Notas de Fundamentos de Álgebra

Pedro F. dos Santos, Joana Ventura

2014

Índice

Introdução

Estas notas foram escritas para a disciplina de Fundamentos de Álgebra (FA), do Mestrado em Matemática e Aplicações do Instituto Superior Técnico e contêm a matéria leccionada durante os primeiros semestres de 2010/2011 e de 2014/15.

Actualmente, esta disciplina é direccionada a dois perfis distintos de alunos. Para os alunos que tenham iniciado o 1º ciclo de estudos na Licenciatura em Matemática Aplicada e Computação é a segunda disciplina de Álgebra abstracta e, como tal, deve aprofundar o seu conhecimento de estruturas algébricas introduzidas na disciplina de Introdução à Álgebra (IA) – grupos e anéis – e estudar novas estruturas – módulos e álgebras. Para os alunos do Mestrado em Matemática e Aplicações que não tenham tido contacto anterior com a álgebra abstracta, FA tem que cumprir o objectivo adicional de servir de introdução a esta área da matemática.

O objectivo deste texto é proporcionar aos alunos da disciplina uma fonte unificada de estudo que seja apropriada para os dois perfis de alunos a que a disciplina se dirige.

O programa da disciplina é o seguinte:

I. Teoria elementar de grupos: subgrupos, subgrupos normais; isomorfismos. Grupos quociente, isomorfismos canónicos. Acções de grupos; teoremas de Sylow.

II. Teoria elementar de anéis: subanéis, ideais e anéis quociente. Anéis de polinómios, fracções, domínios de factorização única, domínios de ideais principais, domínios euclidianos.

III. Teoria elementar de módulos: módulos finitamente gerados e módulos livres. Produto tensorial. Sucessões exactas, Hom e dualidade. Módulos sobre domínios integrais e sobre domínios de ideais principais. Aplicações: classificação de grupos abelianos finitamente gerados, forma canónica de Jordan.

Nos capítulos 1, 2 e 4 cobrem-se os tópicos do programa. No Capítulo 3 discutem-se brevemente algumas noções e exemplos básicos de Teoria das Categorias com o objectivo dar uma visão unificada do estudo das várias estruturas algébricas do programa. Nas duas lições que restavam após o tratamento dos tópicos do programa (Capítulo 5 e final do Capítulo 4) optou-se por discutir brevemente a teoria de estrutura de anéis como tópico suplementar (para o que foi necessário estudar módulos Noetherianos, Artinianos e semi-simples, no final do Capítulo 4). Esta opção tem a vantagem de ser fácil de implementar no tempo disponível e de ser intelectualmente satisfatória por fornecer alguma teoria de estrutura para a categoria dos anéis, à semelhança do que é feito no Capítulo 1 para grupos. No ano de 2014/15, nas duas lições finais, optou-se por uma introdução à teoria de representação de grupos finitos (Capítulo 6), fazendo uma abordagem (quase) sem referência aos teoremas de estrutura de módulos semi-simples do Capítulo 5 para, deste modo, ser possível escolher tópicos suplementares de forma independente.

De maneira geral, usa-se Hungerford [**Hun74**] e Serre [**Ser77**] como referência. A outra referência utilizada é o livro de Rui Loja Fernandes e Manuel Ricou [**FR04**].

Grupos

1. Grupos e monóides: definições básicas

Definição 1.1. *Uma* operação binária *num conjunto S é uma função*

$$S \times S \to S$$
$$(x, y) \mapsto xy$$

(a) a operação diz-se associativa *se*

$$(xy)z = x(yz), \qquad \forall\, x, y, z \in S.$$

Neste caso, S diz-se um semi-grupo*;*

(b) a operação tem identidade *se existir um elemento $\mathbf{1} \in S$ tal que*

$$\mathbf{1}x = x\mathbf{1} = x, \qquad \forall\, x \in S.$$

Diz-se que $\mathbf{1}$ é o elemento identidade de S ou a identidade de S. Por vezes escreve-se $\mathbf{1}_S$ para distinguir das identidades de outras operações.

Se a operação satisfaz (a) e (b), S diz-se um monóide*;*

(c) a operação diz-se comutativa *ou* abeliana *se*

$$xy = yx, \qquad \forall\, x, y \in S;$$

(d) se S é um monóide, diz-se que $x \in S$ tem inverso *se existir $y \in S$ tal que*

$$xy = yx = \mathbf{1};$$

(e) se S é um monóide tal que todos os elementos têm inverso, diz-se que S é um grupo*.*

Proposição 1.2. *Seja S um semi-grupo. Então*

(a) se S tem identidade, esta é única;

(b) se S é um monóide e $x \in S$ tem inverso, este é único.

Notação 1.3.

1. Se $\star$: $S \times S \to S$ é uma operação binária em S, utiliza-se a notação $(S, \star)$ para denotar o conjunto S munido da estrutura dada pela operação $\star$, que pode ser de grupo, monóide, semi-grupo, etc.
2. No caso de operações abelianas é habitual usar o símbolo $+$ para a operação e $\mathbf{0}$ para a identidade, a que também se chama *zero*. Esta notação designa-se por *aditiva*.
3. A notação utilizada na Definição 1.1, em que a operação de grupo é representada por justaposição ($(x, y) \mapsto xy$), designa-se *multiplicativa*.

4. Em notação multiplicativa, denota-se o inverso de um elemento x por x^{-1}.
5. Em notação aditiva, denota-se por $-x$ o inverso de um elemento x.

Proposição 1.4. *Seja S um monóide e sejam $a, b \in S$ elementos invertíveis. Então*

(i) a^{-1} é invertível e $(a^{-1})^{-1} = a$;
(ii) ab é invertível e $(ab)^{-1} = b^{-1}a^{-1}$.

Como consequência desta última proposição, dado um monóide S, temos que o conjunto $S^\times := \{a \in S \mid a \text{ é invertível}\}$ é um grupo para a mesma operação de S.

Definição 1.5. *Se $(G, \cdot)$ é um grupo, define-se*

$$x^n := \begin{cases} \overbrace{x \cdots x}^{n \text{ vezes}} & n > 0 \\ \mathbf{1} & n = 0 \\ \underbrace{x^{-1} \cdots x^{-1}}_{-n \text{ vezes}} & n < 0. \end{cases}$$

Se $(G, +)$ é um grupo abeliano, define-se

$$nx := \begin{cases} \overbrace{x + \cdots + x}^{n \text{ vezes}} & n > 0 \\ 0 & n = 0 \\ \underbrace{-x - \cdots - x}_{-n \text{ vezes}} & n < 0. \end{cases}$$

Exemplos 1.6.

1. $(\mathbb{N}, +)$ é um semi-grupo abeliano;
2. $(\mathbb{N}_0, +)$ é um monóide abeliano;
3. $(\mathbb{Z}, +)$ é um grupo abeliano;
4. $(\mathbb{Z}, \cdot)$ é um monóide abeliano e $\mathbb{Z}^\times = \{\pm 1\}$;
5. $\mathbb{K}^\times := (\mathbb{K} \setminus \{0\}, \cdot)$ é um grupo abeliano, onde $\cdot$ denota a operação de multiplicação e $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$;
6. o conjunto das matrizes reais $n \times n$, $M_n(\mathbb{R})$, com a operação de multiplicação, é um monóide não abeliano. O mesmo é verdade para $M_n(\mathbb{K})$ com $\mathbb{K} = \mathbb{Q}, \mathbb{C}$ ou $\mathbb{Z}$.

Exemplo 1.7. O conjunto

$$\{f \colon \{1, \ldots, n\} \to \{1, \ldots, n\} \mid f \text{ é bijectiva}\},$$

com a operação de composição é um grupo, que é não abeliano se $n > 2$ – Exercício 1.1.3. Este grupo designa-se *grupo simétrico* de ordem n e denota-se por S_n.

Notação 1.8.

1. Dados $\sigma, \tau \in S_n$, escreve-se $\sigma\tau$ para denotar a composição $\sigma \circ \tau$;
2. o elemento $i \mapsto \sigma(i)$ é por vezes denotado por $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$;
3. a notação $\sigma = (\, i_1 \; i_2 \; \cdots \; i_k \,)$ denota a permutação

$$\begin{aligned} i_1 &\mapsto i_2 \\ i_2 &\mapsto i_3 \\ &\vdots \\ i_k &\mapsto i_1. \end{aligned}$$

Permutações deste tipo denominam-se *permutações cíclicas* ou *ciclos*. Se $k = 2$, diz-se que σ é uma *transposição*.

Exercícios

1.1.1. Demonstre as Proposições 1.2 e 1.4.

1.1.2. Seja G um semigrupo. Mostre que G é um grupo sse as seguintes condições se verificam:
(i) $\exists\, e \in G\ \forall\, a \in G\ ea = a$ (identidade à esquerda) e
(ii) $\forall\, a \in G\ \exists\, b \in G\ ba = e$ (inverso à esquerda).
Sugestão: Assumindo (i) e (ii), mostre primeiro que $a^2 = a \Rightarrow a = e$.

1.1.3. Mostre que o conjunto $\{f\colon \{1,\ldots,n\} \to \{1,\ldots,n\} \mid f \text{ é bijectiva}\}$, com a operação de composição é um grupo, que é não abeliano se $n > 2$ – Ver Exemplo 1.7.

1.1.4. Seja $\sigma \in S_n$. Mostre que
(a) $\exists \sigma_1, \ldots, \sigma_k$ permutações cíclicas disjuntas[1] *t.q.* $\sigma = \sigma_1 \cdots \sigma_k$.
(b) Se $\sigma \in S_n$ é uma permutação cíclica, então σ é um produto de transposições.

1.1.5. Seja $\sigma = (i_1\ i_2\ \cdots\ i_r) \in S_n$ um ciclo. Mostre que $\tau\sigma\tau^{-1} = (\tau(i_1)\ \tau(i_2)\ \cdots\ \tau(i_r))$, para todo o $\tau \in S_n$.

1.1.6. Seja D_3 o conjunto das isometrias de um triângulo equilátero (isometrias do plano que deixam o triângulo invariante) munido da operação de composição. Sejam $\sigma, \tau \in D_3$, respectivamente uma reflexão em torno de um eixo de simetria e uma rotação de $2\pi\mathrm{i}/3$ em torno do centro do triângulo. Mostre que os elementos de D_3 se podem escrever de forma única como $\sigma^i\tau^j$, $i = 0, 1$, $j = 0, 1, 2$.

1.1.7. Seja G um grupo tal que $a^2 = \mathbf{1}$ para todo o $a \in G$. Mostre que G é abeliano

1.1.8. Seja G um grupo finito contendo um número par de elementos. Mostre que existe $a \in G \setminus \{\mathbf{1}\}$ tal que $a^2 = \mathbf{1}$.

[1] $\sigma, \tau \in S_n$ dizem-se disjuntas se $\{i \mid \sigma(i) \neq i\} \cap \{i \mid \tau(i) \neq i\} = \varnothing$

2. Operações definidas por passagem ao quociente

Recorde-se que uma relação de equivalência num conjunto X é uma relação[2] $\sim$ tal que

(i) $x \sim x$, $\forall x \in X$ (reflexividade);

(ii) $x \sim y \Rightarrow y \sim x$, $\forall x, y \in X$ (simetria);

(iii) $x \sim y \ \wedge \ y \sim z \Rightarrow x \sim z$, $\forall x, y, z \in X$ (transitividade).

O conjunto das classes de equivalência desta relação denota-se $X/\sim$ ou X/R e designa-se *quociente de X por $\sim$*.

Definição 2.1. *Seja S um semi-grupo. Uma* relação de conguência *em S é uma relação de equivalência $\sim$ tal que*

$$x_1 \sim x_2 \ \wedge \ y_1 \sim y_2 \ \Rightarrow \ x_1 y_1 \sim x_2 y_2.$$

(ou seja, $\sim$ preserva a operação de S.)

Proposição 2.2. *Seja R uma relação de congruência num semi-grupo S. Então S/R é um semi-grupo. Se S é abeliano, S/R também o é. Analogamente, S/R é um grupo (monóide) se S o é.*

Demonstração. Denotando por $[x]$ a classe de equivalência de $x \in S$, define-se

$$[x][y] \coloneqq [xy]. \qquad \square$$

Exemplo 2.3. Seja $m \in \mathbb{N}$. Consideremos a relação de equivalência em $\mathbb{Z}$ dada por: $x \sim y \Leftrightarrow m \mid (x - y)$. Designamos o conjunto das classes de equivalência por $\mathbb{Z}_m$. Designamos a classe de x por $\underline{x}$. Temos

- $\mathbb{Z}_m = \{\underline{0}, \underline{1}, \ldots, \underline{m-1}\}$ (m elementos);
- $\underline{x_1} + \underline{x_2} \coloneqq \underline{x_1 + x_2}$ define um grupo abeliano, pois

$$\begin{aligned} x_1 \sim x_2 \ \wedge \ y_1 \sim y_2 &\Leftrightarrow m \mid x_2 - x_1 \ \wedge \ m \mid y_2 - y_1 \\ &\Rightarrow m \mid (x_2 + y_2 - (x_1 + y_1)) \\ &\Leftrightarrow x_1 + y_1 \sim x_2 + y_2. \end{aligned}$$

Notação 2.4. Diz-se que $\mathbb{Z}_m$ é o *grupo dos inteiros módulo m*.

Observação 2.5. Os elementos de $\mathbb{Z}_m$ são os restos da divisão por m e a operação em $\mathbb{Z}_m$ consiste em somar em $\mathbb{Z}$ e tomar o resto da divisão por m.

Exemplo 2.6. $\mathbb{Z}_2 = \{\underline{0}, \underline{1}\}$. A tabela de adição é:

$$\begin{aligned} \underline{0} + \underline{0} &= \underline{0} \\ \underline{1} + \underline{0} &= \underline{1} \\ \underline{1} + \underline{1} &= \underline{0}. \end{aligned}$$

Exercícios

1.2.1. Mostre que $\mathbb{Z}_m$ é um monóide abeliano para a seguinte operação:

$$\underline{a}\,\underline{b} \coloneqq \underline{ab},$$

e que se verfica a propriedade *distributiva*:

$$\underline{a}(\underline{b} + \underline{c}) = \underline{a}\,\underline{b} + \underline{a}\,\underline{c} \quad \forall\, \underline{a}, \underline{b}, \underline{c} \in \mathbb{Z}_m.$$

[2] Uma relação num conjunto X é um subconjunto $R \subset X \times X$. Dizemos que x e y estão em relação se $(x, y) \in R$. Frequentemente usamos um símbolo, como $\sim$, para representar a relação e escrevemos $x \sim y$ para denotar que x e y estão em relação.

1.2.2. Considere o grupo aditivo $(\mathbb{Q}, +)$ e mostre que:
   (a) a relação definida por $a \sim b \Leftrightarrow a - b \in \mathbb{Z}$ é uma relação de congruência;
   (b) o conjunto das classes de equivalência $\mathbb{Q}/\mathbb{Z}$ é um grupo abeliano infinito.

1.2.3. Seja p um número primo e defina-se $\mathbb{Z}(p^\infty) \subset \mathbb{Q}/\mathbb{Z}$ por

$$\mathbb{Z}(p^\infty) = \left\{ \left[\frac{a}{p^n} \right] \in \mathbb{Q}/\mathbb{Z} \mid a \in \mathbb{Z}, n \geq 0 \right\} .$$

Mostre que $\mathbb{Z}(p^\infty)$ é um grupo infinito para a operação soma de $\mathbb{Q}/\mathbb{Z}$.

3. Homomorfismos de grupos

Definição 3.1. *Sejam G, H grupos. Uma função $f\colon G \to H$ diz-se um* homomorfismo de grupos *se*

$$\forall x, y \in G \quad f(xy) = f(x)f(y)$$

(ou seja, f preserva produtos).

Se f é um homomorfismo bijectivo, diz-se que é um isomorfismo de grupos. *Se $H = G$ e f é um isomorfismo, i.e., se $f\colon G \to G$ é um isomorfismo, f diz-se um* automorfismo *de G.*

Notação 3.2. Para denotar que dois grupos, G e H, são isomorfos, escreve-se $G \cong H$. O conjunto dos automorfismos do grupo G denota-se por $\mathrm{Aut}(G)$.

Exemplos 3.3.

1. $\mathrm{GL}_n(\mathbb{C}) \coloneqq \{A \in M_n(\mathbb{C}) \mid A \text{ é invertível}\}$, com a operação de produto de matrizes, é um grupo e $\det\colon \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ é um homomorfismo de grupos, pois
$$\det(AB) = \det A \det B.$$
O homomorfismo det não pode ser um isomorfismo se $n > 1$ porque $M_n(\mathbb{C})$ não é abeliano nesse caso.
2. $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ é um isomorfismo.
3. Seja $G = \{z \in \mathbb{C} \mid z^m = 1\} \subset \mathbb{C} \setminus \{0\}$. G tem m elementos:
$$z_k = \exp\left(\frac{2\pi k \mathrm{i}}{m}\right), \qquad k = 0, \ldots, m-1,$$
e é um grupo abeliano para a multiplicação de números complexos. A função
$$\begin{aligned} f\colon \mathbb{Z}_m &\to G \\ \underline{k} &\mapsto \exp\left(\frac{2\pi \mathrm{i}}{m}\right) \end{aligned}$$
é um isomorfismo de grupos.

Exemplo 3.4. A função $f\colon \mathbb{Z} \to \mathbb{Z}_m; k \mapsto \underline{k}$ define um homomorfismo sobrejectivo de grupos, chamado homomorfismo *canónico* ou *projecção canónica*.

Exemplo 3.5. Sejam $k, m \in \mathbb{N}$, a função $f\colon \mathbb{Z}_k \to \mathbb{Z}_{km}; \underline{j} \mapsto \underline{jm}$ está bem definida:

$$f(\underline{j + rk}) = \underline{jm + rkm} = \underline{jm} = f(\underline{j}).$$

e é um homomorfismo:

$$f(\underline{j} + \underline{j'}) = f(\underline{j + j'}) = \underline{(j + j')m} = \underline{jm} + \underline{j'm} = f(\underline{j}) + f(\underline{j'}).$$

Vejamos que f é injectivo,

$$f(\underline{j}) = f(\underline{j'}) \Leftrightarrow \underline{jm} = \underline{j'm} \Leftrightarrow km \mid (jm - j'm) \Leftrightarrow k \mid (j - j') \Leftrightarrow \underline{j} = \underline{j'}.$$

Definição 3.6. *Seja $f\colon G \to H$ um homomorfismo de grupos. Define-se*

- $\ker f \coloneqq \{x \in G \mid f(x) = \mathbf{1}_H\} \subset G$;
- $\mathrm{im}\, f \coloneqq \{f(x) \mid x \in G\} \subset H$.

Diz-se que $\ker f$ *é o* núcleo *de f e* $\mathrm{im}\, f$ *é a* imagem *de f.*

Definição 3.7. *Seja G um grupo e seja $\varnothing \neq H \subset G$ um subconjunto fechado para o produto (*i.e., *$a, b \in H \Rightarrow ab \in H$). Se H é um grupo para a operação de G, diz-se que H é um* subgrupo *de G e denota-se $H < G$.*

Proposição 3.8. *Seja G um grupo e seja $H \subset G$ tal que $H \neq \varnothing$. Então $H < G$* sse *$\forall x, y \in H, xy^{-1} \in H$.*

Exemplo 3.9. Seja $G = \mathbb{Z}$, $m \in \mathbb{N}$ e $H = m\mathbb{Z} \subset \mathbb{Z}$. Temos $H < \mathbb{Z}$.

Exemplo 3.10. $\mathbb{R}^\times < \mathbb{C}^\times$.

Exemplo 3.11. Seja $H = \{\underline{0}, \underline{2}\} \subset \mathbb{Z}_4$. Temos $H < \mathbb{Z}_4$.

Proposição 3.12. *Seja $f\colon G \to H$ um homomorfismo de grupos. Então* $\ker f$ *é um subgrupo de G e* $\operatorname{im} f$ *é um subgrupo de H.*

Demonstração. Basta aplicar a Proposição 3.8. Note que $\ker f \neq \varnothing$ e $\operatorname{im} f \neq \varnothing$ pois $f(\mathbf{1}_G) = \mathbf{1}_H$ (pelo Exercício 1.3.1), logo $\mathbf{1}_G \in \ker f$ e $\mathbf{1}_H \in \operatorname{im} f$. □

Teorema 3.13. *Seja $f\colon G \to H$ um homomorfismo de grupos. Temos*

(a) f é injectivo sse $\ker f = \{\mathbf{1}\}$*;*

(b) f é um isomorfismo sse *existe um homomorfismo $g\colon H \to G$* t.q. *$f \circ g = \mathrm{id}_H$ e $g \circ f = \mathrm{id}_G$.*

Demonstração.

(a) Note-se que $\{\mathbf{1}\} < \ker f$. Temos
$\boxed{\Rightarrow}$ $f(x) = \mathbf{1} \Rightarrow x = \mathbf{1}$ pois f é injectiva.
$\boxed{\Leftarrow}$ $f(x) = f(x') \Rightarrow f(x^{-1}x') = \mathbf{1} \Rightarrow x^{-1}x' = \mathbf{1} \Leftrightarrow x' = x$.

(b) Exercício. □

Exemplo 3.14. Sejam $k, m \in \mathbb{N}$. Recorde-se o homomorfismo $f\colon \mathbb{Z}_k \to \mathbb{Z}_{km}; \underline{j} \mapsto \underline{jm}$. Concluímos que $\{\underline{0}, \underline{m}, \ldots, \underline{(k-1)m}\} = \operatorname{im} f < \mathbb{Z}_{km}$.

Exemplo 3.15. Seja $m \in \mathbb{N}$. O subgrupo $m\mathbb{Z} < \mathbb{Z}$ é o núcleo da projecção canónica $\mathbb{Z} \to \mathbb{Z}_m$.

Exemplo 3.16. Considere-se a aplicação $\varphi\colon S_n \to \mathrm{GL}_n(\mathbb{R})$ dada por

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \mapsto \varphi(\sigma) = \left(e_{\sigma(1)} \cdots e_{\sigma(n)}\right).$$

Ou seja, $\varphi(\sigma)$ representa a transformação linear $e_i \mapsto e_{\sigma(i)}$. Desta definição segue $\varphi(\sigma\tau)(e_i) = e_{\sigma(\tau(i))}$. Temos

$$\varphi(\sigma)\varphi(\tau)(e_i) = \varphi(\sigma)(e_{\tau(i)}) = e_{(\sigma(\tau(i))},$$

pelo que φ é um homomorfismo. Como $\det(\varphi(\sigma)) \in \mathbb{Z}^\times = \{\pm 1\} < \mathbb{R}^\times$ e $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ é um homomorfismo,

$$\det\circ\varphi\colon S_n \to \mathbb{Z}^\times$$

é também um homomorfismo, a que se chama *sinal* e que se costuma denotar por sgn.

Definição 3.17. *O* grupo alternado *é o seguinte subgrupo de S_n:*

$$A_n \coloneqq \ker(\det\circ\varphi\colon S_n \to \mathbb{Z}^\times).$$

Observação 3.18. Os elementos de A_n dizem-se permutações pares, os de $S_n \setminus A_n$ dizem-se permutações ímpares – ver Exercício 1.3.9.

Proposição 3.19. *Seja G um grupo e sejam $H_i < G$, $i \in I$. Então $\cap_{i\in I} H_i < G$.*

Definição 3.20. *Seja G um grupo e seja $X \subset G$, define-se*

$$\langle X \rangle \coloneqq \bigcap_{H<G, X\subset H} H.$$

Diz-se que $\langle X \rangle$ é o subgrupo de G gerado por X.

Exemplo 3.21. Seja $G = \mathbb{Z}$ e $X = \{m\}$. Temos $\langle X \rangle = m\mathbb{Z}$.

Notação 3.22. Se $X = \{x\}$ escreve-se $\langle x \rangle$ em vez de $\langle\{x\}\rangle$. Da mesma forma, escreve-se $\langle x_1, \ldots, x_n \rangle$ em vez de $\langle\{x_1, \ldots, x_n\}\rangle$.

Teorema 3.23. *Seja G um grupo e seja $X \subset G$, então*

$$\langle X \rangle = \left\{ a_1^{n_1} \cdots a_k^{n_k} \mid k \in \mathbb{N}, a_1 \ldots, a_k \in X, n_1, \ldots, n_k \in \mathbb{Z} \right\}.$$

Exemplo 3.24. Seja $G = \mathbb{Z}$ e $X = \{2, 3\}$, então $\langle X \rangle = \mathbb{Z}$ pois $1 = 3 - 2 \in \langle X \rangle$.

Exercícios

1.3.1. Seja $f : G \to H$ um homomorfismo de grupos. Mostre que $f(\mathbf{1}_G) = \mathbf{1}_H$ e que $f(a^{-1}) = f(a)^{-1}$ para todo o $a \in G$. Mostre, através de um exemplo, que a primeira afirmação pode ser falsa se G e H são monóides que não são grupos.

1.3.2. Mostre que um grupo G é abeliano *sse* $f : G \to G$, $f(x) = x^{-1}$ é um automorfismo.

1.3.3. Mostre que $D_3 \cong S_3$.

1.3.4. Demonstre a Proposição 3.8.

1.3.5. Mostre que todos os subgrupos de $\mathbb{Z}$ são da forma dos do Exemplo 3.9.

1.3.6. Mosre que conjunto $\{\sigma \in S_n \mid \sigma(n) = n\}$ é um subgrupo isomorfo a S_{n-1}.

1.3.7. Seja $f \colon G \to H$ um homomorfismo de grupos e seja $J < H$. Define-se

$$f^{-1}(J) \coloneqq \{x \in G \mid f(x) \in J\}.$$

Mostre que $f^{-1}(J) < G$.

1.3.8. Seja G um grupo e $\mathrm{Aut}(G)$ o conjunto dos automorfismos de G. Mostre que $\mathrm{Aut}(G)$ é um grupo com a operação de composição.

1.3.9. (Ver Exercício 1.1.4 e Definição 3.17.)

(a) Seja $\sigma \in S_n$. Mostre que $\sigma \in A_n$ *sse*

$$\sigma = \sigma_1 \cdots \sigma_r, \text{ onde } \sigma_i \text{ são transposições} \quad \Rightarrow \quad r \text{ é par.}$$

(b) Mostre que, se $\sigma_i, \tau_j \in S_n$ são transposições, então

$$\sigma_1 \cdots \sigma_r = \tau_1 \cdots \tau_s, \quad \Rightarrow \quad r \text{ e } s \text{ são ambos pares ou ímpares.}$$

1.3.10. Seja G um grupo e sejam $H_i < G$, $i \in I$.

(a) Demonstre a Proposição 3.19, i.e., mostre que $\cap_{i \in I} H_i < G$.

(b) Mostre que $\cup_{i \in I} H_i$ não é subgrupo em geral.

1.3.11. Demonstre o Teorema 3.23.

1.3.12. (a) Seja G o grupo, para a multiplicação de matrizes, gerado pelas matrizes complexas

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \text{e} \qquad B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

onde $i^2 = -1$. Mostre que G é um grupo não abeliano contendo 8 elementos.
Sugestão: Verifique que $BA = A^3B$, portanto qualquer elemento de Q_8 é da forma A^iB^j. Verifique também que $A^4 = B^4 = I \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ é a identidade de G.

(b) Mostre que $\mathbb{H}_8 \coloneqq \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}$ é um grupo, onde $\mathbb{H}$ é o conjunto dos quaterniões.

(c) Seja $Q_8 = \langle a, b \mid a^2 = b^2, a^4 = 1, bab^{-1} = a^{-1} \rangle$. Mostre que $G \cong \mathbb{H}_8 \cong Q_8$.

A qualquer um destes grupos chamamos *grupo quaternião*, que geralmente é denotado por Q_8 independentemente da sua apresentação.

1.3.13. Mostre que o subgrupo aditivo $\mathbb{Z}(p^\infty)$ de $\mathbb{Q}/\mathbb{Z}$ (ver Exercício 1.2.3) é gerado pelo conjunto $\left\{ \left[\frac{1}{p^n} \right] \mid n \in \mathbb{N} \right\}$.

4. Grupos cíclicos

Definição 4.1. *Um grupo G diz-se* finitamente gerado *se existem $a_1, \ldots, a_n \in G$* t.q. *$G = \langle a_1, \ldots, a_n \rangle$. Neste caso, $a_1, \ldots, a_n$ dizem-se geradores de G. Se se existe $a \in G$* t.q. *$G = \langle a \rangle$, G diz-se cíclico.*

Observação 4.2. Os grupos cíclicos são abelianos.

Exemplo 4.3. $\mathbb{Z}$, $\mathbb{Z}_m$ são grupos cíclicos.

A proposição seguinte mostra que todos os grupos cíclicos são desta forma.

Proposição 4.4. *Seja G um grupo cíclico, então $G \cong \mathbb{Z}$ ou $G \cong \mathbb{Z}_m$, para algum $m \in \mathbb{N}$.*

Demonstração. Seja $x \in G$ um gerador de G. Consideremos $f\colon \mathbb{Z} \to G$ *t.q.* $f(j) \coloneqq x^j$. Claramente f é sobrejectivo:

$$\forall\, j_1, j_2 \in \mathbb{Z}, \qquad f(j_1 + j_2) = x^{j_1+j_2} = x^{j_1} x^{j_2}.$$

Seja m *t.q.* $\ker f = \langle m \rangle = m\mathbb{Z}$. Se $m = 0$, $G \cong \mathbb{Z}$. Se $m > 0$, então o homomorfismo

$$\begin{aligned} \underline{f}\colon \mathbb{Z}_m &\to G \\ \underline{j} &\mapsto x^j, \end{aligned}$$

está bem definido e é sobrejectivo. Vejamos que é também injectivo:

$$\underline{f}(\underline{j}) = \mathbf{1} \Leftrightarrow x^j = 1 \Leftrightarrow j \in \langle m \rangle \Leftrightarrow \underline{j} = 0.$$

Concluímos que $G \cong \mathbb{Z}_m$. □

Observação 4.5.

1. Se $f\colon G \to H$ é um homomorfismo e G é cíclico então $\operatorname{im} f$ é cíclico;
2. se $a \in G$, $\langle a \rangle$ é um subgrupo cíclico de G;
3. se $f\colon G \to H$ é um homomorfismo e $a \in G$, então $f(\langle a \rangle) = \langle f(a) \rangle$.

