ÁLGEBRA COMUTATIVA

Jorge Picado

Departamento de Matemática

Universidade de Coimbra

2013

Capítulo 1

Anéis (revisitados)

Pré-requisitos

- noções básicas de grupos, anéis, domínios de integridade e corpos.
- os anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{Z}_n, +_n, \times_n)$; anéis de polinómios.
- divisibilidade, mdc e mmc.
- ideais principais, ideais primos e ideais maximais. Domínios de ideais principais (DIP).

(`www.mat.uc.pt/~picado/corpos/apontamentos.html`: Capítulos 1 e 2)

Ao longo do curso, se nada for dito em contrário, assumiremos que A denota um **anel comutativo com identidade**. Denotaremos por A^* o conjunto das unidades de A.

1. Divisibilidade. Elementos primos e irredutíveis

Dois elementos $a, b \in A$ dizem-se *associados* se existir $u \in A^*$ tal que $a = ub$.
Diz-se que a *divide* b (e escreve-se $a \mid b$) se existir $c \in A$ tal que $ac = b$.

Propriedades básicas:

(1) A relação "ser associado" (que denotaremos por $\sim$) é uma relação de equivalência, em que a classe de cada elemento a é o conjunto $aA^* = \{au \mid u \in A^*\}$.

(2) A relação $\mid$ é reflexiva e transitiva mas nunca é simétrica ($1 \mid 0$ mas $0 \nmid 1$) e não é necessariamente anti-simétrica (pense por exemplo em $\mathbb{Z}$, no facto de $2 \mid -2$ e $-2 \mid 2$; mas em $\mathbb{Z}_2$ já é anti-simétrica).

(3) Se $a \mid b$ e $c \mid d$ então $ac \mid bd$.

(4) Num domínio de integridade, $\langle a \rangle \subseteq \langle b \rangle$ se e só se $b \mid a$. Como $p \mid q$ e $q \mid p$ se e só se p e q forem associados, então $\langle a \rangle = \langle b \rangle$ se e só se a e b são associados. Além disso, $a \in A^*$ se e só se $\langle a \rangle = A$.

(5) Se A é um domínio de integridade então $A[x]^* = A^*$.

Demonstração. Exercício. ∎

O Teorema da Factorização Única nos inteiros e nos anéis de polinómios (com coeficientes num domínio de integridade) são tão importantes que é natural averiguar se se podem generalizar a outros anéis. Por outro lado, os anéis de polinómios exibem tantas semelhanças com o anel $\mathbb{Z}$ dos inteiros que é bem possível que não sejam mera coincidência, e sejam sim casos particulares de resultados válidos num contexto muito mais geral.

Como sabemos, os inteiros primos podem ser caracterizados de várias maneiras. Por exemplo, um inteiro $p \neq 0$ não invertível é primo se e só se

$$p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b.$$

Equivalentemente, p é primo se e só se

$$p = ab \Rightarrow a = \pm 1 \text{ ou } b = \pm 1.$$

É claro que podemos adaptar qualquer uma destas condições a um domínio de integridade qualquer. Como deixam de ser equivalentes teremos que arranjar um nome diferente para denominar os elementos que verificam a segunda:

Seja D um domínio de integridade.

- Um elemento $p \in D$ diz-se *primo* se $p \neq 0$, $p \notin D^*$, e $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.
- Um elemento $q \in D$ diz-se *irredutível* se $q \neq 0$, $q \notin D^*$, e $q = ab \Rightarrow a \in D^*$ ou $b \in D^*$.

Portanto, os elementos irredutíveis são os que apenas admitem factorizações triviais e um elemento $p \neq 0$ é primo se e só se o respectivo ideal principal $\langle p \rangle$ é primo. As tabelas seguintes comparam estas definições em 3 exemplos importantes: $\mathbb{Z}$, $C[x]$ (C: corpo) e $D[x]$ (D: domínio).

DOMÍNIO	$\mathbb{Z}$
unidades	$\mathbb{Z}^* = \{-1, 1\}$
primo	$p \neq 0, \pm 1$ $p\|ab \Rightarrow p\|a$ ou $p\|b$
irredutível	$p \neq 0, \pm 1$ $p = ab \Rightarrow a \in \mathbb{Z}^*$ ou $b \in \mathbb{Z}^*$ isto é $p = ab \Rightarrow a = 1$ ou $a = -1$ ou $b = 1$ ou $b = -1$

DOMÍNIO	$\boldsymbol{C[x]}$ (C: corpo)
unidades	$C[x]^* = \{p(\boldsymbol{x}) \in C[x] : gr(p(\boldsymbol{x})) = 0\}$
primo	$gr(p(\boldsymbol{x})) \geq 1$ $p(\boldsymbol{x})\|a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow p(\boldsymbol{x})\|a(\boldsymbol{x})$ ou $p(\boldsymbol{x})\|b(\boldsymbol{x})$
irredutível	$gr(p(\boldsymbol{x})) \geq 1$ $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow a(\boldsymbol{x}) \in C[x]^*$ ou $b(\boldsymbol{x}) \in C[x]^*$ isto é $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow gr(a(\boldsymbol{x})) = 0$ ou $gr(b(\boldsymbol{x})) = 0$

DOMÍNIO	$\boldsymbol{D[x]}$ (D: domínio de integridade)
unidades	$D[x]^* = \{p(\boldsymbol{x}) \in D[x] : gr(p(\boldsymbol{x})) = 0, p(\boldsymbol{x}) = c \in D^*\}$
primo	$p(\boldsymbol{x}) \neq 0$, $p(\boldsymbol{x}) \notin D[x]^*$ $p(\boldsymbol{x})\|a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow p(\boldsymbol{x})\|a(\boldsymbol{x})$ ou $p(\boldsymbol{x})\|b(\boldsymbol{x})$
irredutível	$p(\boldsymbol{x}) \neq 0$, $p(\boldsymbol{x}) \notin D[x]^*$ $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow a(\boldsymbol{x}) \in D[x]^*$ ou $b(\boldsymbol{x}) \in D[x]^*$ isto é $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow a(\boldsymbol{x}) = c \in D^*$ ou $b(\boldsymbol{x}) = d \in D^*$

Como sabemos, além de $\mathbb{Z}$, também em $C[x]$ os elementos primos coincidem com os elementos irredutíveis. Não é esse o caso em todos os domínios de inte-

gridade, mas é possível identificar extensas classes de domínios onde estas duas noções são equivalentes.

Proposição 1.1. *Seja D um domínio de integridade e $u \in D^*$.*

(1) *Se p é primo então up é primo. Se q é irredutível então uq é irredutível.*

(2) *Todo o elemento primo é irredutível.*

Demonstração. (1) Exercício.

(2) Se p é primo e $p = ab$ então $p \mid ab$ e, portanto, $p|a$ ou $p|b$. Se, por exemplo, $p|a$, então existe $x \in D$ tal que $a = px$. Concluímos então que $p = ab = pxb$, e como $p \neq 0$, $1 = xb$, ou seja, b é uma unidade. De igual forma, se $p|b$ concluímos que a é invertível. ∎

A implicação recíproca da de (2) é, em geral, falsa. Por exemplo, no domínio

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\},$$

3 é irredutível mas não é primo, uma vez que 3 divide $(2 + \sqrt{-5})(2 - \sqrt{-5})$ (pois $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 3 \cdot 3$) mas não divide $2 + \sqrt{-5}$ nem $2 - \sqrt{-5}$. Note que neste exemplo não há factorizações únicas:

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}),$$

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Proposição 1.2. *Seja D um domínio de integridade e $p \in D$, $p \neq 0$.*

(1) *p é primo se e só se o ideal principal $\langle p \rangle$ é primo.*

(2) *Se o ideal principal $\langle p \rangle$ é maximal então p é irredutível.*

Demonstração. São consequência imediata das definições e das propriedades básicas que já verificámos. ∎

A recíproca da afirmação (2) não é, em geral, verdadeira: 2 é um elemento irredutível de $\mathbb{Z}[x]$ mas $\langle 2 \rangle$ não é um ideal maximal de $\mathbb{Z}[x]$ pois $\langle 2 \rangle \subset \langle 2, x \rangle \subset \mathbb{Z}[x]$. O problema neste exemplo reside no facto de o ideal $\langle 2, x \rangle$ não ser principal (e, portanto, $\mathbb{Z}[x]$ não ser um DIP). Com efeito:

Proposição 1.3. *Seja D um domínio de ideais principais. Então $\langle p \rangle$ é maximal se e só se p é irredutível.*

Demonstração. Seja p irredutível e $\langle p\rangle \subseteq \langle a\rangle$. Então $a \mid p$, e portanto ou $a \in D^*$ (e logo $\langle a\rangle = D$), ou a é um associado de p (e logo $\langle a\rangle = \langle p\rangle$). Assim, $\langle p\rangle$ é maximal. ∎

(Onde usámos a hipótese de D ser um DIP?)

Corolário 1.4. *Num domínio de ideais principais, um elemento é irredutível se e só se é primo.*

Demonstração. Seja p um elemento irredutível e suponhamos que $p \mid ab$. Consideremos o ideal principal $I = \langle p\rangle$. Pela proposição anterior, I é maximal pelo que o anel quociente D/I é um corpo (logo não tem divisores de zero). Mas

$$(a + I) \cdot (b + I) = ab + I = I,$$

uma vez que, por hipótese, $ab \in I$. Então, necessariamente um dos factores é nulo, isto é, $a + I = I$ ou $b + I = I$. Isto significa precisamente que $a \in I$ ou $b \in I$, ou seja, $p \mid a$ ou $p \mid b$. ∎

Observação. É claro que se nos tivéssemos lembrado (Corpos e Equações Algébricas) que

todo o ideal maximal é primo,

ou que

I é primo sse D/I é um domínio de integridade,

a prova era ainda mais rápida: decorre imediatamente de 1.2 e 1.3.

2. Domínios de factorização única

Um domínio de integridade D diz-se um *domínio de factorização única* (abreviadamente, DFU) se as seguintes duas condições são satisfeitas para todo o elemento não nulo $a \in D \setminus D^*$:

(F) Existem elementos **irredutíveis** $p_1, p_2, \ldots, p_n$ tais que

$$a = p_1 p_2 \cdots p_n. \tag{2.1.1}$$

(U) Se $p_1, p_2, \ldots, p_n$ e $q_1, q_2, \ldots, q_m$ são irredutíveis e $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, então $m = n$ e existe uma permutação $\pi \in S_n$ tal que $p_i \sim q_{\pi(i)}$ para $i = 1, 2, \ldots, n$.

Por outras palavras, num domínio de factorização única, todo o elemento não nulo e não invertível possui uma factorização num produto de elementos irredutíveis, e esta decomposição é única a menos da ordem dos factores e de produto por unidades; após reordenação, para cada i existe uma unidade u_i tal que $p_i = q_i u_i$.

Por exemplo, em $\mathbb{Z}$,

$$1 \times 5 = 5 \times 1 = (-1) \times (-5) = (-5) \times (-1)$$

são as únicas factorizações do primo 5 e

$$1 \times (-5) = (-5) \times 1 = (-1) \times 5 = 5 \times (-1)$$

são as únicas factorizações do primo -5. Pelo Teorema Fundamental da Aritmética, $\mathbb{Z}$ é um domínio de factorização única. Pelo Teorema da Factorização Única em $C[x]$ (estudado no ano passado) $C[x]$ é também um DFU. Outro exemplo de domínio de factorização única é o anel dos *inteiros de Gauss*,

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

O exemplo $\mathbb{Z}[\sqrt{-5}]$ que vimos logo a seguir à Proposição 1.1 mostra que nem todo o domínio de integridade é um DFU.

Chama-se também *anéis de Gauss* aos domínios de factorização única. O Corolário 1.4 pode ser estendido aos domínios de factorização única:

Teorema 2.1. *Seja D um domínio de integridade. Então D é um DFU se e só se as seguintes condições se verificam:*

(1) *Todo o elemento irredutível é primo.*

(2) *toda a cadeia ascendente de ideais principais estabiliza, isto é, se*

$$\langle d_1 \rangle \subseteq \langle d_2 \rangle \subseteq \cdots \subseteq \langle d_n \rangle \subseteq \cdots$$

é uma cadeia ascendente de ideais, então existe um natural k tal que

$$\langle d_n \rangle = \langle d_k \rangle \text{ para todo o } n \geq k.$$

(Equivalentemente, a condição (2) significa que, sempre que $\cdots d_n \mid d_{n-1} \mid \cdots \mid d_1$ em D, então existe um natural k tal que $d_n \sim d_k$ para todo o $n \geq k$.)

Demonstração. Seja D um DFU e $p \in D$ um elemento irredutível. Se $p \mid ab$ então $ab = px$ para algum $x \in D$, onde x, a e b possuem factorizações do tipo (2.1.1):

$$x = p_1 p_2 \cdots p_n,\ a = q_1 q_2 \cdots q_m,\ b = r_1 r_2 \cdots r_k$$

com p_i, q_i, r_i irredutíveis em D. Logo $pp_1p_2\cdots p_n = q_1q_2\cdots q_m r_1 r_2 \cdots r_k$, e pela unicidade da factorização, p é associado de algum q_i ou de algum r_j. No primeiro caso, $p \mid a$, e no segundo, $p \mid b$. Logo, p é primo.

Por outro lado, seja

$$\langle d_1\rangle \subseteq \langle d_2\rangle \subseteq \cdots \subseteq \langle d_n\rangle \subseteq \cdots$$

uma cadeia ascendente de ideais principais. Claro que podemos supor $d_1 \neq 0$ e $d_i \notin D^*$ para todo o i. Seja

$$p_{i,1}\, p_{i,2}\, \cdots\, p_{i,n_i}$$

a factorização de cada d_i em factores irredutíveis. Como $d_i \mid d_1$ para qualquer i, os factores irredutíveis de d_i são factores de d_1, pelo que $n_i \leq n_1$. É então evidente que não poderão existir na cadeia mais de n_1 ideais distintos entre si. Consequentemente, existe um natural k tal que $\langle d_n\rangle = \langle d_k\rangle$ para todo o $n \geq k$.

Reciprocamente, suponhamos que D é um domínio de integridade que verifica as condições (1) e (2). Seja $a \in D \setminus D^*$ um elemento não nulo. Suponhamos por absurdo que a não é factorizável num produto de irredutíveis. Definamos por indução uma sucessão $\{a_n\}_{n\in\mathbb{N}}$ tal que

$$a_1 = a, a_{n+1} \mid a_n \quad \text{e} \quad a_n \nsim a_{n+1},$$

do seguinte modo:

Como a não é irredutível, $a = bc$ onde b e c não são unidades. É claro que b e c não podem ser ambos factorizáveis num produto de irredutíveis. Suponhamos (sem perda de generalidade) que b não o é; definimos $a_2 = b$. Claro que $a_2 \mid a_1$ e $a_1 \nsim a_2$. Como a_2 não é irredutível, podemos repetir o raciocínio e definir a_3 nas condições requeridas, e assim sucessivamente.

Os ideais principais gerados pelos a_n's satisfazem

$$\langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \subset \langle a_n\rangle \subset \cdots$$

contradizendo a condição (2) de toda a cadeia ascendente de ideias principais estabilizar. Concluímos assim que todos os elementos não nulos em $D \setminus D^*$ são factorizáveis em produtos de elementos irredutíveis.

Quanto à unicidade, suponhamos que

$$p_1p_2\cdots p_n = q_1q_2\cdots q_m$$

com, digamos, $n \leq m$. Como os p_i's e q_j's são irredutíveis, por (1) são primos. Mas

$$p_n \mid q_1q_2\cdots q_m$$

logo p_n é associado de algum q_j (que designamos por $q_{\pi(n)}$). Excluindo estes dois elementos, e repetindo o raciocínio, concluímos por exaustão que $n = m$ e $p_i \sim q_{\pi(i)}$ para alguma permutação $\pi \in S_n$. ∎

Este resultado justifica o uso indiferente nos DFU's da expressão "*factorização irredutível*" ou "*factorização prima*" para designar factorizações do tipo (2.1.1). É evidente que nas factorizações (2.1.1) podemos agrupar os elementos irredutíveis que sejam associados entre si e reescrever a factorização na forma

$$a = uq_1^{n_1} q_2^{n_2} \cdots q_k^{n_k} \tag{2.1.2}$$

onde $u \in D^*$, $q_1, q_2, \ldots, q_k$ são irredutíveis (=primos), não associados dois a dois, e $n_1, n_2, \ldots, n_k \in \mathbb{N}$.

Corolário 2.2. *Todo o domínio de ideais principais é um domínio de factorização única.*

Demonstração. Pelo teorema anterior bastará mostrar que qualquer DIP satisfaz as condições (1) e (2). A primeira é verdade pelo Corolário 1.4. Quanto à segunda, consideremos a cadeia

$$\langle d_1 \rangle \subseteq \langle d_2 \rangle \subseteq \cdots \subseteq \langle d_n \rangle \subseteq \cdots$$

É um exercício simples verificar que $\bigcup_{i=1}^{\infty} \langle d_i \rangle$ é um ideal, necessariamente principal, por hipótese, e portanto $\bigcup_{i=1}^{\infty} \langle d_i \rangle = \langle d \rangle$. Isto significa que existe k tal que $d \in \langle d_k \rangle$ e então, claramente, $\langle d_n \rangle = \langle d_k \rangle$ para qualquer $n \geq k$. ∎

O recíproco é falso, como o exemplo $\mathbb{Z}[x]$ mostra (não é um DIP pois o ideal $\langle 2, x \rangle$ não é principal, e é um DFU como veremos na secção seguinte).

Seja D um domínio de integridade e $a, b \in D$.

- Um elemento $d \in D$ diz-se um *máximo divisor comum* de a e b se $d \mid a$, $d \mid b$ e se, para qualquer divisor comum d' de a e b, $d' \mid d$.
- Um elemento $m \in D$ diz-se um *mínimo múltiplo comum* de a e b se $a \mid m$, $b \mid m$ e se, para qualquer múltiplo comum m' de a e b, $m \mid m'$.

Observe que se d é um máximo divisor comum de a e b então o conjunto dos máximos divisores comuns de a e b, que denotaremos por $\mathrm{mdc}(a, b)$, é o conjunto $dD^* = \{du \mid u \in D^*\}$. (Analogamente para os mínimos múltiplos comuns; neste caso, denotaremos o respectivo conjunto por $\mathrm{mmc}(a, b)$.)

Proposição 2.3. *Seja D um DFU e $a, b \in D$. Suponhamos que*

$$a = uq_1^{r_1} q_2^{r_2} \cdots q_k^{r_k} \quad e \quad b = vq_1^{s_1} q_2^{s_2} \cdots q_k^{s_k}$$

para certos primos $q_1, q_2, \ldots, q_k$, unidades u, v e $r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_k \in \mathbb{N}_0$. Então:

(1) $d = q_1^{\min(r_1,s_1)} \cdots q_k^{\min(r_k,s_k)} \in \operatorname{mdc}(a,b)$ *e* $m = q_1^{\max(r_1,s_1)} \cdots q_k^{\max(r_k,s_k)} \in \operatorname{mmc}(a,b)$.

(2) *Se $d' \in \operatorname{mdc}(a,b)$ e $m' \in \operatorname{mmc}(a,b)$, então existe $w \in D^*$ tal que $d'm' = wab$.*

(Note que é possível que, para algum primo q_i, tenhamos $r_i = 0$ ou $s_i = 0$; isso quer dizer que esse primo aparece efectivamente na factorização de a mas não na de b, ou vice-versa.)

Demonstração. (1) É claro que d é um divisor comum de a e b. Seja d' um outro divisor comum. É claro que não pode existir nenhum primo p que divida d' sem dividir a e b, e assim, é possível escrever

$$d' = wq_1^{t_1} \cdots q_k^{t_k}$$

com $w \in D^*$. Como $d' \mid a$ e $d' \mid b$, necessariamente $t_i \leq r_i, s_i$, e portanto

$$p_i^{t_i} \mid p_i^{\min(r_i,s_i)} \quad \text{e} \quad d' \mid d.$$

A prova para o mmc é análoga.

