

Universidade do Minho
Escola de Ciências

Módulos e Anéis

resolução dos exercícios propostos

Mestrado em Matemática e Computação

SUZANA MENDES GONÇALVES
Departamento de Matemática

1 Módulos

exercício 1. Sejam R um anel e G um grupo aditivo abeliano. Mostre que G pode ser visto como um módulo$-R$ à direita, considerando trivialmente a família de ações $\{\lambda_a\}_{a\in R}$, com

$$\begin{array}{rccc} \lambda_a: & G & \longrightarrow & G \\ & x & \longmapsto & xa = 0_G \end{array}$$

para todo o $a \in R$.

(i) Sabemos que $(G, +)$ é um grupo abeliano.

(ii) Para quaisquer $x, y \in G$ e $a \in R$, temos $x + y \in G$, pelo que

$$(x + y)a = 0_G = 0_G + 0_G = xa + ya.$$

(iii) Para quaisquer $x \in G$ e $a, b \in R$, sabemos que $a + b \in R$ e, portanto,

$$x(a + b) = 0_G = 0_G + 0_G = xa + xb.$$

(iv) Para quaisquer $x \in G$ e $a, b \in R$, sabemos que $ab \in R$ e, portanto,

$$x(ab) = 0_G = 0_G b = (xa)b.$$

Por (i)-(iv), G é um módulo$-R$ à direita.

exercício 2. Seja G um grupo aditivo abeliano. Prove que G, com

$$nx = \begin{cases} \underbrace{x + \cdots + x}_{n \text{ vezes}} & \text{se } n > 0 \\ 0_G & \text{se } n = 0 \\ -(\underbrace{x + \cdots + x}_{-n \text{ vezes}}) & \text{se } n < 0 \end{cases}$$

para quaisquer $x \in G$ e $n \in \mathbb{Z}$, é um módulo$-\mathbb{Z}$ à esquerda unitário.

(i) Sabemos que $(G, +)$ é um grupo abeliano.

(ii) Sejam $x, y \in G$ e $n \in \mathbb{Z}$. Se $n = 0$, então

$$n(x+y) = 0_G = 0_G + 0_G = nx + ny.$$

Por outro lado, se $n > 0$, então, pela associatividade e comutatividade de $+$ em G,

$$n(x+y) \;=\; \underbrace{(x+y)+\cdots+(x+y)}_{n \text{ vezes}} \;=\; \underbrace{(x+\cdots+x)}_{n \text{ vezes}} + \underbrace{(y+\cdots+y)}_{n \text{ vezes}} \;=\; nx+ny.$$

Por último, se $n < 0$, então

$$n(x+y) \;=\; -\underbrace{((x+y)+\cdots+(x+y))}_{-n \text{ vezes}} \;=\; -\underbrace{(x+\cdots+x)}_{-n \text{ vezes}} + \Bigg(-\underbrace{(y+\cdots+y)}_{-n \text{ vezes}}\Bigg) \;=\; nx+ny.$$

(iii) Sejam $x \in G$ e $n, m \in \mathbb{Z}$. Se $n = 0$, então $n + m = m$ e

$$(n+m)x = mx = 0_G + mx = nx + mx.$$

De igual modo, para $m = 0$, concluímos que $(n+m)x = nx + mx$. Suponhamos que $n, m > 0$. Então,

$$(n+m)x \;=\; \underbrace{x+\cdots+x}_{n+m \text{ vezes}} \;=\; \underbrace{(x+\cdots+x)}_{n \text{ vezes}} + \underbrace{(x+\cdots+x)}_{m \text{ vezes}} \;=\; nx+mx.$$

Por outro lado, se $n, m < 0$, então $n + m < 0$ e

$$(n+m)x \;=\; -\underbrace{(x+\cdots+x)}_{-(n+m) \text{ vezes}} \;=\; -\underbrace{(x+\cdots+x)}_{-n \text{ vezes}} + \Bigg(-\underbrace{(x+\cdots+x)}_{-m \text{ vezes}}\Bigg) \;=\; nx+mx.$$

Assumamos, agora, que $n > 0 > m$ (o caso em que $m > 0 > n$ é análogo). Se $m = -n$, então $n + m = 0$ e

$$(n+m)x = 0x = 0_G = nx - nx = nx + mx.$$

Se $|n| > |m|$, então $n > n + m > 0$ e

$$(n+m)x \;=\; \underbrace{(x+\cdots+x)}_{n+m \text{ vezes}} \;=\; \underbrace{(x+\cdots+x)}_{n \text{ vezes}} + \Bigg(-\underbrace{(x+\cdots+x)}_{-m \text{ vezes}}\Bigg) \;=\; nx+mx.$$

Por fim, se $|n| < |m|$, então $m < n + m < 0$ e

$$(n+m)x \;=\; -\underbrace{(x+\cdots+x)}_{-(n+m) \text{ vezes}} \;=\; \underbrace{(x+\cdots+x)}_{n \text{ vezes}} + \Bigg(-\underbrace{(x+\cdots+x)}_{-m \text{ vezes}}\Bigg) \;=\; nx+mx.$$

(iv) Sejam $x \in G$ e $n, m \in \mathbb{Z}$. Se $n = 0$, então $nm = 0$ e

$$(nm)x = 0x = 0_G = 0(mx) = n(mx).$$

De igual modo, se $m = 0$, então $nm = 0$ e

$$(nm)x = 0x = 0_G = n0_G = n(mx).$$

Suponhamos que $n, m > 0$. Então, $nm > 0$ e

$$(nm)x = \underbrace{x + \cdots + x}_{nm \text{ vezes}} = \underbrace{\underbrace{(x + \cdots + x)}_{m \text{ vezes}} + \cdots + \underbrace{(x + \cdots + x)}_{m \text{ vezes}}}_{n \text{ vezes}} = n(mx).$$

Se $n, m < 0$, também se tem $nm > 0$ e

$$(nm)x = \underbrace{x + \cdots + x}_{nm \text{ vezes}} = -\left(\underbrace{-(x + \cdots + x)}_{nm \text{ vezes}}\right) = \underbrace{-\left(\underbrace{-(x + \cdots + x)}_{-m \text{ vezes}} - \cdots - \underbrace{(x + \cdots + x)}_{-m \text{ vezes}}\right)}_{-n \text{ vezes}}$$

$$= -\underbrace{(mx + \cdots + mx)}_{-n \text{ vezes}} = n(mx).$$

Assumamos, agora, que $n > 0$ e $m < 0$. Então, $nm < 0$ e

$$(nm)x = -\underbrace{(x + \cdots + x)}_{-nm \text{ vezes}} = \underbrace{-\underbrace{(x + \cdots + x)}_{-m \text{ vezes}} - \cdots - \underbrace{(x + \cdots + x)}_{-m \text{ vezes}}}_{n \text{ vezes}}$$

$$= \underbrace{(mx + \cdots + mx)}_{n \text{ vezes}} = n(mx).$$

Por último, se $n < 0$ e $m > 0$. Então, $nm < 0$ e

$$(nm)x = -\underbrace{(x + \cdots + x)}_{-nm \text{ vezes}} = -\left(\underbrace{\underbrace{(x + \cdots + x)}_{m \text{ vezes}} + \cdots + \underbrace{(x + \cdots + x)}_{m \text{ vezes}}}_{-n \text{ vezes}}\right)$$

$$= -\underbrace{(mx + \cdots + mx)}_{-n \text{ vezes}} = n(mx).$$

Por (i)-(iv), G é um módulo$-\mathbb{Z}$ à esquerda. Para mostrar que G é unitário basta observar que, para todo o $x \in G$,

$$1x = \underbrace{x}_{1 \text{ vez}} = x.$$

exercício 3. Sejam R um anel e S um subanel de R. Então, R é um módulo$-S$ à direita, com $xa = x \cdot_R a$, para quaisquer $x \in R$, $a \in S$.

(i) Sabemos que $(R, +)$ é um grupo abeliano.

(ii) Dados $x, y \in R$ e $a \in S$, temos $x + y, a \in R$ e, pela distributividade (à direita) da multiplicação em relação à adição em R,

$$(x + y)a = (x + y) \cdot_R a = x \cdot_R a + y \cdot_R a = xa + ya.$$

(iii) Dados $x \in R$ e $a, b \in S$, temos $x, a, b \in R$ e, pela distributividade (à esquerda) da multiplicação em relação à adição em R,

$$x(a + b) = x \cdot_R (a + b) = x \cdot_R a + x \cdot_R b = xa + xb.$$

(iv) Sejam $x \in R$ e $a, b \in S$. Então, $x, a, b \in R$. Como a multiplicação é associativa em R,

$$x(ab) = x \cdot_R (a \cdot_R b) = (x \cdot_R a) \cdot_R b = (xa)b.$$

Por (i)-(iv), R é um módulo$-S$ à direita.

exercício 4. Sejam R, S anéis, $\varphi : R \to S$ um homomorfismo de anéis e M um módulo$-S$ à direita. Então, M é um módulo$-R$ à direita, com $xa = x\varphi(a)$, para quaisquer $x \in M$, $a \in R$.

(i) Sabemos que $(M, +)$ é um grupo abeliano, pois M é um módulo$-S$.

(ii) Sejam $x, y \in M$ e $a \in R$. Então, $\varphi(a) \in S$. Como M é um módulo$-S$, temos

$$(x + y)a = (x + y)\varphi(a) = x\varphi(a) + y\varphi(a) = xa + ya.$$

(iii) Sejam $x \in M$ e $a, b \in R$. Então, $\varphi(a), \varphi(b) \in S$ e, por M ser módulo$-S$, temos $x(\varphi(a) + \varphi(b)) = x\varphi(a) + x\varphi(b)$. Logo, como φ é um homomorfismo de anéis,

$$x(a + b) = x\varphi(a + b) = x\left(\varphi(a) + \varphi(b)\right) = x\varphi(a) + x\varphi(b) = xa + xb.$$

(iv) Sejam $x \in M$ e $a, b \in R$. Então, $\varphi(a), \varphi(b) \in S$ e, por M ser módulo$-S$, temos $x\left(\varphi(a)\varphi(b)\right) = \left(x\varphi(a)\right)\varphi(b)$. Assim, sendo φ um homomorfismo de anéis,

$$x(ab) = x(\varphi(ab)) = x(\varphi(a)\varphi(b)) = (x\varphi(a))\varphi(b) = (xa)\varphi(b) = (xa)b.$$

Por (i)-(iv), M é um módulo$-R$ à direita.

exercício 5. Considere o grupo abeliano $(\mathbb{Z}_5, +)$. Defina uma família de operações unárias

$$\left\{\lambda_{[a]_{15}} : \mathbb{Z}_5 \to \mathbb{Z}_5\right\}_{a\in\mathbb{Z}}$$

que concedam uma estrutura de módulo$-\mathbb{Z}_{15}$ a $\mathbb{Z}_5$.

Dados $[a]_{15} \in \mathbb{Z}_{15}$ e $[x]_5 \in \mathbb{Z}_5$, com $a, x \in \mathbb{Z}$, temos que $xa \in \mathbb{Z}$ e, portanto, $[xa]_5 \in \mathbb{Z}_5$. Definamos então

$$\begin{array}{rccc} \lambda_{[a]_{15}} : & \mathbb{Z}_5 & \longrightarrow & \mathbb{Z}_5 \\ & [x]_5 & \longmapsto & [xa]_5 \end{array}$$

para todo o $x \in \mathbb{Z}$.

Comecemos por mostrar que $\lambda_{[a]_{15}}$ é uma aplicação. Se $x, y \in \mathbb{Z}$ são tais que $[x]_5 = [y]_5$, então $5|(x-y)$. Logo, $5|(x-y)a = xa - ya$, donde concluímos que $[xa]_5 = [ya]_5$. Assim, $\lambda_{[a]_{15}}([x]_5) = \lambda_{[a]_{15}}([y]_5)$. Portanto, $\lambda_{[a]_{15}}$ é uma aplicação.

Vejamos agora que $\lambda_{[a]_{15}} = \lambda_{[b]_{15}}$ sempre que $[a]_{15} = [b]_{15}$. Ora, dados $a, b \in \mathbb{Z}$ tais que $[a]_{15} = [b]_{15}$, sabemos que $15|(a-b)$. Como $5|15$, podemos concluir que $5|(a-b)$ e, para todo o $x \in \mathbb{Z}$, $5|x(a-b) = xa - xb$. Logo, para todo o $x \in \mathbb{Z}$, $[xa]_5 = [xb]_5$, ou seja, $\lambda_{[a]_{15}}([x]_5) = \lambda_{[b]_{15}}([x]_5)$. Por outras palavras, vimos que $\lambda_{[a]_{15}}$ está bem definida e não depende do representante escolhido para a classe $[a]_{15}$.

Mostremos então que $\mathbb{Z}_5$ fica com uma estrutura de módulo$-\mathbb{Z}_{15}$ à direita.

(i) Sabemos que $(\mathbb{Z}_5, +)$ é um grupo abeliano.

(ii) Sejam $[x]_5, [y]_5 \in \mathbb{Z}_5$ e $[a]_{15} \in \mathbb{Z}_{15}$, com $x, y, a \in \mathbb{Z}$. Temos

$$([x]_5+[y]_5)[a]_{15} = [x+y]_5[a]_{15} = [(x+y)a]_5 = [xa+ya]_5 = [xa]_5+[ya]_5 = [x]_5[a]_{15}+[y]_5[a]_{15}.$$

(iii) Sejam $[x]_5 \in \mathbb{Z}_5$ e $[a]_{15}, [b]_{15} \in \mathbb{Z}_{15}$, com $x, a, b \in \mathbb{Z}$. Temos

$$[x]_5([a]_{15}+[b]_{15}) = [x]_5[a+b]_{15} = [x(a+b)]_5 = [xa+xb]_5 = [xa]_5+[xb]_5 = [x]_5[a]_{15}+[x]_5[b]_{15}.$$

(iv) Sejam $[x]_5 \in \mathbb{Z}_5$ e $[a]_{15}, [b]_{15} \in \mathbb{Z}_{15}$, com $x, a, b \in \mathbb{Z}$. Temos

$$[x]_5\left([a]_{15}[b]_{15}\right) = [x]_5[ab]_{15} = [x(ab)]_5 = [(xa)b]_5 = [xa]_5[b]_{15} = \left([x]_5[a]_{15}\right)[b]_{15}.$$

Por (i)-(iv), $\mathbb{Z}_5$ é um módulo$-\mathbb{Z}_{15}$ à direita.

exercício 6. Prove que todo o espaço vetorial V não nulo sobre um corpo $\mathbb{K}$ é um módulo$-\mathbb{K}$ à esquerda fiel unitário.

Seja V um espaço vetorial não nulo sobre um corpo $\mathbb{K}$. Então, estão definidas duas operações: uma adição de elementos de V, $+ : V \times V \to V$, e uma multiplicação de um elemento de $\mathbb{K}$ por um elemento de V, $\cdot : \mathbb{K} \times V \to V$, tais que são satisfeitas as seguintes propriedades:

(V_1) $\forall x, y \in V, \quad x + y = y + x$;

(V_2) $\forall x, y, z \in V, \quad x + (y + z) = (x + y) + z$;

(V_3) $\exists 0_V \in V \, \forall x \in V, \quad x + 0_V = 0_V + x = x$;

(V_4) $\forall x \in V \, \exists x' \in V : \quad x + x' = x' + x = 0_V$;

(V_5) $\forall x, y \in V \, \forall \alpha \in \mathbb{K}, \quad \alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$;

(V_6) $\forall x \in V \, \forall \alpha, \beta \in \mathbb{K}, \quad (\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$;

(V_7) $\forall x \in V \, \forall \alpha, \beta \in \mathbb{K}, \quad (\alpha\beta) \cdot x = \alpha \cdot (\beta \cdot x)$;

(V_8) $\forall x \in V, \quad 1 \cdot x = x$.

Vejamos que V é módulo$-\mathbb{K}$ à esquerda.

(i) Porque $+$ é uma operação binária em V e por $(V_1) - (V_4)$, sabemos que $(V, +)$ é um grupo abeliano.