Definição 4.6. *Seja G um grupo e seja $a \in G$. A* ordem *de G é a sua cardinalidade $|G|$. A* ordem *de a é a ordem do grupo $\langle a \rangle$, e denota-se este número por $|a|$. Ou seja, $|a| = |\langle a \rangle|$.*

Exemplo 4.7. Seja $G = \{z \in \mathbb{C} \mid |z| = 1\} < \mathbb{C}^\times$ e seja $a = \exp(2\pi \mathrm{i}/3) \in G$. Então $|a| = 3$. Se $a' = \exp(\pi \mathrm{i} x)$ com $x \in \mathbb{R} \setminus \mathbb{Q}$ então $|a'| = \infty$.

Proposição 4.8. *Seja G um grupo e seja $a \in G$. Se $|a| = \infty$, então*

i. $a^k = \mathbf{1} \Leftrightarrow k = 0$;
ii. $a^k = a^m \Leftrightarrow k = m, \forall m, k \in \mathbb{Z}$;

Se $|a| = m \in \mathbb{N}$, então

i. $m = \min\{k \in \mathbb{N} \mid a^k = \mathbf{1}\}$;
ii. $a^k = \mathbf{1} \Leftrightarrow m \mid k$;
iii. $a^r = a^s \Leftrightarrow \underline{r} = \underline{s}$ *em* $\mathbb{Z}_m$ i.e., $r \equiv s \mod m$;
iv. $\langle a \rangle = \{\mathbf{1}, a, a^2, \ldots, a^{m-1}\}$;
v. $\forall k \in \mathbb{N},\ k \mid m \Rightarrow |a^k| = \frac{m}{k}$.

A proposição seguinte mostra que todos os subgrupos de grupos cíclicos são igualmente cíclicos.

Proposição 4.9. *Seja G um grupo cíclico, seja $a \in G$ um gerador e seja $\{\mathbf{1}\} \neq H < G$. Então $H = \langle a^m \rangle$ onde $m = \min\{k \in \mathbb{N} \mid a^k \in H\}$.*

Proposição 4.10. *Seja G um grupo cíclico de ordem finita m e seja $k \in \mathbb{N}$ t.q. $k \mid m$. Então G tem exactamente um subgrupo (cíclico) de ordem k.*

O teorema seguinte identifica o conjunto dos geradores de um grupo cíclico.

Teorema 4.11. *Seja $G = \langle a \rangle$ um grupo cíclico.*

1. *Se $|G| = \infty$ os geradores de G são a e a^{-1}.*
2. *Se $|G| = m$, os geradores de G são os elementos de $\{a^k \mid \text{MDC}(k, m) = 1\}$.*

Demonstração.

1. Claramente a e a^{-1} são geradores. Se $G = \langle b \rangle$ então $b = a^m$ para algum m, logo $\langle b \rangle = \{a^{mk} \mid k \in \mathbb{Z}\}$. Logo, se $m \neq \pm 1$, temos $\langle b \rangle \neq G$, pois a tem ordem infinita.
2. Recorde-se que $\text{MDC}(k, m) = 1 \Leftrightarrow \exists r, s : rk + sm = 1$, logo
$$a = (a^k)^r (a^m)^s \Rightarrow G = \langle a \rangle \subset \langle a^k \rangle.$$
Reciprocamente, se $\langle a^k \rangle = G$ existe r *t.q.* $a^{rk} = a$, ou equivalentemente
$$rk \equiv 1 \mod m \Leftrightarrow \exists s : rk + sm = 1. \qquad \square$$

Exercícios

1.4.1. (a) Mostre que $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.
(b) Mostre que $\text{Aut}(\mathbb{Z}_m) \cong (\mathbb{Z}_m^\times, \cdot)$, para $m \in \mathbb{N}$.
Sugestão: Quais os geradores de $\mathbb{Z}_m$?
(c) Seja G um grupo cíclico. Conclua que $\text{Aut}(G)$ é um grupo abeliano. Será $\text{Aut}(G)$ sempre cíclico?

1.4.2. Demonstre a Proposição 4.8.

1.4.3. Seja G um grupo e $a, b, c \in G$. Mostre que $|a| = |a^{-1}|$, $|ab| = |ba|$ e $|cac^{-1}| = |a|$.

1.4.4. Seja G um grupo abeliano, $a, b \in G$ com $|a| = n$ e $|b| = m$. Mostre que G contém um elemento de ordem $\text{MMC}(n, m)$.
Sugestão: Considere primeiro o caso em que $\text{MDC}(n, m) = 1$.

1.4.5. Seja G um grupo abeliano de ordem pq onde p e q são coprimos. Supondo que exitem $a, b \in G$ tais que $|a| = p$ e $|b| = q$, mostre que G é cíclico.

1.4.6. Seja $f : G \to H$ um homomorfismo, seja $a \in G$ tal que $f(a)$ tem ordem finita em H. Mostre que ou $|a|$ é infinita ou $|f(a)|$ divide $|a|$.

1.4.7. (a) Considere o grupo $G = GL_2(\mathbb{Q})$. Mostre que $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ tem ordem 4 e $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ tem ordem 3, mas AB tem ordem infinita em G.
(b) Reciprocamente, mostre que o grupo aditivo[3] $\mathbb{Z}_2 \times \mathbb{Z}$ contém elementos não nulos a e b de ordem infinita tais que $a + b$ tem ordem finita.

1.4.8. Demonstre as Proposições 4.9 e 4.10.

1.4.9. Considere novamente o grupo $\mathbb{Z}(p^\infty)$ do Exercício 1.2.3 e seja $H < \mathbb{Z}(p^\infty)$. Demonstre as seguintes afirmações:
(a) Qualquer elemento de $\mathbb{Z}(p^\infty)$ tem ordem finita p^n, para algum $n \geq 0$.
(b) Se pelo menos um elemento de H tem orden p^k e nenhum elemento de H tem ordem maior do que p^k, então H é o grupo cíclico gerado por $[\frac{1}{p^k}]$ e, portanto, $H \cong \mathbb{Z}_{p^k}$.

[3] Se G e H são grupos, o conjunto $G \times H$ é um grupo com a operação definida componente a componente, e identidade $(\mathbf{1}_G, \mathbf{1}_H)$.

(c) Se o conjunto das ordens dos elementos de H não é majorado, então $H = \mathbb{Z}(p^\infty)$.

(d) Os únicos subgrupos próprios de $\mathbb{Z}(p^\infty)$ são os grupos cíclicos $C_n = \langle [\frac{1}{p^n}] \rangle$, para $n \in \mathbb{N}$. Além disso, $\langle 0 \rangle = C_0 < C_1 < C_2 < \cdots$.

(e) Sejam $x_1, x_2, \ldots$ elementos de um grupo abeliano G tal que $|x_1| = p$, $px_2 = x_1$, $px_3 = x_2$, ..., $px_{n+i} = x_n$, ... O subgrupo gerado pelos x_i, para $i \geq 1$, é isomorfo a $\mathbb{Z}(p^\infty)$.
Sugestão: Verifique que a aplicação dada por $x_i \mapsto [\frac{1}{p^i}]$ está bem definida e é um isomorfismo.

1.4.10. Mostre que um grupo que possua apenas um número finito de subgrupos é finito.

1.4.11. Seja G um grupo abeliano e defina-se $T = \{g \in G \mid |g| \text{ é finita}\}$. Mostre que T é um subgrupo[4] de G. Será a hipótese de G ser abeliano necessária?

1.4.12. Seja G um grupo infinito. Mostre que G é cíclico *sse* G é isomorfo a cada um dos seus subgrupos próprios.

[4]Este subgrupo chama-se o *subgrupo de torção* de G e também se denota por $\mathrm{Tor}(G)$.

5. Classes laterais esquerdas, quociente por um subgrupo

Definição 5.1. *Seja G um grupo, seja $H < G$ e sejam $a, b \in G$. Diz-se que a é* congruente *à esquerda com b módulo H se*

$$a^{-1}b \in H.$$

De forma análoga define-se congruência à direita módulo H: $ba^{-1} \in H$.

Proposição 5.2. *(1) A relação de congruência à esquerda (direita)* mod H *é uma relação de equivalência.*

(2) A classe de equivalência de $a \in G$ relativamente a esta relação de equivalência é o conjunto

$$aH \coloneqq \{ah \mid h \in H\} \subset G$$

(respectivamente, $Ha \coloneqq \{ha \mid h \in H\}$ para a congruência à direita).

(3) $|aH| = |Ha| = |H|$.

Os conjuntos, aH (Ha), $a \in G$, dizem-se classes laterais esquerdas *(respectivamente, direitas) de H em G.*

Notação 5.3. Se G é um grupo abeliano não há diferença entre classes laterais esquerdas e direitas. Neste caso, é frequente usar a notação aditiva $(G, +)$ e as classes laterais são então denotadas por $a + H$.

Recorde-se que as classes de equivalência de uma relação de equivalência $\sim$ num conjunto S formam uma partição de S: denotando $[a] = \{s \in S \mid s \sim a\}$, tem-se

a) $S = \bigcup_{a \in S} [a]$;
b) $a, b \in S \Rightarrow [a] \cap [b] = \varnothing \vee [a] = [b]$.

A primeira asserção é óbvia. A segunda é consequência da transitividade da relação:

$$c \in [a] \cap [b] \Rightarrow a \sim c \sim b \Rightarrow a \sim b.$$

Corolário 5.4. *Seja $H < G$, então as classes laterais esquerdas aH, $a \in G$, formam uma partição de G em conjuntos com o mesmo cardinal;*

Definição 5.5. *Denotamos por G/H o conjunto das classes esquerdas de H em G e por $[G : H]$ o seu cardinal: $[G : H] \coloneqq |G/H|$.*

Corolário 5.6. *Se $H < G$, temos*

$$|G| = [G : H]|H|.$$

Se $|G| < \infty$, então

- $\forall H < G,\ |H| \mid |G|$, *e*
- *(Teorema de Lagrange)* $\forall g \in G,\ |g| \mid |G|$.

Demonstração. A partição

$$G = \bigcup_{gH \in G/H} gH$$

dá uma bijecção $G \to G/H \times H$. □

Teorema 5.7. *Sejam $K < H < G$, então*

$$[G : K] = [G : H][H : K].$$

Demonstração. Caso G finito:

$$\begin{aligned} &|G| = [G:H]|H| \ \wedge \ |H| = [H:K]|K| \\ \Rightarrow &|G| = [G:H][H:K]|K| \\ \Rightarrow &[G:H][H:K] = [G:K]. \end{aligned}$$

□

Exemplo 5.8. Seja $G = S_3$ e $H = \langle(12)\rangle$. Então $|S_3| = [G:H]|H|$ e $|H| = 2$, logo $[G:H] = 3$.

Definição 5.9. *Seja G grupo e sejam $R_1, \ldots, R_k \subset G$. Define-se*

$$R_1 \cdots R_k \coloneqq \{r_1 \cdots r_k \mid r_1 \in R_1, \ldots, r_k \in R_k\} \subset G.$$

Teorema 5.10. *Sejam $H, K < G$* t.q. *H, K são finitos, então*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Demonstração. Seja $J = H \cap K$. Temos $J < H$ e

$$[H:J] = \frac{|H|}{|J|}.$$

Seja $H = h_1 J \cup \cdots \cup h_n J$ uma partição de H em classes esquerdas de J. Então

$$HK = (h_1 J \cup \cdots \cup h_n J)\, K = h_1 K \cup \cdots \cup h_n K$$

é uma partição, pois

$$h_i K = h_j K \Leftrightarrow h_i^{-1} h_j \in K \Rightarrow h_i^{-1} h_j \in J.$$

Concluímos que

$$|HK| = n|K| = [H:J]|K| = \frac{|H||K|}{|J|} = \frac{|H||K|}{|H \cap K|}.$$

□

Exercícios

1.5.1. Demonstre a Proposição 5.2.

1.5.2. Demonstre o Teorema 5.7 no caso de G infinito.

1.5.3. Seja G um grupo finito. Mostre que as seguintes afirmações são equivalentes:
(i) $|G|$ é primo;
(ii) $G \neq \{\mathbf{1}\}$ e G não contém subgrupos próprios;
(iii) $G \cong \mathbb{Z}_p$ para algum primo p.

1.5.4. (Pequeno Teorema de Fermat) Seja $a \in \mathbb{Z}$ e p um primo tal que $p \nmid a$. Mostre que $a^{p-1} \equiv 1 \pmod{p}$.

1.5.5. Prove que há apenas dois grupos de ordem 4, a menos de isomorfismos, nomeadamente $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Sugestão: use o Teorema de Lagrange para concluir que um grupo de ordem 4 que não é cíclico consiste na identidade e três elementos de ordem 2.

1.5.6. Sejam H, K subgrupos do grupo G. Mostre que HK é um subgrupo de G *sse* $HK = KH$.

1.5.7. Seja G um grupo de ordem $p^k m$, com p um primo e $\mathrm{MDC}(p, m) = 1$. Seja $H < G$ de ordem p^k e $K < G$ de ordem p^d, com $0 < d \leq k$, tal que $K \not\subset H$. Mostre que HK não é um subgrupo de G.

1.5.8. (a) Sejam H, K subgrupos do grupo G. Mostre que $[H : H \cap K] \leq [G:K]$. Se $[G:K]$ é finito, mostre que a igualdade verifica-se se e só se $G = HK$.
(b) Se H e K são subgrupos de índice finito no grupo G tais que $[G:H]$ e $[G:K]$ são coprimos, mostre que $G = HK$.

6. Subgrupos normais; grupo quociente

Em seguida estudamos a classe dos subrupos N de um grupo G para os quais as classes esquerdas e direitas coincidem.

Notação 6.1. *ASCSE* $\equiv$ *as seguintes condições são equivalentes.*

Teorema 6.2. *Seja G um grupo e seja $N < G$. ASCSE:*

a) as relações de congruência módulo N à esquerda e à direita coincidem;
b) $\forall\, g \in G\ gN = Ng$
c) $\forall\, g \in G\ \exists g' \in G$ t.q. $gN = Ng'$;
d) $\forall\, g \in G\ gNg^{-1} \subset N$;
e) $\forall\, g \in G\ gNg^{-1} = N$;

Demonstração.

$\boxed{a) \Leftrightarrow b)}$ exercício;

$\boxed{b) \Rightarrow c)}$ exercício;

$\boxed{c) \Rightarrow d)}$ $gN = Ng' \Rightarrow \exists\, n \in N : g = ng' \Rightarrow gNg^{-1} = Ng'g^{-1} = Ng'(g')^{-1}n^{-1} \subset N$;

$\boxed{d) \Rightarrow e)}$ $\forall\, g \in G,\ gNg^{-1} \subset N \Rightarrow \forall\, g \in G,\ N \subset g^{-1}Ng \Leftrightarrow \forall\, g \in G,\ N \subset gNg^{-1}$;

$\boxed{e) \Rightarrow b)}$ $\forall\, g \in G,\ gNg^{-1} = N \Leftrightarrow \forall\, g \in G,\ gN = Ng$. □

Definição 6.3. *Seja G um grupo e seja $N < G$. Diz-se que N é um subgrupo* normal *de G se satisfaz as condições equivalentes do teorema anterior e, nesse caso, escreve-se*

$$N \lhd G.$$

Observação 6.4. A propriedade de ser normal é uma propriedade da inclusão $N < G$, não é uma propriedade do grupo N.

Exemplo 6.5. Seja $\tau \in D_3$ *t.q.* $\tau^3 = 1$ (*cf.* Exercício 1.1.6), então $\langle \tau \rangle \lhd G$.

A importância dos subgrupos normais decorre do resultado seguinte.

Teorema 6.6. *Seja $N \lhd G$. Consideremos o conjunto G/N das classes esquerdas de N em G. Então G/N tem uma estrutura de grupo cuja operação é dada pela seguinte fórmula*

$$(gN)(g'N) \coloneqq gg'N.$$

Com esta estrutura a projecção canónica $\pi\colon G \to G/N$ é um homomorfismo sobrejectivo de grupos t.q. $\ker \pi = N$.

Demonstração.

1. A operação está bem definida: temos
$$(gnN)(g'n'N) = (gng'n')N.$$
Como $N \lhd G$, temos $ng' \in Ng' = g'N$, logo $\exists\, n'' \in N$ *t.q.* $ng' = g'n''$ e portanto,
$$(gng'n')N = (gg'n''n')N = gg'N.$$
2. As propriedades da operação em G/H seguem das propriedades da operação em G, *e.g.*,
$$(gN)(g^{-1}N) = \mathbf{1}N = N$$
$$(\mathbf{1}N)(gN) = gN = N = (gN)(\mathbf{1}N)$$
3. Por definição do produto em G/N, π é um homomorfismo.
4. $\pi(g) = N \Leftrightarrow gN = \mathbf{1}N \Leftrightarrow g \in N$. □

Proposição 6.7.

(a) $H, J \lhd G \Rightarrow H \cap J \lhd G$;

(b) $H \lhd G$ *e* $H < K < G \Rightarrow H \lhd K$;

(c) $H \lhd G, K < G \Rightarrow HK < G$.

O resultado seguinte caracteriza os subgrupos normais como os núcleos de homomorfismos.

Teorema 6.8. *Seja G um grupo. Então $H \lhd G$* sse *existe um homomorfismo de grupos $\phi\colon G \to K$, para algum grupo K,* t.q.

$$\ker \phi = H.$$

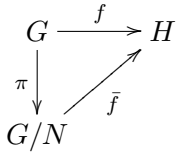
Demonstração. $\boxed{\Rightarrow}$ $H \lhd G \Rightarrow H = \ker(\pi\colon G \to G/H)$;

$\boxed{\Leftarrow}$ Seja $H = \ker \phi$. Temos

$$h \in H \Leftrightarrow \phi(h) = \mathbf{1} \Leftrightarrow \forall_{g\in G}\ \phi(g)\phi(h)\phi(g^{-1}) = \mathbf{1} \Leftrightarrow \forall_{g\in G}\ \phi\left(ghg^{-1}\right) = \mathbf{1}$$

$\therefore \quad \forall_{g\in G}\ gHg^{-1} = H.$ □

Teorema 6.9 (Propriedade universal do grupo quociente)**.** *Seja $f\colon G \to H$ um homomorfismo de grupos e seja $N \lhd G$* t.q. *$N < \ker f$. Então existe um homomorfismo $\bar{f}\colon G/N \to H$ que factoriza f como no diagrama seguinte*



onde $\pi\colon G \to G/N$ é a projecção canónica. Ou seja, tem-se a seguinte factorização

$$\boxed{f = \bar{f} \circ \pi}$$

Além disso, tem-se

$$\boxed{\operatorname{im} \bar{f} = \operatorname{im} f} \qquad e \qquad \boxed{\ker \bar{f} = \ker f/N}$$

onde usámos $\ker f/N$ *para denotar* $\pi(\ker f)$.

Demonstração. Define-se $\bar{f}(gN) \coloneqq f(g)$. Como $N < \ker f$ segue que $\bar{f}$ está bem definido:

$$\bar{f}\,(gnN) = f(gn) = f(g) = \bar{f}\,(gN)\,,$$

e é um homomorfismo porque $\bar{f}$ o é. Da definição de $\bar{f}$ segue que $f = \bar{f} \circ \pi$ e $\operatorname{im} \bar{f} = \operatorname{im} f$. Quanto ao núcleo, temos

$$\bar{f}(gN) = \mathbf{1} \Leftrightarrow f(g) = \mathbf{1} \Leftrightarrow g \in \ker f \Leftrightarrow gN \in \ker f/N.$$ □

Exercícios

1.6.1. Seja $H < G$ *t.q.* $[G : H] = 2$. Mostre que $H \lhd G$.

1.6.2. Demonstre a Proposição 6.7.

1.6.3. Mostre que $H \lhd G/N$ se e só se $H = K/N$ com $K \lhd G$ e $N < K$.

1.6.4. Seja $\{N_i \mid i \in I\}$ uma família de subgrupos normais de G. Mostre que $\cap_{i\in I} N_i \lhd G$.

1.6.5. Seja $H < S_4$ o subgrupo formado pelas permutações σ tais que $\sigma(4) = 4$. Será H normal em S_4?

1.6.6. Mostre que todos os subgrupos de Q_8 são normais.

1.6.7. Seja G um grupo finito, seja $H < G$ com $|H| = n$. Se H é o único subgrupo de G de ordem n, mostre que $H \lhd G$.

1.6.8. O *grupo diedral* é definido por $D_n \coloneqq \langle a, b \mid |a| = n, |b| = 2, bab = a^{-1} \rangle$. Mostre que
(a) $|D_n| = 2n$;
(b) $\langle a \rangle \lhd D_n$ e $D_n/\langle a \rangle \cong \mathbb{Z}_2$.

1.6.9. Seja G o subgrupo de S_n ($n \geq 3$) gerado pelas permutações $\sigma = (1\ 2\ \cdots\ n)$ e

$$\tau = \begin{cases} (2\ n)(3\ n-1)\cdots(\frac{n}{2}\ \frac{n}{2}+2) & \text{se } n \text{ é par} \\ (2\ n)(3\ n-1)\cdots(\frac{n+1}{2}\ \frac{n+1}{2}+1) & \text{se } n \text{ é ímpar} \end{cases}$$

(a) Mostre que[5] $G \cong D_n$. (Ver exercício anterior para a definição de D_n.)
Sugestão: Considere primeiro os casos particulares de $n = 4$ e $n = 5$, em seguida generalize para um n arbitrário.
(b) Será G normal em S_n?

1.6.10. (a) Dê exemplos de subgrupos H e K de D_4 tais que $H \lhd K$ e $K \lhd D_4$ mas $H \not\lhd D_4$.
(b) Se H é um subgrupo cíclico de um grupo G e $H \lhd G$, mostre que qualquer subgrupo de H é normal em G. (Compare com a alínea anterior.)

1.6.11. Seja $H < \mathbb{Z}(p^\infty)$ tal que $H \neq \mathbb{Z}(p^\infty)$, mostre que $\mathbb{Z}(p^\infty)/H \cong \mathbb{Z}(p^\infty)$.
Sugestão: Se $H = \langle [\frac{1}{p^n}] \rangle$, seja $x_i = [\frac{1}{p^{i+n}}]$ e use o Exercício 1.4.9(e).

[5] Se considerarmos um polígono regular de n lados com os vértices numerados consecutivamente de 1 a n, esta descrição de D_n corresponde a descrever as simetrias deste polígono através de permutações dos vértices, nomeadamente, σ é uma rotação de um ângulo $\frac{2\pi}{n}$ com centro no centro no polígono, e τ é uma reflexão em relação a um "diâmetro".

7. Teoremas de isomorfismo

Teorema 7.1 (1º Teorema do Isomorfismo)**.** *Um homomorfismo $f\colon G \to H$ induz um isomorfismo*

$$\bar{f}\colon \frac{G}{\ker f} \xrightarrow{\cong} \operatorname{im} f.$$

Demonstração. Aplicando o Teorema 6.9 com $N = \ker f$, obtemos $\operatorname{im} \bar{f} = \operatorname{im} f$ e $\ker \bar{f} = \{\mathbf{1}\}$, ou seja, $\bar{f}$ é um isomorfismo. □

Corolário 7.2 (2º Teorema do isomorfismo)**.** *Sejam $K < G$ e $N \lhd G$, então $N \cap K \lhd K$, $NK < G$ e*

$$\frac{K}{N \cap K} \cong \frac{NK}{N}.$$

Demonstração. Seja $\pi\colon G \to G/N$ a projecção canónica e seja $f\colon K \to G/N$ a sua restrição a K. Temos

$$\ker f = N \cap K \quad \text{e} \quad \operatorname{im} f = \pi(K) = \frac{KN}{N} = \frac{NK}{N},$$

logo $\bar{f}\colon K/N\cap K \to G/N$ induz um isomorfismo $K/N\cap K \cong NK/K$. Na igualdade $NK = KN$ usámos $N \lhd G$, que também implica $NK < G$ (Proposição 6.7). □

Teorema 7.3. *Sejam $H \lhd G$ e $K \lhd G$* t.q. *$K < H$. Então*

$$\frac{H}{K} \lhd \frac{G}{K} \quad e \quad \frac{G/K}{H/K} \cong \frac{G}{H}\ .$$

Demonstração. Temos

$$\forall_{h\in H}\, (gK)\,(hK)\left(g^{-1}K\right) = \left(ghg^{-1}\right)K \in H/K.$$

Sejam

$$\varrho_1\colon G \to \frac{G}{K}, \qquad \varrho_2\colon \frac{G}{K} \to \frac{G/K}{H/K}$$

as projecções canónicas. Consideremos $f = \varrho_2 \circ \varrho_1\colon G \to \frac{G/K}{H/K}$. Temos,

$$\ker f = \varrho_1^{-1}(\ker \varrho_2) = \varrho_1^{-1}(H/K) = H,$$

logo

$$\frac{G}{H} \cong \frac{G/K}{H/K}.$$ □

Nota 7.4. No teorema anterior, usámos H/K para denotar o subgrupo de G/K dado pela imagem de H pela aplicação canónica $G \to G/K$.

Exemplo 7.5. Seja $\varphi\colon \mathbb{R}^\times \to \mathbb{R}^\times; a \mapsto a^2$. Temos $\operatorname{im}\varphi = \mathbb{R}^+$ e $\ker\varphi = \{\pm 1\}$. Obtemos, $\bar{\varphi}\colon \mathbb{R}^\times/\{\pm 1\} \xrightarrow{\cong} (\mathbb{R}^+, \cdot)$.

8. Produto directo e produto semidirecto de grupos

Definição 8.1. *Sejam H, K grupos. O produto cartesiano $H \times K$ com a seguinte operação*

$$(h_1, k_1)(h_2, k_2) \coloneqq (h_1h_2, k_1k_2)$$

é um grupo, a que se chama produto directo *de H, K e que se denota $H \times K$.*

Exemplo 8.2. Consideremos $f\colon \mathbb{R}^\times \to \mathbb{Z}^\times \times \mathbb{R} \coloneqq (\{\pm 1\}, \cdot) \times (\mathbb{R}, +)$ dada por

$$f(x) \coloneqq \left(\frac{x}{|x|}, \log|x|\right), \qquad x \in \mathbb{R}^\times.$$

Denotando por $(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 + y_2)$ o produto em $\mathbb{Z}^\times \times \mathbb{R}$, temos

$$f(xy) = \left(\frac{xy}{|xy|}, \log|xy|\right) = \left(\frac{x}{|x|}, \log|x|\right)\left(\frac{y}{|y|}, \log|y|\right),$$

portanto, f é um homomorfismo de grupos $\mathbb{R}^\times \to \mathbb{Z}^\times \times \mathbb{R}$. Como f é bijectivo e $\mathbb{Z}^\times \cong \mathbb{Z}_2$, concluímos que

$$\mathbb{R}^\times \cong \mathbb{Z}_2 \times \mathbb{R}.$$

Exemplo 8.3. Sejam H, K grupos. No produto directo $G = H \times K$ é habitual identificar H com $H \times \{\mathbf{1}_K\}$ e K com $\{\mathbf{1}_H\} \times K$. Com estas identificações, temos

$$H \lhd G \quad \text{e} \quad K \lhd G.$$

De facto,

$$(h_1, k)(h_2, \mathbf{1}_K)(h_1^{-1}, k^{-1}) = (h_1 h_2 h_1^{-1}, k\mathbf{1}_K k^{-1}) = (h_1 h_2 h_1^{-1}, \mathbf{1}_K) \in H,$$

portanto $H \lhd G$. De forma análoga, mostra-se $K \lhd G$.

Observação 8.4. Uma propriedade importante do produto directo $G = H \times K$ é o facto de os elementos de H e K comutarem em G.

Definição 8.5. *Seja G um grupo e sejam $H, K < G$. Diz-se que G é o* produto directo interno *de H e K se as seguintes condições se verificam*

(i) $H \cap K = \{\mathbf{1}\}$

(ii) $hk = kh, \forall\, h \in H, \forall\, k \in K$

(iii) $G = HK$ *(ver Definição 5.9)*

Observação 8.6. Se G é o produto directo interno de H, K, tem-se $H \times K \cong G$. O isomorfismo é dado por $(h, k) \mapsto hk$.

Notação 8.7. Se $H, K < G$, escrevemos $G = H \times K$ para denotar que G é o produto directo interno de H e K.

Exemplo 8.8. Seja $G = O(3) = \{A \in M_3(\mathbb{R}) \mid AA^T = I\}$ e sejam

$$H = SO(3) \coloneqq \{A \in O(3) \mid \det A = 1\}$$
$$K = \{\pm I\} \cong \mathbb{Z}_2.$$

Temos

$$O(3) = SO(3) \times \{\pm I\}.$$

Exemplo 8.9. Seja $G = D_6 = \langle a, b \mid |a| = 6, |b| = 2, bab^{-1} = a^{-1}\rangle$ (ver Exercício 1.6.8) e sejam $A = \langle a^3\rangle$ e $B = \langle a^2, ab\rangle$. Então

$$D_6 = A \times B \cong \mathbb{Z}_2 \times D_3 \cong \mathbb{Z}_2 \times S_3\ .$$

Proposição 8.10. *Seja G um grupo e sejam $H, K < G$. Temos $G = H \times K$* sse *$H \lhd G$, $K \lhd G$, $H \cap K = \{\mathbf{1}_G\}$ e $G = HK$.*

Demonstração. $\boxed{\Rightarrow}$ Temos que provar $H \lhd G$ e $K \lhd G$. Sejam $g \in G$ e $x \in H$. Temos $g = hk$, com $h \in H$ e $k \in K$, logo

$$\begin{aligned} gxg^{-1} &= hkx\,(hk)^{-1} = hkxk^{-1}h^{-1} \\ &= hxh^{-1} \in H, \end{aligned}$$

portanto $H \lhd G$. Da mesma forma segue $K \lhd G$.

$\boxed{\Leftarrow}$ Temos que mostrar que os elementos de H comutam com K. De forma equivalente,

$$\forall h \in H, k \in K \qquad \underbrace{hkh^{-1}k^{-1}}_{g} = \mathbf{1}_G.$$

Ora,

$$k^{-1} \in K, \quad hkh^{-1} \in K \Rightarrow g \in K$$
$$h \in H, \quad kh^{-1}k^{-1} \in H \Rightarrow g \in H$$
$$\therefore g = \mathbf{1}_G. \qquad \square$$

Lema 8.11. *Sejam N, H grupos e $\theta : H \to \mathrm{Aut}(N)$ um homomorfismo de grupos. O produto cartesiano $N \times H$ com a seguinte operação*

$$(n_1, h_1)(n_2, h_2) = (n_1\theta(h_1)(n_2), h_1h_2) \quad \forall\, n_1, n_2 \in N \;\forall\, h_1, h_2 \in H$$

é um grupo.