(2) Já sabemos que $d' = u'd$ e $m' = v'm$ para alguns $u', v' \in D^*$. Assim, $d'm' = u'v'dm$ e

$$\begin{aligned} dm &= q_1^{\min(r_1,s_1)+\max(r_1,s_1)} \cdots q_k^{\min(r_k,s_k)+\max(r_k,s_k)} \\ &= q_1^{r_1+s_1} \cdots q_k^{r_k+s_k} = u^{-1}v^{-1}ab. \end{aligned}$$

Basta tomar $w = u'v'u^{-1}v^{-1}$. ∎

Este último resultado generaliza o resultado básico dos inteiros que afirma que o máximo divisor comum é o produto dos factores primos comuns elevados ao menor expoente (e o mínimo múltiplo comum é o producto dos factores primos comuns e não comuns elevados ao maior expoente). Há muitas outras propriedades dos inteiros que se estendem aos DFU's e muitas vezes as próprias demonstrações estendem-se imediatamente ao caso geral. É o caso da prova da infinitude dos números primos em $\mathbb{Z}$ (atribuída a Euclides):

Proposição 2.4. *Num DFU que não é um corpo, existe um número infinito de elementos primos não associados.*

Demonstração. Seja D um DFU e suponhamos por absurdo que $p_1, \ldots, p_n$ era uma família completa de primos não associados de D (claro que esta família não é vazia pois D não é um corpo). Mas o elemento $a = p_1 \ldots p_n + 1$ não é divisível por nenhum dos primos naquela família (pois $p_i \mid a \Rightarrow p_i \mid a - p_1 p_2 \ldots p_n = 1$ e, como é óbvio, $p_i \mid 1$ sse $p_i \in D^*$, um absurdo). Consequentemente, a não admitiria nenhuma factorização em primos, o que é absurdo. ∎

3. Domínios de factorização única e polinómios

Quando estudámos polinómios em CORPOS E EQUAÇÕES ALGÉBRICAS provámos que se A é um corpo então $A[x]$ é um DFU. Vamos agora demonstrar que, mais geralmente, se A é um DFU também $A[x]$ o é. Começamos por determinar os irredutíveis em $A[x]$ de grau zero:

Proposição 3.1. *Seja D um domínio de integridade e $p(x) = a \in D$ um polinómio de grau 0. Então $p(x)$ é irredutível em $D[x]$ se e só se a for irredutível em D.*

Demonstração. Suponhamos que $p(x) = a$ é irredutível em $D[x]$ e $a = bc$ em D. Então b ou c pertencem a $D[x]^* = D^*$ o que mostra que a é irredutível em D.

Reciprocamente, se a for irredutível em D e $p(x) = a = q(x)r(x)$ em $D[x]$ então $\mathrm{gr}(q(x)) = \mathrm{gr}(r(x)) = 0$. Assim $q(x) = b$ e $r(x) = c$ com $b, c \in D$, $b, c \neq 0$. Como $a = bc$, pelo menos um dos elementos b ou c é uma unidade de D, ou seja, um dos polinómios $q(x)$ ou $r(x)$ é uma unidade de $D[x]$. ∎

Seja D um domínio de integridade e $p(x) \in D[x]$.

- $p(x)$ é um *polinómio primitivo* se $\mathrm{gr}(p(x)) \geq 1$ e os únicos divisores de $p(x)$ de grau zero forem unidades.
- Uma *factorização própria* de $p(x)$ é uma decomposição do tipo $p(x) = a(x)b(x)$ com $\mathrm{gr}(a(x)), \mathrm{gr}(b(x)) < \mathrm{gr}(p(x))$.

Por exemplo, $p(x) = 2x^2 + 2$ não é primitivo em $\mathbb{Z}[x]$ pois 2 divide $p(x)$ (mas em $\mathbb{Q}[x]$ já $p(x)$ é primitivo). Também não admite factorizações próprias em $\mathbb{Z}[x]$ (apesar de admitir a factorização $2(x^2 + 1)$).

Quanto aos irredutíveis não constantes:

Proposição 3.2. *Seja D um domínio de integridade. Se o grau de $p(x) \in D[x]$ for maior ou igual a 1, então $p(x)$ é irredutível em $D[x]$ se e só se for um polinómio primitivo que não admite factorizações próprias.*

Demonstração. Suponhamos que $p(x)$ é irredutível com $\mathrm{gr}(p(x)) \geq 1$. Por absurdo, se não fosse primitivo, podíamos factorizá-lo pondo em evidência um mdc dos seus coeficientes, e nessa factorização nenhum dos factores era uma unidade, uma contradição. Por outro lado, se admitisse uma factorização própria, é claro que também não poderia ser irredutível.

Reciprocamente, se $p(x)$ é primitivo sem factorizações próprias, claramente não é o polinómio nulo nem uma unidade. Se $p(x) = q(x)r(x)$ então, por hipótese, ou $q(x)$ ou $r(x)$ tem de ter grau zero. Suponhamos, sem perda de generalidade, que é $q(x)$. Portanto, $q(x) = a \in D$. Como $q(x) \mid p(x)$ e $p(x)$ é primitivo, necessariamente $q(x)$ é uma unidade. Logo $p(x)$ é irredutível. ∎

Teorema 3.3. *Seja D um DFU. Todo o elemento não nulo de $D[x] \setminus D[x]^*$ é um produto de elementos irredutíveis em $D[x]$. Estes são*

- *de grau zero, irredutíveis (=primos) em D, ou*
- *polinómios primitivos que não admitem factorizações próprias.*

Demonstração. Faremos a demonstração por indução sobre o grau n de $p(x)$:

Se $n = 0$, $p(x) = a \in D$ e portanto é claramente um produto de irredutíveis de D (por D ser um DFU).

Tomemos $p(x)$ de grau n e suponhamos, como hipótese de indução, que o resultado é válido para todos os polinómios de grau $< n$.

Se $p(x)$ admitir uma factorização própria então $p(x) = q(x)r(x)$ com $\mathrm{gr}(q(x)), \mathrm{gr}(r(x)) < n$ e, pela hipótese de indução, ambos são factorizáveis em polinómios dos dois tipos descritos. No caso em que $p(x)$ não admite factorizações próprias, se $p(x)$ for primitivo então é irredutível e está provado; se não for primitivo, podemos escrever $p(x) = aq(x)$ onde a é um mdc dos coeficientes de $p(x)$, não é unidade, e $q(x)$ é primitivo e também não tem factorizações próprias. Factorizando agora a em factores primos (usando o facto de D ser um DFU), e tendo em conta que $q(x)$ é irredutível por ser primitivo e não admitir factorizações próprias, chegamos à conclusão pretendida. ∎

Falta somente garantir a unicidade das factorizações para concluirmos que $D[x]$ é um DFU. Para isso vamos fazer o mesmo que se faz em $\mathbb{Z}$, em $C[x]$ ou na demonstração de que todo o DIP é DFU (Corolário 2.2): garantir que todos os irredutíveis mencionados no teorema anterior são primos em $D[x]$.

Proposição 3.4. *Seja D um DFU e p um elemento primo de D. Então $p(x) = p$ é primo em $D[x]$.*

Demonstração. Suponhamos que $p(x) \mid q(x)r(x)$ em $D[x]$ com

$$q(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \text{e} \quad r(x) = b_m x^m \cdots + b_1 x + b_0.$$

Queremos provar que $p(x) \mid q(x)$ ou $p(x) \mid r(x)$, isto é, p divide todos os coeficientes de $q(x)$ ou todos os coeficientes de $r(x)$. Suponhamos, por absurdo, que isso não acontece (ou seja, que p não divide um dos factores de $q(x)$ e um dos factores de $r(x)$). Seja s o maior índice tal que $p \nmid a_s$ e t o maior índice tal que $p \nmid b_t$. Então $p \mid a_i$ e $p \mid b_j$ para quaisquer $i > s$ e $j > t$. Como o coeficiente c_{s+t} de x^{s+t} no produto $q(x)r(x)$ é igual a

$$a_{s+t}b_0 \cdots + a_{s+1}b_{t-1} + a_s b_t + a_{s-1}b_{t+1} + \cdots + a_0 b_{s+t}$$

e $p \nmid a_s b_t$, então $p \nmid c_{s+t}$ (pois por definição de s e t, p divide todas as outras parcelas em c_{s+t}). Isto contradiz o facto de p, por hipótese, dividir todos os coeficientes do produto $q(x)r(x)$. ∎

Lema 3.5. *Seja D um DFU, K o seu corpo de fracções, $p(x), q(x) \in D[x]$ e suponhamos que $p(x)$ é primitivo. Se $p(x) \mid q(x)$ em $K[x]$ então $p(x) \mid q(x)$ em $D[x]$.*

Demonstração. Por hipótese, $q(x) = r(x)p(x)$ para algum

$$r(x) = \frac{a_n}{b_n}x^n + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0} \in K[x] \quad (a_i, b_i \in D,\ b_i \neq 0).$$

Seja c um elemento de $\text{mmc}(b_0, b_1, \ldots, b_n)$ e $f(x) = cr(x) \in D[x]$. Então $cq(x) = cr(x)p(x) = f(x)p(x)$. Se c é uma unidade então $r(x) \in D[x]$ e imediatamente $p(x) \mid q(x)$ em $D[x]$. Caso contrário, seja $d \in D$ um dos factores primos de c.

> (Cuidado: apesar de d dividir c em D, não é óbvio que $d|f(x)$ em $D[x]$;
> nem sequer sabemos se $c|f(x)$ em $D[x]$ pois $r(x) \in K[x]$.)

Como $d \mid f(x)p(x)$ então, pela proposição anterior, $d \mid f(x)$ ou $d \mid p(x)$. Mas $p(x)$ é primitivo, logo $d \nmid p(x)$ e necessariamente $d \mid f(x)$. Então $(1/d)f(x) \in D[x]$ e,

como $(1/d)f(x) = (c/d)r(x)$, c/d é múltiplo de todos os b_i $(i = 0, 1, \ldots, n)$, o que é impossível pois c/d divide estritamente c e $c \in \text{mmc}(b_0, b_1, \ldots, b_n)$. Portanto, c é mesmo uma unidade e $r(x) \in D[x]$. ∎

Lema 3.6. [Lema de Gauss] *Seja D um DFU e K o seu corpo de fracções. Se $p(x) \in D[x]$, $p(x) \neq 0$, com $p(x) = q(x)r(x)$, $q(x), r(x) \in K[x]$, então existe $a \in K$, $a \neq 0$, tal que*

$$q'(x) := aq(x) \in D[x], \quad r'(x) := (1/a)r(x) \in D[x] \quad e \quad p(x) = q'(x)r'(x).$$

(Isto implica que $p(x) \in D[x]$ não admite factorizações próprias em $D[x]$ sse é irredutível em $K[x]$.)

Demonstração. Seja c um múltiplo dos denominadores dos coeficientes de $q(x)$. É claro que $cq(x) \in D[x]$. Seja agora d um mdc dos coeficientes de $cq(x)$. Pondo-o em evidência obtemos $cq(x) = dq'(x)$, sendo $q'(x) \in D[x]$ primitivo. Então

$$p(x) = \frac{c}{d}\, q(x) \cdot \frac{d}{c}\, r(x) = q'(x)\frac{d}{c}\, r(x).$$

Bastará então tomar $a := c/d$. De facto: $aq(x) \in D[x]$; como $q'(x) \in D[x]$ é primitivo e divide $p(x)$ em $K[x]$, pelo lema anterior divide $p(x)$ em $D[x]$; assim, $(1/a)r(x) = p(x)/q'(x) \in D[x]$. ∎

Proposição 3.7. *Seja D um DFU e $p(x) \in D[x]$ um polinómio primitivo que não admite factorizações próprias. Então $p(x)$ é primo em $D[x]$.*

Demonstração. Suponhamos então que $p(x) \mid q(x)r(x)$, com $q(x), r(x) \in D[x]$, e seja K o corpo das fracções de D. Comecemos por verificar que $p(x)$ é irredutível em $K[x]$. Se não fosse, teríamos $p(x) = p_1(x)p_2(x)$, $p_1(x), p_2(x) \in K[x]$, ambos com grau ≥ 1. Então, pelo Lema de Gauss, teríamos $p(x) = p_1'(x)p_2'(x)$, com $p_1'(x), p_2'(x) \in D[x]$ de grau ≥ 1 ($\text{gr}(p_1'(x)) = \text{gr}(p_1(x))$ e $\text{gr}(p_2'(x)) = \text{gr}(p_2(x))$), o que é contraditório com a hipótese.

Portanto, $p(x)$ é irredutível em $K[x]$, e como $K[x]$ é um DFU, $p(x)$ é primo em $K[x]$ e portanto $p(x) \mid q(x)$ ou $p(x) \mid r(x)$ em $K[x]$. Como $p(x)$ é primitivo, o Lema 3.5 assegura-nos que $p(x) \mid q(x)$ ou $p(x) \mid r(x)$ em $D[x]$, e portanto, que $p(x)$ é primo em $D[x]$. ∎

Demonstrámos assim que todos os irredutíveis de $D[x]$ são primos e podemos assim obter finalmente o tão desejado teorema:

Teorema 3.8. *Seja D um DFU. Então $D[x]$ é um DFU.*

Demonstração. A factorização em irredutíveis existe pelo Teorema 3.3. Provámos em 3.4 e 3.7 que todos os irredutíveis nestas factorizações são primos. Isto é suficiente para garantirmos a unicidade das factorizações:

Sejam

$$p_1(x)\cdots p_n(x) = q_1(x)\cdots q_m(x)$$

duas factorizações em irredutíveis (que já sabemos serem primos) do mesmo elemento de $D[x]$. Vamos usar indução sobre n. Para $n = 1$ temos $p_1(x) = q_1(x)\cdots q_m(x)$. Como $p_1(x)$ é irredutível, não admite factorizações próprias, logo $m = 1 = n$ e $q_1(x) = p_1(x)$.

Supondo agora que o resultado vale para $n-1$, consideremos

$$p_1(x)\cdots p_n(x) = q_1(x)\cdots q_m(x)$$

duas factorizações do mesmo elemento em irredutíveis de $D[x]$. Como

$$p_1(x) \mid q_1(x)\cdots q_m(x)$$

e $p_1(x)$ é primo, existe i tal que $p_1(x) \mid q_i(x)$; reordenando os q_i's podemos supor $i = 1$. Como $q_1(x)$ é irredutível, $q_1(x) = u_1(x)p_1(x)$ onde $u_1(x)$ é uma unidade. Aplicando a lei do corte obtemos

$$p_2(x)\cdots p_n(x) = (u_1(x)q_2(x))\cdots q_m(x).$$

A decomposição da direita ainda é uma decomposição em irredutíveis e a da esquerda tem $n-1$ factores. Pela hipótese de indução, $m-1 = n-1$ (ou seja, $m = n$) e, após reordenação, $p_i(x) \sim q_i(x)$ $(i = 1, 2, \ldots, n)$. ∎

Em particular, $\mathbb{Z}[x]$ é um DFU, assim como $D[x, y] := D[x][y]$.

Terminamos com alguns critérios de irredutibilidade que permitem identificar alguns polinómios irredutíveis de $D[x]$ quando D é um DFU, e que generalizam resultados estudados em CORPOS E EQUAÇÕES ALGÉBRICAS.

Proposição 3.9. [Critério de Eisenstein] *Seja D um DFU e K o seu corpo de fracções. Se*

$$p(x) = a_n x^n + \cdots a_1 x + a_0 \in D[x]$$

e existe um primo $p \in D$ tal que

$$p \mid a_i \quad (i = 0, 1, \ldots, n-1), \quad p \nmid a_n \quad \text{e } p^2 \nmid a_0$$

então $p(x)$ é irredutível em $K[x]$.

(Equivalentemente, pelo Lema de Gauss, $p(x)$ não tem factorizações próprias em $D[x]$; portanto, será irredutível em $D[x]$ se for primitivo.)

Demonstração. Se, por absurdo, $p(x)$ não for irredutível em $K[x]$ então, pelo Lema de Gauss, admite uma factorização própria em $D[x]$

$$q(x)r(x) = (b_s x^s + \cdots b_1 x + b_0)(c_t x^t + \cdots c_1 x + c_0) \quad (s, t \geq 0).$$

Como $b_0 c_0 = a_0$ é divisível por p e não por p^2, um dos factores não é divisível por p (digamos b_0) e necessariamente $p \mid c_0$. Como $b_s c_t = a_n$ e $p \nmid a_n$, então $p \nmid c_t$. Seja k o menor índice tal que $p \nmid c_k$ (já vimos que $0 < k \leq t = n - s < n$). Como

$$a_k = b_0 c_k + b_1 c_{k-1} + \cdots$$

e $p \nmid b_0 c_k$ (mas divide todas as outras parcelas), então $p \nmid a_k$, uma contradição. ∎

O próximo resultado ajuda a encontrar as raízes em K de um polinómio com coeficientes em D.

Proposição 3.10. [das raízes fraccionárias] *Seja D um DFU, K o seu corpo de fracções e*

$$p(x) = a_n x^n + \cdots a_1 x + a_0 \in D[x].$$

Se $c/d \in K$ é uma raiz de $p(x)$ com $c, d \in D$ tais que $1 \in \mathrm{mdc}(c, d)$, então $c \mid a_0$ e $d \mid a_n$ em D. Em particular, se $c \in D$ é uma raiz de $p(x)$ então $c \mid a_0$.

Demonstração. Por hipótese

$$0 = p\left(\frac{c}{d}\right) = \frac{a_n c^n + a_{n-1} c^{n-1} d + \cdots + a_1 c d^{n-1} + a_0 d^n}{d^n}.$$

Portanto, $a_n c^n + a_{n-1} c^{n-1} d + \cdots + a_1 c d^{n-1} + a_0 d^n = 0$. Daqui podemos concluir que

$$a_n c^n + a_{n-1} c^{n-1} d + \cdots + a_1 c d^{n-1} = -a_0 d^n$$

e

$$-a_n c^n = a_{n-1} c^{n-1} d + \cdots + a_1 c d^{n-1} + a_0 d^n.$$

Da primeira identidade segue que $c \mid a_0 d^n$ e da segunda que $d \mid a_n c^n$. Como $1 \in \mathrm{mdc}(c, d)$, então $c \mid a_0$ e $d \mid a_n$ (Exercício 1.16). ∎

4. Domínios Euclidianos

As demonstrações de que $\mathbb{Z}$ e $C[x]$ (para qualquer corpo C) são DIP's (estudadas no ano passado) são formalmente muito parecidas e assentam no algoritmo da divisão. Isto sugere que possa haver uma classe genérica de anéis contida na classe dos DIP's onde aquelas demonstrações podem ser reformuladas, baseadas numa generalização do algoritmo da divisão. Essa classe é a classe dos domínios euclidianos.

Um domínio de integridade D diz-se um *domínio euclidiano* se for possível definir em D uma função $\delta\colon D \setminus \{0\} \to \mathbb{N}$ tal que

- para quaisquer $a, b \in D$ $(b \neq 0)$ existem $q, r \in D$ tais que $a = qb + r$ onde ou $r = 0$ ou $\delta(r) < \delta(b)$.

δ diz-se uma *função euclidiana* em D.

Os anéis $\mathbb{Z}$ com a função módulo e $C[x]$ (C corpo) com a função grau (em rigor, para que a função tenha valores positivos teremos que adicionar uma unidade ao grau) são domínios euclidianos. Observe que $\delta(a) = |a|$ não é uma função euclidiana em $\mathbb{Q}$. Qualquer corpo C é um domínio euclidiano, com função euclidiana δ definida por $\delta(x) = 1$ para todo o $x \in C \setminus \{0\}$.

Alguns autores acrescentam à definição de função euclidiana a condição

$$\delta(a) \leq \delta(ab) \text{ para quaisquer } a, b \in D \setminus \{0\} \tag{4.1.1}$$

mas isso é desnecessário pois as duas definições descrevem as mesmas classes de domínios. De facto:

Proposição 4.1. *Se D é um domínio euclidiano com função euclidiana δ então*

$$\widetilde{\delta}(a) = \min_{b \neq 0} \delta(ab)$$

define uma função euclidiana em D com as seguintes propriedades:

(1) $\widetilde{\delta}(a) \leq \widetilde{\delta}(ab)$ *para quaisquer a, b em $D \setminus \{0\}$.*

(2) $\widetilde{\delta}(1)$ *é o valor mínimo de δ em $D \setminus \{0\}$.*

(3) $\widetilde{\delta}(a) \leq \delta(a)$ *para qualquer a em $D \setminus \{0\}$.*

Demonstração. Começamos por demonstrar as propriedades (1)-(3) e deixamos para o fim a prova de que $\widetilde{\delta}$ é de facto uma função euclidiana em D.