(ii) Sejam $x, y \in V$ e $\alpha \in \mathbb{K}$. Por (V_5),
$$\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y.$$

(iii) Sejam $x \in V$ e $\alpha, \beta \in \mathbb{K}$. Por (V_6),
$$(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x.$$

(iv) Sejam $x \in V$ e $\alpha, \beta \in \mathbb{K}$. Por (V_7),
$$(\alpha\beta) \cdot x = \alpha \cdot (\beta \cdot x).$$

Por (i)-(iv), V é um módulo$-\mathbb{K}$ à esquerda. Por (V_8), V é um módulo unitário. Vejamos que V é fiel. Sabemos que $0_{\mathbb{K}} \in \text{an}(V)$. Tomemos agora $\alpha \in \text{an}(V)$. Pretendemos mostrar que $\alpha = 0_{\mathbb{K}}$. Por definição de $\text{an}(V)$, $\alpha \cdot x = 0_V$ para todo o $x \in V$. Em particular, se $y \in V \setminus \{0_V\}$, então $\alpha \cdot y = 0_V$ (recordemos que, por hipótese, V é não nulo). Como $\{y\}$ é um conjunto linearmente independente e $\alpha \cdot y = 0_V$, podemos concluir que $\alpha = 0_{\mathbb{K}}$. Assim, $\text{an}(V) = \{0_{\mathbb{K}}\}$ e V é fiel.

exercício 7. Sejam R um anel e M um módulo$-R$ à direita. Mostre que, para quaisquer $n, r \in \mathbb{N}$, $a, a_1, \ldots, a_r \in R$ e $x, x_1, \ldots, x_r \in M$, se tem:

(a) $n(xa) = x(na) = (nx)a$.

(b) $\left(\sum_{i=1}^{r} x_i\right) a = \sum_{i=1}^{r} (x_i a)$.

(c) $x \left(\sum_{i=1}^{r} a_i\right) = \sum_{i=1}^{r} (x a_i)$.

(a) $n(xa) = x(na) = (nx)a$.

Vamos demonstrar as igualdades por indução sobre n. É claro que, para $n = 1$, temos

$$n(xa) = 1(xa) = xa = x(1a) = (1x)a.$$

Tomemos agora $k \in \mathbb{N}$ tal que $k(xa) = x(ka) = (kx)a$. Então,

$$(k+1)(xa) \;=\; \underbrace{xa + \cdots + xa}_{k+1 \text{ vezes}} \;=\; \underbrace{xa + \cdots + xa}_{k \text{ vezes}} + xa \;=\; k(xa) + xa$$

Como M é módulo$-R$ à direita, $kx \in M$ e $ka \in R$, sabemos que $x(ka)+xa = x(ka+a)$ e $(kx)a + xa = (kx + x)a$. Pela hipótese de indução e pela definição de múltiplo, tanto em M como em R, temos

$$(k+1)(xa) = x(ka) + xa = x(ka + a) = x\left((k+1)a\right)$$

e

$$(k+1)(xa) = (kx)a + xa = (kx + x)a = \left((k+1)x\right)a.$$

Logo, pelo Princípio de Indução Matemática, $n(xa) = x(na) = (nx)a$, para todo o $n \in \mathbb{N}$.

(b) $\left(\sum_{i=1}^{r} x_i\right) a = \sum_{i=1}^{r} (x_i a)$.

Vamos demonstrar a igualdade por indução sobre r. É claro que, para $r = 1$, temos

$$\left(\sum_{i=1}^{r} x_i\right) a = \left(\sum_{i=1}^{1} x_i\right) a = x_1 a = \sum_{i=1}^{1} (x_i a) = \sum_{i=1}^{r} (x_i a).$$

Tomemos agora $k \in \mathbb{N}$ tal que $\left(\sum_{i=1}^{k} x_i\right) a = \sum_{i=1}^{k} (x_i a)$. Então, pela hipótese de indução e como M é módulo$-R$ e $\sum_{i=1}^{k} x_i$, $x_{k+1} \in M$, $a \in R$, temos

$$\left(\sum_{i=1}^{k+1} x_i\right) a = \left(\sum_{i=1}^{k} x_i + x_{k+1}\right) a = \left(\sum_{i=1}^{k} x_i\right) a + x_{k+1} a = \sum_{i=1}^{k} (x_i a) + x_{k+1} a = \sum_{i=1}^{k+1} (x_i a).$$

Assim, pelo Princípio de Indução Matemática, $\left(\sum_{i=1}^{r} x_i\right) a = \sum_{i=1}^{r} (x_i a)$, para todo $r \in \mathbb{N}$.

(c) $x\left(\sum_{i=1}^{r} a_i\right) = \sum_{i=1}^{r}(xa_i)$.

O resultado vai ser demonstrado por indução sobre r. Para $r = 1$, temos

$$x\left(\sum_{i=1}^{r} a_i\right) = x\left(\sum_{i=1}^{1} a_i\right) = xa_1 = \sum_{i=1}^{1}(xa_1) = \sum_{i=1}^{r}(xa_i).$$

Seja $k \in \mathbb{N}$ tal que $x\left(\sum_{i=1}^{k} a_i\right) = \sum_{i=1}^{k}(xa_i)$. Pela hipótese de indução e como M é módulo$-R$ e $x \in M$, $\sum_{i=1}^{k} a_i$, $a_{k+1} \in R$, temos

$$x\left(\sum_{i=1}^{k+1} a_i\right) = x\left(\sum_{i=1}^{k} a_i + a_{k+1}\right) = x\left(\sum_{i=1}^{k} a_i\right) + xa_{k+1} = \sum_{i=1}^{k}(xa_i) + xa_{k+1} = \sum_{i=1}^{k+1}(xa_i).$$

Assim, pelo Princípio de Indução Matemática, $x\left(\sum_{i=1}^{r} a_i\right) = \sum_{i=1}^{r}(xa_i)$, para todo $r \in \mathbb{N}$.

2 Submódulos

exercício 1. Sejam R um anel unitário, M um módulo$-R$ à direita unitário e N uma parte não vazia de M. Mostre que são equivalentes as seguintes condições:

(i) N é submódulo$-R$ de M.

(ii) Para quaisquer $x, y \in N$ e quaisquer $a, b \in R$, $xa + yb \in N$.

(iii) Para quaisquer $x, y \in N$ e qualquer $b \in R$, $x + yb \in N$.

(iv) Para quaisquer $x, y \in N$ e qualquer $b \in R$, $x + y \in N$ e $yb \in N$.

Suponhamos que N é um submódulo$-R$ de M. Então, N é um módulo$-R$ à direita. Sejam $x, y \in N$ e $a, b \in R$. Por definição de módulo, sabemos que $xa, yb \in N$. Sendo N fechado para a adição, temos $xa + yb \in N$, para quaisquer $x, y \in N$ e quaisquer $a, b \in R$.

Assumamos agora que, para quaisquer $x, y \in N$ e quaisquer $a, b \in R$, $xa + yb \in N$. Como R é unitário, existe $1_R \in \mathbb{R}$. Assim, dados $x, y \in N$ e $b \in R$, temos $x1_R + yb \in N$. Ora, M é módulo$-R$ unitário e $x \in N \subseteq M$. Portanto, $x1_R = x$. Logo, temos $x + yb \in N$, para quaisquer $x, y \in N$ e qualquer $b \in R$.

Suponhamos agora que, para quaisquer $x, y \in N$ e qualquer $b \in R$, $x + yb \in N$. Sejam $x, y \in N$ e $b \in R$. Sabemos que $1_R \in R$ e $0_M \in N$. Assim, por hipótese, $x + y1_R \in N$ e $0_M + yb \in N$. Mas $y1_R = y$ (por M ser unitário) e $0_M + yb = yb$ (por 0_M ser elemento neutro da adição e $yb \in M$). Portanto, concluímos que $x + y \in N$ e $yb \in N$, para quaisquer $x, y \in N$ e $b \in R$.

Finalmente, assumamos que, para quaisquer $x, y \in N$ e qualquer $b \in R$, $x + y \in N$ e $yb \in N$. Pretendemos mostrar que N é módulo$-R$. Como N é uma parte não vazia de M, existe $z \in N$. Logo,

$$0_M = z0_R \in N.$$

Mais, para quaisquer $x, y \in N$, temos $y(-1_R) \in N$ e, portanto, $x + y(-1_R) \in N$. Mas, sendo M um módulo$-R$ unitário, sabemos que $y(-1_R) = (-y)1_R = -y$, donde concluímos que

$$x - y = x + y(-1_R) \in N.$$

Assim, podemos afirmar que $(N, +)$ é um subgrupo de $(M, +)$ e, em particular, $(N, +)$ é um grupo abeliano. Como $N \subseteq M$ e as condições (ii)–(iv) da definição de módulo$-R$ à direita são satisfeitas por M, é claro que também o são por N. Assim, N é um módulo$-R$ à direita, e $N \leq_R M$.

exercício 2. Sejam R um anel, M um módulo$-R$ à direita, X um subconjunto não vazio de M e D um ideal direito de R. Mostre que XD é um submódulo$-R$ de M.

Seja $x \in XD$. Então, existem $n \in \mathbb{N}$, $x_1, x_2, \ldots, x_n \in X$ e $d_1, d_2, \ldots, d_n \in D$ tais que

$$x = x_1 d_1 + x_2 d_2 + \cdots + x_n d_n.$$

Como $X \subseteq M$, temos que $x_1, x_2, \ldots, x_n \in M$. De modo análogo, $d_1, d_2, \ldots, d_n \in R$, pois $D \subseteq R$. Sendo M um módulo$-R$, concluímos que $x_1 d_1, x_2 d_2, \ldots, x_n d_n \in M$ e, portanto, $x \in M$, Assim, $XD \subseteq M$.

É claro que, se X é um conjunto não vazio de M, existe $x_1 \in X$, Também sabemos que $0_R \in D$, uma vez que D é ideal direito de R. Assim, $0_M = x_1 0_R \in XD$ e XD é uma parte não vazia de M.

Tomemos, agora, $x, y \in XD$ e $a \in R$. Então, existem $n, m \in \mathbb{N}$, $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m \in X$ e $d_1, d_2, \ldots, d_n$, $e_1, e_2, \ldots, e_m \in D$ tais que

$$x = x_1 d_1 + x_2 d_2 + \cdots + x_n d_n \quad \text{e} \quad y = y_1 e_1 + y_2 e_2 + \cdots + y_m e_m.$$

Como M é um módulo$-R$, temos

$$\begin{aligned} x - y &= (x_1 d_1 + x_2 d_2 + \cdots + x_n d_n) - (y_1 e_1 + y_2 e_2 + \cdots + y_m e_m) \\ &= x_1 d_1 + x_2 d_2 + \cdots + x_n d_n + y_1(-e_1) + y_2(-e_2) + \cdots + y_m(-e_m). \end{aligned}$$

e

$$\begin{aligned} xa &= (x_1 d_1 + x_2 d_2 + \cdots + x_n d_n)a = (x_1 d_1)a + (x_2 d_2)a + \cdots + (x_n d_n)a \\ &= x_1(d_1 a) + x_2(d_2 a) + \cdots + x_n(d_n a). \end{aligned}$$

Ora, para cada $i \in \{1, \ldots, m\}$, $-e_i \in D$ pois $e_i \in D$ e D é ideal direito de R. Também, para cada $j \in \{1, \ldots, n\}$, $d_j a \in D$ porque $d_j \in D$, $a \in R$ e D é ideal direito de R. Assim, por definição, $x - y \in XD$ e $xa \in XD$.

Pela Proposição 22, XD é um submódulo$-R$ de M.

exercício 3. Seja G um grupo abeliano. Dados $n \in \mathbb{Z}$ e $a \in G$, definimos

$$na = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ vezes}} & \text{se } n > 0 \\ 0 & \text{se } n = 0 \\ -(\underbrace{a + \cdots + a}_{-n \text{ vezes}}) & \text{se } n < 0 \end{cases}$$

Sabemos que G é um módulo-$\mathbb{Z}$ à esquerda. Mostre que os submódulos-$\mathbb{Z}$ de G são exatamente os subgrupos de G.

Se $H \leq_{\mathbb{Z}} G$, então $H \subseteq G$ e H é módulo$-\mathbb{Z}$. Em particular, $H \subseteq G$ e $(H, +)$ é um grupo. Logo, H é um subgrupo de G. Reciprocamente, suponhamos que H é um subgrupo de G. Porque G é um módulo$-\mathbb{Z}$ à esquerda, sabemos que

(i) $(G, +)$ é um grupo abeliano;

(ii) $n(x + y) = nx + ny$, para quaisquer $n \in \mathbb{Z}$ e $x, y \in G$;

(iii) $(n + m)x = nx + mx$, para quaisquer $n, m \in \mathbb{Z}$ e $x \in G$;

(iv) $(nm)x = n(mx)$, para quaisquer $n, m \in \mathbb{Z}$ e $x \in G$.

Como H é subgrupo de G, é claro que

(i) $(H, +)$ é um grupo abeliano;

(ii) $n(x + y) = nx + ny$, para quaisquer $n \in \mathbb{Z}$ e $x, y \in H$;

(iii) $(n + m)x = nx + mx$, para quaisquer $n, m \in \mathbb{Z}$ e $x \in H$;

(iv) $(nm)x = n(mx)$, para quaisquer $n, m \in \mathbb{Z}$ e $x \in H$.

Logo, H é um módulo$-\mathbb{Z}$ que é subconjunto de G e, portanto, H é submódulo$-\mathbb{Z}$ de G.

exercício 4. Sejam R um anel comutativo, M um módulo$-R$ à direita e $a \in R$. Prove que $Ma \leq_R M$.

Por definição, $Ma = \left\{ \sum_{i=1}^{n} (x_i a) : n \in \mathbb{N} \wedge x_i \in M \right\}$. Mas M é um módulo$-R$, pelo que facilmente se verifica que

$$Ma = \{xa : x \in M\}$$

(basta usar a alínea (b) do exercício 7 da ficha 1).

Por definição de módulo$-R$, temos $xa \in M$ para qualquer $x \in M$, uma vez que $a \in R$. Logo, $Ma \subseteq M$. Como $0_M = 0_M a$, concluímos que $0_M \in Ma$ e, portanto, Ma é uma parte não vazia de M. Tomemos $x, y \in Ma$ e $b \in R$. Então, existem $x_1, y_1 \in M$ tais que $x = x_1 a$ e $y = y_1 a$. Assim, como M é módulo$-R$ e R é comutativo,

$$x - y = x_1 a - y_1 a = (x_1 - y_1)a,$$

com $x_1 - y_1 \in M$, e

$$xb = (x_1 a)b = x_1(ab) = x_1(ba) = (x_1 b)a,$$

com $x_1 b \in M$. Por isso, $x - y, xb \in Ma$. Logo, $Ma \leq_R M$.

exercício 5. Sejam R um anel, M um módulo$-R$ à direita e N, L submódulos$-R$ de M. Prove que $N \cup L$ é um submódulo$-R$ de M se e só se $N \subseteq L$ ou $L \subseteq N$.

Suponhamos que $N \cup L$ é um submódulo$-R$ de M e que $N \not\subseteq L$. Então, existe $n \in N \setminus L$. Para todo o $\ell \in L$, temos $n, \ell \in N \cup L$ e, como $N \cup L \leq_R M$, $n - \ell \in N \cup L$. Se $n - \ell \in L$, então $n = (n - \ell) + \ell \in L$, o que contradiz a escolha de n. Portanto, $n - \ell \in N$. Assim, $\ell = n - (n - \ell) \in N$. Ou seja, $L \subseteq N$, como pretendíamos mostrar.

Reciprocamente, suponhamos que $N \subseteq L$ ou $L \subseteq N$. Então, $N \cup L = L$ ou $N \cup L = N$, pelo que, por hipótese, $N \cup L$ é um submódulo$-R$ de M.

3 Submódulos gerados

exercício 1. Sejam R um anel unitário e M um módulo$-R$ à direita unitário. Mostre que, para todo o $x \in M$, $\langle x \rangle = xR$.

Seja $x \in M$. Vamos provar que xR é o menor submódulo$-R$ de M que contém $\{x\}$.

