Capítulo 3

Módulos

Todos os resultados, e respectivas demonstrações, deste capítulo são transcritos dos capítulos 6 e 8 do livro

INTRODUÇÃO À ÁLGEBRA, IST Press, Lisboa, 2004

da autoria de Rui Loja Fernandes e Manuel Ricou.

1. Módulos sobre anéis

O estudo de módulos sobre um anel chama-se ÁLGEBRA LINEAR, pois este é o cenário natural para estudar os conceitos de independência linear, dimensão, etc.

Exemplos motivadores. (1) Seja $(V, +, \cdot)$ um espaço vectorial sobre um corpo K. Dados $k \in K$ e $v \in V$, a multiplicação escalar $(k, v) \mapsto k \cdot v$ é uma operação do corpo K no grupo abeliano $(V, +)$ que satisfaz as seguintes propriedades:

(1) $k(v_1 + v_2) = kv_1 + kv_2$, $k \in K$, $v_1, v_2 \in V$.

(2) $(k + l)v = kv + lv$, $k, l \in K$, $v \in V$.

(3) $k(lv) = (kl)v$, $k, l \in K$, $v \in V$.

(4) $1v = v$, $v \in V$.

(2) Seja $(G, +)$ um grupo abeliano. Dados $n \in \mathbb{Z}$ e $g \in G$, a correspondência

$$(n, g) \mapsto ng := \begin{cases} \underbrace{g + g \cdots + g}_{n \text{ vezes}} & \text{se } n \geq 0 \\ \underbrace{(-g) + (-g) \cdots + (-g)}_{-n \text{ vezes}} & \text{se } n < 0 \end{cases}$$

define uma operação do anel $\mathbb{Z}$ no grupo abeliano $(G,+)$ que satisfaz as seguintes propriedades:

(1) $n(g_1+g_2)=ng_1+ng_2$, $n\in\mathbb{Z}$, $g_1,g_2\in G$.

(2) $(n+m)g=ng+mg$, $n,m\in\mathbb{Z}$, $g\in G$.

(3) $n(mg)=(nm)g$, $n,m\in\mathbb{Z}$, $g\in G$.

(4) $1g=g$, $g\in G$.

(3) Seja $T\colon \mathbb{R}^3\to\mathbb{R}^3$ a transformação linear cuja matriz relativamente à base canónica $e_1=(1,0,0)$, $e_2=(0,1,0)$, $e_3=(0,0,1)$ é a matriz

$$\begin{pmatrix} 2 & 0 & 0\\ 0 & 3 & 1\\ 0 & 0 & 3 \end{pmatrix}.$$

Sejam ainda

$$T^0=I,\quad T^k=\underbrace{T\circ T\circ\cdots\circ T}_{k\text{ vezes}}.$$

Dados $p(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbb{R}[x]$ e $v\in\mathbb{R}^3$, a correspondência

$$(p(x),v)\mapsto p(x)\cdot v:=a_nT^n(v)+\cdots+a_1T(v)+a_0$$

define uma operação do anel $\mathbb{R}[x]$ no grupo abeliano $(\mathbb{R}^3,+)$ que satisfaz as seguintes propriedades:

(1) $p(x)\cdot(v_1+v_2)=p(x)\cdot v_1+p(x)\cdot v_2$, $p(x)\in\mathbb{R}[x]$, $v_1,v_2\in\mathbb{R}^3$.

(2) $(p(x)+q(x))\cdot v=p(x)\cdot v+q(x)\cdot v$, $p(x)\in\mathbb{R}[x]$, $p(x),q(x)\in\mathbb{R}[x]$, $v\in\mathbb{R}^3$.

(3) $p(x)\cdot(q(x)\cdot v)=(p(x)q(x))\cdot v$, $p(x),q(x)\in\mathbb{R}[x]$, $v\in\mathbb{R}^3$.

(4) $1v=v$, $v\in\mathbb{R}^3$.

É claro que este exemplo pode ser estendido a uma transformação linear T arbitrária.

Em todos estes três exemplos existe uma estrutura comum, a chamada estrutura de *módulo*:

Módulo sobre um anel unitário

Um *módulo M sobre um anel unitário A* (abreviadamente, um *A-módulo*) é um grupo abeliano $(M, +)$ em conjunto com uma operação

$$A \times M \to M, \quad (a, v) \mapsto av$$

de um anel unitário A em M que satisfaz as seguintes propriedades:

(1) $a(v_1 + v_2) = av_1 + av_2$, $a \in A$, $v_1, v_2 \in M$.

(2) $(a + b)v = av + bv$, $a, b \in A$, $v \in M$.

(3) $a(bv) = (ab)v$, $a, b \in A$, $v \in M$.

(4) $1v = v$, $v \in M$.

Em rigor, os módulos acabados de definir são os chamados "A-módulos à esquerda"; de modo análogo, podemos definir os "A-módulos à direita". Todos os resultados deste capítulo são verdadeiros *mutatis mutandis* para os módulos à direita. Claro que se o anel A for comutativo, não faz sentido distinguir entre módulos à esquerda e à direita.

Notação. Denotamos por 0_A e 0_M os neutros de $(A, +)$ e $(M, +)$. Quanto ao neutro multiplicativo de $(A, \cdot)$ usaremos a notação 1_A. Como $(M, +)$ é um grupo abeliano, a notação nv ($n \in \mathbb{Z}$, $v \in M$) continua a fazer sentido; do mesmo modo, podemos também falar no elemento na ($n \in \mathbb{Z}$, $a \in A$).

Proposição 1.1. *Seja M um A-módulo. Para quaisquer $a \in A$, $v \in M$ e $n \in \mathbb{Z}$ temos:*

(1) $a0_M = 0_M$.

(2) $0_A v = 0_M$.

(3) $(-a)v = -(av) = a(-v)$.

(4) $n(av) = a(nv) = (na)v$.

Demonstração. Exercício. ∎

Um *submódulo* N de um A-módulo $(M, +)$ é um subconjunto de M no qual as restrições da operação $+$ em M e da operação do anel A em M satisfazem a definição de A-módulo. Claramente,

trata-se de um subgrupo de $(M, +)$ *que é fechado para a multiplicação por elementos de* A (*isto é, se* $a \in A$ *e* $v \in N$, *então* $av \in N$).

Exemplos. (1) Como vimos nos exemplos motivadores, um grupo abeliano G é um $\mathbb{Z}$-módulo (e inversamente, qualquer $\mathbb{Z}$-módulo é um grupo abeliano), um espaço vectorial V sobre um corpo K é um K-módulo e $\mathbb{R}^3$ é um $\mathbb{R}[x]$-módulo (mais geralmente, qualquer espaço vectorial V sobre um corpo K é um $K[x]$-módulo). No primeiro exemplo, os submódulos de G são os subgrupos de G, enquanto no segundo, os submódulos coincidem com os subespaços lineares. É habitual chamar *espaço vectorial* a qualquer módulo sobre um anel de divisão D (um anel diz-se de *divisão* se for um anel unitário onde todo o elemento não nulo é uma unidade; portanto, um corpo é um anel de divisão comutativo). No terceiro exemplo, os submódulos são os subespaços de V invariantes pela transformação T.

(2) Todo o ideal (à esquerda) I de um anel A é um A-módulo para a operação $A \times I \to I$ dada pela multiplicação em A: se $a \in A$ e $b \in I$ então $ab \in I$. De igual forma, A/I é um A-módulo, pois se $a \in A$ e $b + I \in A/I$, então $a(b + I) = ab + I$.

(3) Para todo o subanel B de um anel A, A é um B-módulo. Em particular, os anéis $A[x_1, \ldots, x_n]$ são A-módulos.

(4) Seja G um grupo abeliano, e $End(G)$ o anel dos endomorfismos de G. Então G é um $End(G)$-módulo com a multiplicação $\phi g := \phi(g)$ ($\phi \in End(G)$, $g \in G$).

(5) Seja $\phi\colon A \to B$ um homomorfismo de anéis. Se M é um B-módulo então também é um A-módulo: a adição é a mesma e a multiplicação é definida por $av := \phi(a)v$ ($a \in A$, $v \in M$). Chama-se a este A-módulo o *levantamento* de M por ϕ, que se denota por $\phi^* M$.

HOMOMORFISMO DE A-MÓDULOS
Um *homomorfismo de A-módulos* $\phi\colon M_1 \to M_2$ é uma aplicação entre A-módulos que satisfaz: (1) $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$, $v_1, v_2 \in M$. (2) $\phi(av) = a\phi(v)$, $a \in A$, $v \in M$.

Os homomorfismos de A-módulos também são por vezes designados de *aplicações A-lineares* ou simplesmente *transformações lineares*.

Note que os homomorfismos de $\mathbb{Z}$-módulos são os homomorfismos de grupos abelianos enquanto os homomorfismos $\phi\colon V_1 \to V_2$ entre espaços vectoriais (K-módulos) são precisamente as transformações lineares usuais.

Se $\phi\colon M_1 \to M_2$ é um homomorfismo, o seu núcleo $N(\phi)$ e a sua imagem $Im(\phi)$ são submódulos de M_1 e M_2, respectivamente.

2. Algumas construções importantes

Apresentamos de seguida, resumidamente, alguns exemplos importantes de construções canónicas de módulos e homomorfismos de A-módulos. Em todas elas será necessário verificar que os módulos e homomorfismos introduzidos satisfazem de facto a definição de módulo e de homomorfismo.

Intersecções e geração

Se $\{N_i\}_i \in I$ é uma família de submódulos de um A-módulo M, então $\bigcap_{i\in I} N_i$ é um submódulo de M.

Logo, para qualquer $S \subseteq M$ não vazio, a intersecção de todos os submódulos de M que contêm S é um submódulo $\langle S\rangle$, a que se chama *módulo gerado por* S. É fácil verificar que

$$\langle S\rangle = \{a_1v_1 + \cdots a_rv_r \mid a_i \in A, v_i \in S\}.$$

(Cuidado: isto só vale para A-módulos unitários, para os não unitários, os elementos de $\langle S\rangle$ são da forma $\sum_i a_iv_i + \sum_j n_jv'_j$, onde $a_i \in A$, $n_j \in \mathbb{Z}$ e $v_i, v'_j \in S$.)

Somas

Se $\{N_i\}_i \in I$ é uma família de submódulos de um A-módulo M, ao A-módulo $\langle\bigcup_{i\in I} N_i\rangle$ chama-se *soma* dos submódulos N_i, que se denota por

$$\sum_{i\in I} N_i.$$

Se $I = \{1, 2, \ldots, m\}$ é finito, escreve-se $\sum_{i=1}^m N_i$ ou ainda $N_1 + N_2 + \cdots + N_m$. Em geral,

$$\sum_{i\in I} N_i = \{a_1v_1 + \cdots + a_mv_m \mid a_i \in A, v_i \in \bigcup_{i\in I} N_i\} = \{v_{i_1} + \cdots + v_{i_m} \mid v_{i_j} \in N_{i_j}\}.$$

Quocientes

Se M é um A-módulo e N é um seu submódulo, então a inclusão canónica $\iota\colon N \to M$ é uma aplicação A-linear. O grupo quociente M/N possui uma estrutura natural de A-módulo:

$$a(v + N) := av + N. \quad (a \in A, v \in M).$$

De facto, esta operação está bem definida (se $v + N = v' + N$ então $v - v' \in N$, logo $a(v - v') \in N$, isto é, $av + N = av' + N$) e satisfaz claramente as condições (1)-(4) na definição de A-módulo.

Este módulo chama-se o *módulo quociente* de M por N.

De modo análogo aos grupos e anéis, temos:

- A projecção canónica $\pi\colon M \to M/N$ é uma aplicação A-linear.

• Teoremas do Isomorfismo

(1º) *Se* $\phi\colon M_1 \to M_2$ *é um homomorfismo de* A*-módulos, então*

$$Im(\phi) \simeq M_1/N(\phi).$$

(2º) *Se* N_1 *e* N_2 *são submódulos de um* A*-módulo* M*, então*

$$\frac{N_1 + N_2}{N_2} \simeq \frac{N_1}{N_1 \cap N_2}.$$

(3º) *Se* N *e* P *são submódulos de um* A*-módulo* M *e* $P \subseteq N \subseteq M$*, então* P *é um submódulo de* N *e*

$$\frac{M/P}{N/P} \simeq M/N.$$

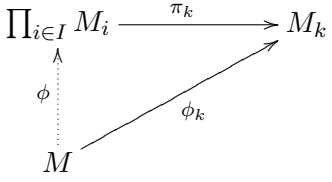
Produtos directos

Seja $\{M_i\}_{i\in I}$ uma família de A-módulos. O A-módulo $\prod_{i\in I} M_i$, chamado *produto directo* da família de módulos $\{M_i\}_{i\in I}$, é definido do seguinte modo:

- conjunto suporte: produto cartesiano $\{(v_i)_{i\in I} \mid v_i \in M_i\}$ dos M_i.
- operação de grupo: $(v_i)_{i\in I} + (w_i)_{i\in I} = (v_i + w_i)_{i\in I}$.
- multiplicação: $a(v_i)_{i\in I} = (av_i)_{i\in I}$.

Para cada $k \in I$, a *projecção canónica* $\pi_k\colon \prod_{i\in I} M_i \to M_k$ é o homomorfismo de A-módulos que a cada $(v_i)_{i\in I} \in \prod_{i\in I} M_i$ associa o elemento $v_k \in M_k$.

Note que para cada A-módulo M e homomorfismos $\{\phi_i\colon M \to M_i\}_{i\in I}$, existe um único homomorfismo $\phi\colon M \to \prod_{i\in I} M_i$ tal que, para cada $k \in I$, o diagrama



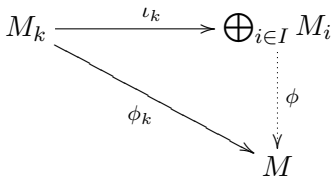
comuta (Exercício 3.3). Além disso, esta propriedade determina $\prod_{i\in I} M_i$ a menos de um isomorfismo.

Somas directas

A *soma directa* de uma família $\{M_i\}_{i\in I}$ de A-módulos, que denotamos por $\bigoplus_{i\in I} M_i$, é o submódulo de $\prod_{i\in I} M_i$ formado pelos elementos $(v_i)_{i\in I}$ nos quais apenas um número finito de v_i's é não nulo.

Para cada $k \in I$, a *injecção canónica* $\iota_k \colon M_k \to \bigoplus_{i\in I} M_i$ é o homomorfismo de A-módulos que a cada $v_k \in M_k$ associa o elemento $(v_i)_{i\in I} \in \bigoplus_{i\in I} M_i$ em que $v_i = 0$ para $i \neq k$..

De modo dual aos produtos directos, para cada A-módulo M e homomorfismos $\{\phi_i \colon M_i \to M\}_{i\in I}$, existe um único homomorfismo $\phi \colon \bigoplus_{i\in I} M_i \to M$ tal que, para cada $k \in I$, o diagrama



comuta (Exercício 3.4). Esta propriedade determina $\bigoplus_{i\in I} M_i$ a menos de um isomorfismo.

No caso em que $I = \{1, 2, \ldots, k\}$ é finito, a soma directa e o produto directo coincidem. Nesse caso, é costume representar ambos por $\bigoplus_{i=1}^{k} M_i$ ou ainda

$$M_1 \oplus \cdots \oplus M_k.$$

Proposição 2.1. *Sejam $M, M_1, \ldots, M_k$ módulos sobre um anel A. Então*

$$M \simeq M_1 \oplus \cdots \oplus M_k$$

se e só se existem homomorfismos de A-módulos $\overline{\pi}_j \colon M \to M_j$ e $\overline{\iota}_j \colon M_j \to M$ tais que:

(1) $\overline{\pi}_j \circ \overline{\iota}_j = \mathrm{id}_{M_j}$, *para* $j = 1, \ldots, k$.

(2) $\overline{\pi}_i \circ \overline{\iota}_j = 0$, *para* $i \neq j$.

(3) $\overline{\iota}_1 \circ \overline{\pi}_1 + \cdots + \overline{\iota}_k \overline{\pi}_k = \mathrm{id}_M$.

Demonstração. $\Rightarrow$: Seja $\phi \colon M \to M_1 \oplus \cdots \oplus M_k$ um isomorfismo de A-módulos. Basta considerar $\overline{\pi}_j = \pi_j \circ \phi$ e $\overline{\iota}_j = \phi^{-1} \circ \iota_j$.

$\Leftarrow$: Sejam $\phi\colon M \to M_1 \oplus \cdots \oplus M_k$ e $\psi\colon M_1 \oplus \cdots \oplus M_k \to M$ os homomorfismos definidos respectivamente por

$$\phi(v) = (\overline{\pi}_j(v))_{j=1,\ldots,k} \quad \text{e} \quad \psi((v_j)_{j=1,\ldots,k}) = \overline{\iota}_1(v_1) + \cdots + \overline{\iota}_k(v_k).$$

As propriedades (1), (2) e (3) asseguram $\phi \circ \psi = \mathrm{id}_{M_1 \oplus \cdots \oplus M_k}$ e $\psi \circ \phi = \mathrm{id}_M$, o que mostra que ϕ é um isomorfismo com inversa ψ. ∎

Proposição 2.2. *Sejam M um A-módulo e $\{M_i\}_{i\in I}$ uma família de submódulos de M. Então $M = \bigoplus_{i\in I} M_i$ se e só se se as seguintes condições se verificam:*

(1) $M = \sum_{i\in I} M_i$.

(2) $M_j \cap (M_{i_1} + \cdots + M_{i_k}) = \{0\}$ *se* $j \notin \{i_1, \ldots, i_k\}$.

Demonstração. Seja $\phi\colon \bigoplus_{i\in I} M_i \to M$ o homomorfismo de A-módulos definido por $(v_i)_I \mapsto \sum_I v_i$.
$\Rightarrow$: Por hipótese, ϕ é um isomorfismo. É evidente que a sobrejectividade de ϕ garante que $M = \sum_I M_i$. Quanto à asserção (2), seja

$$v \in M_j \cap (M_{i_1} + \cdots + M_{i_k}) \quad (j \neq i_1, \ldots, i_k).$$

Então $v = v_1 + \cdots + v_k$ $(v_j \in M_{i_j}, j = 1, \ldots, k)$. Consideremos $(u_i)_I$ e $(w_i)_I$ em $\bigoplus_{i\in I} M_i$ definidos por

$$(u_i)_I = \begin{cases} 0 & \text{se } i \neq j \\ v & \text{se } i = j \end{cases} \quad \text{e} \quad (w_i)_I = \begin{cases} 0 & \text{se } i \neq i_1, \ldots, i_k \\ v_i & \text{se } i = i_1, \ldots, i_k. \end{cases}$$

Como $\phi((u_i)_I) = v = \phi((w_i)_I)$ e ϕ é injectivo, então $(u_i)_I = (w_i)_I$, ou seja, $v = 0 = v_1 = \cdots = v_k$.

