CAPÍTULO 1

Preliminares

Neste primeiro capítulo, resumimos vários conceitos e resultados básicos sobre anéis e sobre módulos sobre anéis que serão usados ao longo do curso. Muitos desses conceitos serão interpretados na linguagem da teoria de álgebras que, em geral, consideramos sobre um corpo e assumimos serem de dimensão finita. O nosso objectivo primordial é o de aplicar estes conceitos à teoria da representação de álgebras e, mais particularmente, à teoria da representação de grupos finitos.

1.1. Generalidades sobre anéis

1.1.1. Um *anel* $(R, +, \cdot)$ é um conjunto R, munido de duas operações binárias: a adição $(a, b) \mapsto a + b$ e a multiplicação $(a, b) \mapsto a \cdot b$, tais que:

(a) $(R, +)$ é um grupo abeliano com elemento neutro 0 (ou 0_R).

(b) $(R, \cdot)$ é um semigrupo com identidade 1 (ou 1_R) – de modo que $\cdot$ é associativa e $a \cdot 1 = 1 \cdot a = a$ para todo $a \in R$.

(c) Valem as leis distributivas à esquerda e à direita:

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

[A multiplicação não é necessariamente comutativa.]

Por convenção, escrevemos ab em vez de $a \cdot b$ e referimo-nos a um anel apenas por R (subentendendo as operações $+$ e $\cdot$).

De agora em diante, salvo menção em contrário, R denota um anel arbitrário.

1.1.2. Para quaisquer $a, b, c \in R$, tem-se:

(a) $a0 = 0a = 0$.

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

(c) $(-a)(-b) = ab$;

(d) $a(b - c) = ab - ac$ e $(a - b)c = ac - bc$.

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

Permitimos que $1 = 0$ e, neste caso, temos $R = \{0\}$ – de facto, $a = a \cdot 1 = a \cdot 0 = 0$ para todo $a \in R$.

1.1.3. Dizemos que um elemento $a \in R$ é:

- um *divisor de zero esquerdo* se existe $0 \neq b \in R$ tal que $ab = 0$;
- um *divisor de zero direito* se existe $0 \neq b \in R$ tal que $ba = 0$.

Dizemos que R é um *domínio* (ou um *domínio de integridade*) se $R \neq \{0\}$ e se, para quaisquer $a, b \in R$,

$$ab = 0 \quad \Longrightarrow \quad a = 0 \text{ ou } b = 0.$$

Sendo assim, num domínio, não existem divisores de zero, nem esquerdo, nem direito.

1.1.4. Dizemos que um elemento $a \in R$ é:

- um *invertível à esquerda* se existe $a' \in R$ tal que $aa' = 1$ e, neste caso, a' diz-se um *inverso direito* de a;
- um *invertível à direita* se existe $a'' \in R$ tal que $a''a = 1$ e, neste caso, a'' diz-se um *inverso esquerdo* de a.

Se $a \in R$ tem um inverso direito $a' \in R$ e, também, um inverso esquerdo $a'' \in R$, então

$$a'' = a'' \cdot 1 = a''(aa') = (a''a)a' = 1 \cdot a' = a'.$$

Nesta situação, dizemos que a é um *elemento invertível* (ou uma *unidade*) de R e dizemos que $a' = a''$ é o *inverso* de a; prova-se que este inverso é de facto único, o que permite denotá-lo por a^{-1}.

Denotamos por $R^\times$ (ou por $U(R)$) o conjunto de todos os elementos invertíveis de R; é fácil verificar que $R^\times$ é um grupo multiplicativo com respeito à multiplicação de R.

Dizemos que R é um *anel de divisão* se $R \neq \{0\}$ e $R^\times = R \setminus \{0\}$. Um *corpo* é (por definição) um anel de divisão comutativo.

1.1.5. Definimos a *característica* de R, que denotamos por $\mathrm{car}(R)$, como sendo o menor número natural n tal que $n \cdot 1 = 0$; para qualquer $n \in \mathbb{N}$, definimos $n \cdot 1 = 1 + \cdots + 1$ (n parcelas). No caso em que $n \cdot 1 \neq 0$ para todo $n \in \mathbb{N}$, definimos $\mathrm{car}(R) = 0$.

1.1.6. Lema. *Se R é um domínio de integridade, então, ou $\mathrm{car}(R) = 0$, ou $\mathrm{car}(R)$ é um número primo.*

Demonstração. Exercício. □

1.1.7. Um subconjunto $S \subseteq R$ diz-se um *subanel*, e escrevemos $S \leq R$, se:

(a) $1 \in S$;

(b) se $a, b \in S$, então $a - b \in S$;

(c) se $a, b \in S$, então $ab \in S$.

É fácil verificar que qualquer subanel de R é um anel com respeito às operações de R.

1.1.8. Exemplo (*Produto directo de anéis*). Seja I um conjunto de índices e, para cada $i \in I$, seja R_i um anel. Definimos o *produto directo* $\prod_{i\in I} R_i$ como sendo o conjunto

$$\prod_{i\in I} R_i = \big\{(a_i)_{i\in I} \colon a_i \in R_i,\ i \in I\big\};$$

trata-se de um anel com respeito às operações definidas naturalmente componente-a-componente:

$$(a_i)_{i\in I} + (b_i)_{i\in I} = (a_i + b_i)_{i\in I} \quad \text{e} \quad (a_i)_{i\in I} \cdot (b_i)_{i\in I} = (a_i b_i)_{i\in I}$$

para quaisquer $a_i, b_i \in R_i$, $i \in I$.

No caso em que $I = \{i_1, \ldots, i_n\}$ é finito, também escrevemos $R_{i_1} \times \cdots \times R_{i_n}$ em vez de $\prod_{i\in I} R_i$.

Se $R_i = R$ para todo $i \in I$, escrevemos R^I em vez de $\prod_{i\in I} R_i$, isto é,

$$R^I = \prod_{i\in I} R.$$

No caso em que I é finito com n elementos, temos

$$R^I = R^n = \big\{(a_1, \ldots, a_n) \colon a_1, \ldots, a_n \in R\big\};$$

para evitar confusões(*), usamos a notação $R^{(n)}$ em vez de R^n.

1.1.9. Exemplo (*Anéis de matrizes*). Se $m, n \in \mathbb{N}$, denotamos por $\mathbb{M}_{m,n}(R)$ o conjunto constituído por todas as matrizes de tipo $m \times n$ com coeficientes no anel R; no caso em que $m = n$, escrevemos $\mathbb{M}_n(R)$ em vez de $\mathbb{M}_{n,n}(R)$. É fácil verificar que, para qualquer $n \in \mathbb{N}$, $\mathbb{M}_n(R)$ é um anel para as operações usuais de adição e multiplicação de matrizes.

O grupo das unidades do anel $\mathbb{M}_n(R)$ é o grupo constituído por todas as matrizes invertíveis e é denotado por $\mathrm{GL}_n(R)$; chamamos a $\mathrm{GL}_n(R)$ o *grupo linear completo* de grau n sobre R.

1.1.10. Exemplo (*Anéis de polinómios*). Denotamos por $R[X]$ o conjunto constituído por todas as funções $p \colon \mathbb{N}_0 \to R$ tais que o suporte

$$\operatorname{supp}(p) = \big\{n \in \mathbb{N}_0 \colon p(n) \neq 0\big\}$$

é finito. Em $R[X]$, definimos as operações de adição e multiplicação pelas fórmulas

$$(p + q)(n) = p(n) + q(n) \qquad \text{e} \qquad (pq)(n) = \sum_{0\leq m\leq n} p(m)q(n - m).$$

É fácil verificar que, com respeito a estas operações, $R[X]$ é um anel, a que chamamos o *anel de polinómios na indeterminada X com coeficientes em R*. Notemos que a "indeterminada" X

(*)Em particular, com o conjunto $R^n = \big\{a_1 \cdots a_n \colon a_1, \ldots, a_n \in R\big\}$.

corresponde à função $X\colon \mathbb{N}_0 \to R$ definida por

$$X(n) = \begin{cases} 1, & \text{se } n = 1, \\ 0, & \text{se } n \neq 1, \end{cases}$$

e que qualquer função $p \in R[X]$ se escreve de maneira unica como uma soma (finita)

$$p = \sum_{n\in\mathbb{N}_0} p(n)X^n;$$

notemos que X^0 é a identidade de $R[X]$. [Por conseguinte, $R[X]$ é isomorfo ao anel de polinómios usual.]

De forma análoga, para qualquer $n \in \mathbb{N}$, podemos definir o *anel de polinómios* $R[X_1, \ldots, X_n]$ *em* n *indeterminadas* $X_1, \ldots, X_n$ *com coeficientes em* R como sendo o conjunto de todas as funções $p\colon (\mathbb{N}_0)^n \to R$ tais que o suporte

$$\operatorname{supp}(p) = \big\{\alpha \in (\mathbb{N}_0)^n \colon p(\alpha) \neq 0\big\}$$

é finito. A estrutura de anel em $R[X_1, \ldots, X_n]$ é dada pelas operações

$$(p+q)(\alpha) = p(\alpha) + q(\alpha) \qquad \text{e} \qquad (pq)(\alpha) = \sum_{\substack{\beta,\gamma\in(\mathbb{N}_0)^n \\ \beta+\gamma=\alpha}} p(\beta)q(\gamma)$$

para todo $\alpha \in (\mathbb{N}_0)^n$. Nesta situação, para cada $1 \leq i \leq n$, a "indeterminada" X_i corresponde à função $X_i\colon \mathbb{N}_0 \to R$ definida por

$$X_i(\alpha) = \begin{cases} 1, & \text{se } \alpha = (\delta_{i,1}, \ldots, \delta_{i,n}), \\ 0, & \text{caso contrário;} \end{cases}$$

aqui $\delta_{i,j}$ é o *símbolo de Kronecker* usual.

Para qualquer $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{N}_0)^n$, definimos o *monómio* $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, de modo que qualquer $p \in R[X_1, \ldots, X_n]$ se escreve de maneira unica como uma soma (finita)

$$p = \sum_{\alpha\in(\mathbb{N}_0)^n} p(\alpha)X^\alpha.$$

[Por conseguinte, $R[X_1, \ldots, X_n]$ é isomorfo ao anel de polinómios usual.]

Notemos que R pode ser encarado como um subanel de $R[X_1, \ldots, X_n]$ e que

$$R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n].$$

1.1.11. Exemplo (*Anel de grupo*). Dado um grupo (arbitrário) G (que consideramos multiplicativo), definimos RG como sendo o conjunto constituído por todas as funções $\alpha\colon G \to R$ tais que o suporte

$$\operatorname{supp}(\alpha) = \big\{g \in G \colon \alpha(g) \neq 0\big\}$$

é finito. Em RG, definimos as operações de adição e multiplicação pelas fórmulas

$$(\alpha+\beta)(g) = \alpha(g) + \beta(g) \qquad \text{e} \qquad (\alpha\beta)(g) = \sum_{h\in G} \alpha(h)\beta(h^{-1}g).$$

Com respeito a estas operações, RG é um anel, a que chamamos o *anel do grupo G com coeficientes em R.*

A cada $g \in G$, associamos a função $\varepsilon_g \colon G \to R$ definida por

$$\varepsilon_g(h) = \delta_{g,h}, \qquad h \in G,$$

de modo que qualquer elemento $\alpha \in RG$ se escreve de maneira única como uma soma finita

$$\alpha = \sum_{g \in G} \alpha(g)\varepsilon_g.$$

Além disso, o subconjunto $\bar{G} = \{\varepsilon_g \colon g \in G\}$ é um grupo (com respeito à multiplicação definida em RG) e a correspondência $g \mapsto \varepsilon_g$, para $g \in G$, define um isomorfismo de grupos $G \cong \bar{G}$. Esta observação justifica a identificação do anel RG com o conjunto de todas as somas formais finitas

$$\sum_{g \in G} \alpha_g g, \qquad \alpha_g \in R \ (g \in G),$$

de modo que uma função $\alpha \in RG$ corresponde à soma formal $\sum_{g \in G} \alpha(g)g$.[(*)]

1.1.12. Se R e S são anéis, um *homomorfismo (de anéis)* $\varphi \colon R \to S$ é uma aplicação de R em S tal que:

(a) $\varphi(a+b) = \varphi(a) + \varphi(b)$ para quaisquer $a, b \in R$;

(b) $\varphi(ab) = \varphi(a)\varphi(b)$ para quaisquer $a, b \in R$;

(c) $\varphi(1_R) = 1_S$.

Tem-se $\varphi(0_R) = 0_S$.

Se $\varphi \colon R \to S$ é um homomorfismo de anéis, dizemos que:

(a) φ é um *isomorfismo* se φ é bijectivo; quando existe um isomorfismo $\varphi \colon R \to S$, dizemos que os anéis R e S são isomorfos e escrevemos $R \cong S$.

(b) φ é um *epimorfismo* se φ é sobrejectivo.

(c) φ é um *monomorfismo* se φ é injectivo $\varphi \colon R \to S$.

Um homomorfismo $\varphi \colon R \to R$ diz-se um *endomorfismo* e um isomorfismo $\varphi \colon R \to R$ diz-se um *automorfismo.*

Para qualquer homomorfismo de anéis $\varphi \colon R \to S$, definimos:

- a *imagem de* φ por $\mathrm{Im}(\varphi) = \varphi(R) = \{\varphi(a) \colon a \in R\}$;
- o *núcleo de* φ por $\ker(\varphi) = \varphi^{-1}(0) = \{a \in R \colon \varphi(a) = 0\}$.

(*) Salvo menção em contrário, faremos esta identificação ao longo do curso; isto é, identificaremos $g \in G$ com a função $\varepsilon_g \in \bar{G}$.

É fácil verificar que $\mathrm{Im}(\varphi)$ é um subanel de S, enquanto que $\ker(\varphi)$ é um ideal de R (no sentido da definição seguinte).

