuem esta mesma propriedade, ou seja, os módulos cujos seus submódulos são somandos diretos. Faremos isto através do conceito de semissimplicidade.

3.1 Noções Gerais

A ideia de uma estrutura simples já apareceu neste texto. Vamos lembrar algumas coisas que já foram ditas anteriormente e introduzir conceitos novos. Iniciamos com as seguintes definições básicas.

Definição 3.1.1. Sejam R um anel e M um R-módulo à esquerda. Dizemos que M é um módulo:

- *simples*, se $M \neq 0$ e os únicos submódulos de M são os triviais, a saber, 0 e M;
- *semissimples*, se todo R-submódulo de M é um somando direto de M.

Muitas vezes na literatura o termo *módulo irredutível* aparece como sinônimo de módulo simples e o termo *módulo completamente redutível*, como sinônimo de

módulo semissimples. Antes de apresentarmos alguns exemplos, vamos relembrar uma caracterização de módulo simples.

Proposição 3.1.2. *Sejam R um anel e M um R-módulo à esquerda. Então as seguintes afirmações são equivalentes:*

(i) M *é simples;*

(ii) M *é cíclico e gerado por qualquer de seus elementos não nulos;*

(iii) $M \simeq M/I$*, para algum ideal à esquerda maximal* I *de* R*.*

Passamos agora a apresentar alguns exemplos de módulos simples e semissimples.

Exemplo 3.1.3. Os $\mathbb{Z}$-módulos simples são isomorfos a $\mathbb{Z}/p\mathbb{Z}$, onde p é um número primo.

Exemplo 3.1.4. Todo ideal minimal de um anel R é um módulo simples.

Exemplo 3.1.5. Sejam $\Bbbk$ um corpo (ou um anel de divisão) e V um $\Bbbk$-espaço vetorial. Consideremos $S = End_{\Bbbk}(V)$ o anel das transformações lineares de V em V. Então V se torna um S-módulo à esquerda via a seguinte ação de S: $f \cdot v = f(v),\ \forall f \in S, v \in V$. Afirmamos que V é um S-módulo simples.

De fato, pois se fixamos $v \in V \setminus \{0\}$ e tomamos arbitrariamente $u \in V$, então existe $f \in S$ tal que $f(v) = u$, ou seja, $V = Su$ é um módulo cíclico gerado por qualquer um de seus elementos não nulos. O resultado segue então da Proposição 3.1.2.

Exemplo 3.1.6. Todo módulo simples é semissimples, mas o módulo nulo é semissimples e não é simples.

Exemplo 3.1.7. Se $\Bbbk$ é um corpo ou um anel de divisão, então todo $\Bbbk$-espaço vetorial é um módulo semissimples.

De fato, pois se W é um subespaço de V, então, tomando uma base de W e completando a uma base de V, podemos verificar facilmente que W é um somando direto de V.

Antes do próximo exemplo, vamos introduzir um conceito novo.

Definição 3.1.8. Sejam R um anel e M um R-módulo à esquerda. Dizemos que M é *indecomponível*, se $M \neq 0$ e M não pode ser escrito como uma soma direta de quaisquer de seus submódulos, isto é, se $M = N \oplus L$, então $N = 0$ ou $L = 0$.

Se $\Bbbk$ é um corpo ou um anel de divisão, então um $\Bbbk$-espaço vetorial V é indecomponível se, e somente se, V é unidimensional. Assim, os conceitos de módulo simples e módulo indecomponível coincidem sobre espaços vetoriais, mas não é sempre assim, quando trabalhamos com módulos. De fato, todo módulo simples é

indecomponível, mas a recíproca não vale: $\mathbb{Z}$ é um $\mathbb{Z}$-módulo indecomponível que não é simples, pois os seus $\mathbb{Z}$-submódulos são da forma $n\mathbb{Z}$, para $n \in \mathbb{Z}$. Mas se $m, n \in \mathbb{Z}$, então $n\mathbb{Z} \cap m\mathbb{Z} = mdc(m, n)\mathbb{Z}$. Como todo módulo indecomponível que não é simples não pode ser semissimples, o próximo exemplo é imediato.

Exemplo 3.1.9. $\mathbb{Z}$, visto como um módulo sobre si mesmo, não é semissimples.

Na sequência, apresentaremos alguns resultados fundamentais que serão úteis para se obter caracterizações da semissimplicidade. Começamos por observar que segue diretamente da definição, que todo módulo quociente e todo submódulo de um módulo semissimples é também semissimples.

Lema 3.1.10. *Todo módulo semissimples contém um submódulo simples.*

Demonstração. Sejam R um anel e M um R-módulo à esquerda semissimples (logo, $M \neq 0$). Consideremos $m \in M$, $m \neq 0$. Como Rm é um submódulo de M, basta mostrarmos que Rm contém um submódulo simples. Para tanto, consideremos a família $\mathcal{F}$ de todos os submódulos de Rm que não contém m, a qual é não vazia, pois $0 \in \mathcal{F}$. Aplicando agora o Lema de Zorn, obtemos que existe um elemento maximal em $\mathcal{F}$, digamos N. Da observação feita antes do enunciado deste lema, segue que $Rm = N \oplus N'$. Vamos mostrar que N' é um módulo simples. Inicialmente, observamos que $N' \neq 0$, pois $m = n + n'$, com $n \in N$ e $n' \in N'$, e como $m \notin N$, segue que $n' \neq 0$. Além disso, se $0 \neq N''$ é um submódulo de N', então devemos ter $N' = N'' \oplus P$, para algum submódulo P de N'. Agora, pela maximalidade de N, devemos ter $m \in N \oplus N''$, de modo que $N \oplus N'' = Rm$. Mas então,

$$N \oplus N'' = Rm = N \oplus N' = N \oplus (N'' \oplus P)$$

de onde segue que $P = 0$, uma vez que $m \in N \oplus N''$. Portanto, $N'' = N'$ e temos que N' é simples, como queríamos mostrar. □

Para apresentarmos o nosso próximo resultado, o qual dá uma caracterização dos módulos semissimples, vamos convencionar que a soma (direta ou não) de uma família vazia de submódulos é igual ao módulo nulo. Esta convenção é útil para que nossa argumentação seja válida inclusive no caso em que $M = 0$.

Teorema 3.1.11. *Sejam R um anel e M um R-módulo à esquerda. As seguintes afirmações são equivalentes:*

(i) *M é semissimples;*

(ii) *M é uma soma de uma família de submódulos simples;*

(iii) *M é uma soma direta de uma família de submódulos simples.*

Demonstração. Se $M = 0$, não há nada a mostrar, pelas nossas convenções assumidas antes. Portanto, em toda a demostração, vamos supor $M \neq 0$.

$(i) \Rightarrow (ii)$ Seja $N = \sum_{i\in I} S_i$, onde $\{S_i\}_{i\in I}$ é a família de todos os R-submódulos simples de M, a qual não é vazia pelo Lema anterior, ou seja, $N \neq 0$. Assim, deve existir um submódulo P de M tal que $M = N \oplus P$. Se ocorrer que $P \neq 0$, então, pelo Lema anterior, existe T submódulo simples de P, já que P deve ser semissimples, por ser submódulo de um módulo semissimples. Mas então, $P \cap N = 0$, uma contradição. Portanto, só podemos ter $P = 0$ e, consequentemente, $M = N$. Isto mostra que M é uma soma de submódulos simples.

$(ii) \Rightarrow (iii)$ Suponhamos que $M = \sum_{i\in I} S_i$, onde $\{S_i\}_{i\in I}$ é uma família de submódulos simples de M. Consideremos a família $\mathcal{F} := \{J \subseteq I : \sum_{j\in J} M_j \text{ é uma soma direta }\}$. Pelas nossas convenções, $\mathcal{F} \neq \emptyset$. Como toda cadeia em $\mathcal{F}$ possui uma cota superior em $\mathcal{F}$ (a saber, a união de seus membros), segue do Lema de Zorn que existe $I' \in \mathcal{F}$ um elemento maximal. Seja $M' = \oplus M_{j\in I'}$. Afirmamos que $M' = M$. De fato, pois para cada $i \in I$, M_i é um módulo simples, de onde decorre que $M_i \cap M' = M_i$ ou $M_i \cap M' = 0$. Se ocorrer a segunda condição, então $I' \cup \{i\} \supsetneq I'$, o que contradiz a maximalidade de I'. Portanto, $M_i \subseteq M'$, para todo $i \in I$, ou seja, $M = M'$, como queríamos mostrar.

$(iii) \Rightarrow (i)$ Suponhamos que M seja uma soma direta de submódulos simples, digamos $M = \oplus_{i\in I} M_i$, onde M_i é um módulo simples, para todo $i \in I$. Seja N um submódulo de M. Usando a mesma argumentação acima, $N \cap M_i = M_i$ ou $N \cap M_i = 0$. Então é fácil verificar que $N = \oplus_{j\in J} M_j$, onde $J = \{i \in I : M_i \cap N = M_i\}$. Portanto, como $M = (\oplus_{j\in J} M_j) \oplus (\oplus_{j\in I\setminus J} M_j) = N \oplus K$, onde $K = \oplus_{j\in I\setminus J} M_j$, e segue que M e semissimples. □

Observamos que na prova de $(ii) \Rightarrow (iii)$, de fato mostramos que toda soma de submódulos simples é uma soma direta. Na sequência, vamos transportar o conceito de semissimplicidade de módulos para anéis, via o módulo regular. Mais precisamente, temos a seguinte definição.

Definição 3.1.12. Seja R um anel. Dizemos que R é um anel semissimples à esquerda (resp. à direita), se o módulo regular ${}_RR$ (resp. R_R) é semissimples.

Mais adiante vamos mostrar que o conceito de semissimplicidade para anéis é simétrico, isto é, um anel é semissimples à esquerda se, e somente se, é semissimples à direita. Isto nos permite falar em anéis semissimples, sem usar nenhum adjetivo de lateralidade. Antecipando-nos a este fato, passaremos a escrever que R é um anel semissimples, sem especificar lateralidade, independentemente de qual dos módulos regulares estamos considerando no momento.

Suponhamos agora que R é um anel semissimples (à esquerda), então $R = \oplus_{j\in J} I_j$, onde I_j é um ideal à esquerda simples, para todo $j \in J$. Como estamos supondo que R tem unidade, então devemos ter $1_R = \sum_{j=1}^{n} a_j$, onde $a_j \in I_j$, $1 \leq j \leq n$. Segue dai que se $r \in R$, então $r = r1 = r\sum_{j=1}^{n} a_j = \sum_{j=1}^{n} ra_j \in \sum_{j=1}^{n} I_j$, de onde segue que $R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$, onde cada I_j $(1 \leq j \leq n)$ é um

ideal à esquerda minimal de R. Esta argumentação mostra que todo anel semissimples possui uma série de composição (à esquerda), e portanto, se R é semissimples (à esquerda), então R é artiniano à esquerda e noetheriano à esquerda. Assim, o seguinte resultado é claro.

Proposição 3.1.13. *Todo anel semissimples é simultaneamente artiniano e noetheriano (à esquerda e à direita).*

Vamos apresentar agora alguns exemplos.

Exemplo 3.1.14. Se D é um anel de divisão, então $R = \mathcal{M}_n(D)$ é um anel simples, como já sabemos. Além disso, o módulo regular ${}_RR$ é semissimples, de onde segue que R é um anel semisimples.

De fato, pois $I_k := \{(a_{ij}) : a_{ij} = 0, \text{ se } j \neq k\}$ (conjunto de todas matrizes com entradas não nulas somente na k-ésima coluna) é um ideal à esquerda minimal de R, como já visto antes, logo um submódulo à esquerda simples de ${}_RR$. Como ${}_RR = I_1 \oplus I_2 \oplus \cdots \oplus I_n$, segue que R é um anel semissimples à esquerda. Analogamente, usando ideais à direita da forma $I_k := \{(a_{ij}) : a_{ij} = 0, \text{ se } i \neq k\}$, concluimos da mesma forma que R_R é semissimples, ou seja, R é um anel semissimples também à direita. Este é o fato que será usado mais adiante para mostrarmos que um anel R é semissimples à esquerda se, e somente se, R é um anel semissimples à direita.