$\Leftarrow$: É evidente que a condição (1) garante que ϕ é sobrejectivo. Quanto à injectividade, suponhamos que $\phi((v_i)_I) = \phi((w_i)_I)$, isto é, $\sum_I v_i = \sum_I w_i$. Então $\sum_I (v_i - w_i) = 0$. Sejam $i_1, \ldots, i_k$ os índices de I tais que $v_i - w_i \neq 0$. É claro que para $j \notin \{i_1, \ldots, i_k\}$, $v_j = w_j$. Quanto ao caso $j \in \{i_1, \ldots, i_k\}$ temos $-(v_j - w_j) = \sum_{i\in\{i_1,\ldots,i_k\}\setminus\{j\}} (v_i - w_i)$. Como o elemento da esquerda está em M_j e o da direita pertence a $\sum_{i\in\{i_1,\ldots,i_k\}\setminus\{j\}} M_i$, podemos concluir por (2) que $v_j - w_j = 0$, isto é, $v_j = w_j$. Em conclusão, $(v_i)_I = (w_i)_I$. ∎

Corolário 2.3. *Sejam M um A-módulo e $\{M_i\}_{i\in I}$ uma família de submódulos de M. Se $M = \bigoplus_{i\in I} M_i$, então cada $v \in M$ escreve-se de modo único na forma $v_{i_1} + \cdots + v_{i_r}$ $(i_k \in I, v_{i_k} \in M_{i_k})$.*

Demonstração. Pela proposição, $M = \sum_{i\in I} M_i$, logo cada $v \in M$ pode escrever-se na forma $v_{i_1} + \cdots + v_{i_r}$ para alguns $v_{i_k} \in M_{i_k}$. Quanto à unicidade, sejam

$$v_{i_1} + \cdots + v_{i_r} + v_{j_1} + \cdots + v_{j_s} = w_{i_1} + \cdots + w_{i_r} + w_{k_1} + \cdots + w_{k_t}$$

duas maneiras de escrever $v \in M$ como elemento de $\sum_{i\in I} M_i$ (onde o índice em cada elemento indica o submódulo a que o elemento pertence; os índices i, j e k são todos distintos dois a dois). Denotemos os conjuntos $1, \ldots, r$, $1, \ldots, s$ e $1, \ldots, t$ por $\overline{r}, \overline{s}$ e $\overline{t}$ respectivamente. Então, para cada $n \in \overline{r}$, o elemento

$$v_{i_n} - w_{i_n} = \sum_{m\in\overline{r}, m\neq n} (w_{i_m} - v_{i_m}) + \sum_{m\in\overline{t}} w_{k_m} - \sum_{m\in\overline{s}} v_{j_m}$$

está na intersecção

$$M_{i_n} \cap \Big(\sum_{m\in\overline{r}, m\neq n} M_{i_m} + \sum_{m\in\overline{t}} M_{k_m} + \sum_{m\in\overline{s}} M_{j_m} \Big)$$

logo é zero. Portanto, $v_{i_n} = w_{i_n}$ para $n = 1, \ldots, r$. Além disso, para cada $n \in \overline{s}$, o elemento

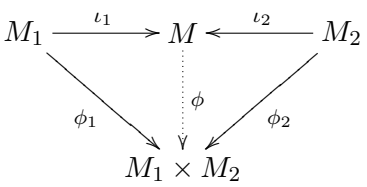
$$v_{j_n} = \sum_{m\in\overline{r}} (w_{i_m} - v_{i_m}) + \sum_{m\in\overline{t}} w_{k_m} - \sum_{m\in\overline{s}, m\neq n} v_{j_m}$$

está na intersecção

$$M_{j_n} \cap \Big(\sum_{m\in\overline{r}} M_{i_m} + \sum_{m\in\overline{t}} M_{k_m} + \sum_{m\in\overline{s}, m\neq n} M_{j_m} \Big)$$

logo também é igual a zero. Portanto, $v_{j_n} = 0$ para qualquer $n \in \overline{s}$. De modo análogo, pode provar-se que $w_{k_n} = 0$ para qualquer $n \in \overline{t}$. ∎

Observação. A Proposição 2.2 também pode ser demonstrada, alternativamente, usando a propriedade universal das somas directas (Exercício 3.4). Para tornar a notação menos pesada provaremos isso aqui somente para o caso $I = \{1, 2\}$.
$\Rightarrow$: Por hipótese, M e as inclusões $\iota_1 \colon M_1 \to M$ e $\iota_2 \colon M_2 \to M$ satisfazem a propriedade universal da soma directa $M_1 \oplus M_2$. Em particular, para os homomorfismos $\phi_1 \colon M_1 \to M_1 \times M_2$ $(v_1 \mapsto (v_1, 0))$ e $\phi_2 \colon M_2 \to M_1 \times M_2$ $(v_2 \mapsto (0, v_2))$, existe um único homomorfismo ϕ que torna o diagrama



comutativo. Seja $v \in M_1 \cap M_2$. Então $\phi(v) = \phi(\iota_1(v)) = \phi_1(v) = (v, 0)$ mas, por outro lado, $\phi(v) = \phi(\iota_2(v)) = \phi_2(v) = (0, v)$. Logo $v = 0$.
$\Leftarrow$: Pelo Exercício 3.4, basta verificar que $M = M_1 + M_2$ e os homomorfismos $\iota_1 \colon M_1 \to M_1 + M_2$ e $\iota_2 \colon M_2 \to M_1 + M_2$ definidos ambos por $v \mapsto v$ satisfazem a propriedade universal da soma directa $M_1 \oplus M_2$, o que é simples. De facto, para qualquer A-módulo N e homomorfismos $\phi_1 \colon M_1 \to N$ e $\phi_2 \colon M_2 \to N$, existe um único homomorfismo $\phi \colon M_1 + M_2 \to N$, pois, necessariamente, para cada $v_i \in M_i$ $(i = 1, 2)$, $\phi(v_i) = \phi(\iota_i(v_i)) = \phi_i(v_i)$, pelo que, para cada $v = v_1 + v_2 \in M_1 + M_2$ (note que, pelo corolário, v_1 e v_2 são únicos), $\phi(v) = \phi_1(v_1) + \phi_2(v_2)$. É simples verificar que a aplicação ϕ definida deste modo é de facto um homomorfismo de A-módulos.

3. Independência linear

Seja M um A-módulo e $\emptyset \neq S \subseteq M$.

INDEPENDÊNCIA LINEAR

Os elementos de S dizem-se *linearmente independentes* se, para toda a família finita $\{v_1, \ldots, v_n\}$ de elementos de S e $a_1, \ldots, a_n \in A$, se tem

$$a_1 v_1 + \cdots + a_n v_n = 0 \;\Rightarrow\; a_1 = \cdots = a_n = 0.$$

Caso contrário, diz-se que os elementos de S são *linearmente dependentes*.

CONJUNTO GERADOR

S diz-se *gerador* de M se $M = \langle S \rangle$. Neste caso, qualquer elemento $v \in M$ pode ser escrito como uma combinação linear (em geral, não única) de elementos de S:

$$v = \sum_{i=1}^{k} a_i v_i, \quad a_i \in A, v_i \in S.$$

M diz-se um A-módulo de *tipo finito* se possui um conjunto gerador finito.

BASE

S é uma *base* de M se é um conjunto gerador cujos elementos são linearmente independentes. Neste caso, qualquer elemento $v \in M$ pode ser escrito de forma única como uma combinação linear de elementos de S:

$$v = \sum_{i=1}^{k} a_i v_i, \quad a_i \in A, v_i \in S.$$

M diz-se um A-módulo *livre* se possui uma base.

Exemplos. (1) Qualquer espaço vectorial é um módulo livre.

(2) O grupo abeliano $\mathbb{Z}_n$, visto como um $\mathbb{Z}$-módulo, não é livre, pois em $\mathbb{Z}_n$ não existem conjuntos linearmente independentes. De facto, dado $g \in \mathbb{Z}_n$, existe sempre um inteiro não nulo m tal que $mg = 0$.

(3) Qualquer anel A é um A-módulo livre com base $\{1\}$. Os submódulos coincidem com os ideais de A. Em particular, um submódulo pode não ser livre, e mesmo sendo livre pode ter uma base de cardinalidade > 1.

(4) O grupo abeliano

$$\mathbb{Z}^k \equiv \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{k \text{ vezes}}$$

é livre. Uma base é dada por $S = \{g_1, \ldots, g_k\}$ onde $g_i = (0, \ldots, 0, 1, 0, \ldots, 0)$.

Um A-módulo M diz-se *cíclico* se é gerado por um elemento, isto é, $M = \langle v \rangle$ para algum $v \in M$. Nesse caso, a aplicação $A \to M$, dada por $a \mapsto av$, é um homomorfismo sobrejectivo de A-módulos. Pelo primeiro Teorema do Isomorfismo,

$$M \simeq \frac{A}{\operatorname{ann} v}$$

onde o ideal $\operatorname{ann} v = N(\phi) = \{a \in A \mid av = 0\}$ é o chamado *aniquilador* de v. Se $\operatorname{ann} v = \{0\}$, diz-se que v é um *elemento livre*, pois neste caso $M = \langle v \rangle \simeq A$ é livre. O conjunto dos elementos de M que não são livres designa-se por $\operatorname{Tor}(M)$ (*torção* de M).

Módulo livre gerado por X
Sejam X um conjunto arbitrário e A um anel. Se a cada $x \in X$ associarmos uma cópia de A podemos formar o A-módulo livre $M = \bigoplus_{x \in X} A$. A este módulo chama-se *módulo livre gerado* pelo conjunto X. Os elementos de M são as sequências $(a_x)_{x \in X}$ onde $a_{x_1} = a_1 \in A, \ldots, a_{x_r} = a_r \in A$ e $a_x = 0$ para $x \neq x_i$ $(i = 1, \ldots, r)$. É costume representar estes elementos como somas formais $a_1 x_1 + \cdots + a_r x_r$.

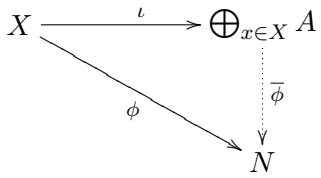
Note que este módulo é um módulo livre pois tem uma base evidente (a *base canónica*): $\{e_x \mid x \in X\}$ onde cada $e_x = (a_y)_{y \in X}$ é definido por

$$a_y = \begin{cases} 1 & \text{se } y = x \\ 0 & \text{se } y \neq x. \end{cases}$$

(Portanto, cada e_x tem coordenada 1 na posição x e 0 nas outras; na notação das somas formais, $e_x = x$.)

O módulo livre gerado por X e a função $\iota \colon X \to \bigoplus_{x \in X} A$ definida por $x \mapsto e_x$ satisfazem a seguinte propriedade universal:

Lema 3.1. *Para todo o A-módulo N e toda a função $\phi\colon X \to N$, existe um único homomorfismo de A-módulos $\overline{\phi}\colon \bigoplus_{x\in X} A \to N$ que torna o seguinte diagrama comutativo.*



Demonstração. Seja N um A-módulo arbitrário e $\phi\colon X \to N$ uma função arbitrária. A unicidade de $\overline{\phi}$ é evidente: se quisermos que o diagrama seja comutativo, necessariamente $\overline{\phi}$ terá que aplicar cada e_x em $\phi(x)$. Como $(e_x)_{x\in X}$ é uma base de $\bigoplus_{x\in X} A$, bastará então definir $\overline{\phi}$ num v arbitrário em $\bigoplus_{x\in X} A$ por $\overline{\phi}(v) = \overline{\phi}(\sum_x a_x e_x) = \sum_x a_x \overline{\phi}(e_x) = \sum_x a_x \phi(x)$. Trata-se, como é óbvio, de um homomorfismo de A-módulos. ∎

Surpreendentemente (ou talvez não!) os módulos livres gerados por um conjunto descrevem, a menos de isomorfismo, <u>todos</u> os módulos livres:

Proposição 3.2. *Seja A um anel. As seguintes afirmações são equivalentes para qualquer A-módulo M:*

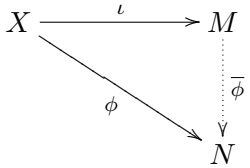
(i) *M é livre.*

(ii) *Existe uma família de submódulos cíclicos $\{N_i\}_{i\in I}$ de M, com $N_i \simeq A$, tais que $M \simeq \bigoplus_{i\in I} N_i$.*

(iii) *$M \simeq \bigoplus_{x\in X} A$ para algum conjunto $X \neq \emptyset$.*

(iv) *Existe um conjunto $X \neq \emptyset$ e uma função $\iota\colon X \to M$ com a seguinte propriedade universal:*

Para todo o A-módulo N e qualquer função $\phi\colon X \to N$ existe um único homomorfismo de A-módulos $\overline{\phi}\colon M \to N$ tal que o seguinte diagrama é comutativo.



Demonstração. (i)⇒(ii): Suponhamos que M é livre com uma base $\{e_i\}_{i\in I}$. Então, para cada $i \in I$, $N_i := \langle e_i \rangle$ é um submódulo cíclico de M isomorfo a A. A aplicação

$$\phi\colon \bigoplus_{i\in I} N_i \to M$$

que aplica cada $(v_i)_{i\in I}$ em $\sum_{i\in I} v_i$ é um isomorfismo de A-módulos.
(ii)⇒(iii): Trivial.
(iii)⇒(iv): Seja $\psi\colon \bigoplus_{x\in X} A \to M$ um isomorfismo de A-módulos Como $(e_x)_{x\in X}$ é uma base de $\bigoplus_{x\in X} A$, então $(\psi(e_x))_{x\in X}$ é uma base de M. Basta agora considerar a aplicação $\iota\colon X \to M$ definida por $\iota(x) = \psi(e_x)$ e prosseguir a demonstração como no Lema.
(iv)⇒(i): Basta verificar que $\{\iota(x)\}_{x\in X}$ é uma base de M.

Verifiquemos primeiro que $\{\iota(x)\}_{x\in X}$ é linearmente independente. Para isso tomemos para N o módulo livre gerado por X, $\bigoplus_{x\in X} A$, e para ϕ a função que a cada $x \in X$ faz corresponder o elemento e_x da base canónica. Por hipótese, existe um homomorfismo de A-módulos $\overline{\phi}\colon M \to N$ tal que $\overline{\phi}\circ\iota = \phi$ (observe que, como o módulo livre gerado por X satisfaz a propriedade universal de M referida no enunciado (pelo Lema), então $\overline{\phi}$ é um isomorfismo). Suponhamos agora que

$$a_1\iota(x_1) + a_2\iota(x_2) + \cdots + a_n\iota(x_n) = 0.$$

Aplicando $\overline{\phi}$ a ambos os membros e usando a igualdade $\overline{\phi}\circ\iota = \phi$ obtemos

$$a_1\phi(x_1) + a_2\phi(x_2) + \cdots + a_n\phi(x_n) = 0,$$

isto é,

$$a_1 e_{x_1} + a_2 e_{x_2} + \cdots + a_n e_{x_n} = 0.$$

Como $\{e_x\}_{x\in X}$ é uma base, necessariamente

$$a_1 = a_2 = \cdots = a_n = 0.$$

Por fim, verifiquemos que $\{\iota(x)\}_{x\in X}$ é um conjunto gerador de M. Seja $v \in M$. Então $\overline{\phi}(v) \in \bigoplus_{x\in X} A$ pelo que

$$\begin{aligned}\overline{\phi}(v) &= a_{x_1}e_{x_1} + \cdots + a_{x_n}e_{x_n} = a_{x_1}\phi(x_1) + \cdots + a_{x_n}\phi(x_n) = \\ &= a_{x_1}\overline{\phi}\iota(x_1) + \cdots + a_{x_n}\overline{\phi}\iota(x_n) = \overline{\phi}(a_{x_1}\iota(x_1) + \cdots + a_{x_n}\iota(x_n))\end{aligned}$$

para alguns $x_1, \ldots, x_n \in X$ e $a_{x_1}, \ldots, a_{x_n} \in A$. Como $\overline{\phi}$ é injectiva, então $v = a_{x_1}\iota(x_1) + \cdots + a_{x_n}\iota(x_n)$. ∎

Portanto, todo o A-módulo livre M que admite uma base finita $\{e_1, \ldots, e_n\}$ satisfaz $M \simeq \bigoplus_{i=1}^{n} A \equiv A^n$. Será que qualquer outra base de M tem a mesma cardinalidade? Por outras palavras, será que $A^n \simeq A^m$ implica $n = m$? Não! (Exercício 3.9).

Mas no caso infinito temos:

Proposição 3.3. *Se um A-módulo livre M possui uma base infinita, então todas as bases de M têm a mesma cardinalidade.*

Demonstração. Sejam $\{e_i\}_{i\in I}$ e $\{f_j\}_{j\in J}$ duas bases de M com I infinito. Então:

(a) *J também é infinito*: Suponhamos, por absurdo, que $J = \{1, 2, \ldots, m\}$. Então para cada $j \in J$ existem elementos $a_{j,k} \in A$ $(k = 1, 2, \ldots, n_j)$ e $i_{j,k} \in I$ tais que

$$f_j = \sum_{k=1}^{m_j} a_{j,k}\, e_{i_{j,k}}.$$

Mas isto significa que

$$E = \{e_{i_{1,1}}, \ldots, e_{i_{1,n_1}}, e_{i_{2,1}}, \ldots, e_{i_{2,n_2}}, \ldots, e_{i_{m,n_m}}\}$$

é um conjunto (finito) que gera M. Em particular, cada $e_i \notin E$ é uma combinação linear de elementos de E, o que contraria o facto de $\{e_i\}_{i\in I}$ ser linearmente independente.

(b) *Existe $\varphi\colon I \to \mathcal{P}_{fin}(J) \times \mathbb{N}$ injectiva*[1]: (Trata-de de um resultado geral de teoria dos conjuntos.) Seja $\psi\colon I \to \mathcal{P}_{fin}(J)$ a aplicação que a cada $i \in I$ faz corresponder o conjunto $\{j_1, \ldots, j_m\}$, onde $j_1, \ldots, j_m$ são os (únicos) índices de J tais que

$$e_i = a_{j_1} f_{j_1} + \cdots + a_{j_m} f_{j_m} \quad (a_{j_1}, \ldots, a_{j_m} \neq 0).$$

Esta aplicação não é injectiva, mas se $P \subseteq \mathcal{P}_{fin}(J)$, então $\psi^{-1}(P)$ é finito (porquê?). Logo podemos ordenar os elementos de $\psi^{-1}(P)$. Definamos agora ϕ do seguinte modo: como I é uma união disjunta dos $\psi^{-1}(P)$, basta definir ϕ em cada $\psi^{-1}(P)$; para cada $i \in \psi^{-1}(P)$ fazemos $\phi(i) := (P, \alpha)$ onde α é o número ordinal de i na ordenação de $\psi^{-1}(P)$.

(c) $|J| = |I|$: Como J é infinito, temos, por (b),

$$|I| \leq |\mathcal{P}_{fin}(J) \times \mathbb{N}| = |\mathcal{P}_{fin}(J)| = |J|.$$

Trocando os papéis de I e J podemos concluir também que $|J| \leq |I|$. Logo, pelo Teorema de Schröder-Bernstein (da teoria dos conjuntos), $|I| = |J|$.

■

[1] Designamos por $\mathcal{P}_{fin}(J)$ o conjunto das partes finitas de J. Se J é infinito, este conjunto tem o mesmo cardinal que J.

Dimensão
Um anel A possui a *propriedade de invariância dimensional* se, para qualquer A-módulo livre M, todas as bases de M possuem a mesma cardinalidade. Nesse caso, ao cardinal comum das bases de M chama-se *dimensão* de M, e escreve-se $\dim_A M$.

