Miguel Ângelo Couto

Anéis Primitivos e Teorema da Densidade

Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
2013

Agradecimentos

Em primeiro lugar queria agradecer ao meu orientador, o Professor Doutor Christian Lomp, por toda a ajuda e paciência com que me orientou ao longo de todo o trabalho. Foi um trabalho com várias fases, durante as quais se mostrou sempre disponível para me esclarecer todas as dúvidas e, por isso, sinto-me privilegiado pela oportunidade de ter podido trabalhar consigo. Um muito Obrigado.

Queria também agradecer aos meus amigos que em várias alturas se mostraram disponíveis para me ajudar ao ler a minha tese em busca de erros matemáticos e ortográficos. A todos vocês, o mais sincero Obrigado.

Prefácio

Na Teoria dos Anéis estudam-se várias classes de anéis com propriedades interessantes, os anéis simples e os anéis semisimples, os anéis primos e os anéis semiprimos. Esta tese foca-se sobre uma classe de anéis chamados *anéis primitivos*, que são anéis que possuem um módulo simples e fiel; esta tese tem como objectivo estudá-los e aprofundar várias das suas propriedades. Nesta tese será também estudado o *Teorema da Densidade*, que está bastante relacionado com os anéis primitivos e que tem inúmeros corolários que pretendemos aprofundar.

O Capítulo 1 reúne os conceitos básicos e resultados elementares da Teoria dos Anéis que são necessários para compreender os capítulos seguintes e no Capítulo 2 são abordados anéis de polinómios que são fontes de exemplos muito importantes de anéis não comutativos e que (com algumas condições) servirão também como exemplo de anéis primitivos.

No Capítulo 3 é introduzido o conceito fulcral desta tese - os anéis primitivos - e são estudadas algumas propriedades simples destes anéis, bem como alguns exemplos. Para além disso, é abordada uma questão que surge directamente da definição de anel primitivo: a questão da unicidade do módulo simples fiel. Por fim, são estudados ainda alguns exemplos de anéis livres que são primitivos e é analisada a noção de anel primitivo noutras classes de anéis.

O Capítulo 4 é dedicado à segunda parte importante desta tese, o Teorema da Densidade de Jacobson, que tem uma grande importância e constitui um resultado basilar na Teoria dos Anéis Não-comutativos. Neste capítulo é ainda esclarecida a origem topológica do uso do termo "densidade" neste contexto. Além disso, iremos ver que o Teorema da Densidade oferece uma caracterização dos anéis primitivos, o Teorema da Estrutura dos Anéis Primitivos, bem como alguns outros corolários que também serão aprofundados neste capítulo.

Miguel Couto

Conteúdo

1 Teoria de Anéis e Módulos Elementar

Neste Capítulo vamos abordar alguns conceitos e resultados básicos da Teoria de Anéis e Módulos, que serão necessários para compreender os capítulos seguintes.

Definição 1.1 *Um anel é um conjunto não vazio R com duas operações binárias $+$ (a adição) e $\cdot$ (a multiplicação) que satisfazem as seguintes propriedades:*

$(R, +, 0)$ é um grupo abeliano:

1. $\forall a, b, c \in R, (a + b) + c = a + (b + c)$
2. $\forall a, b \in R, a + b = b + a$
3. $\exists\, 0 \in R : \forall a \in R, a + 0 = a$
4. $\forall a \in R, \exists - a \in R : a + (-a) = 0$

A multiplicação é associativa:

5. $\forall a, b, c \in R, (a \cdot b) \cdot c = a \cdot (b \cdot c)$

A multiplicação é distributiva em relação à adição:

6. $\forall a, b, c \in R, a \cdot (b + c) = a \cdot b + a \cdot c$
7. $\forall a, b, c \in R, (a + b) \cdot c = a \cdot c + b \cdot c$

O elemento neutro da adição 0 chama-se zero do anel R. Um anel diz-se unitário se a multiplicação tem elemento neutro, ou seja, se existe $1 \in R$ tal que

$$a \cdot 1 = a = 1 \cdot a, \quad \forall a \in R.$$

Este elemento de R diz-se a identidade de R.

Ao longo de toda esta tese, só iremos considerar anéis R unitários com identidade $1 \neq 0$. Logo, não incluímos o anel nulo $R = 0$. O símbolo da multiplicação é omitido passando a escrever-se ab em vez de $a \cdot b$.

Um anel diz-se *comutativo* se a multiplicação for comutativa:

$$ab = ba, \quad \forall a, b \in R.$$

Sejam R, S dois anéis. Uma aplicação $f : R \to S$ diz-se um *homomorfismo de anéis* se $\forall r_1, r_2 \in R$,

1. $f(r_1 + r_2) = f(r_1) + f(r_2)$

2. $f(r_1 r_2) = f(r_1)f(r_2)$

3. $f(1_R) = 1_S$

Um homomorfismo $f : R \to R$ diz-se um endomorfismo de R. Um homomorfismo bijectivo diz-se um isomorfismo.

O *núcleo* de um homomorfismo $f : R \to S$ é $\mathrm{Ker}(f) = \{r \in R : f(r) = 0\}$ e a *imagem* de f é $Im(f) = \{f(r) : r \in R\}$.

Um subconjunto A de um anel R diz-se um *subanel* se $\forall a, b \in A, a - b, ab \in A$. Um caso particular e importante dos subanéis são os ideais: $I \subset R$ diz-se um *ideal à esquerda* (resp. *à direita*) se

$$\forall a, b \in I, \forall r \in R, \qquad a - b \in I \text{ e } ra \in I \text{ (resp. } ar \in I).$$

Se I for um ideal à esquerda e à direita, diz-se um *ideal* (*bilateral*) de R. Por exemplo, o núcleo $\mathrm{Ker}(f)$ de um homomorfismo $f : R \to S$ é um ideal de R.

O resultado seguinte tem um papel muito importante na Teoria dos Anéis.

Lema 1.2 (Lema de Zorn) *Seja X um conjunto não vazio parcialmente ordenado. Se qualquer cadeia (de elementos de X) tem um majorante em X, então X tem pelo menos um elemento maximal.*

Este Lema é de facto equivalente ao Axioma da Escolha e a sua demonstração pode ser encontrada em [6, Theorem 9.3]. Vamos usar este resultado para demonstrar a Proposição seguinte.

Um ideal à esquerda I de R diz-se *maximal* se não existem ideais à esquerda não triviais entre I e R.

Proposição 1.3 (Teorema de Krull, 1929 [14]) *Qualquer anel R contém um ideal à esquerda maximal.*

Demonstração. Seja $X = \{I \text{ ideal à esquerda de } R : 1 \notin I\}$. Este conjunto é não vazio, porque contém o ideal nulo 0, e é parcialmente ordenado pela inclusão.

Seja $C = \{I_\lambda : \lambda \in \Lambda\}$ uma cadeia de elementos de X e consideremos

$$J = \bigcup_{\lambda \in \Lambda} I_\lambda.$$

Vamos ver que J é um majorante de C em X.

Em primeiro lugar, vejamos que $J \in X$: sejam $r \in R$ e $a, b \in J$ quaisquer; existem $\lambda, \mu \in \Lambda$ tais que $a \in I_\lambda$ e $b \in I_\mu$. Como C é totalmente ordenado, $I_\lambda \subseteq I_\mu$ ou $I_\mu \subseteq I_\lambda$, logo $a, b \in I_\mu$ ou $a, b \in I_\lambda$. Como ambos são ideais à esquerda, então

$$a - b, ra \in I_\mu \subset J \quad \text{ou} \quad a - b, ra \in I_\lambda \subset J.$$

Deste modo, J é um ideal à esquerda de R. Como $1 \notin I_\lambda, \forall \lambda \in \Lambda$, então $1 \notin J$. Portanto, $J \in X$.

Para além disso, claro que J é um majorante de qualquer elemento de C: $\forall \lambda, I_\lambda \subseteq J$. Ou seja, toda a cadeia de X tem um majorante em X. Pelo Lema de Zorn, X tem um elemento maximal, ou seja, R tem um ideal à esquerda maximal. □

Um argumento inteiramente análogo permite-nos concluir que qualquer anel contém também um ideal à direita maximal e um ideal bilateral maximal.

Observação: Note-se que a existência de identidade $1 \in R$ é essencial para a validade do resultado anterior: de facto, existem anéis sem identidade que não têm ideal à esquerda maximal. Um exemplo pode ser encontrado em [8].

Um anel R diz-se um *domínio* se $ab = 0 \Rightarrow a = 0 \vee b = 0$. Um domínio comutativo diz-se um *domínio integral*. Um elemento $a \in R$ diz-se *invertível à esquerda* (resp. *à direita*) se existe $b \in R$ tal que $ba = 1$ (resp. $ab = 1$). Se $a \in R$ for invertível à esquerda e à direita, diz-se *invertível*. R diz-se um *anel de divisão* se qualquer elemento não nulo for invertível. Um anel de divisão comutativo diz-se um *corpo*.

1.1 Módulos

Nesta secção, vamos introduzir a noção de *módulo* e alguns conceitos básicos relacionados.

Definição 1.4 *Seja R um anel. Um R-módulo à esquerda é um grupo abeliano $(M, +, 0_M)$ com acção escalar*

$$\cdot : R \times M \longrightarrow M$$

que satisfaz: $\forall r, s \in R$, $\forall m, n \in M$,

1. $r \cdot (s \cdot m) = (rs) \cdot m$
2. $(r + s) \cdot m = r \cdot m + s \cdot m$
3. $r \cdot (m + n) = r \cdot m + r \cdot n$
4. $1 \cdot m = m$

Exemplos.

1. Os módulos são claramente uma generalização dos espaços vectoriais, nos quais os escalares em vez de pertencerem a um anel de divisão pertencem a um anel. Deste modo, os espaços vectoriais são exemplos de módulos.

2. Qualquer grupo abeliano $(M, +, 0)$ é um módulo sobre $\mathbb{Z}$, com acção definida por

$$n \cdot m = \underbrace{m + \ldots + m}_{n \text{ vezes}} \qquad \text{com } n \in \mathbb{N} \text{ e } m \in M.$$

   E $0 \cdot m = 0$ e para inteiros negativos n definimos

$$n \cdot m = (-n) \cdot (-m) = \underbrace{(-m) + \ldots + (-m)}_{-n \text{ vezes}}$$

   Facilmente se vê que esta acção define uma estrutura de $\mathbb{Z}$-módulo em M.

3. Qualquer anel R é um módulo sobre si próprio.

   Dado um anel $(R, +, \cdot)$, é fácil ver que o produto no anel R verifica as 4 propriedades de acção escalar num módulo, ou seja, R tem estrutura de R-módulo (R é um módulo sobre si próprio!). Esta relação entre módulos e anéis permite transportar resultados da teoria dos módulos para a teoria dos anéis.

   Mais geralmente, um ideal à esquerda I de R tem estrutura de R-módulo com a acção definida como o produto em R:

$$\text{dados } r \in R \text{ e } a \in I, \text{ temos } ra \in I$$

   logo a acção está bem definida e satisfaz as 4 propriedades desejadas (porque é o produto em R).

4. Produto Cartesiano

   Dada uma família de R-módulos $\{M_i\}_{i \in I}$, o produto cartesiano $\prod_{i \in I} M_i$ é o conjunto de todas as funções $f : I \to \bigcup_{i \in I} M_i$ tal que $f(i) \in M_i, \forall i \in I$. O produto cartesiano tem também estrutura de R-módulo:

   - A soma define-se componente a componente: dados $f, g \in \prod_{i \in I} M_i$, define-se $\forall i \in I, (f + g)(i) = f(i) + g(i) \in M_i$ (pela soma em M_i).
   - A acção de R também se define em cada componente: dado $f \in \prod_{i \in I} M_i$, define-se $\forall i \in I, (r \cdot f)(i) = r \cdot f(i)$ (pela acção de R em M_i).

No caso particular de termos uma colecção finita de R-módulos $M_1, \ldots, M_n$, o produto cartesiano é dado por

$$\begin{aligned}\prod_{i=1}^{n} M_i &= \left\{ f : \{1, \ldots, n\} \to \bigcup_{i=1}^{n} M_i : f(i) \in M_i \right\} \\ &= \{ f = (f(1), \ldots, f(n)) : f(i) \in M_i \} \\ &= \{ (m_1, \ldots, m_n) : m_i \in M_i \}\end{aligned}$$

e é usualmente também representado por $M_1 \times \ldots \times M_n$. Pelo que foi dito também ele tem estrutura de R-módulo. Por fim, o produto cartesiano de n cópias de um módulo M é usualmente representado por $M \times \ldots \times M = M^n$.

Dados dois R-módulos à esquerda M e N, uma aplicação $f : M \longrightarrow N$ diz-se um homomorfismo de R-módulos[1] (ou aplicação R-linear) se

1. $(m+n)f = (m)f + (n)f, \qquad \forall m, n \in M$
2. $(r \cdot m)f = r \cdot (m)f, \qquad \forall r \in R, \forall m \in M$

O conjunto dos homomorfismos entre M e N escreve-se $Hom_R(M, N)$. Um homomorfismo bijectivo diz-se um *isomorfismo*. Um homomorfismo $f : M \to M$ diz-se um *endomorfismo* de M e o conjunto dos endomorfismos de M escreve-se $\mathrm{End}_R(M)$.

O *núcleo* de um homomorfismo $f : M \longrightarrow N$ é o conjunto

$$\mathrm{Ker}(f) = \{ m \in M \mid (m)f = 0_N \}$$

e a *imagem* de f é

$$\mathrm{Im}(f) = \{ (m)f \in N \mid m \in M \}.$$

Proposição 1.5 *Sejam R um anel e M um grupo abeliano. Então, M é um R-módulo à esquerda se e só se existe um homomorfismo de anéis*

$$\varphi : R \longrightarrow \mathrm{End}_{\mathbb{Z}}(M).$$

Demonstração. Supondo que M é um R-módulo à esquerda, definimos

$$\begin{aligned}\varphi : R &\to \mathrm{End}_{\mathbb{Z}}(M) \\ r &\mapsto \varphi_r : M \to M \\ &\qquad m \mapsto r \cdot m, \ \forall m \in M.\end{aligned}$$

[1] Ao longo desta tese, o valor que um homomorfismo de módulos $f : M \to N$ toma num elemento $m \in M$ será representado por $(m)f$, isto é, aplicando a função à direita do elemento. Todas as restantes funções como homomorfismos de anéis e derivadas seguirão a notação usual.

Para cada $r \in R$, φ_r é um $\mathbb{Z}$-homomorfismo de M: $\forall m_1, m_2, m \in M$,

$$\varphi_r(m_1 + m_2) = r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2 = \varphi_r(m_1) + \varphi_r(m_2).$$

$$\varphi_r(nm) = r \cdot (nm) = r \cdot (\underbrace{m + \ldots + m}_{n \text{ vezes}}) = \underbrace{r \cdot m + \ldots + r \cdot m}_{n \text{ vezes}} = n(r \cdot m) = n\varphi_r(m)$$

para $n \geq 0$. Para n negativo, a igualdade $\varphi_r(nm) = n\varphi_r(m)$ prova-se de forma análoga.

Vejamos que φ é um homomorfismo de anéis: $\forall m \in M$,

$$\varphi_{r+s}(m) = (r+s) \cdot m = r \cdot m + s \cdot m = \varphi_r(m) + \varphi_s(m) = (\varphi_r + \varphi_s)(m)$$

$$\varphi_{rs}(m) = (rs) \cdot m = r \cdot (s \cdot m) = \varphi_r(s \cdot m) = \varphi_r(\varphi_s(m)) = (\varphi_r \circ \varphi_s)(m)$$

logo

$$\varphi_{r+s} = \varphi_r + \varphi_s \qquad \text{e} \qquad \varphi_{rs} = \varphi_r \circ \varphi_s.$$

Para além disso, $\varphi_1(m) = 1 \cdot m = m$, donde $\varphi_1 = id_M$.

Reciprocamente, dado um homomorfismo de anéis $\varphi : R \to \mathrm{End}_{\mathbb{Z}}(M)$, definimos a acção

$$r \cdot m = \varphi(r)(m), \qquad \forall r \in R, \forall m \in M.$$

Logo, $\forall r, s \in R, \forall m, n \in M$:

1. $(rs) \cdot m = \varphi(rs)(m) = (\varphi(r) \circ \varphi(s))(m) = \varphi(r)(\varphi(s)(m)) = r \cdot (s \cdot m)$
2. $(r+s) \cdot m = \varphi(r+s)(m) = (\varphi(r) + \varphi(s))(m) = \varphi(r)(m) + \varphi(s)(m) = r \cdot m + s \cdot m$
3. $r \cdot (m+n) = \varphi(r)(m+n) = \varphi(r)(m) + \varphi(r)(n) = r \cdot m + r \cdot n$
4. $1_R \cdot m = \varphi(1_R)(m) = id_M(m) = m$

Logo, M é um R-módulo à esquerda. □

Tendo em conta a Proposição anterior, o anulador de um R-módulo M define-se por

$$\mathrm{Ann}(M) = \mathrm{Ker}(\varphi) = \{r \in R : \varphi_r \equiv 0\} = \{r \in R : r \cdot m = 0, \forall m \in M\}.$$

Daqui resulta imediatamente que o anulador é um ideal de R.

Para além disso, o módulo M diz-se fiel se φ for injectiva, ou seja, $\mathrm{Ann}(M) = 0$; por outras palavras, o único elemento de R que anula todos os elementos de M é o zero. Então, M é fiel se e só se R é isomorfo a $\varphi(R)$, um subanel de $\mathrm{End}_{\mathbb{Z}}(M)$.

Dado um R-módulo à esquerda M, um R-submódulo de M é um subgrupo aditivo N de M tal que

$$\forall a \in R,\ \forall n \in N, \quad a \cdot n \in N$$

e escreve-se $N \leq M$. Neste caso, pode definir-se o módulo quociente: o grupo quociente M/N é também um R-módulo à esquerda com acção definida por

$$\forall a \in R,\ \forall m + N \in M/N, \quad a \cdot (m + N) = a \cdot m + N$$

e dizemos que M/N é o módulo quociente: $\forall m, n \in M, \forall a, b \in R$,

1. A acção está bem definida: se $m + N = n + N$, então $m - n \in N$ e, sendo N um submódulo, $a \cdot (m - n) = a \cdot m - a \cdot n \in N$, logo $a \cdot m + N = a \cdot n + N$.
2. $a \cdot (b \cdot (m + N)) = a \cdot (b \cdot m + N) = a \cdot (b \cdot m) + N = (ab) \cdot m + N = (ab) \cdot (m + N)$
3. $(a + b) \cdot (m + N) = (a + b) \cdot m + N = (a \cdot m + b \cdot m) + N =$
   $(a \cdot m + N) + (b \cdot m + N) = a \cdot (m + N) + b \cdot (m + N)$
4. $a \cdot ((m+N)+(n+N)) = a \cdot ((m+n)+N) = a \cdot (m+n)+N = (a \cdot m+a \cdot n)+N =$
   $(a \cdot m + N) + (a \cdot n + N) = a \cdot (m + N) + a \cdot (n + N)$
5. $1 \cdot (m + N) = 1 \cdot m + N = m + N$

Exemplo: O núcleo e a imagem de um homomorfismo $f : M \longrightarrow N$ são, respectivamente, submódulos de M e N.

Observação 1: No caso particular do R-módulo R, um R-submódulo é um ideal à esquerda de R (e o recíproco também vale). Neste caso, se I é um ideal à esquerda de R, então o grupo abeliano R/I tem estrutura de R-módulo, com acção

$$a \cdot (b + I) = ab + I.$$

Proposição 1.6 *Seja I um ideal à esquerda de R. $J = \mathrm{Ann}(R/I)$ é o maior ideal bilateral contido em I.*

Demonstração. Já sabemos que J é um ideal bilateral. Como

$$J \cdot (R/I) = JR + I = J + I$$

e J é o anulador de R/I, então $J + I = 0 + I$, ou seja, $J \subseteq I$. Se K é um ideal bilateral de R contido em I, então

$$K \cdot (R/I) = KR + I = K + I = 0 + I \Rightarrow K \subseteq \mathrm{Ann}(R/I) = J. \qquad \square$$

Seja I um ideal à esquerda de um anel R. Então,

- R/I é fiel se e só se o único ideal bilateral contido em I é 0.
- Se I for um ideal bilateral, $\mathrm{Ann}(R/I) = I$ e R/I é um anel.

Observação 2: Consideremos um R-módulo à esquerda M com anulador $I = \mathrm{Ann}(M)$. Então, R/I é um anel e M tem também estrutura de R/I-módulo, com a acção

$$(a+I)\cdot m = a\cdot m :$$

A acção está bem definida: se $a+I = b+I$, então $a-b \in I = \mathrm{Ann}(M)$, logo $\forall m \in M, (a-b)\cdot m = 0_M \Leftrightarrow a\cdot m = b\cdot m$. De facto, esta é uma acção de módulo, porque é a mesma acção de R sobre M.

Com esta construção, temos a propriedade adicional de que M é um R/I-módulo fiel:

$$(b+I)\cdot M = 0 \Rightarrow b\cdot M = 0 \Rightarrow b \in \mathrm{Ann}(M) = I \Rightarrow b+I = 0+I.$$

Teorema 1.7 (Teorema do Isomorfismo) *Sejam M e N dois R-módulos à esquerda. Para qualquer $f : M \to N$ homomorfismo, existe um homomorfismo injectivo $\overline{f} : M/\mathrm{Ker}f \to N$ tal que*

$$(m+\mathrm{Ker}f)\overline{f} = (m)f, \quad \forall m \in M.$$

Demonstração. A teoria dos grupos já nos garante a existência de um homomorfismo de grupos $\overline{f}$. Resta ver que $\overline{f}$ é R-linear: dados quaisquer $a \in R$ e $m+\mathrm{Ker}f \in M/\mathrm{Ker}f$,

$$(a\cdot(m+\mathrm{Ker}f))\,\overline{f} = (a\cdot m+\mathrm{Ker}f)\overline{f} = (a\cdot m)f = a\cdot(m)f = a\cdot(m+\mathrm{Ker}f)\overline{f}.$$

Por fim, $\overline{f}$ é injectiva porque se $(m+\mathrm{Ker}f)\overline{f} = 0_N$, então $(m)f = 0$, ou seja, $m \in \mathrm{Ker}f$ e $m+\mathrm{Ker}f = 0+\mathrm{Ker}f$. □

E, deste teorema, decorre imediatamente que dado um homomorfismo $f : M \longrightarrow N$, temos o seguinte isomorfismo de R-módulos:

$$M/\mathrm{Ker}f \cong \mathrm{Im}f.$$

Para terminar esta primeira parte de conceitos básicos, enunciamos a seguinte proposição que relaciona os endomorfismos de M^n com os endomorfismos de M. O anel das matrizes $n\times n$ de um anel R é

$$\mathcal{M}_n(R) = \left\{ \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix} : a_{i,j} \in R \right\}.$$

Proposição 1.8 *Seja M um R-módulo à esquerda. Então, temos um isomorfismo entre os anéis*

$$\mathrm{End}_R(M^n) \cong \mathcal{M}_n(\mathrm{End}({}_RM)).$$

Demonstração. Em primeiro lugar, definimos os R-homomorfismos seguintes:

$$\begin{array}{rcl} e_i : M & \to & M^n \\ m & \mapsto & (0,\ldots,0,\underbrace{m}_{\text{i-ésima posição}},0,\ldots,0) \end{array} \qquad e \qquad \begin{array}{rcl} \pi_j : M^n & \to & M \\ (m_1,\ldots,m_n) & \mapsto & m_j \end{array}$$

Note-se que $\sum_{i=1}^n \pi_i \circ e_i$ é a aplicação identidade de M^n, porque

$$(m_1,\ldots,m_n)\left(\sum_{i=1}^n \pi_i \circ e_i\right) = \sum_{i=1}^n (0,\ldots,0,m_i,0,\ldots,0) = (m_1,\ldots,m_n).$$

Para além disso, $e_i \circ \pi_j = \begin{cases} id_M, \text{ se } i = j \\ 0_M, \text{ se } i \neq j \end{cases}$, porque $\forall m \in M$

$$(m)(e_i \circ \pi_j) = (0,\ldots,0,m,0,\ldots,0)\pi_j = \begin{cases} m, \text{ se } i = j \\ 0, \text{ se } i \neq j \end{cases}.$$

Definimos a função

$$\begin{array}{rcl} \varphi : \mathrm{End}(M^n) & \to & \mathcal{M}_n(\mathrm{End}(M)) \\ f & \mapsto & \varphi(f) = (e_i \circ f \circ \pi_j)_{i,j} \end{array}$$

isto é, dado um endomorfismo $f \in \mathrm{End}_R(M^n)$, definimos $f_{i,j} = e_i \circ f \circ \pi_j$ (que são R-endomorfismos de M) e construímos a matriz $n \times n$ de endomorfismos de M:

$$\begin{pmatrix} f_{1,1} & f_{1,2} & \cdots & f_{1,n} \\ f_{2,1} & f_{2,2} & \cdots & f_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n,1} & f_{n,2} & \cdots & f_{n,n} \end{pmatrix}.$$

Facilmente se vê que φ é um homomorfismo de anéis: $\forall f, g \in End(M^n)$,

- $\varphi(f+g) = (e_i \circ (f+g) \circ \pi_j)_{i,j} = ((e_i \circ f + e_i \circ g) \circ \pi_j)_{i,j} = (e_i \circ f \circ \pi_j + e_i \circ g \circ \pi_j)_{i,j} = (e_i \circ f \circ \pi_j)_{i,j} + (e_i \circ g \circ \pi_j)_{i,j} = \varphi(f) + \varphi(g)$.
- $\varphi(f)\varphi(g) = (e_i \circ f \circ \pi_j)_{i,j}(e_i \circ g \circ \pi_j)_{i,j} = \left(\sum_{k=1}^n (e_i \circ f \circ \pi_k) \circ (e_k \circ g \circ \pi_j)\right)_{i,j} = \left(e_i \circ f \circ (\sum_{k=1}^n \pi_k \circ e_k) \circ g \circ \pi_j\right)_{i,j} = (e_i \circ (f \circ g) \circ \pi_j)_{i,j} = \varphi(f \circ g)$
- $\varphi(id) = (e_i \circ id \circ \pi_j)_{i,j} = (e_i \circ \pi_j)_{i,j} = Id_{\mathrm{End}(M)}$.

Por outro lado, definimos a aplicação

$$\begin{array}{rcl} \psi : \mathcal{M}_n(\mathrm{End}(M)) & \to & \mathrm{End}(M^n) \\ (f_{i,j})_{i,j} & \mapsto & \psi((f_{i,j})) = \sum_{i,j=1}^{n} \pi_i \circ f_{i,j} \circ e_j \end{array}$$

que está bem definida, porque a composição e soma de homomorfismos é um homomorfismo.