O próximo exemplo é fundamental e mostra como podemos fabricar mais exemplos de anéis semissimples.

Exemplo 3.1.15. Suponhamos que $R_1, R_2, \ldots, R_t$ são anéis semissimples. Então $R = R_1 \times R_2 \times \cdots \times R_t$ é um anel semissimples.

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

$$ {}_RR = \oplus_{i=1}^{t} R_i = \oplus_{i=1}^{t} (\oplus_{l=1}^{n_i} I_l) $$

e segue que ${}_RR$ é um módulo semissimples, ou seja, R é um anel semissimples, como queríamos mostrar.

Como uma consequência dos dois exemplos acima, temos o seguinte.

Exemplo 3.1.16. Sejam $D_1, D_2, ..., D_r$ anéis de divisão. Então

$$ R := \mathcal{M}_{n_1}(D_1) \times \mathcal{M}_{n_2}(D_2) \times \cdots \times \mathcal{M}_{n_r}(D_r) $$

é um anel semissimples.

Na verdade vale muito mais que isto. Veremos que, a menos de isomorfismos, todo anel semissimples é deste tipo, ou seja, o exemplo acima classifica todos os anéis semissimples. Este é o conteúdo do Teorema de Wedderburn-Artin, o qual será apresentado na próxima seção.

3.2 O Teorema de Wedderburn-Artin

Nesta seção, como diz seu título, vamos apresentar o assim conhecido Teorema de Wedderburn-Artin, o qual nos dá uma classificação dos anéis semissimples. Faremos isto a partir da estrutura do módulo regular ${}_RR$.

O resultado original de Wedderburn classifica as álgebras finito-dimensionais sobre um corpo qualquer. Estas álgebras eram chamadas de *sistemas de números hipercomplexos* naquela época. Vinte anos mais tarde, Artin generalizou o resultado de Wedderburn para anéis satisfazendo ACC e DCC simultaneamente, substituindo a finito-dimensionalidade pelo comprimento finito do módulo regular. Nossa exposição segue uma linha mais atual do que aquelas usadas nos trabalhos originais. Por exemplo, usamos apenas a artianidade do módulo regular, pois esta implica sua noetherianidade, conforme o Teorema de Hopkins-Levitzki, o qual é apresentado no último capítulo.

Começaremos nossa tarefa com o seguinte resultado importante.

Teorema 3.2.1. *Seja R um anel. Então as seguintes afirmações são equivalentes:*

(i) O módulo regular ${}_RR$ é semissimples;

(ii) Todos os R-módulos à esquerda são semissimples;

(iii) Todos os R-módulos à esquerda finitamente gerados são semissimples;

(iv) Todos os R-módulos à esquerda cíclicos são semissimples.

Demonstração. As implicações $(ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$ são claras. Assim, só precisamos mostrar a implicação $(i) \Rightarrow (ii)$. Para tanto, suponhamos que o módulo regular ${}_RR$ seja semissimples e consideremos M um R-módulo à esquerda. Como $M = \sum_{m\in M} Rm$, basta mostrar que Rm é semissimples, para todo $m \in M$. De fato, pois se ${}_RR = \oplus_{i=1}^{k} I_i$, onde I_i é um ideal à esquerda minimal de R, segue que

$$Rm = (I_1 \oplus I_2 \oplus \cdots \oplus I_k)m = I_1m \oplus I_2m \oplus \cdots \oplus I_km$$

e assim, só precisamos mostrar que cada um dos módulos I_im é um R-submódulo simples de Rm. Para esta finalidade, fixamos $i \in \{1, 2, ..., k\}$ e consideremos L um R-submódulo de I_im. Se $L \neq 0$, podemos tomar $0 \neq x \in L$ para obter $x = a_im$, para algum $a_i \in I_i$. Mas então, $(L : m)_i = \{r \in I_i : rm \in L\}$ é um R-submódulo de I_i, como é fácil ver, de onde segue que $(L : m) = I_i$, já que $0 \neq a_i \in (L : m)$ e I_i é simples. Portanto, $L = I_im$, e segue que I_im é simples. Como i foi tomado arbitrário, temos o resultado pretendido. Isto finaliza a demonstração do teorema. □

Para apresentar a classificação dos anéis semissimples, vamos necessitar de alguns resultados auxiliares, que passaremos a discutir no que segue. Para o primeiro deles, usaremos a seguinte notação: se R é um anel semissimples e I é um ideal à esquerda minimal de R, então escreveremos R_I para denotar o conjunto

$R_I := \sum \{J \lhd_l R : J \simeq I\}$. Com estas notações, podemos enunciar o seguinte resultado.

Lema 3.2.2. *Com as notações acima, valem as seguintes afirmações:*

(i) R_I *é um ideal (bilateral) de* R*.*

(ii) Se I *e* J *são ideais à esquerda minimais de* R *tais que* $I \not\simeq J$*, então* $R_I R_J = 0$*.*

Demonstração. (i) Precisamos apenas mostrar que R_I absorve multiplicação pela direita. Para tanto, basta mostrar que se $J \lhd_l R$ é tal que $J \simeq I$, então $Jr \subseteq R_I$, para todo $r \in R$. Com esta finalidade, dado $r \in R$, consideramos a aplicação $f_r : J \to R$, definida por $f_r(x) = xr$, para cada $x \in J$. Assim, f_r é um R-homomorfismo, pois se $a \in R, x \in J$, então $f_r(ax) = (ax)r = a(xr) = af_r(x)$. Mas então, $\mathcal{N}uc\, f_r = 0$ ou $\mathcal{N}uc\, f_r = J$, uma vez que J é um ideal à esquerda minimal de R. No primeiro caso, temos $Jr = \mathcal{I}m\, f_r \simeq J \simeq I$ e no segundo, $Jr = 0$. Assim, em ambos os casos, devemos ter $Jr \subseteq R_I$, o que mostra o resultado desejado.

(ii) Sejam I e J ideais à esquerda minimais de R tais que $I \not\simeq J$. Queremos mostrar que $R_I R_J = 0$. Para tanto, basta mostrar que se $L, K \lhd_l R$ são tais que $L \simeq I$ e $K \simeq J$, então $LK = 0$, pois todo elemento $x \in R_I$ é da forma $x = \sum_{i=1}^{n} a_i$, com $a_i \in L_i \simeq I$ $(1 \leq i \leq n)$, e todo elemento $y \in R_J$ é da forma $y = \sum_{j=1}^{m} b_j$, com $b_j \in K_j \simeq J$ $(1 \leq j \leq m)$. Observamos agora que se $L \simeq I$ e $y \in K \simeq J$, então $Ly = 0$, pois do contrário, deveríamos ter $Ly = K$, pela minimalidade de K. Assim, teríamos

$$I \simeq L \overset{(i)}{\simeq} Ly = K \simeq J$$

o que é uma contradição. Logo, só podemos ter $R_I R_J = 0$, como queríamos mostrar. □

Seja R um anel semissimples (à esquerda). Então, o módulo regular ${}_R R$ é semissimples e podemos escrever

$${}_R R = \underbrace{I_{11} \oplus \cdots \oplus I_{1n_1}}_{R_{I_1}} \oplus \cdots \oplus \underbrace{I_{r1} \oplus \cdots \oplus I_{rn_r}}_{R_{I_r}}$$

onde $R_{I_k} = \sum\{J \lhd_l R : J \text{ é minimal e } J \simeq I_k\}, 1 \leq k \leq r$. Neste caso, pelo resultado acima, temos $R = R_{I_1} \oplus \cdots R_{I_r}$ como anel. Os ideais R_{I_l} na decomposição acima são chamados de *componentes homogêneas* de R.

Para investigar a estrutura de um anel semissimples, precisamos entender um pouco mais suas componentes homogêneas, bem como conhecer um pouco mais a estrutura de anéis que são soma de ideais. O próximo resultado tem esta finalidade.

Antes, porém, observamos que se $R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$, com $I_j \lhd R$, $1 \leq j \leq n$, e $J \lhd R$, então $J = J_1 \oplus J_2 \oplus \cdots \oplus J_n$, onde $J_k \lhd I_k$ $(1 \leq k \leq n)$.

De fato, pois como estamos assumindo que R tem unidade, devemos ter $1_R = e_1 + e_2 \cdots e_n$, com $e_i \in I_i$, $1 \leq i \leq n$. Assim, $1 = 1^2 = \sum_{ij} e_i e_j = \sum_{i=1}^{n} e_i^2$, pois $e_i e_j \in I_i I_j \subseteq I_i \cap I_j = 0$, se $i \neq j$. Segue então da unicidade da escrita em uma soma direta que $e_i^2 = e_i$, isto é, $\{e_i\}_{i=1}^n$ é uma família de elementos idempotentes ortogonais de R. Além disso, como $r = 1r = r1$, segue que estes elementos são centrais (isto é, comutam com todos os elementos de R). Portanto, $J = RJ = (I_1 \oplus I_2 \oplus \cdots \oplus I_n)J = Je_1 \oplus Je_2 \oplus \cdots \oplus Je_n$, onde $Je_i \lhd Re_i = I_i$, $(1 \leq i \leq n)$.

Lema 3.2.3. *Sejam R um anel e $I_1, I_2, ..., I_r; J_1, J_2, ..., J_s$ ideais (bilaterais) indecomponíveis de R tais que $R = I_1 \oplus I_2 \oplus \cdots \oplus I_r = J_1 \oplus J_2 \oplus \cdots \oplus J_s$. Então, $r = s$ e, após uma permutação nos índices, se necessário, $I_i = J_i$, $1 \leq i \leq r$.*

Demonstração. Suponhamos $R = I_1 \oplus \cdots \oplus I_r = J_1 \oplus \cdots \oplus J_s$, então segue que $J_1 \lhd R$ e, usando a argumentação acima, temos que $J_1 = I_1' \oplus \cdots \oplus I_r'$, com $I_i' \lhd I_i$, $1 \leq i \leq r$. Mas como J_1 é indecomponível como ideal, concluimos que existe $k \in \{1, 2, ..., r\}$ tal que $J_1 = I_k'$ (i. é, os demais ideais I_l' na decomposição de J_1 são nulos). Reordenando os índices, se necessário, podemos escrever $J_1 = I_1'$. Assim, temos $J_1 \subseteq I_1$. Argumentando de modo análogo ao que fizemos acima, mas com I_1 em lugar de J_1, obtemos a outra inclusão, ou seja, $J_1 = I_1$. Repetindo-se esta argumentação tantas vezes quanto necessário, o lema fica demosntrado. □

O próximo resultado descreve mais precisamente a estrutura das componentes homegêneas de um anel semissimples.

Lema 3.2.4. *Seja R um anel semissimples (à esquerda). Então $R = R_1 \oplus \cdots \oplus R_r$, onde cada R_i, $1 \leq i \leq r$, é um anel simples com unidade, que possui um único ideal à esquerda minimal, a menos de isomorfismos.*

Demonstração. Pelos resultados anteriores, está claro que se R é semissimples, então podemos escrever $R = R_1 \oplus \cdots \oplus R_r$, onde cada R_i, $1 \leq i \leq r$, é um ideal bilateral, e portanto, um subanel de R, que contém um único ideal à esquerda minimal, a menos de isomorfismos. Mais ainda, por uma argumentação anterior, se $1_R = e_1 + e_2 + \cdots + e_r$, então $e_i^2 = e_i$, $R_i = e_i R = Re_i$ e R_i é um anel com unidade e_i $(1 \leq i \leq r)$.