(1) Sejam a, b em $D \setminus \{0\}$. Pela definição de $\widetilde{\delta}$, $\widetilde{\delta}(ab) = \delta(abc_0)$ para algum $c_0 \in D \setminus \{0\}$. Mas abc_0 é um múltiplo de a logo $\widetilde{\delta}(a) \leq \delta(abc_0) = \widetilde{\delta}(ab)$.

(2) Óbvio (da definição de $\widetilde{\delta}$).

(3) $\widetilde{\delta}(a) = \min_{b \neq 0} \delta(ab) \leq \delta(a \cdot 1) = \delta(a)$.

Mostremos agora que D admite um algoritmo da divisão relativamenta a $\widetilde{\delta}$. Sejam $a, b \in D$ com $b \neq 0$. Claro que $\widetilde{\delta}(b) = \delta(bc_0)$ para algum $c_0 \in D \setminus \{0\}$. Pelo algoritmo da divisão em (D, δ) para o par a, bc_0 existem $q, r \in D$ tais que $a = (bc_0)q_0 + r_0$ com $r_0 = 0$ ou $\delta(r_0) < \delta(bc_0)$. Basta agora tomar $q = c_0 q_0$ e $r = r_0$. De facto, $a = bq + r$, e $r = 0$ ou (usando a propriedade (3)) $\widetilde{\delta}(r) \leq \delta(r) < \delta(bc_0) = \widetilde{\delta}(b)$. ∎

Proposição 4.2. *Todo o domínio euclidiano é um DIP.*

Demonstração. Seja I um ideal arbitrário de um domínio euclidiano D. Se $I = \{0\}$, então $I = \langle 0 \rangle$ é um ideal principal. Podemos pois admitir que $I \neq \{0\}$. Nesse caso seja $N = \{\delta(a) \mid a \in I, a \neq 0\} \subseteq \mathbb{N}$. É claro que N é não vazio (pois $I \neq \{0\}$), pelo que tem um mínimo. Seja b um elemento de $I \setminus \{0\}$ onde esse mínimo é atingido. Provemos que $I = \langle b \rangle$. Como $b \in I$, é óbvio que $\langle b \rangle \subseteq I$. Por outro lado, se $a \in I$, usando a definição de domínio euclidiano, existem $q, r \in D$ tais que $a = qb + r$ com $r = 0$ ou $\delta(r) < \delta(b)$. Dado que I é um ideal, podemos concluir que $r = a - qb \in I$. Mas então $r = 0$ (se r fosse não nulo, teríamos $r \in I \setminus \{0\}$ com $\delta(r) < \delta(b)$, um absurdo). Assim, a é um múltiplo de b pelo que pertence ao ideal $\langle b \rangle$. ∎

Por outro lado, nem todo o DIP é um domínio euclidiano. O anel

$$\mathbb{Z}\Big[\frac{1 + i\sqrt{19}}{2}\Big]$$

é um exemplo.

Uma vez que o algoritmo de Euclides para a determinação do mdc em $\mathbb{Z}$ (ou em $C[x]$) depende apenas do algoritmo da divisão, é previsível que se possa generalizar a qualquer domínio euclidiano.

Proposição 4.3. [Algoritmo de Euclides] *Em qualquer domínio euclidiano D,* $\mathrm{mdc}(a, b) \neq \emptyset$ *para quaisquer $a, b \in D \setminus \{0\}$. Um elemento deste conjunto pode ser obtido dividindo a por b e, iterando, dividindo sucessivamente os sucessivos divisores pelos sucessivos restos, até que o resto seja zero. O último resto não nulo r_t será esse elemento (e, consequentemente,* $\mathrm{mdc}(a, b) = \{u\, r_t \mid u \in D^*\}$*).*

Demonstração. Como D é um DFU, $\text{mdc}(a,b) \neq \emptyset$ pela Proposição 2.3. Quanto ao algoritmo de cálculo de um elemento desse conjunto, ele termina pois cada divisão sucessiva origina um novo resto r_{t+1} com $\delta(r_{t+1}) < \delta(r_t)$ e estes valores são sempre não negativos. Resta-nos mostrar que o elemento encontrado pelo algoritmo é de facto um mdc de a e b. Faremos a demonstração por indução sobre $\delta(b)$.

Se $\delta(b) = 1$ então $b \mid a$ (pois $a = q_1 b + r_1$ com $r_1 = 0$ ou $\delta(r_1) < \delta(b) = 1$; como a última condição é impossível, então $r_1 = 0$). Portanto $a = q_1 b$ e é óbvio que $b \in \text{mdc}(a,b)$.

Suponhamos que o algoritmo funciona para qualquer b tal que $\delta(b) < n$. Consideremos então b com $\delta(b) = n$. Então existem $q_1, r_1 \in D$ tais que

$$a = q_1 b + r_1 \qquad (*)$$

com $r_1 = 0$ ou $\delta(r_1) < \delta(b) = n$. Se $r_1 = 0$ então $a = q_1 b$ e é óbvio que $b \in \text{mdc}(a,b)$. Caso contrário, podemos usar a hipótese de indução e ter a garantia de que usando o algoritmo para b e r_1 encontramos no final um elemento d em $\text{mdc}(b, r_1)$. Só precisamos de garantir que $d \in \text{mdc}(a,b)$. Em primeiro lugar, como $d \mid r_1$ e $d \mid b$ então, usando $(*)$, $d \mid a$. Por outro lado, se $c \mid a$ e $c \mid b$ então, novamente por $(*)$, $c \mid r_1$ e portanto $c \mid d$. ∎

Resumindo:

ALGORITMO DE EUCLIDES

Sejam $a, b \in D$, com $b \neq 0$.

- Se $b \mid a$, então $b \in \text{mdc}\,(a,b)$.
- Se $b \nmid a$, usamos a definição de domínio euclidiano repetidamente, do seguinte modo:

$$\begin{array}{ll} a = q_1 b + r_1 & 0 < \delta(r_1) < \delta(b) \\ b = q_2 r_1 + r_2 & 0 < \delta(r_2) < \delta(r_1) \\ r_1 = q_3 r_2 + r_3 & 0 < \delta(r_3) < \delta(r_2) \\ \quad\vdots & \quad\vdots \\ r_{t-2} = q_t r_{t-1} + r_t & 0 < \delta(r_t) < \delta(r_{t-1}) \\ r_{t-1} = q_{t+1} r_t. & \end{array}$$

  Como $\delta(b)$ é finito, o processo terá que parar ao cabo de um número finito de passos. Então $r_t \in \text{mdc}\,(a,b)$.

Exemplo. Calculemos $\mathrm{mdc}(114, 87)$ (em $\mathbb{Z}$) pelo método de Euclides das divisões sucessivas e apresentemos uma expressão desse mdc como combinação linear inteira $p \times 114 + q \times 87$ de 114 e 87 (ver Exercício 1.21):

$$114 = 1 \times 87 + 27, \quad 87 = 3 \times 27 + 6, \quad 27 = 4 \times 6 + \boxed{3}, \quad 6 = 2 \times \boxed{3}.$$

Portanto, $\mathrm{mdc}(114, 87) = \{3, -3\}$.

A partir da penúltima divisão, substituindo sucessivamente, obtemos:

$$\begin{aligned} 3 &= 27 - 4 \times 6 \\ &= 27 - 4 \times (87 - 3 \times 27) \\ &= 13 \times 27 - 4 \times 87 \\ &= 13 \times (114 - 1 \times 87) - 4 \times 87 \\ &= 13 \times 114 - 17 \times 87. \end{aligned}$$

Portanto, $p = 13$ e $q = -17$.

Alternativamente, podemos calcular p e q sem fazer as substituições sucessivas, observando que podemos representar uma divisão $a = qb + r$ na forma matricial

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r \end{pmatrix}.$$

Assim, as sucessivas divisões no método de Euclides dão-nos

$$\begin{aligned} \begin{pmatrix} 114 \\ 87 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 87 \\ 27 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 27 \\ 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 6 \\ 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 0 \end{pmatrix}. \end{aligned}$$

Mas

$$\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix},$$

como é fácil de verificar. Logo, fazendo o produto dos inversos pela ordem inversa, obtemos

$$\begin{aligned} \begin{pmatrix} 3 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 114 \\ 87 \end{pmatrix} \\ &= \begin{pmatrix} 13 & -17 \\ -29 & 38 \end{pmatrix} \begin{pmatrix} 114 \\ 87 \end{pmatrix}, \end{aligned}$$

o que mostra que $3 = 13 \times 114 - 17 \times 87$.

Proposição 4.4. *O anel dos inteiros de Gauss, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, é um domínio euclidiano, com*

$$\delta(a + bi) := |a + bi|^2 = a^2 + b^2.$$

Demonstração. Teremos que mostrar que para quaisquer $a+bi, c+di \in \mathbb{Z}[i]$ com $c + di \neq 0$, existem $q_1 + q_2 i$ e $r_1 + r_2 i$ em $\mathbb{Z}[i]$ tais que

$$a+bi = (c+di)(q_1+q_2i)+(r_1+r_2i) \quad \text{onde } r_1 = r_2 = 0 \text{ ou } r_1^2+r_2^2 < c^2+d^2. \quad (4.4.1)$$

Se tal for possível, teremos necessariamente (em $\mathbb{C}$) o seguinte:

$$\begin{aligned} r_1 + r_2 i &= (a + bi) - (c + di)(q_1 + q_2 i) \\ &= (c + di)\Big[\frac{a + bi}{c + di} - (q_1 + q_2 i)\Big]. \end{aligned}$$

Denotando $\frac{a+bi}{c+di} \in \mathbb{C}$ por $u + vi$ (note que $u, v \in \mathbb{Q}$) é claro que no caso em que $u, v \in \mathbb{Z}$ basta fazer $q_1 = u, q_2 = v$ e $r_1 + r_2 i = 0$. Caso contrário, como

$$\begin{aligned} r_1 + r_2 i &= (c + di)\Big[(u + vi) - (q_1 + q_2 i)\Big] \\ &= (c + di)\Big[(u - q_1) + (v - q_2)i\Big] \\ &= [c(u - q_1) - d(v - q_2)] + [c(v - q_2) + d(u - q_1)]i, \end{aligned}$$

então

$$\begin{aligned} r_1^2 + r_2^2 &= [c(u - q_1) - d(v - q_2)]^2 + [c(v - q_2) + d(u - q_1)]^2 \\ &= (c^2 + d^2)[(u - q_1)^2 + (v - q_2)^2], \end{aligned}$$

donde

$$r_1^2 + r_2^2 < c^2 + d^2 \Leftrightarrow \boxed{(u - q_1)^2 + (v - q_2)^2 < 1}$$

o que mostra que neste caso para satisfazer (4.4.1) basta encontrar inteiros q_1 e q_2 tais que $(u - q_1)^2 + (v - q_2)^2 < 1$. Será isto possível? Claro que sim: basta tomar para q_1 o inteiro mais próximo de u e para q_2 o inteiro mais próximo de v (de facto, nesse caso $(u - q_1)^2 + (v - q_2)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$).

(Repare que esta não é a única solução, o que mostra que esta divisão euclidiana em $\mathbb{Z}[i]$ não tem necessariamente quociente e resto únicos.)

Depois de calculados q_1 e q_2 basta tomar $r_1 + r_2 i = (a + bi) - (c + di)(q_1 + q_2 i)$.

■

Resumindo:

ALGORITMO DA DIVISÃO em $\mathbb{Z}[i]$

Sejam $a+bi, c+di \in \mathbb{Z}[i]$, com $c+di \neq 0$.

- Calcule-se $u+vi = \dfrac{a+bi}{c+di}$ em $\mathbb{C}$.
- Se $u, v \in \mathbb{Z}$, faça-se $q_1 = u, q_2 = v$ e $r_1 = r_2 = 0$.
- Caso contrário, tome-se para q_1 um inteiro tal que

$$(u-q_1)^2 \leq \frac{1}{4}$$

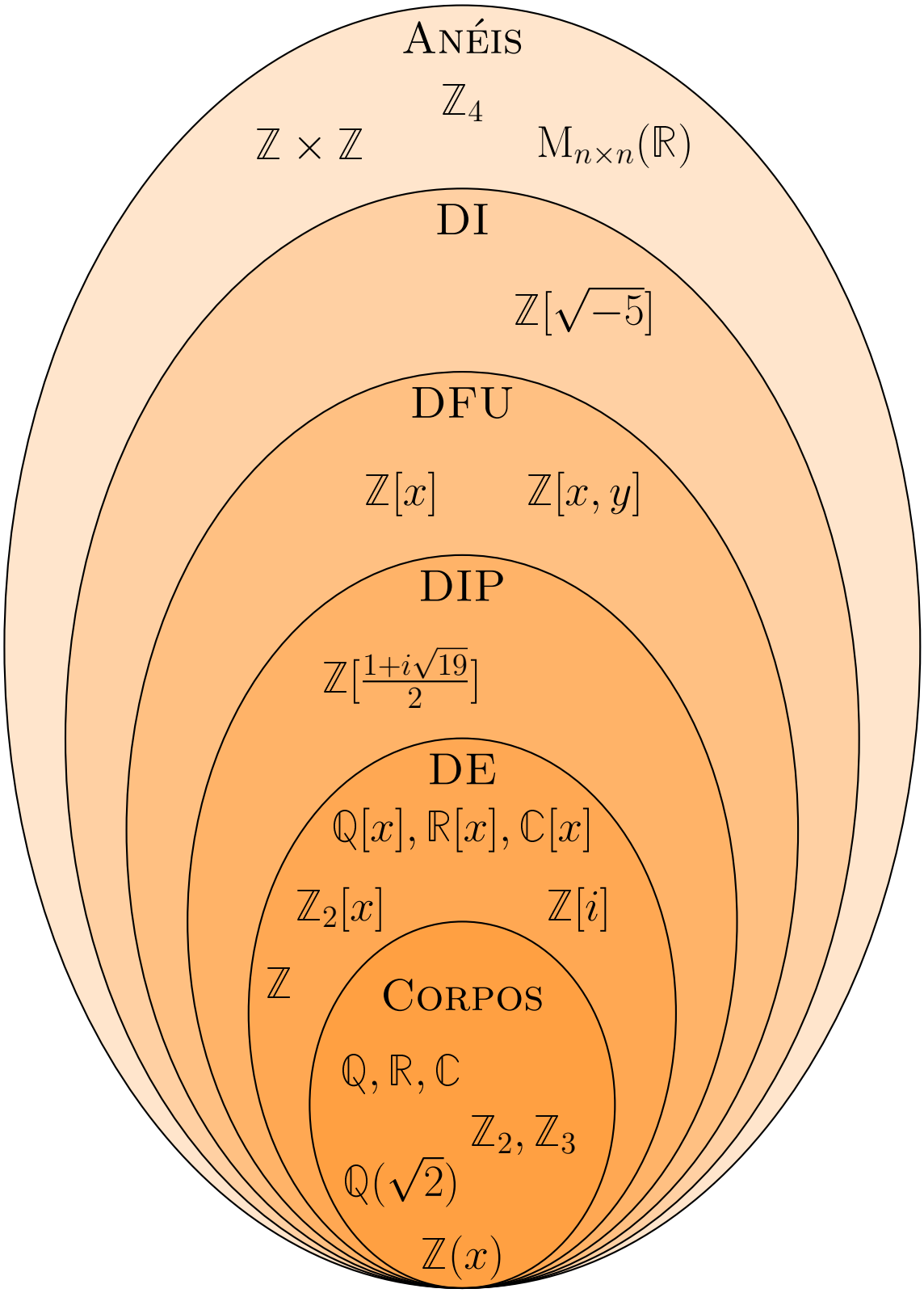
e para q_2 um inteiro tal que

$$(v-q_2)^2 \leq \frac{1}{4}.$$

O resto $r_1 + r_2 i$ é calculado pela fórmula

$$r_1 + r_2 i = (a+bi) - (c+di)(q_1 + q_2 i).$$

A figura seguinte resume as relações de inclusão entre as diversas classes de domínios de integridade estudadas neste capítulo.


ANÉIS
$\mathbb{Z}_4$
$\mathbb{Z} \times \mathbb{Z}$
$\mathrm{M}_{n\times n}(\mathbb{R})$
DI
$\mathbb{Z}[\sqrt{-5}]$
DFU
$\mathbb{Z}[x]$
$\mathbb{Z}[x, y]$
DIP
$\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$
DE
$\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$
$\mathbb{Z}_2[x]$
$\mathbb{Z}[i]$
$\mathbb{Z}$
CORPOS
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$
$\mathbb{Z}_2, \mathbb{Z}_3$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Z}(x)$

5. Teoremas do isomorfismo para anéis

Terminamos este primeiro capítulo com um tema diferente: vamos generalizar os teoremas de isomorfismos, estudados em Grupos, aos anéis, resultados de que necessitaremos ao longo do curso. É claro que tendo as demonstrações para os grupos na mão, estas são facilmente adaptáveis aos anéis (bastando verificar as propriedades relativamente à segunda operação dos anéis em causa); aqui (com o propósito de que o texto seja auto-contido) apresentaremos as demonstrações completas. Dado um homomorfismo de anéis $\phi\colon A \to B$, denotaremos o seu *núcleo* $\{a \in A \mid \phi(a) = 0\}$, que é um ideal de A, por $N(\phi)$.

Sejam A e B anéis e I um ideal de A. Investiguemos a relação entre os homomorfismos $\widetilde{\phi}\colon A/I \to B$ e os homomorfismos $\phi\colon A \to B$. Uma vez que a aplicação quociente usual

$$\begin{array}{rccc} \pi\colon & A & \to & A/I \\ & a & \mapsto & a+I \end{array}$$

é um homomorfismo de anéis, não é difícil provar o seguinte:

Lema 5.1. (1) *Seja $\widetilde{\phi}\colon A/I \to B$ um homomorfismo de anéis. Então a composição $\phi = \widetilde{\phi} \circ \pi\colon A \to B$ é um homomorfismo de anéis tal que $N(\phi) \supseteq I$.*

(2) *Reciprocamente, seja $\phi\colon A \to B$ um homomorfismo de anéis tal que $N(\phi) \supseteq I$. Então existe um (único) homomorfismo $\widetilde{\phi}\colon A/I \to B$ tal que $\widetilde{\phi} \circ \pi = \phi$.*

Demonstração. (1) É claro que ϕ é um homomorfismo de anéis pois é a composição de dois homomorfismos de anéis. Além disso, $N(\phi) \supseteq I$: se $a \in I$ então $a + I = I$ é o zero de A/I, e portanto $\phi(a) = \widetilde{\phi}(\pi(a)) = \widetilde{\phi}(a + I)$ é o zero de B.

(2) Se $\phi\colon A \to B$ é um homomorfismo de anéis tal que $N(\phi) \supseteq I$, então

$$b + I = a + I \Leftrightarrow b - a \in I \Rightarrow b - a \in N(\phi) \Leftrightarrow \phi(b) = \phi(a).$$

Isto garante que a correspondência $a + I \mapsto \phi(a)$ é independente da escolha do representante de $a + I$, ou seja, define uma aplicação $\widetilde{\phi}\colon A/I \to B$. É evidente que $\widetilde{\phi}$ é um homomorfismo, pois

$$\widetilde{\phi}(a+I) + \widetilde{\phi}(b+I) = \phi(a) + \phi(b) = \phi(a+b) = \widetilde{\phi}(a+b+I) = \widetilde{\phi}((a+I) + (b+I))$$

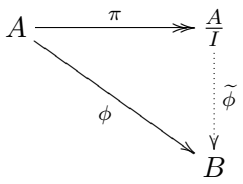
e

$$\widetilde{\phi}(a+I) \cdot \widetilde{\phi}(b+I) = \phi(a) \cdot \phi(b) = \phi(a \cdot b) = \widetilde{\phi}(ab+I) = \widetilde{\phi}((a+I) \cdot (b+I)).$$

■

Portanto, qualquer homomorfismo $\widetilde{\phi}\colon A/I \to B$ é da forma $\widetilde{\phi}(a+I) = \phi(a)$ para algum homomorfismo $\phi\colon A \to B$ definido no anel original A.