Dado $f \in \mathrm{End}(M^n)$, pela linearidade de f temos que

$$\begin{aligned} \psi(\varphi(f)) &= \psi((e_i \circ f \circ \pi_j)_{i,j}) = \sum_{i,j=1}^{n} \pi_i \circ (e_i \circ f \circ \pi_j) \circ e_j \\ &= \left(\sum_{i=1}^{n} \pi_i \circ e_i\right) \circ f \circ \left(\sum_{j=1}^{n} \pi_j \circ e_j\right) = f \end{aligned}$$

e dada $F = (f_{i,j})_{i,j} \in \mathcal{M}_n(\mathrm{End}(M))$ temos que

$$\begin{aligned} \varphi(\psi((f_{i,j})_{i,j})) &= \varphi\left(\sum_{i,j=1}^{n} \pi_i \circ f_{i,j} \circ e_j\right) = \left(e_k \circ \left(\sum_{i,j=1}^{n} \pi_i \circ f_{i,j} \circ e_j\right) \circ \pi_l\right)_{k,l} \\ &= \left(\sum_{i=1}^{n} (e_k \circ \pi_i) \circ f_{i,j} \circ \sum_{j=1}^{n} (e_j \circ \pi_l)\right)_{k,l} = (f_{k,l})_{k,l} \end{aligned}$$

Logo, φ e ψ são inversos. □

1.2 Módulos Livres

Definição 1.9 *Sejam R um anel e M um R-módulo à esquerda.*

1. *Um subconjunto $N \subset M$ diz-se um conjunto de geradores se*

$$\forall m \in M,\ \exists\, m_1, \ldots, m_k \in N,\ \exists\, a_1, \ldots, a_k \in R :\ m = \sum_{i=1}^{k} a_i m_i.$$

2. *Um subconjunto $N \subset M$ diz-se linearmente independente se*

$$\forall m_1, \ldots, m_k \in N, \forall a_1, \ldots, a_k \in R, \sum_{i=1}^{k} a_i m_i = 0 \ \Rightarrow\ a_1 = a_2 = \ldots = a_k = 0.$$

3. *Um subconjunto $N \subset M$ diz-se uma <u>base</u> se for um conjunto linearmente independente de geradores.*

4. *Um módulo M com uma base diz-se um <u>módulo livre</u>.*

A noção de módulo *livre* generaliza claramente as noções de base e dimensão de espaços vectoriais, por isso, qualquer espaço vectorial é exemplo de um módulo livre. Vejamos outro exemplo: se M for um módulo livre com base B, o módulo produto M^n também o é com base $\{e_{1,b}, \ldots, e_{n,b} : b \in B\}$, onde

$$e_{i,b} = (0, \ldots, 0, \underbrace{b}_{\text{i-ésima posição}}, 0, \ldots, 0).$$

À semelhança do que se verifica com os espaços vectoriais, um homomorfismo de módulos fica determinado pelos valores que toma numa base:

Proposição 1.10 *Sejam M e N dois R-módulos à esquerda. Suponhamos que M é um módulo livre com base B. Para qualquer função $f : B \to N$, existe um único homomorfismo de R-módulos $g : M \to N$ tal que $(b)g = (b)f, \forall b \in B$.*

Demonstração. Vejamos em primeiro lugar a existência de g. Seja $B = \{b_1, \ldots, b_k\}$ uma base de M, então qualquer elemento $m \in M$ pode ser escrito de forma única $m = \sum_{i=1}^{k} a_i b_i$, onde $a_1, \ldots, a_k \in R$. O homomorfismo $g : M \to N$ define-se por

$$(m)g = \sum_{i=1}^{k} a_i (b_i) f, \qquad \text{se } m = \sum_{i=1}^{k} a_i b_i.$$

Pela unicidade da representação de m como combinação linear de elementos da base, g está bem-definida e, de facto, é um homomorfismo de R-módulos:

1. Dados $m, n \in M$, existem elementos $r_1, \ldots, r_k, s_1, \ldots, s_k \in R$ tais que $m = \sum_{i=1}^{k} r_i b_i$ e $n = \sum_{i=1}^{k} s_i b_i$. Então,

$$(m+n)g = \left(\sum_{i=1}^{k} (r_i + s_i) b_i \right) g = \sum_{i=1}^{k} (r_i + s_i)(b_i) f = \sum_{i=1}^{k} r_i (b_i) f + \sum_{i=1}^{k} s_i (b_i) f = (m)g + (n)g.$$

2. Quanto à R-linearidade, dados $m \in M$ e $r \in R$, escrevemos $m = \sum_{i=1}^{k} a_i b_i$, logo

$$(rm)g = \left(\sum_{i=1}^{k} r a_i b_i \right) g = \sum_{i=1}^{k} r a_i (b_i) f = r \sum_{i=1}^{k} a_i (b_i) f = r(m)g.$$

Quanto à unicidade, para qualquer homomorfismo $h : M \to N$ com $(b)h = (b)f$ para todo $b \in B$, tem-se que para qualquer $m = \sum_{i=1}^{k} a_i b_i$, utilizando a R-linearidade de h:

$$(m)h = \sum_{i=1}^{k} a_i (b_i) h = \sum_{i=1}^{k} a_i (b_i) f = (m)g.$$

□

Ainda relativamente aos módulos livres, qualquer módulo livre M é isomorfo a (uma soma direta)

$$R^{(B)} = \{f : B \to R \mid \exists\, F \subset B \text{ finito} : f(b) = 0, \forall b \notin F\},$$

onde B é uma base de M: definindo para cada $b \in B$

$$e_b(c) = \begin{cases} 1 & \text{se } c = b \\ 0 & \text{se } c \neq b \end{cases},$$

é fácil ver que $\{e_b : b \in B\}$ é uma base de $R^{(B)}$; pela Proposição 1.10 existe um único homomorfismo $g : R^{(B)} \to M$ tal que $(e_b)g = b, \forall b \in B$. A aplicação g é claramente sobrejectiva. A injectividade de g resulta da independência linear de B. Portanto,

$$M \cong R^{(B)}.$$

1.3 Módulos e Anéis Artinianos

Definição 1.11 *Seja R um anel.*

1. *Um R-módulo M à esquerda diz-se artiniano[2] se verifica a* CONDIÇÃO DE CADEIA DESCENDENTE (CCD)*: qualquer cadeia descendente de submódulos de M*

$$N_1 \geq N_2 \geq N_3 \geq \ldots$$

termina, isto é,

$$\exists\, j : N_l = N_j, \;\; \forall l \geq j.$$

2. *Um anel R diz-se artiniano à esquerda se é um R-módulo à esquerda artiniano.*

Exemplos:

1. $\mathbb{Z}$ não é um anel artiniano à esquerda.
2. $\mathbb{Z}_n$ é um anel artiniano à esquerda, para $n \geq 2$.
3. $K[t]/\langle t^n \rangle$ é um anel artiniano à esquerda (K corpo, $n \geq 1$).
4. $\mathcal{M}_n(R)$, com R artiniano à esquerda, é artiniano à esquerda.

Note-se que uma definição análoga à anterior relativamente a cadeias ascendentes dá origem às noções de módulo *noetheriano*[3] e anel *noetheriano à esquerda*.

[2]Esta designação é usada em homenagem ao matemático austríaco do século XX Emil Artin.
[3]Em homenagem à matemática alemã do século XX Emmy Noether.

1.4 Módulos e Anéis Simples e Semisimples

Definição 1.12 *Seja R um anel. Um R-módulo $M \neq 0$ diz-se simples se 0 e M são os seus únicos submódulos.*

Um submódulo N diz-se *simples* se os únicos submódulos que contém são 0 e N. Estudando R como um R-módulo, os submódulos simples são os ideais à esquerda minimais.

Teorema 1.13 (Caracterização dos Módulos Simples) *Seja R um anel. São equivalentes as afirmações seguintes:*

1. *M é um R-módulo simples.*
2. *Para qualquer $0 \neq m \in M$, $Rm = M$.*
3. *$M \cong R/I$, com I ideal à esquerda maximal de R.*

Demonstração.
(1) $\Leftrightarrow$ (2) Supondo que M é simples, como Rm é um submódulo de M não nulo (porque contém $m \neq 0$), então $Rm = M$. Reciprocamente dado um submódulo N não nulo de M, existe $0 \neq n \in N$ e temos que $0 \neq Rn \subset N$. Por hipótese $Rn = M$, logo $N = M$. Ou seja, M é simples.
(1) $\Rightarrow$ (3) Supondo que M é simples, por (2) temos que $M = Rm$ (para qualquer $m \neq 0$). Então, o homomorfismo de R-módulos

$$\begin{array}{rcl} f : R & \to & Rm = M \\ r & \mapsto & rm \end{array}$$

é sobrejectivo e pelo Teorema do Isomorfismo $M \simeq R/\mathrm{Ker}(f)$. O seu núcleo é um submódulo de R (ou seja, um ideal à esquerda) maximal, porque se $\mathrm{Ker}(f) \leq J \leq R$ então $(J)f \leq M$ e, sendo M simples, $(J)f = 0$ ou $(J)f = M$, isto é $J = \mathrm{Ker}(f)$ ou $J = R$.
(3) $\Rightarrow$ (1) Os submódulos de R/I são da forma J/I, onde J é um ideal à esquerda de R que contém I. Como I é maximal, $J = I$ ou $J = R$, isto é, $J/I = 0$ ou $J/I = R/I$. Deste modo, R/I é um módulo simples. □

Exemplos:

1. $\mathbb{Z}_p$ é um $\mathbb{Z}$-módulo simples se e só se p é primo.
2. $K[t]/\langle f \rangle$ é um $K[t]$-módulo simples se e só se f é um polinómio irredutível sobre K (onde K é um corpo).

Os módulos simples têm várias propriedades, nomeadamente a seguinte enunciada num lema conhecido como Lema de Schur.

Lema 1.14 (Lema de Schur) *Sejam M e N dois R-módulos à esquerda simples. Então, qualquer homomorfismo $f : M \to N$ é o homomorfismo nulo ou é bijectivo. Em particular, o conjunto dos endomorfismos* $\mathrm{End}({}_RM)$ *de um módulo simples é um anel de divisão.*

Demonstração. Sejam M e N dois R-módulos à esquerda simples (em particular, são não nulos) e $f : M \to N$ um homomorfismo. Como $\mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ são submódulos de M e N, respectivamente, pela simplicidade destes módulos temos que $\mathrm{Ker}(f)$ é 0 ou M e $\mathrm{Im}(f)$ é 0 ou N.

Se $\mathrm{Ker}(f) = 0$, então $\mathrm{Im}(f) \neq 0$ (caso contrário, $M = 0$), logo $\mathrm{Im}(f) = N$. Assim, f é injectivo e sobrejectivo, ou seja, uma bijecção. Se $\mathrm{Ker}(f) = M$, então $\mathrm{Im}(f) \neq N$ (caso contrário, $N = 0$), logo $\mathrm{Im}(f) = 0$. Deste modo, f é o homomorfismo nulo.

Logo, qualquer endomorfismo $0 \neq f \in \mathrm{End}({}_RM)$ é bijectivo, isto é, tem inverso. Como a função inversa de um homomorfismo é também um homomorfismo, $\mathrm{End}({}_RM)$ é um anel de divisão. □

Lema 1.15 *R é um R-módulo à esquerda simples se e só se R é um anel de divisão.*

Demonstração. Se R for um módulo simples, então para qualquer $0 \neq a \in R, Ra = R$ o que implica que existe $b \in R$ tal que $ba = 1$. Com o mesmo argumento b tem um inverso à esquerda, digamos c, isto é $cb = 1$. Logo,

$$c = c1 = cba = 1a = a,$$

ou seja, b é o inverso de a (à esquerda e à direita).

Reciprocamente, supondo que R é um anel de divisão, dado $0 \neq a \in R$ qualquer, temos que $1 = a^{-1}a \in Ra$, logo $Ra = R$ e pelo Teorema 1.13 R é um R-módulo simples. □

Para definirmos o conceito de módulo semisimples, é necessária a noção de soma directa:

Notação: Dada uma família $\{M_i\}_{i\in I}$ de R-módulos, a sua soma directa $\bigoplus_{i\in I} M_i$ é o submódulo de $\prod_{i\in I} M_i$ que consiste de funções $f : I \to \bigcup_{i\in I} M_i$ tal que $f(i) = 0$, para quase todo $i \in I$, ou seja, existe $J = \{j_1, \ldots, j_n\}$ tal que $f(i) = 0$ para $i \in I \setminus J$. É claro que no caso de uma colecção finita de módulos as noções de soma directa e produto cartesiano coincidem.

Definição 1.16 *Seja R um anel. Um R-módulo M diz-se semisimples se*

$$\forall N \leq M,\ \exists\, L \leq M :\ N \oplus L = M.$$

Como um módulo simples só tem os submódulos triviais, então é claramente semisimples.

Teorema 1.17 (Caracterização dos Módulos Semisimples) *As afirmações seguintes são equivalentes:*

(a) *M é um R-módulo semisimples.*

(b) *$M = \bigoplus_{i\in I} N_i$, onde $N_i \leq M$ são submódulos simples.*

A demonstração deste Teorema pode ser encontrada em [15, Theorem 2.4]. Nela é utilizado o facto de que "qualquer módulo semisimples não nulo tem um submódulo simples", que é uma consequência do Lema de Zorn (1.2) semelhante à vista na Proposição 1.3.

Um anel R diz-se semisimples se é um R-módulo à esquerda semisimples. Pelo Teorema anterior, qualquer anel semisimples $R = \bigoplus_i I_i$ é soma directa de ideais à esquerda minimais.

Observação: Por vezes, um tal anel é chamado de semisimples *à esquerda*. No entanto, mostra-se que um anel é semisimples à esquerda se e só se é semisimples à direita, daí que usemos apenas a designação *semisimples*.

Definição 1.18 *Um anel R diz-se um anel simples se 0 e R são os seus únicos ideais bilaterais.*

Observações:

- Um anel simples *não* é necessariamente simples enquanto R-módulo à esquerda, uma vez que este último é um anel cujos únicos ideais *à esquerda* são 0 e R. A noção de anel simples é, portanto, mais geral do que esta.

- Ao passo que a noção de anel semisimples envolve ideais *à esquerda*, a noção de anel simples envolve apenas ideais *bilaterais*. Daí que (ao contrário do que se verifica nos módulos)

$$\text{anel simples} \not\Rightarrow \text{anel semisimples}.$$

Exemplo: $\mathcal{M}_n(R)$ é um anel simples, se R for simples.

Seja J um ideal de $\mathcal{M}_n(R)$. Definimos

$$I = \{a_{11} \in R : (a_{ij})_{i,j} \in J\},$$

que é um ideal de R: dados $a, b \in I$, existem $(a_{ij})_{ij}, (b_{ij})_{ij} \in J$ tais que $a_{11} = a$ e $b_{11} = b$, logo

- $a + b$ é a 1ª entrada da matriz $(a_{ij} + b_{ij})_{ij} = (a_{ij})_{ij} + (b_{ij})_{ij} \in J$ (porque J é ideal), logo $a + b \in I$.
- ra é a 1ª entrada da matriz $(ra_{ij})_{ij} = r(a_{ij})_{ij} \in J$ (porque J é ideal), logo $ra \in I$.

Vejamos que $J = \mathcal{M}_n(I) = \{(a_{ij})_{ij} \in \mathcal{M}_n(R) \mid a_{ij} \in I, \forall i, j\}$. Definimos as matrizes da forma

$$E_{ij} = \begin{pmatrix} 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix} \qquad \text{com } 1 \leq i, j \leq n$$

que formam uma base de $\mathcal{M}_n(R)$ sobre R como módulo à esquerda. Vejamos algumas propriedades destas matrizes: é claro que $E_{ij}E_{kl} = \delta_{jk}E_{il}$ e $\forall A = (a_{ij})_{ij} \in \mathcal{M}_n(R)$

$$\begin{aligned} E_{kl}AE_{mn} &= E_{kl}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{ij}\right)E_{mn} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{kl}E_{ij}E_{mn} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\delta_{il}E_{kj}E_{mn} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\delta_{il}\delta_{jm}E_{kn} = a_{lm}E_{kn}. \end{aligned}$$

Por um lado, se $A = (a_{ij})_{ij} \in J$, para quaisquer i e j temos que $E_{1i}AE_{j1} = a_{ij}E_{11} \in J$ (porque J é ideal), logo $a_{ij} \in I$. Logo, $J \subset \mathcal{M}_n(I)$.

Por outro lado, dada $A = (a_{ij})_{ij} \in \mathcal{M}_n(I)$, temos que para cada $a_{ij} \in I$ existe uma matriz $B^{ij} \in J$ cuja primeira entrada é a_{ij}, logo

$$A = \sum_{i,j=1}^{n} a_{ij}E_{ij} = \sum_{i,j=1}^{n} E_{i1}B^{ij}E_{1j} \in J \quad \text{(porque } J \text{ é ideal)}.$$

Portanto, $J = \mathcal{M}_n(I)$. Como R é simples, $I = 0$ ou $I = R$, logo $J = 0$ ou $J = \mathcal{M}_n(R)$. Ou seja, $\mathcal{M}_n(R)$ é um anel simples. □

No próximo Capítulo que aborda os anéis de polinómios há uma secção (2.3) onde iremos ver mais exemplos de anéis simples.

O centro de um anel R é dado por

$$Z(R) = \{a \in R : ab = ba, \forall b \in R\},$$

ou seja, é o conjunto dos elementos de R que comutam com todos os outros elementos de R. Este conjunto não é vazio, porque contém 0 e 1.

Proposição 1.19 *Se R for um anel simples, então $Z(R)$ é um corpo.*

Demonstração. Seja $0 \neq a \in Z(R)$. O ideal Ra é bilateral (porque a é central) não nulo (porque $0 \neq a \in Ra$). Como R é simples, temos $Ra = R$; em particular, existe $b \in R$ tal que

$$ba = ab = 1.$$

Resta ver que $b \in Z(R)$: como a é central,

$$cb = 1cb = bacb = bcab = bc1 = bc, \qquad \forall c \in R. \qquad \square$$

O Teorema seguinte, da autoria de Emil Artin e Joseph Wedderburn, dá uma caracterização dos anéis semisimples.

Teorema 1.20 (Teorema de Artin-Wedderburn) *Um anel R é semisimples à esquerda se e só se*

$$R \cong \mathcal{M}_{n_1}(D_1) \times \ldots \times \mathcal{M}_{n_t}(D_t),$$

onde $D_1, \ldots, D_t$ são anéis de divisão e $n_1, \ldots, n_t > 0$. O número t é único e os anéis $\mathcal{M}_{n_i}(D_i)$ são unicamente determinados a menos da ordem. Neste caso, R tem exactamente t submódulos simples não-isomorfos.

A demonstração deste Teorema pode ser encontrada em [15, Theorem 3.5].

Dado um R-módulo à esquerda M, define-se o *socle* de M como

$$Soc(M) = \sum_{R\text{-submódulos } N \text{ simples}} N.$$

Se M não tiver submódulos simples, define-se $Soc(M) = 0$. No caso particular ${}_RR$, o socle de R, $Soc(R)$, é a soma dos seus ideais à esquerda minimais.

Lema 1.21 *$Soc(R)$ é um ideal bilateral.*

Demonstração. Se $Soc(R) = 0$, então é um ideal bilateral. Suponhamos que $Soc(R) \neq 0$. Como $Soc(R)$ é a soma de ideais à esquerda, então claro que é um ideal à esquerda. Vejamos que também é um ideal à direita.

Sejam I um ideal à esquerda minimal de R e $0 \neq r \in R$ quaisquer. Consideremos o homomorfismo de anéis

$$\begin{array}{rcl} \varphi : I & \to & Ir \\ a & \mapsto & ar \end{array}.$$

Como $\mathrm{Ker}(\varphi)$ é um ideal à esquerda de I e I é minimal, então:

- Ou $\mathrm{Ker}(\varphi) = 0$, donde $I \cong Ir$, ou seja, Ir é um ideal à esquerda minimal, logo $Ir \subset Soc(R)$.
- Ou $\mathrm{Ker}(\varphi) = I$, donde $Ir = 0$, em particular, $Ir \subset Soc(R)$.

Em ambos os casos, $Ir \subset Soc(R)$. Portanto, $Soc(R)$ é um ideal à direita de R. □

Note-se que dados dois submódulos N_1, N_2 simples de M distintos, temos que $N_1 \cap N_2 = 0$: se $0 \neq a \in N_1 \cap N_2$, como N_1 e N_2 são R-submódulos temos $0 \neq Ra \subset N_1 \cap N_2$, e sendo N_1 e N_2 simples temos $N_1 = Ra = N_2$. Portanto,

$$Soc(M) = \bigoplus_{\text{alguns } R\text{-submódulos } N \text{ simples}} N$$

e o análogo vale para $Soc(R)$.

Teorema 1.22 *As afirmações seguintes são equivalentes para um anel R:*

1. *R é um anel simples e artiniano à esquerda.*
2. *R é um anel simples e semisimples.*
3. *R é um anel simples e possui um ideal à esquerda minimal não nulo.*
4. *$R \cong \mathcal{M}_n(D)$, com $n > 0$ e D um anel de divisão.*

Demonstração.

(1) ⇒ (3) Em geral, se um R-módulo M é artiniano à esquerda então tem um submódulo simples: caso contrário, poderíamos construir uma cadeia decrescente infinita de submódulos de M (o que é uma contradição). No caso particular $M = R$, temos que R tem um ideal à esquerda minimal (não nulo).

(3) ⇒ (2) Consideremos $Soc(R)$. Por hipótese, $Soc(R) \neq 0$ e é um ideal bilateral (pelo Lema 1.21). Como R é simples, então

$$R = Soc(R) = \bigoplus_{\text{alguns ideais à esquerda } I \text{ minimais}} I.$$

Pelo Teorema 1.17, R é semisimples.

(2) ⇒ (4) Se R é semisimples, pelo Teorema de Artin-Wedderburn $R = \mathcal{M}_{n_1}(D_1) \times \ldots \times \mathcal{M}_{n_t}(D_t)$, onde $t \geq 1$ e D_i são anéis de divisão. Como $I = \mathcal{M}_{n_1}(D_1)$ é um ideal (não nulo) de R e R é simples, então $R = \mathcal{M}_n(D)$.

(4) ⇒ (1) Já sabemos que $R = \mathcal{M}_n(D)$ é um anel simples. Para além disso, também é artiniano à esquerda, porque R é um espaço vectorial sobre D de dimensão n^2, logo qualquer cadeia descendente de ideais à esquerda termina. □

1.5 O Radical de Jacobson

Definição 1.23 *O radical de Jacobson de um anel R é*

$$\mathrm{Jac}(R) = \bigcap_{\text{ideais à esquerda } I \text{ maximais}} I$$

Proposição 1.24 (Caracterização do Radical de Jacobson) *As afirmações são equivalentes:*

(a) $y \in \mathrm{Jac}(R)$.

(b) $1 - xy$ *é invertível à esquerda,* $\forall x \in R$.

(c) $y \cdot M = 0$, *para todo o* R*-módulo à esquerda* M *simples.*

Portanto,

$$\mathrm{Jac}(R) = \bigcap_{R-\text{módulo à esquerda } M \text{ simples}} \mathrm{Ann}(M),$$

ou seja, $\mathrm{Jac}(R)$ *anula todos os* R*-módulos à esquerda simples. Em particular,* $\mathrm{Jac}(R)$ *é um ideal bilateral de* R.

A demonstração desta Proposição pode ser consultada em [15, Lemma 4.1].

Definição 1.25 *Um anel* R *diz-se* <u>semiprimitivo</u> *(ou Jacobson-semisimples, ou até J-semisimples) se*

$$\mathrm{Jac}(R) = 0.$$

Proposição 1.26 *Um anel semisimples é semiprimitivo.*

Demonstração. Suponhamos que R é semisimples. Como $\mathrm{Jac}(R)$ é um ideal (bilateral, logo à esquerda) de R, então

$$\exists\, I \text{ ideal à esquerda de } R : I \oplus \mathrm{Jac}(R) = R.$$

Então existem $x \in I$ e $y \in \mathrm{Jac}(R)$ tais que $x + y = 1$. Como $y \in \mathrm{Jac}(R)$, pela Proposição 1.24 $x = 1 - y$ é invertível à esquerda, logo $Rx = R$. Como $x \in I$, então $R = Rx \subset I$, donde $I = R$ ou seja $\mathrm{Jac}(R) = 0$. Portanto, R é semiprimitivo. □

Deste modo, os anéis da forma $\mathcal{M}_{n_1}(D_1) \times \ldots \times \mathcal{M}_{n_k}(D_k)$, com $D_1, \ldots, D_k$ anéis de divisão, são exemplos de anéis semiprimitivos. Em geral, a implicação da Proposição anterior é estrita mas para anéis artinianos à esquerda é uma equivalência:

Proposição 1.27 *Para anéis artinianos à esquerda,*

$$\textit{Semisimples} \iff \textit{Semiprimitivo.}$$

A demonstração desta Proposição pode ser encontrada em [15, Theorem 4.14].

Um ideal $I \leq R$ diz-se nilpotente se $\exists\, n \in \mathbb{N} : I^n = 0$.

Proposição 1.28 *Qualquer ideal nilpotente está contido no* $\mathrm{Jac}(R)$.

Demonstração. Suponhamos que um ideal $I \leq R$ é nilpotente, com $I^n = 0$. Dado $y \in I$, temos que $\forall x \in R, xy \in I$ (porque I é um ideal), então $(xy)^n = 0, \forall x \in R$. Como

$$(1 + xy + (xy)^2 + \ldots + (xy)^{n-1})(1 - xy) =$$

$$= 1 - xy + xy - (xy)^2 + (xy)^2 - \ldots + (xy)^{n-1} - \underbrace{(xy)^n}_{=0} = 1$$

ou seja, $1 - xy$ é invertível à esquerda, $\forall x \in R$. Pela Proposição 1.24, $y \in \mathrm{Jac}(R)$. Portanto, $I \subset \mathrm{Jac}(R)$. □

1.6 Anéis Primos e Semiprimos

Definição 1.29 *Seja R um anel.*

- *R diz-se um anel primo se*

$$\forall I, J \textit{ ideais com } IJ = 0 \Rightarrow I = 0 \textit{ ou } J = 0.$$

- *R diz-se um anel semiprimo se*

$$\forall A \textit{ ideal com } A^2 = 0 \Rightarrow A = 0;$$

  por outras palavras, R não tem ideais nilpotentes não triviais.

- *Um ideal I de R diz-se primo (resp. semiprimo) se R/I é um anel primo (resp. semiprimo).*

Exemplos.

1. Qualquer anel simples é claramente primo. Por exemplo, o anel das matrizes $\mathcal{M}_n(K)$ sobre um anel de divisão K e o anel quociente $\mathbb{Q}[x]/\langle p \rangle$ sobre um polinómio irredutível p são exemplos de anéis simples, logo são primos.

2. É claro que um anel primo é semiprimo, logo os exemplos anteriores também são semiprimos.

3. Tendo em conta a Proposição 1.28, um anel semiprimitivo é semiprimo, logo

$$\mathcal{M}_{n_1}(D_1) \times \ldots \times \mathcal{M}_{n_k}(D_k),$$

onde $D_1, \ldots, D_k$ são anéis de divisão, é um exemplo de um anel semiprimo.

Já vimos que o centro de um anel simples é um corpo. Sendo os anéis primos uma generalização dos anéis simples, não é de surpreender o seguinte resultado:

Proposição 1.30 *O centro $Z(R)$ de um anel primo R é um domínio integral.*

Demonstração. Sejam $0 \neq a \in Z(R)$ e $b \in R$ tal que $ab = 0$. Queremos ver que $b = 0$. Como a é central, $RaR = Ra$ logo

$$(RaR)(RbR) = RaRbR = RabR = 0$$

e, sendo R primo, $RaR = 0$ (donde a=0, o que é impossível) ou $RbR = 0$ (donde $b = 0$). Portanto, $Z(R)$ é um domínio integral. □

Podemos reunir todas as classes de anéis vistas anteriormente e as relações entre elas no seguinte esquema de implicações:

$$\begin{array}{ccccc} \text{Semisimples} & \Longrightarrow & \text{Semiprimitivo} & \Longrightarrow & \text{Semiprimo} \\ \Uparrow (+\text{CCD}) & & & & \Uparrow \\ \text{Simples} & & \Longrightarrow & & \text{Primo} \end{array}$$

Os ANÉIS PRIMITIVOS, que é o conceito central da minha tese, constituem uma classe de anéis que como iremos ver no Capítulo 3 se encontra entre os anéis simples e os anéis primos.

Para terminar este capítulo de resultados básicos na Teoria de Anéis e Módulos, vejamos o seguinte resultado que enuncia que, à semelhança da Proposição 1.27, para anéis artinianos à esquerda as implicações horizontais anteriores são na realidade equivalências:

Proposição 1.31 *Para anéis artinianos à esquerda,*

1. *Semisimples $\Longleftrightarrow$ Semiprimitivo $\Longleftrightarrow$ Semiprimo.*

2. *Simples $\Longleftrightarrow$ Primo.*

Demonstração. Vejamos a demonstração da primeira afirmação: basta ver que se R é semiprimo e artiniano à esquerda então é semiprimitivo.

Consideremos $Soc(R)$, que é a soma (directa) de alguns ideais à esquerda minimais de R. Relembre-se que um ideal à esquerda minimal pode ser visto como um R-módulo à esquerda simples. Como o $\mathrm{Jac}(R)$ anula todos os módulos simples, então

$$\mathrm{Jac}(R)Soc(R) = \bigoplus_{\text{alguns ideais à esquerda } I \text{ minimais}} \mathrm{Jac}(R)I = 0.$$

Se R for artiniano à esquerda, então qualquer ideal à esquerda J não nulo de R contém um ideal à esquerda minimal, caso contrário poderíamos construir uma cadeia descendente infinita de ideais à esquerda de R (o que é uma contradição). Ou seja, $Soc(J) \neq 0$.

Em particular, para $J = \mathrm{Jac}(R)$ tem-se que $Soc(J) = \mathrm{Jac}(R) \cap Soc(R)$ (porque qualquer ideal à esquerda de J é intersecção de um ideal à esquerda de R com J) e portanto $Soc(J)^2 \subseteq \mathrm{Jac}(R)Soc(R) = 0$. Como R é semiprimo então $Soc(J) = 0$. Pelo parágrafo anterior, $J = \mathrm{Jac}(R) = 0$ e R é semiprimitivo.

Vejamos a demonstração da segunda afirmação: basta ver que se R é primo e artiniano à esquerda então é simples.