(i) Como R é anel unitário e M é módulo$-R$ unitário, existe 1_R e $x1_R = x$. Logo, $x \in xR$ e, portanto, $\{x\} \subseteq xR$.

(ii) Porque M é módulo$-R$, temos $xR \subseteq M$. Como vimos em (i), $x \in xR$ e, portanto, xR é uma parte não vazia de M. Tomemos, então, $y, z \in xR$ e $a \in R$. Ora, por definição de xR, existem $b, c \in R$ tais que $y = xb$ e $z = xc$, donde segue que

$$y - z = xb - xc = x(b - c) \quad \text{e} \quad ya = (xb)a = x(ba),$$

uma vez que M é módulo$-R$. Assim, $y - z, ya \in xR$, pois $b - c, ba \in R$. Logo, concluímos que xR é submódulo$-R$ de M.

(iii) Suponhamos que N é um submódulo$-R$ de M que contém $\{x\}$. Dado $y \in xR$, existe $a \in R$ tal que $y = xa$. Como $x \in N$ e N é submódulo$-R$ de M, sabemos que $xa \in N$, ou seja, $y \in N$. Assim, $xR \subseteq N$.

Por (i)–(iii), $xR = \langle x \rangle$.

exercício 2. Seja R um anel unitário. Sejam 1 a identidade de R e 0 o zero de R. Prove que

$$R^n = \langle \{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\} \rangle.$$

Por definição, $R^n = \{(a_1, \ldots, a_n) : \forall_{i \in \{1,\ldots,n\}}, a_i \in R\}$.

(i) Por hipótese, existe $1 \in R$. Dado $i \in \{1, \ldots, n\}$, denotemos por e_i o elemento $(e_{i1}, \ldots, e_{in})$ de R^n tal que $e_{ij} = \begin{cases} 0 \text{ se } i \neq j \\ 1 \text{ se } i = j \end{cases}$. É claro que $\{e_1, \ldots, e_n\} \subseteq R^n$.

(ii) Sabemos que R^n é um módulo$-R$ à direita. Em particular, R^n é um submódulo$-R$ de R^n.

(iii) Suponhamos, por último, que L é um submódulo$-R$ de R^n que contém $\{e_1, \ldots, e_n\}$. Pretendemos mostrar que $R^n \subseteq L$. Para tal, tomemos $(a_1, \ldots, a_n) \in R^n$. Então, pela definição da ação de R em R^n,

$$(a_1, \ldots, a_n) = (a_1, 0, \ldots, 0) + \cdots + (0, \ldots, 0, a_n) = e_1 a_1 + \cdots + e_n a_n.$$

Ora, para cada $i \in \{1, \ldots, n\}$, $e_i \in L$ e $a_i \in R$. Sendo L um módulo$-R$, concluímos que $e_i a_i \in L$ e, portanto,

$$(a_1, \ldots, a_n) = e_1 a_1 + \cdots + e_n a_n \in L.$$

Logo, $R^n \subseteq L$.

Por (i)–(iii), R^n é o menor submódulo de R^n que contém $\{e_1, \ldots, e_n\}$. Por outras palavras, $R^n = \langle \{e_1, \ldots, e_n\} \rangle = \langle \{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\} \rangle$.

exercício 3. Seja R um anel e M um módulo$-R$ à direita não nulo e finitamente gerado. Mostre que M tem um submódulo maximal.

Sendo M um módulo$-R$ não nulo e finitamente gerado, existem $n \in \mathbb{N}$ e $x_1, \ldots, x_n \in M$ tais que

$$M = \langle \{x_1, \ldots, x_n\} \rangle = \sum_{i=1}^{n} \langle x_i \rangle.$$

Consideremos a família $\mathcal{F}$ de todos os submódulos próprios de M, isto é,

$$\mathcal{F} = \{N \leq_R M : N \subsetneq M\}.$$

Sabemos que $\{0_M\} \leq_R M$. Por hipótese, $\{0_M\} \in \mathcal{F}$, pelo que $\mathcal{F} \neq \emptyset$.

Consideremos uma cadeia não vazia $\mathscr{C} = \{N_i\}_{i \in I}$ de elementos de $\mathcal{F}$. Vamos mostrar que $\mathscr{C}$ admite majorante. Seja $N = \bigcup_{i \in I} N_i$. Por $\mathscr{C}$ ser uma cadeia, para quaisquer $i, j \in I$, $N_i \subseteq N_j$ ou $N_j \subseteq N_i$. Assim, $N_i \cup N_j \subseteq N_j$ ou $N_i \cup N_j \subseteq N_i$. Em ambos os casos, existe $k \in I$ tal que $N_i \cup N_j \subseteq N_k$. Logo, N é um submódulo$-R$ de M.

Suponhamos que $N = M = \langle \{x_1, \ldots, x_n\} \rangle$. Para cada $j \in \{1, \ldots, n\}$, $x_j \in M = N = \bigcup_{i \in I} N_i$. Logo, existe $i_j \in I$ tal que $x_j \in N_{i_j}$. Como $\mathscr{C}$ é uma cadeia, existe $k \in I$ tal que $N_{i_1} \cup N_{i_2} \cup \cdots \cup N_{i_n} \subseteq N_k$. Logo, $x_1, \ldots, x_n \in N_k$. Temos, então, que N_k é um submódulo$-R$ de M que contém $\{x_1, \ldots, x_n\}$ e, portanto, podemos concluir que

$$M = \langle \{x_1, \ldots, x_n\} \rangle \subseteq N_k,$$

o que contradiz o facto de N_k ser um submódulo próprio de M. Assim, N é um submódulo próprio de M e, portanto, $N \in \mathcal{F}$. Por definição, N é um majorante de $\mathscr{C}$.

Deste modo, vimos que toda a cadeia não vazia de $\mathcal{F}$ admite majorante. Pelo Lema de Zorn, podemos afirmar que $\mathcal{F}$ tem elemento maximal. Ou seja, M tem um submódulo maximal.

exercício 4. Considere $\mathbb{Q}$ como módulo$-\mathbb{Z}$ à direita. Seja $X \subseteq \mathbb{Q}$ tal que $\mathbb{Q} = \langle X \rangle$. Prove que, para todo o $x_0 \in X$, $\mathbb{Q} = \langle X \setminus \{x_0\} \rangle$.

Seja $x_0 \in X$. Vamos mostrar que $x_0 \in \langle X \setminus \{x_0\} \rangle$. Escrevamos $X = \{x_0\} \dot{\cup} \{x_i : i \in I\}$. Como $\frac{x_0}{2} \in \langle X \rangle$, existem $n_0 \in \mathbb{Z}$ e $n_i \in \mathbb{Z}$, $i \in I$, tais que os n_i são quase todos nulos e

$$\frac{x_0}{2} = x_0 n_0 + \sum_{i \in I} x_i n_i.$$

Então, $x_0 = x_0(2n_0) + \sum_{i \in I} x_i(2n_i)$, donde

$$x_0(1 - 2n_0) = \sum_{i \in I} x_i(2n_i). \tag{1}$$

Como $n_0 \in \mathbb{Z}$, é claro que $1 - 2n_0 \neq 0$. Portanto, $\frac{x_0}{1 - 2n_0} \in \mathbb{Q}$. Por hipótese, $\mathbb{Q}$ é gerado por X e, portanto, existem $m_0 \in \mathbb{Z}$ e $m_i \in \mathbb{Z}$, $i \in \mathbb{Z}$, tais que os m_i são quase todos nulos e

$$\frac{x_0}{1 - 2n_0} = x_0 m_0 + \sum_{i \in I} x_i m_i.$$

Assim, por (1),

$$\begin{aligned}
x_0 &= x_0 \left((1 - 2n_0)m_0\right) + \sum_{i \in I} x_i \left((1 - 2n_0)m_i\right) \\
&= \left(x_0(1 - 2n_0)\right) m_0 + \sum_{i \in I} x_i \left((1 - 2n_0)m_i\right) \\
&= \left(\sum_{i \in I} x_i 2n_i \right) m_0 + \sum_{i \in I} x_i((1 - 2n_0)m_i) \\
&= \sum_{i \in I} x_i(2n_i m_0) + \sum_{i \in I} x_i((1 - 2n_0)m_i) \\
&= \sum_{i \in I} x_i \left((2n_i m_0) + (1 - 2n_0)m_i\right).
\end{aligned}$$

Temos $n_0, m_0, n_i, m_i \in \mathbb{Z}$ e n_i, m_i são quase todos nulos. Portanto, para cada $i \in I$, $(2n_i m_0) + (1 - 2n_0)m_i \in \mathbb{Z}$. Mais, $(2n_i m_0) + (1 - 2n_0)m_i$ são quase todos nulos. Por outras palavras, vimos que $x_0 \in \langle X \setminus \{x_0\} \rangle$. Logo, $\langle X \setminus \{x_0\} \rangle$ é um submódulo$-\mathbb{Z}$ de $\mathbb{Q}$ que contém X, pelo que

$$\mathbb{Q} = \langle X \rangle \subseteq \langle X \setminus \{x_0\} \rangle \subseteq \mathbb{Q},$$

e a igualdade pretendida segue.

exercício 5. Considere $\mathbb{Q}$ como módulo$-\mathbb{Z}$ à direita. Prove que $\mathbb{Q}$ é infinitamente gerado.

Seja $X \subseteq \mathbb{Q}$ tal que $\mathbb{Q} = \langle X \rangle$. Vamos começar por mostrar que $\mathbb{Q} = \langle X \setminus \{x_1, \ldots, x_n\} \rangle$, para todo o $n \in \mathbb{N}$ e quaisquer $x_1, \ldots, x_n \in X$. Se $n = 1$, para todo o $x_1 \in X$, temos, pelo exercício anterior, que $\mathbb{Q} = \langle X \setminus \{x_1\} \rangle$. Suponhamos, agora que $\mathbb{Q} = \langle X \setminus \{x_1, \ldots, x_k\} \rangle$, para $k \in \mathbb{N}$ e $x_1, \ldots, x_k \in X$. Então, $Y = X \setminus \{x_1, \ldots, x_k\} \subseteq \mathbb{Q}$ é tal que $\mathbb{Q} = \langle Y \rangle$. Se tomarmos $x_{k+1} \in X \setminus \{x_1, \ldots, x_k\}$, temos que $\langle X \setminus \{x_1, \ldots, x_k, x_{k+1}\} \rangle = \langle (X \setminus \{x_1, \ldots, x_k\}) \setminus \{x_{k+1}\} \rangle = \langle Y \setminus \{x_{k+1}\} \rangle = \mathbb{Q}$, novamente pelo exercício anterior. Desta forma, dado $X \subseteq \mathbb{Q}$ tal que $\mathbb{Q} = \langle X \rangle$, concluímos que $|X| > n$, para todo o $n \in \mathbb{N}$ e, portanto, X não é finito.

4 Módulos quociente

exercício 1. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M. Mostre que a relação binária ρ_N definida em M por

$$x \,\rho_N\, y \quad \Leftrightarrow \quad y - x \in N \qquad (x, y \in M)$$

é uma relação de congruência em M.

Comecemos por mostrar que ρ_N é uma relação de equivalência.

(i) Seja $x \in M$. Como N é um submódulo$-R$ de M, sabemos que $0_M \in N$. Ora, $x - x = 0_M$. Logo, $x - x \in N$ e, por definição de ρ_N, temos

$$x \,\rho_N\, x.$$

Portanto, ρ_N é reflexiva.

(ii) Sejam $x, y \in M$ tais que $x \,\rho_N\, y$. Por definição, $y - x \in N$. Assim, $-(y-x) = -y+x = x - y \in N$, uma vez que N é um submódulo$-R$ de M. Logo, temos

$$y \,\rho_N\, x.$$

Vimos, então, que ρ_N é simétrica.

(iii) Sejam $x, y, z \in M$ tais que $x \,\rho_N\, y$ e $y \,\rho_N\, z$. Por definição de ρ_N, $y - x \in N$ e $z - y \in N$. Sendo N um submódulo$-R$ de M, temos $(z - y) + (y - x) \in N$, ou seja, $z - x \in N$. Portanto,

$$x \,\rho_N\, z$$

e ρ_N é transitiva.

Por (i)–(iii), ρ_N é uma relação de equivalência.

Tomemos, agora, $x, y, z, w \in N$ tais que $x \,\rho_N\, y$ e $z \,\rho_N\, w$. Tomemos, também, $a \in R$. Por definição de ρ_N, temos $y - x, w - z \in N$. Como N é um submódulo$-R$ de M, concluímos que $(y + w) - (x + z) = y + w - x - z = (y - x) + (w - z) \in N$ e $ya - xa = (y - x)a \in N$. Portanto, $(x + z) \,\rho_N\, (y + w)$ e $xa \,\rho_N\, ya$. Logo, ρ_N é uma relação de congruência em M.

exercício 2. Sejam R um anel unitário, M um módulo$-R$ à direita unitário e N um submódulo$-R$ de M. Verifique que M/N é unitário.

Sabemos que M/N é um módulo$-R$. Dado $A \in M/N$, existe $x \in M$ tal que $A = x + N$. Por definição da ação de R em M/N, temos

$$A1_R = (x + N)1_R = x1_R + N.$$

Como M é um módulo$-R$ à direita unitário, temos $x1_R = x$. Logo,

$$A1_R = x1_R + N = x + N = A,$$

pelo que M/N é um módulo$-R$ unitário.

exercício 3. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M, com $N \subsetneq M$. Prove que N é um submódulo maximal de M se e só se M/N for um módulo$-R$ simples.

Suponhamos que N é um submódulo maximal de M e seja P um submódulo$-R$ de M/N. Então, existe um submódulo$-R$ T de M tal que $N \subseteq T$ e $P = T/N$. Por hipótese, de $N \subseteq T \subseteq M$, concluímos que $T = N$ ou $T = M$. Assim, $P = N/N = \{N\} = \{0_{M/N}\}$ ou $P = M/N$. Portanto, os únicos submódulos de M/N são $\{0_{M/N}\}$ e M/N, ou seja, M/N é um módulo$-R$ simples.

Reciprocamente, admitamos que M/N é um módulo$-R$ simples. Pretendemos mostrar que N é um submódulo maximal de M. Para tal, tomemos T submódulo$-R$ de M tal que $N \subseteq T \subseteq M$. Então, T/N é submódulo$-R$ de M/N. Por hipótese, $T/N = \{0_{M/N}\}$ ou $T/N = M/N$. Logo, $T = N$ ou $T = M$. Por outras palavras, vimos que N é submódulo$-R$ maximal de M.

5 Morfismos$-R$

exercício 1. Sejam R um anel unitário, M e M' módulos$-R$ à direita unitários e $\varphi : M \to M'$ uma aplicação. Prove que são equivalentes as seguintes condições.

(a) φ é um morfismo$-R$.

(b) Para quaisquer $x, y \in M$ e $a, b \in R$, $\varphi(xa + yb) = \varphi(x)a + \varphi(y)b$.

(c) Para quaisquer $x, y \in M$ e $a \in R$, $\varphi(xa + y) = \varphi(x)a + \varphi(y)$.

Assumamos que φ é um morfismo$-R$. Sejam $x, y \in M$ e $a, b \in R$. Sendo M um módulo$-R$ à direita, sabemos que $xa, yb \in M$. Como φ é um morfismo e $xa, yb \in M$, temos $\varphi(xa + yb) = \varphi(xa) + \varphi(yb)$. Mais, $\varphi(xa) = \varphi(x)a$ e $\varphi(yb) = \varphi(y)b$. Assim,

$$\varphi(xa + yb) = \varphi(x)a + \varphi(y)b.$$

Vimos, então, que (a) implica (b).

Suponhamos agora que, para quaisquer $x, y \in M$ e $a, b \in R$, $\varphi(xa + yb) = \varphi(x)a + \varphi(y)b$. Em particular, para quaisquer $x, y \in M$ e $a \in R$, $\varphi(xa + y1_R) = \varphi(x)a + \varphi(y)1_R$. Como M é unitário e $y \in M$, temos $y1_R = y$. De igual modo, como M' é unitário e $\varphi(y) \in M'$, concluímos que $\varphi(y)1_R = \varphi(y)$. Logo,

$$\varphi(xa + y) = \varphi(x)a + \varphi(y),$$

e (b) implica (c).