1.1.13. Dizemos que um subconjunto $\mathcal{I} \subseteq R$ é:

- um *ideal esquerdo*, e escrevemos $\mathcal{I} \trianglelefteq_{\mathrm{esq}} R$, se:
  (a) $0 \in \mathcal{I}$;
  (b) se $a, b \in \mathcal{I}$, então $a - b \in \mathcal{I}$;
  (c) se $a \in \mathcal{I}$ e $r \in R$, então $ra \in \mathcal{I}$.
- um *ideal direito*, e escrevemos $\mathcal{I} \trianglelefteq_{\mathrm{dir}} R$, se:
  (a) $0 \in \mathcal{I}$;
  (b) se $a, b \in \mathcal{I}$, então $a - b \in \mathcal{I}$;
  (c) se $a \in \mathcal{I}$ e $r \in R$, então $ar \in \mathcal{I}$.
- um *ideal* (ou, um *ideal bilateral*), e escrevemos $\mathcal{I} \trianglelefteq R$, se:
  (a) $0 \in \mathcal{I}$;
  (b) se $a, b \in \mathcal{I}$, então $a - b \in \mathcal{I}$;
  (c) se $a \in \mathcal{I}$ e $r, s \in R$, então $ras \in \mathcal{I}$.

Sendo assim, $\mathcal{I} \subseteq R$ é um ideal se e só se $\mathcal{I}$ é, simultaneamente, um ideal esquerdo e um ideal direito.

1.1.14. Para qualquer ideal bilateral $\mathcal{I} \trianglelefteq R$, definimos o *anel quociente* $R/\mathcal{I}$ como sendo o conjunto

$$R/\mathcal{I} = \big\{a + \mathcal{I} \colon a \in R\big\}$$

munido das operações:

$$(a + \mathcal{I}) + (b + \mathcal{I}) = (a + b) + \mathcal{I} \quad \text{e} \quad (a + \mathcal{I})(b + \mathcal{I}) = (ab) + \mathcal{I}$$

para todos $a, b \in R$. Aqui, para qualquer $a \in R$, $a + \mathcal{I} = \big\{a + b \colon b \in \mathcal{I}\big\}$ é a *classe lateral* de a relativamente a $\mathcal{I}$; para quaisquer $a, b \in R$, tem-se

$$a + \mathcal{I} = b + \mathcal{I} \iff a - b \in \mathcal{I}.$$

Chamamos *epimorfismo canónico* ao homomorfismo $\pi \colon R \to R/\mathcal{I}$ definido por

$$\pi(r) = r + \mathcal{I}, \qquad r \in R;$$

de facto, π é um homomorfismo sobrejectivo tal que $\ker(\pi) = \mathcal{I}$.

1.1.15. Teorema (Primeiro teorema do isomorfismo). *Se $\varphi\colon R \to S$ um homomorfismo de anéis, então existe um isomorfismo (natural)*

$$R/\ker(\varphi) \cong \operatorname{Im}(\varphi)$$

(dado pela correspondência $a + \ker(\varphi) \mapsto \varphi(a)$ para $a \in R$).

Demonstração. Exercício. □

1.1.16. Teorema (Segundo teorema do isomorfismo). *Para qualquer ideal $\mathfrak{I} \trianglelefteq R$ e qualquer subanel $S \leq R$, tem-se $S + \mathfrak{I} \leq R$, $\mathfrak{I} \trianglelefteq S + \mathfrak{I}$ e $S \cap \mathfrak{I} \trianglelefteq S$; além disso, existe um isomorfismo (natural)*

$$(S + \mathfrak{I})/\mathfrak{I} \cong S/(S \cap \mathfrak{I})$$

(dado pela correspondência $a + \mathfrak{I} \mapsto a + (S \cap \mathfrak{I})$ para $a \in S$).

Demonstração. Exercício. □

1.1.17. Teorema (Terceiro teorema do isomorfismo). *Para quaisquer ideais $\mathfrak{I}, \mathfrak{J} \trianglelefteq R$ tais que $\mathfrak{I} \subseteq \mathfrak{J}$, tem-se $\mathfrak{J}/\mathfrak{I} \trianglelefteq R/\mathfrak{I}$; além disso, existe um isomorfismo (natural)*

$$(R/\mathfrak{I})/(\mathfrak{J}/\mathfrak{I}) \cong R/\mathfrak{J}$$

(dado pela correspondência $(a + \mathfrak{I}) + (\mathfrak{J}/\mathfrak{I}) \mapsto a + \mathfrak{J}$ para $a \in R$).

Demonstração. Exercício. □

1.1.18. Teorema. *Sejam $\mathfrak{I} \trianglelefteq R$ e $\pi\colon R \to R/\mathfrak{I}$ o epimorfismo canónico. Então:*

(a) *A correspondência $S \mapsto S/\mathfrak{I}$ define uma bijecção entre o conjunto $\{S \leq R\colon \mathfrak{I} \subseteq S\}$ e o conjunto dos subanéis de $R/\mathfrak{I}$.*

(b) *A correspondência $\mathfrak{J} \mapsto \mathfrak{J}/\mathfrak{I}$ define uma bijecção entre o conjunto $\{\mathfrak{J} \trianglelefteq R\colon \mathfrak{I} \subseteq \mathfrak{J}\}$ e o conjunto dos ideais de $R/\mathfrak{I}$.*

Demonstração. Exercício. □

1.1.19. Lema. (a) *A intersecção de qualquer família de subanéis de R é um subanel de R.*

(b) *A intersecção de qualquer família de ideais de R é um ideal de R..*

Demonstração. Exercício. □

1.1.20. Para qualquer subconjunto $X \subseteq R$, definimos:

- O *subanel gerado* por X como sendo o menor subanel de R que contém X; pelo Lema 1.1.19(a), o subanel gerado por X é a intersecção de todos os subanéis de R que contém X.

- O *ideal gerado* por X, que denotamos por $\langle X\rangle$, como sendo o menor ideal de R que contém X; pelo Lema 1.1.19(b), $\langle X\rangle$ é a intersecção de todos os ideais de R que contém X.

Quando $X = \{x_1, \ldots, x_n\}$ é finito, escrevemos $\langle X\rangle = \langle x_1, \ldots, x_n\rangle$.

Mais geralmente, se $X_1, \ldots, X_n \subseteq R$, definimos

$$\langle X_1, \ldots, X_n\rangle = \langle X_1 \cup \cdots \cup X_n\rangle;$$

obviamente, $\langle X_1, \ldots, X_n\rangle$ é o menor ideal de R que contém os subconjuntos $X_1, \ldots, X_n$. Esta notação estende-se a qualquer família $\big\{X_i \colon i \in I\big\}$ de subconjuntos de R; assim,

$$\big\langle X_i \colon i \in I\big\rangle = \left\langle \bigcup_{i\in I} X_i \right\rangle.$$

Se $X = \{x\}$, então

$$\langle x\rangle = \big\{rxs \colon r, s \in R\big\};$$

dizemos que $\langle x\rangle$ é um *ideal principal* de R. Em particular, tem-se $\langle 1\rangle = R$; em geral, para qualquer $a \trianglelefteq R$, tem-se $\langle a\rangle = R$ se e só se $a \in R^\times$.

Qualquer ideal que contenha $X \subseteq R$ também contém todas as somas finitas $\sum_{x\in X} r_x x s_x$ onde $r_x, s_x \in R$, para $x \in X$, são quase todos nulos; e, como o conjunto de todas estas somas finitas é um ideal $\mathcal{I}$ de R, tem-se $\langle X\rangle = \mathcal{I}$.

Como caso particular, o ideal $\big\langle \mathcal{I}_i \colon i \in I\big\rangle$ gerado por uma família de ideais $\big\{\mathcal{I}_i \colon i \in I\big\}$ de R é constituído por todas as somas finitas $\sum_{i\in I} a_i$ em que $a_i \in \mathcal{I}_i$ para $i \in I$; por isso, faz sentido definir

$$\sum_{i\in I} \mathcal{I}_i = \big\langle \mathcal{I}_i \colon i \in I\big\rangle.$$

Notemos que, quando $\mathcal{I}_1, \ldots, \mathcal{I}_n \trianglelefteq R$, obtemos a *soma de ideais*

$$\mathcal{I}_1 + \cdots + \mathcal{I}_n = \big\{a_1 + \cdots + a_n \colon a_k \in \mathcal{I}_k,\ 1 \leq k \leq n\big\}.$$

1.1.21. Proposição. *Para qualquer $\mathcal{I} \trianglelefteq R$, denotamos por $\mathbb{M}_n(\mathcal{I})$ o subconjunto de $\mathbb{M}_n(R)$ constituído por todas as matrizes com coeficientes em $\mathcal{I}$. Então, a correspondência $\mathcal{I} \mapsto \mathbb{M}_n(\mathcal{I})$ define uma bijecção entre o conjunto dos ideais de R e o conjunto dos ideais de $\mathbb{M}_n(R)$.*

Demonstração. Fica como exercício provar que $\mathbb{M}_n(\mathcal{I}) \trianglelefteq \mathbb{M}_n(R)$ para todo $\mathcal{I} \trianglelefteq R$.

Reciprocamente, seja $\mathcal{J} \trianglelefteq \mathbb{M}_n(R)$ e, para quaisquer $1 \leq i, j \leq n$, seja $c_{i,j} \colon \mathbb{M}_n(R) \to R$ a aplicação definida por

$$c_{i,j}(A) = a_{i,j}, \qquad A \in \mathbb{M}_n(R),$$

onde $a_{i,j}$ é o (i,j)-ésimo coeficiente de A. Definamos

$$\mathcal{I} = \big\{a \in R \colon c_{1,1}(A) = a \text{ para algum } A \in \mathcal{J}\big\}$$

e observemos que $\mathcal{I} \trianglelefteq R$. Com efeito, sejam $a, b \in \mathcal{I}$ e $r \in R$; sejam $A, B \in \mathcal{J}$ tais que $c_{1,1}(A) = a$ e $c_{1,1}(B) = b$. Então, $a - b = c_{1,1}(A - B)$, logo $a - b \in \mathcal{I}$ (porque $A - B \in \mathcal{J}$). Por outro lado, para quaisquer $1 \leq i, j \leq n$, seja $E_{i,j} \in \mathbb{M}_n(R)$ a matriz com coeficiente 1 na posição (i, j) e coeficiente 0 em todas as outras entradas; de modo que qualquer matriz $M \in \mathbb{M}_n(R)$ é da forma

$$M = \sum_{1 \leq i,j \leq n} c_{i,j}(M) E_{i,j}.$$

Temos $ra = c_{1,1}(rE_{1,1}A)$ e $ar = c_{1,1}(A(rE_{1,1}))$, logo $ra, ar \in \mathcal{I}$ (porque $rE_{1,1}A, A(rE_{1,1}) \in \mathcal{J}$).

Finalmente, provemos que $\mathcal{J} = \mathbb{M}_n(\mathcal{I})$. Se $A \in \mathcal{J}$, então $E_{1,i}AE_{j,1} = c_{i,j}(A)E_{1,1} \in \mathcal{J}$ e, portanto, $c_{i,j}(A) = c_{1,1}(c_{i,j}(A)E_{1,1}) \in \mathcal{I}$ para todos $1 \leq i, j \leq n$, o que implica que $\mathcal{J} \subseteq \mathbb{M}_n(\mathcal{I})$. Por outro lado, para qualquer $M \in \mathbb{M}_n(\mathcal{J})$ e quaisquer $1 \leq i, j \in n$, temos $c_{i,j}(M) \in \mathcal{I}$, logo existe $A_{i,j} \in \mathcal{J}$ tal que $c_{1,1}(A_{i,j}) = c_{i,j}(M)$. Como $c_{i,j}(M)E_{i,j} = E_{i,1}A_{i,j}E_{1,j} \in \mathcal{I}$, concluímos que $M = \sum_{1 \leq i,j \leq n} c_{i,j}(M)E_{i,j} \in \mathcal{J}$, provando que $\mathbb{M}_n(\mathcal{I}) \subseteq \mathcal{J}$. □

1.2. Módulos sobre anéis

1.2.1. Por um *R-módulo esquerdo* entendemos um grupo abeliano M, com respeito a uma adição $(m, n) \mapsto m + n$, munido de uma multiplicação escalar

$$R \times M \to M, \qquad (a, m) \mapsto am,$$ (*)

que satisfaz as propriedades seguintes para quaisquer $a, b \in R$ e quaisquer $m, n \in M$:

(a) $a(m + n) = am + an$;

(b) $(a + b)m = am + bm$;

(c) $a(bm) = (ab)m$;

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

Quando necessário (caso haja perigo de ambiguidade), escrevemos ${}_RM$ para indicar que M é considerado como um R-módulo esquerdo.

Analogamente, por um *R-módulo direito* entendemos um grupo abeliano M, com respeito a uma adição $(m, n) \mapsto m + n$, munido de uma multiplicação escalar

$$M \times R \to M, \qquad (m, a) \mapsto ma,$$ (†)

que satisfaz as propriedades seguintes para quaisquer $a, b \in R$ e quaisquer $m, n \in M$:

(a) $(m + n)a = ma + na$;

(b) $m(a + b) = ma + mb$;

(c) $(ma)b = m(ab)$;

(*) Por vezes, sempre que isso se justificar, escrevemos $a \cdot m$ em vez de am.

(†) Por vezes, sempre que isso se justificar, escrevemos $m \cdot a$ em vez de ma.

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

Quando necessário (caso haja perigo de ambiguidade), escrevemos M_R para indicar que M é considerado como um R-módulo direito.

1.2.2. Observação. Se M é um R-módulo esquerdo (resp., direito), então

(a) $0_R \cdot m = 0_M$ (resp., $m \cdot 0_R = 0_M$) para todo $m \in M$;

(b) $a \cdot 0_M = 0_M$ (resp., $0_M \cdot a = 0_M$) para todo $a \in R$.

1.2.3. Exemplos. (a) Se R é um anel comutativo, então qualquer R-módulo esquerdo M tem uma estrutura de R-módulo direito em que a multiplicação escalar $M \times R \to M$ é definida por

$$m \cdot a = am, \qquad m \in M,\ a \in R;$$

por exemplo, temos

$$m \cdot (ab) = (ab)m = (ba)m = b(am) = b(m \cdot a) = (m \cdot a) \cdot b$$

para qualquer $m \in M$ e quaisquer $a, b \in R$.[(*)]

(b) Seja R é um anel munido de um anti-automorfismo[(†)] $\phi\colon R \to R$, então qualquer R-módulo esquerdo M tem uma estrutura de R-módulo direito em que a multiplicação escalar $M \times R \to M$ é definida por

$$m \cdot a = \phi(a)m, \qquad m \in M,\ a \in R.^{(\ddagger)}$$

Por exemplo, se G é um grupo (e R é um anel arbitrário), então o anel de grupo RG admite o anti-automorfismo $\phi\colon RG \to RG$ em que, para qualquer $\alpha \in RG$, a função $\phi(\alpha) \in RG$ é definida por

$$\phi(\alpha)(g) = \alpha(g^{-1}), \qquad g \in G.$$

Deste modo, qualquer RG-módulo esquerdo é também um RG-módulo direito (e reciprocamente).

