ÁLGEBRA

Pedro V. Silva

Mestrado em Matemática – Fundamentos e Aplicações 2003/04

Departamento de Matemática Pura

Faculdade de Ciências do Porto

Índice

1 ANÉIS E MÓDULOS

Uma *operação binária* num conjunto S (não vazio) é uma função do tipo $f : S \times S \to S$. É habitual representar $f(a, b)$ na forma $a \cdot b$ ou outra equivalente. Um *semigrupo* é uma estrutura algébrica da forma $(S, \cdot)$, onde S designa um conjunto não vazio e $\cdot$ uma operação binária associativa em S, isto é, satisfazendo a condição

$$\forall a, b, c \in S \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Se S tiver elemento neutro para a operação $\cdot$, isto é, se

$$\exists e \in S \; \forall a \in S \quad a \cdot e = e \cdot a = a,$$

dizemos que $(S, \cdot)$ é um *monóide*. É fácil verificar que o elemento neutro, caso exista, é único. O monóide $(S, \cdot)$ (com elemento neutro e) diz-se um *grupo* se todo o elemento de S tiver inverso, isto é, se a condição

$$\forall a \in S \; \exists b \in S : \quad a \cdot b = b \cdot a = e$$

for satisfeita. Um semigrupo $(S, \cdot)$ diz-se *comutativo* se

$$\forall a, b \in S \quad a \cdot b = b \cdot a.$$

Um grupo comutativo é geralmente designado como grupo *abeliano*.

Um *anel* é uma estrutura algébrica da forma $(R, +, \cdot)$, onde:

- $(R, +)$ é um grupo abeliano;
- $(R, \cdot)$ é um monóide;
- $$\forall a, b, c \in S \quad \begin{array}{l}(\; a \cdot (b + c) = (a \cdot b) + (a \cdot c) \\ \qquad \wedge \; (b + c) \cdot a = (b \cdot a) + (c \cdot a) \;).\end{array}$$

A propriedade expressa pela terceira condição é designada por *distributividade*. Os elementos neutros da soma e do produto são designados por 0 e 1 respectivamente. É habitual escrever ab em vez de $a \cdot b$. Um anel com um único elemento diz-se *trivial*. é fácil ver que um anel é não-trivial se e só se $1 \neq 0$. A menos que se diga o contrário, todos os anéis considerados neste curso são não-triviais. Em geral, para simplificar notação, representamos um anel $(R, +, \cdot)$ pelo conjunto R simplesmente.

Exemplo 1.1 *Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, com as operações usuais de soma e produto, são anéis.*

Exemplo 1.2 *Anéis de matrizes*

Seja R um anel e $n \in N$. Designamos por $M_n(R)$ o conjunto de todas as matrizes $n \times n$ com entradas em R. Com a soma e produto usuais de matrizes, $M_n(R)$ constitui um anel. Relembramos que os elementos de $M_n(R)$ se podem representar na forma $a = (a_{ij})$, onde i, j tomam valores no conjunto $\{1, \ldots, n\}$. Soma e produto podem então ser definidas através das expressões

$$(a + b)_{ij} = a_{ij} + b_{ij},$$

$$(ab)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Designamos por ε_{ij} a matriz em $M_n(R)$ cuja entrada (i, j) é 1, sendo as restantes 0. É claro que

$$a = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} \varepsilon_{ij}$$

para toda a matriz $a \in M_n(R)$. □

Exemplo 1.3 *Anéis de polinómios*

Seja R um anel. O anel dos polinómios em x com coeficientes em R, designado por $R[x]$, consiste em todas as somas formais do tipo $\sum_{i \geq 0} r_i x^i$ ($r_i \in R$) tais que apenas um número finito de coeficientes r_i são diferentes de 0; soma e produto são definidas por

$$(\sum_{i \geq 0} r_i x^i) + (\sum_{i \geq 0} s_i x^i) = \sum_{i \geq 0} (r_i + s_i) x^i,$$

$$(\sum_{i\geq 0} r_i x^i)(\sum_{i\geq 0} s_i x^i) = \sum_{i\geq 0}\sum_{j\geq 0}(r_i s_j)x^{i+j}.$$

O coeficiente (não nulo) do termo de maior grau é designado por *coeficiente-guia*. □

Exemplo 1.4 *Anéis de grupo*

Seja R um anel e G um grupo . O anel de grupo $R[G]$ consiste em todas as somas formais do tipo $\sum_{g\in G} r_g g$ ($r_g \in R$) tais que apenas um número finito de coeficientes r_g são diferentes de 0; soma e produto são definidas por

$$(\sum_{g\in G} r_g g) + (\sum_{g\in G} s_g g) = \sum_{g\in G}(r_g + s_g)g,$$

$$(\sum_{g\in G} r_g g)(\sum_{g\in G} s_g g) = \sum_{g\in G}\sum_{h\in G}(r_g s_h)(gh).$$

□

Um anel diz-se *comutativo* se o produto for comutativo. Um anel satisfazendo a condição

$$ab = 0 \Rightarrow (a = 0 \vee b = 0)$$

diz-se um *domínio*; um domínio comutativo diz-se um *domínio de integridade*. Um elemento $r \in R$ diz-se *invertível à esquerda* (respectivamente *à direita*) se existir $b \in R$ tal que $ba = 1$ (respectivamente $ab = 1$). Dizemos que r é *invertível* se existir $b \in R$ tal que $ab = ba = 1$. Se todos os elementos de $R\backslash\{0\}$ forem invertíveis (o que equivale a $(R\backslash\{0\}, \cdot)$ constituir um grupo), dizemos que R é um *anel de divisão*. Um anel de divisão comutativo diz-se um *corpo*.

Seja $S \subseteq R$. Dizemos que S é um *subanel* de R se $0, 1 \in S$ e S constitui um anel com as operações induzidas de R. A condição sobre as operações induzidas equivale a exigir que

$$a, b \in S \Rightarrow a + b, -a, ab \in S.$$

Uma função $\varphi : R \to S$ entre anéis R e S diz-se um *homomorfismo* (de anéis) se

- $1\varphi = 1$

- $(a+b)\varphi = a\varphi + b\varphi$
- $(ab)\varphi = a\varphi\, b\varphi$

para todos $a, b \in R$.

Um subgrupo aditivo L de um anel R diz-se um *ideal à esquerda* de R se

$$\forall r \in R\, \forall x \in L \quad rx \in L.$$

Nesse caso escrevemos $L \trianglelefteq_e R$. Dualmente, definimos *ideal à direita* com a notação $L \trianglelefteq_d R$. Se $L \subseteq R$ é simultaneamente ideal à esquerda e à direita de R, dizemos que L é um *ideal* de R e escrevemos $L \trianglelefteq R$.

Introduzimos agora um poderoso axioma da teoria de conjuntos que desempenhará um papel importante ao longo do curso: o Axioma da Escolha, sob a forma habitualmente conhecida por Lema de Zorn:

Axioma 1.5 *Seja $(X, \leq)$ um conjunto parcialmente ordenado não vazio em que toda a cadeia (subconjunto de X em que todos os elementos são comparáveis) admite um majorante (elemento de X que é maior ou igual que todos os elementos da cadeia). Então $(X, \leq)$ tem elementos maximais.*

Um exemplo de aplicação do Lema de Zorn no contexto da Teoria de Anéis é dado pelo seguinte resultado. Um ideal (respectivamente ideal à esquerda, à direita) diz-se *maximal* se for próprio e não estiver contido em nenhum outro ideal (respectivamente ideal à esquerda, à direita) próprio de R.

Teorema 1.6 *Todo o anel tem ideais (respectivamente ideais à esquerda, à direita) maximais.*

Dem. Seja R um anel. Então R tem ideais próprios (pelo menos $\{0\}$). Consideremos o conjunto dos ideais próprios de R (parcialmente) ordenado pela inclusão. Se $(A_i)_{i\in I}$ é uma cadeia de ideais próprios de R, então $\cup_{i\in I} A_i$ é ainda um ideal próprio de R (note-se que $1 \notin \cup_{i\in I} A_i$), logo a cadeia é majorada e R tem ideais maximais pelo Lema de Zorn.

Os outros casos são análogos. □

Seja R um anel. Definimos um R-módulo (à esquerda) como sendo um grupo abeliano M munido de uma operação $R \times M \to M$ (designada por produto escalar) tal que

- $r(x + x') = rx + rx'$
- $(r + r')x = rx + r'x$
- $r(r'x) = (rr')x$
- $1x = x$

para todos $r, r' \in R$ e $x, x' \in M$. Dualmente, define-se R-módulo *à direita*, com o produto escalar $M \times R \to M$. Ao longo do curso, concentraremos as nossas atenções nos módulos à esquerda, omitindo os resultados análogos para módulos à direita.

Exemplo 1.7 *Um anel R é R-módulo à esquerda e à direita de si próprio, com o produto escalar igual ao produto de R. Os seus submódulos são então, respectivamente, os ideais à esquerda e os ideais à direita.*

Exemplo 1.8 *Os módulos sobre um corpo F são precisamente os espaços vectoriais sobre F.*

Exemplo 1.9 *Os $\mathbb{Z}$-módulos são essencialmente os grupos abelianos, pois todo o grupo abeliano tem subjacente uma estrutura natural de $\mathbb{Z}$-módulo.*

Dado um R-módulo M, dizemos que $N \subseteq M$ é um *submódulo* de M se

- N é um subgrupo aditivo de M;
- $\forall r \in R \, \forall x \in N \quad rx \in N$.

Então N é ele próprio um R-módulo e escrevemos $N \leq M$. Caso $N \neq M$, o submódulo N diz-se *próprio* e escrevemos $N < M$.

Sejam M e N R-módulos. Uma função $\varphi : M \to N$ diz-se um *homomorfismo* (de R-módulos) se

- $(x + y)\varphi = x\varphi + y\varphi$
- $(rx)\varphi = r(x\varphi)$

para todos $x, y \in M$ e $r \in R$. Analogamente se define homomorfismo de R-módulos à direita. Se $N = M$, dizemos que φ é um *endomorfismo* de M. Dizemos que o homomorfismo $\varphi : M \to N$ é um *isomorfismo* se for invertível. É fácil de ver que um homomorfismo é um isomorfismo se e só se for bijectivo. Se existir um isomorfismo entre dois R-módulos M e N, escrevemos $M \cong N$ e dizemos que M e N são *isomorfos*.

Dado um homomorfismo (de R-módulos) $\varphi : M \to N$, definimos o *núcleo* de φ como sendo $\text{Ker}\varphi = 0\varphi^{-1}$. É imediato que $\text{Ker}\varphi \leq M$.

Dado um submódulo N de um R-módulo M, designamos por M/N o conjunto dos subconjuntos de M da forma $x+N$. Estes subconjuntos definem uma partição de M. Definimos uma estrutura de R-módulo em M/N através de

$$(x + N) + (y + N) = (x + y) + N,$$
$$r(x + N) = rx + N.$$

Os detalhes ficam como exercício. Dizemos que M/N é o módulo *quociente* de M por N. Analogamente se define o quociente de um anel por um seu ideal. É imediato que a projecção

$$\begin{array}{rcl} \varphi : M & \to & M/N \\ x & \mapsto & x + N \end{array}$$

é um homomorfismo com núcleo N, logo os núcleos de homomorfismos de domínio M são precisamente os submódulos de M.

Teorema 1.10 *Seja $\varphi : M \to M'$ um homomorfismo de R-módulos e seja $N \leq Ker\varphi$. Então a função $\Phi : M/N \to M'$ definida por $(x + N)\Phi = x\varphi$ é um homomorfismo. Além disso, se φ for sobrejectiva e $N = Ker\varphi$, então Φ é um isomorfismo.*

Dem. Exercício. □

Corolário 1.11 *Seja M um R-módulo. Se $M_1, M_2 \leq M$, então $M_1 + M_2$, $M_1 \cap M_2 \leq M$ e*

$$(M_1 + M_2)/M_2 \cong M_1/(M_1 \cap M_2).$$

Dem. Exercício. □

Corolário 1.12 *Seja M um R-módulo. Se $K \leq N \leq M$, então $N/K \leq M/K$ e*

$$(M/K)/(N/K) \cong M/N.$$

Dem. Exercício. □

Estes resultados são genericamente conhecidos como os teoremas do homomorfismo e do isomorfismo.

Dado um R-módulo (à esquerda) M, designamos por $\mathrm{End}_R M$ o conjunto dos endomorfismos de M. Considerando as operações de soma e composição de funções em $\mathrm{End}_R M$, obtemos uma estrutura de anel, ficando a verificação dos detalhes como exercício. Analogamente, dado um R-módulo à direita M, designamos por $\mathrm{End}M_R$ o conjunto dos endomorfismos de M. Considerando as operações de soma e a operação dual da composição de funções em $\mathrm{End}M_R$, obtemos também uma estrutura de anel.

Dado um subconjunto X de um R-módulo M, designamos por RX o conjunto de todos os elementos de R da forma

$$r_1x_1 + r_2x_2 + \ldots + r_nx_n,$$

onde $n \geq 0$, $r_i \in R$ e $x_i \in X$ para $i = 1, \ldots, n$. É um exercício simples mostrar que RX é um submódulo de M, de facto o *menor* submódulo de M contendo X. Dizemos que RX é o submódulo de M *gerado* por X. Dado $N \leq M$, dizemos que $X \subseteq M$ *gera* N se $N = RX$. Dizemos que N é

- *finitamente gerado* se $N = RX$ para algum subconjunto finito X de M;
- *cíclico* se $N = Rx$ para algum $x \in X$.

No caso particular dos ideais à esquerda gerados por um único elemento, usa-se a terminologia *ideal à esquerda principal*.

Um subconjunto X de M diz-se *independente* se

$$r_1x_1 + \ldots + r_nx_n = 0 \quad \Rightarrow \quad r_1 = \ldots = r_n = 0$$

para quaisquer $r_1, \ldots, r_n \in R$ e $x_1, \ldots, x_n \in X$ distintos. Dizemos que X é uma *base* de M se X for independente e gerar M. O R-módulo M diz-se *livre* se tiver uma base. A propriedade seguinte é geralmente referida como a *propriedade universal*.

Teorema 1.13 *Seja M um R-módulo com base X. Seja N um R-módulo e $\varphi : X \to N$ uma função. Então existe um e um só homomorfismo $\Phi : M \to N$ tal que $\Phi\,|_X = \varphi$.*

Dem. Exercício. □

É muito fácil mostrar que nem todos os R-módulos são livres (por exemplo, um grupo abeliano finito não-trivial não é livre enquanto $\mathbb{Z}$-módulo) mas a situação simplifica-se no caso dos anéis de divisão:

Teorema 1.14 *Seja M um módulo sobre um anel de divisão D. As condições seguintes são equivalentes para um subconjunto X de M:*

(i) X é um subconjunto gerador minimal de M;

(ii) X é um subconjunto independente maximal de M;

(iii) X é uma base de M.

Dem. (i) $\Rightarrow$ (ii). Seja X um subconjunto gerador minimal de M. Suponhamos que $d_1x_1 + \ldots + d_nx_n = 0$ com $d_i \in D$ e $x_i \in X$ distintos. Se $d_j \neq 0$ para algum j, então $d_jx_j \in D(X\backslash\{x_j\})$ e logo

$$x_j = d_j^{-1}d_jx_j \in D(X\backslash\{x_j\}),$$

o que implica $M = DX = D(X\backslash\{x_j\})$, contradizendo (i). Logo X é independente. Como X gera M, é imediato que X é maximal.

(ii) $\Rightarrow$ (i). Seja X um subconjunto independente maximal de M. Seja $y \in M$. Vamos mostrar que $y \in DX$. Se $y \in X$, é imediato. Caso contrário, $X \cup \{y\}$ é dependente e resulta da independência de X que $dy \in DX$ para algum $d \in D\backslash\{0\}$. Logo $y = d^{-1}dy \in DX$ e concluimos que X gera M. Por outro lado, se $X' \subset X$, resulta da independência de X que $X \not\subseteq DX'$. Logo X' não gera M e X é gerador minimal.

(i),(ii) $\Rightarrow$ (iii). Por definição.

(iii) $\Rightarrow$ (ii). Suponhamos que X é uma base de M. Por definição, X é independente. Seja $y \in M\backslash X$. Como $y \in M = DX$, $X \cup \{y\}$ é dependente e logo X é independente maximal. □

Corolário 1.15 *Seja M um módulo sobre um anel de divisão D. Então M é livre.*

Dem. Pelo resultado anterior, basta mostrar que M tem um subconjunto independente maximal, o que resulta facilmente do Lema de Zorn. □

Mostramos a seguir que duas bases de um módulo sobre um anel de divisão têm necessariamente a mesma cardinalidade.

Teorema 1.16 *Seja M um módulo sobre um anel de divisão. Se X e Y são bases de M, então $|X| = |Y|$.*

Dem. Vamos provar apenas o caso em que o módulo é finitamente gerado, usando indução sobre a cardinalidade mínima n de uma base de M. Como o caso $n = 0$ ($M = \{0\}$) é trivial, assumimos que $|X| = n > 0$ é uma base de M de cardinalidade mínima e que o resultado é válido para módulos com bases de cardinalidade inferior. Sejam $X = \{x_1, \ldots, x_n\}$ e $Y = \{y_1, \ldots, y_m\}$. Dado $d \in D\backslash\{0\}$, temos que $\{dy_1, \ldots, dy_m\}$ é também uma base de M. Usando este facto, e trocando a ordem dos y_i caso necessário, podemos assumir que $x_1 \in y_1 + N$, onde $N = D(Y\backslash\{y_1\})$. Para cada $i = 2, \ldots, n$, suponhamos que $x_i \in \lambda_i y_1 + N$. Note-se que $x_1 \notin N$, caso contrário $y_1 \in N$ e Y não seria independente. É um exercício simples mostrar que

$$X' = \{x_2 - \lambda_2 x_1, \ldots, x_n - \lambda_n x_1\}$$

é uma base de N. Como $|X'| = n-1$ e $\{y_2, \ldots, y_m\}$ é claramente uma base de N, resulta da hipótese de indução que $n-1 = m-1$. Logo $|Y| = m = n = |X|$ e o teorema é válido. □

A cardinalidade de uma base de um D-módulo livre (D anel de divisão) diz-se a *dimensão* de M (sobre D) e é designada por $[M : D]$.

Teorema 1.17 *Se $\{x_1, \ldots, x_n\}$ é uma base do R-módulo M, então $End_R M \cong M_n(R)$.*

Dem. Definimos uma função $\varphi : M_n(R) \to \mathrm{End}_R M$ do seguinte modo: dada uma matriz $a = (a_{ij}) \in M_n(R)$, então $a\varphi$ é o endomorfismo de M definido por

$$x_i(a\varphi) = \sum_{j=1}^{n} a_{ij} x_j$$

para $i = 1, \ldots, n$. Pela propriedade universal dos módulos livres, a função φ está bem definida.

Os restantes detalhes ficam como exercício. □

Os conceitos envolvidos na definição de base podem ser generalizados do seguinte modo. Seja M um R-módulo. Dada uma família $(M_i)_{i\in I}$ de submódulos de M, é claro que $\cap_{i\in I} M_i$ é o maior submódulo de M contido em todos os M_i. Seja $\sum_{i\in I} M_i$ o conjunto de todos os elementos de M da forma $x_{j_1} + \ldots + x_{j_n}$ com $n \geq 0$, $j_i \in I$ e $x_{j_i} \in M_{j_i}$ para $i = 1, \ldots, n$. É fácil de ver que $\sum_{i\in I} M_i$ é o menor submódulo de M que contém todos os M_i. Estas duas operações definem o *supremo* e o *ínfimo* no conjunto dos submódulos de M, parcialmente ordenado pela relação de inclusão. Um conjunto parcialmente ordenado onde existem sempre o supremo e o ínfimo de dois elementos diz-se um *reticulado*, pelo que é habitual falar do reticulado dos submódulos de um módulo.