Demonstração. A operação é associativa:

$$\begin{aligned}
(n_1, h_1)\big((n_2, h_2)(n_3, h_3)\big) &= (n_1, h_1)(n_2\theta(h_2)(n_3), h_2h_3) && \text{por definição}\\
&= (n_1\theta(h_1)(n_2\theta(h_2)(n_3)), h_1h_2h_3) && \text{por definição}\\
&= (n_1\theta(h_1)(n_2)\theta(h_1)(\theta(h_2)(n_3))), h_1h_2h_3) && \text{porque } \theta(h_1) \text{ é um homomorfismo}\\
&= (n_1\theta(h_1)(n_2)\theta(h_1h_2)(n_3)), h_1h_2h_3) && \text{porque } \theta \text{ é um homomorfismo,}\\
& && \text{logo } \theta(h_1) \circ \theta(h_2) = \theta(h_1h_2)\\
&= (n_1\theta(h_1)(n_2), h_1h_2)(n_3, h_3) && \text{por definição}\\
&= \big((n_1, h_1)(n_2, h_2)\big)(n_3, h_3) && \text{por definição}
\end{aligned}$$

A identidade é $(\mathbf{1}_N, \mathbf{1}_H)$:

$$(n, h)(\mathbf{1}_N, \mathbf{1}_H) = (n\theta(h)(\mathbf{1}_N), h\mathbf{1}_H) = (n\mathbf{1}_N, h) = (n, h)$$
$$(\mathbf{1}_N, \mathbf{1}_H)(n, h) = (\mathbf{1}_N\theta(\mathbf{1}_H)(n), \mathbf{1}_Hh) = (\mathbf{1}_N\,\mathrm{id}_N(n), h) = (n, h)$$

onde $\mathrm{id}_N : N \to N$ é o homomorfismo identidade, i.e, a identidade do grupo $\mathrm{Aut}(N)$.

O inverso de (n, h) é $(\theta(h^{-1})(n^{-1}), h^{-1})$:

$$\begin{aligned}
&(n, h)(\theta(h^{-1})(n^{-1}), h^{-1})\\
&\quad = (n\theta(h)(\theta(h^{-1})(n^{-1})), hh^{-1}) && \text{por definição}\\
&\quad = (n\theta(\mathbf{1}_H)(n^{-1}), \mathbf{1}_H) && \text{porque } \theta(h) \circ \theta(h^{-1}) = \theta(hh^{-1}) = \theta(\mathbf{1}_H)\\
&\quad = (\mathbf{1}_N, \mathbf{1}_H) && \text{porque } \theta(\mathbf{1}_H) = \mathrm{id}_N
\end{aligned}$$

e

$$\begin{aligned}
&(\theta(h^{-1})(n^{-1}), h^{-1})(n, h)\\
&\quad = (\theta(h^{-1})(n^{-1})\theta(h^{-1})(n), h^{-1}h) && \text{por definição}\\
&\quad = (\theta(h^{-1})(n^{-1}n), \mathbf{1}_H) && \text{porque } \theta(h^{-1}) \text{ é um homomorfismo}\\
&\quad = (\mathbf{1}_N, \mathbf{1}_H) && \text{porque } \theta(h^{-1}) \text{ é um homomorfismo} \qquad \square
\end{aligned}$$

Definição 8.12. *O grupo do lema anterior chama-se* produto semidirecto *de N por H e denota-se por $N \rtimes H$ ou $N \overset{\theta}{\rtimes} H$.*

Note que a ordem do produto semidirecto é $|N \rtimes H| = |N \times H| = |N||H|$.

Observação 8.13. Tal como no caso do produto directo, identificamos N com $N \times \{\mathbf{1}_H\}$ e verifica-se que $N \lhd N \rtimes H$ – Exercício 1.8.5.

Exemplo 8.14. Seja $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_4)$ o homomorfismo definido por

$$\begin{aligned} \theta(\underline{1}) : \mathbb{Z}_4 &\to \mathbb{Z}_4 \\ x &\mapsto -x \ . \end{aligned}$$

Vamos ver que $\mathbb{Z}_4 \rtimes \mathbb{Z}_2 \cong D_4$. Recorde que $D_4 = \langle a, b \mid |a| = 4, |b| = 2, bab^{-1} = a^{-1} \rangle$. Em $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$ temos, com as operações em $\mathbb{Z}_2$ e $\mathbb{Z}_4$ escritas em notação aditiva (claro!),

$$(\underline{0}, \underline{1})(x, \underline{0}) = (\underline{0} + \theta(\underline{1})(x), \underline{1} + \underline{0}) = (-x, \underline{1}) = (-x, \underline{0})(\underline{0}, \underline{1}) \qquad \forall\, x \in \mathbb{Z}_4 \ ,$$

onde se usou $\theta(\underline{0}) = \mathrm{id}_{\mathbb{Z}_4}$ na última igualdade, portanto

$$(\underline{0}, \underline{1})(\underline{1}, \underline{0})(\underline{0}, \underline{1})^{-1} = (-\underline{1}, \underline{0}) \ .$$

Também é fácil de verificar que $(\underline{1}, \underline{0})$ e $(\underline{0}, \underline{1})$ têm ordens 4 e 2, respectivamente. Portanto, a aplicação $\psi : \mathbb{Z}_4 \rtimes \mathbb{Z}_2 \to D_4$ dada por

$$\psi(\underline{1}, \underline{0}) = a \qquad \text{e} \qquad \psi(\underline{0}, \underline{1}) = b$$

é um homomorfismo de grupos sobrejectivo. Como $|\mathbb{Z}_4 \rtimes \mathbb{Z}_2| = |\mathbb{Z}_4||\mathbb{Z}_2| = 8 = |D_4|$ e ψ é sobrejectivo, concluimos que ψ é um isomorfismo.

Observação 8.15. O produto directo de grupos abelianos é sempre um grupo abeliano. No caso do producto semidirecto isso já não é verdade, como mostra o exemplo anterior.

Exercícios

1.8.1. Mostre que $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.

1.8.2. Mostre que $S_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$.

1.8.3. Sejam $N \lhd G$ e $K < G$ tais que $N \cap K = \{\mathbf{1}\}$ e $NK = G$.
   (a) Mostre que $G/N \cong K$.
   (b) Será sempre verdade que $G \cong N \times K$?

1.8.4. Sejam $N_1 \lhd G_1$ e $N_2 \lhd G_2$.
   (a) Mostre que $N_1 \times N_2 \lhd G_1 \times G_2$ e
   $$\frac{G_1}{N_1} \times \frac{G_2}{N_2} \cong \frac{G_1 \times G_2}{N_1 \times N_2},$$
   com um isomorfismo ψ definido pela expressão $\psi([g_1], [g_2]) = [(g_1, g_2)]$.
   (b) Seja $\widetilde{\pi} \colon G_1 \times G_2 \to G_1/N_1 \times G_2/N_2; (g_1, g_2) \mapsto ([g_1], [g_2])$. Mostre que $\psi \circ \widetilde{\pi}$ é a projecção canónica $G_1 \times G_2 \to \frac{G_1 \times G_2}{N_1 \times N_2}$.

1.8.5. Identificando N com $N \times \{\mathbf{1}_H\}$, mostre que $N \lhd N \rtimes H$.

1.8.6. Seja G um grupo e $N \lhd G$, $H < G$ tais que $N \cap H = \{\mathbf{1}\}$.
   (a) Mostre que a aplicação $\gamma : H \to \mathrm{Aut}(N)$, $h \mapsto c_h$, onde $c_h(n) = hnh^{-1}$ para todo o $n \in N$, é um homomorfismo de grupos.
   (b) Mostre que $\psi : N \rtimes H \to G$, $\psi(n, h) = nh$, é um homomorfismo injectivo de grupos cuja imagem é NH. Quando ψ é também sobrejectivo, i.e. $G = NH$, dizemos que G é o *produto semidirecto interno* de N e H e escrevemos $G = N \rtimes H$.

1.8.7. Considere os subgrupos $N = \langle (12)(34), (13)(24) \rangle$ e $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$ do grupo S_4. Mostre que $N \lhd S_4$ e que $S_4 = N \rtimes H$. Conclua que $S_4 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes S_3$.

1.8.8. Mostre que Q_8 não pode ser descrito como o produto semidirecto interno de subgrupos próprios.

1.8.9. Mostre que $S_n = A_n \rtimes \mathbb{Z}_2$, $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$, para $n \geq 3$.

9. Acções de grupos

Definição 9.1. *Seja G um grupo e X um conjunto. Uma* acção à esquerda *de G em X é uma função $G \times X \to X$ denotada habitualmente por justaposição, $(g, x) \mapsto gx$,* t.q.

i. $\forall\, x \in X \quad \mathbf{1}x = x$;

ii. $\forall\, g_1, g_2 \in G, \forall x \in X \quad g_1(g_2 x) = (g_1 g_2)x$.

Diz-se que X é um conjunto-G.

Observação 9.2. Também se define acção à direita: é uma função $X \times G \to X; (x, g) \mapsto xg$ *t.q.*

$$(xg_1)g_2 = x(g_1 g_2), \qquad \forall g_1, g_2 \in G, \quad \forall x \in X.$$

Excepto menção em contrário, *todas as acções consideradas são acções à esquerda.*

Observação 9.3. Seja

$$S_X \coloneqq \{f \colon X \to X \mid f \text{ é bijectiva}\}.$$

Com a operação de composição, S_X é um grupo – o grupo das permutações de X. Uma acção de G em X define uma função $T \colon G \to S_X$ dada por

$$T(g)(x) = gx, \qquad g \in G, x \in X,$$

que pertence a S_X, pois

$$\forall\, x \in X \quad g^{-1}gx = x \Leftrightarrow T(g^{-1}) \circ T(g) = \mathrm{id}_X$$

logo, $T(g^{-1}) = T(g)^{-1}$.

Proposição 9.4. *Dar uma acção de G em X é equivalente a dar um homomorfismo de grupos $T \colon G \to S_X$.*

Definição 9.5. *Seja X um conjunto com uma acção de G. Seja $T \colon G \to S_X$ o correspondente homomorfismo de grupos. Se T é injectivo, a acção diz-se* efectiva*, ou seja:*

$$(\forall x \in X \quad gx = x) \Rightarrow g = \mathbf{1}.$$

Exemplos 9.6.

1. Seja G um grupo. Então G age em G por multiplicação à esquerda:

   $$(g, x) \mapsto gx, \qquad g, x \in G.$$

   Esta acção é efectiva: $gx = x \Leftrightarrow g = \mathbf{1}$.
2. A multiplicação à direita define uma acção de G em G à direita.
3. G também age à esquerda em G da seguinte forma:

   $$(g, x) \mapsto g \star x \coloneqq xg^{-1},$$

   pois $(g_1 g_2) \star x = x(g_1 g_2)^{-1} = (xg_2^{-1})g_1^{-1} = g_1 \star (g_2 \star x)$.

Teorema 9.7 (Cayley)**.** *Seja G um grupo, então G é isomorfo a um subgrupo do grupo S_G de permutações de G. Em particular, se $|G| = n$, G é isomorfo a um subgrupo do grupo simétrico S_n (Exemplo 1.7).*

Demonstração. O homomorfismo $T \colon G \to S_G$ correspondente à acção por multiplicação à esquerda é injectivo. □

Exemplos 9.8.

1. Seja G um grupo. G age à esquerda em G por conjugação – $(g, x) \mapsto g \star x \coloneqq gxg^{-1}$ –, pois

   $$g_1 \star (g_2 \star x) = g_1 \star (g_2 x g_2^{-1}) = (g_1 g_2)x(g_2^{-1} g_1^{-1}) = (g_1 g_2) \star x.$$

   Em geral, esta acção não é efectiva: $gxg^{-1} = x \Leftrightarrow gx = xg$.

2. $\mathrm{GL}_n(\mathbb{R})$ age em $\mathbb{R}^n$ da forma óbvia: $(A, v) \mapsto Av$. Esta acção é efectiva:
$$(Av = v \quad \forall v \in \mathbb{R}^n) \Leftrightarrow A = I.$$
3. $\mathrm{O}(n, \mathbb{R}) \coloneqq \{A \in M_n(\mathbb{R}) \mid AA^T = I\}$ age em $\mathbb{R}^n$ da mesma forma que $\mathrm{GL}_n(\mathbb{R})$.
4. Seja k um corpo (*e.g.*, $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$), então $k^\times$ age em $k^n \setminus \{0\}$ por multiplicação.

Definição 9.9. *Sejam $G \times X \to X; (g, x) \to g \star_1 x$ e $G \times Y \to Y; (g, y) \to g \star_2 y$ acções do grupo G e sejam $T_1 \colon G \to S_X$ e $T_2 \colon G \to S_Y$ os homomorfismos correspondentes. Diz-se que uma função $\phi \colon X \to Y$ é* equivariante *se*
$$\forall g \in G \quad \forall x \in X \qquad \phi(g \star_1 x) = g \star_2 \phi(x),$$
i.e.,
$$\phi(T_1(g)(x)) = T_2(g)(\phi(x)),$$
ou, de forma equivalente, o diagrama seguinte é comutativo para todo o $g \in G$
$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ {\scriptstyle T_1(g)}\downarrow & & \downarrow{\scriptstyle T_2(g)} \\ X & \xrightarrow{\phi} & Y \end{array}$$
Se existir $\phi \colon X \to Y$ equivariante e bijectiva, diz-se que as acções são equivalentes.

Exemplo 9.10. Seja G um grupo. Consideremos as duas acções à esquerda de G em G definidas acima:
$$(g, x) \mapsto gx, \qquad (g, x) \mapsto g \star x = xg^{-1}.$$
Seja $\phi \colon G \to G$ a bijecção $x \mapsto x^{-1}$. Vejamos que ϕ é equivariante:
$$\phi(gx) = (gx)^{-1} = x^{-1}g^{-1} = \phi(x)g^{-1} = g \star \phi(x).$$
Concluímos que as duas acções são equivalentes.

Definição 9.11. *Seja $G \times X \to X; (g, x) \mapsto gx$ uma acção. A órbita-G de $x \in X$ é o conjunto*
$$\mathcal{O}_x = \{gx \mid g \in G\}.$$

Observação 9.12. A relação
$$x \sim y \Leftrightarrow \exists g \in G : gx = y$$
é uma relação de equivalência:

reflexividade: $\mathbf{1}x = x$;

simetria: $x \sim y \Leftrightarrow \exists g : gx = y \Rightarrow g^{-1}y = x \Rightarrow y \sim x$;

transitividade: $x \sim y \wedge y \sim z \Leftrightarrow \exists g_1, g_2 : g_1 x = y \wedge g_2 y = z \Rightarrow (g_2 g_1)x = z \Rightarrow x \sim z$.

A classe de equivalência de x é a órbita $\mathcal{O}_x$.

Definição 9.13. *Seja $G \times X \to X$ uma acção. Define-se o quociente de X pela acção de G como o quociente de X pela relação de equivalência definida na Observação 9.12 ($X/\sim$) e é denotado X/G. Se $|X/G| = 1$, a acção diz-se* transitiva.

Observação 9.14.

1. Os elementos de X/G são as órbitas da acção;
2. $X = \bigcup_{[x] \in X/G} \mathcal{O}_x$ é uma partição de X.

Exemplos 9.15. 1. As órbitas da acção de $\mathrm{O}_n(\mathbb{R})$ em $\mathbb{R}^n$ são as esferas centradas na origem:
   - $A \in \mathrm{O}_n(\mathbb{R}) \Rightarrow |Av| = |v|$
   - $|v| = |v'| \Rightarrow \exists A \in \mathrm{O}_n(\mathbb{R}) : Av = v'$.
2. As órbitas da acção de $k^\times$ em $k^n \setminus \{\mathbf{0}\}$ são os subespaços lineares de k^n com dimensão 1. Define-se $\mathbb{P}(k^n) \coloneqq (k^n \setminus \{\mathbf{0}\})/k^\times$.

3. Seja $H < G$. Então H age em G por multiplicação à esquerda: $H \times G \to G; (h, g) \mapsto hg$. As órbitas desta acção são as classes laterais direitas de H em G: $\mathcal{O}_g = Hg$, $g \in G$.
   Se $H \neq G$ a acção não é transitiva.
4. Recorde-se que um grupo G age em si próprio por conjugação: $(g, x) \mapsto gxg^{-1}$. As órbitas desta acção chamam-se *classes de conjugação* e denotam-se $\mathrm{Cl}(x)$, $x \in G$.
   Note-se que
   $$\mathrm{Cl}(x) = \{x\} \Leftrightarrow \forall g' \in G,\ gg' = g'g,$$
   pelo que, os elementos cuja órbita tem um só elemento são os que comutam com todos os outros.
5. Como caso particular do exemplo anterior, considere a acção por conjugação de S_4 em si próprio. Pelo Exercício 1.9.2, as órbitas são as seguintes classes de conjugação
   $$\mathrm{Cl}(1), \quad \mathrm{Cl}((1\ 2)), \quad \mathrm{Cl}((1\ 2\ 3)), \quad \mathrm{Cl}((1\ 2\ 3\ 4)) \quad \text{e} \quad \mathrm{Cl}((1\ 2)(3\ 4)).$$
6. O grupo $G = \mathrm{GL}_n(\mathbb{C})$ age por conjugação no conjunto $X = \mathrm{M}_n(\mathbb{C})$ (que contém G). Da Álgebra Linear sabemos que cada matriz $A \in \mathrm{M}_n(\mathbb{C})$ tem uma *forma canónica de Jordan* J, i.e., existe $S \in \mathrm{GL}_n(\mathbb{C})$ tal que $A = SJS^{-1}$ onde
   $$J = \begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_k \end{bmatrix}_{n\times n} \quad \text{e} \quad J_i = \begin{bmatrix} \lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix}$$
   (e $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ são os valores prórios de A). A menos da ordem[6] dos blocos B_i, esta matriz J é única, portanto, $B \in \mathrm{Cl}(A)$ sse B e A têm a mesma forma canónica de Jordan.

Definição 9.16. *Seja G um grupo. Define-se* o centro *de G, $Z(G)$ ou $C(G)$, como*
$$Z(G) = \{g \in G \mid gg' = g'g, \quad \forall g' \in G\} = \{g \in G \mid |\mathrm{Cl}(g)| = 1\} < G.$$

Exemplo 9.17. Seja $H = \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4)\rangle < S_4$. Então $H \cong D_4$ e $Z(H) = \{1, (1\ 3)(2\ 4)\} \cong \mathbb{Z}_2$.

Definição 9.18. *Sejam X um conjunto-G e $x \in X$. Define-se o* grupo de isotropia *de x:*
$$G_x \coloneqq \{g \in G \mid gx = x\} < G.$$

Proposição 9.19. *Seja X um conjunto-G e sejam $x, y \in X$* t.q. *$y = gx$, com $g \in G$. Então $G_y = gG_xg^{-1}$.*

Demonstração. Temos,
$$h \in G_y \Leftrightarrow hy = y \Leftrightarrow hgx = gx \Leftrightarrow g^{-1}hgx = x \Leftrightarrow g^{-1}hg \in G_x$$
$$\therefore\ g^{-1}G_yg = G_x. \qquad \square$$

Definição 9.20. *Se $\forall x \in X$, $G_x = \{\mathbf{1}\}$, diz-se que a acção é* livre.

Exemplos 9.21.

1. A acção de G em G por multiplicação à esquerda (direita) é livre:
   $$gx = x \Leftrightarrow g = \mathbf{1}.$$
2. Se $H < G$, G age à esquerda nas classes esquerdas de H:
   $$(g', gH) \mapsto g'gH.$$
   Esta acção não é livre, pois $G_H = H$ e, em geral, $G_{gH} = gHg^{-1}$.

[6] Note que "trocar a ordem dos blocos" corresponde a permutar linhas e colunas em J, o que pode ser obtido por conjugação por *matrizes de permutação*.

3. A acção de G em G por conjugação não é livre:

$$G_g = \{g' \mid g'g = gg'\}.$$

Definição 9.22. *Seja G um grupo e seja $g \in G$. O* centralizador *de g, $C_G(g)$, é o grupo de isotropia de g para a acção de conjugação de G em G:*

$$C_G(g) \coloneqq \{g' \mid g'g = gg'\}.$$

Observação 9.23. Como $g^i g = g^{i+1} = gg^i$ para quaisquer $i \in \mathbb{Z}$ e $g \in G$, temos $C_G(g) > \langle g \rangle$.

Definição 9.24. *Dados $H < G$, define-se o* centralizador *e o* normalizador *de H em G respectivamente por*

$$C_G(H) \coloneqq \{g \in G \mid gh = hg\} \qquad e \qquad N_G(H) \coloneqq \{g \in G \mid gHg^{-1} \subset H\}.$$

Observação 9.25. $N_G(H)$ é o maior subgrupo de G em que H é normal – ver Exercício 1.9.8, alíneas (c) e (d).

Proposição 9.26. *Seja X um conjunto-G. Para cada $x \in X$, a aplicação $\phi\colon G/G_x \to \mathcal{O}_x$*

$$\phi(gG_x) = gx$$

é uma bijecção equivariante. Portanto, $\mathcal{O}_x$ é equivalente a G/G_x. Em particular, se a acção é transitiva, $X \cong G/G_x$.

Demonstração.

1. ϕ está bem definida: $h \in G_x \Rightarrow (gh)x = gx$.
2. ϕ é injectiva: $gx = g'x \Leftrightarrow g^{-1}g' \in G_x$.
3. ϕ é sobrejectiva e é equivariante por construção:

$$\phi(g'(gG_x)) = \phi((g'g)G_x) = (g'g)x = g'\phi(gG_x). \qquad \square$$

Exemplo 9.27. Seja $X = S^2 \coloneqq \{x \in \mathbb{R}^3 \mid |x| = 1\}$ e sejam $G = O(3)$, $x_0 = e_1 \coloneqq (0,0,1) \in S^2$. Recorde-se que G age em X por $(A, x) \mapsto Ax$. Temos

$$G_{x_0} = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & B \end{smallmatrix}\right) \mid B \in O(2) \right\} \cong O(2). \tag{9.1}$$

Como a acção é transitiva, concluímos que $S^2 \cong O(3)/O(2)$, onde $O(2)$ é visto como subgrupo de $O(3)$ através da inclusão $B \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & B \end{smallmatrix}\right)$.

Proposição 9.28. *Seja X um conjunto-G finito e seja $X = \bigcup_{i=1}^n \mathcal{O}_{x_i}$ uma partição em órbitas. Então,*

$$|X| = \sum_{i=1}^{n} [G : G_{x_i}] \tag{9.2}$$

Demonstração. Segue de $|\mathcal{O}_{x_i}| = |G/G_{x_i}| = [G : G_{x_i}]$. $\square$

Exercícios

1.9.1. Demonstre a Proposição 9.4.

1.9.2. Determine as classes de conjugação em S_n.
Sugestão: Use o exercício 1.9.5, e recorde que qualquer permutação é o produto de ciclos disjuntos. Conclua que duas permutações são conjugadas em S_n sse tem o mesmo tipo de factorização em ciclos disjuntos.

1.9.3. Seja G um grupo. Mostre que $Z(G) \lhd G$.

1.9.4. Mostre que $Z(H \times K) = Z(H) \times Z(K)$.

1.9.5. Determine $Z(Q_8)$, $Z(D_4)$ e $Z(D_6)$.

1.9.6. Seja $n \in \mathbb{N}$ *t.q.* $n > 2$. Mostre que $Z(S_n) = \{\mathbf{1}\}$.

1.9.7. Mostre que, se $G/Z(G)$ é cíclico, então G é abeliano.

1.9.8. Seja G um grupo e $H < G$. Prove as seguintes propriedades:
(a) $C_G(x) = C_G(\langle x \rangle)$ para todo o $x \in G$;
(b) $C_G(H) \lhd N_G(G)$;
(c) $H \lhd N_G(H)$;
(d) Se $H < K < G$ e $H \lhd K$, então $K < N_G(H)$.

1.9.9. (a) Seja G um grupo. Considere a acção de G em G por conjugação. Dado $x \in G$, determine o subgrupo de isotropia G_x.
(b) Determine o número de elementos de S_4 que comutam com $\sigma = (12)(34)$.

1.9.10. Seja N um grupo de ordem 5.
(a) Calcule a ordem do grupo $\mathrm{Aut}(N)$.
(b) Seja G um grupo de ordem ímpar tal que $N \lhd G$. Mostre que $N < Z(G)$.

1.9.11. Seja $G = GL_2(\mathbb{F}_5)$, onde $\mathbb{F}_5$ é o corpo com 5 elementos, i.e., $\mathbb{F}_5 = (\mathbb{Z}_5, +, \cdot)$.
(a) Mostre que $|G| = 480$.
Sugestão: Comece por notar que a primeira coluna de uma matriz $S \in G$ é um elemento arbitrário de $(\mathbb{F}_5)^2 \setminus \{0\}$.
(b) Seja $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ e seja $\mathcal{O}_A = \{SAS^{-1} \mid S \in G\}$. Mostre que $\mathcal{O}_A$ tem 30 elementos.

1.9.12. Seja G um grupo e seja $H < G$. Considere a acção de G em G/H por multiplicação à esquerda.
(a) Seja $g \in G$. Calcule o grupo de isotropia G_{gH}.
(b) Mostre que, se $f : G/H \to G/H$ é uma função equivariante, então f é da forma $f(gH) = gkH$ para algum $k \in N_G(H)$.

1.9.13. Seja G um grupo que age transitivamente num conjunto X, e sejam $x \in X$ e $H < G$. Mostre que H age transitivamente em X se e só se $G = HG_x$.

1.9.14. Seja G um grupo contendo um elemento $a \in G$ que tem precisamente dois conjugados. Mostre que G contém um subgrupo normal próprio $N \neq \{\mathbf{1}\}$.

1.9.15. Seja G um grupo. Um automorfismo $f \in \mathrm{Aut}(G)$ diz-se *interior* se

$$\exists\, g \in G \quad \forall\, x \in G \quad t.q. \quad f(x) = gxg^{-1}.$$

O conjunto dos automorfismo interiores denota-se por $\mathrm{Inn}(G)$.
(a) Mostre que $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.
(b) Mostre que $\mathrm{Inn}(G) \cong G/Z(G)$.

1.9.16. Se $H < G$, mostre que o grupo quociente $N_G(H)/C_G(H)$ é isomorfo a um subgrupo de $\mathrm{Aut}(H)$.

1.9.17. Dê um exemplo de um automorfismo de $\mathbb{Z}_6$ que **não** é um automorfismo interior.

1.9.18. Mostre que o centro de S_4 é $Z(S_4) = \{\mathbf{1}\}$ e conclua que $S_4 \cong \mathrm{Inn}(S_4)$.

1.9.19. Seja G um grupo contendo um subgrupo próprio de índice finito. Mostre que G contém um subgrupo próprio normal de índice finito.

1.9.20. Seja G um grupo tal que $|G| = pn$ com $p > n$, p primo, e seja $H < G$ tal que $|H| = p$. Mostre que $H \lhd G$.

10. Teoremas de Sylow

Recorde-se que se G é um grupo finito e $g \in G$, então $|g| \mid |G|$. Este resultado é conhecido como *Teorema de Lagrange*. É natural perguntar se a recíproca se verifica, *i.e.*, dado $m \mid |G|$, se existe $g \in G$ *t.q.* $|g| = m$?

Em geral, a resposta é negativa. No entanto, a resposta é positiva se $m = p$ é primo, como veremos a seguir.

Nos resultados que se seguem iremos utilizar a acção de conjugação de um grupo G em diversos conjuntos, que revemos brevemente:

1. G age em G por conjugação. Para cada $x \in G$, temos

$$\begin{aligned} \mathcal{O}_x &= \left\{gxg^{-1} \mid g \in G\right\} \\ G_x &= C_G(x) = \{g \in G \mid gx = xg\} \\ |\mathcal{O}_x| &= \left|\frac{G}{G_x}\right| = [G : C_G(x)]\,. \end{aligned}$$

2. G age por conjugação no conjunto dos seus subgrupos. Dado $H < G$, temos

$$G_H = N_G(H) = \left\{g \in G \mid gHg^{-1} \subset H\right\} < G.$$

Teorema 10.1. *Seja G um grupo* t.q. $|G| = p^m$ *(p primo) e seja X um conjunto-G finito. Consideremos o subconjunto*

$$X_0 = \{x \in X \mid \forall g \in G,\, gx = x\}\,.$$

Então,

$$|X| \equiv |X_0| \mod p.$$

Demonstração. Sejam $x_1, \ldots, x_n \in X$ representantes das órbitas com mais que um elemento. Temos,

$$|X| = |X_0| + \sum_{i=1}^{n} [G : G_{x_i}] \Rightarrow |X| \equiv |X_0| \mod p,$$

pois $p \mid [G : G_{x_i}]$ se $G_{x_i} \neq G$. □

Corolário 10.2. *Se $|G| = p^m$ (p primo), então*

$$|Z(G)| = p^k,$$

com $k \geq 1$.

Demonstração. Como $Z(G) < G$, temos apenas que provar $|Z(G)| \neq 1$ (ver Corolário 5.6). Do Teorema 10.1, obtemos,

$$|G| \equiv |Z(G)| \mod p,$$

pois $Z(G)$ é o conjunto das órbitas com 1 só elemento para a acção de conjugação. Logo $|Z(G)| \neq 1$. □

Teorema 10.3 (Cauchy)**.** *Seja G um grupo finito e seja p um primo* t.q. $p \mid |G|$. *Então G contém um elemento de ordem p.*

Demonstração. Seja $X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = \mathbf{1}\}$. Definimos uma acção $\mathbb{Z}_p \times X \to X$ cujo correspondente homomorfismo $T\colon \mathbb{Z}_p \to S_X$ é dado pela expressão seguinte:

$$T(\underline{1})(g_1, \ldots, g_p) \coloneqq (g_2, \ldots, g_p, g_1).$$

Temos

$$g_1 \cdots g_p = \mathbf{1} \Leftrightarrow g_1(g_2 \cdots g_p g_1)g_1^{-1} = \mathbf{1} \Leftrightarrow g_2 \cdots g_p g_1 = g_1^{-1}\mathbf{1}g_1 = \mathbf{1}.$$

logo $(g_2, \ldots, g_p, g_1) \in X$. Portanto, $T(\underline{1})$ define de facto uma função $X \to X$, que é claramente bijectiva. Como além disso, $T(\underline{1})^p = \mathrm{id}_X$, concluímos que T define um homomorfismo

$$T \colon \mathbb{Z}_p \to S_X,$$

ou seja, define uma acção em X. Temos

$$X_0 = \{(g, \ldots, g) \mid g \in G \wedge g^p = \mathbf{1}\},$$

logo

$$1 \leq |X_0| \equiv |X| \mod p.$$

Mas $|X| = |G|^{p-1} \equiv 0 \mod p$, portanto $|X_0| \geq p$. Ou seja, G tem elementos de ordem p. □

Definição 10.4. *Seja $p \in \mathbb{N}$ um primo. Um grupo H diz-se um* grupo-p *se $\forall h \in H$, $|h|$ é uma potência de p.*

Se $H < G$ é um grupo-p, diz-se que H é um subgrupo-p *de G. Se $|H| = p^k$, k diz-se o* expoente *de H.*

Exemplos 10.5.