(c) Muitas vezes, é útil considerar o *anel oposto*

$$R^{\mathrm{op}} = \left\{a^{\mathrm{op}} \colon a \in R\right\}$$

(*) De modo análogo, qualquer R-módulo direito M tem uma estrutura de R-módulo esquerdo definindo $a \cdot m = ma$ para $a \in R$ e $m \in M$.

(†) Se R e S são anéis, uma aplicação $\varphi\colon R \to S$ diz-se um *anti-homomorfismo* se:

(a) $\varphi(a + b) = \varphi(a) + \varphi(b)$ para quaisquer $a, b \in R$;

(b) $\varphi(ab) = \varphi(b)\varphi(a)$ para quaisquer $a, b \in R$;

(c) $\varphi(1_R) = 1_S$.

Usamos os termos *"anti-monomorfismo"*, *"anti-epimorfismo"* e *"anti-isomorfismo"* com o significado óbvio.

(‡) De modo análogo, qualquer R-módulo direito M tem uma estrutura de R-módulo esquerdo definindo $a \cdot m = m\phi(a)$ para $a \in R$ e $m \in M$.

de R em que a correspondência $a \mapsto a^{\mathrm{op}}$, para $a \in R$, define uma bijecção $R \to R^{\mathrm{op}}$ e em que a adição e a multiplicação são definidas por

$$a^{\mathrm{op}} + b^{\mathrm{op}} = (a+b)^{\mathrm{op}} \quad \text{e} \quad a^{\mathrm{op}} b^{\mathrm{op}} = (ba)^{\mathrm{op}}, \qquad a, b \in R.$$

Notemos que:

(a) Existe um isomorfismo de anéis $R \cong (R^{\mathrm{op}})^{\mathrm{op}}$ (em que $a \mapsto (a^{\mathrm{op}})^{\mathrm{op}}$ para $a \in R$).

(b) Se R e S são anéis, então uma aplicação $\varphi\colon R \to S$ é um anti-homomorfismo se e só se a aplicação $\varphi^{\mathrm{op}}\colon R \to S^{\mathrm{op}}$, definida por $\varphi^{\mathrm{op}}(a) = \varphi(a)^{\mathrm{op}}$ para todo $a \in R$, é um homomorfismo de anéis.

É fácil verificar que, qualquer R-módulo esquerdo M é um R^{op}-módulo direito em que a multiplicação escalar $M \times R^{\mathrm{op}} \to M$ é definida por

$$m a^{\mathrm{op}} = am, \qquad m \in M,\ a \in R.^{(*)}$$

Nota. A teoria dos R-módulos esquerdos é inteiramente análoga à teoria dos R-módulos direitos (com modificações óbvias). Para evitar "duplicações", escolhemos considerar apenas a teoria dos R-módulos esquerdos e, por isso, salvo indicação explícita em contrário, definimos um *R-módulo* (ou um *módulo sobre R*) como sendo um R-módulo esquerdo. No entanto, muitas vezes (por exemplo, no estudo das representações de um grupo), é necessário considerar, tanto módulos esquerdos, como módulos direitos.

1.2.4. Se M e N são R-módulos, dizemos que uma aplicação $\varphi\colon M \to N$ é um *R-homomorfismo* (ou, uma *aplicação R-linear*) se:

(a) $\varphi(m+m') = \varphi(m) + \varphi(m')$ para todos $m, m' \in M$;

(b) $\varphi(am) = a\varphi(m)$ (resp., $\varphi(ma) = \varphi(m)a$) para todo $a \in R$ e todo $m \in M$.

Para qualquer R-homomorfismo $\varphi\colon M \to N$, definimos:

- a *imagem de φ* por $\mathrm{Im}(\varphi) = \varphi(M) = \big\{\varphi(m)\colon m \in M\big\}$;
- o *núcleo de φ* por $\ker(\varphi) = \varphi^{-1}(0) = \big\{m \in M\colon \varphi(m) = 0\big\}$.

Se $\varphi\colon M \to N$ é um R-homomorfismo, dizemos que:

(a) φ é um *R-isomorfismo* se φ é bijectivo; quando existe um R-isomorfismo $\varphi\colon M \to N$, dizemos que M e N são *R-módulos isomorfos* e escrevemos $M \cong_R N$.

(b) φ é um *R-epimorfismo* se φ é sobrejectivo.

(c) φ é um *R-monomorfismo* se φ é injectivo.

$^{(*)}$De modo análogo, qualquer R-módulo direito M tem uma estrutura de R^{op}-módulo esquerdo definindo $a \cdot m = ma^{\mathrm{op}}$ para $a \in R$ e $m \in M$.

Denotamos por $\mathrm{Hom}_R(M,N)$ o conjunto de todos os R-homomorfismos de M em N. Quando $M=N$, um R-homomorfismo $\varphi\colon M\to M$ diz-se um *R-endomorfismo* e um R-endomorfismo $\varphi\colon M\to M$ diz-se um *R-automorfismo* se é bijectivo. Denotamos por $\mathrm{End}_R(M)$ o conjunto de todos os R-endomorfismos de M e por $\mathrm{GL}_R(M)$ (ou apenas por $\mathrm{GL}(M)$) o conjunto de todos os R-automorfismos de M; é fácil verificar que $\mathrm{End}_R(M)$ é um anel com respeito à adição e à composição de aplicações(*) e que $\mathrm{GL}_R(M)$ é um grupo com respeito à composição de aplicações(†).

1.2.5. Exemplos. (a) Qualquer grupo abeliano A é um $\mathbb{Z}$-módulo. Usando a notação aditiva, para quaisquer $n\in\mathbb{Z}$ e $a\in A$, definimos

$$na=\begin{cases} a+\ldots+a\ (n \text{ parcelas}) & \text{se } n>0,\\ 0 & \text{se } n=0,\\ (-a)+\ldots+(-a)\ (-n \text{ parcelas}) & \text{se } n<0.\end{cases}$$

(b) Para qualquer $n\in\mathbb{N}$,

$$R^{(n)}=\big\{(a_1,\ldots,a_n)\colon a_1,\ldots,a_n\in R\big\}$$

é um R-módulo esquerdo por meio da multiplicação escalar definida por

$$r(a_1,\ldots,a_n)=(ra_1,\ldots,ra_n),\qquad r,a_1,\ldots,a_n\in R,$$

e um R-módulo direito por meio da multiplicação escalar definida por

$$(a_1,\ldots,a_n)r=(a_1r,\ldots,a_nr),\qquad r,a_1,\ldots,a_n\in R.$$

Em particular, tomando $n=1$, concluímos que $R=R^{(1)}$ é um R-módulo esquerdo e também um R-módulo direito; referimo-nos a este R-módulo como sendo o *R-módulo regular (esquerdo ou direito)* e usamos a notação ${}_RR$ ou R_R conforme o caso considerado.

(c) Para quaisquer $m,n\in\mathbb{N}$, $\mathbb{M}_{m,n}(R)$ é um R-módulo esquerdo em que a multiplicação escalar é definida pela correspondência

$$(r,A)\mapsto rA,\qquad r\in R,\ A\in\mathbb{M}_{m,n}(R),$$

e um R-módulo direito em que a multiplicação escalar é definida pela correspondência

$$(A,r)\mapsto Ar\qquad A\in\mathbb{M}_{m,n}(R),\ r\in R.$$

Mais geralmente, $\mathbb{M}_{m,n}(R)$ é um $\mathbb{M}_m(R)$-módulo esquerdo em que a multiplicação escalar é definida pela correspondência

$$(A,B)\mapsto AB,\qquad A\in\mathbb{M}_m(R),\ B\in\mathbb{M}_{m,n}(R),$$

(*)Ao longo do curso, dadas duas aplicações $\alpha\colon X\to Y$ e $\beta\colon Y\to Z$ (onde X, Y e Z são conjuntos arbitrários), denotamos por $\alpha\beta$ a aplicação composta $\alpha\beta\colon X\to Z$; assim, $\alpha\beta$ é definida por $(\alpha\beta)(x)=\alpha(\beta(x))$ para todo $x\in X$.

(†)Trata-se, obviamente, do grupo das unidades de $\mathrm{End}_{\Bbbk}(M)$.

e um $\mathbb{M}_n(R)$-módulo direito em que a multiplicação escalar é definida pela correspondência

$$(B, A) \mapsto BA, \qquad B \in \mathbb{M}_{m,n}(R),\ A \in \mathbb{M}_m(R).$$

(d) Qualquer ideal esquerdo $\mathcal{L}$ de R é um R-módulo esquerdo e qualquer ideal direito $\mathcal{D}$ de R é um R-módulo direito; em qualquer dos casos, a multiplicação escalar é dada pela multiplicação do anel R. Em particular, tomando $\mathcal{L} = \mathcal{D} = R$, obtemos o R-módulo regular (esquerdo ou direito).

(f) Para qualquer ideal (bilateral) $\mathcal{I} \trianglelefteq R$, o anel quociente $R/\mathcal{I}$ é um R-módulo esquerdo por meio da multiplicação escalar definida por

$$r(a + \mathcal{I}) = (ra) + \mathcal{I}, \qquad r, a \in R,$$

e um R-módulo direito por meio da multiplicação escalar definida por

$$(a + \mathcal{I})r = (ar) + \mathcal{I}, \qquad r, a \in R.$$

(g) O anel polinomial $R[X]$ é um R-módulo esquerdo por meio da multiplicação escalar em que, para quaisquer $a \in R$ e $p \in R[X]$, o polinómio $ap \in R[X]$ é definida por

$$(ap)(n) = ap(n), \qquad n \in \mathbb{N};$$

de modo análogo, o anel polinomial $R[X_1, \ldots, X_n]$ é um R-módulo esquerdo.

(h) Se G é um grupo, o anel de grupo RG é um R-módulo esquerdo por meio da multiplicação escalar em que, para quaisquer $r \in R$ e $\alpha \in RG$, a função $r\alpha\colon G \to R$ é definida por

$$(r\alpha)(g) = r\alpha(g), \qquad g \in G.$$

1.2.6. Se M é um R-módulo, dizemos que um subconjunto $N \subseteq M$ é um *submódulo* (ou um *R-submódulo*, e escrevemos $N \leq_R M$, se:

(a) $0 \in N$;

(b) se $a, b \in N$, então $a - b \in N$;

(c) se $a \in R$ e $m \in N$, então $am \in N$.

Como exemplos, se $\varphi\colon M \to N$ é um R-homomorfismo, então

$$\operatorname{Im}(\varphi) \leq_R M \qquad \text{e} \qquad \ker(\varphi) \leq_R N.$$

1.2.7. Para qualquer R-módulo M e qualquer submódulo $N \leq_R M$, definimos o *R-módulo quociente* M/N como sendo o conjunto

$$M/N = \big\{m + N\colon m \in M\big\}$$

munido das operações:

$$(m + N) + (m' + N) = (m + m') + N \quad \text{e} \quad a(m + N) = (am) + I$$

para todos $m, m' \in M$ e todo $a \in R$. Aqui, para qualquer $m \in M$, $m + N = \{m + n \colon n \in N\}$ é a *classe lateral* de m relativamente a N; para quaisquer $m, m' \in M$, tem-se

$$m + N = m' + N \iff m - m' \in N.$$

Chamamos *R-epimorfismo canónico* ao R-homomorfismo $\pi \colon M \to M/N$ definido por

$$\pi(m) = m + N, \qquad m \in M;$$

de facto, π é um epimorfismo e tem-se $\ker(\pi) = N$.

1.2.8. Teorema (Primeiro teorema do isomorfismo). *Se M e N são R-módulos e $\varphi \colon M \to N$ é um R-homomorfismo, então existe um R-isomorfismo (natural)*

$$M/\ker(\varphi) \cong_R \operatorname{Im}(\varphi)$$

(dado pela correspondência $m + \ker(\varphi) \mapsto \varphi(m)$ para $m \in M$).

Demonstração. Exercício. □

1.2.9. Teorema (Segundo teorema do isomorfismo). *Se M é um R-módulo e $N, N' \leq_R M$, então existe um R-isomorfismo (natural)*

$$(N + N')/N' \cong_R N/(N \cap N')$$

(dado pela correspondência $n + N' \mapsto n + (N \cap N')$ para $n \in N$).

Demonstração. Exercício. □

1.2.10. Teorema (Terceiro teorema do isomorfismo). *Se M é um R-módulo e $N, N' \leq_R M$ são tais que $N \subseteq N'$, então existe um isomorfismo (natural)*

$$(M/N)/(N'/N) \cong_R M/N'$$

(dado pela correspondência $(m + N) + (N'/N) \mapsto m + N'$ para $m \in M$).

Demonstração. Exercício. □

1.2.11. Teorema. *Se M é um R-módulo, $N \leq_R M$ e $\pi \colon M \to M/N$ é o R-epimorfismo canónico, então a correspondência $N' \mapsto N'/N$ define uma bijecção entre o conjunto*

$$\{N' \leq_R M \colon N \subseteq N'\}$$

e o conjunto dos submódulos de M/N.

Demonstração. Exercício. □

1.2.12. Lema. *Se M é um R-módulo, então a intersecção de qualquer família de submódulos de M é um submódulo de M.*

Demonstração. Exercício. □

1.2.13. Se M é um R-módulo e $X \subseteq M$, então o *submódulo gerado* por X, que denotamos por $\langle X\rangle_R$, é o menor submódulo de R que contém X. De acordo com o Lema 1.2.12, $\langle X\rangle_R$ é a intersecção de todos os submódulos de M que contém X.

Quando $X = \{m_1, \ldots, m_t\}$ é finito, escrevemos $\langle X\rangle_R = \langle m_1, \ldots, m_t\rangle_R$. Se $M = \langle m_1, \ldots, m_t\rangle_R$ para alguns $m_1, \ldots, m_t \in M$, dizemos que M é um *R-módulo finitamente gerado*.

