notas para a unidade curricular de

Módulos e Anéis

Mestrado em Matemática

Universidade do Minho 2016/2017

1. Módulos

1.1. Módulos, submódulos e homomorfismos

Definição. Seja R um anel. Dá-se o nome de *módulo à direita sobre* R (ou *mod*$-R$ *à direita*) a um sistema algébrico formado por um conjunto M, uma operação binária $+$ (adição) e uma família de operações unárias $(\lambda_a)_{a\in R}$, $\lambda_a : M \to M$, $x \mapsto \lambda_a(x) = xa$, que verificam as seguintes propriedades:

i. $(M, +)$ é um grupo abeliano;

ii. $(x + y)a = xa + ya$, para quaisquer $a \in R$ e $x, y \in M$;

iii. $x(a + b) = xa + xb$, para quaisquer $a, b \in R$ e $x \in M$;

iv. $x(ab) = (xa)b$, para quaisquer $a, b \in R$ e $x \in M$.

Definição. Se R é um anel unitário e M é um mod$-R$ à direita, dizemos que M é *unitário* se $x1_R = x$, para todo o $x \in M$.

Proposição. Sejam R um anel e M um mod$-R$ à direita. Então, para quaisquer $n, r \in \mathbb{N}$, $a, b, a_1, \ldots, a_r \in R$ e $x, y, x_1, \ldots, x_r \in M$:

(a) $x0_R = 0_M$;

(b) $0_M a = 0_M$;

(c) $x(-a) = -(xa) = (-x)a$;

(d) $x(a - b) = xa - xb$;

(e) $(x - y)a = xa - ya$;

(f) $n(xa) = x(na) = (nx)a$;

(g) $(\sum_{i=1}^{r} x_i)a = \sum_{i=1}^{r}(x_i a)$;

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

Demonstração. [exercício]

Definição. Sejam R um anel e M um mod$-R$ à direita. Define-se o *anulador* de M como sendo o conjunto $\mathrm{an}(M) = \{a \in R : Ma = 0_M\} = \{a \in R : xa = 0_M, \forall x \in M\}$.

Proposição. Sejam R um anel e M um mod$-R$ à direita. Então, $\mathrm{an}(M)$ é um ideal de R.

Demonstração. Como $0_R \in \text{an}(M)$, temos que $\text{an}(M) \neq \emptyset$.
Sejam $a, b \in \text{an}(M)$. Então, $a, b \in R$ e $xa = xb = 0_M$, para todo o $x \in M$. Sendo R um anel, $a - b \in R$. Dado $x \in M$,

$$x(a-b) = xa - xb = 0_M - 0_M = 0_M,$$

pelo que $a - b \in \text{an}(M)$.
Se $a \in \text{an}(M)$ e $r \in R$, então $a, r \in R$ e $xa = 0_M$ para todo o $x \in M$. Logo, $ar, ra \in R$ e, dado $x \in M$,

$$x(ar) = (xa)r = 0_M r = 0_M.$$

Além disso, $xr \in M$ e, uma vez que $a \in \text{an}(M)$,

$$x(ra) = (xr)a = 0_M.$$

Assim, $ar, ra \in \text{an}(M)$. Logo, $\text{an}(M)$ é um ideal de R. □

Definição. Sejam R um anel e M um mod$-R$ à direita. Dizemos que M é um *módulo$-R$ fiel* se $\text{an}(M) = \{0_R\}$.

Exemplos.

1. Todo o espaço vetorial V não nulo sobre um corpo K é um módulo-K à direita fiel unitário.
2. Sejam R um anel e $n \in \mathbb{N}$. Então, R^n é um módulo$-R$ à direita. Se R for um anel unitário, então R^n é um módulo$-R$ à direita fiel unitário.
3. Se R é um anel unitário, então $R[x]$ é um módulo$-R$ à direita fiel unitário.

Definição. Sejam R um anel e M um módulo$-R$ à direita. Sejam X e Y subconjuntos não vazios de M e B um subconjunto não vazio de R. Definimos os conjuntos $X + Y$ e XB do seguinte modo:

$$X + Y = \{x + y : x \in X \wedge y \in Y\}, \qquad XB = \left\{ \sum_{i=1}^{n} x_i b_i : n \in \mathbb{N} \wedge x_i \in X \wedge b_i \in B \right\}.$$

Proposição. Sejam R um anel, M um módulo$-R$ à direita, X, Y subconjuntos não vazios de M, B, C subconjuntos não vazios de R. Então.

(a) se $X \subseteq Y$, então $XB \subseteq YB$;

(b) se $B \subseteq C$, então $XB \subseteq XC$;

(c) $X(B + C) \subseteq XB + XC$. Mais, a igualdade verifica-se se $0_R \in B \cap C$;

(d) $X(BC) = (XB)C$;

(e) $(X+Y)B \subseteq XB+YB$. Mais, a igualdade verifica-se se $0_M \in X \cap Y$.

Demonstração. [exercício]

Definição. Sejam R um anel e M um módulo$-R$ à direita. Dizemos que N é um *submódulo*$-R$ *de* M se N for um subsistema algébrico que é módulo$-R$ à direita e escrevemos $N \leq_R M$.

Proposição. Sejam R um anel e M um módulo$-R$ à direita. Uma parte não vazia N de M é submódulo$-R$ de M se e só se para quaisquer $x, y \in N$ e qualquer $a \in R$ se tiver $x-y \in N$ e $xa \in N$.

Demonstração. [exercício]

Proposição. Sejam R um anel unitário, M um módulo$-R$ à direita unitário e N uma parte não vazia de M. Então, são equivalentes as seguintes condições.

(a) N é submódulo$-R$ de M.

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

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

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

Demonstração. [exercício]

Proposição. Sejam R um anel unitário, M um módulo$-R$ à direita unitário e N um submódulo$-R$ de M. Então, N é módulo$-R$ unitário.

Demonstração. Como N é submódulo$-R$ de M, sabemos que $N \subseteq M$ e N é módulo$-R$ à direita.
Dado $x \in N$, temos que $x \in M$ e, uma vez que M é unitário,

$$x1_R = x.$$

Logo, para todo o $x \in N$, $x1_R = x$, pelo que N é unitário. □

Exemplos.

1. Seja R um anel. Se M é um módulo$-R$ à direita, então $\{0\}$ e M são submódulos$-R$ de M. O submódulo$-R$ $\{0\}$ diz-se o *submódulo nulo* e o submódulo$-R$ M diz-se o *submódulo impróprio*.

2. Dado um anel R, o próprio R é um módulo$-R$ à direita, que representamos por R_R. Os submódulos$-R$ de R_R são exatamente os ideais direitos de R.

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

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

G é um módulo-$\mathbb{Z}$ à direita. Os submódulos-$\mathbb{Z}$ de G são exatamente os subgrupos de G.

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

Proposição. Sejam R um anel comutativo, M um módulo$-R$ à direita e $a \in R$. Então, $Ma \leq_R M$.

Demonstração. [exercício]

Definição. Sejam R um anel e M um módulo$-R$ à direita. Dizemos que M é um *módulo$-R$ simples* se existirem precisamente dois submódulos$-R$ de M.

Exemplo. Seja R um anel de divisão. Então, os únicos ideais direitos de R são $\{0\}$ e R, pelo que os submódulos$-R$ de R_R são exatamente $\{0\}$ e R. Portanto, R_R é um módulo$-R$ simples.

Definição. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M. Dizemos que N é um *submódulo maximal de M* se N for elemento maximal da família dos submódulos próprios de M, ou seja, se $N \leq_R M$, $N \subsetneq M$ e, para todo o $P \leq_R M$, se $N \subseteq P \subseteq M$, então $P = N$ ou $P = M$.

Proposição. Sejam R um anel, M um módulo$-R$ à direita e N, L submódulos$-R$ de M. Então,

(a) $N + L$ é um submódulo$-R$ de M;

(b) $N \cap L$ é um submódulo$-R$ de M;

(c) $N \cup L$ é um submódulo$-R$ de M se e só se $N \subseteq L$ ou $L \subseteq N$.

Demonstração. [exercício]

Definição. Sejam R um anel, M um módulo$-R$ à direita, I um conjunto não vazio e $\{N_i\}_{i \in I}$ uma família de submódulos$-R$ de M. Definimos a soma da família $\{N_i\}_{i \in I}$ de submódulos$-R$ de M como sendo o conjunto

$$\sum_{i \in I} N_i = \left\{ \sum_{i \in I} x_i : \quad x_i \in N_i, \quad x_i \text{ quase todos nulos} \right\}.$$

Proposição. Sejam R um anel, M um módulo$-R$ à direita e I um conjunto não vazio e $\{N_i\}_{i\in I}$ uma família de submódulos$-R$ de M. Então,

(a) $\sum_{i\in I} N_i$ é um submódulo$-R$ de M;

(b) $\bigcap_{i\in I} N_i$ é um submódulo$-R$ de M;

(c) se, para quaisquer $i, j \in I$, existe $k \in I$ tal que $N_i \cup N_j \subseteq N_k$, então $\bigcup_{i\in I} N_i$ é um submódulo$-R$ de M.

Demonstração. [exercício]

Sejam R um anel, M um módulo$-R$ à direita e X um subconjunto de M. Consideremos o conjunto $\mathcal{B}$ de todos os submódulos$-R$ de M que contêm X, isto é,

$$\mathcal{B} = \{N \leq_R M : X \subseteq N\}.$$

É claro que $\mathcal{B} \neq \emptyset$. De facto, $M \in \mathcal{B}$. Se considerarmos $\bigcap_{N\in\mathcal{B}} N$, podemos concluir que

$$\bigcap_{N\in\mathcal{B}} N \leq_R M \quad \text{e} \quad X \subseteq \bigcap_{N\in\mathcal{B}} N.$$

Aém disso, para todo o $N' \in \mathcal{B}$,

$$\bigcap_{N\in\mathcal{B}} N \subseteq N'.$$

Definição. Sejam R um anel, M um módulo$-R$ à direita e X um subconjunto de M. Então, a interseção de todos os submódulos$-R$ de M que contêm X diz-se o *submódulo de M gerado por X*, e representa-se por $\langle X\rangle$. Se $X = \{x\}$ para algum $x \in M$, escrevemos $\langle x\rangle$ em vez de $\langle\{x\}\rangle$.

Proposição. Sejam R um anel, M um módulo$-R$ à direita e X um subconjunto de M. Então, P é o submódulo$-R$ gerado por X se e só se se verificam as seguintes condições:

(i) $P \leq_R M$;

(ii) $X \subseteq P$;

(iii) $\forall L \leq_R M, \quad X \subseteq L \implies P \subseteq L$.

Demonstração. [exercício]

Proposição. Sejam R um anel e M um módulo$-R$ à direita. Então,

(a) $\langle\emptyset\rangle = \{0\}$;

(b) para todo o $x \in M$, $\langle x \rangle = \{nx + xa : \quad n \in \mathbb{Z} \wedge a \in R\}$;

(c) se $I \neq \emptyset$ e $X = \{x_i\}_{i \in I}$,

$$\begin{aligned} \langle X \rangle &= \left\{ \sum_{i \in I} n_i x_i + \sum_{i \in I} x_i a_i : \quad n_i \in \mathbb{Z} \wedge a_i \in R, \quad n_i, a_i \text{ quase todos nulos} \right\}. \\ &= \sum_{i \in I} \langle x_i \rangle \end{aligned}$$

Demonstração. [exercício]

Proposição. Sejam R um anel unitário e M um módulo$-R$ à direita unitário. Então, para todo o $x \in M$,

$$\langle x \rangle = xR.$$

Demonstração. [exercício]

Sejam R um anel, M um módulo$-R$ à direita e N, L submódulos$-R$ de M. Já vimos que $N + L$ é um submódulo$-R$ de M.

Vejamos se $N \cup L \subseteq N + L$. Tomemos $x \in N \cup L$. Então, $x \in N$ ou $x \in L$. Se $x \in N$, então $x = x + 0 \in N + L$. De modo análogo, se $x \in L$, $x = 0 + x \in N + L$. Assim, $N \cup L \subseteq N + L$.

Consideremos, agora, um submódulo$-R$ T de M tal que $N \cup L \subseteq T$. Pretendemos mostrar que $N + L \subseteq T$. Dado $x \in N + L$, sabemos que existem $n \in N$ e $\ell \in L$ tais que $x = n + \ell$. Ora, $n, \ell \in N \cup L$ e, portanto, $n, \ell \in T$. Como T é um submódulo$-R$ de M, podemos concluir que $x = n + \ell \in T$.

Vimos, assim, que $\langle N \cup L \rangle = N + L$.

Proposição. Sejam R um anel, M um módulo$-R$ à direita, I um conjunto não vazio e $\{N_i\}_{i \in I}$ uma família de submódulos$-R$ de M. Então,

$$\langle \bigcup_{i \in I} N_i \rangle = \sum_{i \in I} N_i.$$

Demonstração. [exercício]

Proposição. Sejam R um anel, M um módulo$-R$ à direita e N, P e Q submódulos$-R$ de M tais que $N \subseteq Q$. Então,

$$(N + P) \cap Q = N + (P \cap Q).$$

Demonstração. Como N, P e Q são submódulos$-R$ de M, sabemos que $N + P$ e $P \cap Q$ são também submódulos$-R$ de M. Logo, $(N + P) \cap Q$ e $N + (P \cap Q)$ são submódulos$-R$ de M.

Comecemos por verificar que $N + (P \cap Q) \subseteq (N + P) \cap Q$. Como $N \subseteq N + P$ e $N \subseteq Q$, sabemos que $N \subseteq (N + P) \cap Q$. Por outro lado, de $P \subseteq N + P$, podemos concluir que $P \cap Q \subseteq (N + P) \cap Q$. Logo,

$$N \cup (P \cap Q) \subseteq (N + P) \cap Q.$$

Ora, $N + (P \cap Q) = \langle N \cup (P \cap Q) \rangle$, pelo que, por definição de submódulo gerado, se tem $N + (P \cap Q) \subseteq (N + P) \cap Q$.

Para provar que $(N+P) \cap Q \subseteq N+(P \cap Q)$, consideremos $x \in (N+P) \cap Q$. Então, $x = n+p$ para algum $n \in N$ e algum $p \in P$. Como $N \subseteq Q$, sabemos que $n \in Q$. Também $x \in Q$, pelo que

$$p = x - n \in Q,$$

uma vez que $Q \leq_R M$. Portanto, $x = n+p$, com $n \in N$ e $p \in P \cap Q$ e, assim, $x \in N+(P \cap Q)$. Logo, $(N + P) \cap Q \subseteq N + (P \cap Q)$. □

Definição. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M. Dizemos que N é *finitamente gerado* ou um *submódulo$-R$ de tipo finito* se N for gerado por um seu subconjunto finito X. Se $X = \{x\}$, então $N = \langle x \rangle$ diz-se um submódulo$-R$ cíclico. Se N não for finitamente gerado, dizemos que N é *infinitamente gerado.*

Exemplos.

1. Seja R um anel unitário. Então, $R = \langle 1 \rangle$ e $R^n = \langle \{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\} \rangle$.
2. Seja R um anel unitário. Então $R[x] = \langle \{1, x, x^2, \ldots\} \rangle$. Mais, não existe nenhum conjunto finito que gere $R[x]$.

Proposição. Seja R um domínio de integridade comutativo e com identidade. Então, R é domínio de ideais principais se e só se todo o submódulo$-R$ de um módulo$-R$ unitário e cíclico é módulo$-R$ cíclico.

Demonstração. Admitamos que todo o submódulo$-R$ de um módulo$-R$ unitário e cíclico é módulo$-R$ cíclico. Seja I um ideal de R. Por definição, I é submódulo$-R$ de R_R. Ora, $R_R = \langle 1 \rangle$, pelo que R_R é um módulo$-R$ unitário e cíclico. Por hipótese, I é módulo$-R$ cíclico, ou seja, existe $a \in I$ tal que $I = \langle a \rangle$. Como $\langle a \rangle = aR = (a)$, podemos concluir que I é um ideal principal e, portanto, R é um domínio de ideais principais.

Suponhamos agora que R é um domínio de ideais principais e sejam M um módulo$-R$ à direita unitário e cíclico e N um submódulo$-R$ de M. Então, sendo M cíclico, existe $a \in R$ tal que

$$M = \langle a \rangle = aR.$$

Consideremos $I = \{r \in R : ar \in N\}$. Como $N \neq \emptyset$ e $N \subseteq M = aR$, temos que $I \neq \emptyset$.

Por definição, $I \subseteq R$. Dados $x, y \in I$ e $r \in R$, sabemos que $ax, ay \in N$. Mais, $x - y \in R$ (pois R é um anel) e $a(x-y) = ax - ay \in N$ (pois $N \leq_R M$). Logo, $x - y \in I$.
Também $xr \in R$, pois R é anel, e $a(xr) = (ax)r \in N$, uma vez que $N \leq_R M$. Assim, $xr \in I$.
Vimos que I é um ideal de R. Sendo R domínio de ideais principais, existe $i \in I$ tal que

$$I = (i) = iR.$$

Por definição de I, $(ai)R = a(iR) = aI \subseteq N$. Mostremos que $N \subseteq (ai)R$. Dado $n \in N$, existe $r \in R$ tal que $n = ar$, pois $N \subseteq M = aR$. Novamente pela definição de I, $r \in I$, pelo que existe $r' \in R$ tal que $r = ir'$ e, portanto,

$$n = ar = a(ir') = (ai)r', \text{ com } r' \in R.$$

Assim, $n \in (ai)R$ e $N = (ai)R = \langle ai \rangle$. Logo, N é cíclico. □

Definição. Sejam $n \in \mathbb{N}$, R um anel, M um módulo$-R$ à direita e $X = \{x_1, \ldots, x_n\} \subseteq M$. Diz-se que $y \in M$ é *combinação linear dos elementos* x_i, ou *combinação linear dos elementos de* X, se existirem elementos $a_i \in R$, com $i \in \{1, \ldots, n\}$, tais que

$$y = x_1 a_1 + \cdots + x_n a_n.$$

Os elementos a_i, com $i \in \{1, \ldots, n\}$, dizem-se os *coeficientes da combinação linear.*

Definição. Sejam R um anel, M um módulo$-R$ à direita, I um conjunto não vazio e $X = \{x_i\}_{i \in I} \subseteq M$. Diz-se que $y \in M$ é *combinação linear dos elementos* x_i, $i \in I$, ou *combinação linear dos elementos de* X, se y for combinação linear dos elementos de uma subfamília finita não vazia de X, isto é, se existirem $k \in \mathbb{N}$, $x_{i_1}, \ldots, x_{i_k} \in X$, $a_1, \ldots, a_k \in R$ tais que

$$y = x_{i_1} a_1 + \cdots + x_{i_k} a_k.$$

Proposição. Sejam R um anel unitário, M um módulo$-R$ à direita unitário e N um submódulo$-R$ de M. Então, N é submódulo$-R$ de tipo finito se e só se existir um subconjunto finito não vazio X de N tal que todo o elemento de N é combinação linear dos elementos de X.

Demonstração. [exercício]

Proposição. Sejam R um anel unitário, M um módulo$-R$ à direita unitário, $X = \{x_i\}_{i \in I}$ e $Y = \{y_j\}_{j \in J}$ famílias não vazias de elementos de M. Então, X e Y geram o mesmo submódulo$-R$ de M se e só se todo o elemento x_i, com $i \in I$, for combinação linear dos elementos de Y e todo o elemento y_j, com $j \in J$, for combinação linear dos elementos de X.

Demonstração. [exercício]

Definição. Sejam R um anel, M um módulo$-R$ à direita, N um submódulo$-R$ de M e S um subconjunto de M. Designa-se por *quociente residual de* N *por* S o conjunto

$$(N : S) = \{a \in R : \quad Sa \subseteq N\}.$$

Proposição. Sejam R um anel, M um módulo$-R$ à direita, N um submódulo$-R$ de M e S um subconjunto de M. Então,

(a) $(N : S)$ é ideal direito de R;

(b) se $S \leq_R M$, então $(N : S)$ é ideal de R.

Demonstração. Comecemos por verificar a veracidade de (a). Se $S = \emptyset$, então $(N : S) = R$ é ideal direito de R. Suponhamos, pois, que $S \neq \emptyset$. Então, $S0_R = \{0_M\} \subseteq N$, pelo que $0_R \in (N : S)$ e, portanto, $(N : S) \neq \emptyset$. Por definição, $(N : S) \subseteq R$. Dados $a, b \in (N : S)$ e $r \in R$, sabemos que $a, b \in R$ e $Sa \subseteq N$, $Sb \subseteq N$. Como R é anel, $a - b, ar \in R$. Sendo N um submódulo$-R$ de M, temos que, para todo o $s \in S$, $s(a-b) = sa-sb \in N$ e $s(ar) = (sa)r \in N$ (pois $sa, sb \in N$). Logo, $S(a - b) \subseteq N$ e $S(ar) \subseteq N$, pelo que $a - b, ar \in (N : S)$. Portanto, $N : S$ é um ideal direito de R.

Suponhamos agora que $S \leq_R M$. Por (a), $(N : S)$ é ideal direito de R. Resta provar que, dados $a \in (N : S)$ e $r \in R$, se tem $ra \in (N : S)$. Ora, se $a \in (N : S)$ e $r \in R$, então $a \in R$ e $Sa \subseteq N$. É claro que $ra \in R$, pois R é um anel. Para todo o $s \in S$, $sr \in S \leq_R M$. Logo,

$$s(ra) = (sr)a \in Sa \subseteq N,$$

pelo que $ra \in (N : S)$, como pretendíamos mostrar. Assim, $(N : S)$ é um ideal de R. □

Exemplo. Sejam R um anel e M um módulo$-R$ à direita. Se $N = \{0_M\}$ e $S \neq \emptyset$ é um submódulo$-R$ de M, então

$$(\{0\} : S) = \{a \in R : \quad Sa \subseteq \{0\}\} = \{a \in R : \quad Sa = \{0\}\} = \mathrm{an}(S).$$

Definição. Sejam R um anel, I um ideal direito de R e S um subconjunto de R. Então, R_R é um módulo$-R$ à direita e I é um submódulo$-R$ de R_R. O conjunto $(I : S)$ designa-se por *quociente residual à direita*.

Proposição. Sejam R um anel, M um módulo$-R$ à direita, N, N_1 e N_2 submódulos$-R$ de M e S, S_1 e S_2 subconjuntos de M. Então,

(a) $(N_1 : S) + (N_2 : S) \subseteq (N_1 + N_2 : S)$;

(b) $(N : S_1) \cap (N : S_2) \subseteq (N : S_1 + S_2)$;

(c) se $0_M \in S_1 \cap S_2$,
$$(N : S_1) \cap (N : S_2) \subseteq (N : S_1 + S_2);$$

(d) se $\{N_i\}_{i \in I}$ é uma família não vazia de submódulos$-R$ de M,

$$\Big(\bigcap_{i \in I} N_i : S\Big) = \bigcap_{i \in I} (N_i : S).$$

Demonstração. [exercício]

Proposição. Seja D um ideal direito de R tal que $(D : R) \subseteq D$. Então, $(D : R)$ é elemento maximal do conjunto de ideais de R que estão contidos em D.

Demonstração. Como $R_R \leq_R R_R$, $(D : R)$ é ideal de R. Por hipótese, $(D : R) \subseteq D$. Seja I um ideal de R tal que $I \subseteq D$ e suponhamos que $(D : R) \subseteq I \subsetneq D$. Pretendemos mostrar que $I \subseteq (D : R)$. Ora, dado $a \in I$, $Ra \subseteq I$, pois I é um ideal de R. Como $I \subseteq D$, temos que $Ra \subseteq D$. Logo, $a \in (D : R)$, uma vez que $a \in I \subseteq R$. Portanto, $I \subseteq (D : R)$. Vimos, assim, que $(D : R)$ é maximal no conjunto de ideais de R que estão contidos em D. □

Definição. Sejam R um anel e M um módulo$-R$ à direita. Uma relação de equivalência ρ em M diz-se uma *relação de congruência em* M se, para quaisquer $x, y, z, w \in M$ e $a \in R$,

$$x \,\rho\, y \;\text{ e }\; z \,\rho\, w \implies (x + z) \,\rho\, (y + w)$$

e

$$x \,\rho\, y \implies (xa) \,\rho\, (ya).$$

Proposição. Sejam R um anel e M um módulo$-R$ à direita.

(a) Se N é um submódulo$-R$ de M, então 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.

(b) Se ρ é uma relação de congruência definida em M, então existe um e um só submódulo$-R$ N_ρ de M tal que, para quaisquer $x, y \in M$,

$$y - x \in N_\rho \quad \Leftrightarrow \quad x \,\rho\, y.$$

Demonstração. (a) [exercício]
Verifiquemos a veracidade de (b).

Seja ρ uma relação de congruência definida em M e seja C_0 a classe de equivalência de 0_M em M, isto é, $C_0 = \{x \in M : x \,\rho\, 0_M\}$. Como ρ é reflexiva, $0_M \in C_0$ e, portanto, $C_0 \neq \emptyset$. Sejam $x, y \in C_0$ e $a \in R$. Então, $x, y \in M$ e $x \,\rho\, 0_M$, $y \,\rho\, 0_M$. Uma vez que ρ é uma relação de congruência, temos que

$$x \,\rho\, 0_M \;\text{ e }\; y \,\rho\, 0_M \implies (x + y) \,\rho\, (0_M + 0_M).$$

Logo, $(x+y) \,\rho\, 0_M$ e, assim, $x+y \in C_0$. Como ρ é reflexiva e $-x \in M$, temos que $(-x) \,\rho\, (-x)$. Portanto,

$$x \,\rho\, 0_M \;\text{ e }\; (-x) \,\rho\, (-x) \implies (x - x) \,\rho\, (0_M - x),$$

pelo que $-x\,\rho\,0_M$ e, então, $-x \in C_0$. Também

$$x\,\rho\,0_M \implies (xa)\,\rho\,(0_M a),$$

ou seja, $(xa)\,\rho\,0_M$. Logo, $xa \in C_0$ e C_0 é um submódulo$-R$ de M.

Vejamos, agora, que, dados $x, y \in M$,

$$y - x \in C_0 \quad \Leftrightarrow \quad x\,\rho\,y.$$

Suponhamos que $y - x \in C_0$. Então, $y - x\,\rho\,0_M$. Como $x \in M$ e ρ é reflexiva, $x\,\rho\,x$. Logo, $[(y-x)+x]\,\rho\,(0_M + x)$, pelo que $y\,\rho\,x$. Como ρ é simétrica, $x\,\rho\,y$.
Admitamos que $x\,\rho\,y$. Como M é módulo$-R$ à direita, $-x \in M$ e, portanto, $(-x)\,\rho\,(-x)$. Logo, $[x+(-x)]\,\rho\,[y+(-x)]$, ou seja $0_M\,\rho\,(y-x)$. Como ρ é simétrica, temos que $(y-x)\,\rho\,0_M$ e, portanto, $y - x \in C_0$.

Finalmente, suponhamos que N é um submódulo$-R$ de M tal que, para quaisquer $x, y \in M$,

$$y - x \in N \quad \Leftrightarrow \quad x\,\rho\,y.$$

Queremos mostrar que $N = C_0$. Ora, dado $x \in N$, $0_M - x \in N$ (pois N é submódulo$-R$ de M). Por hipótese, $x\,\rho\,0_M$, ou seja, $x \in C_0$. Por outro lado, se $x \in C_0$, então $x\,\rho\,0_M$ e, portanto, $-x = 0_M - x \in N$. Como N é um submódulo$-R$ de M, $x \in N$ e $N = C_0$. □

Exemplos.

1. Sejam R um anel e M um módulo$-R$ à direita. Então, $\{0\}$ é um submódulo$-R$ de M e $\rho_{\{0\}}$ é a relação identidade.

2. Sejam R um anel e M um módulo$-R$ à direita. Então, M é um submódulo$-R$ de M e ρ_M é a relação universal.

Proposição. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M. Então, o grupo quociente M/N é um módulo$-R$ à direita com a ação de R em M/N dada por

$$(x + N)a = (xa) + N \qquad (x \in M, a \in R).$$

Demonstração. [exercício]

Definição. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M. O módulo$-R$ M/N diz-se o *módulo quociente de M por N*.

Proposição. Sejam R um anel unitário, M um módulo$-R$ à direita unitário e N um submódulo$-R$ de M. Então, M/N é unitário.

Demonstração. [exercício]

Proposição. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M. Então, os submódulos$-R$ de M/N são exatamente os conjuntos T/N, com T submódulo$-R$ de M que contém N.

Demonstração. [exercício]

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

Demonstração. Admitamos que N é um submódulo maximal de M. Então, N é elemento maximal da família dos submódulos próprios de M. Como $N \subsetneq M$, sabemos que

$$M/N \neq \{N\}.$$

Seja $\overline{T}$ um submódulo$-R$ de M/N. Pela proposição anterior, $\overline{T} = T/N$ para algum T submódulo$-R$ de M tal que $N \subseteq T$. Como N é submódulo maximal de M e $N \subseteq T \subseteq M$, podemos concluir que $T = N$ ou $T = M$, pelo que

$$\overline{T} = N/N = \{N\} \text{ ou } \overline{T} = M/N.$$

Assim, M/N é módulo$-R$ simples.

Suponhamos, agora, que M/N é um módulo$-R$ simples e seja P um submódulo$-R$ de M tal que $N \subseteq P \subsetneq M$. Pela proposição anterior, P/N é um submódulo$-R$ de M/N. Logo, por hipótese, $P/N = \{N\}$ ou $P/N = M/N$. Assim, $P = N$ ou $P = M$. Como P é submódulo próprio de M, concluímos que $P = N$. Portanto, N é submódulo maximal de M. □

Proposição. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M. Então,

(a) se M é um módulo$-R$ de tipo finito, M/N é também de tipo finito;

(b) se N e M/N são módulos$-R$ de tipo finito, M é também módulo$-R$ de tipo finito.

Demonstração. [exercício]

Definição. Sejam R um anel e M, M' módulos$-R$ à direita. Uma aplicação $\varphi : M \to M'$ diz-se um *homomorfismo*$-R$ ou *morfismo*$-R$ se, para quaisquer $x, y \in M$ e $a \in R$,

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

Se φ for injetivo [respetivamente: sobrejetivo, bijetivo], dizemos que φ é um *monomorfismo*$-R$ [respetivamente: *epimorfismo*$-R$, *isomorfismo*$-R$].
Quando $M = M'$, dizemos que φ é um *endomorfismo*$-R$. Mais, se φ for um endomorfismo$-R$ bijetivo, dizemos que φ é um *automorfismo*$-R$.

Exemplos.

1. Sejam R um anel e M, M' módulos$-R$ à direita. A aplicação $\varphi_0 : M \to M'$, $x \mapsto 0_{M'}$, é um morfismo$-R$, designado por *morfismo nulo*.

2. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M. Então, N é módulo$-R$ à direita. A aplicação $\iota : N \to M$, $x \mapsto x$, é um monomorfismo$-R$, designado por *inclusão*.

   Se $N = M$, então ι é um automorfismo$-R$, o automorfismo *identidade*, e representa-se por id_M.

3. Sejam R um anel, M um módulo$-R$ à direita e N um submódulo$-R$ de M. A aplicação $\pi : M \to M/N$, $x \mapsto x+N$, é um epimorfismo$-R$, designado por *epimorfismo canónico*.

Proposição. Sejam R um anel unitário, M e M' módulos$-R$ à direita unitários e $\varphi : M \to M'$ uma aplicação. 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 $a \in R$, $\varphi(xa + y) = \varphi(x)a + \varphi(y)$.

Demonstração. [exercício]

Proposição. Sejam R um anel e M, M' e M'' módulos$-R$ à direita. Então,

(a) se $\varphi : M \to M'$ e $\psi : M' \to M''$ são morfismos$-R$, a composição $\psi \circ \varphi : M \to M''$ é ainda um morfismo$-R$.

(b) se $\varphi : M \to M'$ é um isomorfismo$-R$, a inversa $\varphi^{-1} : M' \to M$ é também um isomorfismo$-R$.

Demonstração. [exercício]

Proposição. Sejam R um anel, M e M' módulos$-R$ à direita e $\varphi : M \to M'$ um morfismo$-R$. Então,

(a) $\varphi(0_M) = 0_{M'}$;

(b) $\varphi(-x) = -\varphi(x)$, para todo o $x \in M$;

(c) $\varphi(x - y) = \varphi(x) - \varphi(y)$, para quaisquer $x, y \in M$;

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

(d) 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;

Demonstração. [exercício]

Proposição. Sejam R um anel, M e M' módulos$-R$ à direita e $\varphi : M \to M'$ um isomorfismo$-R$. Então,

$$\mathrm{an}(M) = \mathrm{an}(M').$$

Demonstração. [exercício]

Definição. Sejam R um anel, M e M' módulos$-R$ à direita e $\varphi : M \to M'$ um morfismo$-R$. Definimos o *núcleo de* φ como sendo o conjunto $\mathrm{Ker}(\varphi) = \{x \in M : \ \varphi(x) = 0_{M'}\}$. A *imagem de* φ é o conjunto $\mathrm{Im}(\varphi) = \{\varphi(x) : x \in M\}$.

Proposição. Sejam R um anel, M e M' módulos$-R$ à direita e $\varphi : M \to M'$ um morfismo$-R$. Então,

(a) $\mathrm{Ker}(\varphi)$ é um submódulo$-R$ de M;

(b) $\mathrm{Im}(\varphi)$ é um submódulo$-R$ de M'.

Demonstração. [exercício]

Proposição. Sejam R um anel, M e M' módulos$-R$ à direita e $\varphi : M \to M'$ um morfismo$-R$. Então, φ é um monomorfismo$-R$ se e só se $\mathrm{Ker}(\varphi) = \{0_M\}$.

Demonstração. [exercício]

Proposição. Sejam R um anel, M e M' módulos$-R$ à direita e $\varphi : M \to M'$ um morfismo$-R$. A relação binária ρ definida por

$$x \,\rho\, y \quad \Leftrightarrow \quad \varphi(x) = \varphi(y) \qquad (x, y \in M)$$

é uma relação de congruência em M. Mais, o submódulo$-R$ de M associado a ρ é $\mathrm{Ker}(\varphi)$.

Demonstração. [exercício]

Teorema [Teorema do Homomorfismo]. Sejam R um anel, M e M' módulos$-R$ à direita e $\varphi : M \to M'$ um morfismo$-R$. Então,

$$M/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi).$$

Demonstração. [exercício]

Teorema [Primeiro Teorema do Isomorfismo]. Sejam R um anel, M e M' módulos$-R$ à direita, $\varphi : M \to M'$ um morfismo$-R$ e N um submódulo$-R$ de M tal que $\mathrm{Ker}(\varphi) \subseteq N$. Então,

$$M/N \simeq \mathrm{Im}(\varphi)/\varphi(N).$$

Demonstração. [exercício]

Corolário. Sejam R um anel, M um módulo$-R$ à direita e N e L submódulos$-R$ de M tais que $L \subseteq N$. Então,

$$M/N \simeq (M/L)/(N/L).$$

Demonstração. [exercício]

Teorema [Segundo Teorema do Isomorfismo]. Sejam R um anel, M um módulo$-R$ à direita e N e L submódulos$-R$ de M. Então,

$$(N + L)/L \simeq N/(N \cap L).$$

Demonstração. [exercício]

Proposição. Sejam R um anel, M e M' módulos$-R$ à direita e $\varphi : M \to M'$ um morfismo$-R$. Se N é um submódulo$-R$ de M e $X = \{x_i\}_{i\in I}$ é um conjunto de geradores de N, então $X' = \{\varphi(x_i)\}_{i\in I}$ é um conjunto de geradores de $\varphi(N)$.

Demonstração. Como φ é um morfismo$-R$ e N é um submódulo$-R$ de M, temos que $\varphi(N)$ é um submódulo$-R$ de M'. Além disso, $X \subseteq N$ implica que $\varphi(X) \subseteq \varphi(N)$, ou seja, $X' \subseteq \varphi(N)$. Por definição de submódulo gerado, $\langle X' \rangle \subseteq \varphi(N)$.

Dado $y \in \varphi(N)$, sabemos que existe $x \in N$ tal que $y = \varphi(x)$. Como $N = \langle \{x_i\}_{i\in I} \rangle$ e $x \in N$, existem $n_i \in \mathbb{Z}$ e $a_i \in R$, quase todos nulos, tais que

$$x = \sum_{i\in I} n_i x_i + \sum_{i\in I} x_i a_i.$$

Logo,

$$\begin{aligned} y &= \varphi(x) = \varphi(\sum_{i\in I} n_i x_i) + \varphi(\sum_{i\in I} x_i a_i) \\ &= \sum_{i\in I} \varphi(n_i x_i) + \sum_{i\in I} \varphi(x_i a_i) \\ &= \sum_{i\in I} n_i \varphi(x_i) + \sum_{i\in I} \varphi(x_i) a_i \end{aligned} ,$$

com n_i, a_i quase todos nulos. Portanto, $y \in \langle \{\varphi(x_i)\}_{i\in I} \rangle = \langle X' \rangle$, pelo que $\varphi(N) \subseteq \langle X' \rangle$. Assim, $\varphi(N) = \langle \varphi(X) \rangle$. □

Proposição. 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. Então, φ é um epimorfismo$-R$ se e só se $X' = \{\varphi(x_i)\}_{i\in I}$ é um conjunto de geradores de M'.