Para finalizar a demonstração, precisamos mostrar agora que estes anéis R_i são simples, para cada $i \in \{1, 2, ..., r\}$. De fato, pois se fixarmos $i \in \{1, 2, ..., r\}$ e considerarmos $0 \neq I \lhd R_i$, segue que $I \lhd R$. Como todo ideal de R é também um ideal à esquerda, obtemos que I é um R-submódulo do módulo regular ${}_R R$, ou seja, I é um módulo semissimples (por ser submódulo de um módulo semissimples). Assim, I possui um ideal à esquerda minimal, digamos I_0. Pela argumentação feita no Lema 3.2.3, segue que $I_0 = Re$, para um certo idempotente $e \in R$. Considerando então a componente homogênea de R correspondente a este ideal minimal I_0, devemos ter $R_{I_0} = R_j$, para algum $j \in \{1, 2, ..., r\}$. Pela construção dos $R_j's$, só podemos ter $R_{I_0} = R_i$. Por outro lado, se $J \lhd_l R$ é um ideal à esquerda

minimal de R tal que $J \subseteq R_i$, então existe um isomorfismo $\varphi : I_0 \to J$ e segue que

$$J \simeq \varphi(I_0) = \varphi(Re) = \varphi(Ree) = \varphi(I_0 e) = I_0\varphi(e) \subseteq I$$

de onde se obtém que $I = R_i$, ou seja, R_i é um anel simples. Isto finaliza a nossa demonstração. □

Neste momento, sabemos que todo anel semissimples é uma soma direta de suas componentes homogêneas, e que cada uma destas é um anel simples que possui um único ideal à esquerda minimal, a menos de isomorfismos. Descendo um degrau a mais, vamos estudar a estrutura destes últimos anéis. Começamos esta tarefa com o seguinte resultado importante.

Lema 3.2.5. (Lema de Schur) *Sejam R um anel e M um R-módulo à esquerda simples. Então, $End_R(M)$ é um anel de divisão.*

Demonstração. Seja $f : M \to M$ um R-endomorfismo de M. Então, $\mathcal{N}uc\, f$ e $\mathcal{I}m\, f$ são R-submódulos de M. Como M é simples, segue que estes módulos são nulos ou iguais a M. Portanto, f é o homomorfismo nulo ou f é um isomorfismo, como é fácil verificar. Assim, $End_R(M)$ é um anel de divisão, como queríamos mostrar. □

Na verdade, o argumento usado na demonstração do Lema de Schur mostra que se M e N são dois R-módulos simples e $f : M \to N$ é um R-homomorfismo, então f é um isomorfismo ou é o homomorfismo nulo. Assim, ou dois R-módulos simples são isomorfos ou não existe nenhum homomorfismo não nulo entre eles. Muitas vezes encontramos na literatura o Lema de Schur dizendo exatamente isto.

Proposição 3.2.6. ***(Rieffel)*** *Seja R um anel simples. Suponhamos que R contenha um ideal à esquerda não nulo I e seja $D = End_R(I)$. Então $R \simeq End(I_D)$ como anéis.*

Demonstração. Consideremos a aplicação

$$\begin{array}{rccl} \varphi: & R & \to & End(I_D) \\ & r & \mapsto & \varphi_r: \begin{array}{ccc} I & \to & I \\ a & \mapsto & ra \end{array} \end{array}$$

Afirmamos que φ é um homomorfismo de anéis. De fato, pois se $r, s \in R$ e $a \in I$, então temos

$$\varphi(r+s)(a) = \varphi_{r+s}(a) = (r+s)a = ra+sa = \varphi_r(a)+\varphi_s(a) = (\varphi(r)+\varphi(s))(a)$$

e

$$\varphi(rs)(a) = \varphi_{rs}(a) = (rs)a = r(sa) = \varphi_r(sa) = \varphi_r(\varphi_s(a)) = (\varphi(r) \circ \varphi(s))(a)$$

Além disso, como R é um anel simples, segue que $\mathcal{N}uc\,\varphi = 0$ ou $\mathcal{N}uc\,\varphi$ = R. Mas como $\varphi(1_R) = id_I \in End(I_D)$, só podemos ter $\mathcal{N}uc\,\varphi = 0$ e segue que φ

é injetora. Para mostrar a sobrejetividade de φ vamos mostrar primeiro que $\varphi(I)$ é um ideal à esquerda de $End(I_D)$, onde vamos considerar $End(I_D)$ como um anel de operadores agindo à esquerda de I.

Começamos por observar que se $a \in I$, então existe um R-homomorfismo definido da seguinte maneira: $g_a : I \to I$, $g_a(x) = xa$, para todo $x \in I$. De fato, pois se $x, y \in I$ e $r \in R$, então $g_a(x+y) = (x+y)a = xa + ya = g_a(x) + g_a(y)$ e $g_a(rx) = (rx)a = r(xa) = rg_a(x)$. Portanto, $g_a \in D$, ou seja, a multiplicação à direita por um elemento de I é um operador do anel D.

Tomando então $a, b \in I$ e $h \in End(I_D)$, temos

$$h \cdot (\varphi_a(b)) = h(ab) = h(a)b = \varphi_{h(a)}(b)$$

ou seja, $h \circ \varphi_a = \varphi_{h(a)} \in End(I_D)$, para todos $a \in I$, $h \in End(I_D)$, de onde segue que $End(I_D)\varphi(I) \subseteq \varphi(I)$, ou seja, $\varphi(I) \lhd_l End(I_D)$, como queríamos mostrar.

Agora, pelo fato de R ser um anel simples e $I \neq 0$, segue que $IR = R$ (pois $IR \lhd R$). Assim, $\varphi(R) = \varphi(IR) = \varphi(I)\varphi(R)$. Portanto, $End(I_D)\varphi(R) = End(I_D)\varphi(I)\varphi(R) \subseteq \varphi(I)\varphi(R) = \varphi(R)$, ou seja, $\varphi(R)$ é um ideal à esquerda de $End(I_D)$. Para finalizar nossa demonstração, basta observar que $1_{End(I_D)} = id_I = \varphi(1_R) \in \varphi(R)$, para concluir que $\varphi(R) = End(I_D)$, isto é, φ é sobrejetora. □

Sabendo que as componentes homogêneas de um anel semissimples são anéis simples que possuem um ideal à esquerda minimal, o resultado acima passa a nos interessar justamente quando o ideal I do enunciado é minimal. Mais precisamente, o seguinte corolário será muito útil.

Corolário 3.2.7. *Seja R um anel simples que contém um ideal à esquerda minimal. Então $R \simeq \mathcal{M}_n(D)$, para algum $n \in \mathbb{N}$ e D um anel de divisão.*

Demonstração. Seja I um ideal à esquerda minimal de R. Pelo Lema de Schur (Lema 3.2.5) segue que $D = End(_RI)$ é um anel de divisão. Então, I possui uma estrutura de (R, D)-bimódulo, como visto antes, e segue da proposição anterior que $End(I_D)$ é um anel simples, pois $R \simeq End(I_D)$ como anéis.

Afirmamos agora que $dim_D I < \infty$. De fato, pois se $dim_D I = \infty$, então $K = \{f \in End(I_D) : dim_D \mathcal{I}m\, f < \infty\}$ é um ideal próprio de $End(I_D)$, o que produz uma contradição com a simplicidade do anel $End(I_D)$. Logo, só podemos ter $dim_D I = n$, algum $n \in \mathbb{N}$. Mas neste caso, $End(I_D)$ é o anel das transformações lineares de I em I, ou seja, $End(I_D) \simeq \mathcal{M}_n(D)$, e o resultado está demonstrado. □

Já vimos antes que as matrizes coluna são exemplos de módulos simples sobre um anel de matrizes com entradas em um anel de divisão. Veremos agora que, a menos de isomorfismos, estes são os únicos tais módulos.

Lema 3.2.8. *Seja R um anel simples que possui um ideal à esqueda minimal I. Então R possui, a menos de isomorfismo, um único módulo à esquerda simples e fiel isomorfo a I. Além disso, nestas condições, $R \simeq I^{(n)}$, onde $I^{(n)}$ significa a soma direta de n cópias de I.*

Demonstração. Como R é simples, $An_R(I) \lhd R$ e R tem unidade, segue que $An_R(I) = 0$, ou seja, I é um R-módulo à esquerda simples e fiel. Seja agora M um R-módulo à esquerda simples e fiel qualquer. Como $An_R(M) = 0$, deve existir $m \in M$ tal que $Im \neq 0$, de onde segue que $Im = M$, pela simplicidade de M. Mas então, a aplicação $\varphi : I \to M$ definida por $\varphi(x) = xm$ é um R-epimorfismo. Mais ainda, como $\mathcal{N}uc\,\varphi \lhd_l I$, segue que $\mathcal{N}uc\,\varphi = 0$ e, consequentemente, φ é um R-isomorfismo, ou seja, $M \simeq I$. Portanto, a menos de isomorfismo, R possui um único módulo à esquerda simples e fiel.

Para a última parte do Lema, basta observar que nas hipóteses assumidas, $R \simeq \mathcal{M}_n(D)$, onde $D = End_R(I)$ e $n = dim_D I$. Portanto, $R \simeq \mathcal{M}_n(D) \simeq I^{(n)}$, onde $I = \{(a_{ij}) \in \mathcal{M}_n(D) : a_{ij} = 0, \text{ se } i \neq 1\}$. □

Estamos agora em condições de enunciar o teorema de Wedderburn-Artin, que é o principal resultado deste capítulo.

Teorema 3.2.9. (Wedderburn-Artin) *Seja R um anel semissimples à esquerda. Então*

$$R \simeq \mathcal{M}_{n_1}(D_1) \times \mathcal{M}_{n_2}(D_2) \times \cdots \times \mathcal{M}_{n_t}(D_t)$$

onde $D_1, D_2, ..., D_t$ são anéis de divisão e $n_1, n_2, ..., n_t$ são inteiros positivos. O número t e os pares ordenados (D_i, n_i) são unicamente determinados a menos de permutações. Além disso, existem exatamente t R-módulos à esquerda simples e fiéis, dois a dois não isomorfos.

Demonstração. Quase todo o trabalho para a demonstração deste resultado já foi feito antes. Precisamos somente mostrar as unicidades. Para tanto, suponhamos que R seja um anel semissimples tal que $R \simeq \mathcal{M}_{n_1}(D_1) \times \mathcal{M}_{n_2}(D_2) \times \cdots \times \mathcal{M}_{n_t}(D_t)$ e também $R \simeq \mathcal{M}_{l_1}(D'_1) \times \mathcal{M}_{l_2}(D'_2) \times \cdots \times \mathcal{M}_{l_s}(D'_s)$, onde D_i, D'_l são anéis de divisão, $1 \leq i \leq t$, $1 \leq l \leq s$. Seja V_i o único módulo simples e fiel sobre o anel $R_i = \mathcal{M}_{n_i}(D_i)$. Então V_i se torna um R-módulo à esquerda, definindo-se $R_i \cdot V_j = 0$, se $j \neq i$. Desta forma, V_i é um R-módulo à esquerda simples. Além disso, se $i \neq j$, segue que $V_i \not\simeq V_j$. De fato, pois se $\phi : V_i \to V_j$ é um R-isomorfismo, então, para todo $r \in R$, teríamos $\phi(rv) = r\phi(v)$, para todo $v \in V_i$, mas tomando $r = (0, ..., 1_{R_j}, 0, ..., 0) \in R$ obtemos $r\phi(v) = \phi(rv) = \phi(0) = 0$, ou seja, $r \in An_R(V_j) = 0$, já que $v \in V_i$ foi tomado arbitrário e $\phi(V_i) = V_j$. Esta contradição mostra que $V_i \not\simeq V_j$.

Portanto, repetindo-se este argumento com a outra decomposição de R, obtemos que

$$V_1^{(n_1)} \oplus \cdots \oplus V_t^{(n_t)} \simeq {}_RR \simeq V_1'^{(l_1)} \oplus \cdots \oplus V_s'^{(l_s)}$$

e segue então do Teorema de Jordan-Holder (Teorema 2.2.2) que $s = t$, $n_i = l_i$ e ${}_RV_i \simeq {}_RV'_i$, $1 \leq i \leq r$.

Para finalizar a prova, basta observar agora que

$$D_i' \simeq End_{R_i'}(V_i') \simeq End_R(V_i') \simeq End_R(V_i) \simeq End_{R_i}(V_i) = D_i$$

Isto completa a prova do teorema. □

Uma consequência direta deste resultado é que o conceito de semissimplicidade é simétrico. Como já foi observado antes, tanto o módulo regular à direita quanto o módulo regular à esquerda de um anel de matrizes sobre um anel de divisão são semissimples. Mais precisamente, temos o seguinte resultado.

Corolário 3.2.10. *Seja R um anel. Então R é semissimples à esquerda se, e somente se, R é semissimples à direita.*

O seguinte resultado é muitas vezes referido na literatura como sendo o Teorema de Wedderburn-Artin, e nos dá uma classificação dos anéis artinianos simples.