Se R for primo, então é semiprimo e pela primeira afirmação R é semisimples. Logo pelo Teorema de Artin-Wedderburn $R = \mathcal{M}_{n_1}(D_1) \times \ldots \times \mathcal{M}_{n_t}(D_t)$, para $t \geq 1$ e $D_1, \ldots, D_t$ anéis de divisão.

Se $t > 1$, então $I = \mathcal{M}_{n_1}(D_1)$ e $J = \mathcal{M}_{n_2}(D_2)$ são ideais com $IJ = 0$, porque a multiplicação é componente a componente. Como R é primo, $I = 0$ ou $J = 0$, o que é uma contradição. Logo, $t = 1$ e $R = \mathcal{M}_n(D)$ é um anel simples. □

No próximo Capítulo vamos estudar o anel dos polinómios e duas variantes dele, que são exemplos importantes na área dos Anéis Não-comutativos.

2 Anéis de Polinómios Não Comutativos

Seja K um anel. O anel dos polinómios com coeficientes em K numa indeterminada x denota-se por $K[x]$ e é o conjunto das funções $\varphi : \mathbb{N} \to K$ que só têm um número finito de imagens $\varphi(n)$ não nulas. Assim sendo, um elemento φ de $K[x]$ pode ser representado por

$$\sum_{i=0}^{n} a_i x^i, \qquad \text{onde } a_i = \varphi(i) \in K \text{ e } n \in \mathbb{N}_0.$$

As operações neste anel são a adição e multiplicação usuais de polinómios:

$$\left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$\text{e} \qquad \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_i b_j\right) x^k.$$

Dado um polinómio não nulo

$$f = \sum_{i=0}^{n} a_i x^i, \qquad \text{com } a_n \neq 0,$$

o grau de f é $\deg(f) = n$ e o coeficiente guia de f é $\mathrm{cg}(f) = a_n$. Se $\mathrm{cg}(f) = 1$ o polinómio diz-se *mónico*.

Observação: Se K é um domínio, então $K[x]$ também é um domínio. Se f e g são elementos não nulos de $K[x]$ tais que $fg = 0$, então $\mathrm{cg}(f)\mathrm{cg}(g) = 0$ e, sendo K um domínio, $\mathrm{cg}(f) = 0$ ou $\mathrm{cg}(g) = 0$, o que é absurdo (porque por definição o coeficiente guia é não nulo). Logo, $f = 0$ ou $g = 0$.

Podemos construir versões modificadas do anel de polinómios se deixarmos de assumir que os elementos de K comutam com x.

2.1 O Anel de Operadores Diferenciais

Mantendo $K[x]$ como um módulo livre sobre K com a adição usual de polinómios, vamos alterar a multiplicação segundo a seguinte fórmula

$$xa = ax + \delta(a),$$

onde $\delta(a) \in K$ depende de a.

Para que a multiplicação de polinómios seja associativa, tem de se verificar $x(ab) = (xa)b$, ou seja,

$$(ab)x + \delta(ab) = (ax + \delta(a))b = a(bx + \delta(b)) + \delta(a)b = abx + (a\delta(b) + \delta(a)b)$$

e, sendo $K[x]$ um K-módulo livre com base $\{1, x, x^2, \ldots\}$, temos então que

$$\delta(ab) = \delta(a)b + a\delta(b). \tag{1}$$

Analogamente, para garantir a distributividade terá que se verificar $x(a+b) = xa + xb$, isto é,

$$(a+b)x + \delta(a+b) = ax + \delta(a) + bx + \delta(b)$$

e de forma análoga

$$\delta(a+b) = \delta(a) + \delta(b). \tag{2}$$

Dada a semelhança com o operador derivada, uma aplicação $\delta : K \mapsto K$ com estas duas propriedades (1) e (2) chama-se uma *derivada* de K. Vimos então que, se $xa = ax + \delta(a)$ definir um produto em $K[x]$, então δ é uma derivada. Há um teorema [13, Theorem 1.7.1] que nos garante que, de facto, dada uma derivada δ existe uma estrutura de anel no módulo livre $K[x]$ tal que $xa = ax + \delta(a)$, que denotamos por $K[x;\delta]$ e designamos por *anel de operadores diferenciais*.

Definindo $\delta^0 = id$ e $\delta^n = \delta \circ \delta^{n-1}$ (para $n > 0$), podemos generalizar a fórmula $xa = ax + \delta(a)$ para calcular o produto $x^n a$ em $K[x;\delta]$:

$$x^n a = \sum_{i=0}^{n} \binom{n}{i} \delta^i(a) x^{n-i}$$

Demonstração. O caso $n = 1$ é trivial: $xa = ax + \delta(a) = \delta^0(a)x + \delta(a)x^0$. Supondo que a fórmula vale para n, então

$$\begin{aligned}
x^{n+1}a &= x^n(xa) = x^n(ax + \delta(a)) \\
&= \sum_{i=0}^{n} \binom{n}{i} \delta^i(a) x^{n-i+1} + \sum_{i=0}^{n} \binom{n}{i} \delta^{i+1}(a) x^{n-i} \\
&= ax^{n+1} + \sum_{i=1}^{n} \binom{n}{i} \delta^i(a) x^{n-i+1} + \sum_{i=0}^{n-1} \binom{n}{i} \delta^{i+1}(a) x^{n-i} + \delta^{n+1}(a) \\
&= ax^{n+1} + \sum_{i=1}^{n} \binom{n}{i} \delta^i(a) x^{(n+1)-i} + \sum_{i=1}^{n} \binom{n}{i-1} \delta^i(a) x^{n-(i-1)} + \delta^{n+1}(a) \\
&= ax^{n+1} + \sum_{i=1}^{n} \left[\binom{n}{i} + \binom{n}{i-1} \right] \delta^i(a) x^{(n+1)-i} + \delta^{n+1}(a) \\
&= ax^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} \delta^i(a) x^{(n+1)-i} + \delta^{n+1}(a) \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} \delta^i(a) x^{(n+1)-i}
\end{aligned}$$

Observação: Se K é um domínio, então $K[x;\delta]$ também é um domínio. Suponhamos que f e g são polinómios não nulos de $K[x;\delta]$ tais que $fg=0$; se $a=\mathrm{cg}(f)$ e $b=\mathrm{cg}(g)$, podemos escrever $f=ax^n+$ (termos de menor grau) e $g=bx^m+$ (termos de menor grau), logo

$$\begin{aligned} fg &= a(x^n b)x^m + (\text{termos de menor grau}) \\ &= \sum_{i=0}^{n} \binom{n}{i} a\delta^i(b)x^{n+m-i} + (\text{termos de menor grau}) \\ &= (ab)x^{n+m} + (\text{termos de menor grau}) \end{aligned}$$

logo $\mathrm{cg}(f)\mathrm{cg}(g)=ab=0$ e, sendo K um domínio, $\mathrm{cg}(f)=0$ ou $\mathrm{cg}(g)=0$, o que é uma contradição (porque por definição o coeficiente guia é não nulo). Logo, $f=0$ ou $g=0$.

2.1.1 A Primeira Álgebra de Weyl

Consideremos $K=K_0[y]$, onde K_0 é um anel, e $\delta=\frac{\partial}{\partial y}$ a derivada formal de diferenciação do Cálculo:

$$\frac{\partial}{\partial y}\left(\sum_{i=0}^{n} a_i y^i\right) = \sum_{i=1}^{n} i a_i y^{i-1}.$$

No anel diferencial $K[x;\frac{\partial}{\partial y}] = K_0[y][x;\frac{\partial}{\partial y}]$, os elementos são da forma $\sum a_i(y)x^i$ e a multiplicação é determinada por

$$xy = yx + \frac{\partial}{\partial y}(y) = yx + 1.$$

Este anel diferencial

$$A_1(K_0) = K_0[y]\left[x;\frac{\partial}{\partial y}\right] \text{ designa-se por } 1^{\text{a}} \text{ Álgebra de Weyl.}$$

Esta construção pode ser repetida indutivamente, gerando assim outras álgebras de Weyl:

$$A_n(K_0) = A_1(A_{n-1}(K_0)) \qquad n\text{-ésima Álgebra de Weyl}$$

Observação: Se K_0 é um domínio, então $K_0[y]$ é um domínio, logo $A_1(K_0)$ é um domínio e analogamente todas as outras álgebras de Weyl são domínios.

2.1.2 Derivadas Interiores

Uma derivada δ em K diz-se *interior* se existe algum $c\in K$ tal que

$$\delta(a) = ca - ac, \qquad \forall a\in K.$$

Note-se que isto é de facto uma derivada:

- $\delta(a+b) = c(a+b) - (a+b)c = ca + cb - ac - bc = (ca - ac) + (cb - bc) = \delta(a) + \delta(b)$.
- $\delta(ab) = c(ab) - (ab)c = cab - acb + acb - abc = (ca - ac)b + a(cb - bc) = \delta(a)b + a\delta(b)$.

Exemplo. A derivada $\frac{\partial}{\partial y}$ do anel $K[y]$ não é interior, porque $\frac{\partial}{\partial y}(y) = 1$ e y comuta com qualquer elemento de $K[y]$ (logo, se $\frac{\partial}{\partial y}$ fosse interior, $\frac{\partial}{\partial y}(y) = cy - yc = 0$).

Embora sejam muito simples, as derivadas interiores não trazem nada de novo, no sentido de que: se δ é uma derivada interior então $K[x;\delta] \cong K[t]$ (para uma nova indeterminada t). De facto,

$$(x-c)a = ax + \delta(a) - ca = ax - ac = a(x-c), \forall a \in K,$$

$$\text{e} \quad x(x-c) = x^2 - xc = x^2 - (cx + \delta(c)) = x^2 - cx = (x-c)x,$$

logo $t = x - c$ comuta com qualquer polinómio em x.

Para além disso, as potências de t são algebricamente independentes: se este polinómio

$$\sum_{i=0}^{n} a_i t^i = \sum_{i=0}^{n} a_i (x-c)^i = 0$$

é o polinómio nulo, queremos ver que todos os coeficientes a_i são nulos.

Lema 2.1 *Sejam a, b elementos de um anel R tal que $ab = ba$. Então,*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Demonstração. Para $n = 1$, a afirmação $a + b = a^1 b^0 + a^0 b^1$ é óbvia. Supondo que vale para $n-1$, então

$$\begin{aligned}
(a+b)^n &= (a+b) \sum_{i=0}^{n-1} \binom{n-1}{i} a^{(n-1)-i} b^i \\
&= \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-i} b^i + \sum_{i=0}^{n-1} \binom{n-1}{i} b a^{(n-1)-i} b^i \\
&= \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-i} b^i + \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-(i+1)} b^{i+1} \\
&\quad \text{porque } a \text{ e } b \text{ comutam} \\
&= \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-i} b^i + \sum_{i=1}^{n} \binom{n-1}{i-1} a^{n-i} b^i \\
&= a^n + \sum_{i=1}^{n-1} \left[\binom{n-1}{i} + \binom{n-1}{i-1} \right] a^{n-i} b^i + b^n \\
&= \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i. \qquad \square
\end{aligned}$$

Como $\delta(-c) = 0$, x e $-c$ comutam e do Lema anterior resulta que

$$0 = \sum_{i=0}^{n} a_i(x-c)^i = \sum_{i=0}^{n}\sum_{j=0}^{i} a_i \binom{i}{j}(-c)^{i-j}x^j = \sum_{j=0}^{n}\left[\sum_{i=j}^{n}\binom{i}{j}a_i(-c)^{i-j}\right]x^j$$

e, sendo $K[x;\delta]$ um K-módulo livre à esquerda com base $1, x, x^2, \ldots$, temos que todos os coeficientes são nulos, isto é, para cada $j = 0, 1, \ldots, n$,

$$\sum_{i=j}^{n}\binom{i}{j}a_i(-c)^{i-j} = a_j + \sum_{i=j+1}^{n}\binom{i}{j}a_i(-c)^{i-j} = 0$$

$$\text{logo} \qquad a_j = -\sum_{i=j+1}^{n}\binom{i}{j}a_i(-c)^{i-j},$$

ou seja, cada coeficiente a_j é combinação linear dos coeficientes a_i com $i > j$. Como $a_n = 0$ deduz-se que $a_j = 0$ para todo j. Deste modo,

$$K[x;\delta] \cong K[t].$$

2.2 O Anel dos Polinómios Torcidos

Analogamente ao que foi feito para $K[x;\delta]$, podemos manter $K[x]$ como um módulo livre sobre K com a adição usual de polinómios mas alterar a multiplicação segundo a seguinte fórmula

$$xa = \sigma(a)x,$$

onde $\sigma(a) \in K$ depende de a.

Seja $\sigma : K \mapsto K$ uma aplicação. Para que a multiplicação de polinómios seja associativa e distributiva, é necessário que:

- $x(ab) = (xa)b \Leftrightarrow \sigma(ab)x = (\sigma(a)x)b = \sigma(a)\sigma(b)x$
- $x(a+b) = xa + xb \Leftrightarrow \sigma(a+b)x = \sigma(a)x + \sigma(b)x = (\sigma(a) + \sigma(b))x$
- $x = x1 = \sigma(1)x$

e, sendo $K[x]$ um K-módulo livre com base $\{1, x, x^2, \ldots\}$, então $\sigma(ab) = \sigma(a)\sigma(b), \sigma(a+b) = \sigma(a) + \sigma(b)$ e $\sigma(1) = 1$, ou seja, σ é um endomorfismo de K.

É possível mostrar que dado um endomorfismo σ de K existe uma estrutura de anel no módulo livre $K[x]$ tal que $xa = \sigma(a)x$ para todo $a \in K$ e esse anel diz-se o *anel dos polinómios torcidos* e denota-se por $K[x;\sigma]$. Então, a multiplicação de polinómios à esquerda é definida por

$$\left(\sum a_i x^i\right)\left(\sum b_j x^j\right) = \sum a_i \sigma^i(b_j)x^{i+j}.$$

Observação: Um polinómio à esquerda é um polinómio com coeficientes à esquerda, $\sum_{i=0}^{n} a_i x^i$, e um polinómio à direita tem os coeficientes à direita, $\sum_{i=0}^{n} x^i a_i$. No anel dos polinómios torcidos, qualquer polinómio à direita é um polinómio à esquerda, porque

$$\sum_{i=0}^{n} x^i a_i = \sum_{i=0}^{n} \sigma^i(a_i) x^i$$

mas o recíproco não é válido, porque σ^i pode não ser sobrejectiva.

No anel dos operadores diferenciais, qualquer polinómio à direita é à esquerda (porque $xa = ax + \delta(a)$) e qualquer polinómio à esquerda é à direita (porque $ax = xa - \delta(a)$), logo não é relevante especificar a lateralidade do polinómio.

2.3 Simplicidade

Nesta secção, vamos ver alguns resultados sobre os ideais (bilaterais) dos anéis $K[x]$, $K[x;\delta]$ e $K[x;\sigma]$ e vamos ver também condições para que o anel dos operadores diferenciais $K[x;\delta]$ seja simples.

O anel dos polinómios $K[x]$ tem uma propriedade muito importante, nele é válido o Algoritmo da Divisão: dados dois polinómios f e g, com $g \neq 0$, existem dois polinómios únicos q (o quociente) e r (o resto) tais que

$$f = qg + r,$$

com $r = 0$ ou $\deg(r) < \deg(g)$.

Esta propriedade permite-nos obter o seguinte resultado sobre os ideais de $K[x]$:

Proposição 2.2 *Seja K um anel de divisão. Os ideais (bilaterais) de $R = K[x]$ são da forma*

$$I = R \cdot f,$$

onde f é um polinómio de I de grau minimal, com coeficientes centrais.

Demonstração. Em primeiro lugar, vejamos que $I = Rf$ com f central é um ideal de R: para qualquer elemento f de um anel R, o conjunto dos múltiplos à esquerda $Rf = \{gf : g \in R\}$ é um ideal à esquerda e, se f for central (i.e. $fg = gf$ para todo g), então para qualquer elemento h de R e elemento gf de Rf tem-se que $(gf)h = (gh)f$ que pertence de novo a Rf.

Seja I um ideal não nulo de $R = K[x]$. Dado $0 \neq f \in I \leq R$ de grau minimal, temos que para qualquer polinómio $g \in I$ existem $q, r \in R$ tais que $g = qf + r$, onde $r = 0$ ou $\deg(r) < \deg(f)$. Como I é um ideal e $f, g \in I$, então $r = g - qf \in I$, e como f tem grau minimal, então $r = 0$, ou seja, $g = qf$. Portanto, $I = R \cdot f$.

Para além disso, como K é um anel de divisão podemos escolher um gerador de I da forma

$$f = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0.$$

Para qualquer elemento $d \in K$, o polinómio

$$df - fd = (da_{n-1} - a_{n-1}d)x^{n-1} + \ldots + (da_1 - a_1d)x + (da_0 - a_0d)$$

pertence a I e tem grau inferior ao de f. Pela minimalidade do grau de f, temos que $df - fd = 0$, isto é, $da_i = a_id$. Sendo d um elemento qualquer de K, os coeficientes a_i de f são centrais. □

2.3.1 Simplicidade no Anel de Operadores Diferenciais

Nesta subsecção vamos demonstrar um Teorema (2.4) que nos dá condições para que o anel dos operadores diferenciais $K[x;\delta]$ seja simples. Para isso, é necessário introduzir algumas definições:

Definição 2.3 *Seja K um anel e δ uma derivada nele. Um ideal I de K diz-se δ-ideal se $\delta(I) \subseteq I$. Dizemos que K é δ-simples se $K \neq 0$ e os seus únicos δ-ideais são 0 e K.*

Claro que um anel simples K, cujos únicos ideais são 0 e K, é δ-simples, porque $\delta(0) = 0$ e $\delta(K) \subset K$.

Para além disso, um anel K diz-se uma $\mathbb{Q}$-álgebra se existe um homomorfismo injectivo

$$\begin{array}{ccc} \mathbb{Q} & \to & K \\ \frac{a}{b} & \mapsto & \frac{a}{b} \cdot 1_K \end{array}.$$

Teorema 2.4 *Seja K uma $\mathbb{Q}$-álgebra com derivada δ. $R = K[x;\delta]$ é um anel simples se e só se K é δ-simples e δ não é uma derivada interior de K.*

Demonstração.
($\Longrightarrow$)
Se δ é interior, então $R \cong K[t]$ que claramente não é um anel simples; por exemplo, RtR é um ideal não nulo e diferente de R.

Se K tem um ideal $I \neq 0$ e $I \neq K$ tal que $\delta(I) \subset I$, então definimos

$$J = \left\{ \sum a_i x^i \in R : a_i \in I \right\} = I.R$$

o conjunto dos polinómios com coeficientes em I. Vejamos que J é um ideal de R:

$$\sum a_i x^i + \sum b_i x^i = \sum \underbrace{(a_i + b_i)}_{\in I \text{ porque } I \text{ é ideal.}} x^i \in J$$

$$x \cdot \sum a_i x^i = \sum (x a_i) x^i = \sum (a_i x + \delta(a_i)) x^i = \sum \underbrace{a_i}_{\in I} x^{i+1} + \sum \underbrace{\delta(a_i)}_{\in I \text{ porque } I \text{ é } \delta\text{-ideal}} x^i \in J$$

Logo, J é um ideal à esquerda.

$$(\sum a_i x^i) \cdot b = \sum a_i (x^i b) = \sum_i \sum_{j=0}^{i} \underbrace{a_i \binom{i}{j} \delta^j(b)}_{\in I \text{ porque } a_i \in I \text{ e } I \text{ é um ideal.}} x^{i-j} \in J$$

Logo, J é também ideal à direita.

Portanto, J é um ideal de R e $J \neq 0$ (porque $I \neq 0$) e $J \neq R$ (caso contrário, $1 \in J$ logo $1 \in I$ e $I = R$). Como R tem um ideal J não trivial, R não é simples.

($\Longleftarrow$)

Suponhamos que K é δ-simples mas R não é simples, digamos com ideal $I \neq 0$ e $I \neq R$. Queremos mostrar que δ é uma derivada interior.

Sejam

$$n = \min_{0 \neq f \in I} \{\deg(f)\}$$

e

$$J = \{\mathrm{cg}(f) : 0 \neq f \in I, \deg(f) = n\} \cup \{0\}.$$

Vejamos que J é um ideal bilateral de K:

- sejam $a, b \in J \setminus \{0\}$.
  - se $a = b$, então $a - b = 0 \in J$
  - se $a \neq b$, consideremos $f, g \in I$ de grau n com $a = \mathrm{cg}(f)$ e $b = \mathrm{cg}(g)$. Então, $f - g = (a-b)x^n + (\text{termos de grau } \leq n-1) \in I$ (porque I é ideal), tem grau n e tem coeficiente guia $a - b$, logo
  $$a - b \in J.$$
- sejam $\lambda \in K$ e $a \in J \setminus \{0\}$.
  - se $\lambda a = 0$, então $\lambda a \in J$.
  - se $\lambda a \neq 0$, tomamos $a = \mathrm{cg}(f)$, com $f \in I$ de grau n. Então, $\lambda f = (\lambda a)x^n + (\text{termos de grau } \leq n-1) \in I$ (porque I é ideal), tem grau n e tem coeficiente guia λa, logo
  $$\lambda a \in J.$$

- sejam $\lambda \in K$ e $a \in J \setminus \{0\}$.
  - se $a\lambda = 0$, então $a\lambda \in J$.
  - se $a\lambda \neq 0$, tomamos $a = \mathrm{cg}(f)$, com $f \in I$ de grau n. Então,

$$\begin{aligned} f\lambda &= (ax^n + \text{termos de grau } \leq n-1)\lambda \\ &= ax^n\lambda + (\text{termos de grau } \leq n-1) \\ &= a\lambda x^n + \sum_{i=1}^{n} a\binom{n}{i}\delta^i(\lambda)x^{n-i} + (\text{termos de grau } \leq n-1) \\ &= (a\lambda)x^n + (\text{termos de grau } \leq n-1) \end{aligned}$$

    ou seja, $f\lambda \in I$ (porque I é ideal), tem grau n e tem coeficiente guia $a\lambda$, logo

$$a\lambda \in J.$$

Portanto, J é um ideal não nulo de K. Vejamos que é um δ-ideal:

- seja $a \in J$.
  - Se $\delta(a) = 0$, então $\delta(a) \in J$.
  - Se $\delta(a) \neq 0$, consideremos $f = \sum_{i=0}^{n} a_i x^i \in I$ com coeficiente guia a. Então,

$$\begin{aligned} xf - fx &= \sum_{i=0}^{n}(xa_i)x^i - \sum_{i=0}^{n} a_i x^{i+1} \\ &= \sum_{i=0}^{n} a_i x^{i+1} + \sum_{i=0}^{n}\delta(a_i)x^i - \sum_{i=0}^{n} a_i x^{i+1} \\ &= \delta(a)x^n + \delta(a_{n-1})x^{n-1} + \ldots + \delta(a_0) \end{aligned}$$

    isto é, $xf - fx \in I$ (porque I é ideal) tem grau n e coeficiente guia $\delta(a)$, logo

$$\delta(a) \in J.$$

Como K é δ-simples, temos que $J = K$, logo $1 \in J$, isto é, existe um polinómio

$$f = x^n + dx^{n-1} + (\text{termos de grau } \leq n-2) \qquad \text{em I.}$$

Então, $\forall a \in K$

$$\begin{aligned} af - fa &= (ax^n + adx^{n-1} + \text{termos de grau } \leq n-2) - (x^n a + dx^{n-1}a + \\ &\quad \text{termos de grau } \leq n-2) \\ &= ax^n + adx^{n-1} - \sum_{i=0}^{n}\binom{n}{i}\delta^i(a)x^{n-i} - d\sum_{j=0}^{n-1}\binom{n-1}{j}\delta^j(a)x^{n-1-j} \\ &\quad + (\text{termos de grau } \leq n-2) \\ &= ax^n + adx^{n-1} - ax^n - n\delta(a)x^{n-1} - dax^{n-1} + (\text{termos de grau } \leq n-2) \\ &= (ad - da - n\delta(a))x^{n-1} + (\text{termos de grau } \leq n-2). \end{aligned}$$

Como $af - fa \in I$ (porque I é ideal) tem grau $n-1$ e n é o grau minimal dos polinómios em I, então $af - fa$ é o polinómio nulo, logo

$$ad - da - n\delta(a) = 0, \quad \forall a \in K$$

e como $\mathbb{Q} \subset K$,

$$\delta(a) = \frac{ad - da}{n} = a\left(\frac{d}{n}\right) - \left(\frac{d}{n}\right)a, \qquad \forall a \in K.$$

Portanto, δ é uma derivada interior de K. □

Corolário 2.5 (Teorema de Amitsur) *Sejam K um anel simples de característica 0 e δ uma derivada não interior de K. Então, $R = K[x;\delta]$ é um anel simples.*

Demonstração. Como $carK = 0$, podemos fazer a seguinte identificação:

$$n \in \mathbb{N} \longmapsto n1_K = \underbrace{1_K + \ldots + 1_K}_{n \text{ vezes}} \in K.$$

De facto, $n1_K \in Z(K)$, porque $\forall a \in K$

$$(n1_K)a = (1_K + \ldots + 1_K)a = a + \ldots + a = a(1_K + \ldots + 1_K) = a(n1_K).$$

Como K é simples, pela Proposição 1.19 o seu centro $Z(K)$ é um corpo, logo podemos ainda fazer a identificação:

$$\frac{a}{b} \in \mathbb{Q} \leftrightarrow (a1_K)(b1_K)^{-1} \in Z(K) \subset K.$$

Então, K é uma $\mathbb{Q}$-álgebra. Como K é simples, então é δ-simples. Pelo Teorema 2.4, $R = K[x;\delta]$ é um anel simples. □

Por exemplo,

$$\mathbb{Q}\left[x;\frac{\partial}{\partial x}\right], \mathbb{R}\left[x;\frac{\partial}{\partial x}\right], \mathbb{C}\left[x;\frac{\partial}{\partial x}\right] \qquad \text{são anéis simples.}$$

Em particular para as álgebras de Weyl temos o seguinte resultado:

Corolário 2.6 *Seja K_0 um anel (resp. domínio) simples de característica 0. Então, as álgebras de Weyl $A_n(K_0)$ são anéis (resp. domínios) simples.*

Demonstração. Como $A_n(K_0) = A_1(A_{n-1}(K_0))$, basta provar que

$$A_1(K_0) = K_0[y]\left[x; \frac{\partial}{\partial y}\right] \text{ é um anel (resp. domínio) simples}$$

para qualquer anel (resp. domínio) simples K_0.

Como já foi referido anteriormente, $\frac{\partial}{\partial y}$ não é uma derivada interior de $K_0[y]$, porque y é central e $\delta(y) = 1$. Vejamos que, embora $K_0[y]$ não seja simples, ele é $\frac{\partial}{\partial y}$-simples.

Seja I um $\frac{\partial}{\partial y}$-ideal não nulo de $K_0[y]$. Queremos ver que $I = K_0[y]$. Seja $f = ay^n + \ldots$ $(a \neq 0)$ um polinómio de I de grau minimal (n). Então,

$$\frac{\partial}{\partial y}(f) = nay^{n-1} + \ldots.$$

$\frac{\partial}{\partial y}(f) \in I$ (porque I é $\frac{\partial}{\partial y}$-ideal) tem grau $n-1$, logo é o polinómio nulo, em particular, $na = 0$; como $a \neq 0$ e $carK_0 = 0$, então $n = 0$. Ou seja, $f = a$ é um polinómio constante não nulo que pertence a $I \cap K_0$, que é um ideal de K_0; sendo K_0 simples, $I \cap K_0 = K_0$, em particular, $1 \in I \cap K_0 \subset I$ e, deste modo,

$$I = K_0[y].$$

Portanto, $K_0[y]$ é $\frac{\partial}{\partial y}$-simples e $\frac{\partial}{\partial y}$ é uma derivada não interior; pelo Teorema de Amitsur, $A_1(K_0)$ é um anel simples. □

Observação: A condição $carK_0 = 0$ é essencial.
Suponhamos que K_0 tem característico $p > 0$. Vejamos por indução que $x^m y = yx^m + mx^{m-1}$:

- $m = 1 : xy = yx + \delta(y) = yx + 1$
- $m \to m + 1$:

$$\begin{aligned} x^{m+1}y &= x(x^m y) = x(yx^m + mx^{m-1}) = (yx+1)x^m + mx^m \\ &= yx^{m+1} + x^m + mx^m = yx^{m+1} + (m+1)x^m \end{aligned}$$

Então, $x^p y = yx^p + px^{p-1} = yx^p$, isto é x^p comuta com y, pelo que x^p comuta com qualquer polinómio de $K_0[y]$; como comuta também com qualquer polinómio em x, temos que

$$A_1(K_0)x^p \text{ é de facto um ideal bilateral}$$

não nulo (porque contém x^p) e diferente de $A_1(K_0)$ (porque não contém 1). Portanto,

$$A_1(K_0) \text{ não é um anel simples.}$$

□

2.3.2 Simplicidade no Anel dos Polinómios Torcidos

Ao longo desta secção, consideremos K um anel de divisão. Nesta secção, vamos ver um resultado sobre os ideais do anel $K[x;\sigma]$. Para enunciá-lo vejamos as seguintes definições:

Definição 2.7 *Seja K um anel de divisão.*

1. *Um automorfismo é um homomorfismo $\sigma : K \to K$ bijectivo.*
2. *Um automorfismo $\sigma : K \to K$ diz-se interior se existe $a \in K$ tal que $\sigma(b) = aba^{-1}, \forall b \in K$.*
3. *Um automorfismo $\sigma : K \to K$ diz-se ter ordem interior finita se para algum $n \in \mathbb{N}$ σ^n é interior, isto é, se $\exists\, n, \exists\, a \in K : \sigma^n(b) = aba^{-1}, \forall b \in K$.*

Nota: No caso K comutativo, o único automorfismo interior é a identidade, porque $\sigma(b) = aba^{-1} = baa^{-1} = b, \forall b$. Logo, σ é um automorfismo de ordem interior finita se $\exists\, n \in \mathbb{N} : \sigma^n = id$.