Mais geralmente, se $X_1, \ldots, X_n \subseteq R$, definimos

$$\langle X_1, \ldots, X_n\rangle_R = \langle X_1 \cup \cdots \cup X_n\rangle_R;$$

obviamente, $\langle X_1, \ldots, X_n\rangle_R$ é o menor submódulo de R que contém todos os subconjuntos $X_1, \ldots, X_n$. Esta notação estende-se a qualquer família $\big\{X_i \colon i \in I\big\}$ de subconjuntos de R; sendo assim,

$$\big\langle X_i \colon i \in I\big\rangle_R = \left\langle \bigcup_{i\in I} X_i \right\rangle.$$

Se $X = \{m\}$ para $m \in M$, então

$$\langle m\rangle_R = Rm = \big\{am \colon a \in R\big\};$$

dizemos que $\langle m\rangle_R$ é um *submódulo cíclico* de M; em particular, dizemos que M é um *R-módulo cíclico* se $M = Rm = \langle m\rangle_R$ para algum $m \in M$. É fácil verificar que, para qualquer $m \in M$, a correspondência $a \mapsto am$, para $a \in R$, define um R-homomorfismo $\varphi \colon R \to M$ em que

$$\operatorname{Im}(\varphi) = Rm \qquad \text{e} \qquad \ker(\varphi) = \operatorname{Ann}_R(m) = \big\{a \in R \colon am = 0\big\}$$

(ao submódulo $\operatorname{Ann}_R(m) \leq_R R$ chamamos o *anulador* de m em R); por conseguinte,

$$Rm \cong_R R/\operatorname{Ann}_R(m), \qquad m \in M.$$

Qualquer submódulo que contenha $X \subseteq R$ também contém todas as *combinações R-lineares* (finitas) $\sum_{x\in X} a_x x$ onde $a_x \in R$, para $x \in X$, são quase todos nulos; como o conjunto de todas estas combinações R-lineares é um submódulo N de M, tem-se $\langle X\rangle_R = N$.

Em particular, o submódulo $\big\langle N_i \colon i \in I\big\rangle_R$ gerado por uma família de submódulos $\big\{N_i \colon i \in I\big\}$ de M é constituído por todas as somas finitas $\sum_{i\in I} n_i$ em que $n_i \in N_i$ para $i \in I$; por isso, faz sentido definir

$$\sum_{i\in I} N_i = \big\langle N_i \colon i \in I\big\rangle_R.$$

Notemos que, quando $N_1, \ldots, N_t \leq_R M$, obtemos a *soma de submódulos*

$$N_1 + \cdots + N_t = \big\{n_1 + \cdots + n_t \colon n_k \in N_k,\ 1 \leq k \leq t\big\}.$$

1.2.14. Se $\{M_i \colon i \in I\}$ uma família de R-módulos, definimos:

- O *produto directo* $\prod_{i\in I} M_i$ como sendo o conjunto
$$\prod_{i\in I} M_i = \{(m_i)_{i\in I} \colon m_i \in R_i,\ i \in I\};$$
trata-se de um R-módulo com respeito às operações definidas naturalmente componente-a-componente:
$$(m_i)_{i\in I} + (n_i)_{i\in I} = (m_i + n_i)_{i\in I} \quad \text{e} \quad a(m_i)_{i\in I} = (am_i)_{i\in I}$$
para quaisquer $m_i, n_i \in M_i$ $(i \in I)$ e qualquer $a \in R$.
- A *soma directa externa* $\coprod_{i\in I} M_i$ como sendo o subconjunto de $\prod_{i\in I} M_i$ constituído por todas as sequências $(m_i)_{i\in I}$ que têm suporte finito; isto é, o conjunto $\{i \in I \colon m_i \neq 0\}$ é finito. É fácil verificar que
$$\coprod_{i\in I} M_i \leq_R \prod_{i\in I} M_i,$$
isto é, $\coprod_{i\in I} M_i$ é um submódulo de $\prod_{i\in I} M_i$

No caso em que $I = \{i_1, \ldots, i_n\}$ é finito, usamos as notações $M_{i_1} \times \cdots \times M_{i_n}$ (para o produto directo) e $M_{i_1} \dotplus \cdots \dotplus M_{i_n}$ (para a soma directa externa); nesta situação, é claro que
$$M_{i_1} \dotplus \cdots \dotplus M_{i_n} = M_{i_1} \times \cdots \times M_{i_n}.$$

Se M é um R-módulo e $M_i = M$ para todo $i \in I$, escrevemos M^I em vez de $\prod_{i\in I} M_i$, isto é,
$$M^I = \prod_{i\in I} M;$$
analogamente, definimos
$$M^{(I)} = \coprod_{i\in I} M_i.$$
No caso em que I é finito com n elementos, temos
$$M^I = M^{(I)} = M^{(n)} = \{(m_1, \ldots, m_n) \colon m_i \in M,\ 1 \leq i \leq n\}.$$

1.2.15. Teorema. *Sejam M um R-módulo e $\{N_i \colon i \in I\}$ uma família de submódulos de M satisfazendo:*

(a) $M = \sum_{i\in I} N_i$;

(b) *para qualquer $i \in I$, $N_i \cap \left(\sum_{j\in I\setminus\{i\}} N_j\right) = \{0\}$.*

Então, existe um R-isomorfismo natural
$$M \cong_R \coprod_{i\in I} N_i$$
em que $m \in M$ corresponde à sequência $(n_i)_{i\in I} \in \coprod_{i\in I} N_i$ se e só se $m = \sum_{i\in I} n_i$.

Demonstração. Exercício. □

1.2.16. Dado um R-módulo M, dizemos que M é a *soma directa interna* de uma família de submódulos $\{N_i \colon i \in I\}$, e escrevemos

$$M = \bigoplus_{i \in I} N_i$$

se são satisfeitas as duas condições do Teorema 1.2.15, isto é, se:

(a) $M = \sum_{i \in I} N_i$;

(b) para qualquer $i \in I$, $N_i \cap \big(\sum_{j \in I \setminus \{i\}} N_j\big) = \{0\}$.

Equivalentemente, tem-se $M = \bigoplus_{i \in I} N_i$ se e só se qualquer elemento $m \in M$ se escreve de maneira única como uma soma $m = \sum_{i \in I'} m_i$ em que $I' \subseteq I$ é finito e $m_i \in N_i$ para qualquer $i \in I'$.

No caso em que $I = \{i_1, \ldots, i_n\}$ é finito, também usamos a notação $M = N_{i_1} \oplus \cdots \oplus N_{i_n}$.

1.2.17. Proposição. *Sejam M um R-módulo e $\{N_i \colon i \in I\}$ uma família de submódulos de M. Então,*

$$M = \bigoplus_{i \in I} N_i$$

se e só se existe um conjunto $\{\pi_i \colon i \in I\}$ de R-endomorfismos de M satisfazendo as condições seguintes:

(a) *Para qualquer $i \in I$, $\mathrm{Im}(\pi_i) = N_i$.*

(b) *Para quaisquer $i, j \in I$,*

$$\pi_i \pi_j = \delta_{i,j} \pi_i = \begin{cases} \pi_i, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases}$$

(c) *Para qualquer $m \in M$, existe um conjunto finito $I' \subseteq I$ tal que*

$$m = \sum_{i \in I'} \pi_i(m).$$

Demonstração. Exercício: basta observar que $M = \bigoplus_{i \in I} N_i$ se e só se cada $m \in M$ se escreve de maneira única como uma soma

$$m = \sum_{i \in I} \pi_i(m)$$

onde $\pi_i(m) \in N_i$, para $i \in I$, e onde $I' = \{i \in I \colon \pi_i(m) \neq 0\}$ é um conjunto finito. □

1.2.18. Na situação da Proposição 1.2.17, dizemos que $\pi_i \in \mathrm{End}_R(M)$, para $i \in I$, são as *projecções (ortogonais)* associadas à soma directa $M = \bigoplus_{i \in I} N_i$; para cada $i \in I$, dizemos que $\pi_i \in \mathrm{End}_R(M)$ é a *i-ésima projecção (ortogonal).* Aqui, usamos o termo "ortogonal" com o sentido da condição (b) da proposição, isto é, $\pi_i \pi_j = 0$ sempre que $i, j \in I$ e $i \neq j$.

Mais geralmente, considerando um anel arbitrário R, dizemos que um elemento $e \in R$ é um *idempotente* se $e^2 = e$; assim, cada projecção π_i é um idempotente no anel $\mathrm{End}_R(M)$. É

fácil verificar que, se $e \in R$ é idempotente, então $1 - e \in R$ também é idempotente e que $e(1-e) = (1-e)e = 0$.

Dizemos que dois idempotentes $e, e' \in R$ são *ortogonais* se

$$ee' = e'e = 0.$$

Mais geralmente, dizemos que um subconjunto $\{e_i \colon i \in I\} \subseteq R$ é um *conjunto ortogonal de idempotentes* se

$$e_i e_j = \delta_{i,j} e_i, \qquad i, j \in I;$$

dito de outro modo, $\{e_i \colon i \in I\}$ é um conjunto ortogonal de idempotentes se e só se e_i, $i \in I$, são idempotentes ortogonais dois-a-dois.

Em particular, as projecções (ortogonais) associadas a uma soma directa $M = \bigoplus_{i \in I} N_i$ formam um conjunto ortogonal de idempotentes em $\mathrm{End}_R(M)$.

1.3. Módulos livres e módulos projectivos

1.3.1. Se M é um R-módulo, dizemos que um subconjunto $\mathcal{B} \subseteq M$ é:

- *linearmente dependente (sobre R)* se existem elementos $m_1, \ldots, m_t \in \mathcal{B}$, distintos dois-a-dois, tais que
$$a_1 m_1 + \cdots + a_t m_t = 0$$
para alguns $a_1, \ldots, a_t \in R$ não todos nulos.
- *linearmente independente (sobre R)* se $\mathcal{B}$ não é linearmente dependente (sobre R); por conseguinte, $\mathcal{B}$ é linearmente independente se e só se, para quaisquer $m_1, \ldots, m_t \in \mathcal{S}$, distintos dois-a-dois, e quaisquer $a_1, \ldots, a_t \in R$,
$$a_1 m_1 + \cdots + a_t m_t = 0 \quad \Longrightarrow \quad a_1 = \ldots = a_t = 0.$$
- uma *R-base* (ou, simplesmente, uma *base*) de M se $\mathcal{B}$ é linearmente independente (sobre R) e se $M = \langle \mathcal{B} \rangle_R$; por conseguinte, $\mathcal{B}$ é um R-base de M se e só se qualquer $m \in M$ se escreve de maneira única como uma combinação R-linear
$$m = a_1 m_1 + \cdots + a_t m_t$$
para alguns $a_1, \ldots, a_t \in R$ e $m_1, \ldots, m_t \in \mathcal{B}$.

Dizemos que M é um *R-módulo livre* se M possui uma R-base.

1.3.2. Exemplos. (a) Para qualquer conjunto I, $R^{(I)}$ é um R-módulo livre com base $\mathcal{B} = \{e_i \colon i \in I\}$ onde

$$e_i = (\delta_{i,j})_{j \in I}, \qquad i \in I;$$

referimo-nos a $\mathcal{B}$ como a *base canónica* de $R^{(I)}$.

(b) Para quaisquer $m, n \in \mathbb{N}$, $\mathbb{M}_{m,n}(R)$ é um R-módulo livre com base

$$\mathcal{B} = \big\{E_{i,j} \colon 1 \leq i \leq m,\ 1 \leq j \leq n\big\}$$

onde, para quaisquer $1 \leq i \leq m$ e $1 \leq j \leq n$, $E_{i,j} \in \mathbb{M}_{m,n}(R)$ é a matriz com coeficiente 1 na posição (i, j) e coeficiente 0 em todas as outras entradas.

(c) O anel polinomial $R[X]$ é um R-módulo livre com base $\mathcal{B} = \big\{X^n \colon n \in \mathbb{N}_0\big\}$; notemos que $R[X]$ é um $R[X]$-módulo livre com ($R[X]$-)base $\{1\}$. Mais geralmente, o anel polinomial $R[X_1, \ldots, X_n]$ é um R-módulo livre com base $\mathcal{B} = \big\{X^\alpha \colon \alpha \in (\mathbb{N}_0)^n\big\}$.

(d) Se G é um grupo, o anel de grupo RG é um R-módulo livre com base $\bar{G} = \big\{\varepsilon_g \colon g \in G\big\}$; recorde que, para qualquer $g \in G$, $\varepsilon_g \colon G \to R$ é a função definida por $\varepsilon_g(h) = \delta_{g,h}$ para todo $h \in G$. Identificando RG com o conjunto de todas as somas formais (finitas) $\sum_{g \in G} a_g g$, em que $a_g \in R$ para $g \in G$, podemos afirmar que G é uma R-base de RG.

1.3.3. Lema. *Um R-módulo M é livre se e só se $M \cong_R R^{(I)}$ para algum conjunto I.*

Demonstração. ($\Rightarrow$) Supondo que M é livre, basta escolher uma base $\big\{m_i \colon i \in I\big\}$ de M e definir $\varphi \colon R^{(I)} \to M$ por

$$\varphi\big((a_i)_{i \in I}\big) = \sum_{i \in I} a_i m_i, \qquad (a_i)_{i \in I} \in R^{(I)}.$$

É fácil verificar que φ é um R-isomorfismo.

($\Leftarrow$) Se $\varphi \colon R^{(I)} \to M$ é um R-isomorfismo e $\mathcal{B} = \big\{e_i \colon i \in I\big\}$ é a base canónica de $R^{(I)}$, então $\varphi(\mathcal{B}) = \big\{\varphi(e_i) \colon i \in I\big\}$ é uma R-base de M (exercício). □

1.3.4. Exemplos. (a) Para quaisquer $m, n \in \mathbb{N}$, $\mathbb{M}_{m,n}(R) \cong_R R^{(m \times n)}$.

(b) $R[X] \cong_R R^{(\mathbb{N}_0)}$ e $R[X_1, \ldots, X_n] \cong_R R^{((\mathbb{N}_0)^n)}$.

(c) Se G é um grupo, $RG \cong_R R^{(G)}$.

1.3.5. Lema. *Um R-módulo M é livre se e só se existe um subconjunto $\big\{m_i \colon i \in I\big\}$ de elementos de M tais que:*

(a) $M = \bigoplus_{i \in I} Rm_i$.

(b) $\mathrm{Ann}_R(m_i) = \{0\}$ *para todo* $i \in I$.

Demonstração. ($\Rightarrow$) Supondo que M é livre, basta escolher uma base $\big\{m_i \colon i \in I\big\}$ de M.