Os anéis comutativos são um exemplo de anéis de invariância dimensional:

Proposição 3.4. *Os anéis comutativos possuem a propriedade de invariância dimensional.*

Demonstração. Sejam $\{e_1, \ldots, e_n\}$ e $\{f_1, \ldots, f_m\}$ bases de um A-módulo livre M. Então existem $b_{ji}, c_{ij} \in A$, $i = 1, \ldots, n$, $j = 1, \ldots, m$ tais que

$$f_j = \sum_{i=1}^{n} b_{ji} e_i, \quad e_i = \sum_{j=1}^{m} c_{ij} f_j.$$

Por substituição, obtemos

$$f_j = \sum_{i=1}^{n} b_{ji} \sum_{k=1}^{m} c_{ik} f_k = \sum_{k=1}^{m} \sum_{i=1}^{n} b_{ji} c_{ik} f_k$$

e

$$e_i = \sum_{j=1}^{m} c_{ij} \sum_{k=1}^{n} b_{jk} e_k = \sum_{k=1}^{n} \sum_{j=1}^{m} c_{ij} b_{jk} e_k.$$

Então, como $\{e_1, \ldots, e_n\}$ e $\{f_1, \ldots, f_m\}$ são bases de M, concluímos que

$$\sum_{i=1}^{n} b_{ji} c_{ik} = \begin{cases} 1 & \text{se } j = k \\ 0 & \text{se } j \neq k \end{cases} \quad \text{e} \quad \sum_{j=1}^{m} c_{ij} b_{jk} = \begin{cases} 1 & \text{se } i = k \\ 0 & \text{se } i \neq k. \end{cases}$$

Portanto, introduzindo as matrizes $B = (b_{ji})_{j=1,i=1}^{m,n}$ e $C = (c_{ij})_{i=1,j=1}^{n,m}$, temos

$$BC = I_{m \times m} \quad \text{e} \quad CB = I_{n \times n}.$$

Como A é comutativo então, pelo Exercício 3.11, $m = n$. ∎

Exemplos. $\mathbb{Z} \oplus \mathbb{Z} = \mathbb{Z} \times \mathbb{Z}$ é livre (o par de elementos $(1, 0)$ e $(0, 1)$ constitui uma base). Como $\mathbb{Z}$ é um anel comutativo, tem a propriedade da invariância dimensional, pelo que $\dim(\mathbb{Z} \oplus \mathbb{Z}) = 2$. Analogamente, $\dim(\mathbb{Z}^n) = n$ e $\dim(\bigoplus_{i \in \mathbb{N}} \mathbb{Z}) = |\mathbb{N}| = \omega$.

Os anéis de divisão são outro exemplo de anéis de invariância dimensional (por isso faz sentido falar em dimensão de um módulo sobre um anel de divisão[2]):

[2]Neste caso, tal como quando o anel é um corpo, é habitual chamar ao módulo um *espaço vectorial*.

Proposição 3.5. *Seja A um anel de divisão e M um A-módulo. Então:*

(1) *Todo o subconjunto $X \subseteq M$ linearmente independente maximal é uma base de M.*

(2) *M possui uma base.*

(3) *A possui a propriedade de invariância dimensional.*

Demonstração. (1) Seja W o subespaço de M gerado por X. Como X é linearmente independente, X é uma base de W. Se $W = M$, nada resta a provar. Caso contrário, existe $v \in M \setminus W$, não nulo. Consideremos o conjunto $X \cup \{v\}$. Se $av + a_1v_1 + \cdots + a_nv_n$ $(a, a_i \in D, v_i \in X)$ e $a \neq 0$, então $v = a^{-1}(av) = -a^{-1}a_1v_1 - \cdots - a^{-1}a_nv_n \in W$, o que contradiz a escolha de v. Portanto $a = 0$, o que implica $a_i = 0$ para qualquer i (pois X é linearmente independente). Consequentemente, $X \cup \{v\}$ é um subconjunto linearmente independente de M, contradizendo a maximalidade de X. Logo $W = M$ e X é uma base de M.
(2) Uma vez que $\varnothing$ é um conjunto linearmente independente de M, bastará provar o seguinte:

> *Todo o subconjunto linearmente independente de M está contido numa base de M.*

Para isso, seja X um subconjunto linearmente independente de M e seja $\mathcal{S}$ o conjunto de todos os subconjuntos linearmente independentes de M que contêm X. Como $X \in \mathcal{S}$, $\mathcal{S} \neq \varnothing$. Podemos ordenar $\mathcal{S}$ por inclusão. Se $\{C_i \mid i \in I\}$ é uma cadeia em $\mathcal{S}$ então o conjunto $C = \bigcup_{i \in I} C_i$ é linearmente independente (verifique...) e portanto um elemento de $\mathcal{S}$. Claramente, C é um majorante para a cadeia $\{C_i \mid i \in I\}$. Então, pelo Lema de Zorn, $\mathcal{S}$ contém um elemento maximal B que contém X e é necessariamente um subconjunto linearmente independente maximal de M. Por (a), B é uma base de M.
(3) Sejam E e F bases de M. Se E ou F são infinitas, a Proposição 3.3 garante que $|E| = |F|$. Assumimos assim que E e F são finitas, digamos $E = \{e_1, \ldots, e_n\}$ e $F = \{f_1, \ldots, f_m\}$. Então $0 \neq f_m = a_1e_1 + \cdots + a_ne_n$ para alguns $a_i \in D$. Se a_k é o primeiro a_i não nulo, então

$$e_k = a_k^{-1}f_m - a_k^{-1}a_{k+1}e_{k+1} - \cdots - a_k^{-1}a_ne_n.$$

Portanto, o conjunto $E' = \{f_m, e_1, \ldots, e_{k-1}, e_{k+1}, \ldots, e_n\}$ gera M (porque E o faz). Em particular,

$$f_{m-1} = s_mf_m + t_1e_1 + \cdots + t_{k-1}e_{k-1} + t_{k+1}e_{k+1} + \cdots + t_ne_n \quad (s_m, t_i \in D).$$

Nem todos os t_i podem ser nulos (senão, $f_{m-1} - s_m f_m = 0$, contradizendo a independência linear de F). Se t_j é o primeiro t_i não nulo, então e_j é uma combinação linear de f_{m-1}, f_m e dos e_i para $i \neq j, k$. Consequentemente, o conjunto $\{f_{m-1}, f_m\} \cup \{e_i \mid i \neq j, k\}$ gera M (porque E' o faz). Em particular, f_{m-2} é uma combinação linear de f_{m-1}, f_m e dos e_i com $i \neq j, k$. O processo de juntarmos um f e retirarmos um e pode assim ser repetido. No final do passo k teremos um conjunto formado por $f_m, f_{m-1}, \ldots, f_{m-k+1}$ e $n-k$ dos e_i, que gera M. Se $n < m$, então ao cabo de n passos concluiremos que $\{f_m, f_{m-1}, \ldots, f_{m-n+1}\}$ gera M. Como $m - n + 1 \geq 2$, f_1 seria uma combinação linear de $f_m, \ldots, f_{m-n+1}$, uma contradição. Portanto, $m \leq n$ necessariamente. Um argumento similar com os papéis de E e F trocados mostra que $n \leq m$. Logo $n = m$. ∎

Observação. A asserção (2) desta proposição garante que todo o A-módulo sobre um anel de divisão A é livre. O recíproco também é válido (ou seja, se todo o A-módulo é livre então A é um anel de divisão) mas a demonstração sai fora do âmbito deste curso.

4. Módulos sobre domínios de integridade

Nesta secção os anéis A são domínios de integridade. Este caso é muito importante em Álgebra Linear por causa da seguinte propriedade.

Proposição 4.1. *Seja M um módulo sobre um domínio de integridade D. Então* $\operatorname{Tor}(M)$ *é um D-submódulo de M.*

Demonstração. Recordemos (p. 57) que

$$\operatorname{Tor}(M) = \{v \in M \mid \exists\, a \in D \setminus \{0\} \colon av = 0\}.$$

Então, para quaisquer $v_1, v_2 \in \operatorname{Tor}(M)$ existem $a_1, a_2 \in D$ não nulos tais que $a_1 v_1 = 0 = a_2 v_2$. Logo, para quaisquer $d_1, d_2 \in D$,

$$a_1 a_2 (d_1 v_1 + d_2 v_2) = a_2 d_1 a_1 v_1 + a_1 d_2 a_2 v_2 = 0,$$

o que mostra que $d_1 v_1 + d_2 v_2 \in \operatorname{Tor}(M)$ pois $a_1 a_2 \neq 0$ (porque D é um domínio). ∎

A $\operatorname{Tor}(M)$ chama-se *submódulo de torção* de M. Se $M = \operatorname{Tor}(M)$ diz-se que M é um *módulo de torção*; se $\operatorname{Tor}(M) = \{0\}$ diz-se que M é um *módulo livre de torção.*

Exemplos. (1) Se M é um D-módulo livre, então $\mathrm{Tor}\,(M) = \{0\}$. De facto, se $\{e_i\}_I$ é uma base de M e $v \in \mathrm{Tor}(M)$ então, por um lado, existem $a_1, \ldots, a_n \in D$ tais que $v = a_1 e_{i_1} + \cdots + a_n e_{i_n}$ e, por outro lado, existe $a \in D$ não nulo tal que $av = 0$. Mas então $aa_1 e_{i_1} + \cdots + aa_n e_{i_n} = 0$, logo $aa_1 = \cdots = aa_n = 0$. Como $a \neq 0$ e estamos num domínio de integridade, necessariamente $a_1 = \cdots = a_n = 0$, isto é, $v = 0$.

Portanto, todo o D-módulo livre é livre de torção.
(2) No entanto, o recíproco desta última afirmação é falso: o $\mathbb{Z}$-módulo $\mathbb{Q}$ é livre de torção (pois se $n \in \mathbb{Z}$ e $\frac{p}{q} \in \mathbb{Q} \setminus \{0\}$, então $n\frac{p}{q} = 0 \Leftrightarrow np = 0 \Rightarrow n = 0$), mas não é um $\mathbb{Z}$-módulo livre (quaisquer dois racionais são linearmente dependentes:

$$(p_2 q_1)\frac{p_1}{q_1} - (p_1 q_2)\frac{p_2}{q_2} = 0;$$

por outro lado, nenhum racional gera todos os racionais – aliás, nenhum conjunto finito de racionais consegue gerar todos os racionais!).
(3) Os $\mathbb{Z}$-módulos $\mathbb{Z}_n$ são módulos de torção.
(4) Se V é um espaço vectorial de dimensão finita sobre um corpo K e $T\colon V \to V$ é uma transformação linear, então V é um $K[x]$-módulo de torção.

Os módulos de torção satisfazem as seguintes propriedades básicas (as respectivas demonstrações são deixadas como exercício):

(1) Se $\phi\colon M_1 \to M_2$ é um homomorfismo de D-módulos, então

$$\phi(\mathrm{Tor}\,(M_1)) \subseteq \mathrm{Tor}\,(M_2).$$

Se ϕ é injectivo, então

$$\phi(\mathrm{Tor}\,(M_1)) = \mathrm{Tor}\,(M_2) \cap \mathrm{Im}(\phi).$$

Se ϕ é sobrejectivo com $\mathrm{N}(\phi) \subseteq \mathrm{Tor}\,(M_1)$, então

$$\phi(\mathrm{Tor}\,(M_1)) = \mathrm{Tor}\,(M_2).$$

(2) Se M é um D-módulo, então $M/\mathrm{Tor}\,(M)$ é um D-módulo livre de torção.

(3) Se $\{M_i\}_{i\in I}$ é uma família de D-módulos, então

$$\mathrm{Tor}\,(\bigoplus_{i\in I} M_i) = \bigoplus_{i\in I} \mathrm{Tor}\,(M_i).$$

Proposição 4.2. *Seja D um domínio de integridade tal que para todo o D-módulo livre M os submódulos N de M são livres. Então D é um domínio de ideais principais.*

Demonstração. No caso particular em que M é o próprio D, trata-se de um D-módulo livre. Então, por hipótese, todos os ideais I de D são D-módulos livres. Mas uma base de I só pode conter um elemento pois quaisquer dois elementos $a, b \in I$ são linearmente dependentes:

$$(-b)a + ab = 0.$$

Finalmente, se $\{d\}$ é uma base de I, em particular $I = \langle d \rangle$, logo I é principal. ∎

O recíproco de 4.2 também é válido:

Teorema 4.3. *Se D é um DIP e M é um D-módulo livre, então qualquer submódulo $N \subseteq M$ é livre e* $\dim N \leq \dim M$.

Demonstração. A demonstração é longa e muito técnica pelo que não a apresentaremos na aula. Veja-a em [Rui Loja Fernandes e Manuel Ricou, Introdução à Álgebra, IST Press, Lisboa, 2004], pp. 305-307. ∎

5. Módulos de tipo finito sobre um DIP

Nesta secção estudaremos módulos de tipo finito sobre um DIP e veremos que é possível fazer uma classificação completa de todos eles. Já sabemos que para qualquer domínio D, "livre" implica "livre de torção". Agora veremos que o recíproco é válido para módulos de tipo finito sobre DIP's.

Proposição 5.1. *Seja M um módulo de tipo finito sobre um DIP D. Se* $\mathrm{Tor}\,(M) = 0$*, então M é livre.*

Demonstração. Seja S um conjunto gerador finito de M. Em S escolhemos um conjunto $\mathcal{B} = \{v_1, \ldots, v_n\}$ maximal linearmente independente. Provemos que $\mathcal{B}$ é uma base de M. Para isso, basta mostrar que $\langle \mathcal{B} \rangle = S$.

Seja então $v \in S$. É claro que existem $a_v, a_{1,v}, \ldots, a_{n,v} \in D$ $(a_v \neq 0)$ tais que $a_v v = a_{1,v}v_1 + \cdots + a_{n,v}v_n$ (o caso $v \in \mathcal{B}$ é trivial; o caso em que $v \in S \setminus \mathcal{B}$ é consequência do facto do conjunto $\{v_1, \ldots, v_n, v\}$ ser linearmente dependente). Como M é livre de torção e

$$a := \prod_{v \in S} a_v \neq 0,$$

a aplicação $w \mapsto aw$ define um homomorfismo injectivo $\phi\colon M \to M$. Por outro lado, $\phi(M) \subseteq \bigoplus_{i=1}^{n} Dv_i$: de facto, para cada $v \in S$,

$$\phi(v) = av = (\prod_{v \neq s \in S} a_s)a_v v = (\prod_{v \neq s \in S} a_s)(a_{1,v}v_1 + \cdots + a_{n,v}v_n) \in \bigoplus_{i=1}^{n} Dv_i;$$

consequentemente, para cada $w \in M$, como $w = a_1 s_1 + \cdots + a_n s_n$ para alguns $s_i \in S$, então $\phi(w) = a_1\phi(s_1) + \cdots a_n\phi(s_n) \in \bigoplus_{i=1}^n Dv_i$.

Em conclusão, M é isomorfo a $\phi(M)$, que é um submódulo do módulo livre $\bigoplus_{i=1}^n Dv_i$. Logo, pelo Teorema 4.3, M é livre. ∎

Teorema 5.2. *Seja M um módulo de tipo finito sobre um DIP D. Então $M = \mathrm{Tor}\,(M) \oplus L$, onde L é um módulo livre.*

Demonstração. O módulo $M/\mathrm{Tor}\,(M)$ é livre de torção e de tipo finito logo é livre (pela proposição anterior). Assim, existem elementos $e_1, \ldots, e_n$, linearmente independentes, tais que

$$M/\mathrm{Tor}\,(M) = \bigoplus_{i=1}^{n} D(e_i + \mathrm{Tor}\,(M)).$$

Seja $L = \bigoplus_{i=1}^n De_i$. Então:
(1) $\underline{\mathrm{Tor}\,(M) \cap L = \{0\}}$: Se $v \in \mathrm{Tor}\,(M) \cap L$ então existem escalares $d, d_1, \ldots, d_n \in D$ $(d \neq 0)$ tais que

$$dv = 0, \quad v = \sum_{i=1}^{n} d_i\, e_i.$$

Portanto, $0 = dv = (dd_1)e_1 + \cdots + (dd_n)e_n$ donde $dd_1 = \cdots = dd_n = 0$. Pela lei do corte, $d_1 = \cdots = d_n = 0$, o que implica $v = 0$.
(2) $\underline{M = \mathrm{Tor}\,(M) + L}$: Seja $\pi\colon M \to M/\mathrm{Tor}\,(M)$ a projecção canónica. Para cada $v \in M$, $\pi(v) = v + \mathrm{Tor}\,(M)$, e existem escalares $d_1, \ldots, d_n \in D$ tais que $\pi(v) = \sum_{i=1}^n d_i\pi(e_i)$. Então

$$v = (v - \sum_{i=1}^{n} d_i e_i) + (\sum_{i=1}^{n} d_i e_i) \in \mathrm{Tor}\,(M) + L$$

pois $v - \sum_{i=1}^n d_i e_i \in \mathrm{N}(\pi) = \mathrm{Tor}\,(M)$. ∎

Observação. O factor livre L na decomposição em 5.2 não é único pois depende da escolha de uma base em $M/\mathrm{Tor}\,(M)$. Mas, como vimos na demonstração acima, tem uma base com o mesmo número de elementos n que a base escolhida em $M/\mathrm{Tor}\,(M)$. Como D é de invariância dimensional, todas estas bases têm o mesmo número de elementos n, pelo que $\dim L = n$ e, portanto, a dimensão de L é um invariante da decomposição.

Chama-se *característica* de M a esta dimensão (dimensão da parte livre de M). Portanto, a característica de M classifica, a menos de isomorfismo, a parte livre de M.

Para classificar os módulos de tipo finito sobre um DIP falta pois classificar os módulos de torção, em que o factor livre L é nulo. É o que faremos em seguida. Esta classificação tem várias aplicações importantes no estudo das transformações lineares de um espaço vectorial e na classificação dos grupos abelianos finitos.

Denotamos por $M_n(D)$ o anel das matrizes $n \times n$ com entradas num DIP D. Necessitaremos dos seguintes resultados sobre diagonalização de matrizes em $M_n(D)$, que não demonstraremos em pormenor.

Lema 5.3. *Seja $A \in M_n(D)$ uma matriz de característica r. Se A é equivalente a uma matriz diagonal*

$$\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$$

na qual $d_1 \mid d_2 \mid \cdots \mid d_n$, então

$$d_i = 0, \text{ para } i > r, \qquad e\ d_i = \frac{\Delta_i}{\Delta_{i-1}}, \text{ para } i \leq r$$

(*onde $\Delta_0 = 1$ e Δ_i é um maior divisor comum dos menores de dimensão i da matriz A*).

Proposição 5.4. *Seja $A \in M_n(D)$. Existem matrizes invertíveis $P, Q \in M_n(D)$ tais que*

$$Q^{-1}AP = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$$

onde $d_1 \mid d_2 \mid \cdots \mid d_n$. Os elementos $d_1, \ldots, d_n$ são únicos a menos de associados.

(As matrizes A e $Q^{-1}AP$ dizem-se *equivalentes*. À matriz diagonal $Q^{-1}AP$ chama-se *forma normal*, ou *canónica*, de A. Os elementos $d_1, \ldots, d_n$ chamam-se *factores invariantes* de A.)