Demonstração. [exercício]

Teorema. Sejam R um anel, M, M' e M'' módulos$-R$ à direita, $\varphi : M \to M'$ um morfismo$-R$ e $\psi : M \to M''$ um epimorfismo$-R$ tal que $\mathrm{Ker}(\psi) \subseteq \mathrm{Ker}(\varphi)$. Então,

(a) existe um e um só morfismo$-R$ $\theta : M'' \to M'$ tal que $\theta \circ \psi = \varphi$;

(b) $\mathrm{Ker}(\theta) \simeq \mathrm{Ker}(\varphi)/\mathrm{Ker}(\psi)$;

(c) θ é monomorfismo$-R$ se e só se $\mathrm{Ker}(\varphi) = \mathrm{Ker}(\psi)$;

(d) θ é isomorfismo$-R$ se e só se $\mathrm{Ker}(\varphi) = \mathrm{Ker}(\psi)$ e φ é epimorfismo$-R$.

Demonstração.

(a) Consideremos a correspondência $\theta : M'' \to M'$ definida por $\theta(m'') = \varphi(m)$, onde $m \in M$ é tal que $\psi(m) = m''$. Suponhamos que $m'' \in M''$ e $m, m_1 \in M$ são tais que $\psi(m) = \psi(m_1) = m''$. Então, $\psi(m - m_1) = \psi(m) - \psi(m_1) = 0_{M''}$, pelo que $m - m_1 \in \mathrm{Ker}(\psi) \subseteq \mathrm{Ker}(\varphi)$. Logo, $m - m_1 \in \mathrm{Ker}(\varphi)$ e, portanto, $\varphi(m) = \varphi(m_1)$. Assim, θ é uma aplicação.

Vejamos agora se θ é um morfismo$-R$. Sejam $m_1'', m_2'' \in M''$ e $a \in R$. Então, $\theta(m_1'') = \varphi(m_1)$ e $\theta(m_2'') = \varphi(m_2)$, onde $m_1, m_2 \in M$ são tais que $\psi(m_1) = m_1''$ e $\psi(m_2) = m_2''$. Portanto,

$$\theta(m_1'' + m_2'') = \theta(\psi(m_1) + \psi(m_2)) = \theta(\psi(m_1 + m_2).$$

Por definição de θ, $\theta(\psi(m_1 + m_2)) = \varphi(m_1 + m_2)$. Logo, como φ é um morfismo$-R$,

$$\theta(m_1'' + m_2'') = \varphi(m_1) + \varphi(m_2) = \theta(m_1'') + \theta(m_2'').$$

Por outro lado,

$$\theta(m_1''a) = \theta(\psi(m_1)a) = \theta(\psi(m_1a)) = \varphi(m_1a) = \varphi(m_1)a = \theta(m_1'')a.$$

Logo, θ é um morfismo$-R$.

Dado $m \in M$,

$$(\theta \circ \psi)(m) = \theta(\psi(m)) = \varphi(m),$$

pelo que $\theta \circ \psi = \varphi$.

Resta mostrar que θ é único nas condições enunciadas. Suponhamos, pois, que $\phi : M'' \to M'$ é um morfismo$-R$ tal que $\phi \circ \psi = \varphi$. Para provar que $\theta = \phi$, tomemos $m \in M''$. Como ψ é sobrejetiva, existe $m \in M$ tal que $m'' = \psi(m)$. Logo,

$$\phi(m'') = \phi(\psi(m)) = (\phi \circ \psi)(m) = \varphi(m) = (\theta \circ \psi)(m) = \theta(\psi(m)) = \theta(m'').$$

(b) Como $\psi : M \to M''$ é um morfismo$-R$ e $\mathrm{Ker}(\varphi) \leq_R M$, temos que a restrição de ψ a $\mathrm{Ker}(\varphi)$, $\psi_{|\mathrm{Ker}(\varphi)} : \mathrm{Ker}(\varphi) \to M''$, é um morfismo$-R$. Pelo Teorema do Homomorfismo,

$$\mathrm{Ker}(\varphi)/\mathrm{Ker}(\psi_{|\mathrm{Ker}(\varphi)}) \simeq \psi_{|\mathrm{Ker}(\varphi)}(\mathrm{Ker}(\varphi)). \qquad (*)$$

Vejamos que $\mathrm{Ker}(\psi_{|\mathrm{Ker}(\varphi)}) = \mathrm{Ker}(\psi)$. É claro que

$$\mathrm{Ker}(\psi_{|\mathrm{Ker}(\varphi)}) \subseteq \mathrm{Ker}(\psi).$$

Seja $x \in \mathrm{Ker}(\psi)$. Então, $x \in M$ e $\psi(x) = 0_{M''}$. Por hipótese, $\mathrm{Ker}(\psi) \subseteq \mathrm{Ker}(\varphi)$, pelo que $x \in \mathrm{Ker}(\varphi)$. Logo, $\psi_{|\mathrm{Ker}(\varphi)}(x)$ está definida e

$$\psi_{|\mathrm{Ker}(\varphi)}(x) = \psi(x) = 0_{M''}.$$

Portanto, $x \in \mathrm{Ker}(\psi_{|\mathrm{Ker}(\varphi)})$. Assim, $\mathrm{Ker}(\psi) \subseteq \mathrm{Ker}(\psi_{|\mathrm{Ker}(\varphi)})$.

Verifiquemos, agora, que $\mathrm{Ker}(\theta) = \psi_{|\mathrm{Ker}(\varphi)}(\mathrm{Ker}(\varphi))$. Dado $x \in \mathrm{Ker}(\theta)$, sabemos que $x \in M''$ e $\theta(x) = 0_{M'}$. Como ψ é um epimorfismo$-R$ e $x \in M''$, existe $m \in M$ tal que $\psi(m) = x$. Da igualdade $\theta \circ \psi = \varphi$, vem

$$\varphi(m) = \theta(\psi(m)) = \theta(x) = 0_{M'},$$

pelo que podemos concluir que $m \in \mathrm{Ker}(\varphi)$. Logo, $x = \psi(m) \in \psi(\mathrm{Ker}(\varphi)) = \psi_{|\mathrm{Ker}(\varphi)}(\mathrm{Ker}(\varphi))$.

Reciprocamente, se $x \in \psi_{|\mathrm{Ker}(\varphi)}(\mathrm{Ker}(\varphi))$, então existe $m \in \mathrm{Ker}(\varphi)$ tal que $x = \psi_{|\mathrm{Ker}(\varphi)}(m)$. Logo,

$$\theta(x) = \theta(\psi_{|\mathrm{Ker}(\varphi)}(m)) = \theta(\psi(m)) = (\theta \circ \psi)(m) = \varphi(m) = 0_{M'}$$

e, portanto, $x \in \mathrm{Ker}\theta$.

De $(*)$, concluímos que $\mathrm{Ker}(\theta) \simeq \mathrm{Ker}(\varphi)/\mathrm{Ker}(\psi)$.

(c) Sabemos que θ é um monomorfismo$-R$ se e só se $\mathrm{Ker}(\theta) = \{0_{M''}\}$, o que, pela alínea (b), é equivalente a $\mathrm{Ker}(\varphi)/\mathrm{Ker}(\psi) = \{\mathrm{Ker}(\psi)\}$. Mas esta última igualdade é válida se e só se $\mathrm{Ker}(\varphi) = \mathrm{Ker}(\psi)$.

(d) Sabemos que θ é um isomorfismo$-R$ se e só se for um monomorfismo$-R$ e um epimorfismo$-R$. Como ψ é um epimorfismo$-R$ e $\theta \circ \psi = \varphi$, θ é um epimorfismo$-R$ se e só se φ é um epimorfismo$-R$. Logo, pela alínea anterior, θ é um isomorfismo$-R$ se e só se $\mathrm{Ker}(\varphi) = \mathrm{Ker}(\psi)$ e φ é um epimorfismo$-R$. □

Notação. 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'.

Proposição. Sejam R um anel e M e M' dois módulos$-R$ à direita. Então,

(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 $\varphi a : M \to M'$, $x \mapsto \varphi(xa)$.

Demonstração. [exercício]

Proposição. Sejam R um anel, M, M', M'' módulos$-R$ à direita, $\varphi, \varphi_1, \varphi_2 \in \mathrm{Hom}_R(M, M')$ e $\psi, \psi_1, \psi_2 \in \mathrm{Hom}_R(M', M'')$. 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) $\psi \circ (-\varphi) = -(\psi \circ \varphi) = (-\psi) \circ \varphi$.

Demonstração. [exercício]

Notação. 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.

Proposição. Sejam R um anel e M um módulo$-R$ à direita. Então,

(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 $\mathrm{GL}_R(M)$.

Demonstração. [exercício]

1.2. Somas diretas de módulos

Proposição. Sejam R um anel e $\{M_i\}_{i \in I}$ uma família de módulos$-R$ à direita. O produto cartesiano

$$P = \prod_{i \in I} M_i = \{(x_i)_{i \in I} : \quad \forall i \in I,\, x_i \in M_i\},$$

munido com as seguintes operações

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I} \qquad ((x_i)_{i \in I}, (y_i)_{i \in I} \in P),$$

$$(x_i)_{i \in I}.a = (x_i a)_{i \in I} \qquad ((x_i)_{i \in I} \in P, a \in R),$$

é um módulo$-R$ à direita.

Demonstração. [exercício]

Definição. Sejam R um anel e $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita. Ao módulo$-R$ à direita $\prod_{i\in I} M_i$ chamamos *produto direto dos módulos* M_i.

Se $M_i = M$ para todo o $i \in I$, então representamos $\prod_{i\in I} M_i$ por M^I. Mais, se I tem n elementos, com $n \in \mathbb{N}$, representamos $\prod_{i\in I} M_i$ por M^n.

Por convenção, se $I = \emptyset$, $\prod_{i\in I} M_i = \{0\}$.

Proposição. Sejam R um anel e $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita. O conjunto S definido por

$$S = \{(x_i)_{i\in I} : \ \forall i \in I,\, x_i \in M_i,\ x_i \text{ quase todos nulos}\}$$

é um submódulo$-R$ do produto direto $\prod_{i\in I} M_i$.

Demonstração. [exercício]

Definição. Sejam R um anel e $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita. Ao submódulo$-R$ $\{(x_i)_{i\in I} : \ \forall i \in I,\, x_i \in M_i,\ x_i \text{ quase todos nulos}\}$ de $\prod_{i\in I} M_i$ chamamos *soma direta externa dos módulos* M_i e representamo-lo por

$$\bigoplus_{i\,\in\, I}{}_{\mathrm{e}} M_i$$

Se $I = \emptyset$, então $\bigoplus_{i\,\in\, I}{}_{\mathrm{e}} M_i \ = \{0\}$

Se os módulos$-R$ à direita M_i, com $i \in I$, representarem todos o mesmo módulo M, representamos a soma direta externa por $M^{(I)}$.

Se I for um conjunto finito, então $\prod_{i\in I} M_i = \bigoplus_{i\,\in\, I}{}_{\mathrm{e}} M_i$.

Se I for um conjunto com 1 elemento, digamos i_0, então $\prod_{i\in I} M_i = M_{i_0}$.

Definição. Sejam R um anel e $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita. Para cada $j \in I$, a aplicação

$$\begin{array}{rccc} p_j : & \prod_{i\in I} M_i & \to & M_j \\ & (x_i)_{i\in I} & \mapsto & x_j \end{array}$$

designa-se por *projeção canónica* e a aplicação

$$\begin{array}{rccc} \iota_j : & M_j & \to & \prod_{i\in I} M_i, \\ & x_j & \mapsto & (y_i)_{i\in I} \end{array}$$

onde $y_i = x_j$ se $i = j$ e $y_i = 0_{M_i}$ se $i \neq j$, designa-se por *inclusão canónica*.
A restrição da projeção canónica p_j à soma direta externa dos módulos M_i representa-se por p'_j. A aplicação de M_j na soma direta externa dos módulos M_i que a cada $x_j \in M_j$ faz corresponder $\iota_j(x_j)$ representa-se por ι'_j.

Proposição. Sejam R um anel e $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita. Para cada $j \in I$, p_j e p'_j são epimorfismos$-R$ e ι_j e ι'_j são monomorfismos$-R$.

Demonstração. [exercício]

Proposição. Sejam R um anel e $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita. Dados $j, k \in I$ com $j \neq k$,

$$p_j \circ \iota_j = \mathrm{id}_{M_j}$$

e

$$p_j \circ \iota_k = \varphi_0.$$

Demonstração. [exercício]

Observemos que, dado $x \in \bigoplus_{i\in I} M_i$, $x = (x_i)_{i\in I}$, com $x_i \in M_i$, x_i quase todos nulos.

Sejam $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ as únicas componentes de x não nulas. Então,

$$x = (x_i)_{i\in I} = \iota'_{i_1}(x_{i_1}) + \cdots + \iota'_{i_k}(x_{i_k}) = \sum_{i\in I} \iota'_i(x_i).$$

Teorema [Propriedade Universal do Produto Direto]. Sejam R um anel e $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita. Seja $P = \prod_{i\in I} M_i$. Então,

(a) O módulo$-R$ à direita P e a família de projeções $\{p_i\}_{i\in I}$ verificam a seguinte propriedade:

[P$_1$] Para todo o módulo$-R$ à direita F e toda a família de morfismos$-R$ $\{\varphi_i\}_{i\in I}$, com $\varphi_i : F \to M_i$ para cada $i \in I$, existe um e um só morfismo$-R$ $f : F \to P$ tal que

$$p_i \circ f = \varphi_i \text{ para todo o } i \in I.$$

(b) Sejam T um módulo$-R$ à direita e $\{\rho_i\}_{i\in I}$, com $\rho_i : T \to M_i$ para cada $i \in I$, uma família de morfismos$-R$ que verificam a propriedade [P$_1$]. Então, existe um isomorfismo $f : T \to P$ tal que $\rho_i = p_i \circ f$ para todo o $i \in I$.

Demonstração.

(a) Sejam F um módulo$-R$ à direita e $\{\varphi_i\}_{i\in I}$, com $\varphi_i : F \to M_i$ para cada $i \in I$, uma família de morfismos$-R$. Consideremos a correspondência $f : F \to P$ definida por

$$\begin{array}{rccc} f: & F & \to & P \\ & x & \mapsto & (\varphi_i(x))_{i\in I} \end{array}$$

Não é difícil de verificar que f é um morfismo$-R$ tal que $p_i \circ f = \varphi_i$ para todo o $i \in I$, e que é único nestas condições. [exercício]

(b) Pela alínea a, existe um e um só morfismo$-R$ $f : T \to P$ tal que

$$p_i \circ f = \rho_i \text{ para todo o } i \in I.$$

Por outro lado, como T e $\{\rho_i\}_{i\in I}$ verificam a propriedade $[\mathrm{P}_1]$, temos que existe um e um só morfismo $g : P \to T$ tal que

$$\rho_i \circ g = p_i \text{ para todo o } i \in I.$$

Dado $i \in I$,

$$\rho_i \circ (g \circ f) = (\rho_i \circ g) \circ f = p_i \circ f = \rho_i$$

e

$$\rho_i \circ \mathrm{id}_T = \rho_i.$$

Ora, por hipótese, existe um e um só morfismo$-R$ $h : T \to T$ tal que $\rho_i \circ h = \rho_i$ para todo o $i \in I$. Logo, podemos concluir que

$$g \circ f = \mathrm{id}_T,$$

donde segue que g é sobrejetiva e f é injetiva.

De modo análogo, para todo o $i \in I$,

$$p_i \circ (f \circ g) = (p_i \circ f) \circ g = \rho_i \circ g = p_i$$

e

$$p_i \circ \mathrm{id}_P = p_i.$$

Por (a), existe um e um só morfismo$-R$ $h' : P \to P$ tal que $p_i \circ h' = p_i$ para todo o $i \in I$. Logo, podemos concluir que

$$f \circ g = \mathrm{id}_P$$

e, portanto, f é sobrejetiva e g é injetiva.

Assim, f é um isomorfismo, como pretendíamos mostrar. □

Teorema [Propriedade Universal da Soma Direta Externa]. Sejam R um anel, $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita e $\overline{M} = \bigoplus_{i \in I}{}_{\mathrm{e}} M_i$.

(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) 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]. Então, existe um isomorfismo $f : \overline{M} \to T$ tal que $\rho_i = f \circ \iota'_i$ para todo o $i \in I$.

Demonstração. [exercício]

Definição. Sejam R um anel, M um módulo$-R$ à direita e $\{N_i\}_{i\in I}$ uma família não vazia de submódulos$-R$ de M. Dizemos que N é *soma direta interna dos submódulos*$-R$ N_i, e escrevemos

$$\bigoplus_{i \in I}{}_{\mathrm{i}} N_i,$$

se:

[D_1] $N = \sum_{i\in I} N_i$;

[D_2] Cada elemento x de N se escreve, de uma única maneira, na forma $x = \sum_{i\in I} x_i$, com $x_i \in N_i$ para cada $i \in I$.

Se I é finito, representamos $\bigoplus_{i \in I}{}_{\mathrm{i}} N_i$ por $N_1 \oplus \cdots \oplus N_k$, onde $k = |I|$.

Exemplo. Sejam R um anel, $\{M_i\}_{i\in I}$ uma família de módulos$-R$ à direita e $\overline{M} = \bigoplus_{i \in I}{}_{\mathrm{e}} M_i$. Para cada $i \in I$, seja $\overline{M}_i = \iota'_i(M_i)$, isto é,

$$\overline{M}_i = \{(x_i)_{i\in I} : \quad x_j = 0_{M_j}, \quad \text{quando} \quad j \neq i\}.$$

Então, para cada $i \in I$, $\overline{M}_i$ é um submódulo$-R$ de $\overline{M}$ e $\overline{M} = \bigoplus_{i \in I}{}_{\mathrm{i}} \overline{M}_i$,

Proposição. Sejam R um anel, M um módulo$-R$ à direita, N um submódulo$-R$ de M e $\{N_i\}_{i\in I}$ uma família de submódulos$-R$ de M. Então, N é soma direta interna dos submódulos$-R$ N_i se e só se a aplicação

$$\begin{array}{rccc} g : & \bigoplus_{i \in I}{}_{\mathrm{e}} N_i & \to & N \\ & (x_i)_{i\in I} & \mapsto & \sum_{i\in I} x_i \end{array}$$

for isomorfismo$-R$.

Demonstração. [exercício]

Proposição. Sejam R um anel, M um módulo$-R$ à direita, N um submódulo$-R$ de M e $\{N_i\}_{i\in I}$ uma família de submódulos$-R$ de M. Então, N é soma direta interna dos submódulos$-R$ N_i se e só se

[D$'_1$] $N = \sum_{i\in I} N_i$;

[D$'_2$] Para cada $j \in I$,

$$N_j \cap \left(\sum_{i\neq j} N_i\right) = \{0_M\}.$$

Demonstração. Admitamos que $N = \bigoplus_{i\,\in\, I} N_i$. Então, são satisfeitas as condições [D$_1$] e [D$_2$]. Para mostrar que a condição [D$'_2$] se verifica, tomemos $j \in I$ e $x \in N_j \cap \left(\sum_{i\neq j} N_i\right)$. Por definição de interseção de conjuntos, $x \in N_j$ e $x \in \sum_{i\neq j} N_i$. Logo,

$$x = \sum_{i\neq j} x_i,$$

onde $x_i \in N_i$ para todo o $i \in I \setminus \{j\}$. Portanto,

$$x = \sum_{i\in I} y_i = \sum_{i\in I} z_i,$$

onde $y_j = x$ e $y_i = 0_M$ para todo o $i \in I \setminus \{j\}$ e $z_j = 0_M$ e $z_i = x_i$ para todo o $i \in I \setminus \{j\}$. Por [D$_2$], $y_i = z_i$ para todo o $i \in I$. Em particular,

$$x = y_j = z_j = 0_M$$

e, portanto, $N_j \cap \left(\sum_{i\neq j} N_i\right) = \{0_M\}$.

Reciprocamente, suponhamos que são satisfeitas as condições [D$'_1$] e [D$'_2$]. Para mostrar que a condição [D$_2$] se verifica, tomemos $x \in N$ e suponhamos que

$$x = \sum_{i\in I} x_i = \sum_{i\in I} y_i,$$

com $x_i, y_i \in N_i$ para cada $i \in I$. Então, dado $j \in J$,

$$x_j - y_j = \sum_{i\neq j} y_i - \sum_{i\neq j} x_i,$$

ou seja,

$$x_j - y_j = \sum_{i \neq j} (y_i - x_i).$$

Ora, sendo $\{N_i\}_{i \in I}$ uma família de submódulos$-R$ de M, temos que $x_j - y_j \in N_j$ e $y_i - x_i \in N_i$ para todo o $i \in I \setminus \{j\}$. Portanto,

$$x_j - y_j \in N_j \cap \left(\sum_{i \neq j} N_i \right) = \{0_M\},$$

pelo que $x_j - y_j = 0_M$. Assim, $x_j = y_j$ para todo o $j \in I$. Por outras palavras, x escreve-se de maneira única na forma $x = \sum_{i \in I} x_i$, com $x_i \in N_i$ para cada $i \in I$ e, portanto, [D_2] é satisfeita.

Por definição, $N = \bigoplus_{i \in I} N_i$. □

1.3. Módulos livres e sequências exatas

No que se segue, R é um anel não nulo unitário, M é um módulo$-R$ à direita unitário e I é um conjunto não vazio.

Definição. Dizemos que $M \neq \{0\}$ é *módulo$-R$ livre* se existir uma família $X = \{m_i\}_{i \in I}$, com $m_i \in M$, tal que todo o elemento $m \in M$ se pode escrever, de maneira única, na forma

$$m = \sum_{i \in I} m_i r_i,$$

onde $r_i \in R$ são quase todos nulos.
Neste caso, dizemos que X é *base (livre) de M*.
Se $M = \{0\}$, consideramos que M é um módulo$-R$ livre de base $\emptyset$.

Proposição. Seja M um módulo$-R$ livre e $X = \{m_i\}_{i \in I}$ uma base de M. Então,

(a) $\sum_{i \in I} m_i r_i = 0 \quad \Leftrightarrow \quad r_i = 0$, para todo o $i \in I$.

(b) Para todo o $i \in I$, $m_i R$ e R são módulos-R isomorfos.

Exemplos.

1. R_R é um módulo$-R$ livre de base $\{1\}$.

2. $R^{(I)}$ é um módulo$-R$ livre de base $\{e_i\}_{i \in I}$, com $e_i = (y_j^i)_{j \in I}$, onde

$$y_j^i = \begin{cases} 1, & \text{se } j = i \\ 0, & \text{se } j \neq i \end{cases} .$$

Proposição. Seja M um módulo livre não nulo de base $X = \{x_i\}_{i\in I}$. Então,

$$M = \bigoplus_{i\in I} x_i R \ .$$

Demonstração. [exercício]

Lema. Seja M um módulo$-R$ não nulo. Então, M é módulo$-R$ livre se e só se M é isomorfo a $R_R^{(I)}$, para um certo conjunto I.

Demonstração. Admitamos que M é um módulo$-R$ livre. Então, existe uma família $X = \{x_i\}_{i\in I}$, com $x_i \in M$, tal que todo o elemento m de M se escreve, de maneira única, na forma $m = \sum_{i\in I} m_i r_i$, onde $r_i \in R$ são quase todos nulos. Consideremos a correspondência

$$\begin{array}{rccc} \varphi: & R_R^{(I)} & \to & M \\ & (a_i)_{i\in I} & \mapsto & \displaystyle\sum_{i\in I} x_i a_i \\ & {\scriptstyle a_i \text{ q.t. nulos}} & & \end{array} .$$

Não é difícil de verificar que φ é um isomorfismo$-R$. [exercício]

Suponhamos, agora, que M é isomorfo a $R_R^{(I)}$ e seja φ um isomorfismo$-R$ de $R_R^{(I)}$ em M. Sabemos que $R^{(I)}$ é um módulo$-R$ livre de base $\{e_i\}_{i\in I}$, com $e_i = (y_j^i)_{j\in I}$, onde

$$y_j^i = \begin{cases} 1, & \text{se } j = i \\ 0, & \text{se } j \neq i \end{cases} .$$

Consideremos a família $X = \{\varphi(e_i)\}_{i\in I}$. Verifica-se que X é uma base de M [exercício] e, portanto, M é um módulo$-R$ livre. □

Proposição. Todo o módulo$-R$ unitário é imagem epimorfa de um módulo$-R$ livre.

Demonstração. Seja M um módulo$-R$ unitário e seja $X = \{x_i\}_{i\in I}$ um conjunto de geradores de M. Consideremos a correspondência

$$\begin{array}{rccc} \varphi: & R_R^{(I)} & \to & M \\ & \displaystyle\sum_{i\in I} e_i r_i & \mapsto & \displaystyle\sum_{i\in I} x_i r_i \end{array} .$$

Prova-se que φ é um epimorfismo$-R$ [exercício]. □

Observação. Na demonstração do resultado anterior, define-se um epimorfismo$-R$ φ de $R_R^{(I)}$ em M. Logo,

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

No que se segue, R é um anel.

Definição. Seja M um módulo$-R$ à direita. Se N é um submódulo$-R$ de M, dizemos que N é *parcela direta de* M se existir L submódulo$-R$ de M tal que $M = N \oplus_i L$.

Definição. Sejam M e P módulos$-R$ à direita. Um monomorfismo $\varphi : M \to P$ diz-se *cindível* se $\mathrm{Im}(\varphi)$ for parcela direta de P. Um epimorfismo $\psi : M \to P$ diz-se *cindível* se $\mathrm{Ker}(\psi)$ for parcela direta de M.

Observação. Observe-se que, se $\varphi : M \to P$ é um monomorfismo, então $\mathrm{Ker}(\varphi) = \{0\}$ e, portanto, $M = \mathrm{Ker}(\varphi) \oplus_i M$, pelo que $\mathrm{Ker}(\varphi)$ é parcela direta de M. Analogamente, se $\psi : M \to P$ é um epimorfismo, então $\mathrm{Im}(\psi) = P$ e, portanto, $P = \mathrm{Im}(\psi) \oplus_i \{0\}$, pelo que $\mathrm{Im}(\psi)$ é parcela direta de P.

Proposição. Sejam M, P e L módulos$-R$.

(1. Se $\varphi : M \to P$ é um morfismo$-R$, são equivalentes as seguintes afirmações:

   (a) φ é um monomorfismo$-R$ cindível.

   (b) Existe um morfismo$-R$ $\beta : P \to M$ tal que $\beta \circ \varphi = \mathrm{id}_M$.

2. Se $\psi : P \to L$ é um morfismo$-R$, são equivalentes as seguintes afirmações:

   (a) ψ é um epimorfismo$-R$ cindível.

   (b) Existe um morfismo$-R$ $\gamma : L \to P$ tal que $\psi \circ \gamma = \mathrm{id}_L$.

Demonstração.

1. Admitamos que φ é um monomorfismo$-R$ cindível. Por definição, existe P_1 submódulo$-R$ de P tal que
$$P = \mathrm{Im}(\varphi) \oplus_i P_1.$$
Seja $p \in P$. Então, existem um e um só $x \in \mathrm{Im}(\varphi)$ e um e um só $p_1 \in P_1$ tais que $p = x + p_1$. Como $x \in \mathrm{Im}(\varphi)$ e φ é um monomorfismo$-R$, existe um e um só $m \in M$ tal que $x = \varphi(m)$. Consideremos a aplicação
$$\begin{array}{rccc} \beta : & P & \to & M \\ & p & \mapsto & m \end{array},$$
onde $m \in M$ é tal que $p = \varphi(m) + p_1$. Verifiquemos que β está nas condições da afirmação (b).

   Sejam $p, p' \in P$ e $a \in R$. Então, $p = \varphi(m) + p_1$ e $p' = \varphi(m') + p'_1$, para alguns $m, m' \in M$ e $p_1, p'_1 \in P_1$. Temos que
$$\begin{aligned} \beta(p + p') &= \beta[(\varphi(m) + p_1) + (\varphi(m') + p'_1)] \\ &= \beta[\varphi(m + m') + (p_1 + p'_1)] \\ &= m + m' = \beta(p) + \beta(p') \end{aligned}$$

e

$$\begin{aligned}\beta(pa) &= \beta[(\varphi(m)+p_1)a] \\ &= \beta[\varphi(ma)+(p_1a)] \ , \\ &= ma = \beta(p)a\end{aligned}$$

pelo que β é um morfismo$-R$.

Vejamos, agora, se $\beta \circ \varphi = \mathrm{id}_M$. Dado $m \in M$,

$$(\beta \circ \varphi)(m) = \beta(\varphi(m)) = \beta[\varphi(m)+0] = m = \mathrm{id}_M(m),$$

pelo que $\beta \circ \varphi = \mathrm{id}_M$.

Reciprocamente, admitamos que existe um morfismo$-R$ β de P em M tal que $\beta \circ \varphi = \mathrm{id}_M$. Então, β é sobrejetiva e φ é injetiva e, portanto, φ é um monomorfismo$-R$. Mostremos que $P = \mathrm{Im}(\varphi) + \mathrm{Ker}(\beta)$.

Como $\mathrm{Im}(\varphi)$ e $\mathrm{Ker}(\beta)$ são submódulos$-R$ de P, temos que

$$\mathrm{Im}(\varphi) + \mathrm{Ker}(\beta) \leq_R P.$$

Dado $p \in P$, sabemos que $\beta(p) \in M$ e $(\varphi \circ \beta)(p) \in P$. Temos que

$$p = (\varphi \circ \beta)(p) + p - (\varphi \circ \beta)(p) = \varphi(\beta(p)) + [p - (\varphi \circ \beta)(p)].$$

É claro que $\varphi(\beta(p)) \in \mathrm{Im}(\varphi)$. Por outro lado, $p - (\varphi \circ \beta)(p) \in \mathrm{Ker}(\beta)$, uma vez que

$$\beta[p - (\varphi \circ \beta)(p)] = \beta(p) - (\beta \circ \varphi)(\beta(p)) = \beta(p) - \beta(p) = 0.$$

Logo, $P = \mathrm{Im}(\varphi) + \mathrm{Ker}(\beta)$.

Resta mostrar que $\mathrm{Im}(\varphi) \cap \mathrm{Ker}(\beta) = \{0\}$. Dado $x \in \mathrm{Im}(\varphi) \cap \mathrm{Ker}(\beta)$, existe $m \in M$ tal que $x = \varphi(m)$ e $\beta(x) = 0$. Ora,

$$0 = \beta(x) = \beta(\varphi(m)) = (\beta \circ \varphi)(m) = \mathrm{id}_M(m) = m,$$

pelo que $x = \varphi(m) = \varphi(0) = 0$.

Vimos, assim, que as condições [D$'_1$] e [D$'_2$] são satisfeitas e, portanto,

$$P = \mathrm{Im}(\varphi) \oplus_i \mathrm{Ker}(\beta).$$

Assim, φ é um monomorfismo$-R$ cindível.

2. [exercício] □

Definição. Sejam $\{N_i\}_{i\in\mathbb{Z}}$ uma família de módulos$-R$, $\{\alpha_i\}_{i\in\mathbb{Z}}$ uma família de morfismos$-R$, com $\alpha_i : N_i \to N_{i+1}$. Considere-se a sequência

$$\mathscr{S} \qquad \ldots \xrightarrow{\alpha_{i-2}} N_{i-1} \xrightarrow{\alpha_{i-1}} N_i \xrightarrow{\alpha_i} N_{i+1} \xrightarrow{\alpha_{i+1}} \ldots$$

1. $\mathscr{S}$ diz-se uma *sequência exata* se, para todo o $i \in \mathbb{Z}$, $\mathrm{Im}(\alpha_{i-1}) = \mathrm{Ker}(\alpha_i)$.

2. $\mathscr{S}$ diz-se uma *sequência exata cindível*, ou simplesmente *sequência cindível*, se for exata e, para todo o $i \in \mathbb{Z}$, $\mathrm{Im}(\alpha_{i-1}) = \mathrm{Ker}(\alpha_i)$ for parcela direta de N_i.

3. Uma *sequência exata curta* é uma sequência exata da forma

$$\{0\} \xrightarrow{\alpha} N \xrightarrow{f} M \xrightarrow{g} W \xrightarrow{\beta} \{0\}$$

Observemos que se $\mathscr{S}$ é uma sequência exata curta, então

$$\alpha: \begin{array}{ccc} \{0\} & \to & N \\ 0 & \mapsto & 0 \end{array}, \qquad \beta: \begin{array}{ccc} W & \to & \{0\} \\ w & \mapsto & 0 \end{array}.$$

Além disso, como $\mathrm{Im}(\alpha) = \mathrm{Ker}(f)$, temos que $\mathrm{Ker}(f) = \{0\}$ e, portanto, f é um monomorfismo$-R$. Por outro lado, como $\mathrm{Im}(g) = \mathrm{Ker}(\beta) = W$, temos que g é um epimorfismo$-R$. Pelo Teorema do Homomorfismo, $M/\mathrm{Ker}(g) \cong \mathrm{Im}(g)$. Ora, $\mathrm{Ker}(g) = \mathrm{Im}(f)$, $\mathrm{Im}(g) = W$ e $N \cong \mathrm{Im}(f)$. Logo,

$$M/N \cong W.$$

Proposição. Seja $\mathscr{S}$ a sequência $\{0\} \longrightarrow N \xrightarrow{f} M \xrightarrow{g} W \longrightarrow \{0\}$, onde M, N e W são módulos$-R$ e f e g são morfismos$-R$. Então, $\mathscr{S}$ é uma sequência curta exata se e só se f é um monomorfismo$-R$, g é um epimorfismo$-R$ e $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

Demonstração. [exercício]

Proposição. 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 equivalente 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.

Demonstração. [exercício Sugestão. Prove que $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$ e $(b) \Rightarrow (d) \Rightarrow (a)$.]

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, $\mathscr{S}$ é cindível se e só se $\mathrm{Im}(f) = \mathrm{Ker}(g)$ é parcela direta de M, ou seja, se e só se existe um submódulo$-R$ L de M tal que

$$M = \mathrm{Im}(f) \oplus_i L = \mathrm{Ker}(g) \oplus_i L.$$

Pelo Teorema do Homomorfismo,

$$M/N \cong W. \quad (\star)$$

Por outro lado, como $M = \mathrm{Ker}(g) \oplus_i L$, podemos considerar o epimorfismo$-R$

$$\begin{array}{rccc} p: & M = \mathrm{Ker}(g) \oplus_i L & \to & L \\ & k + \ell & \mapsto & \ell \end{array}$$

Novamente pelo Teorema do Homomorfismo, $M/\mathrm{Ker}(p) \cong \mathrm{Im}(p)$, ou seja, $M/\mathrm{Ker}(g) \cong L$. Como $\mathrm{Ker}(g) = \mathrm{Im}(f) \cong N$, temos que

$$M/N \cong L. \quad (\star\star)$$

Por $(\star)$ e $(\star\star)$, temos que $L \cong W$. Então,

$$\mathscr{S} \text{ é cindível se e só se } M \cong N \oplus_e W.$$

Proposição. Seja $\mathscr{S} \quad \{0\} \longrightarrow N \xrightarrow{f} M \xrightarrow{g} W \longrightarrow \{0\}$ uma sequência exata.

1. As seguintes condições são equivalentes:

   (a) $\mathscr{S}$ é cindível.

   (b) existe um morfismo$-R$ $f_0 : M \to N$ tal que $f_0 \circ f = \mathrm{id}_N$.

   (c) existe um morfismo$-R$ $g_0 : W \to M$ tal que $g \circ g_0 = \mathrm{id}_W$.

2. Se $\mathscr{S}$ for cindível, então existem morfismos$-R$ $f_0 : M \to N$ e $g_0 : W \to M$ tais que $f_0 \circ f = \mathrm{id}_N$ e $g \circ g_0 = \mathrm{id}_W$ e a sequência

   $$\mathscr{S}' \quad \{0\} \longrightarrow W \xrightarrow{g_0} M \xrightarrow{f_0} N \longrightarrow \{0\}$$

   seja exata cindível.

Demonstração.

1. Comecemos por mostrar que (a) é equivalente a (b). Sabemos que $\mathscr{S}$ é cindível se e só se f é um monomorfismo$-R$ cindível e tal é equivalente a dizer que existe $f_0 : M \to N$ morfismo$-R$ tal que $f_0 \circ f = \mathrm{id}_N$.

   Vejamos, agora, que (a) é equivalente a (c). Sabemos que $\mathscr{S}$ é cindível se e só se g é um epimorfismo$-R$ cindível. Ora, este facto é equivalente a dizer que existe $g_0 : W \to M$ morfismo$-R$ tal que $g \circ g_0 = \mathrm{id}_W$.

   Verificámos, assim, que as três condições dadas são equivalentes.

2. Admitamos que $\mathscr{S}$ é cindível. Por 1., existem morfismos$-R$ $f_0 : M \to N$ e $g_0 : W \to M$ tais que $f_0 \circ f = \mathrm{id}_N$ e $g \circ g_0 = \mathrm{id}_W$. Da primeira igualdade, concluímos que f_0 é sobrejetiva e, portanto, é um epimorfismo$-R$. Da segunda igualdade, concluímos que g_0 é injetiva e, assim, g_0 é um monomorfismo$-R$.

   Consideremos a sequência $\mathscr{S}' \quad \{0\} \longrightarrow W \xrightarrow{g_0} M \xrightarrow{f_0} N \longrightarrow \{0\}$. Pretendemos mostrar que

   $$\mathrm{Im}(g_0) = \mathrm{Ker}(f_0).$$

Como $\mathscr{S}$ é cindível, $\mathrm{Im}(f) = \mathrm{Ker}(g)$ é parcela direta de M. Então, existe M_1 submódulo$-R$ de M tal que $M = \mathrm{Im}(f) \oplus_i M_1 = \mathrm{Ker}(g) \oplus_i M_1$.

Para todo o $m \in M$, $f_0(m) = n$ onde $m = f(n) + m_1$. Por outro lado, dado $x \in W$, $g_0(x) = m_2$, onde $m_2 \in M_1$ é tal que $g(m_2) = x$.