($\Leftarrow$) Seja $\big\{m_i \colon i \in I\big\}$ um subconjunto de M satisfazendo as condições (a) e (b). Justificamos que $\big\{m_i \colon i \in I\big\}$ é uma base de M. Ora, (a) implica que $M = \big\langle m_i \colon i \in I\big\rangle$. Para provarmos a independência linear, sejam $i_1, \ldots, i_t \in I$, distintos dois-a-dois, e sejam $a_1, \ldots, a_t \in R$ tais que $a_1 m_{i_1} + \cdots + a_t m_{i_t} = 0$. Por (a), concluímos que $a_s m_{i_s} = 0$ para qualquer $1 \leq s \leq t$. Sendo assim, $a_s \in \mathrm{Ann}_R(m_{i_s})$ e, portanto, (b) implica que $a_s = 0$ para qualquer $1 \leq s \leq t$. □

1.3.6. Proposição (Extensão R-linear). *Seja L um R-módulo livre com base $\mathcal{B}$. Então, para qualquer R-módulo M e qualquer aplicação $\alpha\colon \mathcal{B} \to M$, existe um e um só R-homomorfismo $\varphi\colon L \to M$ tal que $\varphi(b) = \alpha(b)$ para qualquer $b \in \mathcal{B}$.*

Demonstração. Exercício. □

1.3.7. Proposição. *Para qualquer R-módulo M, existe um R-módulo livre L e um R-epimorfismo $\pi\colon L \to M$. Em particular, qualquer R-módulo é quociente de um R-módulo livre.*

Demonstração. Escolhemos um conjunto de geradores $\mathcal{S} = \{m_i\colon i \in I\}$ de M (em último caso, podemos tomar $\mathcal{S} = M$) e consideramos o R-módulo livre $L = R^{(I)}$ e a base canónica $\mathcal{B} = \{e_i\colon i \in I\}$ de $R^{(I)}$. É claro que a correspondência $e_i \mapsto m_i$, para $i \in I$, define uma aplicação sobrejectiva de $\mathcal{B}$ em $\mathcal{S}$ que podemos estender R-linearmente (de modo natural) a um R-epimorfismo $\pi\colon R^{(I)} \to M$.

Para a última asserção, basta notar que $M = \operatorname{Im}(\pi) \cong_R L/\ker(\pi)$. □

1.3.8. Uma sequência (finita ou infinita) R-módulos e R-homomorfismos

$$\cdots \longrightarrow M_{k-1} \xrightarrow{\varphi_{k-1}} M_k \xrightarrow{\varphi_k} M_{k+1} \longrightarrow \cdots$$

diz-se *exacta em M_k* se $\ker(\varphi_k) = \operatorname{Im}(\varphi_{k-1})$ e diz-se uma *sequência exacta* se for exacta em M_k para todo k, excepto no termo inicial ou no termo final.

Em particular, se M, M' e M'' são R-módulos, então:

- Uma sequência $0 \longrightarrow M' \xrightarrow{\varphi} M$ é exacta se e só se $\varphi\colon M' \to M$ é um R-monomorfismo.
- Uma sequência $M \xrightarrow{\psi} M'' \longrightarrow 0$ é exacta se e só se $\psi\colon M \to M''$ é um R-epimorfismo.
- Uma sequência $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ é exacta se e só se $\varphi\colon M' \to M$ é um R-monomorfismo, $\psi\colon M \to M''$ é um R-epimorfismo e $\operatorname{Im}(\varphi) = \ker(\psi)$.

1.3.9. Se M, M' e M'' são R-módulos, dizemos que uma sequência exacta

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

é *cindível* se o submódulo $N = \operatorname{Im}(\varphi) = \ker(\psi)$ de M é uma parcela directa de M, isto é, existe $N' \leq_R M$ tal que $M = N \oplus N'$. Notemos que, como φ é injectivo, $M' \cong_R \operatorname{Im}(\varphi) = N$, logo

$$M \cong_R M' \dotplus N'$$

(em que $(m', n') \in M' \dotplus N'$ corresponde a $\varphi(m') + n' \in M$). Por outro lado, como ψ é sobrejectivo,

$$M'' = \operatorname{Im}(\psi) \cong_R M/\ker(\psi) = M/N \cong_R N'$$

e, portanto, existe um R-isomorfismo $\theta\colon M \to M' \dotplus M''$ em que

$$\theta(\varphi(m') + n') = (m', \psi(n')), \qquad m' \in M',\ n' \in N'.$$

Além disso, é fácil verificar que

$$\theta\varphi = \iota_{M'} \quad \text{e} \quad \psi = \pi_{M''}\theta;$$

aqui, $\iota_{M'}\colon M' \to M' \dotplus M''$ é a inclusão natural (dada pela correspondência $m' \mapsto (m', 0)$ para $m' \in M'$) e $\pi_{M''}\colon M' \dotplus M'' \to M''$ é a projecção natural (dada pela correspondência $(m', m'') \mapsto m''$ para $m' \in M'$ e $m'' \in M''$).

1.3.10. Teorema. *Para qualquer sequência exacta* $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ *de* R*-módulos, as afirmações seguintes são equivalentes:*

(a) *A sequência* $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ *é cindível.*

(b) *Existe um* R*-homomorfismo* $\sigma\colon M \to M'$ *tal que* $\sigma\varphi = \mathrm{id}_{M'}$.

(c) *Existe um* R*-homomorfismo* $\tau\colon M'' \to M$ *tal que* $\psi\tau = \mathrm{id}_{M''}$.

Nesta situação, tem-se

$$M = \mathrm{Im}(\varphi) \oplus \ker(\sigma) = \ker(\psi) \oplus \mathrm{Im}(\tau) \cong_R M' \dotplus M''.$$

Demonstração. (a) $\Rightarrow$ (b),(c). Pelo que observámos acima, existe um R-isomorfismo $\theta\colon M \to M' \dotplus M''$ tal que

$$\theta\varphi = \iota_{M'} \qquad \text{e} \qquad \psi = \pi_{M''}\theta.$$

Então, (b) e (c) são verdadeiras com

$$\sigma = \pi_{M'}\theta \qquad \text{e} \qquad \tau = \theta^{-1}\iota_{M''}.$$

(b) $\Rightarrow$ (a),(c). Para qualquer $m \in M$, temos

$$\sigma(m - \varphi(\sigma(m)) = \sigma(m) - (\sigma\varphi)(\sigma(m) = 0$$

(porque $\sigma\varphi = \mathrm{id}_{M'}$), logo $m - \varphi(\sigma(m)) \in \ker(\sigma)$, de onde se conclui que

$$M = \ker(\sigma) + \mathrm{Im}(\varphi).$$

Por outro lado, seja $m \in \ker(\sigma) \cap \mathrm{Im}(\varphi)$ e seja $m' \in M'$ tal que $m = \varphi(m')$. Como $m \in \ker(\sigma)$, obtemos

$$0 = \sigma(m) = \sigma(\varphi(m')) = (\sigma\varphi)(m') = m'$$

e, portanto, $m = \varphi(m') = 0$. Segue-se que $\ker(\sigma) \cap \mathrm{Im}(\varphi) = \{0\}$, logo

$$M = \ker(\sigma) \oplus \mathrm{Im}(\varphi),$$

o que prova (a).

Para provarmos (c), comecemos por considerar o R-homomorfismo $\tau'\colon M \to M''$ dado por

$$\tau'(m) = m - \varphi(\sigma(m)), \qquad m \in M.$$

Para qualquer $m' \in M'$, temos

$$(\tau'\varphi)(m') = \tau'(\varphi(m')) = \varphi(m') - \varphi(\sigma(\varphi(m'))) = \varphi(m') - \varphi(m') = 0$$

(porque $\sigma\varphi = \mathrm{id}_{M'}$) e, portanto, $\varphi(m') \in \ker(\tau')$. Como $\psi\colon M \to M''$ é sobrejectivo, temos $M'' = \mathrm{Im}(\psi)$, de modo que podemos definir a aplicação $\tau\colon M'' \to M$ por

$$\tau(\psi(m)) = \tau'(m), \qquad m \in M;$$

τ está bem-definida porque, se $m, n \in M$ são tais que $\psi(m) = \psi(n)$, então $m - n \in \ker(\psi) = \mathrm{Im}(\varphi) \subseteq \ker(\tau')$, logo $\tau'(m) = \tau'(n)$. É claro que τ é um R-homomorfismo que satisfaz

$$(\tau\psi)(m) = \tau'(m) = m - \varphi(\sigma(m)) = m - (\varphi\sigma)(m), \qquad m \in M.$$

Por conseguinte, temos $\mathrm{id}_M = \tau\psi + \varphi\sigma$ e, portanto,

$$\psi = \psi\,\mathrm{id}_M = \psi(\tau\psi + \varphi\sigma) = \psi\tau\psi + \psi\varphi\sigma = \psi\tau\psi$$

(porque $\psi\varphi = 0$). Como ψ é sobrejectivo, resulta que $\psi\tau = \mathrm{id}_{M''}$: se $m'' \in M''$, temos $m'' = \psi(m)$ para algum $m \in M$, logo

$$(\psi\tau)(m'') = (\psi\tau)(\psi(m)) = (\psi\tau\psi)(m) = \psi(m) = m''.$$

Isto prova que (c) é verdadeira.

(c) $\Rightarrow$ (a),(b). Exercício: a prova é análoga a (b) $\Rightarrow$ (a),(c). □

1.3.11. Proposição. *Se L é um R-módulo livre, então qualquer sequência exacta*

$$0 \longrightarrow M' \longrightarrow M \xrightarrow{\pi} L \longrightarrow 0$$

de R-módulos é cindível.

Demonstração. Seja $\mathcal{B} = \{e_i\colon i \in I\}$ uma R-base de L. Como π é sobrejectivo, para cada $i \in I$, existe $m_i \in M$ tal que $\pi(m_i) = e_i$. Por extensão R-linear, existe um e um só R-homomorfismo $\tau\colon L \to M$ tal que

$$\tau(e_i) = m_i, \qquad i \in I.$$

Como $\pi(\tau(e_i)) = \pi(m_i) = e_i$ para todo $i \in I$, segue-se que $\pi\tau = \mathrm{id}_L$ e, portanto, a sequência é cindível (pelo Teorema 1.3.10). □

1.3.12. Corolário. *Para qualquer R-módulo M, valem as propriedades seguintes:*

(a) *Se $N \leq_R M$ é tal que M/N é livre, então $M \cong_R N \dotplus (M/N)$.*

(b) *Se L é um R-módulo livre e $\pi\colon M \to L$ é um R-epimorfismo, então $M \cong_R \ker(\pi) \dotplus L$.*

Demonstração. (a) Se M/N é livre, a sequência exacta

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

é cindível.

(b) Basta tomar $N = \ker(\pi)$ e aplicar (a) (porque $L \cong_R M/\ker(\pi)$). □

1.3.13. Teorema. *Se D é um anel de divisão, então qualquer D-módulo é livre; mais precisamente, se M é um D-módulo, $\mathcal{S}$ é um conjunto de geradores de M e $\mathcal{B}_0 \subseteq \mathcal{S}$, então existe uma base $\mathcal{B}$ de M tal que $\mathcal{B}_0 \subseteq \mathcal{B} \subseteq \mathcal{S}$.*

Demonstração. Seja M um D-módulo arbitrário, seja $\mathcal{S}$ um conjunto de geradores de M e seja $\mathcal{B}_0 \subseteq \mathcal{S}$ um subconjunto linearmente independente (permitimos que $\mathcal{B}_0 = \emptyset$). Aplicamos o Lema de Zorn$^{(*)}$ ao conjunto

$$\Sigma = \big\{\mathcal{B} \subseteq \mathcal{S} \colon \mathcal{B} \text{ é linearmente independente e } \mathcal{B}_0 \subseteq \mathcal{B}\big\}$$

munido da ordem parcial dada pela inclusão; é claro que $\Sigma \neq \emptyset$ (porque $B_0 \in \Sigma$). Se $\big\{\mathcal{B}_i \colon i \in I\big\}$ é uma cadeia em Σ, então a união $\bigcup_{i\in I} \mathcal{B}_i$ é um subconjunto linearmente independente de Σ e, portanto, qualquer cadeia em Σ é majorada. Pelo Lema de Zorn, Σ tem pelo menos um elemento maximal, isto é, existe um subconjunto linearmente independente maximal $\mathcal{B} \subseteq \mathcal{S}$ que contém $\mathcal{B}_0$. Verificamos que $\mathcal{S} \subseteq \langle\mathcal{B}\rangle_D$, de modo que $M = \langle\mathcal{S}\rangle_D \subseteq \langle\mathcal{B}\rangle_D \subseteq M$, logo $M = \langle\mathcal{B}\rangle_D$ e, portanto, $\mathcal{B}$ é uma base de M. Seja $m \in \mathcal{S} \setminus \mathcal{B}$. Uma vez que $\mathcal{B}_0 \subseteq \mathcal{B} \subseteq \mathcal{B} \cup \{m\} \subseteq \mathcal{S}$, tem-se $\mathcal{B} \cup \{m\} \notin \Sigma$ (porque $\mathcal{B} \in \Sigma$ é maximal) e, portanto, $\mathcal{B} \cup \{m\}$ é linearmente dependente. Deste modo, existem $m_1, \ldots, m_t \in \mathcal{B}$ e $a, a_1, \ldots, a_t \in D$, não todos nulos, tais que

$$a_1 m_1 + \cdots + a_t m_t + am = 0.$$

Se $a = 0$, então $a_1 m_1 + \cdots + a_t m_t = 0$ e, portanto, $a_1 = \cdots = a_t = 0$ (porque $m_1, \ldots, m_t \in \mathcal{B}$ são linearmente independentes. Como isto não pode acontecer, tem de ser $b \neq 0$, logo existe o inverso $a^{-1} \in D$ (porque D é anel de divisão). Por conseguinte,

$$v = a^{-1}(av) = -(a^{-1}a_1 m_1 + \cdots + a^{-1}a_t m_t) \in \langle\mathcal{B}\rangle_D.$$

Como se queria. □

1.3.14. Corolário. *Se D é um anel de divisão e M é um D-módulo, então:*

(a) *Qualquer subconjunto linearmente independente de M pode ser estendido a uma base de M.*

(b) *Qualquer subconjunto linearmente independente maximal de M é uma base de M.*

(c) *Qualquer subconjunto de geradores minimal de M é uma base de M.*

Demonstração. Exercício. □

1.3.15. Dizemos que um R-módulo P é um *R-módulo projectivo* se, para quaisquer R-módulos M e N, qualquer R-epimorfismo $\psi \colon M \to N$ e qualquer R-homomorfismo $\varphi \colon P \to N$, existe um R-homomorfismo $\theta \colon P \to M$ tal que $\varphi = \psi\theta$. Isto significa que, para quaisquer R-módulos M

$^{(*)}$ O Lema de Zorn afirma que: *Se $\Sigma \neq \emptyset$ é um conjunto parcialmente ordenado no qual toda a cadeia tem majorante, então Σ tem pelo menos um elemento maximal.*

e N e qualquer R-epimorfismo $\psi\colon M \to N$, a correspondência $\theta \mapsto \psi\theta$, para $\theta \in \mathrm{Hom}_R(P, M)$, define uma aplicação sobrejectiva

$$\psi_*\colon \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N).$$

1.3.16. Teorema. *Para qualquer R-módulo P, as afirmações seguintes são equivalentes:*

(a) *P é projectivo.*

(b) *Qualquer sequência exacta $0 \longrightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} P \longrightarrow 0$ de R-módulos é cindível.*

(c) *Existe um R-módulo Q tal que $P \dotplus Q$ é um R-módulo livre.*

(d) *Para quaisquer R-módulos M e N e qualquer R-epimorfismo $\psi\colon M \to P$, a correspondência $\theta \mapsto \psi\theta$, para $\theta \in \mathrm{Hom}_R(P, M)$, define uma aplicação sobrejectiva $\psi_*\colon \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, P)$.*

Demonstração. (a) $\Rightarrow$ (b). Como P é projectivo, existe um R-homomorfismo $\theta\colon P \to M$ tal que $\mathrm{id}_P = \psi\theta$ e, portanto, pelo Teorema 1.3.10, a sequência $0 \longrightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} P \longrightarrow 0$ é cindível.