Dizemos que a família $(M_i)_{i\in I}$ de submódulos de M é *independente* se

$$M_i \cap \sum_{j\in I\setminus\{i\}} M_j = 0$$

para todo $i \in I$. Se $M = \sum_{i\in I} M_i$ e $(M_i)_{i\in I}$ é independente, dizemos que M é *soma directa* dos submódulos M_i e escrevemos

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

Em particular, se X for uma base de M, temos $M = \oplus_{x\in X} Rx$.

É frequente usar a notação de soma directa num contexto mais geral, que descrevemos a seguir. Dada uma família $(M_i)_{i\in I}$ de R-módulos, seja $\prod_{i\in I} M_i$ o *produto directo* dos módulos M_i. O produto $\prod_{i\in I} M_i$ tem uma estrutura natural de R-módulo dada por

$$(x_i)_i + (y_i)_i = (x_i + y_i)_i,$$

$$r(x_i)_i = (rx_i)_i.$$

Designamos por $\oplus_{i\in I} M_i$ o submódulo de $\prod_{i\in I} M_i$ constituído por todos os $(x_i)_i$ tais que $x_i = 0$ para todos os valores de i excepto um número finito. Em particular, tem-se então $M \oplus N = M \times N$.

1.1 APÊNDICE: Anéis de polinómios

Seja $f = r_n x^n + \ldots + r_1 x + r_0 \in R[x]$ (é usual omitir termos em que os coeficientes são nulos). Se $r_n \neq 0$, dizemos que f tem *grau* n, designado pela notação $\mathrm{gr}(f)$. Por convenção, atribuímos ao polinómio nulo $f = 0$ o grau $-\infty$.

Lema 1.18 *Seja D um domínio. Então $D[x]$ é um domínio.*

Dem. Sejam $f, g \in D[x]$ não nulos, digamos

$$f = a_n x^n + \ldots + a_1 x + a_0, \qquad g = b_m x^m + \ldots + b_1 x + b_0$$

com $a_n, b_m \neq 0$. Então $fg = a_n b_m x^{n+m} + h$ para algum $h \in D[x]$ de grau $< n + m$. Como D é um domínio, temos $a_n b_m \neq 0$, logo $fg \neq 0$ e $D[x]$ é um domínio. □

O resultado seguinte generaliza o algoritmo de divisão dos números inteiros ao caso da divisão (à esquerda) de polinómios.

Teorema 1.19 *Seja D um anel de divisão e sejam $f, g \in D[x]$ com $g \neq 0$. Então existem $q, r \in D[x]$ tais que $f = qg + r$ e $gr(r) < gr(g)$. Além do mais, q e r são únicos.*

Dem. Seja

$$Y = \{f - hg \mid h \in D[x]\}.$$

Seja $r \in Y$ de grau mínimo, e seja $q \in D[x]$ tal que $r = f - qg$. Suponhamos que $gr(r) \geq \mathrm{gr}(g)$. Podemos escrever

$$r = r_n x^n + \ldots + r_1 x + r_0 \quad \text{e} \quad g = s_m x^m + \ldots + s_1 x + s_0$$

com $r_n, s_m \neq 0$. Como $n \geq m$, temos $r = r_n s_m^{-1} x^{n-m} g + p$ para algum $p \in D[x]$ com $\mathrm{gr}(p) < n$. Logo

$$p = r - r_n s_m^{-1} x^{n-m} g = f - (q + r_n s_m^{-1} x^{n-m}) g \in Y,$$

contradizendo a minimalidade de $\mathrm{gr}(r)$. Logo $\mathrm{gr}(r) < \mathrm{gr}(g)$.

Suponhamos agora que $f = q_1 g + r_1 = q_2 g + r_2$ com $\mathrm{gr}(r_1), \mathrm{gr}(r_2) < \mathrm{gr}(g)$. Então $(q_1 - q_2)g = r_2 - r_1$. Se $q_1 - q_2 \neq 0$, resulta imediatamente que

$$\mathrm{gr}(r_2 - r_1) = \mathrm{gr}(q_1 - q_2) + \mathrm{gr}(g) \geq \mathrm{gr}(g),$$

contradizendo $\mathrm{gr}(r_1), \mathrm{gr}(r_2) < \mathrm{gr}(g)$. Logo $q_1 = q_2$ e consequentemente $r_1 = r_2$, provando a unicidade. □

A demonstração anterior contém de facto o princípio de um algoritmo que permite calcular efectivamente q e r. Sejam

$$f = a_n x^n + \ldots + a_1 x + a_0 \quad \text{e} \quad g = b_m x^m + \ldots + b_1 x + b_0$$

com $a_n, b_m \neq 0$. Se $\text{gr}(f) < \text{gr}(g)$, tomamos $q = 0$ e $r = f$. Se $\text{gr}(f) \geq \text{gr}(g)$, escrevemos

$$f = a_n b_m^{-1} x^{n-m} g + p$$

para algum $p \in D[x]$ com $\text{gr}(p) < \text{gr}(f)$, e reduzimos o problema da divisão de f por g à divisão de p por g. Como o grau dos dividendos não pode diminuir indefinidamente, o algoritmo acaba por terminar ao fim de um número finito de passos.

Observamos também que, de forma dual, podemos considerar a divisão à direita $f = gq' + r$, sendo tudo absolutamente análogo ao caso da divisão à esquerda.

Um domínio D diz-se um *domínio de ideais à esquerda principais* se todo o ideal à esquerda de D for principal, ou seja, da forma Da, para algum $a \in D$.

Teorema 1.20 *Seja D um domínio. Então $D[x]$ é um domínio de ideais à esquerda principais.*

Dem. Seja $R = D[x]$ e $L \trianglelefteq_e R$. Se $L = 0$, temos $L = R0$ trivialmente, logo podemos assumir que $L \neq 0$. Seja $g \in L \backslash \{0\}$ de grau mínimo. É claro que $Rg \subseteq L$. Reciprocamente, seja $f \in L$. Pelo algoritmo de divisão, existem $q, r \in R$ tais que $f = qg + r$ e $\text{gr}(r) < \text{gr}(g)$. Como $r = f - qg \in L$, resulta da minimalidade de $\text{gr}(g)$ que $r = 0$. Logo $f = qg \in Rg$ e $L = Rg$. Logo $D[x]$ é um domínio de ideais à esquerda principais. $\square$

Uma simples adaptação da demonstração permite demonstrar que $\mathbb{Z}$ é também um domínio de ideais à esquerda principais.

1.2 APÊNDICE: $\mathbb{Z}$-módulos finitamente gerados

Vamos investigar a estrutura dos $\mathbb{Z}$-módulos finitamente gerados. Principiamos por apresentar alguns lemas de grande utilidade.

Lema 1.21 *Seja M um $\mathbb{Z}$-módulo livre sobre $\{x_1, \ldots, x_n\}$ e seja $N \leq M$. Então N é livre e tem uma base de cardinalidade $\leq n$.*

Dem. Vamos usar indução sobre n. O caso $n = 0$ é obviamente trivial, logo assumimos que $n > 0$ e que o resultado é válido para dimensões inferiores. Seja

$$M' = \oplus_{i=2}^{n} \mathbb{Z}x_i.$$

É claro que $M = \mathbb{Z}x_1 \oplus M'$. Definimos $N' = N \cap M'$. Como M' é um $\mathbb{Z}$-módulo livre sobre $\{x_2, \ldots, x_n\}$ e $N' \leq M'$, resulta da hipótese de indução que N' é livre e tem uma base $\{y_1, \ldots, y_k\}$ com $k \leq n-1$. Se $N \subseteq M'$, a situação está trivialmente resolvida, logo assumimos que $N \not\subseteq M'$. Então existe $y_0 = rx_1 + a \in N$ com $r \in \mathbb{Z}\backslash\{0\}$ e $a \in M'$. Podemos assumir que $r > 0$ e é mínimo entre os possíveis elementos de $\mathbb{N}$.

Vejamos que N é gerado por $\{y_0, y_1, \ldots, y_k\}$. Dado $z \in N$, podemos escrever $z = sx_1 + b$ com $s \in \mathbb{Z}$ e $b \in M'$. Podemos assumir sem perda de generalidade que $s \geq 0$. Podemos escrever $s = qr + t$ com $q \geq 0$ e $0 \leq t < r$. Como $z - qy_0 \in N$ é da forma $tx_1 + (b - qa)$, temos que $t > 0$ contradiria a minimalidade de r. Logo $t = 0$ e portanto

$$z - qy_0 = b - qa \in N \cap M' = N' = \oplus_{j=1}^{k-1} \mathbb{Z}y_j,$$

o que prova que $z \in \mathbb{Z}y_0 + (\oplus_{j=1}^{k-1} \mathbb{Z}y_j)$. Logo N é gerado por $\{y_0, y_1, \ldots, y_k\}$.

Suponhamos agora que $p_0y_0 + p_1y_1 + \ldots + p_ky_k = 0$ para alguns $p_0, \ldots, p_k \in \mathbb{Z}$. Então

$$0 \in p_0y_0 + M' = p_0rx_1 + M'$$

e logo $p_0rx_1 \in M'$, implicando $p_0 = 0$ pois $r \neq 0$. Daqui resulta que $p_1y_1 + \ldots + p_ky_k = 0$ e a independência de $\{y_1, \ldots, y_k\}$ garante que $p_1 = \ldots = p_k = 0$. Logo $\{y_0, y_1, \ldots, y_k\}$ é independente e consequentemente uma base de N. Como $k + 1 \leq n$, o resultado está demonstrado por indução. □

Lema 1.22 *Seja M um $\mathbb{Z}$-módulo finitamente gerado e seja*

$$M_f = \{a \in M \mid ka = 0 \text{ para algum } k \in \mathbb{N}\}.$$

Então M_f é um submódulo finito de M.

Dem. É um simples exercício mostrar que $M_f \leq M$. Consideremos um homomorfismo sobrejectivo $\varphi : P \to M$, onde P é um $\mathbb{Z}$-módulo livre. Como M é finitamente gerado, podemos assumir que P é finitamente gerado. Como $M_f\varphi^{-1} \leq P$, resulta do lema anterior que $M_f\varphi^{-1}$ é finitamente gerado. Logo

também $M_f = (M_f\varphi^{-1})\varphi$ é finitamente gerado. Podemos então escrever $M_f = \mathbb{Z}x_1 + \ldots \mathbb{Z}x_n$ para alguns $x_1, \ldots, x_n \in M_f$. Como $x_1, \ldots, x_n \in M_f$, existe $k \in \mathbb{N}$ tal que $kx_1 = \ldots = kx_n = 0$. Logo

$$M_f = \{0, \ldots, k-1\}x_1 + \ldots + \{0, \ldots, k-1\}x_n$$

e consequentemente M_f é finito. □

Podemos agora demonstrar o seguinte resultado:

Teorema 1.23 *Seja M um $\mathbb{Z}$-módulo finitamente gerado. Então existe $N \leq M$ livre sobre uma base finita tal que $M = N \oplus M_f$.*

Dem. Seja $M' = M/M_f$. Como M é finitamente gerado, M' é finitamente gerado. Seja S um conjunto gerador (finito) de M'. Tomamos um subconjunto independente maximal $S' = \{x'_1, \ldots, x'_n\}$ de S e definimos N' como sendo o submódulo de M' gerado por S'. É claro que N' é livre de base S'.

Dado $y \in S\backslash S'$, temos $ky + k_1x'_1 + \ldots + k_nx'_n = 0$ para alguns $k, k_1, \ldots, k_n \in \mathbb{Z}$ não todos os nulos, caso contrário S' não seria maximal entre os subconjuntos independentes de S. Além disso, S' independente implica que $k \neq 0$. Como S é finito, concluimos que existe algum $k \in \mathbb{N}$ tal que $k(S\backslash S') \subseteq N'$ e consequentemente $kM' \leq N'$. Como N' é um $\mathbb{Z}$-módulo livre, resulta do Lema 1.21 que kM' é livre sobre uma base finita.

Seja

$$\begin{array}{rcl} \varphi : M' & \to & kM' \\ y' & \mapsto & ky'. \end{array}$$

É claro que φ é um homomorfismo sobrejectivo de $\mathbb{Z}$-módulos. Se $y'\varphi = 0$ para $y' = y + M_f$ então $ky + M_f = M_f$ e portanto $ky \in M_f$. Logo $rky = 0$ para algum $r \in \mathbb{N}$ e concluimos que $y \in M_f$, isto é, $y' = 0$. Logo φ é um isomorfismo de $\mathbb{Z}$-módulos, o que implica em particular que M' é livre sobre uma base finita, digamos $\{z_1 + M_f, \ldots, z_r + M_f\}$.

Seja N o submódulo de M gerado por $\{z_1, \ldots, z_r\}$. Como a independência de $\{z_1 + M_f, \ldots, z_r + M_f\}$ implica claramente a independência de $\{z_1, \ldots, z_r\}$, concluimos que N é livre de base $\{z_1, \ldots, z_r\}$. Falta mostrar que $M = N \oplus M_f$. Seja $a \in M$. Então

$$a + M_f = k_1(z_1 + M_f) + \ldots + k_r(z_r + M_f)$$

para alguns $k_1, \ldots, k_r \in \mathbb{Z}$. Logo $a = k_1z_1 + \ldots + k_rz_r + b$ para algum $b \in M_f$ e $a \in N + M_f$. Logo $M = N + M_f$. Finalmente, suponhamos que $a \in N \cap M_f$,

digamos $a = k_1 z_1 + \ldots + k_r z_r$. Como $a \in M_f$, temos $ka = 0$ para algum $k \in \mathbb{N}$. Logo $kk_1 z_1 + \ldots + kk_r z_r = 0$. Como $\{z_1, \ldots, z_r\}$ é independente, isto implica $kk_1 = \ldots = kk_r = 0$ e consequentemente $k_1 = \ldots = k_r = 0$. Logo $a = 0$, pelo que $N \cap M_f = 0$ e $M = N \oplus M_f$. $\square$

É possível mostrar (embora não o façamos neste curso) que todo o $\mathbb{Z}$-módulo finito é isomorfo a um produto directo da forma $(\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_n\mathbb{Z})$ para alguns $m_1, \ldots, m_n \geq 2$. Como todo o $\mathbb{Z}$-módulo livre sobre uma base finita é a menos de isomorfismo um produto da forma $\mathbb{Z} \times \ldots \times \mathbb{Z}$, daqui resulta o seguinte:

Teorema 1.24 *A menos de isomorfismo, todo o $\mathbb{Z}$-módulo finitamente gerado é isomorfo a um produto directo da forma*

$$\mathbb{Z} \times \ldots \times \mathbb{Z} \times (\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_n\mathbb{Z}),$$

com $m_1, \ldots, m_n \geq 2$.

Note-se que na expressão anterior podem estar omissos os factores de qualquer um dos tipos.

1.3 Exercícios

1.1. Um anel R diz-se booleano se todos os seus elementos forem idempotentes (isto é, se $a^2 = a$ para todo $a \in R$). Mostre que um anel booleano é comutativo e satisfaz $a + a = 0$ para todo $a \in R$.

1.2. Seja G um grupo abeliano e seja $\mathrm{End}(G)$ o conjunto dos endomorfismos de G.

   a) Mostre que $(\mathrm{End}(G), +, \circ)$ é um anel.

   b) Dado um anel R, mostre que G admite uma estrutura de R-módulo à direita se e só se existe um homomorfismo de anéis $\varphi : R \to \mathrm{End}(G)$.

1.3. Mostre que se todo o elemento não nulo de um anel R é invertível à esquerda então R é um anel de divisão.

1.4. Seja R um anel e G um grupo. Mostre que $R[G]$ é um anel de divisão se e só se R é um anel de divisão e G é trivial.

1.5. Seja K um corpo. Dizemos que $f \in K[x]\backslash K$ é irredutível se e só se f não é produto de polinómios de grau inferior. Dado $f \in K[x]\backslash K$, mostre que $K[x]/(fK[x])$ é um corpo se e só se f for irredutível.

1.6. Seja C um anel comutativo tal que todo o ideal de C é um C-módulo livre. Mostre que C é um domínio de ideais principais.

1.7. Mostre que um submódulo de um módulo livre não é necessariamente livre (*Sugestão*: considere o anel $\mathbb{Z} \times \mathbb{Z}$).

1.8. Sejam $m, n \in \mathbb{N}$. Mostre que os anéis $\mathbb{Z}/mn\mathbb{Z}$ e $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ são isomorfos se e só se $(m, n) = 1$.

2 ANÉIS PRIMITIVOS E ANÉIS PRIMOS

Uma das abordagens clássicas no estudo da teoria de anéis consiste em estudar inicialmente uma classe particular de anéis ditos primitivos. Em seguida, considera-se uma classe mais geral, os anéis ditos semiprimitivos. Finalmente, estuda-se o radical de Jacobson de um anel R, o menor ideal J de R tal que R/J é semiprimitivo.

Um R-módulo M diz-se *simples* se não tiver submódulos próprios não nulos. Analogamente, um anel R diz-se *simples* se não tiver ideais próprios não nulos.

Lema 2.1 *Todo o anel de divisão é simples.*

Dem. Exercício. □

Dado um subconjunto S de um R-módulo M, definimos o *aniquilador* de S como sendo

$$\mathrm{Ann}_R S = \{r \in R \mid rS = 0\}.$$

É imediato que $\mathrm{Ann}_R M$ é um ideal de R. Se $\mathrm{Ann}_R M = 0$, dizemos que M é um R-módulo *fiel*. Por exemplo, R é um R-módulo fiel.

Um anel R diz-se *primitivo* se existir um R-módulo simultaneamente simples e fiel.

Teorema 2.2 *Todo o anel simples é primitivo.*

Dem. Seja R um anel simples. Pelo Teorema 1.6, R tem um ideal à esquerda maximal L. Então L é um submódulo do R-módulo R e podemos considerar o R-módulo quociente R/L.

É um exercício elementar mostrar que o R-módulo R/L é simples. Como $\mathrm{Ann}_R(R/L) \trianglelefteq R$, $1 \notin \mathrm{Ann}_R(R/L)$ e R é simples, resulta que $\mathrm{Ann}_R(R/L) = 0$ e logo R/L é também fiel. Logo R é primitivo. □

Lema 2.3 *Seja M um R-módulo não nulo. Então M é simples se e só se $M \cong R/L$ para algum ideal à esquerda maximal L de R.*

Dem. Suponhamos que M é simples e fixemos $x \in M\backslash\{0\}$. Consideremos o homomorfismo

$$\begin{array}{rccc} \varphi : R & \rightarrow & M \\ r & \mapsto & rx \end{array}$$

Como M é simples e $R\varphi$ é um submódulo não nulo de M, resulta que φ é sobrejectivo. Logo $M \cong R/\mathrm{Ker}\varphi$ pelo Teorema do Homomorfismo. É claro que $\mathrm{Ker}\varphi \lhd_e R$. Vejamos que $\mathrm{Ker}\varphi$ é maximal. Suponhamos que $\mathrm{Ker}\varphi \subset L'$ para algum $L' \lhd_e R$. Então $0 < L'\varphi \leq M$, logo $M = L'\varphi$ pois M é simples. Em particular, $x = ax$ para algum $a \in L'$ e logo

$$1 = (1-a) + a \in \mathrm{Ker}\varphi + L' = L',$$

contradizendo $L' \lhd_e R$. Conclui-se assim que $\mathrm{Ker}\varphi$ é maximal.

A implicação recíproca já foi observada na demonstração do teorema anterior. □

Uma caracterização alternativa dos anéis primitivos é dada pelo seguinte resultado.