Corolário 3.2.11. *Um anel artiniano é simples se, e somente se, é isomorfo a um anel de matrizes sobre um anel de divisão.*

Demonstração. Seja R um anel artiniano e simples. Como R tem unidade, segue que todo ideal à esquerda é um R-módulo fiel. Além disso, como R é artiniano, todo R-módulo à esquerda possui um R-submódulo simples. Portanto, nas condições acima, ou R é um anel de divisão ou R é um anel simples que possui um ideal à esquerda minimal. Portanto, $R \simeq \mathcal{M}_n(D)$, para algum $n \in \mathbb{N}$ e D um anel de divisão. A recíproca é clara. □

Note que se R é uma $\Bbbk$-álgebra finito-dimensional e semissimples, então $R \simeq \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_r}(D_r)$, onde cada D_i é uma $\Bbbk$-álgebra de divisão de dimensão n_i sobre $\Bbbk$, pelo Teorema de Wedderburn-Artin. Oberve agora que se $\Bbbk$ é um corpo algebricamente fechado e D é uma $\Bbbk$-álgebra de dimensão n, então o conjunto $\{1, a, a^2, ..., a^n\}$, com $0 \neq a \in D$, é linearmente dependente sobre $\Bbbk$, de onde segue que a é algébrico sobre $\Bbbk$, ou seja, $a \in \Bbbk$, de modo que $D = \Bbbk$.

Portanto, se R é uma $\Bbbk$-álgebra finito-dimensional e semissimples e $\Bbbk$ é algebricamente fechado, então $R \simeq \mathcal{M}_{n_1}(\Bbbk) \times \cdots \times \mathcal{M}_{n_r}(\Bbbk)$. Tomando então $\Bbbk = \mathbb{C}$, obtemos que toda $\mathbb{C}$-álgebra finito dimensional e semissimples é da forma $\mathcal{M}_{n_1}(\mathbb{C}) \times \cdots \times \mathcal{M}_{n_r}(\mathbb{C})$, recuperando o resultado de T. Molien, que classifica os sistemas de números hipercomplexos sobre $\mathbb{C}$, obtido em sua tese de doutorado em 1892.

Finalizaremos esta seção com mais alguns exemplos.

Exemplo 3.2.12. O anel $\mathbb{Z}/n\mathbb{Z}$ é semissimples se, e somente se, n é livre de quadrados.

De fato, pois se $n = p_1 p_2 ... p_k$, com p_i e p_j primos distintos, sempre que $i \neq j$, então temos $\mathbb{Z}/n\mathbb{Z} \simeq \Pi_{i=1}^{k} \mathbb{Z}/p_i\mathbb{Z}$, e cada um dos anéis $\mathbb{Z}/p_i\mathbb{Z}$ é um corpo, portanto

um anel simples e artiniano. Mostre a recíproca (veja também os exercícios no final do capítulo 5 para uma outra sugestão, usando o radical de Jacobson).

Apresentaremos agora um exemplo de um anel simples e não artiniano, mostrando que existem anéis simples que não são semissimples.

Exemplo 3.2.13. Sejam $R_1 \subseteq R_2 \subseteq \cdots \subseteq R_n \subseteq \cdots$ uma cadeia de anéis simples com a mesma unidade e consideremos $R = \cup R_i$. Então R é um anel simples.

De fato, pois se $I \lhd R$, $I \neq 0$, então $I \cap R_j$ é um ideal não nulo de R_j, para algum $j \geq 1$. Mas como R_j é simples, segue que $I \cap R_j = R_j$, ou seja, $1_R = 1_{R_j} \in I \cap R_j \subseteq I$, e segue que $I = R$.

Agora, no exemplo acima, consideramos $R_i = \mathcal{M}_{2^i}(D)$, onde D é um anel de divisão. Consideramos a inclusão $R_i \hookrightarrow R_{i+1}$ via $M \mapsto \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}$. Assim, $R = \cup_{i \geq 0} R_i$, onde $R_0 = D$, e segue do exemplo anterior que R é um anel simples.

Observamos agora que se tomamos o elemento $e_i \in R_i$, como sendo a matriz que possui o elemento 1 na entrada $(1,1)$ e zeros nas demais, e consideramos e_i como elemento de R, via a inclusão acima, segue que $e_{i+1} = e_{i+1}e_i \in R_{i+1}$, e portanto temos uma cadeia decrescente $Re_0 \supseteq Re_1 \supseteq \cdots \supseteq Re_n \supseteq \cdots$.

Por fim, note que $e_i \notin Re_{i+1}$. De fato, pois do contrário, existiria $j > i$ tal que $e_i \in R_j\, e_{i+1}$ e teríamos $e_i = Me_{i+1}$, para alguma matriz M. Mas a entrada $(2^{i+1}, 2^{i+1})$ da matriz Me_{i+1} é nula, enquanto que a entrada $(2^{i+1}, 2^{i+1})$ da matriz e_i é 1. Portanto, a cadeia acima é estritamente decrescente e R não é artiniano à esquerda.

Exercícios

1. Seja R um anel. Mostre que R é semissimples se, e somente se, toda sequencia exata curta de R-módulos à esquerda cinde.

2. Mostre que toda imagem homomórfica de um anel semissimples é também um anel semissimples.

3. Seja R um anel semissimples e artiniano. Mostre que se $ab = 0$ implicar $a = 0$ ou $b = 0$, para todos elementos de $a, b \in R$, então R é um anel de divisão (i. é., todo anel artiniano semissimples sem divisores de zero é um anel de divisão).

4. Seja M um R-módulo à esquerda semissimples. Mostre que M é uma soma finita de submódulos simples se, e somente se, M é finitamente gerado.

5. Mostre que $\mathbb{Q}$ é um Z-módulo indecomponível que não é simples. Conclua daí que $\mathbb{Q}$ não é um Z-módulo semissimples.

Capítulo 4

Uma Aplicação da semissimplicidade

A ideia deste capítulo é apresentar alguma aplicação da semissimplicidade. Escolhemos para tanto uma aplicação na teoria de grupos, pois uma das mais interessantes aplicações da semissimplicidade aparece na teoria de representação de grupos finitos. Vamos procurar apresentar aqui a conexão entre estes dois tópicos. Não entraremos em datelhes mais profundos e possivelmente seja necessário consultar algum outro texto mais específico, para dar maior suporte. Algumas indicações bibliográficas neste sentido são dadas no final do texto.

4.1 Ações de grupos em conjuntos

Vamos assumir neste capítulo que todos os grupos são finitos, embora alguns resultados sejam válidos para grupos quaisquer. Iniciamos lembrando o que é uma ação de um grupo em um conjunto.

Definição 4.1.1. Sejam G um grupo e X um conjunto. Dizemos que G age em X se existir uma aplicação

$$\begin{array}{rccc} \alpha: & G \times X & \to & X \\ & (g,x) & \mapsto & g \cdot x \end{array}$$

satisfazendo as seguintes condições

(i) $1_G \cdot x = x, \forall x \in X$;

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

Observe que na definição acima, escrevemos $g \cdot x$ para indicar a imagem do par ordenado $(g, x) \in G \times X$ pela ação α, para simplificar a notação. Muitas vezes faremos exatamente assim.

Exemplo 4.1.2. Seja G um grupo e X um conjunto. Então a ação trivial de G em X é definida por $g \cdot x = x, \forall x \in X$.

Exemplo 4.1.3. Sejam $\Bbbk$ um corpo e V um espaço vetorial. Então a ação de $\Bbbk$ sobre V determina uma ação do grupo multiplicativo $\Bbbk^\times := \Bbbk \setminus \{0\}$ no conjunto V de maneira natural.

Exemplo 4.1.4. Seja X um conjunto. Então o grupo $(\mathcal{B}ij\,(X), \circ)$, das permutações de elementos de X, age em X de maneira natural, via $\sigma \cdot x = \sigma(x)$, para todos $\sigma \in \mathcal{B}ij\,(X)$ e $x \in X$.

Exemplo 4.1.5. Todo grupo G age em si mesmo via multiplicação, isto é, a aplicação $\alpha : G \times G \to G$, dada por $\alpha(g, h) = g \cdot h = gh$ define uma ação de G em G, chamada de ação regular.

Dizemos que uma ação α de um grupo G em um conjunto X é *fiel*, se α for uma aplicação injetora ou, equivalentemente, se $\alpha_g(x) = \alpha_h(x), \forall x \in X$, então $g = h$. A ação regular de um grupo em si mesmo e a ação do grupo multiplicativo $\Bbbk^\times$ sobre um $\Bbbk$-espaço vetorial são exemplos de ações fiéis.

4.2 Representações de grupos finitos

Se G age em X, dizemos que X é um *G-conjunto*. Observamos que se G é um grupo e X é um G-conjunto, então para cada $g \in G$ fica definido uma função $\alpha_g : X \to X$, dada por $\alpha_g(x) = g \cdot x$. Mais ainda, α_g é de fato uma bijeção com inversa $\alpha_{g^{-1}}$, pois se $x \in X$, então $\alpha_g(\alpha_{g^{-1}}(x)) = \alpha_g(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = gg^{-1} \cdot x = 1_G \cdot x = x$. Analogamente, $\alpha_{g^{-1}} \circ \alpha_g = id_X$. Portanto, $\alpha_g^{-1} = \alpha_{g^{-1}}$. Assim, se um grupo G age em um conjunto X, fica definido um homomorfismo de grupos $\alpha : G \to \mathcal{B}ij\, X$, dado por $g \mapsto \alpha_g$. Um tal homomorfismo de grupos é dito uma *representação de G por permutações*.

Podemos, assim, recuper o Teorema de Cayley, o qual afirma que todo grupo G é isomorfo a um subgrupo de um grupo de permutações. Para ver isto, basta tomar $X = G$ e considerar a ação de G sobre si mesmo via multilicação. Desta forma, α é injetivo. De fato, se $g \in G$ é tal que $\alpha_g = id_G$, então $g \cdot x = gx = x$, para todo $x \in G$, de onde segue que $g = 1_G$.

Reciprocamente, se $\alpha : G \to \mathcal{B}ij(X)$, $g \mapsto \alpha_g$, é uma representação por permutações, então fica definido uma ação de G em X, via $g \cdot x := \alpha_g(x), \forall x \in X$. Assim, as ações de um grupo em um conjunto estão em correspondência biunívoca com as representações de G por permutações.

O que de fato nos interessa nesta seção são as chamadas representações lineares de um grupo. Vamos passar a defini-las agora.

Consideremos $\Bbbk$ um corpo e V um $\Bbbk$-espaço vetorial n-dimensional. Se G é um grupo finito que age em V, então podemos definir a aplicação $\psi : G \to End_\Bbbk(V)$, definida por $\psi(g) = \psi_g$, onde $\psi_g(v) = g \cdot v$, para todo $g \in G, v \in V$. Considerando o conjunto $End_\Bbbk(V)$, das transformações lineares de V em V, munido com a operação de composição de funções, segue que ψ é uma aplicação

que preserva estas operações. De fato, pois se $g, h \in G$ e $u, v \in V$, então $\psi(gh)(v) = \psi_{gh}(v) = gh \cdot v = g \cdot (h \cdot v) = \psi_g(\psi_h(v)) = \psi_g \circ \psi_h(v)$. Além disso, $\psi(1_G)(v) = 1_G \cdot v = v, \forall v \in V$, isto é, $\psi(1_G) = id_V$.

Mas como $End_{\Bbbk}(V)$ não é, em geral, um grupo, não podemos falar em uma representação de G, de espécie alguma. Para corrigir este problema, restringimos o conjunto $End_{\Bbbk}(V)$ ao conjunto das transformações lineares bijetoras de V em V. Na literatura, este conjunto vem sempre representado por $GL_n(V)$ (ou $GL_{n,\Bbbk}(V)$, quando se faz necessário explicitar o corpo base). Assim, pelos argumentos discutidos acima e mantendo as mesmas notações, a aplicação $\psi : G \to GL_n(V)$, dada por $\psi(g)(v) = g \cdot v$ é um homomorfismo de grupos. Podemos então enunciar a seguinte definição.