Admitamos, por último, que, para quaisquer $x, y \in M$ e $a \in R$, $\varphi(xa + y) = \varphi(x)a + \varphi(y)$. Tomando $a = 1_R$, temos

$$\varphi(x + y) = \varphi(x1_R + y) = \varphi(xa + y) = \varphi(x)a + \varphi(y) = \varphi(x)1_R + \varphi(y) = \varphi(x) + \varphi(y),$$

pois M e M' são unitários. Por outro lado, se tomarmos $y = 0_M$, sabemos que $\varphi(y) = \varphi(0_M) = 0_{M'}$ e, portanto,

$$\varphi(xa) = \varphi(xa + 0_M) = \varphi(xa + y) = \varphi(x)a + \varphi(y) = \varphi(x)a + 0_{M'} = \varphi(x)a.$$

Logo, φ é um morfismo$-R$ e (c) implica (a).

Concluímos, assim, que as três condições apresentadas são equivalentes.

exercício 2. Sejam R um anel, M e M' módulos$-R$ à direita e $\varphi : M \to M'$ um morfismo$-R$. Mostre que

(a) se N é um submódulo$-R$ de M, $\varphi(N)$ é um submódulo$-R$ de M'.

(b) se N' é um submódulo$-R$ de M', $\varphi^{\leftarrow}(N')$, o conjunto imagem inversa de N' por φ, é um submódulo$-R$ de M.

(a) se N é um submódulo$-R$ de M, $\varphi(N)$ é um submódulo$-R$ de M'.

Suponhamos que N é um submódulo$-R$ de M. Então, N é uma parte não vazia de M tal que, para quaisquer $x, y \in N$ e $a \in R$, se tem $x - y \in N$ e $xa \in N$.

Sabemos que $0_M \in N$. Como φ é um morfismo$-R$, temos $\varphi(0_M) = 0_{M'}$. Ora, por definição de $\varphi(N)$, $\varphi(N) \subseteq M'$ e $0_{M'} \in \varphi(N)$. Assim, $\varphi(N)$ é uma parte não vazia de M'.

Tomemos, agora, $z, w \in \varphi(N)$ e $a \in R$. Então, existem $x, y \in N$ tais que $z = \varphi(x)$ e $w = \varphi(y)$, pelo que

$$z - w = \varphi(x) - \varphi(y) = \varphi(x - y) \quad \text{e} \quad za = \varphi(x)a = \varphi(xa).$$

Como N é um submódulo$-R$ de M, sabemos que $x - y \in N$ e $xa \in N$. Logo, $z - w \in \varphi(N)$ e $za \in \varphi(N)$.

Assim, $\varphi(N)$ é um submódulo$-R$ de M'.

(b) se N' é um submódulo$-R$ de M', $\varphi^{\leftarrow}(N')$, o conjunto imagem inversa de N' por φ, é um submódulo$-R$ de M.

Suponhamos que N' é um submódulo$-R$ de M'. Então, N' é uma parte não vazia de M' tal que, para quaisquer $x', y' \in N'$ e $a \in R$, se tem $x' - y' \in N'$ e $x'a \in N'$.

Como $0_{M'} \in N'$ e $\varphi(0_M) = 0_{M'}$ (pois φ é um morfismo$-R$), temos que $0_M \in \varphi^{\leftarrow}(N')$. Por definição de $\varphi^{\leftarrow}(N')$, $\varphi^{\leftarrow}(N') \subseteq M$. Logo, $\varphi^{\leftarrow}(N')$ é uma parte não vazia de M.

Tomemos, agora, $x, y \in \varphi^{\leftarrow}(N')$ e $a \in R$. Então, $\varphi(x), \varphi(y) \in N'$, pelo que

$$\varphi(x) - \varphi(y) \in N' \quad \text{e} \quad \varphi(x)a \in N'.$$

Mas φ é um morfismo$-R$ e, portanto, $\varphi(x - y), \varphi(xa) \in N'$. Por definição de conjunto imagem inversa, $x - y, xa \in \varphi^{\leftarrow}(N')$.

Portanto, $\varphi^{\leftarrow}(N')$ é um submódulo$-R$ de M.

exercício 3. Sejam R um anel e M e M' dois módulos$-R$ à direita. Representamos por $\mathrm{Hom}_R(M, M')$ o conjunto de todos os morfismos$-R$ de M em M'. Prove que

(a) $\mathrm{Hom}_R(M, M')$, algebrizado com a operação usual de adição de aplicações entre grupos aditivos, é um grupo abeliano.

(b) Se R for um anel comutativo, é possível introduzir em $\mathrm{Hom}_R(M, M')$ uma estrutura de módulo$-R$, definindo, para todo o $a \in R$ e todo o $\varphi \in \mathrm{Hom}_R(M, M')$, a aplicação $\varphi a : M \to M'$, $x \mapsto \varphi(xa)$.

(a) $\mathrm{Hom}_R(M, M')$, algebrizado com a operação usual de adição de aplicações entre grupos aditivos, é um grupo abeliano.

(i) Seja φ_0 a aplicação de M em M' que a cada $x \in M$ faz corresponder $0_{M'}$. Como $0_{M'} + 0_{M'} = 0_{M'}$ e $0_{M'}a = 0_{M'}$, para todo o $a \in R$, temos que φ_0 é um morfismo$-R$. Assim, $\mathrm{Hom}_R(M, M')$ é um conjunto não vazio.

(ii) Sejam $\varphi, \psi \in \mathrm{Hom}_R(M, M')$. Para quaisquer $x, y \in M$ e $a \in R$, temos

$$\begin{aligned}(\varphi + \psi)(x + y) &= \varphi(x + y) + \psi(x + y) = \varphi(x) + \varphi(y) + \psi(x) + \psi(y)\\ &= \varphi(x) + \psi(x) + \varphi(y) + \psi(y) = (\varphi + \psi)(x) + (\varphi + \psi)(y)\end{aligned}$$

e

$$(\varphi + \psi)(xa) = \varphi(xa) + \psi(xa) = \varphi(x)a + \psi(x)a = (\varphi(x) + \psi(x))a = (\varphi + \psi)(x)a.$$

Assim, $\varphi + \psi \in \mathrm{Hom}_R(M, M')$ e $(\mathrm{Hom}_R(M, M'), +)$ é um grupóide.

(iii) Dados $\varphi, \psi, \delta \in \mathrm{Hom}_R(M, M')$, temos, para todo o $x \in M$,

$$\begin{aligned}((\varphi + \psi) + \delta)(x) &= (\varphi + \psi)(x) + \delta(x) = (\varphi(x) + \psi(x)) + \delta(x)\\ &= \varphi(x) + (\psi(x) + \delta(x)) = \varphi(x) + (\psi + \delta)(x) = (\varphi + (\psi + \delta))(x),\end{aligned}$$

uma vez que a adição é associativa em M'. Logo, $(\varphi + \psi) + \delta = \varphi + (\psi + \delta)$.

(iv) Dados $\varphi, \psi \in \mathrm{Hom}_R(M, M')$, para todo o $x \in M$,

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x) = \psi(x) + \varphi(x) = (\psi + \varphi)(x),$$

pelo que $\varphi + \psi = \psi + \varphi$, e a adição é comutativa em $\mathrm{Hom}_R(M, M')$.

(v) Para todo o morfismo$-R$ $\varphi : M \to M'$, dado $x \in M$,

$$(\varphi + \varphi_0)(x) = \varphi(x) + \varphi_0(x) = \varphi(x) + 0_{M'} = \varphi(x).$$

Portanto, $\varphi + \varphi_0 = \varphi$.

(vi) Seja $\varphi \in \mathrm{Hom}_R(M, M')$. Consideremos a aplicação $\psi : M \to M'$ definida por $\psi(x) = -\varphi(x)$, para todo o $x \in M$. Vejamos que $\psi \in \mathrm{Hom}_R(M, M')$ e $\psi = -\varphi$. Para quaisquer $x, y \in M$ e $a \in R$,

$$\psi(x+y) = -\varphi(x+y) = -(\varphi(x)+\varphi(y)) = -\varphi(x)-\varphi(y) = -\varphi(x)+(-\varphi(y)) = \psi(x)+\psi(y)$$

e

$$\psi(xa) = -\varphi(xa) = -(\varphi(x)a) = -\varphi(x)a.$$

Logo, ψ é um morfismo$-R$ de M em M'. Mais, dado $x \in M$,

$$(\psi + \varphi)(x) = \psi(x) + \varphi(x) = -\varphi(x) + \varphi(x) = 0_{M'} = \varphi_0(x),$$

pelo que $\psi + \varphi = \varphi_0$ e, portanto, $\psi = -\varphi$.

Por (i)-(vi), $(\mathrm{Hom}_R(M, M'), +)$ é um grupo abeliano.

(b) Se R for um anel comutativo, é possível introduzir em $\mathrm{Hom}_R(M, M')$ uma estrutura de módulo$-R$, definindo, para todo o $a \in R$ e todo o $\varphi \in \mathrm{Hom}_R(M, M')$, a aplicação $\varphi a : M \to M'$, $x \mapsto \varphi(xa)$.

Sejam $\varphi \in \mathrm{Hom}_R(M, M')$ e $a \in R$. Pretendemos mostrar que φa é um morfismo$-R$. Dados $x, y \in M$ e $b \in R$, como φ é um morfismo$-R$ e M' é módulo$-R$, temos

$$\begin{aligned}(\varphi a)(x+y) &= \varphi((x+y)a) = \varphi(x+y)a = (\varphi(x)+\varphi(y))a \\ &= \varphi(x)a + \varphi(y)a = \varphi(xa) + \varphi(ya) = (\varphi a)(x) + (\varphi a)(y)\end{aligned}$$

e, como M é módulo$-R$ e $ab = ba$ (pois R é anel comutativo),

$$(\varphi a)(xb) = \varphi((xb)a) = \varphi(x(ba)) = \varphi(x(ab)) = \varphi((xa)b) = \varphi(xa)b = (\varphi a)(x)b.$$

Assim, φa é um morfismo$-R$ de M em M'.

Ora, dados $\varphi, \psi \in \mathrm{Hom}_R(M, M')$ e $a, b \in R$, temos, para todo o $x \in M$,

(i) $((\varphi+\psi)a)(x) = (\varphi+\psi)(xa) = \varphi(xa)+\psi(xa) = (\varphi a)(x)+(\psi a)(x) = (\varphi a+\psi a)(x)$;

(ii) $(\varphi(a+b))(x) = \varphi(x(a+b)) = \varphi(xa+xb) = \varphi(xa)+\varphi(xb) = (\varphi a)(x)+(\varphi b)(x) = (\varphi a+\varphi b)(x)$;

(iii) $(\varphi(ab))(x) = \varphi(x(ab)) = \varphi(x(ba)) = \varphi((xb)a) = (\varphi a)(xb) = ((\varphi a)b)(x)$.

Portanto, $(\varphi+\psi)a = \varphi a + \psi a$, $\varphi(a+b) = \varphi a + \varphi b$ e $\varphi(ab) = (\varphi a)b$.

Vimos, então, que $\mathrm{Hom}_R(M, M')$ é um módulo$-R$.

exercício 4. Sejam R um anel, M, M', M'' módulos$-R$ à direita, $\varphi, \varphi_1, \varphi_2 \in \mathrm{Hom}_R(M, M')$ e $\psi, \psi_1, \psi_2 \in \mathrm{Hom}_R(M', M'')$. Mostre que são válidas as seguintes igualdades:

(a) $\psi \circ (\varphi_1 + \varphi_2) = (\psi \circ \varphi_1) + (\psi \circ \varphi_2)$.

(b) $(\psi_1 + \psi_2) \circ \varphi = (\psi_1 \circ \varphi) + (\psi_2 \circ \varphi)$.

(c) $\psi \circ (-\varphi) = -(\psi \circ \varphi) = (-\psi) \circ \varphi$.

(a) $\psi \circ (\varphi_1 + \varphi_2) = (\psi \circ \varphi_1) + (\psi \circ \varphi_2)$.

Seja $x \in M$. Por definição de composição de aplicações,

$$(\psi \circ (\varphi_1 + \varphi_2))(x) = \psi\left((\varphi_1 + \varphi_2)(x)\right).$$

Por outro lado, por definição de adição de aplicações, $(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x)$. Como $\varphi_1(x), \varphi_2(x) \in M'$ e ψ é um morfismo$-R$ de M' em M'', temos

$$\psi\left((\varphi_1 + \varphi_2)(x)\right) = \psi\left(\varphi_1(x) + \varphi_2(x)\right) = \psi(\varphi_1(x)) + \psi(\varphi_2(x)).$$

Novamente pela definição de composição e de adição de aplicações, concluímos que

$$\psi(\varphi_1(x)) + \psi(\varphi_2(x)) = (\psi \circ \varphi_1)(x) + (\psi \circ \varphi_2)(x) = \left((\psi \circ \varphi_1) + (\psi \circ \varphi_2)\right)(x).$$

Sendo $\psi \circ (\varphi_1 + \varphi_2)$ e $(\psi \circ \varphi_1) + (\psi \circ \varphi_2)$ morfismos$-R$ de M em M'', podemos concluir a igualdade.

(b) $(\psi_1 + \psi_2) \circ \varphi = (\psi_1 \circ \varphi) + (\psi_2 \circ \varphi)$.

As aplicações $(\psi_1 + \psi_2) \circ \varphi$ e $(\psi_1 \circ \varphi) + (\psi_2 \circ \varphi)$ são morfismos$-R$ de M em M''. Por definição de composição e adição de aplicações, para todo o $x \in M$,

$$\begin{aligned}
\left((\psi_1 + \psi_2) \circ \varphi\right)(x) &= (\psi_1 + \psi_2)\left(\varphi(x)\right) \\
&= \psi_1\left(\varphi(x)\right) + \psi_2\left(\varphi(x)\right) \\
&= (\psi_1 \circ \varphi)(x) + (\psi_2 \circ \varphi)(x) \\
&= \left((\psi_1 \circ \varphi) + (\psi_2 \circ \varphi)\right)(x)
\end{aligned}$$

Assim, $(\psi_1 + \psi_2) \circ \varphi = (\psi_1 \circ \varphi) + (\psi_2 \circ \varphi)$.

(c) $\psi \circ (-\varphi) = -(\psi \circ \varphi) = (-\psi) \circ \varphi$.

Denotemos por φ_0 o morfismo$-R$ de M em M' que aplica todo o elemento de M em $0_{M'}$ e por ψ_0 o morfismo$-R$ de M' em M'' que aplica todo o elemento de M' em $0_{M''}$. Pelas alíneas anteriores, para todo o $x \in M$,

$$\begin{aligned}
\left((\psi \circ (-\varphi)) + (\psi \circ \varphi)\right)(x) &= \left(\psi \circ (-\varphi + \varphi)\right))(x) \\
&= (\psi \circ \varphi_0)(x) \\
&= \psi(\varphi_0(x)) \\
&= \psi(0_{M'}) \\
&= 0_{M''}
\end{aligned}$$

e

$$\begin{aligned}(((-\psi)\circ\varphi)+(\psi\circ\varphi))(x) &= ((-\psi)+\psi)\circ\varphi)(x)\\ &= (\psi_0\circ\varphi)(x)\\ &= \psi_0(\varphi(x))\\ &= 0_{M''}.\end{aligned}$$

Vimos, então, que os morfismos$-R$ $(\psi\circ(-\varphi))+(\psi\circ\varphi)$ e $((-\psi)\circ\varphi)+(\psi\circ\varphi)$ transformam todo o elemento de M em $0_{M''}$, ou seja, os morfismos são iguais e são o elemento zero de $(\mathrm{Hom}_R(M', M''), +)$. Portanto, $\psi\circ(-\varphi) = (-\psi)\circ\varphi$ é simétrico de $\psi\circ\varphi$, como pretendíamos mostrar.

exercício 5. Sejam R um anel e M um módulo$-R$ à direita. Representamos por $\mathrm{End}_R(M)$ o conjunto $\mathrm{Hom}_R(M, M)$ de todos os morfismos$-R$ de M em M. Prove que

(a) $\mathrm{End}_R(M)$, algebrizado com as operações usuais de adição e de composição de aplicações entre grupos aditivos, é um anel unitário (que é subanel do anel $\mathrm{End}(M)$ de todos os endomorfismos de $(M, +)$).