Teorema 2.4 *Um anel R é primitivo se e só se existe $L \lhd_e R$ tal que $L + A = R$ para todo o ideal não nulo A de R.*

Dem. Suponhamos que R é primitivo. Então R tem um módulo simples e fiel M. Pelo lema anterior, podemos assumir que $M = R/L$ para algum $L \lhd_e R$ maximal. Seja $0 \neq A \lhd R$. Como M é fiel, temos $\mathrm{Ann}_R M = 0$. Dado $a \in A\backslash\{0\}$, resulta que $a \notin \mathrm{Ann}_R M$ e logo $ar + L = a(r+L) \neq L$ para algum $r \in R$. Como $ar \in A$, conclui-se que $A \not\subseteq L$. Como $L \subset L + A \trianglelefteq_e R$, resulta da maximalidade de L que $L + A = R$.

Reciprocamente, se existe $L \lhd_e R$ tal que $L + A = R$ para todo o ideal não nulo A de R, podemos pelo Lema de Zorn tomar $L' \lhd_e R$ maximal tal que $L \subseteq L'$. Pelo lema anterior, R/L' é simples. Suponhamos que $\mathrm{Ann}_R(R/L') \neq 0$. Como $\mathrm{Ann}_R(R/L') \trianglelefteq R$, obtemos $L + \mathrm{Ann}_R(R/L') = R$. Como $L, \mathrm{Ann}_R(R/L') \subseteq L'$, obtemos $L' = R$, absurdo, pois L' é maximal. Logo $\mathrm{Ann}_R(R/L') = 0$ e R/L' é fiel. Logo R é primitivo. □

Corolário 2.5 *Seja R um anel comutativo. Então R é primitivo se e só se R for um corpo.*

Dem. Suponhamos que R é primitivo. Pelo teorema anterior existe $L \lhd_e R$ tal que $L + A = R$ para todo o ideal não nulo A de R. Como R é comutativo, L é ele próprio um ideal de R. Como $L + L = L \subset R$, concluimos que $L = 0$. Mas então $R = L + A = A$ para todo o ideal não nulo A de R, logo o único ideal não nulo de R é o próprio R. Em particular, $Ra = R$ para todo $a \in R\backslash\{0\}$ e logo R é um corpo.

A implicação recíproca é imediata. □

Pretendemos obter uma caracterizção estrutural dos anéis primitivos, relacionando-os com anéis da forma $\mathrm{End}M_D$. O resultado seguinte, conhecido como Lema de Schur, permite-nos seleccionar o anel de divisão apropriado.

Lema 2.6 *Se M é um R-módulo simples, então $D = End_R M$ é um anel de divisão.*

Dem. Seja $\varphi \in D\backslash\{0\}$. Então $\mathrm{Ker}\varphi < M$, logo $\mathrm{Ker}\varphi = 0$ pois M é simples. Logo φ é injectivo. Temos também $0 \neq M\varphi \leq M$, logo M simples implica também que $M\varphi = M$ e logo φ é um isomorfismo. mas então $\varphi^{-1} \in D$ e portanto D é um anel de divisão. □

Seja D um anel de divisão e seja M um D-módulo à direita. Dado um subanel R de $\mathrm{End}M_D$, podemos ver M como um R-módulo (à esquerda) através da acção

$$\begin{array}{rcl} R \times M & \to & M \\ (\varphi, x) & \mapsto & x\varphi \end{array}$$

Dizemos que R é um subanel *denso* de $\mathrm{End}M_D$ se, dado um subconjunto $\{x_1, \ldots, x_n\} \subseteq M$ D-independente, se tem: para todos $y_1, \ldots, y_n \in M$, existe $r \in R$ tal que $rx_i = y_i$ para $i = 1, \ldots, n$.

Vamos agora demonstrar o famoso Teorema da Densidade de Jacobson:

Teorema 2.7 *As condições seguintes são equivalentes para um anel R:*

(i) R é primitivo;

(ii) R é isomorfo a um subanel denso de $EndM_D$, onde D designa um anel de divisão e M um D-módulo à direita.

Dem. (i) $\Rightarrow$ (ii). Suponhamos que R tem um módulo simples e fiel M. Pelo Lema de Schur, $D = \mathrm{End}_R M$ é um anel de divisão. É um simples exercício verificar que

$$\begin{array}{rcl} \rho : R & \to & \mathrm{End}M_D \\ r & \mapsto & \rho_r, \end{array}$$

onde

$$\begin{array}{rcl} \rho_r : M & \to & M \\ x & \mapsto & rx, \end{array}$$

é um homomorfismo de anéis que se diz a *representação regular* de R. Além disso,

$$\mathrm{Ker}\rho = \{r \in R \mid rM = 0\} = \mathrm{Ann}_R M = 0,$$

logo ρ é injectivo e R é isomorfo ao subanel $R\rho$ de $\mathrm{End}M_D$. Por comodidade de notação, identificamos R com $R\rho$. Vamos mostrar que R é denso em $\mathrm{End}M_D$ usando indução sobre o cardinal n de um subconjunto $\{x_1, \ldots, x_n\} \subseteq M$ D-independente.

Como M é simples, temos $Rx = M$ para todo $x \in M\backslash\{0\}$, logo a condição de densidade é válida para $n = 1$. Suponhamos que é válida para $n \geq 1$. Seja $\{x_1, \ldots, x_{n+1}\} \subseteq M$ D-independente. Vamos mostrar que existe $r \in R$ tal que $rx_{n+1} \neq 0$ e $rx_i = 0$ para $i \leq n$.

Suponhamos, pelo contrário, que $rx_1 = \ldots = rx_n = 0$ implica $rx_{n+1} = 0$ para todo $r \in R$. Pela hipótese de indução, os elementos do produto directo M^n são da forma $(rx_1, \ldots, rx_n)$ $(r \in R)$. Logo

$$\begin{array}{rcl} \varphi : \quad M^n & \to & M \\ (rx_1, \ldots, rx_n) & \mapsto & rx_{n+1} \end{array}$$

é um homomorfismo bem definido. Mas então pode-se verificar que para $i = 1, \ldots, n$ a função $d_i : M \to M$ definida por

$$xd_i = (0, \ldots, 0, x, 0, \ldots, 0)\varphi$$

(onde x ocorre na i-ésima componente) é um R-homomorfismo e além disso temos

$$x_{n+1} = (x_1, \ldots, x_n)\varphi = \sum_{i=1}^{n} x_i d_i,$$

o que contradiz a D-independência de $\{x_1, \ldots, x_{n+1}\}$. Logo existe $r \in R$ tal que $rx_{n+1} \neq 0$ e $rx_i = 0$ para $i \leq n$.

Por simetria, encontramos para cada $j \in \{1, \ldots, n+1\}$ algum $r_j \in R$ tal que $r_j x_j \neq 0$ e $r_j x_i = 0$ para $i \neq j$. Sejam $y_1, \ldots, y_{n+1} \in M$ quaisquer. Como M é simples, para $j = 1, \ldots, n+1$ existe $r'_j \in R$ tal que $r'_j(r_j x_j) = y_j$. Seja $r = \sum_{i=1}^{n+1} r'_j r_j$. Para $i = 1, \ldots, n+1$, temos

$$rx_i = \sum_{i=1}^{n+1} r'_j r_j x_i = r'_i r_i x_i = y_i$$

e portanto a condição de densidade é válida para o caso $n+1$. Por indução, concluimos que R é (isomorfo a) um subanel denso de EndM_D.

(ii) $\Rightarrow$ (i). Suponhamos que R é isomorfo a um subanel denso de EndM_D. Sem perda de generalidade, podemos assumir que R é mesmo um subanel de EndM_D. Já sabemos que podemos ver M como um R-módulo (à esquerda) através da acção

$$\begin{array}{rcl} R \times M & \to & M \\ (\varphi, x) & \mapsto & x\varphi \end{array}$$

É claro que $\varphi \cdot M = 0$ implica $\varphi = 0$, logo M é um R-módulo fiel. Por outro lado, como R é denso em EndM_D e $\{x\}$ é D-independente para todo $x \in M\backslash\{0\}$, obtemos $Rx = M$ para todo $x \in M\backslash\{0\}$. Concluimos assim que M é um R-módulo simples e portanto R é primitivo. $\square$

Passamos agora a ocupar-nos de outra noção central na Teoria de Anéis. Um anel R diz-se *primo* se

$$AB = 0 \Rightarrow (A = 0 \vee B = 0)$$

para todos $A, B \trianglelefteq R$.

O resultado seguinte oferece-nos caracterizações alternativas.

Lema 2.8 *As condições seguintes são equivalentes para um anel R:*

(i) R é primo;

(ii) $Ann_R L = 0$ para todo $0 \neq L \trianglelefteq_e R$;

(iii) $r_1 R r_2 \neq 0$ para todos $r_1, r_2 \in R\backslash\{0\}$.

Dem. Exercício. $\square$

Teorema 2.9 *Todo o anel primitivo é primo.*

Dem. Seja R um anel primitivo e seja M um R-módulo fiel e simples. Sejam A e B ideais de R não nulos. Então o submódulo BM de M é não nulo pois M é fiel. Como M é simples, resulta que $BM = M$. Analogamente, $AM \neq 0$ e logo

$$(AB)M = A(BM) = AM \neq 0.$$

Logo $AB \neq 0$ e R é primo. □

O recíproco deste teorema é falso:

Exemplo 2.10 *O anel $\mathbb{Z}$ é primo mas não primitivo.*

Dem. É claro que $\mathbb{Z}$ é primo pois $m\mathbb{Z}n \neq 0$ para todos $m, n \in \mathbb{Z}\backslash\{0\}$. Como $\mathbb{Z}$ é comutativo, $\mathbb{Z}$ primitivo implicaria que $\mathbb{Z}$ fosse um corpo por um resultado anterior, o que obviamente não acontece. Logo $\mathbb{Z}$ não é primitivo. □

Contudo, com uma condição adicional, podemos garantir que um anel primo seja primitivo. Dizemos que $L \trianglelefteq_e R$ é *minimal* se for não nulo e não contiver estritamente nenhum ideal à esquerda não nulo de R. Ao contrário do que acontece com os ideais à esquerda maximais, um anel não tem necessariamente ideais à esquerda minimais: veja-se o caso de $\mathbb{Z}$, onde os ideais (à esquerda) são da forma $n\mathbb{Z}$.

Teorema 2.11 *Seja R um anel primo. Se R tiver um ideal à esquerda minimal, então R é primitivo.*

Dem. Seja L um ideal à esquerda minimal de R. Como R é primo, então $\mathrm{Ann}_R L = 0$ pelo Lema 2.8. Logo L é fiel enquanto R-módulo. Por outro lado, L minimal implica que L é também um R-módulo simples, logo R é primitivo. □

Corolário 2.12 *Seja R um anel primo com um ideal à esquerda minimal L. Então, a menos de isomorfismo, L é o único R-módulo simples e fiel.*

Dem. Vimos na demonstração do teorema anterior que L é um R-módulo simples e fiel. Seja M um R-módulo simples e fiel qualquer. Como M é fiel, temos $LM \neq 0$, logo existe $x_0 \in M$ tal que $Lx_0 \neq 0$. Consideremos o homomorfismo de R-módulos

$$\begin{array}{rcl} \varphi : L & \to & M \\ a & \mapsto & ax_0. \end{array}$$

Temos $\mathrm{Ker}\varphi < L$ e logo, por minimalidade de L, concluimos que $\mathrm{Ker}\varphi = 0$ e φ é injectivo. Por outro lado, $0 < L\varphi \leq M$. Como M é simples, resulta que $L\varphi = M$. Logo φ é um isomorfismo e $M \cong L$. □

2.1 APÊNDICE: Anéis com ideais à esquerda minimais

Um elemento $e \in R$ diz-se *idempotente* se $e^2 = e$. Em particular, 0 e 1 são idempotentes.

Lema 2.13 *Seja R um anel e seja $e \in R$ idempotente. Seja $L = Re$. Então $End_R L \cong eRe$.*

Dem. Consideremos a função

$$\begin{array}{rcl} \Gamma : \mathrm{End}_R L & \to & eRe \\ \varphi & \mapsto & e\varphi. \end{array}$$

A função Γ está bem definida pois

$$e\varphi = e^2\varphi = e(e\varphi) \in eL = eRe$$

para todo $\varphi \in \mathrm{End}_R L$. Dados $\varphi, \psi \in \mathrm{End}_R L$, temos

$$(\varphi + \psi)\Gamma = e(\varphi + \psi) = e\varphi + e\psi = \varphi\Gamma + \psi\Gamma,$$

$$(\varphi\psi)\Gamma = e\varphi\psi = (e\varphi \cdot e)\psi = (e\varphi)(e\psi) = (\varphi\Gamma)(\psi\Gamma)$$

e $1_L\Gamma = e$, logo Γ é um homomorfismo de anéis.

Temos

$$\mathrm{Ker}\Gamma = \{\varphi \in \mathrm{End}_R L \mid e\varphi = 0\} = 0,$$

logo Γ é injectivo. Finalmente, seja $a \in eRe$. Seja

$$\begin{array}{rcl} \varphi_a : L & \to & L \\ x & \mapsto & xa. \end{array}$$

É simples rotina verificar que $\varphi_a \in \mathrm{End}_R L$ e $\varphi_a\Gamma = e\varphi_a = ea = a$, logo Γ é sobrejectiva e consequentemente um isomorfismo. □

Teorema 2.14 *Seja R um anel primo com ideal à esquerda minimal L. Então existe $e \in L\backslash\{0\}$ idempotente tal que eRe é um anel de divisão.*

Dem. Como R é primo, temos $L^2 \neq 0$ pelo Lema 2.8. Logo existe $a \in L$ tal que $La \neq 0$. Como $0 \neq La \leq L$ e L é minimal, obtemos $La = L$. Em particular, $a = ea$ para algum $e \in L$. Daqui se conclui que $a = e^2a$ e logo $(e - e^2)a = 0$. Ora $\mathrm{Ann}_L a \leq L$ e como $e \notin \mathrm{Ann}_L a$, temos de facto $\mathrm{Ann}_L a < L$. Como L é minimal, obtemos $\mathrm{Ann}_L a = 0$ e logo $e - e^2 \in \mathrm{Ann}_L a$ implica $e = e^2$. Concluimos assim que e é idempotente.

Como $0 \neq Re \leq L$, resulta da minimalidade de L que $L = Re$. Pelo lema anterior, obtemos $eRe \cong \mathrm{End}_R L$. Como L é um R-módulo simples, resulta do Lema de Schur que $\mathrm{End}_R L$ é um anel de divisão. Logo eRe é um anel de divisão. □

O resultado seguinte relaciona ideais à esquerda minimais com ideais à direita minimais.

Teorema 2.15 *Seja R um anel primo e seja $r \in R$. Então Rr é um ideal à esquerda minimal de R se e só se rR for um ideal à direita minimal.*

Dem. Suponhamos que Rr é um ideal à esquerda minimal. Consideremos $0 \neq r' = ra \in rR$. Queremos mostrar que $r \in r'R$. Pelo teorema anterior, existe $e \in (Rr)\backslash\{0\}$ idempotente tal que eRe é um anel de divisão. Como $Re = Rr$ por minimalidade de Rr, temos $r = r_1 e$ para algum $r_1 \in R$. Logo $r' = ra = r_1 ea$. Como R é primo, resulta do Lema 2.8 que $r_1 eaRr_1 ea \neq 0$. Logo existe $r_2 \in R$ tal que $0 \neq r_1(ear_2r_1e) \in r'R$. Como eRe é um anel de divisão, podemos concluir que

$$r = r_1 e \in r_1(ear_2r_1e)R \subseteq r'R,$$

pois ear_2r_1e tem inverso. Logo rR é um ideal à direita minimal de R.

A implicação recíproca segue por simetria. □

2.2 APÊNDICE: O Teorema de Connell

Pretendemos apresentar o famoso Teorema de Connell que caracteriza os anéis de grupo primos. O caso dos anéis de polinómios é bastante mais simples e servir-nos-à de aperitivo.

Teorema 2.16 *Seja R um anel. Então R é primo se e só se $R[x]$ for primo.*

Dem. Suponhamos que R é primo. Sejam $f, g \in R[x]$ não nulos. Podemos escrever $f = f' + ax^n$ e $g = g' + bx^m$ com $\mathrm{gr}(f') < n$, $\mathrm{gr}(g') < m$ e $a, b \in R\backslash\{0\}$. Como R é primo, resulta do Lema 2.8 que $arb \neq 0$ para algum $r \in R$. Como

$$frg = f'rg' + f'rbx^m + ax^nrg' + arbx^{n+m}$$

e $\mathrm{gr}(f'rg' + f'rbx^m + ax^nrg') < n + m$, concluimos que $frg \neq 0$ e portanto $R[x]$ é primo pelo Lema 2.8.

Reciprocamente, suponhamos que $R[x]$ é primo. Sejam $A, B \trianglelefteq R$ tais que $AB = 0$. É imediato que $A[x], B[x] \trianglelefteq R[x]$ e $A[x] \cdot B[x] = 0$. Como $R[x]$ é primo, concluimos que $A[x] = 0$ ou $B[x] = 0$. Logo $A = 0$ ou $B = 0$, e resulta que R é um anel primo. □

Para apresentar o Teorema de Connell, precisamos de recordar o conceito de *subgrupo normal* de um grupo G. Um subgrupo H de um grupo G diz-se normal se $gH = Hg$ para todo $g \in G$.

Teorema 2.17 *Seja K um corpo e G um grupo. Então o anel de grupo $K[G]$ é primo se e só se G não tiver nenhum subgrupo normal finito não trivial.*

Dem. Suponhamos que H é um subgrupo normal finito não trivial de G, isto é, com mais de um elemento. Seja

$$\alpha = \sum_{h \in H} h \in K[G].$$

Vejamos que α comuta com todos os elementos de $K[G]$. De facto, como H é normal, temos

$$g\alpha = g\sum_{h \in H} h = \sum_{h' \in gH} h' = \sum_{h' \in Hg} h' = \sum_{h \in H} hg = \alpha g$$

para todo $g \in G$, e daqui resulta facilmente que α comuta com todos os elementos de $K[G]$. Além disso, como $g \in H$ se e só se $gH = H$, resulta que para $g \in H$ se tem

$$g\alpha = g\sum_{h \in H} h = \sum_{h' \in gH} h' = \sum_{h' \in H} h' = \alpha.$$

Se $|H| = n$, obtemos

$$\alpha^2 = \sum_{h \in H} h\alpha = \sum_{h \in H} \alpha = n\alpha.$$

Logo $\alpha(\alpha - n1) = \alpha^2 - n\alpha = 0$. Como α comuta com todos os elementos de $K[G]$, resulta que

$$\alpha\, K[G]\, (\alpha - n1) = 0.$$

Ora $\alpha \neq 0$ e como H é não trivial temos também $\alpha - n1 \neq 0$, logo $K[G]$ não é primo pelo Lema 2.8.

A demonstração da implicação recíproca é bastante mais complexa, pelo que a omitimos. $\square$

Observamos que a implicação directa do teorema anterior é válida para qualquer anel K, o que já não acontece com a sua recíproca.

2.3 Exercícios

2.1. Mostre que um anel R é um anel de divisão se e só se todo o R-módulo é livre (*Sugestão*: considere R-módulos simples).

2.2. Sejam R um anel e $n \in \mathbb{N}$. Mostre que os ideais de $M_n(R)$ são da forma $M_n(I)$, com $I \trianglelefteq R$.

2.3. Mostre que se R é primitivo então $M_n(R)$ é primitivo.

2.4. Seja R um anel e seja $e \in R\backslash\{0\}$ idempotente. Mostre que se R é primitivo então eRe é primitivo.

2.5. Mostre que um domínio R com um ideal à esquerda minimal Ra é um anel de divisão.

2.6. Mostre que se $L \trianglelefteq_e R$ é minimal, $r \in R$ e $Lr \neq 0$, então Lr é também um ideal à esquerda minimal de R.