Proposição 2.8 *Seja K um anel de divisão com um endomorfismo σ. Se σ não é um automorfismo de ordem interior finita, então os ideais não nulos de $R = K[x;\sigma]$ são $R \cdot x^m, m \geq 0$.*

Demonstração. Em primeiro lugar, vejamos que cada $I = R \cdot x^m$ é um ideal:

- dados $fx^m, gx^m \in I$, temos que $fx^m - gx^m = (f-g)x^m \in I$.
- dado $fx^m \in I$, $g = \sum_{i=0}^{n} a_i x^i \in R$, claro que $gfx^m \in I$ e

$$fx^m \cdot g = fx^m \cdot \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} f\sigma^m(a_i)x^{m+i} = \left(\sum_{i=0}^{n} f\sigma^m(a_i)x^i\right) x^m \in I.$$

Reciprocamente, seja I um ideal não nulo de R. À semelhança do que acontece no anel $K[x]$, o ideal I é gerado por um polinómio de grau minimal, digamos

$$f = x^m + a_{m-1}x^{m-1} + \ldots + a_n x^n,$$

com $m \geq n \geq 0$. Note-se que podemos tomar f mónico, porque K é um anel de divisão. O nosso objectivo é mostrar que todos os coeficientes a_i são nulos. Em primeiro lugar, $\forall i, \sigma(a_i) = a_i$:

$$fx - xf = x^{m+1} + a_{m-1}x^m + \ldots + a_n x^{n+1} - x^{m+1} - xa_{m-1}x^{m-1} - \ldots - xa_n x^n$$

$$= (a_{m-1} - \sigma(a_{m-1}))x^m + \ldots + (a_n - \sigma(a_n))x^{n+1},$$

isto é $fx - xf \in I$ (porque I é ideal) e tem o mesmo grau de f, logo $fx - xf = cf$, para algum $c \in K$. Comparando os coeficientes de x^n, temos que $c = 0$ logo $fx - xf = 0$, donde

$$\sigma(a_i) = a_i, \qquad \forall i = n, \ldots, m-1.$$

Seja $a \in K$.

$$\begin{aligned} fa - \sigma^m(a)f &= x^m a + a_{m-1}x^{m-1}a + \ldots + a_n x^n a \\ &\quad -\sigma^m(a)x^m - \sigma^m(a)a_{m-1}x^{m-1} - \ldots - \sigma^m(a)a_n x^n \\ &= \sigma^m(a)x^m + a_{m-1}\sigma^{m-1}(a)x^{m-1} + \ldots + a_n\sigma^n(a)x^n \\ &\quad -\sigma^m(a)x^m - \sigma^m(a)a_{m-1}x^{m-1} - \ldots - \sigma^m(a)a_n x^n \\ &= (a_{m-1}\sigma^{m-1}(a) - \sigma^m(a)a_{m-1})x^{m-1} + \ldots + (a_n\sigma^n(a) - \sigma^m(a)a_n)x^n. \end{aligned}$$

$fa - \sigma^m(a)f \in I$ (porque I é um ideal) e tem grau $m-1$, estritamente inferior ao de f, logo $fa - \sigma^m(a)f = 0$. Então, $\forall i = n, \ldots, m-1$,

$$a_i\sigma^i(a) = \sigma^m(a)a_i \Leftrightarrow \sigma^i(a_i)\sigma^i(a) = \sigma^m(a)\sigma^m(a_i) \Leftrightarrow \sigma^i(a_i a) = \sigma^m(aa_i).$$

Note-se que σ é injectiva: o núcleo de σ é um ideal de K e, como K é um anel de divisão, então os únicos ideais são 0 e K, ou seja, σ é injectiva ou $\sigma \equiv 0$ (que não é um endomorfismo, o que é absurdo). Então, $a_i a = \sigma^{m-i}(aa_i) = \sigma^{m-i}(a)a_i$ e, portanto, se algum $a_i \neq 0$

$$\sigma^{m-i}(a) = a_i a a_i^{-1}, \qquad \forall a \in K$$

e σ seria um automorfismo de ordem interior finita. Portanto, todos os $a_i = 0$, logo $f = x^m$ e $I = R \cdot x^m$. □

Em particular, se K for um anel de divisão e σ não for um automorfismo de ordem interior finita, então $K[x;\sigma]$ *não* é um anel simples.

Por outro lado, se σ for um automorfismo de ordem finita, digamos $\sigma^m = id$, pela fórmula $x^m a = \sigma^m(a)x^m$ temos que x^m é central em $K[x;\sigma]$. Mas como x^m não é invertível (em $K[x;\sigma]$, logo em $Z(K[x;\sigma])$), então o centro de $K[x;\sigma]$ não é um corpo e por 1.19 $K[x;\sigma]$ não é simples.

Portanto, se K for um anel de divisão $K[x;\sigma]$ *não* é simples.

Ao longo do próximo capítulo, iremos introduzir o conceito central desta tese - os ANÉIS PRIMITIVOS - e explorar várias das suas propriedades.

3 Anéis Primitivos

Neste capítulo vamos introduzir o conceito central desta tese, a noção de *anel primitivo*:

um anel que tem um módulo simples e fiel.

Começamos por estudar algumas propriedades básicas desta nova classe de anéis, acompanhadas de alguns exemplos. De seguida, debruçamo-nos sobre o problema:

Quantos módulos simples e fiéis tem um anel primitivo?
E sobre que condições esse módulo é único?

Para além disso, vamos explorar mais exemplos de anéis primitivos, nomeadamente alguns anéis livres. E, por fim, terminamos este capítulo estudando a noção de primitividade em classes especiais de anéis (a classe dos anéis artinianos à esquerda e a classe dos anéis comutativos) e introduzindo a noção de *ideal primitivo*.

Para motivar a definição de anel primitivo à esquerda, vejamos a seguinte caracterização de um anel semiprimitivo (ou J-semisimples):

Proposição 3.1 *Um anel R é semiprimitivo se e só se R tem um módulo à esquerda M semisimples e fiel.*

Demonstração. Suponhamos que existe um R-módulo à esquerda M semisimples e fiel. Podemos escrever $M = \bigoplus_{i\in I} M_i$, onde M_i são R-módulos simples. Pela Proposição 1.24 qualquer elemento do $\mathrm{Jac}(R)$ anula todos os módulos simples M_i, então

$$\mathrm{Jac}(R)\cdot M = \bigoplus_{i\in I} \mathrm{Jac}(R)\cdot M_i = 0.$$

Como M é fiel, $\mathrm{Jac}(R) = 0$, ou seja, R é semiprimitivo.

Reciprocamente, suponhamos que $\mathrm{Jac}(R) = 0$. Queremos ver que existe um R-módulo à esquerda semisimples e fiel. Seja $\{M_i : i \in I\}$ um conjunto de representantes de classes de equivalência de R-módulos à esquerda simples, isto é, se M é um R-módulo simples então $M \cong M_i$ (para algum $i \in I$) e $M_i \ncong M_j$ (para $i \neq j$). Definindo

$$M = \bigoplus_{i\in I} M_i,$$

temos que M é semisimples (porque é soma directa de módulos simples) e pela Proposição 1.24

$$\mathrm{Ann}(M) = \bigcap_{i\in I} \mathrm{Ann}(M_i) = \mathrm{Jac}(R).$$

Como $\mathrm{Jac}(R) = 0$, então M é um R-módulo fiel e, sendo assim, é o módulo procurado.□

Motivada pela Proposição anterior, temos então a seguinte definição:

Definição 3.2 *Um anel R diz-se primitivo à esquerda (resp. à direita) se R tem um módulo à esquerda (resp. à direita) simples e fiel.*

Antes de vermos alguns exemplos de anéis primitivos à esquerda, vamos estudar algumas das suas propriedades, começando por relacioná-los com outras classes já bem conhecidas de anéis.

Proposição 3.3 *1. Um anel simples é primitivo à esquerda (e à direita).*

2. Um anel primitivo à esquerda é semiprimitivo e primo.

Demonstração. Suponhamos que R é simples. Para qualquer R-módulo M, $\mathrm{Ann}(M)$ é um ideal (bilateral) de R, logo $\mathrm{Ann}(M) = 0$ ou $\mathrm{Ann}(M) = R$. Neste último teríamos $R \cdot M = 0$, em particular $M = 1 \cdot M = 0$. Então, qualquer R-módulo não nulo é fiel.

Pela Proposição 1.3, qualquer anel R tem um ideal à esquerda maximal I. Então, R/I é um R-módulo à esquerda simples (pela Proposição 1.13) e fiel (pelo parágrafo anterior). Portanto, R é um anel primitivo à esquerda.

Se R é um anel primitivo à esquerda, isto é, tem um módulo M simples e fiel, então M é semisimples e fiel e pela Proposição 3.1 R é semiprimitivo. Visto doutra forma, sendo M um R-módulo simples e fiel, $\mathrm{Ann}(M) = 0$ e pela Proposição 1.24 $\mathrm{Jac}(R) = 0$.

Resta-nos ver que R é primo, isto é

$$\text{se } I, J \neq 0 \text{ são ideais, então } IJ \neq 0.$$

Seja $I \neq 0$ um ideal qualquer de R. Então, $I \cdot M$ é um R-submódulo de M: dados $r \in R$ e $\sum_{i=1}^{n} a_i \cdot m_i \in I \cdot M$ (onde $a_i \in I, m_i \in M, \forall i$) temos que

$$r \cdot \left(\sum_{i=1}^{n} a_i \cdot m_i \right) = \sum_{i=1}^{n} (ra_i) \cdot m_i \in I \cdot M \quad \text{(porque } I \text{ é um ideal).}$$

Como ${}_RM$ é fiel, então $I \cdot M \neq 0$ (caso contrário, $I \subset \mathrm{Ann}(M) = 0$). Como M é simples, então $I \cdot M = M$. Considerando outro ideal $J \neq 0$ de R e aplicando um argumento análogo, temos

$$(JI) \cdot M = J \cdot (I \cdot M) = J \cdot M = M,$$

em particular, $JI \neq 0$, ou seja, R é um anel primo. □

Então, os anéis simples são exemplos de anéis primitivos à esquerda, nomeadamente os anéis de divisão (por exemplo $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$) e os anéis de matrizes $\mathcal{M}_n(D)$ sobre anéis de divisão D; para além disso, tendo em conta os Teoremas 2.5 e 2.6, temos ainda os

exemplos do anel de operadores diferenciais $K[x;\delta]$ (com K anel simples de característica 0 e δ derivada não interior de K) e as álgebras de Weyl $A_n(K_0)$ (com K_0 anel simples de característica 0).

Tendo em conta as relações entre anéis primitivos e as outras classes referidas na Proposição anterior, podemos completar o quadro de implicações apresentado no Capítulo 1:

$$\begin{array}{ccccc} \text{Semisimples} & \Longrightarrow & \text{Semiprimitivo} & \Longrightarrow & \text{Semiprimo} \\ \Uparrow (+\text{CCD}) & & \Uparrow & & \Uparrow \\ \text{Simples} & \Longrightarrow & \text{Primitivo (à esquerda)} & \Longrightarrow & \text{Primo} \end{array}$$

Vejamos agora um exemplo muito importante de um anel primitivo:

Exemplo 3.1:

Sejam K um anel de divisão e V_K um espaço vectorial sobre K (à direita) e consideremos o anel $E = \text{End}(V_K)$. Podemos munir V com estrutura de E-módulo à direita, através da seguinte acção:

$$v \cdot \varphi = (v)\varphi \qquad \forall \varphi \in E, v \in V.$$

Verificam-se as 4 propriedades de acção de um módulo:

- $v \cdot (\psi \circ \varphi) = (v)(\psi \circ \varphi) = ((v)\psi)\varphi = (v \cdot \psi)\varphi = (v \cdot \psi) \cdot \varphi$.
- $v \cdot (\varphi + \psi) = (v)(\varphi + \psi) = (v)\varphi + (v)\psi = v \cdot \varphi + v \cdot \psi$.
- $(u + v) \cdot \varphi = (u + v)\varphi = (u)\varphi + (v)\varphi = u \cdot \varphi + v \cdot \varphi$, pela K-linearidade do homomorfismo φ.
- $v \cdot 1_E = (v)id_V = v$.

Logo, V é um E-módulo à direita e, de facto, é simples e fiel:

- V fiel: $V \cdot \varphi = 0 \Leftrightarrow (v)\varphi = 0, \forall v \in V \Leftrightarrow \varphi \equiv 0$.
- V simples: sejam $W \neq 0$ um E-submódulo e $0 \neq v \in V$ qualquer. Queremos mostrar que $v \in W$. Tomando $0 \neq w \in W$, existe uma base de V da forma $\{w\} \cup \{e_i : i \in I\}$, logo podemos escrever

  $$v = w\lambda + \sum_{i \in I} e_i \mu_i \qquad \text{para } \lambda, \mu_i \in K.$$

  Para cada $i \in I$, definimos o K-homomorfismo φ_i determinado por $w \mapsto e_i$ e $e_j \mapsto 0, \forall j$. Definimos o K-homomorfismo

  $$\varphi = id\lambda + \sum_{i \in I} \varphi_i \mu_i.$$

Note-se que esta soma não é infinita, porque v é combinação linear finita dos vectores da base.

Então,

$$w \cdot \varphi = (w)\varphi = (w)id\lambda + \sum_{i \in I}(w)\varphi_i\mu_i = w\lambda + \sum_{i \in I} e_i\mu_i = v.$$

Como $\varphi \in E$ e $w \in W$ e W é um E-submódulo, então $w \cdot \varphi = v \in W$. Deste modo, $W = V$. Assim sendo, V é simples.

Portanto,

$$\underline{E = \mathrm{End}(V_K) \text{ é um anel primitivo à direita.}}$$

Se $\dim(V_K) = n < \infty$, então $E \cong \mathcal{M}_n(K)$ é um anel simples e artiniano. Mas se $\dim(V_K)$ é infinita, então E é um exemplo de um anel que é primitivo à esquerda mas não é simples:

$$I = \{f \in \mathrm{End}(V_K) \mid \dim(\mathrm{Im}(f)) < \infty\}$$

é um ideal não trivial de $\mathrm{End}(V_K)$:

1. dados $f, g \in I$, temos que $\mathrm{Im}(f \pm g) \subset \mathrm{Im}(f) + \mathrm{Im}(g)$, logo

   $$\dim \mathrm{Im}(f \pm g) \leq \dim(\mathrm{Im}(f) + \mathrm{Im}(g)) \leq \dim \mathrm{Im}(f) + \dim \mathrm{Im}(g) < \infty.$$

   Então, $f \pm g \in I$.

2. sejam $f \in I$ e $g \in E$.

   Por um lado, como $\mathrm{Im}(g \circ f) \subset \mathrm{Im}(f)$, $\dim \mathrm{Im}(g \circ f) \leq \dim \mathrm{Im}(f) < \infty$, logo $g \circ f \in I$. Por outro lado, como $\mathrm{Im}(f \circ g) = \mathrm{Im}(g|_{\mathrm{Im}(f)})$, então

   $$\dim \mathrm{Im}(f \circ g) = \dim \mathrm{Im}(g|_{\mathrm{Im}(f)}) = \dim \mathrm{Im}(f) - \dim \mathrm{Ker}(g|_{\mathrm{Im}(f)}) \leq \dim \mathrm{Im}(f) < \infty,$$

   logo $f \circ g \in I$.

Este exemplo é bastante importante, porque mais tarde iremos ver que qualquer anel R primitivo à esquerda "é parecido" com $\mathrm{End}(V_K)$ num certo sentido.

Observação: Enquanto que a noção de semiprimitividade é simétrica à-esquerda/à-direita, a noção de primitividade não é. De facto, em 1964 G.Bergman publicou um artigo [2] onde construiu um exemplo de um anel que é primitivo à direita mas não o é à esquerda. Mais tarde, A.V. Jategaonkar encontrou outros exemplos [17, Chapter 2.1 E].

Vejamos agora um resultado simples que caracteriza os anéis primitivos.

Proposição 3.4 (Caracterização dos Anéis Primitivos) *Um anel R é primitivo à esquerda (resp. à direita) se e só se R tem um ideal à esquerda (resp. à direita) maximal que não contém ideais bilaterais não nulos.*

Demonstração.

($\Longrightarrow$) Suponhamos que M é um R-módulo simples e fiel. Pelo Teorema 1.13, $M \cong R/I$, onde I é um ideal à esquerda maximal de R. Sendo M fiel, $\mathrm{Ann}(R/I) = 0$ e pela Proposição 1.6 este é o maior ideal bilateral contido em I. Portanto, I é o ideal à esquerda procurado.

($\Longleftarrow$) Suponhamos que R tem um ideal à esquerda I maximal que não contém ideais bilaterais não nulos. R/I é um R-módulo à esquerda com acção

$$a(b+I) = ab + I.$$

Pelo Teorema 1.13, R/I é um módulo simples. Como $\mathrm{Ann}(R/I)$ é (o maior) ideal bilateral de R contido em I, então por hipótese $\mathrm{Ann}(R/I) = 0$. Portanto, R é primitivo à esquerda. □

Exemplo 1: Sejam K um anel de divisão e σ um endomorfismo de K que *não* é um automorfismo de ordem interior finita.

Seja $R = K[x;\sigma]$. Dado $a \in K \setminus \{0\}$, $x^m \notin R(x-a)$, caso contrário

$$x^m = (b_{m-1}x^{m-1} + b_{m-2}x^{m-2} \ldots + b_1 x + b_0)(x-a)$$

$$= b_{m-1}x^m + (b_{m-2} - b_{m-1}\sigma^{m-1}(a))x^{m-1} + \ldots + (b_0 - b_1\sigma(a))x - b_0 a$$

e comparando os coeficientes, teríamos que $b_0 = 0 \Rightarrow b_1 = 0 \Rightarrow \ldots \Rightarrow b_{m-1} = 0$ e x^m seria 0, o que é uma contradição. Então, pela Proposição 2.8 $R(x-a)$ não contém nenhum ideal não nulo de R.

Para além disso, $R(x-a)$ é um ideal à esquerda maximal de R: se J é um ideal à esquerda de R que contém estritamente $R(x-a)$, então existe $f \in J \setminus R(x-a)$ e pelo algoritmo da divisão, existem $q, r \in R$ tais que $f = q(x-a) + r$, onde $\deg(r) < \deg(x-a) = 1$ (logo $\deg(r) = 0$, ou seja, $r \in K$ é uma constante) ou $r = 0$ (o que é absurdo, já que $f \notin R(x-a)$); como $f, x-a \in J$, então $r \in J$ e é uma constante; sendo K um anel de divisão, $1 \in J$, donde $J = R$. Portanto, $R(x-a)$ é ideal à esquerda maximal.

Como $R(x-a)$ é um ideal à esquerda maximal de R que não contém ideais bilaterais não nulos, pela caracterização anterior temos que o anel dos polinómios torcidos $R = K[x;\sigma]$ é primitivo à esquerda, sendo $R/R(x-a)$ um módulo simples e fiel.

Exemplo 2: Sejam K um anel de divisão, que não é algébrico sobre o seu centro $Z(K)$, e $R = K[x]$.

Tomemos $a \in K$ que não seja algébrico sobre $Z(K)$. $R(x-a)$ é um ideal à esquerda maximal de R (tal como no exemplo anterior) e não contém ideais não nulos: se $R(x-a)$ contém um ideal $I \neq 0$, então pela Proposição 2.2 $I = R \cdot g$, com $g \in Z(K)[x]$. Como $g \in I \subset R(x-a)$, então $g(x) = f(x)(x-a)$, logo a é uma raíz de g (um polinómio com coeficientes em $Z(K)$), isto é a é algébrico sobre $Z(K)$, o que é absurdo.

Pela caracterização anterior, $R = K[x]$ é um anel primitivo à esquerda e $R/R(x-a)$ é um R-módulo à esquerda simples fiel. Analogamente, mostra-se que $R/(x-a)R$ é um R-módulo à direita simples e fiel, logo R é também primitivo à direita.

3.1 Unicidade do Módulo Simples e Fiel

Uma questão que surge directamente da definição de anel primitivo (à esquerda) é

Quantos módulos simples fiéis tem um anel primitivo, a menos de isomorfismo?

ou então

Quando é que um anel primitivo tem um único módulo simples e fiel, a menos de isomorfismo?

Ora, na classe dos anéis com um *ideal lateral minimal*, as noções de primitivo à esquerda e primitivo à direita são equivalentes (e até equivalentes à noção de primo!) e, para além disso, estas propriedades implicam a unicidade do módulo à esquerda (resp. à direita) simples e fiel, a menos de isomorfismo.

Para demonstrar este resultado, precisamos do seguinte lema:

Lema 3.5 *Sejam R um anel semiprimo e $a \in R$. Se Ra é um ideal à esquerda minimal, então aR é um ideal à direita minimal.*

Demonstração. Sejam R um anel semiprimo e $a \in R$. Supondo que Ra é minimal, queremos ver que aR é minimal. De facto, basta ver que $xR = aR$, para qualquer $0 \neq x \in aR$ (isto é, para ideais principais): porque se $0 \neq I \leq aR$ é um ideal à direita, então tomando $x \in I$ temos

$$0 \neq xR \leq I \leq aR$$

e $xR = aR \Rightarrow I = aR$.

Provemos, então, a minimalidade de aR em relação a ideais principais. Seja $0 \neq x \in aR$, digamos $x = ab$. Então, $I = RxR \neq 0$ é um ideal bilateral. Como R é semiprimo, $I^2 \neq 0$, isto é

$$I^2 = (RxR)(RxR) = RxRRxR = RxRxR = R(xRx)R \neq 0,$$

logo $xRx \neq 0$, ou seja, $\exists\, s \in R : xsx \neq 0$ e (escrevendo $x = ab$) $absab \neq 0$. Definimos a aplicação

$$\begin{array}{rcl} \varphi : Ra & \to & Ra \\ y & \mapsto & ybsa \end{array}$$

A aplicação está bem definida, porque $ybsa = (ybs)a \in Ra, \forall y \in Ra$. Para além disso, φ é um homomorfismo de R-módulos: $\forall y_1, y_2, y \in Ra, \forall \lambda \in R$,

- $(y_1 + y_2)\varphi = (y_1 + y_2)bsa = y_1bsa + y_2bsa = (y_1)\varphi + (y_2)\varphi$.
- $(\lambda y)\varphi = (\lambda y)bsa = \lambda(ybsa) = \lambda(y)\varphi$.

Como Ra é um R-módulo simples, pelo Lema de Schur $\mathrm{End}(Ra)$ é um anel de divisão. Como $\varphi \in \mathrm{End}(Ra)$ e não é a aplicação nula (porque $(a)\varphi = absa$ e $absab \neq 0$), então φ tem uma aplicação inversa $\psi : Ra \to Ra$. Então, pela R-linearidade de ψ

$$a = ((a)\varphi)\psi = (absa)\psi = ab(sa)\psi = x(sa)\psi \in xR,$$

donde $aR \subset xR \subset aR$, logo $xR = aR$.

Portanto, aR é minimal. □

Observação: A hipótese "R é um anel semiprimo" é essencial.

Por exemplo, seja K um anel de divisão e

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in K \right\}.$$

A matriz $E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ gera o ideal minimal à esquerda $RE_{11} = KE_{11}$ mas o ideal à direita que gera $E_{11}R = E_{11}K + E_{12}K$ não é minimal, porque contém o ideal $I = E_{12}K$, onde $E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Este anel R não é semiprimo: de facto, $I^2 = 0$.

Usando o lema anterior, demonstremos o teorema seguinte:

Teorema 3.6 *Seja R um anel com um ideal à esquerda minimal I. As afirmações seguintes são equivalentes:*

1. *R é primitivo à esquerda.*
2. *R é primitivo à direita.*
3. *R é primo.*

Neste caso, R tem também um ideal à direita minimal J. Para além disso, qualquer R-módulo à esquerda (resp. à direita) simples e fiel é isomorfo a ${}_RI$ (resp. J_R).

Demonstração. Já foi visto que (1) ou (2) implicam (3), na Proposição 3.3. Vejamos que (3) $\Rightarrow$ (1): suponhamos que R é primo. Claro que ${}_RI$ é um R-módulo simples e afirmamos que também é fiel: se $r \in R$ é tal que $rI = 0$, então

$$(RrR)(IR) = Rr(RI)R = R(rI)R = 0$$

e como RrR e IR são ideais bilaterais e R é primo, então $RrR = 0$ (e neste caso $r = 0$) ou $IR = 0$ (e neste caso $I = 0$, o que é absurdo porque I é minimal). Logo, $r = 0$, ou seja, ${}_RI$ é fiel. Portanto, R é primitivo à esquerda.

Para demonstrar (3) $\Rightarrow$ (2), basta ver que sendo R um anel primo então é também semiprimo e pelo Lema anterior R tem também um ideal à direita minimal J e um argumento análogo mostra que R é um anel primitivo à direita (sendo J_R o seu módulo simples e fiel).

Agora consideramos um R-módulo à esquerda M simples e fiel qualquer. Como M é fiel, $I \cdot m \neq 0$, para algum $m \in M$ (caso contrário $I \cdot M = 0$ e, sendo M fiel, $I = 0$ o que é absurdo, porque é minimal). Como $I \cdot m \neq 0$ é submódulo de M e M é simples, então $I \cdot m = M$.

A aplicação

$$\begin{array}{rcl} \varphi : I & \to & I \cdot m = M \\ a & \mapsto & a \cdot m \end{array}$$

é um homomorfismo de R-módulos:

$$(a+b)\varphi = (a+b) \cdot m = a \cdot m + b \cdot m = (a)\varphi + (b)\varphi$$

$$\text{e} \qquad (ra)\varphi = (ra) \cdot m = r \cdot (a \cdot m) = r \cdot (a)\varphi.$$

Como I e M são R-módulos simples, pelo Lema de Schur φ é um isomorfismo. Portanto, $M \cong I$. O argumento para R-módulos à direita é inteiramente análogo. $\square$

Exemplo 3.1 (continuação) Seja K um anel de divisão e V_K um espaço vectorial à direita sobre K. Já vimos que $E = \mathrm{End}(V_K)$ é um anel primitivo à direita.

Em primeiro lugar, dados quaisquer elementos $v, w \in V \setminus \{0\}$, existe uma aplicação $f \in E$ tal que $(v)f = w$: se v e w são linearmente independentes, então podemos decompor $V = vK \oplus wK \oplus U$ e definimos o K-homomorfismo $f : V \to V$ determinado por

$$v \mapsto w \qquad \text{e} \qquad w \mapsto v \qquad \text{e} \qquad u \in U \mapsto u.$$

Claro que $f \in E$ e $(v)f = w$. Se v e w não forem independentes, digamos $w = v\lambda$, definimos $f = id\lambda$ (que pertence a E) e $(v)f = v\lambda = w$.

Fixado $0 \neq v \in V$, definimos a aplicação entre E-módulos

$$\begin{array}{rccc} \varphi : & E_E & \to & V_E \\ & f & \mapsto & (v)f \end{array}$$

- φ é um E-homomorfismo: $\forall f, g \in E$,

$$(f+g)\varphi = (v)(f+g) = (v)f + (v)g = (f)\varphi + (g)\varphi$$

$$(f \circ g)\varphi = (v)(f \circ g) = ((v)f)g = (v)f \cdot g = (f)\varphi \cdot g$$

- φ é sobrejectiva, pelo comentário inicial.