É habitual descrever a conclusão em (2), de modo mais abreviado, por um diagrama comutativo (onde a seta a ponteado serve para indicar que desejamos afirmar a existência do homomorfismo correspondente):



Observe ainda que o Lema nos diz com exactidão quais os homomorfismos $\phi\colon A \to B$ para os quais existe algum homomorfismo $\widetilde{\phi}\colon A/I \to B$ dado por $\widetilde{\phi}(a+I) = \phi(a)$ (ou seja, tal que $\widetilde{\phi} \circ \pi = \phi$):

Proposição 5.2. *Sejam A e B anéis, I um ideal de A e $\pi\colon A \to A/I$ o homomorfismo quociente usual.*

(1) *Os homomorfismos de anéis $\widetilde{\phi}\colon A/I \to B$ são as funções dadas por $\widetilde{\phi}(\pi(a)) = \phi(a)$, onde $\phi\colon A \to B$ é um qualquer homomorfismo de anéis com núcleo $N(\phi) \supseteq I$.*

(2) *Sendo $\phi\colon A \to B$ um homomorfismo de anéis com núcleo $N(\phi) \supseteq I$ e $\widetilde{\phi}\colon A/I \to B$ o correspondente homomorfismo de anéis dado por $\widetilde{\phi}(\pi(x)) = \phi(x)$, então*

$$N(\widetilde{\phi}) = \frac{N(\phi)}{I} = \pi(N(\phi))$$

e, em particular, $\widetilde{\phi}$ é injectiva se e só se $N(\phi) = I$.

Demonstração. (1) Imediato pelo Lema.

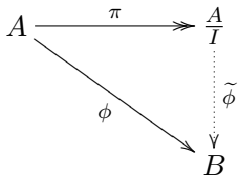
(2) Determinemos o núcleo de $\widetilde{\phi}$:

$$\begin{aligned} N(\widetilde{\phi}) &= \{a+I \mid \widetilde{\phi}(a+I) = 0\} = \{a+I \mid \phi(a) = 0\} \\ &= \{a+I \mid a \in N(\phi)\} = \pi(N(\phi)) = N(\phi)/I. \end{aligned}$$

É então evidente que $\widetilde{\phi}$ é injectiva se e só se $N(\widetilde{\phi}) = \{I\}$, o que ocorre se e só se $N(\phi) = I$. ∎

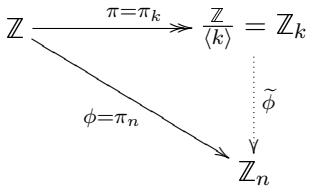
Portanto, para cada homomorfismo $\phi\colon A \to B$ tal que $N(\phi) \supseteq I$, existe um homomorfismo $\widetilde{\phi}$ (com núcleo igual a $N(\phi)/I$) que torna o seguinte diagrama

comutativo:



(5.2.1)

Exemplos. (1) Tomemos $A = \mathbb{Z}$, $B = \mathbb{Z}_n$ e $I = \langle k \rangle$. A aplicação $\phi = \pi_n \colon \mathbb{Z} \to \mathbb{Z}_n$ dada por $\phi(a) = a \,(\mathrm{mod}\, n)$ é um homomorfismo de anéis. Então, se $n \mid k$, é evidente que $N(\phi) \supseteq I$, pelo que a proposição anterior produz o diagrama comutativo

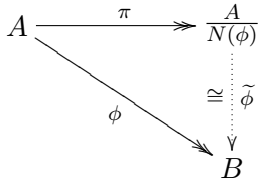


(2) Tomemos $A = \mathbb{Q}[x]$, $B = \mathbb{Q}$ e $\phi \colon \mathbb{Q}[x] \to \mathbb{Q}$ definido por $\phi(p(x)) = p(1)$. O núcleo de ϕ é (de acordo com o Teorema do Resto), $\langle x - 1 \rangle$. Sendo $I = \langle m(x) \rangle$ o ideal de $\mathbb{Q}[x]$ gerado pelo polinómio $m(x)$, a proposição anterior garante a existência de um homomorfismo de anéis $\widetilde{\phi} \colon \mathbb{Q}[x]/I \to \mathbb{Q}$, dado por $\widetilde{\phi}(p(x) + I) = p(1)$, desde que $(x - 1) \mid m(x)$ (isto é, $p(1) = 0$).

Quando o homomorfismo ϕ é sobrejectivo e I é o núcleo de ϕ, a proposição anterior reduz-se ao chamado Primeiro Teorema do Isomorfismo, um resultado central da Teoria dos Anéis (tal como a sua versão para grupos é um resultado central da Teoria dos Grupos), que usaremos repetidamente ao longo do curso:

Teorema 5.3. [Primeiro Teorema do Isomorfismo] *Seja $\phi \colon A \to B$ um homomorfismo sobrejectivo de anéis. Os anéis $A/N(\phi)$ e B são isomorfos. Em particular, existe um isomorfismo de anéis $\widetilde{\phi}$ tal que $\widetilde{\phi} \circ \pi = \phi$.* ∎

Este teorema exprime, em particular, a comutatividade do seguinte diagrama (onde a seta a ponteado significa a existência do homomorfismo correspondente, que é neste caso um *isomorfismo*):



(5.3.1)

Note que, mesmo quando ϕ não é sobrejectivo, o teorema se aplica automaticamente à imagem $B' = \phi(A)$.

Exemplos. (1) Supondo n e m naturais primos entre si, podemos mostrar que os anéis $\mathbb{Z}_{nm}$ e $\mathbb{Z}_n \oplus \mathbb{Z}_m$ são isomorfos. Para isso, definimos $\phi\colon \mathbb{Z} \to \mathbb{Z}_n \oplus \mathbb{Z}_m$ da forma "óbvia", tomando $\phi(a) = (\pi_n(a), \pi_m(a))$. O cálculo do núcleo de ϕ é simples:

$$a \in N(\phi) \Leftrightarrow \pi_n(a) = 0 \text{ e } \pi_m(a) = 0 \Leftrightarrow n \mid a \text{ e } m \mid a \Leftrightarrow nm \mid a.$$

Portanto, $N(\phi) = \langle nm \rangle$. Observe ainda que, como $\text{mdc}(n, m) = 1$, ϕ é sobrejectiva. Imediatamente, pelo Primeiro Teorema do Isomorfismo, obtemos um isomorfismo $\widetilde{\phi}\colon \mathbb{Z}/\langle nm \rangle = \mathbb{Z}_{nm} \to \mathbb{Z}_n \oplus \mathbb{Z}_m$, dado por $\widetilde{\phi}(\pi_{nm}(x)) = (\pi_n(x), \pi_m(x))$. Em conclusão, $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ sempre que $\text{mdc}(n, m) = 1$.

(2) Seja $\alpha \in \mathbb{C}$ um elemento algébrico sobre $\mathbb{Q}$, $\alpha \notin \mathbb{Q}$, e $m(x)$ o seu polinómio mínimo. Recorde que a aplicação $\phi\colon \mathbb{Q}[x] \to \mathbb{C}$ definida por $\phi(p(x)) = p(\alpha)$ é um homomorfismo de anéis com núcleo $N(\phi) = \langle m(x) \rangle$. Além disso, $\phi(\mathbb{Q}[x]) = \mathbb{Q}[\alpha]$. Logo, o Primeiro Teorema do Isomorfismo diz-nos que

$$\frac{\mathbb{Q}[x]}{\langle m(x) \rangle} \cong \mathbb{Q}[\alpha].$$

Por outro lado, $m(x)$ é irredutível, pelo que $\mathbb{Q}[x]/\langle m(x) \rangle$ é um corpo, e portanto

$$\frac{\mathbb{Q}[x]}{\langle m(x) \rangle} \cong \mathbb{Q}[\alpha] = \mathbb{Q}(\alpha).$$

O Primeiro Teorema do Isomorfismo pode ser aplicado para esclarecer a natureza do anel $B + I/I$ quando I e B são subanéis de A, sendo I um ideal.

Teorema 5.4. [Segundo Teorema do Isomorfismo] *Seja A um anel, I um ideal de A e B um subanel de A. Então $B + I$ é um subanel de A, I é um ideal de $B + I$, $B \cap I$ é um ideal de B e existe um isomorfismo de anéis*

$$\frac{B + I}{I} \cong \frac{B}{B \cap I}.$$

Demonstração. É fácil de verificar que se I é um ideal de A e B um subanel de A, então $B + I$ é igualmente um subanel de A, I é um ideal de $B + I$ e $B \cap I$ é um ideal de B (verifique!).

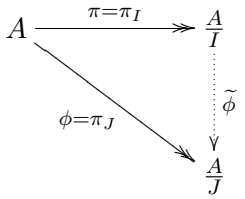
Consideremos a aplicação canónica $\pi\colon A \to A/I$ restrita a B, ou seja, a função $\phi\colon B \to A/I$ definida por $\phi(b) = \pi(b) = b + I$ para qualquer $b \in B$. É um exercício simples verificar que ϕ é um homomorfismo de anéis com núcleo $N(\phi) = \{b \in B \mid b \in I\} = B \cap I$. Por outro lado, $\phi(B)$ é um subanel de A/I, ou seja, $\phi(B) = K/I$ onde K é um subanel de A que contém necessariamente B e I, donde $B + I \subseteq K$. Mas para qualquer $k \in K$ existe $b \in B$ tal que $\phi(b) = k + I$, isto é, $b + I = k + I$;

portanto, existe $x := k-b \in I$ tal que $k = b+x$. Logo $K = B+I$. Então, aplicando o Teorema do Isomorfismo ao homomorfismo sobrejectivo $\phi\colon B \to \phi(B) = K/I$, obtemos um isomorfismo

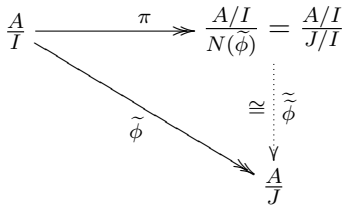
$$\frac{B}{N(\phi)} = \frac{B}{B \cap I} \xrightarrow{\ \widetilde{\phi}\ } \frac{K}{I} = \frac{B+I}{I}$$

■

Finalmente, podemos usar ainda o Primeiro Teorema do Isomorfismo para estudar os anéis quociente formados a partir de anéis quociente de A ("quocientes de quocientes de anéis"). Com efeito, seja A um anel e I e J ideais de A com $I \subseteq J$. Sejam $\pi_J\colon A \to A/J$ e $\pi_I\colon A \to A/I$ os respectivos homomorfismos quociente. Note que $N(\pi_J) = J \supseteq I = N(\pi_I)$. Pelo Lema 5.1(2), dados $\phi = \pi_J$ (que é sobrejectivo) e $\pi = \pi_I$, existe um homomorfismo $\widetilde{\phi}\colon A/I \to A/J$ tal que o seguinte diagrama é comutativo:



O homomorfismo $\widetilde{\phi}$ é claramente sobrejectivo (porque π_J o é). Além disso, pela Proposição 5.2, sabemos que $N(\widetilde{\phi}) = J/I$. Aplicando o Primeiro Teorema do Isomorfismo ao homomorfismo $\widetilde{\phi}$, obtemos imediatamente um isomomorfismo $\widetilde{\widetilde{\phi}}$ tal que o diagrama



comuta. Portanto:

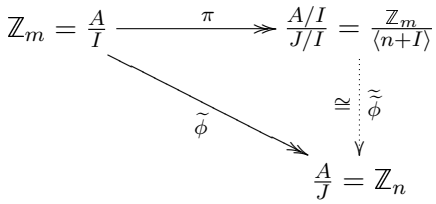
Teorema 5.5. [Terceiro Teorema do Isomorfismo] *Seja A um anel, I e J ideais de A com $I \subseteq J$. Então I é um ideal de J, J/I é um ideal de A/I e temos o isomorfismo de anéis*

$$\frac{A/I}{J/I} \cong \frac{A}{J}.$$

■

(Isto mostra que os quocientes de quocientes de A são isomorfos a quocientes de A.)

Exemplo. Com $A = \mathbb{Z}$, suponhamos que $n \mid m$. Consideremos $I = \langle m \rangle$ e $J = \langle n \rangle$. Neste caso $A/I = \mathbb{Z}_m$, $A/J = \mathbb{Z}_n$ e $J/I = \langle n + I \rangle \subseteq \mathbb{Z}_m$. Então, pelo Terceiro Teorema do Isomorfismo, $\mathbb{Z}_m / \langle n + I \rangle \cong \mathbb{Z}_n$:



Em particular, os anéis quociente formados a partir dos anéis $\mathbb{Z}_m$ são anéis $\mathbb{Z}_n$.

Exercícios

1.1. Mostre que num domínio de integridade D:

(a) $\langle a\rangle \subseteq \langle b\rangle$ sse $b \mid a$.

(b) $\langle a\rangle = \langle b\rangle$ sse $a \sim b$.

(c) $\langle a\rangle = D$ sse $a \in D^*$.

(d) $D[x]^* = D^*$.

1.2. Mostre que num domínio de integridade D:

(a) $u \in D^*$ sse $u \mid d$ para todo o $d \in D$.

(b) Qualquer associado de uma unidade é uma unidade.

(c) Qualquer associado de um elemento irredutível é irredutível.

1.3. Demonstre a Proposição 1.2.

1.4. Verifique que um anel (comutativo com identidade) A é um domínio de integridade se e só $ab \in \langle 0\rangle \Rightarrow a \in \langle 0\rangle$ ou $b \in \langle 0\rangle$.

1.5. (a) Determine as unidades do *anel dos inteiros de Gauss* $\mathbb{Z}[i]$.

(b) Verifique que $1 \pm i$ são elementos irredutíveis de $\mathbb{Z}[i]$. Observe que $2 \in \mathbb{Z}[i]$ não é irredutível em $\mathbb{Z}[i]$ apesar de o ser em $\mathbb{Z}$.

1.6. Seja D um domínio de integridade onde é possível definir uma função $N\colon D \to \mathbb{N}_0$ (chamada *norma*) com as seguintes propriedades:

(1) $N(a) = 0$ sse $a = 0$.

(2) $N(a) = 1$ sse $a \in D^*$.

(3) $N(ab) = N(a)N(b)$ para quaisquer $a, b \in D \setminus \{0\}$.

Mostre que todo o elemento de $D \setminus D^*$ não nulo admite uma factorização como produto de elementos irredutíveis.

1.7. Considere o anel $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ onde $d \neq 0, 1$ é *livre de quadrados*, isto é, para qualquer primo $p \in \mathbb{Z}$, $p^2 \nmid d$.

(a) Mostre que $a + b\sqrt{d} = a' + b'\sqrt{d}$ se e só se $a = a'$ e $b = b'$.

(b) Prove que a aplicação $N\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{N}_0$ definida por $N(a + b\sqrt{d}) = |a^2 - db^2|$ é uma norma (recorde o exercício anterior).

(c) Conclua que em $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[i\sqrt{5}]$ os elementos 3 e $2 \pm \sqrt{-5}$ são irredutíveis.

(d) Mostre que em $\mathbb{Z}[\sqrt{-5}]$ todos os elementos admitem factorizações em irredutíveis, mas a decomposição não é, em geral, única.

1.8. Seja C um corpo. Verdadeiro ou falso?

(a) Se $a, b, c \in C^*$ então $a \in \text{mdc}(b, c)$.

(b) C é um DFU.

1.9. Seja D um DIP e $a, b \in D$. Prove que:

(a) $d \in \text{mdc}(a, b)$ se e só se $\langle d\rangle = \langle a, b\rangle = \langle a\rangle + \langle b\rangle$.

(b) $m \in \text{mmc}(a, b)$ se e só se $\langle m\rangle = \langle a\rangle \cap \langle b\rangle$.

(c) Se $d \in \text{mdc}(a, b)$ então existem $p, q \in D$ tais que $d = pa + qb$ (*Relação de Bézout*).

1.10. Seja D um domínio de integridade e $a_1, \ldots, a_n \in D$.

(a) Defina $\text{mdc}(a_1, \ldots, a_n)$ e $\text{mmc}(a_1, \ldots, a_n)$.

(b) Mostre que se $d' \in \text{mdc}(a_1, \ldots, a_{n-1})$ e $d \in \text{mdc}(d', a_n)$ então $d \in \text{mdc}(a_1, \ldots, a_n)$.

(c) Enuncie e demonstre o resultado análogo para mmc's.

1.11. Seja A um anel comutativo com identidade e seja $\mathcal{S}$ o conjunto das sequências infinitas $(a_n)_{n\in\mathbb{N}_0}$ de elementos de A. Defina $+$ e $\cdot$ em $\mathcal{S}$ por

$$(a_n)_{n\in\mathbb{N}_0} + (b_n)_{n\in\mathbb{N}_0} = (a_n + b_n)_{n\in\mathbb{N}_0} \quad \text{e} \quad (a_n)_{n\in\mathbb{N}_0} \cdot (b_n)_{n\in\mathbb{N}_0} = (c_n)_{n\in\mathbb{N}_0}$$

onde $c_n = a_0b_n + a_1b_{n-1} + \cdots + a_nb_0$ para $n = 0, 1, 2, \ldots$. Mostre que:

(a) $(\mathcal{S}, +, \cdot)$ é um anel comutativo com identidade.

(b) $(a_n)_{n\in\mathbb{N}_0} \in \mathcal{S}^*$ se e só se $a_0 \in A^*$.

(c) Se A é um corpo então $\mathcal{S}$ é um domínio de ideais principais.

1.12. Seja D um DFU e C o seu corpo de fracções. Mostre que é possível escrever qualquer elemento de C como a/b com $a, b \in D$ elementos *coprimos* (ou *primos entre si*, isto é, tais que $\text{mdc}(a, b) = D^*$).

1.13. Seja $A = \{p(x) \in \mathbb{R}[x] \colon p(x) \text{ não tem monómio de grau } 1\}$.

(a) Verifique que A é um anel (subanel de $\mathbb{R}[x]$).

(b) Verifique que todos os polinómios de grau 2 ou 3 são irredutíveis em A.

(c) Verifique que os polinómios $x^2(x^2 + x)^2$ e $x^3(x^2 + x)$ não têm mdc em A. Que pode dizer do mmc?

(d) Prove que todo o elemento de A se factoriza como produto de irredutíveis, mas esta factorização nem sempre é única.

(**Observação:** este exercício mostra que um subanel de um DFU não é necessariamente um DFU.)

1.14. Seja D um domínio de integridade.

(a) Verifique que se $p(x) \in D[x]$ é primitivo e $q(x) \mid p(x)$, com $\mathrm{gr}(q(x)) \geq 1$, então $q(x)$ é primitivo.

(b) Mostre que todo o polinómio primitivo de $D[x]$ admite factorizações em irredutíveis em $D[x]$.

1.15. Seja D um DFU, $a \in D$, com $a \neq 0$, e $p(x), q(x) \in D[x]$ tais que $q(x) \mid ap(x)$ e $q(x)$ é primitivo. Prove que $q(x) \mid p(x)$.

1.16. Seja D um DFU. Mostre que, para quaisquer $a, b, c \in D$, se $1 \in \mathrm{mdc}(a, b)$ e $a \mid bc$ então $a \mid c$.

1.17. Seja D um domínio euclidiano com função euclidiana δ.

(a) Prove que $a \in D$ é uma unidade se $\delta(a)$ for um mínimo do conjunto $\{\delta(x) \mid x \in D, x \neq 0\}$. Mostre que se $\delta(a) \leq \delta(ab)$ para quaisquer $a, b \in D \setminus \{0\}$, então a implicação recíproca também é verdadeira.

(b) Revisite o Exercício 1.5, resolvendo-o agora usando o facto de $\mathbb{Z}[i]$ ser um domínio euclidiano.

1.18. Calcule em $\mathbb{Z}[i]$:

(a) $\mathrm{mdc}(2, 3 + i)$.

(b) $\langle 2 \rangle + \langle 3 + i \rangle$.

(c) $\langle 2 \rangle \cap \langle 3 + i \rangle$.

(d) $\mathrm{mdc}(9 - 5i, -9 + 13i)$.

1.19. Seja D um domínio euclidiano com função euclidiana δ (satisfazendo $\delta(a) \leq \delta(ab)$ para quaisquer $a, b \in D \setminus \{0\}$). Seja $I \neq \{0\}$ um ideal de D. Prove que se existir $a \in I$ tal que $\delta(a) = \delta(1)$, então $I = D$.