Demonstração. A unicidade dos d_i's segue imediatamente do Lema. Relativamente à primeira parte, limitamo-nos a indicar um algoritmo (de "eliminação") que permite obter a diagonalização através de operações elementares nas linhas e colunas da matriz $A = (a_{ij})$ (o registo destas operações permite no final determinar as matrizes P e Q requeridas).

Denotemos por E_{ij} a matriz cujas entradas são todas zero, com excepção da entrada (i, j) que é igual a 1. A multiplicação à esquerda (resp. direita) das seguintes matrizes (invertíveis) por uma matriz A permite efectuar as seguintes operações elementares usuais em A:

- Troca das linhas i, j (resp. colunas i, j):

$$P_{ij} = I - E_{ii} - E_{jj} + E_{ij} + E_{ji} = \begin{pmatrix} & & & i & & & j & & \\ 1 & & & & & & & & \\ & \ddots & & \vdots & & & \vdots & & \\ & & 1 & & & & & & \\ & \cdots & & \boxed{0} & & \cdots & \boxed{1} & & \\ & & & & 1 & & & & \\ & & & \vdots & & \ddots & \vdots & & \\ & & & & & & 1 & & \\ & \cdots & & \boxed{1} & & \cdots & \boxed{0} & & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix}$$

- Multiplicação de linhas (resp. colunas) por unidades $u \in D^*$:

$$D_i(u) = I + (u-1)E_{ii} = \begin{pmatrix} & & & i & & & \\ 1 & & & & & & \\ & \ddots & & \vdots & & & \\ & & 1 & & & & \\ & & & \boxed{u} & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

- Soma de um múltiplo $a \in D$ de uma linha (resp. coluna) a outra linha (resp. coluna):

$$T_{ij}(a) = I + aE_{ij} = \begin{pmatrix} & & i & & j & & \\ 1 & & & & & & \\ & \ddots & \vdots & & \vdots & & \\ & & 1 & \cdots & \boxed{a} & & \\ & & & \ddots & \vdots & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

Seja então A uma matriz arbitrária $n \times n$. Chamamos *comprimento* $\delta(d)$ de um elemento $d \in D$ não nulo ao número de factores primos que ocorrem na sua factorização.

Diagonalização de matrizes com entradas num DIP

(1) Se $A = 0$ não há nada a fazer. Caso contrário, alguma entrada é não nula de comprimento mínimo e podemos, com operações elementares, transportá-la para a posição $(1,1)$.

(2) Seja a_{1k} uma entrada tal que $a_{11} \nmid a_{1k}$. Trocando as colunas 2 e k podemos supor que esta entrada é a_{12}. Se $d = \mathrm{mdc}(a_{11}, a_{12})$, existem $p, q \in D$ tais que $pa_{11} + qa_{12} = d$. Para $r = a_{12}d^{-1}$ e $s = a_{11}d^{-1}$, as matrizes

$$P = \begin{pmatrix} p & r & & & \\ q & -s & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} s & r & & & \\ q & -p & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix},$$

são inversas uma da outra. Então, multiplicando A à direita pela matriz P, obtemos uma matriz equivalente a A cuja primeira linha é igual a

$$\begin{pmatrix} d & 0 & a_{13} & \cdots & a_{1n} \end{pmatrix}$$

onde $\delta(d) < \delta(a_{11})$. De igual modo, se na nova matriz $a_{11} \nmid a_{k1}$, podemos por um processo semelhante calcular um novo elemento d cujo comprimento é menor que $\delta(a_{11})$ e determinar uma matriz equivalente na qual o valor mínimo de δ foi reduzido.

Como a função δ toma valores em $\mathbb{N}$, repetindo este processo conseguiremos, ao cabo de um número finito de passos, chegar a uma matriz na qual $a_{11} \mid a_{1k}$ e $a_{11} \mid a_{k1}$ para qualquer k.

(3) Efectuando operações elementares nas linhas e colunas dessa matriz é então possível obter uma matriz equivalente à matriz original A que é da forma

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & \overline{a}_{22} & \cdots & \overline{a}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \overline{a}_{n2} & \cdots & \overline{a}_{nn} \end{pmatrix}.$$

(4) Continuando este processo para a segunda linha e a segunda coluna, etc., obteremos finalmente uma matriz

$$\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$$

equivalente à matriz original A.

DIAGONALIZAÇÃO DE MATRIZES COM ENTRADAS NUM DIP

(5) Por fim, se $d_1 \nmid d_2$, adicionamos a segunda linha à primeira linha e repetimos todo o processo novamente. Obteremos no final uma matriz diagonal na qual $d_1 \mid d_2$ (pois o comprimento $\delta(d_1)$ diminui sempre).
Procedendo desta forma repetidamente, chegaremos a uma matriz diagonal na qual $d_1 \mid d_2 \mid \cdots \mid d_n$, como pretendido. ∎

Cuidado: As matrizes P e Q não são, em geral, inversas uma da outra; portanto, este resultado não diz que uma matriz pode ser diagonalizada com uma simples mudança de base.

Além de permitir garantir a unicidade dos factores invariantes (a menos de associados), o Lema 5.3 fornece um método de cálculo destes factores (mais eficiente que o método da "eliminação"):

ALGORITMO DE CÁLCULO DOS FACTORES INVARIANTES

Seja $r = \text{car}(A)$. Então:

- $d_1 = \Delta_1$ (Δ_1 =mdc dos menores de A de dimensão 1)
- $d_2 = \dfrac{\Delta_2}{\Delta_1}$ (Δ_2 =mdc dos menores de A de dimensão 2)

  $\vdots$
- $d_r = \dfrac{\Delta_r}{\Delta_{r-1}}$ (Δ_r =mdc dos menores de A de dimensão r)
- $d_i = 0$ para $i > r$.

As fórmulas do Lema 5.3 também garantem imediatamente o seguinte:

Corolário 5.5. *Os factores invariantes são únicos a menos de associados. Duas matrizes são equivalentes se e só se possuem os mesmos factores invariantes.* ∎

Exemplo. Seja $D = \mathbb{C}[x]$ e consideremos a matriz

$$A = \begin{pmatrix} x-2 & 0 & 0 \\ -1 & x & -1 \\ -2 & 4 & x-4 \end{pmatrix}.$$

Calculando os menores, obtemos

$$\Delta_1 = 1, \Delta_2 = x-2, \Delta_3 = (x-2)^3.$$

Logo $d_1 = 1, d_2 = x-2$ e $d_3 = (x-2)^2$ e

$$A \sim \begin{pmatrix} 1 & & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)^2 \end{pmatrix}.$$

Usando o método de eliminação podemos obter as matrizes P e Q explicitamente:

$$\begin{pmatrix} 0 & -1 & 0 \\ -1 & -x+2 & 0 \\ 1 & x-4 & 1 \end{pmatrix} \begin{pmatrix} x-2 & 0 & 0 \\ -1 & x & -1 \\ -2 & 4 & x-4 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & x \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)^2 \end{pmatrix}.$$

Recordemos o aniquilador de $v \in M$ da página 59:

$$\operatorname{ann} v = \{a \in D \mid av = 0\}.$$

Como se trata de um ideal então $\operatorname{ann} v = \langle d \rangle$ para algum $d \in D$. Ao elemento d (definido a menos de associados) chama-se *ordem*[3] de v e a $\langle d \rangle$ chama-se o *ideal de ordem* de v. É claro que o submódulo cíclico $\langle v \rangle$ é isomorfo a $D/\operatorname{ann} v = D/\langle d \rangle$.

A primeira classificação que podemos obter é a seguinte:

Teorema 5.6 (Decomposição em factores cíclicos invariantes). *Seja M um módulo de tipo finito sobre um DIP D. Então*

$$M = \langle v_1 \rangle \oplus \cdots \oplus \langle v_k \rangle,$$

onde $\operatorname{ann} v_1 \supseteq \operatorname{ann} v_2 \supseteq \cdots \supseteq \operatorname{ann} v_k$. *Escrevendo* $\operatorname{ann} v_i = \langle d_i \rangle$, *temos um isomorfismo*

$$M \simeq \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_k \rangle}$$

onde $d_1 \mid d_2 \mid \cdots \mid d_k$. Os ideais $\langle d_1 \rangle, \ldots, \langle d_k \rangle$ são determinados unicamente por M.

(Os ideais $\langle d_i \rangle$ desta decomposição e os seus geradores chamam-se *factores invariantes* do módulo M.)

[3] Observe que nos $\mathbb{Z}$-módulos, isto é, nos grupos abelianos, este conceito coincide precisamente com a ordem usual de um elemento do grupo, a menos do sinal (pois neste caso as unidades são ± 1).

Demonstração. Já sabemos que se M tem característica r então

$$M = \mathrm{Tor}(M) \oplus \langle v_1 \rangle \oplus \cdots \oplus \langle v_r \rangle$$

onde cada v_i é linearmente independente. Portanto, $\operatorname{ann} v_i = \{0\}$ e

$$M \simeq \mathrm{Tor}(M) \oplus \underbrace{D \oplus \cdots \oplus D}_{r \text{ parcelas}}.$$

Basta então demonstrar o resultado para módulos de torção $M = \mathrm{Tor}(M)$.

Seja $M = \langle w_1, \ldots, w_n \rangle$ e $L = \bigoplus_{i=1}^{n} D$ (o módulo livre gerado pelos w_i's). Designemos por $\{e_1, \ldots, e_n\}$ a base canónica de L e seja $\pi \colon L \to M$ a projecção canónica

$$(d_i)_{i=1,\ldots,n} \longmapsto \sum_{i=1}^{n} d_i w_i.$$

Claro que $\pi(e_i) = w_i$ e $M \simeq L/\mathrm{N}(\pi)$. Pelo Teorema 4.3, $N = \mathrm{N}(\pi)$ é um submódulo livre de L e $\dim N \leq \dim L$. Por outro lado, como $\mathrm{Tor}(M) = M$, então para cada $w \in L$ existe $a \neq 0$ tal que $a(w + N) = 0$, ou seja, $aw \in N$. Logo existem $a_1, \ldots, a_n \in D$ não nulos tais que $a_1 e_1, \ldots, a_n e_n \in N$ o que garante que $\dim N \geq \dim L$. Portanto, $\dim N = \dim L = n$.

Seja $\{f_1, \ldots, f_n\}$ uma base de N. Existem escalares $a_{ij} \in D$ tais que

$$f_i = \sum_{j=1}^{n} a_{ji} e_j, \quad i = 1, \ldots, n.$$

Se mudarmos de bases em L e N (para novas bases $\{e'_1, \ldots, e'_n\}$ e $\{f'_1, \ldots, f'_n\}$, com matrizes de mudança de base Q e P, respectivamente), então

$$e'_i = \sum_{j=1}^{n} q_{ji} e_j, \quad f'_i = \sum_{j=1}^{n} p_{ji} f_j,$$

e obteremos novas relações

$$f'_i = \sum_{j=1}^{n} b_{ji} e'_j, \quad i = 1, \ldots, n,$$

onde as matrizes $A = (a_{ij})$, $B = (b_{ij})$, $P = (p_{ij})$ e $Q = (q_{ij})$ satisfazem

$$B = Q^{-1} A P.$$

Como vimos na Proposição 5.4, podemos escolher as matrizes invertíveis P e Q (isto é, as bases de L e N) tais que $B = \mathrm{diag}(d_1, \ldots, d_n)$ com $d_1 \mid \cdots \mid d_n$. Mas isto significa que

$$f'_i = d_i e'_i, \quad i = 1, \ldots, n.$$

Seja $w'_i = \pi(e'_i) \in M$. Então $\operatorname{ann} w'_i = \langle d_i \rangle$:

$$\begin{aligned} dw'_i = 0 &\Leftrightarrow \pi(de'_i) = 0 \Leftrightarrow de'_i \in \mathrm{N}(\pi) \\ &\Leftrightarrow de'_i = a_1 f'_1 + \cdots a_n f'_n \quad \text{(pois } \{f'_1, \ldots, f'_n\} \text{ é uma base de } N) \\ &\Leftrightarrow de'_i = a_1 d_1 e'_1 + \cdots a_n d_n e'_n \Leftrightarrow d = a_i d_i \Leftrightarrow d \in \langle d_i \rangle. \end{aligned}$$

Bastará agora mostrar que $M = \langle w'_1 \rangle \oplus \cdots \oplus \langle w'_n \rangle$:

- $\underline{M = \sum_{i=1}^{n} \langle w'_i \rangle}$: é evidente, pois os e'_i geram L e $\pi \colon L \to M$ é sobrejectiva.
- $\underline{\langle w'_k \rangle \cap \sum_{i \neq k} \langle w'_i \rangle = \{0\}}$: Seja w um elemento desta intersecção. Então existem $a_i \in D$ tais que $w = a_k w'_k = \sum_{i \neq k} a_i w'_i$. Isto implica que, em L, $a_k e'_k - \sum_{i \neq k} a_i e'_i \in N$. Como os vectores f'_i formam uma base de N e $f'_i = d_i e'_i$, então existem $b_i \in D$ tais que $a_i = b_i d_i$, $i = 1, \ldots, n$. Mas então $w = a_k w'_k = \pi(a_k e'_k) = \pi(b_k d_k e'_k) = \pi(b_k f'_k) = 0$.

A unicidade dos factores invariantes é consequência imediata de um facto provado mais adiante (Observação 5.11). ∎

Em conclusão, os factores invariantes dos módulos de tipo finito sobre um DIP formam um conjunto de *invariantes completos* para este tipo de módulos:

Corolário 5.7. *Dois módulos de tipo finito sobre um DIP são isomorfos se e só se possuem os mesmos factores invariantes.* ∎

Podemos ainda obter uma classificação alternativa, baseada no facto de em D todo o elemento $a \in D \setminus \{0\}$ ter uma factorização (única) em factores primos

$$a = u \cdot p_1 \cdots p_n \qquad (u \in D^*).$$

Lema 5.8. *Seja M um módulo sobre um DIP D e sejam $a, b \in D$, $a, b \neq 0$.*

(1) *Se $M = \langle v \rangle$ com $\operatorname{ann} v = \langle ab \rangle$ e $\operatorname{mdc}(a, b) = 1$, então*

$$M \simeq \frac{D}{\langle ab \rangle} \simeq \frac{D}{\langle a \rangle} \oplus \frac{D}{\langle b \rangle}.$$

(2) *Se $M = \langle v_1 \rangle + \langle v_2 \rangle$ com $\operatorname{ann} v_1 = \langle a \rangle$, $\operatorname{ann} v_2 = \langle b \rangle$ e $\operatorname{mdc}(a, b) = 1$, então*

$$M \simeq \frac{D}{\langle a \rangle} + \frac{D}{\langle b \rangle} \simeq \frac{D}{\langle ab \rangle}.$$

Demonstração. (1) Seja $M = \langle v \rangle$ com $\operatorname{ann} v = \langle ab \rangle$. Claro que, como $\operatorname{ann} v$ é o núcleo do homomorfismo sobrejectivo $D \to M$ $(d \mapsto dv)$, então $M \simeq D/\langle ab \rangle$. Sejam $v_1 = av \in M$ e $v_2 = bv \in M$. Então $\operatorname{ann} v_1 = \langle a \rangle$ e $\operatorname{ann} v_2 = \langle b \rangle$. Sejam $r, s \in D$ tais que $1 = ra + sb$. Então $v = (ra + sb)v = rv_1 + sv_2 \in \langle v_1 \rangle + \langle v_2 \rangle$. Logo $M = \langle v_1 \rangle + \langle v_2 \rangle$. Por outro lado, se $w \in \langle v_1 \rangle \cap \langle v_2 \rangle$ então $aw = 0 = bw$ pelo que $w = (ra + sb)w = 0$. Portanto, por 2.2,

$$M = \langle v_1 \rangle \oplus \langle v_2 \rangle \simeq \frac{D}{\langle a \rangle} \oplus \frac{D}{\langle b \rangle}.$$

(2) Sejam $r, s \in D$ tais que $1 = ra+sb$. Se $w \in \langle v_1 \rangle \cap \langle v_2 \rangle$ então $w = (ra+sb)w = 0$, pelo que $M = \langle v_1 \rangle \oplus \langle v_2 \rangle$. Seja $v = v_1 + v_2 \in M$. É evidente que $\operatorname{ann} v = \langle ab \rangle$, pelo que $D/\langle ab \rangle \simeq \langle v \rangle$. Mas $\langle v \rangle = M$, pois $v_1 = (ra + sb)v_1 = sbv_1 = sbv$ e $v_2 = (ra + sb)v_2 = rav_2 = rav$. Logo $M \simeq D/\langle ab \rangle$. ∎

Exemplo. Por exemplo, se $d \in D$ tem a factorização prima $d = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, então

$$\frac{D}{\langle d \rangle} \simeq \frac{D}{\langle p_1^{n_1} \rangle} \oplus \frac{D}{\langle p_2^{n_2} \rangle} \oplus \cdots \oplus \frac{D}{\langle p_k^{n_k} \rangle}.$$

Teorema 5.9 (Decomposição em factores cíclicos primários). *Seja M um módulo de tipo finito sobre um DIP D. Então*

$$M = L \oplus \langle w_1 \rangle \oplus \cdots \oplus \langle w_t \rangle \simeq L \oplus \frac{D}{\langle p_1^{n_1} \rangle} \oplus \cdots \oplus \frac{D}{\langle p_t^{n_t} \rangle},$$

onde L é um submódulo livre de dimensão igual à característica de M, $\operatorname{ann} w_i = \langle p_i^{n_i} \rangle$, e os elementos $p_1, \ldots, p_t \in D$ são primos. Os ideais $\langle p_i^{n_i} \rangle$ são determinados unicamente (a menos da ordem) por M.

(Os geradores dos ideais $\langle p_i^{n_i} \rangle$ desta decomposição chamam-se *divisores elementares* do módulo M.)