2.7. Dado um anel R, seja $\mathrm{Soc}(R)$ a soma dos ideais à esquerda minimais de R, caso existam; caso contrário, seja $\mathrm{Soc}(R) = 0$. Mostre que $\mathrm{Soc}(R) \trianglelefteq R$.

2.8. Mostre que se R é primo e $\mathrm{Soc}(R) \neq 0$ então $\mathrm{Soc}(R)$ é a intersecção dos ideais de R.

3 ANÉIS SEMI-SIMPLES

Um conjunto parcialmente ordenado $(A, \leq)$ satisfaz a *condição de cadeia ascendente* se não existir em A nenhuma cadeia infinita do tipo $a_1 < a_2 < \ldots$. Analogamente, $(A, \leq)$ satisfaz a *condição de cadeia descendente* se não existir em A nenhuma cadeia infinita do tipo $a_1 > a_2 > \ldots$.

Um R-módulo M diz-se *noetheriano* (respectivamente *artiniano*) se o seu reticulado de submódulos satisfizer a condição de cadeia ascendente (respectivamente condição de cadeia descendente).

Teorema 3.1 *Seja M um R-módulo e $N \leq M$. Então:*

(i) M é noetheriano se e só se N e M/N são noetherianos;

(ii) M é artiniano se e só se N e M/N são artinianos.

Dem. (i) A implicação directa constitui um exercício elementar.

Reciprocamente, suponhamos que N e M/N são noetherianos. Suponhamos que $M_1 < M_2 < \ldots$ é uma cadeia infinita de submódulos de M. Então temos

$$M_1 \cap N \leq M_2 \cap N \leq \ldots$$

e

$$(M_1 + N)/N \leq (M_2 + N)/N \leq \ldots$$

Como N e M/N são noetherianos, estas duas sucessões são necessariamente estacionárias, logo existe algum $k \in \mathbb{N}$ tal que $M_k \cap N = M_{k+1} \cap N$ e $(M_k + N)/N = (M_{k+1} + N)/N$. Seja $x \in M_{k+1}$. Então $x \in M_{k+1} + N = M_k + N$, logo $x = y + z$ para alguns $y \in M_k$ e $z \in N$. Resulta que

$$z = x - y \in M_{k+1} \cap N = M_k \cap N,$$

logo $x = y + z \in M_k$ e $M_{k+1} = M_k$, absurdo. Logo M é noetheriano.

(ii) Análogo. □

Corolário 3.2 *Seja M um R-módulo e sejam $M_1, \ldots, M_t$ submódulos de M tais que $M = \sum_{i=1}^{t} M_i$. Então M é noetheriano (respectivamente artiniano) se e só se M_i for noetheriano (respectivamente artiniano) para $i = 1, \ldots, t$.*

Dem. Consideramos o caso noetheriano (o caso artiniano é análogo). A implicação directa resulta imediatamente do teorema anterior.

Provamos a implicação recíproca por indução sobre t. Sendo o caso $t = 1$ trivial, suponhamos que $t > 1$ e que o resultado é válido para $t - 1$. Seja $N = \sum_{i=1}^{t-1} M_i$. Por hipótese de indução, N é noetheriano. Pelo Teorema do Isomorfismo, temos

$$M/N = (N + M_t)/N \cong M_t/(N \cap M_t).$$

Como M_t é noetheriano, resulta do teorema anterior que $M_t/(N \cap M_t)$ também o é, e consequentemente M/N. Logo N e M/N são ambos noetherianos e portanto M é igualmente noetheriano. □

Um anel R diz-se *noetheriano à esquerda* (à direita) se for noetheriano enquanto R-módulo (respectivamente R-módulo à direita). Diz-se *artiniano à esquerda* (à direita) se for artiniano enquanto R-módulo (respectivamente R-módulo à direita). Por outras palavras, R é noetheriano (respectivamente artiniano) à esquerda se satisfizer a condição de cadeia ascendente (respectivamente condição de cadeia descendente) para ideais à esquerda. Finalmente, R diz-se *noetheriano* (respectivamente *artiniano*) se for noetheriano (respectivamente artiniano) à esquerda e à direita.

Exemplo 3.3 *O anel $\mathbb{Z}$ é noetheriano mas não artiniano.*

O resultado seguinte será útil posteriormente.

Lema 3.4 *Seja $\varphi : R \to T$ um homomorfismo sobrejectivo de anéis com R artiniano à esquerda. Então T é artiniano à esquerda.*

Dem. Exercício. □

O resultado seguinte é um dos mais famosos da teoria de anéis não comutativos, conhecido por Teorema de Wedderburn-Artin.

Teorema 3.5 *As condições seguintes são equivalentes para um anel R:*

(i) R *é primitivo e artiniano à esquerda;*

(ii) $R \cong M_n(D)$ *para algum anel de divisão* D *e algum* $n \in N$*;*

(iii) R *é artiniano simples.*

Dem. (i) $\Rightarrow$ (ii). Suponhamos que R é primitivo e artiniano à esquerda. Pelo Teorema da Densidade de Jacobson, podemos assumir que R é um subanel denso de $\mathrm{End}M_D$, onde D designa um anel de divisão e M um D-módulo à direita. Suponhamos que a dimensão de M (sobre D) é infinita. Então existe um subconjunto D-independente de M da forma $\{x_1, x_2, x_3, \ldots\}$. Para cada $i \in \mathbb{N}$, seja

$$L_i = \mathrm{Ann}_R\{x_1, \ldots, x_i\}.$$

Temos uma cadeia $L_1 \geq L_2 \geq \ldots$ de ideais à esquerda. Como R é um subanel denso de $\mathrm{End}M_D$, todas as inclusões são estritas, o que contradiz a hipótese de R ser artiniano à esquerda. Logo a dimensão de M (sobre D) é finita (digamos n). Seja $\{x_1, \ldots, x_n\}$ uma base de M enquanto D-módulo à direita. Resulta da condição de densidade que $R = \mathrm{End}M_D$. Logo $R \cong M_n(D)$ pelo Teorema 1.17.

(ii) $\Rightarrow$ (iii). Assumimos que $R = M_n(D)$, com D anel de divisão. Podemos ver R como um D-módulo através da ação definida por $(dr)_{ij} = dr_{ij}$. É fácil de ver que $\{\varepsilon_{ij} \mid i, j = 1, \ldots n\}$ é uma base do D-módulo R, logo a dimensão de R enquanto D-módulo é n^2.

Suponhamos que R não é Artiniano à esquerda. Então existe uma cadeia de ideais à esquerda de R da forma

$$L_0 > L_1 > \ldots > L_{n^2+1}.$$

Para cada $i \in \{0, \ldots, n^2\}$, fixemos $x_i \in L_i \backslash L_{i+1}$. Suponhamos que $d_0x_0 + \ldots + d_{n^2}x_{n^2} = 0$ para alguns $d_i \in D$. Como $d_ix_i = (d_i1_R)x_i$, temos $d_1x_1 + \ldots + d_{n^2}x_{n^2} \in L_1$ e logo $d_0x_0 \in L_1$. Como $x_0 \notin L_1$, concluimos que $d_0 = 0$. Aplicando sucessivamente este raciocínio, obtemos $d_0 = d_1 = \ldots = d_{n^2} = 0$ e logo $\{x_0, \ldots, x_{n^2}\}$ é um subconjunto D-independente de R. Como qualquer subconjunto D-independente pode ser estendido a uma base pelo Lema de Zorn, e a dimensão de R enquanto D-módulo é n^2, isto contradiz o Teorema 1.16. Logo R é Artiniano à esquerda. Analogamente se mostra que R é Artiniano à direita.

Seja $0 \neq A \trianglelefteq R$. Tomemos $a \in A\backslash\{0\}$. Como $a \neq 0$, temos $a_{ij} \neq 0$ para alguns $i, j \in \{1, \ldots, n\}$. Seja $x \in R$. Logo

$$x_{kl}\varepsilon_{kl} = (x_{kl}a_{ij}^{-1}\varepsilon_{ki})(a_{ij}\varepsilon_{ij})\varepsilon_{jl} = (x_{kl}a_{ij}^{-1}\varepsilon_{ki})a\varepsilon_{jl} \in A$$

para todos $k, l \in \{1, \ldots, n\}$. Como

$$x = \sum_{k=1}^{n}\sum_{l=1}^{n} x_{kl}\varepsilon_{kl},$$

concluimos que $A = R$ e logo R é simples.

(iii) $\Rightarrow$ (i). Imediato pois vimos anteriormente que todo o anel simples é primitivo. $\square$

Dizemos que um ideal A de um anel R é *primitivo* (respectivamente *primo*) se o anel quociente R/P for primitivo (respectivamente primo). O resultado seguinte resume algumas caracterizações alternativas do quociente de ideal primo. Note-se que $AB \subseteq A \cap B$ para todos $A, B \trianglelefteq R$.

Lema 3.6 *As seguintes condições são equivalentes para $P \lhd R$:*

(i) P é um ideal primo;

(ii) se $A, B \lhd R$ e $AB \subseteq P$, então $A \subseteq P$ ou $B \subseteq P$;

(iii) se $a, b \in R$ e $aRb \subseteq P$, então $a \in P$ ou $b \in P$.

Dem. Exercício. $\square$

O anel R diz-se *semiprimitivo* se

$$\bigcap\{A \trianglelefteq R \mid \ A \text{ é primitivo}\} = 0.$$

Analogamente, dizemos que R é *semiprimo* se

$$\bigcap\{A \trianglelefteq R \mid \ A \text{ é primo}\} = 0.$$

Se R é semiprimitivo e $\{P_i \mid i \in I\}$ designa o conjunto dos ideais primitivos de R, então a função

$$\begin{array}{rccc} \varphi: & R & \to & \prod_{i\in I} R/P_i \\ & r & \mapsto & (r + P_i)_i \end{array}$$

é um homomorfismo injectivo de anéis em que cada uma das projecções $R \to R/P_i$ é sobrejectiva. Diz-se então que R é *produto subdirecto* dos anéis R/P_i e portanto um anel semiprimitivo é produto subdirecto de anéis primitivos. Analogamente, um anel semiprimo é produto subdirecto de anéis primos.

Esta terminologia poder-se-ia naturalmente generalizar a outras classes de anéis. No caso do conceito de anel simples, temos o seguinte resultado:

Lema 3.7 *Seja R um anel e $A \lhd R$. Então o quociente R/A é simples se e só se o ideal A for maximal.*

Dem. Exercício. □

Logo não há necessidade de definir ideais simples. Todavia, podemos definir o conceito de anel semi-simples. Um anel R diz-se *semi-simples* se

$$\bigcap \{A \trianglelefteq R \mid \ A \text{ é maximal}\} = 0.$$

O teorema seguinte apresentar-nos-á diversas caracterizações equivalentes dos anéis artinianos semi-simples. Antes, enunciamos um pequeno lema.

Lema 3.8 *Seja $R = M_n(D)$, onde D é um anel de divisão e $n \in N$. Então $R\varepsilon_{uu}$ é um ideal à esquerda minimal de R para $u = 1, \ldots, n$.*

Dem. Exercício. □

Relembramos que $\mathrm{Soc}(R)$, dito o *soco* de R, é definido como sendo a soma dos ideais à esquerda minimais de R, caso existam; caso contrário, $\mathrm{Soc}(R) = 0$.

Teorema 3.9 *As seguintes condições são equivalentes para um anel R:*

(i) *R é artiniano semi-simples;*

(ii) *R é semiprimo e artiniano à esquerda;*

(iii) *R é isomorfo a um produto directo finito de anéis artinianos simples;*

(iv) *$Soc(R) = R$.*

Dem. (i) $\Rightarrow$ (ii). Como todo o anel simples é primitivo e logo primo, resulta que todo o anel semi-simples é semiprimo.

(ii) $\Rightarrow$ (iii). Seja R semiprimo e artiniano à esquerda. Suponhamos que R tem uma infinidade de ideais primos $P_1, P_2, \ldots$ (todos distintos). Como R é artiniano à esquerda, a cadeia

$$P_1 \supseteq P_1 \cap P_2 \supseteq P_1 \cap P_2 \cap P_3 \supseteq \ldots$$

é estacionária em $P_1 \cap \ldots \cap P_t$ para algum t. Mas então $P_1 \cap \ldots \cap P_{t+1} = P_1 \cap \ldots \cap P_t$ implica

$$P_1 \ldots P_t \subseteq P_1 \cap \ldots \cap P_t \subseteq P_{t+1}.$$

Pelo Lema 3.6, concluimos que $P_i \subseteq P_{t+1}$ para algum $i \in \{1, \ldots, t\}$. Como R/P_i é primo e artiniano à esquerda pelo Lema 3.4, resulta do Teorema de Wedderburn-Artin que R/P_i é artiniano simples. Em particular, pelo Lema 3.7, P_i é um ideal maximal. Como $P_i \subseteq P_{t+1} \subset R$, resulta que $P_i = P_{t+1}$, absurdo. Logo R tem um número finito de ideais primos, digamos $P_1, \ldots, P_t$.

Como R é semiprimo, temos $\cap_{i=1}^{t} P_i = 0$. É imediato que

$$\begin{array}{rccc} \varphi: & R & \to & \prod_{i=1}^{t} R/P_i \\ & r & \mapsto & (r + P_i)_i \end{array}$$

é um homomorfismo injectivo de anéis. Vejamos que φ é sobrejectivo.

Por simetria, basta mostrar que $(1, 0, 0, \ldots, 0) \in R\varphi$, isto é, que existe $r \in R$ tal que

$$r + P_1 = 1 + P_1, \quad r + P_2 = P_2, \ldots, r + P_t = P_t,$$

ou seja, que

$$1 - r \in P_1, \quad r \in P_2 \cap \ldots \cap P_t.$$

Vimos atrás que os ideais P_i são na realidade ideais maximais de R. Como $P_1 \subset P_1 + P_i$, resulta que $P_1 + P_i = R$ para $i = 2, \ldots, t$. Logo, para cada $i = 2, \ldots, t$, existem $a_i \in P_1$ e $b_i \in P_i$ tais que $a_i + b_i = 1$. Mas então

$$1 = 1^{t-1} = (a_2 + b_2) \ldots (a_t + b_t) = a + b_2 \ldots b_t$$

para algum $a \in P_1$. Tomando $r = b_2 \ldots b_t$, obtemos $1 - r = a \in P_1$ e $r \in P_2 \cap \ldots \cap P_t$. Logo φ é sobrejectivo e consequentemente um isomorfismo

de anéis. Cmo já observámos que cada R/P_i é artiniano simples, então R é isomorfo a um produto directo finito de anéis artinianos simples.

(iii) $\Rightarrow$ (i). Suponhamos que $R = R_1 \times \ldots \times R_k$ com $R_1, \ldots, R_k$ anéis artinianos simples. Como os ideais

$$A_i = R_1 \times \ldots \times R_{i-1} \times \{0\} \times R_{i+1} \times \ldots \times R_k$$

são maximais para $i = 1, \ldots, k$ e $\cap_{i=1}^{k} A_i = 0$, resulta que R é semi-simples.

Para mostrar que R é artiniano, basta mostrar que o produto directo de dois anéis artinianos $R_1 \times R_2$ é ainda artiniano. De facto, verifica-se facilmente que um ideal à esquerda L de um anel deste tipo é sempre da forma $L_1 \times L_2$, onde L_i é ideal à esquerda de R_i para $i = 1, 2$: temos

$$L = (1,0)L + (0,1)L = L\pi_1 \times \{0\} + \{0\} \times L\pi_2 = L\pi_1 \times L\pi_2,$$

onde π_1 e π_2 designam as projecções em R_1 e R_2 respectivamente. Sendo R_1 e R_2 artinianos, é claro que não pode haver nenhuma cadeia infinita da forma

$$L_1 \times L_1' > L_2 \times L_2' > \ldots$$

e portanto R é artiniano à esquerda. Analogamente se mostra que R é artiniano à direita.

(iii) $\Rightarrow$ (iv). Consideremos primeiro o caso em que $R = M_n(D)$, com $n \geq 1$ e D anel de divisão. Pelo Lema 3.8, $R\varepsilon_{uu}$ é um ideal à esquerda minimal de R para $u = 1, \ldots, n$. É imediato que $R = \sum_{u=1}^{n} R\varepsilon_{uu}$, logo concluimos pelo Teorema de Wedderburn-Artin que um anel artiniano simples R satisfaz $\mathrm{Soc}(R) = R$.

Suponhamos agora que $R = R_1 \times \ldots \times R_k$ com cada R_i artiniano simples. Se L_i é um ideal à esquerda minimal de R_i, então

$$\{0\} \times \ldots \times \{0\} \times L_i \times \{0\} \times \ldots \times \{0\}$$

é um ideal à esquerda minimal de R. Daqui resulta facilmente que $\mathrm{Soc}(R) = R$.

(iv) $\Rightarrow$ (ii). Suponhamos que $\mathrm{Soc}(R) = R$. Em particular, $1 \in L_1 + \ldots + L_t$ para alguns ideais à esquerda minimais $L_1, \ldots, L_t$. Daqui se conclui que $R = L_1 + \ldots + L_t$. Como cada L_i é simples enquanto R-módulo, resulta trivialmente que cada L_i é um R-módulo artiniano. Logo, pelo Corolário 3.2, $R = L_1 + \ldots + L_t$ é também um R-módulo artiniano, e consequentemente um anel artiniano à esquerda.

Para cada $i = 1, \ldots, t$, seja

$$P_i = \mathrm{Ann}_R L_i.$$

Sejam $a, b \in R$ tais que $aRb \subseteq P_i$. Se $b \notin P_i$, então RbL_i é um submódulo não nulo de L_i; como L_i é simples, isto implica $RbL_i = L_i$ e portanto

$$aL_i = aRbL_i \subseteq P_i L_i = 0,$$

donde se conclui que $a \in \mathrm{Ann}_R L_i = P_i$. Pelo Lema 3.6, P_i é um ideal primo para $i = 1, \ldots, t$. Como

$$\cap_{i=1}^{t} P_i = \cap_{i=1}^{t} \mathrm{Ann}_R L_i \subseteq \mathrm{Ann}_R R = 0,$$

resulta que R é semiprimo. □

Terminamos esta secção introduzindo algumas noções relativas a módulos que levarão a uma nova caracterização dos anéis artinianos semi-simples.

Dado um R-módulo M, definimos o *soco* de M, designado por $\mathrm{Soc}(M)$, como sendo a soma dos submódulos simples de M, caso existam; caso contrário, $\mathrm{Soc}(M) = 0$. Dizemos que M é *semi-simples* se $\mathrm{Soc}(M) = M$.

Dado $N \leq M$, dizemos que $K \leq M$ é um *complemento* de M se $M = N \oplus K$. Se N tiver um complemento em M, dizemos que N é *parcela directa* de M. Finalmente, diz-se que M é *complementado* se todo o submódulo de M tiver um complemento.

Exemplo 3.10 *(i) O complemento não é necessariamente único.*

(ii) Nem todos os módulos são complementados.

Dem. (i) O submódulo $\mathbb{R} \times \{0\}$ do $\mathbb{R}$-módulo $\mathbb{R}^2$ tem complementos $\{0\} \times \mathbb{R}$ e $\{(x, x) \mid x \in \mathbb{R}\}$.

(ii) O $\mathbb{Z}$-módulo $\mathbb{Q}$ não é complementado, pois $\mathbb{Z} < \mathbb{Q}$ não tem complemento. □

Veremos em seguida que estes dois conceitos aparentemente distintos se equivalem, mas provamos antes um lema útil.