1.20. Seja D um domínio euclidiano com função euclidiana δ (satisfazendo $\delta(a) \leq \delta(ab)$ para quaisquer $a, b \in D \setminus \{0\}$). Mostre que se n é um inteiro tal que $\delta(1) + n > 0$, então a função $\delta' \colon D \setminus \{0\} \to \mathbb{N}$ definida por $\delta'(a) = \delta(a) + n$ é também uma função euclidiana em D.

1.21. Seja D um domínio euclidiano. Mostre, usando o método das divisões sucessivas (Euclides), que dados $a, b \in D$ (não simultaneamente nulos), existem $p, q \in D$ tais que $pa + qb \in \text{mdc}(a, b)$.

1.22. Seja A um anel comutativo com 1. Mostre que as seguintes condições são equivalentes:

(i) A é um corpo.

(ii) $A[x]$ é um domínio euclidiano.

(iii) $A[x]$ é um DIP.

1.23. Seja $\phi\colon A \to B$ um homomorfismo de anéis. Mostre que:

(a) $\phi(0) = 0$ e $\phi(-a) = -\phi(a)$.

(b) $N(\phi)$ é um ideal de A.

(c) ϕ é injectiva sse $N(\phi) = \{0\}$.

(d) $\phi(A)$ é um subanel de B.

1.24. Seja A um anel. Sendo I um ideal de A e B um subanel de A, mostre que:

(a) $B + I$ é um subanel de A e I é um ideal de $B + I$.

(b) A correspondência $a \mapsto a + I$ define um homomorfismo sobrejectivo $\pi\colon A \to A/I$ com núcleo I.

(c) A correspondência $b \mapsto b + I$ define um homomorfismo $B \to A/I$ com núcleo $B \cap I$ e imagem $(B + I)/I$.

1.25. (a) Sejam A um DIP, B um domínio de integridade e $\phi\colon A \to B$ um homomorfismo sobrejectivo de anéis com $N(\phi) \neq \{0\}$.

(i) Prove que $N(\phi)$ é um ideal maximal de A.

(ii) Conclua que B é um corpo.

(b) Sendo D um domínio de integridade, mostre que $D[x]$ é um DIP se e só se D é um corpo.

1.26. Prove que os anéis $\mathbb{Z}_n \oplus \mathbb{Z}_m$ e $\mathbb{Z}_{nm}$ são isomorfos se $\text{mdc}(n, m) = 1$. Mais geralmente, mostre que $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_d \oplus \mathbb{Z}_k$ para $d = \text{mdc}(n, m)$ e $k = \text{mmc}(n, m)$.

Soluções de exercícios seleccionados

1.11. (a) É fácil verificar que $\mathcal{S}$ é um anel comutativo com 1. A sequência $(1, 0, 0, \dots)$ é a identidade de $\mathcal{S}$.

(b) Consideremos $(a_n)_{n\in\mathbb{N}_0} \in \mathcal{S}$. Suponhamos que (a_n) é uma unidade. Então existe uma sequência $(b_n)_{n\in\mathbb{N}_0}$ tal que $(a_n)\cdot(b_n) = 1$. Logo, $a_0b_0 = 1$ e portanto a_0 é uma unidade de A.

Reciprocamente, suponhamos que $a_0 \in A^*$ e consideremos a sequência (b_n) definida por

$$b_0 = a_0^{-1}, \quad b_1 = -a_0^{-1}(a_1a_0^{-1}), \quad \dots, \quad b_k = -a_0^{-1}(a_1b_{k-1}+\cdots+a_kb_0), \quad k \geq 2.$$

É claro que $a_0b_0 = 1$, $a_0b_1 + a_1b_0 = a_0(-a_0^{-1}(a_1a_0^{-1})) + a_1a_0^{-1} = 0, \dots,$ $a_kb_0+a_{k-1}b_1+\cdots+a_0b_k = a_kb_0+a_{k-1}b_1+\cdots+a_0(-a_0^{-1}(a_1b_{k-1}+\cdots+a_kb_0)) =$ 0. Então $(a_n)\cdot(b_n) = 1$, o que prova que (a_n) é uma unidade de $\mathcal{S}$.

(c) Suponhamos que A é um corpo. Seja I um ideal de $\mathcal{S}$. Se $I = \{0\}$, então I é um ideal principal. Suponhamos então que $I \neq \{0\}$. Seja (a_n) um elemento não nulo de I. Definimos a *ordem* $\mathrm{o}(a_n)$ de uma sequência não nula (a_n) de $\mathcal{S}$ como sendo o primeiro inteiro não negativo tal que $a_n \neq 0$ e $a_i = 0$ para $i < n$. Existe uma sequência (a_n) tal que $\mathrm{o}(a_n) = \kappa \leq \mathrm{o}(b_n)$ para qualquer $(b_n) \in I$. Seja (c_n) a sequência tal que $c_i = a_{\kappa+i}$ para todo o $i \geq 0$. Então $(c_n)^{-1}$ existe e $(c_n)^{-1}\cdot(a_n) = (d_n) \in I$. Além disso, $d_\kappa = 1$ e $d_i = 0$ para todo o $i \neq \kappa$. Provemos que $I = \langle(d_n)\rangle$. Claramente $\langle(d_n)\rangle \subseteq I$. Seja $(u_n) \in I$ com ordem m. Então $m \geq \kappa$. Seja $(r_n) \in \mathcal{S}$ tal que $r_{m-\kappa+i} = u_{m+i}$ para qualquer $i \geq 0$ e $r_i = 0$ para qualquer $i \leq m - \kappa$. É fácil verificar que $(u_n) = (r_n)\cdot(d_n) \in \langle(d_n)\rangle$. Logo, $I = \langle(d_n)\rangle$.

1.14. (a) Seja $d \in D$ um divisor de $q(x)$ de grau zero. Como $d \mid p(x)$ então d é uma unidade.

(b) Seja $p(x)$ um polinómio primitivo de $D[x]$. Faremos a demonstração por indução sobre o grau $n \geq 1$ de $p(x)$:

Se $n = 1$ então $p(x)$ não admite factorizações próprias e, sendo primitivo, é irredutível e está provado.

Tomemos $p(x)$ de grau n e suponhamos, como hipótese de indução, que o resultado é válido para todos os polinómios de grau $< n$. Se $p(x)$ admitir uma factorização própria então $p(x) = q(x)r(x)$ com $\mathrm{gr}(q(x)), \mathrm{gr}(r(x)) < n$ e, pela hipótese de indução, ambos são factorizáveis em polinómios irredutíveis, o que nos dá uma factorização de $p(x)$ em irredutíveis. No caso em que $p(x)$

não admite factorizações próprias, como é primitivo, então é irredutível e está provado.

1.16. Seja $p_1p_2\cdots p_n$ a factorização de a em primos. Para cada $i = 1, 2, \ldots, n$, $p_i \mid bc$ logo $p_i \mid b$ ou $p_i \mid c$. Mas como a e b são primos entre si e $p_i \mid a$ (para qualquer i), se p_i dividisse b para algum i teríamos $p_i \mid 1$, isto é, $p_i \in D^*$, um absurdo. Logo nenhum p_i divide b pelo que $p_i \mid c$ para $i = 1, 2, \ldots, n$ e portanto $a \mid c$.

1.17. (b) $\mathbb{Z}[i]$ é um domínio euclidiano com função euclidiana

$$\delta(a + ib) = |a + ib|^2 = a^2 + b^2$$

que satisfaz a propriedade $\delta(xy) = \delta(x)\delta(y)$. As unidades de $\mathbb{Z}[i]$ são ± 1 e $\pm i$, pois $\delta(a + ib) = 1$ se e só se $a + ib \in \{\pm 1, \pm i\}$.

Se $1 \pm i = (a + ib)(c + id)$ então $\delta(1 \pm i) = \delta(a + ib)\delta(c + id)$, isto é, $2 = \delta(a + ib)\delta(c + id)$. Como 2 é primo em $\mathbb{Z}$, então $\delta(a + ib) = 1$ (ou seja, $a + ib$ é uma unidade) ou $\delta(c + id) = 1$ (ou seja, $c + id$ é uma unidade).

Claro que 2 é irredutível em $\mathbb{Z}$ porque é primo. Mas em $\mathbb{Z}[i]$, $2 = (1+i)(1-i)$, logo é redutível em $\mathbb{Z}[i]$.

1.18. (a) Pelo exercício anterior, $2 = (1 + i)(1 - i)$ é a factorização (única) de 2 em irredutíveis (primos). Como $3 + i = (1 + i)(2 - i)$ é a factorização de $3 + i$ em primos (de facto, $2 - i$ também é irredutível pois $\delta(2 + i) = 5$ é um inteiro primo), então $1 + i \in \text{mdc}(2, 3 + i)$. Logo,

$$\text{mdc}(2, 3 + i) = \{1 + i, -1 - i, -1 + i, 1 - i\}.$$

(b) Como em qualquer DIP, $\langle a\rangle + \langle b\rangle = \langle \text{mdc}(a, b)\rangle$, então $\langle 2\rangle + \langle 3 + i\rangle = \langle \text{mdc}(2, 3 + i)\rangle = \langle 1 + i\rangle = \{(a + ib)(1 + i) \mid a, b \in \mathbb{Z}\} = \{(a - b) + i(a + b) \mid a, b \in \mathbb{Z}\}$.

(c) Como em qualquer DIP, $\langle a\rangle \cap \langle b\rangle = \langle \text{mmc}(a, b)\rangle$, então $\langle 2\rangle \cap \langle 3 + i\rangle = \langle \text{mmc}(2, 3+i)\rangle = \langle (1+i)(1-i)(2-i)\rangle = \langle 4-2i\rangle = \{(4a+2b)+i(-2a+4b) \mid a, b \in \mathbb{Z}\}$.

1.22. (i)⇒(ii): Sendo A um corpo, dados $a(x), b(x) \in A[x]$ com $b(x) \neq 0$ sabemos que existem $q(x), r(x) \in A[x]$ tais que $a(x) = q(x)b(x) + r(x)$ com $r(x) = 0$ ou $gr(r(x)) < gr(b(x))$ (equivalentemente, $gr(r(x)) + 1 < gr(b(x)) + 1$). Portanto, fazendo $\delta(p(x)) = gr(p(x)) + 1$, temos claramente uma função euclidiana em $A[x]$.

(ii)⇒(iii): Basta aplicar a Proposição 4.2 que assegura que todo o domínio euclidiano é um DIP.

(iii)⇒(i): Seja $a \neq 0$ em A. Teremos que mostrar que a é invertível. Para isso consideremos o ideal $I = \langle a, x\rangle$ de $A[x]$, que é principal. Portanto, existe $p(x) \in A[x]$ tal que $I = \langle p(x)\rangle$. Como $a, x \in I$ então existem $a(x)$ e $b(x)$ em $A[x]$ tais que $a = a(x)p(x)$ e $x = b(x)p(x)$. Consequentemente, $gr(p(x)) = 0$ (observe que $A[x]$ sendo um domínio de integridade, implica necessariamente que A o seja), isto é, $p(x) = d \in A$. Então $x = b(x)d$, o que implica que $cd = 1$ para algum $c \in A$. Portanto d é uma unidade e $I = \langle d\rangle = A[x]$. Daqui podemos concluir que $1 \in I$, isto é, $1 = ap_1(x) + xp_2(x)$ para algum par $p_1(x), p_2(x)$ em $A[x]$. Isto implica $1 = ab$ para algum $b \in A$ e a é assim invertível.

1.26. A primeira parte do exercício foi provada no exemplo da página 26. Quanto à segunda parte:

Sejam

$$n = p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t} \quad \text{e} \quad m = p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$$

as decomposições primas de n e m ($n_i, m_i \in \mathbb{N}_0$). Então

$$d = p_1^{\min(n_1,m_1)}p_2^{\min(n_2,m_2)}\cdots p_t^{\min(n_t,m_t)}$$

e

$$k = p_1^{\max(n_1,m_1)}p_2^{\max(n_2,m_2)}\cdots p_t^{\max(n_t,m_t)}.$$

Pelo resultado da primeira parte podemos concluir que

$$\mathbb{Z}_d \cong \mathbb{Z}_{p_1^{\min(n_1,m_1)}} \oplus \mathbb{Z}_{p_2^{\min(n_2,m_2)}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\min(n_t,m_t)}}$$

e

$$\mathbb{Z}_k \cong \mathbb{Z}_{p_1^{\max(n_1,m_1)}} \oplus \mathbb{Z}_{p_2^{\max(n_2,m_2)}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\max(n_t,m_t)}}.$$

Logo $\mathbb{Z}_d \oplus \mathbb{Z}_k \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$ pois $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$ e $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{m_t}}$.

Capítulo 2

Anéis de polinómios a várias indeterminadas

Todos os resultados, e respectivas demonstrações, deste capítulo são transcritos do livro

Polinómios, Textos de Matemática, Vol. 20, Universidade de Lisboa, 2010

da autoria de Pedro Jorge Freitas.

1. Polinómios a várias indeterminadas

Seja A um anel. Como sabemos, o anel $A[x]$ dos *polinómios a uma indeterminada* x é o conjunto das sucessões

$$\boldsymbol{p} = (p_0, p_1, \ldots, p_n, 0, 0, \ldots), \quad p_i \in A$$

ou, equivalentemente, das somas formais

$$\boldsymbol{p} = p_0 + p_1 x + p_2 x^2 + \cdots + p_n x^n = \sum_{i=0}^{n} p_i x^i,$$

munido das operações de *soma* e *produto de convolução* definidas por

$$(\boldsymbol{p} + \boldsymbol{q})_i = p_i + q_i \quad \text{e} \quad (\boldsymbol{p} \star \boldsymbol{q})_i = \sum_{j=0}^{i} p_j q_{i-j}.$$

Agora, o anel $A[x_1, \ldots, x_n]$ dos *polinómios a* n *indeterminadas* $x_1, \ldots, x_n$ define-se simplesmente por iteração: $A[x_1, \ldots, x_n] := A[x_1, \ldots, x_{n-1}][x_n]$.

Esta definição corresponde à ideia que uma soma de monómios a n indeterminadas se deve escrever como um polinómio na última, pondo-a em evidência em cada monómio. Por exemplo, o polinómio $2x^2y^3 + x^3y + 2y^3 + 5x + 2y \in \mathbb{R}[x, y]$ pode escrever-se como um polinómio em y com coeficientes em $\mathbb{R}[x]$:

$$(2x^2 + 2)y^3 + (x^3 + 2)y + 5x.$$

Proposição 1.1. *Seja $p \in A[x_1, \ldots, x_n]$. Então existem um natural m e coeficientes $a_{i_1 \ldots i_n}$ $(0 \leq i_1, \ldots, i_n \leq m)$ tais que*

$$p = \sum_{i_1, \ldots, i_n = 0}^{m} a_{i_1 \ldots i_n} \, x_1^{i_1} \cdots x_n^{i_n}.$$

Além disso, os coeficientes $a_{i_1 \ldots i_n}$ nesta representação canónica são únicos.

Demonstração. Demonstremos o resultado por indução sobre n.

Se $n = 1$, o resultado é válido (como sabemos do estudo do anel $A[x]$). Suponhamos então o resultado válido para $n - 1$ e consideremos $p \in A[x_1, \ldots, x_n]$. Como, por definição, $A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$ então, usando o caso $n = 1$, podemos assumir que existem polinómios $p_1, \ldots, p_k \in A[x_1, \ldots, x_{n-1}]$ tais que

$$p = \sum_{j=0}^{k} p_k x_n^j.$$

Agora, pela hipótese de indução, para cada p_j existem coeficientes $a_{i_1 \ldots i_{n-1}, j}$, com $0 \leq i_1, \ldots, i_{n-1} \leq l_j$ tais que

$$p_j = \sum_{i_1, \ldots, i_{n-1} = 0}^{l_j} a_{i_1 \ldots i_{n-1}, j} \, x_1^{i_1} \cdots x_{n-1}^{i_{n-1}}.$$

Seja m o maior dos inteiros l_j $(1 \leq j \leq n - 1)$ e k. Introduzindo monómios com coeficientes nulos se necessário, e chamando i_n ao índice j, obtemos

$$p = \sum_{i_n=0}^{m} \Big(\sum_{i_1, \ldots, i_{n-1} = 0}^{m} a_{i_1 \ldots i_{n-1} i_n} \, x_1^{i_1} \cdots x_{n-1}^{i_{n-1}} \Big) x_n^{i_n} = \sum_{i_1, \ldots, i_n = 0}^{m} a_{i_1 \ldots i_n} \, x_1^{i_1} \cdots x_n^{i_n},$$

o que prove a primeira parte do resultado.

Quanto à unicidade dos coeficientes, pode ser provada de modo similar, usando indução sobre n. Para $n = 1$, o resultado é consequência da definição. Supondo que o resultado vale para $n - 1$, consideremos duas possíveis representações canónicas do mesmo polinómio p:

$$p = \sum_{i_1, \ldots, i_n = 0}^{m} a_{i_1 \ldots i_n} \, x_1^{i_1} \cdots x_n^{i_n} = \sum_{i_1, \ldots, i_n = 0}^{m} a'_{i_1 \ldots i_n} \, x_1^{i_1} \cdots x_n^{i_n}.$$

Olhando cada membro como polinómio de $A[x_1,\ldots,x_{n-1}][x_n]$, temos

$$\sum_{i_n=0}^{m}\Big(\sum_{i_1,\ldots,i_{n-1}=0}^{m} a_{i_1\ldots i_{n-1}i_n}\, x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}\Big)x_n^{i_n} = \sum_{i_n=0}^{m}\Big(\sum_{i_1,\ldots,i_{n-1}=0}^{m} a'_{i_1\ldots i_{n-1}i_n}\, x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}\Big)x_n^{i_n}.$$

Então, pelo caso $n=1$, podemos concluir que

$$\sum_{i_1,\ldots,i_{n-1}=0}^{m} a_{i_1\ldots i_{n-1}i_n}\, x_1^{i_1}\cdots x_{n-1}^{i_{n-1}} = \sum_{i_1,\ldots,i_{n-1}=0}^{m} a'_{i_1\ldots i_{n-1}i_n}\, x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}$$

para qualquer i_n entre 1 e m. Finalmente, pela hipótese de indução,

$$a_{i_1\ldots i_{n-1}i_n} = a'_{i_1\ldots i_{n-1}i_n}$$

para quaisquer $1 \le i_1,\ldots,i_{n-1} \le m$. ∎

Notação. Em questões teóricas é útil simplificar a escrita usando *expoentes e índices múltiplos* (permitindo recuperar a notação usada nos polinómios a uma indeterminada). Basta para cada n-úplo de inteiros não negativos $i=(i_1,\ldots,i_n)$ abreviar $x_1^{i_1}\cdots x_n^{i_n}$ por $\overline{x}^i$.

Por exemplo, o polinómio $x_1^2x_2 - x_1x_2 + 4x_1 \in \mathbb{R}[x_1,x_2]$ abrevia-se por

$$\overline{x}^{(2,1)} - \overline{x}^{(1,1)} + 4\overline{x}^{(1,0)}.$$

Vamos também denotar $A[x_1,\ldots,x_n]$ simplesmente por $A[\overline{x}]$ sempre que isso não cause confusão.

Note que se i e j forem dois expoentes múltiplos, então $\overline{x}^i\overline{x}^j = \overline{x}^{i+j}$ (onde a soma $i+j$ é feita coordenada a coordenada), pela comutatividade do anel $A[\overline{x}]$. Isto permite recuperar o formalismo da soma e do produto de polinómios a uma indeterminada:

Proposição 1.2. *Sejam* $p=\sum_{i\in\mathbb{N}_0^n} a_i\,\overline{x}^i$ *e* $q=\sum_{i\in\mathbb{N}_0^n} b_i\,\overline{x}^i$ *em* $A[\overline{x}]$. *Então*

$$p+q = \sum_{i\in\mathbb{N}_0^n}(a_i+b_i)\,\overline{x}^i \qquad e \qquad pq = \sum_{k\in\mathbb{N}_0^n}\Big(\sum_{i+j=k} a_ib_j\Big)\,\overline{x}^k.$$

Demonstração. A primeira identidade é simples de verificar. Quanto à da multiplicação, é consequência da distributividade:

$$pq = \Big(\sum_{i\in\mathbb{N}_0^n} a_i\,\overline{x}^i\Big)\Big(\sum_{j\in\mathbb{N}_0^n} b_j\,\overline{x}^j\Big) = \sum_{i,j\in\mathbb{N}_0^n} a_ib_j\,\overline{x}^i\overline{x}^j = \sum_{i,j\in\mathbb{N}_0^n} a_ib_j\,\overline{x}^{i+j}.$$

Agrupando as parcelas comuns onde ocorre $\overline{x}^k$, obtemos

$$pq = \sum_{k\in\mathbb{N}_0^n} \Big(\sum_{i+j=k} a_i b_j \Big) \overline{x}^k. \qquad \blacksquare$$

Os polinómios da forma $ax_1^{i_1}\cdots x_n^{i_n}$ são chamados *monómios* e os da forma $x_1^{i_1}\cdots x_n^{i_n}$ *monómio primitivos*. Diz-se que um monómio primitivo *ocorre* num polinómio p se o seu coeficiente em p for diferente de zero.