Definição 4.2.1. Sejam G um grupo finito, $\Bbbk$ um corpo e V um $\Bbbk$-espaço vetorial n dimensional. Chamamos de uma representação linear de G em V, a todo homomorfismo $\psi : G \to GL_n(V)$. A dimensão n de V sobre $\Bbbk$ é dita o grau desta representação.

As representações lineares de um grupo finito G em um $\Bbbk$-espaço vetorial n dimensional V dão origem as chamadas *ações lineares de G em V*, da seguinte maneira. Suponhamos que G age em V via $\rho : G \times V \to V$, segundo a Definição 4.1.1. Então, para cada $g \in G$ está definida uma aplicação $\rho_g : V \to V$. Dizemos que a ação de G em V é *linear* se ρ_g é uma transformação linear, para cada $g \in G$. Assim, escrevendo $g \cdot v$ para denotar $\rho_g(v)$, dizemos que a ação de G em V é linear, se:

- $1_G \cdot v = v, \forall v \in V$;
- $g \cdot (h \cdot v) = gh \cdot v, \forall g, h \in G, \forall v \in V$;
- $g \cdot (\alpha u + \beta v) = \alpha(g \cdot u) + \beta(g \cdot v)$.

Estas ações lineares nos permitem considerar, com mais precisão, aquilo que gostaríamos de chamar de um G-módulo. Para tanto, precisamos considerar o anel de grupo de G sobre $\Bbbk$. Dados um grupo G e um corpo $\Bbbk$, definimos o *anel de grupo de G sobre $\Bbbk$* como sendo o $\Bbbk$-espaço vetorial com base $G = \{g_1, g_2, ..., g_n\}$, ou seja

$$\Bbbk[G] := \oplus_{i=1}^{n} \alpha_i g_i,\ \alpha_i \in \Bbbk,\ 1 \leq i \leq n$$

com a soma usual de vetores e com uma multiplicação induzida por

$$(\alpha_i g_i)(\alpha_j g_j) = \alpha_i \alpha_j g_i g_j$$

estendida por linearidade. É fácil verificar que desta forma $\Bbbk[G]$ é um anel com unidade $1_{\Bbbk} 1_G$, onde 1_G denota o elemento neutro do grupo G.

Também é fácil verificar que as aplicações $\varphi : G \to \Bbbk[G]$, dada por $\varphi(x) = 1_{\Bbbk} x$ é uma imersão de G em $\Bbbk[G]$, e que $\psi : \Bbbk \to \Bbbk[G]$, dada por $\psi(a) = a 1_G$ é uma imersão de $\Bbbk$ em $\Bbbk[G]$. Identificando os elementos $a \in \Bbbk$ com os elementos

da forma $a1_G$, e os elementos $g \in G$ com os elementos da forma $1_{\Bbbk}g$, obtemos que $ag = ga$, para todo $a \in \Bbbk$ e todo $g \in G$. Portanto, podemos mostrar que o anel $\Bbbk[G]$ só é comutativo se G for um grupo abeliano.

A conexão entre o anéis de grupo e ações lineares de um grupo em um espaço vetorial é dada no seguinte resultado.

Proposição 4.2.2. *Sejam G um grupo, $\Bbbk$ um corpo e V um $\Bbbk$-espaço vetorial. Então G age linearmente em V se, e somente se, V é um $\Bbbk[G]$-módulo (à esquerda).*

Demonstração. Suponhamos que G age linearmente em V via ρ. Definimos uma ação de $\Bbbk[G]$ em V da seguinte forma: Para $x = \sum \alpha_i g_i \in \Bbbk[G]$ e $v \in V$, tomamos $x \cdot v := \sum \alpha_i (g_i \cdot v)$. Desta maneira, V se transforma num $\Bbbk[G]$-módulo à esquerda. As propriedades aditivas seguem facilmente da linearidade das aplicações ρ_g, para cada $g \in G$. Além disso, dados $x = \sum \alpha_i g_i, y = \sum \beta_j h_j \in \Bbbk[G]$ e $v \in V$, temos $x \cdot (y \cdot v) = \sum_i \alpha_i g_i \cdot (\sum_j \beta_j h_j \cdot v) = \sum_{i,j} \alpha_i \beta_j g_i h_j \cdot v = xy \cdot v$. Reciprocamente, se V é um $\Bbbk[G]$-módulo à esquerda, então definimos $\rho : G \times V \to V$, por $\rho_g(v) = (1_{\Bbbk[G]} g) \cdot v$. É fácil verificar que esta aplicação ρ define uma ação linear de G em V. □

De acordo com o resultado acima, podemos então fazer as seguintes definições.

Definição 4.2.3. Seja G um grupo finito que age linearmente em um $\Bbbk$-espaço vetorial V. Então, dizemos que a representação associada a esta ação linear é:

- *irredutível*, se V é um $\Bbbk[G]$-módulo simples,
- *semissimples*, se V é um $\Bbbk[G]$-módulo semissimples,
- *regular*, se $V = \Bbbk[G]$ e a ação de G é induzida pela multiplicação de G.

Exemplo 4.2.4. Sejam $G = \{e, g, g^2\}$ o grupo cíclico de ordem 3, $\Bbbk = \mathbb{C}$ o corpo dos números complexos e ρ a representação regular de G em $\mathbb{C}$. Assim, as transformações lineares ρ_g possuem as seguintes matrizes na base $\mathcal{B} = \{e, g, g^2\}$:

$$[\rho_e]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \ [\rho_g]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \text{ e } [\rho_{g^2}]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Vamos agora na direção de mostrar que $\Bbbk[G]$ é um anel semissimples, com algumas hipóteses razoáveis sobre $\Bbbk$. A semissimplicidade de $\Bbbk[G]$ vai garantir que todo $\Bbbk[G]$-módulo à esquerda é semissimples, ou seja, uma soma de módulos simples. Como as representações lineares de G estão em correspondência com os $\Bbbk[G]$-módulos, segue que as representações lineares de G são somas de representações irredutíveis. Portanto, para classificar as representações lineares de um grupo finito, basta classificar as representações irredutíveis deste grupo. E é justamente nesta tarefa que o Teorema de Wedderburn-Artin vem em nosso auxílio.

Para facilitar nossa exposição, a partir de agora, vamos assumir que $\Bbbk$ é um corpo de característica zero. Vamos apresentar o resutado que nos permite analisar uma representação de um grupo finito por meio de suas representações irredutíveis.

Teorema 4.2.5. (Teorema de Maschke) *Sejam G um grupo finito, $\Bbbk$ um corpo (de característica zero). Então $\Bbbk[G]$ é um anel semissimples.*

Demonstração. Seja $n =\mid G \mid$. Consideremos V um $\Bbbk[G]$-submódulo à esquerda. Para mostrar que $\Bbbk[G]$ é semissimples, precisamos mostrar que $\Bbbk[G] = V \oplus W$ para um certo $\Bbbk[G]$-submódulo à esquerda W. Como todo $\Bbbk[G]$-módulo possui uma estrutura de $\Bbbk$-espaço vetorial, podemos escrever $\Bbbk[G] = V \oplus U$, onde U é um $\Bbbk$-espaço vetorial (isto é, podemos decompor o $\Bbbk$-espaço vetorial $\Bbbk[G]$ como uma soma direta de $\Bbbk$-espaços vetoriais). Consideremos a projeção linear $\pi : \Bbbk[G] \to V$ com núcleo U, associada a decomposição $\Bbbk[G] = V \oplus U$. Assim, π é uma aplicação $\Bbbk$-linear, mas não necessariamente $\Bbbk[G]$-linear. O que vamos fazer agora é construir uma aplicação $\Bbbk[G]$-linear a partir de π, para obter nossa decomposição pretendida.

Vamos definir $\pi^* : \Bbbk[G] \to \Bbbk[G]$, por

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

Vamos mostrar agora que $\pi^*(\Bbbk[G]) = V$ e que $\Bbbk[G] = V \oplus (id - \pi^*)(\Bbbk[G])$, como $\Bbbk[G]$-módulos.

Tomando $y \in \Bbbk[G]$ e $g \in G$, segue que $\pi(gy) \in V$, de onde se deduz que

$$\pi^*(gy) = \frac{1}{n} \sum_{g \in G} g^{-1}\pi(gy) \in V$$

Além disso, se $x \in V$, então

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

ou seja, $\mathcal{I}m\,\pi^* = V$. Mais ainda, $(\pi^*)^2 = \pi^*$. Portanto, π^* é uma projeção e segue que

$$\Bbbk[G] = \pi^*(\Bbbk[G]) \oplus (id - \pi^*)(\Bbbk[G]) = V \oplus (id - \pi^*)(\Bbbk[G])$$

Resta mostrar agora que $W = (id - \pi^*)(\Bbbk[G])$ é um $\Bbbk[G]$-submódulo, ou seja, que π^* é um $\Bbbk[G]$-homomorfismo. Para tanto, consideremos $h \in G$, $x \in \Bbbk[G]$. Então temos

$$h^{-1}\pi^*(hx) = \frac{1}{n} \sum_{g \in G} h^{-1}g^{-1}\pi(ghx) = \frac{1}{n} \sum_{y \in G} y^{-1}\pi(yx) = \pi^*(x)$$

ou seja,

$$\pi^*(hx) = h\pi^*(x), \forall h \in G, x \in \Bbbk[G].$$

Assim, tomando um elemento qualquer de W, da forma $(id - \pi^*)(x)$, obtemos

$$h((id - \pi^*)(x)) = hx - \pi^*(hx) = (id - \pi^*)(hx) \in W.$$

Isto termina a nossa demostração. □

Gostaríamos de observar que uma peça fundamental na argumentação acima foi usar o fato de que $n =\mid G \mid$ é um elemento invertível em $\Bbbk$. Foi justamente neste momento que usamos a hipótese de que a característica de $\Bbbk$ é zero. De fato, esta mesma argumentação funciona bem se supormos, em lugar de característica zero, que a característica de $\Bbbk$ não divide a ordem de G.

Quando assumimos que $\Bbbk$ é um corpo algebricamente fechado, podemos dizer mais a respeito do anel de grupo $\Bbbk[G]$. Para o próximo resultado, vamos lembrar da teoria de grupos que dois elementos $x, y \in G$, onde G é um grupo qualquer, são ditos conjugados, se existe $g \in G$ tal que $x = gyg^{-1}$. Mais ainda, a relação *x está relacionado com y se, e somente se, x e y são conjugados*, determina em G uma relação de equivalência, cujas classes são chamadas de *classes de conjugação* de G.

Corolário 4.2.6. *Sejam G um grupo finito de ordem n, $\Bbbk$ um corpo algebricamente fechado (de característica zero). Então*

$$\Bbbk[G] \simeq \mathcal{M}_{n_1}(\Bbbk) \oplus \mathcal{M}_{n_2}(\Bbbk) \oplus \cdots \oplus \mathcal{M}_{n_r}(\Bbbk)$$

onde $n = n_1^2 + n_2^2 + \cdots n_r^2$. Além disso, $\Bbbk[G]$ possui exatamente r módulos simples não isomorfos de dimensões respectivamente iguais a $n_1, n_2, ..., n_r$ sobre $\Bbbk$, e r coincide com o número de classes de conjugação de G.

Demonstração. Pelo Teorema de Maschke, $\Bbbk[G]$ é um anel semissimples. Do Teorema de Wedderburn-Artin, segue que

$$\Bbbk[G] \simeq \mathcal{M}_{n_1}(D_1) \oplus \mathcal{M}_{n_2}(D_2) \oplus \cdots \oplus \mathcal{M}_{n_r}(D_r)$$

onde $D_i = End_{\Bbbk[G]}(V_i)$ é um anel de divisão, sendo V_i módulos simples sobre $\Bbbk[G]$. Assim, D_i é finito-dimensional sobre $\Bbbk$, de onde segue que $D_i = \Bbbk$, pois $\Bbbk$ é algebricamente fechado. Portanto,

$$\Bbbk[G] \simeq \mathcal{M}_{n_1}(\Bbbk) \oplus \mathcal{M}_{n_2}(\Bbbk) \oplus \cdots \oplus \mathcal{M}_{n_r}(\Bbbk)$$

como afirmado no enunciado. Além disso, computando dimensões sobre $\Bbbk$, obtemos do isomorfismo acima que

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

Resta mostrar que o número de classes de conjugação de G é igual a r. Começamos observando que $dim_{\Bbbk} Z(\Bbbk[G]) = r$. De fato, pois o centro de um anel de matrizes $\mathcal{M}_n(\Bbbk)$ é o conjunto das matrizes escalares αI_n, e com isto, segue do isomorfismo acima que $dim_{\Bbbk} Z(\Bbbk[G]) = r$.