Demonstração. Seja

$$M = \langle v_1 \rangle \oplus \cdots \oplus \langle v_k \rangle$$

a decomposição de M em factores cíclicos invariantes. Se $\operatorname{ann} v_i = d_i$, então $d_1 \mid d_2 \mid \cdots \mid d_{k-r}$ e $d_{k-r+1} = \cdots = d_k = 0$, onde r é a característica de M. Portanto,

$$\begin{aligned} M &= \underbrace{\langle v_1 \rangle \oplus \cdots \oplus \langle v_{k-r} \rangle}_{\operatorname{Tor}(M)} \oplus \underbrace{\langle v_{k-r+1} \rangle \oplus \cdots \oplus \langle v_k \rangle}_{r \text{ parcelas}} \\ &= \underbrace{\langle v_1 \rangle \oplus \cdots \oplus \langle v_{k-r} \rangle}_{\operatorname{Tor}(M)} \oplus \underbrace{D \oplus \cdots \oplus D}_{r \text{ parcelas}} \\ &\simeq \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_{k-r} \rangle} \oplus \underbrace{D \oplus \cdots \oplus D}_{r \text{ parcelas}}. \end{aligned}$$

Basta então tomar para L o módulo livre (de dimensão r)

$$\langle v_{k-r+1}\rangle \oplus \cdots \oplus \langle v_k\rangle = D \oplus \cdots \oplus D.$$

Por outro lado, se $p_1^{n_1}, \ldots, p_t^{n_t}$ são as potências primas que entram nas decomposições primas dos $d_1, \ldots, d_{k-r}$, o Lema 5.8 assegura que

$$\frac{D}{\langle d_1\rangle} \oplus \cdots \oplus \frac{D}{\langle d_{k-r}\rangle} \simeq \frac{D}{\langle p_1^{n_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle p_t^{n_t}\rangle}.$$

Portanto,

$$M \simeq L \oplus \frac{D}{\langle p_1^{n_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle p_t^{n_t}\rangle}.$$

Quanto à unicidade, sejam

$$M \simeq L \oplus \frac{D}{\langle p_1^{n_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle p_t^{n_t}\rangle} \simeq L \oplus \frac{D}{\langle q_1^{m_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle q_s^{m_s}\rangle} \tag{5.9.1}$$

duas decomposições de M em factores cíclicos primários. Para cada primo $p \in D$, a chamada *componente p-primária* de qualquer módulo M é o submódulo

$$\{v \in M \mid p^k v = 0 \text{ para algum } k \in \mathbb{N}\}.$$

É claro que $\mathrm{Tor}(M) = \bigoplus_{p \text{ primo}} M(p)$. Neste caso, como M é de tipo finito, apenas um número finito de parcelas não é zero. Além disso, de (5.9.1) segue que

$$\begin{aligned} M(p) &\simeq \bigoplus_{\{i\colon p_i \sim p\}} \frac{D}{\langle p_i^{n_i}\rangle} \simeq \bigoplus_{\{i\colon p_i \sim p\}} \frac{D}{\langle p^{n_i}\rangle} \\ &\simeq \bigoplus_{\{i\colon q_i \sim p\}} \frac{D}{\langle q_i^{m_i}\rangle} \simeq \bigoplus_{\{i\colon q_i \sim p\}} \frac{D}{\langle p^{m_i}\rangle}. \end{aligned}$$

Portanto, a lista de primos nas duas decomposições é a mesma, e basta demonstrar a unicidade das decomposições para o caso $M = M(p)$. Sejam então

$$M(p) \simeq \frac{D}{\langle p^{n_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle p^{n_t}\rangle} \simeq \frac{D}{\langle p^{m_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle p^{m_s}\rangle}$$

duas decomposições de $M(p)$. Ordenemos as parcelas das decomposições, de forma que $n_1 \leq n_2 \leq \cdots \leq n_t$ e $m_1 \leq m_2 \leq \cdots \leq m_s$. Se $v_t \in M$ é tal que $\operatorname{ann} v_t = \langle p^{n_t}\rangle$, então a segunda decomposição mostra que $p^{m_s} v_t = 0$, logo $m_s \geq n_t$. De igual forma, vemos que $n_t \geq m_s$, logo $n_t = m_s$. O módulo quociente $M(p)/\langle v_s\rangle$ admite as decomposições

$$M(p)/\langle v_s\rangle \simeq \frac{D}{\langle p^{n_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle p^{n_{t-1}}\rangle} \simeq \frac{D}{\langle p^{m_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle p^{m_{s-1}}\rangle}.$$

Prosseguindo este raciocínio de forma indutiva, concluímos que $n_i = m_i$ e $t = s$, como pretendíamos. ∎

Temos assim um conjunto alternativo de invariantes completos que classificam os módulo de tipo finito sobre um DIP:

Corolário 5.10. *Dois módulos de tipo finito sobre um DIP são isomorfos se e só se possuem a mesma lista de divisores elementares e a mesma característica.* ∎

Observação 5.11. Vimos na demonstração do Teorema 5.9 que a decomposição em factores cíclicos invariantes determina univocamente uma decomposição de M em factores cíclicos primários. Reciprocamente, seja

$$M \simeq L \oplus \frac{D}{\langle p_1^{n_1} \rangle} \oplus \cdots \oplus \frac{D}{\langle p_t^{n_t} \rangle}$$

a decomposição de M em factores cíclicos primários. Sejam $p_1, \ldots, p_r$ os primos distintos (isto é, não associados entre si) que aparecem nesta lista. Listemos as respectivas potências que aparecem na decomposição, na seguinte tabela:

$$\begin{array}{cccc} p_1^{n_{11}} & p_2^{n_{12}} & \cdots & p_r^{n_{1r}} \\ p_1^{n_{21}} & p_2^{n_{22}} & \cdots & p_r^{n_{2r}} \\ \vdots & \vdots & & \vdots \\ p_1^{n_{s1}} & p_2^{n_{s2}} & \cdots & p_r^{n_{sr}} \end{array}$$

(onde s é o número de ocorrências do primo que aparece mais vezes e $n_{1j} \leq n_{2j} \leq \cdots \leq n_{sj}$, $j = 1, \ldots, r$; eventualmente, alguns dos n_{ij} terão que ser nulos). Seja d_i o produto das potências primas na linha i:

$$d_i = p_1^{n_{i1}} \cdot p_2^{n_{i2}} \cdots p_r^{n_{ir}}.$$

É evidente que $d_1 \mid d_2 \mid \cdots \mid d_s$. Então, como as potências primas que aparecem em cada d_i são primas entre si, pelo Lema 5.8 podemos concluir que

$$M = L \oplus \mathrm{Tor}(M) \simeq L \oplus \frac{D}{\langle p_1^{n_1} \rangle} \oplus \cdots \oplus \frac{D}{\langle p_n^{n_t} \rangle} \simeq L \oplus \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_s \rangle}.$$

Se a dimensão da parte livre L é m, então acrescentamos à lista dos d_i's os elementos $d_{s+1} = \cdots = d_{s+m} = 0$ e temos a decomposição de M em factores cíclicos invariantes.

Em conclusão, dada a lista dos $\{p_j^{n_{ij}}\}$, os d_i ficam determinados (a menos de associados), como acabámos de ver. Reciprocamente, dada a lista dos $\{d_i\}$, os $\{p_j^{n_{ij}}\}$ são as potências primas na decomposição dos d_i's. Logo, a unicidade dos factores invariantes decorre da unicidade dos divisores elementares acima provada.

Exemplos. (1) Seja

$$\frac{D}{\langle p_1 \rangle} \oplus \frac{D}{\langle p_2^2 \rangle} \oplus \frac{D}{\langle p_1 \rangle} \oplus \frac{D}{\langle p_2^2 \rangle} \oplus \frac{D}{\langle p_3 \rangle} \oplus \frac{D}{\langle p_4 \rangle} \oplus \frac{D}{\langle p_1^4 \rangle} \oplus \frac{D}{\langle p_2^5 \rangle} \oplus \frac{D}{\langle p_3^2 \rangle} \oplus \frac{D}{\langle p_4^5 \rangle}$$

a decomposição de um módulo M em factores cíclicos primários. Os seus divisores elementares são

$$p_1, p_2^2, p_1, p_2^2, p_3, p_4, p_1^4, p_2^5, p_3^2, p_4^5$$

e dispõem-se de acordo com a seguinte tabela:

$$\begin{array}{cccc} p_1 & p_2^2 & p_3^0 & p_4^0 \\ p_1 & p_2^2 & p_3 & p_4 \\ p_1^4 & p_2^5 & p_3^2 & p_4^5 \end{array}$$

Portanto, os seus factores invariantes são

$$d_1 = p_1 p_2^2, \quad d_2 = p_1 p_2^2 p_3 p_4, \quad d_3 = p_1^4 p_2^5 p_3^2 p_4^5,$$

pelo que a sua decomposição em factores cíclicos invariantes é

$$\frac{D}{\langle p_1 p_2^2 \rangle} \oplus \frac{D}{\langle p_1 p_2^2 p_3 p_4 \rangle} \oplus \frac{D}{\langle p_1^4 p_2^5 p_3^2 p_4^5 \rangle}.$$

(2) Se $n \in \mathbb{N}$ admite a factorização prima $n = p_1^{n_1} \cdots p_t^{n_t}$, então

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$$

é a decomposição do grupo abeliano $\mathbb{Z}_n$ (como $\mathbb{Z}$-módulo) em factores cíclicos primários. Os seus divisores elementares são os $p_i^{n_i}$ e existe apenas o factor invariante n.

(3) O grupo abeliano

$$G = \mathbb{Z}_{20} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{108} = \frac{\mathbb{Z}}{\langle 2^2 \times 5 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2^3 \times 5 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2^2 \times 3^3 \rangle}$$

decompõe-se em factores cíclicos primários da seguinte maneira:

$$\begin{aligned} G &\simeq \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2^3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^3 \rangle} \\ &\simeq \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{27}. \end{aligned}$$

Os respectivos divisores elementares são então as potências primas $2^2, 5, 2^3, 5, 2^2, 3^3$. Consequentemente, os factores invariantes são

$$\begin{array}{ccccccc} 2^2 & \times & 3^0 & \times & 5^0 & = & 4 \\ 2^2 & \times & 3^0 & \times & 5 & = & 20 \\ 2^3 & \times & 3^3 & \times & 5 & = & 1080 \end{array}$$

e a decomposição em factores cíclicos invariantes é

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{1080}.$$

6. Módulos e anéis noetherianos. Teorema da Base de Hilbert

A Álgebra Comutativa (isto é, o estudo dos anéis e módulos comutativos) é um ramo da Álgebra que, durante a primeira metade do séc. XX, devido ao trabalho pioneiro de Emmy Noether (1822-1935) e do seu aluno Emil Artin, aduiriu um papel central não só na Álgebra mas noutras áreas da Matemática (como, por exemplo, a Geometria Algébrica). Nesta secção final estudaremos brevemente os módulos e anéis noetherianos, fechando um ciclo iniciado no primeiro capítulo (Teorema 2.1) com a caracterização dos domínios de factorização única em termos de cadeias ascendentes de ideais principais: os módulos e anéis noetherianos satisfazem uma condição análoga.

Ao longo da secção, A designa um anel comutativo.

MÓDULOS E ANÉIS NOETHERIANOS
Um A-módulo M diz-se *noetheriano* se toda a cadeia ascende de submódulos de M, $$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k \subseteq \cdots ,$$ estabiliza, isto é, existe $k \in \mathbb{N}$ tal que $$M_k = M_{k+1} = \cdots .$$ Em particular, um anel A diz-se *noetheriano* se, como A-módulo, é noetheriano. (Como neste caso os submódulos de A são precisamente os ideais de A, isto significa que toda a cadeia ascendente de ideais de A estabiliza; portanto, todo o domínio de factorização única é noetheriano.)

Proposição 6.1. *Seja M um A-módulo. As seguintes afirmações são equivalentes:*

(1) *M é noetheriano.*

(2) *Todo o submódulo de M é de tipo finito.*

(3) *Qualquer conjunto não vazio $\{M_i\}_{i\in I}$ de submódulos de M possui um elemento maximal.*

Demonstração. (1)⇒(2): Seja N um submódulo de um módulo noetheriano M, gerado por um conjunto S. Se $v_1 \in S$ e $N = \langle v_1 \rangle$, não há nada a provar. Caso

contrário, existe $v_2 \in S \setminus \langle v_1 \rangle$ tal que $\langle v_1 \rangle \subset \langle v_1, v_2 \rangle$. Prosseguindo indutivamente obtemos $v_1, \ldots, v_n \in S$ tais que

$$\langle v_1 \rangle \subset \langle v_1, v_2 \rangle \subset \cdots \subset \langle v_1, \ldots, v_n \rangle.$$

Claro que, como M é noetheriano, existe um natural k tal que $N = \langle v_1, \ldots, v_k \rangle$.
(2)⇒(1): Se

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k \subseteq \cdots,$$

é uma cadeia ascendente de submódulos de M, o módulo $\bigcup_{k=1}^{\infty} M_k$ é de tipo finito (pois é um submódulo de M). Seja $S = \{v_1, \ldots, v_r\}$ um seu conjunto gerador. Claro que, para cada $i \in \{1, \ldots, r\}$ existe $k_i \in \mathbb{N}$ tal que $v_i \in M_{k_i}$. Seja $k_0 = \max\{k_1, \ldots, k_r\}$. Então $S \subseteq \bigcup_{k=1}^{k_0} = M_{k_0}$, logo $M_{k_0} = M_{k_0+1} = \cdots$ e M é noetheriano.
(1)⇒(3): Seja $\mathcal{P} = \{M_i\}_{i \in I}$ um conjunto não vazio de submódulos de M. Fixemos um M_1 em $\mathcal{P}$. Se M_1 é maximal, não há nada a provar. Senão, existe um $M_2 \in \mathcal{P}$ tal que $M_1 \subset M_2$. Procedendo indutivamente, obtemos uma cadeia ascendente

$$M_1 \subset M_2 \subset \cdots \subset M_n.$$

Como M é noetheriano, existe um natural k tal que $M_k = M_{k+1} = \cdots$. É evidente que M_k é um elemento maximal de $\mathcal{P}$.
(3)⇒(1): Seja

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k \subseteq \cdots,$$

uma cadeia ascendente de submódulos de M. A família $\{M_k\}_{k \in \mathbb{N}}$ possui um elemento maximal M_{k_0}, por hipótese. Mas então $M_{k_0} = M_{k_0+1} = \cdots$ e M é noetheriano. ∎

Exemplos. (1) Como todo o ideal de um DIP é principal, todo o DIP é noetheriano. Em particular, $\mathbb{Z}$ e $K[x]$ são anéis noetherianos.

(2) Veremos já a seguir (Teorema de Hilbert) que se A é um anel noetheriano, o anel dos polinómios $A[x_1, \ldots, x_n]$ também é noetheriano. No entanto, o A-módulo $A[x_1, \ldots, x_n]$ não é noetheriano pois não possui um conjunto gerador finito.

(3) Em qualquer sequência exacta de A-módulos

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

M_2 é noetheriano se e só se M_1 e M_3 são noetherianos.

(4) Se $M_1, \ldots, M_k$ são submódulos noetherianos de um A-módulo M e $M = \sum_{i=1}^{k} M_i$, então M é noetheriano.

(5) Pela proposição anterior, se M é um A-módulo noetheriano, então M é de tipo finito. O recíproco também é válido desde que A seja noetheriano: se A é um anel noetheriano e M um A-módulo de tipo finito, então M é noetheriano.

As demonstrações destes factos encontram-se na bibliografia.

Podemos agora demonstrar o primeiro dos dois teoremas famosos de Hilbert na área, fundamental para a teoria das variedades algébricas na Geometria Algébrica.

Teorema 6.2 (Teorema da Base de Hilbert). *Seja A um anel noetheriano. Então o anel de polinómios $A[x_1, \ldots, x_n]$ é noetheriano.*

Demonstração. Basta demonstrar que $A[x]$ é noetheriano sempre que A é noetheriano. Para isso mostraremos que todo o ideal $I \subseteq A[x]$ é de tipo finito.

Comecemos por definir ideais I_j de A ($j = 0, 1, 2, \ldots$) da seguinte forma:

- $0 \in I_j$;
- $a \neq 0$ pertence a I_j se e só se existe um polinómio $p(x) \in I$ de grau j com coeficiente de maior grau $a_j = a$ (isto é, $p(x) = ax^j + a_{j-1}x^{j-1} + \cdots + a_1x + a_0$).

Assim,

$$I_0 = \{0\} \cup \{a \mid \exists\, p(x) \in I \colon p(x) = a\}$$
$$I_1 = \{0\} \cup \{a \mid \exists\, p(x) \in I \colon p(x) = ax + b\}$$
$$I_2 = \{0\} \cup \{a \mid \exists\, p(x) \in I \colon p(x) = ax^2 + bx + c\}, \text{ etc.}$$

Estes ideais formam uma cadeia ascendente

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_k \subseteq \cdots$$

De facto, se $a \in I_k$, então existe $p(x) \in I$ da forma

$$p(x) = ax^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0;$$

logo, $xp(x) = ax^{k+1} + a_{k-1}x^k + \cdots + a_1x^2 + a_0x \in I$ e, portanto, $a \in I_{k+1}$.

Como A é noetheriano, existe $k_0 \in \mathbb{N}$ tal que $I_{k_0} = I_{k_0+1} = \cdots$; além disso, os ideais $I_0, \ldots, I_{k_0}$ são de tipo finito (pela proposição anterior). Para cada $j \in \{0, \ldots, k_0\}$ seja

$$I_j = \langle \{a_{j1}, a_{j2} \ldots, a_{jn_j}\} \rangle.$$

Por definição de I_j existem polinómios $p_{ij}(x)$ em I da forma

$$p_{ij}(x) = a_{ji}x^j + \cdots \qquad (i = 1, \ldots, n_j).$$

Para terminar a demonstração provaremos que

$$I = \langle \{p_{ji}(x) \mid j = 0, 1, \ldots, k_0,\ i = 1, 2, \ldots, n_j\} \rangle.$$

Seja então $p(x) = ax^k + \cdots \in I$ um polinómio em I de grau k. Provemos por indução sobre k que $p(x) \in \langle \{p_{ji}(x) \mid j = 0, 1, \ldots, k_0,\ i = 1, 2, \ldots, n_j\} \rangle$:

- $\boxed{k=0:}$ Óbvio.
- $\boxed{\text{Hipótese de indução:}}$ o resultado vale para polinómios de grau $\leq k-1$.
- $\boxed{k>0:}$ Há a considerar dois casos:

  (1) Se $k \leq k_0$, então $a \in I_k$. Existem, pois, coeficientes $b_i \in A$ tais que $a = \sum_{i=1}^{n_k} b_i a_{ki}$. Mas então $p(x) - \sum_{i=1}^{n_k} b_i p_{ki}(x)$ é um polinómio em I de grau $\leq k-1$ e, pela hipótese de indução, pertence a $\langle\{p_{ji}(x)\}\rangle$. Logo, $p(x) \in \langle\{p_{ji}(x)\}\rangle$.

  (2) Se $k > k_0$, então $a \in I_{k_0}$. Existem, pois, coeficientes $b_i \in A$ tais que $a = \sum_{i=1}^{n_{k_0}} b_i a_{k_0 i}$. Mas então $p(x) - \sum_{i=1}^{n_{k_0}} b_i p_{k_0 i}(x) x^{k-k_0}$ é um polinómio em I de grau $\leq k-1$. Logo, $p(x) \in \langle\{p_{ji}(x)\}\rangle$. ∎

Deste teorema e da proposição anterior podemos concluir imediatamente o seguinte:

Corolário 6.3. *Seja A um anel noetheriano. Então todo o ideal de $A[x_1, \ldots, x_n]$ é de tipo finito.* ∎

Isto significa que em qualquer ideal I de $A[x_1, \ldots, x_n]$ existem polinómios $p_1, \ldots, p_m \in I$ tais que todo o polinómio $p(x_1, \ldots, x_n) \in I$ pode ser escrito na forma

$$p(x_1, \ldots, x_n) = \sum_{i=1}^{m} a_i(x_1, \ldots, x_n)\, p_i(x_1, \ldots, x_n)$$

(onde os coeficientes $a_i(x_1, \ldots, x_n)$ pertencem a $A[x_1, \ldots, x_n]$). Isto justifica o termo "base" no nome do teorema (mas, em geral, os coeficientes a_i não são únicos).

Para terminar vejamos como estes factos são importantes para o estudo das chamadas *variedades algébricas*, isto é, conjuntos dos zeros de uma família de polinómios.