Proposição 1.3. *Sejam A e B anéis, $A \subseteq B$, e $b_1, \ldots, b_n \in B$. Existe um (único) homomorfismo de anéis $\varphi_{b_1,\ldots,b_n}\colon A[x_1,\ldots,x_n] \to B$ que*

- *deixa fixos os elementos de $A \subseteq A[x_1,\ldots,x_n]$ e*
- *aplica x_i em b_i, para cada $1 \leq i \leq n$.*

Demonstração. A existência pode ser provada por indução sobre n. O caso $n = 1$ é conhecido do ano passado. Supondo válido o resultado para $n-1$, existe um homomorfismo de anéis $\sigma\colon A[x_1,\ldots,x_{n-1}] \to B$ que fixa os elementos de A e tal que $\sigma(x_i) = b_i$ para $i = 1, 2, \ldots, n-1$. Mas (como vimos no ano passado), para cada homomorfismo de anéis $f\colon A \to B$, a aplicação $\overline{f}\colon A[x] \to B[x]$ definida por $\overline{f}(\sum_{i=0}^n a_i\, x^i) = \sum_{i=0}^n f(a_i)\, x^i$ é também um homomorfismo de anéis. Aplicando este resultado à nossa situação obtemos um homomorfismo $\overline{\sigma}\colon A[x_1,\ldots,x_{n-1}][x_n] \to B[x_n]$ dado pela correspondência

$$p_0 + p_1 x_n + \cdots + p_m x_n^m \longmapsto \sigma(p_0) + \sigma(p_1)x_n + \cdots + \sigma(p_m)x_n^m.$$

Por outro lado, pelo resultado a uma variável, existe um homomorfismo $\tau\colon B[x_n] \to B$ tal que $\tau(b) = b$ para qualquer $b \in B$ e $\tau(x_n) = b_n$. Compondo τ com $\overline{\sigma}$ obtemos um homomorfismo nas condições do enunciado. De facto, para cada $a \in A$, $\tau\overline{\sigma}(a) = \tau(a) = a$, $\tau\overline{\sigma}(x_i) = \tau(\sigma(x_i)) = \tau(b_i) = b_i$ para $i = 1, \ldots, n-1$ e $\tau\overline{\sigma}(x_n) = \tau(x_n) = b_n$.

Quanto à unicidade, suponhamos que ψ era outro homomorfismo nessas condições. Então

$$\begin{aligned}
\psi\Big(\sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, x_1^{i_1}\cdots x_n^{i_n} \Big) &= \sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, \psi(x_1^{i_1}\cdots x_n^{i_n}) \\
&= \sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, \psi(x_1)^{i_1}\cdots\psi(x_n)^{i_n} \\
&= \sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, b_1^{i_1}\cdots b_n^{i_n} \\
&= \tau\overline{\sigma}\Big(\sum_{i_1,\ldots,i_n=0}^{m} a_{i_1,\ldots,i_n}\, x_1^{i_1}\cdots x_n^{i_n} \Big),
\end{aligned}$$

o que termina a demonstração. ∎

O homomorfismo $\varphi_{b_1,\ldots,b_n}$ é o designado *homomorfismo de substituição*. Denotaremos a imagem $\varphi_{b_1,\ldots,b_n}(p)$ por $p(b_1,\ldots,b_n)$.

A imagem de $A[x_1,\ldots,x_n]$ por $\varphi_{b_1,\ldots,b_n}$ é exactamente o subanel de B gerado por $A \cup \{b_1,\ldots,b_n\}$, que denotamos por $A[b_1,\ldots,b_n]$. Sendo A um domínio de integridade, denotamos por $A(b_1,\ldots,b_n)$ o corpo das fracções de $A[b_1,\ldots,b_n]$ (que podemos considerar contido em B, a menos de isomorfismo, se B for um corpo; neste caso, $A(b_1,\ldots,b_n)$ é o menor subcorpo de B que contém $A \cup \{b_1,\ldots,b_n\}$).

Como os coeficientes dos polinómios a várias indeterminadas são eles próprios polinómios, então uma raiz de um elemento de $A[x_1,\ldots,x_n] = A[x_1,\ldots,x_{n-1}][x_n]$ é um polinómio nas indeterminadas $x_1,\ldots,x_{n-1}$. Temos assim que usar outro nome ("zero") para os n-úplos que anulam o polinómio:

ZEROS de um polinómio

$(b_1,\ldots,b_n) \in B^n$ é um *zero* de $p \in A[\overline{x}]$ se $\varphi_{b_1,\ldots,b_n}(p) = 0$, ou seja, $p(b_1,\ldots,b_n) = 0$.

Dado $p \in A[\overline{x}]$, a função $A^n \to A$ definida por $a \mapsto p(a) = \varphi_a(p)$ é chamada a *função polinomial* associada a p.

Por exemplo, o polinómio $x \in \mathbb{R}[x,y]$ tem infinitos zeros (todos os pares $(0,b)$ com $b \in \mathbb{R}$) mas como elemento de $\mathbb{R}[y][x]$ tem grau 1 logo não pode ter mais do que uma raiz em $\mathbb{R}[y]$ (e como polinómio de grau zero em $\mathbb{R}[x][y]$ não pode ter raízes em $\mathbb{R}[x]$).

Proposição 1.4. *Seja D um domínio de integridade infinito, e sejam $B_1,\ldots,B_n \subseteq D$ conjuntos infinitos. Se $p \in D[x_1,\ldots,x_n]$ é tal que $p(b_1,\ldots,b_n) = 0$ para qualquer $(b_1,\ldots,b_n) \in B_1 \times \cdots \times B_n$, então $p = 0$.*

Demonstração. Mais uma vez demonstramos o resultado por indução sobre n. O caso $n = 1$ foi provado no ano passado ("*um polinómio $p(x) \in D[x]$ de grau $n \geq 0$ não pode ter mais do que n raízes em D*"). Suponhamos então o resultado válido para $n-1$, e seja

$$p = \sum_{i \in \mathbb{N}_0} p_i(x_1,\ldots,x_{n-1})\, x_n^i \in D[x_1,\ldots,x_n].$$

Para cada $1 \leq i \leq n-1$ sejam $b_i \in B_i$ quaisquer e consideremos $h(x_n) = p(b_1,\ldots,b_{n-1},x_n) \in D[x_n]$. É claro que h se anula em $B_n \subseteq A$, um conjunto

infinito. Como num domínio infinito D dois polinómios em $D[x]$ diferentes definem funções polinomiais diferentes, então $h(x_n) = 0$ em $D[x_n]$, o que quer dizer que os seus coeficientes são nulos, isto é, $p_i(b_1, \ldots, b_{n-1}) = 0$ para qualquer $i \in \mathbb{N}_0$. Como os elementos $b_1, \ldots, b_{n-1}$ são arbitrários, concluimos que os polinómios $p_i \in D[x_1, \ldots, x_{n-1}]$ se anulam sempre que $b_1 \in B_1, \ldots, b_{n-1} \in B_{n-1}$. Por hipótese de indução, isso significa que são nulos. Assim, $p = 0$ como pretendíamos. ∎

Portanto, se $p, q \in D[x_1, \ldots, x_n]$ definem a mesma função polinomial, então $p = q$. De facto, basta ver que $p - q$ se anula em D^n, com D infinito; daí decorre, pelo resultado, que $p - q = 0$, isto é, $p = q$.

2. Factorização de polinómios a várias indeterminadas

Proposição 2.1. *Se D é um domínio de integridade (resp. DFU) então $D[x_1, \ldots, x_n]$ é também um domínio de integridade (resp. DFU).*

Demonstração. Capítulo 1. ∎

Assim, se D for um domínio de integridade, podemos formar o corpo das fracções de $A[x_1, \ldots, x_n]$, que denotaremos por $A(x_1, \ldots, x_n)$.

GRAU de um polinómio

(1) Seja $x_1^{i_1} \cdots x_n^{i_n}$ um monómio de $A[x_1, \ldots, x_n]$. Chama-se *grau* deste monómio à soma dos expoentes dos x_i's:

$$\mathrm{gr}(x_1^{i_1} \cdots x_n^{i_n}) := i_1 + \cdots + i_n.$$

(2) Seja $p \in A[x_1, \ldots, x_n]$ um polinómio não nulo. Chama-se *grau* de p ao máximo dos graus dos monómios que ocorrem em p. Por convenção, diz-se que o grau do polinómio nulo é $-\infty$.
(3) Um polinómio diz-se *homogéneo* se todos os seus monómios tiverem o mesmo grau.

Tal como nos polinómios a uma indeterminada, é verdade que

$$\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q)$$

quando os coeficientes pertencem a um domínio de integridade. No entanto, não podemos usar indução para provar isso. Necessitaremos então do seguinte resultado envolvendo polinómios homogéneos:

Proposição 2.2. *Seja A um anel comutativo. Então qualquer polinómio $p \in A[x_1, \ldots, x_n]$ se escreve, de modo único, como soma de parcelas homogéneas.*

Demonstração. Para provar a existência, basta partir da representação canónica de p como soma de monómios, e agrupar os monómios do mesmo grau numa mesma parcela: se $p = \sum_{i \in \mathbb{N}_0^n} a_i \, \overline{x}^i$, então

$$p = a_{(0,\ldots,0)} + \sum_{i_1+\cdots+i_n=1} a_i \, \overline{x}^i + \sum_{i_1+\cdots+i_n=2} a_i \, \overline{x}^i + \cdots$$

Quanto à unicidade, consideremos $p = p_0 + p_1 \cdots + p_m = p'_0 + p'_1 + \cdots + p'_k$ onde p_j e p'_j são homogéneos de grau j para cada j. Reagrupando as parcelas podemos escrever

$$p_0 - p'_0 = (p'_1 + \cdots + p'_k) - (p_1 + \cdots + p_m),$$

em que, sendo não nulos, o polinómio da esquerda tem grau 0 e o da direita tem grau ≥ 1, um absurdo. Assim, têm de ser nulos, pelo que $p_0 = p'_0$ e $p_1 + \cdots + p_m = p'_1 + \cdots + p'_k$. Iterando o argumento para as parcelas de grau 1, concluímos que também são iguais e podemos cortá-las. E assim sucessivamente, chegaremos à conclusão que para $j \leq \min\{m, k\}$, $p_j = p'_j$. Suponhamos, sem perda de generalidade, que $k \leq m$. Se $k < m$ teríamos $p_{k+1} + \cdots + p_m = 0$, o que é impossível por p_j ser homogéneo de grau j. Logo $m = k$. ∎

Teorema 2.3. *Seja D um domínio de integridade. Então* $\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q)$ *para quaisquer polinómios $p, q \in D[x_1, \ldots, x_n]$.*

Demonstração. Se $p = 0$ ou $q = 0$ o resultado é óbvio. Suponhamos então $p \neq 0$, $q \neq 0$, $\mathrm{gr}(p) = n$ e $\mathrm{gr}(q) = m$. Provaremos primeiro o caso em que p e q são homogéneos. É simples de verificar que o grau de qualquer monómio que ocorra em pq é igual a $n + m$, por causa da homogeneidade. Temos pois de garantir apenas que, depois das simplificações, o produto pq não é zero. Isso é garantido pelo facto de $D[x_1, \ldots, x_n]$ ser um domínio de integridade.

No caso geral, decompomos p e q em parcelas homogéneas (usando a proposição anterior) $p = p_0 + \cdots + p_n$ e $q = q_0 + \cdots + q_m$ onde $\mathrm{gr}(p_i) = i$, $\mathrm{gr}(q_j) = j$ e $p_n, q_m \neq 0$. Então

$$pq = p_n q_m + p_n\Big(\sum_{i=0}^{m-1} q_j\Big) + \Big(\sum_{i=0}^{n-1} p_i\Big) q_m + \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} p_i q_j,$$

onde todos os polinómios que aparecem nos somatórios à direita têm grau menor que $p_n q_m$, pelo caso já demonstrado. Logo $\mathrm{gr}(pq) = \mathrm{gr}(p_n q_m) = n + m$, pelo mesmo motivo. ∎

A Proposição 2.1, no caso dos DFU, diz-nos que faz sentido falar da decomposição de um polinómio em factores irredutíveis.

[RECORDE que esses irredutíveis estão descritos no Teorema 3.3 do Capítulo 1.]

Exemplos. (1) É fácil de ver, usando o Teorema 3.3 do Capítulo 1, que polinómios como $xy+1$ ou $x+1$ são irredutíveis em $\mathbb{Z}[x,y]$. Por exemplo, o polinómio $xy+1$, considerado como elemento de $\mathbb{Z}[x][y]$, é primitivo pois os seus coeficientes, x e 1, são co-primos e não tem factorizações próprias (por ter grau 1). Assim, pelo Teorema 3.3, o polinómio é irredutível em $\mathbb{Z}[x,y]$. Quanto a $x+1 \in \mathbb{Z}[x][y]$, é um elemento do anel de coeficientes $\mathbb{Z}[x]$, e é irredutível por ser primitivo e não admitir factorizações próprias. Assim, sendo irredutível em $\mathbb{Z}[x]$, é irredutível em $\mathbb{Z}[x][y] = \mathbb{Z}[x,y]$, pelo mesmo teorema.

(2) O polinómio $xy^2 - x \in \mathbb{Z}[x,y] = \mathbb{Z}[x][y]$ admite a factorização $x(y^2-1)$. No entanto, não é própria pois $x \in \mathbb{Z}[x]$ (que é o anel dos coeficientes). Uma factorização própria seria por exemplo $(xy-x)(y+1)$. A factorização completa em irredutíveis é $x(y-1)(y+1)$.

(3) Vimos que se um polinómio a uma indeterminada tivesse uma raiz a então era divisível por $(x-a)$. Apliquemos este resultado ao polinómio $y^n - x^n \in \mathbb{Z}[x,y] = \mathbb{Z}[x][y]$ $(n>1)$. Como polinómio em y tem apenas termo de grau n e termo independente. Além disso, se substituirmos a indeterminada y por x (um elemento do anel dos coeficientes), verificamos que x é raiz do polinómio. Assim, o polinómio é divisível por $y-x$ em $\mathbb{Z}[x,y]$. Usando a regra de Ruffini para fazer a divisão obtemos

	(n)	$(n-1)$	$(n-2)$	$\cdots$	(1)	(0)
	1	0	0	$\cdots$	0	$-x^n$
x		x	x^2	$\cdots$	x^{n-1}	x^n
	1	x	x^2	$\cdots$	x^{n-1}	0

Portanto

$$y^n - x^n = (y-x)(y^{n-1} + xy^{n-2} + x^2y^{n-3} + \cdots + x^{n-2}y + x^{n-1}).$$

Logo, $y^n - x^n$ nunca é irredutível para $n > 1$.

Proposição 2.4. *Sejam A um anel, $\sigma \in S_n$ e $k < n$ um inteiro. Então $A[x_1,\ldots,x_n]$ é isomorfo a $A[x_{\sigma(1)},\ldots,x_{\sigma(n)}]$ e igual a $A[x_1,\ldots,x_k][x_{k+1},\ldots,x_n]$. Portanto,*

$$A[x_1,\ldots,x_n] \cong A[x_{\sigma(1)},\ldots,x_{\sigma(k)}][x_{\sigma(k+1)},\ldots,x_{\sigma(n)}].$$

Demonstração. Consideremos o homomorfismo de substituição

$$\varphi\colon A[x_1,\ldots,x_n] \to A[x_{\sigma(1)},\ldots,x_{\sigma(n)}]$$

que aplica x_i em x_i (não se trata da aplicação identidade pois cada indeterminada x_i desempenha um papel diferente no primeiro anel e no segundo). Este homomorfismo tem como inverso o homomorfismo de substituição ψ com a mesma correspondência $x_i \mapsto x_i$, desta vez de $A[x_{\sigma(1)},\ldots,x_{\sigma(n)}]$ para $A[x_1,\ldots,x_n]$. A conclusão de que são inversos um do outro segue do facto de que $\psi\varphi$ vai de $A[x_1,\ldots,x_n]$ para si próprio, aplica x_i em x_i e fixa A: como a identidade é outro homomorfismo de substituição verificando as mesmas condições, tem de ser o mesmo, pela unicidade. Assim, $\psi\varphi = \mathrm{id}$. Analogamente, $\varphi\psi = \mathrm{id}$.

A segunda parte do resultado segue por indução: o caso $n = 2$ é evidente e supondo o resultado válido para $n-1$ temos

$$\begin{aligned} A[x_1,\ldots,x_k][x_{k+1},\ldots,x_n] &= (A[x_1,\ldots,x_k][x_{k+1},\ldots,x_{n-1}])[x_n] \\ &\overset{\text{hip. ind.}}{=} A[x_1,\ldots,x_{n-1}][x_n] = A[x_1,\ldots,x_n]. \end{aligned}$$ ∎

Este resultado diz-nos que podemos, a menos de isomorfismo, considerar quaisquer indeterminadas como coeficientes, e quaisquer outras como indeterminadas propriamente ditas.

Seja $p \in A[x_1,\ldots,x_n]$. Chama-se *grau* de p em x_i ao grau de p considerado como elemento de $A[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n][x_i]$.

Apresentamos agora vários exemplos que ilustram como se podem aplicar os critérios de irredutibilidade estudados para provar que certos polinómios de $A[x_1,\ldots,x_n]$ são irredutíveis, ou para os factorizar. Note que as definições de elemento irredutível e elemento primo dependem apenas dos conceitos de factorização e de unidade num anel, pelo que são conservadas por isomorfismo. Assim, por exemplo, quando estamos a discutir a irredutibilidade ou primalidade de um polinómio em $\mathbb{C}[x,y,z]$ podemos considerá-lo como pertencendo a $\mathbb{C}[x,z][y]$ ou a $\mathbb{C}[z][x,y]$, por exemplo, conforme der mais jeito.

É preciso, porém, algum cuidado com o conceito de factorização própria pois esta depende do anel de coeficientes que estejamos a considerar.

Exemplo. O polinómio $x^n + y + 1$ considerado em $\mathbb{Z}[y][x]$ verifica as condições do critério de Eisenstein, com $p = y + 1$ (irredutível em $\mathbb{Z}[y]$). Portanto o polinómio não admite factorização própria em $\mathbb{Z}[y][x]$. Como 1 é mdc dos seus coeficientes, 1 e $y + 1$, o polinómio é irredutível em $\mathbb{Z}[y][x] = \mathbb{Z}[x,y]$.

Proposição 2.5. *Sejam A e B domínios de integridade, $f\colon A \to B$ um homomorfismo e $\overline{f}\colon A[x] \to B[x]$ a extensão definida na demonstração da Proposição 1.3. Seja $p(x) \in A[x]$, $p(x) \neq 0$, tal que $\mathrm{gr}(\overline{f}(p(x))) = \mathrm{gr}(p(x))$. Então, se $\overline{f}(p(x))$ não admitir uma factorização própria em $B[x]$, também $p(x)$ não admite factorizações próprias em $A[x]$.*

Demonstração. Suponhamos, por absurdo, que $p(x)$ tem uma factorização própia em $A[x]$:

$$p(x) = q(x)r(x), \quad \mathrm{gr}(q(x)), \mathrm{gr}(r(x)) < \mathrm{gr}(p(x)).$$

Então $\overline{f}(p(x)) = \overline{f}(q(x))\overline{f}(r(x))$, $\mathrm{gr}(\overline{f}(q(x))) \leq \mathrm{gr}(q(x)), \mathrm{gr}(\overline{f}(r(x))) \leq \mathrm{gr}(r(x))$, mas como $\mathrm{gr}(\overline{f}(p(x))) = \mathrm{gr}(p(x))$, temos de ter também igualdade nos graus dos factores e portanto $\mathrm{gr}(\overline{f}(q(x))), \mathrm{gr}(\overline{f}(r(x))) < \mathrm{gr}(\overline{f}(p(x)))$, o que contraria o facto de $\overline{f}(p(x))$ não admitir factorizações próprias em $B[x]$. ∎

Aplicando este resultado ao homomorfismo de substituição, obtemos imediatamente o seguinte corolário:

Corolário 2.6. [Critério de substituição] *Seja D um DFU e*

$$p \in D[x_1, \ldots, x_n, y] = D[x_1, \ldots, x_n][y].$$

Suponhamos que, para certos elementos $a_1, \ldots, a_n \in D$, o polinómio $p(a_1, \ldots, a_n, y)$ ten o mesmo grau em y que p, e não tem factorizações próprias em $D[y]$. Então p não tem factorizações próprias em $D[x_1, \ldots, x_n][y]$.