1. $\mathbb{Z}_p$ é um grupo-p finito;
2. $\mathbb{Z}(p^\infty) = \left\{[\frac{a}{b}] \in \mathbb{Q}/\mathbb{Z} \mid \exists n : b = p^n\right\}$ é um grupo-p infinito.

Corolário 10.6. *Seja G um grupo finito. Então G é um grupo-p* sse *$|G| = p^n$, para algum n.*

Demonstração.

$\boxed{\Leftarrow}$ se $g \in G$, então $|g| \mid p^n$;

$\boxed{\Rightarrow}$ seja $m = |G|$. Se $q \mid m$ é primo, então pelo Teorema de Cauchy (10.3), $\exists g$ *t.q.* $|g| = q$, logo $q = p$. □

Definição 10.7. *Seja G um grupo finito* t.q. *$|G| = p^n m$, com p primo e* $\mathrm{MDC}(p, m) = 1$. *Um subgrupo-p de expoente n de G diz-se um* subgrupo-p de Sylow *de G.*

Exemplo 10.8. Seja $G = \mathbb{Z}_3 \times \mathbb{Z}_4$. Então $H = \{\underline{0}\} \times \mathbb{Z}_4$ é um subgrupo-2 de Sylow de G. Se considerarmos $\mathbb{Z}_2 < \mathbb{Z}_4$, como habitualmente (ver Proposição 4.10), então $K = \{\underline{0}\} \times \mathbb{Z}_2$ é um subgrupo-2 de G.

Teorema 10.9 (Sylow I)**.** *Seja G um grupo finito e sejam $p, k \in \mathbb{N}$* t.q. *p é primo e $p^k \mid |G|$. Então G tem um subgrupo-p de expoente k. Em particular, G tem um subgrupo-p de Sylow.*

Demonstração. O resultado é válido se $|G| = p$ ou $|G| = 1$. Prosseguimos por indução em $|G|$. Supomos o resultado válido para todo G' *t.q.* $|G'| < |G|$ e $|G'| \mid |G|$.

Consideremos a acção de G em G por conjugação. Obtemos,

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)],$$

onde $x_1, \ldots, x_n$ são representantes das classes de conjugação (as órbitas da acção com mais de um elemento). Então:

- $p \nmid |Z(G)| \Rightarrow \exists\, i : p \nmid [G : C_G(x_i)] \Rightarrow p^k \mid |C_G(x_i)|$
  Note-se que $C_G(x_i) \neq G$, pois $x_i \notin Z(G)$.
  Da hipótese de indução, aplicada a $C_G(x_i)$, segue que $\exists\, H < C_G(x_i)$ *t.q.* $|H| = p^k$.
- $p \mid |Z(G)| \Rightarrow \exists\, g \in Z(G) : |g| = p$ (pelo Teorema 10.3).
  Note-se que $\langle g \rangle \lhd G$. Consideremos a projecção canónica $\pi \colon G \to G/\langle g \rangle$. Pela hipótese de indução – aplicada a $G/\langle g \rangle$ – $\exists\, \bar{H} < G/\langle g \rangle$ *t.q.* $|\bar{H}| = p^{k-1}$.

Seja $H = \pi^{-1}(\bar{H}) < G$. Temos

$$\begin{aligned} |H| &= [H : \langle g \rangle]\, |\langle g \rangle| \\ &= |H/\langle g \rangle|\, p \\ &= |\pi(H)|\, p \\ &= |\bar{H}|\, p \\ &= p^k. \end{aligned}$$

□

Teorema 10.10 (Sylow II)**.** *Seja G um grupo finito e p um primo. Então,*

i. todo o subgrupo-p de G está contido num subgrupo-p de Sylow;

ii. todos os subgrupos-p de Sylow de G são conjugados. Se P é um subgrupo-p de Sylow e n é o número de subgrupos-p de Sylow de G temos,

$$n \mid [G : P];$$

iii. se n é o número de subgrupos-p de Sylow de G, temos $n \equiv 1 \mod p$.

Demonstração.

i. Seja $H < G$ um subgrupo-p e seja $P < G$ um subgrupo-p de Sylow. H age em G/P da seguinte forma:

$$(h, gP) \mapsto hgP.$$

Seja $G/P = \cup_{i=1}^{n} \mathcal{O}_{g_i P}$ uma partição em órbitas para esta acção. Então temos,

$$|G/P| = \sum_{i=1}^{n} |\mathcal{O}_{g_i P}| = \sum_{i=1}^{n} [H : H_{g_i P}],$$

e por P ser um subgrupo-p de Sylow, temos $p \nmid |G/P|$. Ora,

$$\begin{aligned} p \nmid |G/P| &\Rightarrow \exists i : p \nmid [H : H_{g_i P}] \\ &\Leftrightarrow H = H_{g_i P} \qquad \text{(pois } H \text{ é um grupo-}p\text{)} \\ &\Leftrightarrow H g_i P = g_i P \\ &\Leftrightarrow g_i^{-1} H g_i P = P \\ &\Leftrightarrow g_i^{-1} H g_i \subset P \\ &\Leftrightarrow H \subset g_i P g_i^{-1}. \end{aligned}$$

Como $g_i P g_i^{-1}$ é um subgrupo de Sylow, a asserção $i.$ segue.

ii. Seja P' outro subgrupo-p de Sylow, sabemos da demonstração de $i.$, existe $g_i \in G$ *t.q.* $P' \subset g_i P g_i^{-1}$, logo

$$P' = g_i P g_i^{-1}.$$

Consideremos a acção de G em $\Pi \coloneqq \{P \mid P < G \text{ é subgrupo-}p \text{ de Sylow}\}$ por conjugação. Do que acabámos de demonstrar segue que a acção é transitiva, logo

$$|\Pi| = [G : G_P] = [G : N_G(P)].$$

Concluímos que $|\Pi| \mid [G : P]$, pois $P < N_G(P)$.

iii. Consideremos de novo o conjunto Π dos subgrupos-p de Sylow de G e fixemos $P \in \Pi$. Consideremos a acção de P em Π por conjugação. Seja

$$\Pi_0 \coloneqq \{P_i \mid |\mathcal{O}_{P_i}| = 1\}.$$

Pelo Teorema 10.1, temos

$$|\Pi| \equiv |\Pi_0| \mod p.$$

Vejamos que $\Pi_0 = \{P\}$: seja $P_i \in \Pi_0$, *i.e.*,

$$\begin{aligned} & PP_iP^{-1} = P_i \\ \Rightarrow & P \subset N_G(P_i) \\ \Rightarrow & P,\ P_i \text{ são subgrupos-}p \text{ de Sylow de } N_G(P_i) \\ \Rightarrow & \exists g \in N_G(P_i) : gP_ig^{-1} = P \\ \Rightarrow & P_i = P \text{ pois } P_i \lhd N_G(P_i). \end{aligned}$$

□

Exemplo 10.11. Seja G um grupo de ordem 6. Seja m o número de subgrupos-3 de Sylow de G. Temos,

$$m \mid 2 \quad \text{e} \quad m \equiv 1 \mod 3,$$

logo $m = 1$. Seja n o número de subgrupos-2 de Sylow. Temos,

$$n \mid 3 \quad \text{e} \quad n \equiv 1 \mod 2,$$

logo $n = 1$ ou $n = 3$. Os dois casos podem ocorrer, como veremos de seguida.

Sejam $x, y \in G$ *t.q.* $|x| = 3$ e $|y| = 2$. Temos,

$$G = \left\{x^i y^j \mid i = 0, 1, 2,\ j = 0, 1\right\}.$$

De facto,

$$x^i y^j = x^r y^s \Leftrightarrow x^{i-r} = y^{s-j} \Rightarrow 3 \mid i - r \equiv 0 \ \wedge\ 2 \mid s - j.$$

Como $|i - r| < 3$ e $|s - j| < 2$, segue $i - r = s - j = 0$.

Em particular,

$$yx = x^i y^j, \qquad \text{para algum } i,\ j.$$

Como $i = 0$ ou $j = 0$ é impossível, restam os casos

$$yx = xy \quad \text{ou} \quad yx = x^2 y,$$

que podem ambos ocorrer:

<u>1º Caso:</u> $G = \mathbb{Z}_6$.

<u>2º Caso:</u> $G \cong D_3$. O isomorfismo é dado por $x \mapsto \tau$, $y \mapsto \sigma$ onde τ é uma rotação de $2\pi/3$ e σ é uma reflexão (*cf.* Exercício 1.1.6).

Neste caso, os subgrupos de Sylow-2 são:

$$\begin{aligned} & \langle y \rangle, \\ & \langle xyx^2 \rangle = \langle xx^2yx \rangle = \langle x^2 y \rangle, \\ & \langle x^2 yx \rangle = \langle xy \rangle. \end{aligned}$$

Exemplo 10.12. Seja A_4 o subgrupo de S_4 das permutações pares. Dado que $|A_4| = \frac{|S_4|}{2} = 2^2 \cdot 3$, os subgrupos-2 de Sylow têm ordem 4 e os subgrupos-3 de Sylow têm ordem 3. Sejam n e m o número de subgrupos-2 e subgrupos-3 de Sylow, respectivamente. Então

$$n \mid 3 \quad \text{e} \quad n \equiv 1 \mod 2, \qquad m \mid 4 \quad \text{e} \quad m \equiv 1 \mod 3,$$

portanto, $n \in \{1, 3\}$ e $m \in \{1, 4\}$.

Atendendo à factorização em ciclos disjuntos dos elementos em A_4, conclui-se que qualquer $\sigma \in A_4 \setminus \{\mathbf{1}\}$ é um ciclo-3 ou o produto de duas transposições disjuntas.

Seja P um subgrupo-2 de Sylow. Pela observação anterior, se $\sigma \in P \setminus \{\mathbf{1}\}$, então $\sigma = (a\ b)(c\ d)$, com $a, b, c, d \in \{1, 2, 3, 4\}$ todos distintos. Como há exactamente 3 permutações desta forma,

$$P = \{\mathbf{1}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

é o único subgrupo-2 de Sylow. Exercício: Verifique que de facto se tem $P \lhd A_4$.

No caso dos subgrupos-3 de Sylow, cada um é gerado por um ciclo-3, portanto

$$Q_1 = \langle (2\ 3\ 4) \rangle, \quad Q_2 = \langle (1\ 3\ 4) \rangle, \quad Q_3 = \langle (1\ 2\ 4) \rangle \quad \text{e} \quad Q_4 = \langle (1\ 2\ 3) \rangle$$

são os subgrupos-3 de Sylow e são grupos conjugados em A_4. Por exemplo:

$$Q_2 = (1\ 2)(3\ 4)Q_1(1\ 2)(3\ 4),$$
$$Q_3 = (1\ 3)(2\ 4)Q_1(1\ 3)(2\ 4) \quad \text{e}$$
$$Q_4 = (1\ 4)(2\ 3)Q_1(1\ 4)(2\ 3).$$

Exercícios

1.10.1. Seja G um grupo e $N \lhd G$ tais que N e G/N são grupos-p. Mostre que G é um grupo-p.

1.10.2. Mostre que qualquer grupo de ordem p^2, com p primo, é abeliano.
Sugestão: Use o Exercício 1.9.7.

1.10.3. Seja G um grupo-p finito e seja $H \lhd G$ tal que $H \neq \{\mathbf{1}\}$. Mostre que $H \cap Z(G) \neq \{\mathbf{1}\}$.

1.10.4. Seja G um grupo-p finito, i.e., $|G| = p^n$. Mostre que G contém um subgrupo normal de ordem p^k, para cada $0 \leq k \leq n$.

1.10.5. Seja G um grupo finito tal que P é um subgrupo-p de Sylow normal em G, e seja $f : G \to G$ um homomorfismo. Mostre que $f(P) < P$.

1.10.6. Seja P um subgrupo-p de Sylow do grupo G
(a) Mostre que $N_G(N_G(P)) = N_G(P)$.
(b) Mostre que, se $H < G$ contém $N_G(P)$, então $N_G(H) = H$.

1.10.7. Seja $D_6 = \langle a, b \mid |a| = 6, |b| = 2, bab^{-1} = a^{-1} \rangle$ o grupo das simetrias de um hexágono regular, onde $a \in D_6$ é uma rotação de $\pi/3$ e $b \in D_6$ é uma reflexão.
(a) Mostre que $\varphi(a) = (1\ 2\ 3\ 4\ 5\ 6)$ e $\varphi(b) = (1\ 2)(3\ 6)(4\ 5)$ definem um homomorfismo injectivo $\varphi : D_6 \longrightarrow S_6$ e, portanto,
$$D_6 \cong \langle (1\ 2\ 3\ 4\ 5\ 6), (1\ 2)(3\ 6)(4\ 5) \rangle < S_6.$$
(b) Determine os subgrupos de Sylow de D_6.

1.10.8. Determine os subgrupos de Sylow de D_{2p}, onde p é um primo ímpar.

1.10.9. Determine os subgrupos-2 e os subgrupos-3 de Sylow de S_3 e S_4.

1.10.10. Determine os subgrupos-p de Sylow de A_5 e S_6.

1.10.11. Seja $p \in \mathbb{N}$ um primo.
(a) Determine as ordens dos subgrupos-p de Sylow de S_p.
(b) Mostre que o número de subgrupos-p de Sylow de S_p é $(p-2)!$.
Sugestão: Calcule o número de geradores dos subgrupos-p de Sylow.
(c) Mostre que, se $H < S_p$ é um subgrupo-p de Sylow de S_p, então $|N_{S_p}(H)| = p(p-1)$.

1.10.12. Sejam p um número primo, G um grupo finito tal que $p \mid |G|$, $H \lhd G$ e $P < H$ um subgrupo-p de Sylow de H. Mostre que $G = HN_G(P)$.

1.10.13. Seja G um grupo que age transitivamente num conjunto X, seja $x \in X$ e seja $P < G_x$ um subgrupo de Sylow de G_x. Define-se
$$\mathrm{Fix}(P) \coloneqq \{y \in X \mid g \cdot y = y \ \forall\, g \in P\} \subset X\ .$$
(a) Mostre que $N_G(P)$ age em $\mathrm{Fix}(P)$ por restrição da acção de G em X, i.e., se $g \in N_G(P)$ e $y \in \mathrm{Fix}(P)$ então $g \cdot y \in \mathrm{Fix}(P)$.
(b) Mostre que a acção de $N_G(P)$ em $\mathrm{Fix}(P)$ é transitiva.
Sugestão: Comece por notar que $g \cdot y \in \mathrm{Fix}(P)$ se e só se $g^{-1}Pg < G_y$.

1.10.14. Se $|G| = p^n q$, com $p > q$ primos, mostre que G contém um único subgrupo normal de índice q.

1.10.15. Classifique, a menos de isomorfismos, os grupos não abelianos de ordem 12.

11. Os Teoremas de Sylow como teoremas de estrutura

Recorde-se que dados grupos G, H, definimos o produto directo $G \times H$. Esta operação pode ser generalizada para um número arbitrário de factores.

Definição 11.1. *Seja $\{G_i\}_{i\in I}$ uma família de grupos. Define-se o* produto directo *dos G_i como o produto cartesiano $\prod_{i\in I} G_i$ munido da operação seguinte:*

$$(g_i)_{i\in I}\,(g_i')_{i\in I} \coloneqq (g_i g_i')_{i\in I}\ .$$

Há um subgrupo do produto directo que representa também uma operação importante em teoria de grupos.

Definição 11.2. *Seja $\{G_i\}_{i\in I}$ uma família de grupos. Define-se a* soma directa *dos G_i como o subgrupo $\oplus_{i\in I} G_i$ do produto directo dado por:*

$$\bigoplus_{i\in I} G_i = \{(g_i)_{i\in I} \mid g_i = \mathbf{1}_{G_i} \textit{excepto para um conjunto finito de índices } i\}\ .$$

Observação 11.3. Note-se que, se I é finito, $\oplus_{i\in I} G_i = \prod_{i\in I} G_i$. No caso em que os grupos G_i são abelianos e I é finito é habitual usar a notação aditiva $\oplus_{i\in I} G_i$ em vez de $\prod_{i\in I} G_i$.

Teorema 11.4. *Seja G um grupo abeliano finito. Então existe um isomorfismo*

$$G \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{k_i}},$$

onde $p_1, \ldots, p_n$ são primos. Esta decomposição é única a menos de reordenação.

Demonstração. Mais à frente iremos demonstrar um resultado que inclui este como caso particular. □

Observação 11.5. Daqui segue que o subgrupo-p de Sylow de G satisfaz

$$P \cong \bigoplus_{j\in\{i \mid p=p_i\}} \mathbb{Z}_{p_j^{k_j}}$$

e segue também que, se $P_1, \ldots, P_k$ são os subgrupos de Sylow de G, então

$$G \cong P_1 \oplus \cdots \oplus P_k.$$

Questão 11.6. Será que dado um grupo finito G, não necessariamente abeliano, cujos os subgrupos de Sylow são $P_1, \ldots, P_k$, se tem

$$G \cong P_1 \times \cdots \times P_k?$$

A resposta a esta questão em geral é negativa, mas veremos que é positiva para uma classe importante de grupos finitos.

Para precisar melhor este resultado necessitamos do conceito de produto directo interno de um número arbitrário, mas finito, de subgrupos, à semelhança do que já foi feito para dois subgrupos – ver Definição 8.5 e Proposição 8.10.

Definição 11.7. *Seja G um grupo e sejam $G_i < G$, com $i = 1, \ldots, n$. Diz-se que G é o* produto directo interno *dos G_i se as seguintes condições se verificam*

(i) $G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_n) = \{\mathbf{1}\}, \forall\, i$

(ii) $xy = yx, \forall\, x \in G_i, \forall\, y \in G_j, \forall\, i \neq j,$

(iii) $G = G_1 \cdots G_n$ *(ver Definição 5.9)*

Proposição 11.8. *Seja G um grupo finito e sejam $G_1, \ldots, G_k \lhd G$* t.q.*, para todo i, $G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_k) = \{\mathbf{1}\}$ e $|G| = |G_1| \cdots |G_k|$. Então*

(a) G_i *comuta com* G_j*;*
(b) $G = G_1 \cdots G_k$ *(Definição 5.9).*

12. Teoria de estrutura de grupos: grupos nilpotentes e grupos resolúveis

Definição 12.1. *Seja* G *um grupo. Define-se*

$$Z_1(G) \coloneqq Z(G).$$

Para $i \geq 1$*, definimos recursivamente*

$$Z_{i+1}(G) \coloneqq \pi_i^{-1}\left(Z(G/Z_i(G))\right),$$

onde $\pi_i \colon G \to G/Z_i(G)$ *é a projecção canónica.*

Proposição 12.2. $Z_i(G) \lhd G$*.*

Obtemos assim uma sucessão ascendente de subgrupos normais de G:

$$\{\mathbf{1}\} \lhd Z_1(G) \lhd \cdots \lhd Z_n(G) \lhd \cdots$$

Definição 12.3. *Um grupo* G *diz-se* nilpotente *se existe* $n \in \mathbb{N}$ t.q. $Z_n(G) = G$*.*

Exemplo 12.4. Se G é um grupo abeliano, então G é nilpotente, pois $G = Z(G) = Z_1(G)$.

Teorema 12.5. *Os grupos-p finitos são grupos nilpotentes.*

Demonstração. Suponhamos que $i \geq 1$ é *t.q.* $Z_i(G) \neq G$. Como $Z_i(G) \lhd G$, podemos considerar o quociente $G/Z_i(G)$, que é um grupo-p finito. Pelo Corolário 10.2, obtemos $Z(G/Z_i(G)) \neq \{\mathbf{1}\}$ e portanto $Z_{i+1}(G) \supsetneq Z_i(G)$. Como $|G| < \infty$, a sucessão $Z_i(G)$ tem que terminar eventualmente com $Z_i(G) = G$. □

Teorema 12.6. *O produto directo de grupos nilpotentes é nilpotente.*

Demonstração. Sejam H, K grupos nilpotentes se seja $G = H \times K$. Vejamos que $Z_i(G) = Z_i(H) \times Z_i(K)$. Para $i = 1$, do Exercício 1.9.4, temos:

$$Z(G) = Z(H) \times Z(K).$$

Vamos mostrar que o resultado é válido em geral por indução em i.

Suponhamos que o resultado é válido para i. Então a projecção $\pi_i \colon G \to G/Z_i(G)$ pode escrever-se como uma composta da seguinte forma:

$$G \xrightarrow{\widetilde{\pi}} \frac{H}{Z_i(H)} \times \frac{K}{Z_i(K)} \xrightarrow[\cong]{\psi} \frac{H \times K}{Z_i(H) \times Z_i(K)} = \frac{G}{Z_i(G)},$$

onde $\widetilde{\pi}$ é dado por $(h,k) \mapsto ([h],[k])$ e ψ é um isomorfismo dado por $([h],[k]) \mapsto [(h,k)]$ (ver Exercício 1.8.4).

Temos,

$$\begin{aligned}
Z_{i+1}(G) &= \pi^{-1}\left(Z(G/Z_i(G))\right) \\
&= \widetilde{\pi}^{-1}\psi^{-1}\left(Z(G/Z_i(G))\right) \\
&= \widetilde{\pi}^{-1}\left(Z\left(\frac{H}{Z_i(H)} \times \frac{K}{Z_i(K)}\right)\right) \\
&= \widetilde{\pi}^{-1}\left(Z\left(\frac{H}{Z_i(H)}\right) \times Z\left(\frac{K}{Z_i(K)}\right)\right) \\
&= Z_{i+1}(H) \times Z_{i+1}(K).
\end{aligned}$$

□

Lema 12.7. *Seja* $H \lneq G$ t.q. G *é um grupo nilpotente. Então* $H \lneq N_G(H)$*.*

Demonstração. Definindo $Z_0(G) \coloneqq \{\mathbf{1}\}$ existe $i \in \mathbb{N}_0$ *t.q.*

1. $Z_i(G) < H$;
2. $Z_{i+1}(G) \not< H$.

Note-se que como $G = Z_n(G)$, temos $i \leq n$.

Seja $a \in Z_{i+1}(G) \setminus H$ e recorde-se que

$$Z_{i+1}(G) = \pi^{-1}\left(Z\left(G/Z_i(G)\right)\right),$$

onde π é a projecção canónica $G \to G/Z_i(G)$. Logo $\pi(a) \in Z(G/Z_i(G))$.

Seja $h \in H$. Temos,

$$\begin{aligned}\pi(a)\pi(h) = \pi(h)\pi(a) &\Leftrightarrow \pi(a)\pi(h)\pi(a)^{-1}\pi(h)^{-1} = Z_i(G)\\ &\Leftrightarrow aha^{-1}h^{-1} \in Z_i(G) < H\\ &\Rightarrow aha^{-1} \in H\\ &\Leftrightarrow a \in N_G(H).\end{aligned}$$

$$\therefore H \lneq N_G(H).$$ □

Corolário 12.8. *Seja G um grupo nilpotente finito e seja $P < G$ um subgrupo de Sylow. Então $P \lhd G$.*

Demonstração. Note-se que se $P < G$ é um subgrupo-p de Sylow, então P é subgrupo-p de Sylow de $N_G(P)$, pois $N_G(P) < G$. Mais, P é o único subgrupo-p de Sylow de $N_G(P)$, pois $P \lhd N_G(P)$. Daqui segue

$$N_G(N_G(P)) = N_G(P).$$

De facto, dado $g \in N_G(N_G(P))$, temos $g^{-1}Pg$ é subgrupo-p de Sylow de $N_G(P)$ e portanto $g^{-1}Pg = P$, *i.e.*, $g \in N_G(P)$.

Do Lema 12.7, concluímos que $N_G(P) = G$, ou seja, $P \lhd G$. □

Teorema 12.9. *Seja G um grupo finito. Então G é nilpotente* sse *G é o produto directo interno dos seus subgrupos de Sylow.*

Demonstração.

$\boxed{\Leftarrow}$ Segue dos seguintes factos já demonstrados: 1. os grupos-p finitos são nilpotentes (Teorema 12.5); 2. o produto directo de grupos nilpotentes é nilpotente (Teorema 12.6).

$\boxed{\Rightarrow}$ Sejam $P_1, \ldots, P_k$ os subgrupos de Sylow de G. Pelo corolário anterior, temos $P_i \lhd G$ e portanto só há um subgrupo de Sylow para cada primo. Portanto,

$$|G| = |P_1| \cdots |P_k| \quad \text{e} \quad P_i \cap (P_1 \cdots P_{i-1}P_{i+1} \cdots P_k) = \{\mathbf{1}\} \text{ para qualquer } i.$$

Daqui segue (ver Proposição 11.8) $G = P_1 \cdots P_k$. Concluímos que

$$G = P_1 \times \cdots \times P_k.$$ □

Corolário 12.10. *Seja G um grupo nilpotente finito e seja $m \in \mathbb{N}$* t.q. *$m \mid |G|$. Então existe $H < G$* t.q. *$|H| = m$.*

Exemplo 12.11. O grupo simétrico $G = S_n$ não é nilpotente se $n > 2$, pois:

$$Z(S_n) = \{\mathbf{1}\}$$

(ver Exercício 1.9.6), logo

$$\begin{aligned}Z_1(G) &= \{\mathbf{1}\}\\ Z_2(G) &= \pi^{-1}(Z\left(S_n/\{\mathbf{1}\}\right)) = \pi^{-1}(\{\mathbf{1}\})\\ &\vdots\\ Z_i(G) &= \{\mathbf{1}\}, \quad \forall i.\end{aligned}$$

Exemplo 12.12. O corolário anterior não é uma equivalência: do exemplo anterior temos que S_4 não é nilpotente, mas dado $m \mid |S_4|$ existe $H < S_4$ com $|H| = m$. Por exemplo:

$m = 2, 2^2, 3$: consequência do Teorema de Sylow I 10.9;

$m = 6$: $H = \{\sigma \in S_4 \mid \sigma(4) = 4\} \cong S_3$, portanto $|H| = 6$.

$m = 12$: $|A_4| = 12$ e $A_4 < S_4$.

Exemplo 12.13. Seja $\mathbb{H}_8$ o subgrupo de $\mathbb{H}^\times$ cujos elementos são ± 1, $\pm i$, $\pm j$, $\pm k$. Então $\mathbb{H}_8$ é nilpotente pois é um grupo-2 finito (de expoente 3). Portanto existe n (≤ 3) *t.q.* $C_n(\mathbb{H}_8) = \mathbb{H}_8$.

Temos $Z(\mathbb{H}_8) = \{\pm 1\}$ e $\mathbb{H}_8/Z(\mathbb{H}_8)$ tem ordem 4, pelo que $\mathbb{H}_8/Z(\mathbb{H}_8) \cong \mathbb{Z}_4$ ou $\mathbb{H}_8/Z(\mathbb{H}_8) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Concluímos que $Z_2(\mathbb{H}_8) = \mathbb{H}_8$, *i.e.*, $n = 2$.

Definição 12.14. *Seja G um grupo. Define-se o* comutador *de $a, b \in G$ como*

$$[a, b] \coloneqq aba^{-1}b^{-1} = ab(ba)^{-1} \in G.$$

Proposição 12.15. *Sejam $g, a, b, c \in G$. Então*

(i) $[a, b]^{-1} = [b, a]$;

(ii) $[a, b] = \mathbf{1} \Leftrightarrow ab = ba$;

(iii) $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$;

(iv) $[a, bc] \cdot [b, ca] \cdot [c, ab] = \mathbf{1}$;

(v) se H é um grupo e $\phi \in \mathrm{Hom}(G, H)$, então

$$\phi([a, b]) = [\phi(a), \phi(b)]\,.$$

Definição 12.16. *Seja G um grupo e sejam $A, B < G$. Denota-se por $[A, B]$ o subgrupo*

$$[A, B] = \langle \{[a, b] \mid a \in A, b \in B\} \rangle.$$

Observação 12.17. Os elementos de $[A, B]$ são da forma

$$[a_1, b_1]^{\pm 1} \cdots [a_s, b_s]^{\pm 1}, \qquad a_i \in A, b_i \in B.$$

Por outro lado, da igualdade $[a, b]^{-1} = [b, a]$ segue

$$[A, B] = [B, A].$$

Definição 12.18. *Seja G um grupo. O* grupo derivado *de G é o subgrupo $[G, G]$ e é denotado por $G^{(1)}$ ou G'. Também se diz que $G^{(1)}$ é o* subgrupo dos comutadores*, mas é importante notar que os seus elementos não são todos comutadores.*

Exemplo 12.19. Um grupo G é abeliano *sse* $G^{(1)}$ é trivial.

Exemplo 12.20. Recorde-se que $D_3 = \{x^i y^j \mid i = 0, 1, 2\, j = 0, 1\}$, com $yx = x^2 y$, $|x| = 3$ e $|y| = 2$ (Exercício 1.1.6). Temos

$$[x, y] = xyx^{-1}y^{-1} = xyx^2y = x^3yxy = x^5y^2 = x^2y^2 = x^2.$$

Mostre que $D_3^{(1)} = \langle x \rangle \cong \mathbb{Z}_3$.

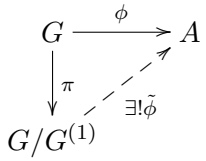
Nota 12.21. Muitos autores definem o comutador de a, b como $a^{-1}b^{-1}ab$, o que corresponde na Definição 12.18 a $[a^{-1}, b^{-1}]$. O subgrupo derivado que se obtém com ambas definições é o mesmo.