Seja $e \in E$ uma projecção de V em vK, isto é, um homomorfismo $e : V \to vK$ sobrejectivo que deixa fixos os elementos de vK. Vejamos que $\mathrm{Ker}(\varphi) = \{f \in E : (v)f = 0\} = (1-e)E$: por um lado,

$$(v)\left((1-e)E\right) = (v - (v)e)E = (v-v)E = 0 \Rightarrow (1-e)E \subset \mathrm{Ker}(\varphi)$$

e, por outro lado, se $f \in \mathrm{Ker}(\varphi)$ (isto é $(v)f = 0$), então

$$(V)(ef) = (vK)f \underbrace{=}_{f \text{ é } K\text{-linear}} (v)fK \underbrace{=}_{(v)f = 0} 0,$$

logo $f = f - ef = (1-e)f \in (1-e)E$, isto é $\mathrm{Ker}(\varphi) \subset (1-e)E$.

Pelo Teorema do Isomorfismo, temos que

$$V = \mathrm{Im}(\varphi) \cong E/\mathrm{Ker}(\varphi) = \left(eE \oplus (1-e)E\right)/(1-e)E \cong eE$$

e como V é um E-módulo simples, então eE é um ideal à direita minimal de E.

Pelo Teorema 3.6, a menos de isomorfismo $eE \cong V_E$ é o único E-módulo à direita simples e fiel e analogamente Ee é o único E-módulo à esquerda simples e fiel. □

Estudemos a unicidade dos R-módulos simples e fiéis em alguns exemplos de anéis primitivos à esquerda que *não* têm ideal à esquerda minimal.

Exemplo 1: O anel dos operadores diferenciais $K[x;\delta]$.

Sejam K um anel de divisão de característica zero e δ uma derivação não interior de K. Pelo Teorema de Amitsur (2.5), o anel de polinómios diferencial $R = K[x;\delta]$ é um anel simples. Sendo $R(x-a)$ um ideal à esquerda maximal de R, para qualquer $a \in K$, pela prova da Proposição 3.3 temos que $R = K[x;\delta]$ é um anel primitivo à esquerda e

$$M_a = R/R(x-a) \text{ é um } R\text{-módulo à esquerda simples e fiel,}$$
$$\text{com acção } f \cdot (g + R(x-a)) = fg + R(x-a).$$

Quando é que $M_a \cong M_b$ como R-módulos?

Usando a decomposição $R = R(x-a) \oplus K$, podemos identificar $M_a \cong K$. Como $xc = cx + \delta(c) = c(x-a) + ca + \delta(c)$, então a acção de R sobre $K \cong M_a$ é determinada por

$$x * c = ca + \delta(c).$$

Se $\varphi : M_a \to M_b$ é um R-isomorfismo e $(1 + R(x-a))\varphi = c + R(x-b)$, então

$$0 = (x - a + R(x-a))\varphi = xc - ac + R(x-b) = cb + \delta(c) - ac + R(x-b).$$

Como $R(x-b) \cap K = 0, cb + \delta(c) - ac = 0$, isto é, $a = cbc^{-1} + \delta(c)c^{-1}$. Note-se que c^{-1} existe, porque K é anel de divisão e $c \neq 0$ (já que é imagem da classe de 1 pelo isomorfismo φ).

Reciprocamente, se existir $c \neq 0$ tal que $a = cbc^{-1} + \delta(c)c^{-1}$, definimos

$$(r + R(x-a))\varphi = rc + R(x-b)$$

e facilmente se vê que φ preserva as acções de R sobre M_a e M_b. Para além disso, φ é claramente bijectiva (a sua inversa é a multiplicação por c^{-1}) e portanto $M_a \cong M_b$.

Portanto, $M_a \cong M_b$ se e só se $\exists\, c \in K \setminus \{0\} : a = cbc^{-1} + \delta(c)c^{-1}$. Neste caso, dizemos que a é δ-conjugado com b.

É claro que δ é uma relação de equivalência em K e as classes de isomorfismo dos R-módulos do tipo M_a estão em correspondência biunívoca com as classes de equivalência de δ em K.

Note-se que a classe de equivalência de 0 é constituída por elementos da forma $\delta(c)c^{-1}$, onde $c \in K \setminus \{0\}$. Deste modo, existem dois R-módulos simples e fiéis não-isomorfos se K possui algum elemento que não é da forma $\delta(c)c^{-1}$.

Exemplo 2: O anel dos polinómios torcidos $K[x;\sigma]$.

Sejam K um anel de divisão e σ um endomorfismo de K, que *não* é um automorfismo de ordem interior finita. Já vimos anteriormente que $R = K[x;\sigma]$ é um anel primitivo à esquerda e que os módulos $M_a = R/R(x-a)$, com $a \neq 0$, são simples e fiéis.

Usando a decomposição $R = R(x-a) \oplus K$, vamos identificar M_a com K. Como $xc = \sigma(c)x = \sigma(c)(x-a) + \sigma(c)a$, a acção de R sobre $K \cong M_a$ é determinada por

$$x * c = \sigma(c)a.$$

Quando é que $M_a \cong M_b$ como R-módulos?

Supondo que $\varphi : M_a \to M_b$ é um R-isomorfismo e $(1 + R(x-a))\varphi = c + R(x-b)$, então

$$0 = (x - a + R(x-a))\varphi = xc - ac + R(x-b) = \sigma(c)b - ac + R(x-b).$$

Como $R(x-b) \cap K = 0, \sigma(c)b - ac = 0$, ou seja, $a = \sigma(c)bc^{-1}$.

Reciprocamente, se existir $c \neq 0$ tal que $a = \sigma(c)bc^{-1}$, definimos

$$(r + R(x-a))\varphi = rc + R(x-b)$$

e mostra-se que φ preserva as acções de R sobre M_a e M_b. Para além disso, claro que φ é um homomorfismo bijectivo (a sua inversa é a multiplicação por c^{-1}).

Dizemos que $a \neq 0$ é σ-conjugado com $b \neq 0$ se $a = \sigma(c)bc^{-1}$, para algum $c \neq 0$. Vimos, então, que $M_a \cong M_b$ se e só se a e b são σ-conjugados. Ou seja, as classes de isomorfismo dos R-módulos do tipo M_a estão em correspondência biunívoca com as classes de σ-conjugação de $K \setminus \{0\}$.

Em particular, os σ-conjugados de 1 são os elementos da forma $\sigma(c)c^{-1}$. Deste modo, $K[x;\sigma]$ tem mais do que um módulo simples e fiel se existir algum elemento de K que não é da forma $\sigma(c)c^{-1}$.

Exemplo 2.1: Um anel primitivo à esquerda com um número infinito de módulos simples e fiéis distintos.

Sejam

$$K = Frac(\mathbb{R}[t]) = \left\{ \frac{f(t)}{g(t)} : f(t), g(t) \in \mathbb{R}[t], g(t) \neq 0 \right\},$$

dito o *corpo das fracções* de $\mathbb{R}[t]$ e σ o $\mathbb{R}$-automorfismo de K que envia $t \mapsto t+1$. Como K é comutativo, um automorfismo β tem ordem interior finita se e só se $\beta^n = id$ para algum n. Como $\sigma^n(t) = t + n \neq t$, então σ não é um automorfismo de ordem interior finita.

Em K definimos

$$\deg\left(\frac{f}{g}\right) = \deg(f) - \deg(g), \qquad f, g \in \mathbb{R}[t] \setminus \{0\}.$$

Se $a(t)$ é σ-conjugada com $b(t)$, então existe $c(t) \in K$ tal que

$$a(t) = \sigma(c(t))b(t)c(t)^{-1} = \frac{c(t+1)}{c(t)}b(t),$$

logo $a(t)$ e $b(t)$ têm o mesmo grau. Logo, $R = K[x;\sigma]$ tem uma infinidade de módulos simples e fiéis não isomorfos, por exemplo,

$$M_1, M_t, M_{t^2}, \ldots.$$

Exemplo 3: O anel dos polinómios $K[x]$.

Seja K um anel de divisão, que não é algébrico sobre o seu centro $Z(K)$. Já vimos que $R = K[x]$ é um anel primitivo à esquerda e já vimos que

$$M_a = R/R(x-a)$$

são R-módulos simples e fiéis.

Quando se verifica $M_a \cong M_b$ como R-módulos?

Analogamente aos exemplos anteriores, podemos identificar $M_a \cong K$ e tendo em conta que $xc = cx = c(x-a)+ca$ temos que a acção de R sobre K é determinada por $x*c = ca$.

Se $\varphi : M_a \to M_b$ é um R-isomorfismo e $(1 + R(x-a))\varphi = c + R(x-b)$, temos que

$$0 = (x - a + R(x-a))\varphi = xc - ac + R(x-b) = cb - ac + R(x-b).$$

Como $R(x-b) \cap K = 0, cb - ac = 0$, isto é, $a = cbc^{-1}$. Reciprocamente, se existe $c \neq 0$ tal que $a = cbc^{-1}$, definimos

$$(r + R(x-a))\varphi = rc + R(x-b)$$

que é um R-homomorfismo bijectivo, logo $M_a \cong M_b$.

Portanto, as classes de isomorfismo dos módulos do tipo M_a estão em correspondência biunívoca com as classes de conjugação de K (relativamente à relação anterior). Note-se que nenhum outro elemento de K é conjugado com 1, logo $K[x]$ tem módulos simples fiéis (do tipo M_a) não isomorfos.

Vejamos na próxima secção mais exemplos de anéis primitivos, nomeadamente alguns anéis livres.

3.2 K-anéis livres

Sejam K um anel e X um conjunto não vazio. Define-se o monóide livre X^* como o conjunto de todas as palavras $x_1x_2\ldots x_n$ com letras $x_i \in X$. A palavra vazia de comprimento 0 denotamos por 1. O K-anel livre de X é o conjunto das funções $f : X^* \to K$ que dão valor 0 a quase todas as palavras, isto é

$$R = K\langle X\rangle = \{f : X^* \to K \mid \exists\, F \subseteq X^* \text{ finito tal que } f(w) = 0, \forall w \notin F\}.$$

O conjunto F na definição diz-se o *suporte* da função f. Define-se a adição de funções usando a soma em K

$$(f+g)(w) = f(w) + g(w), \qquad \forall w \in X^*,\ \forall f, g \in R$$

e a multiplicação é definida por

$$(f * g)(w) = \sum_{uv=w} f(u)g(v),$$

onde o somatório percorre todas as possibilidades de uma decomposição de w em prefixos u e sufixos v. Alternativamente se $w = x_1 \ldots x_n$ então

$$(f * g)(x_1 \ldots x_n) = f(1)g(x_1 \ldots x_n) + \sum_{i=1}^{n-1} f(x_1 \ldots x_i)g(x_{i+1} \ldots x_n) + f(x_1 \ldots x_n)g(1).$$

O anel R tem estrutura de K-módulo pela multiplicação de um escalar $r \in K$ com uma função $f \in R$ definida por

$$(r \cdot f)(w) = rf(w).$$

Para cada palavra $w \in X^*$ temos a função

$$f_w(v) = \begin{cases} 0, & \text{se } v \neq w \\ 1, & \text{se } v = w \end{cases}.$$

Logo, podemos representar $f \in R$ por $f = \lambda_1 \cdot f_{w_1} + \ldots + \lambda_n \cdot f_{w_n}$, onde $\lambda_i = f(w_i) \in K$ e $F = \{w_1, \ldots, w_n\}$ é o suporte de f. As palavras chamam-se também monómios e os elementos de R podem ser vistos como polinómios não comutativos

$$\lambda_1 w_1 + \ldots + \lambda_n w_n,$$

onde a função f_{w_i} é simplesmente representada por w_i. Note-se que segundo a multiplicação de duas funções $f_w * f_v = f_{wv}$, isto é, $w * v = wv$ é a sua concatenação.

Assim, podemos estudar

$$R = K\langle X\rangle = \{\lambda_1 w_1 + \ldots + \lambda_n w_n : \lambda_i \in K, w_i \in X^*\}$$

com a soma usual e a multiplicação determinada pela concatenação. Para além disso, a estrutura de K-módulo baseia-se no produto em K.

Observações:

1. R diz-se *livre* porque tem a propriedade universal: dado um homomorfismo de anéis $\varphi_0 : K \to K'$ e um subconjunto $\{a_i : i \in I\} \subset K'$ tal que cada a_i comuta com $\varphi_0(K)$, existe um único homomorfismo de anéis $\varphi : R \to K'$ que extende φ_0 (isto é, $\varphi|_K = \varphi_0$) e $\varphi(x_i) = a_i$.

2. Qualquer anel livre com um número numerável de letras pode ser mergulhado no anel livre com duas letras $K\langle x, y\rangle$.

$$\begin{array}{ccccc} K\langle x_0, x_1, x_2, \ldots\rangle & \cong & K\langle x, xy, xy^2, \ldots\rangle & \subset & K\langle x, y\rangle \\ x_n & \leftrightarrow & xy^n & & \end{array}$$

Vejamos exemplos de K-anéis livres que são primitivos à esquerda.

Sejam K um corpo e $V = \bigoplus_{i=1}^{\infty} e_i K$ um espaço vectorial sobre K à direita com base numerável $\{e_1, e_2, \ldots\}$. Designemos $E = \mathrm{End}(V_K)$. Definimos a aplicação K-linear determinada por

$$\begin{array}{rcll} f : V & \to & V & \\ e_1 & \mapsto & 0 & \\ e_i & \mapsto & e_{i-1} & \text{para } i > 1 \end{array}$$

e, dada uma função $r : \mathbb{N} \to \mathbb{N}$ com $\lim_{m\to\infty} r(m) = \infty$, consideremos ainda um endomorfismo $g \in E$ com a seguinte propriedade:

$$\forall m \geq 1, \;\; g^m(e_1) = e_{r(m)}, \tag{3}$$

ou seja, as sucessivas imagens de e_1 por g percorrem elementos da base tão grandes quanto se queira.

Consideremos ainda o K-subespaço gerado por f e g em E

$$R = K\langle f, g\rangle = \left\{ \sum_{i=1}^{n} \lambda_i x_{i_1} \ldots x_{i_n} : x_{i_k} \in \{f, g\}, \lambda_i \in K \right\} \subset E.$$

V é um R-módulo à esquerda com a acção $h \cdot v = h(v)$.

- ${}_R V$ é simples:

  Consideremos um R-submódulo $W \neq 0$ de V. Em particular, $f(W) = f \cdot W \subset W$ e $g(W) = g \cdot W \subset W$. Seja $w \neq 0$ um vector de W com a menor representação como combinação linear de e_i's, digamos

$$w = e_{i_1} a_1 + \ldots + e_{i_n} a_n,$$

com $i_1 < \ldots < i_n$ e cada $a_j \neq 0$. Então,

$$\begin{aligned} f^{i_1}(w) &= f^{i_1}(e_{i_1}a_1 + e_{i_2}a_2 + \ldots + e_{i_n}a_n) \\ &= \underbrace{f^{i_1}(e_{i_1})}_{0}a_1 + \underbrace{f^{i_1}(e_{i_2})}_{e_{i_2-i_1}}a_2 + \ldots + \underbrace{f^{i_1}(e_{i_n})}_{e_{i_n-i_1}}a_n \qquad \text{porque } f \text{ é } K\text{-linear} \\ &= e_{i_2-i_1}a_2 + \ldots + e_{i_n-i_1}a_n \end{aligned}$$

é um elemento de W (porque W é um R-submódulo) com uma representação de comprimento $n-1$ (menor que a de w), logo $f^{i_1}(w) = 0$ e $a_2 = \ldots = a_n = 0$, ou seja, $w = e_{i_1}a_1 \in W \Rightarrow e_{i_1} \in W$ (porque K é um corpo) e, sendo W um R-submódulo, temos que

$$f^{i_1-1}(e_{i_1}) = e_1 \in W.$$

Como $\lim_{m\to\infty} r(m) = \infty$, $\forall i \geq 1, \exists\, m \geq 1 : r(m) > i$, logo

$$f^{r(m)-i}\left(g^m(e_1)\right) = f^{r(m)-i}(e_{r(m)}) = e_i \in W,$$

porque W é um R-submódulo. Sendo que qualquer elemento da base $e_1, e_2 \ldots$ pertence a W, então $W = V$.

- ${}_RV$ é fiel: se $h \cdot v = h(v) = 0, \forall v \in V$ então $h = 0$.

Portanto, $\underline{R = K\langle f, g\rangle \text{ é um anel primitivo à esquerda.}}$

Agora escolhendo funções g (com a propriedade (3)), podemos obter vários exemplos de anéis primitivos à esquerda.

Exemplo 1: $K\langle x, y\rangle/\langle xy - 1\rangle$ é primitivo à esquerda (com K corpo).

Consideremos

$$\begin{aligned} g : V &\to V \\ e_i &\mapsto e_{i+1} \end{aligned}$$

Como $g^m(e_1) = e_{m+1}$, a função g tem a propriedade (3). Então, $K\langle f, g\rangle$ é primitivo à esquerda. Há uma relação óbvia entre f e g: $fg = id_V$. Consideremos o K-homomorfismo determinado por

$$\begin{aligned} \psi : K\langle x, y\rangle/\langle xy - 1\rangle &\to K\langle f, g\rangle \\ x &\mapsto f \\ y &\mapsto g \end{aligned} \quad .$$

ψ é claramente sobrejectiva; vejamos que é injectiva.

Em primeiro lugar, qualquer elemento de $K\langle x, y\rangle/\langle xy - 1\rangle$ pode ser escrito como combinação linear de monómios da forma

$$y^i x^j,$$

porque $xy = 1$ em $K\langle x, y\rangle/\langle xy - 1\rangle$ e se u e v são monómios então $uxyv = uv$ e assim pode-se reduzir qualquer monómio a um da forma $y^i x^j$.

Por redução ao absurdo, suponhamos que ψ tem núcleo não nulo, digamos

$$\gamma = \sum_{i,j} a_{ij} y^i x^j \in \mathrm{Ker}(\psi).$$

Seja k o menor índice tal que $a_{ik} \neq 0$ para algum i, ou seja, $\forall j < k, \forall i, a_{ij} = 0$.

Como $\psi(\gamma) = 0$ é o polinómio nulo, então

$$\begin{aligned} 0 &= \psi(\gamma)(e_{k+1}) = \sum_{i,j} a_{ij} g^i f^j(e_{k+1}) \\ &= \sum_i a_{ik} g^i(e_1) = \sum_i a_{ik} e_{i+1}, \end{aligned}$$

porque $\forall j < k, a_{ij} = 0$ e $\forall j > k, f^j(e_{k+1}) = 0$. Como $\{e_1, e_2 \ldots .\}$ é uma base de V, então

$$a_{ik} = 0, \forall i,$$

o que contraria a hipótese sobre k. Portanto, $\mathrm{Ker}(\psi) = 0$.

Deste modo, $K\langle x, y\rangle/\langle xy - 1\rangle \cong K\langle f, g\rangle$, logo

$$K\langle x, y\rangle/\langle xy - 1\rangle \text{ é primitivo à esquerda.}$$

Exemplo 2: $K\langle x, y\rangle$ é primitivo à esquerda (com K corpo).

Consideremos

$$\begin{aligned} g : V &\to V \\ e_i &\mapsto e_{i^2+1} \end{aligned}$$

Como $i < i^2 + 1$, $r(m) = m^2 + 1$ é uma sucessão estritamente crescente, logo g tem a propriedade (3). Considerando o K-homomorfismo determinado por

$$\begin{aligned} \psi : K\langle x, y\rangle &\to K\langle f, g\rangle \\ x &\mapsto f \\ y &\mapsto g \end{aligned} \quad ,$$

que é claramente sobrejectivo, vejamos que ψ também é injectivo: através de ψ, podemos estudar V como um $K\langle x, y\rangle$-módulo à esquerda com acção determinada por

$$\begin{cases} x \cdot e_i = f(e_i) = e_{i-1} \\ y \cdot e_i = g(e_i) = e_{i^2+1} \end{cases}$$

$$\mathrm{Ker}(\psi) = \{z \in K\langle x, y\rangle : \psi(z) = 0\} = \{z \in K\langle x, y\rangle : z \cdot v = 0, \forall v \in V\} = \mathrm{Ann}_{K\langle x,y\rangle}(V)$$

ou seja, mostrar que ψ é injectiva equivale a mostrar que ${}_{K\langle x,y\rangle}V$ é fiel.

Definição 3.7 *$z \in K\langle x, y\rangle$ é <u>eventualmente zero</u> em V se $\exists\, N \in \mathbb{N}$ tal que $z \cdot e_i = 0$, para $i > N$.*

O nosso objectivo é mostrar que $z = 0$ é o único elemento que é eventualmente zero, donde se conclui que ${}_{K\langle x,y\rangle}V$ é fiel. Antes disso, precisamos de algumas propriedades dos monómios de $K\langle x, y\rangle$:

seja $H \in K\langle x, y\rangle$ um monómio, cujo grau em y é m.

Afirmação 1:

$$\underline{\text{Existe um único polinómio mónico } p_H(t) \in \mathbb{Z}[t] \text{ de grau } 2^m \text{ e}}$$
$$\underline{\text{um número } i_H \geq 1 \text{ tal que } He_i = e_{p_H(i)} \text{ para todos } i > i_H.}$$

Ou seja, para índices i suficientemente grandes $He_i = e_{p_H(i)}$. Por exemplo, ao monómio $H = yx^5$ corresponde o polinómio $p_H(t) = (t-5)^2 + 1$ que é mónico e tem grau $2 = 2^1$: para $i_H = 5$ e $i > 5$,

$$He_i = (yx^5)e_i = ye_{i-5} = e_{(i-5)^2+1}.$$

Procedemos por indução no comprimento de H (visto como uma palavra em $\{x, y\}^*$).

- Se o comprimento de H é 1, então $H = x$ ou $H = y$. No primeiro caso, $p_x(t) = t-1$ é mónico e tem grau $1 = 2^0$ e para $i_x = 1$ e $i > 1$ tem-se $He_i = e_{i-1} = e_{p_x(i)}$. Se $H = y$ então $p_y(t) = t^2 + 1$ é mónico e tem grau $2 = 2^1$ e para $i_y = 1$ e $i > 1$ tem-se que $He_i = e_{i^2+1} = e_{p_y(i)}$.

- Suponhamos que a afirmação é válida para todos os monómios H de comprimento l. Seja G um monómio de comprimento $l + 1$, então $G = Hx$ ou $G = Hy$ onde H é um monómio de comprimento l (e de grau em y igual a m). Por hipótese, existe $p_H(t) \in \mathbb{Z}[t]$ mónico com grau 2^m e $i_H \geq 1$ tal que $He_i = e_{p_H(i)}$ para $i > i_H$.

  Se $G = Hx$ então $Ge_i = He_{i-1} = e_{p_H(i-1)}$ para $i > i_H + 1$. Logo, $p_G(t) = p_H(t-1) \in \mathbb{Z}[t]$ é mónico e tem grau 2^m.

  Se $G = Hy$ então $Ge_i = He_{i^2+1} = e_{p_H(i^2+1)}$ para $i > i_H$. Logo, $p_G(t) = p_H(t^2+1) \in \mathbb{Z}[t]$ é mónico e tem grau 2^{m+1}. Note-se que o grau de y em G é $m + 1$.

Quanto à unicidade do polinómio, suponhamos que existem dois polinómios $p_H(t)$ e $q_H(t)$ com a mesma propriedade, então para índices i suficientemente grandes tem-se $e_{p_H(i)} = He_i = e_{q_H(i)}$. Logo, p_H e q_H coincidem num número infinito de valores o que implica que os polinómios p_H e q_H são iguais (porque $p_H - q_H \in \mathbb{Z}[t]$ tem um número infinito de raízes, o que apenas se verifica para o polinómio nulo; qualquer outro polinómio tem apenas um número finito de raízes). Portanto, o polinómio p_H é único. □

Afirmação 2:

Se H e H' forem monómios diferentes, então os polinómios p_H e $p_{H'}$ são diferentes.

Sem perda de generalidade, podemos assumir que G e G' são monómios que não terminam na mesma letra (caso contrário, tomam-se os maiores submonómios de G e G' que não acabam na mesma letra), digamos

$$G = Hx \qquad \text{e} \qquad G' = H'y.$$

Quanto a G', $G'e_i = H'ye_i = H'e_{i^2+1} = e_{p_{H'}(i^2+1)}$, logo o polinómio que lhe corresponde é $p_{G'}(t) = p_{H'}(t^2+1)$ cujas potências de t são todas pares.

Quanto a G que termina em x, vejamos por indução (no comprimento de G) que o polinómio que lhe corresponde é da forma

$$p_G(t) = t^{(2^m)} - nt^{(2^m-1)} + \text{termos de menor grau},$$

onde m é o grau de y em G e $n > 0$.

- Se G tem comprimento 1, $G = x$ cujo polinómio é $p_G(t) = t - 1 = t^{(2^0)} - 1t^{(2^0-1)}$.
- Suponhamos que todos os monómios que terminam em x de comprimento l têm a propriedade indicada. Seja G um monómio que termina em x de comprimento $l+1$. Então, $G = xH$ ou $G = yH$, onde H é um monómio de comprimento l que termina em x. Por hipótese de indução, $p_H(t) = t^{(2^m)} - nt^{(2^m-1)} + \text{termos de menor grau}$, onde m é o grau de y em H e $n > 0$.

  Se $G = xH$, $Ge_i = xHe_i = xe_{p_H(i)} = e_{p_H(i)-1}$ logo o seu polinómio é

  $$p_G(t) = p_H(t) - 1 = t^{(2^m)} - nt^{(2^m-1)} + \text{termos de menor grau}$$

  que é da forma pretendida. Note-se que, de facto, m é o grau de y em G.

  Se $G = yH$, $Ge_i = yHe_i = ye_{p_H(i)} = e_{p_H(i)^2+1}$ logo o seu polinómio é

  $$\begin{aligned} p_G(t) &= p_H(t)^2 + 1 \\ &= \left(t^{(2^m)} - nt^{(2^m-1)} + \text{termos de menor grau}\right)^2 + 1 \\ &= \left(t^{(2^m)}\right)^2 - 2nt^{(2^m-1)}t^{(2^m)} + \text{termos de menor grau} \\ &= t^{(2^{m+1})} - 2nt^{(2^{m+1}-1)} + \text{termos de menor grau}, \end{aligned}$$

  que é da forma pretendida. Note-se que, de facto, $m+1$ é o grau de y em G.

Enquanto que todas as potências de t do polinómio de G' são pares, o polinómio de G tem pelo menos uma potência ímpar. Portanto, os polinómios p_G e $p_{G'}$ são diferentes. □

Afirmação 3: $\underline{z \text{ eventualmente zero} \Rightarrow z = 0.}$

Suponhamos que $z = \sum_{j=1}^{n} a_j H_j$ é eventualmente zero, com $a_j \in K$ e H_j monómios diferentes; então para i suficientemente grande

$$0 = ze_i = \left(\sum_{j=1}^{n} a_j H_j\right) e_i = \sum_{j=1}^{n} a_j e_{p_{H_j}(i)}.$$

Como os polinómios p_{H_j} são diferentes, para i suficientemente grande $p_{H_j}(i)$'s são diferentes, logo a igualdade anterior implica que todos os a_j's são 0. E, assim, $z = 0$. □

Portanto, $K\langle x, y\rangle \cong K\langle f, g\rangle$, logo

$$K\langle x, y\rangle \text{ é um anel primitivo à esquerda.}$$

Exemplo 3: Os K-anéis livres com um número finito e um número infinito numerável de letras

$$K\langle x_1, \ldots, x_n\rangle \text{ e } K\langle x_1, x_2, \ldots\rangle \text{ são primitivos à esquerda.}$$

Tomando novamente a função g determinada por $g(e_i) = e_{i^2+1}$ (do Exemplo 2), sejam $R_n = K\langle f, fg, \ldots, fg^n\rangle$ e $R_\infty = K\langle f, fg, fg^2, \ldots\rangle = \bigcup_{n=1}^{\infty} R_n$.

Afirmação: ${}_{R_2}V$ é simples, onde $R_2 = K\langle f, fg, fg^2\rangle$.

O argumento já foi utilizado anteriormente. Seja $0 \neq W \leq V$ um R_2-submódulo de V. Tomando $w = e_{i_1}a_1 + \ldots + e_{i_n}a_n$ um elemento não nulo de W com comprimento mínimo, temos que $f^{i_1}(w) = e_{i_2-i_1}a_2 + \ldots + e_{i_n-i_1}a_n \in W$ (porque W é R_2-submódulo e $f \in R_2 \Rightarrow f^{i_1} \in R_2$) e tem comprimento $n-1$, logo $f^{i_1}(w) = 0$, ou seja, $a_2 = \ldots = a_n = 0$ e $w = e_{i_1}a_1$, donde $e_{i_1}a_1a_1^{-1} = e_{i_1} \in W$ e, assim, $f^{i_1-1}(e_{i_1}) = e_1 \in W$.