Mostremos, pois, que $\mathrm{Im}(g_0) = \mathrm{Ker}(f_0)$. Dado $m \in \mathrm{Ker}(f_0)$, $f_0(m) = 0_N$ e, portanto, $m = f(0_N) + m_1 = 0_M + m_1 = m_1 \in M_1$. Assim, $m = g_0(g(m)) \in \mathrm{Im}(g_0)$, pelo que

$$\mathrm{Ker}(f_0) \subseteq \mathrm{Im}(g_0).$$

Reciprocamente, consideremos $m_2 \in \mathrm{Im}(g_0)$. Então, existe $y \in W$ tal que $g_0(y) = m_2$. Temos que

$$f_0(m_2) = f_0(g_0(y)) = f_0(0_M + g_0(y)) = 0_M,$$

uma vez que $g_0(y) \in M_1$. Portanto, $m \in \mathrm{Ker}(f_0)$ e, portanto,

$$\mathrm{Im}(g_0) \subseteq \mathrm{Ker}(f_0).$$

Logo, $\mathscr{S}'$ é uma sequência exata curta. Como existe um morfismo$-R$ $g : M \to W$ tal que $g \circ g_0 = \mathrm{id}_W$, $\mathscr{S}'$ é exata cindível por 1. □

Lema de Zassenhauss. Se N, P, Q e L são submódulos$-R$ de M tais que $N \subseteq P$ e $Q \subseteq L$, então

$$(N + (P \cap L))/(N + (P \cap Q)) \cong (Q + (P \cap L))/(Q + (N \cap L)).$$

Demonstração. Se $Q \subseteq L$, então $(P \cap Q) \subseteq (P \cap L)$, o que implica que $N + (P \cap L) = N + (P \cap L) + (P \cap Q)$. Pelo Teorema do Isomorfismo,

$$\begin{aligned}(N + (P \cap L))/(N + (P \cap Q)) &= [(P \cap L) + (N + (P \cap Q))]/(N + (P \cap Q)) \\ &\cong (P \cap L)/[(P \cap L) \cap (N + (P \cap Q)) \\ &= (P \cap L)/((P \cap L \cap N) + (P \cap Q)) \\ &= (P \cap L)/((N \cap L) + (P \cap Q))\end{aligned}.$$

De modo análogo, como $N \subseteq P$, temos que $N \cap L \subseteq P \cap L$ e, portanto, $Q + (P \cap L) = Q + (P \cap L) + (N \cap L)$. Logo,

$$\begin{aligned}(Q + (P \cap L))/(Q + (N \cap L)) &= [(P \cap L) + (Q + (N \cap L))]/(Q + (N \cap L)) \\ &\cong (P \cap L)/[(P \cap L) \cap (Q + (N \cap L)) \\ &= (P \cap L)/((P \cap L \cap Q) + (N \cap L)) \\ &= (P \cap L)/((N \cap L) + (P \cap Q))\end{aligned}.$$

Portanto,

$$(N + (P \cap L))/(N + (P \cap Q)) \cong (Q + (P \cap L))/(Q + (N \cap L)).$$

□

Definição.

1. Se existirem $N_0, N_1, \ldots, N_k$ submódulos$-R$ de M tais que

$$\mathscr{B} \quad \{0\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = M,$$

dizemos que $\mathscr{B}$ é uma *cadeia normal de submódulos$-R$ de M*. Dado $i \in \{1, \ldots, k\}$, a N_i/N_{i-1} chamamos o *$i-$ésimo fator da cadeia $\mathscr{B}$*.

2. Se existirem $L_0, L_1, \ldots, L_r$ submódulos$-R$ de M tais que

$$\mathscr{B} \quad \{0\} = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_r = M,$$

dizemos que a cadeia $\mathscr{B}$ tem *comprimento r*.

3. Sejam $\mathscr{B} \quad \{0\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = M$ e $\mathscr{C} \quad \{0\} = P_0 \subseteq P_1 \subseteq \cdots \subseteq P_t = M$ cadeias normais de submódulos$-R$ de M. Diz-se que as cadeias são *isomorfas*, e escreve-se $\mathscr{B} \cong \mathscr{C}$, se existir uma bijeção δ entre os conjuntos $I = \{1, \ldots, k\}$ e $J = \{1, \ldots, r\}$ tal que

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

4. A cadeia $\mathscr{C}$ diz-se um *refinamento* da cadeia $\mathscr{B}$ e $\mathscr{B}$ uma *subcadeia* de $\mathscr{C}$ se as cadeias forem iguais ou se a cadeia $\mathscr{B}$ se obtiver de $\mathscr{C}$ por omissão de alguns elementos da cadeia.

5. A cadeia $\mathscr{B} \quad \{0\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = M$ diz-se uma *série de composição de M* se, para todo o $i \in \{1, \ldots, k\}$, N_{i-1} for submódulo maximal de N_i (ou, equivalentemente, se N_i/N_{i-1} for módulo simples).

6. M diz-se um *módulo$-R$ de comprimento finito* se M for módulo nulo ou admitir uma série de composição.

Proposição. O isomorfismo de cadeias é uma relação de equivalência no conjunto das cadeias de M.

Demonstração. [exercício]

Exemplos.

1. Seja K um corpo e seja E um espaço vetorial sobre K, de base $(e_1, \ldots, e_n)$. Então,

$$\{0\} \subsetneq \langle e_1 \rangle \subsetneq \langle e_1, e_2 \rangle \subsetneq \cdots \subsetneq \langle e_1, \ldots, e_n \rangle = E.$$

Dado $j \in \{1, \ldots, n\}$, seja L submódulo$-K$ de E tal que $\langle e_1, \ldots, e_j \rangle \subseteq L \subseteq \langle e_1, \ldots, e_j, e_{j+1} \rangle$. Então, $\dim(L) \in \{j, j+1\}$. Mais, se $\dim(L) = j$, então $L = \langle e_1, \ldots, e_j \rangle$. Por outro lado, se $\dim(L) = j+1$, então $L = \langle e_1, \ldots, e_j, e_{j+1} \rangle$.

Portanto, a série considerada é uma série de composição.

2. Consideremos o anel $\mathbb{Z}$ e o módulo$-\mathbb{Z}$ $\mathbb{Z}_{\mathbb{Z}}$. Suponhamos que N é um submódulo$-\mathbb{Z}$ de $\mathbb{Z}_{\mathbb{Z}}$ tal que $\{0\} \subsetneq N \subsetneq \mathbb{Z}$. Então, N é um ideal de $\mathbb{Z}$. Ora, $\mathbb{Z}$ é domínio de ideais principais, pelo que existe $t \in \mathbb{Z}$ tal que $N = t\mathbb{Z}$. Como $N \neq \{0\}$ e $N \neq \mathbb{Z}$, temos que $t \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Temos, pois,

$$\{0\} \subsetneq t\mathbb{Z} \subsetneq \mathbb{Z}.$$

Mais,

$$\{0\} \subsetneq t^2\mathbb{Z} \subseteq t\mathbb{Z} \subsetneq \mathbb{Z}.$$

Suponhamos que $t^2\mathbb{Z} = t\mathbb{Z}$. Então, existe $a \in \mathbb{Z}$ tal que $t = t^2a$, pelo que $ta = 1$ e, portanto, $t = 1$ ou $t = -1$, o que contradiz a nossa hipótese. Assim,

$$\{0\} \subsetneq t^2\mathbb{Z} \subsetneq t\mathbb{Z} \subsetneq \mathbb{Z}.$$

De modo análogo, concluímos que

$$\{0\} \subsetneq t^4\mathbb{Z} \subsetneq t^2\mathbb{Z} \subsetneq t\mathbb{Z} \subsetneq \mathbb{Z}$$

e assim sucessivamente, pelo que $\mathbb{Z}$ não admite série de composição.

3. Consideremos o anel $\mathbb{Z}$ e o módulo$-\mathbb{Z}$ $\mathbb{Z}/6\mathbb{Z}$. As cadeias

$$\mathscr{B} \quad \{6\mathbb{Z}\} \subseteq 2\mathbb{Z}/6\mathbb{Z} \subseteq \mathbb{Z}/6\mathbb{Z}$$

e

$$\mathscr{C} \quad \{6\mathbb{Z}\} \subseteq 3\mathbb{Z}/6\mathbb{Z} \subseteq \mathbb{Z}/6\mathbb{Z}$$

são isomorfas.

Proposição. Sejam $\mathscr{B} \quad \{0\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = M$ 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 $\mathscr{B}$. Então, $\mathscr{C}$ é uma série de composição de M.

Demonstração. [exercício]

Teorema de Shreier. Quaisquer duas cadeias normais de submódulos$-R$ de M admitem refinamentos isomorfos.

Demonstração. Sejam

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

e

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

cadeias normais de submódulos$-R$ de M. Sejam $I = \{0, 1, \ldots, k\}$ e $J = \{0, 1, \ldots, t\}$.
Para cada $i \in I \setminus \{k\}$, consideremos

$$N_{i,j} = N_i + (N_{i+1} \cap P_j), \quad \text{para cada } j \in J.$$

De modo análogo, para cada $j \in J \setminus \{t\}$, consideremos

$$P_{i,j} = P_j + (P_{j+1} \cap N_i), \quad \text{para cada } i \in I.$$

Não é difícil de verificar que $N_{i,0} = N_i$, $N_{i,t} = N_{i+1}$, $N_{i,j} \subseteq N_{i,j+1}$, $P_{0,j} = P_j$, $P_{k,j} = P_{j+1}$ e $P_{i,j} \subseteq P_{i+1,j}$ [exercício].
Desta forma, obtemos os seguintes refinamentos:

$$\begin{aligned} \mathscr{B}^* \quad \{0\} = N_0 = N_{0,0} \subseteq N_{0,1} \subseteq \quad & N_{0,t} = N_1 = N_{1,0} \subseteq \cdots \subseteq N_{1,t} \subseteq \cdots \subseteq \\ & \subseteq N_{k-1} = N_{k-1,0} \subseteq N_{k-1,1} \subseteq \cdots \subseteq N_{k-1,t} = N_k = M \end{aligned}$$

e

$$\begin{aligned} \mathscr{C}^* \quad \{0\} = P_0 = P_{0,0} \subseteq P_{1,0} \subseteq \quad & P_{k,0} = P_1 = P_{0,1} \subseteq \cdots \subseteq P_{k,1} \subseteq \cdots \subseteq \\ & \subseteq P_{t-1} = P_{0,t-1} \subseteq P_{1,t-1} \subseteq \cdots \subseteq P_{k,t-1} = P_t = M. \end{aligned}$$

Em cada cadeia, temos $kt + 1$ submódulos$-R$ de M. Mais, pelo Lema de Zassenhauss,

$$N_{i,j+1}/N_{i,j} = (N_i + (N_{i+1} \cap P_{j+1}))/(N_i + (N_{i+1} \cap P_j)) \cong (P_j + (N_{i+1} \cap P_{j+1}))/(P_j + (N_i \cap P_{j+1})) = P_{i+1,j}/P_{i,j}.$$

□

Teorema de Jordan-Hölder. Seja M um módulo$-R$ não nulo e de comprimento finito. Então,

(a) Toda a cadeia normal de M do tipo

$$\mathscr{D} \quad \{0\} = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_r = M$$

admite um refinamento que é uma série de composição.

(b) Quaisquer duas séries de composição são isomorfas.

Demonstração. [exercício]

Definição. Seja M um módulo$-R$ de comprimento finito. Se M for não nulo, dá-se o nome de *comprimento de* M, e representa-se por $\mathscr{L}(M)$, ao comprimento de qualquer uma das séries de composição de M.
Se $M = \{0\}$, então consideramos $\mathscr{L}(M) = 0$.

Proposição. Seja N um submódulo$-R$ de M. Então,

(a) M é módulo$-R$ de comprimento finito se e só se N e M/N forem módulos de comprimento finito.

(b) Se M for um módulo$-R$ de comprimento finito, então $\mathscr{L}(M) = \mathscr{L}(N) + \mathscr{L}(M/N)$.

Demonstração. Sabemos que $\{0\} \subseteq N \subseteq M$.

Se $N = \{0\}$, então $M/N = M/\{0\} \cong M$ e, portanto, $\mathscr{L}(M) = \mathscr{L}(M/N) = 0 + \mathscr{L}(M/N) = \mathscr{L}(N) + \mathscr{L}(M/N)$.

Se $N = M$, então $M/N = M/M = \{M\}$, pelo que $\mathscr{L}(M/N) = 0$ e

$$\mathscr{L}(M) = \mathscr{L}(N) = \mathscr{L}(N) + 0 = \mathscr{L}(N) + \mathscr{L}(M/N).$$

Se $M = \{0\}$, então $\mathscr{L}(M) = \mathscr{L}(N) = \mathscr{L}(M/N) = 0$.

Resta, pois, provar o resultado para quando temos a cadeia $\mathscr{B} \quad \{0\} \subsetneq N \subsetneq M$. Comecemos por demonstrar 1. Nesse sentido, admitamos que M é módulo$-R$ de comprimento finito. Como M é não nulo, pelo Teorema de Jordan-Hölder, a cadeia $\mathscr{B}$ admite um refinamento que é série de composição de M, digamos

$$\mathscr{B}^* \quad \{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = N \subsetneq N_{k+1} \subsetneq \cdots \subsetneq N_{k+r} = M.$$

Ora, a cadeia $\mathscr{C} \quad \{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = N$ é série de composição de N. Logo, N é módulo$-R$ de comprimento finito e $\mathscr{L}(N) = k$.
Consideremos, agora, a cadeia de M/N

$$\mathscr{D} \quad \{N\} = N/N = N_k/N \subsetneq N_{k+1}/N \subsetneq \cdots \subsetneq N_{k+r}/N = M/N.$$

Sabemos que, para todo o $i \in \{1, \ldots, r\}$,

$$(N_{k+i}/N)/(N_{k+i-1}/N) \cong N_{k+i}/N_{k+i-1}.$$

Como N_{k+i}/N_{k+i-1} é um módulo$-R$ simples, também $(N_{k+i}/N)/(N_{k+i-1}/N)$ o é. Logo, N_{k+i-1}/N é submódulo$-R$ maximal de N_{k+i}/N e $\mathscr{D}$ é série de composição de M/N. Logo, M/N é módulo$-R$ de comprimento finito e $\mathscr{L}(M/N) = r$.

Reciprocamente, suponhamos que N e M/N são módulos$-R$ de comprimento finito. Sejam

$$\mathscr{C} \quad \{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = N$$

uma série de composição de N e

$$\mathscr{D} \quad \{N\} = \overline{P_0} \subsetneq \overline{P_1} \subsetneq \cdots \subsetneq \overline{P_r} = M/N$$

uma série de composição de M/N. Então, para todo o $j \in \{0, \ldots, r\}$, existe P_j submódulo$-R$ de M tal que

$$\overline{P_j} = P_j/N.$$

Consideremos a cadeia

$$\mathscr{B} \quad \{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = N = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r = M.$$

Sabemos que N_i/N_{i-1} é módulo$-R$ simples, para todo o $i \in \{1, \ldots, k\}$. Como

$$P_j/P_{j-1} \cong (P_j/N)/(P_{j-1}/N) = \overline{P_j}/\overline{P_{j-1}}$$

e $\overline{P_j}/\overline{P_{j-1}}$ é um módulo$-R$ simples, para todo o $j \in \{1, \ldots, r\}$, podemos concluir que $\mathscr{B}$ é série de composição de M e M tem comprimento finito. Mais,

$$\mathscr{L}(M) = k + r = \mathscr{L}(N) + \mathscr{L}(M/N).$$

□

Corolário. Seja M um módulo$-R$ de comprimento finito.

(a) Se M' for isomorfo a M, então M' é de comprimento finito e $\mathscr{L}(M') = \mathscr{L}(M)$.

(b) Se N e P forem submódulos$-R$ de M tais que $N \subseteq P$ e $\mathscr{L}(N) = \mathscr{L}(P)$, então $N = P$.

Demonstração. [exercício]

Sejam M um módulo$-R$ não nulo e de comprimento finito. Suponhamos que N é submódulo$-R$ de M e P é submódulo maximal de N. A cadeia

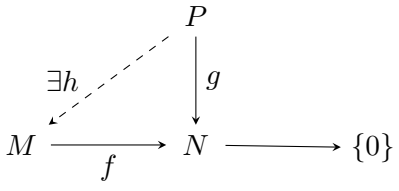
$$\{0\} \subseteq P \subsetneq N \subseteq M$$

admite um refinamento que é série de composição de M. Um dos fatores da cadeia é N/P. Como todas as séries de composição são isomorfas, N/P é, a menos de um isomorfismo, fator de todas as séries de composição de M.

1.4. Módulos projetivos

No que se segue, R é um anel não nulo e unitário e todos os módulos$-R$ são unitários.

Definição. Um módulo$-R$ P diz-se um *módulo projetivo* se, para todos os módulos$-R$ M e N, todo o morfismo$-R$ $g : P \to N$ e todo o epimorfismo$-R$ $f : M \to N$, existe um morfismo$-R$ $h : P \to M$ tal que $f \circ h = g$.



Observemos que $f : M \to N$ é um epimorfismo se e só se a sequência $M \xrightarrow{f} N \xrightarrow{\varphi_0} \{0\}$ é exata, ou seja, $\mathrm{Im}(f) = \mathrm{Ker}(\varphi_0) = N$

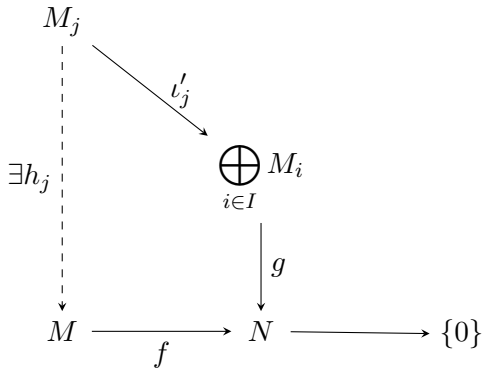
Exemplo. O módulo R_R é um módulo projetivo. De facto, se M e N forem módulos$-R$, $g : P \to N$ um morfismo$-R$ e $f : M \to N$ um epimorfismo$-R$, então, como R é unitário, $1 \in R$ e $g(1) \in N$, e, assim, existe $m \in M$ tal que $f(m) = g(1)$. Se considerarmos a correspondência

$$\begin{array}{rccc} h: & R_R & \longrightarrow & M, \\ & r & \longmapsto & mr \end{array}$$

facilmente verificamos que h é um morfismo$-R$ tal que $f \circ h = g$. [exercício]

Proposição. Seja $\{M_i\}_{i\in I}$ uma família de módulos$-R$. Então, $\bigoplus_{i\in I} M_i$ é um módulo projetivo se e só se M_i é um módulo projetivo, para todo o $i \in I$.

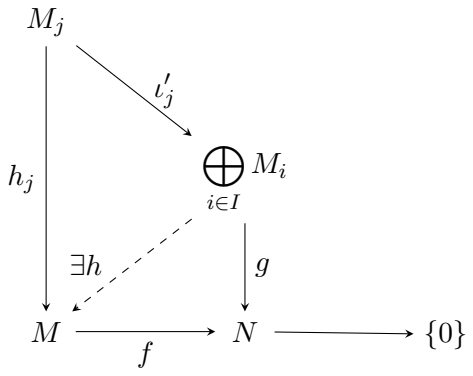
Demonstração. Admitamos que, para cada $i \in I$, M_i é um módulo projetivo. Sejam M, N módulos, $g : \bigoplus_{i\in I} M_i \to N$ um morfismo$-R$ e $f : M \to N$ um epimorfismo$-R$. Dado $j \in I$, $\iota'_j : M_j \to \bigoplus_{i\in I} M_i$ é um morfismo$-R$. Logo, $g \circ \iota'_j : M_j \to N$ é um morfismo$-R$.
Como M_j é um módulo projetivo, existe $h_j : M_j \to M$ morfismo$-R$ tal que $f \circ h_j = g \circ \iota'_j$.



Pela Propriedade Universal da Soma Direta, existe um e um só morfismo$-R$ $h : \bigoplus_{i\in I} M_i \to M$ tal que

$$h \circ \iota'_j = h_j,$$

para todo o $j \in I$.

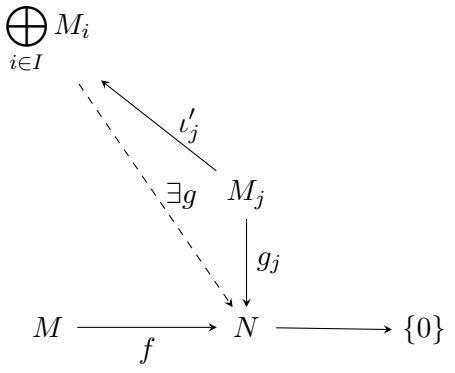


Em seguida verificamos que $f \circ h = g$.
Ora, dado $x \in \bigoplus_{i\in I} M_i$, $x = (x_i)_{i\in I} = \sum_{j\in I} \iota'_j(x_j)$. Logo,

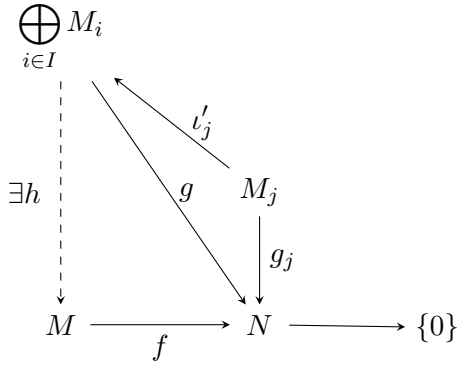
$$\begin{aligned}(f \circ h)(x) &= (f \circ h)\left(\sum_{j\in I} \iota'_j(x_j)\right) = f\left[h\left(\sum_{j\in I} \iota'_j(x_j)\right)\right] \\ &= f\left(\sum_{j\in I}(h \circ \iota'_j)(x_j)\right) = f\left(\sum_{j\in I} h_j(x_j)\right) \\ &= \sum_{j\in I}(f \circ h_j)(x_j) = \sum_{j\in I}(g \circ \iota'_j)(x_j) \\ &= g\left(\sum_{j\in I} \iota'_j(x_j)\right) = g(x).\end{aligned}$$

Por definição, $\bigoplus_{i\in I} M_i$ é um módulo projetivo.

Admitamos, agora, que $\bigoplus_{i\in I} M_i$ é módulo projetivo. Pretendemos mostrar que, dado $j \in I$, M_j é módulo projetivo. Consideremos, pois, M e N módulos$-R$, $g_j : M_j \to N$ um morfismo$-R$ e $f : M \to N$ epimorfismo$-R$.
Temos que $\iota'_j : M_j \to \bigoplus_{i\in I} M_i$ e $g_j : M_j \to N$ são morfismos$-R$, para todo o $j \in I$. Pela Propriedade Universal da Soma Direta, existe um morfismo $g : \bigoplus_{i\in I} M_i \to M$ tal que $g \circ \iota'_j = g_j$.



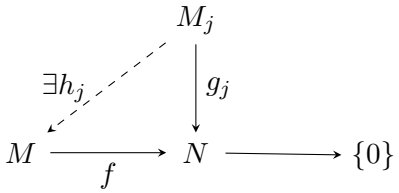
Como $\bigoplus_{i\in I} M_i$ é um módulo projetivo, existe um morfismo $h : \bigoplus_{i\in I} M_i \to M$ tal que $f \circ h = g$.



Consideremos $h_j : M_j \to M$ tal que $h_j = h \circ \iota'_j$. Como h_j é a composição de dois morfimos$-R$, h_j é um morfismo$-R$. Dado $x_j \in M_j$,

$$(f \circ h_j)(x_j) = f[h_j(x_j)] = f\{h[\iota'_j(x_j)]\} = (f \circ h)[\iota'_j(x_j)] = (g \circ \iota'_j)(x_j) = g_j(x_j).$$

Assim, h_j é um morfismo$-R$ tal que $f \circ h_j = g_j$.



Portanto, M_j é módulo projetivo. □

Proposição. Todo o módulo$-R$ isomorfo a um módulo projetivo é também um módulo projetivo.

Demonstração. [exercício]

Proposição. Todo o módulo$-R$ livre é projetivo.

Demonstração. [exercício]

Corolário. Todo o módulo$-R$ (unitário) é imagem epimorfa de um módulo projetivo.

Demonstração. [exercício]

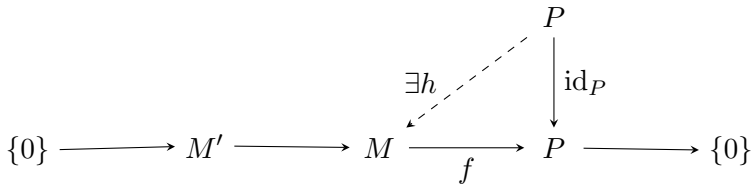
Teorema. Seja P um módulo$-R$. Então, são equivalentes as seguintes condições:

(a) P é módulo projetivo.

(b) Toda a sequência exata $\{0\} \longrightarrow M' \longrightarrow M \xrightarrow{f} P \longrightarrow \{0\}$ é cindível.

(c) P é isomorfo a uma parcela direta dum módulo$-R$ livre.

Demonstração. Comecemos por mostrar que (a) implica (b). Consideremos a sequência exata $\{0\} \longrightarrow M' \longrightarrow M \xrightarrow{f} P \longrightarrow \{0\}$. Como M e P são módulos$-R$, a aplicação $\mathrm{id}_P : P \to P$ é um morfismo$-R$ e $f : M \to P$ é um epimorfismo$-R$, sabemos que existe $h : P \to M$ morfismo$-R$ tal que $f \circ h = \mathrm{id}_P$ (uma vez que P é módulo projetivo).



Logo, f é epimorfismo cindível e, portanto, a sequência é cindível.

Mostremos, agora, que (b) implica (c). Uma vez que P é um módulo$-R$ unitário, sabemos que P é imagem epimorfa de um módulo$-R$ livre. Assim, existem um módulo$-R$ livre L e um epimorfismo$-R$ $g : L \to P$.
Consideremos a sequência

$$\{0\} \longrightarrow \mathrm{Ker}(g) \xrightarrow{\iota} L \xrightarrow{g} P \longrightarrow \{0\}.$$

Como ι é um monomorfismo$-R$, g é um epimorfismo$-R$ e $\mathrm{Im}(\iota) = \mathrm{Ker}(g)$, a sequência é exata. Por hipótese, a sequência é cindível. Logo,

$$L \cong \mathrm{Ker}(g) \oplus P.$$

Vimos, portanto, que P é isomorfo a uma parcela direta de um módulo$-R$ livre.

Finalmente, vejamos que (c) implica (a). Suponhamos, pois, que existem L módulo$-R$ livre e M e N submódulos$-R$ de L tais que $L = M \oplus_i N$ e $P \cong M$.
Como L é um módulo$-R$ livre, L é módulo projetivo e, portanto, os seus submódulos$-R$ M e N são também módulos projetivos. Sendo P isomorfo a M, podemos concluir que P é módulo projetivo. □

Proposição. Seja P um módulo$-R$. Então, P é módulo projetivo se e só se P é isomorfo a uma parcela direta de todo o módulo do qual é módulo quociente.

Demonstração. Admitamos que P é módulo projetivo. Sejam M um módulo$-R$ e N um submódulo$-R$ de M tais que $P \cong M/N$. Dado um isomorfismo$-R$ $\varphi : M/N \to P$, consideremos a sequência

$$\{0\} \longrightarrow N \xrightarrow{\iota} M \xrightarrow{f} P \longrightarrow \{0\},$$

onde $f : M \to P$ é definida por $f(x) = \varphi(x + N)$ para todo o $x \in M$ e ι é a inclusão.
É claro que ι é um monomorfismo$-R$ e, como φ é um isomorfismo, f é um morfismo$-R$. Mais, para todo o $p \in P$, existe $x \in M$ tal que $p = \varphi(x + N) = f(x)$ e, portanto, f é um epimorfismo$-R$.

Vejamos que $\mathrm{Im}(\iota) = \mathrm{Ker}(f)$. Dado $\iota(n) \in \mathrm{Im}(\iota)$, com $n \in N$,

$$f(\iota(n)) = f(n) = \varphi(n + N) = \varphi(N) = 0_P,$$

pelo que $\iota(n) \in \mathrm{Ker}(f)$. Por outro lado, se $x \in \mathrm{Ker}(f)$, então

$$f(x) = 0 \Leftrightarrow \varphi(x + N) = 0 \Leftrightarrow x + N \in \mathrm{Ker}(\varphi).$$

Como φ é um monomorfismo$-R$, $x + N = N$ e, portanto, $x \in N$. Logo, $x = \iota(x) \in \mathrm{Im}(\iota)$.

Vimos, portanto, que a sequência

$$\{0\} \longrightarrow N \xrightarrow{\iota} M \xrightarrow{f} P \longrightarrow \{0\},$$

é exata. Como P é um módulo projetivo, a sequência é cindível. Logo,

$$M \cong N \oplus P.$$

Reciprocamente, admitamos que P é isomorfo a uma parcela direta de todo o módulo do qual é módulo quociente. Sabemos que P é imagem epimorfa de um módulo$-R$ livre. Logo, existe L módulo$-R$ livre e $\varphi : L \to P$ epimorfismo$-R$. Temos que

$$P \cong L/\mathrm{Ker}(\varphi).$$

Por hipótese, P é isomorfo a uma parcela direta de L, módulo$-R$ livre. Pela proposição anterior, P é módulo projetivo. □

Definição. Seja M um módulo$-R$.

1. Diz-se que uma família $\{x_i\}_{i\in I}$ de elementos de M é uma *família de suporte finito* se o conjunto dos $i \in I$ tais que $x_i \neq 0$ for finito.

2. Designa-se por *forma linear sobre* M todo o elemento de $M^* = \mathrm{Hom}_R(M, R_R)$.

Proposição. Sejam P um módulo$-R$ e $X = \{x_i\}_{i\in I}$ uma família de geradores de P. São equivalentes as seguintes condições:

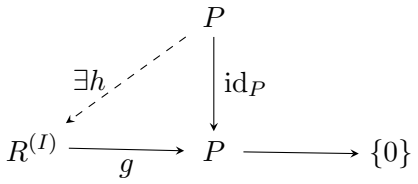
(a) P é projetivo.

(b) existe uma família $\{f_i\}$ de formas lineares sobre P tal que, para todo o $x \in P$, a família $\{f_i(x)\}_{i\in I}$ é de suporte finito e $x = \sum_{i\in I} x_i f_i(x)$.

Demonstração. Admitamos que P é projetivo. O módulo $R^{(I)}$ é um módulo$-R$ livre de base $Y = \{e_i\}_{i\in I}$. Consideremos a aplicação inclusão de Y em $R^{(I)}$, $\iota : Y \to R^{(I)}$, e a aplicação $f : Y \to P$ definida por $f(e_i) = x_i$ para todo o $i \in I$. Então, existe um e um só morfismo$-R$ $g : R^{(I)} \to P$ tal que $g|_Y = f$, definido por

$$g(\sum_{i\in I} e_i r_i) = \sum_{i\in I} f(e_i) r_i.$$

Mais, g é um epimorfismo$-R$.
Como P é projetivo, existe $h : P \to R^{(I)}$ morfismo$-R$ tal que $g \circ h = \mathrm{id}_P$.



Para cada $j \in I$, consideremos $p'_j : R^{(I)} \to R$ e $f_j = p'_j \circ h$.
Prova-se que $\{f_i\}_{i\in I}$ é uma família de formas lineares sobre P. Mais, para todo o $x \in P$, $\{f_i(x)\}_{i\in I}$ é de suporte finito e $x = \sum_{i\in I} x_i f_i(x)$. [exercício]

Reciprocamente, admitamos que existe uma família $\{f_i\}_{i\in I}$ de formas lineares sobre P tal que, para todo o $x \in P$, a família $\{f_i(x)\}_{i\in I}$ é de suporte finito e $x = \sum_{i\in I} x_i f_i(x)$. Consideremos a sequência

$$\{0\} \longrightarrow \mathrm{Ker}(g) \xrightarrow{\iota} R^{(I)} \xrightarrow{g} P \longrightarrow \{0\}.$$

A aplicação $h : P \to R^{(I)}$, definida por $h(x) = \sum_{i\in I} e_i f_i(x)$, onde $x = \sum_{i\in I} x_i f_i(x)$, é um morfismo$-R$. Não é difícil de verificar que $g \circ h = \mathrm{id}_P$. [exercício]. Logo, g é um epimorfismo$-R$ cindível e a sequência é cindível. Portanto,

$$R^{(I)} \cong \mathrm{Ker}(g) \oplus P.$$

Como $R^{(I)}$ é um módulo$-R$ livre, P é um módulo projetivo. □

Proposição. Sejam M um módulo$-R$ e $M^* = \mathrm{Hom}_R(M, R_R)$. Dados $f, g \in M^*$ e $r \in R$, definimos $f + g, rf \in M^*$ por

$$(f+g)(x) = f(x) + g(x), \qquad (rf)(x) = rf(x).$$

Então, $(M^*, +)$ é um grupo abeliano e M^* é um módulo$-R$ à esquerda.

Demonstração. [exercício]

Observemos que, dada uma forma linear $f \in M^* = \mathrm{Hom}(M, R_R)$, $\mathrm{Im}(f)$ é um submódulo$-R$ de R_R. Logo, $\sum_{f\in M^*} \mathrm{Im}(f)$ é um submódulo$-R$ de R_R ou, equivalentemente, $\sum_{f\in M^*} \mathrm{Im}(f)$ é um ideal direito de R.
Prova-se que $\sum_{f\in M^*} \mathrm{Im}(f)$ é, de facto, um ideal de R. [exercício]

Definição. A $\sum_{f\in M^*} \mathrm{Im}(f)$ dá-se o nome de *ideal traço de* M e representa-se por $t(M)$.

Proposição. Seja P um módulo$-R$ projetivo. Então,

(a) $P\,t(P) = P$.

(b) $t(P)^2 = t(P)$.

Demonstração.

(a) Como $t(P)$ é um ideal de R, temos que $t(P) \subseteq R$. Sendo P é um módulo$-R$, concluímos que $P\,t(P) \subseteq P$. Vejamos que $P \subseteq P\,t(P)$.

Seja $x \in P$. Como P é projetivo, existe uma família de formas lineares $\{f_i\}_{i\in I}$ de P tal que $\{f_i(x)\}_{i\in I}$ é de suporte finito e

$$x = \sum_{i\in I} x_i f_i(x),$$

onde $\{x_i\}$ é uma família de geradores de P.

Para todo o $i \in I$, $x_i \in P$ e $f_i(x) \in \mathrm{Im}(f_i) \subseteq t(P)$. Mais, $f_i(x)$ são quase todos nulos e, portanto, $x \in P\,t(P)$.

(b) Uma vez que $t(P)$ é ideal de R e $t(P) \subseteq R$, podemos concluir que

$$t(P)^2 = t(P)\,t(P) \subseteq t(P).$$

Consideremos, agora, $x \in t(P)$. Então,

$$x \in \sum_{f\in P^*} \mathrm{Im}(f),$$

ou seja,

$$x = \sum_{f\in P^*} f(y_j),$$

com $f(y_j) \in \mathrm{Im}(f)$, para todo o $f \in P^*$, tais que $f(y_j)$ são quase todos nulos.

Por definição, para cada $f \in P^*$, temos que $y_j \in P$. Ora, P é projetivo e, assim,

$$y_j = \sum_{i\in I} x_i f_i(y_j).$$

Logo,

$$x = \sum_{f\in P^*} f\left(\sum_{i\in I} x_i f_i(y_j)\right) = \sum_{f\in P^*}\sum_{i\in I} f(x_i) f_i(y_j) \in t(P)t(P) = t(P^2).$$

□

Observemos que, pelo resultado anterior, para todo o $n \in \mathbb{N}$,

$$P\,t(P)^n = P.$$

No que se segue, R é um domínio de integridade comutativo e com identidade e K é o corpo de frações de R.

Se S é um anel e R é um subanel de S, então S é um módulo$-R$, uma vez que, dados $x \in S$ e $r \in R$, $xr \in S$. Ora, a correspondência

$$\begin{array}{rccc} f: & R & \to & K \\ & x & \mapsto & \dfrac{x}{1} \end{array}$$

é um monomorfismo$-R$ e R é um subanel de K. Logo, K é um módulo$-R$.

Definição. Seja I um submódulo$-R$ de K. Define-se

$$I^{-1} = \{x \in K : xI \subseteq R\}.$$

Proposição. Seja I um submódulo$-R$ de K. Então, I^{-1} é submódulo$-R$ de K.

Demonstração. [exercício]

Por definição de I^{-1}, podemos afirmar que $I^{-1}I \subseteq R$.

Definição. Seja I um submódulo$-R$ de K. Dizemos que I é *invertível* se $I^{-1}I = R$.

Exemplo. O anel dos inteiros $\mathbb{Z}$ é um domínio de integridade comutativo e com identidade e $\mathbb{Q}$ é o corpo das frações de $\mathbb{Z}$. Consideremos

$$I = \left\{ \frac{a}{2} : a \in \mathbb{Z} \right\}.$$

Facilmente se verifica que I é um submódulo$-\mathbb{Z}$ de $\mathbb{Q}$ e que $I^{-1} = 2\mathbb{Z}$. Mais, $I^{-1}I = \mathbb{Z}$. Logo, I é submódulo$-\mathbb{Z}$ de $\mathbb{Q}$ invertível. [exercício]

Lema. Seja I um submódulo$-R$ de K. Então, são equivalentes as seguintes condições:

(a) I é invertível.

(b) Existem elementos $n \in \mathbb{N}$, $q_j \in K$, $a_j \in I$, com $1 \leq j \leq n$, tais que

(i) $q_j I \subseteq R$, para todo o $j \in \{1, \ldots, n\}$;

(ii) $\displaystyle\sum_{j=1}^{n} q_j a_j = 1$.