Observamos agora que para cada classe de conjugação $\mathcal{C}_i$ de G, podemos considerar o elemento $c_i = \sum_{x \in \mathcal{C}_i} x \in \Bbbk[G]$. Assim, se $g \in G$, então $g^{-1} c_i g = c_i$, e segue daí que todos estes elementos c_i estão no centro de $\Bbbk[G]$. Além disso, como

podemos considerar $\{c_i\}$ um subconjunto de G, segue que $\{c_i\}$ é um conjunto linearmente independente sobre $\Bbbk$ (por ser um subconjunto de uma $\Bbbk$-base de $\Bbbk[G]$). Mais ainda, se $\sum_{g\in G}\alpha_g g \in Z(\Bbbk[G])$, então para cada $h \in G$, temos

$$\sum_{g\in G}\alpha_g g = h^{-1}(\sum_{g\in G}\alpha_g g)h = \sum_{g\in G}\alpha_g h^{-1}gh$$

ou seja, da escrita única dos elementos de $\Bbbk[G]$, segue que $\alpha_g = \alpha_{h^{-1}gh}$, o que por sua vez implica que $\sum_{g\in G}\alpha_g$ é uma combinação linear dos elementos do conjunto $\{c_i\}$. Portanto, $\{c_i\}$ é uma $\Bbbk$-base de $Z(\Bbbk[G])$ e, consequentemente,

$$r = dim_{\Bbbk}Z(\Bbbk[G]) = \text{ número de classes de conjugação de } G$$

e o Corolário está demonstrado. □

4.3 Representações irredutíveis de S_3 sobre $\mathbb{C}$

Nesta breve seção, como uma aplicação do que foi discutido até aqui, vamos classificar as representações irredutíveis de S_3 (o grupo das permutações de três elementos) sobre $\mathbb{C}$. Assim, considerando S_3 como o grupo das permutações dos símbolos $1, 2$ e 3, e notando uma permutação por $(a_1a_2...a_r)$, para dizer que o elemento a_i é levado no elemento a_{i+1}, $1 \leq i \leq r-1$ e a_r é levado em a_1, deixando fixos os elementos que não aparecem nesta escrita, temos $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ e $\mid S_3 \mid = 6$.

Lembramos ainda da teoria de grupos que S_3 é um grupo gerado por dois elementos, digamos τ e σ, sujeitos às seguintes relações: $\tau^2 = (1)$, $\sigma^3 = (1)$ e $\sigma\tau = \tau\sigma^2$. Por exemplo, podemos tomar $\tau = (12)$ e $\sigma = (123)$. Mais ainda, S_3 possui um subgrupo normal de índice dois, a saber, $N =< \sigma >$. Além disso, como elementos conjugados em S_n possuem a mesma estrutura de ciclos, segue que existem 3 classes de conjugação em S_3, a saber, $\mathcal{C}_1 = \{(1)\}, \mathcal{C}_2 = \{(12), (13), (23)\}$ e $\mathcal{C}_3 = \{(123), (132)\}$. Estas informações serão usadas no decorrer de nossa argumentação.

Usando então o Corolário 4.2.6, obtemos que

$$\mathbb{C}S_3 \simeq \mathcal{M}_{n_1}(\mathbb{C}) \oplus \mathcal{M}_{n_2}(\mathbb{C}) \oplus \mathcal{M}_{n_3}(\mathbb{C})$$

com $6 = n_1^2 + n_2^2 + n_3^2$. Como $\mathbb{C}S_3$ não é comutativo, segue que pelo menos um dos índices n_i deve ser diferente de 1. Portanto, $n_1 = n_2 = 1$ e $n_3 = 2$, ou seja, S_3 possui duas representações irredutíveis unidimensionais e uma bidimensional. Assim, podemos melhorar a decomposição de $\mathbb{C}S_3$ para a forma

$$\mathbb{C}S_3 \simeq \mathbb{C} \oplus \mathbb{C} \oplus \mathcal{M}_2(\mathbb{C})$$

Vamos encontrar as representações de grau 1 de S_3 sobre $\mathbb{C}$. Seja então V um $\mathbb{C}$-espaço vetorial unidimensional, digamos $V = \mathbb{C}v$. Observamos agora que a

ação trivial $\rho : G \to GL_1(V)$, $\rho_g = id_V$, para todo $g \in S_3$ é uma representação linear de S_3 sobre $\mathbb{C}$, como é fácil verificar.

Seja $N =< \sigma >$ um subgrupo normal de índice 2. Definimos então $\rho : S_3 \to GL_1(V)$, por $\rho_g = id_V$, se $g \in N$ e $\rho_g = -id_V$, se $g \notin N$. Assim, se $g, h \in S_3$, com $gh \in N$ então ou $g, h \in N$ ou $g, h \notin N$ e, consequentemente, $\rho_{gh} = id_V = \rho_g \circ \rho_h$. O mesmo acontece, se $gh \notin N$ (verifique!). Assim, ρ é uma representação linear de S_3 sobre $\mathbb{C}$.

Procurando a representação irredutível de grau dois de S_3 sobre $\mathbb{C}$, e tendo em mente as relações dos geradores de S_3, observamos que se $\omega \in \mathbb{C}$ é uma raiz cúbica primitiva da unidade, então

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

e

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

portanto, a aplicação $\varphi : S_3 \to \mathcal{M}_2(\mathbb{C})$, induzida por

$$\tau \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ e } \sigma \mapsto \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$$

é claramente um isomorfismo de grupos. Assim, tomando V um $\mathbb{C}$-espaço vetorial de dimensão 2, digamos com base $\mathcal{B} = \{e_1, e_2\}$, podemos definir $\rho : S_3 \to GL_2(V)$, induzida por

$$\rho_x : e_1 \mapsto e_2, \quad \rho_x : e_2 \mapsto e_1, \quad \rho_y : e_1 \mapsto \omega e_1 \quad \text{e} \quad \rho_y : e_2 \mapsto \omega^2 e_2$$

para obtermos uma representação linear de S_3 sobre $\mathbb{C}$.

Vamos verificar agora que a representação acima é de fato irredutível. Para tanto, precisamos mostrar que não existe nenhum subespaço unidimensional de V que seja invariante pela ação linear de S_3 dada por:

$$x \cdot e_1 = e_2, \quad x \cdot e_2 = e_1, \quad y \cdot e_1 = \omega e_1 \quad \text{e} \quad y \cdot e_2 = \omega^2 e_2.$$

De fato, pois é evidente que o subespaço $\mathbb{C}e_1$ não é fixo por x. Dado W um subespaço unidimensional de V, segue que existe $\lambda \in \mathbb{C}$ tal que $W = \mathbb{C}(e_1 + \lambda e_2)$. Suponhamos que W seja invariante por esta ação de S_3. Então devemos ter

$$x \cdot (e_1 + \lambda e_2) = e_2 + \lambda e_1 \in \mathbb{C}(e_1 + \lambda e_2)$$

de onde segue que existe $\alpha \in \mathbb{C}$ tal que $\lambda e_1 + e_2 = \alpha e_1 + \alpha\lambda e_2$, ou seja, só podemos ter $\alpha = \lambda = 1$ ou $\alpha = \lambda = -1$. Agora, por outro lado, temos

$$y \cdot (e_1 + e_2) = \omega e_1 + \omega^2 e_2 \notin \mathbb{C}(e_1 + e_2)$$

e

$$y \cdot (e_1 - e_2) = \omega e_1 - \omega^2 e_2 \notin \mathbb{C}(e_1 + e_2)$$

o que é uma contradição.

Portanto, não existe nenhum subespaço unidimensional de V que fique fixo pela ação de S_3, isto é, V não possui nenhum $\mathbb{C}S_3$-submódulo próprio, ou ainda, V é um $\mathbb{C}S_3$-módulo simples e, portanto, V é uma representação irredutível de grau 2 de S_3 sobre $\mathbb{C}$. Completamos assim a classificação das representações lineares irredutíveis de S_3 sobre $\mathbb{C}$.

Exercícios

1. O objetivo deste exercício é mostrar que se G é um grupo cíclico de ordem n e $\Bbbk$ é um corpo de característica zero (ou cuja característica não divida a ordem de G), então existe um isomorfismo de anéis

   $$k[G] \simeq \frac{\Bbbk[X]}{< X^n - 1 >}$$

   Seja $\Bbbk$ um corpo de característica zero e $G =< a : a^n = 1 >$, um grupo cíclico de ordem n gerado por um elemento a. Mostre que:

   (i) $\Phi : \Bbbk[X] \to \Bbbk[G]$, dado por $\Phi(f(x)) = f(a)$ é um epimorfismo de anéis.

   (ii) $\mathcal{N}uc\,\Phi =< X^n - 1 >$.

   (iii) Conclua que $\Bbbk[G] \simeq \Bbbk[X]/ < X^n - 1 >$ como anéis.

2. *(Continuação do exercíco anterior)* Com as mesmas hipóteses do exercício anterior, use o Teorema Chinês de Restos para concluir que

   $$\Bbbk[G] \simeq \frac{\Bbbk[X]}{< p_1(X) >} \oplus \cdots \oplus \frac{\Bbbk[X]}{< p_t(X) >}$$

   onde $X^n - 1 = p_1(X) \cdots p_t(X)$ é a fatoração de $X^n - 1$ em fatores irredutíveis em $\Bbbk[X]$.

3. *(Continuação do exercíco anterior)* Assumindo que $\xi_i \in \Bbbk$ é uma raiz de $p_i(X)$, $1 \leq i \leq t$, nas hipóteses do exercício anteior, mostre que

   $$\Bbbk[G] \simeq \Bbbk(\xi_1) \oplus \cdots \oplus \Bbbk(\xi_t)$$

   ou seja, neste caso, o anel de grupo $\Bbbk[G]$ é uma soma direta de extensões ciclotômicas de $\Bbbk$.

4. Considere G o grupo cíclico de ordem 7. Mostre que $\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q}(\xi)$, onde ξ é uma raiz sétima primitiva da unidade.

5. Determine todas as representações lineares irredutíveis de $\mathcal{S}_4$.

Capítulo 5

J-semissimplicidade

No capítulo 3, estudamos a semissimplicidade de um anel, usando para tal a estrutura de seus módulos. Agora, pretendemos dar uma outra abordagem a este tópico, mas olhando internamente a estrutura do próprio anel. Este é o tema do presente capítulo.

Para atingir nosso objetivo, na primeira seção introduzindo o conceito de radical de Jacobson de um anel e discutiremos algumas de suas propriedades. Na seção seguinte vamos mostrar que, num certo sentido, o radical de Jacobson dá uma medida de quão longe o anel está de ser semissimples. Assim, estudar a J-semissimplicidade de um anel seria naturalmente o próximo passo a ser dado no estudo dos anéis não comutativos, segundo nossa linha de trabalho.

5.1 O radical de Jacobson

Vamos introduzir o conceito de radical de Jacobson de um anel, sem entrarmos em detalhes mais finos sobre a teoria dos radicais. Para que nossa definição se torne mais natural, observamos que um corpo $\mathbb{k}$ age fielmente sobre qualquer $\mathbb{k}$-espaço vetorial e, em particular, sobre seus espaços vetoriais unidimensionais (simples). O mesmo já não acontece quando passamos ao contexto dos módulos sobre anéis. Como os módulos semissimples são soma de seus submódulos simples, segue que os elementos do anel base que anulam todos os módulos simples passam a ser indesejáveis para o estudo da semissimplicidade. Desta forma, vamos reuní-los inicialmente num conjunto, que depois será visto ser um ideal de fato. Mais precisamente, temos o seguinte conceito.