(b) os automorfismos$-R$ de M são os elementos invertíveis do anel $(\mathrm{End}_R(M), +, \circ)$.

(c) o conjunto dos automorfismos$-R$ de M, algebrizado com a operação de composição de aplicações, constitui um grupo (o chamado *grupo linear do módulo* M, que se representa por $\mathrm{Aut}_R(M)$ ou $\mathrm{GL}_R(M)$).

(a) $\mathrm{End}_R(M)$, algebrizado com as operações usuais de adição e de composição de aplicações entre grupos aditivos, é um anel unitário (que é subanel do anel $\mathrm{End}(M)$ de todos os endomorfismos de $(M, +)$).

Pelo exercício 1, $(\mathrm{End}_R(M), +)$ é um grupo abeliano. Sabemos que a composição de dois morfismos$-R$ de M em M é ainda um morfismo$-R$ de M em M. Como a composição de aplicações é associativa, concluímos que $(\mathrm{End}_R(M), \circ)$ é um semigrupo. Pelo exercício 2, a composição é distributiva, à esquerda e à direita, em relação à adição. Portanto, $(\mathrm{End}_R(M), +, \circ)$ é um anel. É claro que a identidade id_M é um morfismo$-R$, pelo que $\mathrm{id}_M \in \mathrm{End}_R(M)$, e $(\mathrm{End}_R(M), +, \circ)$ é um anel unitário.

(b) os automorfismos$-R$ de M são os elementos invertíveis do anel $(\mathrm{End}_R(M), +, \circ)$.

Sabemos que os elementos invertíveis de $(\mathrm{End}_R(M), +, \circ)$ são os endomorfismos$-R$ bijetivos, ou seja, os automorfismos$-R$.

(c) o conjunto dos automorfismos$-R$ de M, algebrizado com a operação de composição de aplicações, constitui um grupo (o chamado *grupo linear do módulo* M, que se representa por $\mathrm{Aut}_R(M)$ ou $\mathrm{GL}_R(M)$).

Como a composição de dois automorfismos$-R$ de M é ainda um automorfismo$-R$ de M, a identidade definida em M é um automorfismo$-R$ de M e a aplicação inversa de um automorfismo$-R$ de M é ainda um automorfismo$-R$ de M, podemos concluir que o conjunto dos automorfismos$-R$ de M, munido da operação de composição, é um grupo.

exercício 6. Sejam R um anel, M e M' módulos$-R$ à direita, $\varphi : M \to M'$ um morfismo$-R$ e $X = \{x_i\}_{i\in I}$ um conjunto de geradores de M. Mostre que φ é um epimorfismo$-R$ se e só se $X' = \{\varphi(x_i)\}_{i\in I}$ é um conjunto de geradores de M'.

Como $\varphi : M \to M'$ é um morfismo$-R$ e $X = \{x_i\}_{i\in I}$ é um conjunto de geradores de M, temos que $\{\varphi(x_i)\}_{i\in I}$ é um conjunto de geradores de $\varphi(M)$. Logo, $\{\varphi(x_i)\}_{i\in I}$ é um conjunto de geradores de M' se e só se $\varphi(M) = M'$.

Por outro lado, sabemos que φ é um epimorfismo$-R$ se e só se $\varphi(M) = M'$. Portanto, φ é um epimorfismo$-R$ se e só se $X' = \{\varphi(x_i)\}_{i\in I}$ é um conjunto de geradores de M', como pretendíamos mostrar.

6 Produto direto e soma direta

exercício 1. Sejam R um anel, M um módulo$-R$ à direita e N_1, N_2 dois submódulos$-R$ de M tais que $N_1 \cap N_2 = \{0_M\}$. Prove que a correspondência $\theta : N_1 \oplus_{\mathrm{e}} N_2 \to N_1 + N_2$ definida por $\theta(x, y) = x + y$ é um isomorfismo$-R$.

Comecemos por verificar que θ é uma aplicação. Dado $(x_1, x_2) \in N_1 \oplus_{\mathrm{e}} N_2$, com $x_1 \in N_1$ e $x_2 \in N_2$, sabemos que $\theta(x_1, x_2) = x_1 + x_2 \in N_1 + N_2$. Mais, se $(x_1, x_2) = (y_1, y_2)$, então $x_1 = y_1$ e $x_2 = y_2$, pelo que $\theta(x_1, x_2) = x_1 + x_2 = y_1 + y_2 = \theta(y_1, y_2)$. Logo, θ é uma aplicação de $N_1 \oplus_{\mathrm{e}} N_2$ em $N_1 + N_2$.

Vejamos agora que θ é um morfismo$-R$. Para tal, tomemos $(x_1, x_2), (y_1, y_2) \in N_1 \oplus_{\mathrm{e}} N_2$ e $a \in R$. Então,

$$\begin{aligned}\theta((x_1, x_2) + (y_1, y_2)) &= \theta(x_1 + y_1, x_2 + y_2) = (x_1 + y_1) + (x_2 + y_2)\\ &= x_1 + y_1 + x_2 + y_2 = x_1 + x_2 + y_1 + y_2 = (x_1 + x_2) + (y_1 + y_2)\\ &= \theta(x_1, x_2) + \theta(y_1, y_2).\end{aligned}$$

e

$$\begin{aligned}\theta((x_1, x_2)a) &= \theta(x_1 a, x_2 a) = x_1 a + x_2 a\\ &= (x_1 + x_2)a = \theta(x_1, x_2)a.\end{aligned}$$

Concluímos, assim, que θ é um morfismo$-R$. Vamos mostrar que θ é sobrejetiva. Dado $y \in N_1 + N_2$, existem $n_1 \in N_1$, $n_2 \in N_2$ tais que $y = n_1 + n_2$. Mais, $(n_1, n_2) \in N_1 \oplus_{\mathrm{e}} N_2$ e $\theta(n_1, n_2) = n_1 + n_2 = y$.

Por último, verifiquemos que θ é injetiva. Dados $(x_1, x_2), (y_1, y_2) \in N_1 \oplus_{\mathrm{e}} N_2$ tais que $\theta(x_1, x_2) = \theta(y_1, y_2)$, temos $x_1 + x_2 = y_1 + y_2$, donde

$$x_1 - y_1 = y_2 - x_2.$$

Ora, $x_1 - y_1 \in N_1$ e $y_2 - x_2 \in N_2$. Logo, $x_1 - y_1 = y_2 - x_2 \in N_1 \cap N_2 = \{0_M\}$ e, portanto, $x_1 - y_1 = 0_M = y_2 - x_2$. Assim, $x_1 = y_1$ e $x_2 = y_2$, pelo que $(x_1, x_2) = (y_1, y_2)$.

Provamos, então, que θ é um isomorfismo$-R$.

exercício 2. Sejam R um anel e $\{M_i\}_{i \in I}$ uma família de módulos$-R$ à direita. Mostre que, para cada $j \in I$, p'_j é um epimorfismo$-R$ e ι'_j é um monomorfismo$-R$.

Seja $j \in I$. Consideremos a aplicação $p'_j : \bigoplus_{i \in I}{}_{\mathrm{e}} M_i \to M_j$ e vejamos que é um morfismo$-R$.

Dados $(x_i)_{i \in I}, (y_i)_{i \in I} \in \bigoplus_{i \in I}{}_{\mathrm{e}} M_i$ e $a \in R$, temos

$$p'_j((x_i)_{i \in I} + (y_i)_{i \in I}) = p'_j((x_i + y_i)_{i \in I}) = x_j + y_j = p'_j((x_i)_{i \in I}) + p'_j((y_i)_{i \in I})$$

e

$$p'_j((x_i)_{i\in I}a) = p'_j((x_ia)_{i\in I}) = x_ja = p'_j((x_i)_{i\in I})a.$$

Logo, p'_j é um morfismo$-R$. Para provar que p'_j é sobrejetivo, tomemos $y_j \in M_j$. Consideremos $(x_i)_{i\in I}$ tal que

$$x_i = \begin{cases} 0_{M_i}, & \text{se } i \neq j \\ y_j, & \text{se } i = j \end{cases}$$

É claro que $(x_i)_{i\in I} \in \bigoplus_{i\in I}{}_{\mathrm{e}} M_i$ e $p'_j((x_i)_{i\in I} = x_j = y_j$, pelo que p'_j é um epimorfismo$-R$.

Consideremos agora a aplicação $\iota'_j : M_j \to \bigoplus_{i\in I}{}_{\mathrm{e}} M_i$. Para cada $x_j \in M_j$, representemos $\iota'_j(x_j)$ por $(x_i)_{i\in I}$, onde, para cada $i \in I \setminus \{j\}$, $x_i = 0_{M_i}$. É claro que $\iota'_j(x_j) \in \bigoplus_{i\in I}{}_{\mathrm{e}} M_i$, uma vez que, para cada $i \in I$, $x_i \in M_i$, e os x_i são quase todos nulos.

Para provar que ι'_j é um morfismo$-R$, tomemos $x_j, y_j \in M_j$ e $a \in R$. Então, $\iota'_j(x_j) = (x_i)_{i\in I}$ e $\iota'_j(y_j) = (y_i)_{i\in I}$. Como M_j é um módulo$-R$, $z_j = x_j + y_j \in M_j$ e $w_j = x_ja \in M_j$. Assim,

$$\iota'_j(x_j + y_j) = \iota'_j(z_j) = (z_i)_{i\in I} \quad \text{e} \quad \iota'_j(x_ja) = \iota'_j(w_j) = (w_i)_{i\in I}.$$

Observemos que, para $i \in I \setminus \{j\}$, temos

$$z_i = 0_{M_i} = 0_{M_i} + 0_{M_i} = x_i + y_i \quad \text{e} \quad w_i = 0_{M_i} = 0_{M_i}a = x_ia.$$

Por outro lado,

$$z_j = x_j + y_j \quad \text{e} \quad w_j = x_ja.$$

Portanto,

$$\iota'_j(x_j + y_j) = (z_i)_{i\in I} = (x_i + y_i)_{i\in I} = (x_i)_{i\in I} + (y_i)_{i\in I} = \iota'_j(x_j) + \iota'_j(y_j)$$

e

$$\iota'_j(x_ja) = (w_i)_{i\in I} = (x_ia)_{i\in I} = (x_i)_{i\in I}a = \iota'_j(x_j)a.$$

Ou seja, ι'_j é um morfismo$-R$. Em seguida, verificamos que ι'_j é injetivo. Suponhamos, então, que $x_j, y_j \in M_j$ são tais que $\iota'_j(x_j) = \iota'_j(y_j)$. Então, $(x_i)_{i\in I} = (y_i)_{i\in I}$, pelo que $x_i = y_i$ para todo o $i \in I$. Em particular, como $j \in I$, temos $x_j = y_j$. Logo, ι'_j é um monomorfismo$-R$.

exercício 3. Considere o anel $\mathbb{Z}$ dos inteiros. Para cada $n \in \mathbb{N}$, seja $M_n = \mathbb{Z}$. Prove que

$$\bigoplus_{n\in\mathbb{N}}{}_{\mathrm{e}} M_n \subsetneq \prod_{n\in\mathbb{N}} M_n.$$

Por definição, $\bigoplus_{n\in\mathbb{N}}{}_{\mathrm{e}} M_n \subseteq \prod_{n\in\mathbb{N}} M_n$. Para cada $n \in \mathbb{N}$, seja $x_n = 1 \in \mathbb{Z} = M_n$. Então, $(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} M_n$. Uma vez que $x_n \neq 0$, para todo o $n \in \mathbb{N}$, temos que $(x_n)_{n\in\mathbb{N}} \notin \bigoplus_{n\in\mathbb{N}}{}_{\mathrm{e}} M_n$.

Logo, a inclusão é própria, isto é, $\bigoplus_{n\,\in\,\mathbb{N}}{}_{\mathrm{e}} M_n \subsetneq \prod_{n\in\mathbb{N}} M_n$.

exercício 4. Sejam R um anel comutativo, M um módulo$-R$ à direita e r um elemento de R.

(a) Mostre que a correspondência $x \to xr$ é um endomorfismo$-R$ de M.

(b) Denotando o núcleo do endomorfismo$-R$ definido em (a) por M_r, prove que

$$M/M_r \simeq Mr.$$

(c) Sejam N_1, N_2 submódulos$-R$ de M tais que $M \simeq N_1 \oplus_{\mathrm{e}} N_2$ e $N_1 \cap N_2 = \{0_M\}$. Mostre que $Mr \simeq N_1 r \oplus_{\mathrm{e}} N_2 r$, com $N_1 r \cap N_2 r = \{0_M\}$, e $M_r \simeq (N_1)_r \oplus_{\mathrm{e}} (N_2)_r$, com $(N_1)_r \cap (N_2)_r = \{0_M\}$.

(a) Mostre que a correspondência $x \to xr$ é um endomorfismo$-R$ de M.

Denotemos por λ_r a correspondência de M em M definida por $\lambda_r(x) = xr$. Por M ser um módulo$-R$, sabemos que λ_r é uma aplicação. Para ver que é um morfismo$-R$, tomemos $x, y \in M$ e $a \in R$. Então, como M é um módulo$-R$,

$$\varphi_r(x+y) = (x+y)r = xr + yr = \varphi_r(x) + \varphi_r(y).$$

Além disso, como R é comutativo,

$$\varphi_r(xa) = (xa)r = x(ar) = x(ra) = (xr)a = \varphi_r(x)a.$$

Portanto, λ_r é um endomorfismo$-R$ de M.

(b) Denotando o núcleo do endomorfismo$-R$ definido em (a) por M_r, prove que $M/M_r \simeq Mr$.

Pelo Teorema do Homomorfismo, $M/\mathrm{Ker}\lambda_r \simeq \mathrm{Im}\lambda_r$. Por definição de λ_r,

$$\mathrm{Im}\,\lambda_r = \{\lambda_r(x) : x \in M\} = \{xr : x \in M\} = Mr.$$

Portanto, $M/M_r \simeq Mr$.

(c) Sejam N_1, N_2 submódulos$-R$ de M tais que $M \simeq N_1 \oplus_{\mathrm{e}} N_2$ e $N_1 \cap N_2 = \{0_M\}$. Mostre que $Mr \simeq N_1 r \oplus_{\mathrm{e}} N_2 r$, com $N_1 r \cap N_2 r = \{0_M\}$, e $M_r \simeq (N_1)_r \oplus_{\mathrm{e}} (N_2)_r$, com $(N_1)_r \cap (N_2)_r = \{0_M\}$.

Como N_1, N_2 são módulos$-R$, temos $N_1 r \subseteq N_1$ e $N_2 r \subseteq N_2$, pelo que $N_1 r \cap N_2 r \subseteq N_1 \cap N_2 = \{0_M\}$. Como $0_M = 0_M r$, é claro que $0_M \in N_1 r \cap N_2 r$. Assim, $N_1 r \cap N_2 r = \{0_M\}$. Pela algebrização da soma direta externa, temos $(N_1 \oplus_{\mathrm{e}} N_2)r = N_1 r \oplus_{\mathrm{e}} N_2 r$.

Seja $\theta : M \to N_1 \oplus_{\mathrm{e}} N_2$ um isomorfismo$-R$. Definamos, para cada $x \in M$, $\theta_r(xr) = \theta(x)r$. Então, θ_r é uma correspondência de Mr em $N_1r \oplus_{\mathrm{e}} N_2r$. Mais, como θ é morfismo$-R$, podemos concluir que θ_r é aplicação: de facto, se $xr = yr$, então $\theta(xr) = \theta(yr)$. Mas $r \in R$, pelo que $\theta(x)r = \theta(xr) = \theta(yr) = \theta(y)r$. Logo, $\theta_r(xr) = \theta_r(yr)$.