Demonstração. Admitamos que I é invertível. Então, $I^{-1}I = R$ e, portanto, $1 \in I^{-1}I$. Logo, existem $n \in \mathbb{N}$, $q_1, \ldots, q_n \in I^{-1}$, $a_1, \ldots, a_n \in I$ tais que

$$1 = \sum_{j=1}^{n} q_j a_j.$$

Dado $j \in \{1, \ldots, n\}$, como $q_j \in I^{-1}$, temos, por definição, que $q_j I \subseteq R$.

Suponhamos, agora, que existem $n \in \mathbb{N}$, $q_j \in K$, $a_j \in I$, com $1 \leq j \leq n$, tais que

(i) $q_j I \subseteq R$, para todo o $j \in \{1, \ldots, n\}$;

(ii) $\sum_{j=1}^{n} q_j a_j = 1$.

Por definição de I^{-1}, $I^{-1}I \subseteq R$. Seja $r \in R$. Então,

$$r = 1.r = \left(\sum_{j=1}^{n} q_j a_j\right) r = \sum_{j=1}^{n} (q_j a_j) r = \sum_{j=1}^{n} q_j (a_j r).$$

Como I é submódulo$-R$ de K, $a_j \in I$, para todo o j, e $r \in R$, podemos concluir que $a_j r \in R$, para todo o j. Assim, $r = \sum_{j=1}^{n} q_j (a_j r)$, com $q_j \in I^{-1}$ e $a_j r \in I$, pelo que $r \in I^{-1}I$. Portanto, $I^{-1}I = R$ e I é submódulo$-R$ invertível de K. □

Proposição. Todo o submódulo$-R$ de K que seja invertível é do tipo finito.

Demonstração. [exercício]
sugestão: mostre que se I é invertível e $1 = \sum_{j=1}^{n} q_j a_j$, então $I = \langle a_1, \ldots, a_n \rangle$.

Proposição. Seja I um submódulo$-R$ não nulo de K. Então, são equivalentes as seguintes condições:

(a) I é módulo$-R$ projetivo.

(b) I é invertível.

Demonstração. Admitamos que I é módulo$-R$ projetivo e seja $X = \{x_\alpha\}_{\alpha \in L}$ uma família de geradores de I. Por hipótese, existe uma família de formas lineares sobre I, $\{f_\alpha\}_{\alpha \in L}$, tal que, para todo o $x \in I$, $\{f_\alpha(x)\}$ é de suporte finito e

$$x = \sum_{\alpha \in L} x_\alpha f_\alpha(x).$$

Assim, dados $x, y \in I \setminus \{0\}$,

$$\frac{f_\alpha(x)}{x}, \frac{f_\alpha(y)}{y} \in K.$$

Como $I \subseteq K$, $x = \frac{a}{b}$, $y = \frac{c}{d}$, com $a, b, c, d \in R$ todos não nulos. Portanto,

$$f_\alpha(x)y = f_\alpha\left(\frac{a}{b}\right)\frac{c}{d} = f_\alpha\left(\frac{ad}{bd}\right)\frac{c}{d} = f_\alpha\left(\frac{ac}{bd}\right)\frac{b}{b} = f_\alpha\left(\frac{bc}{bd}\right)\frac{a}{b} = f_\alpha\left(\frac{c}{d}\right)\frac{a}{b} = f_\alpha(y)x.$$

Logo,

$$\frac{f_\alpha(x)}{x} = \frac{f_\alpha(y)}{y}, \qquad \text{para quaisquer } x, y \in I \setminus \{0\}.$$

Como $x \in I \setminus \{0\}$,

$$x = \sum_{\alpha \in L} x_\alpha f_\alpha(x) = \left(\sum_{\alpha \in L} x_\alpha \frac{f_\alpha(x)}{x} \right) x.$$

Uma vez que $x \neq 0$ e K é corpo, podemos concluir que

$$1 = \sum_{\alpha \in L} x_\alpha \frac{f_\alpha(x)}{x}.$$

Resta-nos provar que $\frac{f_\alpha(x)}{x} I \subseteq R$, para todo o $\alpha \in L$. Dado $y \in I$, se $y = 0$, então $\frac{f_\alpha(x)}{x} y = \frac{f_\alpha(x)}{x}.0 = 0 \in R$. Se $y \neq 0$, então

$$\frac{f_\alpha(x)}{x}.y = \frac{f_\alpha(y)}{y}.y = f_\alpha(y) \in R.$$

Assim, I é invertível.

Admitamos, agora, que I é invertível. Então, existem $n \in \mathbb{N}$, $q_j \in K$, $a_j \in I$, com $1 \leq j \leq n$, tais que

(i) $q_j I \subseteq R$, para todo o $j \in \{1, \ldots, n\}$;

(ii) $\sum_{j=1}^{n} q_j a_j = 1$.

Como já observámos, $I = \langle a_1, \ldots, a_n \rangle$. Definamos, para cada $j \in \{1, \ldots, n\}$, a correspondência

$$\begin{array}{rccc} f_j : & I & \to & R_R \\ & x & \mapsto & q_j x. \end{array}$$

Facilmente se verifica que $f_j \in \mathrm{Hom}(I, R_R) = I^*$, para todo o j [exercício]. Mais, dado $x \in I$,

$$x = 1.x = (\sum_{j=1}^{n} q_j a_j)x = \sum_{j=1}^{n} a_j (q_j x) = \sum_{j=1}^{n} a_j f_j(x).$$

Logo, I é projetivo. □

No que se segue, R é um anel unitário e os módulos$-R$ são módulos$-R$ à direita unitários.

Definição. Sejam P, M módulos$-R$.

1. Dizemos que P é um *módulo gerador de M* (ou um *gerador de M*) se

$$M = \sum_{f \in \mathrm{Hom}_R(P,M)} \mathrm{Im}(f).$$

2. Dizemos que P é *módulo gerador* se for módulo gerador de todos os módulos$-R$.

Proposição. Sejam P, M módulos. Então, P é módulo gerador de M se e só se existir um conjunto não vazio $I \subseteq \mathrm{Hom}_R(P, M)$ tal que

$$M = \sum_{f \in I} \mathrm{Im}(f).$$

Demonstração. [exercício]

Definição. Sejam P, M módulos$-R$. Dizemos que P é *gerador finito de* M se existir um conjunto finito não vazio $I \subseteq \mathrm{Hom}_R(P, M)$ tal que $M = \sum_{f \in I} \mathrm{Im}(f)$.

Exemplos.

1. Se M é imagem epimorfa de P, então P é gerador finito de M. De facto, se M é imagem epimorfa de P, então existe um epimorfismo$-R$ $\varphi : P \to M$. Por definição, $\varphi \in \mathrm{Hom}_R(P, M)$. Logo,

$$M = \mathrm{Im}(\varphi) = \sum_{f \in I} \mathrm{Im}(f), \text{ com } I = \{\varphi\}.$$

2. R_R é módulo gerador. Para mostrar este facto, consideremos M módulo$-R$. Dado $m \in M$, definimos a correspondência

$$\begin{array}{rccc} f_m : & R & \longrightarrow & M \\ & a & \longmapsto & ma \end{array}$$

   Facilmente se verifica que f_m é um morfismo$-R$, para todo o $m \in M$ [exercício]. Vejamos que

$$M = \sum_{m \in M} \mathrm{Im}(f_m).$$

   Para todo o $n \in M$, $n = n.1 = f_n(1) \in \mathrm{Im}(f_n) \subseteq \sum_{m \in M} \mathrm{Im}(f_m)$.

   Dado $m \in M$, $f_m \in \mathrm{Hom}_R(R, M)$ e, portanto, $\mathrm{Im}(f_m)$ é um submódulo$-R$ à direita de M. Logo, $\sum_{m \in M} \mathrm{Im}(f_m) \subseteq M$.

   Assim, $M = \sum_{m \in M} \mathrm{Im}(f_m)$ e R_R é um módulo gerador de M.

Lema. Seja P um módulo$-R$. Então, são equivalentes as seguintes condições:

(a) P é módulo gerador.

(b) Para todo o módulo$-R$ não nulo M e todo o submódulo próprio N de M, existe $g \in \mathrm{Hom}_R(P, M)$ tal que $\mathrm{Im}(g) \not\subseteq N$.

Demonstração. Admitamos que P é módulo gerador. Sejam M um módulo$-R$ não nulo e N um submódulo próprio de M. Como P é gerador de M,

$$M = \sum_{f \in \mathrm{Hom}_R(P,M)} \mathrm{Im}(f).$$

Suponhamos que, para todo o $g \in \mathrm{Hom}_R(P, M)$,

$$\mathrm{Im}(g) \subseteq N.$$

Como $N \leq_R M$, $\sum_{g \in \mathrm{Hom}_R(P,M)} \mathrm{Im}(g) \subseteq N$. Logo,

$$M = \sum_{f \in \mathrm{Hom}_R(P,M)} \mathrm{Im}(f) \subseteq N,$$

o que contradiz o facto de N ser submódulo próprio.
Portanto, existe $g \in \mathrm{Hom}_R(P, M)$ tal que $\mathrm{Im}(g) \not\subseteq N$.

Reciprocamente, admitamos que, para todo o módulo$-R$ não nulo M e todo o submódulo próprio N de M, existe $g \in \mathrm{Hom}_R(P, M)$ tal que $\mathrm{Im}(g) \not\subseteq N$.
Seja T um módulo$-R$. Pretendemos mostrar que P é um módulo gerador de T.

Se $T = \{0\}$, então $f_0 : P \to T$, $x \mapsto 0_T$, é um morfismo$-R$. Além disso, $\mathrm{Im}(f_0) = \{0_T\} = T$, pelo que P é um módulo gerador de T.

Admitamos, agora, que $T \neq \{0\}$. Dado $f \in \mathrm{Hom}_R(P, T)$, $\mathrm{Im}(f) \leq_R T$ e, portanto,

$$\sum_{f \in \mathrm{Hom}_R(P,T)} \mathrm{Im}(f) \subseteq T.$$

Se $\sum_{f \in \mathrm{Hom}_R(P,T)} \mathrm{Im}(f) \subsetneq T$, então $\sum_{f \in \mathrm{Hom}_R(P,T)} \mathrm{Im}(f)$ é um submódulo próprio de T. Por hipótese, existe $g \in \mathrm{Hom}_R(P, T)$ tal que

$$\mathrm{Im}(g) \not\subseteq \sum_{f \in \mathrm{Hom}_R(P,T)} \mathrm{Im}(f),$$

o que é um absurdo.
Logo,

$$\sum_{f \in \mathrm{Hom}_R(P,T)} \mathrm{Im}(f) = T$$

e P é um módulo gerador de T.
Portanto, P é um módulo gerador de todo o módulo$-R$, pelo que P é módulo gerador. □

Corolário. Seja P um módulo$-R$. Então, P é módulo gerador se e só se, para todos os módulos M e M' e todo o $f \in \mathrm{Hom}_R(M, M') \setminus \{f_0\}$, existir $g \in \mathrm{Hom}_R(P, M)$ tal que

$$f \circ g \in \mathrm{Hom}_R(P, M') \setminus \{f_0\}.$$

Demonstração. Admitamos que P é módulo gerador. Sejam M, M' módulos$-R$ e seja $f \in \mathrm{Hom}_R(M, M') \setminus \{f_0\}$. Como $f \neq f_0$, existe $x \in M$ tal que $f(x) \neq 0$. Logo,

$$\mathrm{Ker}(f) \subsetneq M.$$

Ora, M é módulo$-R$ e $\mathrm{Ker}(f)$ é um submódulo próprio de M. Sendo P um módulo gerador, pelo lema anterior, existe $g \in \mathrm{Hom}_R(P, M)$ tal que

$$\mathrm{Im}(g) \not\subseteq \mathrm{Ker}(f).$$

Assim, existe $x \in \mathrm{Im}(g)$ tal que $x \notin \mathrm{Ker}(f)$. Como $x \in \mathrm{Im}(g)$, existe $y \in P$ tal que $x = g(y)$. Uma vez que $x \notin \mathrm{Ker}(f)$, sabemos que $(f \circ g)(y) = f(g(y)) = f(x) \neq 0$. Logo, existe $y \in P$ tal que $(f \circ g)(y) \neq 0$, pelo que $f \circ g \neq f_0$.

É claro que, se $f \in \mathrm{Hom}_R(M, M')$ e $g \in \mathrm{Hom}_R(P, M)$, então

$$f \circ g \in \mathrm{Hom}_R(P, M').$$

Admitamos, agora, que para todos os módulos M e M' e todo o $f \in \mathrm{Hom}_R(M, M') \setminus \{f_0\}$, existe $g \in \mathrm{Hom}_R(P, M)$ tal que $f \circ g \in \mathrm{Hom}_R(P, M') \setminus \{f_0\}$.

Sejam M um módulo$-R$ não nulo e N um submódulo próprio de M. Consideremos

$$\pi_N : \quad M \quad \longrightarrow \quad M/N.$$

Então, M e M/N são módulos$-R$ e $\pi_N \in \mathrm{Hom}_R(M, M/N)$. Como N é submódulo próprio de M, existe $x \in M \setminus N$. Logo, $x + N \neq N$ e, portanto, $\pi_N(x) \neq N$. Assim,

$$\pi_N \neq f_0.$$

Por hipótese, existe $g \in \mathrm{Hom}_R(P, M)$ tal que $\pi_N \circ g \in \mathrm{Hom}_R(P, M/N) \setminus \{f_0\}$. Como $\pi_N \circ g \neq f_0$, existe $y \in P$ tal que $(\pi_N \circ g)(y) \neq 0_{M/N}$, ou seja,

$$g(y) + N \neq N.$$

Portanto, $g(y) \notin N$, pelo que $\mathrm{Im}(g) \not\subseteq N$ (pois $g(y) \in \mathrm{Im}(g)$ e $g(y) \notin N$). Pelo Lema anterior, P é módulo gerador. □

Proposição. Seja P um módulo$-R$. Então, são equivalentes as seguintes condições:

(a) P é módulo gerador.

(b) Existem $n \in \mathbb{N}$, $p_1, \ldots, p_n \in P$ e $f_1, \ldots, f_n \in P^*$ tais que

$$1 = \sum_{i=1}^{n} f_i(p_i).$$

Demonstração. Iremos demonstrar que (b) é condição suficiente para (a). A implicação contrária fica como exercício.

Admitamos que existem $n \in \mathbb{N}$, $p_1, \ldots, p_n \in P$ e $f_1, \ldots, f_n \in P^*$ tais que $1 = \sum_{i=1}^{n} f_i(p_i)$.

Seja M um módulo$-R$. Pretendemos mostrar que P é um módulo gerador de M. Ora, dado $x \in M$,

$$x = x.1 = x\left(\sum_{i=1}^{n} f_i(p_i)\right) = \sum_{i=1}^{n} x f_i(p_i).$$

Consideremos, pois, para cada $i \in \{1, \ldots, n\}$, a correspondência

$$\begin{array}{rccc} g_{x,i}: & P & \longrightarrow & M \\ & p & \longmapsto & x f_i(p). \end{array}$$

Não é difícil de verificar que $g_{x,i}$ é um morfismo$-R$. De facto, dados $p, q \in P$ e $a \in R$,

$$g_{x,i}(p+q) = x f_i(p+q) = x[f_i(p) + f_i(q)] = x f_i(p) + x f_i(q) = g_{x,i}(p) + g_{x,i}(q)$$

e

$$g_{x,i}(pa) = x f_i(pa) = x[f_i(p)a] = [x f_i(p)]a = g_{x,i}(p)a.$$

Portanto, $g_{x,i} \in \mathrm{Hom}_R(P, M)$ para todo o $i \in \{1, \ldots, n\}$.

Assim, dado $x \in M$,

$$x = \sum_{i=1}^{n} x f_i(p_i) = \sum_{i=1}^{n} g_{x,i}(p_i) \in \sum_{i=1}^{n} \mathrm{Im}(g_{x,i}).$$

Portanto, $M \subseteq \sum_{f \in \mathrm{Hom}_R(P,M)} \mathrm{Im}(f)$. Como $\sum_{f \in \mathrm{Hom}_R(P,M)} \mathrm{Im}(f)$ é um submódulo$-R$ de M, podemos concluir que

$$M = \sum_{f \in \mathrm{Hom}_R(P,M)} \mathrm{Im}(f).$$

Assim, P é um módulo gerador de M e, por definição, P é módulo gerador. □

Definição. Seja M um módulo$-R$. Diz-se que M é *livre de torção* se

$$\forall m \in M \setminus \{0\},\ \forall a \in R \setminus \{0\},\ ma \neq 0.$$

Proposição. Todo o módulo não nulo e livre de torção é módulo fiel.

Demonstração. [exercício]

Exemplo. O conjunto $\mathbb{Z}_6$ é um módulo$-\mathbb{Z}_6$. É fácil de verificar que $\mathbb{Z}_6$ não é livre de torção: de facto, $\bar{3}, \bar{2} \in \mathbb{Z}_6 \setminus \{\bar{0}\}$ mas $\bar{3} \cdot \bar{2} = \bar{0}$. No entanto, $\mathbb{Z}_6$ é um módulo fiel, uma vez que, dado $\bar{a} \in \mathrm{an}(\mathbb{Z}_6)$, temos que $\bar{b} \cdot \bar{a} = \bar{0}$, para todo o $\bar{b} \in \mathbb{Z}_6$ e, em particular, $\bar{1} \cdot \bar{a} = \bar{0}$, pelo que $\bar{a} = \bar{0}$. Assim, $\mathrm{an}(\mathbb{Z}_6) = \{\bar{0}\}$ e $\mathbb{Z}_6$ é um módulo fiel.

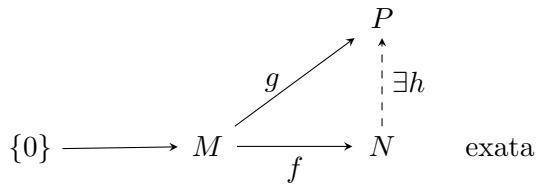
Proposição. Todo o módulo gerador é módulo fiel.

Demonstração. [exercício]

1.5. Módulos injetivos

No que se segue, R é um anel unitário e todos os módulos$-R$ são unitários.

Definição. Seja P um módulo$-R$. Dizemos que P é um *módulo injetivo* se, para todos os módulos$-R$ M e N, todo o morfismo$-R$ $g : M \to P$ e todo o monomorfismo$-R$ $f : M \to N$, existir um morfismo$-R$ $h : N \to P$ tal que $h \circ f = g$.



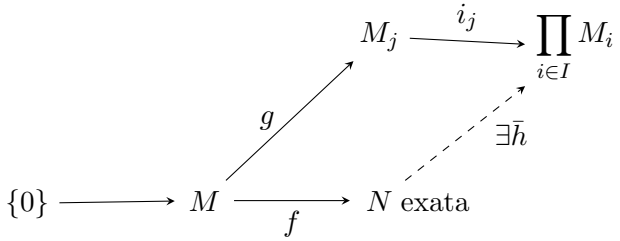
Proposição. Seja $\{M_i\}_{i\in I}$ uma família de módulos$-R$. Então, $\prod_{i\in I} M_i$ é injetivo se e só se cada M_i é injetivo.

Demonstração. A verificação de que $\prod_{i\in I} M_i$ é injetivo sempre que cada M_i o for fica como exercício.

Admitamos que $\prod_{i\in I} M_i$ é injetivo e consideremos $j \in I$. Para mostrar que M_j é injetivo, tomemos M, N módulos$-R$, $g : M \to M_j$ morfismo$-R$ e $f : M \to N$ monomorfismo$-R$.
A correspondência

$$\begin{array}{rccc} i_j : & M_j & \longrightarrow & \prod_{i\in I} M_i \\ & x_j & \longmapsto & (y_i)_{i\in I}, \end{array}$$

onde $y_i = \begin{cases} x_j, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}$, é um monomorfismo$-R$. Como g é um morfismo$-R$, concluímos que $i_j \circ g$ é um morfismo$-R$. Assim, temos M, N módulos$-R$, $i_j \circ g : M \to \prod_{i\in I} M_i$ morfismo$-R$ e $f : M \to N$ monomorfismo$-R$.



Por hipótese, existe um morfismo$-R$ $\bar{h} : N \to \prod_{i\in I} M_i$ tal que $\bar{h} \circ f = i_j \circ g$.
Consideremos a correspondência $h : N \to M_j$ definida por

$$h(x) = (p_j \circ \bar{h})(x),$$

para todo o $x \in N$.
Como h é uma composição de morfismos$-R$, h é um morfismo$-R$. Dado $y \in M$,

$$\begin{aligned}(h \circ f)(y) &= h[f(y)] = (p_j \circ \bar{h})[f(y)] \\ &= p_j[(\bar{h} \circ f)(y)] = p_j[(i_j \circ g)(y)] \\ &= (p_j \circ i_j)[g(y)] = g(y)\end{aligned}$$

Logo, $h \circ f = g$ e, por definição, M_j é um módulo injetivo. □

Corolário. Seja $\{M_i\}_{i\in F}$ uma família de módulos$-R$, com F finito. Então, $\bigoplus_{i\in F} M_i$ é injetivo se e só se cada M_i o for.

Corolário. Toda a parcela direta de um módulo injetivo é módulo injetivo.

Proposição. Todo o módulo isomorfo a um módulo injetivo é um módulo injetivo.

Demonstração. [exercício]

Proposição. Seja $\{M_i\}_{i\in I}$ uma família de módulos$-R$ tais que $\bigoplus_{i\in I} M_i$ é módulo injetivo. Então, M_j também é módulo injetivo para todo o $j \in I$.

Demonstração. Seja $j \in I$. Como

$$\bigoplus_{i\in I} M_i \cong M_j \oplus \left(\bigoplus_{i\in I\setminus\{j\}} M_i \right),$$

concluímos que $M_j \oplus \left(\bigoplus_{i\in I\setminus\{j\}} M_i \right)$ é um módulo injetivo, pelo que tanto M_j como $\bigoplus_{i\in I\setminus\{j\}} M_i$ são módulos injetivos.

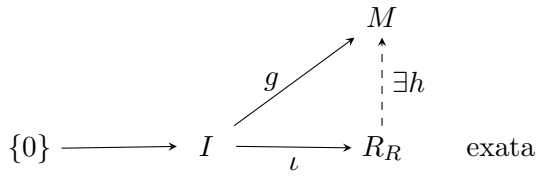
Assim, para todo o $j \in I$, M_j é um módulo injetivo. □

Teorema [Critério de Baer]. Seja M um módulo$-R$. Então, são equivalentes as seguintes condições:

(i) M é um módulo injetivo.

(ii) Para todo o ideal direito I de R e todo o morfismo$-R$ $g : I \to M$, existe $x \in M$ tal que $g(a) = xa$ para todo o $a \in I$.

Demonstração. Admitamos que M é um módulo injetivo. Sejam I um ideal direito de R e $g : I \to M$ um morfismo$-R$. Como I é um ideal direito de R, I é um submódulo$-R$ de R_R. A inclusão $\iota : I \to R_R$ é um monomorfismo$-R$.

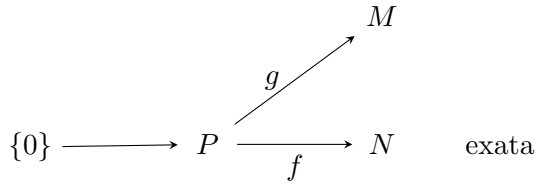


Como M é injetivo, existe um morfismo$-R$ $h : R_R \to M$ tal que $h \circ \iota = g$. Uma vez que $1 \in R_R$, $h(1) \in M$. Seja $x = h(1)$. Então, para todo o $a \in I$,

$$g(a) = (h \circ \iota)(a) = h[\iota(a)] = h(a) = h(1 \cdot a) = h(1) \cdot a = xa,$$

como pretendíamos mostrar.

Suponhamos, agora, que para todo o ideal direito I de R e todo o morfismo$-R$ $g : I \to M$, existe $x \in M$ tal que $g(a) = xa$ para todo o $a \in I$.
Sejam P, N módulos$-R$, $g : P \to M$ um morfismo$-R$ e $f : P \to N$ um monomorfismo$-R$.



Consideremos

$$\mathcal{F} = \{(N_i, h_i) : f(P) \leq_R N_i \leq_R N,\ h_i \in \mathrm{Hom}_R(N_i, M),\ h_i \circ f = g\}.$$

Comecemos por mostrar que $\mathcal{F} \neq \emptyset$. Para tal, consideremos a correspondência

$$\begin{array}{rccc} \varphi : & f(P) & \longrightarrow & M \\ & f(p) & \longmapsto & g(p) \end{array}.$$

Então, $f(P) \leq_R N$, $\varphi \in \mathrm{Hom}_R(f(P), M)$ e $\varphi \circ f = g$ [exercício]. Logo,

$$(f(P), \varphi) \in \mathcal{F},$$

pelo que $\mathcal{F} \neq \emptyset$.

Consideremos a relação binária $\leq$ definida em $\mathcal{F}$ por

$$(N_i, h_i) \leq (N_j, h_j) \ \text{ se e só se } \ N_i \leq_R N_j \ \text{ e } \ h_j|_{N_i} = h_i.$$

Iremos mostrar que $\leq$ é uma relação de ordem parcial em $\mathcal{F}$.

(i) É claro que, para todo o $(N_i, h_i) \in \mathcal{F}$, $N_i \leq_R N_i$ e $h_i|_{N_i} = h_i$, pelo que $\leq$ é reflexiva.

(ii) Sejam $(N_i, h_i), (N_j, h_j) \in \mathcal{F}$ tais que $(N_i, h_i) \leq_R (N_j, h_j)$ e $(N_j, h_j) \leq_R (N_i, h_i)$. Então, $N_i \leq_R N_j$ e $N_j \leq_R N_i$, donde podemos concluir que $N_i \subseteq N_j$ e $N_j \subseteq N_i$, ou seja, $N_i = N_j$. Como $h_j|_{N_i} = h_i$, temos que

$$h_j = h_j|_{N_j} = h_j|_{N_i} = h_i.$$

Portanto, $(N_i, h_i) = (N_j, h_j)$ e $\leq$ é antissimétrica.

(iii) Sejam $(N_i, h_i), (N_j, h_j), (N_k, h_k) \in \mathcal{F}$ tais que $(N_i, h_i) \leq_R (N_j, h_j)$ e $(N_j, h_j) \leq_R (N_k, h_k)$. Então,

$$\begin{array}{lll} N_i \leq_R N_j & \text{e} & h_j|_{N_i} = h_i \\ N_j \leq_R N_k & \text{e} & h_k|_{N_j} = h_j. \end{array}$$

Logo, $N_i \leq_R N_k$ e, como $N_i \subseteq N_j$,

$$h_k|_{N_i} = \left(h_k|_{N_j}\right)|_{N_i} = h_j|_{N_i} = h_i.$$

Assim, $(N_i, h_i) \leq (N_k, h_k)$ e $\leq$ é transitiva

Por (i)–(iii), $(\mathcal{F}, \leq)$ é um conjunto parcialmente ordenado. Vejamos que toda a cadeia não vazia de $\mathcal{F}$ admite majorante. Para tal, consideremos uma cadeia $\mathcal{C}$ não vazia de $\mathcal{F}$ e seja

$$Q = \bigcup_{(N_i, h_i) \in \mathcal{C}} N_i.$$

Então, Q é um submódulo$-R$ de N. Definamos $h \in \mathrm{Hom}_R(Q, M)$ tal que

$$h|_{N_i} = h_i.$$

Por definição, $(Q, h) \in \mathcal{F}$ e, para todo o $(N_i, h_i) \in \mathcal{C}$, $(N_i, h_i) \leq (Q, h)$. Logo, (Q, h) é um majorante de $\mathcal{C}$.

Vimos, então, que toda a cadeia não vazia de $\mathcal{F}$ admite majorante. Pelo Lema de Zorn, $\mathcal{F}$ admite elemento maximal. Seja (N_1, h_1) um elemento maximal de $\mathcal{F}$. Mostremos que $N_1 = N$.

Por definição de $\mathcal{F}$, $N_1 \subseteq N$. Seja $x \in N$ e definamos $I = \{a \in R : xa \in N_1\}$. Não é difícil de verificar que I é um ideal direito de R. Consideremos a correspondência

$$\begin{array}{rccc} \gamma : & I & \longrightarrow & M \\ & a & \longmapsto & h_1(xa) \end{array}.$$

Verifiquemos que γ é um morfismo$-R$. Dados $a, b \in I$ e $r \in R$,

$$\gamma(a + b) = h_1[x(a + b)] = h_1(xa + xb) = h_1(xa) + h_1(xb) = \gamma(a) + \gamma(b)$$

e

$$\gamma(ar) = h_1[x(ar)] = h_1[(xa)r] = h_1(xa) \cdot r = \gamma(a) \cdot r.$$

Logo, γ é um morfismo$-R$ e, por hipótese, existe $y \in M$ tal que

$$\gamma(a) = ya,$$

para todo o $a \in I$.
Temos que $N_1 \leq_R N_1 + xR \leq_R N$ e $f(P) \leq_R N_1$. Logo,

$$f(P) \leq_R N_1 + xR.$$

Consideremos a correspondência

$$\begin{array}{rccc} h' : & N_1 + xR & \longrightarrow & M \\ & n + xb & \longmapsto & h_1(n) + yb. \end{array}$$

Comecemos por verificar que h' está bem definida. Suponhamos que $n + xb = n' + xb'$.

$$n + xb = n' + xb' \Leftrightarrow n - n' = x(b' - b).$$

Ora, como $n - n' \in N_1$ e $b' - b \in R$, podemos concluir que $b' - b \in I$. Por definição,

$$\gamma(b' - b) = h_1[x(b' - b)] = h_1(n - n') = h_1(n) - h_1(n').$$

Por outro lado,

$$\gamma(b' - b) = y(b' - b) = yb' - yb.$$

Portanto, $h_1(n) - h_1(n') = yb' - yb$, pelo que $h_1(n) + yb = h_1(n') + yb'$, ou seja,

$$h'(n + xb) = h'(n' + xb')$$

e h' é uma função de $N_1 + xR$ em M.
Facilmente se verifica que h_1 é um morfismo$-R$ [exercício].
Para mostrar que $h' \circ f = g$, tomemos $p \in P$. Então, $f(p) \in f(P) \subseteq N_1$ e

$$(h' \circ f)(p) = h'[f(p)] = h'[f(p) + x \cdot 0] = h_1[f(p)] + y \cdot 0 = (h_1 \circ f)(p) = g(p),$$

pelo que $h' \circ f = g$. Assim,

$$(N_1 + xR, h') \in \mathcal{F}.$$

Dado $n \in N_1$,

$$h'(n) = h'(n + x \cdot 0) = h_1(n) + y \cdot 0 = h_1(n),$$

donde

$$h'|_{N_1} = h_1.$$

Como $N_1 \leq_R N$ e $h'|_{N_1} = h_1$,

$$(N_1, h_1) \leq (N_1 + xR, h').$$

Mas (N_1, h_1) é elemento maximal de $\mathcal{F}$ e, portanto, $N_1 = N_1 + xR$. Logo, $N \subseteq N_1$.

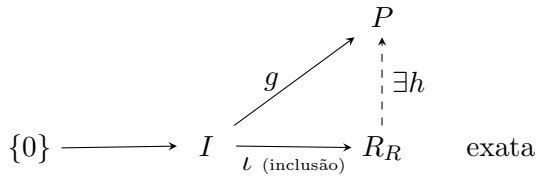
Portanto, $(N, h_1) \in \mathcal{F}$ e existe um morfismo$-R$ $h_1 : N \to M$ tal que $h_1 \circ f = g$. □

Corolário. Seja P um módulo$-R$. Então, são equivalentes as seguintes condições:

(a) P é módulo injetivo.

(b) Para todo o ideal direito I de R e todo o morfismo$-R$ $g : I \to P$, existe um morfismo$-R$ $h : R \to P$ tal que $h \circ \iota = g$, onde $\iota : I \to R$ é a inclusão.

Demonstração. Admitamos que P é módulo injetivo. Sejam I um ideal direito de R e $g : I \to P$ um morfismo$-R$. Sabemos que R_R é módulo$-R$ e I é submódulo$-R$ de R_R.



Como P é injetivo, existe um morfismo$-R$ $h : R_R \to P$ tal que $h \circ \iota = g$.

Reciprocamente, admitamos que, para todo o ideal direito I de R e todo o morfismo$-R$ $g : I \to P$, existe um morfismo$-R$ $h : R \to P$ tal que $h \circ \iota = g$.
Então, dados um ideal direito I de R e um morfismo$-R$ $g : I \to P$, existe um morfismo$-R$ $h : R \to P$ tal que $h \circ \iota = g$. Como $1 \in R$, $h(1) \in P$. Seja $x = h(1)$. Para todo o $a \in I$,

$$g(a) = (h \circ \iota)(a) = h[\iota(a)] = h(a) = h(1 \cdot a) = h(1) \cdot a = xa.$$

Vimos, então, que existe $x \in P$ tal que $g(a) = xa$ para todo o $a \in I$. Pelo Critério de Baer, P é módulo injetivo. □

Definição. Sejam R um domínio de integridade comutativo e com identidade e M um módulo$-R$. Dizemos que M é um *módulo$-R$ divisível* se, para todo o $r \in R \setminus \{0\}$, se tiver $Mr = M$, isto é,

$$\forall x \in M,\ \forall r \in R \setminus \{0\},\ \exists y \in M :\ x = yr.$$

Exemplo. Consideremos o grupo abeliano $(\mathbb{Q}, +)$. Então, $\mathbb{Q}$ é módulo$-\mathbb{Z}$ à esquerda. Mais,

$$\forall \frac{p}{q} \in \mathbb{Q},\ \forall r \in \mathbb{Z} \setminus \{0\},\ \frac{p}{q} = \frac{p}{qr} r,\ \text{com}\ \frac{p}{qr} \in \mathbb{Q}.$$

Logo, $\mathbb{Q}$ é módulo$-\mathbb{Z}$ divisível.

Proposição. Seja R um domínio de integridade comutativo. Então,

(a) Todo o módulo quociente de um módulo$-R$ divisível é módulo$-R$ divisível.

(b) A soma direta de módulos$-R$ divisíveis é um módulo$-R$ divisível.

Demonstração. [exercício]

Proposição. Sejam R um domínio de integridade comutativo e M um módulo livre de torção. Se M é divisível, então M é injetivo.

Demonstração. Admitamos que M é divisível. Sejam I um ideal direito de R e $g : I \to M$ um morfismo$-R$.
Se $g = \varphi_0$, então, para todo o $a \in I$,

$$g(a) = 0_M = 0_M \cdot a.$$

Logo, existe $x = 0_M \in M$ tal que $g(a) = xa$ para todo o $a \in I$.

Admitamos, agora, que $g \neq \varphi_0$. Então, existe $b \in I$ tal que $g(b) \neq 0_M$. Como g é morfismo$-R$, podemos concluir que $b \neq 0_R$. Ora, M é divisível e $g(b) \in M$, $b \in R \setminus \{0\}$. Logo, existe $y \in M$ tal que $g(b) = yb$.
Seja $a \in I$. Pretendemos mostrar que $g(a) = ya$. Como R é comutativo, $ab = ba$ e, portanto,

$$g(a)b = g(ab) = g(ba) = g(b)a = (yb)a = y(ba) = y(ab) = (ya)b.$$

Assim, $g(a)b - (ya)b = 0_M$, ou seja, $[g(a) - ya]b = 0_M$. Uma vez que M é livre de torção e $b \neq 0_R$, temos que $g(a) - ya = 0_M$, isto é,

$$g(a) = ya.$$

Assim, existe $y \in M$ tal que $g(a) = ya$ para todo o $a \in I$.

Pelo Critério de Baer, M é injetivo. □

Proposição. Sejam R um domínio de integridade comutativo e com identidade e K o corpo de frações de R. Então, todo o espaço vetorial sobre K é um módulo$-R$ injetivo.

Demonstração. [exercício]

Proposição. Seja R um domínio de ideais principais. Então um módulo$-R$ é injetivo se e só se for divisível.

Demonstração. Seja M um módulo$-R$.
Admitamos que M é um módulo injetivo. Dados $m \in M$ e $r \in R \setminus \{0\}$, rR é ideal direito de R. Consideremos a correspondência

$$\begin{array}{rccc} f: & rR & \longrightarrow & M \\ & rs & \longmapsto & ms \end{array}$$

Comecemos por mostrar que f é uma aplicação. Dado $x \in rR$, existe $s \in R$ tal que $x = rs$. Sendo M um módulo$-R$, $ms \in M$. Logo, $f(x) = f(rs) = ms \in M$.
Se $rs, rs' \in rR$ são tais que $rs = rs'$, então $rs - rs' = 0$, ou seja, $r(s - s') = 0$. Como R é um domínio de integridade e $r \neq 0$, $s - s' = 0$, isto é, $s = s'$. Logo,

$$f(rs) = ms = ms' = f(rs').$$

Vejamos, agora, que f é um morfismo$-R$. Sejam $rs, rs' \in rR$ e $a \in R$. Então,

$$f(rs + rs') = f[r(s + s')] = m(s + s') = ms + ms' = f(rs) + f(rs')$$

e

$$f[(rs)a] = f[r(sa)] = m(sa) = (ms)a = f(rs)a.$$

Ora, rR é ideal direito de R e $f : rR \to M$ é um morfismo$-R$. Como M é injetivo, existe $x \in M$ tal que $f(rs) = x(rs)$ para todo o $rs \in rR$. Em particular, como $1 \in R$ e $r = r \cdot 1$, temos que

$$m = m \cdot 1 = f(r \cdot 1) = x(r \cdot 1) = xr.$$

Vimos, pois, que, dados $m \in M$ e $r \in R \setminus \{0\}$, existe $x \in M$ tal que $m = xr$. Portanto, M é divisível.