Definição 5.1.1. Sejam R um anel e $\mathcal{S}$ a família dos R-módulos à esquerda simples. O *radical de Jacobson* de R é definido como sendo o conjunto

$$J(R) := \cap_{V \in \mathcal{S}} \, An_R(V)$$

.

Observamos que o radical de Jacobson de um anel é de fato um ideal bilateral. Note que se V é um R-módulo, então $An_R(V)$ é um ideal bilateral. Assim, $J(R)$ está definido como uma intersecção de ideais bilaterais, sendo assim ele próprio um ideal bilateral de R. Além disso, claramente $1_R \notin J(R)$, ou seja, $J(R) \neq R$.

Observamos também que $J(R/J(R)) = 0$. Esta condição sempre deve ser satisfeita para que um ideal possa ser um radical, mas como não introduzimos o conceito formal de radical de um anel, precisamos verificar esta igualdade. De fato, basta observar que todo R-módulo à esquerda simples é também um $R/J(R)$-módulo simples, com ação dada por $(r + J(R))v = rv$, para todo $v \in V$, onde V é um R-módulo à esquerda simples. Esta ação está bem definida, pois $J(R) \subseteq An_R(V)$, por definição.

A discussão acima nos diz que, num certo sentido, o anel $R/J(R)$ não possui elementos indesejáveis ao estudo da semissimplicidade de um anel, conferindo ao radical de Jacobson um papel importante neste estudo.

Existem várias formas equivalentes de definir o radical de Jacobson de um anel. No que segue, vamos apresentar algumas destas formas, as quais dependem muito mais da estrutura interna do anel do que de seus módulos. Isto vai também na direção de facilitar o cálculo do radical de Jacobson, quando necessário. Para facilitar nossa escrita, vamos fixar alguma notação antes.

Observação 5.1.2. Seja R um anel. Escreveremos:

(i) $\mathcal{M}ax_l(R)$, para denotar a família de todos os ideais à esquerda maximais de R;

(ii) $\mathcal{M}ax_r(R)$, para denotar a família de todos os ideais à direita maximais de R.

Observe agora que se $x \in J(R)$ e $\mathfrak{M} \in \mathcal{M}ax_l(R)$, então $R/\mathfrak{M}$ é um R-módulo à esquerda simples, de onde segue que $x(R/\mathfrak{M}) = 0$, ou seja, $xR \subseteq \mathfrak{M}$, ou ainda, $x \in \mathfrak{M}$. Portanto, temos

$$x \in \cap\{\mathfrak{M} : \mathfrak{M} \in \mathcal{M}ax_l(R)\}$$

Reciprocamente, se $x \in \cap\{\mathfrak{M} : \mathfrak{M} \in \mathcal{M}ax_l(R)\}$ e V é um R-módulo à esquerda simples, então sabemos que $V = Rv$, para todo elemento não nulo $v \in V$, e que $An_R(v) \in \mathcal{M}ax_l(R)$. Logo, $xv = 0$, para todo elemento $v \in V \setminus \{0\}$. Portanto, $xV = 0$ e temos que $x \in An_R(V)$. Como V foi tomado arbitrário, segue finalmente que $x \in J(R)$.

A argumentação acima produz o nosso próximo resultado que muitas vezes aparece como uma definição do radical de Jacobson de uma anel.

Proposição 5.1.3. *Seja R um anel. Então, $J(R) = \cap\mathcal{I}$, onde $\mathcal{I}$ percorre a família dos ideais à esquerda maximais de R.*

Embora esta caracterização do radical de Jacobson seja mais conveniente para se fazer cálculos, não decorre imediatamente dela que $J(R)$ seja um ideal bilateral. Aliás, esta caracterização do radical de Jacobson via interseção de ideais à

esquerda maximais, se tomada como definição, deveria produzir o conceito de radical de Jacobson à esquerda e, de modo análogo, teríamos o conceito de radical de Jacobson à direita, como sendo a interseção de todos os ideais à direita maximais de R. Felizmente, pode-se mostrar que estas duas interseções de fato coincidem, e o conceito de radical de Jacobson se torna simétrico. Para ver que estas interseções coincidem, vamos usar uma nova caracterização do radical de Jacobson ao nível de seus elementos.

Proposição 5.1.4. *Seja R um anel. As seguintes afirmações são equivalentes:*

(i) $x \in J(R)$.

(ii) $1 - rx$ *possui um inverso à esquerda, para todo* $r \in R$.

(iii) $1 - rxt$ *é um elemento invertível em* R, *para todos* $r, t \in R$.

Demonstração. $(i) \Rightarrow (ii)$ Suponhamos que exista $r \in R$ tal que $1-rx$ não possui um inverso à esquerda em R. Assim, $R(1 - rx)$ é um ideal à esquerda próprio de R e, portanto, deve existir $\mathfrak{M} \in \mathcal{M}ax_l(R)$ tal que $R(1 - rx) \subseteq \mathfrak{M}$. Mas então, como $1 - rx \in \mathfrak{M}$ e $x \in J(R) = \cap\{\mathfrak{N} : \mathfrak{N} \in \mathcal{M}ax_l(R)\}$ (Proposição 5.1.3), segue que $1 \in \mathfrak{M}$, o que não pode ocorrer.

$(ii) \Rightarrow (i)$ Seja $x \in R$ e suponhamos que $1 - rx$ possua um inverso à esquerda, para toda a escolha de $r \in R$. Queremos mostrar que $x \in \cap\{\mathfrak{M} : \mathfrak{M} \in \mathcal{M}ax_l(R)\}$. De fato, pois se existir $\mathfrak{M} \in \mathcal{M}ax_l(R)$ tal que $x \notin \mathfrak{M}$, então $\mathfrak{M} + Rx = R$, de onde segue que existem elementos $a \in \mathfrak{M}, r \in R$ tais que $a + rx = 1$, ou seja, $1 - rx = a \in \mathfrak{M}$, o que não pode ocorrer.

$(i) \Rightarrow (iii)$ Sejam $x \in J(R)$ e $r, t \in R$. Então, $xt \in J(R)$ e $1 - r(xt)$ tem inverso à esquerda, pela argumentação acima. Assim, existe $s \in R$ tal que $s(1 - rxt) = 1$. Agora, como $-rxt \in J(R)$, segue que $1 - s(-rst)$ possui inverso à esquerda, ou seja, existe $u \in R$ tal que $u(1 - s(-rxt)) = 1$. Mas então $s = 1 + srxt$ e daí, $1 = u(1 - s(-rst)) = u(1 + srxt) = us$, de onde segue que s é um elemento invertível em R, por ter inverso tanto à esquerda como à direita e, além disso, $u = 1 - rxt$. Portanto, $1 - rxt$ é um elemento invertível em R.

$(iii) \Rightarrow (i)$ Se $1 - rxt$ é um elemento invertível em R, para toda a escolha de $r, t \in R$, então escolhendo $t = 1$, obtemos que $1 - rx$ tem inversa à esquerda, para todo $r \in R$, e segue que $x \in J(R)$, pela argumentação feita em $(ii) \Rightarrow (i)$. □

A simetria do ítem (iii) da Proposição 5.1.4 garante então o seguinte resultado.

Corolário 5.1.5. *Seja R um anel. Então,*

$$J(R) = \cap\{\mathfrak{M} : \mathfrak{M} \in \mathcal{M}ax_l(R)\} = \cap\{\mathfrak{N} : \mathfrak{N} \in \mathcal{M}ax_r(R)\}$$

O próximo resultado é um fato muito utilizado em teoria de anéis, o qual confere uma maior importância ao radical de Jacobson.

Proposição 5.1.6. (Lema de Nakayama) *Seja R um anel e M um R-módulo à esquerda finitamente gerado. Se $J(R)M = M$, então $M = 0$.*

Demonstração. Seja $M = Rm_1 + \cdots + Rm_s$ um R-módulo não nulo, onde $\{m_1, ..., m_s\}$ é um conjunto minimal de geradores. Então, $m_1 \neq 0$ e podemos tomar um submódulo maximal de M que contém m_1, o qual existe pelo Lema de Zorn. De fato, a família de submódulos próprios de M que contém Rm_1 é um sistema indutivo (prove isto!). Vamos chamar um tal submódulo de N. Assim, $V = M/N$ é um R-módulo à esquerda simples, de onde segue que $J(R)V = 0$. Portanto, $J(R)M \subseteq \mathcal{N}uc\,\pi$, onde $\pi : M \to M/N$ é a projeção canônica. Portanto, $J(R)M \neq M$, e o Lema de Nakayama está provado. □

Cabe observar que a hipótese de M ser finitamente gerado não pode ser enfraquecida. De fato, pois se

$$M = \mathbb{Z}_{(p)} := \{\frac{a}{b} : p \text{ não divide } b\}$$

então M é um $\mathbb{Z}$-submódulo de $\mathbb{Q}$, onde (p) denota o ideal de $\mathbb{Z}$ gerado pelo primo p. Assim, podemos mostrar que $(p)\mathbb{Q} = \mathbb{Q}$, mas $\mathbb{Q} \neq 0$.

Chamamos a atenção para o fato de que M ter sido tomado finitamente gerado como R-módulo à esquerda foi fundamental na argumentação feita acima, quando usamos que a família de R-submódulos de M que contém Rm_1 é um sistema indutivo.

Uma consequência importante do Lema de Nakayama, e que nos será útil mais a frente, é o fato que $J(R)$ é um ideal nilpotente, sempre que R for um anel artiniano à esquerda. Mais precisamente, temos o seguinte.

Definição 5.1.7. Sejam R um anel e I um ideal (ideal à esquerda, ideal á direita) de R. Dizemos que I é *nilpotente*, se existir $n \geq 1$ tal que $I^n = 0$, onde $I^n := \left\{ \sum_{\text{finita}} a_1 a_2 ... a_n : a_i \in I \right\}$. O menor inteiro positivo n tal que $I^n = 0$ é chamado de *índice de nilpotência* de I.

Exemplo 5.1.8. Seja R um anel comutativo e M um R-módulo não nulo. Então podemos mostrar facilmente que

$$\begin{pmatrix} R & M \\ 0 & R \end{pmatrix} := \left\{ \begin{pmatrix} r & m \\ 0 & r \end{pmatrix} : r \in R, m \in M \right\}$$

é um anel comutativo. Com esta notação,

$$I = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix}$$

é um ideal nilpotente com índice de nilpotência igual a 2, pois é fácil ver que $I^2 = 0$ e $I \neq 0$.

Podemos então enunciar o nosso resultado.

Proposição 5.1.9. *Seja R um anel artiniano à esquerda. Então $J(R)$ é um ideal nilpotente.*

Demonstração. Como todo ideal (bilateral) é também um ideal à esquerda, a cadeia descendente

$$J(R) \supseteq J(R)^2 \supseteq \cdots \supseteq J(R)^n \supseteq \cdots$$

deve estacionar, ou seja, existe índice m tal que $J(R)^m = J(R)^{m+1}$. Seja $I = J(R)^m$. Afirmamos que $I = 0$. De fato, pois do contrário, como $I^2 = I$, a família de ideais à esquerda K de R tais que $IK \neq 0$ seria não vazia e, portanto, teria um elemento minimal, pela artianidade de R. Chamando um tal elemento de L, segue que $L = Ry$, para todo $y \in L \setminus \{0\}$. Mas então, $IL = IRy = Iy = L$, pois Iy é um R-submódulo não nulo de L tal que $I(Iy) = I^2y = Iy \neq 0$. Portanto,

$$J(R)L = J(R)IL = IL = L$$

e, como $L = Ry$ é finitamente gerado, segue do Lema de Nakayama (Proposição 5.1.6) que $L = 0$, uma contradição. □

O resultado acima não vale em geral, sem a hipótese de artianidade de R. Para ver isto, considere R o anel das matrizes infinitas $\mathbb{N} \times \mathbb{N}$ triangulares superiores, com apenas um número finito de entradas não nulas em um corpo. Neste caso, é possível mostrar que $J(R)$ é o conjunto de todas tais matrizes que possuem as entradas da diagonal principal nulas e que $J(R)$ não é um ideal nilpotente.

O conceito de nilpotência pode ser feito para elementos. Com ele, podemos relaxar um pouco a condição de nilpotência para ideais.