Seja K um corpo e $A = K[x_1, \ldots, x_n]$ o anel dos polinómios a n indeterminadas com coeficientes em K. Neste caso, podemos interpretar os polinómios $p \in A$ como funções $p\colon K^n \to K$. O conjunto dos zeros de p é o conjunto

$$\mathcal{Z}(p) = \{a \in K^n \mid p(a) = 0\}.$$

Mais geralmente, dada uma família de polinómios $F \subseteq A$, o conjunto dos zeros desta família é o conjunto

$$\mathcal{Z}(F) = \{a \in K^n \mid p(a) = 0, \forall\, a \in K\}.$$

CONJUNTOS ALGÉBRICOS E VARIEDADES ALGÉBRICAS

Um subconjunto $Y \subseteq K^n$ é um *conjunto algébrico* se existe $F \subseteq A$ tal que $Y = \mathcal{Z}(F)$. Desta forma, obtemos uma correspondência que a subconjuntos $F \subseteq A$ associa conjuntos algébricos de K^n.
Chama-se *variedade algébrica* a todo o subconjunto algébrico $Y \subseteq K^n$ *irredutível* (isto é, que não pode ser expresso como uma união $Y = Y_1 \cup Y_2$ de dois subconjuntos algébricos próprios).

Se $F \subseteq A$ e $I = \langle F \rangle$ é o ideal gerado por F, é óbvio que $\mathcal{Z}(F) = \mathcal{Z}(I)$. O Teorema da Base de Hilbert mostra que qualquer conjunto algébrico Y é de facto o conjunto dos zeros de uma família finita de polinómios: $Y = \mathcal{Z}(p_1, \ldots, p_m)$.

Por outro lado, a um subconjunto $Y \subseteq K^n$ arbitrário podemos associar o ideal de A formado pelos polinómios que se anulam em Y:

$$\mathcal{I}(Y) = \{p \in A \mid p(a) = 0, \forall\, a \in Y\}.$$

As correspondências $F \mapsto \mathcal{Z}(F)$ e $Y \mapsto \mathcal{I}(Y)$ satisfazem o seguinte:

- $F_1 \subseteq F_2 \Rightarrow \mathcal{Z}(F_2) \subseteq \mathcal{Z}(F_1)$.
- $Y_1 \subseteq Y_2 \Rightarrow \mathcal{I}(Y_2) \subseteq \mathcal{I}(Y_1)$.

Quais são os conjuntos fechados para estas correspondências, isto é, os conjuntos Y e F tais que $\mathcal{Z}(\mathcal{I}(Y)) = Y$ e $\mathcal{I}(\mathcal{Z}(F)) = F$?

Dado um conjunto $O \subseteq K^n$, diz-se que O é *aberto* se $K^n \setminus O$ é um conjunto algébrico. É um exercício simples verificar que:

(Z1) $\emptyset$ e K^n são abertos.

(Z2) Se $\{O_j\}_{j \in J}$ são abertos, então $\bigcup_{j \in J} O_j$ é aberto.

(Z3) Se $\{O_1, \ldots, O_m\}$ são abertos, então $\bigcap_{i=1}^{m} O_j$ é aberto.

Portanto, a família dos abertos de K^n é uma topologia (a chamada *topologia de Zariski*). Os fechados desta topologia são, por definição, os conjuntos algébricos. A condição sobre cadeias de ideais ascendentes quando traduzida em termos desta topologia significa o seguinte[4]: toda a cadeia ascendente de abertos

$$O_1 \subseteq O_2 \subseteq \cdots \subseteq O_n \subseteq \cdots$$

estabiliza, isto é, existe $k \in \mathbb{N}$ tal que $O_k = O_{k+1} = \cdots$ ..

[4] A uma topologia que satisfaz esta condição chama-se *topologia noetheriana*.

Se $Y \subseteq K^n$ é um conjunto arbitrário, então $\mathcal{Z}(\mathcal{I}(Y))$ é o fecho $\overline{Y}$ de Y na topologia de Zariski (Exercícios 3.26, 3.27).

O segundo teorema de Hilbert nesta área (o famoso Teorema dos Zeros de Hilbert[5]) afirma que

$$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I},$$

onde $\sqrt{I}$ é o chamado *radical* de I:

$$\sqrt{I} = \{p \in A \mid \exists\, m \in \mathbb{N}\colon p^m \in I\}.$$

Em conclusão, os conjuntos fechados para as correspondências $F \mapsto \mathcal{Z}(F)$ e $Y \mapsto \mathcal{I}(Y)$ são precisamente os fechados na topologia de Zariski em K^n (ou seja, os conjuntos algébricos de K^n) e os *ideais radicais* de $K[x_1, \ldots, x_n]$, isto é, os ideais $I \subseteq K[x_1, \ldots, x_n]$ tais que $\sqrt{I} = I$. Portanto:

> *Existe uma correspondência bijectiva entre conjuntos algébricos $Y \subseteq K^n$ e ideais radicais $I \subseteq K[x_1, \ldots, x_n]$.*
>
> *Nesta correspondência, às variedades algébricas correspondem os ideais primos.*[6]

De facto, se Y é uma variedade algébrica e $p(x_1, \ldots, x_n)q(x_1, \ldots, x_n) \in \mathcal{I}(Y)$, então $Y \subseteq \mathcal{Z}(pq) = \mathcal{Z}(p) \cup \mathcal{Z}(q)$, logo $Y = (Y \cap \mathcal{Z}(p)) \cup (Y \cap \mathcal{Z}(q))$; como Y é irredutível, vemos que ou $Y = Y \cap \mathcal{Z}(p)$ ou $Y = Y \cap \mathcal{Z}(q)$, isto é, ou $Y \subseteq \mathcal{Z}(p)$ ou $Y \subseteq \mathcal{Z}(q)$, o que significa que $p \in \mathcal{I}(Y)$ ou $q \in \mathcal{I}(Y)$; portanto, $\mathcal{I}(Y)$ é um ideal primo.

Isto mostra como o estudo de zeros de polinómios está intimamente relacionado com o estudo dos anéis comutativos e dos seus ideais e como proposições sobre variedades algébricas correspondem a certas proposições de Álgebra Comutativa sobre ideais primos e ideais radicais.

[5] *Nullstellensatz von Hilbert*, na designação alemã.

[6] Note que todo o ideal primo é um ideal radical.

Exercícios

3.1. Mostre que:

(a) Se $\phi\colon M_1 \to M_2$ é um homomorfismo de A-módulos, o seu núcleo $N(\phi)$ e a sua imagem $\mathrm{Im}(\phi)$ são submódulos de M_1 e M_2 respectivamente.

(b) Um homomorfismo de $\mathbb{Z}$-módulos é um homomorfismo de grupos abelianos.

(c) Se V_1 e V_2 são espaços vectoriais sobre um corpo K, os K-homomorfismos $\phi\colon V_1 \to V_2$ são as transformações lineares usuais.

3.2. Seja V um espaço vectorial sobre um corpo K e $T\colon V \to V$ uma transformação linear.

(a) Mostre que V é um $K[x]$-módulo quando se define multiplicação de um elemento $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ por um elemento $v \in V$ por

$$p(x)v = a_n T^n(v) + \cdots + a_1 T(v) + a_0 v.$$

(b) Quais são os submódulos do $K[x]$-módulo V ?

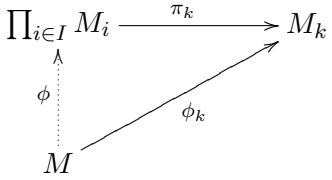
(c) Seja $V = \mathbb{R}^n$ e $T\colon \mathbb{R}^n \to \mathbb{R}^n$ definida por

$$T(v_1, \ldots, v_n) = (v_n, v_1, \ldots, v_{n-1}).$$

Determine os elementos $v \in \mathbb{R}^n$ tais que $(x^2 - 1)v = 0$.

3.3. Seja $\{M_i\}_{i\in I}$ uma família de A-módulos. Mostre que:

(a) Dado um A-módulo M e homomorfismos $\{\phi_i\colon M \to M_i\}_{i\in I}$, existe um único homomorfismo $\phi\colon M \to \prod_{i\in I} M_i$ tal que, para cada $k \in I$, o diagrama

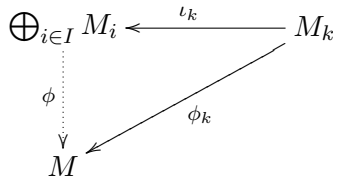


comuta.

(b) $\prod_{i\in I} M_i$ é determinado a menos de um isomorfismo pela propriedade expressa em (a).

3.4. Seja $\{M_i\}_{i\in I}$ uma família de A-módulos. Mostre que:

(a) Dado um A-módulo M e homomorfismos $\{\phi_i\colon M_i \to M\}_{i\in I}$, existe um único homomorfismo $\phi\colon \bigoplus_{i\in I} M_i \to M$ tal que, para cada $k \in I$, o diagrama



comuta.

(b) $\bigoplus_{i\in I} M_i$ é determinado a menos de um isomorfismo pela propriedade expressa em (a).

3.5. Sejam M_1 e M_2 dois submódulos de um A-módulo M. Prove que:

(a) Se

(1) $M = M_1 + M_2$,

(2) $M_1 \cap M_2 = \{0\}$,

então cada $v \in M$ escreve-se de modo único na forma $v_1 + v_2 \in M_1 + M_2$.

(b) $M = M_1 \oplus M_2$ se e só se as condições (1) e (2) se verificam.
(Portanto, $M_1 + M_2 = M_1 \oplus M_2$ se e só se $M_1 \cap M_2 = \{0\}$.)

3.6. Uma sucessão de homomorfismos de A-módulos

$$M_0 \xrightarrow{\phi_1} M_1 \xrightarrow{\phi_2} M_2 \longrightarrow \cdots \xrightarrow{\phi_n} M_n$$

diz-se *exacta* se $\mathrm{Im}(\phi_i) = N(\phi_{i+1})$, $i = 1, 2, \ldots, n-1$. Mostre que:

(a) Se $N \subseteq M$ é um submódulo, então a sucessão

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0$$

é exacta.

(b) Se M_1 e M_2 são A-módulos, então a sucessão

$$0 \longrightarrow M_1 \xrightarrow{\iota_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0$$

é exacta.

3.7. (**Lema pequeno dos Cinco**) Considere o seguinte diagrama comutativo de A-módulos e homomorfismos

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_3} & & \downarrow{\scriptstyle \phi_4} & & \\ 0 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & 0 \end{array}$$

onde as linhas horizontais são exactas. Mostre que:

(a) Se ϕ_2 e ϕ_4 são injectivos então ϕ_3 é injectivo.

(b) Se ϕ_2 e ϕ_4 são sobrejectivos então ϕ_3 é sobrejectivo.

(c) Se ϕ_2 e ϕ_4 são isomorfismos então ϕ_3 é um isomorfismo.

3.8. (**Lema dos Cinco**) Considere o seguinte diagrama comutativo de A-módulos e homomorfismos

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_3} & & \downarrow{\scriptstyle \phi_4} & & \downarrow{\scriptstyle \phi_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

onde as linhas horizontais são exactas. Mostre que:

(a) Se ϕ_2 e ϕ_4 são injectivos e ϕ_1 é sobrejectivo então ϕ_3 é injectivo.

(b) Se ϕ_2 e ϕ_4 são sobrejectivos e ϕ_5 é injectivo então ϕ_3 é sobrejectivo.

(c) Se ϕ_1, ϕ_2, ϕ_4 e ϕ_5 são isomorfismos então ϕ_3 é um isomorfismo.

3.9. Considere o $\mathbb{R}$-módulo $\mathbb{R}$ e a soma directa $\mathbb{R}^\infty = \bigoplus_{i=1}^{\infty} \mathbb{R}$. Mostre que:

(a) O conjunto $A = \mathrm{End}(\mathbb{R}^\infty)$ das transformações $\mathbb{R}$-lineares de $\mathbb{R}^\infty$ é um anel unitário para as operações seguintes:

$$\begin{aligned} (f+g)((a_n)_{n\in\mathbb{N}}) &= f((a_n)_{n\in\mathbb{N}}) + g((a_n)_{n\in\mathbb{N}}) \\ (fg)((a_n)_{n\in\mathbb{N}}) &= (f\circ g)((a_n)_{n\in\mathbb{N}}). \end{aligned}$$

(b) O anel A da alínea anterior, visto como A-módulo, satisfaz $A \simeq A \oplus A$, isto é, A, além da base singular $\{1\}$, também possui uma base com 2 elementos.

3.10. Seja A um anel comutativo. Mostre que:

(a) Se $B, C \in M_n(A)$, então $BC = I_{n\times n}$ implica $CB = I_{n\times n}$.

(b) Se B é uma matriz $m \times n$, C é uma matriz $n \times m$, $BC = I_{m\times m}$ e $CB = I_{n\times n}$, então $m = n$.

3.11. Seja A um anel comutativo, e M um A-módulo.

(a) Mostre que, se $v \in \mathrm{Tor}(M)$, então $\langle v\rangle \subseteq \mathrm{Tor}(M)$.

(b) É $\mathrm{Tor}(M)$ um submódulo de M ?

3.12. Seja D um domínio de integridade e M um D-módulo. Mostre que:

(a) Se M é livre então é livre de torção.

(b) $M/\mathrm{Tor}(M)$ é um D-módulo livre de torção.

3.13. Mostre que se V é um espaço vectorial de dimensão finita sobre um corpo K e $T\colon V \to V$ uma transformação linear, então V é um $K[x]$-módulo de torção.

3.14. Mostre que:

(a) Se $\phi\colon M_1 \to M_2$ é um homomorfismo de D-módulos, então $\phi(\mathrm{Tor}\,(M_1)) \subseteq \mathrm{Tor}\,(M_2)$. Se ϕ é injectivo, então $\phi(\mathrm{Tor}\,(M_1)) = \mathrm{Tor}\,(M_2) \cap \mathrm{Im}(\phi)$. Se ϕ é sobrejectivo com $\mathrm{N}(\phi) \subseteq \mathrm{Tor}\,(M_1)$, então $\phi(\mathrm{Tor}\,(M_1)) = \mathrm{Tor}\,(M_2)$.

(b) Se M é um D-módulo, então $M/\mathrm{Tor}\,(M)$ é um D-módulo livre de torção.

(c) Se $\{M_i\}_{i\in I}$ é uma família de D-módulos, então

$$\mathrm{Tor}\,(\bigoplus_{i\in I} M_i) = \bigoplus_{i\in I} \mathrm{Tor}\,(M_i).$$

3.15. Seja A um anel comutativo. Mostre que $\mathrm{End}_A(A^n)$ é isomorfo ao anel $M_n(A)$ das matrizes $n \times n$ com entradas em A.

3.16. Determine matrizes diagonais equivalentes às matrizes

(a) $\begin{pmatrix} 36 & 12 \\ 16 & 18 \end{pmatrix}$ sobre $\mathbb{Z}$. (b) $\begin{pmatrix} x-1 & -2 & -1 \\ 0 & x & 1 \\ 0 & -2 & x-3 \end{pmatrix}$ sobre $\mathbb{R}[x]$.

3.17. Mostre que se p é um primo, as seguintes duas matrizes de $M_n(\mathbb{Z}_p)$ são equivalentes:

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

3.18. Seja D um domínio de ideais principais e p_1, p_2, p_3, p_4 elementos primos de D. Determine as decomposições do D-módulo

$$\frac{D}{\langle p_1\, p_2^2\, p_3\rangle} \oplus \frac{D}{\langle p_1\, p_2^3\, p_3^2\, p_4\rangle} \oplus \frac{D}{\langle p_1^3\, p_2^2\, p_4^5\rangle}$$

em factores cíclicos invariantes e em factores cíclicos primários.

3.19. Sejam M_1 e M_2 dois D-módulos cíclicos de ordens a e b, respectivamente. Mostre que se $\mathrm{mdc}(a,b) \neq 1$, então os factores invariantes de $M_1 \oplus M_2$ são $\mathrm{mdc}(a,b)$ e $\mathrm{mmc}(a,b)$.

3.20. Determine todos os grupos abelianos de ordem 120.

3.21. Seja $T\colon V \to V$ uma transformação linear de um espaço vectorial de dimensão finita sobre um corpo K e suponha que $V \simeq \langle v\rangle$ (como $K[x]$-módulo), onde $\mathrm{ann}(v) = \langle (x-\lambda)^m\rangle$. Mostre que os elementos

$$\{(x-\lambda)^{m-1}v, \ldots, (x-\lambda)v, v\}$$

formam uma base de V sobre K.

3.22. Mostre que:

(a) Todo o DIP é noetheriano.

(b) Se $0 \to M_1 \to M_2 \to M_3 \to 0$ é uma sequência exacta de A-módulos, então M_2 é noetheriano se e só se M_1 e M_3 são noetherianos.

(c) Se $M_1, \ldots, M_k$ são submódulos noetherianos de um A-módulo M e $M = \sum_{i=1}^{k} M_i$, então M é noetheriano.

(d) Se A é um anel noetheriano e M é um A-módulo de tipo finito, então M é noetheriano.

3.23. Mostre que um anel A é noetheriano se e só se todo o ideal $I \subseteq A$ é finitamente gerado.

3.24. Seja A um anel comutativo e seja N um submódulo de um A-módulo M. Prove que se M é noetheriano, então N e M/N também são noetherianos.

3.25. Seja M um módulo noetheriano e $f\colon M \to M$ um homomorfismo sobrejectivo. Mostre que:

(a) Para cada $n \in \mathbb{N}$, f^n é um homomorfismo sobrejectivo e $N(f^n) \subseteq N(f^{n+1})$.

(b) Existe um natural k tal que $N(f^k) = N(f^{k+1})$.

(c) f é um isomorfismo.

3.26. Seja K um corpo e $A = K[x_1, \ldots, x_n]$. Se $F \subseteq A$ é uma família de polinómios, designamos por $\mathcal{Z}(F)$ o conjunto dos zeros comuns aos polinómios de F:

$$\mathcal{Z}(F) = \{a \in K^n \mid p(a) = 0, \forall p \in F\}.$$

Um *conjunto algébrico* $Y \subseteq K^n$ é um conjunto para o qual existe uma família $F \subseteq A$ tal que $Y = \mathcal{Z}(F)$. Dado um conjunto $O \subseteq K^n$, diz-se que O é *aberto* se $K^n \setminus O$ é um conjunto algébrico. Mostre que:

(a) $\emptyset$ e K^n são abertos.

(b) Se $\{O_j\}_{j \in J}$ são abertos, então $\bigcup_{j \in J} O_j$ é aberto.

(c) Se $\{O_1, \ldots, O_m\}$ são abertos, então $\bigcap_{i=1}^{m} O_j$ é aberto.

3.27. Pelo exercício anterior, a família dos abertos de K^n é uma topologia (a chamada *topologia de Zariski*). Os fechados desta topologia são os conjuntos algébricos. Mostre que:

(a) A topologia de Zariski em K não é *Hausdorff* (ou *separável*, isto é, existem $a, b \in K$, com $a \neq b$, para os quais não é possível encontrar abertos disjuntos O_a e O_b tais que $a \in O_a$ e $b \in O_b$).