Admitamos, agora, que M é um módulo$-R$ divisível. Sejam I um ideal direito de R e $g : I \to M$ um morfismo$-R$.
Como R é comutativo e I é um ideal direito de R, podemos concluir que I é um ideal de R. Além disso, sendo R um domínio de ideais principais, existe $x \in I$ tal que $I = xR$.
Se $I = \{0_R\}$, então $g(0_R) = 0_M = 0_M \cdot 0_R$. Suponhamos, então, que $I \neq \{0_R\}$. Como $I = xR$, temos que $x \neq 0_R$. Sendo M divisível e $g(x) \in M$, $x \in R \setminus \{0\}$, existe $y \in M$ tal que $g(x) = yx$.
Ora, dado $a \in I$, existe $r \in R$ tal que $a = xr$ e, portanto,

$$g(a) = g(xr) = g(x)r = (yx)r = y(xr) = ya.$$

Assim, existe $y \in M$ tal que $g(a) = ya$ para todo o $a \in I$ e, pelo Critério de Baer, M é injetivo. □

Se D é um grupo abeliano aditivo, então D é um módulo$-\mathbb{Z}$. Um anel R é também um módulo$-\mathbb{Z}$. Assim, faz sentido falar do grupo abeliano aditivo $\mathrm{Hom}_{\mathbb{Z}}(R, D)$. Este grupo é, de facto, um módulo$-R$ à direita e à esquerda, se considerarmos as seguintes ações: dados $f \in \mathrm{Hom}_{\mathbb{Z}}(R, D)$ e $r \in R$, definimos fr e rf em $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ por

$$fr : \begin{array}{ccc} R & \longrightarrow & D \\ s & \longmapsto & f(rs) \end{array}, \qquad rf : \begin{array}{ccc} R & \longrightarrow & D \\ s & \longmapsto & f(sr) \end{array}$$

Lema. Sejam R um anel e D um módulo$-\mathbb{Z}$ divisível. Então, $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ é módulo$-R$ à direita injetivo.

Demonstração. Sejam I um ideal direito de R e $f : I \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ um morfismo$-R$. Pretendemos mostrar que existe $g \in \mathrm{Hom}_{\mathbb{Z}}(R, D)$ tal que $f(a) = ga$ para todo o $a \in I$.
Consideremos a correspondência

$$\overline{f} : \begin{array}{ccc} I & \longrightarrow & D \\ a & \longmapsto & f(a)(1) \end{array}$$

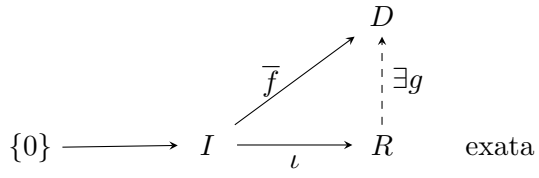
Dados $a, b \in I$, se $a = b$ então $f(a) = f(b)$ e, portanto, $f(a)(1) = f(b)(1)$. Logo, $\overline{f}$ está bem definida.
Vejamos que $\overline{f}$ é um morfismo$-\mathbb{Z}$. Sejam $a, b \in I$ e $n \in \mathbb{Z}$. Então,

$$\overline{f}(a + b) = f(a + b)(1) = (f(a) + f(b))(1) = f(a)(1) + f(b)(1) = \overline{f}(a) + \overline{f}(b)$$

e

$$\overline{f}(na) = f(na)(1) = [nf(a)](1) = n \cdot f(a)(1) = n\overline{f}(a).$$

Logo, $\overline{f} \in \mathrm{Hom}_{\mathbb{Z}}(I, D)$.
Como D é divisível e $\mathbb{Z}$ é um domínio de ideais principais, D é um módulo injetivo. Por definição, existe um morfismo$-\mathbb{Z}$ $g : R \to D$ tal que $g \circ \iota = \overline{f}$.



Em seguida, mostramos que $f(a) = ga$ para todo o $a \in I$. Sejam $a \in I$ e $r \in R$. Então,

$$f(a)(r) = f(a)(r \cdot 1) = (f(a) \cdot r)(1) = f(ar)(1) = \overline{f}(ar) = (g \circ \iota)(ar) = g(ar) = ga(r).$$

Logo, $f(a) = ga$. Pelo Critério de Baer, $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ é um módulo$-R$ à direita injetivo. □

Proposição. Todo o módulo$-\mathbb{Z}$ é submódulo de um módulo$-\mathbb{Z}$ divisível.

Demonstração. Seja M um módulo$-\mathbb{Z}$. Como todo o módulo é imagem epimorfa de um módulo livre, existe L módulo$-\mathbb{Z}$ livre tal que M é imagem epimorfa de L, isto é,

$$\exists K \leq_{\mathbb{Z}} L : M \cong L/K.$$

Sendo L um módulo$-\mathbb{Z}$ livre, $L \cong \mathbb{Z}^{(I)}$ para algum conjunto I. Então,

$$M \cong \mathbb{Z}^{(I)}/K \leq_{\mathbb{Z}} \mathbb{Q}^{(I)}/K.$$

Ora, $\mathbb{Q}^{(I)}$ é um módulo$-\mathbb{Z}$ divisível pois $\mathbb{Q}$ é um módulo$-\mathbb{Z}$ divisível e a soma direta de módulos divisíveis é ainda um módulo divisível. Como todo o módulo quociente de um módulo divisível é também divisível, $\mathbb{Q}^{(I)}/K$ é divisível.

A menos de um isomorfismo, M é submódulo de um módulo$-\mathbb{Z}$ divisível. □

Proposição. Seja M um módulo$-R$. Então, são equivalentes as seguintes condições:

(a) M é um módulo$-R$ injetivo.

(b) M é parcela direta de todo o módulo que o contém.

Demonstração. [exercício]

1.6. Extensões essenciais

No que se segue, R é um anel unitário e todos os módulos são módulos$-R$ unitários.

Definição. Seja M um módulo$-R$. Diz-se que um submódulo$-R$ N de M é *submódulo essencial de* M, e escreve-se $N \leq_e M$, se $N \cap P \neq \{0\}$ para todo o P submódulo$-R$ não nulo de M.
Neste caso, dizemos que M é *extensão essencial de* N.

É claro que M é submódulo essencial de M. Por outro lado, $\{0\}$ não é submódulo essencial de M.

Proposição. Sejam M um módulo$-R$ e N um submódulo$-R$ de M. Então, são equivalentes as seguintes condições:

(a) N é submódulo essencial de M.

(b) $mR \cap N \neq \{0\}$, para todo o $m \in M \setminus \{0\}$.

(c) para cada $m \in M \setminus \{0\}$, existe $r \in R$ tal que $mr \in N \setminus \{0\}$.

Demonstração [exercício]

Definição. Seja I um ideal direito de R. Diz-se que I é *ideal direito essencial de* R se I for submódulo$-R$ essencial de R_R.

Proposição.

(a) Sejam N, M, T módulos$-R$ tais que $N \leq_R M \leq_R T$. Então,

$$N \leq_e T \quad \text{se e só se} \quad N \leq_e M \text{ e } M \leq_e T$$

(b) Sejam N_1, N_2, M_1, M_2 submódulos de um módulo$-R$ M. Se $N_1 \leq_e M_1$ e $N_2 \leq_e M_2$, então $N_1 \cap N_2 \leq_e M_1 \cap M_2$.

(c) Sejam M, P módulos$-R$, N um submódulo$-R$ de M e $f : P \to M$ um morfismo$-R$.

(i) Se $N \leq_e M$, então $f^{\leftarrow}(N) \leq_e P$.

(ii) Se f for um monomorfismo$-R$ e $Q \leq_e P$, então $f(Q) \leq_e f(P)$.

(d) Sejam $\{N_i\}_{i \in I}$ e $\{M_i\}_{i \in I}$ famílias de módulos$-R$ tais que, para todo o $i \in I$, $N_i \leq_e M_i$. Então, a soma direta externa dos M_i, com $i \in I$, é extensão essencial da soma direta externa dos N_i, com $i \in I$.

(e) Sejam $\{N_i\}_{i \in I}$ e $\{P_i\}_{i \in I}$ famílias de submódulos de um módulo$-R$ M. Se existir a soma direta interna $\bigoplus_{i \in I}{}_{\mathrm{i}} N_i$ e, para todo o $i \in I$, $N_i \leq_e P_i$, então existe a soma direta interna $\bigoplus_{i \in I}{}_{\mathrm{i}} P_i$ e

$$\bigoplus_{i \in I}{}_{\mathrm{i}} N_i \ \leq_e \ \bigoplus_{i \in I}{}_{\mathrm{i}} P_i \ .$$

Demonstração. A demonstração dos resultados em (a)–(c) fica como exercício.

(d) Seja $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} M_i \setminus \{\overline{0}\}$. Então, x tem um número finito de componentes não nulas, digamos $x_{j_1}, \ldots, x_{j_k}$.

Como $x_{j_1} \in M_{j_1} \setminus \{0\}$ e $N_{j_1} \leq_e M_{j_1}$, existe $r_1 \in R$ tal que $x_{j_1} r_1 \in N_{j_1} \setminus \{0\}$. Consideremos $xr_1 = (x_i r_1)_{i\in I}$.

Se $x_{j_n} r_1 = 0$ para todo o $n \in \{1, \ldots, k\}$, então

$$xr_1 = (x_i r_1)_{i\in I} \in \bigoplus_{i\in I} N_i \setminus \{\overline{0}\}.$$

Se $x_{j_2} r_1 \neq 0$, então $x_{j_2} \in M_{j_2} \setminus \{0\}$ e $N_{j_2} \leq_e M_{j_2}$, pelo que existe $r_2 \in R$ tal que $x_{j_2} r_1 r_2 \in N_{j_2} \setminus \{0\}$. Consideremos $xr_1r_2 = (x_i r_1 r_2)_{i\in I}$.

Como $x_1 r_1 \in N_1$ e $r_2 \in R$, temos que $x_1 r_1 r_2 \in N_1$.

Se $x_{j_n} r_1 r_2 = 0$ para todo o $n \in \{3, \ldots, k\}$, então

$$xr_1r_2 = (x_i r_1 r_2) \in \bigoplus_{i\in I} N_i \setminus \{0\}.$$

Se $x_{j_3} r_1 r_2 \neq 0$, continua-se o processo seguindo o mesmo raciocínio.

Assim, existe $r \in R$ tal que $xr \in \bigoplus_{i\in I} N_i \setminus \{\overline{0}\}$. Portanto,

$$\bigoplus_{i\in I} N_i \leq_e \bigoplus_{i\in I} M_i.$$

(e) Admitamos que existe a soma direta interna $\bigoplus_{i\in I} N_i$ e que $N_i \leq_e P_i$, para todo o $i \in I$.

Como existe $\bigoplus_{i\,\in\, I} {}_i N_i$,

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

para todo o $j \in I$. Suponhamos que existe $j \in I$ tal que

$$P_j \cap \left(\sum_{i\in I\setminus\{j\}} P_i \right) \neq \{0\}.$$

Então, existe $x \in P_j \cap \left(\sum_{i\in I\setminus\{j\}} P_i \right) \setminus \{0\}$. Como $x \in \sum_{i\in I\setminus\{j\}} P_i$,

$$x = \sum_{i\in I\setminus\{j\}} x_i,$$

com $x_i \in P_i$ para cada $i \in I \setminus \{j\}$, x_i quase todos nulos. Ou seja,

$$x = x_{\alpha_1} + \cdots + x_{\alpha_k},$$

com $x_{\alpha_i} \in P_{\alpha_i}$, para todo o $\imath \in \{1, \ldots, k\}$, e $\alpha_i \neq j$, para todo o $i \in \{1, \ldots, k\}$.
Como $x \in P_j \setminus \{0\}$ e $N_j \leq_e P_j$, existe $r \in R$ tal que $xr \in N_j \setminus \{0\}$. Assim,

$$xr = (x_{\alpha_1} + \cdots + x_{\alpha_k})r = x_{\alpha_1}r + \cdots + x_{\alpha_k}r.$$

Suponhamos que $x_{\alpha_i}r \neq 0$, para todo o $i \in \{1, \ldots, k\}$. Em particular, $x_{\alpha_1}r \in P_{\alpha_1} \setminus \{0\}$. Como $N_{\alpha_1} \leq_e P_{\alpha_1}$, existe $r_1 \in R$ tal que $x_{\alpha_1}rr_1 \in N_{\alpha_1} \setminus \{0\}$.
Se $x_{\alpha_2}rr_1 + \cdots + x_{\alpha_k}rr_1 = 0$, então

$$xrr_1 = x_{\alpha_1}rr_1 \in (N_j \cap N_{\alpha_1}) \setminus \{0\}.$$

Logo, $(N_j \cap N_{\alpha_1}) \neq \{0\}$ e $N_j \cap \left(\sum_{i \in I \setminus \{j\}} N_i \right) \neq \{0\}$, uma contradição.
Se $x_{\alpha_2}rr_1 \neq 0$, segue-se um raciocínio idêntico ao utilizado em (d) e chega-se sempre a um absurdo.
Logo, $P_j \cap \left(\sum_{i \in I \setminus \{j\}} P_i \right) = \{0\}$ para todo o $j \in I$, pelo que existe $\bigoplus_{i \in I}{}_{\mathrm{i}} P_i$.
Por (d), $\bigoplus_{i \in I}{}_{\mathrm{e}} N_i \leq_e \bigoplus_{i \in I}{}_{\mathrm{e}} P_i$. Como

$$\bigoplus_{i \in I}{}_{\mathrm{i}} N_i \cong \bigoplus_{i \in I}{}_{\mathrm{e}} N_i \quad \text{e} \quad \bigoplus_{i \in I}{}_{\mathrm{i}} P_i \cong \bigoplus_{i \in I}{}_{\mathrm{e}} P_i ,$$

temos que

$$\bigoplus_{i \in I}{}_{\mathrm{i}} N_i \leq_e \bigoplus_{i \in I}{}_{\mathrm{i}} P_i .$$

□

Lema. Seja N um submódulo essencial de um módulo$-R$ M. Então, para todo o $m \in M$, $(N : m) = \{r \in R : mr \in N\}$ é ideal direito essencial de R.

Demonstração. Já foi visto que $(N : m)$ é ideal direito de R. Seja $I \leq_R R_R$ tal que $(N : m) \cap I = \{0\}$ e suponhamos que $mI \neq \{0\}$.
Como $mI \leq_R M$ e $mI \neq \{0\}$, temos que $N \cap mI \neq \{0\}$. Logo, existe $a \in (N \cap mI) \setminus \{0\}$. Visto que $a \in mI$, existe $i \in I$ tal que $a = mi$. Por definição, $i \in (N : m) \cap I = \{0\}$. Logo,

$$a = m \cdot 0 = 0,$$

um absurdo, que resulta de supormos que $mI \neq \{0\}$. Assim, $mI = \{0\} \subseteq N$ e, por definição, $I \subseteq (N : m)$. Logo,

$$I = (N : m) \cap I = \{0\}.$$

Portanto, $(N : m) \leq_e R$ e $(N : m)$ é ideal direito essencial de R. $\square$

Corolário. Sejam M um módulo$-R$ e N um submódulo essencial de M. Então, para todo o $m \in M$, existe um ideal direito essencial I_m de R tal que $mI_m \subseteq N$.

Demonstração. [exercício]

Definição. Sejam M um módulo$-R$ e N um submódulo$-R$ de M.

1. Dá-se o nome de *complemento de N em M* a qualquer submódulo$-R$ de M que seja elemento maximal do conjunto $\mathcal{A} = \{X \leq_R M : X \cap N = \{0\}\}$.

2. Diz-se que um submódulo$-R$ P de M é *complemento em M* se for complemento de algum submódulo$-R$ de M.

Proposição. Seja M um módulo$-R$. Então, todo o submódulo$-R$ de M admite um complemento.

Demonstração. [exercício]
sugestão: use o Lema de Zorn.

Proposição. Sejam M um módulo$-R$, N um submódulo$-R$ de M e K um complemento de N em M. Então,

(a) existe $K \oplus_i N$ e $K \oplus_i N \leq_e M$.

(b) $(K \oplus_i N)/K \leq_e M/K$.

Demonstração.

(a) Como K é complemento de N em M, K é elemento maximal da família

$$\mathcal{A} = \{X \leq_R M : X \cap N = \{0\}\}.$$

Em particular, $K \cap N = \{0\}$. Logo, existe $K \oplus_i N$.

É claro que $K \oplus_i N$ é submódulo$-R$ de M, uma vez que K e N são submódulos$-R$ de M.

Seja P um submódulo$-R$ de M tal que $(K \oplus_i N) \cap P = \{0\}$. Pretendemos mostrar que $P = \{0\}$. Ora, $K + P$ é submódulo$-R$ de M. Dado $x \in (K + P) \cap N$, existem $k \in K$ e $p \in P$ tais que $x = k + p$, pelo que

$$x - k = p \in (K \oplus_i N) \cap P = \{0\}.$$

Portanto, $x = k$ e, assim, $x \in K \cap N$. Mas $K \cap N = \{0\}$, pelo que $x = 0$ e

$$(K + P) \cap N = \{0\}.$$

Por definição, $K + P \in \mathcal{A}$. Como K é elemento maximal de $\mathcal{A}$ e $K \subseteq K + P$, podemos concluir que $K = K + P$ e, portanto, $P \subseteq K$. Logo, $P \subseteq K \oplus_i N$ e

$$P = (K \oplus_i N) \cap P = \{0\}.$$

Portanto, $K \oplus_i N \leq_e M$.

(b) [exercício].

□

Corolário. Todo o submódulo$-R$ de um módulo$-R$ M é parcela direta de um submódulo essencial de M.

Demonstração. [exercício]

Definição. Sejam M um módulo$-R$ e N um submódulo$-R$ de M. Dizemos que M é *extensão essencial própria de* N se $N \leq_e M$ e $N \neq M$.

Proposição. Toda a parcela direta de um módulo$-R$ M não admite extensões próprias contidas em M.

Demonstração. Seja N uma parcela direta de um módulo$-R$ M. Então, N é submódulo$-R$ de M e existe L submódulo$-R$ de M tal que

$$M = N \oplus_i L.$$

Suponhamos que N admite uma extensão essencial própria contida em M, digamos P. Então, $N \leq_e P$ e $N \neq P$. Como existe $N \oplus_i L$, temos que $N \cap L = \{0\}$. Portanto,

$$N \cap (P \cap L) = \{0\}.$$

Ora, $P \cap L \leq_R P$, $N \leq_e P$ e $N \cap (P \cap L) = \{0\}$. Logo, $P \cap L = \{0\}$ e, assim,

$$P = P \cap M = P \cap (N + L) = N + (P \cap L) = N + \{0\} = N,$$

o que contradiz o facto de P ser extensão essencial própria de N. Vimos, portanto, que N não admite extensões essenciais próprias contidas em M. □

Proposição. Sejam M um módulo$-R$ e N um submódulo$-R$ de M. Então, são equivalentes as seguintes condições:

(a) N não admite extensões essenciais próprias contidas em M.

(b) N é submódulo complemento em M.

(c) Existe K submódulo$-R$ de M tal que $N \cap K = \{0\}$ e $(N \oplus K)/N \leq_e M/N$

Demonstração. Iremos mostrar que (a) é equivalente a (b) e que (b) é equivalente a (c).

Admitamos que N não admite extensões essenciais próprias contidas em M. Seja K um complemento de N em M. Então, K é elemento maximal de

$$\mathcal{A} = \{X \leq_R M : X \cap N = \{0\}\}.$$

Mais, existe $K \oplus_i N$ e $K \oplus_i N \leq_e M$.
Consideremos o conjunto

$$\mathcal{B} = \{X \leq_R M : X \cap K = \{0\}\}.$$

Como $N \leq_R M$ e $N \cap K = \{0\}$, concluímos que $N \in \mathcal{B}$.
Suponhamos que existe $P \in \mathcal{B}$ tal que $N \subseteq P$. Como $P \in \mathcal{B}$, temos que $P \leq_R M$ e $P \cap K = \{0\}$. Dado $x \in P$, se $x = 0$, então $x \in N$. Se $x \neq 0$, então $x \in M \setminus \{0\}$ e, portanto, existe $r \in R$ tal que $xr \in (K \oplus_i N) \setminus \{0\}$ (uma vez que $K \oplus_i N \leq_e M$). Assim, existem $k \in K$ e $n \in N$ tais que

$$xr = k + n,$$

pelo que $xr - n = k \in P \cap K = \{0\}$. Logo, existe $r \in R$ tal que $xr \in N \setminus \{0\}$, pelo que $N \leq_e P$. Por hipótese, $P = N$ e, portanto, N é elemento maximal de $\mathcal{B}$. Por definição, N é complemento de K em M, pelo que N é submódulo complemento em M.

Admitamos, agora, que N é submódulo complemento em M. Então, existe $K \leq_R M$ tal que N é complemento de K em M. Assim, N é elemento maximal de

$$\mathcal{A} = \{X \leq_R M : X \cap K = \{0\}\}.$$

Suponhamos que existe $P \leq_R M$ tal que $N \leq_e P$ e $N \neq P$. Temos que $K \leq_R M$ e $N \cap K = \{0\}$. Logo, $K \cap P \leq_R P$ e

$$N \cap (K \cap P) = (N \cap K) \cap P = \{0\} \cap P = \{0\}.$$

Como $N \leq_e P$, $K \cap P = \{0\}$. Assim, $P \in \mathcal{A}$ e $N \subseteq P$. Como N é elemento maximal de $\mathcal{A}$, concluímos que $N = P$, um absurdo. Logo, N não admite extensões essenciais próprias contidas em M.

Admitamos que N é submódulo complemento em M. Então, existe $K \leq_R M$ tal que N é complemento de K em M. Por definição, $N \cap K = \{0\}$. Portanto, existe $N \oplus_i K$ e $(N \oplus_i K)/N \leq_e M/N$.

Admitamos que existe $K \leq_R M$ tal que $N \cap K = \{0\}$ e $(N \oplus K)/N \leq_e M/N$. Consideremos

$$\mathcal{B} = \{X \leq_R M : X \cap K = \{0\}\}.$$

Por hipótese, $N \in \mathcal{B}$. Suponhamos que existe $P \leq_R M$ tal que $P \cap K = \{0\}$ e $N \subseteq P$. Como $P \leq_R M$ e $N \subseteq P$, temos que $P/N \leq_R M/N$. Ora, $N \subseteq P$ e, portanto,

$$P \cap (N \oplus K) = N + (P \cap K) = N + \{0\} = N.$$

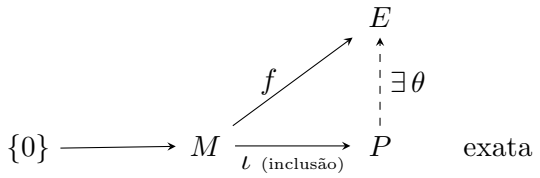
Logo,

$$P/N \cap (N \oplus K)/N = [P \cap (N \oplus K)]/N = N/N = \{N\}.$$

Como $(N \oplus K)/N \leq_e M/N$, temos que $P/N = \{N\}$. Assim, $P = N$.
Vimos, então, que N é elemento maximal de $\mathcal{B}$ e, portanto, N é complemento de K em M. Logo, N é submódulo complemento em M. □

Proposição. Sejam E um módulo$-R$ injetivo, M um módulo$-R$ e $f : M \to E$ um monomorfismo$-R$. Então, para toda a extensão essencial P de M existe $\theta : P \to E$ que prolonga f.

Demonstração. Seja P uma extensão essencial de M. Então, $M \leq_e P$.



Como E é injetivo, existe um morfismo$-R$ $\theta : P \to E$ tal que $\theta \circ \iota = f$. Logo, $\theta|_M = f$.

Falta mostrar que θ é um monomorfismo$-R$ [exercício. sugestão: mostre que $M \cap \mathrm{Ker}(\theta) = \{0\}$]. □

Proposição. Seja M um módulo$-R$. Então, M é um módulo injetivo se e só se M não admite extensões essenciais próprias.

Demonstração. Admitamos que M é um módulo injetivo. Seja P uma extensão essencial de M. Então, P é módulo$-R$ e $M \subseteq P$. Como M é parcela direta de todo o módulo$-R$ que o contém (pois é injetivo), M é parcela direta de P. Assim, existe $L \leq_R P$ tal que $P = M \oplus_i L$. Como existe $M \oplus_i L$, sabemos que $M \cap L = \{0\}$. Sendo M um submódulo essencial de P, temos, por definição, $L = \{0\}$. Portanto,

$$P = M \oplus_i L = M \oplus_i \{0\} = M,$$

pelo que M não admite extensões essenciais próprias.

Admitamos, agora, que M não admite extensões essenciais próprias. Seja P um módulo$-R$ que contém M e seja K um complemento de M em P. Então, $(M \oplus_i K)/K \leq_e P/K$. Mas M não admite extensões essenciais próprias. Logo [porquê?],

$$(M \oplus_i K)/K = P/K,$$

pelo que $M \oplus_i K = P$. Assim, M é parcela direta de P.
Vimos que M é parcela direta de todo o módulo$-R$ que o contém, pelo que M é injetivo. □

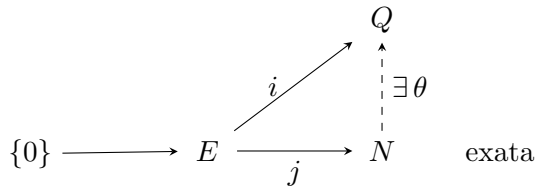
Proposição. Todo o módulo$-R$ admite uma extensão essencial maximal.

Demonstração. Seja M um módulo$-R$. Como todo o módulo$-R$ é submódulo$-R$ de um módulo$-R$ injetivo, existe Q módulo$-R$ injetivo tal que $M \leq_R Q$. Consideremos

$$\mathcal{A} = \{X \leq_R Q : M \leq_e X\}.$$

É claro que $M \in \mathcal{A}$ e, portanto, $\mathcal{A} \neq \emptyset$. Mais, $(\mathcal{A}, \subseteq)$ é um c.p.o.. Consideremos uma cadeia não vazia de elementos de $\mathcal{A}$, digamos $\mathcal{C} = \{X_\alpha\}_{\alpha \in I}$. Seja $Y = \bigcup_{\alpha \in I} X_\alpha$. Como $\mathcal{C}$ é cadeia e $X_\alpha \leq_R Q$ para todo o $\alpha \in I$, Y é submódulo$-R$ de Q. Vejamos se Y é extensão essencial de M. Para tal, tomemos $x \in Y \setminus \{0\}$. Então, existe $\beta \in I$ tal que $x \in X\beta \setminus \{0\}$. Como X_β é extensão essencial de M, existe $r \in R$ tal que $xr \in M \setminus \{0\}$. Assim, Y é extensão essencial de M. Por definição, $Y \in \mathcal{A}$ e, portanto, $\mathcal{C}$ admite majorante. Pelo Lema de Zorn, $\mathcal{A}$ admite elemento maximal, digamos E.

De seguida, verificamos que E é extensão essencial maximal de M. Seja N uma extensão essencial de M tal que $E \subseteq N$.



Como Q é módulo$-R$ injetivo e $i : E \to Q$ é um monomorfismo$-R$, existe um morfismo$-R$ θ que prolonga i, isto é, existe um monomorfismo$-R$ $\theta : N \to Q$ tal que $\theta|_E = i$. Assim,

$$E = i(E) = \theta|_E(E) = \theta(E) \subseteq \theta(N)$$

e $\theta(N) \leq_R Q$. Como θ é um monomorfismo e $M \leq_e N$, temos que

$$M = i(M) = \theta|_E(M) = \theta(M) \leq_e \theta(N).$$

Por definição, $\theta(N) \in \mathcal{A}$. Sendo E um elemento maximal, temos que $E = \theta(N)$. Assim, $\theta(E) = \theta(N)$. Sendo θ um monomorfismo$-R$, $E = N$.

Portanto, E é uma extensão essencial maximal de M. □

Proposição. Seja N uma extensão de M. São equivalentes as seguintes condições:

(a) N é extensão essencial maximal de M.

(b) N é módulo injetivo e extensão essencial de M.

(c) N é extensão injetiva minimal de M.

Demonstração. Admitamos que N é extensão essencial maximal de M. Em particular, N é extensão essencial de M. Seja P uma extensão essencial de N. Como $M \leq_e N$ e $N \leq_e P$, temos que $M \leq_e P$, pelo que $M \leq_e P$. Mas N é extensão essencial maximal de M e $N \subseteq P$.

Logo, $N = P$ e N não admite extensões essenciais próprias. Assim, N é um módulo injetivo e extensão essencial de M.

Admitamos, agora, que N é módulo injetivo e extensão essencial de M. Então, N é extensão injetiva de M. Seja Q um módulo$-R$ injetivo tal que $M \leq_R Q \leq_R N$. Como $M \leq_e N$, temos que $M \leq_e Q$ e $Q \leq_e N$. Mas Q é injetivo e, portanto, Q não admite extensões essenciais próprias. Logo, $Q = N$ e N é extensão injetiva minimal.

Suponhamos que N é extensão injetiva minimal de M. Então, N é módulo injetivo e $M \leq_R N$. Consideremos

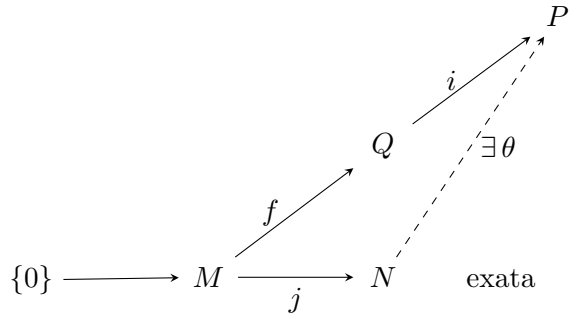
$$\mathcal{A} = \{X \leq_R N : M \leq_e X\}.$$

Na demonstração do resultado anterior, vimos que $\mathcal{A}$ admite um elemento maximal, digamos E. Mais, vimos que E é uma extensão essencial maximal de M contida em N. Como E é extensão essencial maximal de M, E é um módulo injetivo, pelo que vimos acima. Ora, N é extensão injetiva minimal de M e $E \subseteq N$. Portanto, $E = N$. Em particular, N é extensão essencial maximal de M. □

Definição. Seja M um módulo$-R$. Designa-se por *invólucro injetivo de* M toda a extensão de M que satisfaça uma das condições da proposição anterior.

Proposição. Sejam N uma extensão essencial maximal de um módulo$-R$ M, P uma extensão essencial maximal de um módulo$-R$ Q e $f : M \to Q$ um isomorfismo$-R$. Então, existe um isomorfismo$-R$ $\theta : N \to P$ tal que $\theta|_M = f$.

Demonstração. Como N é uma extensão essencial maximal de M, $M \leq_e N$ e N é módulo$-R$ injetivo. De modo análogo, $Q \leq_e P$ e P é módulo$-R$ injetivo.



Como P é módulo$-R$ injetivo, existe um morfismo$-R$ $\theta : N \to P$ tal que $\theta \circ j = i \circ f$. Comecemos por mostrar que $\theta|_M = f$. Dado $m \in M$,

$$\theta(m) = \theta(j(m)) = (\theta \circ j)(m) = (i \circ f)(m) = i(f(m)) = f(m).$$

Logo, $\theta|_M = f$. Em particular, $M \cap \mathrm{Ker}(\theta) = \mathrm{Ker}(\theta|_M) = \mathrm{Ker}(f) = \{0\}$. Sendo N uma extensão essencial de M, podemos concluir que $\mathrm{Ker}(\theta) = \{0\}$. Assim, θ é um monomorfismo. Logo, $N \cong \theta(N)$. Como N é módulo$-R$ injetivo, $\theta(N)$ também o é. Ora,

$$Q = f(M) = \theta(M) \leq_R \theta(N) \leq_R P.$$

Sendo P uma extensão injetiva minimal de Q, temos que $\theta(N) = P$. Portanto, θ é um isomorfismo$-R$. □

Corolário. Sejam M um módulo$-R$ e N e P invólucros injetivos de M. Então, existe um isomorfismo$-R$ $\theta : N \to P$ tal que θ estende a identidade de M.

Demonstração. [exercício]

Observação. O invólucro injetivo de um módulo$-R$ M é único a menos de isomorfismo e representa-se por $E(M)$.

Proposição. Seja N um módulo$-R$ e M uma extensão essencial de N. Então, $E(N) = E(M)$.

Demonstração. [exercício]

Proposição. Seja $\{M_i\}_{i\in I}$ uma família de módulos$-R$. Se $\bigoplus_{i\in I} E(M_i)$ for módulo$-R$ injetivo, então

$$E\left(\bigoplus_{i\in I} M_i\right) = \bigoplus_{i\in I} E(M_i).$$

Demonstração. Por definição, $M_i \leq_e E(M_i)$, para todo o $i \in I$. Logo,

$$\bigoplus_{i\in I} M_i \leq_e \bigoplus_{i\in I} E(M_i).$$

Mas, por hipótese, $\bigoplus_{i\in I} E(M_i)$ é um módulo$-R$ injetivo. Então, $\bigoplus_{i\in I} E(M_i)$ é um módulo$-R$ injetivo e é extensão essencial de $\bigoplus_{i\in I} M_i$. Por outras palavras, $\bigoplus_{i\in I} E(M_i)$ é invólucro injetivo de $\bigoplus_{i\in I} M_i$, isto é,

$$\bigoplus_{i\in I} E(M_i) = E\left(\bigoplus_{i\in I} M_i\right).$$

□

Corolário. Sejam $s \in \mathbb{N}$ e $M_1, \ldots, M_s$ módulos$-R$. Então,

$$E\left(\bigoplus_{i=1}^{s} M_i\right) = \bigoplus_{i=1}^{s} E(M_i).$$

Demonstração. [exercício]

2. Anéis

2.1. Idempotentes

No que se segue, R é um anel não nulo.

Definição. Um elemento e de R diz-se um *idempotente* se $e^2 = e$.
Um idempotente e diz-se um *idempotente central* se

$$e \in Z(R) = \{a \in R : \, ar = ra, \, \forall r \in R\}.$$

Exemplos.

1. $0 \in R$ é um idempotente central, pois para todo o $r \in R$, $0 \cdot r = 0 = r \cdot 0$.
2. Se R é um anel unitário, então $1 \in R$ é um idempotente central, uma vez que $1 \cdot r = r = r \cdot 1$ para todo o $r \in R$.

Observações. Sejam $e, f \in R$ idempotentes.

1. Para todo o $a \in fR$, $fa = a$.

   De facto, dado $a \in fR$, existe $r \in R$ tal que $a = fr$ e, portanto,

   $$fa = f(fr) = (ff)r = f^2 r = fr = a.$$

2. Para todo o $b \in Rf$, $bf = b$.

   Seja $b \in Rf$. Então, existe $r \in R$ tal que $b = rf$ e, assim,

   $$bf = (rf)f = r(ff) = rf^2 = rf = b.$$

3. Para todo o $c \in eRf$, $ecf = c$.

   Se $c \in eRf$, então existe $r \in R$ tal que $c = erf$, pelo que

   $$ecf = e(erf)f = (ee)r(ff) = e^2 rf^2 = erf = c.$$

Proposição. Seja $f \in R$ um idempotente. Então, são equivalentes as seguintes condições:

(a) f é um idempotente central.

(b) f comuta com todos os idempotentes de R.

Demonstração. Suponhamos que f é um idempotente central. Então, $f \in Z(R)$, ou seja, f comuta com todos os elementos de R. Em particular, f comuta com todos os idempotentes de R.

Reciprocamente, admitamos que f comuta com todos os idempotentes de R e consideremos $x \in R$.
Não é difícil de verificar que $f + fx - fxf$ e $f + xf - fxf$ são idempotentes [exercício]. Por hipótese,

$$f(f + fx - fxf) = (f + fx - fxf)f \quad \text{e} \quad f(f + xf - fxf) = (f + xf - fxf)f,$$

donde se conclui que

$$fx = fxf \quad \text{e} \quad fxf = xf.$$

[exercício] Assim, $fx = xf$ para todo o $x \in R$ e, por definição, f é um idempotente central. □

Proposição. Seja R um anel unitário. Se 1 é a identidade em R e $f \in R$ é um idempotente, então

(a) $1 - f \in R$ também é elemento idempotente.

(b) se f for um idempotente central, $1 - f$ também é um idempotente central.

Demonstração. [exercício]

Proposição. Seja $f \in R$ um idempotente. Então,

(a) fRf é subanel de R e f é elemento identidade de fRf.

(b) Se $f \in Z(R)$, a aplicação $\varphi : R \to fRf$, definida por $\varphi(a) = faf$ para todo o $a \in R$, é um epimorfismo de anéis. Mais, se R for um anel unitário, $\text{Ker}(\varphi) = (1 - f)R$.

Demonstração. [exercício]

Proposição. Seja $e \in R$ um idempotente. Então, os anéis $E_R(eR)$ e eRe são isomorfos.

Demonstração. Seja $a \in eR$. Então, $a = ea$. Dado $\varphi \in E_R(eR)$, para todo o $a \in eR$,

$$\varphi(a) = \varphi(ea) = \varphi(e) \cdot a.$$

Em particular, $\varphi(e) = \varphi(e) \cdot e$. Como $\varphi(e) \in eR$, $\varphi(e) = e\varphi(e)$. Logo,

$$\varphi(e) = e \cdot \varphi(e) \cdot e \in eRe.$$

Consideremos a correspondência

$$\begin{array}{rccc} \theta : & E_R(eR) & \longrightarrow & eRe \\ & \varphi & \longmapsto & \varphi(e) \end{array}$$

Prova-se que θ é um isomorfismo$-R$ [exercício] e, portanto, $E_R(eR) \cong eRe$. □

Proposição. Seja $f \in R$ um idempotente. Então,

(a) Se I for um ideal direito de fRf e I' for o ideal direito de R gerado por I, então:

i. $I' = I + IR$.

ii. $I = fI'f = I' \cap fRf$.