Então, W também contém

$$\begin{aligned}
&(fg^2)(e_1) = fg(e_2) = f(e_5) = e_4\\
&(fg^2)^2(e_1) = fg^2(e_4) = fg(e_{17}) = f(e_{290}) = e_{289}\\
&\quad\vdots
\end{aligned}$$

e os restantes elementos intermédios da base (por exemplo, e_2, e_3, e_5) obtêm-se aplicando $f \in R_2$ um número finito de vezes, logo também estão em W. Contendo todos os elementos da base, temos que $W = V$. □

Como $f, fg, fg^2 \in R_n$, $n = 2, 3, \ldots, \infty$, então V é um módulo simples sobre todos estes anéis. E claro que ${}_{R_n}V$ é fiel:

$$h \cdot v = h(v) = 0, \forall v \in V \Rightarrow h = 0.$$

Portanto, todos os anéis R_n são primitivos à esquerda ($n = 2, 3, \ldots, \infty$), logo

$$K\langle x_1, \ldots, x_n\rangle \cong R_n \text{ e } K\langle x_1, x_2, \ldots\rangle \cong R_\infty \text{ também são primitivos à esquerda.}$$

Observações:

1. O argumento da demonstração anterior não pode ser aplicado a $R_1 = K\langle f, fg\rangle$, porque ${}_{R_1}V$ não é simples, uma vez que e_1K é um R_1-submódulo de V não trivial:

$$f(e_1K) = f(e_1)K = 0$$
$$fg(e_1K) = fg(e_1)K = f(e_2)K = e_1K.$$

   Contudo, não há necessidade de trabalhar com R_1, porque o anel livre com 2 variáveis já tinha sido estudado no Exemplo 2.

2. E. Formanek demonstrou que um anel livre sobre um corpo K com qualquer número de indeterminadas (inclui o caso de um número infinito *não* numerável) é também primitivo à esquerda. Essa demonstração pode ser vista em [15, Theorem 11.27].

3.3 Anéis Primitivos e Outras Classes de Anéis

Na classe dos anéis artinianos à esquerda, as noções de primitividade e simplicidade coincidem:

Proposição 3.8 *Seja R um anel artiniano à esquerda (resp. à direita). Então, R é primitivo à esquerda (resp. à direita) se e só se R é um anel simples se e só se $R \cong \mathcal{M}_n(D)$ para um anel de divisão D e $n \geq 1$.*

Demonstração. Tendo em conta as Proposições 3.3 e 1.31, a primeira equivalência é óbvia. Uma maneira alternativa de ver esta equivalência sem recorrer à noção de anel primo é a seguinte: como R é artiniano à esquerda, R tem um ideal à esquerda minimal $I \neq 0$, que pode ser visto como um R-módulo à esquerda que é simples (porque I é minimal). Como R é simples, então $\text{Ann}({}_RI) = 0$ ou $\text{Ann}({}_RI) = R$ (ou seja, $RI = 0$ donde $I = 0$, o que é absurdo). Portanto, I é um R-módulo à esquerda simples e fiel, logo R é primitivo à esquerda.

A segunda equivalência resulta do Teorema 1.22. □

Na categoria dos anéis comutativos, os anéis primitivos (tal como os anéis simples) são os corpos:

Proposição 3.9 *Um anel comutativo R é primitivo (à esquerda) se e só se é um corpo.*

Demonstração. Pela Proposição 3.4, um anel R é primitivo se e só se contém um ideal à esquerda maximal I que só contém 0 como ideal bilateral. Se R for comutativo, I é um ideal bilateral, logo $I = 0$. Sendo $I = 0$ maximal, temos que R é um corpo. □

3.4 Ideais Primitivos

A noção de primitividade também pode ser definida para ideais bilaterais da seguinte forma:

Definição 3.10 *Um ideal bilateral $I \subset R$ diz-se primitivo à esquerda (resp. à direita) se o anel quociente R/I é primitivo à esquerda (resp. à direita).*

A seguinte proposição dá-nos uma caracterização dos ideais primitivos à esquerda, que em muitas fontes bibliográficas é usada como a definição de ideal primitivo [10].

Proposição 3.11 (Caracterização dos ideias primitivos à esquerda) *Um ideal I de R é primitivo à esquerda se e só se I é o anulador de um R-módulo à esquerda simples.*

Demonstração. Suponhamos que $I = \mathrm{Ann}(M)$, onde M é um R-módulo à esquerda simples. Já foi visto no Capítulo 1 que M pode ser visto como um R/I-módulo fiel, com a acção

$$(a + I) \cdot m = a \cdot m.$$

Para além disso, como a acção é a mesma, claro que M é um R/I-módulo simples. Logo, R/I é um anel primitivo à esquerda, ou seja, I é um ideal primitivo à esquerda.

Reciprocamente, suponhamos que R/I é um anel primitivo à esquerda e seja M um R/I-módulo simples e fiel. Então, vendo M como um R-módulo (com acção $a \cdot m = (a + I) \cdot m$), ${}_RM$ permanece simples e o seu anulador em R é I:

$$b \cdot M = 0 \Leftrightarrow (b + I) \cdot M = 0 \Leftrightarrow b + I = 0 + I \Leftrightarrow b \in I.$$

□

Decorre imediatamente desta Proposição que

$$\mathrm{Jac}(R) = \bigcap_{R\text{-módulo à esquerda } M \text{ simples}} \mathrm{Ann}(M) = \bigcap_{I \text{ ideal primitivo à esquerda de } R} I.$$

Vejamos ainda um resultado que envolve ideais primitivos (Teorema 3.13).

Para isso, precisamos previamente da definição de produto subdirecto. Dada uma colecção de anéis $\{R_i\}_{i\in I}$, consideremos o seu produto cartesiano $\prod_{i\in I} R_i$. Para cada $j \in I$, define-se uma aplicação projecção

$$\begin{array}{rcl} \pi_j : \prod_{i\in I} R_i & \to & R_j \\ (x_i)_{i\in I} & \mapsto & x_j \end{array}$$

que é um homomorfismo de anéis. Um produto subdirecto de $\prod_{i\in I} R_i$ é [um anel isomorfo a] um subanel $A \subset \prod_{i\in I} R_i$ tal que

$$\pi_j(A) = R_j, \quad \forall j \in I.$$

Proposição 3.12 *As afirmações são equivalentes:*

(a) *A é um produto subdirecto de $\prod_{i\in I} R_i$*

(b) *A tem uma colecção de ideais $\{J_i\}_{i\in I}$ tais que $\bigcap_{i\in I} J_i = 0$ e $A/J_i \cong R_i$.*

Demonstração.
$(a) \Rightarrow (b)$ Para cada $i \in I$, definimos $J_i = \mathrm{Ker}(\pi_i|_A)$, que é um ideal de A. Então,

$$a = (a_i)_{i\in I} \in \bigcap_{i\in I} J_i \Leftrightarrow \pi_i(a) = a_i = 0, \forall i \in I \Leftrightarrow a = (0)_{i\in I}$$

e, como A é um produto subdirecto de $\prod_{i\in I} R_i$, aplicando o Teorema do Isomorfismo a $\pi_i|_A$, temos que

$$A/J_i = A/\mathrm{Ker}(\pi_i|_A) \cong \pi_i(A) = R_i.$$

$(b) \Rightarrow (a)$ Seja $R_i = A/J_i$ e consideremos $\prod_{i\in I} R_i$. Identificando

$$a \in A \mapsto (a + J_i)_{i\in I},$$

claro que é um homomorfismo sobrejectivo e, para além disso, é injectivo: se $(a+J_i)_{i\in I} = (b + J_i)_{i\in I}$ então

$$a - b \in J_i, \forall i \in I \Leftrightarrow a - b \in \bigcap_{i\in I} J_i = 0 \Leftrightarrow a = b.$$

Logo, A é isomorfo a um subanel de $\prod_{i\in I} R_i$ tal que $\pi_i(A) = A/J_i, \forall j \in I$. □

Teorema 3.13 *Um anel semiprimitivo é produto subdirecto de anéis primitivos à esquerda (e também à direita).*

Demonstração. Sejam R um anel semiprimitivo e $\{M_i\}_{i\in I}$ uma família de representantes das classes de equivalência de R-módulos simples à esquerda. Definimos ainda $J_i = \mathrm{Ann}(M_i)$, que pela Proposição 3.11 é um ideal primitivo à esquerda.

Como R é semiprimitivo,

$$\bigcap_{i\in I} J_i = \mathrm{Jac}(R) = 0$$

e pela Proposição anterior R é produto subdirecto de

$$\prod_{i\in I} R/J_i$$

e cada R/J_i é um anel primitivo (porque J_i é um ideal primitivo). □

O próximo Capítulo é dedicado ao estudo do Teorema da Densidade, o resultado mais importante desta tese, e dos seus vários corolários.

4 Teorema da Densidade

Sejam R um anel, M um R-módulo à esquerda e $K = \mathrm{End}({}_RM)$ o anel dos R-endomorfismos de M. Então, M é um K-módulo à direita com acção $m \cdot f = (m)f$ e a aplicação

$$\begin{array}{rcl} \varphi : R & \to & \mathrm{End}(M_K) \\ a & \mapsto & \varphi_a : M \to M \\ & & m \mapsto am \end{array}$$

é um homomorfismo de anéis. O seu núcleo é

$$\begin{array}{rcl} \mathrm{Ker}(\varphi) & = & \{a \in R : \varphi_a \equiv 0\} = \{a \in R : \varphi_a(m) = 0, \forall m \in M\} \\ & = & \{a \in R : am = 0, \forall m \in M\} = \mathrm{Ann}({}_RM), \end{array}$$

ou seja, se M é um R-módulo fiel, φ é injectiva, logo R é (isomorfo a) um subanel de $\mathrm{End}(M_K)$, que é $\varphi(R)$ a imagem de φ.

Quão grande é a imagem deste homomorfismo?

O Teorema da Densidade diz que se M é semisimples, a imagem é muito grande, no sentido de que:

$$\forall f \in \mathrm{End}(M_K), \ \ \forall x_1, \ldots, x_n \in M, \ \ \exists\, a \in R : \ \ f(x_i) = ax_i$$

isto é, f actua como φ_a nos elementos $x_1, \ldots, x_n$. Neste caso, diz-se que R age densamente sobre M_K. Esta noção de densidade será estabelecida e a sua relação com a Topologia será aprofundada e esclarecida.

Para além disso, iremos ver que o Teorema da Densidade nos irá proporcionar um resultado que caracteriza completamente os anéis primitivos: Teorema da Estrutura dos Anéis Primitivos, que afirma que os anéis primitivos (à esquerda) são subanéis densos de $\mathrm{End}({}_KV)$, onde V é um espaço vectorial (à esquerda) sobre um anel de divisão K.

Para concluir, vamos estudar uma consequência do Teorema da Densidade nas Acções de Grupos sobre Anéis.

Comecemos por trabalhar nos pormenores que não foram especificados na Introdução: sejam R um anel, M um R-módulo à esquerda e $K = \mathrm{End}({}_RM)$.

M é um K-módulo à direita com acção $m \cdot f = (m)f$: $\forall m, n \in M, \forall f, g \in K$.

1. $m \cdot (f \circ g) = (m)(f \circ g) = ((m)f)g = (m \cdot f) \cdot g$.
2. $(m + n) \cdot f = (m + n)f = (m)f + (n)f = m \cdot f + n \cdot f$.
3. $m \cdot (f + g) = (m)(f + g) = (m)f + (m)g = m \cdot f + m \cdot g$.
4. $m \cdot 1_K = (m)id_M = m$.

Definição 4.1 *Sejam R, S dois anéis. M diz-se um (R, S)-bimódulo se é um R-módulo à esquerda (com acção $\cdot$), um S-módulo à direita (com acção $*$) e as duas acções são compatíveis, isto é, $\forall m \in M, r \in R, s \in S$,*

$$(r \cdot m) * s = r \cdot (m * s).$$

O R-módulo à esquerda M é um (R, K)-bimódulo: $\forall a \in R, m \in M, f \in K$ temos

$$(am) \cdot f = (am)f \underbrace{=}_{\text{porque } f \text{ é } R\text{-linear}} a((m)f) = a(m \cdot f).$$

Designamos $\mathrm{End}(M_K) = E$. Os elementos de E comutam com os elementos de K: dados $\varphi \in E$ e $f \in K$

$$\varphi((m)f) = \varphi(m \cdot f) \underbrace{=}_{\text{porque } \varphi \text{ é } K\text{-linear}} \varphi(m) \cdot f = (\varphi(m))f, \qquad \forall m \in M.$$

Definimos a aplicação

$$\begin{array}{rcl} \varphi : R & \to & \mathrm{End}(M_K) \\ a & \mapsto & \varphi_a : M \to M \\ & & \quad m \mapsto am \end{array} .$$

Note-se que esta é a mesma aplicação φ indicada na Proposição 1.5, que de facto tem imagem em $E = \mathrm{End}(M_K)$: φ_a é claramente uma aplicação aditiva e é K-linear, porque

$$\varphi_a(m \cdot f) = a((m)f) \underbrace{=}_{\text{porque } f \text{ é } R\text{-linear}} (am)f = \varphi_a(m) \cdot f.$$

Para além disso, como foi demonstrado na Proposição 1.5 a aplicação φ é um homomorfismo dos anéis R e E.

Vamos agora introduzir a noção de densidade, que é necessária para a apresentação do Teorema da Densidade.

Definição 4.2 *Sejam R e K dois anéis e M um (R,K)-bimódulo. Então, dizemos que R age densamente em M_K se*

$$\forall f \in \mathrm{End}(M_K),\ \forall v_1,\ldots,v_n \in M,\ \exists r \in R : \begin{cases} f(v_1) = rv_1 \\ \quad \vdots \\ f(v_n) = rv_n \end{cases}.$$

Mostra-se (e iremos fazê-lo na subsecção seguinte) que R age densamente sobre M_K se e só se $\varphi(R)$ é um subanel denso de E segundo uma dada topologia $\mathcal{T}$ de E. Daí o uso do termo "densidade".

Para demonstrar o Teorema da Densidade, necessitamos previamente do seguinte Lema: como a aplicação $\varphi : R \to E$ (indicada na página anterior) é um homomorfismo de anéis, qualquer E-submódulo de M é também um R-submódulo (através de φ); o seguinte Lema diz-nos que se M for semisimples então o recíproco também é válido.

Lema 4.3 *Sejam R um anel, M um R-módulo à esquerda, $K = \mathrm{End}({}_RM)$ [que age sobre M à direita: $m \cdot f = (m)f$] e $E = \mathrm{End}(M_K)$ [que age sobre M à esquerda: $\varphi \cdot m = \varphi(m)$]. Se M for um R-módulo semisimples, então qualquer R-submódulo de M é também um E-submódulo.*

Demonstração. Seja W um R-submódulo de M. Como M é semisimples, existe um R-submódulo W' de M tal que $M = W \oplus W'$. Seja

$$\begin{array}{rcll} e : M = W \oplus W' & \to & W & \text{a projecção de } M \text{ em } W. \\ m = w + w' & \mapsto & w & \end{array}$$

Em primeiro lugar, e está bem definida: se $m = w + w' = z + z'$ (com $w, z \in W$ e $w', z' \in W'$), então $w - z = z' - w' \in W \cap W' = 0$, ou seja, $w = z$ e $w' = z'$.

Vejamos que $e \in K$:

1. $(m+n)e = (w + w' + z + z')e = ((w+z) + (w'+z'))e = w + z = (m)e + (n)e$.
2. $(rm)e = (r(w+w'))e = (rw + rw')e = rw = r(m)e$.

Então, $\forall f \in E, \forall w \in W$ temos que

$$f \cdot w = f(w) \underbrace{=}_{(W)e = W} f((w)e) \underbrace{=}_{f \text{ é } K\text{-linear}} (f(w))e \underbrace{\in}_{\text{por definição de } e} W.$$

Portanto, W é um E-submódulo. □

Estamos, então, preparados para apresentar e demonstrar o Teorema da Densidade de Jacobson. Nathan Jacobson demonstrou este teorema pela primeira vez no seu artigo "*Structure theory of simple rings without finiteness assumptions*" [11].

Teorema 4.4 (Teorema da Densidade de Jacobson) *Sejam R um anel, M um R-módulo à esquerda semisimples e $K = \mathrm{End}({}_RM)$.*

Então, R age densamente em M_K.

Demonstração. Designamos $E = \mathrm{End}(M_K)$ e sejam $f \in E$ e $v_1, \ldots, v_n \in M$. Queremos ver que existe $r \in R$ tal que $f(v_i) = rv_i, \forall i$. A ideia da prova (segundo N. Bourbaki) é aplicar o Lema anterior ao R-módulo $\tilde{M} = M^n$.

Em primeiro lugar, $\tilde{M}$ é semisimples, porque é soma directa de cópias de M (cada um dos quais é soma directa de R-módulos simples), logo é soma directa de módulos simples e, assim sendo, é semisimples.

Definimos

$$\tilde{K} = \mathrm{End}({}_R\tilde{M}) = \mathrm{End}({}_RM^n) \cong \mathcal{M}_n(\mathrm{End}({}_RM)) = \mathcal{M}_n(K)$$

e $\tilde{E} = \mathrm{End}(\tilde{M}_{\tilde{K}})$ e

$$\begin{array}{rcl} \tilde{f} : \tilde{M} & \to & \tilde{M} \\ (a_1, \ldots, a_n) & \mapsto & (f(a_1), \ldots, f(a_n)). \end{array}$$

Vejamos que $\tilde{f} \in \tilde{E} = \mathrm{End}(\tilde{M}_{\tilde{K}})$:

1. $\tilde{f}$ é aditiva:

$$\begin{aligned} &\tilde{f}\left((a_1, \ldots, a_n) + (b_1, \ldots, b_n)\right) = \tilde{f}(a_1 + b_1, \ldots, a_n + b_n) \\ &= (f(a_1 + b_1), \ldots, f(a_n + b_n)) = (f(a_1) + f(b_1), \ldots, f(a_n) + f(b_n)) \\ &= (f(a_1), \ldots, f(a_n)) + (f(b_1), \ldots, f(b_n)) = \tilde{f}(a_1, \ldots, a_n) + \tilde{f}(b_1, \ldots, b_n) \end{aligned}$$

2. $\tilde{f}$ é $\tilde{K}$-linear: seja $\tilde{e} \in \tilde{K} \cong \mathcal{M}_n(K)$, digamos $\tilde{e} = (e_{ij})_{i,j=1,\ldots,n}$ com $e_{ij} \in K = \mathrm{End}({}_RM)$. Então, $\forall (a_1, \ldots, a_n) \in \tilde{M}$,

$$\begin{aligned} &\tilde{f}\left[(a_1, \ldots, a_n)\tilde{e}\right] = \tilde{f}\left(\sum_{i=1}^n (a_i)e_{i1}, \ldots, \sum_{i=1}^n (a_i)e_{in}\right) \text{ porque } \tilde{e} = (e_{ij}) \\ &= \left(f\left(\sum_{i=1}^n (a_i)e_{i1}\right), \ldots, f\left(\sum_{i=1}^n (a_i)e_{in}\right)\right) \qquad \text{por definição de } \tilde{f} \\ &= \left(\sum_{i=1}^n \left[f(a_i)\right] e_{i1}, \ldots, \sum_{i=1}^n \left[f(a_i)\right] e_{in}\right) \qquad \text{porque } f \in \mathrm{End}(M_K) \\ &= (f(a_1), \ldots, f(a_n))\, \tilde{e} = \left[\tilde{f}(a_1, \ldots, a_n)\right] \tilde{e}. \end{aligned}$$

Por fim, definimos o R-submódulo de $\tilde{M}$

$$\tilde{W} = R(v_1, \ldots, v_n).$$

Pelo Lema 4.3, $\tilde{W}$ é também um $\tilde{E}$-submódulo de $\tilde{M}$. Em particular,

$$(f(v_1), \ldots, f(v_n)) = \underbrace{\tilde{f}}_{\in \tilde{E}} \cdot \underbrace{(v_1, \ldots, v_n)}_{\in \tilde{W}} \in \tilde{W} = R(v_1, \ldots, v_n),$$

logo existe um $r \in R$ tal que $(f(v_1), \ldots, f(v_n)) = r(v_1, \ldots, v_n)$, ou seja,

$$f(v_i) = rv_i, \qquad i = 1, 2, \ldots, n.$$

□

Observação 1: A hipótese "M é semisimples" é essencial.

Por exemplo, $\mathbb{Q}$ é um $\mathbb{Z}$-módulo com o produto usual como acção e não é semisimples, porque tem $\mathbb{Z}$ como submódulo mas não há decomposição $\mathbb{Q} = \mathbb{Z} \oplus M$: para qualquer elemento $0 \neq q = \frac{a}{b} \in M \subset \mathbb{Q}$ o elemento $0 \neq bq = a \in \mathbb{Z} \cap M$, isto é $\mathbb{Z} \cap M \neq 0$.

À semelhança do que tem sido feito, definimos $K = \mathrm{End}({}_{\mathbb{Z}}\mathbb{Q})$ e $E = \mathrm{End}(\mathbb{Q}_K)$. Note-se que qualquer $f \in K$ verifica

$$(2a)f = 2(a)f, \forall a \in \mathbb{Q} \Leftrightarrow (b)f = 2\left(\frac{b}{2}\right)f, \forall b \in \mathbb{Q} \Leftrightarrow \frac{1}{2}(b)f = \left(\frac{b}{2}\right)f, \forall b \in \mathbb{Q}$$

ou seja, a aplicação $\varphi = \frac{1}{2}id_{\mathbb{Q}}$ é K-linear:

$$\varphi((a)f) = \frac{1}{2}(a)f = \left(\frac{a}{2}\right)f = (\varphi(a))f, \qquad \forall a \in \mathbb{Q}.$$

Contudo,

$$\varphi(1) = \frac{1}{2} \qquad \text{e} \qquad \nexists\, n \in \mathbb{Z} : n \cdot 1 = \frac{1}{2}.$$

Ou seja, o Teorema da Densidade aqui não vale.

Observação 2: No caso importante em que M é um R-módulo *simples*, $K = \mathrm{End}({}_R M)$ é um anel de divisão pelo Lema de Schur, logo M é um espaço vectorial sobre K à direita. Isto sugere que a Álgebra Linear deverá ter aqui um papel importante.

Vejamos o seguinte Corolário imediato do Teorema da Densidade:

Corolário 4.5 *Nas hipóteses do Teorema da Densidade, se M_K for finitamente gerado como K-módulo (à direita), então a aplicação*

$$\begin{array}{rcl} \varphi : R & \to & E = \mathrm{End}(M_K) \\ r & \mapsto & \varphi_r : M \to M \\ & & \qquad m \mapsto rm \end{array}$$

é sobrejectiva.

Demonstração. Sejam $\{v_1, \ldots, v_n\}$ um conjunto de geradores de M enquanto K-módulo, isto é, $\forall m \in M, \exists\, g_i \in K : m = (v_1)g_1 + \ldots + (v_n)g_n$. Seja $f \in E$ qualquer. Pelo Teorema da Densidade, existe $r \in R$ tal que $f(v_1) = rv_1, \ldots, f(v_n) = rv_n$. Dado $m \in M$, escrevemos $m = \sum(v_i)g_i$ com $g_i \in K$; então,

$$\begin{aligned} f(m) &= f\left(\sum_{i=1}^{n}(v_i)g_i\right) = \sum_{i=1}^{n}[f(v_i)]g_i \quad \text{porque } f \in \mathrm{End}(M_K) \\ &= \sum_{i=1}^{n}(rv_i)g_i = \sum_{i=1}^{n} r(v_i)g_i \qquad \text{porque } g_i \text{ são } R\text{-lineares} \\ &= r\left(\sum_{i=1}^{n}(v_i)g_i\right) = rm = \varphi_r(m) \end{aligned}$$

ou seja, $f = \varphi(r)$. Portanto, φ é sobrejectiva. □

Antes de explorarmos mais consequências do Teorema da Densidade, nomeadamente a sua relação com os anéis primitivos, vamos justificar o uso do termo "densidade" na subsecção seguinte.

4.1 A Topologia Finita

Sejam R um anel, M um R-módulo à esquerda, $K = \mathrm{End}(_RM)$ e $E = \mathrm{End}(M_K)$. Consideremos ainda a função $\varphi : R \to E$ já referida anteriormente. O nosso objectivo é mostrar que R age densamente em M_K se e só se $\varphi(R)$ é um subanel denso de E, segundo uma dada topologia $\mathcal{T}$ de E.

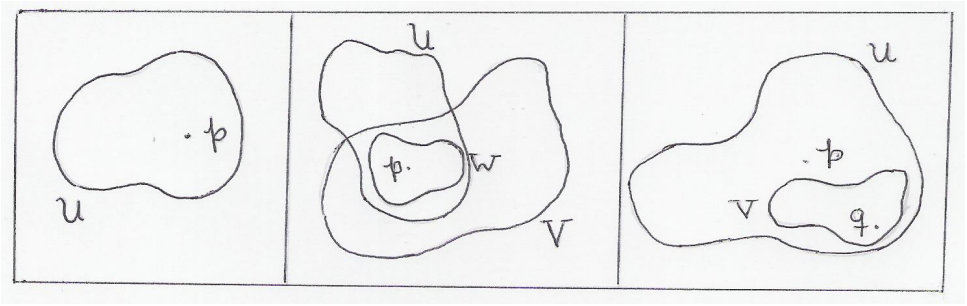
O primeiro passo é claramente introduzir e explorar essa topologia $\mathcal{T}$ de E. Para isso vamos ver um processo geral que permite transformar um conjunto T num espaço topológico.

Seja T um conjunto não vazio. Suponhamos que para cada ponto $p \in T$, existe uma família não vazia $\mathcal{F}(p)$ de subconjuntos de T com as seguintes propriedades:

(U1) $\forall U \in \mathcal{F}(p), p \in U$.

(U2) $\forall U, V \in \mathcal{F}(p), \exists\, W \in \mathcal{F}(p) : W \subseteq U \cap V$.

(U3) $\forall U \in \mathcal{F}(p), \forall q \in U, \exists\, V \in \mathcal{F}(q) : V \subseteq U$.



Os elementos de $\mathcal{F}(p)$ dizem-se vizinhanças de p. Um subconjunto $\mathcal{O} \subset T$ diz-se aberto se $\mathcal{O} = \varnothing$ ou

$$\forall p \in \mathcal{O}, \quad \exists\, U \in \mathcal{F}(p) : \quad U \subset \mathcal{O}.$$

E um subconjunto $S \subset T$ diz-se fechado se o seu complementar $T \backslash S$ for aberto.

Com esta definição de aberto, T tem estrutura de espaço topológico:

1. $\varnothing$ e T são abertos: o primeiro é aberto por definição e o segundo porque para cada ponto $p \in T$, $\mathcal{F}(p)$ é não vazio, logo existe $U \in \mathcal{F}(p)$ e $U \subset T$.

2. $\bigcup T_i$ é aberto, se os conjuntos T_i forem abertos: podemos assumir que nem todos os T_i's são vazios (caso contrário, $\bigcup T_i = \varnothing$ que é aberto); então, como T_i é aberto

$$\forall p \in \bigcup T_i \Rightarrow \exists\, i : p \in T_i \Rightarrow \exists\, U \in \mathcal{F}(p) : U \subset T_i \subset \bigcup T_i,$$

logo $\bigcup T_i$ é aberto.

3. $\bigcap_{i=1}^{n} T_i$ é aberto, se $T_1, \ldots, T_n$ são abertos: se $\bigcap_{i=1}^{n} T_i = \varnothing$, então é um aberto; supondo que $\bigcap_{i=1}^{n} T_i \neq \varnothing$, então como cada T_i é um aberto

$$p \in \bigcap_{i=1}^{n} T_i \Rightarrow p \in T_i, \forall i = 1, \ldots, n \Rightarrow \forall i, \exists\, U_i \in \mathcal{F}(p) : U_i \subset T_i.$$

Usando a propriedade **(U2)** n vezes,

$$\exists\, W \in \mathcal{F}(p) : W \subset \bigcap_{i=1}^{n} U_i \subset \bigcap_{i=1}^{n} T_i.$$

Portanto, $\bigcap_{i=1}^{n} T_i$ é um aberto.

Portanto, esta construção permite de facto munir o conjunto T de uma estrutura de espaço topológico. Note-se que o contrário também é válido, ou seja, se T é um espaço topológico com topologia $\mathcal{T}$, então definindo $\mathcal{F}(p) = \{\mathcal{O} \in \mathcal{T} : p \in \mathcal{O}\}$ satisfaz **(U1)-(U3)**.