Lema 3.11 *Um submódulo de um módulo complementado é complementado.*

Dem. Seja M um módulo complementado e $N \leq M$. Dado $K \leq N$, temos também $K \leq M$. Como M é complementado, temos $M = K \oplus K'$ para algum $K' \leq M$. Vejamos que $K' \cap N$ é um complemento de K em N.

Dado $x \in N$, temos $x = y + y'$ para alguns $y \in K$ e $y' \in K'$. Logo $y' = x - y \in N + K = N$ e logo $y' \in K' \cap N$. Concluimos que $N = K + (K' \cap N)$. Como $K \cap (K' \cap N) = 0$ trivialmente, obtemos $N = K \oplus (K' \cap N)$. Logo N é complementado. $\square$

Teorema 3.12 *Um R-módulo M é semi-simples se e só se é complementado.*

Dem. Suponhamos que M é semi-simples. Então $M = \sum_{i \in I} N_i$, onde $\{N_i \mid i \in I\}$ designa o conjunto dos submódulos simples de M. Seja $N \leq M$. Consideramos o conjunto

$$\mathcal{L} = \{K \leq M \mid N \cap K = \emptyset\}.$$

Como $\{0\} \in \mathcal{L}$, temos que $\mathcal{L} \neq \emptyset$. Além disso, se $(K_j)_{j \in J}$ for uma cadeia em $\mathcal{L}$, então $\cup_{j \in J} K_j \in \mathcal{L}$. Logo, pelo Lema de Zorn, $\mathcal{L}$ tem algum elemento maximal P.

Suponhamos que $(N+P) \cap N_i = 0$ para algum $i \in I$. Se $x \in N \cap (P + N_i)$, então $x = p + x_i$ para alguns $p \in P$ e $x_i \in N_i$, logo $x_i = x - p \in (N + P) \cap N_i = 0$ e portanto $x_i = 0$. Daqui se concluiria que $x = p \in N \cap P = 0$ e consequentemente $N \cap (P + N_i) = 0$, implicando que $P + N_i \in \mathcal{L}$. Como P é maximal em $\mathcal{L}$, resulta que $N_i \subseteq P$, contradizendo $(N + P) \cap N_i = 0$. Logo $(N + P) \cap N_i \neq 0$ para todo $i \in I$. Como cada N_i é simples, temos então $(N + P) \cap N_i = N_i$ para todo $i \in I$ e logo

$$M = \sum_{i \in I} N_i \subseteq N + P \subseteq M.$$

Como $N \cap P = 0$, obtemos $N \oplus P = M$ e logo M é complementado.

Reciprocamente, suponhamos que M é complementado. Seja M' um complemento de $\mathrm{Soc}(M)$ em M. Queremos mostrar que $M' = 0$. Suponhamos que $x \in M' \backslash \{0\}$. É fácil ver que, pelo Lema de Zorn, existe $N < M'$ maximal relativamente a $x \notin N$. Como M' é complementado pelo lema anterior, $N \oplus N' = M'$ para algum $N' \leq M'$. Vamos mostrar que N' é simples, contrariando $M' \cap \mathrm{Soc}(M) = 0$.

Suponhamos então que $0 < P < N'$. Pelo lema anterior P tem um complemento P' em N'. Como $N < N + P \leq M'$, resulta da maximalidade de N que $x \in N + P$. Analogamente, $N < N + P' \leq M'$ implica $x \in N + P'$. Logo $x = y + z = y' + z'$ para alguns $y, y' \in N$, $z \in P$ e $z' \in P'$. Mas então

$$z' - z = y - y' \in N \cap N' = 0,$$

logo $z = z' \in P \cap P' = 0$. Daqui se conclui que $x = y \in N$, absurdo. Logo N' é simples e portanto $N' \subseteq M' \cap \mathrm{Soc}(M) = 0$, contradição. Portanto $M' = 0$ e $M = \mathrm{Soc}(M)$ como se pretendia. □

Teorema 3.13 *As condições seguintes são equivalentes para um anel R:*

(i) R é artiniano semi-simples;

(ii) R é semi-simples enquanto R-módulo;

(iii) R é complementado enquanto R-módulo;

(iv) todo o R-módulo é semi-simples;

(v) todo o R-módulo é complementado.

Dem. A equivalência (i) ⇔ (ii) resulta da equivalência (i) ⇔ (iv) no Teorema 3.9, enquanto as equivalências (ii) ⇔ (iii) e (iv) ⇔ (v) resultam do teorema anterior. Como a implicação (iv) ⇒ (ii) é trivial, resta-nos mostrar que (ii) ⇒ (iv).

Suponhamos que $R = \sum_{i \in I} L_i$, onde os L_i designam ideais à esquerda minimais de R (isto é, os seus submódulos simples). Como vimos na demonstração de (iv) ⇒ (ii) no Teorema 3.9, podemos assumir que I é finito. Seja M um R-módulo e seja $x \in M$. Suponhamos que $L_i x \neq 0$ para algum $i \in I$. Como L_i é um ideal à esquerda minimal, resulta que a função

$$\begin{array}{rcl} \varphi : L_i & \to & L_i x \\ r & \mapsto & rx \end{array}$$

é um isomorfismo de R-módulos. Logo $L_i x$ é um R-módulo simples e portanto $L_i x \subseteq \mathrm{Soc}(M)$. Logo $L_i x \subseteq \mathrm{Soc}(M)$ para todo $i \in I$ e portanto

$$x \in \sum_{i \in I} L_i x \in \mathrm{Soc}(M).$$

Logo $\mathrm{Soc}(M) = M$ e M é semi-simples.

3.1 APÊNDICE: Módulos simples

Um idempotente $e \in R\backslash\{0\}$ diz-se *primitivo* se não existir nenhum idempotente $e' \in R\backslash\{0\}$ tal que $Re' \subset Re$. O conceito de idempotente primitivo permite-nos caracterizar os módulos simples sobre um anel artiniano simples:

Teorema 3.14 *Seja R um anel artiniano simples. Então:*

(i) R tem um idempotente primitivo e;

(ii) Re é um R-módulo simples;

(iii) todo o R-módulo simples é isomorfo a Re.

Dem. (i) Pelo Teorema 3.9, podemos assumir que R é da forma $M_n(D)$ para algum anel de divisão D. Pelo Lema 3.8, $R\varepsilon_{11}$ é um ideal à esquerda minimal de R, logo . $e = \varepsilon_{11}$ é um idempotente primitivo de R.

(ii) Suponhamos que Re não é simples. Como R é artiniano, existe um ideal à esquerda minimal L de R estritamente contido em Re. Como R é simples e consequentemente primo, resulta do Teorema 2.14 que L contém um idempotente $e' \neq 0$ e logo

$$0 \neq Re' \subseteq L \subset Re,$$

contradizendo o facto de e ser um idempotente primitivo. Logo Re é simples.

(iii) Seja M um R-módulo simples. Sendo R simples, então

$$\mathrm{Ann}_R M \lhd R \Rightarrow \mathrm{Ann}_R M = 0,$$

logo M é fiel. Como R é primo e tem um ideal à esquerda minimal, resulta do Corolário 2.12 que todos os R-módulos fiéis e simples são isomorfos. Em particular, todo o R-módulo simples é isomorfo a Re. □

Vamos agora ver o que se passa com os anéis artinianos semi-simples.

Teorema 3.15 *Seja R um anel artiniano semi-simples, digamos $R = R_1 \times \ldots \times R_k$, onde $R_1, \ldots, R_k$ são anéis artinianos simples. Seja e_i um idempotente primitivo de R_i para $i = 1, \ldots, k$. Então:*

(i) $f_i = (0, \ldots, 0, e_i, 0, \ldots, 0)$ é um idempotente primitivo de R para $i = 1, \ldots, k$;

(ii) Rf_i *é um* R*-módulo simples para* $i = 1, \ldots, k$*;*

(iii) todo o R*-módulo simples é isomorfo a algum* Rf_i*;*

(iv) os R*-módulos simples* $Rf_1, \ldots, Rf_k$ *são não isomorfos.*

Dem. (i) Exercício.

(ii) Seja $r \in R$ tal que $Rr < Rf_i$. Então

$$r = (0, \ldots, 0, r_i, 0, \ldots, 0)$$

para algum $r_i \in R_i$. Logo

$$Rr = \{0\} \times \ldots \times \{0\} \times R_i r_i \times \{0\} \times \ldots \times \{0\}$$

e obtemos $R_i r_i < R_i e_i$. Como e_i é um idempotente primitivo de R_i, conclui-se do teorema anterior que $R_i e_i$ é simples, logo $r_i = 0$ e consequentemente $r = 0$. Logo Rf_i é simples.

(iii) Seja M um R-módulo simples. Para $i = 1, \ldots, k$, seja

$$A_i = \{0\} \times \ldots \times \{0\} \times R_i \times \{0\} \times \ldots \times \{0\}.$$

É claro que $A_i \trianglelefteq R$ para todo i. Como

$$M = RM = (\sum_{i=1}^{k} A_i)M,$$

temos $A_j M \neq 0$ para algum j. Logo $A_j M = M$ e designando por A a soma dos restantes A_i obtemos $AM = AA_jM = 0$. Daqui se conclui que a estrutura de R-módulo de M induz naturalmente uma estrutura de R/A-módulo. Como $R/A \cong R_i$, temos então uma estrutura de R_i-módulo associada naturalmente a M, em que

$$r_i x = (0, \ldots, 0, r_i, 0, \ldots, 0)x$$

para todos $r_i \in R_i$ e $x \in M$. Como M é simples enquanto R-módulo, resulta facilmente que M é simples enquanto R_i-módulo. Logo, pelo teorema anterior, existe um isomorfismo $\varphi_i : M \to R_i e_i$ de R_i-módulos. Seja $\varphi : M \to Rf_i$ a função definida por

$$x\varphi = (0, \ldots, 0, x\varphi_i, 0, \ldots, 0).$$

É um exercício simples mostrar que φ é um isomorfismo de R-módulos.

(iv) Suponhamos que $\varphi : Rf_i \to Rf_j$ é um isomorfismo de R-módulos. Então

$$0 \neq f_i\varphi = (f_if_i)\varphi = f_i(f_i\varphi) \in f_iRf_j.$$

Como $f_iRf_j \neq 0$ se e só se $i = j$, o teorema está demonstrado. □

3.2 APÊNDICE: Submódulos essenciais

Um submódulo P de um módulo M diz-se *essencial* se $P \cap N \neq 0$ para todo o submódulo não nulo N de M.

Dado $N \leq M$, dizemos que $N' \leq M$ é um *complemento essencial* de N em M se $N \cap N' = 0$ e $N + N'$ é essencial em M. Vamos mostrar que, ao contrário do que acontece com os complementos, a existência de complementos essenciais pode ser demonstrada, mas antes precisamos de um pequeno lema técnico.

Lema 3.16 *Sejam $A, B, C \leq M$.*

(i) Se $(A + B) \cap C \neq 0$ e $A \cap C = 0$, então $B \cap (A + C) \neq 0$.

(ii) Se $A \leq C \leq A + B$ então $C = A + (B \cap C)$.

Dem. Exercício. □

Teorema 3.17 *Todo o submódulo de M tem um complemento essencial.*

Dem. Pelo Lema de Zorn, existe $N' \leq M$ maximal relativamente à condição $N \cap N' = 0$. Vejamos que $N + N'$ é essencial.

Seja $0 \neq P \leq M$. Se $P \subseteq N'$, então

$$(N + N') \cap P = P \neq 0,$$

logo podemos assumir que $P \not\subseteq N'$. Mas então $N' + P > N'$ e logo $N \cap (N' + P) \neq 0$ por maximalidade de N'. Pelo Lema 3.16(i), obtemos

$$P \cap (N + N') \neq 0.$$

Logo $N + N'$ é essencial. □

Podemos agora obter uma caracterização alternativa do soco de um módulo.

Teorema 3.18 *Seja M um módulo. Então*

$$Soc(M) = \cap\{N \leq M \mid N \text{ é essencial em } M\}.$$

Dem. Seja $P = \cap\{N \leq M \mid N \text{ é essencial em } M\}$. Se $S \leq M$ é simples e $N \leq M$ é essencial, então $0 \neq S \cap N \leq S$, logo $S \cap N = S$ e $S \subseteq N$. Concluimos assim que $S \subseteq P$ e portanto $\mathrm{Soc}(M) \subseteq P$.

Vamos agora ver que P é complementado. Seja $Q \leq P$. Pelo teorema anterior, Q tem um complemento essencial Q' em M. Logo $Q \leq P \leq Q + Q'$ e portanto

$$P = Q + (Q' \cap P)$$

pelo Lema 3.16(ii). Como $Q \cap (Q' \cap P) = 0$, resulta que $Q' \cap P$ é um complemento de Q em P, logo P é complementado.

Pelo Teorema 3.12, P é completamente redutível, logo $P = \mathrm{Soc}(P)$. Como $P \leq M$ implica $\mathrm{Soc}(P) \leq \mathrm{Soc}(M)$, obtemos $P \leq \mathrm{Soc}(M)$ e logo $P = \mathrm{Soc}(M)$ como pretendíamos. □

Corolário 3.19 *As condições seguintes são equivalentes para um módulo M:*

(i) M é semi-simples;

(ii) M não tem submódulos essenciais próprios.

Dem. (i) ⇒ (ii). Se $M = \mathrm{Soc}(M)$, resulta do teorema anterior que

$$M = \cap\{N \leq M \mid N \text{ é essencial em } M\},$$

logo o único submódulo essencial de M é o próprio M.

(ii) ⇒ (i). Se M não tem submódulos essenciais próprios, então

$$\cap\{N \leq M \mid N \text{ é essencial em } M\} = M,$$

logo $M = \mathrm{Soc}(M)$ pelo teorema anterior e consequentemente M é semi-simples. □

3.3 Exercícios

3.1. Mostre que se R é um anel artiniano à esquerda, então $M_n(R)$ é artiniano à esquerda.

3.2. Mostre que se R é um anel artiniano semi-simples, então $M_n(R)$ é artiniano semi-simples.

3.3. Seja R um domínio e seja $n \in \mathbb{N}$ tal que $M_n(R)$ é artiniano semi-simples. Mostre que R é um anel de divisão.

3.4. Dado um anel R, o *centro* $Z(R)$ de R é composto por todos os elementos de R que comutam com todos os outros. Mostre que:

a) se R é simples, $Z(R)$ é um corpo;

b) se R é artiniano semi-simples, $Z(R)$ é um produto directo finito de corpos.

3.5. Mostre que, para todo o módulo M, $\mathrm{Soc}(M)$ é o maior submódulo semi-simples de M.

3.6. Seja M um R-módulo. Mostre que se $R/\mathrm{Ann}_R M$ é artiniano semi-simples então M é semi-simples.

3.7. Mostre que um $\mathbb{Z}$-módulo $N \leq \mathbb{Q}$ é essencial se e só se $N \neq 0$.

3.8. Sejam $K \leq N \leq M$ R-módulos. Mostre que K é essencial em M se e só se K é essencial em N e N é essencial em M.

4 O RADICAL DE JACOBSON

Dado um anel R, definimos o *radical de Jacobson* de R como sendo

$$\mathrm{Jac}(R) = \bigcap\{A \trianglelefteq R \mid \ A \text{ é primitivo}\}.$$

Note-se que se $A \lhd R$ é maximal, então R/A é simples e logo primitivo. Como todo o anel tem ideais maximais pelo Teorema 1.6, resulta que todo o anel tem ideais primitivos e logo $\mathrm{Jac}(R)$ está bem definido. Sendo intersecção de ideais, $\mathrm{Jac}(R)$ é ele próprio um ideal. É também claro que um anel R é semiprimitivo se e só se $\mathrm{Jac}(R) = 0$.

Teorema 4.1 *Seja $A \lhd R$.*

(i) Se $A \subseteq Jac(R)$, então $Jac(R/A) = Jac(R) \,/\, A$.

(ii) $R/Jac(R)$ é semiprimitivo.

(iii) Se $Jac(R/A) = 0$ então $Jac(R) \subseteq A$.

Dem. Usamos a notção

$$\begin{array}{ccc} R & \to & R/A \\ r & \mapsto & \overline{r} \end{array}$$

para o homomorfismo canónico.

(i) Se P é um ideal primitivo de R então $A \subseteq \mathrm{Jac}(R) \subseteq P$, logo pelo Teorema do Isomorfismo temos que

$$\overline{R}/\overline{P} = (R/A)/(P/A) \cong R/P$$

é primitivo e $\overline{P}$ é um ideal primitivo de R/A. Reciprocamente, verificamos que todo o ideal primitivo de R/A é desta forma, logo

$$\mathrm{Jac}(R/A) = \bigcap\{\overline{P} \mid \ P \lhd R \text{ é primitivo}\}.$$

É claro que

$$\overline{\bigcap\{P \mid \ P \lhd R \text{ é primitivo}\}} \subseteq \bigcap\{\overline{P} \mid \ P \lhd R \text{ é primitivo}\}.$$

Reciprocamente, seja $\overline{r} \in \bigcap\{\overline{P} \mid \ P \lhd R \text{ é primitivo}\}$. Como $\overline{r} \in \overline{P} \Rightarrow r \in P$ quando $A \subseteq P \trianglelefteq R$, obtemos $r \in \bigcap\{P \mid \ P \lhd R \text{ é primitivo}\}$ e logo

$$\bigcap\{\overline{P} \mid \ P \lhd R \text{ é primitivo}\} \subseteq \overline{\bigcap\{P \mid \ P \lhd R \text{ é primitivo}\}}.$$

Concluimos assim que

$$\mathrm{Jac}(R/A) = \overline{\bigcap\{P \mid \ P \lhd R \text{ é primitivo}\}} = \overline{\mathrm{Jac}(R)}$$

como pretendíamos.

(ii) Fazendo $A = \mathrm{Jac}(R)$ em (i), obtemos

$$\mathrm{Jac}(R/\mathrm{Jac}(R)) = \mathrm{Jac}(R) \,/\, \mathrm{Jac}(R) = 0,$$

logo $R/\mathrm{Jac}(R)$ é semiprimitivo.

(iii) De forma análoga à demonstração de (i), mostramos que

$$\begin{aligned} \overline{\mathrm{Jac}(R)} \ &\subseteq \ \overline{\bigcap\{P \mid \ P \lhd R \text{ é primitivo e } A \subseteq P\}} \\ &= \ \bigcap\{\overline{P} \mid \ P \lhd R \text{ é primitivo e } A \subseteq P\} = \mathrm{Jac}(R/A). \end{aligned}$$

Logo $\mathrm{Jac}(R/A) = 0$ implica $\overline{\mathrm{Jac}(R)} = 0$ e logo $\mathrm{Jac}(R) \subseteq A$. $\square$

Antes de mostrar como o radical de Jacobson pode ser expresso como intersecção de ideais à esquerda, provamos uma caracterização dos ideais primitivos que se revelará de grande utilidade.

Lema 4.2 *Um ideal $P \trianglelefteq R$ é primitivo se e só se $P = Ann_R M$ para algum R-módulo simples M.*

Dem. Suponhamos que P é um ideal primitivo. Então R/P é um anel primitivo que tem consequentemente um módulo simples e fiel M. É claro que podemos ver M como um R-módulo através do produto escalar

$$\begin{array}{rcl} R \times M & \to & M \\ (r, x) & \mapsto & (r + P)x \end{array}$$

É um exercício simples mostrar que os R-submódulos de M são também R/P-submódulos, logo M é simples enquanto R-módulo. Como

$$\mathrm{Ann}_R M = \{r \in R \mid r + P \in \mathrm{Ann}_{R/P} M = 0\},$$

resulta que $\mathrm{Ann}_R M = P$ e a implicação está provada.