Proposição 12.22 (Propriedades do Derivado)**.** *Sejam G, H grupos. Temos*

(i) $\phi \in \mathrm{Hom}(G, H) \Rightarrow \phi\left(G^{(1)}\right) \subset H^{(1)}$;

(ii) $G^{(1)} \lhd G$;

(iii) $G/G^{(1)}$ *é um grupo abeliano e a projecção canónica* $\pi\colon G \to G/G^{(1)}$ *tem a seguinte propriedade universal: dado um grupo abeliano* A *e* $\phi \in \mathrm{Hom}(G, A)$ $\exists!\tilde{\phi} \in \mathrm{Hom}(G/G^{(1)}, A)$ *que faz comutar*



Demonstração. As asserções (i) e (ii) seguem imediatamente das propriedades dos comutadores. Quanto à asserção (iii): $G/G^{(1)}$ é abeliano, pois de $ab = [a, b]ba$ vem

$$\pi(a)\pi(b) = \pi(b)\pi(a).$$

Quanto ao diagrama:

$$\begin{aligned} A \text{ abeliano} &\Rightarrow G^{(1)} \subset \ker\phi \\ &\Rightarrow \exists!\tilde{\phi} \text{ como no diagrama.} \end{aligned}$$

□

Proposição 12.23. *Seja* G *um grupo e seja* $H \lhd G$ t.q. G/H *é abeliano. Então* $G^{(1)} < H$.

Notação 12.24. Diz-se que $G/G^{(1)}$ é o *abelianizado* de G.

Exemplo 12.25. Do Exemplo 12.20 concluimos que o abelianizado de D_3 é $D_3/D_3^{(1)} \cong \mathbb{Z}_2$.

Exemplo 12.26. Seja $G = \mathbb{H}_8$. Do Exemplo 12.13, sabemos que $\mathbb{H}_8/Z(\mathbb{H}_8)$ é abeliano, logo, pelo exercício anterior, temos

$$\mathbb{H}_8^{(1)} < Z(\mathbb{H}_8) = \{\pm 1\}\ .$$

Como $[i, j] = -1$ concluímos que $\mathbb{H}_8^{(1)} = \{\pm 1\}$.

Definição 12.27. *Seja* G *um grupo. Definimos recursivamente o* n-ésimo subgrupo derivado *de* G *da seguinte forma:*

$$G^{(n+1)} := \left(G^{(n)}\right)^{(1)}.$$

Proposição 12.28. $G^{(n)} \lhd G$.

Observação 12.29. Os subgrupos derivados de G formam uma sucessão decrescente de subgrupos normais de G:

$$\cdots \lhd G^{(n)} \lhd G^{(n-1)} \lhd \cdots \lhd G^{(1)} \lhd G$$

Definição 12.30. *Um grupo* G *diz-se* resolúvel *se existe* $n \in \mathbb{N}$ t.q. $G^{(n)} = \{\mathbf{1}\}$.

Proposição 12.31. *Seja* G *um grupo nilpotente, então* G *é resolúvel.*

Demonstração. Considere-se a sequência crescente de subgrupos

$$\{\mathbf{1}\} =: Z_0(G) < Z_1(G) < Z_2(G) < \cdots < Z_n(G) = G.$$

Note-se que $Z_i(G)/Z_{i-1}(G) \cong Z(G/Z_{i-1}(G))$ é abeliano, portanto

$$Z_i(G)^{(1)} < Z_{i-1}(G).$$

Assim,

$$\begin{aligned} G^{(1)} = Z_n(G)^{(1)} &< Z_{n-1}(G) \\ \Rightarrow G^{(2)} = (Z_n(G))^{(2)} &< Z_{n-1}(G)^{(1)} < Z_{n-2}(G) \\ &\vdots \\ \Rightarrow G^{(n)} = (Z_n(G))^{(n)} &< Z_0(G) = \{\mathbf{1}\}. \end{aligned}$$

□

Exemplo 12.32. Seja $G = D_6 = \langle a, b \mid |a| = 6, |b| = 2, bab^{-1} = a^{-1}\rangle$. Como $D_6^{(1)} = \langle a^2\rangle \cong \mathbb{Z}_3$ é abeliano, então $D_6^{(2)} = \{1\}$, logo D_6 é resolúvel. Como $Z_1(D_6) = Z(D_6) = \langle a^3\rangle$ e $D_6/Z(D_6) \cong S_3$ (ver Exemplo 8.9), então $Z(D_6/Z(D_6)) = \{1\}$, logo $Z_i(D_6) = \{1\}$, para $i \geq 2$, logo D_6 não é nilpotente.

Teorema 12.33. *Sejam G, K grupos. Então*

1. G é resolúvel e $H < G \Rightarrow H$ resolúvel;

2. G resolúvel e $f \in \mathrm{Hom}(G, K) \Rightarrow f(G)$ resolúvel

3. G é resolúvel e $N \lhd G \Rightarrow N$, G/N resolúveis.

Demonstração. 1. $H < G \Rightarrow H^{(i)} < G^{(i)}$;

2. $f(G)^{(i)} = f(G^{(i)})$;

3. por 1., N é resolúvel e, por 2. com $f = \pi : G \to G/N$, G/N é resolúvel. □

Exercícios

1.12.1. Demonstre a Proposição 11.8.

1.12.2. Demonstre a Proposição 12.2.

1.12.3. Seja G um grupo de ordem 45. Determine o número de subgrupos-p de Sylow para cada primo e justifique que G é um grupo abeliano, em particular, nilpotente.

1.12.4. Demonstre o Corolário 12.10.

1.12.5. Seja G um grupo nilpotente finito e $N \lhd G$ t.q $N \neq \{\mathbf{1}\}$. Mostre que $N \cap Z(G) \neq \{\mathbf{1}\}$.

1.12.6. (a) Prove que um grupo finito G é nilpotente *sse* qualquer subgrupo maximal próprio de G é normal.
(b) Se G é finito e nilpotente, conclua que o índice de qualquer subgrupo maximal próprio de G é um primo.
Sugestão: Use o Exercício 1.10.6.

1.12.7. Para que valores $n \geq 3$ é que D_n é um grupo nilpotente?

1.12.8. Demonstre a Proposição 12.15.

1.12.9. Seja $N \lhd G$. Mostre que $[N, G] < N$.

1.12.10. Demonstre a Proposição 12.23.

1.12.11. Demonstre a Proposição 12.28.

1.12.12. Calcule o grupo derivado $G^{(1)}$ nos seguintes casos:
(a) $G = S_n$ (com $n \geq 3$),
(b) $G = A_4$,
(c) $G = D_n$.

1.12.13. Mostre que não existe nenhum grupo cujo subgrupo derivado é o grupo diedral D_n, $n \geq 3$.
Sugestão: Suponha que existe um grupo G tal que $G^{(1)} = D_n$ e seja $K < G^{(1)}$ tal que $K \cong \mathbb{Z}_n$. Mostre que $\varphi\colon G \to \mathrm{Aut}(K)$, dado por $\varphi(g) = c_g$, é um homomorfismo de grupos e estude $\varphi(G^{(1)})$.

13. Séries normais e subnormais

Definição 13.1. *Um grupo G diz-se* simples *se $H \lhd G$ implica $H = G$ ou $H = \{\mathbf{1}\}$.*

Exemplo 13.2. Se G é abeliano então todos os seus subgrupos são normais, logo G é simples se e só se $G \cong \mathbb{Z}_p$, para algum primo $p \in \mathbb{N}$.

Exemplo 13.3. Note-se que $[S_n : A_n] = 2$, logo $A_n \lhd S_n$ e S_n não é um grupo simples.

Exemplo 13.4. Se $n = 3$, então $|A_3| = 3$, logo $A_3 \cong \mathbb{Z}_3$ é simples.

Exemplo 13.5. Se $n = 4$, seja $P = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$, então $P \lhd A_4$, logo A_4 não é simples.

Teorema 13.6. *A_n é simples se e só se $n \neq 4$.*

Demonstração. Ver [**Hun74**, §I.6]. □

Definição 13.7. *Um* série subnormal *de um grupo G é uma cadeia de subgrupos*

$$G_n < G_{n-1} < \cdots < G_1 < G_0 = G$$

tal que $G_{i+1} \lhd G_i$. Os quocientes G_i/G_{i+1} dizem-se factores *da série e o número $|\{i \mid G_i/G_{i+1} \neq \{\mathbf{1}\}|$ diz-se o* comprimento *da série. Se $G_i \lhd G$, $\forall\, i$, a série diz-se* normal.

Exemplo 13.8. $G^{(n)} < G^{(n-1)} < \cdots < G^{(1)} < G$ é uma série normal. Diz-se a *série derivada* de G.

Exemplo 13.9. Seja G nilpotente *t.q.* $G = Z_n(G)$, então fazendo $G_i \coloneqq Z_{n-i}(G)$, a cadeia

$$G_n = Z_0(G) < G_{n-1} = Z(G) < \cdots < G_0 = Z_n(G) = G$$

é uma série normal. Diz-se a *série central superior* de G.

Dada uma série subnormal $G_n < \cdots < G_1 < G_0 = G$ e dado $N < G$ tal que $N \lhd G_i$ e $G_{i+1} < N$ (se $i < n$) podemos obter uma nova série subnormal:

$$G_n < \cdots < G_{i+1} < N < G_i < \cdots < G_1 < G_0 = G.$$

Definição 13.10. *Uma série subnormal obtida por sucessivos passos desta forma, diz-se um* refinamento *de $G_n < \cdots < G_i < \cdots < G_1 < G_0 = G$.*

Definição 13.11. *Seja G um grupo. Uma série subnormal $\{\mathbf{1}\} = G_n < \cdots < G_{i+1} < G_i < \cdots < G_1 < G_0 = G$ diz-se uma* série de composição de G *se os factores G_i/G_{i+1} são simples. A série diz-se* resolúvel *se os factores são abelianos.*

Exemplo 13.12. A série derivada $\{\mathbf{1}\} = G^{(n)} < G^{(n-1)} < \cdots < G^{(1)} < G^{(0)} \coloneqq G$ de um grupo resolúvel é uma série resolúvel.

Teorema 13.13. *Seja G um grupo. Então,*

(a) se G é finito, G tem uma série de composição;

(b) todo o refinamento de uma série resolúvel de G é resolúvel;

(c) uma série subnormal de G é uma série de composição sse *não tem refinamentos próprios.*

Demonstração.

(a) Seja $G_1 < G$ normal maximal (cuja existência é garantida por $|G| < \infty$), então G/G_1 é simples. Supondo $G_1, \ldots, G_i$ escolhidos, prosseguimos escolhendo $G_{i+1} < G_i$ normal maximal. O processo termina com $G_n = \{\mathbf{1}\}$ e $G_n < \cdots < G_1 < G$ é uma série de composição por construção.

(b) Seja $G_n < \cdots < G_0 = G$ uma série resolúvel e seja $N \lhd G_i$ *t.q.* $G_{i+1} \lhd N$ (se $i < n$). Temos

$$\frac{N}{G_{i+1}} < \frac{G_i}{G_{i+1}},$$

logo N/G_{i+1} é abeliano.

Também G_i/N é abeliano pois $G_i^{(1)} < G_{i+1}$ por G_i/G_{i+1} ser abeliano.

(c) Segue da seguinte correspondência bijectiva

$$\{G_{i+1} < N \lhd G_i\} \longleftrightarrow \left\{\tilde{N} \lhd G_i/G_{i+1}\right\}. \qquad \square$$

Teorema 13.14. *Um grupo G é resolúvel* sse *tem uma série resolúvel.*

Demonstração.

$\boxed{\Rightarrow}$ Óbvio.

$\boxed{\Leftarrow}$ Seja $\{\mathbf{1}\} = G_n < \cdots < G_1 < G_0 = G$ uma série resolúvel. Temos

$$\begin{aligned} G/G_1 \text{ abeliano} &\Rightarrow G^{(1)} < G_1 \\ &\Rightarrow G^{(2)} < G_1^{(1)} \\ G_1/G_2 \text{ abeliano} &\Rightarrow G_1^{(1)} < G_2 \Rightarrow G^{(2)} < G_2 \\ &\vdots \\ &\Rightarrow G^{(n)} < G_n = \{\mathbf{1}\} \\ &\Rightarrow G \text{ é resolúvel.} \end{aligned}$$

$\square$

Exemplo 13.15. O grupo D_n é resolúvel porque

$$\{\mathbf{1}\} < \langle a \rangle < D_n$$

é uma série resolúvel: $D_n/\langle a\rangle \cong \mathbb{Z}_2$, onde $a \in D_n$ é um elemento de ordem n – ver Exercício 1.6.8.

Definição 13.16. *Duas séries subnormais dizem-se* equivalentes *se existe uma correspondência bijectiva entre factores não triviais que envia cada factor num grupo isomorfo.*

Ou seja, duas séries subnormais são equivalentes se os seus factores não-triviais são os mesmos a menos de isomorfismo e de reordenação.

Exemplo 13.17. A série derivada (logo resolúvel) do grupo D_6 é

$$\{\mathbf{1}\} < \langle a^2 \rangle < D_6$$

(ver Exemplo 12.32) cujos factores são

$$D_6/\langle a^2\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{e} \quad \langle a^2\rangle \cong \mathbb{Z}_3\ .$$

Do Exemplo 13.15 temos outra série resolúvel para D_6, que não é equivalente à primeira, pois os seus factores são $D_6/\langle a\rangle \cong \mathbb{Z}_2$ e $\langle a\rangle \cong \mathbb{Z}_6$.

Nenhuma delas é uma série de composição. Mas podemos refinar a série do Exemplo 13.15 e obter

$$\{\mathbf{1}\} < \langle a^2\rangle < \langle a\rangle < D_6 \qquad \text{ou} \qquad \{\mathbf{1}\} < \langle a^3\rangle < \langle a\rangle < D_6\ .$$

Cada uma destas séries tem dois factores isomorfos a $\mathbb{Z}_2$ e um isomorfo a $\mathbb{Z}_3$, sendo portanto duas séries de composição equivalentes.

Teorema 13.18 (Jordan-Hölder)**.** *Todas as séries de composição de um grupo G são equivalentes. Em particular, se G é finito existe um lista de grupos finitos simples associada a G.*

Demonstração. Ver [**Hun74**, §II.8]. $\square$

Observação 13.19. Se G é um grupo finito, a lista dos factores simples de uma série de composição só por si não permite identificar o grupo. Por exemplo,

$$\{\underline{0}\} < \langle \underline{2} \rangle < \mathbb{Z}_4 \qquad \text{e} \qquad \{(\underline{0},\underline{0})\} < \langle (\underline{1},\underline{0}) \rangle < \mathbb{Z}_2 \times \mathbb{Z}_2$$

são séries de composição para os grupos abelianos $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$, respectivamente, com factores todos isomorfos a $\mathbb{Z}_2$, no entanto $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Exercícios

1.13.1. Justifique que não existem grupos simples de ordem 20.
Sugestão: Conte os subgrupos-p de Sylow.

1.13.2. Seja G um grupo e $N \lhd G$ um subgrupo normal.
(a) Mostre que, se N e G/N são grupos resolúveis, G é resolúvel.
(b) Dê um exemplo de um grupo G e um subgrupo $N \lhd G$ tais que N e G/N são grupos nilpotentes mas G não é nilpotente.

1.13.3. Seja $G = G_0 > G_1 > \cdots > G_N$ uma série subnormal de um grupo finito G. Mostre que

$$|G| = \left(\prod_{i=0}^{n-1} |G_i/G_{i+1}| \right) |G_n|.$$

1.13.4. Prove que um grupo abeliano tem uma série de composição *sse* é finito.

1.13.5. Mostre que qualquer grupo resolúvel com uma série de composição é finito.

1.13.6. Mostre que qualquer grupo de ordem p^2q, onde p e q são primos, é resolúvel.

1.13.7. Seja G o subgrupo de $(\mathbb{H}^\times, \cdot)$ gerado por $a = e^{\frac{\pi i}{3}}$ e $b = j$.
(a) Calcule os subgrupos $Z_k(G)$ e $G^{(k)}$, com $k \geq 1$, e decida se G é nilpotente e/ou resolúvel.
(b) Determine uma série de composição para G e identifique os seus factores.
Sugestão: Verifique que $|a| = 6$, $|b| = 4$ e $bab^{-1} = a^{-1}$; justifique que qualquer elemento de G se escreve na forma $a^r b^s$ com $r, s \geq 0$.

1.13.8. Seja $G = GL_n(\mathbb{R})$ e considere os seguintes subgrupos:

$$H = \{A \in G \mid A \text{ é triangular superior}\},$$
$$K = \{A \in G \mid A \text{ é triangular superior com 1's na diagonal principal}\},$$
$$D = \{A \in G \mid A \text{ é diagonal}\}.$$

Prove as seguintes afirmações:
(a) K é nilpotente.
(b) $K \lhd H$ e $H/K \cong D$.
(c) H é resolúvel. Sugestão: Use a alínea anterior e o Exercício 1.13.2(a).

Anéis

1. Definições básicas

Definição 1.1. *Um* anel *é um conjunto A com duas operações denotadas por $+$ e por $\cdot$ (ou por justaposição)* t.q.

1. *$(A, +)$ é um grupo abeliano;*
2. *$(A, \cdot)$ é um monóide (com elemento identidade denotado por $\mathbf{1}$ ou $\mathbf{1}_A$);*
3. *verifica-se a propriedade distributiva:*

$$\forall x, y, z \in A \qquad (x + y)z = xz + yz; \quad x(y + z) = xy + xz.$$

Notação 1.2.

1. A identidade de $(A, +)$ é denotada por $\mathbf{0}$ (ou $\mathbf{0}_A$). Se a operação $\cdot$ for comutativa, A diz-se um anel *comutativo*;
2. mais geralmente, usamos a notação aditiva para $(A, +)$ e multiplicativa para $(A, \cdot)$. Em particular denotamos por $-x$ o inverso de x em $(A, +)$ e por x^{-1} o inverso em $(A, \cdot)$, se existir.

Nota 1.3. Na definição de anel dada em [**Hun74**] ou [**FR04**] não se exige que $(A, \cdot)$ tenha identidade e os anéis aqui considerados são aí designados anéis com identidade.

Observação 1.4 (Propriedades básicas da soma e do produto)**.**

1. $\forall x \in A, \quad \mathbf{0} \cdot x + x = (\mathbf{0} + \mathbf{1})x = \mathbf{1} \cdot x = x \Rightarrow \mathbf{0} \cdot x = \mathbf{0}$;
2. $\forall x, y \in A, \quad (-x)y + xy = (-x + x)y = \mathbf{0} \cdot x = \mathbf{0} \Rightarrow -xy = (-x)y$;
3. para cada $n \in \mathbb{Z}$, temos $n(xy) = (nx)y = x(ny)$;

Definição 1.5. *$A^\times = (\{x \in A \mid x \text{ é invertível em } (A, \cdot)\}, \cdot)$ é um grupo que se designa por* grupo das unidades *de A.*

Exemplos 1.6. 1. $(\mathbb{Z}, +, \cdot)$ é um anel comutativo; $\mathbb{Z}^\times = (\{\pm 1\}, \cdot)$;

2. se $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, então $(\mathbb{K}, +, \cdot)$ é um anel comutativo; $\mathbb{K}^\times = (\mathbb{K} \setminus \{0\}, \cdot)$;
3. $(M_n(\mathbb{R}), +, \cdot)$ é um anel não comutativo se $n > 1$; $M_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$;
4. mais geralmente, se A é um anel, então $(M_n(A), +, \cdot)$ é um anel com as operações de soma e produto dadas pelas mesmas fórmulas que em $M_n(\mathbb{R})$;
5. $(\mathbb{Z}_m, +, \cdot)$ é um anel comutativo em que o produto é definido pela fórmula $\underline{i} \cdot \underline{j} \coloneqq \underline{i \cdot j}$ (*cf.* Exercício 1.2.1); tem-se

$$\mathbb{Z}_m^\times = \{\underline{k} \in \mathbb{Z}_m \mid \mathrm{MDC}(k, m) = 1\},$$

pois

$$xk \equiv 1 \mod m \quad \text{tem solução } \textit{sse } \mathrm{MDC}(k,m) = 1;$$

6. se $(G,+)$ é um grupo abeliano, então

$$\mathrm{End}(G) = \{f : G \to G \mid f \text{ é um homomorfismo de grupo}\}$$

é um anel, onde a soma de $f, g \in \mathrm{End}(G)$ é dada por $(f+g)(x) = f(x) + g(x)$ e o produto é a composição $f \circ g$.

Definição 1.7. *Um elemento $a \in A$ diz-se um* divisor de zero à esquerda (direita) *se existe $x \in A \setminus \{\mathbf{0}\}$* t.q. *$ax = \mathbf{0}$ (*resp.*) $xa = \mathbf{0}$. Se a é divisor de zero à esquerda e à direita, diz-se simplesmente que é um* divisor de zero.

Exemplo 1.8. Em $\mathbb{Z}_6$, $\underline{3}$ é um divisor de zero, pois $\underline{2} \cdot \underline{3} = \underline{3} \cdot \underline{2} = 0$.

Definição 1.9. *Se A é um anel comutativo sem divisores de zero* t.q. *$\mathbf{1} \neq \mathbf{0}$, diz-se que A é um um* domínio integral. *Um anel D* t.q. *$\mathbf{1} \neq \mathbf{0}$ e $D^\times = D \setminus \{\mathbf{0}\}$ diz-se um* anel de divisão. *Um anel de divisão comutativo diz-se um* corpo.

Exemplos 1.10 (Domínios integrais, corpos e anéis de divisão)**.**

1. $\mathbb{Z}$ é um domínio integral;
2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ e $\mathbb{F}_p \coloneqq \mathbb{Z}_p$ (p primo) são corpos;
3. o anel de polinómios $(\mathbb{Z}[x], +, \cdot)$ é um domínio integral;
4. se n não é primo, $\mathbb{Z}_n$ não é um domínio integral;
5. o espaço vectorial real $\mathbb{H} = \mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot i \oplus \mathbb{R} \cdot j \oplus \mathbb{R} \cdot k$ tem uma estrutura de anel em que o produto é determinado por: $i^2 = j^2 = k^2 = -1$, $ij = k$; e pelo facto de a multiplicação por elementos de $\mathbb{R} \cdot 1$ coincidir com a multiplicação por escalares (como espaço vectorial-$\mathbb{R}$). $\mathbb{H}$ é um anel de divisão (não comutativo). Diz-se o anel dos *quaterniões*.

Exemplo 1.11. Seja G um grupo. Consideremos o conjunto $\mathbb{Z}(G)$ das *somas formais* de G com coeficientes em $\mathbb{Z}$, *i.e.*, é o conjunto dos símbolos $\sum_{i=1}^n r_i g_i$ *t.q.* $n \in \mathbb{N}$, $r_i \in \mathbb{Z}$, $g_i \in G$, com as seguintes identificações e operações:

$$\sum_{i=1}^n r_i g_i + 0 \cdot g = \sum_{i=1}^n r_i g_i, \quad \forall g \in G$$

$$\sum_{i=1}^n r_i g_i + \sum_{i=1}^n s_i g_i = \sum_{i=1}^n (r_i + s_i) g_i$$

$$\sum_{i=1}^n r_i g_i + \sum_{i=n+1}^m r_i g_i = \sum_{i=1}^m r_i g_i$$

$$\sum_{i=1}^n r_i g_i \cdot \sum_{j=1}^m s_j h_j = \sum_{i=1}^n \sum_{j=1}^m r_i s_j g_i h_j$$

Com esta estrutura, $\mathbb{Z}(G)$ é um anel que é comutativo *sse* G o é e, em geral, tem divisores de zero – Exercício 2.1.2.

Exemplo 1.12. Mais geralmente, se A é um anel e G é um grupo, define-se o anel de grupo de G com coeficientes em A como o conjunto das somas formais

$$A(G) = \left\{ \sum_{i=1}^n a_i g_i \mid a_i \in A, g_i \in G, n \in \mathbb{N} \right\}$$

com as identificações e operações análogas às do exemplo anterior. O anel $A(G)$ é comutativo *sse* A e G o são.

Definição 1.13. *Sejam A, B anéis. Uma função $f\colon A \to B$ diz um* homomorfismo de anéis *se*

$$\forall a, b \in A \;\; f(a+b) = f(a) + f(b), \qquad f(ab) = f(a)f(b), \qquad f(\mathbf{1}_A) = \mathbf{1}_B.$$

Nota 1.14. Tal como referido anteriormente, em [**Hun74**] ou [**FR04**] consideram-se anéis sem identidade e, por isso, não se exige a condição $f(\mathbf{1}_A) = \mathbf{1}_B$ na definição de homomorfismo de anéis.

Exemplos 1.15.

1. Se A é um anel, a função $f\colon \mathbb{Z} \to A$ definida por
$$f(n) \coloneqq n \cdot \mathbf{1}_A$$
é um homomorfismo de anéis e é único. Portanto, para todo o anel A, $|\operatorname{Hom}(\mathbb{Z}, A)| = 1$.
2. A função $f\colon \mathbb{Z} \to \mathbb{Z}_m$ definida por
$$f(n) \coloneqq \underline{n}$$
é um homomorfismo sobrejectivo de anéis.
3. A inclusão $i\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$ é um homomorfismo injectivo de anéis.

Definição 1.16. *Seja A um anel. Um* subanel *de A é um subconjunto $B \subset A$ tal que a inclusão $B \subset A$ é um homomorfismo de anéis $(B, +_A, \cdot_A) \to (A, +_A, \cdot_A)$. Em particular, tem-se $\mathbf{0}_A, \mathbf{1}_A \in B$.*

Exemplos 1.17.

1. $\mathbb{Z} \subset \mathbb{Q}$ é um subanel;
2. se A é um anel, o centro de A, definido por
$$Z(A) \coloneqq \{x \in A \mid \forall a \in A, xa = ax\} \;,$$
é um subanel de A pois $\mathbf{0}_A, \mathbf{1}_A \in Z(A)$ e
$$\forall a \in A, \quad \begin{cases} xa = ax \\ ya = ay \end{cases} \Rightarrow \begin{cases} (x \pm y)a = a(x \pm y) \\ (xy)a = (xa)y = a(xy) \end{cases}$$

Exercícios

2.1.1. Considere o grupo abeliano $G = \mathbb{Z} \oplus \mathbb{Z}$. Mostre que $\operatorname{End}(G)$ é um anel não comutativo.

2.1.2. Seja G um grupo. Mostre que $\mathbb{Z}(G)$ é um anel. Dê um exemplo em que $\mathbb{Z}(G)$ tem divisores de zero.

2.1.3. Seja $\mathbb{H}$ o anel dos quaterniões e recorde que $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ é um grupo. Qual a diferença entre o anel $\mathbb{H}$ e o anel de grupo $\mathbb{R}(\mathbb{H}_8)$?

2.1.4. (Fórmula do caloiro) Seja A um anel comutativo de característica um primo p. Mostre que $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$, para $n \geq 0$.

2.1.5. Seja A um anel comutativo de característica um primo p. Mostre que $f : A \to A$, $f(a) = a^p$ é um homomorfismo de anéis.

2.1.6. Um elemento a num anel A diz-se *nilpotente* se $a^n = 0$ para algum n. Prove que num anel comutativo, se a e b são nilpotentes, então $a + b$ também é nilpotente. Mostre que este resultado pode ser falso se o anel não for comutativo.

2. Ideais e anéis quociente

Definição 2.1. *Seja A um anel. Um* ideal à esquerda (direita) *de A é um subgrupo abeliano $I < A$* t.q.

$$\forall a \in A,\, \forall x \in I,\, ax \in I \qquad \textit{(respectivamente } xa \in I\textit{)}.$$

*Um ideal bilateral (*i.e.*, ideal à esquerda e à direita) diz-se simplesmente um* ideal.

Exemplos 2.2.

1. $I = \langle n \rangle < \mathbb{Z}$ é um ideal. Todos os ideais de $\mathbb{Z}$ são desta forma;
2. Seja $I_k < M_n(\mathbb{R})$ o conjunto das matrizes cujas colunas são todas nulas excepto a k-ésima. Então I_k é um ideal à esquerda:

   $$A \in I_k \quad \Leftrightarrow \quad \forall i \neq k \quad Ae_i = \mathbf{0}.$$

   Seja $B \in M_n(\mathbb{R})$, então

   $$(BA)e_i = B(Ae_i) = \mathbf{0}.$$

   No entanto, I_k não é um ideal à direita, como ilustra o seguinte exemplo no caso $n = 2$: temos

   $$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I_1$$

   mas

   $$A \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \notin I_1.$$

3. Seja $f\colon A \to B$ um homomorfismo de anéis, então $\ker f$ é um ideal de A.
4. Seja A um anel se seja $a \in A$, então

   $$Aa \coloneqq \{xa \mid x \in A\} \text{ é um ideal à esquerda,}$$
   $$aA \coloneqq \{ax \mid x \in A\} \text{ é um ideal à direita.}$$

Definição 2.3 (Ideais principais)**.** *Os ideais aA e Aa dizem-se* ideais principais à esquerda e à direita*, respectivamente.*

Exemplo 2.4. Em $\mathbb{Z}$ todos os ideais são principais.

Definição 2.5. *Um ideal I (à esquerda, direita) diz-se* próprio *se $I \neq A$.*

Observação 2.6. Um ideal $I \neq \{\mathbf{0}\}$ é próprio *sse* I não contém nenhum elemento invertível.

Exemplo 2.7. Se D é um anel de divisão (*e.g.*, um corpo) então D não tem nenhum ideal próprio não nulo (à esquerda ou à direita).

Proposição 2.8. *Seja A um anel e seja $I \subset A$* t.q. *$I \neq \varnothing$. Então, I é um ideal esquerdo (direito)* sse *$\forall x, y \in I$, $\forall a \in A$*

(i) $x, y \in I \Rightarrow x - y \in I$

(ii) $x \in I, a \in A \Rightarrow ax \in I$ *(resp.* $xa \in I$*).*

Proposição 2.9. *Sejam $\{I_k \mid k \in K\}$ ideais (esquerdos, direitos) de um anel. Então $\cap_{k\in K} I_k$ é um ideal (resp. esquerdo, direito).*

Definição 2.10. *Seja A um anel e seja $X \subset A$. O* ideal gerado *por X é*

$$(X) \coloneqq \bigcap_{I \textit{ ideal t.q. } X \subset I} I.$$

Notação 2.11. $(x_1, \ldots, x_n) \coloneqq (\{x_1, \ldots, x_n\})$.

Proposição 2.12. $(x) = \{\sum_{i=1}^{n} a_i x b_i \mid a_i, b_i \in A, n \in \mathbb{N}\}$.

Demonstração. Seja $J = \{\sum_{i=1}^{n} a_i x b_i \mid a_i, b_i \in A, n \in \mathbb{N}\}$. Para ver que $(x) = J$, temos de verificar que (1º) J é um ideal que contém x e (2º) que qualquer outro ideal I contendo x também contém J.