Voltando ao nosso conjunto $E = \mathrm{End}(M_K)$, vamos muni-lo de uma estrutura de espaço topológico. Para isso começamos (como anteriormente) com a definição das vizinhanças: uma vizinhança de uma aplicação $f \in E$ é um conjunto da forma

$$U(f; x_1, \ldots, x_n) = \{g \in E : g(x_1) = f(x_1), \ldots, g(x_n) = f(x_n)\},$$

com quaisquer $x_1, \ldots, x_n \in M$. Uma vizinhança de f é o conjunto das aplicações de E que coincidem com f num número finito de pontos $x_1, \ldots, x_n$. Assim sendo, a família de vizinhanças de f é

$$\mathcal{F}(f) = \{U(f; x_1, \ldots, x_n) : x_1, \ldots, x_n \in M, n \geq 1\}$$

e não é vazia, porque por exemplo $U(f; 0) \in \mathcal{F}(f)$.

Vejamos que esta definição de vizinhança em E satisfaz as propriedades:

(U1) Claro que $f \in U(f; x_1, \ldots, x_n)$, para quaisquer $x_1, \ldots, x_n \in M$.

(U2) Sejam $U(f; x_1, \ldots, x_n)$ e $U(f; y_1, \ldots, y_m)$ duas vizinhanças de f.

Se $g \in U(f; x_1, \ldots, x_n, y_1, \ldots, y_m)$ então

$$\begin{cases} g(x_i) = f(x_i), & i = 1, \ldots, n \\ g(y_i) = f(y_i), & i = 1, \ldots, m \end{cases}$$

ou seja, $g \in U(f; x_1, \ldots, x_n) \cap U(f; y_1, \ldots, y_m)$. Isto é,

$$U(f; x_1, \ldots, x_n, y_1, \ldots, y_m) \subset U(f; x_1, \ldots, x_n) \cap U(f; y_1, \ldots, y_m).$$

(U3) Consideremos $g \in U(f; x_1, \ldots, x_n)$, isto é, $g(x_i) = f(x_i), i = 1, \ldots, n$.

Se $h \in U(g; x_1, \ldots, x_n)$, então $h(x_i) = g(x_i) = f(x_i), i = 1, \ldots, n$, ou seja, $h \in U(f; x_1, \ldots, x_n)$. Deste modo,

$$U(g; x_1, \ldots, x_n) \subset U(f; x_1, \ldots, x_n).$$

Portanto, $E = \mathrm{End}(M_K)$ é um espaço topológico, com a seguinte definição de aberto: $\mathcal{O} \subseteq E$ é aberto se $\mathcal{O} = \varnothing$ ou

$$\forall f \in \mathcal{O}, \quad \exists\, x_1, \ldots, x_n \in M : \quad U(f; x_1, \ldots, x_n) \subset \mathcal{O}.$$

Esta topologia designa-se por Topologia Finita.

E tem agora estrutura de anel e de espaço topológico e estas duas estruturas interagem bem, isto é, E é um anel topológico:

Definição 4.6 *R diz-se um anel topológico se R é um anel e um espaço topológico e as duas funções*

$$\begin{array}{rcl} \phi : R \times R & \to & R \\ (x, y) & \mapsto & x - y \end{array} \qquad e \qquad \begin{array}{rcl} \psi : R \times R & \to & R \\ (x, y) & \mapsto & xy \end{array}$$

são contínuas, isto é, a imagem recíproca de qualquer aberto é um aberto.

Lema 4.7 *Dados dois espaços topológicos T_1 e T_2, cuja topologia está definida por um sistema de vizinhanças, uma aplicação $f : T_1 \to T_2$ é contínua se e só se a imagem recíproca de qualquer vizinhança é um aberto.*

Demonstração. Seja $\mathcal{O} \subset T_2$ um aberto. Se $f^{-1}(\mathcal{O}) = \varnothing$, então $f^{-1}(\mathcal{O})$ é aberto. Se $f^{-1}(\mathcal{O}) \neq \varnothing$, dado $q \in f^{-1}(\mathcal{O})$ temos $f(q) \in \mathcal{O}$ que é aberto, logo existe uma vizinhança $U_{f(q)} \subset \mathcal{O}$ que contém $f(q)$. Por hipótese, $f^{-1}(U_{f(q)})$ é um aberto e contém q, logo existe uma vizinhança

$$U_q \subset f^{-1}(U_{f(q)}) \subset f^{-1}(\mathcal{O}).$$

Portanto, $f^{-1}(\mathcal{O})$ é um aberto. □

Vejamos que para $E = \mathrm{End}(M_K)$ as funções são contínuas

$$\begin{array}{rcl} \phi : E \times E & \to & E \\ (f, g) & \mapsto & f - g \end{array} \qquad \mathrm{e} \qquad \begin{array}{rcl} \psi : E \times E & \to & E \\ (f, g) & \mapsto & f \circ g \end{array}$$

Continuidade de $\phi(f,g) = f - g$:

Pelo Lema 4.7, basta ver que a imagem recíproca de qualquer vizinhança é um aberto: consideremos uma vizinhança $U(p; x_1, \ldots, x_n)$ e um elemento da sua imagem recíproca $(f,g) \in \phi^{-1}(U(p; x_1, \ldots, x_n))$.

1. $\phi^{-1}(U(f-g; x_1, \ldots, x_n)) \subset \phi^{-1}(U(p; x_1, \ldots, x_n))$

$$\begin{aligned} & (f,g) \in \phi^{-1}(U(p; x_1, \ldots, x_n)) \\ \Rightarrow\ & \phi(f,g) = f - g \in U(p; x_1, \ldots, x_n) \\ \Rightarrow\ & U(f-g; x_1, \ldots, x_n) \subset U(p; x_1, \ldots, x_n) \qquad \text{pela propriedade } \mathbf{(U3)} \\ \Rightarrow\ & \phi^{-1}(U(f-g; x_1, \ldots, x_n)) \subset \phi^{-1}(U(p; x_1, \ldots, x_n)) \end{aligned}$$

2. $U(f; x_1, \ldots, x_n) \times U(g; x_1, \ldots, x_n) \subset \phi^{-1}(U(f-g; x_1, \ldots, x_n))$

$$\begin{aligned} & (h,k) \in U(f; x_1, \ldots, x_n) \times U(g; x_1, \ldots, x_n) \\ \Rightarrow\ & \begin{cases} h(x_i) = f(x_i), & i = 1, \ldots, n \\ k(x_i) = g(x_i), & i = 1, \ldots, n \end{cases} \\ \Rightarrow\ & (h-k)(x_i) = (f-g)(x_i), \quad i = 1, \ldots, n \\ \Rightarrow\ & \phi(h,k) = h - k \in U(f-g; x_1, \ldots, x_n) \\ \Rightarrow\ & (h,k) \in \phi^{-1}(U(f-g; x_1, \ldots, x_n)) \end{aligned}$$

Então, (f,g) tem uma vizinhança $U(f; x_1, \ldots, x_n) \times U(g; x_1, \ldots, x_n)$ (na topologia produto de $E \times E$) que por 1. e 2. está contida em $\phi^{-1}(U(p; x_1, \ldots, x_n))$. Portanto, $\phi^{-1}(U(p; x_1, \ldots, x_n))$ é um aberto. Isto termina a demonstração de que $\phi(f,g) = f - g$ é contínua.

Continuidade de $\psi(f,g) = f \circ g$: (a demonstração é análoga)

Pelo Lema 4.7, basta ver que a imagem recíproca de qualquer vizinhança é um aberto: consideremos uma vizinhança $U(p; x_1, \ldots, x_n)$ e um elemento da sua imagem recíproca $(f,g) \in \psi^{-1}(U(p; x_1, \ldots, x_n))$.

1. $\psi^{-1}(U(f \circ g; x_1, \ldots, x_n)) \subset \psi^{-1}(U(p; x_1, \ldots, x_n))$

$$\begin{aligned} & (f,g) \in \psi^{-1}(U(p; x_1, \ldots, x_n)) \\ \Rightarrow\ & \psi(f,g) = f \circ g \in U(p; x_1, \ldots, x_n) \\ \Rightarrow\ & U(f \circ g; x_1, \ldots, x_n) \subset U(p; x_1, \ldots, x_n) \qquad \text{pela propriedade } \mathbf{(U3)} \\ \Rightarrow\ & \psi^{-1}(U(f \circ g; x_1, \ldots, x_n)) \subset \psi^{-1}(U(p; x_1, \ldots, x_n)) \end{aligned}$$

2. $U(f; g(x_1), \ldots, g(x_n)) \times U(g; x_1, \ldots, x_n) \subset \psi^{-1}\left(U(f \circ g; x_1, \ldots, x_n)\right)$

$$\begin{aligned}
& (h,k) \in U(f; g(x_1), \ldots, g(x_n)) \times U(g; x_1, \ldots, x_n) \\
\Rightarrow\ & \begin{cases} h(g(x_i)) = f(g(x_i)), & i = 1, \ldots, n \\ k(x_i) = g(x_i), & i = 1, \ldots, n \end{cases} \\
\Rightarrow\ & (h \circ k)(x_i) = h(k(x_i)) = h(g(x_i)) = f(g(x_i)) = (f \circ g)(x_i), \quad i = 1, \ldots, n \\
\Rightarrow\ & \psi(h,k) = h \circ k \in U(f \circ g; x_1, \ldots, x_n) \\
\Rightarrow\ & (h,k) \in \psi^{-1}(U(f \circ g; x_1, \ldots, x_n))
\end{aligned}$$

Então, (f, g) tem uma vizinhança $U(f; g(x_1), \ldots, g(x_n)) \times U(g; x_1, \ldots, x_n)$ (na topologia produto de $E \times E$) que por 1. e 2. está contida em $\psi^{-1}\left(U(p; x_1, \ldots, x_n)\right)$. Portanto, $\psi^{-1}\left(U(p; x_1, \ldots, x_n)\right)$ é um aberto. Isto termina a demonstração de que $\psi(f, g) = f \circ g$ é contínua.

PORTANTO, $\mathrm{End}(M_K)$ É UM ANEL TOPOLÓGICO.

Definição 4.8 *Sejam T um espaço topológico e $A \subset T$ um subconjunto.*

1. *$t \in T$ diz-se aderente a A se qualquer vizinhança de t intersecta A.*
2. *O conjunto dos pontos aderentes a A diz-se o fecho de A e escreve-se $\bar{A}$.*
3. *A diz-se denso se $\bar{A} = T$, ou seja, qualquer vizinhança de qualquer ponto de T intersecta A.*

Finalmente estabelecemos na seguinte Proposição a ponte entre a noção de densidade introduzida nos anéis e a noção topológica que acabamos de referir. Incluímos ainda uma 3ª propriedade (equivalente às duas noções), que nos irá ser útil nas próximas secções.

Proposição 4.9 *Sejam R um anel, M um R-módulo à esquerda, $K = \mathrm{End}({}_RM)$ e $E = \mathrm{End}(M_K)$. Consideremos ainda a aplicação natural $\varphi : R \to E$. São equivalentes as afirmações seguintes:*

1. *R age densamente em M_K:*

$$\forall f \in E, \forall x_1, \ldots, x_n \in M, \exists\, r \in R : f(x_i) = rx_i.$$

2. *$\varphi(R)$ é um subconjunto denso em E (com a topologia finita):*

$$\forall f \in E, \forall x_1, \ldots, x_n \in M, U(f; x_1, \ldots, x_n) \cap \varphi(R) \neq \varnothing.$$

Se M for simples, então K é um anel de divisão e as duas afirmações anteriores são ainda equivalentes a:

3. $\forall x_1, \ldots, x_n \in M$ *linearmente independentes sobre* K, $\forall y_1, \ldots, y_n \in M$,

$$\exists\, r \in R : rx_i = y_i.$$

Demonstração. A equivalência entre (1) e (2) é clara:

$$\begin{aligned} & \forall f \in E, \forall x_1, \ldots, x_n, \exists\, r \in R : f(x_i) = rx_i \\ \Leftrightarrow\ & \forall f \in E, \forall x_1, \ldots, x_n, \exists\, \varphi_r \in \varphi(R) : f(x_i) = \varphi_r(x_i) \\ \Leftrightarrow\ & \forall f \in E, \forall x_1, \ldots, x_n, \exists\, \varphi_r \in \varphi(R) : \varphi_r \in U(f; x_1, \ldots, x_n) \\ \Leftrightarrow\ & \forall f \in E, \forall x_1, \ldots, x_n, U(f; x_1, \ldots, x_n) \cap \varphi(R) \neq \varnothing \end{aligned}$$

(1) $\Rightarrow$ (3) Consideremos n vectores linearmente independentes sobre K $x_1, \ldots, x_n$ e n vectores quaisquer $y_1, \ldots, y_n$. Existe uma base de V da forma $\{x_1, \ldots, x_n\} \cup \{u_i : i \in I\}$. Definimos o homomorfismo $f : M \to M$ K-linear determinado por

$$x_i \mapsto y_i \qquad \text{e} \qquad u_i \mapsto u_i.$$

Por (1) existe um elemento $r \in R$ tal que

$$y_i = f(x_i) = rx_i.$$

(3) $\Rightarrow$ (1) Sejam $f \in E$ e $x_1, \ldots, x_n \in M$. Seja $\{x_{i_1}, \ldots, x_{i_s}\}$ um subconjunto linearmente independente maximal de $\{x_1, \ldots, x_n\}$ (ou seja, os restantes vectores são combinações K-lineares de $x_{i_1}, \ldots, x_{i_s}$). Aplicando (3) aos vectores linearmente independentes $x_{i_1}, \ldots, x_{i_s}$ e aos vectores $f(x_{i_1}), \ldots, f(x_{i_s})$, temos que

$$\exists\, r \in R : rx_{i_j} = f(x_{i_j}).$$

Como os restantes vectores são combinações K-lineares de $x_{i_1}, \ldots, x_{i_s}$ e f é K-linear, temos que

$$f(x_i) = rx_i, \quad i = 1, \ldots, n.$$

□

Então, podemos reescrever o Teorema da Densidade de Jacobson da seguinte forma:

Teorema 4.10 (Teorema da Densidade - Versão Topológica) *Sejam* R *um anel,* M *um* R*-módulo à esquerda semisimples e* $K = \mathrm{End}({}_RM)$*. Então,*

R *é denso no anel* $E = \mathrm{End}(M_K)$ *relativamente à topologia finita.*

4.2 O Teorema da Estrutura dos Anéis Primitivos

Uma das mais importantes consequências do Teorema da Densidade é o Teorema da Estrutura dos Anéis Primitivos, que dá uma caracterização surpreendente destes anéis. É esta a relação entre os Anéis Primitivos e o Teorema da Densidade.

Teorema 4.11 (Teorema da Estrutura dos Anéis Primitivos) *Um anel R é primitivo se e só se é um subanel denso de um anel de aplicações lineares* $\mathrm{End}(M_K)$ *de um espaço vectorial M sobre um anel de divisão K.*

Neste caso, M é um R-módulo simples e fiel e $K = \mathrm{End}({}_RM)$ (que é um anel de divisão, pelo Lema de Schur). Para além disso,

1. *se* $\dim M_K = n$ *é finita, então $R \cong \mathcal{M}_n(K)$, que é simples e artiniano à esquerda.*
2. *se* $\dim M_K$ *é infinita, então R não é artiniano à esquerda e para cada $n \in \mathbb{N}$, existe um subanel R_n de R que admite um homomorfismo sobrejectivo $R_n \twoheadrightarrow \mathcal{M}_n(K)$.*

Observações:

1. Por vezes em certos livros este teorema é chamado de *Teorema da Densidade* [5] ou de *Teorema da Densidade para Anéis Primitivos* [9].
2. Este Teorema pode ser visto como uma generalização do Teorema de Artin-Wedderburn para anéis artinianos à esquerda (Teorema 1.22), na medida em que para anéis artinianos à esquerda as noções de simples e primitivo são equivalentes, logo o Teorema 1.22 enuncia o mesmo que a alínea (1).
3. Neste teorema vê-se claramente que a noção de primitivo estende a noção de simples ao contexto de dimensão infinita mas coincidem em dimensão finita. Como vimos no Teorema 3.8, R é primitivo e artiniano à esquerda se e só se R é simples e artiniano à esquerda se e só se $R \cong \mathcal{M}_n(D)$ (onde D é um anel de divisão).

Demonstração.

($\Longleftarrow$) Suponhamos que R é denso em $\mathrm{End}(M_D)$, onde M é um espaço vectorial sobre um anel de divisão D. Então, M é um R-módulo com acção

$$\phi \cdot m = \phi(m), \qquad \phi \in R,\ m \in M.$$

- ${}_RM$ é fiel, porque se $\phi \cdot m = \phi(m) = 0, \forall m \in M$ então $\phi \equiv 0$.
- ${}_RM$ é simples: dado $0 \neq m \in M$, existe uma base de M que contém m; então pela Proposição 4.9 para qualquer $n \in M$ existe uma aplicação linear $\phi \in R$ tal que

  $$\phi \cdot m = n$$

  e, deste modo, $Rm = M$. Logo, ${}_RM$ é simples.

Então, R é um anel primitivo à esquerda.

($\Longrightarrow$) Supondo que R é primitivo à esquerda, seja M um R-módulo simples e fiel. Então, pelo Lema de Schur $K = \mathrm{End}({}_RM)$ é um anel de divisão. Consideremos a aplicação natural $\varphi : R \to \mathrm{End}(M_K)$.

Como M é um R-módulo simples, em particular é semisimples, logo pelo Teorema da Densidade R age densamente em M_K. Pela Proposição 4.9, $\varphi(R)$ é denso em $\mathrm{End}(M_K)$. Sendo ${}_RM$ fiel, a aplicação φ é injectiva, logo $R \cong \varphi(R)$ que é denso em $\mathrm{End}(M_K)$.

Quanto à segunda parte da demonstração, supondo que R é primitivo à esquerda, sejam M um R-módulo simples e fiel e $K = \mathrm{End}({}_RM)$ (que é um anel de divisão). Então,

1. Supondo que $\dim M_K = n$, pelo Corolário 4.5 e pela Proposição 1.8

$$R \cong \varphi(R) = \mathrm{End}(M_K) \cong \mathrm{End}(K^n)_K \cong \mathcal{M}_n(\mathrm{End}(K)_K) \cong \mathcal{M}_n(K)$$

   e R é simples e artiniano à esquerda.

2. Suponhamos que $\dim M_K$ é infinita e seja $v_1, v_2, \ldots$ uma sucessão de vectores linearmente independentes de M. Definimos M_n como o K-subespaço de M gerado por $v_1, \ldots, v_n$:

$$M_n = \sum_{i=1}^{n} v_i K.$$

   Para além disso, definimos $R_n = \{r \in R : rM_n \subset M_n\}$ que é um subanel de R:

   - $a, b \in R_n \Rightarrow (a-b)M_n = aM_n - bM_n \subset M_n$ (porque M_n é um subespaço)
   - $a, b \in R_n \Rightarrow (ab)M_n = a(bM_n) \subset aM_n \subset M_n$

   Assim, M_n é um R_n-módulo à esquerda com a acção de R sobre M.

   Definimos a aplicação

$$\begin{array}{rcl} \varphi : R_n & \to & \mathrm{End}(M_n)_K \\ r & \mapsto & \varphi_r : M_n \to M_n \ , \\ & & \quad m \mapsto rm \end{array}$$

   que está bem definida, porque φ_r é de facto K-linear.

   - φ é um homomorfismo de anéis: $\forall m \in M_n$,

$$\varphi_{r+s}(m) = (r+s)m = rm + sm = \varphi_r(m) + \varphi_s(m) = (\varphi_r + \varphi_s)(m)$$

$$\varphi_{rs}(m) = (rs)m = r(sm) = \varphi_r(\varphi_s(m)) = (\varphi_r \circ \varphi_s)(m).$$

$$\text{e} \quad \varphi_1(m) = 1m = m = id_{M_n}(m).$$

- φ é sobrejectiva: seja $\phi \in \mathrm{End}(M_n)_K$; note-se que $\mathrm{End}(M_n)_K$ é um subconjunto de $\mathrm{End}(M_K)$: escrevendo $M = M_n \oplus M'$ como soma directa de subespaços vectoriais, qualquer endomorfismo $f \in \mathrm{End}(M_n)_K$ pode ser visto como um endomorfismo de M com imagem zero em M'.

  Como R é denso em $\mathrm{End}(M_K)$, pela Proposição 4.9 tomando os vectores linearmente independentes $v_1, \ldots, v_n$ e os vectores $\phi(v_1), \ldots, \phi(v_n)$

  $$\exists\, r \in R : rv_i = \phi(v_i)$$

  e pela K-linearidade de ϕ temos que $rM_n \subset \phi(M_n) \subset M_n$, isto é $r \in R_n$, logo $\phi = \varphi_r$.

Portanto, pelo Teorema do Isomorfismo (para anéis)

$$R_n \twoheadrightarrow R_n/\mathrm{Ker}(\varphi) \cong \mathrm{End}(M_n)_K \cong \mathrm{End}(K^n)_K \cong \mathcal{M}_n(\mathrm{End}(K)_K) \cong \mathcal{M}_n(K).$$

Para além disso, para cada n o núcleo de φ é um ideal de R_n que designamos por $I_n = \{r \in R : rM_n = 0\}$. Tomando os vectores linearmente independentes $v_1, \ldots, v_n, v_{n+1}$, novamente pela Proposição 4.9 existe $r \in R$ tal que

$$rv_1 = \ldots = rv_n = 0 \quad \text{e} \quad rv_{n+1} \neq 0,$$

ou seja, $r \in I_n$ mas $r \notin I_{n+1}$. Então, $I_1 \supsetneq I_2 \supsetneq \ldots$ é uma cadeia infinita estritamente decrescente de ideais (à esquerda) de R. Portanto, R não é artiniano à esquerda. □

Com esta caracterização, podemos obter mais exemplos de anéis primitivos, procurando exemplos de anéis densos de aplicações lineares.

Exemplo:

Seja V_K um espaço vectorial à direita sobre um corpo K com base numerável $\{e_1, e_2, \ldots\}$, isto é

$$V = \bigoplus_{i \in \mathbb{N}} e_i K.$$

Consideremos ainda o anel $E = \mathrm{End}(V_K)$.

Para cada n pode-se mergulhar $\mathcal{M}_n(K)$ em $\mathcal{M}_{n+1}(K)$ da seguinte forma:

$$M \in \mathcal{M}_n(K) \mapsto \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{M}_{n+1}(K).$$

A reunião de todos os anéis de matrizes $\mathcal{M}_\infty(K) = \bigcup_{n=1}^{\infty} \mathcal{M}_n(K)$ é um anel mas sem identidade. Juntando a identidade, obtemos o anel

$$R = \mathcal{M}_\infty(K) \oplus A \cdot \mathbf{1} = \{M + a \cdot \mathbf{1} \mid a \in A, M \in \mathcal{M}_n(K), n \geq 1\},$$

onde por definição $M \times (a \cdot \mathbf{1}) = aM = (a \cdot \mathbf{1}) \times M$ para qualquer $n \geq 1$ e $M \in \mathcal{M}_n(K)$. De facto, R é um anel: dados $r_1 = M + a \cdot \mathbf{1}, r_2 = N + b \cdot \mathbf{1} \in R$, podemos assumir que $M, N \in \mathcal{M}_n(K)$ usando se necessário um mergulho de anéis de matrizes. Então,

$$r_1 - r_2 = (M + a \cdot \mathbf{1}) - (N + b \cdot \mathbf{1}) = (M - N) + (a - b) \cdot \mathbf{1} \in R$$

$$r_1 r_2 = (M + a \cdot \mathbf{1})(N + b \cdot \mathbf{1}) = (MN) + (ab) \cdot \mathbf{1} \in R.$$

R pode ser visto como um subconjunto de E da seguinte forma: dado $r = M + a \cdot \mathbf{1} \in R$ com $a \in A$ e $M \in \mathcal{M}_n(K)$, identificamos r com o endomorfismo $f : V \to V$ que corresponde à matriz

$$\begin{pmatrix} M & & & \\ & a & & \\ & & a & \\ & & & \ddots \end{pmatrix} \quad \text{ou seja} \quad \begin{array}{rcll} f : V & \to & V & \\ e_i & \mapsto & Me_i, & 1 \leq i \leq n \\ e_i & \mapsto & ae_i, & i \geq n+1 \end{array}.$$

Vejamos que a identificação anterior é um homomorfismo de anéis: dados $r = M + a \cdot \mathbf{1}$ e $s = N + b \cdot \mathbf{1}$, com $M, N \in \mathcal{M}_n(K)$, que correspondem a f e g, respectivamente, temos que

1. $r + s = (M + N) + (a + b) \cdot \mathbf{1}$ corresponde ao endomorfismo h, onde

$$h(e_i) = \begin{cases} (M+N)e_i, & 1 \leq i \leq n \\ (a+b)e_i, & i \geq n+1 \end{cases} = \begin{cases} Me_i + Ne_i, & 1 \leq i \leq n \\ ae_i + be_i, & i \geq n+1 \end{cases} = f(e_i) + g(e_i).$$

2. $rs = (MN) + (ab) \cdot \mathbf{1}$ corresponde ao endomorfismo h, onde

$$h(e_i) = \begin{cases} (MN)e_i, & 1 \leq i \leq n \\ (ab)e_i, & i \geq n+1 \end{cases} = \begin{cases} M(Ne_i), & 1 \leq i \leq n \\ a(be_i), & i \geq n+1 \end{cases} = f(g(e_i)).$$

Para além disso, R é um subanel denso de E: sejam $f \in E$ e $x_1, \ldots, x_n \in V$. Queremos ver que existe $r \in R$ tal que $f(x_i) = rx_i$. Como $x_1, \ldots, x_n$ são um número finito de elementos de V, então ao todo são combinações lineares de um número finito de e_i's, digamos

$$x_1, \ldots, x_n \in \bigoplus_{i=1}^{m} e_i K = W.$$

Designando $f|_W = M \in \mathcal{M}_m(K)$, basta tomar $r = M + \mathbf{1}$, que claramente opera cada x_i da mesma forma que f. Portanto,

R é um anel primitivo à esquerda.

O exemplo anterior é da autoria de Kaplansky e surgiu na sequência da pergunta

O que se pode dizer sobre o centro $Z(R)$ de um anel primitivo à esquerda?

Já vimos que o centro de um anel simples é um corpo (1.19) e o centro de um anel primo é um domínio integral (1.30). Como um anel primitivo R é primo, então o seu centro $Z(R)$ é um domínio integral. De facto, $Z(R)$ pode ser *qualquer* domínio integral.

Sejam A um domínio integral, $K = Frac(A)$ o corpo das fracções de A e consideremos o anel primitivo R construído no exemplo anterior. Se $r = M + a \cdot \mathbf{1} \in Z(R)$ então $M \in Z(\mathcal{M}_n(K)) \Rightarrow M = bI_n$; para além disso,

$$\begin{pmatrix} M & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} b & & & \\ & \ddots & & \\ & & b & \\ & & & a \end{pmatrix} \in Z(\mathcal{M}_{n+1}(K)),$$

logo $b = a$ e $r = a \cdot \mathbf{1}$. Então, $Z(R) = \{a \cdot \mathbf{1} : a \in A\} \cong A$.

4.3 Teorema de Kaplansky

Nesta secção vamos ver uma aplicação simples do Teorema da Estrutura dos Anéis Primitivos: o Teorema de Kaplansky, no âmbito da teoria dos Anéis com Identidade Polinomial.

A primeira vez que apareceu o noção de *identidade polinomial* foi em 1922 num artigo de M. Dehn. [3]. Nos 25 anos seguintes, houve apenas dois resultados significativos na área:

1. Em 1937 W. Wagner construíu identidades polinomiais para matrizes $n \times n$ [18].
2. Em 1943 M. Hall provou o seguinte Teorema [7, Theorem 6.2]:

   Teorema 4.12 (Teorema de Hall) *Seja D uma álgebra de divisão tal que $[x,y]^2$ é central, $\forall x, y \in D$. Então, D é comutativo ou* $\dim D_{Z(D)} = 4$.

No entanto, todos estes artigos provinham da área de Geometria Projectiva. Até que em 1948, I. Kaplansky usa pela primeira vez o termo de *identidade polinomial* num artigo [12] onde demonstra um teorema, conhecido como Teorema de Kaplansky, que generaliza o Teorema de Hall.

Este teorema é a base da teoria dos Anéis com Identidade Polinomial.

Existem ainda outros 2 Teoremas que são fundamentais nesta área: o Teorema de E.C. Posner e o Teorema de M. Artin. Para mais informações sobre a teoria de Anéis com Identidade Polinomial, deve consultar-se [4].