(b) Se L for ideal de R, então $fLf = L \cap fRf$.

Demonstração. [exercício]

Proposição. Sejam $e, f \in R$ idempotentes. Então, são equivalentes as seguintes condições:

(a) eR e fR são módulos$-R$ direitos isomorfos.

(b) Re e Rf são módulos$-R$ esquerdos isomorfos.

(c) existem $x \in eRf$ e $y \in fRe$ tais que $xy = e$ e $yx = f$.

Demonstração. Iremos mostrar que as condições (b) e (c) são equivalentes. A demonstração de que (a) é equivalente a (c) é análoga.

Admitamos que Re e Rf são módulos-R esquerdos isomorfos. Seja $\varphi : Re \to Rf$ um isomorfismo-R. É claro que $e = e^2 \in Re$. Consideremos $x = \varphi(e) \in Rf$. Então,

$$x = \varphi(e) = \varphi(e)f = \varphi(e^2)f = e\varphi(e)f \in eRf.$$

Como $f = f^2 \in Rf$, existe $y = \varphi^{-1}(f) \in Re$. Portanto,

$$y = \varphi^{-1}(f) = \varphi^{-1}(f)e = \varphi^{-1}(f^2)e = f\varphi^{-1}(f)e \in fRe.$$

Facilmente se verifica que $xy = e$ e $yx = f$ [exercício].

Reciprocamente, admitamos que existem $x \in eRf$ e $y \in fRe$ tais que $xy = e$ e $yx = f$. Consideremos as correspondências $h : Re \to Rf$ e $g : Rf \to Re$ definidas respetivamente por $h(a) = ax$, para todo o $a \in Re$, e $g(b) = by$, para todo o $b \in Rf$.
Prova-se que h e g são morfismos-R tais que $h \circ g = \mathrm{id}_{\mathrm{Rf}}$ e $g \circ h = \mathrm{id}_{\mathrm{Re}}$ [exercício]. Logo, h e g são isomorfismos-R, pelo que Re e Rf são módulos-R esquerdos isomorfos. □

Definição. Diz-se que I é um *ideal direito* [respetivamente: *esquerdo*, *bilateral*] *minimal de* R se I for elemento minimal do conjunto parcialmente ordenado, para a relação de inclusão, dos ideais direitos [respetivamente: esquerdos, bilaterais] não nulos de R.

Proposição. Seja I um ideal direito minimal de R tal que $I^2 \neq \{0\}$. Então, existe $e \in R$ idempotente tal que $I = eR$.

Demonstração. Como $I^2 \neq \{0\}$, existe $i \in I$ tal que $iI \neq \{0\}$. Ora, $iI \subseteq I$, uma vez que I é ideal direito de R e $I \subseteq R$. Sendo I um ideal direito minimal de R, podemos concluir que $I = iI$.

Como $i \in I = iI$ e $i \neq 0$, existe $e \in I \setminus \{0\}$ tal que $i = ie$. Consideremos

$$r(i) = \{r \in R : ir = 0\}.$$

Temos que $r(i) \cap I$ é ideal direito de R contido em I [exercício], pelo que $r(i) \cap I = \{0\}$ ou $r(i) \cap I = I$ (pois I é ideal direito minimal de R). Suponhamos que $r(i) \cap I = I$. Então, $e \in I = r(i) \cap I \subseteq r(i)$, pelo que $ie = 0$ e, portanto, $i = 0$, uma contradição. Logo,

$$r(i) \cap I = \{0\}.$$

Como $ie^2 = (ie)e = ie$, sabemos que $i(e^2 - e) = 0$. Assim, $e^2 - e \in r(i) \cap I = \{0\}$, pelo que $e^2 = e$. Portanto, e é um idempotente.

Falta mostrar que $I = eR$. Como $e \in I$ e I é ideal direito de R, é claro que $eR \subseteq I$. Ora, eR é um ideal direito não nulo de R, pois $e = e^2 \in eR \setminus \{0\}$. Como I é ideal direito minimal, podemos concluir que $I = eR$. □

Proposição. Sejam R um anel unitário e f um elemento idempotente de R. Então,

$$R = fR \oplus_i (1 - f)R.$$

Demonstração. [exercício]

Definição. Sejam $a, b \in R$. Dizemos que a e b são *ortogonais* se $ab = 0 = ba$.

Exemplo. Se R é um anel unitário e f é um elemento idempotente de R, então f e $1 - f$ são ortogonais.

Definição. Seja $f \in R \setminus \{0\}$ um idempotente. Dizemos que f é *primitivo* se f não for soma de dois idempotentes ortogonais não nulos, isto é, se não existirem $e_1, e_2 \in R \setminus \{0\}$ idempotentes ortogonais tais que $f = e_1 + e_2$.

Proposição. Seja $e \in R \setminus \{0\}$ um idempotente. Então, e é primitivo se e só se for o único elemento idempotente não nulo de eRe.

Demonstração. Admitamos que e é primitivo. Como e é idempotente,

$$e = e^2 = ee = e^2e = eee \in eRe.$$

Consideremos $f \in eRe$ idempotente. Como $f \in eRe$, temos$f = efe$. Não é difícil de verificar que $e - efe$ e efe são idempotentes ortogonais [exercício]. Ora, $e = (e - efe) + efe$ e e é primitivo. Logo,

$$e - efe = 0 \quad \text{ou} \quad efe = 0,$$

ou seja, $f = e$ ou $f = 0$. Portanto, e é o único idempotente não nulo de eRe.

Reciprocamente, admitamos que e é o único idempotente não nulo de eRe e suponhamos que $e = e_1 + e_2$, com e_1, e_2 idempotentes ortogonais não nulos. Então,

$$ee_1 = (e_1 + e_2)e_1 = e_1^2 + e_2e_1 = e_1 + 0 = e_1$$

e

$$e_1e = e_1(e_1 + e_2) = e_1^2 + e_1e_2 = e_1 + 0 = e_1.$$

Assim, $e_1e = e_1 = ee_1$ e

$$e_1 = ee_1 = e^2e_1 = e(ee_1) = e(e_1e) = ee_1e \in eRe.$$

Logo, e_1 é um idempotente não nulo de eRe e, portanto, $e_1 = e$. Mas tal implica que $e_2 = e - e_1$ seja nulo, uma contradição. Então, podemos concluir que e é primitivo. □

Definição. Seja $a \in R$. Dizemos que a é *nilpotente* se existir $n \in \mathbb{N}$ tal que $a^n = 0$. Se a for nilpotente, ao menor natural n tal que $a^n = 0$ chamamos *grau de nilpotência de* a.

Exemplos.

1. 0 é (o único) elemento nilpotente de R de grau 1.
2. Consideremos o anel de todas as matrizes quadradas de ordem 2 com entradas inteiras, $\mathcal{M}_2(\mathbb{Z})$. A matriz $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ é um elemento nilpotente de grau 2.

Definição. Seja X um subconjunto não vazio de R.

1. Dizemos que X é um *subconjunto nilpotente* se existir $n \in \mathbb{N}$ tal que $X^n = \{0\}$. Se X for nilpotente, ao menor dos naturais n tais que $X^n = \{0\}$ damos o nome de *grau de nilpotência de* X.
2. Dizemos que X é um *subconjunto T-nilpotente à esquerda* se, para toda a sucessão $(a_n)_{n\in\mathbb{N}}$ de elementos de X, existir $n_0 \in \mathbb{N}$ tal que $a_1 \dots a_{n_0} = 0$.
3. Dizemos que X é um *subconjunto T-nilpotente à direita* se, para toda a sucessão $(a_n)_{n\in\mathbb{N}}$ de elementos de X, existir $n_0 \in \mathbb{N}$ tal que $a_{n_0} \dots a_1 = 0$.
4. Dizemos que X é *nilconjunto* se todos os elementos de X forem nilpotentes. Se X for ideal direito [respetivamente: esquerdo, bilateral] de R e um nilconjunto, dizemos que X é um *nilideal direito* [respetivamente: *esquerdo*, *bilateral*]

Proposição. As seguintes condições são verdadeiras.

(a) Todo o subconjunto de R que seja nilpotente é T-nilpotente à esquerda e à direita.

(b) Todo o subconjunto de R que seja T-nilpotente à esquerda ou à direita é um nilconjunto.

(c) Todo o subconjunto de R que seja nilpotente é um nilconjunto.

Demonstração. [exercício]

Proposição. Sejam R um anel unitário e $a \in R$. Se a é nilpotente, então $1 - a$ é invertível em R.

Demonstração. [exercício]

Proposição. Seja $a \in R$. Então, aR é nilideal direito se e só se Ra é nilideal esquerdo.

Demonstração. [exercício]

Proposição. As seguintes condições são verdadeiras.

(a) Se R for anel unitário e I for um ideal direito [respetivamente: esquerdo] nilpotente de R, então o ideal bilateral gerado por I também é nilpotente.

(b) A soma de um número finito de nilideais bilaterais de R é ainda um nilideal bilateral de R.

(c) A soma de um número finito de ideais nilpotentes de R é ainda um ideal nilpotente de R.

Demonstração. [exercício]

Proposição. Seja I um nilideal bilateral de R. Para todo o idempotente $r + I \in R/I$, existe um idempotente $e \in R$ tal que $r + I = e + I$.

Demonstração. Seja $r + I$ um idempotente de R/I, com $r \in R$. Então, $r^2 + I = (r + I)^2 = r + I$, pelo que

$$r^2 - r \in I.$$

Como I é nilideal bilateral, existe $n \in \mathbb{N}$ tal que $(r^2 - r)^n = 0$. Ora, $rr^2 = r^2 r$, pelo que

$$(r^2 - r)^n = r^{2n} - nr^{2n-1} + \binom{n}{2} r^{2n-2} - \cdots + (-1)^{n-1} nr^{n+1} + (-1)^n r^n.$$

Logo,

$$(-1)^{n+1} r^n = r^{2n} - nr^{2n-1} + \binom{n}{2} r^{2n-2} - \cdots + (-1)^{n-1} nr^{n+1}$$

e, portanto, $r^n = r^{n+1} p(r)$, com $p(r) \in \mathbb{Z}(r)$. Assim, $r^n = r^{n+1} p(r) = r^n r p(r) = r^{n+2} p(r)^2 = r^{2n} p(r)^n$.
Consideremos $e = r^n p(r)^n$. Então,

$$e^2 = [r^{2n} p(r)^n] p(r)^n = r^n p(r)^n = e.$$

Não é difícil de verificar que $(r + I)^n = r + I$. Logo,

$$e + I = r^n p(r)^n + I = (r^n + I)(p(r)^n + I) = (r + I)^n (p(r)^n + I)$$
$$= (r + I)^{2n} (p(r)^n + I) = (r^{2n} p(r)^n) + I = r^n + I = (r + I)^n = r + I. \quad \square$$

Lema. Seja R um anel sem ideais nilpotentes não nulos. Então, R não possui ideais esquerdos ou direitos nilpotentes não nulos.

Demonstração. [exercício]

Definição. Um anel R diz-se um *anel simples* se $R^2 \neq \{0\}$ e $\{0\}$ e R são os únicos ideias de R.

Proposição. Seja R um anel simples. Então, R é anel sem ideais nilpotentes não nulos.

Demonstração. Como R é um anel simples, $R^2 \neq \{0\}$ e os únicos ideias de R são $\{0\}$ e R. Ora, R^2 é um ideal de R, pelo que podemos concluir que $R^2 = R$. Assim, $R^k = R$ para todo o $k \in \mathbb{N}$.

Seja I um ideal nilpotente de R. Então, existe $n \in \mathbb{N}$ tal que $I^n = \{0\}$. Por hipótese, como os únicos ideais de R são $\{0\}$ e R, temos que $I = \{0\}$ ou $I = R$. Suponhamos que $I = R$. Então, $R^n = \{0\}$, ou seja, $R = \{0\}$, uma contradição. Logo, $I = \{0\}$, pelo que R não admite ideais nilpotentes não nulos. □

Teorema. Sejam R um anel sem ideais nilpotentes não nulos e $f \in R \setminus \{0\}$ um elemento idempotente. Então, fR é ideal direito minimal de R se e só se fRf for anel de divisão.

Demonstração. Admitamos que fR é ideal direito minimal de R. Como $f = f^2 \in fR$ e $f \neq 0$, sabemos que $fR \neq \{0\}$.
Por outro lado, fRf é anel não nulo e f é elemento identidade em fRf.
Dado $fxf \in fRf \setminus \{0\}$, temos que $fxfR \subseteq fR$ e $fxfR$ é ideal direito de R. Ora, fR é ideal direito minimal de R, pelo que $fxfR = \{0\}$ ou $fxfR = fR$.
Mas $fxf = fxf^2 = (fxf)f \in fxfR$, pelo que $fxfR \neq \{0\}$. Portanto, $fxfR = fR$.

Então, $f = f^2 \in fR = fxfR$, pelo que existe $r \in R$ tal que $f = fxfr$. Portanto,

$$f = f^2 = (fxfr)f = fxf^2rf = (fxf)(frf),$$

pelo que fxf é invertível à direita. Por outras palavras, vimos que todo o elemento não nulo de fRf é invertível à direita. Assim, todo o elemento não nulo de fRf é invertível e fRf é anel de divisão.

Reciprocamente, admitamos que I é ideal direito de R tal que $\{0\} \subsetneq I \subseteq fR$. Dado $x \in I$, $x \in fR$ e, portanto, $x = fx$. Assim, $I = fI$. Suponhamos que $If = \{0\}$. Então,

$$I^2 = II = (fI)(fI) = f(If)I = \{0\},$$

pelo que I é nilpotente. Por hipótese, $I = \{0\}$, uma contradição. Logo, $If \neq \{0\}$ e existe $a \in I$ tal que $af \neq 0$. Como $a \in I$, $a = fa$. Assim, $faf = (fa)f = af \neq 0$ e, sendo fRf um anel de divisão, faf é invertível em fRf. logo, existe $r \in R$ tal que $f = (faf)(frf)$. Portanto,

$$f = (fa)(f^2rf) = afrf \in aR \subseteq I.$$

Sendo I um ideal direito de R, $fR \subseteq I$. Vimos, pois que $I = fR$ e fR é ideal direito minimal de R. □

Observação. Se R é um anel e f é um idempotente não nulo de R tal que fR é um ideal direito minimal de R, então fRf é um anel de divisão.

Teorema. Sejam R um anel sem ideais nilpotentes não nulos e $f \in R \setminus \{0\}$ um elemento idempotente. Então, Rf é ideal esquerdo minimal de R se e só se fRf for anel de divisão.

Demonstração. [exercício]

Corolário. Sejam R um anel sem ideais nilpotentes não nulos e $f \in R \setminus \{0\}$ um elemento idempotente. Então, fR é ideal direito minimal de R se e só se Rf é ideal esquerdo minimal de R. □

Proposição. Seja J_0 a interseção dos ideais J de R tais que R/J não contém ideais nilpotentes não nulos. Então, o anel R/J_0 não contém ideais nilpotentes não nulos.

Demonstração. Seja I/J_0 um ideal nilpotente de R/J_0. Então, existe $n \in \mathbb{N}$ tal que $(I/J_0)^n = \{J_0\}$, pelo que $I^n \subseteq J_0$.

Seja J um ideal de R tal que R/J não contém ideais nilpotentes não nulos. Por definição de J_0, temos que $J_0 \subseteq J$. Logo, $I^n \subseteq J$, pelo que $(I + J)^n \subseteq J$. Portanto,

$$((I + J)/J)^n = ((I + J)^n + J)/J = \{J\}.$$

Assim, $(I + J)/J$ é um ideal nilpotente de R/J, pelo que $(I + J)/J = \{J\}$ e $I + J = J$. Portanto, $I \subseteq J$. Por outras palavras, vimos que $I \subseteq J$ para todo o ideal J de R tal que R/J não contém ideais nilpotentes não nulos. Portanto, $I \subseteq J_0$. Como $J_0 \subseteq I$, temos que $I = J_0$ e $I/J_0 = \{J_0\}$. Logo, R/J_0 não admite ideais nilpotentes não nulos. □

Definição. Sejam I_1, I_2, I_3,... ideais direitos tais que $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$. Tais ideais verificam a *condição de cadeia ascendente* se existir $p \in \mathbb{N}$ tal que $I_n = I_p$ para todo o $n \geq p$.

Lema. Seja R um anel tal que os anuladores direitos de subconjuntos de R verificam a condição de cadeia ascendente. Então, todo o ideal direito T-nilpotente à direita é nilpotente.

Demonstração. Seja I um ideal direitode R T-nilpotente à direita. É claro que

$$I \supseteq I^2 \supseteq I^3 \supseteq \ldots,$$

pelo que

$$r(I) \subseteq r(I^2) \subseteq r(I^3) \subseteq \ldots$$

Por hipótese, existe $p \in \mathbb{N}$ tal que $r(I^n) = r(I^p)$ para todo o $n \geq p$.

Suponhamos que I não é nilpotente. Em particular, $I^{p+1} \neq \{0\}$ e, portanto, existe $i_1 \in I$ tal que $I^p i_1 \neq \{0\}$. Assim, $i_1 \notin r(I^p) = r(I^{p+1})$ e, por definição, $I^{p+1} i_1 \neq \{0\}$. Logo, existe $i_2 \in I$ tal que $I^p i_2 i_1 \neq \{0\}$. Também $i_2 i_1 \notin r(I^p) = r(I^{p+1})$, pelo que $I^{p+1} i_2 i_1 \neq \{0\}$.

Construímos, assim, uma sucessão $(i_m)_{m\in\mathbb{N}}$, com $i_m \in I$ tal que $i_m \dots i_2 i_1 \neq 0$, o que contradiz o facto de I ser T-nilpotente à direita. Logo, I é nilpotente. □

No que se segue, R é um anel não nulo.

Proposição. Seja M um módulo-R não nulo e do tipo finito. Então, todo o submódulo-R próprio de M está contido num submódulo maximal de M.

Demonstração. Sendo M um módulo-R do tipo finito, existem $t \in \mathbb{N}$ e $x_1, \dots, x_t \in M$ tais que $M = \langle x_1, \dots, x_t \rangle$. Consideremos um submódulo-R N próprio de M e a família

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

Uma vez que N é submódulo-R próprio de M, $N \in \mathcal{F}$ e $\mathcal{F} \neq \emptyset$. Então, $(\mathcal{F}, \subseteq)$ é um conjunto parcialmente ordenado. Seja $\mathcal{C} = \{P_i\}_{i\in I}$ uma cadeia não vazia de elementos de $\mathcal{F}$. Tomemos

$$Q = \bigcup_{i\in I} P_i.$$

Como $\mathcal{C}$ é uma cadeia e $P_i \leq_R M$ para todo o $i \in I$, temos que Q é submódulo-R de M. Dado $j \in I$, $P_j \subseteq Q$. Uma vez que $N \leq_R P_j$ e $P_j \leq_R Q$, sabemos que $N \leq_R Q$. Logo,

$$N \leq_R Q \leq_R M.$$

Suponhamos que $Q = M$. Então, como $M = \langle x_1, \dots, x_t \rangle$, existem $i_1, \dots, i_t \in I$ tais que $x_1 \in P_{i_1}, \dots, x_t \in P_{i_t}$. Mas $\mathcal{C}$ é uma cadeia e, portanto, existe $k \in I$ tal que $P_{i_\ell} \subsetneq P_k$ para todo o $\ell \in \{1, \dots, t\}$. Assim, $x_1, \dots, x_t \in P_k$, pelo que $P_k = \langle x_1, \dots, x_t \rangle = M$, um absurdo. Logo, $Q \lneq_R M$ e, por definição, $Q \in \mathcal{F}$. Então, $\mathcal{C}$ admite majorante, Q.

Vimos que toda a cadeia não vazia de elementos de $\mathcal{F}$ admite majorante. Pelo Lema de Zorn, $\mathcal{F}$ admite elemento maximal L. Pretendemos mostrar que L é um submódulo-R maximal de M. Suponhamos que tal não se verifica. Então, existe $T \leq_R M$ tal que $L \lneq_R T \lneq_R M$.
Como $L \in \mathcal{F}$, $L \leq_R M$ e $N \leq_R L \lneq_R M$. Assim, $T \leq_R M$ e $N \leq_R T \lneq_R M$, pelo que $T \in \mathcal{F}$, o que contradiz o facto de L ser elemento maximal de $\mathcal{F}$. Logo, L é submódulo-R maximal de M e contém N. □

Corolário. Seja M um módulo-R não nulo e de tipo finito. Então, M contém submódulos-R maximais.

Demonstração. Como M é não nulo, $\{0\}$ é submódulo-R próprio de M. Pela proposição anterior, $\{0\}$ está contido num submódulo-R maximal de M. Logo, M contém, pelo menos, esse submódulo-R maximal. □

Definição. Seja I um ideal direito [respetivamemte: esquerdo] de R. Dizemos que I é um *ideal direito maximal de* R [respetivamente: *ideal esquerdo maximal de* R] se I for submódulo-R maximal de R_R [respetivamente: ${}_R R$].

Definição. Seja I um ideal de R. Dizemos que I é *ideal maximal de* R se for elemento maximal do c.p.o, para a relação de inclusão, dos ideais próprios de R.

Exemplo. Os ideais maximais do anel $\mathbb{Z}$ são todos os ideais $p\mathbb{Z}$ com p primo. [exercício!]

Teorema de Krull. Seja R um anel unitário. Então, todo o ideal direito [respetivamente: esquerdo] próprio de R está contido num ideal direito [respetivamente: esquerdo] maximal de R.

Demonstração. Como R é anel unitário, $R_R = \langle 1 \rangle$ é módulo-R não nulo e de tipo finito. Seja I um ideal direito próprio de R. Então, I é submódulo-R próprio de R_R. Pela proposição anterior, I está contido num submódulo maximal de R, isto é, num ideal direito maximal de R.

De um modo dual, obtemos o resultado relativo a ideais esquerdos próprios de R. □

Teorema. Seja R um anel unitário. Então, todo o ideal próprio de R está contido num ideal maximal de R.

Demonstração. [exercício!]

Corolário. Se R é um anel unitário, então R admite ideais direitos [respetivamente: esquerdos, bilaterais].

Demonstração. [exercício!]

Proposição. Seja I um ideal direito [respetivamente: esquerdo, bilateral] próprio de R. Então, I é ideal direito [respetivamente: esquerdo, bilateral] maximal de R se e só se $(I : a)_d = R$ [respetivamente: $(I : a)_e = R$, $(I : a) = R$] para qualquer $a \in R \setminus I$.

Demonstração. Seja I um ideal direito próprio de R. Admitamos que I é ideal direito maximal de R e tomemos $a \in R \setminus I$. Então, $(I : a)_d$ é ideal direito de R e, por definição, $I \subsetneq (I : a)_d$. Como I é maximal, $(I : a)_d = R$.

Reciprocamente, admitamos que $(I : a)_d = R$ para todo o $a \in R \setminus I$. Seja L um ideal direito de R tal que $I \subsetneq L \subseteq R$. Como $I \subsetneq L$, existe $a \in L \setminus I \subseteq R \setminus I$. Por hipótese, $(I : a)_d = R$. Logo,

$$R = (I : a)_d \subseteq L \subseteq R$$

e, portanto, $L = R$. Portanto, I é ideal direito maximal de R. □

Proposição. Todo o submódulo simples de M está contido em todos os submódulos essenciais de M.

Demonstração. Seja N um submódulo simples de M. Então $N \leq_R M$, $N \neq \{0\}$ e os únicos submódulos-R de N são $\{0\}$ e N.
Seja P um submódulo essencial de M. Como $N \neq \{0\}$ e $N \leq_R M$, $P \cap N \neq \{0\}$. Assim, $P \cap N \leq_R N$ e $P \cap N \neq \{0\}$. Sendo N um submódulo simples, $P \cap N = N$ e, portanto, $N \subseteq P$. Logo, N está contido em todos os submódulos essenciais de M. □

Proposição. Sejam R um anel unitário e M um módulo-R unitário. Então, M é módulo-R simples se e só se existe um ideal direito maximal I de R tal que M e R/I são módulos-R isomorfos.

Demonstração. Admitamos que M é módulo-R simples. Então, M é não nulo e os únicos submódulos-R de M são $\{0\}$ e M.
Como $M \neq \{0\}$, existe $x \in M \setminus \{0\}$. Sendo R um anel unitário e M um módulo-R unitário, $x \in xR$. Logo, $xR \neq \{0\}$. Assim, $\{0\} \neq xR \leq_R M$, o que implica que $xR = M$ (pois M é módulo-R simples).
Consideremos, então, a aplicação $\theta : R \to M$ definida por $\theta(r) = xr$ para todo o $r \in R$. Não é difícil de verificar que θ é um epimorfismo-R [exercício!]. Pelo Teorema do Homomorfismo,

$$R/\text{Ker}\theta \cong \theta(R) = M.$$

Temos que $\text{Ker}\theta = \{a \in R : \theta(a) = 0\} = \{a \in R : xa = 0\} = r(x)$. Resta provar que $r(x)$ é um ideal direito maximal de R.
Facilmente se prova que $r(x)$ é ideal direito de R. Como $x \neq 0$, $1 \notin r(x)$ e, portanto, $r(x)$ é um ideal direito próprio de R. Seja $b \in R \setminus r(x)$. Então, $xb \neq 0$ (pois $b \notin r(x)$). Como M é módulo-R, $xb \in M$. Logo, $xb \in M \setminus \{0\}$ e, assim, $M = xbR$
Mas $x \in M$, pelo que existe $c \in R$ tal que $x = xbc$. Assim,

$$0 = x - xbc = x(1 - bc),$$

pelo que $1-bc \in r(x)$. Logo, $1 \in (r(x), b)_d$, pelo que $R \subseteq (r(x), b)_d$. Por definição, $(r(x), b)_d \subseteq R$. Logo $(r(x), b)_d = R$ e $r(x)$ é ideal direito maximal de R.

Reciprocamente, admitamos que existe um ideal direito maximal I de R tal que M e R/I são módulos-R isomorfos. Como I é ideal direito maximal, I é submódulo-R maximal de R_R Logo, R/I é módulo simples. Por isomorfismo, M é também módulo simples. □

Observação.

1. Sejam R um anel unitário e M um módulo-R unitário. Então, M é um módulo-R simples se e só se M é um módulo cíclico não nulo e os anuladores direitos de elementos não nulos de M são ideais direitos maximais de R.

2. Se um módulo não for de tipo finito, pode não conter submódulos maximais. Consideremos, por exemplo, o conjunto dos números racionais $\mathbb{Q}$. Ora, $\mathbb{Q}$ é um módulo-$\mathbb{Z}$ e não é do tipo finito. Suponhamos que $\mathbb{Q}$ contém um submódulo-$\mathbb{Z}$ maximal N. Então, $\mathbb{Q}/N$ é um módulo-$\mathbb{Z}$ simples e, portanto, $\mathbb{Q}/N$ é módulo-ZZ cíclico não nulo.

   Seja $a + N \in \mathbb{Q}/N \setminus \{N\}$. Então, $\mathbb{Q}/N = (a + N)\mathbb{Z}$ e $r(a + N)$ é um ideal direito maximal de $\mathbb{Z}$. Assim, existe p primo tal que

   $$r(a + N) = p\mathbb{Z}.$$

   Como $a, p \in \mathbb{Q}$, é claro que existe $c \in \mathbb{Q}$ tal que $a = pc$. Ora,

   $$c + N \in Q/N = (a + N)\mathbb{Z},$$

   pelo que existe $t \in \mathbb{Z}$ tal que $c + N = (a + N)t$. Assim,

   $$a + N = pc + N = (c + N)p = (a + N)tp = N,$$

uma vez que $p \in p\mathbb{Z} = r(a + N)$. Chegamos, pois, a uma contradição que resulta de supormos que $\mathbb{Q}$ contém um submódulo-$\mathbb{Z}$ maximal. Logo, $\mathbb{Q}$ não admite submódulos-$\mathbb{Z}$ maximais.

3. Se R não for unitário, então R não possui necessariamente ideais direitos maximais. Consideremos $(\mathbb{Q}, +, .)$, com $a.b = 0$ para todos os $a, b \in \mathbb{Q}$. Então, $(\mathbb{Q}, +, .)$ é um anel comutativo não unitário. Mais, I é um ideal de $(\mathbb{Q}, +, .)$ se e só se $(I, +)$ é subgrupo de $(\mathbb{Q}, +)$. Mas esta última condição é equivalente a I é submódulo-$\mathbb{Z}$ de $\mathbb{Q}$. Por **2.**, I não é submódulo-$\mathbb{Z}$ maximal de $\mathbb{Q}$ e, portanto, I não é ideal direito maximal de $\mathbb{Q}$.

Proposição. Sejam R um anel comutativo unitário e I um ideal de R. Então, I é ideal maximal de R se e só se R/I é corpo.

Demonstração. Admitamos que I é ideal direito maximal de R. Então, $I \subsetneq R$ e, assim, $R/I \neq \{I\}$. Como R é um anel comutativo unitário, também R/I é comutativo e unitário. Seja $a + I \in R/I \setminus \{I\}$. Como I é ideal direito maximal de R, sabemos que $(I, a)_d = R$. Sendo R unitário, $(I, a) = I + aR$. Logo, $I + aR = R$. Portanto, existem $i \in I$, $r \in R$ tais que $1 = i + ar$. Logo,

$$1 + I = (i + ar) + I = ar + I = (a + I)(r + I).$$

Por outras palavras, vimos que todos os elementos não nulos de R/I são invertíveis à direita. Logo, todos os elementos não nulos de R/I são invertíveis e R/I é corpo.

Reciprocamente, admitamos que R/I é corpo e tomemos $a \in R \setminus I$. Pretendemos mostrar que $(I, a) = R$. Ora, como $a \notin I$, $a + I \in R/I \setminus \{I\}$. Logo, existe $b \in R$ tal que

$$(a + I)(b + I) = 1 + I,$$

ou seja, $1 - ab \in I$. Portanto, $1 \in I + aR = (I, a)$ e, assim, $R \subseteq (I, a)$. Então, $(I, a) = R$ e I é ideal maximal de R. □

Observação.

1. Seja R um anel de divisão. Então, $R \neq \{0\}$ e os únicos ideais de R são $\{0\}$ e R. Portanto, R é um anel simples.

2. Seja R um anel comutativo, unitário e simples. Então, os únicos ideais de R são $\{0\}$ e T. Em particular, $\{0\}$ é um ideal maximal de R, pelo que $R/\{0\}$ é corpo. Como R é isomorfo a $R/\{0\}$, R é corpo.

3. Existem anéis unitários e simples que não são anéis de divisão. Consideremos, por exemplo, o conjunto $\mathcal{M}_2(\mathbb{R})$ de todas as matrizes quadradas reais de ordem 2. Sabemos que $\mathcal{M}_2(\mathbb{R})$ não é anel de divisão: basta tomar a matriz $P = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ que é não nula e não invertível.

Seja I um ideal não nulo de $\mathcal{M}_2(\mathbb{R})$ e seja $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in I \setminus \{0\}$. Suponhamos, sem perdas de generalidade, que $a_{11} \neq 0$. Facilmente se verifica que $PAP = \begin{bmatrix} a_{11} & 0 \\ 0 & 0 \end{bmatrix}$. Mais, sendo I um ideal, $PAP \in I$. Como $a_{11} \neq 0$, existe a_{11}^{-1}. Temos que

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_{11}^{-1} & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & 0 \\ 0 & 0 \end{bmatrix} \in I;$$

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I;$$

$$\begin{bmatrix} 0 & a_{11} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_{11} & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in I;$$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_{11}^{-1} & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & a_{11} \\ 0 & 0 \end{bmatrix} \in I;$$

$$\begin{bmatrix} 0 & 0 \\ a_{11} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & 0 \\ 0 & 0 \end{bmatrix} \in I;$$

$$\begin{bmatrix} 0 & 0 \\ 0 & a_{11} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a_{11} & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in I;$$

e

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & a_{11}^{-1} \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & a_{11} \end{bmatrix} \in I.$$

Portanto, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in I$, pelo que

$$\mathcal{M}_2(\mathbb{R}) = \langle \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \rangle \subseteq I.$$

Logo, $I = \mathcal{M}_2(\mathbb{R})$ e $\mathcal{M}_2(\mathbb{R})$ é simples e unitário.

Proposição. Sejam R um anel e I um ideal de R. Então, I é ideal maximal de R se e só se R/I for anel simples.

Demonstração. Admitamos que I é ideal maximal de R. Então, $I \subsetneq R$ e, portanto, $R/I \neq \{I\}$. Seja P/I um ideal de R/I. Então, $I \subseteq P$ e P é ideal de R. Como I é ideal maximal de R, $P = I$ ou $P = R$. Se $P = I$, então $P/I = \{I\}$. Se $P = R$, então $P/I = R/I$. Logo, R/I é um anel simples.

Reciprocamente, admitamos que R/I é um anel simples. Então, $R/I \neq \{I\}$ e, portanto, $I \subsetneq R$. Seja P um ideal de R tal que $I \subsetneq P \subseteq R$. Então, P/I é ideal não nulo de R/I. Sendo R/I um anel simples, podemos concluir que $P/I = R/I$. Logo, $P = R$. Portanto, I é ideal maximal de R. □

Proposição. Seja R um anel unitário. Então, são equivalentes as seguintes condições:

(a) (0) é ideal direito [respetivamente: esquerdo] maximal;

(b) R_R [respetivamente: ${}_RR$] é módulo-R simples;

(c) Todo o elemento não nulo de R é invertível à direita;

(d) Todo o elemento não nulo de R é invertível.

Demonstração. Admitamos que (0) é ideal direito maximal. Então, (0) é submódulo maximal de R_R. Assim, dado um submódulo N de R_R, temos que $\{0\} \subseteq N \subseteq R_R$ e, pela maximalidade de (0), segue que $N = \{0\}$ ou $N = R$. Portanto, os únicos submódulos-R de R_R são $\{0\}$ e R_R. Logo, R_R é módulo-R simples.

Suponhamos, agora, que R_R é um módulo-R simples. Seja $a \in R \setminus \{0\}$. Então, aR é submódulo-R de R_R e é não nulo (uma vez que $a = a1 \in aR$), pelo que $aR = R$. Como $1 \in R$, existe $b \in R$ tal que $1 = ab$. Por outras palavras, vimos que todos os elementos não nulos de R são invertíveis à direita.

Admitamos que todos os elementos não nulos de R são invertíveis à direita e tomemos $a \in R \setminus \{0\}$. Por hipótese, existe $b \in \mathbb{R} \setminus \{0\}$ tal que $ab = 1$. Como $b \in R \setminus \{0\}$, existe $c \in R \setminus \{0\}$ tal que $bc = 1$. Ora,

$$a = a.1 = a(bc) = (ab)c = 1.c = c.$$

Assim, existe $b \in R \setminus \{0\}$ tal que $ab = 1 = ba$ e a é invertível. Portanto, todos os elementos não nulos de R são invertíveis.

Por fim, suponhamos que todo o elemento não nulo de R é invertível. Seja $r \in R \setminus \{0\}$. Pretendemos mostrar que $((0), r)_d = R$. Como $r \neq 0$, existe $a \in R \setminus \{0\}$ tal que $ar = ra = 1$. Logo, $1 \in rR = ((0), r)_d$, pelo que $R \subseteq ((0), r)_d$.Portanto, $(0), r)_d = R$ e (0) é ideal direito maximal de R. □

No que se segue, R é um anel não nulo.

Definição. Seja S um subconjunto não vazio de R.

1. Diz-se que S é um *conjunto multiplicativamente fechado* ou *multiplicativo* se, para todos os elementos $a, b \in S$, se tiver $ab \in S$.

2. Diz-se que S é um *conjunto semimultiplicativamente fechado* ou *semimultiplicativo* se, para todos os elementos $a, b \in S$, existir um elemento $c \in R$ tal que $acb \in S$.

Proposição. Todo o subconjunto multiplicativo de R é um conjunto semimultiplicativo.

Seja S um subconjunto multiplicativo de R e sejam $a, b \in S$. Por definição, $aa \in S$ e, portanto, $aab = (aa)b \in S$. Logo, existe $a \in S$ tal que $aab \in S$, pelo que S é semimultiplicativo. □

Exemplos.

1. $\{0\}$ é um conjunto multiplicativo.
2. Seja $a \in R$. Então, $S_a = \{a^n : n \in \mathbb{N}\}$ é multiplicativo.

2.2. Ideais primos

No que se segue, R é um anel comutativo.

Definição. Seja P um ideal próprio de R.

1. Diz-se que P é um *ideal completamente primo* se R/P for domínio de integridade.
2. Diz-se que P é um *ideal primo* se, para quaisquer elementos $a, b \in R$ tais que $aRb \subseteq P$ se tiver $a \in P$ ou $b \in P$.

Proposição. Seja P um ideal de R. Se P é completamente primo, então P é ideal primo de R.

Demonstração. Admitamos que P é completamente primo. Então, R/P é domínio de integridade. Dados $a, b \in R$ tais que $aRb \subseteq P$, temos que $aab \in P$. Logo,

$$(a + P)(a + P)(b + P) = aab + P = P.$$

Sendo R/P um domínio de integridade, $a + P = P$ ou $b + P = P$. Logo, $a \in P$ ou $b \in P$, pelo que P é um ideal primo. □

Proposição. Seja P um ideal de R. Então, são equivalentes as seguintes condições.

(a) P é ideal primo de R.

(b) O conjunto $S = R \setminus P$ é semimultiplicativo.