Definição 5.1.10. Seja R um anel e $x \in R$. Então dizemos que x é um *elemento nilpotente*, se existir $n \geq 1$ tal que $x^n = 0$. O menor tal inteiro é chamado de *índice de nilpotência de x*. Um ideal I (resp. ideal à esquerda, ideal à direita)de R é dito um *nil ideal* (resp. nil ideal à esquerda, nil ideal à direita), se todo elemento de I é nilpotente.

Note que todo ideal nilpotente é um nil ideal, mas a recíproca nem sempre vale. Por exemplo, tomando $R = \frac{\mathbb{Z}[x_1,x_2,,x_3,\ldots]}{<x_1^2,x_2^2,x_3^3,\ldots>}$ e I, o ideal de R gerado pelos elementos $\overline{x_1}, \overline{x_2}, \overline{x_3}, \ldots$, então I é claramente um nil ideal, mas não é nilpotente. Também, no exemplo das matrizes infinitas dado acima, o radical de Jacobson é de fato um nil ideal que não é nilpotente.

Podemos enunciar o seguinte resultado geral.

Lema 5.1.11. *Sejam R um anel e I um nil ideal à esquerda de R. Então, $I \subseteq J(R)$.*

Demonstração. Sejam $x \in I$ e $r \in R$. Como I é um nil ideal à esquerda, segue que rx é um elemento nilpotente, pois $rx \in I$. Digamos que o índice de nilpotência de rx seja n. Então, temos

$$(1 + rx + (rx)^2 + (rx)^3 + \cdots + (rx)^{n-1})(1 - rx) = 1$$

de onde segue que $1-rx$ possui inverso à esquerda. Consequentemente, aplicando a Proposição 5.1.4, obtemos que $x \in J(R)$, pois $r \in R$ foi tomado arbitrário. □

Finalizamos esta seção observando que segue da Proposição 5.1.9 e do Lema 5.1.11, que o radical de Jacobson é o maior ideal nilpotente de um anel artiniano à esquerda. Portanto, o ideal utilizado por Wedderburn está definido para esta classe de anéis, possibilitando que seus resultados sejam generalizados para estes anéis, como foi feito por Artin.

5.2 J-semissimplicidade

Um dos objetivos desta seção é o de esclarecer a frase dita na introdução deste capítulo, onde se afirma que num certo sentido, o radical de Jacobson mede o quão longe um anel está de ser semissimples.

Teorema 5.2.1. *Seja R um anel. Se R é semissimples, então $J(R) = 0$. A recíproca é verdadeira se R for artiniano à esquerda.*

Demonstração. Suponhamos R semissimples. Então ${}_RR$ é semissimples, de onde segue que ${}_RR$ é uma soma (direta) de R-módulos à esquerda simples. Assim, se $x \in J(R)$, x anula todos estes módulos simples, ou seja, $xR = 0$, de onde se obtém que $x = 0$.

Reciprocamente, suponhamos que R é artiniano à esquerda e $J(R) = 0$. Consideremos I_1 um ideal à esquerda minimal de R (o qual existe pela artinianidade de ${}_RR$). Vamos mostrar que I_1 é um somando direto de ${}_RR$. De fato, pois como $J(R) = 0$, deve existir $\mathfrak{M} \in \mathcal{M}ax_l(R)$ que não contém I_1, pelo Teorema 5.1.3. Assim, devemos ter $\mathfrak{M} \cap I_1 = 0$, pela simplicidade de I_1. Além disso, pela maximalidade de $\mathfrak{M}$, segue que $\mathfrak{M} + I_1 = R$, ou seja, $R = \mathfrak{M} \oplus I_1$.

Agora é só observar que $\mathfrak{M}$ é artiniano à esquerda, por ser submódulo de um módulo artiniano, e repetir a argumentação acima, com $\mathfrak{M}$ em lugar de ${}_RR$, para obter ${}_RR = I_1 \oplus I_2 \oplus \cdots \oplus I_r$, onde I_j é um ideal à esquerda minimal de R. Portanto ${}_RR$ é semissimples, como queríamos mostrar. □

Note que na argumentação acima só usamos a artinianidade de R para garantir a existência de ideais minimais. Assim, o seguinte corolário fica evidente.

Corolário 5.2.2. *Seja R um anel tal que $J(R) = 0$. Então todo ideal à esquerda minimal, se existir, é um somando direto do módulo regular ${}_RR$.*

Observamos também que a hipótese de artianidade é fundamental na recíproca do teorema acima, pois

$$J(\mathbb{Z}) = \cap \left\{ \frac{\mathbb{Z}}{p\mathbb{Z}} : p \text{ é um primo} \right\} = 0$$

e $\mathbb{Z}$ não é semissimples, como visto antes.

Após esta discussão introdutória, apresentamos o conceito chave desta seção.

Definição 5.2.3. Seja R um anel. Dizemos que R é *Jacobson semissimples* (ou simplesmente, *J-semissimples*), se $J(R) = 0$.

Usando esta terminologia, o Teorema 5.2.1 pode ser reescrito na seguinte forma.

Corolário 5.2.4. *Seja R um anel. Então as seguintes afirmações são equivalentes:*

(i) R é semissimples;

(ii) R é artiniano à esquerda e J-semissimples.

O seguinte resultado é imediato.

Corolário 5.2.5. *Seja R um anel artiniano à esquerda. Então, $R/J(R)$ é o maior anel fator de R que é semissimples.*

Portanto, se R é um anel artiniano à esquerda, segue do Teorema de Wedderburn-Artin que

$$R/J(R) \simeq \oplus_{i=1}^{m} \mathcal{M}_{n_i}(D_i)$$

onde $n_i = dim_{D_i}(V_i)$, $D_i = End_R(V_i)$ e $\{V_1, V_2, ..., V_m\}$ é um sistema de representantes das classes de isomorfismos de R-módulos à esquerda simples.

Como já foi mencionado antes, nenhuma das condições de cadeia para módulos implicam na outra, em geral. Mas no caso do módulo regular ${}_RR$ (resp. R_R), surpreendentemente, a condição de cadeia descendente implica a condição de cadeia ascendente. Isto foi observado independentemente por Hopkins e Levistky, aproximadamente dez anos após os trabalhos de Artin que estenderam o Teorema de Wedderburn, usando ambas as condições de cadeia em lugar da finito-dimensionalidade usada originalmente por este último. Vamos finalizar esta seção, apresentado uma versão mais elementar do resultado de Hopkins-Levistky.

Teorema 5.2.6. (Teorema de Hopkins-Levistky - versão fraca) *Seja R um anel. Se R é artiniano à esquerda, então R é noetheriano à esquerda.*

Demonstração. Suponhamos R artiniano à esquerda. Segue então da Proposição 5.1.9 que $J(R)$ é nilpotente, digamos, com índice de nilpotência n. Assim, $J(R)^n = 0$, e podemos considerar a cadeia decrescente

$$R = J(R)^0 \supset J(R)^2 \supset \cdots \supset J(R)^n = 0.$$

Para obter o resultado desejado, vamos mostrar que cada um dos R-módulos à esquerda $N_i = J^i/J^{i+1}$ tem comprimento finito. De fato, como quocientes de um anel artiniano à esquerda, N_i é artiniano, para cada índice i. Observe agora que N_i é anulado por $J(R)$, de onde segue que N_i é um $R/J(R)$-módulo. Como $R/J(R)$ é semissimples, pelo Corolário 5.2.5, segue que N_i é semissimples como $R/J(R)$-módulo. Como a estrutura de R-módulo e de $R/J(R)$-módulo de N_i coincidem, segue que cada um dos R-módulos N_i é semissimples e artiniano, de onde segue que possuem comprimento finito, pelos resultados do Capítulo 3. Isto mostra que o módulo regular ${}_RR$ possui uma série de composição, de onde obtemos que ${}_RR$ é noetheriano, ou seja, R é um anel noetheriano à esquerda, como queríamos mostrar. □

Note que $\mathbb{Z}$ é um noetheriano mas não é artiniano. Logo, a condição de cadeia ascendente não implica a condição descendente nem mesmo para anéis. Assim, para anéis com unidade, a artinianidade é uma condição mais forte que a noetherianidade.

Exercícios

1. Seja $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, onde $n = p_1^{e_1} \dots p_k^{e_k}$, com $p_i \neq p_j$, se $i \neq j$. Mostre que:
   (i) Os ideais de $\mathbb{Z}_n$ são da forma $< a > / < n >$, onde $a \mid n$ em $\mathbb{Z}$.
   (ii) Os ideais maximais de $\mathbb{Z}_n$ são da forma $< p_i > / < n >$.
   (iii) $J(\mathbb{Z}_n) =< m > / < n >$.
   (iv) Como $\mathbb{Z}_n$ é um $\mathbb{Z}$-módulo artiniano (por ser finito), conclua que $\mathbb{Z}_n$ é semissimples se, e somente se, n é livre de quadrados.

2. Seja R um anel. Mostre que $J(\mathcal{M}_n(R)) = \mathcal{M}_n(J(R))$. Mostre também que se $R = \Pi_{i\in I}\ R_i$, então $J(R) = \Pi_{i\in I}\ J(R_i)$. O que se pode dizer, a partir deste resultado, sobre o radical de Jacobson de anéis semissimples?

3. Sejam R um anel e I um ideal de R tal que R/I é um anel J-semissimples. Mostre que $I \supseteq J(R)$. Conclua daí que $J(R)$ é o menor ideal I de R tal que o anel fator R/I é J-semissimples.

4. Sejam R e S dois anéis e $f : R \to S$ um epimorfismo de anéis. Mostre que $f(J(R)) \subseteq J(S)$.

5. Mostre que a soma de ideais nilpotentes de um anel R é um ideal nilpotente. Veja que o mesmo resultado não vale para nil ideais, em geral. Se R é artiniano, então todo nil ideal é nilpotente e, neste caso, a soma de nil ideais é um nil ideal.

Referências Bibliográficas

[1] ARTIN, E. Zur Theorie der hyperkomplexen Zahlen. *Abh. Math. Sem. Univ. Hamburgo*, v. 5, p. 251-260, 1927.

[2] ARTIN, E. The influence of J. H. M. Wedderburn on the development of modern algebra. *Bull. Amer. Math. Soc.*, v. 56, n. 1, p. 65-72, 1950.

[3] DENNIS,R. K.; FARB, B. *Noncommutative Algebra*. New York: Springer-Verlang, 1993.

[4] DORNHOFF, L., *Group Representation Theory - Part A: Ordinary Representation Theory*. New York: Marcel Dekker, 1971.

[5] DROZD, Y. A.; KIRICHENKO, V. V.; *Finite Dimensional Algebras*. Berlin Heidelberg: Springer Verlang, 1994.

[6] FERRERO, M.; *Teoremas de Estructura para Álgebras Semissimples, XV Escuela Venezoelana de Matemáticas*. Mérida: 2002.

[7] GOLDMAN, O. A characterization of semi-simple rings with descending chain condiction. *Bull. Amer. Math. Soc.*, v. 52, n. 12, p. 1021 - 1027, 1946.

[8] HOPKINS, C. Rings with minimal conditions on left ideals. *Ann. of Math.*, v. 40, n. 3, p. 712-730, 1939.

[9] LAM, T. Y.; *A First Course in Noncommutative Rings*. New York: Springer-verlang, 1991.

[10] LAMBEK, J. *Lectures on Modules and Rings*. New York: Chelsea Publishing Co., 1976.

[11] LAVITZKI, J. On rings which satisfy the minimum condition for the right-hand ideals. *Compositio Math.*, v. 7, p. 214 - 222, 1939.

[12] MILIES, C. P.; *Anéis e módulos*. São Paulo: Edusp, 1972.

[13] MILIES, C. P.; SEHGAL, S. K.; *An Introduction to Group Rings*. Dordrecht: Kluwer Academic Publishers, 2002.

[14] MOLIEN, T. Über systeme höher complexes zahlen, *Mathematische Annalen*, v. 41, p. 83 - 156, 1893.

[15] RIBENBOIM, P.; *Rings and Modules*. Interscience Publishers, 1969.

[16] WEDDERBURN, J. H. M. On hypercomplex numbers. *Proc. London Math. Soc.*, v. 6, p. 77-117, 1908