(b) Se $Y \subseteq K^n$ e $\mathcal{I}(Y) = \{p \in A \mid p(a) = 0, \ \forall\, a \in Y\}$, então $\mathcal{Z}(\mathcal{I}(Y))$ é o fecho $\overline{Y}$ de Y na topologia de Zariski.

3.28. Mostre que em $\mathbb{Z}$, sendo $p_1^{n_1} \cdots p_t^{n_t}$ a factorização prima de a, então

$$\sqrt{\langle a \rangle} = \langle p_1 \cdots p_t \rangle.$$

3.29. Seja A um anel comutativo e $I, I_1, \ldots, I_r$ ideais de A. Mostre que:

(a) $\sqrt{\sqrt{I}} = \sqrt{I}$.

(b) $\sqrt{I_1 \cdots I_r} = \sqrt{\bigcap_{j=1}^{r} I_j} = \bigcap_{j=1}^{r} \sqrt{I_j}$.

(c) $\sqrt{I^r} = \sqrt{I}$.

Soluções de exercícios seleccionados

3.2. **(b)** $W \subseteq V$ é um submódulo de V se e só se

(1) W é um subgrupo de $(V, +)$.

(2) $p(x) \in K[x], v \in W \Rightarrow p(x)v \in W$.

Então:

Proposição. *W é um submódulo de V se é só se é um subespaço vectorial de V invariante pela transformação T (isto é, $T(v) \in W$ para qualquer $v \in W$).*

Demonstração. $\Rightarrow$: Aplicando (2) a polinómios $p(x)$ de grau zero obtemos $av \in W$ para qualquer $a \in K$. Portanto, conjuntamente com (1), isto assegura que W é um subespaço vectorial.

Aplicando agora (2) ao polinómio $p(x) = x$ podemos concluir que xv, isto é, $T(v)$ pertence a W. Assim, W é necessariamente invariante por T.

A implicação recíproca é óbvia pois é evidente que, usando a hipótese, $p(x)v = a_n T^n(v) + \cdots + a_1 T(v) + a_0 v \in W$ para qualquer polinómio $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ e qualquer $v \in W$. ∎

(c) Seja $v = (v_1, v_2, \ldots, v_n) \in \mathbb{R}^n$. Então

$$(x^2 - 1)v = T^2(v) - v = (v_{n-1}, v_n, v_1, \ldots, v_{n-2}) - (v_1, v_2, v_3, \ldots, v_n).$$

Logo $(x^2 - 1)v = 0$ se e só se $v_1 = v_3$, $v_2 = v_4$, $v_3 = v_5$, …, $v_{n-1} = v_1$ e $v_n = v_2$. Portanto, se n é par, $(x^2 - 1)v = 0$ se e só se $v = (v_1, v_2, v_1, \ldots, v_2)$ $(v_1, v_2 \in \mathbb{R})$; se n é ímpar, $(x^2 - 1)v = 0$ se e só se $v = (v_1, v_1, v_1, \ldots, v_1)$ $(v_1 \in \mathbb{R})$.

3.3. **(a)** Seja $v \in M$. A condição $\pi_k \circ \phi = \phi_k$ $(k \in I)$ significa que $\pi_k(\phi(v)) = \phi_k(v)$ para cada $v \in M$, o que implica necessariamente que $\phi(v)$ tenha que ser igual a $(\phi_k(v))_{k \in I}$. Isto garante a unicidade de ϕ. Basta agora verificar que a aplicação ϕ definida deste modo é de facto um homomorfismo de A-módulos, o que é fácil, pois é uma consequência imediata da definição das operações de A-módulo no produto directo $\prod_{i \in I} M_i$:

- $\phi(v) + \phi(w) = (\phi_k(v))_{k \in I} + (\phi_k(w))_{k \in I} = (\phi_k(v) + \phi_k(w))_{k \in I} = (\phi_k(v + w))_{k \in I} = \phi(v + w)$.
- $a\phi(v) = a(\phi_k(v))_{k \in I} = (a\phi_k(v))_{k \in I} = (\phi_k(av))_{k \in I} = \phi(av)$.

(b) Seja N um outro A-módulo e $p_k\colon N \to M_k$ $(k \in I)$ homomorfismos de A-módulos que satisfazem a propriedade expressa em (a). Então existem homomorfismos (únicos) $\phi\colon N \to \prod_{i\in I} M_i$ e $\psi\colon \prod_{i\in I} M_i \to N$ tais que $\pi_k \circ \phi = p_k$ e $p_k \circ \psi = \pi_k$ para cada $k \in I$. Então $p_k = p_k \circ \psi \circ \phi$ e $\pi_k = \pi_k \circ \phi\psi$ donde segue, pela propriedade (a), que $\psi\phi = \mathrm{id}_N$ e $\phi\psi = \mathrm{id}_{\prod_{i\in I} M_i}$. Portanto, N é isomorfo a $\prod_{i\in I} M_i$.

3.4. **(a)** Para cada $v \in M_k$, $\iota_k(v)$ é o elemento $(e_i^{v,k})_{i\in I}$ de $\bigoplus_{i\in I} M_i$ definido por

$$e_i^{v,k} = \begin{cases} v & \text{se } i = k \\ 0 & \text{se } i \neq k. \end{cases}$$

Assim, para cada $(v_k)_{k\in I} \in \bigoplus_{i\in I} M_i$, se denotarmos por F o conjunto finito de índices em I tais que $v_k \neq 0$, temos $(v_k)_{k\in I} = \sum_{k\in F} \iota_k(v_k)$. Logo, $\phi((v_k)_{k\in I})$ terá que ser necessariamente igual a $\sum_{k\in F} \phi(\iota_k(v_k))$. Como $\phi \circ \iota_k = \phi_k$ $(k \in I)$, então necessariamente

$$\phi((v_k)_{k\in I}) = \sum_{k\in F} \phi_k(v_k).$$

Isto garante a unicidade de ϕ. Como cada um dos ϕ_k é um homomorfismo de A-módulos, é evidente que a aplicação ϕ definida deste modo é também um homomorfismo de A-módulos.

(b) Pode resolver-se de modo análogo a 3.3(b).

3.7. **(a)** Consideremos o diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_3} & & \downarrow{\scriptstyle \phi_4} & & \\ 0 & \longrightarrow & N_2 & \xrightarrow[g_2]{} & N_3 & \xrightarrow[g_3]{} & N_4 & \longrightarrow & 0 \end{array}$$

onde ϕ_2 e ϕ_4 são injectivos e suponhamos que $\phi_3(m_3) = 0$. Então $\phi_4 f_3(m_3) = g_3\phi_3(m_3) = 0$ e, como ϕ_4 é injectiva, $f_3(m_3) = 0$, isto é, $m_3 \in \mathrm{N}(f_3) = \mathrm{Im}(f_2)$. Assim, existe $m_2 \in M_2$ tal que $f_2(m_2) = m_3$. Mas então $\phi_2(m_2) \in \mathrm{N}(g_2)$ pois $g_2\phi_2(m_2) = \phi_3 f_2(m_2) = \phi_3(m_3) = 0$. Além disso, pela exactidão da sucessão, $\mathrm{N}(g_2) = \{0\}$ (isto é, g_2 é injectiva). Portanto, $\phi_2(m_2) = 0$. Finalmente, como ϕ_2 é injectiva, então $m_2 = 0$ e, consequentemente, $m_3 = 0$.

(b) Suponhamos desta vez que ϕ_2 e ϕ_4 são sobrejectivos. Seja $n_3 \in N_3$. Pela sobrejectividade de ϕ_4 existe $m_4 \in M_4$ tal que $\phi_4(m_4) = g_3(n_3)$. Mas pela exactidão da sucessão, $\mathrm{Im}(f_3) = M_4$ (isto é, f_3 é sobrejectiva), logo

$m_4 = f_3(m_3)$ para algum $m_3 \in M_3$. Agora $g_3\phi_3(m_3) = \phi_4 f_3(m_3) = g_3(n_3)$, pelo que $g_3(\phi_3(m_3) - n_3) = 0$, ou seja, $\phi_3(m_3) - n_3 \in \mathrm{N}(g_3) = \mathrm{Im}(g_2)$. Logo, $\phi_3(m_3) - n_3 = g_2(n_2)$ para algum $n_2 \in N_2$, e como ϕ_2 também é sobrejectiva, $g_2(n_2) = g_2\phi_2(m_2)$ para algum $m_2 \in M_2$. Finalmente, $\phi_3 f_2(m_2) = g_2\phi_2(m_2) = g_2(n_2) = \phi_3(m_3) - n_3$, pelo que $n_3 = \phi_3(m_3) - \phi_3(f_2(m_2)) = \phi_3(m_3 - f_2(m_2))$.

(c) Consequência imediata de (a) e (b).

3.8. **(a)** Consideremos o diagrama

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_3} & & \downarrow{\scriptstyle \phi_4} & & \downarrow{\scriptstyle \phi_5} \\ N_1 & \xrightarrow[g_1]{} & N_2 & \xrightarrow[g_2]{} & N_3 & \xrightarrow[g_3]{} & N_4 & \xrightarrow[g_4]{} & N_5 \end{array}$$

onde ϕ_1 é sobrejectivo e ϕ_2 e ϕ_4 são injectivos e suponhamos que $\phi_3(m_3) = 0$. Então $g_3\phi_3(m_3) = 0$, ou seja, $\phi_4 f_3(m_3) = 0$. Logo, pela injectividade de ϕ_4:

$$\begin{aligned} f_3(m_3) = 0 &\Leftrightarrow m_3 \in \mathrm{N}(f_3) = \mathrm{Im}(f_2) \\ &\Rightarrow \exists\, m_2 \in M_2 \colon f_2(m_2) = m_3 \\ &\Rightarrow \exists\, m_2 \in M_2 \colon 0 = \phi_3(m_3) = \phi_3 f_2(m_2) = g_2\phi_2(m_2) \\ &\Rightarrow \exists\, m_2 \in M_2 \colon \phi_2(m_2) \in \mathrm{N}(g_2) = \mathrm{Im}(g_1) \\ &\Rightarrow \exists\, n_1 \in N_1 \colon g_1(n_1) = \phi_2(m_2). \end{aligned}$$

Como ϕ_1 é sobrejectivo, então existe $m_1 \in M_1$ tal que $\phi_1(m_1) = n_1$ ou seja $\phi_2 f_1(m_1) = g_1\phi_1(m_1) = \phi_2(m_2)$. Finalmente, pela injectividade de ϕ_2 decorre que $f_1(m_1) = m_2$, isto é, $m_2 \in \mathrm{Im}(f_1) = \mathrm{N}(f_2)$. Logo, $0 = f_2(m_2) = m_3$, e $m_3 = 0$ como desejávamos demonstrar.

(b) Suponhamos desta vez que ϕ_1 é injectivo e ϕ_2 e ϕ_4 são sobrejectivos. Seja $n_3 \in N_3$. Pela sobrejectividade de ϕ_4 existe $m_4 \in M_4$ tal que $\phi_4(m_4) = g_3(n_3)$. Mas $\phi_5 f_4(m_4) = g_4\phi_4(m_4) = g_4 g_3(n_3) = 0$ logo, pela injectividade de ϕ_5, $m_4 \in \mathrm{N}(f_4) = \mathrm{Im}(f_3)$. Então

$$\begin{aligned} &\exists\, m_3 \in M_3 \colon m_4 = f_3(m_3) \\ \Rightarrow &\exists\, m_3 \in M_3 \colon g_3(n_3) = \phi_4(m_4) = \phi_4 f_3(m_3) = g_3\phi_3(m_3) \\ \Leftrightarrow &\exists\, m_3 \in M_3 \colon g_3(\phi_3(m_3) - n_3) = 0 \\ \Leftrightarrow &\exists\, m_3 \in M_3 \colon \phi_3(m_3) - n_3 \in \mathrm{N}(g_3) = \mathrm{Im}(g_2) \\ \Rightarrow &\exists\, n_2 \in N_2 \colon g_2(n_2) = \phi_3(m_3) - n_3. \end{aligned}$$

Como ϕ_2 é sobrejectivo, então existe $m_2 \in M_2$ tal que $\phi_2(m_2) = n_2$ e então $\phi_3 f_2(m_2) = g_2\phi_2(m_2) = \phi_3(m_3) - n_3$, ou seja,

$$n_3 = \phi_3(m_3) - \phi_3 f_2(m_2) = \phi_3(m_3 - f_2(m_2)).$$

(c) Consequência imediata de (a) e (b).

3.9. **(b)** $\mathbb{R}^\infty$ é o $\mathbb{R}$-módulo livre gerado por $\mathbb{N}$. Seja $\{e_n \mid n \in \mathbb{N}\}$ a sua base canónica ($e_n = (0, 0, \ldots, 0, 1, 0, \ldots)$), e consideremos as funções $f_1, f_2 \in A$ definidas respectivamente por

$$f_1(e_n) = \begin{cases} e_{\frac{n}{2}} & \text{se } n \text{ é par} \\ 0 & \text{se } n \text{ é ímpar} \end{cases} \quad \text{e} \quad f_2(e_n) = \begin{cases} e_{\frac{n+1}{2}} & \text{se } n \text{ é ímpar} \\ 0 & \text{se } n \text{ é par.} \end{cases}$$

Quanto à independência linear, consideremos uma combinação linear nula de f_1 e f_2, $\phi_1 \circ f_1 + \phi_2 \circ f_2 = 0$. Isto significa que, para cada $n \in \mathbb{N}$, $\phi_1(f_1(e_n)) + \phi_2(f_2(e_n)) = 0$, ou seja,

$$\begin{cases} \phi_1(e_{\frac{n}{2}}) = 0 & \text{se } n \text{ par} \\ \\ \phi_2(e_{\frac{n+1}{2}}) = 0 & \text{se } n \text{ ímpar.} \end{cases}$$

É claro que, como $\{\frac{n}{2} \mid n \text{ é par}\} = \mathbb{N} = \{\frac{n+1}{2} \mid n \text{ é ímpar}\}$, isto significa ainda que $\phi_1(e_n) = 0 = \phi_2(e_n)$ para qualquer natural n. Logo, $\phi_1 = \phi_2 = 0$.

Trata-se também de um conjunto gerador de A: cada $f \in A$ pode escrever-se na forma $\phi_1 \circ f_1 + \phi_2 \circ f_2$ onde $\phi_1(e_n) = g(e_{2n})$ e $\phi_2(e_n) = g(e_{2n-1})$ para cada $n \in \mathbb{N}$.

Podemos imediatamente estender este raciocínio e obter uma base

$$\{f_1, f_2, \ldots, f_m\}$$

de A com um qualquer número m de elementos:

$$f_1(e_n) = \begin{cases} e_{\frac{n}{m}} & \text{se } m \mid n \\ 0 & \text{senão} \end{cases}, \quad f_2(e_n) = \begin{cases} e_{\frac{n+1}{m}} & \text{se } m \mid (n+1) \\ 0 & \text{senão} \end{cases}, \ldots$$

$$\ldots, \quad f_m(e_n) = \begin{cases} e_{\frac{n+(m-1)}{m}} & \text{se } m \mid (n + (m-1)) \\ 0 & \text{senão.} \end{cases}$$

3.10. **(a)** $BC = I_{n\times n}$ implica $\det(B)\det(C) = 1$, pelo que $\det(B) \in A^*$. Então B é uma matriz invertível, isto é, existe $B^{-1} \in M_n(A)$ tal que $BB^{-1} = B^{-1}B = I_{n\times n}$. Logo $C = I_{n\times n}B^{-1} = B^{-1}$ e $CB = I_{n\times n}$.

(b) Suponhamos sem perda de generalidade que $m \geq n$. Se, por absurdo, $m > n$, teríamos:

$$I_{m\times m} = BC = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \begin{pmatrix} C_1 & C_2 \end{pmatrix} = \begin{pmatrix} B_1C_1 & B_1C_2 \\ B_2C_1 & B_2C_2 \end{pmatrix}$$

onde $B_1, C_1 \in M_n(A)$, B_2 é uma matriz $(m-n)\times n$ e C_2 é uma matriz $n\times(m-n)$. Imediatamente teríamos $B_1C_1 = I_{n\times n}$ e $B_2C_2 = I_{(m-n)\times(m-n)}$. Então, por (a), $C_1B_1 = I_{n\times n}$. Mas, por outro lado,

$$I_{n\times n} = CB = \begin{pmatrix} C_1 & C_2 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} = C_1B_1 + C_2B_2.$$

Logo $C_2B_2 = 0$. A contradição desejada é agora óbvia: $B_2 = B_2C_2B_2 = 0$, $C_2 = C_2B_2C_2 = 0$ e portanto $B_2C_2 = 0$ seria um bloco diagonal da matriz $BC = I_{m\times m}$.

3.11. **(b)** Pode não ser, como vimos na demonstração da Proposição 4.1: só conseguimos garantir isso caso A seja um domínio de integridade.

3.12. **(a)** Suponhamos que M é livre, isto é, possui uma base $\{e_i\}_{i\in I}$. Sejam $v \in M \setminus \{0\}$ e $d \in D \setminus \{0\}$. Podemos escrever v na forma

$$v = \sum_{j=1}^{m} a_j\, e_{i_j}$$

para alguns $a_j \in D$ não nulos. Multiplicando por d obtemos

$$dv = \sum_{j=1}^{m} da_j e_{i_j}.$$

Se $dv = 0$ então, como os e_i são linearmente independentes, $da_j = 0$ para $j = 1, \ldots, m$. Como D é um domínio de integridade e $d \neq 0$ então $a_j = 0$ para $j = 1, \ldots, m$, isto é, $v = 0$ (um absurdo!). Portanto, $dv \neq 0$ para quaisquer $v \in M \setminus \{0\}$ e $d \in D \setminus \{0\}$. Logo $\mathrm{Tor}(M) = \{0\}$.

(b) Seja $v + \mathrm{Tor}(M)$ um elemento não nulo de $M/\mathrm{Tor}(M)$ (portanto $v \notin \mathrm{Tor}(M)$). Seja $d \in D \setminus \{0\}$. Então $d(v + \mathrm{Tor}(M)) = dv + \mathrm{Tor}(M)$. Mas $v \notin \mathrm{Tor}(M)$ implica obviamente $dv \notin \mathrm{Tor}(M)$ pelo que $d(v + \mathrm{Tor}(M)) \neq 0$, donde

$$\mathrm{Tor}(M/\mathrm{Tor}(M)) = \{0\}$$

como desejávamos provar.