(b) $\Rightarrow$ (c). Pela Proposição 1.3.7, existe uma sequência exacta

$$0 \longrightarrow \ker(\pi) \longrightarrow L \xrightarrow{\pi} P \longrightarrow 0$$

onde L é algum R-módulo livre. Por (b), esta sequência é cindível, o que implica que $L \cong_R P \dotplus Q$ em que $Q = \ker(\pi)$.

(c) $\Rightarrow$ (d). Seja Q um R-módulo tal que $P \dotplus Q'$ é um R-módulo livre. Sejam M um R-módulo e $\beta\colon M \to P$ um R-epimorfismo. Definamos $\psi'\colon M \dotplus Q \to P \dotplus Q$ por

$$\psi'(m, q) = (\psi(m), q), \qquad m \in M,\ q \in Q.$$

É claro que ψ' é sobrejectivo, logo existe uma sequência exacta

$$0 \longrightarrow \ker(\psi') \longrightarrow M \dotplus P' \xrightarrow{\psi'} P \dotplus Q \longrightarrow 0.$$

Como $P \dotplus Q$ é livre, esta sequência é cindível (pela Proposição 1.3.11) e, portanto, existe um R-homomorfismo $\tau\colon P \dotplus Q \to M \dotplus Q$ tal que $\psi'\tau = \mathrm{id}_{P \dotplus Q}$.

Agora, seja N um R-módulo arbitrário. Então, a correspondência $\phi \mapsto \psi'\phi$ define um aplicação sobrejectiva $\psi_*\colon \mathrm{Hom}_R(N, M \dotplus Q) \to \mathrm{Hom}_R(N, P \dotplus Q)$: de facto, se $\psi\colon N \to P \dotplus Q$ é um R-homomorfismo, então, $\tau\psi\colon N \to M \dotplus Q$ é um R-homomorfismo tal que

$$(\psi'\tau)\psi = \mathrm{id}_{P \dotplus Q}\, \psi = \psi.$$

Para terminar, seja $\tau\colon N \to P$ um R-homomorfismo qualquer e consideremos o R-homomorfismo $\tau'\colon N \to P \dotplus Q$ definido por

$$\tau'(n) = (\tau(n), 0), \qquad n \in N;$$

assim, $\tau' = \iota_P \tau$ onde $\iota_P \colon P \to P \dotplus Q$ é a inclusão natural (dada pela correspondência $p \mapsto (p, 0)$ para $p \in P$) Pelo acabámos de observar, existe um R-homomorfismo $\phi' \colon N \to M \dotplus Q$ tal que $\theta' = \psi'\phi'$. Considerando as projecções naturais $\pi_M \colon M \dotplus Q \to$ e $\pi_P \colon P \dotplus Q \to P$, observamos que $\psi\pi_M = \pi_P\psi'$ e, portanto, pondo $\theta = \pi_M\phi'$, obtemos um R-homomorfismo $\theta \colon N \to M$ tal que

$$\begin{aligned}\psi\theta = \psi(\pi_M\phi') = (\psi\pi_M)\phi' = (\pi_P\psi')\phi' = \pi_P(\psi'\phi') \\ = \pi_P\tau' = \pi_P(\iota_P\tau) = (\pi_P\iota_P)\tau = \mathrm{id}_P\tau = \tau\end{aligned}$$

(uma vez que $\pi_P\iota_P = \mathrm{id}_P$). Por conseguinte, temos $\tau = \psi_*(\theta)$, provando que

$$\psi_* \colon \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, P)$$

é sobrejectiva.

(d) $\Rightarrow$ (a). Dados quaisquer R-módulos M e N e qualquer R-epimorfismo $\psi \colon M \to N$, há que provar que a aplicação

$$\psi_* \colon \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$$

é sobrejectiva. Comecemos por considerar uma sequência exacta

$$0 \longrightarrow K \longrightarrow L \xrightarrow{\pi} P \longrightarrow 0$$

onde L é um R-módulo livre. Por (d), existe um R-homomorfismo $\tau \colon P \to L$ tal que

$$\mathrm{id}_P = \pi_*(\tau) = \pi\tau.$$

Seja $\varphi \colon P \to N$ um R-homomorfismo arbitrário. Seja $\mathcal{B} = \{e_i \colon i \in I\}$ uma R-base de L e, para cada $i \in I$, consideremos a imagem $(\varphi\pi)(e_i) \in N$. Como $\psi \colon M \to N$ é sobrejectivo, para cada $i \in I$, existe $m_i \in M$ tal que $\psi(m_i) = (\varphi\pi)(e_i)$ e, portanto, por extensão R-linear, existe um e um só R-homomorfismo $\sigma \colon L \to M$ tal que

$$\sigma(e_i) = m_i, \qquad i \in I.$$

Como $(\psi\sigma)(e_i) = \psi(m_i) = (\varphi\pi)(e_i)$ para todo $i \in I$, concluímos que

$$\psi\sigma = \varphi\pi.$$

Pondo $\theta = \sigma\tau$, deduzimos que

$$\psi_*(\theta) = \psi\theta = \psi\sigma\tau = \varphi\pi\theta = \varphi\,\mathrm{id}_P = \varphi,$$

o que prova que ψ_* é sobrejectiva. □

1.3.17. Corolário. *Qualquer R-módulo livre é projectivo.*

1.4. Condições de cadeia

1.4.1. Dizemos que um conjunto parcialmente ordenado $(\Gamma, \leq)$ satisfaz:

- a *condição de cadeia ascendente* se qualquer cadeia ascendente $x_1 \leq x_2 \leq x_3 \leq \ldots$ em Γ é estacionária (isto é, existe $n \in \mathbb{N}$ tal que $x_n = x_{n+1} = \ldots$).
- a *condição de cadeia descendente* se qualquer cadeia descendente $x_1 \geq x_2 \geq x_3 \geq \ldots$ em Γ é estacionária (isto é, existe $n \in \mathbb{N}$ tal que $x_n = x_{n+1} = \ldots$).

1.4.2. Teorema. *Se $(\Gamma, \leq)$ qualquer conjunto parcialmente ordenado, então:*

(a) *$(\Gamma, \leq)$ satisfaz a condição de cadeia ascendente se e só se qualquer subconjunto não-vazio de Γ tem pelo menos um elemento maximal.*

(b) *$(\Gamma, \leq)$ satisfaz a condição de cadeia descendente se e só se qualquer subconjunto não-vazio de Γ tem pelo menos um elemento minimal.*

Demonstração. Exercício. □

1.4.3. Seja M um R-módulo (esquerdo ou direito) e denotemos por $\mathrm{Sub}(M)$ o conjunto dos submódulos de M parcialmente ordenado com respeito à inclusão. Dizemos que:

- M é *noetheriano* se $\mathrm{Sub}(M)$ satisfaz a condição de cadeia ascendente.
- M é *artiniano* se $\mathrm{Sub}(M)$ satisfaz a condição de cadeia descendente.

1.4.4. Teorema. *Um R-módulo M é noetheriano se e só se qualquer submódulo de M é finitamente gerado.*

Demonstração. ($\Rightarrow$) Seja $N \leq_R M$ e consideremos o subconjunto

$$\Gamma = \big\{ N' \leq_R N \colon N' \text{ é finitamente gerado} \big\}$$

de $\mathrm{Sub}(M)$. Γ é não-vazio (porque $\{0\} \in \Gamma$), logo tem pelo menos um elemento maximal N'. Se $N' \neq N$, existe $n \in N \setminus N'$ e podemos formar $N' + Rn \leq_R N$. É claro que $N' + Rn$ é finitamente gerado, logo $N' + Rn \in \Gamma$, o que contraria a maximalidade de N'. Sendo assim, $N' = N$ e, portanto, N é finitamente gerado.

($\Leftarrow$) Seja $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$ uma cadeia ascendente em $\mathrm{Sub}(M)$ e seja $N = \bigcup_{k \in \mathbb{N}} N_k$. É claro que $N \leq_R M$, logo N é finitamente gerado. Se $\{n_1, \ldots, n_t\}$ é um conjunto de geradores de N, tem de existir $r \in \mathbb{N}$ tal que $n_1, \ldots, n_t \in N_r$ e, portanto,

$$N = \langle n_1, \ldots, n_t \rangle \subseteq N_s \subseteq N, \qquad s \geq r.$$

Segue-se que $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$ é estacionária e, portanto, M é noetheriano. □

1.4.5. Dizemos que R é um *anel noetheriano à esquerda* se o R-módulo regular esquerdo ${}_RR$ é noetheriano; assim sendo, as condições seguintes são equivalentes:

- R é noetheriano à esquerda;
- todo o ideal esquerdo de R é finitamente gerado;
- qualquer família de ideais esquerdos de R tem pelo menos um elemento maximal.

De maneira análoga, dizemos que R é um *anel noetheriano à direita* se o R-módulo regular direito R_R é noetheriano; assim, as condições seguintes são equivalentes:

- R é noetheriano à direita;
- todo o ideal direito de R é finitamente gerado;
- qualquer família de ideais direitos de R tem pelo menos um elemento maximal.

Finalmente, dizemos que R é um *anel noetheriano* se R é noetheriano à esquerda e à direita.

1.4.6. Dizemos que:

- R é um *anel artiniano à esquerda* se o R-módulo regular esquerdo ${}_RR$ é artiniano.
- R é um *anel artiniano à direita* se o R-módulo regular direito R_R é artiniano.
- R éum *anel artiniano* se R é artiniano à esquerda e à direita.

1.4.7. Proposição. *Se M é um R-módulo e $N \leq_R M$, então:*

(a) *M é noetheriano se e só se N e M/N são noetherianos.*

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

Demonstração. (a) ($\Rightarrow$) Se $N' \leq_R N$, então $N' \leq_R M$, logo N' é finitamente gerado (porque M é noetheriano). Pelo Teorema 1.4.4, segue-se que N é noetheriano. Por outro lado, os submódulos de M/N são da forma M'/N onde $N \leq_R M' \leq_R M$; como M' é finitamente gerado (porque M é noetheriano), também M'/N é finitamente gerado. Pelo Teorema 1.4.4, segue-se que M/N é noetheriano.

($\Leftarrow$) Supomos que N e M/N são noetherianos. Seja $N' \leq_R M$ e consideremos $(N'+N)/N \leq_R M/N$. Como M/N é noetheriano, $(N'+N)/N$ é finitamente gerado e, portanto, como $(N'+N)/N \cong_R N'/(N' \cap N)$, também $N'/(N' \cap N)$ é finitamente gerado, pelo que existem $n'_1, \ldots, n'_r \in N'$ tais que $\{n'_1 + (N' \cap N), \ldots, n'_r + (N' \cap N)\}$ é conjunto de geradores de $N'/(N' \cap N)$. Por outro lado, como N é noetheriano, $N' \cap N \leq_R N$ é finitamente gerado e, portanto, existem $n_1, \ldots, n_s \in N' \cap N$ tais que $\{n_1, \ldots, n_s\}$ é conjunto de geradores de $N' \cap N$. Para terminar, é fácil concluir que $\{n'_1, \ldots, n'_r, n_1, \ldots, n_s\}$ é conjunto de geradores de N'. Pelo Teorema 1.4.4, segue-se que M é noetheriano.

(a) está provada. O argumento para provar (b) é inteiramente análogo. □

1.4.8. Corolário. *Sejam* $\{M_i : i \in I\}$ *uma família de* R*-módulos e* $M = \bigoplus_{i\in I} M_i$.

(a) *Se* M *é noetheriano (resp., artiniano), então* M_i *é noetheriano (resp., artiniano) para todo* $i \in I$.

(b) *Se* I *é finito e* M_i *é noetheriano (resp., artiniano) para todo* $i \in I$*, então* M *é noetheriano (resp., artiniano).*

Demonstração (caso noetheriano). (a) Para cada $i \in I$, consideramos a projecção canónica $\pi_i : M \to M_i$, de modo que $M_i \cong_R M/\ker(\pi_i)$. Como M é noetheriano, a Proposição 1.4.7 assegura que M_i é noetheriano.

(b) Sem perda de generalidade, tomamos $I = \{1, \ldots, n\}$. Fazemos indução sobre n. A afirmação é óbvia quando $n = 1$. Supomos que $n \geq 2$ e observamos que $M \cong_R M_1 \oplus M'$ onde $M' = M_2 \oplus \cdots \oplus M_n$. Por hipótese de indução, sabemos que M' é noetheriano; além disso, por hipótese M_1 também é noetheriano. Como $M_1 \cong_R M/M'$, M/M' também é noetheriano e, portanto, M é noetheriano (pela Proposição 1.4.7). □

1.4.9. Corolário. *Seja* M *é um* R*-módulo.*

(a) *Se* R *é anel noetheriano à esquerda (resp., à direita) e* M *é finitamente gerado, então* M *é noetheriano.*

(b) *Se* R *é anel artiniano à esquerda (resp., à direita) e* M *é finitamente gerado, então* M *é artiniano.*

Demonstração. (a) Como M é finitamente gerado, existe um R-epimorfismo $\pi : R^{(n)} \to M$. Pelo Corolário 1.4.8(b), o R-módulo (esquerdo) $R^{(n)}$ é noetheriano (porque ${}_RR$ é noetheriano) e, portanto, $M \cong_R R^{(n)}/\ker(\pi)$ também é noetheriano.