Dados $xr, yr \in Mr$ e $a \in R$, temos

$$\begin{aligned}\theta_r(xr + yr) &= \theta_r((x + y)r) = \theta(x + y)r = (\theta(x) + \theta(y))r \\ &= \theta(x)r + \theta(y)r = \theta_r(xr) + \theta_r(yr)\end{aligned}$$

e

$$\begin{aligned}\theta_r((xr)a) &= \theta_r(x(ra)) = \theta_r(x(ar)) = \theta_r((xa)r) = \theta(xa)r \\ &= (\theta(x)a)r = \theta(x)(ar) = \theta(x)(ra) = (\theta(x)r)a = \theta_r(xr)a.\end{aligned}$$

Assim, concluímos que θ_r é um morfismo$-R$. Falta verificar que é bijetivo. Dados $xr, yr \in Mr$, se $\theta_r(xr) = \theta_r(yr)$, então $\theta(x)r = \theta(y)r$, ou seja, $\theta(xr) = \theta(yr)$. Sendo θ injetivo, temos $xr = yr$. Assim, θ_r é injetivo. Por outro lado, dado $(y_1r, y_2r) \in N_1r \oplus_{\mathrm{e}} N_2r$, com $y_1 \in N_1$ e $y_2 \in N_2$, sabemos que $(y_1, y_2) \in N_1 \oplus_{\mathrm{e}} N_2$, pelo que existe $x \in M$ tal que $\theta(x) = (y_1, y_2)$. Logo, $\theta(x)r = (y_1, y_2)r = (y_1r, y_2r)$. É claro que $xr \in Mr$. Mais, $\theta_r(xr) = \theta(x)r = (y_1r, y_2r)$. Portanto, θ_r é sobrejetivo.

Provamos, então, que θ_r é um isomorfismo$-R$ de Mr em $N_1r \oplus_{\mathrm{e}} N_2r$. De seguida, vamos mostrar que $(N_1)_r \cap (N_2)_r = \{0_M\}$. Temos

$$(N_1)_r = \{x_1 \in N_1 : x_1r = 0_M\} \text{ e } (N_2)_r = \{x_2 \in N_2 : x_2r = 0_M\}.$$

Logo, $(N_1)_r \cap (N_2)_r \subseteq N_1 \cap N_2 = \{0_M\}$. Como $0_Mr = 0_M$, é claro que $0_M \in (N_1)_r \cap (N_2)_r$, pelo que $(N_1)_r \cap (N_2)_r = \{0_M\}$.

Dado $x \in M_r$ sabemos que $xr = 0_M$. Logo, $(xr)\theta = 0_M\theta$. Sendo θ um morfismo$-R$, temos $(x\theta)r = (0_M, 0_M)$. Sejam $x_1 \in N_1$, $x_2 \in N_2$ tais que $x\theta = (x_1, x_2)$. Então, $(0_M, 0_M) = (x\theta)r = (x_1, x_2)r = (x_1r, x_2r)$, pelo que $x_1 \in (N_1)_r$ e $x_2 \in (N_2)_r$. Assim, podemos olhar para $\theta_{|_{M_r}}$ como uma aplicação de M_r em $(N_1)_r \oplus_{\mathrm{e}} (N_2)_r$. Mais, sendo θ um isomorfismo$-R$, é claro que $\theta_{|_{M_r}}$ é um morfismo$-R$ injetivo. Falta mostrar que é sobrejetivo. Tomemos $(x_1, x_2) \in (N_1)_r \oplus_{\mathrm{e}} (N_2)_r$. Então, $(x_1, x_2) \in N_1 \oplus_{\mathrm{e}} N_2$ e, portanto, existe $x \in M$ tal que $x\theta = (x_1, x_2)$. Vamos mostrar que $x \in M_r$. Ora, $(xr)\theta = (x\theta)r = (x_1, x_2)r = (x_1r, x_2r) = (0_M, 0_M) = 0_M\theta$. Como θ é injetivo, concluímos que $xr = 0_M$. Assim, $x \in M_r$ e $x\theta_{|_{M_r}} = x\theta = (x_1, x_2)$. Logo, $\theta_{|_{M_r}}$ é um isomorfismo$-R$ de M_r em $(N_1)_r \oplus_{\mathrm{e}} (N_2)_r$.

exercício 5. Sejam R um anel, $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita e $\overline{M} = \bigoplus_{i\,\in\, I}{}^{\mathrm{e}} M_i$. Mostre que

(a) o módulo$-R$ à direita $\overline{M}$ e a família de inclusões $\{\iota'_i\}_{i\in I}$ verificam a seguinte propriedade:

[P_2] Para todo o módulo$-R$ à direita F e toda a família de morfismos$-R$ $\{\varphi_i\}_{i\in I}$, com $\varphi_i : M_i \to F$ para cada $i \in I$, existe um e um só morfismo$-R$ $f : \overline{M} \to F$ tal que

$$f \circ \iota'_i = \varphi_i \quad \text{para todo o } i \in I.$$

(b) se T é um módulo$-R$ à direita e $\{\rho_i\}_{i\in I}$, com $\rho_i : M_i \to T$ para cada $i \in I$, é uma família de morfismos$-R$ que verificam a propriedade [P_2], então existe um isomorfismo $f : \overline{M} \to T$ tal que $\rho_i = f \circ \iota'_i$ para todo o $i \in I$.

(a) o módulo$-R$ à direita $\overline{M}$ e a família de inclusões $\{\iota'_i\}_{i\in I}$ verificam a propriedade [P_2].

Sejam F um módulo$-R$ à direita e $\{\varphi_i\}_{i\in I}$, com $\varphi_i : M_i \to F$ para cada $i \in I$, uma família de morfismos$-R$. Dado $(x_i)_{i\in I} \in \overline{M}$, temos que $x_i \in :_i$ para cada $i \in I$. Mais, os x_i são quase todos nulos. Sendo φ_i um morfismo de M_i em F, é claro que $\varphi_i(x_i) \in F$, para cada $i \in I$. Para além disso, se $x_i = 0_{M_i}$, então $\varphi_i(x_i) = \varphi_i(0_{M_i}) = 0_F$. Portanto, os $\varphi_i(x_i)$ são quase todos nulos. Desta forma, $\sum_{i\in I} \varphi_i(x_i)$ está definida em F.

Consideremos, então, a correspondência de $\overline{M}$ em F definida por

$$\begin{array}{rccc} f: & \overline{M} & \longrightarrow & F \\ & (x_i)_{i\in I} & \longmapsto & \displaystyle\sum_{i\in I} \varphi_i(x_i). \end{array}$$

Se $(x_i)_{i\in I} = (y_i)_{i\in I}$, é claro que $x_i = y_i$ para cada $i \in I$, pelo que $\varphi_i(x_i) = \varphi_i(y_i)$. Assim, $f((x_i)_{i\in I}) = \sum_{i\in I} \varphi_i(x_i) = \sum_{i\in I} \varphi_i(y_i) = f((y_i)_{i\in I})$. Logo, f está bem definida.

Para provarmos que f é um morfismo$-R$, tomemos $(x_i)_{i\in I}$, $(y_i)_{i\in I} \in \overline{M}$ e $a \in R$. Então, pela algebrização de $\overline{M}$ e por φ_i ser um morfismo$-R$ para cada $i \in I$, temos

$$\begin{aligned} f((x_i)_{i\in I} + (y_i)_{i\in I}) = f((x_i + y_i)_{i\in I}) &= \sum_{i\in I} \varphi_i(x_i + y_i) \\ &= \sum_{i\in I} (\varphi_i(x_i) + \varphi_i(y_i)) = \sum_{i\in I} \varphi_i(x_i) + \sum_{i\in I} (\varphi_i(y_i) \\ &= f((x_i)_{i\in I}) + f((y_i)_{i\in I}) \end{aligned}$$

e

$$f((x_i)_{i\in I}a) = f((x_i a)_{i\in I}) = \sum_{i\in I} \varphi_i(x_i a) = \sum_{i\in I} (\varphi_i(x_i))a = \left(\sum_{i\in I} \varphi_i(x_i)\right) a = f((x_i)_{i\in I})a.$$

Logo, f é um morfismo$-R$. Vamos agora provar que $f \circ \iota'_j = \varphi_j$, para cada $j \in I$.

Seja $j \in I$. À semelhança do que fizemos no exercício 2, dado $x_j \in M_j$, representemos $\iota'_j(x_j)$ por $(x_i)_{i\in I}$, onde, para cada $i \in I \setminus \{j\}$, $x_i = 0_{M_i}$. Então,

$$\begin{aligned}(f \circ \iota'_j)(x_j) = f(\iota'_j(x_j)) = f((x_i)_{i\in I}) &= \sum_{i\in I} \varphi_i(x_i) \\ &= \varphi_j(x_j) + \sum_{i\in I\setminus\{j\}} \varphi_i(0_{M_i}) = \varphi_j(x_j) + \sum_{i\in I\setminus\{j\}} 0_F \\ &= \varphi_j(x_j) + 0_F = \varphi_j(x_j).\end{aligned}$$

Portanto, $f \circ \iota'_j = \varphi_j$, para cada $j \in I$. Falta mostrar a unicidade de f. Para tal, suponhamos que existe $g : \overline{M} \to F$ tal que $g \circ \iota'_j = \varphi_j$. Para cada $(x_i)_i \in I$,

$$f((x_i)_{i\in I}) = \sum_{i\in I} \varphi_i(x_i) = \sum_{i\in I} (g \circ \iota'_i)(x_i) = \sum_{i\in I} g(\iota'_i(x_i)) = g\left(\sum_{i\in I} \iota'_i(x_i)\right) = g((x_i)_{i\in I}).$$

Portanto, $f = g$, e f é único nas condições enunciadas.

(b) se T é um módulo$-R$ à direita e $\{\rho_i\}_{i\in I}$, com $\rho_i : M_i \to T$ para cada $i \in I$, é uma família de morfismos$-R$ que verificam a propriedade [P$_2$], então existe um isomorfismo $f : \overline{M} \to T$ tal que $\rho_i = f \circ \iota'_i$ para todo o $i \in I$.

Sejam T um módulo$-R$ à direita e $\{\rho_i\}_{i\in I}$, com $\rho_i : M_i \to T$ para cada $i \in I$, uma família de morfismos$-R$ que verificam a propriedade [P$_2$]. Por [P$_2$], existe um e um só morfismo$-R$ $f : \overline{M} \to T$ tal que $f \circ \iota'_i = \rho_i$ para cada $i \in I$. De modo análogo, existe um e um só morfismo$-R$ $g : T \to \overline{M}$ tal que $g \circ \rho_i = \iota'_i$ para cada $i \in I$. Assim,

$$(g \circ f) \circ \iota'_i = g \circ (f \circ \iota'_i) = g \circ \rho_i = \iota'_i.$$

Por outro lado, $\mathrm{id}_{\overline{M}} : \overline{M} \to \overline{M}$ é tal que $\mathrm{id}_{\overline{M}} \circ \iota'_i = \iota'_i$. Por [P$_2$], $g \circ f = \mathrm{id}_{\overline{M}}$, donde concluímos que f é injetivo.

Também temos

$$(f \circ g) \circ \rho_i = f \circ (g \circ \rho_i) = f \circ \iota'_i = \rho_i = \mathrm{id}_T \circ \rho_i.$$

Logo, por [P$_2$], $f \circ g = \mathrm{id}_T$ e, portanto, f é sobrejetivo. Assim, concluímos que f é um isomorfismo$-R$.

7 Parcelas diretas

exercício 1. Sejam R um anel, M um módulo$-R$ e N, L, P submódulos$-R$ de M tais que $M = N \oplus L \oplus P$. Mostre que $(N \oplus L) \oplus P = N \oplus (L \oplus P)$.

Como $M = N \oplus L \oplus P$, sabemos que

(1) M=N+L+P;

(2) cada elemento x de M se escreve de forma única como $x = n+\ell+p$, com $n \in N$, $\ell \in L$ e $p \in P$.

Sendo a adição associativa em M, é claro que $N + (L + P) = (N + L) + P$. Vamos verificar que $(N + L) + P$ e $N + L$ são somas diretas internas.

Comecemos por tomar $x \in (N + L) + P$ e suponhamos que $x = y_1 + p_1 = y_2 + p_2$, com $y_1, y_2 \in N + L$ e $p_1, p_2 \in P$. Como $y_1, y_2 \in N + L$, existem $n_1, n_2 \in N$ e $\ell_1, \ell_2 \in L$ tais que $y_1 = n_1 + \ell_1$, $y_2 = n_2 + \ell_2$. De $x = (n_1 + \ell_1) + p_1 = (n_2 + \ell_2) + p_2$, segue que $n_1 + \ell_1 + p_1 = n_2 + \ell_2 + p_2$. Mas, $M = N \oplus L \oplus P$, pelo que $n_1 = n_2$, $\ell_1 = \ell_2$ e $p_1 = p_2$. Assim, $y_1 = y_2$ e $p_1 = p_2$. Portanto, $(N + L) + P = (N + L) \oplus P$.

Vejamos agora que $N + L = N \oplus L$. Para isso, tomemos $n_1, n_2 \in N$ e $\ell_1, \ell_2 \in L$ tais que $n_1 + \ell_1 = n_2 + \ell_2$. Como $0_M \in P$, temos $n_1 + \ell_1 + 0_M = n_2 + \ell_2 + 0_M$, com $n_1, n_2 \in N$, $\ell_1, \ell_2 \in L$ e $0_M \in P$. Porque $M = N \oplus L \oplus P$, concluímos que $n_1 = n_2$ e $\ell_1 = \ell_2$. Logo, $N + L = N \oplus L$.

Assim, $(N+L)+P = (N\oplus L)\oplus P$. De modo análogo, concluímos que $N+(L+P) = N\oplus(L\oplus P)$ e, portanto, $(N \oplus L) \oplus P = N \oplus (L \oplus P)$.

exercício 2. Sejam R um anel, M um módulo$-R$ à direita e $\psi : M \to M$ um morfismo$-R$ tal que $\psi \circ \psi = \psi$. Mostre que

$$M = \text{Ker}\psi \oplus \text{Im}\psi.$$

Como ψ um morfismo$-R$, $\text{Ker}\psi \leq_R M$ e $\text{Im}\psi \leq_R M$. Logo, $\text{Ker}\psi + \text{Im}\psi \leq_R M$. Dado $x \in M$, $(\psi \circ \psi)(x) = \psi(x)$, ou seja, $\psi(\psi(x)) = \psi(x)$. Ora,

$$\begin{aligned} \psi(x) = \psi(\psi(x)) &\Leftrightarrow \psi(x) - \psi(\psi(x)) = 0_M \\ &\Leftrightarrow \psi(x - \psi(x)) = 0_M \\ &\Leftrightarrow x - \psi(x) \in \text{Ker}\psi. \end{aligned}$$

Logo, $x = x-\psi(x)+\psi(x) = (x-\psi(x))+\psi(x)$, com $x-\psi(x) \in \text{Ker}\psi$ e $\psi(x) \in \text{Im}\psi$. Portanto, $M \subseteq \text{Ker}\psi+\text{Im}\psi$, e a igualdade segue. Vamos agora mostrar que $\text{Ker}\psi \cap \text{Im}\psi = \{0_M\}$. Dado

$y \in \mathrm{Ker}\psi \cap \mathrm{Im}\psi$, temos que $\psi(y) = 0_M$ e $y = \psi(x)$ para algum $x \in M$: Logo,

$$0_M = \psi(y) = \psi(\psi(x)) = (\psi \circ \psi)(x) = \psi(x) = y.$$

Assim, $\mathrm{Ker}\psi \cap \mathrm{Im}\psi = \{0_M\}$. Logo, $M = \mathrm{Ker}\psi \oplus \mathrm{Im}\psi$.

exercício 3. Considere o módulo$-\mathbb{Z}$ $\mathbb{Z}/10\mathbb{Z}$ e os submódulos

$$A = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}, \quad B = \{\bar{0}, \bar{5}\}.$$

Verifique se $A \oplus B = \mathbb{Z}/10\mathbb{Z}$.