Demonstração. Admitamos que P é ideal primo de R. Então $P \subsetneq R$ e $S = R \setminus P \neq \emptyset$. Sejam $a, b \in S$. Então, $a \notin P$ e $b \notin P$. Como P é ideal primo, $aRb \not\subset P$. Assim, existe $arb \in aRb$ tais que $arb \notin P$, isto é, $arb \in S$. Portanto, dados $a, b \in S$, existe $r \in R$ tal que $arb \in S$. Por definição, S é semimultiplicativo.

Reciprocamente, admitamos que S é semimultiplicativo. Então, $S \neq \emptyset$ e $P \subsetneq R$. Sejam $a, b \in R$ tais que $aRb \subseteq P$. Suponhamos que $a \notin P$ e $b \notin P$. Então, $a, b \in S = R \setminus P$ e, como S é semimultiplicativo, existe $r \in R$ tal que $arb \in S$. Ou seja, existe $r \in R$ tal que $arb \notin P$,

o que contradiz o facto de aRb estar contido em P. Assim, $a \in P$ ou $b \in P$ e, por definição, P é um ideal primo de R. □

Exemplo. Dado um número primo p, não é difícil de mostrar que $S = \mathbb{Z}\backslash p\mathbb{Z}$ é multiplicativo. De facto, dados $a, b \in S$, se $ab \in p\mathbb{Z}$, então existe $q \in \mathbb{Z}$ tal que $ab = pq$. Ora, $a|ab$. Como $ab = pq$, podemos concluir que $a|pq$ e, assim, existe $r \in \mathbb{Z}$ tal que $a = pqr$. Logo, $a \in p\mathbb{Z}$, o que contradiz o facto de a pertencer a S. Logo, $ab \notin p\mathbb{Z}$ e, portanto, $ab \in S$. Vimos, assim, que S é multiplicativo. Então, podemos concluir que S é semimultiplicativo e, pela proposição anterior, $p\mathbb{Z}$ é ideal primo.

Proposição. Sejam P um ideal primo de R e $k \in \mathbb{N}$. Se $I_1, \ldots, I_k$ forem ideais direitos [respetivamente: esquerdos, bilaterais] de R tais que $I_1 \ldots I_k \subseteq P$, então existe $j \in \{1, \ldots, k\}$ tal que $I_j \subseteq P$.

Demonstração. É claro que o resultado é válido para $k = 1$. Comecemos, pois, por mostrar que o resultado se verifica para $k = 2$. Sejam I_1, I_2 dois ideais direitos de R tais que $I_1 I_2 \subseteq P$. Suponhamos que $I_1 \not\subset P$ e $I_2 \not\subset P$. Então, existem $x_1 \in I_1$, $x_2 \in I_2$ tais que $x_1, x_2 \notin P$. Sendo I_1 um ideal direito de R, $x_1 R \subseteq I_1$. Portanto, $x_1 R x_2 \subseteq I_1 I_2 \subseteq P$. Sendo P um ideal primo, $x_1 \in P$ ou $x_2 \in P$, uma contradição. Logo, $I_1 \subseteq P$ ou $I_2 \subseteq P$.

Suponhamos, agora, que o resultado é válido para $k-1$ e admitamos que $I_1, \ldots, I_{k-1}, I_k$ são ideais direitos de R tais que $I_1 \ldots I_{k-1} I_k \subseteq P$. Como $I_1 \ldots I_{k-1}, I_k$ são ideais direitos de R tais que $(I_1 \ldots I_{k-1}) I_k \subseteq P$, podemos concluir que $I_1 \ldots I_{k-1} \subseteq P$ ou I_k. Por hipótese, de $I_1 \ldots I_{k-1} \subseteq P$, segue que existe $j_0 \in \{1, \ldots, k-1\}$ tal que $I_{j_0} \subseteq P$. Logo, existe $j \in \{1, \ldots, k\}$ tal que $I_j \subseteq P$. □

Corolário. Sejam P um ideal primo de R e I um ideal direito [respetivamente: esquerdo, bilateral] nilpotente de R, Então, $I \subseteq P$.

Demonstração. [exercício!]

Proposição. Sejam P um ideal primo de R, $k \in \mathbb{N}$ e $I_1, \ldots, I_k$ ideais de R tais que $I_1 \cap \cdots \cap I_k = P$. Então, existe $j \in \{1, \ldots, k\}$ tal que $I_j = P$.

Demonstração. Para todo o $i \in \{1, \ldots, k\}$, I_i é um ideal de R e, portanto, $I_1 \ldots I_k \subseteq I_i$. Logo,

$$I_1 \ldots I_k \subseteq I_1 \cap \cdots \cap I_k = P.$$

Pela proposição anterior, como P é ideal primo de R, existe $j \in \{1, \ldots, k\}$ tal que $I_j \subseteq P$. Como $P \subseteq I_j$, temos que $I_j = P$. □

Lema. Sejam $S \subseteq R$ conjunto semimultiplicativo e J ideal de R tais que $J \cap S = \emptyset$. Então, existe P ideal primo de R tal que $J \subseteq P$ e $P \cap S = \emptyset$.

Demonstração. Consideremos a família

$$\mathcal{F} = \{I : I \text{ é ideal de } R, J \subseteq I \text{ e } I \cap S = \emptyset\}.$$

Por hipótese, $J \in \mathcal{F}$ e, portanto, $\mathcal{F} \neq \emptyset$. Não é difícil de verificar que $(\mathcal{F}, \subseteq)$ é um conjunto parcialmente ordenado. Seja $\mathcal{C} = \{I_k\}_{k \in K}$ uma cadeia não vazia de elementos de $\mathcal{F}$ e consideremos

$$Q = \bigcup_{k \in K} I_k.$$

Como $\mathcal{C}$ é uma cadeia, Q é um ideal de R. Para todo o $k \in K$, $J \subseteq I_k$. Logo, $J \subseteq Q$. Assim,

$$Q \cap S = \left(\bigcup_{k \in K} I_k \right) \cap S = \bigcup_{k \in K} (I_k \cap S) = \emptyset.$$

Logo, $Q \in \mathcal{F}$ e, portanto, $\mathcal{C}$ admite majorante. Pelo Lema de Zorn, $\mathcal{F}$ admite elemento maximal, digamos P. Por definição de $\mathcal{F}$, P é um ideal de R que contém J e é tal que $P \cap S = \emptyset$. Falta mostrar que P é um ideal primo.

Como S é um conjunto semimultiplicativo, $S \neq \emptyset$. Assim, $P \subsetneq R$ (uma vez que $P \cap S = \emptyset$). Sejam $a, b \in R$ tais que $aRb \subseteq P$. Suponhamos que $a \notin P$ e $b \notin P$. Então, $P \subsetneq P + (a)$. Como $P + (a)$ é um ideal de R que contém J e P é elemento maximal de $\mathcal{F}$, podemos concluir que

$$(P + (a)) \cap S \neq \emptyset.$$

De modo análogo, concluímos que

$$(P + (b)) \cap S \neq \emptyset.$$

Portanto, existem $r \in (P + (a)) \cap S$ e $s \in (P + (b)) \cap S$. Recordemos que

$$(a) = \{ra + a\ell + na + \sum r_i a \ell_i : r, \ell, r_i, \ell_i \in P, n \in \mathbb{N}\},$$

$$(b) = \{r'b + b\ell' + n'b + \sum r'_i b \ell'_i : r', \ell', r'_i, \ell'_i \in P, n' \in \mathbb{N}\}.$$

Logo,

$$rRs \subseteq (P + (a))R(P + (b)) \subseteq P + (a)R(b) \subseteq P.$$

Como $r, s \in S$ e S é semimultiplicativo, existe $c \in R$ tal que $rcs \in S$. Mas $rcs \in rRs \subseteq P$, o que contradiz o facto de $P \cap S = \emptyset$. Logo, $a \in P$ ou $b \in P$. Por definição, P é ideal primo. □

Corolário. Seja $S \subseteq R$ um conjunto semimultiplicativo tal que $0 \notin S$. Então, existe um ideal primo P tal que $P \cap S = \emptyset$.

Demonstração. [exercício!]

Observação. A interseção de ideais primos não é necessariamente um ideal primo. Consideremos, por exemplo o anel $\mathbb{Z}$ e os ideais $3\mathbb{Z}$ e $5\mathbb{Z}$ de $\mathbb{Z}$. Como 3 e 5 são números primos, $3\mathbb{Z}$ e $5\mathbb{Z}$ são ideais primos de $\mathbb{Z}$. No entanto, $3\mathbb{Z} \cap 5\mathbb{Z} = 15\mathbb{Z}$. Como 15 não é um número primo, $3\mathbb{Z} \cap 5\mathbb{Z}$ não é um ideal primo de $\mathbb{Z}$.

Lema. A interseção de ideais de qualquer cadeia não vazia de ideais primos de R é ideal primo de R.

Demonstração.

1. Seja $I_1 \subseteq I_2 \subseteq \ldots$ uma cadeia ascendente de ideais primos. A interseção de ideais da cadeia é um elemento da cadeia. Logo, é ideal primo de R.

2. Seja $\mathcal{C} = \{I_k\}_{k\in K}$ uma cadeia descendente de ideais primos de R. Consideremos um subconjunto T de K e seja $D = \bigcap_{k\in T} I_k$. Como I_k é um ideal próprio de R para todo o $k \in T$, também D é ideal próprio de R. Sejam $x, y \in R$ tais que $xRy \subseteq D$ e suponhamos que $y \notin D$. Então, existe $t \in T$ tal que $y \notin I_t$. Sendo $\mathcal{C}$ uma cadeia descendente, $y \notin I_k$ para todo o $k \in T$ tal que $I_t \supseteq I_k$. Ora,

$$xRy \subseteq D \subseteq I_k,$$

para todo o $k \in T$ tal que $I_t \supseteq I_k$. Logo, uma vez que I_k é ideal primo, $x \in I_k$. Mas $\mathcal{C}$ é uma cadeia descendente e, portanto, $x \in I_k$ para todo o $k \in T$. Logo, $x \in D$. Portanto, D é ideal primo de R. □

Definição. À família de todos os ideais primos de R dá-se o nome de *espectro de* R e denota-se por $\mathrm{Spec}(R)$.

Definição. Diz-se que R é um *anel primo* se (0) é um ideal primo de R.

Proposição. Seja P um ideal próprio de R, Então P é ideal primo de R se e só se R/P é um anel primo.

Demonstração. Admitamos que P é ideal primo de R. Então, $P \subsetneq R$, pelo que $R/P \neq \{P\}$. Sejam $a+P, b+P \in R/P$ tais que $(a+P)R/P(b+P) \subseteq \{P\}$. Então, $(a+P)R/P(b+P) = \{P\}$. Portanto, para todo o $r \in R$,

$$arb + P = (a + P)(r + P)(b + P) = P,$$

pelo que $arb \in P$. Assim, $aRb \subseteq P$ e, sendo P primo, $a \in P$ ou $b \in P$. Logo, $a + P = P$ ou $b + P = P$. Portanto, $a + P \in \{P\}$ ou $b + P \in \{P\}$, pelo que $\{P\}$ é ideal primo de R/P e R/P é anel primo.

Reciprocamente, admitamos que R/P é anel primo. Então, $\{P\}$ é ideal primo de R/P e, em particular, $P \subsetneq R$. Sejam $a, b \in R$ tais que $aRb \subseteq P$. Então, para todo o $r \in R$, $arb \in P$ e, portanto,

$$(a + P)(r + P)(b + P) = arb + P = P.$$

Logo, $(a+P)R/P(b+P) \subseteq \{P\}$ e, sendo $\{P\}$ ideal primo de R/P, $a+P \in \{P\}$ ou $b+P \in \{P\}$. Assim, $a \in P$ ou $b \in P$. Por outras palavras, P é ideal primo de R. □

Proposição. Sejam R um anel primo e $f \in R$ um idempotente não nulo. Então, fRf é um anel primo.

Demonstração. Como R é um anel primo, sabemos que (0) é ideal primo de R. Por outro lado, sabemos também que fRf é um anel. Sejam $x, y \in fRf$ tais que $x(fRf)y \subseteq (0)$. Então, $x(fRf)y = (0)$. Como $x, y \in fRf$, $x = fxf$ e $y = fyf$. Para todo o $r \in R$,

$$xry = (fxf)r(fyf) = fxf^2rf^2yf = (fxf)(frf)(fyf) = x(frf)y \in x(fRf)y = (0).$$

Logo, $xRy = (0)$, pelo que $x \in (0)$ ou $y \in (0)$ (pois $x, y \in R$ e (0) é ideal primo de R). Portanto, (0) é ideal primo de fRf e fRf é anel primo. □

Definição. Seja P um ideal primo de R. Dizemos que P é *ideal primo minimal de* R se for minimal entre os ideais primos de R.

Proposição. Todo o ideal primo de R contém um ideal primo minimal.

Demonstração. Seja P um ideal primo de R. Consideremos a família

$$\mathcal{F} = \{I : I \text{ é ideal primo de } R \text{ e } I \subseteq P\}.$$

Como P é ideal primo de R e $P \subseteq P$, temos que $P \in \mathcal{F}$. Logo, $\mathcal{F} \neq \emptyset$. Não é difícil de provar que $(\mathcal{F}, \supseteq)$ é um conjunto parcialmente ordenado. Consideremos uma cadeia não vazia $\mathcal{C} = \{\mathcal{I}_\parallel\}_{\parallel \in \mathcal{K}}$ de elementos de $\mathcal{F}$. Pelo Lema anterior, $\bigcap_{k \in K} I_k$ é um ideal primo de R. Mais, $I_k \subseteq P$ para todo o $k \in K$, pelo que $\bigcap_{k \in K} I_k \subseteq P$. Logo, $\bigcap_{k \in K} I_k \in \mathcal{F}$ e $\mathcal{C}$ tem majorante.

Pelo Lema de Zorn, $\mathcal{F}$ admite elemento maximal, digamos Q. Por definição de $\mathcal{F}$, Q é ideal primo de R e $Q \subseteq P$. Seja L um ideal primo de R tal que $(0) \subsetneq L \subseteq Q$. Então, L é ideal primo de L e $L \subseteq P$, pelo que $L \in \mathcal{F}$. Como Q é elemento maximal de $\mathcal{F}$, $L = Q$. Assim, Q é um ideal primo minimal de R contido em P. □.

Observação. Se R é um anel primo, então (0) é o único ideal primo minimal de R.

Proposição. Seja R um anel comutativo. Então, são equivalentes as seguintes condições.

(a) P é ideal primo de R.

(b) P é ideal próprio de R e, para todos os $a, b \in R$ tais que $ab \in P$, tem-se $a \in P$ ou $b \in P$.

(c) P é ideal completamente primo de R.

(d) O conjunto $S = R \setminus P$ é multiplicativo.

Demonstração. Admitamos que P é ideal primo de R. Por definição, $P \subsetneq R$. Sejam $a, b \in R$ tais que $ab \in P$. Como P é ideal de R, $abR \subseteq P$. Sendo R comutativo, $aRb = abR \subseteq P$. Logo, de P ser ideal primo de R segue que $a \in P$ ou $b \in P$.

Admitamos, agora, que a condição **(b)** é válida. Sejam $a + P, b + P \in R/P$ tais que $(a + P)(b + P) = P$. Então,

$$ab + P = (a + P)(b + P) = P,$$

pelo que $ab \in P$. Por hipótese, $a \in P$ ou $b \in P$, ou seja, $a + P = P$ ou $b + P = P$. Logo, R/P é um domínio de integridade e, por definição, P é completamente primo.

Suponhamos, agora, que P é ideal completamente primo de R. Então, P é ideal primo e $P \subsetneq R$. Portanto, $S = R \setminus P \neq \emptyset$. Sejam $a, b \in S$. Então, $a \notin P$ e $b \notin P$. Como P é ideal

primo e vimos que **(a)** implica **(b)**, podemos concluir que $ab \notin P$, ou seja, $ab \in S$. Logo, S é multiplicativo.

Por fim, admitamos que S é multiplicativo. Em particular, S é semimultiplicativo, pelo que P é ideal primo de R. □

Proposição. Sejam R um anel comutativo e I, J ideais de R tais que $J \subseteq I$. Então, I/J é ideal primo de R/J se e só se I é ideal primo de R.

Demonstração. Pelo Teorema do Isomorfismo, R/I é isomorfo a $(R/J)/(I/J)$. Ora, I/J é ideal primo de R/J se e só se $(R/J)/(I/J)$ é anel primo, o que é equivalente a dizer que R/I é anel primo. A última condição é equivalente a dizer que I é ideal primo de R: □.

Exemplos.

1. Os únicos ideais primos de $\mathbb{Z}$ são (0) e $p\mathbb{Z}$, com p primo. Logo, (0) é o único ideal primo minimal de $\mathbb{Z}$.
2. Dado $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$, os únicos ideais primos de $\mathbb{Z}/n\mathbb{Z}$ são os ideais $t\mathbb{Z}/n\mathbb{Z}$ com t primo. Mais, $t\mathbb{Z}/n\mathbb{Z}$ com t primo, é ideal primo minimal de $\mathbb{Z}/n\mathbb{Z}$.
3. Seja K um corpo e x uma indeterminada. Seja $R = K[x]$. Então, $(x-a)R$, com $a \in K$, é ideal primo de R. [exercício!]

Proposição. Sejam R um anel unitário e P um ideal próprio de R. Então, são equivalentes as seguintes condições:

(a) P é ideal primo de R.

(b) Dados I e J ideais direitos de R, se $IJ \subseteq P$ então $I \subseteq P$ ou $J \subseteq P$.

(c) Dados I e J ideais esquerdos de R, se $IJ \subseteq P$ então $I \subseteq P$ ou $J \subseteq P$.

(d) Dados I e J ideais de R, se $IJ \subseteq P$ então $I \subseteq P$ ou $J \subseteq P$.

(e) Não existem ideais L e M de R tais que $P \subsetneq L$, $P \subsetneq M$ e $LM \subseteq P$.

Demonstração. Admitamos que P é ideal primo de R e consideremos I, J ideais direitos de R tais que $IJ \subseteq P$. Por uma proposição anterior, $I \subseteq P$ ou $J \subseteq P$.

Suponhamos agora que, para todos os ideais direitos K, Q de R tais que $KQ \subseteq P$ se tem $K \subseteq P$ ou $Q \subseteq P$. Sejam I, J ideais esquerdos de R tais que $IJ \subseteq P$. Então, IR, JR são dois ideais direitos de R. Além disso,

$$(IR)(JR) = I(RJ)R \subseteq IJR = (IJ)R \subseteq PR \subseteq P.$$

Por hipótese, $IR \subseteq P$ ou $JR \subseteq P$. Como R é unitário, $I \subseteq IR \subseteq P$ ou $J \subseteq JR \subseteq P$.

É imediato que **(c)** implica **(d)**. Admitamos que **(d)** é válida e suponhamos que existem ideais L e M de R tais que $P \subsetneq L$, $P \subsetneq M$ e $LM \subseteq P$. Por hipótese, sendo L e M ideias de

R tais que $LM \subseteq P$, segue que $L \subseteq P$ ou $M \subseteq P$. Assim, $L = P$ ou $M = P$, o que é uma contradição.

Por último, assumamos que **(e)** é válida e tomemos $x, y \in R$ tais que $xRy \subseteq P$. Suponhamos que $y \notin P$. Então, $P \subsetneq P + (y)$ e $P \subseteq P + (x)$. Como

$$(P + (x))(P + (y)) = P + (x)(y) \subseteq P + xRy \subseteq P,$$

podemos concluir que $P = P + (x)$ e, portanto, $x \in P$. □

Corolário. Seja R um anel unitário. Então, são equivalentes as seguintes condições.

(a) Se $a, b \in R \setminus \{0\}$ então $aRb \neq (0)$.

(b) Dados I e J ideais direitos não nulos de R, $IJ \neq (0)$.

(c) Dados I e J ideais esquerdos não nulos de R, $IJ \neq (0)$.

(d) Dados I e J ideais não nulos de R, $IJ \neq (0)$.

(e) R é anel primo.

Proposição. Seja R um anel unitário. Então, todo o ideal maximal de R é primo.

Demonstração. Seja P um ideal maximal de R. Então, $P \subsetneq R$. Suponhamos que existem ideais L e M de R tais que $P \subsetneq L$, $P \subsetneq M$ e $LM \subseteq P$. Como P é ideal maximal de R e $P \subsetneq L$, $P \subsetneq M$, podemos concluir que $L = R = M$. Logo, como R é unitário, $R = R^2 = LM \subseteq P$, uma contradição. Portanto, não existem ideias nas condições consideradas e, pela proposição anterior, P é ideal primo. □

Corolário. Se R é um anel unitário, então R admite ideais primos e ideais primos minimais.

Demonstração. Seja R um anel unitário. Então, R admite ideais maximais. Pela proposição anterior, R admite ideais primos. Como todo o ideal primo contém ideais primos minimais, podemos concluir que R admite ideais primos minimais. □

Observação.

1. Consideremos o conjunto $\mathbb{Z}/2\mathbb{Z}$ munido da adição usual e do produto '.' definido por $\bar{a}.\bar{b} = \bar{0}$. Então, $(\mathbb{Z}/2\mathbb{Z}, +, .)$ é um anel comutativo não unitário. É fácil de verificar que $(\bar{0})$ é um ideal maximal. No entanto, não é um ideal primo: $\bar{1}.\bar{1} = \bar{0} \in (\bar{0})$ mas $\bar{1} \notin (\bar{0})$.

2. $\mathbb{Z} \times \{0\}$ é ideal de $\mathbb{Z} \times \mathbb{Z}$. Como $\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \{0\} \cong \mathbb{Z}$, o anel $\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \{0\}$ é um domínio de integridade. Logo, $\mathbb{Z} \times \{0\}$ é ideal primo de $\mathbb{Z} \times \mathbb{Z}$. No entanto, $\mathbb{Z} \times \{0\}$ não é ideal maximal, uma vez que se tem

$$\mathbb{Z} \times \{0\} \subsetneq \mathbb{Z} \times 2\mathbb{Z} \subsetneq \mathbb{Z} \times \mathbb{Z}.$$

Teorema. Seja R um anel comutativo e unitário tal que $a^2 = a$ para todo o $a \in R$. Então, I é ideal primo de R se e só se I é ideal maximal de R.

Demonstração. Pela proposição anterior, se I é um ideal maximal de R então I é um ideal primo de R. Suponhamos, então, que I é ideal primo de R. Assim, $I \subsetneq R$ e R/I é um anel não nulo. Sendo R anel comutativo e unitário, também R/I é comutativo e unitário. Seja $a \in R \setminus I$. Então, $a \notin I$ e $a + I \neq I$. Como $a^2 = a$, temos que $a^2 - a = 0 \in I$, ou seja, $a(a-1) \in I$. Por hipótese, $a \in I$ ou $a - 1 \in I$. Mas $a \notin I$, pelo que podemos concluir que $a - 1 \in I$. Por outras palavras, $a + I = 1 + I$. Logo, $a + I$ é invertível e R/I é um corpo. Portanto, I é idea maximal de R. □

Proposição. Sejam R um anel comutativo e unitário e $P \neq (0)$ um ideal primo minimal. Então, todo o elemento de P é divisor de zero.

Demonstração. Sejam $p \in P$ e $S = \{p^k a : k \in \mathbb{N}, a \in R \setminus P\}$. Como P é ideal primo de R, $P \subsetneq R$ e $1 \notin P$. Logo, $p = p^1 1 \in S$ e $S \neq \emptyset$.

Sejam $x, y \in S$. Então, existem $k, t \in \mathbb{N}$ e $a, b \in R \setminus P$ tais que $x = p^k a$, $y = p^t b$. Como R é comutativo, $xy = (p^k a)(p^t b) = p^k p^t ab = p^{k+t}(ab)$. Sendo P um ideal primo, sbemos que $ab \notin P$ (pois $a \notin P$ e $b \notin P$). Logo, $xy \in S$ e S é um conjunto multiplicativo.

Suponhamos que $0 \notin S$. Então, existe um ideal primo Q de R tal que $Q \cap S = \emptyset$. Como $p \in S$, sabemos que $p \notin Q$. Suponhamos que existe $x \in Q \setminus P$. Então, $px \in S$. Mais, como $p \in R$ e $x \in Q$, temos que $px \in Q$. Logo, $px \in Q \cap S$, uma contradição. Assim, $Q \subsetneq P$, o que contradiz o facto de P ser ideal primo minimal. Portanto, $0 \in S$, pelo que existem $n \in \mathbb{N}$ e $a \in R \setminus P$ tais que $p^n a = 0$. Seja k o menor natural tal que $p^k a = 0$. Se $k = 1$, então $pa = 0$, com $a \neq 0$, pelo que p é divisor de zero. Se $k > 1$, então $0 = p^k a = p(p^{k-1}a)$, com $p^{k-1}a \neq 0$, pelo que, também neste caso, p é divisor de zero. □

Proposição. Seja R um anel unitário e primo. Então, o centro de R é domínio de integridade.

Demonstração. O centro de R, $Z(R)$, é um anel comutativo e unitário. Como R é um anel primo, o ideal (0) é ideal primo de R. Vamos mostrar que (0) é ideal primo de $Z(R)$. Para tal, consideremos I, J ideais de $Z(R)$ tais que $IJ = (0)$. Então, como $J \subseteq Z(R)$,

$$(RI)(RJ) = (RI)(JR) = R(IJ)R = (0).$$

Ora, (0) é ideal primo de R e RI, RJ são ideais esquerdos de R. Logo, $RI = (0)$ ou $RJ = (0)$. Sendo R unitário, podemos concluir que $I = (0)$ ou $J = (0)$. Assim, (0) é ideal primo de $Z(R)$ e, portanto, $Z(R)/(0)$ é domínio de integridade. Como $Z(R) \cong Z(R)/(0)$, temos que $Z(R)$ é domínio de integridade. □

Definição. Dizemos que R é um *anel reduzido* se não contiver elementos nilpotentes não nulos.

Proposição. Seja R um anel primo. Então, R é domínio de integridade se e só se R é anel reduzido.

Demonstração. Admitamos que R é domínio de integridade. Seja a um elemento nilpotente de R. Por definição, existe $n \in \mathbb{N}$ tal que $a^n = 0$, onde n é o grau de nilpotência de a. Se $n = 1$, então $0 = a^1 = a$. Se $n > 1$, então $aa^{n-1} = a^n = 0$. Como R é domínio de integridade, $a = 0$ ou $a^{n-1} = 0$. Mas n é o grau de nilpotência de a, pelo que $a = 0$. Logo, R não admite elementos nilpotentes não nulos e, por definição, R é anel reduzido.

Admitamos agora que R é anel reduzido. Sejam $a, b \in R$ tais que $ab = 0$. Como R é anel primo, (0) é ideal primo de R. Em particular, $(0) \subsetneq R$. É claro que, para todo o $x \in R$, $abx = 0$. Logo,

$$(bxa)^2 = (bxa)(bxa) = bx(abx)a = bx.0.a = 0.$$

Sendo R um anel reduzido, podemos concluir que $bxa = 0$ (pois bxa é nilpotente). Então, $bRa = (0)$. Como (0) é ideal primo de R, temos que $b \in (0)$ ou $a \in (0)$, ou seja, $b = 0$ ou $a = 0$. Por definição, R é domínio de integridade. □

Lema. Sejam $n \in \mathbb{N}$ e R um anel tal que, para todo o $b \in R$, $b \in RbR$. Então, $\mathcal{I}$ é ideal de $\mathcal{M}_n(R$ se e só se $\mathcal{I} = \mathcal{M}_n(I)$ onde I é um ideal de R.

Demonstração. Admitamos que $\mathcal{I} = \mathcal{M}_n(I)$, onde I é um ideal de R. Como I é ideal de R, $0 \in I$ e $I \subseteq R$. Logo, $A = [a_{ij}]$, com $a_{ij} = 0$ para quaisquer $i, j \in \{1, \ldots, n\}$, é um elemento de $\mathcal{M}_n(I) = \mathcal{I}$ e, portanto, $\mathcal{I} \neq \emptyset$. Mais, como $I \subseteq R$, é claro que $\mathcal{I} = \mathcal{M}_n(I) \subseteq \mathcal{M}_n(R)$.

Dadas duas matrizes $A = [a_{ij}], B = [b_{ij}] \in \mathcal{I}$, sabemos que a_{ij}, $b_{ij} \in I$ para quaisquer $i, j \in \{1, \ldots, n\}$. Logo, sendo I um ideal de R, $a_{ij} - b_{ij} \in I$. Portanto, $A - B = [a_{ij} - b_{ij}] \in \mathcal{I}$.

Se $C = [c_{ij}]$ é uma matriz em $\mathcal{M}_n(R)$, então $c_{ij} \in R$ para quaisquer $i, j \in \{1, \ldots, n\}$, e, por I ser um ideal de R, $a_{ik}c_{kj}$, $c_{ik}a_{kj} \in I$ para qualquer $k \in \{1, \ldots, n\}$. Portanto,

$$AC = \left[\sum_{k=1}^{n} a_{ik}c_{kj}\right], CA = \left[\sum_{k=1}^{n} c_{ik}a_{kj}\right] \in \mathcal{I}.$$

Logo, $\mathcal{I}$ é um ideal de $\mathcal{M}_n(R)$.

Reciprocamente, suponhamos que $\mathcal{I}$ é um ideal de $\mathcal{M}_n(R)$ e consideremos

$$I = \{b \in R : \text{ existe } [a_{ij}] \in \mathcal{I} \text{ e existe } (k, \ell) \in \{1, \ldots, n\} \times \{1, \ldots, n\} \text{ tais que } a_{k\ell} = b\}.$$

Como $\mathcal{I}$ é um ideal de $\mathcal{M}_n(R)$, a matriz nula é um elemento de $\mathcal{I}$. Logo, $0 \in I$ e $I \neq \emptyset$.

Seja $a \in R$. Representemos por $[a]_{(m,t)}$ a matriz $[a_{ij}]$ cujo elemento na posição (m, t) é igual a a e os restantes elementos são todos nulos. Dado $c \in I$, existem $V = [v_{ij}] \in \mathcal{I}$ e $(p, q) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ tais que $v_{pq} = c$. Como $c \in I \subseteq R$, $c \in RcR$ (por hipótese). Assim, existe $k \in \mathbb{N}$ e existem a_ℓ, $b_\ell \in R$, com $\ell \in \{1, \ldots, k\}$, tais que

$$c = \sum_{\ell=1}^{k} a_\ell c b_\ell.$$

Dados $a, b \in R$, para qualquer $(s,r) \in \{1,\ldots,n\} \times \{1,\ldots,n\}$,

$$[a]_{(s,p)} V [b]_{(q,r)} = \left[\sum_{\ell} a_{w\ell} v_{\ell j}\right] [b]_{(q,r)} = \left[\sum_{m} \left(\sum_{\ell} a_{w\ell} v_{\ell m}\right) b_{mt}\right]$$
$$= \left[\sum_{\ell} a_{w\ell} \left(\sum_{m} v_{\ell m} b_{mt}\right)\right] = [a_{sp} v_{pq} b_{qr}]_{(s,r)} = [acb]_{(s,r)} \in \mathcal{I}.$$

Então, $[a_\ell c b_\ell]_{(s,r)} \in \mathcal{I}$, para todo o $\ell \in \{1,\ldots,k\}$. Como $\mathcal{I}$ é um ideal, $\sum_{\ell} [a_\ell c b_\ell]_{(s,r)} \in \mathcal{I}$, ou seja, $[c]_{(s,r)} \in \mathcal{I}$.

Sejam $c, d \in I$. Para todo o $(s,r) \in \{1,\ldots,n\} \times \{1,\ldots,n\}$, temos que $[c]_{(s,r)}$, $[d_{(s,r)}] \in \mathcal{I}$. Como $\mathcal{I}$ é um ideal, $[c-d]_{(s,r)} \in \mathcal{I}$. Logo, por definição, $c - d \in I$.

Dados $c \in I$ e $a \in R$, temos que $[c]_{(s,r)} \in \mathcal{I}$ e $[a]_{(r,s)} \in \mathcal{M}_n(R)$. Logo, como $\mathcal{I}$ é um ideal, $[ca]_{(s,s)} = [c]_{(s,r)}[a]_{(r,s)} \in \mathcal{I}$ e $[ac]_{(r,r)} = [a]_{(r,s)}[c]_{(s,r)} \in \mathcal{I}$, pelo que ca, $ac \in I$. Por outras palavras, vimos que I é um ideal de R.

Falta provar que $\mathcal{I} = \mathcal{M}_n(I)$. Por definição de I, é claro que $\mathcal{I} \subseteq \mathcal{M}_n(I)$. Tomemos, agora, $C \in \mathcal{M}_n(I)$. Então,

$$C = [c_{ij}] = \sum_{i,j} [c_{ij}]_{(i,j)}.$$

Como $c_{ij} \in I$, sabemos que $[c_{ij}]_{(i,j)} \in \mathcal{I}$. Logo, $C \in \mathcal{I}$, pois $\mathcal{I}$ é um ideal. Assim, $\mathcal{I} = \mathcal{M}_n(I)$, com I ideal de R. □

Proposição. Sejam R um anel, I, I' ideais de R e $n \in \mathbb{N}$. Então, $\mathcal{M}_n(I)\mathcal{M}_n(I') = \mathcal{M}_n(II')$.

Demonstração. [exercício!]

Exemplo. Seja R um anel unitário e $n \in \mathbb{N}$. Consideremos o anel $\mathcal{M}_n(R)$ de todas as matrizes quadradas de ordem n com entradas em R. Então, os ideais primos de $\mathcal{M}_n(R)$ são os ideais $\mathcal{M}_n(P)$ onde P é ideal primo de R. [exercício!]

2.3. Somas diretas de anéis

Proposição. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. O produto cartesiano

$$P = \prod_{i\in I} R_i = \{a = (a_i)_{i\in I} : \quad \forall i \in I,\, a_i \in R_i\},$$

munido com as seguintes operações

$$(a_i)_{i\in I} + (b_i)_{i\in I} = (a_i + b_i)_{i\in I} \qquad ((a_i)_{i\in I}, (b_i)_{i\in I} \in P),$$

$$(a_i)_{i\in I}.(b_i)_{i\in I} = (a_i b_i)_{i\in I} \qquad ((a_i)_{i\in I}, (b_i)_{i\in I} \in P),$$

é um anel.

Demonstração. [exercício!]

Definição. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Ao anel $\prod_{i\in I} R_i$ chamamos *produto direto dos anéis* R_i.
Se $R_i = R$ para todo o $i \in I$, então representamos $\prod_{i\in I} R_i$ por R^I.
Se $a = (a_i)_{i\in I} \in P$, para todo o $i \in I$, dizemos que a_i é a *componente índice* i *do elemento* a.

Definição. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Para todo o $j \in I$, a correspondência $p_j : \prod_{i\in I} R_i \to R_j$, definida por $p_j((a_i)_{i\in I}) = a_j$ é um epimorfismo de anéis e designa-se por *projeção*. Por outro lado, a correspondência $i_j : R_j \to \prod_{i\in I} R_i$, definida por $i_j((a) = (a_i)_{i\in I}$, onde $a_j = a$ e $a_i = 0_{R_i}$ se $i \neq j$, é um monomorfismo de anéis e designa-se por *inclusão*.

Observemos que, dado $j \in I$, $p_j \circ i_j = \mathrm{id}_{R_j}$ e $p_j \circ i_k = \varphi_0$ sempre que $j \neq k$. Além disso, $\mathrm{Ker}(p_j) \cong \prod_{i\in I\setminus\{j\}} R_i \times \{0_{R_j}\}$

Dados $a = (a_i)_{i\in I}$, $b = (b_i)_{i\in I} \in P$, $a = b$ se e só se $a_i = b_i$ para todo o $i \in I$ ou, equivalentemente, $p_i(a) = p_i(b)$ para todo o $i \in I$.

Para todo o $j \in I$, $R_j \cong i_j(R_j) = \overline{R}_j$. É claro que $\overline{R}_j$ é subanel de $\prod_{i\in I} R_i$. Se $i, j \in I$ são tais que $i \neq j$, então $\overline{R}_i \neq \overline{R}_j$. No entanto, se $R_i = R_j$, então $\overline{R}_i \cong \overline{R}_j$.

Definição. Sejam I um conjunto não vazio e R um anel. A correspondência $\delta : R \to R^I$ definida por $\delta(a) = (a_i)_{i\in I}$, com $a_i = a$ para todo o $i \in I$, diz-se uma *aplicação diagonal* e é um morfismo de anéis.

Proposição. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Então,

1. $\prod_{i\in I} R_i$ é comutativo se e só se R_i é comutativo, para todo o $i \in I$.
2. $\prod_{i\in I} R_i$ é anel unitário se e só se R_i é anel unitário, para todo o $i \in I$.
3. $Z(\prod_{i\in I} R_i) = \prod_{i\in I} Z(R_i)$, onde $Z(R)$ é o centro de um anel R.
4. Seja $\{B_i\}_{i\in I}$ uma família de anéis tais que $B_i \leq R_i$ para todo o $i \in I$. Então,
   - **(i)** $\prod_{i\in I} B_i \leq \prod_{i\in I} R_i$.
   - **(ii)** $\prod_{i\in I} B_i = \prod_{i\in I} R_i$ se e só se $B_i = R_i$ para todo o $i \in I$.

(iii) $\prod_{i\in I} B_i = \{0\}$ se e só se $B_i = \{0\}$ para todo o $i \in I$.

Demonstração [exercício!]

Proposição. Sejam $\{R_i\}_i \in I$, $\{S_i\}_i \in I$ famílias de anéis e $\{\theta_i\}_i \in I$, $\theta_i : R_i \to S_i$, uma família de morfismos. Tem-se que:

1. a aplicação $\theta : \prod_{i\in I} R_i \to \prod_{i\in I} S_i$ definida por $\theta((a_i)_{i\in I}) = (\theta_i(a_i))_{i\in I}$ é um morfismo de anéis. A aplicação θ representa-se também por $\prod_{i\in I} \theta_i$ e designa-se por *produto direto dos morfismos* θ_i.