(b) Análoga. □

1.4.10. Seja M um R-módulo. Dizemos que um submódulo $N \leq_R M$ é *trivial* se $N = \{0\}$ ou $N = M$; no caso contrário, dizemos que N é *não-trivial*. Além disso, se $N \leq_R M$ e $N \neq M$, dizemos que N é um *submódulo próprio* de M.

Dizemos que M é um *R-módulo simples* se $M \neq \{0\}$ e se M não contém submódulos próprios não-triviais; por outras palavras, um R-módulo não-nulo M é simples se e só se $\{0\}$ e M são os únicos submódulos de M.

Um submódulo $N \leq_R M$ diz-se um *submódulo maximal* se $N \neq M$ se não existe $N' \leq_R N$ tal que $N \subsetneq N' \subsetneq M$; por outro lado, $N \leq_R M$ diz-se um *submódulo minimal* se $N \neq M$ se não existe $N' \leq_R N$ tal que $\{0\} \subsetneq N' \subsetneq N$.

É claro que:

- Um submódulo $N \leq_R M$ é maximal se e só se M/N é um R-módulo simples.

- Um submódulo $N \leq_R M$ é minimal se e só se N é um submódulo simples de N.

Por outro lado, do Teorema 1.4.2 resulta imediatamente que:

- Qualquer R-módulo noetheriano não-nulo contém pelo menos um submódulo maximal.
- Qualquer R-módulo artiniano não-nulo contém pelo menos um submódulo minimal.

1.4.11. Seja M um R-módulo. Dizemos que uma cadeia de submódulos

$$M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_n = \{0\}$$

é uma *série de composição* de M se, para qualquer $1 \leq i \leq n$, o R-módulo quociente M_{i-1}/M_i é simples; dizemos que n é o *comprimento* da série (ou mais geralmente, da cadeia) considerada.

Dizemos que um R-módulo M' é um *factor de composição de* M se existe uma série de composição $M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_n = \{0\}$ de M tal que $M' = M_{i-1}/M_i$ para algum $1 \leq i \leq n$.

1.4.12. Lema. *Se um R-módulo M admite uma série de composição com comprimento n, então qualquer cadeia de submódulos de M tem comprimento $\leq n$.*

Demonstração. Fazemos indução sobre n. Se $n = 1$, então M é simples e, portanto, não pode admitir cadeias de submódulos com comprimento ≥ 2.

Suponhamos que $n \geq 2$ e que o lema é verdadeiro para todos os R-módulos que admitem séries de composição com comprimento $\leq n-1$. Seja

$$M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_n = \{0\}$$

uma série de composição de M (com comprimento n) e consideremos o submódulo (simples) $N = M_{n-1}$ e o R-módulo quociente M/N. Então,

$$M/N \supsetneq M_1/N \supsetneq \ldots \supsetneq M_{n-1}/N = \{0\}$$

é uma série de composição de M/N com comprimento $n-1$; notemos que, para qualquer $1 \leq i \leq n-1$, $(M_{i-1}/N)/(M_i/N) \cong_R M_{i-1}/M_i$, pelo que $(M_{i-1}/N)/(M_i/N)$ é um R-módulo simples. Por hipótese de indução, qualquer cadeia de submódulos de M/N tem comprimento $\leq n-1$.

Agora, seja $M = N_0 \supsetneq N_1 \supsetneq \ldots \supsetneq N_r = \{0\}$ uma cadeia de submódulos de M (com comprimento r) e consideremos a cadeia

$$M = N_0 + N \supseteq N_1 + N \supseteq \ldots \supseteq N_r + N \supseteq N = \{0\}.$$

Para cada $1 \leq i \leq n$, $N_i \cap N \leq_R N$, logo $N_i \cap N = \{0\}$ ou $N_i \cap N = N$ (porque N é simples), ou seja, $N_i \cap N = \{0\}$ ou $N \subseteq N_i$. Se $t = \max\{1 \leq i \leq r \colon N \subseteq N_i\}$, então a cadeia acima é

$$M = N_0 \supsetneq N_1 \supsetneq \ldots \supsetneq N_t \supseteq N_{t+1} + N \supseteq \ldots \supseteq N_r + N \supseteq N \supsetneq \{0\}.$$

Para qualquer $t+1 \leq i \leq r$, tem-se

$$(N_{i-1} + N)/(N_i + N) = [N_{i-1} + (N_i + N)]/(N_i + N) \cong_R N_{i-1}/[N_{i-1} \cap (N_i + N)].$$

Como $N_{i-1} \cap (N_i + N) = N_i + (N_{i-1} \cap N)$ (porque $N_i \subseteq N_{i-1}$) e $N_{i-1} \cap N = 0$, concluímos que $N_{i-1} \cap (N_i + N) = N_i$ e, portanto, $(N_{i-1} + N)/(N_i + N) \cong_R N_{i-1}/N_i$ é não-nulo sempre que $i > t + 1$. Assim, $N_i + N \subsetneq N_{i-1}$ sempre que $i > t + 1$ e, portanto, a cadeia acima vem

$$M = N_0 \supsetneq N_1 \supsetneq \ldots \supsetneq N_t \supseteq N_{t+1} + N \supsetneq N_{t+2} + N \supsetneq \ldots \supsetneq N_r + N \supsetneq N \supsetneq \{0\}$$

(podendo eventualmente ser $N_t = N_{t+1} + N$); notemos que $(N_r + N)/N \cong_R N_r/(N_r \cap N) \cong_R N$. Esta cadeia determina a cadeia

$$M/N \supsetneq N_1/N \supsetneq \ldots \supsetneq N_t/N \supseteq (N_{t+1} + N)/N \supsetneq \ldots \supsetneq (N_r + N)/N \supsetneq \{0\}$$

de submódulos de M/N e tem comprimento $s \in \{r - 1, r\}$. Por indução, concluímos que $s \leq n - 1$ e, portanto, $r \leq n$ como queríamos. □

1.4.13. Lema. *Se um R-módulo M admite uma série de composição com comprimento n, então qualquer série de composição de M tem comprimento n e qualquer cadeia de submódulos de M pode ser refinada a uma série de composição.*

Demonstração. É uma aplicação fácil do Lema 1.4.12. □

1.4.14. No caso em que um R-módulo M admite uma série de composição, definimos o *comprimento de M*, que denotamos por $\ell_R(M)$, como sendo o comprimento de qualquer série de composição de M. No caso contrário, em que um R-módulo M não admite séries de composição, dizemos que M tem *comprimento infinito* e definimos $\ell_R(M) = \infty$.

1.4.15. Teorema. *Se M é um R-módulo, então M admite uma série de composição se e só se M é noetheriano e artiniano.*

Demonstração. ($\Rightarrow$) Supomos que M admite uma série de composição com comprimento $n \in \mathbb{N}$.

Para provar que M é noetheriano, seja $M_1 \subseteq M_2 \subseteq M_3 \ldots$ uma cadeia ascendente de submódulos de M. Então, para todo $t \in \mathbb{N}$, a cadeia

$$M \supseteq M_t \supseteq M_{t-1} \supseteq \ldots \supseteq M_1 \supseteq \{0\}$$

tem comprimento $\leq n$, pelo que a cadeia dada tem de ser finita, logo estacionária.

Analogamente se prova que M é artiniano.

($\Leftarrow$) Consideramos o conjunto

$$\Sigma = \big\{N \leq_R M \colon N \text{ admite uma série de composição}\big\}.$$

Temos $\{0\} \in \Sigma$ e, portanto, $\Sigma \neq \emptyset$. Como M é noetheriano, Σ tem pelo menos um elemento maximal; seja N este elemento. Então, N admite uma série de composição

$$N \supsetneq N_1 \supsetneq \ldots \supsetneq N_t = \{0\}.$$

Supomos que $N \neq M$ e consideramos o conjunto

$$\Sigma' = \big\{N' \leq_R M \colon N \subsetneq N'\big\}.$$

Como $M \in \Sigma'$, temos $\Sigma' \neq \emptyset$ e, portanto, como M é artiniano, Σ' tem um elemento minimal; seja N' este elemento. É fácil justificar que o R-módulo N'/N é simples: se $N'' \leq_R M$ é tal que $N \subsetneq N'' \subseteq N'$, então $N'' \in \Sigma'$ e, portanto, $N'' = N'$ (pela minimalidade de N'). Assim,

$$N' \supsetneq N \supsetneq N_1 \supsetneq \ldots \supsetneq N_t = \{0\}$$

é uma série de composição de N' e, portanto, $N' \in \Sigma$, contradizendo a maximalidade de $N \in \Sigma$. Por conseguinte, $N = M$, o que termina a demonstração. □

1.4.16. Proposição. *Se V é um espaço vectorial sobre um corpo $\Bbbk$, as condições seguintes são equivalentes:*

(a) *V é noetheriano.*

(b) *V é artiniano.*

(c) *$\ell_{\Bbbk}(V) < \infty$.*

(d) *$\dim_{\Bbbk}(V) < \infty$.*

Nestas condições, tem-se $\ell_{\Bbbk}(V) = \dim_{\Bbbk}(V)$.

Demonstração. Provamos as implicações seguintes

$$\begin{array}{ccccc} \text{(a)} & \Longleftarrow & \text{(c)} & \Longrightarrow & \text{(b)} \\ & \searrow & \Uparrow & \swarrow & \\ & & \text{(d)} & & \end{array}$$

(c) $\Rightarrow$ (a),(b). É consequência do Teorema 1.4.15.

(d) $\Rightarrow$ (c). Se $n = \dim_{\Bbbk}(V)$ e $\{v_1, \ldots, v_n\}$ é uma base de V, então

$$V = \langle v_1, \ldots, v_n\rangle_{\Bbbk} \supsetneq \langle v_1, \ldots, v_{n-1}\rangle_{\Bbbk} \supsetneq \ldots \supsetneq \langle v_1\rangle_{\Bbbk} \supsetneq \{0\}$$

é uma série de composição de V e, portanto, $\ell_{\Bbbk}(V) = n = \dim_{\Bbbk}(V)$.

(a) $\Rightarrow$ (d). Se V é noetheriano, então V é finitamente gerado (pelo Teorema 1.4.4) e, portanto, $\dim_{\Bbbk}(V) < \infty$.

(b) $\Rightarrow$ (d). Suponhamos que $\dim_{\Bbbk}(V) = \infty$ e seja $\big\{e_i \colon i \in I\big\}$ uma base de V onde I é um conjunto infinito. Seja $J = \big\{i_n \colon n \in \mathbb{N}\big\}$ um subconjunto infinito numerável de I. Se

$$V_n = \big\langle e_i \colon i \in J \setminus \{i_1, \ldots, i_n\}\big\rangle_{\Bbbk}, \qquad n \in \mathbb{N},$$

então

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \ldots$$

é uma cadeia descendente não-estacionária de subespaços vectoriais de V e, portanto, V não é artiniano. □

1.4.17. Teorema (Jordan-Hölder). *Seja M um R-módulo que admite uma série de composição. Se*

$$M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_n = \{0\} \qquad e \qquad M = M'_0 \supsetneq M'_1 \supsetneq \ldots \supsetneq M'_n = \{0\}$$

são séries de composição de M, então existe uma permutação $\sigma \in S_n$[(*)] tal que

$$M_{i-1}/M_i \cong_R M'_{\sigma(i)-1}/M'_{\sigma(i)}, \qquad 1 \leq i \leq n.$$

Demonstração. Fazemos indução sobre $n = \ell_R(M)$.

Se $M_1 = M'_1$, o resultado segue-se por indução.

Suponhamos que $M_1 \neq M'_1$. Como M_1 é um submódulo maximal de M, tem de ser

$$M_1 + M'_1 = M$$

e, portanto,

$$M/M_1 \cong_R M'_1/(M_1 \cap M'_1) \qquad \text{e} \qquad M/M'_1 \cong_R M_1/(M'_1 \cap M_1),$$

de modo que $M_1 \cap M'_1$ é um submódulo maximal de M_1 e de M'_1 (porque M/M_1 e M/M'_1 são simples). Seja

$$(M_1 \cap M'_1) = M''_2 \supsetneq M''_3 \supsetneq \ldots \supsetneq M''_t = \{0\}$$

uma série de composição de $M_1 \cap M'_1$. Então,

$$M \supsetneq M_1 \supsetneq (M_1 \cap M'_1) = M''_2 \supsetneq M''_3 \supsetneq \ldots \supsetneq M''_t = \{0\}$$

e

$$M \supsetneq M'_1 \supsetneq (M_1 \cap M'_1) = M''_2 \supsetneq M''_3 \supsetneq \ldots \supsetneq M''_t = \{0\}$$

são séries de composição de M, logo $t = n - 2$. Por indução, existe $\sigma' \in S_n$ tal que

$$M_{i-1}/M_i \cong_R M''_{\sigma'(i)-1}/M''_{\sigma'(i)}, \qquad 2 \leq i \leq n,$$

e existe $\sigma'' \in S_n$ tal que

$$M'_{i-1}/M'_i \cong_R M''_{\sigma''(i)-1}/M''_{\sigma''(i)}, \qquad 2 \leq i \leq n.$$

O resultado segue-se. □

(*)Ao longo do curso, denotamos por S_n o *grupo simétrico* constituído por todas as permutações do conjunto $[n] = \{1, 2, \ldots, n\}$. Mais geralmente, para qualquer conjunto X, denotamos por S_X o *grupo simétrico* constituído por todas as permutações do conjunto X.