Exemplos. (1) O polinómio

$$x^2y^2 - y^2 + x - 1 \in \mathbb{Z}[x, y],$$

escrito como elemento de $\mathbb{Z}[x][y]$ fica $(x^2-1)y^2+x-1$. Um mdc dos seus coeficientes é $x - 1$, que pode ser posto em evidência, obtendo

$$(x - 1)((x + 1)y^2 + 1) = (x - 1)(xy^2 + y^2 + 1).$$

O primeiro dos factores é claramente irredutível por ser primitivo em $\mathbb{Z}[x]$ e sem factorizações próprias (por ter grau 1). Assim, é irredutível em $\mathbb{Z}[x]$ e, portanto, irredutível em $\mathbb{Z}[x][y] = \mathbb{Z}[x, y]$. Quanto ao segundo factor, é primitivo em $\mathbb{Z}[x][y]$. Fazendo a substituição $x = 2$, obtemos o polinómio $3y^2 + 1$, que não admite factorizações próprias em $\mathbb{Z}[y]$: tem grau 2 e não tem raízes em $\mathbb{Q}$ (logo é irredutível em $\mathbb{Q}[y]$). Assim, o outro factor também é irredutível em $\mathbb{Z}[x][y]$, e terminámos a factorização.

(2) Aplicamos agora o critério das raízes fraccionárias a um polinómio a duas indeterminadas. Seja $p = x^2y^4 + y^4 - x^4 - xy^2$. Se o encararmos como elemento de $\mathbb{Z}[y][x]$, isto é, $-x^4 + y^4x^2 - y^2x + y^4$, vemos que se existirem raízes de p em $\mathbb{Z}[y]$ têm de dividir y^4 em $\mathbb{Z}[y]$. Experimentando as diversas potências de y (e as suas simétricas), vemos que y^2 é raiz e portanto o polinómio é divisível por $x - y^2$. Usando a regra de Ruffini encontramos

$$x^2y^4 + y^4 - x^4 - xy^2 = (x - y^2)(-x^3 - y^2x^2 - y^2).$$

Sejam $A \subseteq B$ anéis e $b = (b_1, \ldots, b_n)$ uma família de elementos de B. A família b diz-se *algebricamente dependente* sobre A se existir um polinómio $p \in A[x_1, \ldots, x_n]$ com $p \neq 0$ tal que $p(b_1, \ldots, b_n) = 0$; caso contrário, diz-se que é *algebricamente independente*.

Exemplos. (1) É claro que as indeterminadas $(x_1, \ldots, x_n)$ são independentes sobre A (pela Proposição 1.1).

(2) O facto de π ser transcendente sobre $\mathbb{Q}$ significa nesta nova linguagem que π é algebricamente independente sobre $\mathbb{Q}$. No entanto, (π, π^2) é algebricamente dependente, pois o par é zero do polinómio $x^2 - y$.

Proposição 2.7. *Sejam $A \subseteq B$ anéis e $b_1, \ldots, b_n \in B$. Então $(b_1, \ldots, b_n)$ é uma família algebricamente independente se e só se o homomorfismo de substituição $\varphi_{b_1,\ldots,b_n}$ for injectivo. Nesse caso, este homomorfismo é um isomorfismo de $A[x_1, \ldots, x_n]$ em $A[b_1, \ldots, b_n]$.*

Demonstração. Se a família é algebricamente independente e $p \in A[\overline{x}]$ for não nulo, isto quer dizer que $\varphi_b(p) = p(b) \neq 0$, o que é equivalente a afirmar que $N(\varphi_b) = \{0\}$. A recíproca é imediata também. ∎

Exercícios

2.1. Prove que, sendo $A \subseteq B$ anéis e $b_1, \ldots, b_n \in B$, então $A[b_1, \ldots, b_n]$ é o menor subanel de B que contém A e os elementos $b_1, \ldots, b_n$ (isto é, é o subanel de B gerado por $A \cup \{b_1, \ldots, b_n\}$).

2.2. Quais dos seguintes polinómios têm factorizações próprias em $\mathbb{Z}[x][y]$? e em $\mathbb{Z}[y][x]$?

(a) $x^2 + xy + x + y$. (b) $xy^2 + x^2y + x^2 + y^2 + 2xy + x + y$.

2.3. Sabendo que $\mathbb{Z}[x, y]$ é um DFU, determine o

$$\text{mdc}\,(x^2y^2 - xy^2 + 2x^2y - 2y^2 - 2xy + x^2 - 4y - x - 2, xy^2 + x^2y + y^2 + 2xy + x^2 + y + x).$$

2.4. Determine a multiplicidade de a como raiz de $p \in A[x]$ nos seguintes casos:

(a) $p = x^3 - yx^2 - y^2x + y^3$, $a = y$, $A = \mathbb{Z}[y]$.

(b) $p = x^2y^2 + 2xy^2 + y^2 + x^2 + 2x + 1$, $a = -1$, $A = \mathbb{Z}[y]$.

2.5. Seja D um domínio de integridade. Mostre que $D[x_1, \ldots, x_n]^* = D^*$.

2.6. Seja D um DFU. Prove que se $p \in D$ é primo em D, então p é primo em $D[x_1, \ldots, x_n]$.

2.7. Factorize os seguintes polinómios num produto de irredutíveis em $\mathbb{Z}[x, y]$, $\mathbb{R}[x, y]$ e $\mathbb{C}[x, y]$.

(a) $x^2 + y^2$. (b) $x^3 - 2y^3$.

2.8. Factorize ou prove que são irredutíveis em $\mathbb{Z}[x, y]$:

(a) $xy^2 + 2x - 4y + 2$.

(b) $x^5y^2 + x^2y + 2xy + y + x$.

(c) $xy^2 + x^2y + xy + x + y + 1$.

2.9. Mostre que os seguintes polinómios são irredutíveis em $\mathbb{C}[x, y, z]$:

(a) $x^2 + y^2 - 1$. (b) $x^2 - y^2 + z^2$.

2.10. Seja C um corpo e $p(x, y) \in C[x, y]$. Prove que p tem um factor de grau 1 em $C[x, y]$ se e só se

- existir $q \in C[x]$ com $\text{gr}(q) \leq 1$ e $p(x, q(x)) = 0$ ou
- existir $r \in C[y]$ com $\text{gr}(r) \leq 1$ e $p(r(y), y) = 0$.

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 $(V, +)$ com 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

$$(p(x),v)\mapsto p(x)\cdot v:=a_nT^n(v)+\cdots+a_1T(v)+a_0v$$

define uma operação do anel $\mathbb{R}[x]$ no grupo abeliano $(\mathbb{R}^3,+)$ com 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 arbitrária T.

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

Módulo sobre um anel

Seja A um anel. Um *módulo M sobre 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 A em M que satisfaz as seguintes propriedades:

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

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

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

Se A possui uma identidade 1_A e

(4) $1_A v = v$, para qualquer $v \in M$,

diz-se que M é um *A-módulo unitário*.

Em rigor, os módulos acabados de definir são os chamados "A-módulos à esquerda"; de modo análogo, podemos definir os "A-módulos à direita". Ao longo do capítulo, caso nada seja dito em contrário, assumiremos que A é um anel comutativo com identidade e os A-módulos referem-se a A-módulos à esquerda unitários. Todos os resultados deste capítulo são verdadeiros *mutatis mutandis* para os módulos 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* de um A-módulo $(M,+)$ é um subconjunto N 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 (unitário ou não) então também é um A-módulo (não necessariamente unitário): 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 ϕ^*M. Será um A-módulo unitário desde que φ preserve a identidade (o que não é verdade para um homomorfismo de anéis arbitrário; é verdade, por exemplo, se φ for sobrejectivo ou mais geralmente se existir um elemento na imagem que não é divisor de zero).

Exercício 1.1. 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 $(x^2 - 1)v = 0$.

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*

$$N(\phi) = \{v \in M_1 \mid \phi(v) = 0\}$$

e a sua *imagem*

$$Im(\phi) = \{\phi(v) \mid v \in M_1\}$$

são submódulos de M_1 e M_2, respectivamente.

Exercício 1.2. 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.

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

$$\sum_{i=1}^{r} a_iv_i + \sum_{j=1}^{t} n_jv'_j,$$

com $a_i \in A$, $n_j \in \mathbb{Z}$ 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 $I = \{1, 2, \ldots, r\}$ é finito, escreve-se $\sum_{i=1}^{r} N_i$ ou ainda $N_1 + N_2 + \cdots + N_r$. Em geral,

$$\begin{aligned}\sum_{i\in I} N_i &= \{a_1v_1 + \cdots + a_rv_r \mid a_i \in A, v_i \in \bigcup_{i\in I} N_i\}\\ &= \{v_{i_1} + \cdots + v_{i_r} \mid r \in \mathbb{N}, i_1, \ldots, i_r \in I, v_{i_j} \in N_{i_j}\}.\end{aligned}$$

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, que se denota por M/N.

Exercício 2.1. Determine os submódulos de M/N.

De modo análogo aos grupos e anéis,

a projecção canónica $\pi\colon M \to M/N$ *é uma aplicação A-linear.* Além disso:

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:

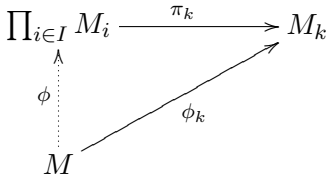
- conjunto suporte: produto cartesiano $\{(v_i)_{i\in I} \mid v_i \in M_i\}$ dos M_i.

- 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 $v_k \in M_k$.

Exercício 2.2. 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).

Somas directas

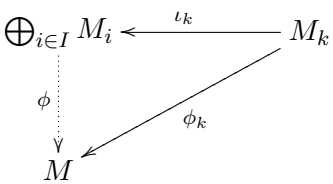
A *soma directa* de uma família $\{M_i\}_{i\in I}$ de A-módulos, que denotamos por $\bigoplus_{i\in I} M_i$, é o submódulo de $\prod_{i\in I} M_i$ formado pelos elementos $(v_i)_{i\in I}$ nos quais apenas um número finito de v_i's é não nulo.

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, tem-se:

Exercício 2.3. Seja $\{M_i\}_{i\in I}$ uma família de A-módulos. Mostre que:

(a) Dado um A-módulo M e homomorfismos $\{\phi_i \colon M_i \to M\}_{i\in I}$, 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).

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 que $\phi \circ \psi = \mathrm{id}_{M_1 \oplus \cdots \oplus M_k}$ 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 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 $(v_i)_{i\in I} \mapsto \sum_{i\in I} v_i$.

$\Rightarrow$: Por hipótese, ϕ é um isomorfismo. É evidente que a sobrejectividade de ϕ garante que $M = \sum_{i\in I} M_i$. 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 $(u_i)_{i\in I}$ e $(w_i)_{i\in I}$ em $\bigoplus_{i\in I} M_i$ definidos por

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

Como $\phi((u_i)_{i\in I}) = v = \phi((w_i)_{i\in I})$ e ϕ é injectivo, então $(u_i)_{i\in I} = (w_i)_{i\in I}$, 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 $\phi((v_i)_{i\in I}) = \phi((w_i)_{i\in I})$, isto é, $\sum_{i\in I} v_i = \sum_{i\in I} w_i$. Então $\sum_{i\in I}(v_i - w_i) = 0$. 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, $(v_i)_{i\in I} = (w_i)_{i\in I}$. ∎

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*

$$v_{i_1} + \cdots + v_{i_r} \quad (i_k \in I, v_{i_k} \in M_{i_k}).$$

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

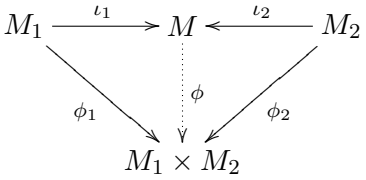
$$v_{j_n} = \sum_{m\in\overline{r}} (w_{i_m} - v_{i_m}) + \sum_{m\in\overline{t}} w_{k_m} - \sum_{m\in\overline{s}, m\neq n} v_{j_m}$$

está na intersecção

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

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 2.3). 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 2.3, 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.

Exercício 2.4. 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 $M_1 \cap M_2 = \{0\}$.)

Exercício 2.5. Uma sucessão de homomorfismos de A-módulos

$$M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \xrightarrow{\phi_3} \cdots \xrightarrow{\phi_n} M_{n+1}$$

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.

Exercício 2.6. (**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.

Exercício 2.7. (**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. 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,

$$M \simeq \frac{A}{\mathrm{an}(v)}$$

onde o ideal $\mathrm{an}(v) = N(\phi) = \{a \in A \mid av = 0\}$ é o chamado *anulador* de v. Se $\mathrm{an}(v) = \{0\}$, 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 $\mathrm{Tor}\,(M)$ (*torção* de M). Assim,

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

Exercício 3.1. 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 ?

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 $a_1 x_1 + \cdots + a_r x_r$.

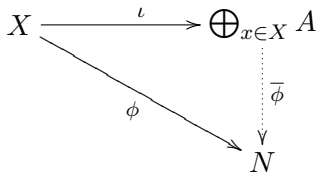
Note que este módulo é um módulo livre pois tem uma base evidente (a *base canónica*): $\{e_x \mid x \in X\}$ onde cada $e_x = (a_y)_{y\in X}$ é definido por

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

(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:*

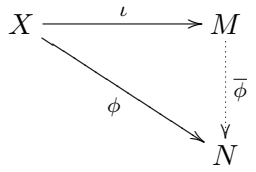
(i) *M é livre.*

(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,

$$a_1e_{x_1} + a_2e_{x_2} + \cdots + a_ne_{x_n} = 0.$$

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, como o exercício seguinte mostra.

Exercício 3.2. 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:

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

(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.

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

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

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), $|I| = |J|$. ∎

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

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

[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.

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 3.3 abaixo, $m = n$. ∎

Exercício 3.3. 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 $m = n$.

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]):

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

$$av + a_1 v_1 + \cdots + a_n v_n \quad (a, a_i \in D, v_i \in X)$$

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

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 (1), 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, $f_{m-1} - s_mf_m = 0$, 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

Vimos no Exercício 3.1 que em geral $\operatorname{Tor}(M)$ não é um submódulo de M. No entanto, isso altera-se se o anel for um domínio de integridade:

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 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). ∎

Assim, nesta secção os anéis considerados são sempre domínios de integridade. Este caso é muito importante em Álgebra Linear, como veremos.

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) 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

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

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

Portanto, todo o D-módulo livre é livre de torção.

(2) No entanto, o recíproco desta última afirmação é falso. Por exemplo, o $\mathbb{Z}$-módulo $\mathbb{Q}$ é livre de torção uma vez que para $n \in \mathbb{Z}$ e $\frac{p}{q} \in \mathbb{Q} \setminus \{0\}$,

$$n\frac{p}{q} = 0 \Leftrightarrow np = 0 \Rightarrow n = 0,$$

mas não é um $\mathbb{Z}$-módulo livre: por um lado, quaisquer dois racionais são linearmente dependentes, pois

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

mas 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.

Exercício 4.1. 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.

Exercício 4.2. 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

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

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 $\mathcal{B} = \{v_1, \ldots, v_n\}$ linearmente independente maximal. Para cada $s \in S$ existem $a_s, a_{1,s}, \ldots, a_{n,s} \in D$ $(a_s \neq 0)$ tais que

$$a_s s = a_{1,s}v_1 + \cdots + a_{n,s}v_n \tag{5.1.1}$$

(o caso $s \in \mathcal{B}$ é trivial e o caso em que $s \in S \setminus \mathcal{B}$ é consequência do facto do conjunto $\{v_1, \ldots, v_n, s\}$ ser linearmente dependente). Como M é livre de torção e

$$a := \prod_{s \in S} a_s \neq 0,$$

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 $s \in S$,

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

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. ∎

Observações. (1) No caso dos espaços vectoriais sobre um corpo K, como $D = K$ é um corpo, em (5.1.1) a_s é invertível e podemos concluir imediatamente que

$$s = (a_s^{-1}a_{1,s})v_1 + (a_s^{-1}a_{2,s})v_2 \cdots + (a_s^{-1}a_{n,s})v_n$$

e a demonstração fica terminada. No entanto, no caso mais geral de D ser um DIP, não podemos usar este argumento, e a demonstração a partir daqui tem que divergir da do teorema de existência de bases em espaços vectoriais (sobre um corpo) de tipo finito.
(2) A inclusão $\phi(M) \subseteq \bigoplus_{i=1}^n Dv_i$ acima é uma igualdade? O seguinte exemplo mostra que temos que ser muito cuidadosos com estes pormenores:

Nos grupos abelianos (isto é, $\mathbb{Z}$-módulos), seja $M = \mathbb{Z}$ e $\phi\colon \mathbb{Z} \to \mathbb{Z}$ definido por $\phi(n) = 2n$. Trata-se de um homomorfismo injectivo e $\phi(M) = 2\mathbb{Z}$. Claro que

M tem a base $\{1\}$; por outro lado, $\phi(M)$ tem a base $\{2\}$ (em particular, significa imediatamente que $\phi(M) \cong \mathbb{Z}$). Temos então

$$M = \mathbb{Z} \cong 2\mathbb{Z} = \phi(M) \subsetneq \mathbb{Z}.$$

Este exemplo mostra como poderemos ter um módulo N estritamente contido em M e isomorfo a M.

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.

Denotemos por $M_n(D)$ o anel das matrizes $n \times n$ com entradas num DIP D.

Exercício 5.1. Seja A um anel comutativo com identidade. Mostre que $\mathrm{End}_A(A^n)$ é isomorfo ao anel $M_n(A)$.

Duas matrizes $A, B \in M_n(D)$ dizem-se *equivalentes*, e escreve-se $A \sim B$, se existem matrizes invertíveis $P, Q \in M_n(D)$ tais que $B = Q^{-1}AP$.

Exercício 5.2. Mostre que a relação $\sim$ é uma relação de equivalência em $M_n(D)$.

Observação. Sejam $\widehat{V} = (\hat{v}_1, \hat{v}_2 \ldots, \hat{v}_n)$ e $\widehat{W} = (\hat{w}_1, \hat{w}_2 \ldots, \hat{w}_n)$ duas bases do D-módulo livre D^n. Existem escalares $a_{ij} \in D$ tais que

$$\hat{v}_i = \sum_{j=1}^{n} a_{ji}\hat{w}_j, \quad (i = 1, \ldots, n).$$

Em termos matriciais, denotando a matriz (a_{ij}) por A, temos

$$\widehat{V} = \widehat{W}A.$$

Se mudarmos para novas bases $\widehat{V}' = (\hat{v}'_1, \ldots, \hat{v}'_n)$ e $\widehat{W}' = (\hat{w}'_1, \ldots, \hat{w}'_n)$ (com matrizes de mudança de base P e Q, respectivamente), então

$$\hat{v}'_i = \sum_{j=1}^{n} p_{ji}\hat{v}_j, \quad \hat{w}'_i = \sum_{j=1}^{n} q_{ji}\hat{w}_j,$$

isto é,

$$\widehat{V}P = \widehat{V}' \quad \text{e} \quad \widehat{W}Q = \widehat{W}'.$$

Juntando tudo obtemos

$$\widehat{V}' = \widehat{W}AP = \widehat{W}'Q^{-1}AP,$$

o que significa que a matriz $B = Q^{-1}AP$ é a matriz da base $\widehat{V}'$ em função de $\widehat{W}'$.

Necessitaremos dos seguintes resultados sobre diagonalização de matrizes em $M_n(D)$, que não demonstraremos em pormenor. Recorde que um *menor* de uma matriz A é o determinante de alguma submatriz quadrada de A (obtida de A mediante eliminação de uma ou mais linhas ou colunas).