(1º) Dados $\sum_{i=1}^{n} a_i x b_i \in J$ e $\sum_{j=1}^{m} c_j x d_j \in J$ com $a_i, b_i, c_j, d_j \in A$, pondo $a_{n+j} = -c_j$ e $b_{n+j} = d_j$, temos

$$\sum_{i=1}^{n} a_i x b_i - \sum_{j=1}^{m} c_j x d_j = \sum_{i=1}^{n+m} a_i x b_j \in J;$$

se $c \in A$, temos

$$c\Big(\sum_{i=1}^{n} a_i x b_i\Big) = \sum_{i=1}^{n} (c a_i) x b_i \in J \qquad \text{e} \qquad \Big(\sum_{i=1}^{n} a_i x b_i\Big) c = \sum_{i=1}^{n} a_i x (b_i c) \in J$$

logo J é um ideal (Proposição 2.8). Pondo $n = 1$, $a_1 = b_1 = \mathbf{1}_A \in A$, obtemos $x = \mathbf{1}_A \cdot x \cdot \mathbf{1}_A \in J$.

(2º) Seja I um ideal de A contendo x. Pelas propriedades de fecho das operações de um ideal, I contém todos os elementos de J. □

Definição 2.13. *Seja A um anel e sejam $X_1, \ldots, X_n \subset A$ subconjuntos não vazios. Define-se*

$$X_1 + \cdots + X_n \coloneqq \{x_1 + \cdots + x_n \mid x_i \in X_i\}$$

$$X_1 \cdots X_n \coloneqq \left\{ \sum_{i=1}^{m} x_{1,i} \cdots x_{n,i} \mid x_{j,i} \in X_j, m \in \mathbb{N} \right\}$$

Notação 2.14. $aX \coloneqq \{a\}X$, $Xa \coloneqq X\{a\}$, $X^n = \underbrace{X \cdots X}_{n \text{ vezes}}$.

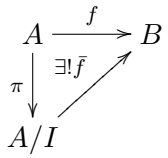
Proposição 2.15. *Sejam $X, Y, Z \subset A$ ideais (esquerdos, direitos). Então*

(a) $X + Y$ e XY são ideais (resp. esquerdos, direitos);
(b) $(X + Y) + Z = X + (Y + Z)$;
(c) $(XY)Z = X(YZ)$;
(d) $X(Y + Z) = XY + XZ$;
(e) $(X + Y)Z = XZ + YZ$.

Teorema 2.16 (Anel quociente)**.** *Seja $I \subset A$ um ideal. Consideremos o grupo quociente A/I e a projecção canónica $\pi\colon A \to A/I$. Então A/I tem uma estrutura de anel dada por*

$$\pi(a)\pi(b) \coloneqq \pi(ab).$$

Se A é comutativo, A/I também o é. A projecção π é um homomorfismo sobrejectivo de anéis t.q. $\ker \pi = I$ *e tem a seguinte propriedade universal: dado $f \in \mathrm{Hom}(A, B)$* t.q. $I \subset \ker f$ *existe um único $\bar{f} \in \mathrm{Hom}(A/I, B)$ que faz comutar o diagrama seguinte*



Tem-se $\ker \bar{f} = \pi(\ker f)$ *e* $\operatorname{im} \bar{f} = \operatorname{im} f$.

Demonstração. 1. O produto está bem definido:

$$\pi(a) = \pi(a') \ \wedge \ \pi(b) = \pi(b') \Leftrightarrow a - a', b - b' \in I.$$
$$\Rightarrow a'b' = ab + \underbrace{(a' - a)b}_{\in I} + \underbrace{a'(b' - b)}_{\in I} \Rightarrow \pi(a'b') = \pi(ab).$$

A identidade em A/I é $\pi(\mathbf{1}_A)$: $\pi(a)\pi(\mathbf{1}_A) = \pi(a\mathbf{1}_A) = \pi(a) = \pi(\mathbf{1}_A a) = \pi(\mathbf{1}_A)\pi(a)$.

2. As propriedades do produto no quociente seguem agora directamente das propriedades do produto em A. Segue que A/I é um anel e é comutativo se A o for.
3. Por construção, π é um homomorfismo sobrejectivo *t.q.* $\ker \pi = I$. Dado f como no enunciado, existe um único homomorfismo de grupos abelianos $\bar{f}$ que faz comutar o diagrama acima. Resta só verificar que $\bar{f}$ é um homomorfismo de anéis, mas isso segue também da construção:
$$\bar{f}(\pi(a))\bar{f}(\pi(b)) = f(a)f(b) = f(ab) = \bar{f}(\pi(ab)) = \bar{f}(\pi(a)\pi(b)),$$
$$\bar{f}(\pi(\mathbf{1}_A)) = f(\mathbf{1}_A) = \mathbf{1}_B.$$ □

Exemplo 2.17. O anel $\mathbb{Z}_m$ é um anel quociente: $\mathbb{Z}_m = \mathbb{Z}/(m)$. A propriedade universal do quociente diz que dar um homomorfismo de $\mathbb{Z}_m$ para um anel A é equivalente a dar $f \in \mathrm{Hom}(\mathbb{Z}, A)$ *t.q.* $(m) \subset \ker f$. O único homomorfismo $\mathbb{Z} \to A$ é dado por $1 \mapsto \mathbf{1}_A$, portanto há um homomorfismo $\mathbb{Z}_m \to A$ se $m \cdot \mathbf{1}_A = \mathbf{0}_A$. Neste caso, o homomorfismo é dado por $\bar{i} \mapsto i \cdot \mathbf{1}_A$. Se $m \cdot \mathbf{1}_A \neq \mathbf{0}_A$, $\mathrm{Hom}(\mathbb{Z}_m, A) = \varnothing$.

Definição 2.18. *Seja A um anel. Define-se a* característica *de A como*
$$\mathrm{car}\, A = \min\{m \in \mathbb{N} \mid m \cdot \mathbf{1}_A = \mathbf{0}_A\},$$
se o mínimo existir. Caso contrário, define-se $\mathrm{car}\, A = 0$.

Exemplos 2.19.

1. $\mathrm{car}(\mathbb{Z}_m) = m$;
2. $\mathrm{car}(\mathbb{Z}) = 0$;
3. $\mathrm{car}(\mathbb{Q}) = \mathrm{car}(\mathbb{R}) = \mathrm{car}(\mathbb{C}) = 0$;
4. $\mathrm{car}\, M_n(A) = \mathrm{car}(A)$.

Proposição 2.20. *Seja A um anel* t.q. $\mathrm{car}(A) = m > 0$. *Então o homomorfismo $\varphi\colon \mathbb{Z}_m \to A; \underline{i} \to i \cdot \mathbf{1}_A$ é injectivo.*

*Se A não tem divisores de zero (*e.g.*, A é um domínio integral), então* $\mathrm{car}\, A = 0$ *ou* $\mathrm{car}\, A$ *é primo.*

Demonstração. A primeira asserção segue de
$$\varphi(\underline{i}) = \mathbf{0}_A \Leftrightarrow i \cdot \mathbf{1}_A = \mathbf{0}_A \Leftrightarrow i \in \{k \in \mathbb{N} \mid k \cdot \mathbf{1}_A = \mathbf{0}_A\} \Rightarrow i \geq m,$$
se $i > 0$. Suponhamos que A não tem divisores de zero e seja $m = d_1 d_2 > 0$ com $d_i > 0$. Então
$$\mathbf{0}_A = m \cdot \mathbf{1}_A = (d_1 \cdot \mathbf{1}_A)(d_2 \cdot \mathbf{1}_A) = (d_2 \cdot \mathbf{1}_A)(d_1 \cdot \mathbf{1}_A) \Rightarrow d_1 \cdot \mathbf{1}_A = \mathbf{0}_A \vee d_2 \cdot \mathbf{1}_A = \mathbf{0}_A$$
$$\Rightarrow m = d_1 \vee m = d_2.$$ □

Corolário 2.21 (Teoremas de Isomorfismo)**.**

1. $f \in \mathrm{Hom}(A, B)$ induz um isomorfismo
$$\bar{f}\colon \frac{A}{\ker f} \xrightarrow{\cong} \mathrm{im}\, f$$
2. sejam $I \subset J$ ideais de um anel A. Então J/I é um ideal de A/I e existe um isomorfismo de anéis
$$\frac{A/I}{J/I} \cong \frac{A}{J}.$$

Demonstração. Os isomorfismos de grupos abelianos correspondentes são também homomorfismos de anéis. □

O resultado seguinte mostra que todos os ideais de A/I são forma acima: J/I, com $J \supset I$ ideal.

Corolário 2.22. *Sejam A um anel, $I \subset A$ um ideal e $\pi\colon A \to A/I$ a projecção canónica. Então existe uma correspondência bijectiva*

$$\{J \mid I \subset J \subset A \text{ é um ideal}\} \xrightarrow{\pi} \left\{\bar{J} \mid \bar{J} \subset A/I \text{ é um ideal}\right\}.$$

Demonstração. Segue do lema seguinte. □

Lema 2.23. *Seja $f\colon A \to B$ um homomorfismo de anéis. Então,*

(a) se $J \subset B$ é um ideal, então $f^{-1}(J) \subset A$ é um ideal (esquerdo, direito, bilateral);

(b) se f é sobrejectivo e $I \subset A$ é um ideal, então $f(I)$ é um ideal (esquerdo, direito, bilateral).

Demonstração.

(a) $f(x) \in J \Rightarrow \forall a \in A\ f(ax) = f(a)f(x) \in J,\ f(xa) = f(x)f(a) \in J$;

(b) sejam $y = f(x) \in f(I)$ e $b = f(a) \in B$. Temos

$$by = f(ax) \in f(I) \ni yb = f(xa).$$ □

Definição 2.24. *Seja A um anel. Um ideal* próprio *$P \subset A$ diz-se* primo *se para todos os ideais $I, J \subset A$,*

$$IJ \subset P \Rightarrow I \subset P \ \vee\ J \subset P.$$

Lema 2.25. *Seja A um anel.*

(a) Se A é comutativo e $I \subset A$ é um ideal, então I é primo sse

$$\forall a, b \in A \quad ab \in I \Rightarrow a \in I \ \vee\ b \in I. \tag{2.1}$$

(b) Se A é não comutativo, então a condição (2.1) *é suficiente para que I seja primo (mas não necessária - ver Exercício 2.2.9).*

Demonstração.

$\boxed{\Leftarrow}$ Sejam J, K ideais *t.q.* $JK \subset I$. Suponhamos $K \not\subset I$. Seja $y \in K \setminus I$. Temos

$$\forall x \in J \quad xy \in I \Rightarrow x \in I$$
$$\therefore J \subset I.$$

Nota: Nesta implicação não usámos a comutatividade de A.

$\boxed{\Rightarrow}$ Se $ab \in I$ então, pela comutatividade de A, $(ab) = (a)(b) \subset I$, portanto

$$(a) \subset I \quad \vee \quad (b) \subset I \quad \Leftrightarrow \quad a \in I \quad \vee \quad b \in I.$$ □

Exemplos 2.26.

1. Seja A um domínio integral. Então $(\mathbf{0})$ é um ideal primo.
2. Seja $A = \mathbb{Z}$. Os ideais $I \subset \mathbb{Z}$ são da forma $I = (m)$ e, se $m \neq 0$, tem-se (m) primo *sse* m é primo, pois
$$\forall a, b \in \mathbb{Z} \quad ab \in (m) \Rightarrow a \in (m) \vee b \in (m)$$
$$\Leftrightarrow \quad \forall a, b \in \mathbb{Z} \quad m \mid ab \Rightarrow m \mid a \vee m \mid b.$$
3. Seja $A = \mathbb{Z}[x]$ e $I = (x)$, então I é um ideal primo, pois
$$f(x)g(x) \in I \Leftrightarrow x \mid f(x)g(x) \Leftrightarrow x \mid f(x) \vee x \mid g(x).$$

Definição 2.27. *Seja A um anel. Um ideal $I \subset A$ diz-se* maximal *se $I \neq A$ e*

$$\forall_{\text{ideal } J \subset A} \quad J \supset I \Rightarrow J = A \vee J = I.$$

De forma análoga, define-se ideal esquerdo maximal *e* ideal direito maximal.

Exemplos 2.28. 1. Sejam $A = \mathbb{Z}$, $I = (m)$ e $J = (n)$. Então $I \subset J$ *sse* $n \mid m$, logo I é maximal *sse* m é primo, ou seja, *sse* I é primo.

2. Sejam $A = \mathbb{R}[x, y]$ e $I = (x, y)$. Temos

$$\begin{aligned} J \supsetneq I \quad &\Rightarrow \quad \exists\, a \in \mathbb{R} \setminus \{0\} : a \in J \\ &\Rightarrow \quad J \supset (a, x, y) = A, \end{aligned}$$

logo I é maximal.

Teorema 2.29. *Seja A um anel e seja $M \subset A$ um ideal* t.q. *A/M é um anel de divisão. Então M é maximal.*

Demonstração. Seja $I \subset A$ um ideal *t.q.* $I \supsetneq M$ e sejam $a \in I \setminus M$ e $\pi \colon A \to A/M$ a projecção canónica. Então $\pi(a) \neq 0$, logo existe $b \in A$ *t.q.*

$$\pi(a)\pi(b) = \mathbf{1}_{A/M} = \pi(\mathbf{1}_A),$$

logo $ab - \mathbf{1}_A \in M$ e portanto $\mathbf{1}_A \in I$, ou seja, $I = A$. □

Exercícios

2.2.1. Dê um exemplo de um anel A e $a \in A$ tais que $\{xay \mid x, y \in A\}$ não é um ideal.

2.2.2. Mostre que conjunto $J_k \coloneqq \{A \in M_n(\mathbb{R}) \mid A^T e_i = \mathbf{0}$, para $i \neq k\}$, com $k = 1, \ldots, n$ fixo, é um ideal à direita mas não à esquerda.

2.2.3. Demonstre a Proposição 2.9, i.e., se $\{I_k \mid k \in K\}$ são ideais (esquerdos, direitos) de um anel A, mostre que $\cap_{k \in K} I_k$ é um ideal (resp. esquerdo, direito).

2.2.4. Demonstre a Proposição 2.15.

2.2.5. Mostre que um anel A é um anel de divisão *sse* A não contém nenhum ideal esquerdo próprio.
Sugestão: Use o Exercício 1.1.2.

2.2.6. Seja A um anel comutativo e seja N o conjunto dos elementos nilpotentes de A (ver Exercício 2.1.6)
(a) Mostre que N é um ideal.
(b) Mostre que A/N é um anel sem elementos nilpotentes não nulos.

2.2.7. Seja A um anel comutativo e $I \subset A$ um ideal. Define-se o *radical* de I por

$$\operatorname{rad}(I) = \{a \in A \mid \exists\, n \text{ t.q. } a^n \in I\}.$$

Mostre que $\operatorname{rad}(I)$ é um ideal.

2.2.8. Seja A um anel e seja $B = M_n(A)$ o anel das matrizes $n \times n$ de entradas em A. Mostre que $J \subset B$ é um ideal *sse* $J = M_n(I)$ (conjunto das matrizes de entradas em I) para algum ideal $I \subset A$.
Sugestão: Dado J, defina I como o conjunto dos elementos de A que são a entrada $(1, 1)$ de alguma matriz $X \in J$ e use as *matrizes elementares* $E_{i,j}$ cujas entradas são todas nulas excepto a (i, j) que vale $\mathbf{1}$. Verifique que $E_{i,j} X E_{k,l} = x_{j,k} E_{i,l}$, onde $X = [x_{ij}]$.

2.2.9. Seja D um anel de divisão e seja $A = M_n(D)$.
(a) Mostre que A não tem ideais próprios, i.e., $\{\mathbf{0}\}$ é um ideal maximal.
Sugestão: use o exercício anterior.
(b) Mostre que A contém divisores de zero. Conclua que
(i) $S \cong S/\{\mathbf{0}\}$ não é um anel de divisão;
(ii) $\{\mathbf{0}\}$ é um ideal primo que não satisfaz a condição (2.1) do Lema 2.25.

2.2.10. Seja $f : A \to B$ um homomorfismo sobrejectivo de anéis e seja $K = \ker f$. Demonstre as seguintes afirmações.

(a) Se $P \subset A$ é um ideal primo contendo K, então $f(P) \subset B$ é um ideal primo.

(b) Se $Q \subset B$ é um ideal primo, então $f^{-1}(Q) \subset A$ é um ideal primo que contém K.

(c) A seguinte correspondência é bijectiva

$$\{P \subset A \text{ ideal primo t.q. } K \subset P\} \longrightarrow \{Q \subset B \text{ ideal primo}\}$$
$$P \longmapsto f(P)$$

(d) Dado um ideal $I \subset A$, qualquer ideal primo em A/I é da forma P/I com $P \subset A$ um ideal primo contendo I.

2.2.11. Determine todos os ideais primos e ideais maximais do anel $\mathbb{Z}_m$

2.2.12. Seja A um anel comutativo e seja $I \subset A$ um ideal contido numa união finita de ideais primos, i.e., $I \subset P_1 \cup \cdots \cup P_n$, onde P_i é primo. Mostre que $I \subset P_i$ para qualquer $i = 1, \ldots, n$.

Sugestão: Por absurdo, assuma que $I \cap P_j \not\subset \cup_{i \neq j} P_i$ para algum j e seja $a_j \in (I \cap P_j) \setminus \big(\cup_{i \neq j} P_i\big)$. Verifique que $a \coloneqq a_1 + a_2 a_3 \cdots a_n \in I$ mas $a \notin P_1 \cup \cdots \cup P_n$.

3. Conjuntos parcialmente ordenados: lema de Zorn

Definição 3.1. *Uma relação de* ordem parcial *num conjunto X é uma relação $\preceq$* t.q.

(i) $a \preceq a$

(ii) $a \preceq b \wedge b \preceq c \Rightarrow a \preceq c$

(iii) $a \preceq b \wedge b \preceq a \Rightarrow a = b$.

Exemplos 3.2.

1. A relação de ordem habitual em $\mathbb{R}$ é uma relação de ordem parcial;
2. Seja X um conjunto. Dados $A, B \subset X$, definindo
$$A \preceq B \Leftrightarrow A \subset B,$$
obtém-se uma relação de ordem parcial no conjunto, $\mathcal{P}(X)$, das partes de X.

Observação 3.3. Podemos ter $A, B \in \mathcal{P}(X)$ sem que $A \preceq B$, nem $B \preceq A$. Ou seja, A, B podem não ser comparáveis.

Se $(X, \preceq)$ é um conjunto parcialmente ordenado *t.q.*
$$\forall a, b \in X \quad a \preceq b \quad \vee \quad b \preceq a,$$
a relação de ordem diz-se *total*.

Exemplo 3.4. $(\mathbb{R}, \leq)$ é um conjunto totalmente ordenado.

Definição 3.5. *Seja $(X, \preceq)$ um conjunto parcialmente ordenado.*

1. Se $Y \subset X$ é t.q. *$(Y, \preceq)$ é totalmente ordenado, diz-se que Y é uma* cadeia *em X.*

2. Um elemento $m \in X$ diz-se maximal *se*
$$\forall x \in X \quad m \preceq x \Rightarrow m = x.$$

3. Se $Z \subset X$ é t.q. *$Z \neq \varnothing$, diz-se que $b \in X$ é um* majorante *de Z se*
$$\forall z \in Z \quad z \preceq b.$$

Teorema 3.6 (Lema de Zorn)**.** *Seja $(X, \preceq)$ um conjunto parcialmente ordenado,* t.q. *$X \neq \varnothing$ e* t.q. *toda a cadeia em X é* limitada *(*i.e.*, tem um majorante). Então X tem um elemento maximal.*

Teorema 3.7. *Seja $I \subset A$ um ideal próprio (esquerdo, direito). Então existe um ideal maximal $M \supset I$ (resp. esquerdo, direito).*

Demonstração. Seja X o conjunto dos ideais (esquerdos, direitos) próprios de A que contêm I munido da relação de inclusão. $X \neq \varnothing$ pois $I \in X$. Seja $Y \subset X$ uma cadeia. Definimos
$$J \coloneqq \bigcup_{K \in Y} K.$$
Vejamos que J é um ideal (resp. esquerdo, direito):
$$x, y \in J \Leftrightarrow \exists K_1, K_2 \in Y : x \in K_1, y \in K_2.$$
Podemos supor $K_1 \subset K_2$, logo $x - y \in K_2 \subset J$. Seja agora $a \in A$ e $x \in J$. Temos
$$aJ \subset J \wedge Ja \subset J, \qquad (\text{resp. } aJ \subset J,\ Ja \subset J)$$
pois $\forall K \in Y$, $aK, Ka \subset K$. Portanto J é um ideal (resp. esquerdo, direito).

Como $\forall K \in Y$, $K \neq A$, temos $\mathbf{1}_A \notin K$, $\forall K \in Y$ e assim $\mathbf{1}_A \notin J$. Portanto $J \in X$, pois claramente $I \subset J$. Concluímos que J é um majorante de Y, porque $J \supset K$ para todo o $K \in Y$, pela definição de J.

Pelo lema de Zorn, existe um ideal maximal $M \supset I$. □

4. Produto de anéis

Definição 4.1. *Seja $\{A_i \mid i \in I\}$ uma família de anéis. Define-se o seu* produto directo *como o produto directo de grupos abelianos $\prod_{i\in I}(A_i, +)$, munido do seguinte produto:*

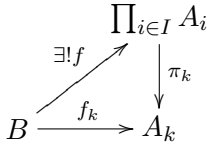
$$(a_i)_{i\in I} \cdot (b_i)_{i\in I} \coloneqq (a_i \cdot b_i)_{i\in I}.$$

Observação 4.2. Para cada $k \in I$, a projecção $\pi_k \colon \prod_{i\in I} A_i \to A_k$ é um homomorfismo de anéis. No entanto, o homomorfismo de grupos abelianos $i_k \colon A_k \to \prod_{i\in I} A_i; a \mapsto (a_i)_{i\in I}$ *t.q.*

$$a_i = \begin{cases} a, & i = k \\ \mathbf{0}, & i \neq k \end{cases}$$

não é um homomorfismo de anéis, pois $i_k(\mathbf{1}_{A_k}) \neq \mathbf{1}$.

Teorema 4.3 (Propriedade universal do produto directo)**.** *Seja B um anel e sejam $f_i \colon B \to A_i$, $i \in I$, homomorfismos de anéis, então existe um único homomorfismo $f \colon B \to \prod_{i\in I} A_i$ que faz comutar o diagrama seguinte*



onde $\pi_k \colon \prod_{i\in I} A_i \to A_k$ é a projecção no k-ésimo factor.

Demonstração. Análogo ao caso do produto directo de grupos. □

Observação 4.4. A asserção da proposição significa que dar um homomorfismo $f \colon B \to \prod_{i\in I} A_i$ é equivalente a dar uma família de homomorfismos $f_i \colon B \to A_i$, $i \in I$.

Teorema 4.5 (Teorema Chinês dos Restos)**.** *Sejam $I_1, \ldots, I_n$ ideais de um anel A* t.q. *$A = I_i + I_j$, $\forall i \neq j$. Dados $a_1, \ldots, a_n \in A$ existe $a \in A$* t.q.

$$a \equiv a_j \mod I_j, \quad j = 1, \ldots, n.$$

Além disso, o elemento a é único $\mod I_1 \cap \cdots \cap I_n$.

Demonstração.

1. Começamos por provar $A = I_1 + I_2 \cap I_3 \cap \cdots \cap I_n$.
   Temos
   $$\begin{aligned} A = A^2 = (I_1 + I_2)(I_1 + I_3) &\subset I_1 + I_2 \cap I_3 \\ \Rightarrow A &= I_1 + I_2 \cap I_3. \end{aligned}$$
   Suponhamos $A = I_1 + I_2 \cap I_3 \cap \cdots \cap I_{k-1}$. Temos
   $$A = A^2 = (I_1 + I_k)(I_1 + I_2 \cap I_3 \cap \cdots \cap I_{k-1}) \subset I_1 + I_2 \cap I_3 \cap \cdots \cap I_k.$$
   Concluímos que $A = I_1 + I_2 \cap I_3 \cap \cdots \cap I_n$.
2. Provamos a primeira asserção do Teorema.
   Por indução em n: suponhamos que o resultado é válido para $n-1$. Sejam $a_1, \ldots, a_n \in A$. Então existe $x \in A$ *t.q.*
   $$x \equiv a_j \mod I_j, \quad j = 2, \ldots, n.$$
   Temos
   $$\begin{aligned} A &= I_1 + I_2 \cap I_3 \cap \cdots \cap I_n \\ \Rightarrow &\exists\, a_1' \in I_1, a_1'' \in I_2 \cap I_3 \cap \cdots \cap I_n : a_1 = x + a_1' + a_1''. \end{aligned}$$

Seja $a \coloneqq x + a_1''$, temos

$$\begin{aligned} a &\equiv x \equiv a_j \mod I_j, \quad j = 2, \dots, n \\ a &\equiv a_1 \mod I_1. \end{aligned}$$

3. Provamos a unicidade de a:

$$\begin{aligned} & a \equiv a_j \equiv a' \mod I_j, j = 1, \dots, n \\ \Rightarrow\, & a - a' \in I_1 \cap \cdots \cap I_n \\ \Leftrightarrow\, & a \equiv a' \mod I_1 \cap \cdots \cap I_n. \end{aligned}$$

□

Exemplo 4.6. Sejam $I_1, \dots, I_n$ ideais de um anel A *t.q.* $A = I_i + I_j$, $i \neq j$. Seja $\varphi\colon A \to \prod_{j=1}^n A/I_j$ o homomorfismo determinado pelas projecções $\pi_j\colon A \to A/I_j$.

Pelo teorema Chinês dos Restos (Teorema 4.5), φ é sobrejectivo e $\ker \varphi = \cap_{i \in I} \ker \pi_i = I_1 \cap \cdots \cap I_n$. Logo, φ induz um isomorfismo

$$\underline{\varphi}\colon A/(I_1 \cap \cdots \cap I_n) \xrightarrow{\cong} \prod_{j=1}^n A/I_j.$$

Exemplo 4.7. Sejam $m_1, \dots, m_r \in \mathbb{N}$ *t.q.* $\mathrm{MDC}(m_i, m_j) = 1$, $i \neq j$, e seja $m = m_1 \cdots m_r$. Então, aplicando o resultado do exemplo anterior com $A = \mathbb{Z}_m = \mathbb{Z}/(m)$ e $I_j = (\underline{m_j}) = (m_j)/(m) \subset \mathbb{Z}/(m)$, obtemos

$$\mathbb{Z}_m \cong \prod_{j=1}^r \frac{\mathbb{Z}/(m)}{(m_j)/(m)} \cong \prod_{j=1}^r \frac{\mathbb{Z}}{(m_j)} = \prod_{j=1}^r \mathbb{Z}_{m_j}.$$

Exercícios

2.4.1. Sejam A e B anéis. Mostre que $(A \times B)^\times = A^\times \times B^\times$.

2.4.2. Sejam A e B anéis, e seja K um ideal de $A \times B$.
   (a) Justifique que $I = \{a \in A \mid (a, \mathbf{0}) \in K\}$ é um ideal de A e $J = \{b \in B \mid (\mathbf{0}, b) \in K\}$ é um ideal de B.
   (b) Dado $(a, b) \in K$, mostre que $(a, \mathbf{0}) \in K$ e $(\mathbf{0}, b) \in K$.
   (c) Mostre que $K = I \times J$. Portanto, qualquer ideal de $A \times B$ é desta forma.
   (d) Generalize a alínea anterior para ideais no produto de anéis $A_1 \times \cdots \times A_n$.

2.4.3. Sejam A e B anéis, $I \subset A$ e $J \subset B$ ideais. Mostre que $(A \times B)/(I \times J) \cong (A/I) \times (B/J)$, através de um isomorfismo de anéis.

5. Anéis Comutativos

Nesta secção A denota um *anel comutativo*. Recorde-se (2.1) que um ideal $P \subset A$ é primo *sse*

$$ab \in P \Rightarrow a \in P \quad \vee \quad b \in P.$$

Teorema 5.1. *Um ideal $P \subset A$ é primo* sse *A/P é um domínio integral.*

Demonstração. Seja $\pi : A \to A/P$ a projecção canónica. O anel A/P é um domínio integral *sse*

$$\forall a, b \in A \quad \pi(a)\pi(b) = \mathbf{0} \Rightarrow \pi(a) = \mathbf{0} \vee \pi(b) = \mathbf{0}.$$

Ou seja,

$$ab \in P \Rightarrow a \in P \vee b \in P.$$ □

Corolário 5.2. *O ideal $(\mathbf{0})$ é primo* sse *A é um domínio integral.*

Teorema 5.3. *Um ideal $M \subset A$ é maximal* sse *A/M é um corpo.*

Demonstração.

$\boxed{\Leftarrow}$ A/M é corpo $\Rightarrow$ A/M é anel de divisão $\Rightarrow$ M é maximal (pelo Teorema 2.29).

$\boxed{\Rightarrow}$ Seja $\pi\colon A \to A/M$ a projecção canónica e seja $a \in A$ *t.q.* $\pi(a) \neq \mathbf{0}$. Como $a \notin M$ e M, por hipótese, é maximal, temos

$$\mathbf{1}_A \in (a) + M \Rightarrow \exists\, b \in A : ab - \mathbf{1}_A \in M \Rightarrow \pi(a)\pi(b) = \pi(ab) = \pi(\mathbf{1}_A) = \mathbf{1}_{A/M}.$$ □

Corolário 5.4. *Seja $M \subset A$ um ideal maximal. Então M é primo.*

Corolário 5.5. *A é um corpo* sse *$(\mathbf{0})$ é maximal.*

Demonstração. $A/(\mathbf{0}) \cong A$. □

Corolário 5.6. *A é um corpo* sse *não tem ideais próprios não nulos.*

Demonstração. A não tem ideais próprios não nulos *sse* $(\mathbf{0})$ é maximal. □

Corolário 5.7. *A é um corpo* sse *para todo o anel B e para todo homomorfismo $f\colon A \to B$ se tem $f = 0$ (caso em que B é o anel trivial) ou f é injectivo.*

Demonstração.

$\boxed{\Rightarrow}$ se A é um corpo, então, como $\ker f$ é um ideal, tem que ser $\ker f = (\mathbf{0})$ ou $\ker f = A$;

$\boxed{\Leftarrow}$ Seja $I \subset A$ um ideal e seja $\pi\colon A \to A/I$ a projecção canónica. Então $\ker \pi = A$ ou $\ker \pi = (\mathbf{0})$. O resultado segue do corolário anterior. □

6. Factorização em anéis comutativos

Definição 6.1. *Seja A um anel comutativo e sejam $a, b \in A$. Se $a \neq \mathbf{0}$, diz-se que a* divide *b se existe $c \in A$* t.q.

$$ac = b.$$

Neste caso, escreve-se $a \mid b$.