1.5. Módulos indecomponíveis. Teorema de Krull-Schmidt.

1.5.1. Dizemos que um R-módulo M é *indecomponível* se $M \neq \{0\}$ e $\{0\}$ e M são as únicas parcelas directas de M; isto é, se, para quaisquer $M_1, M_2 \leq_R M$,

$$M = M_1 \oplus M_2 \quad \Longrightarrow \quad \big(M_1 = \{0\} \ \text{ ou } \ M_1 = M \big).$$

1.5.2. Teorema. *Seja M um R-módulo artiniano, então existem submódulos indecomponíveis $N_1, \ldots, N_t \leq_R M$ tais que $M = N_1 \oplus \cdots \oplus N_t$.*

Demonstração. Seja Σ o conjunto de todos os submódulos não-nulos de M que não podem ser expressos como soma directa finita de submódulos indecomponíveis. Suponhamos que $\Sigma \neq \emptyset$. Então, pelo Teorema 1.4.4, Σ tem um elemento minimal M'. Como $M' \in \Sigma$, temos $M' \neq \{0\}$ e, além disso, M' não pode ser indecomponível. Sendo assim, existem $M_1, M_2 \lneq_R M'$ tais que

$$M' = M_1 \oplus M_2.$$

Por minimalidade de M', temos $M_1, M_2 \notin \Sigma$ e, portanto, existem submódulos indecomponíveis $N'_1, \ldots, N'_r \leq_R M_1$ e $N''_1, \ldots, N''_s \leq_R M_2$ tais que

$$M_1 = N'_1 \oplus \cdots \oplus N'_r \qquad \text{e} \qquad M_2 = N''_1 \oplus \cdots \oplus N''_s.$$

Segue-se que

$$M' = N'_1 \oplus \cdots \oplus N'_r \oplus N''_1 \oplus \cdots \oplus N''_s,$$

uma contradição. □

1.5.3. Lema. *Seja M um R-módulo indecomponível. Seja $N \neq \{0\}$ um R-módulo qualquer e suponhamos que existem um R-monomorfismo $\theta\colon N \to M$ e um R-epimorfismo $\pi\colon M \to N$ tais que $\pi\theta\colon N \to N$ é um R-automorfismo. Então, θ e π são R-isomorfismos.*

Demonstração. Provamos que $M = \ker(\pi) \oplus \theta(N)$.

Se $m \in M$, então existe $n \in N$ tal que $\pi(m) = (\pi\theta)(n) = \pi(\theta(n))$, logo $m - \theta(n) \in \ker(\pi)$ e, portanto, $m = (m - \theta(n)) + \theta(n) \in \ker(\pi) + \theta(N)$. Segue-se que $M \subseteq \ker(\pi) + \theta(N)$ e, portanto,

$$M = \ker(\pi) + \theta(N).$$

Por outro lado, se $m \in \ker(\pi) \cap \theta(N)$, então $\pi(m) = 0$ e existe $n \in N$ tal que $m = \theta(n)$, de modo que $0 = \pi(m) = \pi(\theta(n)) = (\pi\theta)(n)$; como $\pi\theta$ é injectivo, concluímos que $m = 0$ e, portanto,

$$\ker(\pi) \cap \theta(N) = \{0\}.$$

Como M é indecomponível, concluímos que $\ker(\pi) = \{0\}$ (e $\theta(N) = M$) ou $\theta(N) = \{0\}$ (e $\ker(\pi) = M$). Como $\pi(\theta(N)) = (\pi\theta)(N) = N \neq \{0\}$, não pode ser $\theta(N) = \{0\}$, logo $\ker(\pi) = \{0\}$ e $M = \theta(N)$. □

1.5.4. LEMA. *Seja M um R-módulo noetheriano e artiniano e sejam $\tau_1, \ldots, \tau_n \in \mathrm{End}_R(M)$ tais que $\tau = \tau_1 + \cdots + \tau_n$ é um R-automorfismo. Se M é indecomponível, então τ_i é um R-automorfismo para pelo menos um $1 \leq i \leq n$.*

Demonstração. Começamos por considerar o caso $n = 2$. Seja $\tau = \tau_1 + \tau_2$ e sejam $\sigma_1 = \tau_1\tau^{-1}$ e $\sigma_2 = \tau_2\tau^{-1}$, de modo que

$$\sigma_1 + \sigma_2 = (\tau_1 + \tau_2)\tau^{-1} = \tau\tau^{-1} = \mathrm{id}_M\,.$$

Provemos que σ_1 e σ_2 são R-automorfismos de M (de onde resulta que τ_1 e τ_2 também o são). Como $\sigma_2 = \mathrm{id}_M - \sigma_1$, temos

$$\sigma_1\sigma_2 = \sigma_1(\mathrm{id}_M - \sigma_1) = \sigma_1 - (\sigma_1)^2 = (\mathrm{id}_M - \sigma_1)\sigma_1 = \sigma_2\sigma_1$$

e, portanto,

$$\mathrm{id}_M = (\sigma_1 + \sigma_2)^m = \sum_{0\leq k\leq m} \binom{m}{k} (\sigma_1)^k(\sigma_2)^{m-k}, \qquad m \in \mathbb{N}.$$

Se σ_1 e σ_2 são nilpotentes, isto é, se existem $m_1, m_2 \in \mathbb{N}$ tais que $(\sigma_1)^{m_1} = 0$ e $(\sigma_2)^{m_2} = 0$, então $\mathrm{id}_M = (\sigma_1 + \sigma_2)^{m_1+m_2} = 0$, o que não pode acontecer. Assim, pelo menos um dos R-endomorfismos σ_1 ou σ_2 não é nilpotente. Suponhamos que σ_1 não é nilpotente e provemos que σ_1 é um R-automorfismo.

Para cada $r \in \mathbb{N}$, seja

$$N_r = \big\{m \in M \colon (\sigma_1)^r(m) = 0\big\}.$$

Deste modo, obtemos cadeias

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \qquad \text{e} \qquad M \supseteq \sigma_1(M) \supseteq (\sigma_1)^2(M) \supseteq (\sigma_1)^3(M) \supseteq \cdots$$

de submódulos de M. Como M é noetheriano e artiniano, qualquer uma destas cadeias é estacionária e, portanto, existe $m \in \mathbb{N}$ tal que

$$N_m = N_{m+1} = N_{m+2} = \cdots \qquad \text{e} \qquad (\sigma_1)^m(M) = (\sigma_1)^{m+1}(M) = (\sigma_1)^{m+2}(M) = \cdots$$

Ponhamos $\pi = (\sigma_1)^m$ e observemos que $\pi \neq 0$ porque σ_1 não é nilpotente. Além disso, seja $N = \pi(M)$ e consideremos a inclusão $\iota_N \colon N \to M$. Com vista a aplicarmos o Lema 1.5.3, provemos que $\pi = \pi\iota_N$ é um R-automorfismo de $N = \pi(M)$. Ora, temos

$$\pi(N) = \pi(\pi(M)) = \pi^2(M) = (\sigma_1)^{2m}(M) = (\sigma_1)^m(M) = \pi(M) = N$$

e, portanto, $\pi \colon N \to N$ é sobrejectivo. Por outro lado, se $m \in M$ é tal que $\pi(\pi(m)) = 0$, então $(\sigma_1)^{2m}(m) = 0$, logo $m \in N_{2m} = N_m$ e, portanto, $\pi(m) = (\sigma_1)^m(m) = 0$. Segue-se que $\pi \colon N \to N$ é injectivo e, portanto, é um R-automorfismo de N. Pelo Lema 1.5.3, concluímos que $M = \iota_N(N) = N = \pi(M)$ e que $\pi \colon M \to M$ é um R-automorfismo. Como $\pi = (\sigma_1)^m$, é claro que σ_1 também é um R-automorfismo de M, como se queria.

Finalmente, suponhamos que $n \geq 3$. Pondo $\tau = \tau_1 + (\tau_2 + \cdots + \tau_n)$, o que acabámos de provar garante que τ_1 ou $\tau_2 + \cdots + \tau_n$ é um R-automorfismo de M. No primeiro caso, não há mais

nada que provar; no segundo, procedemos recursivamente para concluir que existe $2 \leq i \leq n$ tal que τ_i é um R-automorfismo. □

1.5.5. Teorema (Krull-Schmidt). *Seja M um R-módulo noetheriano e artiniano e suponhamos que*

$$M = N_1 \oplus \cdots \oplus N_r = N'_1 \oplus \cdots \oplus N'_s$$

onde $N_1, \ldots, N_r \leq_R M$ e $N'_1, \ldots, N'_s \leq_R M$ são submódulos indecomponíveis. Então, $r = s$ e existe uma permutação $\sigma \in S_r$ tal que

$$N'_i \cong_R N_{\sigma(i)}, \qquad 1 \leq i \leq r.$$

Demonstração. Procedemos por indução sobre r. O resultado é trivial para $r = 1$; assim, suponhamos que é verdadeiro para todos os R-módulos que admitem uma decomposição em soma directa de $r' < r$ submódulos indecomponíveis.

Para cada $1 \leq i \leq r$ e cada $1 \leq j \leq s$, sejam $\pi_i \colon M \to N_i$ e $\pi'_j \colon M \to N_j$ as projecções asosociadas às decomposições dadas. Então,

$$\mathrm{id}_M = \pi_1 + \cdots + \pi_r = \pi'_1 + \cdots + \pi'_s$$

e

$$\pi_i \pi_{i'} = \pi'_j \pi'_{j'} = 0, \qquad 1 \leq i \neq i' \leq r,\ 1 \leq j \neq j' \leq s.$$

Sendo assim, temos

$$\pi_1 = \pi_1 \,\mathrm{id}_M = \pi_1(\pi'_1 + \cdots + \pi'_s) = \pi_1\pi'_1 + \cdots + \pi_1\pi'_s$$

e, portanto,

$$\mathrm{id}_{N_1} = \tau_1 + \cdots + \tau_s$$

onde $\tau_j = (\pi_1 \pi'_j)_{N_1} \in \mathrm{End}_R(N_1)$ para $1 \leq j \leq s$; notemos que $(\pi_1)_{N_1} = \mathrm{id}_{N_1}$. Como id_{N_1} é um R-automorfismo, o Lema 1.5.4 garante que existe $1 \leq j \leq s$ tal que τ_j é um R-automorfismo de N_1. Sem perda de generalidade, suponhamos que $j = 1$, isto é, τ_1 é um R-automorfismo de N_1. Como τ_1 é a composição

$$N_1 \xrightarrow{\pi'_1} N'_1 \xrightarrow{\pi_1} N_1,$$

concluímos que $\pi'_1 \colon N_1 \to N'_1$ é um R-monomorfismo e $\pi_1 \colon N'_1 \to N_1$ é um R-epimorfismo, de modo que, pelo Lema 1.5.3, $\pi'_1 \colon N_1 \to N'_1$ e $\pi_1 \colon N'_1 \to N_1$ são R-isomorfismos.

De seguida, provamos que a soma $M' = N'_1 + N_2 + \cdots + N_r$ é directa. Para isso, sejam $n'_1 \in N'_1$ e $n_i \in N_i$, para $2 \leq i \leq r$, tais que

$$n'_1 + n_2 + \cdots + n_r = 0.$$

Então,

$$0 = \pi_1(0) = \pi_1(n'_1) + \pi_1(n_2) + \cdots + \pi_1(n_r) = \pi_1(n'_1)$$

e, portanto, $n_1' = 0$ (porque $\pi_1 \colon N_j' \to N_1$ é um R-isomorfismo). Segue-se que $n_2 + \cdots + n_r = 0$, logo $n_2 = \cdots = n_r = 0$ (porque a soma $N_2 + \cdots + N_r = 0$ é directa). Em conclusão,

$$M' = N_1' \oplus N_2 \oplus \cdots + N_r,$$

como se queria. Agora, seja

$$\theta = \pi_1'\pi_1 + \pi_2 + \cdots + \pi_r \in \mathrm{End}_R(M).$$

É fácil verificar que θ é um R-monomorfismo e que $\theta(M) = M'$; além disso, $\theta(N_1) = N_1'$. Provemos que, de facto, $M' = M$. Para isso, a cadeia de submódulos

$$M \supseteq \theta(M) \supseteq \theta^2(M) \supseteq \cdots$$

é estacionária (porque M é artiniano) e, portanto,

$$\theta^t(M) = \theta^{t+1}(M) = \theta^{t+2}(M) = \cdots$$

para algum $t \in \mathbb{N}$. Sendo assim, para cada $m \in M$, existe $m' \in M$ tal que $\theta^t(m) = \theta^{t+1}(m')$, pelo que $\theta^t(m - \theta(m')) = 0$ e, portanto, $m = \theta(m')$ (porque θ é injectivo). Daqui, resulta que $M = \theta(M) = M'$, como se pretende.

Deste modo, construímos um R-automorfismo $\theta \colon M \to M$ tal que $\theta(N_1) = N_1'$. Por conseguinte, obtemos

$$M = \theta(M) = \theta(N_1) \oplus \theta(N_2) \oplus \cdots \oplus \theta(N_r) = N_1' \oplus \theta(N_2) \oplus \cdots \oplus \theta(N_r).$$

Como $M = N_1' \oplus N_2' \oplus \cdots \oplus N_s'$, concluímos que

$$\theta(N_2) \oplus \cdots \oplus \theta(N_r) = N_2' \oplus \cdots \oplus N_s',$$

de modo que, por hipótese de indução, $s - 1 = r - 1$ e existe uma permutação τ de $\{2, \ldots, r\}$ tal que

$$\theta(N_i) \cong_R N_{\tau(i)}', \qquad 2 \leq i \leq r.$$

O resultado segue-se. □

1.5.6. Corolário. *Seja M um R-módulo noetheriano e artiniano e suponhamos que*

$$M = M_1 \oplus \cdots \oplus M_t$$

onde $M_1, \ldots, M_t \leq_R M$ são submódulos indecomponíveis. Se $N \leq_R M$ é uma parcela directa de M, então existem $1 \leq i_1, \ldots, i_r \leq t$ tais que

$$N \cong_R M_{i_1} \oplus \cdots \oplus M_{i_r}.$$

Demonstração. Como N é parcela directa de M, existe $N' \leq_R M$ tal que $M = N \oplus N'$. Como M é artiniano, também N e N' são artinianos e, portanto, existem submódulos indecomponíveis não-nulos $N_1, \ldots, N_r \leq_R N$ e $N_1', \ldots, N_s' \leq_R N'$ tais que

$$N = N_1 \oplus \cdots \oplus N_r \qquad \text{e} \qquad N' = N_1' \oplus \cdots \oplus N_s',$$

de maneira que $M = N_1 \oplus \cdots \oplus N_r \oplus N'_1 \oplus \cdots \oplus N'_s$. Pelo Teorema de Krull-Schmidt, temos $t = r + s$ e, a menos de R-isomorfismo,

$$\{M_1, \ldots, M_t\} = \{N_1, \ldots, N_r, N'_1, \ldots, N'_s\}.$$

o que termina a demonstração. □