Reciprocamente, suponhamos que $P = \mathrm{Ann}_R M$ para algum R-módulo simples M. Podemos ver M como um R/P-módulo através do produto escalar

$$\begin{array}{rcl} R/P \times M & \to & M \\ (r+P, x) & \mapsto & rx \end{array}$$

pois $r + P = r' + P \Rightarrow r - r' \in P = \mathrm{Ann}_R M$ e logo $rx = r'x$. É um exercício elementar mostrar que M é simples e fiel enquanto R/P-módulo. □

Teorema 4.3 *$Jac(R) = \bigcap\{L \lhd_e R \mid$ L é maximal$\}$.*

Dem. Seja $L \lhd_e R$ maximal. Então R/L é um R-módulo simples e logo $\mathrm{Ann}_R(R/L)$ é um ideal primitivo de R pelo resultado anterior. Como

$$r \in \mathrm{Ann}_R(R/L) \Rightarrow r(1+L) = L \Rightarrow r + L = L \Rightarrow r \in L,$$

conclui-se que $\mathrm{Jac}(R) \subseteq \mathrm{Ann}_R(R/L) \subseteq L$ e logo

$$\mathrm{Jac}(R) \subseteq \bigcap\{L \lhd_e R \mid \text{ } L \text{ é maximal}\}.$$

Reciprocamente, seja P um ideal primitivo de R. Pelo lema anterior, temos $P = \mathrm{Ann}_R M$ para algum R-módulo simples M. Seja $x \in M \backslash \{0\}$. Então $\mathrm{Ann}_R x \lhd_e R$. Suponhamos que $\mathrm{Ann}_R x < L \lhd_e R$. Como M é simples, resulta que $Lx = M$, logo $x = ax$ para algum $a \in L$ e

$$1 = a + (1 - a) \in L + \mathrm{Ann}_R x = L.$$

Concluimos assim que $L = R$, portanto $\mathrm{Ann}_R x$ é um ideal à esquerda maximal de R para todo $x \in M \backslash \{0\}$ e

$$P = \mathrm{Ann}_R M = \cap\{\mathrm{Ann}_R x \mid x \in M \backslash \{0\}\}$$

é intersecção de ideais à esquerda maximais de R. Logo

$$\bigcap\{L \lhd_e R \mid \text{ } L \text{ é maximal}\} \subseteq P$$

e consequentemente

$$\bigcap\{L \lhd_e R \mid \text{ } L \text{ é maximal}\} \subseteq \mathrm{Jac}(R)$$

como se pretendia. □

Um elemento $a \in R$ diz-se *quase-invertível à esquerda* se $1-a$ for invertível à esquerda, isto é, se $1 \in R(1-a)$. Se $1-a$ for invertível, dizemos que a é *quase-invertível*. Um subconjunto $S \subseteq R$ diz-se *quase-invertível* (à esquerda) se todos os seus elementos forem quase-invertíveis (à esquerda).

Lema 4.4 *Seja $L \trianglelefteq_e R$. Se L for quase-invertível à esquerda, então L é quase-invertível.*

Dem. Seja $a \in L$ e seja $r \in R$ tal que $r(1-a) = 1$. Então $1-r = -ra \in L$, logo $r = 1-(1-r)$ tem um inverso à esquerda b. Resulta que $b = br(1-a) = 1-a$ e logo $(1-a)r = 1$, pelo que a (e consequentemente L) é quase-invertível. □

Teorema 4.5 *O ideal $Jac(R)$ de R é quase-invertível e contém todos os ideais à esquerda quase-invertíveis de R.*

Dem. Seja $a \in \mathrm{Jac}(R)$. Suponhamos que $R(1-a) \lhd_e R$. Aplicando o Lema de Zorn aos ideais próprios de R que contêm $1-a$, concluimos que existe algum $L \lhd_e R$ maximal tal que $1-a \in L$. Como $a \in L$ pelo Teorema 4.3, obtemos $1 \in L$ e logo $L = R$, absurdo. Logo $R(1-a) = R$ e a é quase-invertível à esquerda. Pelo resultado anterior, $\mathrm{Jac}(R)$ é quase-invertível.

Suponhamos agora que $K \trianglelefteq_e R$ é quase-invertível. Seja $L \lhd_e R$ maximal. Suponhamos que $K \not\subseteq L$. Como L é maximal, então $K + L = R$ e logo $1 = a + b$ para alguns $a \in K$ e $b \in L$. Daqui se conclui que $b = 1 - a$ é invertível e portanto $1 \in L$, absurdo. Logo $K \subseteq L$ e $K \subseteq \mathrm{Jac}(R)$ pelo Teorema 4.3. □

Um elemento $r \in R$ diz-se *nilpotente* se $r^n = 0$ para algum $n \in \mathbb{N}$. Um ideal (respectivamente ideal à esquerda, ideal à direita) A diz-se *nilpotente* se $A^n = 0$ para algum $n \in \mathbb{N}$. Se todos os elementos de A forem nilpotentes, dizemos que A é um *nilideal* (respectivamente nilideal à esquerda, nilideal à direita).

Obviamente, um ideal nilpotente é sempre um nilideal. O recíproco é falso, como mostra o exemplo seguinte.

Exemplo 4.6 *Seja $R = \oplus_{k\in\mathbb{N}} \mathbb{Z} \,/\, 2^k\mathbb{Z}$ e seja*

$$A = \{\sum_{k=1}^{t} 2n_k + 2^k\mathbb{Z} \mid t \geq 0,\ n_k \in \mathbb{Z}\}.$$

Então A é um nilideal de R que não é nilpotente.

Dem. É fácil de ver que $A \trianglelefteq R$ e $(\sum_{k=1}^{t} 2n_k + 2^k\mathbb{Z})^t = 0$, logo A é um nilideal de R.

Para todo $n \in \mathbb{N}$, tem-se $(2 + 2^{n+1}\mathbb{Z})^n = 2^n + 2^{n+1}\mathbb{Z} \neq 0$, logo A não é nilpotente. □

Corolário 4.7 *Todo o nilideal à esquerda de R está contido em $Jac(R)$.*

Dem. Seja N um nilideal à esquerda de R. Pelo Teorema 4.5, basta mostrar que N é quase-invertível. Seja $a \in N$ e seja $t \in \mathbb{N}$ tal que $a^t = 0$. Então

$$1 = 1 - a^t = (1-a)(1+a+a^2+\ldots+a^{t-1}) = (1+a+a^2+\ldots+a^{t-1})(1-a),$$

logo a é quase-invertível e portanto $N \subseteq \mathrm{Jac}(R)$. □

O conceito de nilpotência permite-nos agora provar caracterizações alternativas para os anéis semiprimos.

Teorema 4.8 *As condições seguintes são equivalentes para um anel R:*

(i) R é semiprimo;

(ii) se $A \lhd R$ e $A^2 = 0$, então $A = 0$;

(iii) R não tem ideais nilpotentes não nulos;

(iv) R não tem ideais à esquerda nilpotentes não nulos.

Dem. (i) ⇒ (ii). Suponhamos que R é semiprimo, isto é, que

$$\cap\{P \lhd R \mid \ P \text{ é primo } \} = 0.$$

Seja $A \lhd R$ tal que $A^2 = 0$. Seja $P \lhd R$ primo. Pelo Lema 3.6, $A^2 = 0 \subseteq P$ implica $A \subseteq P$, logo

$$A \subseteq \cap\{P \lhd R \mid \ P \text{ é primo } \} = 0$$

e $A = 0$.

(ii) ⇒ (iii). Se $A \lhd R$ e $A^n = 0$ para algum $n > 1$, então $2n-2 \geq n$ implica $(A^{n-1})^2 = 0$ e logo $A^{n-1} = 0$ por (ii). Repetindo o argumento sucessivamente, acabamos por obter $A = 0$, logo R não tem ideais nilpotentes não nulos.

(iii) $\Rightarrow$ (iv). Se L é um ideal à esquerda nilpotente não nulo de R, então LR é um ideal nilpotente não nulo de R.

(iv) $\Rightarrow$ (i). Suponhamos que R não tem ideais à esquerda nilpotentes não nulos. Seja $r \in R\backslash\{0\}$. Queremos mostrar que existe $P \lhd R$ primo tal que $r \notin P$.

Definimos uma sucessão $s_1, s_2, \ldots$ em $R\backslash\{0\}$ do seguinte modo. Seja $s_1 = r$. Estando s_i definido, tomamos $s_{i+1} \in (s_i R s_i)\backslash\{0\}$. Note-se que nunca pode acontecer $s_i R s_i = 0$, caso contrário Rs_i seria um ideal à esquerda nilpotente não nulo. Seja $S = \{s_1, s_2, \ldots\}$. Resulta facilmente do Lema de Zorn que existe $P \lhd R$ maximal relativamente à propriedade $P \cap S = \emptyset$. Em particular, $r = s_1 \notin P$, logo basta-nos mostrar que P é primo.

Sejam $A, B \trianglelefteq R$ tais que $AB \subseteq P$. Pelo Lema 3.6, basta mostrar que $A \subseteq P$ ou $B \subseteq P$. Suponhamos que $A \not\subseteq P$ e $B \not\subseteq P$. Então $P \subset P+A$ e, por maximalidade de P, $s_i \in P+A$ para algum $i \in \mathbb{N}$. Analogamente, $s_j \in P+B$ para algum $j \in \mathbb{N}$. Prova-se facilmente por indução que $k < l \Rightarrow s_l \in s_k R s_k$. Daqui se conclui que $s_k \in s_i R s_j$ quando $k > i, j$. Em particular,

$$s_k \in (P + A)R(P + B) \subseteq P + AB \subseteq P,$$

contradizendo $P \cap S = \emptyset$. Concluimos assim que $A \subseteq P$ ou $B \subseteq P$ e portanto P é primo. $\square$

Regressamos agora ao contexto dos anéis artinianos (à esquerda). Começamos por apresentar um resultado preliminar.

Teorema 4.9 *Seja M um módulo semi-simples. Então M é artiniano se e só se for noetheriano.*

Dem. Podemos assumir que $M \neq 0$. Construimos uma sucessão (possivelmente finita) $M_1, M_2, \ldots$ de submódulos simples de M do seguinte modo. Seja M_1 um submódulo simples de M. Como M é complementado pelo Teorema 3.12, temos $M = M_1 \oplus N_1$ para algum $N_1 \leq M$. Suponhamos agora que

$$M = M_1 \oplus \ldots \oplus M_k \oplus N_k$$

para $M_1, \ldots, M_k \leq M$ simples e $N_k \leq M$. Caso $N_k = 0$, a sucessão termina aqui. Caso contrário, N_k é complementado pelo Lema 3.11 (e consequentemente semi-simples) e podemos tomar $M_{k+1} \leq N_k$ simples e $N_{k+1} \leq M$ tais que

$$M = M_1 \oplus \ldots \oplus M_{k+1} \oplus N_{k+1}.$$

Se a nossa sucessão for infinita, então as cadeias infinitas

$$M_1 < \oplus_{i=1}^{2} M_i < \oplus_{i=1}^{3} M_i < \dots$$

e

$$\oplus_{i\geq 1} M_i > \oplus_{i\geq 2} M_i > \oplus_{i\geq 3} M_i > \dots$$

mostram que M não pode ser nem artiniano nem noetheriano, logo podemos assumir que a sucessão é finita e consequentemente $M = \oplus_{i=1}^{t} M_i$ para algum $t \in \mathbb{N}$. Mas então, como um módulo simples é trivialmente artiniano e noetheriano, resulta do Corolário 3.2 que M é simultaneamente artiniano e noetheriano. □

Mostramos em seguida uma importante propriedade dos radicais de Jacobson de anéis artinianos à esquerda.

Teorema 4.10 *Se R é artiniano à esquerda, então $Jac(R)$ é nilpotente.*

Dem. Seja $J = \mathrm{Jac}(R)$. Consideremos a cadeia

$$J \geq J^2 \geq J^3 \geq \dots$$

Como R é artiniano à esquerda, temos $J^t = J^{t+1}$ para algum $t \in \mathbb{N}$. Seja $N = J^t$. Então $N = N^2$. Suponhamos que $N \neq 0$. Como R é artiniano à esquerda, possui um ideal à esquerda não nulo L minimal relativamente à propriedade $L = NL$. Seja $a \in L$ tal que $Na \neq 0$. Então $0 \neq Na \subseteq L$ e $Na = N^2a = N(Na)$, logo $L = Na$ por minimalidade de L. Resulta que $a = ra$ para algum $r \in N$ e logo $(1 - r)a = 0$, contrariando o facto de $r \in N \subseteq J$ ser quase-invertível. Logo $J^t = N = 0$ e J é nilpotente. □

O resultado seguinte, conhecido como Teorema de Hopkins-Levitzkii, estabelece a relação existente entre os conceitos de anel artiniano à esquerda e noetheriano à esquerda.

Teorema 4.11 *Um anel R é artiniano à esquerda se e só se satisfizer as seguintes condições:*

(i) R é noetheriano à esquerda;

(ii) $R/Jac(R)$ é artiniano semi-simples;

(iii) Jac(R) é nilpotente.

Dem. Seja $J = \text{Jac}(R)$. Suponhamos que R é artiniano à esquerda. Pelo Lema 3.4, R/J é artiniano à esquerda. Como R/J é além do mais semiprimitivo e logo semiprimo, resulta do Teorema 3.9 que R/J é artiniano semi-simples. Por outro lado, J é nilpotente pelo Teorema 4.10.

Em face disto, podemos assumir que as condições (ii) e (iii) são verificadas, e mostrar que R é artiniano à esquerda se e só se for noetheriano à esquerda. Consideremos a cadeia

$$R = J^0 > J^1 > J^2 > \ldots > J^n = 0$$

e seja $M_i = J^{i-1}/J^i$ para $i = 1, \ldots, n$. Como $JM_i = 0$, podemos ver cada M_i como um R/J-módulo através do produto escalar

$$\begin{array}{rcl} R/J \times M_i & \rightarrow & M_i \\ (r + J, x) & \mapsto & rx. \end{array}$$

Como R/J é artiniano semi-simples, o Teorema 3.13 garante-nos que cada M_i é semi-simples enquanto R/J-módulo. Logo M_i é soma dos seus R/J-submódulos simples, que são também R-submódulos simples, como se pode facilmente verificar. Logo cada M_i é semi-simples enquanto R-módulo.

Se R for artiniano à esquerda, isto é, artiniano enquanto R-módulo, então pelo Teorema 3.1 J^{i-1} e M_i também o são. Logo cada M_i é noetheriano pelo Teorema 4.9. O Teorema 3.1 garante que, para $i = 1, \ldots, t$, $M_i = J^{i-1}/J^i$ e J^i noetherianos implicam J^{i-1} noetheriano. Como $J^t = 0$ é trivialmente noetheriano, uma simples indução permite-nos concluir que $R = J^0$ é noetheriano enquanto R-módulo, ou seja, noetheriano à esquerda.

A implicação recíproca é análoga. □

4.1 APÊNDICE: O Teorema de Amitsur

O resultado seguinte, que fornece condições suficientes para que um anel de polinómios seja semiprimitivo, é conhecido como Teorema de Amitsur.

Teorema 4.12 *Seja R um anel sem nilideais não triviais. Então $R[x]$ é semiprimitivo.*

Dem. Suponhamos que $\mathrm{Jac}(R[x]) \neq 0$. Seja J o conjunto dos polinómios não nulos de $\mathrm{Jac}(R[x])$ com grau mínimo, e seja J_0 o conjunto dos coeficientes-guia dos polinómios de J adicionado do elemento 0. Obviamente, J_0 é um ideal não nulo de R. Vamos mostrar que J_0 é um nilideal.

Seja $p \in J$. Então $xp \in \mathrm{Jac}(R[x])$, logo existe $q \in R[x]$ tal que $(1-xp)q = 1$ pelo Teorema 4.5. Resulta que $q = xpq + 1$, que é o caso $m = 1$ da fórmula

$$q = x^m p^m q + \sum_{i=0}^{m-1} x^i p^i \tag{1}$$

que passamos a provar por indução. Suponhamos que (1) é válida para $m-1$. Então

$$\begin{aligned} q &= x^{m-1}p^{m-1}q + \textstyle\sum_{i=0}^{m-2} x^i p^i = x^{m-1}p^{m-1}(xpq+1) + \sum_{i=0}^{m-2} x^i p^i \\ &= x^m p^m q + \textstyle\sum_{i=0}^{m-1} x^i p^i, \end{aligned}$$

logo (1) é válida para todo m.

Suponhamos que $p = r_0 + r_1 x + \ldots + r_k x^k$ com $r_i \in R$. Se tivermos $a r_k b = 0$ para alguns $a, b \in R$ então apb tem grau $< k$, logo por definição de J temos $apb = 0$. Esta observação será usada repetidamente.

Suponhamos que $q = r'_0 + r'_1 x + \ldots + r'_t x^t$ com $r'_i \in R$. Considere-se $m > t$ em (1). Comparando os coeficientes do monómio x^{m+mk+t} em ambos os lados da igualdade, obtemos $0 = r_k^m r'_t = r_k^{m-1} r_k r'_t$, logo

$$r_k^{m-1} p r'_t = 0$$

pela observação precedente. Logo $r_k^{m-1} r_i r'_t = 0$ para todo i e aplicando de novo o argumento anterior obtemos $r_k^{m-2} p r_i r'_t = 0$, logo

$$r_k^{m-2} p^2 r'_t = 0.$$

Continuando o argumento, obtemos no fim

$$p^m r'_t = 0,$$

logo $x^m p^m r'_t x^t = 0$ e de (1) resulta que

$$q = x^m p^m \sum_{i=0}^{t-1} r'_i x^i + \sum_{i=0}^{m-1} x^i p^i.$$

Repetindo o raciocínio anterior, obtemos $p^m r'_{t-1} = 0$; continuando sucessivamente, obtemos finalmente $p^m r'_0 = 0$ e logo $r_k^m r'_0 = 0$. Mas $q = xpq + 1$ implica $r'_0 = 1$, logo $r_k^m = 0$. Como r_k é um elemento arbitrário de J_0, concluímos que J_0 é um nilideal de R, absurdo.

Logo $\mathrm{Jac}(R[x]) = 0$ e $R[x]$ é semiprimitivo. □

4.2 APÊNDICE: Nilsubsemigrupos de um anel artiniano

O exemplo seguinte mostra-nos como uma propriedade relativa a uma classe geral de anéis pode ser demonstrada partindo de uma classe particular e fazendo uso intermédio do radical de Jacobson.

Dado um anel R, dizemos que $S \subseteq R$ é um *nilsubsemigrupo* de R se S for um subsemigrupo multiplicativo de R constituído por elementos nilpotentes.

Teorema 4.13 *Seja D um anel de divisão, $n \in \mathbb{N}$ e $R = M_n(D)$. Seja S um nilsubsemigrupo de R. Então $S^n = 0$.*

Dem. Vamos usar indução sobre n. O caso $n = 1$ é trivial pois 0 é o único elemento nilpotente de um anel de divisão. Assumimos então que $n > 1$, S é um nilsubsemigrupo de R não nulo e que o teorema é válido para $m < n$.

Seja $L = R\varepsilon_{11}$. Pelo Lema 3.8, L é um ideal à esquerda minimal de R. Considerando L como um D-módulo à direita, temos que a sua dimensão $[L : D]$ é igual a n.

Vamos mostrar que se S_0 é um subconjunto nilpotente de R então $S_0^n = 0$. Note-se que S_0L, o conjunto das somas de produtos de elementos de S_0 por elementos de L, é ainda um D-módulo à direita. Com efeito, se $S_0^n \neq 0$, então $S_0^n L \neq 0$ pois L é fiel pelo Corolário 2.12. Por outro lado, temos $S_0^k L = 0$ para algum $k > n$, pelo que obtemos uma cadeia

$$L \geq S_0L \geq S_0^2L \geq \ldots \geq S_0^{n+1}L$$

de D-módulos à direita. Se $S_0^iL = S_0^{i+1}L$ para algum $i \in \{0, \ldots, n\}$, então $S_0^iL = S_0^kL = 0$ absurdo, pois $S_0^{n+1}L \neq 0$. Logo as inclusões são estritas e obtemos

$$[L : D] > [S_0L : D] > [S_0^2L : D] > \ldots > [S_0^{n+1}L : D],$$

o que contradiz $[L : D] = n$. Logo $S_0^n = 0$.