Como $A \leq_{\mathbb{Z}} \mathbb{Z}/10\mathbb{Z}$ e $B \leq_{\mathbb{Z}} \mathbb{Z}/10\mathbb{Z}$, temos $A + B \leq_{\mathbb{Z}} \mathbb{Z}/10\mathbb{Z}$. Pela análise da tabela

$+$	$\bar{0}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{5}$
$\bar{2}$	$\bar{2}$	$\bar{7}$
$\bar{4}$	$\bar{4}$	$\bar{9}$
$\bar{6}$	$\bar{6}$	$\bar{1}$
$\bar{8}$	$\bar{8}$	$\bar{3}$

,

podemos verificar que $\mathbb{Z}/10\mathbb{Z} = A + B$, uma vez que, para todo o $n \in \{0, 1, \ldots, 9\}$, existem $a \in A$ e $b \in B$ tais que $\bar{n} = a + b$. É claro que $A \cap B = \{\bar{0}\}$. Portanto, $\mathbb{Z}/10\mathbb{Z} = A \oplus B$.

8 Módulos livres

exercício 1. Verifique se $\mathbb{Z}/10\mathbb{Z}$ é um módulo$-\mathbb{Z}$ livre.

Suponhamos que $\mathbb{Z}/10\mathbb{Z}$ é um módulo$-\mathbb{Z}$ livre. Então, existe um conjunto não vazio I tal que $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}^{(I)}$. Seja θ um isomorfismo$-\mathbb{Z}$ de $\mathbb{Z}/10\mathbb{Z}$ em $\mathbb{Z}^{(I)}$. Ora, $\bar{5} \in \mathbb{Z}/10\mathbb{Z}$, com $\bar{5} \neq \bar{0}$, e $2 \in \mathbb{Z} \setminus \{0\}$ são tais que $\bar{5}.2 = \overline{10} = \bar{0}$. Como θ é morfismo$-\mathbb{Z}$,

$$\theta(\bar{5})2 = \theta(\bar{5}.2) = \theta(\bar{0}) = (0)_{i\in I}.$$

Mas $2 \neq 0$, donde segue que $\theta(\bar{5}) = (0)_{i\in I}$, o que contradiz o facto de θ ser injetiva. A contradição resultou de supormos que $\mathbb{Z}/10\mathbb{Z}$ é um módulo$-\mathbb{Z}$ livre. Logo, $\mathbb{Z}/10\mathbb{Z}$ não é livre.

exercício 2. Sejam R um anel unitário e I um conjunto não vazio. Prove que $R^{(I)}$ é um módulo$-R$ livre.

Para cada $i \in I$, definamos $e_i = (y_\alpha^i)_{\alpha\in I}$, onde $y_\alpha^i = \begin{cases} 1_R & \text{se } \alpha = i \\ 0_R & \text{se } \alpha \neq i \end{cases}$ É claro que $y_\alpha^i \in R$, para todo o $\alpha \in I$, e quase todos os y_α^i são nulos. Logo, $e_i \in R^{(I)}$, para cada $i \in I$. Vejamos que $\{e_i\}_{i\in I}$ é uma base de $R^{(I)}$. Para tal, tomemos $(x_i)_{i\in I} \in R^{(I)}$. Então, $x_i \in R$, para cada $i \in I$, e quase todos os x_i são nulos. Sejam $i_1, \ldots, i_k \in I$ todos os índices $j \in I$ tais que $x_j \neq 0_R$. Então,

$$(x_i)_{i\in I} = \sum_{\ell=1}^{k} \iota'_{i_\ell}(x_{i_\ell}) = \sum_{\ell=1}^{k} \iota'_{i_\ell}(1_R)x_{i_\ell} = \sum_{\ell=1}^{k} e_{i_\ell}x_{i_\ell} = \sum_{i\in I} e_i x_i.$$

Mais, se $(x_i)_{i\in I} = \sum_{i\in I} e_i x_i = \sum_{i\in I} e_i y_i$, então $(x_i)_{i\in I} = (y_i)_{i\in I}$, donde concluímos que $x_i = y_i$ para todo o $i \in I$. Logo, $\{e_i\}_{i\in I}$ é uma base de $R^{(I)}$, e $R^{(I)}$ é um módulo$-R$ livre.

exercício 3. Seja R um anel unitário. Prove que todo o módulo$-R$ unitário é isomorfo a um módulo quociente de um módulo$-R$ livre.

Seja M um módulo$-R$ unitário. Então, sabemos que M é imagem epimorfa do módulo$-R$ livre $R^{(I)}$, para algum conjunto não vazio I. Seja $\varphi : R^{(I)} \longrightarrow M$ um epimorfismo$-R$. Pelo Teorema do Homomorfismo,

$$R^{(I)}/\mathrm{Ker}\varphi \cong \mathrm{Im}\varphi = M.$$

Assim, M é isomorfo a um módulo quociente do módulo$-R$ livre $R^{(I)}$.

9 Sequências exatas

exercício 1. Sejam R um anel e M, M' módulos$-R$ à direita. Mostre que a sequência

$$\{0\} \longrightarrow M \xrightarrow{\iota} M \oplus M' \xrightarrow{\pi} M' \longrightarrow \{0\},$$

onde ι é o mergulho canónico e π é a projeção canónica, é exata.

Como ι é um monomorfismo, $\operatorname{Ker}\iota = \{0_M\} = \operatorname{Im}\alpha$, onde $\alpha : \{0\} \longrightarrow M$ é o morfismo$-R$ definido por $0\alpha = 0_M$. Por definição de ι, para todo o $m \in M$, $\iota(m) = (m, 0_{M'})$. Logo, $\operatorname{Im}\iota = M \times \{0_{M'}\}$. Por outro lado, $\pi : M \oplus M' \longrightarrow M'$, definido por $\pi(m, m') = m'$, é um epimorfismo e $\pi(m, m') = 0_{M'}$ se e só se $m' = 0_{M'}$, ou seja, $\operatorname{Ker}\pi = M \times \{0_{M'}\} = \operatorname{Im}\iota$. Como π é um epimorfismo, $\operatorname{Im}\pi = M'$. Por outro lado, $\beta : M' \longrightarrow \{0\}$ é o morfismo$-R$ definido por $\beta(m') = 0$, para todo o $m' \in M'$. Logo, $\operatorname{Ker}\beta = M' = \operatorname{Im}\pi$. Assim, a sequência é exata.

exercício 2. Sejam R um anel e

$$\{0\} \longrightarrow A \longrightarrow B \xrightarrow{f} C \longrightarrow \{0\},$$

$$\{0\} \longrightarrow C \xrightarrow{g} D \longrightarrow E \longrightarrow \{0\}$$

sequências exatas curtas. Mostre que a sequência

$$\{0\} \longrightarrow A \longrightarrow B \xrightarrow{g\circ f} D \longrightarrow E \longrightarrow \{0\}$$

é exata.

Designemos os morfismos$-R$ representados por $\alpha : \{0\} \longrightarrow A$, $\beta : A \longrightarrow B$, $\gamma : C \longrightarrow \{0\}$, $\lambda : \{0\} \longrightarrow C$, $\mu : D \longrightarrow E$ e $\xi : E \longrightarrow \{0\}$. Por hipótese,

$$\operatorname{Im}\alpha = \{0_A\} = \operatorname{Ker}\beta, \qquad \operatorname{Im}\beta = \operatorname{Ker} f, \qquad \operatorname{Im} f = \operatorname{Ker}\gamma = C$$

e

$$\operatorname{Im}\lambda = \{0_C\} = \operatorname{Ker} g, \qquad \operatorname{Im} g = \operatorname{Ker}\mu, \qquad \operatorname{Im}\mu = \operatorname{Ker}\xi = E.$$

Logo, β e g são monomorfismos$-R$ e f e μ são epimorfismos$-R$. Consideremos a sequência

$$\{0\} \xrightarrow{\alpha} A \xrightarrow{\beta} B \xrightarrow{g\circ f} D \xrightarrow{\mu} E \xrightarrow{\xi} \{0\}$$

Sabemos que $\operatorname{Im}\alpha = \operatorname{Ker}\beta$ e $\operatorname{Im}\mu = \operatorname{Ker}\xi$. Vamos verificar que $\operatorname{Im}\beta = \operatorname{Ker}(g \circ f)$ e $\operatorname{Im}(g \circ f) = \operatorname{Ker}\mu$. Dado $b \in B$,

$$b \in \operatorname{Ker}(g \circ f) \Leftrightarrow (g \circ f)(b) = 0_D \Leftrightarrow g(f(b)) = 0_D \Leftrightarrow$$
$$\Leftrightarrow f(b) \in \operatorname{Ker} g \Leftrightarrow f(b) = 0_C \Leftrightarrow b \in \operatorname{Ker} f.$$

Logo, $\mathrm{Ker}(g \circ f) = \mathrm{Ker}\, f = \mathrm{Im}\, \beta$. Por outro lado, dado $d \in D$,

$$d \in \mathrm{Im}(g \circ f) \Leftrightarrow \text{ existe } b \in B \text{ tal que } d = (g \circ f)(b) \Leftrightarrow$$
$$\Leftrightarrow \text{existe } b \in B \text{ tal que } d = g(f(b)) \implies d \in \mathrm{Im}\, g = \mathrm{Ker}\, \mu.$$

Se $d \in \mathrm{Ker}\, \mu = \mathrm{Im}\, g$, então existe $c \in C$ tal que $d = g(c)$. Mas $C = \mathrm{Im}\, f$ e, portanto, existe $b \in B$ tal que $c = f(b)$. Assim,

$$d = g(c) = g(f(b)) = (g \circ f)(b) \in \mathrm{Im}(g \circ f).$$

Logo, $\mathrm{Im}(g \circ f) = \mathrm{Ker}\mu$, e podemos concluir que a sequência é exata.

exercício 3. Seja $\mathscr{S}$ a sequência exata $\{0\} \longrightarrow N \xrightarrow{f} M \xrightarrow{g} W \longrightarrow \{0\}$, com N, M e W módulos$-R$ e f e g morfismos$-R$. Então, são equivalentes as seguintes condições:

(a) $\mathscr{S}$ é uma sequência cindível.

(b) $\mathrm{Im}(f) = \mathrm{Ker}(g)$ é parcela direta de M.

(c) f é monomorfismo cindível.

(d) g é epimorfismo cindível.

sugestão. Prove $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$ e $(b) \Rightarrow (d) \Rightarrow (a)$.

Designemos os morfismos$-R$ representados por $\alpha : \{0\} \longrightarrow N$ e $\beta : W \longrightarrow \{0\}$. Suponhamos que $\mathscr{S}$ é cindível. Então, por definição, $\{0_N\} = \mathrm{Im}\, \alpha = \mathrm{Ker}\, f$ é parcela direta de N, $\mathrm{Im}\, f = \mathrm{Ker}\, g$ é parcela direta de M e $\mathrm{Im}\, g = \mathrm{Ker}\, \beta = W$ é parcela direta de W. Logo, $\mathrm{Im}\, f$=Ker g é parcela direta de M.

Suponhamos agora que $\mathrm{Im}\, f$=Ker g é parcela direta de M. Por hipótese, a sequência $\mathscr{S}$ é exata, pelo que $\{0_N\} = \mathrm{Im}\, \alpha = \mathrm{Ker}\, f$. Portanto, f é um monomorfismo$-R$. Logo, f é um monomorfismo$-R$ tal que $\mathrm{Im}\, f$ é parcela direta de M, ou seja, f é um monomorfismo$-R$ cindível.

Admitamos que f é monomorfismo$-R$ cindível. Então, f é um monomorfismo$-R$ e $\mathrm{Im}\, f$ é parcela direta de M. Sendo a sequência exata, temos $\mathrm{Im}\, \alpha = \mathrm{Ker}\, f$, $\mathrm{Im}\, f = \mathrm{Ker}\, g$ e $\mathrm{Im}\, g = \mathrm{Ker}\, \beta$. Como $N = \{0_N\} \oplus N$ e $W = W \oplus \{0_W\}$, temos que $\{0_N\} = \mathrm{Im}\, \alpha$ é parcela direta de N e $\mathrm{Ker}\, \beta = \mathrm{Im}\, g = W$ é parcela direta de W. Assim, a sequência é cindível.

Suponhamos agora que $\mathrm{Im}\, f$=Ker g é parcela direta de M. Como a sequência $\mathscr{S}$ é exata, sabemos que $\mathrm{Im}\, g = \mathrm{Ker}\, \beta = W$. Logo, g é um epimorfismo$-R$. Mais, g é um epimorfismo$-R$ tal que $\mathrm{Ker}\, g$ é parcela direta de M, ou seja, g é um epimorfismo$-R$ cindível.

Admitamos, por fim, que g é epimorfismo$-R$ cindível. Então, g é um epimorfismo$-R$ e $\mathrm{Ker}\, g$ é parcela direta de M. Como a sequência $\mathscr{S}$ é exata, temos $\{0_N\} = \mathrm{Im}\, \alpha = \mathrm{Ker}\, f$, $\mathrm{Im}\, f = \mathrm{Ker}\, g$ e $\mathrm{Im}\, g = \mathrm{Ker}\, \beta = W$. Logo, $\mathrm{Im}\, \alpha$ é parcela direta de N (pois $N = \{0_N\} \oplus N$)

e $\operatorname{Ker}\beta = \operatorname{Im} g = W$ é parcela direta de W (pois $W = W \oplus \{0_W\}$). Assim, a sequência é cindível.

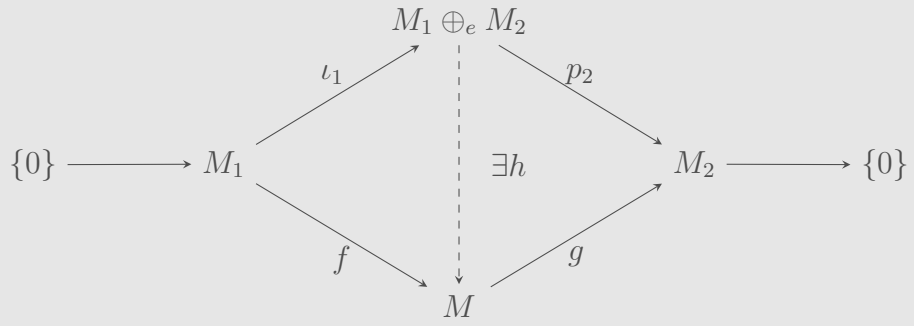
exercício 4. Sejam R um anel, M, M_1, M_2 módulos-R à direita e $\mathcal{S}$ a sequência exata curta

$$\{0\} \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow \{0\}.$$

Mostre que são equivalentes as afirmações

(i) $\mathcal{S}$ é cindível.

(ii) Existe um isomorfismo $h : M_1 \oplus_e M_2 \to M$ para o qual o diagrama



comuta, ou seja, $h \circ \iota_1 = f$ e $g \circ h = p_2$.