Diz-se que a e b são associados *se $a \mid b$ e $b \mid a$. Neste caso, escreve-se $a \sim b$.*

Teorema 6.2. *Seja A um anel comutativo de sejam $a, b, u \in A$. Temos*

1. *$a \mid b \Leftrightarrow (a) \supset (b)$;*
2. *$a \sim b \Leftrightarrow (a) = (b)$;*
3. *u é uma unidade (Definição 1.5)* sse *$(u) = A$;*
4. *a relação $\sim$ é uma relação de equivalência;*

5. *se $a = bu$, onde u é uma unidade, então $a \sim b$. Se A é um domínio integral, a recíproca é válida.*

Demonstração. Demonstramos apenas a última asserção. Suponhamos que A é um domínio integral e que $b = ac$, $a = bc'$ (e ainda $a \neq \mathbf{0}$ e $b \neq \mathbf{0}$ porque $a \sim b$), então

$$b = bcc' \Rightarrow cc' = \mathbf{1} \Rightarrow c, c' \in A^\times. \qquad \square$$

Definição 6.3. *Seja A um anel comutativo. Diz-se que*

1. $c \in A \setminus \{\mathbf{0}\}$ *é* irredutível *se* $c \notin A^\times$ *e*
$$\forall_{a,b \in A} \quad c = ab \Rightarrow a \in A^\times \vee b \in A^\times$$
2. $p \in A \setminus \{\mathbf{0}\}$ *é* primo *se* $p \notin A^\times$ *e*
$$p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

Há uma classe importante de anéis em que os irredutíveis coincidem com os primos.

Definição 6.4. *Um domínio integral D diz-se um* domínio de factorização única (d.f.u.) *se*

(i) $\forall\, d \in D \setminus (D^\times \cup \{\mathbf{0}\})\ \exists c_1, \ldots, c_n$ *irredutíveis* $: d = c_1 \cdots c_n$.

(ii) se $d = c'_1 \cdots c'_m$ *é outra factorização em irredutíveis, então* $m = n$ *e existe* $\sigma \in S_n$ t.q. $c_i \sim c'_{\sigma(i)}$, $i = 1, \ldots, n$.

Exemplos 6.5.

1. $\mathbb{Z}$ é um *d.f.u.*;
2. seja k um corpo, então $k[x]$ é um *d.f.u.*, como veremos à frente;
3. o subanel $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ definido por
$$\mathbb{Z}[\sqrt{-5}] \coloneqq \{m + n\sqrt{-5} \mid m, n \in \mathbb{Z}\}$$
não é um *d.f.u.*, pois
$$9 = 3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$
são duas factorizações não equivalentes em irredutíveis (Exercício 2.6.2).

Exemplos 6.6.

1. Em $\mathbb{Z}$ os elementos primos são os primos usuais e os seus simétricos, e os elementos irredutíveis coincidem com os primos – o que não sucede em geral, como se mostra no exemplo seguinte.
2. Em $\mathbb{Z}_6$, $\underline{2}$ é primo:
$$\begin{aligned} 2 \mid ab \mod 6 &\Leftrightarrow \exists c \in \mathbb{Z} : ab \equiv 2c \mod 6 \\ &\Leftrightarrow ab \in 2c + 6\mathbb{Z} \\ &\Rightarrow 2 \mid a \vee 2 \mid b \\ &\Rightarrow \underline{2} \mid \underline{a} \vee \underline{2} \mid \underline{b}. \end{aligned}$$
No entanto, $\underline{2}$ não é irredutível, pois $\underline{2} = \underline{8} = \underline{4} \cdot \underline{2}$, mas $\underline{4}, \underline{2} \notin \mathbb{Z}_6^\times$.

Teorema 6.7. *Seja D um domínio integral e sejam $a, p, c \in D \setminus \{\mathbf{0}\}$.*

1. *p é primo* sse *(p) é primo e $(p) \neq (\mathbf{0})$;*
2. *c é irredutível* sse *(c) é maximal entre ideais principais;*
3. *se p é primo, então p é irredutível;*
4. *se p é primo e $a \sim p$, então a é primo;*
5. *se c é irredutível e $a \sim c$, então a é irredutível;*
6. *se c é irredutível e $a \mid c$, então $a \in D^\times$ ou $a \sim c$.*

Demonstração. 1. $p \mid ab \Leftrightarrow ab \in (p)$;

2. Pelo Teorema 6.2, c é irredutível *sse*
$$\forall_{a\in D}\ (c)\subset(a)\Leftrightarrow(c)=(a)\vee(a)=D.$$
3. $p=ab\Rightarrow p\mid a\vee p\mid b$
Se $a=pa'$, temos
$$\begin{aligned}p=ab&\Rightarrow p=pa'b\\&\Leftrightarrow p(1-a'b)=\mathbf{0}\\&\Leftrightarrow a'b=\mathbf{1}\\&\Rightarrow b\in D^{\times}.\end{aligned}$$
4. $(p)=(a)\Rightarrow(a)$ primo $\neq(\mathbf{0})\Rightarrow a$ primo;
5. $(c)=(a)\Rightarrow(a)$ maximal entre ideais principais;
6. $a\mid c\Leftrightarrow(a)\supset(c)$, logo $(a)=D$ ou $(a)=(c)$. □

Observação 6.8. Algumas das afirmações anteriores são válidas para qualquer anel comutativo não necessariamente um domínio integral.

Exercícios

2.6.1. Seja D um d.f.u e seja $d\in D\setminus\{\mathbf{0}\}$. Mostre que existe apenas um número finito de ideais principais que contêm o ideal (d).

2.6.2. (Mesmo num domínio integral, nem sempre os irredutíveis são primos.) Considere o anel
$$\mathbb{Z}[\sqrt{-5}]=\left\{m+n\sqrt{-5}\mid m,n\in\mathbb{Z}\right\}$$
e a aplicação $N:\mathbb{Z}[\sqrt{-5}]\to\mathbb{Z}$ dada por
$$N(m+n\sqrt{-5})=(m+n\sqrt{-5})(m-n\sqrt{-5})=m^2+5n^2\ .$$
Demonstre as seguintes afirmações:
(a) $\forall\, a,b\in\mathbb{Z}[\sqrt{-5}]\quad N(ab)=N(a)N(b)$;
(b) $N(a)=0\Leftrightarrow a=0$;
(c) $a\in\mathbb{Z}[\sqrt{-5}]^{\times}\Leftrightarrow N(a)=\pm1$;
(d) $3, 2\pm\sqrt{-5}$ são elementos irredutíveis em $\mathbb{Z}[\sqrt{-5}]$.
(e) 3 não é associado a $2\pm\sqrt{-5}$.
Como $3^2=9=(2+\sqrt{-5})(2-\sqrt{-5})$, conclua que $3, 2\pm\sqrt{-5}$ são elementos irredutíveis que não são primos.

2.6.3. Determine os elementos primos e os elementos irredutíveis de $\mathbb{Z}_{15}$.

7. Factorização em domínios integrais

Teorema 7.1. *Seja D um domínio integral. Então D é um* d.f.u. sse *as seguintes condições se verificam*

(a) os irredutíveis são primos;

(b) toda a cadeia ascendente de ideais principais estabiliza, i.e.*,*

$$(d_1) \subset (d_2) \subset \cdots \subset (d_n) \subset \cdots \Rightarrow \exists N \in \mathbb{N} : \forall n \geq N,\ (d_n) = (d_N).$$

Definição 7.2. *Um domínio integral cujos ideais são principais diz-se um* domínio de ideais principais (*d.i.p.*).

Exemplos 7.3. 1. $\mathbb{Z}$ é um *d.i.p.*;

2. veremos mais à frente que $\mathbb{R}[x]$ é um *d.i.p.*;

3. $\mathbb{Z}[x]$ não é um *d.i.p.* pois $I = (2, x) \subset \mathbb{Z}[x]$ não é um ideal principal.

Corolário 7.4. *Seja D um* d.i.p.*, então D é um* d.f.u.*.*

Demonstração. Vejamos que se verificam as duas condições do Teorema 7.1.

(b) Dada uma cadeia ascendente

$$(d_1) \subset (d_2) \subset \cdots \subset (d_n) \subset \cdots$$

segue facilmente que $\cup_i (d_i)$ é um ideal, logo existe $d \in \cup_i (d_i)$ *t.q.* $(d) = \cup_i (d_i)$. Seja N *t.q.* $d \in (d_N)$. Então

$$\forall i \geq N, \quad (d_i) = (d_N) = (d).$$

(a)

$$\begin{aligned} d \in D \text{ irredutível} &\Leftrightarrow (d) \text{ é maximal entre ideais principais} \\ &\Rightarrow (d) \text{ é maximal} \\ &\Rightarrow (d) \text{ é primo} \\ &\Leftrightarrow d \text{ é primo.} \end{aligned}$$

□

Demonstração do Teorema 7.1.

$\boxed{\Leftarrow}$ Suponhamos que D satisfaz as condições (a) e (b) do enunciado.

1. Seja $d \in D \setminus (D^\times \cup \{\mathbf{0}\})$. Se d não tem uma factorização em irredutíveis, então, em particular, d não é irredutível. Logo $d = d_1' d_1''$ *t.q.* $d_1', d_1'' \notin D^\times$. Podemos supôr que d_1' não tem factorização em irredutíveis, logo $d_1' = d_2' d_2''$ *t.q.* $d_2', d_2'' \notin D^\times$. Prosseguindo, obtemos uma cadeia
$$(d) \subsetneq (d_1') \subsetneq (d_2') \subsetneq \cdots \subsetneq (d_n') \subsetneq \cdots$$
que não estabiliza, o que é uma contradição.
Concluímos que em D todos os elementos têm uma factorização em irredutíveis.
2. Sejam $\prod_{i=1}^n p_i$ e $\prod_{j=1}^m p_j'$ duas factorizações em irredutíveis do mesmo elemento de D. Então, por (a), p_i é primo
$$\begin{aligned} &\Rightarrow p_i \mid p_j' \text{ para algum } j \\ &\Rightarrow p_i \sim p_j'. \end{aligned}$$
Concluímos que $n = m$ e existe $\sigma \in S_n$ *t.q.* $p_i \sim p_{\sigma(i)}', i = 1, \ldots, n$.

$\boxed{\Rightarrow}$ Suponhamos que D é um *d.f.u.*. Vejamos que D satisfaz as condições (a) e (b) do enunciado.

(a) seja $p \in D$ irredutível *t.q.* $p \mid ab$. Por unicidade de factorização $p \sim p'$ *t.q.* p' é factor irredutível de a ou de b. Logo, $p \mid a$ ou $p \mid b$.

(b) Seja

$$(d_1) \subset (d_2) \subset \cdots \subset (d_n) \subset \cdots$$

uma cadeia ascendente. Para todo o n, temos $d_n \mid d_1$, logo todos os factores irredutíveis de d_n dividem d_1. Concluímos que o comprimento da cadeia é limitado pelo número de factores irredutíveis de d_1 (contados com multiplicidade). □

8. Domínios Euclidianos

Definição 8.1. *Um anel comutativo A diz-se um* anel euclidiano *se existe* $\varphi\colon A \setminus \{\mathbf{0}\} \to \mathbb{N}_0$ t.q.

(i) $ab \neq \mathbf{0} \Rightarrow \varphi(a) \leq \varphi(ab)$;

(ii) $a \in A$, $b \in A \setminus \{\mathbf{0}\} \Rightarrow \exists q, r \in A$, t.q.

$$a = qb + r,$$

com $\varphi(r) < \varphi(b)$ *se* $r \neq 0$.

Se adicionalmente A é um domínio integral, diz-se que A é um domínio euclidiano.

Exemplo 8.2. Com a função $\varphi(n) \coloneqq |n|$, $\mathbb{Z}$ é um domínio euclidiano.

Exemplo 8.3. Seja k um corpo. Então $k[x]$ é um domínio euclidiano com $\varphi(f(x)) \coloneqq \deg(f(x))$, como veremos mais tarde.

Teorema 8.4. *Seja A um anel euclidiano, então todos os ideais de A são principais. Em particular, os domínios integrais euclidianos são* d.i.p. *e portanto são* d.f.u..

Demonstração. Seja $I \subset A$ um ideal não nulo ($I = \{\mathbf{0}\}$ é principal) e seja $b \in I \setminus \{\mathbf{0}\}$ *t.q.*

$$\varphi(b) = \min\{\varphi(a) \mid a \in I \setminus \{zero\}\}$$

Dado $x \in I$ sejam q, r *t.q.*

$$x = qb + r$$

e $\varphi(r) < \varphi(b)$, se $r \neq 0$. Pela definição de b, vem $r = 0$. Concluímos que $I = (b)$. □

Definição 8.5. *Seja $X \subset A$* t.q. *$X \neq \varnothing$. Diz-se que $d \in A$ é um* máximo divisor comum *(*mdc*) de X se*

(i) $\forall_{a \in X}\ d \mid a$;

(ii) $c \in A \wedge (\forall_{a \in X}\ c \mid a) \Rightarrow c \mid d$.

Observação 8.6. O máximo divisor comum pode existir ou não e, se existir, não é em geral único.

Exemplo 8.7. Sejam $m, n \in \mathbb{Z}$ então $\exists r, s \in \mathbb{Z}$ *t.q.* $rm + sn = d$ onde d é o máximo divisor comum de m, n. De facto,

$$(m, n) = \bigcap_{\substack{I \text{ ideal} \\ I \supset (m),(n)}} I = \bigcap_{x \mid m,\, x \mid n} (x) = (d). \tag{8.1}$$

Em $\mathbb{Z}$, podemos usar a igualdade (8.1) para definir o máximo divisor comum. O mesmo pode ser feito num *d.i.p.* arbitrário.

Teorema 8.8. *Seja A um anel comutativo e sejam $a_1, \ldots, a_n \in A$*

(a) Se A é um d.f.u. *então existe um* mdc *de $a_1, \ldots a_n$, que é único a menos de multiplicação por uma unidade.*

(b) Se A é um d.i.p. *e $d \in A$ é* t.q.

$$(d) = (a_1, \ldots, a_n)$$

então d é um mdc *de $a_1, \ldots a_n$. Reciprocamente, todos os* mdc *de $(a_1, \ldots, a_n)$ são desta forma.*

Demonstração. (a) Sejam $c_1, \ldots, c_m \in A$ irredutíveis *t.q.*

$$\forall_{c \in A} \ (c \text{ irredutível} \wedge \exists_i : c \mid a_i) \Rightarrow \exists_{j \in \{1,\ldots,m\}} : c \sim c_j.$$

Então, temos factorizações

$$a_i = u_i c_1^{k_1^i} \cdots c_m^{k_m^i}, \qquad i = 1, \ldots, n,$$

t.q. $u_i \in A^\times$ e $k_1^i, \ldots, k_m^i \in \mathbb{N}_0$.
Seja $d = c_1^{r_1} \cdots c_m^{r_m}$, onde

$$r_j = \min\{k_j^i \mid i = 1, \ldots, n\}.$$

Claramente, temos $d \mid a_i$, $i = 1, \ldots, n$. Seja d' *t.q.* $d' \mid a_i$, $i = 1, \ldots, n$, então

$$d' = u' c_1^{s_1} \cdots c_m^{s_m}$$

t.q. $s_j \leq r_j$, $\forall_j$, portanto $d' \mid d$. Concluímos que d é *mdc* de $a_1, \ldots, a_n$.
Se d, d' são *mdc* de $a_1, \ldots, a_n$, então $d \mid d'$ e $d \mid d'$, portanto $d \sim d'$.

(b) Seja d como no enunciado. Por definição, temos $a_i \in (d)$, logo $d \mid a_i$, $i = 1, \ldots, n$. Se $d' \mid a_i$, $i = 1, \ldots, n$, tem-se $a_1, \ldots, a_n \in (d')$, logo

$$(d) \subset (d'),$$

ou seja, $d' \mid d$. Portando d é um *mdc* de $a_1, \ldots, a_n$.

Reciprocamente, se d é um *mdc* de $a_1, \ldots, a_n$, então $(a_1, \ldots, a_n) \subset (d)$. Seja $d' \in A$ *t.q.* $(d') = (a_1, \ldots, a_n)$ então $d \mid d'$, porque $(d') \subset (d)$ e $d' \mid d$, por definição de d. Concluímos que $(d) = (d')$. □

Exercícios

2.8.1. Justifique que $\mathbb{Z}[\sqrt{-5}]$ (ver Exercício 2.6.2) não é um d.f.u.

2.8.2. Mostre que $\mathbb{Z}[\mathrm{i}] \coloneqq \{n + m\mathrm{i} \mid n, m \in \mathbb{Z}\} \subset \mathbb{C}$ é um domínio euclidiano com $\varphi(n + m\mathrm{i}) = n^2 + m^2$, resolvendo as seguintes alíneas:
   (a) Mostre que φ é multiplicativo, i.e., $\varphi(ab) = \varphi(a)\varphi(b)$ para todo o $a, b \in \mathbb{Z}[\mathrm{i}]$ e deduza a propriedade (i) da definição.
   (b) Dados $k, a \in \mathbb{Z}$, com $a > 0$, mostre que existem $q, r \in \mathbb{Z}$ tais que $k = qa + r$, onde $|r| \leq \frac{a}{2}$.
   (c) Prove a propriedade (ii) quando $a \in \mathbb{N}$ e $b = n + m\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$.
   Sugestão: use a alínea anterior para obter $n = q_1 a + r_1$ e $m = q_2 a + r_2$ e considere $q \coloneqq q_1 + q_2\mathrm{i}$ e $r \coloneqq r_1 + r_2\mathrm{i}$.
   (d) Prove a propriedade (ii) para $a, b \in \mathbb{Z}[\mathrm{i}]$.
   Sugestão: se $a = x + y\mathrm{i} \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$, então $a\bar{a} = x^2 + y^2 \in \mathbb{N}$ (onde $\bar{a} = x - y\mathrm{i}$) e use a alínea anterior com $a\bar{a}$ e $b\bar{a}$.

2.8.3. Determine as unidades no anel $\mathbb{Z}[\mathrm{i}]$.
Sugestão para uma resolução "eficiente": descreva as unidades de $\mathbb{Z}[\mathrm{i}]$ à custa da aplicação φ do exercício anterior.

2.8.4. Seja A um anel comutativo de ideais principais. Mostre que qualquer conjunto $X \subset A$, $X \neq \varnothing$, tem um máximo divisor comum.

9. Localização

Definição 9.1. *Seja A um anel comutativo. Um subconjunto $S \subset A$ diz-se* multiplicativo *se $(S, \cdot) \subset (A, \cdot)$ é um submonóide. Ou seja,*

(i) $\mathbf{1} \in S$;

(ii) $\forall_{s_1, s_2 \in S} \quad s_1 \cdot s_2 \in S$.

Definição 9.2. *Seja A um anel comutativo e seja $S \subset A$ um subconjunto multiplicativo. Consideremos a seguinte relação de equivalência em $A \times S$*

$$(a, s) \sim (a', s') \Leftrightarrow \exists_{s'' \in S} : s''(as' - a's) = \mathbf{0}.$$

Denotamos o quociente $A \times S / \sim$ por $S^{-1}A$ e denotamos a classe de equivalência de (a, s) por $\frac{a}{s}$.

Em $S^{-1}A$ definimos as seguintes operações:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$$
$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}$$

Com estas operações, $S^{-1}A$ é um anel comutativo. A identidade de $S^{-1}A$ é $\frac{\mathbf{1}}{\mathbf{1}}$ e o zero é $\frac{\mathbf{0}}{\mathbf{1}}$.

Proposição 9.3. *Nas condições da Definição 9.2*

(a) as operações em $S^{-1}A$ estão bem definidas;

(b) $(S^{-1}A, +, \cdot)$ é um anel com identidade $\frac{\mathbf{1}}{\mathbf{1}}$ e zero $\frac{\mathbf{0}}{\mathbf{1}}$.

Exemplo 9.4. Consideremos o subconjunto multiplicativo $S = \mathbb{Z} \setminus \{0\}$ do anel $\mathbb{Z}$. Denotamos por $[n, m]$ a classe de equivalência de $(n, m) \in \mathbb{Z} \times S$. Definimos

$$f \colon S^{-1}\mathbb{Z} \to \mathbb{Q}; \quad [n, m] \mapsto \frac{n}{m}.$$

f está bem definida, pois

$$\forall_{n, n' \in \mathbb{Z}} \forall_{m, m', m'' \in S} \quad m''(nm' - n'm) = 0 \Leftrightarrow nm' - n'm = 0 \Leftrightarrow \frac{n}{m} = \frac{n'}{m'}.$$

Claramente f é sobrejectiva e

$$\ker f = \{[n, m] \in S^{-1}\mathbb{Z} \mid n = 0\} = \{[0, 1]\},$$

portanto f é um isomorfismo, i.e., a localização de $\mathbb{Z}$ no conjunto multiplicativo $\mathbb{Z} \setminus \{0\}$ é o corpo $\mathbb{Q}$.

Definição 9.5. *Seja A um anel comutativo e seja $S \subset A$ multiplicativo. O homomorfismo $\varphi_S \colon A \to S^{-1}A$ é definido por*

$$\varphi_S(a) := \frac{a}{\mathbf{1}}.$$

Observação 9.6. 1. Se $s \in S$, então $\varphi_S(s) = \frac{s}{\mathbf{1}}$ tem inverso $\frac{\mathbf{1}}{s}$;

2. $\ker \varphi_S = \{a \in A \mid \exists_{s \in S} : as = \mathbf{0}\}$. De facto,

$$\varphi_S(a) = \frac{\mathbf{0}}{\mathbf{1}} \Leftrightarrow \frac{a}{\mathbf{1}} = \frac{\mathbf{0}}{\mathbf{1}} \Leftrightarrow \exists_{s'' \in S} : s''(a \cdot \mathbf{1} - \mathbf{0} \cdot \mathbf{1}) = \mathbf{0} \Leftrightarrow \exists_{s'' \in S} : a \cdot s'' = \mathbf{0}.$$

3. Se S é tal que $\mathbf{0} \in S$ então $S^{-1}A$ é o anel trivial.

Proposição 9.7. *Seja A um domínio integral e seja $S \subset A$ um subconjunto multiplicativo* t.q. *$\mathbf{0} \notin S$. Então $S^{-1}A$ é um domínio integral que contém uma cópia de A (φ_S é injectivo).*

Demonstração.

$$\frac{a_1}{s_1}\cdot\frac{a_2}{s_2}=\frac{\mathbf{0}}{\mathbf{1}}\Leftrightarrow\exists_{s\in S}: s(a_1a_2)=\mathbf{0}\Leftrightarrow a_1a_2=\mathbf{0}\Leftrightarrow a_1=\mathbf{0}\vee a_2=\mathbf{0}$$
$$\Rightarrow \frac{a_1}{s_1}=\frac{\mathbf{0}}{\mathbf{1}}\vee\frac{a_2}{s_2}=\frac{\mathbf{0}}{\mathbf{1}}\ .$$

□

Exemplo 9.8. $\varphi_{\mathbb{Z}\setminus\{0\}}\colon\mathbb{Z}\to(\mathbb{Z}\setminus\{0\})^{-1}\mathbb{Z}\cong\mathbb{Q}$ é um homomorfismo injectivo.

Teorema 9.9. *Seja A um domínio integral e seja $S=A\setminus\{0\}$. Então* $\mathrm{Frac}(A)\coloneqq S^{-1}A$ *é um corpo.*

Demonstração. S é um conjunto multiplicativo pois A não contém divisores de zero. Pela proposição 9.7, só falta ver que qualquer elemento não nulo de $S^{-1}A$ tem inverso:

$$\frac{a}{s}\neq\frac{\mathbf{0}}{\mathbf{1}}\Leftrightarrow a\in S\Rightarrow\frac{a}{s}\cdot\frac{s}{a}=\frac{\mathbf{1}}{\mathbf{1}}.$$

□

Definição 9.10. *Nas condições do Teorema 9.9, diz-se que* $\mathrm{Frac}(A)$ *é o corpo de fracções de A.*

Exemplo 9.11. Seja $A=\mathbb{R}[x]$ e $S=\mathbb{R}[x]\setminus\{0\}$. Temos,

$$\mathrm{Frac}(\mathbb{R}[x])=\mathbb{R}(x)\coloneqq\left\{\frac{p(x)}{q(x)}\mid p(x),q(x)\in\mathbb{R}[x],q(x)\neq0\right\}.$$

Exercícios

2.9.1. Demonstre a Proposição 9.3.

2.9.2. Seja A um anel comutativo e S um subconjunto multiplicativo. Mostre que $\frac{a}{\mathbf{1}}\in S^{-1}A$ é invertível sse $(a)\cap S\neq\varnothing$.

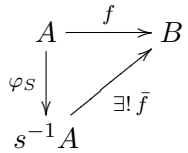
2.9.3. Seja $n\geq2$ e $S=\{\underline{a}\in\mathbb{Z}_n\mid\underline{a}\neq\underline{0},\underline{a}$ não é um divisor de zero$\}$. Mostre que S é um conjunto multiplicativo e determine $S^{-1}\mathbb{Z}_n$.

2.9.4. Seja $n\in\mathbb{N}$ e seja $S\subset\mathbb{Z}_n$ um conjunto multiplicativo. Mostre que existe $m\in\mathbb{N}$ tal que $S^{-1}\mathbb{Z}_n\cong\mathbb{Z}_m$.

2.9.5. Seja A um anel comutativo e S um subconjunto multiplicativo tal que $S\subset A^\times$. Mostre que $\varphi_S:A\to S^{-1}A,\varphi(a)=\frac{a}{\mathbf{1}}$, é um isomorfismo.

2.9.6. Mostre que
(a) $\mathrm{Frac}(\mathrm{Frac}(A))\cong\mathrm{Frac}(A)$ para qualquer domínio integral A;
(b) $\mathrm{Frac}(k)\cong k$ para qualquer corpo k.

2.9.7. Prove a propriedade universal do anel $S^{-1}A$: Sejam A um anel comutativo e $S\subset A$ um subconjunto multiplicativo. Dado um anel comutativo B e um homomorfismo de anéis $f:A\to B$ tais que $f(S)\subset B^\times$, então existe um único homomorfismo $\bar{f}:S^{-1}A\to B$ tal que $\bar{f}\circ\varphi_S=f$, onde $\varphi_S:A\to S^{-1}A$, $\varphi_S(a)=\frac{a}{1}$, i.e., o seguinte diagrama comuta



2.9.8. Seja A um anel comutativo e sejam S e T dois subconjuntos multiplicativos de A tais que $S\subset T$.
(a) Mostre que $\psi:S^{-1}A\to T^{-1}A$, dado por $\psi(\frac{a}{s})=\frac{a}{s}$, define um homomorfismo de anéis.
(b) Se $T\setminus S\subset A^\times$, mostre que ψ é um isomorfismo.

10. Ideais de $S^{-1}A$

Seja $I \subset A$ um ideal, define-se

$$S^{-1}I \coloneqq \left\{ \frac{a}{s} \in S^{-1}A \mid a \in I \right\} \subset S^{-1}A.$$

Proposição 10.1. *$S^{-1}I \subset S^{-1}A$ é um ideal.*

Demonstração. Sejam $\frac{a}{s}, \frac{b}{r} \in S^{-1}I$ com $a, b \in I$. Temos

$$a, b \in I \quad \Rightarrow \quad ar, bs \in I \quad \Rightarrow \quad ar - bs \in I \quad \Rightarrow \quad \frac{a}{s} - \frac{b}{r} = \frac{ar - bs}{sr} \in S^{-1}I \ .$$

Sejam $\frac{a}{s} \in S^{-1}I$, com $a \in I$, e $\frac{b}{s} \in S^{-1}A$. Temos

$$a \in I \quad \Rightarrow \quad ab \in I \quad \Rightarrow \quad \frac{a}{s} \cdot \frac{b}{r} = \frac{ab}{sr} \in S^{-1}I \ .$$

Como $S^{-1}I \neq \varnothing$, pois $\frac{\mathbf{0}}{\mathbf{1}} \in S^{-1}I$ (porque $\mathbf{0} \in I$ e $\mathbf{1} \in S$), concluimos que $S^{-1}I$ é um ideal em $S^{-1}A$. □

Obtemos assim correspondências entre ideais de A e de $S^{-1}A$ dadas por:

$$A \supset I \mapsto S^{-1}I \subset S^{-1}A$$
$$\varphi_S^{-1}(J) \hookleftarrow J \subset S^{-1}A.$$

Proposição 10.2. *Sejam $I, J \subset A$ ideais. Então*

(a) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$;
(b) $S^{-1}(IJ) = S^{-1}I \cdot S^{-1}J$;
(c) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.

Proposição 10.3. *Seja A um anel comutativo de seja $S \subset A$ um subconjunto multiplicativo. Então, dado um ideal $K \subset S^{-1}A$, existe um ideal $I \subset A$* t.q. *$K = S^{-1}I$.*

A proposição seguinte mostra que quando restringidas a certos ideais estas correspondências são bijectivas. Em geral isto não se passa (*cf.* Exemplo 10.7).

Proposição 10.4. *Nas condições da proposição anterior, as correspondências $I \mapsto S^{-1}I$ e $K \mapsto \varphi_S^{-1}(K)$ estabelecem uma correspondência bijectiva:*

$$\{P \subset A \mid P \text{ é ideal primo e } P \cap S = \varnothing\} \leftrightarrow \left\{K \subset S^{-1}A \mid K \text{ ideal é primo}\right\}.$$

Exemplo 10.5. Seja A um anel comutativo e seja $P \subset A$ um ideal primo. Então $S = A \setminus P$ é multiplicativo, pois $\mathbf{1} \in S$ e

$$a, b \in S \Rightarrow ab \in S,$$

pois

$$ab \notin P \Leftarrow a \notin P \ \wedge \ b \notin P.$$

Neste caso, $S^{-1}A$ é denotado A_P e designado *localização de A em P*. Se $I \subset A$ é um ideal, $S^{-1}I$ é denotado I_P.

Teorema 10.6. *Seja A um anel comutativo e seja $P \subset A$ um ideal primo. Então existe uma correspondência bijectiva*

$$\{I \subset A \mid I \subset P \text{ é ideal primo}\} \leftrightarrow \{K \subset A_P \mid K \text{ ideal é primo}\}$$

dada por $I \mapsto I_P$ e $K \mapsto \varphi_{A\setminus P}^{-1}(K)$.