2. $\mathrm{Im}(\theta) = \prod_{i\in I} \mathrm{Im}(\theta_i)$ e $\mathrm{Ker}(\theta) = \prod_{i\in I} \mathrm{Ker}(\theta_i)$. Em particular, θ é um epimorfismo [respetivamente: monomorfismo, isomorfismo] se e só se θ_i é um epimorfismo [respetivamente: monomorfismo, isomorfismo], para todo o $i \in I$.

3. O diagrama

$$\begin{array}{ccc} \prod_{i\in I} R_i & \xrightarrow{\ \theta\ } & \prod_{i\in I} S_i \\ {\scriptstyle p_j}\downarrow & & \downarrow{\scriptstyle \overline{p}_j} \\ R_j & \xrightarrow[\ \theta_j\ ]{} & S_j \end{array}$$

   é comutativo.

Demonstração. [exercício!]

Teorema [Propriedade Universal do Produto Direto de Anéis]. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis.

(a) O anel produto $P = \prod_{i\in I} R_i$ e a família de projeções $\{p_i\}_{i\in I}$ verificam a seguinte propriedade:

   [U] Para qualquer anel F e qualquer família de morfismos $\{\varphi_i\}_{i\in I}$, com $\varphi_i : F \to R_i$ para cada $i \in I$, existe um e um só morfismo $h : F \to P$ tal que

$$p_i \circ h = \varphi_i \ \text{ para todo o } i \in I.$$

(b) Se um anel T e uma família de morfismos $\{\rho_i\}_{i\in I}$, com $\rho_i : T \to R_i$ para cada $i \in I$, verificam a propriedade **[U]**, então existe um isomorfismo $g : T \to P$ tal que $\rho_i = p_i \circ g$ para todo o $i \in I$.

Demonstração. [exercício!]

Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Seja $P = \prod_{i\in I} R_i$. Consideremos o subconjunto

$$A = \{a = (a_i)_{i\in I} \in P : a_i = 0_{R_i} \text{ para quase todos os } i\}$$

de P. Não é difícil de verificar que A é um ideal de P [exercício!]. Em particular, A é um subanel de P.

Definição. Ao subanel $A = \{a = (a_i)_{i\in I} \in P : a_i = 0_{R_i} \text{ para quase todos os } i\}$ dá-se o nome de *soma direta externa dos anéis* R_i e representa-se A por $\dot{\bigoplus_{i\in I}} R_i$.

Se $R_i = R$ para todo o $i \in I$, representamos $\dot{\bigoplus_{i\in I}} R_i$ por $R^{(I)}$.

Para I finito, temos que $\dot{\bigoplus_{i\in I}} R_i = \prod_{i\in I} R_i = R_1 \dot{\oplus} \ldots \dot{\oplus} R_m$, onde $m = |I|$. Se $|I| = 1$, então $\dot{\bigoplus_{i\in I}} R_i = \prod_{i\in I} R_i = R$.

Proposição. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Então,

1. $\dot{\bigoplus_{i\in I}} R_i$ é comutativo se e só se R_i é comutativo, para todo o $i \in I$.
2. $Z(\dot{\bigoplus_{i\in I}} R_i) = \dot{\bigoplus_{i\in I}} Z(R_i)$
3. Seja $\{B_i\}_{i\in I}$ uma família de anéis tais que $B_i \leq R_i$ para todo o $i \in I$. Então,
   - **(i)** $\dot{\bigoplus_{i\in I}} B_i \leq \dot{\bigoplus_{i\in I}} R_i$.
   - **(ii)** $\dot{\bigoplus_{i\in I}} B_i = \dot{\bigoplus_{i\in I}} R_i$ se e só se $B_i = R_i$ para todo o $i \in I$.
   - **(iii)** $\dot{\bigoplus_{i\in I}} B_i = \{0\}$ se e só se $B_i = \{0\}$ para todo o $i \in I$.

Demonstração. [exercício!]

Para todo o j em I, a correspondência $p'_j : \dot{\bigoplus_{i\in I}} R_i \to R_j$, definida por $p'_j((a_i)_{i\in I}) = a_j$ é um epimorfismo de anéis e a correspondência $i'_j : R_j \to \dot{\bigoplus_{i\in I}} R_i$, definida por $i_j((a) = (a_i)_{i\in I}$, onde $a_j = a$ e $a_i = 0_{R_i}$ se $i \neq j$, é um monomorfismo de anéis.

Proposição. Sejam $\{R_i\}_i \in I$, $\{S_i\}_i \in I$ famílias de anéis e $\{\theta_i\}_i \in I$, $\theta_i : R_i \to S_i$, uma família de morfismos. Tem-se que:

1. a aplicação $\theta : \dot{\bigoplus_{i\in I}} R_i \to \dot{\bigoplus_{i\in I}} S_i$ definida por $\theta((a_i)_{i\in I}) = (\theta_i(a_i))_{i\in I}$ é um morfismo de anéis. A aplicação θ representa-se também por $\dot{\bigoplus_{i\in I}} \theta_i$ e designa-se por *soma direta dos morfismos* θ_i.

2. $\mathrm{Im}(\theta) = \dot{\bigoplus_{i\in I}} \mathrm{Im}(\theta_i)$ e $\mathrm{Ker}(\theta) = \dot{\bigoplus_{i\in I}} \mathrm{Ker}(\theta_i)$. Em particular, θ é um epimorfismo [respetivamente: monomorfismo, isomorfismo] se e só se θ_i é um epimorfismo [respetivamente: monomorfismo, isomorfismo], para todo o $i \in I$.

3. O diagrama

$$\begin{array}{ccc} \dot{\bigoplus_{i\in I}} R_i & \xrightarrow{\ \theta\ } & \dot{\bigoplus_{i\in I}} S_i \\ \Big\downarrow{\scriptstyle p'_j} & & \Big\downarrow{\scriptstyle \overline{p}'_j} \\ R_j & \xrightarrow[\ \theta_j\ ]{} & S_j \end{array}$$

é comutativo.

Demonstração. [exercício!]

Exemplo. Consideremos o conjunto $\mathscr{S} = \{\text{sucessões de números reais}\}$, munido das operações de adição e produto definidas por

$$(u_n)_{n\in\mathbb{N}} + (v_n)_{n\in\mathbb{N}} = (u_n + v_n)_{n\in\mathbb{N}},$$

$$(u_n)_{n\in\mathbb{N}}.(v_n)_{n\in\mathbb{N}} = (u_n v_n)_{n\in\mathbb{N}}.$$

O conjunto $(\mathscr{S}, +, .)$ é um anel. Na verdade, $\mathscr{S} = \mathbb{R}^{\mathbb{N}}$, pois

$$\mathscr{S} = \{f : \mathbb{N} \to \mathbb{R} |\, f(n) = u_n, \text{ para } n \in \mathbb{N}, \text{ com } u_n \in \mathbb{R}\}.$$

Considerando

$$\mathscr{S}' = \{\text{sucessões de números reais com quase todos os termos nulos}\},$$

temos que $\mathscr{S}' = \mathbb{R}^{\mathbb{N}}$.

Teorema [Propriedade Universal da Soma Direta de Anéis]. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis.

(a) O anel $A = \dot{\bigoplus_{i\in I}} R_i$ e a família de inclusões $\{i'_j\}_{j\in I}$ verificam a seguinte propriedade:

[U'] Para qualquer anel R e toda a família de morfismos $\{f_j\}_{j\in I}$, com $f_j : R_j \to R$ para cada $j \in I$, onde, sempre que $k \neq \ell$, $f_k(R_k)f_\ell(R_\ell) = 0$, existe um e um só morfismo $g : A \to R$ tal que

$$g \circ i'_j = f_j \text{ para todo o } j \in I.$$

(b) Se um anel T e uma família $\{\rho_j\}_{j\in I}$ de morfismos, onde $\rho_j : R_j \to T$ para cada $j \in I$ e sempre que $k \neq \ell$, $\rho_k(R_k)\rho_\ell(R_\ell) = 0$, satisfizerem a propriedade **[U']**, então

$$T \cong \dot{\bigoplus_{i\in I}} R_i.$$

Demonstração. [exercício!]

Proposição. Sejam R_1, R_2, R_3 anéis. Então,

1. $R_1 \dot{\oplus} R_2 \cong R_2 \dot{\oplus} R_1$.
2. $R_1 \dot{\oplus} (R_2 \dot{\oplus} R_3) \cong (R_1 \dot{\oplus} R_2) \dot{\oplus} R_3 \cong R_1 \dot{\oplus} R_2 \dot{\oplus} R_3$.

Demonstração. [exercício!]

Proposição. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$, $\{B_i\}_{i\in I}$ famílias de anéis tais que B_i é ideal de R_i para todo o $i \in I$. Então,

$$\dot{\bigoplus_{i\in I}}(R_i/B_i) \cong (\dot{\bigoplus_{i\in I}} R_i)/(\dot{\bigoplus_{i\in I}} B_i).$$

Demonstração. [exercício!]

Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Para cada $j \in I$, $R_j \cong i'_j(R_j) = \overline{R}_j \leq \dot{\bigoplus_{i\in I}} R_i = A$. Logo, $\sum_{j\in I} \overline{R}_j \leq A$.

Por outro lado, se $a \in A$, então $a = (a_i)_{i\in I}$, com os a_i quase todos nulos. Logo,

$$a = (a_i)_{i\in I} = \sum_{j\in I} i'_j(a_j) \in \sum_{j\in I} \overline{R}_j.$$

Assim, $A \subseteq \sum_{j\in I} \overline{R}_j$, pelo que $A = \sum_{j\in I} \overline{R}_j$.

Já vimos que, dado $a = (a_i)_{i\in I} \in A$, $a = \sum_{j\in I} a'_j$, onde $a'_j = i'_j(a_j) \in \overline{R}_j$ para todo o $j \in I$.

Suponhamos que $a = \sum_{j\in I} a'_j = \sum_{j\in I} b'_j$, com $a'_j, b'_j \in \overline{R}_j$ para todo o $j \in I$.

Como $b'_j \in \overline{R}_j$, existe $b_j \in R_j$ tal que $b'_j = i'_j(b_j)$. Então, $a_j = p'_j(a) = b_j$ e, assim, $a'_j = b'_j$. Logo, todo o elemento a de A se escreve de modo único como soma de elementos de $\overline{R}_j$.

Não é difícil de verificar que, dados $j, k \in I$ distintos, $\overline{R}_j\overline{R}_k = \{0\}$. Por outras palavras, acabámos de provar o seguinte resultado.

Proposição. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Para todo o $j \in I$, seja $\overline{R}_j = i'_j(R_j)$. Então,

1. $A = \dot{\bigoplus_{i\in I}} R_i = \sum_{j\in I} \overline{R}_j$.
2. Todo o elemento a de A admite uma representação única do tipo $a = \sum_{j\in I} \overline{a}_j$, com $\overline{a}_j \in \overline{R}_j$.
3. Para quaisquer $i, j \in I$ tais que $i \neq j$, $\overline{R}_i\overline{R}_j \neq \{0\}$.

Proposição. Sejam R um anel, I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Então, R é isomorfo ao anel $A = \dot{\bigoplus_{i\in I}} R_i$ se e só se existir em R uma família de subanéis $\{B_i\}_{i\in I}$ tal que

1. $B_i \cong R_i$, para todo o $i \in I$:
2. $R = \sum_{i\in I} B_i$;
3. todo o elemento $a \in R$ admite uma representação única do tipo $a = \sum_{i\in I} b_i$, com $b_i \in B_i$;
4. para quaisquer $i, j \in I$ tais que $i \neq j$, tem-se $B_iB_j = \{0\}$.

Demonstração. [exercício!]

Definição. Sejam R um anel, I um conjunto não vazio e $\{B_i\}_{i\in I}$ uma família de subanéis de R. Diz-se que R é *soma direta interna dos B_i, com $i \in I$* se

[D$_1$] $R = \sum_{i\in I} B_i$;

[D$_2$] todo o elemento $a \in R$ admite uma representação única do tipo $a = \sum_{i\in I} a_i$, com $a_i \in B_i$, a_i quase todos nulos;

[D$_3$] para quaisquer $i, j \in I$ tais que $i \neq j$, tem-se $B_iB_j = \{0\}$.

Escreve-se $R = \bigoplus_{i \in I}{}_i B_i$ ou $R = \bigoplus_{i \in I} B_i$.

Definição. Seja S um subanel de R. Diz-se que S é *parcela direta de* R se existir $T \leq R$ tal que $R = S \oplus_i T$.

Proposição. Sejam R um anel, I um conjunto não vazio e $\{B_i\}_{i \in I}$ uma família de subanéis de R. As seguintes afirmações são equivalentes:

1. $R = \bigoplus_{i \in I}{}_i B_i$

2. [D$_1$] $R = \sum_{i \in I} B_i$;

[D$_2$] todo o elemento $a \in R$ admite uma representação única do tipo $a = \sum_{i \in I} a_i$, com $a_i \in B_i$, a_i quase todos nulos;

[D$'_3$] para todo o $i \in I$, B_i é ideal de R.

3. [D$_1$] $R = \sum_{i \in I} B_i$;

[D$'_2$] para todo o $i \in I$, $B_i \cap \left(\sum_{i \neq j} B_j \right) = \{0\}$;

[D$'_3$] para todo o $i \in I$, B_i é ideal de R.

4. [D$_1$] $R = \sum_{i \in I} B_i$;

[D$'_2$] para todo o $i \in I$, $B_i \cap \left(\sum_{i \neq j} B_j \right) = \{0\}$;

[D$_3$] para quaisquer $i, j \in I$ tais que $i \neq j$, tem-se $B_i B_j = \{0\}$.

5. [D$_1$] $R = \sum_{i \in I} B_i$;

[D$''_2$] se $\sum_{i \in I} a_i = 0$, com $a_i \in B_i$, a_i quase todos nulos, então $a_i = 0$ para todo o $i \in I$;

[D$_3$] para quaisquer $i, j \in I$ tais que $i \neq j$, tem-se $B_i B_j = \{0\}$.

6. [D$_1$] $R = \sum_{i \in I} B_i$;

[D$''_2$] se $\sum_{i \in I} a_i = 0$, com $a_i \in B_i$, a_i quase todos nulos, então $a_i = 0$ para todo o $i \in I$;

[D$'_3$] para todo o $i \in I$, B_i é ideal de R.

Demonstração. [exercício!]

Note-se que $R = R \oplus_i \{0\}$.

Definição. Dizemos que o anel R é *indecomponível* se admitir $\{0\}$ e R como únicas parcelas diretas. Caso contrário, dizemos que R é *decomponível*.

Observação. R é soma direta interna de subanéis de R se e só se R é soma direta interna de ideais de R.

Proposição. Sejam R um anel, I um conjunto não vazio e $\{B_i\}_{i\in I}$ uma família de subanéis de R tais que $R = \bigoplus_{i\in I}{}_i B_i$. Então,

(a) Se $I = \{1, 2\}$, então $R = B_1 \oplus_i B_2 = B_2 \oplus_i B_1$.

(b) Se $I = \{1, 2, 3\}$, então $R = B_1 \oplus_i B_2 \oplus_i B_3 = B_1 \oplus_i (B_2 \oplus_i B_3) = (B_1 \oplus_i B_2) \oplus_i B_3$.

(c) Se $I = J \dot\cup K$, então $R = \left(\bigoplus_{i\in J}{}_i B_i\right) \oplus_i \left(\bigoplus_{i\in K}{}_i B_i\right)$.

Demonstração. Iremos apenas demonstrar a alínea **(c)**. A prova das restantes alíneas fica como exercício. Sejam, pois J, K subconjuntos de I tais que $I = J \dot\cup K$.

[D$_1$] Como $R = \bigoplus_{i\in I}{}_i B_i$, é claro que $R = \sum_{i\in I} B_i = \sum_{i\in J} B_i + \sum_{i\in I\setminus J} B_i = \left(\sum_{i\in J} B_i\right) + \left(\sum_{i\in K} B_i\right)$.

[D$'_2$] Pretendemos mostrar que $\left(\bigoplus_{j\in J}{}_i B_j\right) \bigcap \left(\bigoplus_{k\in K}{}_i B_k\right) = \{0\}$. Tomemos, então, $x \in \left(\bigoplus_{j\in J}{}_i B_j\right) \bigcap \left(\bigoplus_{k\in K}{}_i B_k\right)$. Assim, $x \in \bigoplus_{j\in J}{}_i B_j$, pelo que

$$x = \sum_{j\in J} b_j = \sum_{i\in I} \bar b_i,$$

onde $\bar b_i = b_i$, se $i \in J$, e $\bar b_i = 0$, se $i \notin J$. De modo análogo, como $x \in \bigoplus_{k\in K}{}_i B_k$,

$$x = \sum_{k\in K} c_k = \sum_{i\in I} \bar c_i,$$

onde $\bar c_i = c_i$, se $i \in K$, e $\bar c_i = 0$, se $i \notin K$. Portanto,

$$x = \sum_{i\in I} \bar b_i = \sum_{i\in I} \bar c_i \in \bigoplus_{i\in I}{}_i B_i,$$

donde segue que $\bar b_i = \bar c_i$ para todo o $i \in I$. Em particular, $b_j = 0$, para todo o $j \in J$, e $c_k = 0$, para todo o $k \in K$. Logo, $x = 0$, como pretendíamos mostrar.

[D_3'] Por hipótese, para todo o $i \in I$, B_i é ideal de R. Em particular, para todo o $j \in J$, B_j é ideal de R. Portanto, $\bigoplus_{j\in J}{}_i B_j$ é ideal de R. De modo análogo, concluímos que $\bigoplus_{k\in K}{}_i B_k$ é ideal de R.

Por [D_1], [D_2'] e [D_3'], podemos concluir que $R = \left(\bigoplus_{i\in J}{}_i B_i\right) \oplus_i \left(\bigoplus_{i\in K}{}_i B_i\right)$. □

Proposição. Sejam R um anel, I um conjunto não vazio e $\{A_i\}_{i\in I}$, $\{B_i\}_{i\in I}$ famílias de subanéis de R tais que $B_i \subseteq A_i$ para todo o $i \in I$. Então,

(a) Se $R = \bigoplus_{i\in I}{}_i A_i$ e $B = \sum_{i\in I} B_i$, então $B = \bigoplus_{i\in I}{}_i B_i$.

(b) Se $R = \bigoplus_{i\in I}{}_i A_i = \bigoplus_{i\in I}{}_i B_i$, então $B_i = A_i$ para todo o $i \in I$.

Demonstração. Comecemos por provar o resultado enunciado em **(a)**. Admitamos, então, que $R = \bigoplus_{i\in i}{}_i A_i$ e $B = \sum_{i\in I} B_i$

[D_1] Por hipótese, $B = \sum_{i\in I} B_i$ e, portanto, [D_1] verifica-se.

[D_2'] Seja $i \in I$. Sabemos que $\{0\} \subseteq B_i \cap \left(\sum_{j\neq i} B_j\right)$. Seja $b \in B_i \cap \left(\sum_{j\neq i} B_j\right)$. Então, $b \in B_i \subseteq A_i$ e $b \in \sum_{j\neq i} B_j \subseteq \sum_{j\neq i} A_j$. Logo, $b \in A_i \cap \left(\sum_{j\neq i} A_j\right) = \{0\}$, pelo que $b = 0$. Assim, $B_i \cap \left(\sum_{j\neq i} B_j\right) = \{0\}$.

[D_3] Sejm $i, j \in I$ tais que $i \neq j$. Então, $B_iB_j \subseteq A_iA_j = \{0\}$, pelo que $B_iB_j = \{0\}$.

Por [D_1], [D_2'] e [D_3], podemos concluir que $B = \bigoplus_{i\in I}{}_i B_i$.

Admitamos, agora, que $R = \bigoplus_{i\in I}{}_i A_i = \bigoplus_{i\in I}{}_i B_i$. Dado $i \in I$, sabemos que $B_i \subseteq A_i$. Pretendemos mostrar que $A_i \subseteq B_i$. Ora, dado $a \in A_i$, é claro que $a \in \bigoplus_{i\in I}{}_i A_i = \bigoplus_{i\in I}{}_i B_i$, pelo que

$$a = \sum_{j\in I} \bar{a}_j = \sum_{j\in I} b_j,$$

com $\bar{a}_j \in A_j$, onde $\bar{a}_j = a$ se $j = i$ e $\bar{a}_j = 0$ se $j \neq i$, e $b_j \in B_j \subseteq A_j$. Como $R = \bigoplus_{i\in I}{}_i A_i$, podemos concluir que $\bar{a}_j = b_j$ para todo o $j \in I$. Em particular, $a = \bar{a}_i = b_i \in B_i$. Assim, $A_i = B_i$, como pretendíamos mostrar. □

Definição. Sejam R um anel, I um conjunto não vazio e $\{B_i\}_{i\in I}$ uma família de subanéis de R tais que $R = \bigoplus_{i\in I}{}_i B_i$. Para cada $j \in I$, a correspondência $p_j : R \to B_j$ definida por

$$p_j\left(\sum_{i\in I} b_i\right) = b_j$$

é um epimorfismo de anéis. Por outro lado, a correspondência $i_j : B_j \to R$ definida por

$$i_j(b_j) = b_j$$

é um monomorfismo de anéis.
Os epimorfismos p_j, com $j \in I$ dizem-se as *projeções associadas à soma direta interna* e os monomorfismos i_j, com $j \in J$, dizem-se as *inclusões associadas à soma direta interna.*

Não é difícil de verificar que $\operatorname{Ker} p_j = \sum_{i\in I\setminus\{j\}} B_i = \bigoplus_{i\in I\setminus\{j\}}{}_i B_i$. Logo,

$$R = \bigoplus_{i\in I}{}_i B_i = \left(\bigoplus_{i\in I\setminus\{j\}}{}_i B_i\right) \oplus B_j = \operatorname{Ker} p_j \oplus B_j.$$

Definição. Sejam I um conjunto não vazio, $\{R_i\}_{i\in I}$ uma família de anéis, $P = \prod_{i\in I} R_i$ e $\{p_i : P \to R_i\}_{i\in I}$ a família das projeções. Diz-se que um subanel S de P é *produto subdireto dos anéis R_i, $i \in I$* se, para todo o $i \in I$, $p_i(S) = R_i$, ou seja, se, para todo o $i \in I$, $p_i\big|_S$ é ainda um epimorfismo. Escreve-se

$$S = \prod_{i\in I}{}_S R_i$$

e $p_i\big|_S$, com $i \in I$, são as *projeções associadas ao produto subdireto S.*

Exemplos. Sejam I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis.

1. $\prod_{i\in I} R_i$ é produto subdireto dos anéis R_i, $i \in I$.

2. Temos que $\dot{\bigoplus_{i\in I}} R_i \leq \prod_{i\in I} R_i$. Além disso, $p'_j \equiv p_j\big|_{\dot{\bigoplus_{i\in I}} R_i} : \dot{\bigoplus_{i\in I}} R_i \to R_j$. Logo, $\dot{\bigoplus_{i\in I}} R_i$ é produto subdireto dos anéis R_i, $i \in I$.

3. Suponhamos que $R_i = R$ para todo o $i \in I$. O produto $\prod_{i\in I} R_i$ denota-se por R^I. Consideremos o conjunto

$$T = \{\bar{a} = (a_i)_{i\in I} \in R^I : \text{ existe } a \in R \text{ tal que } a_i = a, \text{ para todo o } i \in I\}.$$

É claro que T é subanel de R^I. Além disso, dado $j \in I$, $p_j\big|_T : T \to R_j = R$ é um epimorfismo, uma vez que $r = p_j\big|_T(\bar{r})$, para todo o $r \in R$. Logo, T é produto subdireto dos anéis R_i, $i \in I$.

Proposição. Sejam I um conjunto não vazio, $\{R_i\}_{i\in I}$ uma família de anéis e S um produto subdireto dos anéis R_i, $i \in I$. Então,

1. S é comutativo se e só se R_j é comutativo para todo o $j \in I$.

2. $\bigcap_{j\in I} \operatorname{Ker} p_j\big|_S = \{\bar{0}\}$.

Demonstração. [exercício!]

Proposição. Sejam I um conjunto não vazio, $\{R_i\}_{i\in I}$ e $\{S_i\}_{i\in I}$ famílias de anéis para os quais existe uma família de epimorfismos $\{\theta_i : R_i \to S_i\}_{i\in I}$ e T um produto subdireto dos anéis R_i, $i \in I$. Então, se $\theta = \prod_{i\in I} \theta_i$, tem-se

(a) $\theta(T)$ é produto subdireto dos anéis S_i, $i \in I$.

(b) Se, para todo o $i \in I$, θ_i é um isomorfismo, então T é isomorfo a um produto subdireto dos anéis S_i, $i \in I$.

Demonstração. [exercício!]

Proposição. Sejam R um anel, I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Então, são equivalentes as condições:

(a) R é isomorfo a um produto subdireto dos anéis R_i, $i \in I$.

(b) Existe uma família $\{\varphi_i : R \to R_i\}_{i\in I}$ de epimorfismos tais que $\bigcap_{i\in I} \operatorname{Ker} \varphi_i = \{0\}$.

(c) Existe uma família $\{B_i\}_{i\in I}$ de ideais de R tais que

(i) $R/B_i \cong R_i$, para todo o $i \in I$.

(ii) $\bigcap_{i\in I} B_i = \{0\}$.

Demonstração. Admitamos que R é isomorfo a um produto subdireto dos anéis R_i, $i \in I$. Sejam $T = \prod_{i\in I}{}_S R_i$ e $\theta : R \to T$ um isomorfismo. Seja $i \in I$. Consideremos a aplicação $\varphi_i : R \to R_i$ dada por $\varphi_i = p_i\big|_T \circ \theta$. Como θ é um isomorfismo e $p_i\big|_T$ é um epimorfismo, também φ_i é um epimorfismo.

Vejamos que $\bigcap_{i\in I} \operatorname{Ker}\varphi_i = \{0\}$. Para isso, tomemos $x \in \bigcap_{i\in I} \operatorname{Ker}\varphi_i$. Então, $x \in \operatorname{Ker}\varphi_i$ para todo o $i \in I$, pelo que $p_i\big|_T \circ \theta(x) = 0$, qualquer que seja o i. Logo, $p_i\big|_T[\theta(x)] = 0$ para todo o $i \in I$ e, portanto, $\theta(x) = \bar{0}$. Sendo θ um isomorfismo, podemos concluir que $x = 0$. Assim, $\bigcap_{i\in I} \operatorname{Ker}\varphi_i = \{0\}$.

Suponhamos, agora, que existe uma família $\{\varphi_i : R \to R_i\}_{i\in I}$ de epimorfismos tais que $\bigcap_{i\in I} \operatorname{Ker}\varphi_i = \{0\}$. Para todo o $i \in I$, $\operatorname{Ker}\varphi_i$ é ideal de R. Seja, então, $B_i = \operatorname{Ker}\varphi_i$. Assim, $\{B_i\}_{i\in I}$ é uma família de ideais de R tal que $\bigcap_{i\in I} B_i = \{0\}$. Pelo Teorema do Homomorfismo,

$$R/_{\operatorname{Ker}\varphi_i} \cong \varphi_i(R),$$

ou seja,

$$R/_{B_i} \cong R_i.$$

Finalmente, admitamos que existe uma família $\{B_i\}_{i\in I}$ de ideais de R tais que

(i) $R/_{B_i} \cong R_i$, para todo o $i \in I$.

(ii) $\bigcap_{i\in I} B_i = \{0\}$.

Consideremos

$$\begin{aligned} \eta\colon R &\to \prod_{i\in I} \left(R/_{B_i}\right) \\ a &\mapsto (a + B_i)_{i\in I}. \end{aligned}$$

Não é difícil de verificar que η é um monomorfismo de anéis [exercício!]. Logo, $R \cong \eta(R)$. Mais,

(I) $\eta(R) \leq \prod_{i\in I} \left(R/_{B_i}\right)$

(II) Dado $j \in I$,

$$p_j(\eta(R)) = p_j\left(\{(a + B_i)_{i\in I} : a \in R\}\right) = \{a + B_j : a \in R\} = R\Big/_{B_j}.$$

Logo, $p_j\big|_{\eta(R)}$ é um epimorfismo.

Por (I) e (II), $\eta(R)$ é produto subdireto dos anéis R/B_i, $i \in I$. Como $R/B_i \cong R_i$ para todo o $i \in I$,

$$R \cong \eta(R) = \prod_{i\in I}{}_S \left(R/B_i\right) \cong \prod_{i\in I}{}_S R_i. \quad \square$$

Corolário. Sejam R um anel, I um conjunto não vazio e $\{B_i\}_{i\in I}$ uma família de ideais de R. Então, $R \Big/ \bigcap_{i\in I} B_i$ é isomorfo a um produto subdireto dos anéis R/B_i, $i \in I$.

Demonstração. Consideremos a família $\left\{ B_j \Big/ \bigcap_{i\in I} B_i \right\}_{j\in I}$ de ideais de $R \Big/ \bigcap_{i\in I} B_i$.

(i) Para todo o $j \in I$,

$$\left(R \Big/ \bigcap_{i\in I} B_i \right) \Big/ \left(B_j \Big/ \bigcap_{i\in I} B_i \right) \cong R/B_j .$$

(ii) $\bigcap_{j\in I} \left(B_j \Big/ \bigcap_{i\in I} B_i \right) = \bigcap_{i\in I} B_i \Big/ \bigcap_{i\in I} B_i = \left\{ \bigcap_{i\in I} B_i \right\}$.

Pela proposição anterior, $R \Big/ \bigcap_{i\in I} B_i$ é isomorfo a um produto subdireto dos anéis R/B_i, $i \in I$. $\square$

Definição. Sejam R um anel, I um conjunto não vazio e $\{R_i\}_{i\in I}$ uma família de anéis. Dizemos que R admite uma *representação como produto subdireto dos anéis* R_i, $i \in I$, ou mais simplesmente que R é *produto subdireto dos anéis* R_i, $i \in I$, se existir $T = \prod_{i\in I}{}_S R_i$ tal que $R \cong T$.

Se $\{p_i\}_{i\in I}$ é a família das projeções associadas a $\prod_{i\in I} R_i$, à família dos epimorfismos $\rho_i = p_i \circ \theta : R \to R_i$, com $i \in I$, dá-se o nome de *projeções associadas à representação* θ *de* R *como produto subdireto dos anéis* R_i, $i \in I$.

Se, para algum j, ρ_j for um isomorfismo, diz-se que a representação é uma *representação trivial*.

Definição. Dizemos que um anel R é *subdiretamente irredutível* se qualquer representação de R como produto subdireto de alguma família de anéis é uma representação trivial. Caso contrário, dizemos que R é *subdiretamente redutível*.

Proposição. Seja R um anel não nulo. São equivalentes as seguintes condições:

(a) R é subdiretamente irredutível.

(b) A interseção de todos os ideais não nulos de R é um ideal não nulo de R.

(c) R possui um ideal não nulo que está contido em todos os ideais não nulos de R.

Demonstração. A equivalência das condições **(b)** e **(c)** é trivial. Vejamos, então, que **(a)** é equivalente a **(b)**.

Comecemos por admitir que R é subdiretamente irredutível. Seja $\{B_i\}_{i\in I}$ a família dos ideais não nulos de R e suponhamos que $\bigcap_{i\in I} B_i = \{0\}$. Pela proposição anterior, R é isomorfo a um produto subdireto T dos anéis R/B_i, $i \in I$. Além disso,

$$T = \{(a + B_i)_{i\in I} : a \in R\}.$$

Para cada $j \in I$,

$$\begin{aligned} \rho_j \colon R &\to R/B_j \\ a &\mapsto a + B_j \end{aligned}$$

e $\operatorname{Ker}\rho_j = B_j$. Por hipótese, existe $i \in I$ tal que ρ_i é um isomorfismo. Assim,

$$\{0\} = \operatorname{Ker}\rho_i = B_i,$$

o que contradiz o facto de B_i ser um ideal não nulo de R. Logo, $\bigcap_{i\in I} B_i \neq \{0\}$ e $\bigcap_{i\in I} B_i$ é um ideal não nulo de R.

Admitamos que a interseção de todos os ideais não nulos de R é um ideal não nulo de R. Suponhamos que $R \overset{\tau}{\cong} T$, onde $T = \prod_{i\in I,S} R_i$, com $\{R_i\}$ família de anéis. Consideremos a família $\{\rho_i : R \to R_i\}_{i\in I}$ onde $\rho_i = p_i \circ \tau$ para todo o $i \in I$. Como p_i é um epimorfismo para todo o $i \in I$ e τ é um isomorfismo, sabemos que ρ_i é um epimorfismo para todo o $i \in I$. Suponhamos que $\operatorname{Ker}\rho_i \neq \{0\}$ para todo o $i \in I$. Por hipótese, a interseção Q de todos os ideais não nulos de R é ainda um ideal não nulo de R. Como $\operatorname{Ker}\rho_i$, $i \in I$, são ideais não nulos de R,

$$Q \subseteq \bigcap_{i\in I} \operatorname{Ker}\rho_i.$$

Logo, $\bigcap_{i\in I} \operatorname{Ker}\rho_i \neq \{0\}$. Assim, existe $x \in \bigcap_{i\in I} \operatorname{Ker}\rho_i \setminus \{0\}$. Para todo o $i \in I$, $x \in \operatorname{Ker}\rho_i$, pelo que

$$p_i(\tau(x)) = (p_i \circ \tau)(x) = \rho_i(x) = 0.$$

Logo, $\tau(x) = \bar{0}$ e, sendo τ um isomorfismo, $x = 0$, uma contradição. Assim, existe $j \in I$ tal que $\operatorname{Ker}\rho_j = \{0\}$ e ρ_j é um isomorfismo. Por definição, R é subdiretamente irredutível. □

Exemplos.

1. Se R é um anel de divisão, então $R \neq \{0\}$ e os únicos ideais de R são $\{0\}$ e R. Logo, a interseção de todos os ideais não nulos de R é o próprio R e, portanto, a interseção de todos os ideais não nulos de R é um ideal não nulo. Pela proposição anterior, R é subdiretamente irredutível.

2. Se R for um anel simples, então R é subdiretamente irredutível.

3. O anel $\mathbb{Z}$ é isomorfo a um produto subdireto dos anéis $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$. De facto, $\{p\mathbb{Z}\}_{p\in\mathbb{P}}$ é uma família de ideais não nulos de $\mathbb{Z}$. Como $\bigcap_{p\in\mathbb{P}} p\mathbb{Z}$ é um ideal de $\mathbb{Z}$, existe $t \in \mathbb{Z}$ tal que $\bigcap_{p\in\mathbb{P}} p\mathbb{Z} = t\mathbb{Z}$. Assim, para todo o $p \in \mathbb{P}$, $t\mathbb{Z} \subseteq p\mathbb{Z}$, pelo que $t = pr_p$ para todo o $p \in \mathbb{P}$. Por outras palavras, $p|t$ para todo o $p \in \mathbb{P}$, donde concluímos que $t = 0$. Assim,

$$\bigcap_{p\in\mathbb{P}} p\mathbb{Z} = \{0\}.$$

Sejam $\pi_p : \prod_{q\in\mathbb{P}} \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$, as projeções associadas ao produto $\prod_{q\in\mathbb{P}} \mathbb{Z}/q\mathbb{Z}$. Dado $j \in I$,

$$\operatorname{Ker} \pi_p = p\mathbb{Z} \neq \{0\}.$$

Logo, π_p não é um isomorfismo e, por definição, $\mathbb{Z}$ é subdiretamente redutível.

Convenção. O anel nulo é subdiretamente irredutível.

Teorema de Birkoff. Todo o anel R é produto subdireto de anéis subdiretamente irredutíveis.

Demonstração. Se $R = \{0\}$, então, por convenção, R é subdiretamente irredutível. Suponhamos, pois, que $R \neq \{0\}$. Então, existe $x \in R \setminus \{0\}$. Seja

$$\mathcal{F}_x = \{I \text{ ideal de } R : x \notin I\}.$$

Não é difícil de provar que $\mathcal{F}_x$ é não vazio e que é um c.p.o. quando munido da operação de inclusão. Mais, toda a cadeia não vazia de elementos de $\mathcal{F}_x$ admite majorante [exercício!]. Assim, pelo Lema de Zorn, existe elemento maximal de $\mathcal{F}_x$, digamos I_x. Por definição, $x \notin I_x$. Vejamos que R/I_x é subdiretamente irredutível. Para tal, iremos mostrar que a interseção de todos os ideais não nulos de R/I_x é um ideal não nulo.

Consideremos a família $\{\overline{T}_k = T_k/I_x : k \in K\}$ de todos os ideais não nulos de R/I_x. Como $\overline{T}_k$ é não nulo, para todo o $k \in K$, sabemos que

$$I_x \subsetneq T_k,$$

para todo o $k \in K$. Mas T_k é ideal de R e I_x é elemento maximal de $\mathcal{F}_x$. Logo, para todo o $k \in K$, $x \in T_k$. Assim,

$$x + I_x \in \bigcap_{k\in K} \overline{T}_k.$$

Como $x \notin I_x$, temos que $x + I_x \neq I_x$. Portanto, R/I_x é subdiretamente irredutível.

Consideremos $\prod_{x \in R\setminus\{0\}} R/I_x$ e a aplicação

$$\begin{aligned} \theta \colon R &\to \prod_{x \in R\setminus\{0\}} R/I_x \\ a &\mapsto (a + I_x)_{x \in R\setminus\{0\}}. \end{aligned}$$

Prova-se que θ é um monomorfismo de anéis [exercício!]. Mais, $\bigcap_{x \in R\setminus\{0\}} I_x = \{0\}$. Logo, R é isomorfo a um produto subdireto dos anéis R/I_x. □