Como $\mathscr{S}$ é uma sequência exata, f é um monomorfismo$-R$, g é um epimorfismo$-R$ e $\operatorname{Im} f = \operatorname{Ker} g$. Suponhamos que $\mathscr{S}$ é cindível. Então, g é um epimorfismo$-R$ cindível, pelo que existe um morfismo$-R$ $g' : M_2 \longrightarrow M$ tal que $g \circ g' = \mathrm{id}_{M_2}$. Consideremos a correspondência

$$\begin{array}{rccc} h: & M_1 \oplus_e M_2 & \longrightarrow & M \\ & (m_1, m_2) & \mapsto & f(m_1) + g'(m_2). \end{array}$$

Dados $m_1 \in M_1$ e $m_2 \in M_2$, temos $f(m_1) \in M$ e $g'(m_2) \in M$. Logo, $f(m_1) + g'(m_2) \in M$. Como f e g' são aplicações, h é também aplicação. Para verificarmos que h é morfismo$-R$, tomemos $(m_1, m_2), (m_1', m_2') \in M_1 \oplus_e M_2$ e $a \in R$. Então, como f e g' são morfismos$-R$,

$$\begin{aligned} h((m_1, m_2) + (m_1', m_2')) &= h((m_1 + m_1', m_2 + m_2')) = f(m_1 + m_1') + g'(m_2 + m_2') \\ &= (f(m_1) + f(m_1')) + (g'(m_2) + g'(m_2')) \\ &= (f(m_1) + g'(m_2)) + (f(m_1') + g'(m_2')) \\ &= h((m_1, m_2)) + h((m_1', m_2')) \end{aligned}$$

e

$$\begin{aligned} h((m_1, m_2)a) &= h((m_1 a, m_2 a)) = f(m_1 a) + g'(m_2 a) \\ &= f(m_1)a + g'(m_2)a = (f(m_1) + g'(m_2))a \\ &= h((m_1, m_2))a. \end{aligned}$$

Assim, h é morfismo$-R$. Vejamos que h é injetivo. Sejam $(m_1, m_2), (m_1', m_2') \in M_1 \oplus_e M_2$ tais que $h((m_1, m_2)) = h(m_1', m_2'))$. Então, $f(m_1) + g'(m_2) = f(m_1') + g'(m_2')$. Como g é aplicação, $g(f(m_1) + g'(m_2)) = g(f(m_1') + g'(m_2'))$. Mais, g é morfismo$-R$, pelo que

$$g(f(m_1)) + g(g'(m_2)) = g(f(m_1')) + g(g'(m_2')).$$

Sabemos que $\operatorname{Im} f = \operatorname{Ker} g$ e $g \circ g' = \mathrm{id}_{M_2}$. Assim, $0_{M_2} + m_2 = 0_{M_2} + m_2'$, ou seja, $m_2 = m_2'$. Logo, de $f(m_1) + g'(m_2) = f(m_1') + g'(m_2')$, concluímos que $f(m_1) = f(m_1')$. Mas f é injetiva, donde segue que $m_1 = m_1'$. Assim, $(m_1, m_2) = (m_1', m_2')$, e h é injetiva.

De seguida, mostramos que h é sobrejetivo. Seja $x \in M$. Tomemos $x' = x - g'(g(x))$. Então,

$$g(x') = g(x) - g(g'(g(x))) = g(x) - (g \circ g')(g(x)) = g(x) - g(x) = 0_{M_2'},$$

pelo que $x' \in \operatorname{Ker} g = \operatorname{Im} f$. Assim, existe $m_1 \in M_1$ tal que $f(m_1) = x'$. Temos $(m_1, g(x)) \in M_1 \oplus_e M_2$ e

$$h((m_1, g(x))) = f(m_1) + g'(g(x)) = x' + g'(g(x)) = x - g'(g(x)) + g'(g(x)) = x.$$

Logo, h é sobrejetivo.

Resta-nos mostrar que $h \circ \iota_1 = f$ e $g \circ h = p_2$. Para todo o $m_1 \in M_1$,

$$(h \circ \iota_1)(m_1) = h(\iota_1(m_1)) = h((m_1, 0_{M_2})) = f(m_1) + g'(0_{M_2}) = f(m_1) + 0_M = f(m_1),$$

pelo que $h \circ \iota_1 = f$. Por outro lado, dado $(m_1, m_2) \in M_1 \oplus_e M_2$,

$$\begin{aligned}(g \circ h)(m_1, m_2) &= g(h((m_1, m_2))) = g(f(m_1) + g'(m_2)) \\ &= g(f(m_1)) + g(g'(m_2)) = 0_M + m_2 = m_2 \\ &= p_2((m_1, m_2))\end{aligned}$$

e, portanto, $g \circ h = p_2$.

Reciprocamente, suponhamos que existe um isomorfismo$-R$ $h : M_1 \oplus_e M_2 \longrightarrow M$ nas condições do enunciado. Então, $M \cong M_1 \oplus_e M_2 \cong M_1 \oplus M_2$ e, portanto, a sequência $\mathscr{S}$ é cindível.

10 Comprimento de um módulo

exercício 1. Considere o módulo$-\mathbb{Z}$ $\mathbb{Z}_{12}$.

(a) Determine todos os submódulos$-\mathbb{Z}$ de $\mathbb{Z}_{12}$.

(b) Verifique que

$$\mathscr{B}: \ \{0\} \subseteq 2\mathbb{Z}_{12} \subseteq \mathbb{Z}_{12}$$

e

$$\mathscr{C}: \ \{0\} \subseteq 3\mathbb{Z}_{12} \subseteq \mathbb{Z}_{12}.$$

são cadeias normais de M.

(c) Construa refinamentos $\mathscr{B}^*$ e $\mathscr{C}^*$ das cadeias $\mathscr{B}$ e $\mathscr{C}$ que sejam séries de composição.

(d) Verifique que os fatores de $\mathscr{B}^*$ e $\mathscr{C}^*$ são isomorfos dois a dois (a menos de ordem).

(a) Determine todos os submódulos$-\mathbb{Z}$ de $\mathbb{Z}_{12}$.

Os submódulos$-\mathbb{Z}$ de $\mathbb{Z}_{12}$ são exatamente os subgrupos (aditivos) de $\mathbb{Z}_{12}$. Ora, os divisores de 12 são 1, 2, 3, 4, 6 e 12. Por isso, os submódulos$-\mathbb{Z}$ de $\mathbb{Z}_{12}$ são: $12\mathbb{Z}_{12} = \{\bar{0}\}$, $6\mathbb{Z}_{12} = \{\bar{0}, \bar{6}\}$, $4\mathbb{Z}_{12} = \{\bar{0}, \bar{4}, \bar{8}\}$, $3\mathbb{Z}_{12} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, $2\mathbb{Z}_{12} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$ e $\mathbb{Z}_{12}$.

(b) Verifique que

$$\mathscr{B}: \ \{0\} \subseteq 2\mathbb{Z}_{12} \subseteq \mathbb{Z}_{12}$$

e

$$\mathscr{C}: \ \{0\} \subseteq 3\mathbb{Z}_{12} \subseteq \mathbb{Z}_{12}.$$

são cadeias normais de $\mathbb{Z}_{12}$.

Sabemos que $\{\bar{0}\}$ é submódulo$-\mathbb{Z}$ de $2\mathbb{Z}_{12}$ e que $2\mathbb{Z}_{12}$ é submódulo$-\mathbb{Z}$ de $\mathbb{Z}_{12}$. Logo, $\mathscr{B}$ é uma cadeia normal de $\mathbb{Z}_{12}$.

De modo análogo, como $\{\bar{0}\}$ é submódulo$-\mathbb{Z}$ de $3\mathbb{Z}_{12}$ e $3\mathbb{Z}_{12}$ é submódulo$-\mathbb{Z}$ de $\mathbb{Z}_{12}$, temos que $\mathscr{C}$ é uma cadeia normal de $\mathbb{Z}_{12}$.

(c) Construa refinamentos $\mathscr{B}^*$ e $\mathscr{C}^*$ das cadeias $\mathscr{B}$ e $\mathscr{C}$ que sejam séries de composição.

Consideremos a cadeia $\mathscr{B}^*: \ \{\bar{0}\} \subseteq 6\mathbb{Z}_{12} \subseteq 2\mathbb{Z}_{12} \subseteq \mathbb{Z}_{12}$. É claro que $\mathscr{B}^*$ é um refinamento de $\mathscr{B}$. Como $6\mathbb{Z}_{12}/\{\bar{0}\} \cong \mathbb{Z}_2$, $2\mathbb{Z}_{12}/6\mathbb{Z}_{12} \cong \mathbb{Z}_3$, $\mathbb{Z}_{12}/2\mathbb{Z}_{12} \cong \mathbb{Z}_2$ e $\mathbb{Z}_2$, $\mathbb{Z}_3$ são módulos simples, concluímos que $\mathscr{B}^*$ é uma série de composição.

De modo análogo, consideremos a cadeia $\mathscr{C}^*: \ \{\bar{0}\} \subseteq 6\mathbb{Z}_{12} \subseteq 3\mathbb{Z}_{12} \subseteq \mathbb{Z}_{12}$. Por definição, $\mathscr{C}^*$ é um refinamento de $\mathscr{C}$. Como $6\mathbb{Z}_{12}/\{\bar{0}\} \cong \mathbb{Z}_2$, $3\mathbb{Z}_{12}/6\mathbb{Z}_{12} \cong \mathbb{Z}_2$, $\mathbb{Z}_{12}/3\mathbb{Z}_{12} \cong \mathbb{Z}_3$ e $\mathbb{Z}_2$, $\mathbb{Z}_3$ são módulos simples, segue que $\mathscr{C}^*$ é uma série de composição.

(d) Verifique que os fatores de $\mathscr{B}^*$ e $\mathscr{C}^*$ são isomorfos dois a dois (a menos de ordem).

Como referimos na alínea anterior,

$$6\mathbb{Z}_{12}/\{\bar{0}\} \cong \mathbb{Z}_2 \cong 6\mathbb{Z}_{12}/\{\bar{0}\},$$

$$2\mathbb{Z}_{12}/\mathbb{Z}_{12} \cong \mathbb{Z}_2 \cong 3\mathbb{Z}_{12}/6\mathbb{Z}_{12},$$

$$2\mathbb{Z}_{12}/6\mathbb{Z}_{12} \cong \mathbb{Z}_3 \cong \mathbb{Z}_{12}/3\mathbb{Z}_{12}.$$

Logo, os fatores de $\mathscr{B}^*$ e $\mathscr{C}^*$ são isomorfos dois a dois

exercício 2. Sejam R um anel e M um módulo$-R$ não nulo de comprimento finito. Sejam

$$\mathscr{B}: \quad \{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = M$$

uma série de composição de M e

$$\mathscr{C}: \quad \{0\} = P_0 \subseteq P_1 \subseteq \cdots \subseteq P_t = M$$

uma cadeia normal de M isomorfa a $\mathscr{B}$. Prove que $\mathscr{C}$ é uma série de composição de M.

Como $\mathscr{B}$ e $\mathscr{C}$ são cadeias isomorfas, existe uma bijeção

$$\delta : \{1, \ldots, t\} \longrightarrow \{1, \ldots, k\}$$

tal que

$$P_i/P_{i-1} \cong N_{\delta(i)}/N_{\delta(i)-1},$$

para todo o $i \in \{1, \ldots, t\}$.

Como $\mathscr{B}$ é uma série de composição, todos os fatores N_j/N_{j-1} são módulos simples. Logo, para cada $i \in \{1, \ldots, t\}$, o quociente P_i/P_{i-1} é simples, por ser isomorfo ao módulo simples $N_{\delta(i)}/N_{\delta(i)-1}$. Assim, todos os fatores da cadeia $\mathscr{C}$ são simples. Portanto, $\mathscr{C}$ é uma série de composição de M.

exercício 3. Sejam R um anel e M, M' módulos$-R$ tais que M é um módulo$-R$ de comprimento finito. Mostre que, se M' é isomorfo a M, então M' é de comprimento finito e $\mathscr{L}(M') = \mathscr{L}(M)$.

Se $M = \{0_M\}$, então $M' = \{0_{M'}\}$, uma vez que $M' \cong M$. Logo, M' é de comprimento finito e

$$\mathscr{L}(M') = 0 = \mathscr{L}(M).$$

Suponhamos agora que $M \neq \{0_M\}$. Como M tem comprimento finito, M admite uma série de composição, digamos

$$\mathscr{B}: \quad \{0_M\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = M.$$

Seja $\varphi : M \longrightarrow M'$ um isomorfismo. Consideremos a cadeia

$$\mathscr{C} : \quad \{0_{M'}\} = \varphi(N_0) \subsetneq \varphi(N_1) \subsetneq \cdots \subsetneq \varphi(N_k) = M'.$$

Pelo 1.º Teorema do Isomorfismo, para cada $i \in \{1, \ldots, k\}$,

$$\varphi(N_i)/\varphi(N_{i-1}) \cong N_i/N_{i-1}.$$

Como N_i/N_{i-1} é simples, concluímos que $\varphi(N_i)/\varphi(N_{i-1})$ também é simples. Logo, $\mathscr{C}$ é uma série de composição de M'. Portanto, M' tem comprimento finito e

$$\mathscr{L}(M') = k = \mathscr{L}(M).$$

exercício 4. Seja M um módulo-R de comprimento finito e $\varphi : M \to M$ um endomorfismo$-R$ injetivo. Prove que φ é sobrejetivo.

sugestão:

(a) Justifique que a sequência

$$0 \longrightarrow M \xrightarrow{\varphi} M \longrightarrow M/\mathrm{Im}(\varphi) \longrightarrow 0.$$

é exata.

(b) Mostre que $\mathscr{L}(M) = \mathscr{L}(\mathrm{Im}(\varphi)) + \mathscr{L}(M/\mathrm{Im}(\varphi))$.

(c) Indique a relação entre $\mathscr{L}(\mathrm{Im}(\varphi))$ e $\mathscr{L}(M)$.

(d) Prove que $M/\mathrm{Im}(\varphi) = \{0\}$ e conclua que φ é sobrejetivo.

(a) Justifique que a sequência

$$0 \longrightarrow M \xrightarrow{\varphi} M \longrightarrow M/\mathrm{Im}(\varphi) \longrightarrow 0.$$

é exata.

Sabemos que φ é um monomorfismo$-R$ e que $\pi : M \to M/\mathrm{Im}(\varphi)$ é um epimorfismo$-R$. Mais, $\mathrm{Im}(\varphi) = \mathrm{Ker}(\pi)$. Assim, a sequência é uma sequência exata curta.

(b) Mostre que $\mathscr{L}(M) = \mathscr{L}(\mathrm{Im}(\varphi)) + \mathscr{L}(M/\mathrm{Im}(\varphi))$.

Como $\mathrm{Im}(\varphi)$ é um submódulo$-R$ de M e M é um módulo$-R$ de comprimento finito, temos que

$$\mathscr{L}(M) = \mathscr{L}(\mathrm{Im}(\varphi)) + \mathscr{L}(M/\mathrm{Im}(\varphi)).$$

(c) Indique a relação entre $\mathscr{L}(\mathrm{Im}(\varphi))$ e $\mathscr{L}(M)$.

Sendo φ injetivo, sabemos que $M \cong \mathrm{Im}(\varphi)$. Pelo exercício 3, $\mathrm{Im}(\varphi)$ é de comprimento finito e $\mathscr{L}(\mathrm{Im}(\varphi)) = \mathscr{L}(M)$.

(d) Prove que $M/\mathrm{Im}(\varphi) = \{0\}$ e conclua que φ é sobrejetivo.

Vimos que $\mathscr{L}(M) = \mathscr{L}(\mathrm{Im}(\varphi)) + \mathscr{L}(M/\mathrm{Im}(\varphi))$. Uma vez que $\mathscr{L}(\mathrm{Im}(\varphi)) = \mathscr{L}(M)$, concluímos que $\mathscr{L}(M/\mathrm{Im}(\varphi)) = 0$. Logo, $M/\mathrm{Im}(\varphi) = \{\mathrm{Im}(\varphi)\}$, pelo que $\mathrm{Im}(\varphi) = M$. Assim, φ é sobrejetivo.

exercício 5. Sejam R um anel e M um módulo$-R$ de comprimento finito. Sejam N e P submódulos$-R$ de M tais que $N \subseteq P$ e $\mathscr{L}(N) = \mathscr{L}(P)$. Prove que $N = P$.

Suponhamos que $N \subsetneq P$. Se $N = \{0_M\}$, então

$$\{0_M\} \subsetneq P$$

é uma cadeia de submódulos de P e, pelo Teorema de Jordan–Hölder, esta cadeia admite um refinamento que é uma série de composição. Logo, $\mathscr{L}(P) > 0$. Por outro lado, $\mathscr{L}(N) = \mathscr{L}(\{0_M\}) = 0$, o que contradiz a hipótese.

Se $N \neq \{0_M\}$, então a cadeia $\{0_M\} \subsetneq N \subsetneq P$ admite um refinamento que é uma série de composição de P, digamos

$$\{0_M\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = N \subsetneq N_{k+1} \subsetneq \cdots \subsetneq N_{k+r} = P,$$

com $r \geq 1$. Assim, a cadeia

$$\{0_M\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = N$$

é uma série de composição de N e

$$\mathscr{L}(N) = k < k + r = \mathscr{L}(P),$$

o que também contradiz a hipótese.

As contradições resultaram de supormos que $N \subsetneq P$. Desta forma, podemos concluir que $N = P$.