Consideremos agora o conjunto $\{T \subseteq S \mid T^n = 0\}$ constituído pelos subconjuntos nilpotentes de S. Este conjunto é não vazio, pois qualquer subconjunto de S com um único elemento é nilpotente. É fácil verificar que as condições do Lema de Zorn são satisfeitas, pelo que podemos concluir que existe um subconjunto nilpotente maximal S_0 de S.

Seja $V = S_0L$. Temos $[V : D] = m$ com $0 < m < n$, pois $0 \neq S_0L < L$. Seja

$$S_1 = \{s \in S \mid sV \subseteq V\}.$$

Obviamente, $S_0 \subseteq S_1$ e S_1 é um subsemigrupo de S. Vamos mostrar que $S_1 = S_0$.

Por definição, podemos ver S_1 como um subsemigrupo de endomorfismos do D-módulo à direita V. Como $\mathrm{End}V_D \cong M_m(D)$ pelo dual do Teorema 1.17 e $m < n$, resulta da hipótese de indução que $S_1^m V = 0$. Analogamente, S_1 actua como subsemigrupo de endomorfismos no módulo quociente L/V através de $s(a + V) = sa + V$, e

$$[L/V : D] = n - m < n.$$

Logo, pela hipótese de indução, obtemos

$$S_1^{n-m}(L/V) = \{V\}$$

e consequentemente $S_1^{n-m}L \subseteq V$. Logo $S_1^n L \subseteq S_1^m V = 0$. Como L é fiel, resulta que $S_1^n = 0$ e logo $S_0 = S_1$ por maximalidade de S_0.

Para completar a demonstração, vamos mostrar que $S = S_0$. Suponhamos que $S_0 \subset S$. Se existir $s \in S\backslash S_0$ tal que $sS_0 \subseteq S_0$, então $sS_0L \subseteq S_0L$ e logo $s \in S_1 = S_0$, absurdo. Logo $sS_0 \not\subseteq S_0$ para todo $s \in S\backslash S_0$. Sejam $s_1 \in S\backslash S_0$ e $s_1' \in S_0$ tais que $s_2 = s_1s_1' \in S\backslash S_0$. Indutivamente, dado $s_i \in S\backslash S_0$, tomamos $s_i' \in S_0$ tal que $s_{i+1} = s_is_i' \in S\backslash S_0$. Então

$$s_{n+1} = s_ns_n' = s_{n-1}s_{n-1}'s_n' = \ldots = s_1s_1' \ldots s_n' \in s_1S_0^n = 0,$$

logo $s_{n+1} \in S_0$ absurdo. Logo $S = S_0$ e $S^n = 0$. □

Passar aos anéis artinianos semi-simples é um simples exercício de produtos directos:

Corolário 4.14 *Seja R um anel artiniano semi-simples. Então existe $m \in \mathbb{N}$ tal que $S^m = 0$ para todo o nilsubsemigrupo S de R.*

Dem. Exercício. □

Podemos agora demonstrar a versão geral do resultado:

Teorema 4.15 *Seja R um anel artiniano à esquerda. Então existe $m \in \mathbb{N}$ tal que $S^m = 0$ para todo o nilsubsemigrupo S de R.*

Dem. Seja $J = \mathrm{Jac}(R)$. Pelo Teorema de Hopkins-Levitzkii, R/J é artiniano semi-simples e J é nilpotente. Pelo corolário anterior, existe $n \in N$ tal que $T^n = \{J\}$ para todo o nilsubsemigrupo T de R/J. Seja $t \in \mathbb{N}$ tal que $J^t = 0$ e seja $m = nt$.

Designamos por $\overline{S}$ a projecção de S em R/J. Como $\overline{S}$ é claramente um nilsubsemigrupo de R/J, resulta da definição de n que $\overline{S}^n = \{J\}$. Logo $S^n \subseteq J$ e $S^m = S^{nt} \subseteq J^t = 0$. $\square$

4.3 Exercícios

4.1. Considere a operação $\circ$ em R definida por $r_1 \circ r_2 = r_1 + r_2 - r_1 r_2$. Mostre que $(\mathrm{Jac}(R), \circ)$ é um grupo e que $r \mapsto 1 - r$ define um homomorfismo injectivo do grupo $(\mathrm{Jac}(R), \circ)$ no grupo dos elementos invertíveis de R.

4.2. Seja $(R_i)_{i \in I}$ uma família de anéis. Mostre que

$$\mathrm{Jac}(\prod_{i \in I} R_i) = \prod_{i \in I} \mathrm{Jac}(R_i).$$

4.3. Seja D um domínio de integridade semiprimitivo. Mostre que se D tem apenas um número finito de ideais maximais então D é um corpo.

4.4. Sejam $p, q \in \mathbb{N}$ primos distintos. Determine o radical de Jacobson dos anéis $\mathbb{Z}/p^2\mathbb{Z}$ e $\mathbb{Z}/pq\mathbb{Z}$.

4.5. Mostre que um anel R é semiprimo se e só se, para todos $A, B \trianglelefteq R$, $AB = 0$ implica $A \cap B = 0$.

4.6. Seja R semiprimo e $L_1, L_2 \trianglelefteq_e R$. Mostre que $L_1 L_2 = 0$ se e só se $L_2 L_1 = 0$.

4.7. Seja N um nilideal do anel R e seja $e \in R$ idempotente. Mostre que eNe é um nilideal de eRe.

4.8. Seja R o anel de matrizes

$$\begin{pmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{Q} \end{pmatrix}$$

Calcule $\mathrm{Jac}(R)$ e mostre que $\mathrm{Jac}(R)$ é um ideal nilpotente.

5 MÓDULOS PROJECTIVOS E INJECTIVOS

Designamos um homomorfismo injectivo (de R-módulos) por *monomorfismo* e um homomorfismo sobrectivo (de R-módulos) por *epimorfismo*.

Uma sequência de homomorfismos de R-módulos

$$\ldots M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \ldots$$

diz-se *exacta em* M se $M'\varphi = \mathrm{Ker}\psi$. Uma sequência da forma

$$\ldots \to M_{i-1} \to M_i \to M_{i+1} \to \ldots$$

diz-se *exacta* se for exacta em M_i para todo i. Em particular,

$0 \to M \xrightarrow{\varphi} N$ é exacta se e só se φ é um monomorfismo;

$M \xrightarrow{\varphi} N \to 0$ é exacta se e só se φ é um epimorfismo;

$0 \to M \xrightarrow{\varphi} N \to 0$ é exacta se e só se φ é um isomorfismo.

Uma sequência exacta da forma

$$0 \to K \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$$

diz-se uma sequência exacta *curta*.

Dizemos que um monomorfismo $\varphi : M \to N$ se *cinde* se existir um homomorfismo $\varphi' : N \to M$ tal que $\varphi\varphi' = 1_M$. Analogamente, um epimorfismo $\psi : M \to N$ cinde-se se existir um homomorfismo $\psi' : N \to M$ tal que $\psi'\psi = 1_N$. Dizemos então que φ' (respectivamente ψ') é uma *cisão* de φ (respectivamente ψ).

Teorema 5.1 *Seja*

$$0 \to K \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$$

uma sequência exacta de R-módulos. Então as condições seguintes são equivalentes:

(i) o epimorfismo ψ cinde-se;

(ii) o monomorfismo φ cinde-se;

(iii) $K\varphi$ é parcela directa de M.

Dem. (i) $\Rightarrow$ (ii). Suponhamos que $\psi' : N \to M$ é uma cisão de ψ. Definimos $\varphi' : M \to K$ do seguinte modo. Como $\psi'\psi = 1_N$, temos $(x - x\psi\psi')\psi = 0$ para todo $x \in M$, logo

$$x - x\psi\psi' \in \mathrm{Ker}\psi = M\varphi$$

e podemos definir

$$\varphi' = (1_M - \psi\psi')\varphi^{-1}.$$

É imediato que φ' é um homomorfismo de M em K e

$$\varphi\varphi' = \varphi(1_M - \psi\psi')\varphi^{-1} = (\varphi - \varphi\psi\psi')\varphi^{-1} = \varphi\varphi^{-1} = 1_K.$$

Logo φ cinde-se.

(ii) $\Rightarrow$ (iii). Suponhamos que $\varphi' : M \to K$ é uma cisão de φ. Vamos mostrar que $M = K\varphi \oplus \mathrm{Ker}\varphi'$.

Dado $x \in M$, temos

$$(x - x\varphi'\varphi)\varphi' = x\varphi' - x\varphi'\varphi\varphi' = x\varphi' - x\varphi' = 0,$$

logo $x - x\varphi'\varphi \in \mathrm{Ker}\varphi'$ e $x \in K\varphi + \mathrm{Ker}\varphi'$. Concluimos assim que $M = K\varphi + \mathrm{Ker}\varphi'$. Suponhamos agora que $x \in K\varphi \cap \mathrm{Ker}\varphi'$. Então $x = a\varphi$ para algum $a \in K$ e $a = a\varphi\varphi' = x\varphi' = 0$. Logo $x = 0$ e $M = K\varphi \oplus \mathrm{Ker}\varphi'$.

(iii) $\Rightarrow$ (i). Suponhamos que $M = K\varphi \oplus M'$ para algum $M' \leq M$. Como $\mathrm{Ker}\psi = K\varphi$, resulta facilmente que $\psi \mid_{M'}$ é um isomorfismo de M' em N. Definimos $\psi' = (\psi \mid_{M'})^{-1}$. É imediato que $\psi'\psi = 1_N$, logo ψ cinde-se. $\square$

Se uma sequência exacta curta $0 \to K \to M \to N \to 0$ satisfaz as condições equivalentes do teorema anterior, dizemos que a sequência se *cinde*.

Corolário 5.2 *Se a sequência exacta curta*

$$0 \to K \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$$

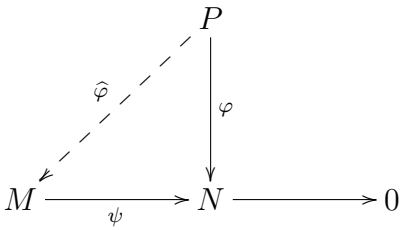
se cinde, então

$$M \cong K \times N.$$

Dem. Resulta da demonstração de (iii) $\Rightarrow$ (i) no teorema anterior que $M = K\varphi \oplus M'$ para algum $M' \leq M$ isomorfo a N. Como $K\varphi \cong K$, obtemos $M \cong K \times N$. $\square$

Dizemos que um R-módulo P é *projectivo* se, para todo o homomorfismo $\varphi : P \to N$ e todo o epimorfismo $\psi : M \to N$, existir um homomorfismo $\widehat{\varphi} : P \to M$ tal que $\widehat{\varphi}\psi = \varphi$.

Esta situação pode ser descrita pelo seguinte diagrama comutativo:



Note-se que a unicidade de $\widehat{\varphi}$ *não* é requerida.

Lema 5.3 *Todo o R-módulo livre é projectivo.*

Dem. Seja P um R-módulo livre de base $\{x_i \mid i \in I\}$. Dados um homomorfismo $\varphi : P \to N$ e um epimorfismo $\psi : M \to N$, podemos escolher, para cada $i \in I$, algum $y_i \in M$ tal que $y_i\psi = x_i\varphi$. Pela propriedade universal dos módulos livres, existe um homomorfismo $\widehat{\varphi} : P \to M$ tal que $x_i\widehat{\varphi} = y_i$ para todo $i \in I$. Logo $x_i\widehat{\varphi}\psi = x_i\varphi$ para todo $i \in I$ e portanto $\widehat{\varphi}\psi = \varphi$. $\square$

Lema 5.4 *Seja $P = \oplus_{i \in I} P_i$ um R-módulo. Então P é projectivo se e só se P_i é projectivo para todo $i \in I$.*

Dem. Para todo $i \in I$, sejam $\iota_i : P_i \to P$ e $\pi_i : P \to P_i$ os homomorfismos canónicos. Seja $\psi : M \to N$ um epimorfismo.

Suponhamos que P é projectivo. Dado um homomorfismo $\varphi_i : P_i \to N$, temos que $\pi_i\varphi_i : P \to N$ é um homomorfismo. Como P é projectivo, existe $\theta : P \to M$ tal que $\theta\psi = \pi_i\varphi_i$. Fazendo $\widehat{\varphi}_i = \iota_i\theta$, obtemos

$$\widehat{\varphi}_i\psi = \iota_i\theta\psi = \iota_i\pi_i\varphi_i = \varphi_i,$$

logo P_i é projectivo para todo $i \in I$.

Reciprocamente, suponhamos que P_i é projectivo para todo $i \in I$. Dado um homomorfismo $\varphi : P \to N$, temos que $\iota_i\varphi : P_i \to N$ é um homomorfismo. Como P_i é projectivo, existe $\theta_i : P_i \to M$ tal que $\theta_i\psi = \iota_i\varphi$. É fácil de ver que $\theta = \sum_{i\in I} \theta_i$ é um homomorfismo de P em N. Além disso,

$$\theta\psi = \sum_{i\in I} \iota_i\theta\psi = \sum_{i\in I} \theta_i\psi = \sum_{i\in I} \iota_i\varphi = \varphi,$$

logo P é projectivo. □

Estamos agora em condições de apresentar diversas caracterizações alternativas do conceito de módulo projectivo.

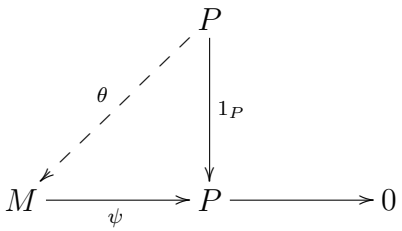
Teorema 5.5 *As condições seguintes são equivalentes para um R-módulo P:*

(i) P é projectivo;

(ii) todo o epimorfismo $\psi : M \to P$ se cinde;

(iii) P é parcela directa de um R-módulo livre.

Dem. (i) ⇒ (ii). Suponhamos que P é projectivo e seja $\psi : M \to P$ um epimorfismo de R-módulos. Considerando o diagrama comutativo



concluimos que existe $\theta : P \to M$ tal que $\theta\psi = 1_P$, logo ψ cinde-se.

(ii) $\Rightarrow$ (iii). Seja M um R-módulo livre tal que existe um epimorfismo $\psi : M \to P$ (a existência de um tal módulo demonstra-se escolhendo uma base em bijecção com um conjunto de geradores de P e aplicando a propriedade universal). Como ψ se cinde por hipótese, existe $\psi' : P \to M$ tal que $\psi'\psi = 1_P$. Consideremos a sequência exacta

$$0 \to \mathrm{Ker}\psi \to M \xrightarrow{\psi} P \to 0.$$

Pelo Corolário 5.2, temos $M \cong \mathrm{Ker}\psi \oplus P$, logo P é parcela directa de um R-módulo livre.

(iii) $\Rightarrow$ (i). Pelos dois lemas anteriores. $\square$

Voltamos a recorrer nos resultados seguintes ao conceito de elemento idempotente de um anel.

Lema 5.6 *Se $e \in R$ é idempotente, então $R = Re \oplus R(1-e)$.*

Dem. Como $1 = e + (1-e)$, temos $R = Re + R(1-e)$. Suponhamos que $re = r'(1-e)$ com $r, r' \in R$. Então

$$re = re^2 = r'(1-e)e = r(e-e^2) = 0,$$

logo $Re \cap R(1-e) = 0$ e $R = Re \oplus R(1-e)$. $\square$

Teorema 5.7 *Um R-módulo P é cíclico e projectivo se e só se $P \cong Re$ para algum $e \in R$ idempotente.*

Dem. Suponhamos que P é cíclico e projectivo. Resulta da demonstração de (ii) $\Rightarrow$ (iii) no teorema anterior que P é isomorfo a uma parcela directa de um R-módulo livre cíclico M. Como $M \cong R$, concluimos que $P \cong P'$ para alguma parcela directa P' de R. Consideremos a projecção $\pi : R \to P'$ e definamos $e = 1\pi$. Então

$$r\pi = (r \cdot 1)\pi = r(1\pi) = re$$

para todo $r \in R$, logo $P' = R\pi = Re$. Daqui resulta em particular que $e^2 = e\pi = e$, pois a projecção π fixa os elementos de P'. Logo e é idempotente e $P \cong P' = Re$.

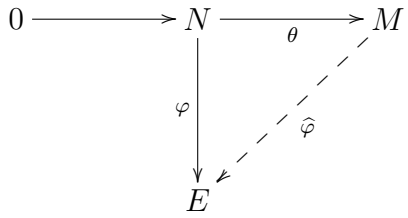
Reciprocamente, suponhamos que $P \cong Re$ para algum $e \in R$ idempotente. Como Re é cíclico, P é cíclico. Além disso, $R = Re \oplus R(1-e)$ pelo lema anterior. Como R é livre e logo projectivo, Conclui-se do Teorema 5.5 que Re é projectivo. Logo P é projectivo. $\square$

Exemplo 5.8 *Nem todos os módulos projectivos são livres.*

Dem. Seja $R = M_2(\mathbb{Z}_2)$ e seja $L = R\varepsilon_{11}$. Pelo corolário anterior, L é um R-módulo projectivo. No entanto, L não pode ser um R-módulo livre (isomorfo a uma soma directa de cópias de R) pois $|L| = 4$ e $|R| = 16$. $\square$

Dizemos que um R-módulo E é *injectivo* se, para todo o homomorfismo $\varphi : N \to E$ e todo o monomorfismo $\theta : N \to M$, existir um homomorfismo $\widehat{\varphi} : M \to E$ tal que $\theta\widehat{\varphi} = \varphi$.

Esta situação pode ser descrita pelo seguinte diagrama comutativo:



Como o monomorfismo θ mergulha N em M, é habitual dizer que $\widehat{\varphi}$ *estende* φ. Tal como no caso da definição de módulo projectivo, a unicidade de $\widehat{\varphi}$ *não* é requerida.

A caracterização seguinte dos módulos injectivos é conhecida por *Critério de Baer*:

Teorema 5.9 *As seguintes condições são equivalentes para um R-módulo E:*

(i) E é injectivo;

(ii) para todo $L \trianglelefteq_e R$, qualquer homomorfismo $\varphi : L \to E$ pode ser estendido a um homomorfismo $\widehat{\varphi} : R \to E$.

Dem. (i) $\Rightarrow$ (ii). Trivial.

(ii) $\Rightarrow$ (i). Suponhamos que a condição (ii) é verificada. Sejam M e N R-módulos e $\varphi : N \to E$ um homomorfismo. Sem perda de generalidade, podemos assumir que $N \leq M$ e que o monomorfismo θ na definição de módulo injectivo é a inclusão. Queremos então mostrar que φ pode ser estendido a um homomorfismo $\widehat{\varphi} : M \to E$.

Definimos

$$\mathcal{L} = \{(N', \varphi') \mid N \leq N' \leq M,\ \varphi' : N' \to E \text{ é homomorfismo e } \varphi' \mid_N = \varphi\}.$$

Definimos uma ordem parcial em $\mathcal{L}$ por

$$(N', \varphi') \leq (N'', \varphi'') \text{ se } N' \leq N'' \text{ e } \varphi'' \mid_{N'} = \varphi'.$$

É um exercício de rotina mostrar que $\mathcal{L}$ satisfaz as condições do Lema de Zorn, logo tem um elemento maximal (N_0, φ_0). Queremos mostrar que $N_0 = M$.