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 máximo divisor comum dos menores de dimensão i da matriz A*).

Proposição 5.4. *Toda a matriz $A \in M_n(D)$ é equivalente a uma matriz*

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

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

(À matriz diagonal 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, teremos que mostrar que 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 $d_1 \mid d_2 \mid \cdots \mid d_n$. Limitamo-nos a indicar um algoritmo (de "eliminação") que permite obter a diagonalização através de operações elementares nas linhas e colunas da matriz A (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:

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

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

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

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

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

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

Seja então $A = (a_{ij})$ 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 (com uma operação elementar do tipo 2) podemos supor que esta entrada é a_{12}. Se $d = \mathrm{mdc}(a_{11}, a_{12})$, existem $r, s, p, q \in D$ tais que $a_{12} = rd$, $a_{11} = sd$ e $pa_{11} + qa_{12} = d$. As matrizes

$$P = \begin{pmatrix} p & r & & \\ q & -s & & \\ & & 1 & \\ & 0 & & \ddots \\ & & & & 1 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} s & r & & \\ q & -p & & \\ & & 1 & \\ & 0 & & \ddots \\ & & & & 1 \end{pmatrix},$$

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:

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

Exercício 5.3. Diagonalize as seguintes 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 $\mathbb{R}[x]$.

Exercício 5.4. Determine as formas normais das seguintes matrizes em $\mathbb{Z}$:

(a) $\begin{pmatrix} -1 & 1 & -2 \\ 0 & -1 & 4 \\ 0 & 0 & 1 \end{pmatrix}$.

(b) $\begin{pmatrix} 0 & 0 & 0 & -8 \\ 1 & 0 & 0 & 16 \\ 0 & 1 & 0 & -14 \\ 0 & 0 & 1 & 6 \end{pmatrix}$.

Exercício 5.5. Mostre que se p é um primo, as seguintes duas matrizes de $M_n(\mathbb{Z}_p)$ são equivalentes:

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

Recordemos o anulador de $v \in M$ da página 62:

$$\operatorname{an}(v) = \{a \in D \mid av = 0\}.$$

Como se trata de um ideal então $\operatorname{an}(v) = \langle d \rangle$ 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 $D/\operatorname{an}(v) = D/\langle d \rangle$.

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, de característica r. Então*

$$M = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle \oplus \langle v_{n+1} \rangle \oplus \cdots \oplus \langle v_{n+r} \rangle,$$

onde $\operatorname{an}(v_1) \supseteq \operatorname{an}(v_2) \supseteq \cdots \supseteq \operatorname{an}(v_n)$ *e* $\operatorname{an}(v_{n+i}) = \{0\}$ $(i = 1, \ldots, r)$. *Escrevendo* $\operatorname{an}(v_i) = \langle d_i \rangle$, *temos um isomorfismo*

$$\begin{aligned} M &\simeq \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_n \rangle} \oplus \frac{D}{\langle d_{n+1} \rangle} \oplus \cdots \oplus \frac{D}{\langle d_{n+r} \rangle} \\ &\simeq \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_n \rangle} \oplus \underbrace{D \oplus \cdots \oplus D}_{r \text{ parcelas}} \end{aligned}$$

onde $d_1 \mid d_2 \mid \cdots \mid d_n$. *A lista de ideais* $\langle d_1 \rangle, \ldots, \langle d_{n+r} \rangle$ *é determinada univocamente por* M.

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

Demonstração. Já sabemos que se M tem característica r então

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

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

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

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

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

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

[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).

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 $\mathrm{an}(w'_i) = \langle d_i \rangle$:

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

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 que provaremos mais adiante (Observação 5.11). ∎

Em conclusão, a lista de factores invariantes dos módulos de tipo finito sobre um DIP (isto é, os n elementos $d_1 \mid d_2 \mid \cdots \mid d_n$ e os r zeros $d_{n+1} = \cdots = d_{n+r} = 0$) forma 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 $\mathrm{an}(v) = \langle ab \rangle$ e $\mathrm{mdc}\,(a, b) = 1$, 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 $\mathrm{an}(v_1) = \langle a \rangle$, $\mathrm{an}(v_2) = \langle b \rangle$ e $\mathrm{mdc}\,(a, b) = 1$, então*

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

Demonstração. (1) Seja $M = \langle v \rangle$ com $\mathrm{an}(v) = \langle ab \rangle$. Claro que, como $\mathrm{an}(v)$ 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 $\mathrm{an}(v_1) = \langle a \rangle$ e $\mathrm{an}(v_2) = \langle b \rangle$. 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 $\mathrm{an}(v) = \langle ab \rangle$, pelo que $D/\langle ab \rangle \simeq \langle v \rangle$. Mas $\langle v \rangle = M$, pois

$$v_1 = (ra + sb)v_1 = sbv_1 = sbv \quad \text{e} \quad v_2 = (ra + sb)v_2 = rav_2 = rav.$$

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*

$$M = \langle w_1 \rangle \oplus \langle w_2 \rangle \oplus \cdots \oplus \langle w_t \rangle \oplus L \simeq \frac{D}{\langle p_1^{n_1} \rangle} \oplus \frac{D}{\langle p_2^{n_2} \rangle} \oplus \cdots \oplus \frac{D}{\langle p_t^{n_t} \rangle} \oplus L,$$

onde L é um submódulo livre de dimensão igual à característica de M, $\operatorname{an}(w_i) = \langle p_i^{n_i} \rangle$*, $n_i \in \mathbb{N}$ e os elementos $p_1, \ldots, p_t \in D$ são primos (não necessariamente distintos). Os ideais $\langle p_i^{n_i} \rangle$ são determinados univocamente (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

$$M \simeq \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_n \rangle} \oplus \underbrace{D \oplus \cdots \oplus D}_{r \text{ parcelas}}$$

a decomposição de M em factores cíclicos invariantes. Basta então tomar para L o módulo livre (de dimensão r) $D \oplus \cdots \oplus D$. Por outro lado, se $p_1^{n_1}, \ldots, p_t^{n_t}$ são as potências primas que entram nas decomposições primas dos $d_1, \ldots, d_n$, o Lema 5.8 assegura que

$$\frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_n \rangle} \simeq \frac{D}{\langle p_1^{n_1} \rangle} \oplus \cdots \oplus \frac{D}{\langle p_t^{n_t} \rangle}.$$

Portanto,

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

Quanto à unicidade, sejam

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

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

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

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 $\mathrm{an}(v_t) = \langle p^{n_t}\rangle$, 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.* ∎

Exercício 5.6. Mostre que $M = \bigoplus_{p \text{ primo}} M(p)$ se $\mathrm{Tor}M = M$.

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

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

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

$$\begin{array}{cccc} p_1^{n_{11}} & p_2^{n_{12}} & \cdots & p_m^{n_{1m}} \\ p_1^{n_{21}} & p_2^{n_{22}} & \cdots & p_m^{n_{2m}} \\ \vdots & \vdots & & \vdots \\ p_1^{n_{s1}} & p_2^{n_{s2}} & \cdots & p_m^{n_{sm}} \end{array}$$

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

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

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

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

Se a dimensão da parte livre L é r, então acrescentamos à lista dos d_i's os elementos $d_{s+1} = \cdots = d_{s+r} = 0$ 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.

Exercício 5.7. 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.

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

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

Exercício 5.8. Sejam M_1 e M_2 dois D-módulos cíclicos de ordens a e b, respectivamente. Mostre que se $\text{mdc}(a, b) \neq 1$, então os factores invariantes de $M_1 \oplus M_2$ são $\text{mdc}(a, b)$ e $\text{mmc}(a, b)$.

Exercício 5.9. Determine todos os grupos abelianos de ordem 120.

Exercício 5.10. 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 $\text{an}(v) = \langle (x - \lambda)^m \rangle$. Mostre que os elementos

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

formam uma base de V sobre K.

Exercício 5.11. Seja $T\colon V \to V$ uma transformação linear de um espaço vectorial de dimensão finita sobre um corpo K, e $d_1(x) \mid \cdots \mid d_s(x)$ os factores invariantes do $K[x]$-módulo V. A $m(x) = d_s(x)$ chama-se *polinómio mínimo* de T e a $p(x) = d_1(x)\cdots d_s(x)$ chama-se *polinómio característico* de T. Mostre que:

(1) $m(x) \neq 0$, $m(T) = 0$ e que se $q(x)$ é um polinómio tal que $q(T) = 0$ então $m(x) \mid q(x)$.

(2) $p(x) \neq 0$, $p(T) = 0$ e $p(x) = \det(xI - T)$.

Exercício 5.12. Seja $T\colon V \to V$ uma transformação linear de um espaço vectorial de dimensão finita sobre um corpo K. Utilizando a decomposição em factores cíclicos invariantes de V como um $K[x]$-módulo, mostre que existe uma base $\{e_1, \ldots, e_n\}$ de V sobre K em relação à qual a matriz de T é

$$R = \begin{pmatrix} R_1 & 0 & \cdots & 0 \\ 0 & R_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & R_m \end{pmatrix}.$$

onde cada R_i é uma matriz $(n_i \times n_i)$ da forma

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 0 & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & -a_{n_i-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n_i-1} \end{pmatrix}.$$

A matriz R chama-se *forma canónica racional* de T.

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 onde primo=irredutível 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.

Exercício 6.1. 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.

Proposição 6.2. *Se*

$$0 \longrightarrow M_1 \xrightarrow{\iota} M_2 \xrightarrow{\pi} M_3 \longrightarrow 0$$

é uma sequência exacta de A-módulos, então M_2 é noetheriano se e só se M_1 e M_3 são noetherianos.

Demonstração. Como ι é injectiva, M_1 é isomorfo ao submódulo $N = \iota(M_1)$ de M_2. Por outro lado, como π é sobrejectiva, pelo Primeiro Teorema do Isomorfismo,

$$M_3 \simeq M_2/N(\pi) = M_2/\iota(M_1) = M_2/N.$$

Basta então provarmos que M_2 é noetheriano se e só se N e M_2/N são noetherianos:

A implicação $\Rightarrow$ já foi provada no Exercício 6.1. Reciprocamente, se S é um submódulo de M_2, temos que mostrar que S é de tipo finito:

Como $(S + N)/N$ é um submódulo de M_2/N, é de tipo finito. Pelo Segundo Teorema do Isomorfismo, $(S + N)/N \simeq S/(S \cap N)$, logo $S/(S \cap N)$ é de tipo finito. Mas $S \cap N$ é um submódulo de N logo também é de tipo finito. Então, pelo Exercício 6.2, S é de tipo finito. ∎

Exercício 6.2. Mostre que se os módulos M/N e N são de tipo finito então M também é de tipo finito.

Corolário 6.3. *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.*

Demonstração. Basta demonstrar o caso $k = 2$ (o resto segue por indução). Se M_1 e M_2 são noetherianos, a sequência exacta (recorde o Exercício 2.5(b))

$$0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$$

mostra que $M_1 \oplus M_2$ é noetheriano. Se $M = M_1 + M_2$ e $\pi\colon M_1 \oplus M_2 \to M$ é o homomorfismo definido por $\pi(v_1, v_2) = v_1 + v_2$, então a sequência exacta

$$0 \longrightarrow N(\pi) \longrightarrow M_1 \oplus M_2 \xrightarrow{\pi} M \longrightarrow 0$$

mostra que M também é notheriano. ∎

Pela proposição 6.1, se M é um A-módulo noetheriano, então M é de tipo finito. O recíproco também é válido desde que A seja noetheriano:

Corolário 6.4. *Seja A um anel noetheriano. Se M é um A-módulo de tipo finito, então M é noetheriano.*

Demonstração. Seja $\{v_1, \ldots, v_n\}$ um conjunto gerador de M e seja

$$\pi\colon \bigoplus_{i=1}^{n} A \to M$$

o homomorfismo definido por

$$\pi(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i v_i.$$

A sequência

$$0 \longrightarrow N(\pi) \longrightarrow \bigoplus_{i=1}^{n} A \xrightarrow{\pi} M \longrightarrow 0$$

é exacta e, pelo corolário anterior, $\bigoplus_{i=1}^{n} A$ é noetheriano. Logo, pela proposição, M é noetheriano. ∎

Exercício 6.3. Mostre que um anel A é noetheriano se e só se todo o ideal $I \subseteq A$ é finitamente gerado.

Exercício 6.4. 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.

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

Teorema 6.5 (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,

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

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 $p_{ji}(x)$ em I da forma

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

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 (portanto, $a \in I_k$). 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, pois nesse caso $o \neq a \in I_0$.
- $\boxed{\text{Hipótese de indução:}}$ 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 $a \in I_k \subseteq I_{k_0}$. 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 $a \in I_k = I_{k_0}$. 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 6.6. *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 6.5, 6.6).

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.

Exercício 6.5. 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:

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

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

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

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.

Exercício 6.6. 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.

Exercício 6.7. Mostre que em $\mathbb{Z}$, sendo $p_1^{n_1} \cdots p_t^{n_t}$ a factorização prima de a, então

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

Exercício 6.8. 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

1.1. **(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 $v = (v_1, v_1, v_1, \ldots, v_1)$ $(v_1 \in \mathbb{R})$.

2.1. Seja S um submódulo de M/N. Consideremos $S' = \{v \in M \mid v + N \in S\}$. Claro que $N \subseteq S'$ e S' é um submódulo de M:

- $0 \in S'$ pois $0 + N = 0 \in S$.
- Se $v_1, v_2 \in S'$ então $(v_1 - v_2) + N = (v_1 + N) - (v_2 + N) \in S$.
- Se $a \in A$ e $v \in S'$ então $(av) + N = a(v + N) \in S$.

Além disso, $S = S'/N$. Reciprocamente, para qualquer submódulo S' de M que contém N, S'/N é um submódulo de M/N. Portanto, o conjunto de submódulos de M/N coincide com o conjunto dos módulos S'/N onde S' é um submódulo de M que contém N.

2.2. **(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)

$$\phi\colon N \to \prod_{i\in I} M_i \quad \text{e} \quad \psi\colon \prod_{i\in I} M_i \to N$$

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 $\prod_{i\in I} M_i$.

2.3. **(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).

2.6. **(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).

2.7. **(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).

3.1. **(b)** Pode não ser, como veremos na demonstração da Proposição 4.1: só conseguimos garantir isso caso A seja um domínio de integridade. Tente encontrar um contra-exemplo.

3.2. **(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:

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

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

3.3. **(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

$$B_1C_1 = I_{n\times n} \quad \text{e} \quad B_2C_2 = I_{(m-n)\times(m-n)}.$$

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 $BC = I_{m\times m}$.

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

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

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 e procedemos do seguinte modo:

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

  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

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

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

  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

  $$P_2^{-1} A P_1 = \begin{pmatrix} 2 & 1 \\ -5 & -3 \end{pmatrix} \begin{pmatrix} 12 & 0 \\ -20 & -38 \end{pmatrix} = \begin{pmatrix} 4 & -38 \\ 0 & 114 \end{pmatrix}.$$

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

  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

  $$P_2^{-1} A P_1 P_3 = \begin{pmatrix} 4 & -38 \\ 0 & 114 \end{pmatrix} \begin{pmatrix} -9 & -19 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ -114 & -228 \end{pmatrix}.$$

  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 <u>linhas</u>, a primeira corresponde a multiplicar à <u>esquerda</u> pela matriz $Q_1 = T_{21}(57) = I + 57E_{21}$, enquanto a segunda corresponde a multiplicar, também à <u>esquerda</u>, pela matriz $Q_2 = D_2(-1) = I - 2E_{22}$:

  $$Q_2 Q_1 P_2^{-1} A P_1 P_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 57 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ -114 & -228 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 228 \end{pmatrix}.$$

- Concluindo,

  $$P = P_1 P_3 = \begin{pmatrix} 1 & 1 \\ -2 & -3 \end{pmatrix} \begin{pmatrix} -9 & -19 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} -10 & -21 \\ 21 & 44 \end{pmatrix}$$

  e

  $$Q^{-1} = Q_2 Q_1 P_2^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 57 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -5 & -3 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -109 & -54 \end{pmatrix}.$$

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

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

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

  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,

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

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

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

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

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

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

5.7. 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

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

5.8. Como $\mathrm{mdc}(a,b) \neq 1$, as decomposições primas de a e b contêm pelo menos um primo comum. Sejam $p_1, \ldots, p_t$ esses primos comuns, $q_1, \ldots, q_k$ os restantes primos em a (caso existam) e $r_1, \ldots, r_l$ os restantes primos em b (caso existam). Portanto,

$$a = p_1^{n_1} \times \cdots \times p_t^{n_t} \times q_1^{m_1} \times \cdots \times q_k^{m_k}$$

e

$$b = p_1^{n_1'} \times \cdots \times p_t^{n_t'} \times r_1^{m_1'} \times \cdots \times r_l^{m_l'}$$

com $n_i, m_i, n_i', m_i' \in \mathbb{N}$. Como

$$M_1 \simeq \frac{D}{\langle a\rangle} \quad \text{e} \quad M_2 \simeq \frac{D}{\langle b\rangle}$$

então

$$M_1 \oplus M_2 \simeq \frac{D}{\langle p_1^{n_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle q_k^{m_k}\rangle} \oplus \frac{D}{\langle p_1^{n'_1}\rangle} \oplus \cdots \oplus \frac{D}{\langle r_l^{m'_l}\rangle}.$$

Portanto, os divisores elementares de $M_1 \oplus M_2$ são

$$p_1^{n_1}, \ldots, p_t^{n_t}, p_1^{n'_1}, \ldots, p_t^{n'_t}, q_1^{m_1}, \ldots, q_k^{m_k}, r_1^{m'_1}, \ldots, r_l^{m'_l}.$$

Consequentemente, os factores invariantes são

$$p_1^{\min(n_1,n'_1)} \times \cdots \times p_t^{\min(n_t,n'_t)} = \mathrm{mdc}(a,b)$$

$$p_1^{\max(n_1,n'_1)} \times \cdots \times p_t^{\max(n_t,n'_t)} \times q_1^{m_1} \times \cdots \times r_l^{m'_l} = \mathrm{mmc}(a,b).$$

Nota: O que muda no caso $\mathrm{mdc}(a,b) = 1$? Nesse caso as famílias de primos que aparecem nas decomposições de a e de b são disjuntas pelo que $t = 0$, os divisores elementares são

$$q_1^{m_1}, \ldots, q_k^{m_k}, r_1^{m'_1}, \ldots, r_l^{m'_l}$$

, potências de primos todos distintos, pelo que só há um factor invariante:

$$q_1^{m_1} \times \ldots \times q_k^{m_k} \times r_1^{m'_1} \times \ldots \times r_l^{m'_l} = ab.$$

5.9. 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).
- $\begin{bmatrix} 2 & \times & 3^0 & \times & 5^0 & = & 2 \\ 2^2 & \times & 3 & \times & 5 & = & 60 \end{bmatrix}$, que corresponde ao grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_{60}$.
- $\begin{bmatrix} 2 & \times & 3^0 & \times & 5^0 & = & 2 \\ 2 & \times & 3^0 & \times & 5^0 & = & 2 \\ 2 & \times & 3 & \times & 5 & = & 30 \end{bmatrix}$, que corresponde ao grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$.

6.1. 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 $N \subseteq S' \subseteq M$ (recorde o Exercício 2.1). 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.

6.2. Seja $\{v_1, \ldots, v_m\} \subseteq M$ tal que $\{v_1 + N, \ldots, v_m + N\}$ é um conjunto gerador de M/N e seja $\{v'_1, \ldots, v'_n\}$ um conjunto gerador de N. Para cada $v \in M$, podemos escrever

$$v + N = \sum_{i=1}^{m} a_i(v_i + N) = (\sum_{i=1}^{m} a_i v_i) + N.$$

Portanto, $v - \sum_{i=1}^{m} a_i v_i \in N$, pelo que existem $b_j \in A$ tais que

$$v - \sum_{i=1}^{m} a_i v_i = \sum_{j=1}^{n} b_j v'_j.$$

Logo

$$v = \sum_{i=1}^{m} a_i v_i + \sum_{j=1}^{n} b_j v'_j,$$

o que mostra que $\{v_1, \ldots, v_m, v'_1, \ldots, v'_n\}$ é um conjunto gerador de M.

6.4. **(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 $x = f^k(y) = 0$.

6.5. **(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.

6.6. **(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 $q(a) = 0$.

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

6.8. (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):

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