3.16. **(a)** Usando o Lema 5.3,

$$\Delta_0 = 1, \quad \Delta_1 = \operatorname{mdc}(12, 16, 18, 36) = 2, \quad \Delta_2 = 36 \times 18 - 16 \times 12 = 456,$$

logo $d_1 = 2/1 = 1$ e $d_2 = 456/2 = 228$. Portanto,

$$A = \begin{pmatrix} 36 & 12 \\ 16 & 18 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & 228 \end{pmatrix} = B.$$

Nota: Se precisarmos de calcular explicitamente as matrizes P e Q tais que $Q^{-1}AP =$, aplicamos o algoritmo de diagonalização da pág. 71 e procedemos do seguinte modo:

- $36 \nmid 12 \rightsquigarrow d = \operatorname{mdc}(36, 12) = 12 = \underbrace{1}_{p} \times 36 + \underbrace{(-2)}_{q} \times 12.$

  Então $r = 12/12 = 1$ e $s = 36/12 = 3$. Fazendo

  $$P_1 = \begin{pmatrix} p & r \\ q & -s \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -2 & -3 \end{pmatrix},$$

  obtemos

  $$AP_1 = \begin{pmatrix} 36 & 12 \\ 16 & 18 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -2 & -3 \end{pmatrix} = \begin{pmatrix} 12 & 0 \\ -20 & -38 \end{pmatrix}.$$

- $12 \nmid -20 \rightsquigarrow d = \operatorname{mdc}(12, -20) = 4 = \underbrace{2}_{p} \times 12 + \underbrace{1}_{q} \times (-20).$

  Então $r = -20/4 = -5$ e $s = 12/4 = 3$. Fazendo

  $$P_2^{-1} = \begin{pmatrix} p & q \\ r & -s \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -5 & -3 \end{pmatrix},$$

  obtemos

  $$P_2^{-1}AP_1 = \begin{pmatrix} 2 & 1 \\ -5 & -3 \end{pmatrix} \begin{pmatrix} 12 & 0 \\ -20 & -38 \end{pmatrix} = \begin{pmatrix} 4 & -38 \\ 0 & 114 \end{pmatrix}.$$

- $4 \nmid -38 \rightsquigarrow d = \operatorname{mdc}(4, -38) = 2 = \underbrace{(-9)}_{p} \times 4 + \underbrace{(-1)}_{q} \times (-38).$

  Então $r = -38/2 = -19$ e $s = 4/2 = 2$. Fazendo

  $$P_3 = \begin{pmatrix} p & r \\ q & -s \end{pmatrix} = \begin{pmatrix} -9 & -19 \\ -1 & -2 \end{pmatrix},$$

  obtemos

  $$P_2^{-1}AP_1P_3 = \begin{pmatrix} 4 & -38 \\ 0 & 114 \end{pmatrix} \begin{pmatrix} -9 & -19 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ -114 & -228 \end{pmatrix}.$$

Nesta matriz já $2 \mid 0$ e $2 \mid 114$ pelo que bastará agora usar operações elementares:

$$\begin{pmatrix} 2 & 0 \\ -114 & -228 \end{pmatrix} \overset{57L_1+L_2}{\longrightarrow} \begin{pmatrix} 2 & 0 \\ 0 & -228 \end{pmatrix} \overset{-L_2}{\longrightarrow} \begin{pmatrix} 2 & 0 \\ 0 & 228 \end{pmatrix}.$$

Ambas as operações são nas linhas, a primeira corresponde a multiplicar à esquerda pela matriz $Q_1 = T_{21}(57) = I + 57E_{21}$, enquanto a segunda corresponde a multiplicar, também à esquerda, pela matriz $Q_2 = D_2(-1) = I - 2E_{22}$:

$$Q_2Q_1P_2^{-1}AP_1P_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 57 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ -114 & -228 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 228 \end{pmatrix}.$$

- Concluindo,

$$P = P_1P_3 = \begin{pmatrix} 1 & 1 \\ -2 & -3 \end{pmatrix} \begin{pmatrix} -9 & -19 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} -10 & -21 \\ 21 & 44 \end{pmatrix}$$

e

$$Q^{-1} = Q_2Q_1P_2^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 57 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -5 & -3 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -109 & -54 \end{pmatrix}.$$

pelo que

$$Q = \begin{pmatrix} -54 & -1 \\ 109 & 2 \end{pmatrix}.$$

Portanto,

$$B = Q^{-1}AP = \begin{pmatrix} 2 & 1 \\ -109 & -54 \end{pmatrix} \begin{pmatrix} 36 & 12 \\ 16 & 18 \end{pmatrix} \begin{pmatrix} -10 & -21 \\ 21 & 44 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 228 \end{pmatrix}.$$

Nota: O facto de na matriz diagonal, obtida após as operações elementares, d_1 $(= 2)$ dividir logo d_2 $(= 228)$ foi um acaso! Podíamos ter obtido uma matriz na qual $d_1 \nmid d_2$. O que fazer nesse caso? Por exemplo, suponhamos que tinha dado $d_1 = 2$ e $d_2 = 7$. Neste caso, continuávamos com a aplicação do algoritmo:

- $$A' = \begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix} \overset{L_1+L_2}{\longrightarrow} \begin{pmatrix} 2 & 7 \\ 0 & 7 \end{pmatrix},$$

  o que equivale a multiplicar a matriz à esquerda por

$$Q_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

- $2 \nmid 7 \rightsquigarrow d = \text{mdc}\,(2,7) = 1 = \underbrace{(-2)}_{p} \times 2 + \underbrace{1}_{q} \times 7.$

  Então $r = 7$ e $s = 2$. Fazendo

  $$P_4 = \begin{pmatrix} p & r \\ q & -s \end{pmatrix} = \begin{pmatrix} -3 & 7 \\ 1 & -2 \end{pmatrix},$$

  obtemos

  $$Q_3 A' P_4 = \begin{pmatrix} 2 & 7 \\ 0 & 7 \end{pmatrix} \begin{pmatrix} -3 & 7 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 7 & -14 \end{pmatrix}.$$

- Finalmente,

  $$\begin{pmatrix} 1 & 0 \\ 7 & -14 \end{pmatrix} \xrightarrow{-7L_1+L_2} \begin{pmatrix} 1 & 0 \\ 0 & -14 \end{pmatrix},$$

  o que corresponde a multiplicar à esquerda pela matriz

  $$Q_4 = \begin{pmatrix} 1 & 0 \\ -7 & 1 \end{pmatrix}.$$

  Assim,

  $$Q_4 Q_3 A' P_4 = \begin{pmatrix} 1 & 0 \\ -7 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix} \begin{pmatrix} -3 & 7 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -14 \end{pmatrix}.$$

(b) $\Delta_0 = 1$, $\Delta_1 = \text{mdc}\,(x-1, -2, -1, \ldots) = 1$;

$\Delta_2 = \text{mdc}\,(x(x-1), x-1, x-2, -2(x-1), \ldots) = 1$ (pois $\text{mdc}\,(x-1, x-2) = 1$);

$\Delta_3 = (x-1)(x(x-3)+2) = (x-1)(x^2-3x+2)$.

Logo $d_1 = 1$, $d_2 = 1$ e $d_3 = (x-1)(x^2-3x+2)$. Portanto,

$$A \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x-1)(x^2-3x+2) \end{pmatrix}.$$

3.18. Como p_1, p_2, p_3, p_4 são primos entre si, usando o Lema 5.8 obtemos

$$\begin{aligned} &\frac{D}{\langle p_1\, p_2^2\, p_3 \rangle} \oplus \frac{D}{\langle p_1\, p_2^3\, p_3^2\, p_4 \rangle} \oplus \frac{D}{\langle p_1^3\, p_2^2\, p_4^5 \rangle} \\ &\qquad \simeq \frac{D}{\langle p_1 \rangle} \oplus \frac{D}{\langle p_2^2 \rangle} \oplus \frac{D}{\langle p_3 \rangle} \oplus \frac{D}{\langle p_1 \rangle} \oplus \frac{D}{\langle p_2^3 \rangle} \oplus \frac{D}{\langle p_3^2 \rangle} \oplus \frac{D}{\langle p_4 \rangle} \oplus \frac{D}{\langle p_1^3 \rangle} \oplus \frac{D}{\langle p_2^2 \rangle} \oplus \frac{D}{\langle p_4^5 \rangle}. \end{aligned}$$

Esta última é a decomposição em factores cíclicos primários. Os respectivos divisores elementares são então as potências primas

$$p_1, p_2^2, p_3, p_1, p_2^3, p_3^2, p_4, p_1^3, p_2^2, p_4^5.$$

Consequentemente, os factores invariantes são

$$\begin{array}{ccccccc} p_1 & \times & p_2^2 & \times & p_3^0 & \times & p_4^0 \\ p_1 & \times & p_2^2 & \times & p_3 & \times & p_4 \\ p_1^3 & \times & p_2^3 & \times & p_3^2 & \times & p_4^5 \end{array}$$

e a decomposição em factores cíclicos invariantes é

$$\frac{D}{\langle p_1\, p_2^2\rangle} \oplus \frac{D}{\langle p_1\, p_2^2\, p_3\, p_4\rangle} \oplus \frac{D}{\langle p_1^3\, p_2^3\, p_3^2\, p_4^5\rangle}.$$

3.20. Seja G um grupo abeliano de ordem 120. Trata-se de um módulo de tipo finito sobre um DIP ($\mathbb{Z}$) pelo que podemos aplicar os teoremas da decomposição em factores invariantes ou divisores elementares. É claro que $\mathrm{Tor}(G) = G$ pelo que a característica de G é zero e G não possui componente livre. Logo, pelo teorema da decomposição em factores primários,

$$G \simeq \frac{\mathbb{Z}}{\langle p_1^{n_1}\rangle} \oplus \cdots \oplus \frac{\mathbb{Z}}{\langle p_t^{n_t}\rangle} \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$$

onde os $p_i^{n_i}$ são os divisores elementares de G. Como

$$120 = |G| = |\mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}| = p_1^{n_1} \times \cdots \times p_t^{n_t}$$

então $p_1^{n_1} \times \cdots \times p_t^{n_t} = 2^3 \times 3 \times 5$. Portanto, existem três possibilidades para os divisores elementares de G:

- $t = 3, p_1^{n_1} = 2^3, p_2^{n_2} = 3, p_3^{n_3} = 5$, que corresponde ao grupo $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.
- $t = 4, p_1^{n_1} = 2, p_2^{n_2} = 2^2, p_3^{n_3} = 3, p_4^{n_4} = 5$, que corresponde ao grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.
- $t = 5, p_1^{n_1} = 2, p_2^{n_2} = 2, p_3^{n_3} = 2, p_4^{n_4} = 3, p_5^{n_5} = 5$, que corresponde ao grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

Em conclusão, existem três grupos distintos com 120 elementos.

Nota: Os factores invariantes correspondentes a cada uma destas decomposições primárias são:

- $2^3 \times 3 \times 5 = 120$, que corresponde ao grupo $\mathbb{Z}_{120}$ (que é de facto isomorfo a $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$, pelo Lema 5.8).
- $\left[\begin{array}{ccccccc} 2 & \times & 3^0 & \times & 5^0 & = & 2 \\ 2^2 & \times & 3 & \times & 5 & = & 60 \end{array}\right.$, que corresponde ao grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_{60}$.
- $\left[\begin{array}{ccccccc} 2 & \times & 3^0 & \times & 5^0 & = & 2 \\ 2 & \times & 3^0 & \times & 5^0 & = & 2 \\ 2 & \times & 3 & \times & 5 & = & 30 \end{array}\right.$, que corresponde ao grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$.

3.24. Pela Proposição 6.1, basta provar que todos os submódulos de N e M/N são de tipo finito:

- Seja S um submódulo de N. Então é um submódulo de M, logo é de tipo finito.
- Por outro lado, todo o submódulo de M/N é da forma S/N onde S é um submódulo de M e $N \subseteq S \subseteq M$. Como M é noetheriano, S possui um conjunto gerador finito $\{v_1, \ldots, v_r\}$. É evidente que então $\{v_1 + N, \ldots, v_r + N\}$ é um conjunto gerador de S/N.

3.25. **(a)** f^n é a composição

$$\underbrace{f \circ f \circ \cdots \circ f}_{n}$$

e a composição de homomorfismos é um homomorfismo donde f^n é um homomorfismo. Claro que sendo f sobrejectivo por hipótese, também cada f^n o é (de facto, para cada $y \in M$ existe $x_1 \in M$ tal que $f(x_1) = y$ e, por sua vez, existe $x_2 \in M$ tal que $f(x_2) = x_1$, ou seja, $f^2(x_2) = f(x_1) = y$; continuando este raciocínio obteremos $x_n \in M$ tal que $f^n(x_n) = y$). Finalmente, se $x \in N(f^n)$, isto é, $f^n(x) = 0$ então $f^{n+1}(x) = f(f^n(x)) = f(0) = 0$ e $x \in N(f^{n+1})$ também.

(b) A cadeia

$$N(f) \subseteq N(f^2) \subseteq N(f^3) \subseteq \cdots$$

é uma cadeia ascendente de submódulos de M. Como M é noetheriano, terá que existir um natural k tal que $N(f^k) = N(f^{k+1})$.

(c) Basta provar que f é injectivo, isto é, $N(f) = \{0\}$. Seja então $x \in N(f)$. Como f^k é sobrejectiva, existe um $y \in M$ tal que $f^k(y) = x$. Mas então $0 = f(x) = f^{k+1}(y)$, ou seja, $y \in N(f^{k+1}) = N(f^k)$. Logo $x = f^k(y) = 0$.

3.26. **(a)** Basta observar que $K^n \setminus \emptyset = K^n = \mathcal{Z}(\{0\})$ e $K^n \setminus K^n = \emptyset = \mathcal{Z}(A)$ (ou $\mathcal{Z}(\{1\})$ ou $\mathcal{Z}(\{x_1, x_1 - 1\})$).

(b) Por hipótese, $K^n \setminus O_j = \mathcal{Z}(F_j)$. Então $K^n \setminus \bigcup_{j\in J} O_j = \bigcap_{j\in J}(K^n \setminus O_j) = \bigcap_{j\in J} \mathcal{Z}(F_j)$. Mas esta intersecção é claramente igual a $\mathcal{Z}(\bigcup_{j\in J} F_j)$, logo está provado.

(c) Por hipótese, $K^n \setminus O_j = \mathcal{Z}(F_j)$ $(j = 1, \ldots, m)$. Então $K^n \setminus \bigcap_{j=1}^m O_j = \bigcup_{j=1}^m (K^n \setminus O_j) = \bigcup_{j=1}^m \mathcal{Z}(F_j)$. Basta agora observar que $\bigcup_{j=1}^m \mathcal{Z}(F_j) = \mathcal{Z}(\bigcap_{j=1}^m \langle F_j \rangle)$:

"$\subseteq$": Se $a \in \mathcal{Z}(F_i)$ então $p(a) = 0$ para qualquer $p \in F_i$. Consequentemente, $p(a) = 0$ para qualquer $p \in \langle F_i \rangle$. Portanto, $a \in \mathcal{Z}(\bigcap_{j=1}^m \langle F_j \rangle)$.

"$\supseteq$": Suponhamos que $a \in K^n$ é tal que $p(a) = 0$ para qualquer $p \in \bigcap_{j=1}^m \langle F_j \rangle$. Por absurdo, se $a \notin \bigcup_{j=1}^m \mathcal{Z}(F_j)$ então existem $p_j \in F_j$ $(j = 1, \ldots, m)$ tais que $p_j(a) \neq 0$. Mas então, como cada $p_j \in \langle F_j \rangle$, $p = p_1 p_2 \ldots p_m \in \bigcap_{j=1}^m \langle F_j \rangle$ e, no entanto, $p(a) \neq 0$, uma contradição.

3.27. **(b)** $\mathcal{Z}(\mathcal{I}(Y))$ é o fecho de $Y \subseteq K^n$ na topologia de Zariski:

- É um fechado porque é claramente um conjunto algébrico.
- $Y \subseteq \mathcal{Z}(\mathcal{I}(Y))$ como é evidente.
- Falta só mostrar que $\mathcal{Z}(\mathcal{I}(Y))$ é o menor fechado (isto é, conjunto algébrico) que contém Y. Seja então W um conjunto algébrico que contém Y. Então $Y \subseteq W = \mathcal{Z}(F_W)$ para algum $F_W \subseteq K^n$ e

$$\mathcal{I}(Y) \supseteq \mathcal{I}(W) = \mathcal{I}(\mathcal{Z}(F_W)). \qquad (*)$$

Provemos que $\mathcal{Z}(\mathcal{I}(Y)) \subseteq W$:
Seja $a \in \mathcal{Z}(\mathcal{I}(Y))$, isto é, tal que $p(a) = 0$ para qualquer $p \in \mathcal{I}(Y)$. Como cada $q \in F_W \subseteq \mathcal{I}(\mathcal{Z}(F_W))$ está em $\mathcal{I}(Y)$ (por $(*)$), então $q(a) = 0$.

3.28. Por definição,

$$\sqrt{\langle a \rangle} = \{b \in \mathbb{Z} \mid \exists n \in \mathbb{N} \colon b^n \in \langle a \rangle\} = \{b \in \mathbb{Z} \mid \exists n \in \mathbb{N} \colon a \mid b^n\}.$$

Mas

$$a \mid b^n \Leftrightarrow p_1^{n_1} \cdots p_t^{n_t} \mid b^n \Leftrightarrow p_i \mid b \ (\forall i = 1, \ldots, t) \Leftrightarrow p_1 \cdots p_t \mid b.$$

Portanto $\sqrt{\langle a \rangle} = \langle p_1 \cdots p_t \rangle$.

3.29. **(a)**

$$\begin{aligned} \sqrt{\sqrt{I}} &= \{a \in A \mid a^n \in \sqrt{I} \text{ para algum } n \in \mathbb{N}\} \\ &= \{a \in A \mid \exists n \in \mathbb{N} \exists m \in \mathbb{N} \colon a^{nm} \in I\} = \sqrt{I}. \end{aligned}$$

(b) Primeira identidade: Se $a \in \sqrt{I_1 \cdots I_r}$, então existe $n \in \mathbb{N}$ tal que $a^n \in I_1 \cdots I_r \subseteq I_1 \cap \cdots \cap I_r$ logo $a \in \sqrt{I_1 \cap \cdots \cap I_r}$. Inversamente, se $a \in \sqrt{I_1 \cap \cdots \cap I_r}$, então existe $n \in \mathbb{N}$ tal que $a^n \in I_1 \cap \cdots \cap I_r$. Portanto, $a^{rn} = a^n \cdot a^n \cdots a^n \in I_1 I_2 \cdots I_r$, pelo que $a \in \sqrt{I_1 \cdots I_r}$.

Segunda identidade: Se $a \in \sqrt{I_1 \cap \cdots \cap I_r}$, então $a^n \in I_1 \cap \cdots \cap I_r$ para algum $n \in \mathbb{N}$, pelo que $a \in \sqrt{I_1} \cap \cdots \cap \sqrt{I_r}$. Inversamente, se $a \in \sqrt{I_1} \cap \cdots \cap \sqrt{I_r}$, então para cada $j = 1, \ldots, r$ existe $n_j \in \mathbb{N}$ tal que $a^{n_j} \in I_j$. Mas então $a^{n_1 + \cdots + n_r} = a^{n_1} \cdots a^{n_r} \in I_1 \cdots I_r \subseteq I_1 \cap \cdots \cap I_r$, o que mostra que $a \in \sqrt{I_1 \cap \cdots \cap I_r}$.

(c) Como $I^r \subseteq I$, então $\sqrt{I^r} \subseteq \sqrt{I}$. Inversamente, se $a \in \sqrt{I}$ então $a^n \in I$ para algum $n \in \mathbb{N}$, pelo que $a^{nr} = \underbrace{a^n \cdots a^n}_{r \text{ factores}} \in I^r$. Logo $a \in \sqrt{I^r}$.

Solução alternativa: trata-se de um caso particular de (b):

$$\sqrt{I^r} = \underbrace{\sqrt{I \cdots I}}_{r \text{ factores}} = \sqrt{\bigcap_{j=1}^{r} I} = \sqrt{I}.$$