Suponhamos que $N_0 < M$. Seja $x \in M \backslash N_0$ e seja

$$L = \{r \in R \mid rx \in N_0\}.$$

Obviamente, temos $L \trianglelefteq_e R$. Definimos

$$\begin{array}{rcl} \psi : L & \to & E \\ a & \mapsto & (ax)\varphi_0 \end{array}$$

que é claramente um homomorfismo de R-módulos. Por hipótese, podemos estender ψ a um homomorfismo $\widehat{\psi} : R \to E$. Seja $x' = 1\widehat{\psi}$. Definimos uma função

$$\begin{array}{rcl} \varphi_1 : N_0 + Rx & \to & E \\ y + rx & \mapsto & y\varphi_0 + rx'. \end{array}$$

Vejamos que φ_1 está bem definida. Suponhamos que $y_1 + r_1 x = y_2 + r_2 x$ com $y_1, y_2 \in N_0$ e $r_1, r_2 \in R$. Então $(r_2 - r_1)x = y_1 - y_2 \in N_0$, logo $r_2 - r_1 \in L$ e

$$\begin{array}{rcl} y_1\varphi_0 + r_1 x' - y_2\varphi_0 - r_2 x' & = & (y_1 - y_2)\varphi_0 + (r_1 - r_2)x' \\ & = & (y_1 - y_2)\varphi_0 + (r_1 - r_2)\widehat{\psi} \\ & = & (y_1 - y_2)\varphi_0 + (r_1 - r_2)\psi \\ & = & (y_1 - y_2 + (r_1 - r_2)x)\varphi_0 \\ & = & 0\varphi_0 = 0, \end{array}$$

logo φ_1 está bem definida. É pura rotina verificar que φ_1 é um homomorfismo que estende φ_0 e $\varphi_1 \mid_N = \varphi$. Logo $(N_0 + Rx, \varphi_1) \in \mathcal{L}$. Como $N_0 < N_0 + Rx$, obtemos

$$(N_0, \varphi_0) < (N_0 + Rx, \varphi_1),$$

em $\mathcal{L}$, contradizendo a maximalidade de (N_0, φ_0). Logo $N_0 = M$ e portanto E é injectivo. $\square$

O resultado seguinte fornece-nos uma nova caracterização dos anéis artinianos semi-simples associada aos conceitos introduzidos nesta secção.

Teorema 5.10 *As seguintes condições são equivalentes para um anel R:*

(i) R é artiniano semi-simples;

(ii) toda a sequência exacta curta de R-módulos cinde-se;

(iii) todo o R-módulo é projectivo;

(iv) todo o R-módulo é injectivo.

Dem. (i) $\Rightarrow$ (iii). Suponhamos que R é artiniano semi-simples. Seja $\psi : M \to P$ um epimorfismo de R-módulos. Pelo Teorema 3.13, M é complementado e logo temos $M = \mathrm{Ker}\psi \oplus M'$ para algum $M' \leq M$. É imediato que $\psi\mid_{M'}: M' \to P$ é um isomorfismo, logo

$$(\psi\mid_{M'})^{-1} : P \to M'$$

é uma cisão de ψ. Pelo Teorema 5.5, P é projectivo. Como P é arbitrário, concluimos que todo o R-módulo é projectivo.

(iii) $\Rightarrow$ (ii). Se todo o R-módulo é projectivo, resulta do Teorema 5.5 que todo o epimorfismo de R-módulos se cinde. Deduzimos assim que toda a sequência exacta curta de R-módulos se cinde.

(ii) $\Rightarrow$ (iv). Seja $\varphi : L \to E$ um homomorfismo de R-módulos, com $L \trianglelefteq_e R$. Como a sequência exacta curta

$$0 \to L \to R \to R/L \to 0$$

se cinde, L é parcela directa de R e logo $R = L \oplus L'$ para algum $L' \trianglelefteq_e R$. Seja $\pi : R \to L$ a projecção canónica e seja $\widehat{\varphi} = \pi\varphi$. é imediato que $\widehat{\varphi} : R \to E$ é um homomorfismo que estende φ, logo E é injectivo pelo Critério de Baer. Como E é arbitrário, concluimos que todo o R-módulo é injectivo.

(iv) $\Rightarrow$ (i). Seja $L \trianglelefteq_e R$ e consideremos o homomorfismo $1_L : L \to L$. Como L é por hipótese injectivo, podemos estender 1_L a um homomorfismo $\varphi : R \to L$. Vejamos que $R = L \oplus \mathrm{Ker}\varphi$.

Dado $r \in R$, temos $r = (r - r\varphi) + r\varphi$. Como $r\varphi \in L$ e

$$(r - r\varphi)\varphi = r\varphi - r\varphi\varphi = r\varphi - r\varphi = 0,$$

conclui-se que $r \in L + \mathrm{Ker}\varphi$. Logo $R = L + \mathrm{Ker}\varphi$. Suponhamos agora que $r \in L \cap \mathrm{Ker}\varphi$. Como $r = r\varphi = 0$, obtemos $R = L \oplus \mathrm{Ker}\varphi$. Logo R é complementado enquanto R-módulo e, pelo Teorema 3.13, R é um anel artiniano semi-simples. $\square$

Terminamos o nosso curso introduzindo uma nova classe de anéis. Um anel R diz-se *regular* se, para todo $r \in R$, existir algum $s \in R$ tal que $rsr = r$.

Teorema 5.11 *As seguintes condições são equivalentes para um anel R:*

(i) *R é regular;*

(ii) *todo o ideal à esquerda principal de R é gerado por um idempotente;*

(iii) *todo o ideal à esquerda finitamente gerado de R é gerado por um idempotente;*

(iv) *todo o ideal à esquerda finitamente gerado de R é parcela directa de R.*

Dem. (i) $\Rightarrow$ (ii). Seja $L = Rr$ um ideal à esquerda principal de R. Sendo R regular, temos $rsr = r$ para algum $s \in R$. Como

$$L = Rr = Rrsr \leq Rsr \leq Rr = L,$$

obtemos $L = Rsr$. Como $(sr)^2 = sr$, concluimos que L é gerado pelo idempotente sr.

(ii) $\Rightarrow$ (iii). Vamos mostrar que se $e, f \in R$, então $L = Re + Rf$ é um ideal à esquerda principal de R. O caso geral de um ideal à esquerda finitamente gerado $Re_1 + \ldots + Re_n$ resulta facilmente deste por indução.

Por (ii), podemos assumir que e e f são ambos idempotentes. Verifica-se facilmente que $L = Re + R(f - fe)$. Por hipótese, temos $R(f - fe) = Rg$ para algum $g \in R$ idempotente. Então $ge \in R(f - fe)e = 0$, logo

$$g = g(g - e) \in R(g - e), \qquad e = g - (g - e) \in R(g - e).$$

Conclui-se assim que

$$L = Re + R(f - fe) = Re + Rg = R(g - e),$$

logo L é principal e a condição (iii) verifica-se.

(iii) $\Rightarrow$ (iv). Resulta da igualdade $R = Re \oplus R(1 - e)$ (Lema 5.6).

(iv) $\Rightarrow$ (i). Seja $r \in R$. Como Rr é parcela directa de R, existe algum $L \trianglelefteq_e R$ tal que $R = Rr \oplus L$. Em particular, $1 = sr + a$ para alguns $s \in R$ e $a \in L$. Logo $r = rsr + ra$. Como $ra = r - rsr$, resulta que $ra \in Rr \cap L = 0$, logo $r = rsr$ e R é consequentemente regular. $\square$

Podemos agora apresentar mais uma caracterização dos anéis artinianos semi-simples.

Teorema 5.12 *Um anel R é artiniano semi-simples se e só se é noetheriano à esquerda e regular.*

Dem. Suponhamos que R é um anel artiniano semi-simples. Pelo Teorema de Hopkins-Levitzkii, R é noetheriano à esquerda. Por outro lado, resulta do Teorema 3.13 que R é complementado enquanto R-módulo. Em particular, todo o ideal à esquerda finitamente gerado de R é parcela directa de R, logo R é regular pelo teorema anterior.

Reciprocamente, suponhamos que R é noetheriano à esquerda e regular. Pelo Teorema 3.13, basta mostrar que R é complementado enquanto R-módulo. Seja $L \trianglelefteq_e R$. Definimos uma sucessão $a_1, a_2, \ldots$ de elementos de L do seguinte modo. Seja $a_1 \in L$ qualquer. Se $a_1, \ldots, a_n \in L$ estão definidos e $L = Ra_1 + \ldots + Ra_n$, a sucessão termina em a_n. Caso contrário, escolhemos

$$a_{n+1} \in L \backslash (Ra_1 + \ldots + Ra_n).$$

Se a sucessão $a_1, a_2, \ldots$ fosse infinita, teríamos uma cadeia infinita da forma

$$Ra_1 < Ra_1 + Ra_2 < Ra_1 + Ra_2 + Ra_3 < \ldots < L,$$

contradizendo o facto de R ser noetheriano à esquerda. Logo a sucessão é finita e temos portanto $L = Ra_1 + \ldots + Ra_n$ para algum $n \in N$. Concluimos assim que L é finitamente gerado. Como R é regular, resulta do teorema anterior que L é parcela directa de R. Logo R é complementado enquanto R-módulo e consequentemente artiniano semi-simples. □

5.1 APÊNDICE: Anéis hereditários

Um anel R diz-se *hereditário* se todo o ideal à esquerda de R for projectivo. A classe dos domínios de ideais à esquerda principais constitui um caso particular importante:

Lema 5.13 *Todo o domínio de ideais à esquerda principais é hereditário.*

Dem. Seja R um domínio de ideais à esquerda principais e seja $L \trianglelefteq_e R$. Então $L = Ra$ para algum $a \in R$. Se $a = 0$ então L é trivialmente projectivo, logo podemos assumir que $a \neq 0$. Como R é um domínio, resulta que

$$\begin{array}{rcl} \varphi : R & \to & L \\ r & \mapsto & ra \end{array}$$

é um isomorfismo de R-módulos, logo $L \cong R$ é livre e portanto projectivo. Logo R é hereditário. $\square$

Vamos agora caracterizar os submódulos dos módulos livres.

Teorema 5.14 *Seja R um anel hereditário e seja F um R-módulo livre. Então todo o submódulo de F é isomorfo a uma soma directa de ideais à esquerda de R.*

Dem. Para simplificar a demonstração, vamos assumir que F tem uma base finita $\{x_1, x_2, \ldots, x_n\}$. Para cada $i \in \{1, \ldots, n+1\}$ seja $F_i = \oplus_{j<i} Rx_j \leq F$ e definamos

$$\begin{array}{rcl} \pi_i : F_i \oplus Rx_i & \to & R \\ y_i + rx_i & \mapsto & r \end{array}$$

para $i = 1, \ldots, n$. É imediato que π_i é um homomorfismo de R-módulos.

O teorema é trivialmente válido para o submódulo F. Suponhamos que $M < F$. Seja $M_i = M \cap F_{i+1}$ para $i = 0, \ldots, n$ e $\varphi_i = \pi_i \mid_{M_i}$ para $i = 1, \ldots, n$. Seja $i \in \{0, \ldots, n-1\}$.Temos

$$\text{Ker}\varphi_{i+1} = F_{i+1} \cap M_{i+1} = F_{i+1} \cap M \cap F_{i+2} = F_{i+1} \cap M = M_i.$$

Seja $L_i = M_{i+1}\varphi_{i+1}$ que é um ideal à esquerda de R. Obtemos uma sequência exacta

$$0 \to M_i \to M_{i+1} \xrightarrow{\varphi_{i+1}} L_i \to 0.$$

Como L_i é projectivo pela hereditariedade de R, a sequência cinde-se pelo Teorema 5.5. Logo, pelo Corolário 5.2, obtemos $M_{i+1} \cong M_i \oplus L_i$. Como $M_0 = 0$, resulta facilmente por indução que

$$M = M_n \cong \oplus_{i=0}^{n-1} L_i.$$

$\square$

Podemos agora obter uma caracterização alternativa dos anéis hereditários.

Corolário 5.15 *Um anel R é hereditário se e só se todo o submódulo de um R-módulo projectivo for projectivo.*

Dem. Suponhamos que R é hereditário e seja $N \leq P$, onde P é um R-módulo projectivo. Como P é parcela directa de um módulo livre, N é submódulo de um módulo livre, e resulta do teorema anterior que N é soma directa de R-módulos projectivos. Logo N é projectivo pelo Lema 5.4.

A implicação recíproca resulta do facto de todo o ideal à esquerda de R ser submódulo de R, que é livre e logo projectivo. □

Corolário 5.16 *Seja R um domínio de ideais à esquerda principais. Então todo o R-módulo projectivo é livre.*

Dem. Seja P um R-módulo projectivo (não nulo). Pelo Lema 5.13, R é hereditário e logo, pelo Teorema 5.14, P é isomorfo a uma soma directa de ideais à esquerda (não nulos) de R. Vimos na demonstração do Lema 5.13 que estes ideais à esquerda são isomorfos a R enquanto R-módulos, logo P é livre. □

Em particular, como $\mathbb{Z}$ é um domínio de ideais à esquerda principais, resulta que os $\mathbb{Z}$-módulos projectivos são precisamente os $\mathbb{Z}$-módulos livres.

5.2 APÊNDICE: $\mathbb{Z}$-módulos injectivos

Dado um elemento $r \in R$, dizemos que r é um *divisor de zero* se $rr' = 0$ ou $r'r = 0$ para algum $r' \in R\backslash\{0\}$. Um R-módulo M diz-se *divisível* se, para todos $x \in M$ e $r \in R$ que não seja divisor de zero, existir $y \in M$ tal que $x = ry$.

Exemplo 5.17 *O $\mathbb{Z}$-módulo $\mathbb{Q}$ é divisível.*

A divisibilidade é uma condição necessária para um módulo ser injectivo:

Teorema 5.18 *Todo o R-módulo injectivo é divisível.*

Dem. Seja E um R-módulo injectivo. Seja $x \in E$ e seja $r \in R$ não divisor de zero. Podemos definir um homomorfismo de R-módulos

$$\begin{array}{rcl} \varphi : Rr & \to & E \\ r'r & \mapsto & r'x \end{array}$$

que está bem definido por r não ser divisor de zero. Pelo Critério de Baer, podemos estender φ a um homomorfismo $\widehat{\varphi} : R \to E$. Seja $y = 1\widehat{\varphi}$. Então

$$x = r\varphi = (r1)\widehat{\varphi} = r(1\widehat{\varphi}) = ry$$

e portanto E é divisível. □

Podemos produzir um recíproco parcial para o resultado anterior:

Teorema 5.19 *Se R é um domínio de ideais à esquerda principais, então todo o R-módulo divisível é injectivo.*

Dem. Seja M um R-módulo divisível. Seja $L \lhd_e R$ e seja $\varphi : L \to M$ um homomorfismo de R-módulos. Como R é um domínio de ideais à esquerda principais, temos $L = Ra$ para algum $a \in R$. Sem perda de generalidade, podemos assumir que $a \neq 0$. Como R é um domínio, a não é divisor de zero, logo $a\varphi = ay$ para algum $y \in M$ pois M é divisível. Seja

$$\begin{array}{rcl} \widehat{\varphi} : R & \to & M \\ r & \mapsto & ry, \end{array}$$

que é um homomorfismo de R-módulos. Para todo $r \in R$, temos

$$(ra)\widehat{\varphi} = ray = r(a\varphi) = (ra)\varphi,$$

logo $\widehat{\varphi}$ estende φ. Pelo Critério de Baer, concluímos que M é injectivo. □

Como $\mathbb{Z}$ é um domínio de ideais à esquerda principais, resulta que os $\mathbb{Z}$-módulos injectivos são precisamente os $\mathbb{Z}$-módulos divisíveis. Vamos ver em seguida que todo o $\mathbb{Z}$-módulo pode ser mergulhado num $\mathbb{Z}$-módulo injectivo. Principiamos por apresentar um resultado preliminar.

Lema 5.20 *(i) Todo o quociente de um módulo divisível é divisível.*

(ii) Todo o produto directo de módulos divisíveis é divisível.

Dem. Exercício. □

Teorema 5.21 *Todo o $\mathbb{Z}$-módulo pode ser mergulhado num $\mathbb{Z}$-módulo injectivo.*

Dem. Para simplificar a demonstração, vamos limitar-nos a provar o caso em que o módulo é finitamente gerado. Atendendo ao Teorema 1.24 e à parte (ii) do lema anterior, basta-nos considerar o caso dos $\mathbb{Z}$-módulos $\mathbb{Z}$ e $Z/n\mathbb{Z}$, onde $n \geq 2$.

O caso de $\mathbb{Z}$ é imediato, pois mergulha em $\mathbb{Q}$ que é divisível e logo injectivo. Fixemos agora $n \geq 2$ e definamos $\mathbb{Q}_n$ como sendo o subconjunto de $\mathbb{Q}$ constituído por todas as fracções do tipo $\frac{p}{q}$, onde $(p, q) = 1$ e $n \mid p$. É um simples exercício provar que $\mathbb{Q}_n \leq \mathbb{Q}$ como $\mathbb{Z}$-módulo. Consideremos o homomorfismo canónico $\varphi : \mathbb{Z} \to \mathbb{Q}/\mathbb{Q}_n$. Como $\mathbb{Z} \cap \mathbb{Q}_n = n\mathbb{Z}$, temos $\text{Ker}\varphi = n\mathbb{Z}$ e resulta do teorema do homomorfismo que

$$\begin{array}{rcl} \overline{\varphi} : \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Q}/\mathbb{Q}_n \\ k + n\mathbb{Z} & \mapsto & k + \mathbb{Q}_n \end{array}$$

é um monomorfismo de $\mathbb{Z}$-módulos. Como $\mathbb{Q}$ é divisível, resulta do lema anterior que $\mathbb{Q}/\mathbb{Q}_n$ é divisível e logo injectivo. Logo $Z/n\mathbb{Z}$ pode ser mergulhado num $\mathbb{Z}$-módulo injectivo. □

Este resultado pode ser utilizado para provar o teorema mais geral que afirma que qualquer R-módulo pode ser mergulhado num R-módulo injectivo, mas a demonstração ultrapassa as fronteiras deste curso.

5.3 Exercícios

5.1. Mostre que $\mathbb{Q}$ não é um $\mathbb{Z}$-módulo projectivo.

5.2. Mostre que se todo o R-módulo cíclico é projectivo então R é um anel artiniano semi-simples (*Sugestão*: observe que para todo $L \lhd_e R$, R/L é um R-módulo cíclico).

5.3. Seja $p \in \mathbb{N}$ primo. Mostre que existe uma sequência exacta curta da forma

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$$

que não se cinde.

5.4. Mostre que o anel $\mathbb{Q} \times \mathbb{Q}$ é hereditário.

5.5. Mostre que um domínio regular é um anel de divisão.

5.6. Mostre que um anel R é regular se e só se $IJ = I \cap J$ para todos $I \trianglelefteq_d R$ e $J \trianglelefteq_e R$. Mostre que se R for comutativo, então é regular se e só se $I^2 = I$ para todo $I \trianglelefteq R$.

5.7. Seja R um anel regular. Mostre que:

a) para todo $a \in R$, existe $b \in R$ tal que $aba = a$ e $bab = b$;

b) $Z(R)$ é regular.

5.8. Mostre que não existem $\mathbb{Z}$-módulos injectivos finitamente gerados não nulos.

Bibliografia

1. N. Jacobson, Basic Algebra I and II (second edition), W. H. Freeman 1985.

2. S. Lang, Algebra, Addison-Wesley 1993.

3. D. S. Passman, The Algebraic Structure of Group Rings, John Wiley 1977.

4. L. H. Rowen, Ring Theory I, Academic Press 1988.