Nesta secção vamos enunciar e demonstrar o Teorema de Kaplansky, que é consequência do Teorema da Estrutura dos Anéis Primitivos. Antes disso, são necessárias algumas definições e resultados.

Seja A um anel comutativo. Representamos por $A\langle X\rangle$ a A-álgebra livre associativa com um número numerável de variáveis $x_1, x_2, \ldots$. Um elemento genérico de $A\langle X\rangle$ é

$$f = \sum_{i=1}^{n} a_i x_{i_1} \ldots x_{i_{k_i}}.$$

Uma $\underline{A\text{-álgebra}}$ é um anel R com um homomorfismo $\varphi : A \to Z(R)$. Dado um polinómio $f \in A\langle X\rangle$ e $r_1, \ldots, r_n \in R$, $f(r_1, \ldots, r_n)$ é o valor de f em $r_1, \ldots, r_n$, ou seja, é a imagem de f por qualquer homomorfismo de A-álgebras

$$\begin{array}{rcl} \varphi : A\langle X\rangle & \to & R \\ x_i & \mapsto & r_i \end{array}$$

Note-se que $f(r_1, \ldots, r_n)$ não depende do homomorfismo φ: porque dados dois homomorfismo $\varphi, \psi : A\langle X\rangle \to R$ que enviam $x_i \mapsto r_i$, temos que

$$\varphi(f) = \sum_{i=1}^{n} a_i \varphi(x_{i_1}) \ldots \varphi(x_{i_{k_i}}) = \sum_{i=1}^{n} a_i r_{i_1} \ldots r_{i_{k_i}} = \sum_{i=1}^{n} a_i \psi(x_{i_1}) \ldots \psi(x_{i_{k_i}}) = \psi(f).$$

Um *monómio* é um elemento da forma $f = a x_{i_1} \ldots x_{i_n} \in A\langle X\rangle$ e diz-se que tem *grau* n.

Definição 4.13 *Seja $f(x_1, \ldots, x_n) \in A\langle X\rangle$ um polinómio.*

- *f diz-se homogéneo de grau n se for uma combinação A-linear de monómios de grau n.*
- *f diz-se linear na variável x_i se for uma combinação A-linear de monómios que têm grau 1 em x_i.*
- *f diz-se multilinear se for linear em todas as variáveis $x_1, \ldots, x_n$.*

Note-se que um polinómio multilinear pode ser escrito

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} a(\sigma) x_{\sigma(1)} \ldots x_{\sigma(n)},$$

onde $a(\sigma) \in A$ e S_n é o grupo simétrico das permutações de $\{1, \ldots, n\}$.

Exemplos:

- $x_1^2 x_2 x_3^3 - 3 x_2 x_3 x_1 x_3^2 x_1$ é homogéneo de grau 6 e linear na variável x_2.
- $x_1 x_2 x_3 - 3 x_3 x_1 x_2$ é multilinear.

Definição 4.14 *Sejam A um anel comutativo e R uma A-álgebra.*
Um polinómio $f(x_1, \ldots, x_n) \in A\langle X\rangle$ diz-se uma identidade polinomial (IP) de R se

$$f(r_1, \ldots, r_n) = 0, \qquad \forall r_1, \ldots, r_n \in R.$$

Neste caso, diz-se que R satisfaz a IP f.

Por exemplo, qualquer anel comutativo satisfaz a identidade polinomial

$$f(x, y) = xy - yx.$$

Um polinómio $f(x_1, \ldots, x_n) \in A\langle X\rangle$ diz-se próprio se na componente homogénea de maior grau de f existe algum coeficiente 1.

Teorema 4.15 *Se R tem uma IP $f \in A\langle X\rangle$ própria, então existe uma IP própria e multilinear $g \in A\langle X\rangle$ com o mesmo grau de f.*

A sua demonstração pode ser consultada em [4].

Teorema 4.16 *Seja K um anel de divisão. $\mathcal{M}_n(K)$ não satisfaz uma IP de grau $\leq 2n-1$.*

Demonstração. Suponhamos que $\mathcal{M}_n(K)$ tem uma IP de grau $2n-1$ (para graus menores, a prova é análoga). Como K é anel de divisão, $\mathcal{M}_n(K)$ tem uma IP própria de grau $2n-1$ e, pelo Teorema 4.15, tem uma IP multilinear (e própria) f de grau $2n-1$. Como K é anel de divisão, podemos assumir que f é da forma

$$f(x_1,\ldots,x_{2n-1}) = x_1x_2\ldots x_{2n-1} + \sum_{id\neq\sigma\in S_{2n-1}} a(\sigma)x_{\sigma(1)}x_{\sigma(2)}\ldots x_{\sigma(2n-1)}.$$

Consideremos as matrizes $E_{11}, E_{12}, E_{22}, E_{23}, \ldots, E_{n-1,n-1}, E_{n-1,n}, E_{nn}$. Esta é uma lista de $2(n-1)+1 = 2n-1$ matrizes e o único produto de todas elas que é não nulo ocorre quando elas estão na ordem acima. Logo,

$$f(E_{11},\ldots,E_{nn}) = E_{11}\ldots E_{nn} = E_{1n} \neq 0,$$

o que é uma contradição. □

Teorema 4.17 (Teorema de Kaplansky) *Seja R um anel primitivo que satisfaz uma identidade polinomial. Então, $R \cong \mathcal{M}_n(K)$, onde K é um anel de divisão.*

Demonstração. Suponhamos que o anel primitivo R satisfaz uma IP. Pelo Teorema 4.15, R satisfaz um polinómio multilinear próprio f.

Sejam M um R-módulo à esquerda simples e fiel e $K = \mathrm{End}(_RM)$. Pelo Teorema da Estrutura dos Anéis Primitivos (4.11), $R \cong \mathcal{M}_n(K)$ ou para qualquer $n \in \mathbb{N}$ existe um subanel R_n de R tal que $R_n \twoheadrightarrow \mathcal{M}_n(K)$.

Pelo Teorema 4.16, nenhum polinómio é identidade polinomial de todos os anéis de matrizes $\mathcal{M}_n(K)$, logo o segundo cenário está excluído. Portanto, $R \cong \mathcal{M}_n(K)$. □

Na próxima secção vamos estudar mais uma (e última) consequência do Teorema da Densidade, nomeadamente nas acções de grupos sobre anéis.

4.4 Acções de Grupos sobre Anéis

Seja R um anel.

Um *automorfismo* de R é um endomorfismo $f : R \to R$ bijectivo e o conjunto dos automorfismos de R representa-se por $Aut(R)$. Uma *acção* de G sobre R é um homomorfismo de grupos

$$\begin{array}{rcl} \varphi : G & \to & Aut(R) \\ g & \mapsto & \varphi_g : R \to R \\ & & \quad x \mapsto \varphi_g(x) = x^g \end{array} .$$

Definimos

$$R^G = \{x \in R : x^g = x, \forall g \in G\},$$

isto é, o conjunto dos elementos de R que são fixos pelas acções de todos os elementos de G. Este conjunto é não vazio, porque $0, 1 \in R^G$. Para além disso, R^G é um subanel de R: $\forall x, y \in R^G$,

1. $\forall g \in G, (x-y)^g = x^g - y^g = x - y \Rightarrow x - y \in R^G$.
2. $\forall g \in G, (xy)^g = x^g y^g = xy \Rightarrow xy \in R^G$.

Um ideal I de R diz-se $\underline{G\text{-estável}}$ se

$$\forall g \in G, \forall x \in I, \quad x^g \in I.$$

Os ideais triviais 0 e R são G-estáveis, porque $\forall g \in G, 0^g = 0$ e $\forall g \in G, \forall x \in R, x^g \in R$. Se 0 e R são os únicos ideais G-estáveis de R, R diz-se $\underline{G\text{-simples}}$.

Proposição 4.18 *Se R é comutativo e G-simples, então R^G é um corpo.*

Demonstração. Seja $0 \neq x \in R^G$ e consideremos Rx, que é um ideal (porque R é comutativo) e é G-estável: como $x \in R^G$

$$(yx)^g = y^g x^g = y^g x \in Rx, \quad \forall y \in R, \forall g \in G.$$

Como $Rx \neq 0$ (porque $x \neq 0$) e R é G-simples, temos que $Rx = R$, em particular existe $y \in R$ tal que

$$yx = 1 = xy.$$

Resta ver que $y \in R^G$: $\forall g \in G$,

$$y^g = y^g 1 = y^g xy = y^g x^g y = (yx)^g y = 1^g y = 1y = y.$$

□

O "skew group ring" $R * G$ é um módulo livre sobre R com base $\{\overline{g} : g \in G\}$, ou seja,

$$R * G = \bigoplus_{g \in G} R\,\overline{g} = \left\{ \sum_{g \in G} a_g \overline{g} : a_g \in R \right\}.$$

$R * G$ tem estrutura de anel, com a soma usual de produtos directos e a multiplicação determinada por

$$a\overline{g} \cdot b\overline{h} = ab^g \overline{gh}, \qquad \forall a, b \in R, \forall g, h \in G.$$

Então, $\forall a, b, c \in R, \forall g, h, i \in G$

1. $(a\overline{g} \cdot b\overline{h}) \cdot c\overline{i} = ab^g \overline{gh} \cdot c\overline{i} = ab^g c^{gh} \overline{ghi} = ab^g (c^h)^g \overline{ghi} = a(bc^h)^g \overline{ghi} = a\overline{g} \cdot bc^h \overline{hi} = a\overline{g} \cdot (b\overline{h} \cdot c\overline{i})$.

   Note-se que $(c^h)^g = \varphi_g(\varphi_h(c)) = (\varphi_g \circ \varphi_h)(c) = \varphi_{gh}(c) = c^{gh}, \forall c \in R$.

2. $(a\overline{g} + b\overline{g}) \cdot c\overline{h} = (a+b)\overline{g} \cdot c\overline{h} = (a+b)c^g \overline{gh} = (ac^g + bc^g)\overline{gh} = ac^g \overline{gh} + bc^g \overline{gh} = a\overline{g} \cdot c\overline{h} + b\overline{g} \cdot c\overline{h}$.

3. $a\overline{g} \cdot (b\overline{h} + c\overline{h}) = a\overline{g} \cdot (b+c)\overline{h} = a(b+c)^g \overline{gh} = a(b^g + c^g)\overline{gh} = ab^g \overline{gh} + ac^g \overline{gh} = a\overline{g} \cdot b\overline{h} + a\overline{g} \cdot c\overline{h}$.

4. A identidade deste anel é $\overline{e}$: $a\overline{g} \cdot \overline{e} = a\overline{ge} = a\overline{g}$ e $\overline{e} \cdot a\overline{g} = a^e \overline{g} = a\overline{g}$.

   Note-se que $a^e = \varphi_e(a) = id_R(a) = a, \forall a \in R$.

R é um módulo à esquerda sobre $R * G$ com a acção

$$\left(\sum_{g \in G} a_g \overline{g} \right) \cdot x = \sum_{g \in G} a_g x^g,$$

$\forall x \in R, \forall \sum_{g \in G} a_g \overline{g} \in R * G$.

A acção é associativa, porque: $\forall \sum_{g \in G} a_g \overline{g}, \sum_{h \in G} b_h \overline{h} \in R * G, \forall x \in R$,

$$\begin{aligned}
\left(\sum_{g \in G} a_g \overline{g} \right) \cdot \left[\left(\sum_{h \in G} b_h \overline{h} \right) \cdot x \right] &= \left(\sum_{g \in G} a_g \overline{g} \right) \cdot \left(\sum_{h \in G} b_h x^h \right) = \sum_{g \in G} a_g \left(\sum_{h \in G} b_h x^h \right)^g \\
&= \sum_{g \in G} a_g \left(\sum_{h \in G} b_h^g (x^h)^g \right) = \sum_{g,h \in G} a_g b_h^g x^{gh} \\
&= \left(\sum_{g,h \in G} a_g b_h^g \overline{gh} \right) \cdot x = \left(\sum_{g,h \in G} (a_g \overline{g})(b_h \overline{h}) \right) \cdot x \\
&= \left[\left(\sum_{g \in G} a_g \overline{g} \right) \left(\sum_{h \in G} b_h \overline{h} \right) \right] \cdot x.
\end{aligned}$$

A acção é distributiva, porque: $\forall \sum_{g\in G} a_g\overline{g}, \sum_{g\in G} b_g\overline{g} \in R*G, \forall x,y \in R$,

$$\begin{aligned}\left(\sum_{g\in G} a_g\overline{g} + \sum_{g\in G} b_g\overline{g}\right)\cdot x &= \left(\sum_{g\in G}(a_g+b_g)\overline{g}\right)\cdot x = \sum_{g\in G}(a_g+b_g)x^g \\ &= \sum_{g\in G}(a_gx^g + b_gx^g) = \left(\sum_{g\in G} a_gx^g\right) + \left(\sum_{g\in G} b_gx^g\right) \\ &= \left(\sum_{g\in G} a_g\overline{g}\right)\cdot x + \left(\sum_{g\in G} b_g\overline{g}\right)\cdot x\end{aligned}$$

$$\begin{aligned}\left(\sum_{g\in G} a_g\overline{g}\right)\cdot (x+y) &= \sum_{g\in G} a_g(x+y)^g = \sum_{g\in G} a_g(x^g+y^g) = \sum_{g\in G}(a_gx^g + a_gy^g) \\ &= \left(\sum_{g\in G} a_gx^g\right) + \left(\sum_{g\in G} a_gy^g\right) = \left(\sum_{g\in G} a_g\overline{g}\right)\cdot x + \left(\sum_{g\in G} a_g\overline{g}\right)\cdot y\end{aligned}$$

E por último, $\overline{e}\cdot x = x^e = x$.

Proposição 4.19 *Se R é um anel comutativo e G-simples, então R é um $R*G$-módulo simples.*

Demonstração. Seja $W \neq 0$ um $R*G$-submódulo de R. W é um ideal à esquerda de R, porque $\forall x,y \in W, \forall r \in R$,

$$x - y \in W \quad \text{e} \quad (r\overline{e})\cdot x = rx^e = rx \in W$$

e, sendo R comutativo, W é um ideal (bilateral) de R. Para além disso, W é G-estável, porque

$$x^g = \overline{g}\cdot x \in W.$$

Como R é G-simples, $W = R$. □

Proposição 4.20 *Consideremos B o subanel de $\mathrm{End}_{\mathbb{Z}}(R)$ gerado por*

$$\begin{array}{rcl} L_a : R & \to & R \\ x & \mapsto & ax \end{array} \qquad e \qquad \begin{array}{rcl} \varphi_g : R & \to & R \\ x & \mapsto & x^g \end{array},$$

para quaisquer $a \in R$ e $g \in G$. Então,

$$R*G/\mathrm{Ann}_{R*G}(R) \cong B.$$

Demonstração. Definimos a aplicação ψ determinada por

$$\begin{aligned} \psi : R*G &\to \mathrm{End}_{\mathbb{Z}}(R) \\ a\overline{g} &\mapsto L_a \circ \varphi_g \end{aligned}$$

Em primeiro lugar, a aplicação ψ está bem definida, isto é, $L_a \circ \varphi_g \in \mathrm{End}_{\mathbb{Z}}(R)$:

1. $(L_a \circ \varphi_g)(x+y) = a(x+y)^g = a(x^g + y^g) = ax^g + ay^g = (L_a \circ \varphi_g)(x) + (L_a \circ \varphi_g)(y)$.
2. $(L_a \circ \varphi_g)(nr) = a(\underbrace{r + \ldots + r}_{n \text{ vezes}})^g = \underbrace{ar^g + \ldots + ar^g}_{n \text{ vezes}} = n(ar^g) = n(L_a \circ \varphi_g)(r)$.

Vejamos que ψ é um homomorfismo de anéis:

1. $\psi(a\overline{g} + b\overline{g}) = \psi((a+b)\overline{g}) = L_{a+b} \circ \varphi_g = (L_a + L_b) \circ \varphi_g = L_a \circ \varphi_g + L_b \circ \varphi_g = \psi(a\overline{g}) + \psi(b\overline{g})$.
2. $\psi((a\overline{g}) \cdot (b\overline{h})) = \psi(ab^g\overline{gh}) = L_{ab^g} \circ \varphi_{gh} = L_a \circ L_{b^g} \circ \varphi_g \circ \varphi_h = L_a \circ \varphi_g \circ L_b \circ \varphi_h = \psi(a\overline{g}) \circ \psi(b\overline{h})$.

   Note-se que $(L_{b^g} \circ \varphi_g)(x) = b^g x^g = (bx)^g = (\varphi_g \circ L_b)(x)$.

O núcleo de ψ é

$$\begin{aligned} \mathrm{Ker}(\psi) &= \left\{ \sum a_g\overline{g} \in R*G : \psi\left(\sum a_g\overline{g}\right) = \sum L_{a_g} \circ \varphi_g \equiv 0 \right\} \\ &= \left\{ \sum a_g\overline{g} \in R*G : \sum (L_{a_g} \circ \varphi_g)(x) = \sum a_g x^g = 0, \forall x \in R \right\} \\ &= \left\{ \sum a_g\overline{g} \in R*G : \left(\sum a_g\overline{g}\right) \cdot x = \sum a_g x^g = 0, \forall x \in R \right\} \\ &= \mathrm{Ann}_{R*G}(R). \end{aligned}$$

e claro que $\mathrm{Im}(\psi) = \langle \psi(a\overline{g}) : a \in R, g \in G \rangle = \langle L_a \circ \varphi_g : a \in R, g \in G \rangle = B$. Pelo Teorema do Isomorfismo,

$$R*G/\mathrm{Ann}_{R*G}(R) = R*G/\mathrm{Ker}(\psi) \cong \mathrm{Im}(\psi) = B.$$

□

Chamamos $\Delta = \mathrm{End}({}_{R*G}R)$, cujos elementos são $f : R \to R$ homomorfismos $R*G$-lineares, isto é,

$$(a\overline{g} \cdot x)f = a\overline{g} \cdot (x)f \Leftrightarrow (ax^g)f = a(x)f^g.$$

R é um Δ-módulo à direita com acção

$$x \cdot f = (x)f.$$

Se R for comutativo e G-simples, então pela Proposição 4.19 R é um $R*G$-módulo simples e pelo Lema de Schur $\Delta = \mathrm{End}({}_{R*G}R)$ é um anel de divisão. Logo, R é um espaço vectorial sobre Δ. Vamos ver um Teorema que majora a dimensão de R sobre Δ.

Para isso, é necessário introduzir uma nova noção: a dimensão uniforme.

4.4.1 Dimensão Uniforme

Dado um R-módulo à esquerda M, a dimensão uniforme de M é dada por

$$\operatorname{udim}(M) = \sup\left\{ n \in \mathbb{N} : \exists\, 0 \neq N_1, \ldots, N_n \leq M : N_i \cap \left(\sum_{j \neq i} N_j \right) = 0 \right\}.$$

Por vezes, esta dimensão é também chamada de *dimensão de Goldie*. Estudando ${}_RR$, a noção de dimensão uniforme pode ser estendida aos anéis.

A dimensão uniforme $\operatorname{udim}(M) = n < \infty$ é finita se e só se [16]:

- Existem n submódulos $0 \neq N_1, \ldots, N_n \leq M$ tais que

$$N_i \cap \left(\sum_{j \neq i} N_j \right) = 0, \quad \forall i.$$

- $\bigoplus_{i=1}^{n} N_i$ é essencial em M, isto é,

$$\forall\, 0 \neq N \leq M, \quad N \cap \left(\bigoplus_{i=1}^{n} N_i \right) \neq 0.$$

Exemplos:

1. $\operatorname{udim}({}_{\mathbb{Z}}\mathbb{Q}) = 1$

   Sejam $0 \neq \frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. Então, $\mathbb{Z}\frac{a}{b} \cap \mathbb{Z}\frac{c}{d} \neq 0$, porque

$$0 \neq ac = cb\frac{a}{b} = ad\frac{c}{d} \in \mathbb{Z}\frac{a}{b} \cap \mathbb{Z}\frac{c}{d}.$$

2. $\operatorname{udim}(\mathbb{Z}) = 1$

   Dados $n, m \neq 0$, $n\mathbb{Z} \cap m\mathbb{Z} = mmc(n, m)\mathbb{Z} \neq 0$.

3. $\operatorname{udim}(\mathbb{C}[x]) = 1$

   Dados $f, g \in \mathbb{C}[x]$, $\langle f \rangle \cap \langle g \rangle = \langle mmc(f, g) \rangle \neq 0$.

Mais geralmente, se R for um domínio integral então $\operatorname{udim}(R) = 1$: dados dois ideais I, J não nulos de R, então IJ é não nulo e está contido em $I \cap J$, em particular $I \cap J \neq 0$. R diz-se um anel uniforme.

É fácil ver que a dimensão uniforme tem a seguinte propriedade [16]:

$$\operatorname{udim}(M^n) = n \times \operatorname{udim}(M).$$

4.4.2 Aplicação do Teorema da Densidade

Vejamos o Teorema que majora a dimensão de R sobre $\Delta = \mathrm{End}({}_{R*G}R)$ e cuja demonstração faz uso do Teorema da Densidade de Jacobson.

Teorema 4.21 *Se R é comutativo e G-simples e G é um grupo finito, então*

$$\dim(R_\Delta) \leq |G|\mathrm{udim}(R),$$

onde $\Delta = \mathrm{End}({}_{R*G}R)$.

Demonstração. Seja $B = \{v_1, \ldots, v_k\} \cup B'$ uma base de R_Δ, ou seja, podemos escrever

$$R = \left(\bigoplus_{i=1}^{k} v_i\Delta\right) \oplus \left(\bigoplus_{b\in B'} b\Delta\right).$$

Para cada $1 \leq i \leq n$, consideremos a projecção

$$\begin{array}{rcl} f_i : R \twoheadrightarrow v_i\Delta & \to & 1_R\Delta \\ v_i & \mapsto & 1_R \end{array}$$

que é Δ-linear, ou seja, $f_i \in \mathrm{End}(R_\Delta)$.

Para além disso, como R é comutativo e G-simples, então pela Proposição 4.19 é um $R*G$-módulo simples. Então, pelo Teorema da Densidade, para cada $i = 1, \ldots, k$, existe $s_i \in R*G$ tal que

$$s_i \cdot v_j = f_i(v_j) = \begin{cases} 0, & \text{se } i \neq j \\ 1_R, & \text{se } i = j \end{cases}.$$

Como $G = \{g_1, \ldots, g_n\}$ é finito, definimos

$$\begin{array}{rccl} \psi : & R^n & \to & R*G \\ & (a_1, \ldots, a_n) & \mapsto & \sum_{k=1}^{n} a_k\overline{g_k} \end{array},$$

que é um homomorfismo de R-módulos. Como qualquer elemento de $R*G$ é da forma $\sum_{k=1}^{n} a_k\overline{g_k}$, então ψ é também sobrejectiva. Então, para cada $i = 1, \ldots, k$, existe $t_i \in R^n$ tal que

$$(t_i)\psi = s_i.$$

Estudando R^n como um R-módulo à esquerda, temos que Rt_i é um R-submódulo de R^n. Vejamos que $\sum_{i=1}^{k} Rt_i$ é de facto um soma directa: seja $z \in Rt_i \cap \left(\sum_{j\neq i} Rt_j\right)$, digamos $z = at_i = \sum_{j\neq i} b_j t_j$. Por um lado, $\forall j \neq i$

$$(z)\psi \cdot v_j = (at_i)\psi \cdot v_j = a(t_i)\psi \cdot v_j = a(s_i \cdot v_j) = 0$$

e, por outro lado, $\forall j \neq i$

$$(z)\psi \cdot v_j = \sum_{l \neq i} (b_l t_l)\psi \cdot v_j = \sum_{l \neq i} b_l (s_l \cdot v_j) = b_j.$$

Logo, $z = \sum_{j \neq i} b_j t_j = 0$.

Então, em R^n existe uma soma directa de k submódulos, logo

$$k \leq \text{udim}(R^n) = n\text{udim}(R) = |G|\text{udim}(R).$$

Como $v_1, \ldots, v_k$ eram quaisquer elementos de R linearmente independentes sobre Δ, então

$$\dim(R_\Delta) \leq |G|\text{udim}(R).$$

□

Observação: $\Delta = \text{End}({}_{R*G}R) \cong R^G = \{r \in R : r^g = r, \forall g \in G\}$.

Consideremos a aplicação

$$\begin{array}{rcl} \psi : \text{End}({}_{R*G}R) & \to & R^G \\ f & \mapsto & (1)f \end{array}$$

que está bem definida, porque

$$(1)f^g = \overline{g} \cdot (1)f = (\overline{g} \cdot 1)f = (1^g)f = (1)f, \forall g \in G.$$

Esta aplicação ψ é um homomorfismo de anéis:

1. $(1)(f + f') = (1)f + (1)f'$
2. $$\begin{array}{rcl} (1)(f \circ f') & = & ((1)f)f' = ((1)f1)f' = ((1)f1^g)f' = ((1)f\overline{g} \cdot 1)f' \\ & = & (1)f\overline{g}(1)f' = (1)f((1)f')^g = (1)f(1)f'. \end{array}$$
3. $\psi(id_R) = (1)id_R = 1$.

Para além disso, ψ é injectiva, porque se $(1)f = (1)f'$ então

$$(r)f = (r\overline{g} \cdot 1)f = r\overline{g} \cdot (1)f = r\overline{g} \cdot (1)f' = (r\overline{g} \cdot 1)f' = (r)f', \quad \forall r \in R$$

e é sobrejectiva, porque dado $r \in R^G$, consideremos $f : x \mapsto xr$ que é $R*G$-linear porque

$$a\overline{g} \cdot (x)f = a\overline{g} \cdot xr = a(xr)^g = ax^g r^g = (ax^g)r = (ax^g)f = (a\overline{g} \cdot x)f.$$

Portanto, $\text{End}({}_{R*G}R) \cong R^G$. □

Portanto, se R é um domínio integral e G-simples e se G é um grupo finito, então pelo Teorema 4.21 R tem dimensão finita sobre R^G (majorada por $|G|$) e R^G é um corpo (pela Proposição 4.18), logo R é artiniano (à esquerda e à direita): porque qualquer ideal (à esquerda ou à direita) é um subespaço sobre R^G com dimensão finita, logo em qualquer cadeia estritamente descendente $I_1 \supset I_2 \supset \ldots$ a dimensão dos I_j diminui pelo menos um, logo a cadeia tem de terminar.

Logo, para qualquer $x \neq 0$ a cadeia $Rx \supseteq Rx^2 \supseteq Rx^3 \supseteq \ldots$ tem de terminar, isto é, existe algum n tal que $Rx^n = Rx^{n+1}$, em particular, $x^n = ax^{n+1}$ para algum $a \in R$, donde $x^n(1 - ax) = 0$. Como R é um domínio integral e $x \neq 0$, temos que $1 = ax$, ou seja, x é invertível. Deste modo, R é um corpo.

Portanto,

$$R^G \leq R \text{ é uma extensão de corpos com } [R : R^G] \leq |G|.$$

Referências

[1] E.A. Behrens, *Ring Theory*, Academic Press (1972).

[2] G.M. Bergman, *A ring primitive on the right but not on the left.*, Proc. Amer. Math. Soc. 15 (1964) 473–475.

[3] M. Dehn, *Über die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme*, Math. Ann. **85** (1922), 184-193.

[4] V. Drensky & E. Formanek, *Polynomial Identity Rings*, Birkhäuser (2004).

[5] B. Farb & R.K. Dennis, *Noncommutative Algebra*, Springer-Verlag (1993).

[6] A. Hajnal & P. Hamburger, *Set Theory*, London Mathematical Society **48** (1999).

[7] M. Hall, *Projective planes*, Trans. Amer. Math. Soc. **54** (1943), 229-277.

[8] M. Henriksen, *A Simple Characterization of Commutative Rings Without Maximal Ideals*, American Mathematical Monthly (1975), 502-505.

[9] N. Jacobson, *Basic Algebra II*, Dover Publications, Inc. (1989)

[10] N. Jacobson, *Structure of Rings*, AMS Colloquium Publication, Vol. **37** (1956).

[11] N. Jacobson, *Structure theory of simple rings without finiteness assumptions* Trans. Am. Math. Soc. **57** (1945), 228-245.

[12] I. Kaplansky, *Rings with a polynomial identity*, Bull. Amer. Math. Soc. **54** (1948), 575-580.

[13] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics **155** Springer (1995).

[14] W. Krull, *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, Mathematische Annalen **10** (1929), 729–744.

[15] T.Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics **131** Springer (1991).

[16] T.Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics **189** Springer (1999).

[17] L.H. Rowen, *Ring Theory*, Academic Press (1991).

[18] W. Wagner, *Über die Grundlagen der projektiven Geometrie und allgemeine Zahlensysteme*, Math. Z. **113** (1937), 528-567.