Exemplo 10.7. Seja $A = \mathbb{Z}$ e $P = (p)$, com $p \in \mathbb{N}$ primo. Temos

$$\mathbb{Z}_{(p)} \coloneqq A_P = \left\{ \frac{r}{s} \in \mathbb{Q} \mid r, s \in \mathbb{Z}, p \nmid s \right\} \subset \mathbb{Q}.$$

Os ideais de $\mathbb{Z}_{(p)}$ são da forma $(p^n)_P$. Temos $(2p)_P = (p)_P$, logo

$$\varphi_S^{-1}((2p)_P) = \varphi_S^{-1}((p)_P) = (p) \neq (2p).$$

Observação 10.8. Se A é um anel comutativo e P é um ideal primo, então há uma correspondência bijectiva entre os ideais primos $Q \subset P$ em A e os ideais primos na localização A_P. Além disso, como qualquer ideal em A_P é da forma I_P para algum ideal $I \subset A$, I_P é um ideal próprio se e só se $I \subset P$, portanto qualquer ideal próprio em A_P verifica $I_P \subset P_P$, ou seja P_P é o único ideal maximal.

Definição 10.9. *Um anel comutativo A diz-se um* anel local *se contém um único ideal maximal.*

Pela obervação anterior, a localização A_P de A num ideal primo $P \subset A$ é um anel local.

Proposição 10.10. *Um anel comutativo A é local se e só se $A \setminus A^\times$ é um ideal.*

Exercícios

2.10.1. Demonstre a proposição 10.2.

2.10.2. Demonstre a proposição 10.3.

2.10.3. Demonstre a proposição 10.4.

2.10.4. Seja D um *d.i.p.* e $S \subset D$ um conjunto multiplicativo tal que $0 \notin S$. Mostre que $S^{-1}D$ é um *d.i.p.*.

2.10.5. Mostre que um domínio integral D é um domínio de factorização única sse qualquer ideal primo não nulo contém um ideal principal não nulo que é primo.
Sugestão para a demonstração de ($\Leftarrow$): Mostre primeiro as seguintes afirmações.
(i) Seja $S = D^\times \cup \{p_1 \cdots p_n \mid n \in \mathbb{N}, p_1 \ldots, p_n \in D \text{ primos}\}$. Então S é um conjunto multiplicativo tal que, se $ab \in S$, então $a \in S$ e $b \in S$.
(ii) Se $S \subset D$ é um conjunto multiplicativo (com $\mathbf{0} \notin S$), então para qualquer $x \in D$ tal que $(x) \cap S = \varnothing$ existe um ideal primo $P \subset D$ tal que $(x) \subset P$ e $P \cap S = \varnothing$.
Sugestão: use a caracterização dos ideais primos em $S^{-1}D$.

2.10.6. Seja D um *d.f.u.* e $S \subset D$ um conjunto multiplicativo tal que $0 \notin S$. Mostre que $S^{-1}D$ é um *d.f.u.*.
Sugestão: Use o Exercício 2.10.5.

2.10.7. Seja $p \in \mathbb{Z}$ um número primo. Qual a relação entre o anel quociente $\mathbb{Z}_p = \mathbb{Z}/(p)$ e a localização $\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z}$, onde $S = \mathbb{Z} \setminus (p)$?

2.10.8. Demonstre a Proposição 10.10.

2.10.9. Seja $p \in \mathbb{Z}$ um primo. Mostre que $A = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ é um anel local.

2.10.10. Seja $f : A \to B$ um homomorfismo de anéis não nulo. Mostre que, se A é local, então $f(A)$ também o é.

2.10.11. Seja A um anel comutativo e seja N o ideal formado pelos elementos nilpotentes de A (ver Exercício 2.2.6). Mostre que N é a intersecção de todos os ideais primos de A.
Sugestão para demonstrar que N contém a intersecção dos ideais primos: Dado $r \in A \setminus N$, encontre um ideal primo $P \subset A$ tal que $r \notin P$ considerando a localização $S^{-1}A$, onde $S = \{r^n \mid n \in \mathbb{N}_0\}$.

11. Anéis de polinómios

Exemplo 11.1. $\mathbb{R}[x]$ é um subanel do anel de funções $f\colon \mathbb{R} \to \mathbb{R}$. Os seus elementos são da forma

$$f(x) = a_n x^n + \cdots + a_0, \qquad a_i \in \mathbb{R},$$

portanto, os coeficientes a_i, $i \in \mathbb{N}_0$, determinam completamente $f(x)$ (se $k > n$, define-se $a_k = 0$). Seja $g(x)$ outro polinómio

$$g(x) = b_m x^m + \cdots + b_0.$$

As operações em termos dos coeficientes são

$$f(x) + g(x) = c_r x^r + \cdots + c_0$$

$$\Rightarrow \boxed{c_k = a_k + b_k} \tag{11.1}$$

$$f(x) \cdot g(x) = d_s x^s + \cdots + d_0$$

$$\Rightarrow \boxed{d_k = \sum_{i+j=k} a_i b_j} \tag{11.2}$$

De seguida pretendemos definir polinómios com coeficientes num anel arbitrário.

Exemplo 11.2. Se definirmos $\mathbb{Z}_2[x]$ como um subanel das funções $\mathbb{Z}_2 \to \mathbb{Z}_2$ então só haveria no máximo quatro polinómios. A definição apropriada tem que ser feita em função dos coeficientes.

Definição 11.3. *Seja A um anel. Considere-se*

$$A[x] \coloneqq \{a\colon \mathbb{N}_0 \to A \mid \exists_{N \in \mathbb{N}_0} : n > N \Rightarrow a(n) = 0\}.$$

Define-se as operações de adição e multiplicação em $A[x]$ da seguinte forma:

$$(a+b)(n) \coloneqq a(n) + b(n) \tag{11.3}$$

$$(a \cdot b)(n) \coloneqq \sum_{i+j=n} a(i)b(j) \tag{11.4}$$

Notação 11.4. 1. x denota a sucessão $x\colon \mathbb{N}_0 \to A$ *t.q.* $x(n) = \begin{cases} 0, & n \neq 1 \\ 1, & n = 1 \end{cases}$

2. $1_{A[x]}$ denota a sucessão $1_{A[x]}\colon \mathbb{N}_0 \to A$ *t.q.* $1_{A[x]}(n) = \begin{cases} 1, & n = 0 \\ 0, & n \neq 0 \end{cases}$.

Se não houver risco de confusão, usamos a 1 para denotar $1_{A[x]}$.

Observação 11.5.

1. $1_{A[x]}$ satisfaz $1_{A[x]} \cdot a = a \cdot 1_{A[x]} = a$, $\forall a \in A[x]$;
2. $x^n(k) = \begin{cases} 1, & k = n \\ 0, & k \neq n \end{cases}$
3. $\forall a \in A[x],\ ax^n = x^n a$;
4. Em geral, se $a \in A[x]$ é *t.q.* $a(n) \in Z(A)$, $\forall n \in \mathbb{N}_0$, segue que $a \in Z(A[x])$.

Proposição 11.6. *Os elementos de $A[x]$ podem ser escritos de forma única como se segue:*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \qquad a_i \in A.$$

Dado outro elemento $g(x) = b_m x^m + \cdots + b_1 x + b_0$, *temos*

$$f(x) + g(x) = \sum_{i=0}^{n+m} (a_i + b_i) x^i \tag{11.5}$$

$$f(x)g(x) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_i b_{i-j} \right) x^i. \tag{11.6}$$

Com esta estrutura $A[x]$ *é um anel* t.q. $x \in Z(A[x])$. *A função* $A \to A[x]; a \mapsto a \cdot 1_{A[x]}$ *é um homomorfismo injectivo de anéis. Se* A *é comutativo, então* $A[x]$ *também o é.*

Exemplo 11.7. $\mathbb{Z}_2[x]$ é um anel comutativo com caraterística 2 e $|\mathbb{Z}_2[x]| = |\mathbb{N}|$.

Definição 11.8 (Homomorfismo de avaliação)**.** *Seja* A *um anel comutativo e seja* $c \in A$, *então existe um homomorfismo* $\mathrm{eval}_c \colon A[x] \to A$ *dado por*

$$\mathrm{eval}_c \left(\sum_{i=0}^{n} a_i x^i \right) \coloneqq \sum_{i=0}^{n} a_i c^i \in A.$$

Notação 11.9. Dado $f(x) \in A[x]$ é habitual usar $f(c)$ para denotar $\mathrm{eval}_c(f(x))$.

Exemplo 11.10. Seja $f(x) = 1 + x + x^2 \in \mathbb{Z}_2[x]$. Temos $f(0) = f(1) = 1$, mas $f(x) \neq 1_{\mathbb{Z}_2[x]}$.

De forma análoga, podemos definir polinómios em várias variáveis, $x_1, \ldots, x_n$ com coeficientes num anel A.

Definição 11.11. *Consideremos o conjunto*

$$A[x_1, \ldots, x_n] \coloneqq \{a \colon \mathbb{N}_0^n \to A \mid \exists N : k_i > N, i = 1, \ldots, n \Rightarrow a(k_1, \ldots, k_n) = 0\}.$$

Dados $a, b \in A[x_1, \ldots, x_n]$ *e dado* $K = (k_1, \ldots, k_n) \in \mathbb{N}_0^n$, *define-se*

$$(a + b)(K) = a(K) + b(K)$$

$$(ab)(K) = \sum_{I+J=K} a(I)b(J).$$

Com estas operações $A[x_1, \ldots, x_n]$ é um anel cuja identidade é a função $1_{A[x_1,\ldots,x_n]} \colon \mathbb{N}_0^n \to A$ dada por

$$1_{A[x_1,\ldots,x_n]}(K) = \begin{cases} 1, & K = (0, \ldots, 0) \\ 0, & \text{caso contrário} \end{cases}$$

Se $x_i \in A[x_1, \ldots, x_n]$ designa a função $\mathbb{N}_0^n \to A$ que vale 0_A em todos os pontos e vale $\mathbf{1}_A$ no i-ésimo vector da base canónica, e_i, então qualquer elemento $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ pode ser escrito de forma única como se segue:

$$f(x_1, \ldots, x_n) = \sum_{0 \leq i_1, \ldots, i_n \leq N} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}. \tag{11.7}$$

Notação 11.12. Dado $I = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ denotamos $x^I \coloneqq x_1^{i_1} \cdots x_n^{i_n}$.

Com esta notação a fórmula (11.7) escreve-se na seguinte forma:

$$f(x_1, \ldots, x_n) = \sum_{I \in \mathbb{N}_0^n} a_I x^I.$$

Observação 11.13. $x_i \in Z(A[x_1, \ldots, x_n])$.

Exemplo 11.14. Seja $f(x, y) = \underline{1} + xy$, $g(x, y) = x + y$ elementos de $\mathbb{Z}_2[x, y]$. Temos

$$f(x, y)g(x, y) = (\underline{1} + xy)(x + y) = x + y + x^2 y + xy^2.$$

11.1. Homomorfismos a partir de anéis de polinómios:

Sejam A e B anéis comutativos. Recorde-se que $A \subset A[x_1, \ldots, x_n]$, portanto dado um homomorfismo $\varphi\colon A[x_1, \ldots, x_n] \to B$, obtemos um homomorfismo por restrição $f \coloneqq \varphi|_A\colon A \to B$. Seja $b_i = \varphi(x_i)$, $i = 1, \ldots, n$. Então φ é determinado por f e por $b_1, \ldots, b_n$:

$$\begin{aligned}\varphi\left(\sum_I a_I x^I\right) &= \sum_I \varphi(a_I x^I) = \sum_I \varphi(a_I)\varphi(x^I) \\ &= \sum_I f(a_I)\varphi(x_1^{i_1} \cdots x_n^{i_n}) = \sum_I f(a_I)\varphi(x_1)^{i_1} \cdots \varphi(x_n)^{i_n} \\ &= \sum_I f(a_I) b_1^{i_1} \cdots b_n^{i_n} \qquad (11.8)\end{aligned}$$

Proposição 11.15. *Dar um homomorfismo $\varphi\colon A[x_1, \ldots, x_n] \to B$ é equivalente a dar um homomorfismo $f\colon A \to B$ e n elementos $b_1, \ldots, b_n \in B$. O homorfismo φ determinado por f, $b_1, \ldots, b_n \in B$ é dado por* (11.8).

Observação 11.16. O anel $A[x_1, \ldots, x_n]$ é determinado a menos de isomorfismo por esta propriedade, *i.e.*, se C é um anel *t.q.* $C \supset A$ e C satisfaz esta propriedade, então $C \cong A[x_1, \ldots, x_n]$.

Para o caso em que A ou B não é comutativo, ver Exercícios 2.11.3.

Proposição 11.17. $A[x_1, \ldots, x_{n+k}] \cong (A[x_1, \ldots, x_n])[x_{n+1}, \ldots, x_{n+k}]$.

Demonstração. Demonstramos o caso $n = k = 1$, *i.e.*, mostramos $A[x, y] \cong A[x][y]$.

Defina-se $\varphi\colon A[x, y] \to A[x][y]$ *t.q.*

$$\begin{aligned}\varphi(a) &= a, \quad \forall a \in A \\ \varphi(x) &= x \\ \varphi(y) &= y,\end{aligned}$$

onde a e x são considerados como polinómios constantes em y com coeficientes em $A[x]$. Definimos também $\psi\colon A[x][y] \to A[x, y]$ *t.q.*

$$\begin{aligned}\psi|_{A[x]} &\equiv \text{inclusão } A[x] \hookrightarrow A[x, y] \\ \psi(y) &= y.\end{aligned}$$

Então, $\varphi \circ \psi$ é um homomorfismo $A[x][y] \to A[x][y]$ *t.q.*

$$\begin{aligned}\varphi \circ \psi|_{A[x]} &= \mathrm{id}_{A[x]} \\ \varphi \circ \psi(y) &= y,\end{aligned}$$

portanto $\varphi \circ \psi = \mathrm{id}_{A[x][y]}$. Da mesma forma,

$$\begin{aligned}\psi \circ \varphi|_A &= \mathrm{id}_A \\ \psi \circ \varphi(x) &= x, \\ \psi \circ \varphi(y) &= y,\end{aligned}$$

logo $\psi \circ \varphi = \mathrm{id}_{A[x,y]}$. □

Exemplo 11.18. Seja $f(x, y) = 3x^2y + 5x + 1 \in \mathbb{Z}[x, y]$, então, o valor do homomorfismo φ da demonstração acima em $f(x, y)$ é

$$\varphi(f(x, y)) = \left(3x^2\right) y + (5x + 1) \cdot 1 \in \mathbb{Z}[x][y].$$

Exercícios

2.11.1. Mostre que $\text{eval}_c : A[x] \to A$ é um homomorfismo de anéis (ver Definição 11.8).

2.11.2. Seja $A = M_2(\mathbb{Z})$.
(a) Dada uma matriz $M \in A$ qualquer, mostre que $(x + M)(x - M) = x^2 - M^2$ em $A[x]$.
(b) Dê um exemplo de matrizes $M, N \in A$ tais que $(N + M)(N - M) \neq N^2 - M^2$.
Conclua que a Proposição 11.15 pode ser falsa se os anéis não forem comutativos.

2.11.3. (Propriedade universal do anel de polinómios $A[x_1, \ldots, x_n]$, quando A não é necessariamente comutativo.) Sejam A, B anéis e $\varphi : A \to B$ um homomorfismo de anéis tal que

$$\exists\, b_1, \ldots, b_n \in B \quad \forall i, j \quad \forall\, a \in A \quad b_i b_j = b_j b_i \quad \text{e} \quad \varphi(a) b_i = b_i \varphi(a)\ .$$

(a) Mostre que existe um único homomorfismo $\bar{\varphi} : A[x_1, \ldots, x_n] \to B$ tal que $\bar{\varphi}|_A = \varphi$ e $\bar{\varphi}(x_i) = b_i$.
(b) Mostre que a propriedade anterior determina o anel $A[x_1, \ldots, x_n]$, a menos de isomorfismos.

2.11.4. Seja A um anel comutativo. Se $f = a_n x^n + \cdots + a_1 x + a_0$ é um divisor de zero em $A[x]$, mostre que existe $b \in A \setminus \{0\}$ tal que $ba_n = \cdots = ba_0 = 0$.

2.11.5. Seja A um anel comutativo e seja S um subconjunto multiplicativo de A. Mostre que $S^{-1}(A[x]) \cong (S^{-1}A)[x]$.

2.11.6. Seja A um anel comutativo e $a \in A$. Mostre que $ax + 1$ é inverível em $A[x]$ se e só se a é nilpotente em A.

12. Séries formais

Definição 12.1. *Seja A um anel. Considere-se*

$$A[[x]] \coloneqq \{a \colon \mathbb{N}_0 \to A\}.$$

Define-se as operações de adição e multiplicação em $A[[x]]$ da seguinte forma:

$$(a+b)(n) \coloneqq a(n) + b(n) \tag{12.1}$$

$$(a \cdot b)(n) \coloneqq \sum_{i+j=n} a(i)b(j) \tag{12.2}$$

$A[[x]]$ diz-se o anel das séries formais de coeficientes em A.

Observação 12.2. A identidade de $A[[x]]$ é a sucessão $1_{A[[x]]}$ dada por

$$1_{A[[x]]}(n) = \begin{cases} 1, & n = 0 \\ 0, & n \neq 0. \end{cases}$$

Notação 12.3. (a) x designa o elemento de $A[[x]]$ cujo valor em $n \in \mathbb{N}_0$ é

$$x(n) \coloneqq \begin{cases} 1, & n = 1 \\ 0, & n \neq 1. \end{cases}$$

(b) $\sum_{n=0}^{\infty} a_n x^n$ denota o elemento de $A[[x]]$ correspondente à sucessão $(a_n)_{n\in\mathbb{N}_0}$.

Observação 12.4. 1. $A[x]$ é um subanel de $A[[x]]$;

2. Se é A comutativo, então $A[[x]]$ é comutativo;

3. Se A é um domínio integral, então $A[[x]]$ é um domínio integral.

Lema 12.5. *Seja $f(x) = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$. Então $f(x) \in A[[x]]^\times$ sse $a_0 \in A^\times$.*

Demonstração. Seja $a_0 \in A^\times$. O inverso à esquerda $g(x) = \sum_{n=0}^{\infty} b_n x^n$ para $f(x)$ é dado pelo resolução do seguinte sistema (infinito) de equações:

$$\begin{aligned} b_0 a_0 = 1 &\Leftrightarrow b_0 = a_0^{-1} \\ b_1 a_0 + b_0 a_1 = 0 &\Leftrightarrow b_1 = -b_0 a_1 a_0^{-1} = -a_0^{-1} a_1 a_0^{-1} \\ &\vdots \\ b_n a_0 + \cdots + b_0 a_n = 0 &\Leftrightarrow b_n = -\left(b_{n-1} a_1 + \cdots + b_0 a_n\right) a_0^{-1}. \end{aligned}$$

De forma análoga obtém-se o inverso à direita $h(x) \in A[[x]]$. Como $g = g \cdot 1 = g(fh) = (gf)h = 1 \cdot h = h$, concluímos que $f(x)$ é uma unidade.

Reciprocamente, se $f(x)$ é uma unidade, então segue da existência de um inverso de $f(x)$ que $a_0 \in A^\times$. □

Exemplo 12.6. Seja $f(x) = \sum_{n=0}^{\infty} x^n \in A[[x]]$. Então, pelo lema anterior $f(x)$ tem um inverso que pode ser calculado resolvendo o sistema correspondente à equação $(f(x))^{-1} f(x) = 1$, obtendo-se $(f(x))^{-1} = 1 - x$. De facto,

$$(1-x)\sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} x^n - \sum_{n=0}^{\infty} x^{n+1} = \sum_{n=0}^{\infty} x^n - \sum_{n=1}^{\infty} x^n = 1.$$

Exercícios

2.12.1. Seja A um anel. Mostre que, para $n \geq 1$,
(a) $M_n(A)[x] \cong M_n\big(A[x]\big)$;
(b) $M_n(A)[[x]] \cong M_n\big(A[[x]]\big)$.

2.12.2. Justifique as seguintes afirmações:
(a) O polinómio $x + 1$ é uma unidade em $\mathbb{Z}[[x]]$, mas não em $\mathbb{Z}[x]$.
(b) O polinómio $x^2 + 3x + 2$ é irredutível em $\mathbb{Z}[[x]]$, mas não em $\mathbb{Z}[x]$.

2.12.3. Se k é um corpo, mostre que $k[[x]]$ é um anel local. Será $k[x]$ um anel local?

2.12.4. Seja k um corpo. Mostre que:
(a) Qualquer $f \in k[[x]] \setminus \{0\}$ se escreve na forma $f = x^k u$ com $k \in \mathbb{N}_0$ e $u \in k[[x]]^\times$.
(b) Os ideais em $k[[x]]$ são $\{0\}$ e (x^k), com $k \in \mathbb{N}_0$, logo $k[[x]]$ é um *d.i.p.*

13. Factorização em anéis de polinómios

Definição 13.1. *Seja A um anel e seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ t.q. $a_n \neq 0$. Diz-se que n é o* grau de f *e denota-se por* $\deg f$. *Se $f = 0$, define-se* $\deg f = -\infty$.

Teorema 13.2. *Para $f, g \in A[x]$, tem-se*

(i) $\deg(f+g) \leq \max\{\deg f, \deg g\}$;

(ii) $\deg(fg) \leq \deg f + \deg g$;

(iii) se os coeficientes de maior grau de f e g não são divisores de zero, então $\deg(fg) = \deg f + \deg g$.

Exemplo 13.3. Seja $A = \mathbb{Z}_6$. Os polinómios $f(x) = \underline{2}x + \underline{1}$ e $g(x) = \underline{3}x^2 + \underline{2}$ em $\mathbb{Z}_6[x]$ têm graus 1 e 2, respectivamente, mas $f(x)g(x) = \underline{3}x^2 + \underline{4}x + \underline{2}$ tem grau 2 (e não $\deg f + \deg g = 3$).

Teorema 13.4 (algoritmo de divisão)**.** *Sejam $f(x), g(x) \in A[x] \setminus \{0\}$ t.q. $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ com $b_n \in A^\times$. Então $\exists! q(x), r(x) \in A[x]$ t.q.*

$$f(x) = q(x)g(x) + r(x) \quad e \quad \deg r(x) < \deg g(x).$$

Demonstração. Se $\deg f < \deg g$, então como $b_n \in A^\times$, temos

$$f = qg + r \Leftrightarrow q = 0 \wedge r = f.$$

Se $\deg f \geq \deg g = n$, sejam $m = \deg f$ e $a_i \in A$, *t.q.*

$$f(x) = a_m x^m + \cdots + a_0.$$

Então, a equação $f = qg + r$, com $q(x) = c_k x^k + \cdots + c_0$ e $\deg r < n$, verifica-se *sse*

(i) $k + n = m$

(ii)

$$\begin{array}{lcl} c_k b_n & = & a_m \\ c_{k-1}b_n + c_k b_{n-1} & = & a_{m-1} \\ & \vdots & \\ c_0 b_n + c_1 b_{n-1} + \cdots + c_k b_{n-k} & = & a_{m-k} = a_n \end{array} \tag{13.1}$$

(iii) $r = f - qg$.

O sistema (13.1) tem solução única:

$$\begin{array}{lcl} c_k & = & a_m b_n^{-1} \\ c_{k-1} & = & (a_{m-1} - c_k b_{n-1})\, b_n^{-1} \\ & \vdots & \\ c_0 & = & (a_n - c_1 b_{n-1} - \cdots - c_r b_{n-k})\, b_n^{-1} \end{array}$$

portanto, o resultado segue. □

Corolário 13.5. *Se k é um corpo, então $k[x]$ é um domínio euclidiano com $\varphi\colon A[x] \setminus \{0\} \to \mathbb{N}_0; f \mapsto \deg f$. Em particular, $k[x]$ é um* d.i.p. *(e portanto um* d.f.u.*).*

Definição 13.6. *Seja $f \in A[x_1, \ldots, x_n]$. Um elemento $\mathbf{c} = (c_1, \ldots, c_n) \in A^n$ diz-se uma* raiz *de f* sse

$$f = \sum_I a_I x^I \Rightarrow \sum_I a_I c_1^{i_1} \cdots c_n^{i_n} = 0.$$

Ou seja, $\mathbf{c}$ é uma raiz de f se $f(\mathbf{c}) \coloneqq f(c_1, \ldots, c_n) = 0$.

Corolário 13.7. *Seja A um anel comutativo, seja $f(x) \in A[x]$ e seja $c \in A$. Então c é uma raiz de $f(x)$* sse *$x - c \mid f(x)$.*

Demonstração. Se $x-c \mid f$ é claro que $f(c)=0$. Suponhamos que $f(c)=0$. Sejam $q,r \in A[x]$ *t.q.* $\deg r < 1$ e

$$f(x) = (x-c)q(x) + r(x).$$

De $f(c)=0$, vem $f(c)=r(c)=0$, *i.e.*, $r=0$, portanto $(x-c) \mid f(x)$. □

Corolário 13.8. *Seja D um domínio integral. Então $f \in D[x] \setminus \{0\}$ tem no máximo $n = \deg f$ raízes distintas.*

Demonstração. Sejam $c_1, c_2, \ldots, c_m$ raízes distintas de f. Então $f(x) = (x-c_1)q_1(x)$, para algum $q_1(x) \in D[x]$. De $f(c_2)=0$ vem $q_1(c_2)=0$ pois $c_2 - c_1 \neq 0$, logo $f(x) = (x-c_1)(x-c_2)q_2(x)$. Prosseguindo, obtemos $f(x) = (x-c_1)\cdots(x-c_m)q_m(x)$ para algum $q_m(x) \in D[x]\setminus\{0\}$, logo $m \leq n = \deg f$. □

Exemplos 13.9. 1. A condição de D não ter divisores de zero é necessária: $f(x) = 2x(x+1) \in \mathbb{Z}_4[x]$ tem 4 raízes;

2. A comutatividade também é necessária: x^2+1 tem infinitas raízes em $\mathbb{H}[x]$.

Exemplos 13.10. 1. Se $k = \mathbb{C}$ então todos os polinómios de grau positivo têm raízes, logo $f \in \mathbb{C}[x]$ é irredutível *sse* $\deg f = 1$.

2. Se k satisfaz a propriedade de 1. então k diz-se *algebricamente fechado*.

3. Se $k = \mathbb{R}$ e $f \in \mathbb{R}[x]$ então existe $c \in \mathbb{C}$ *t.q.* $f(c) = f(\bar{c}) = 0$. Portanto, temos

$$(x-c)(x-\bar{c}) = (x^2 - 2\operatorname{Re}(c)x + |c|^2) \mid f(x) \quad \text{em } \mathbb{R}[x],$$

se $c \notin \mathbb{R}$ e

$$(x-c) \mid f(x) \quad \text{em } \mathbb{R}[x]$$

se $c \in \mathbb{R}$. Concluímos que $f \in \mathbb{R}[x]$ é irredutível *sse* $\deg f = 1$, ou $\deg f = 2$ e f não tem raízes reais.

4. Pode mostrar-se que em $\mathbb{Z}[x]$ há polinómios irredutíveis de todos os graus.

Em geral, se D é um domínio integral:

(a) $D[x]^\times = D^\times$;

(b) se $c \in D$ é irredutível, então o polinómio constante $f(x) = c$ é irredutível em $D[x]$;

(c) se $f(x) = ax + c$ e $a \in D^\times$ então f é irredutível.

13.1. Factorização em $\mathbb{Z}[x]$

Lema 13.11. *Se $f \in \mathbb{Z}[x]$ tem uma factorização não trivial em $\mathbb{Q}[x]$ então f tem uma factorização não trivial em $\mathbb{Z}[x]$.*

Demonstração. Seja $f(x) = g(x)h(x)$ em $\mathbb{Q}[x]$ e sejam $m,n \in \mathbb{Z}$ *t.q.* $g_1 = mg$, $h_1 = nh \in \mathbb{Z}[x]$. Temos

$$mnf(x) = g_1(x)h_1(x) \in \mathbb{Z}[x].$$

Seja p primo *t.q.* $p \mid mn$. Então

$$\begin{aligned} 0 = \underline{g_1}(x)\underline{h_1}(x) \in \mathbb{Z}_p[x] &\Rightarrow \\ \underline{g_1}(x) = 0 \vee \underline{h_1}(x) = 0 &\Leftrightarrow \\ p \mid g_1(x) \vee p \mid h_1(x) &\Rightarrow \\ \frac{mn}{p} f(x) = g_2(x)f_2(x) \quad \text{em } \mathbb{Z}[x]. & \end{aligned}$$

Prosseguindo, obtemos uma factorização não trivial de $f(x)$ em $\mathbb{Z}[x]$. □

Proposição 13.12 (Critério de Eisenstein)**.** *Seja*

$$f(x) = a_m x^m + \cdots + a_0 \in \mathbb{Z}[x]$$

suponha-se que $\exists\, p \in \mathbb{N}$ *primo* t.q.

1. $p \nmid a_m$
2. $p \mid a_{m-1}, \ldots, a_0$
3. $p^2 \nmid a_0$

Então f *é irredutível em* $\mathbb{Q}[x]$.

Demonstração. Suponhamos que f verifica as condições do enunciado. Se f se factoriza em $\mathbb{Q}[x]$, então f factoriza-se em $\mathbb{Z}[x]$:

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$$

com $r, s < m$, $b_i, c_i \in \mathbb{Z}$. Como $p^2 \nmid a_0$, vem $p \nmid b_0$ ou $p \nmid c_0$, mas $p \mid b_0 c_0$. Podemos supor $p \mid b_0$ e $p \nmid c_0$. Então

$$\begin{aligned}
a_1 &= b_0 c_1 + b_1 c_0 && \Rightarrow p \mid b_1 \\
a_2 &= b_0 c_2 + b_1 c_1 + b_2 c_0 && \Rightarrow p \mid b_2 \\
&\vdots \\
a_r &= b_0 c_r + \cdots + b_r c_0 && \Rightarrow p \mid b_r \Rightarrow p \mid a_m. \qquad \text{Contradição!}
\end{aligned}$$

□

Exemplo 13.13. Em $\mathbb{Z}[x]$, temos

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + 1).$$

Seja $f(x) = x^{p-1} + \cdots + 1$. vejamos que f é irredutível. Note-se que $f(x)$ é irredutível *sse* $f(x+1)$ é irredutível, pois

$$f(x) = g(x)h(x) \Rightarrow f(x+1) = g(x+1)h(x+1)$$

e $g(x), h(x)$ são unidades *sse* $g(x+1), h(x+1)$ o forem.

Temos

$$\begin{aligned}
f(x+1) &= \frac{1}{x+1-1}((x+1)^p - 1) \\
&= \frac{1}{x} \sum_{k=1}^{p} \binom{p}{k} x^k \\
&= \sum_{k=1}^{p} \binom{p}{k} x^{k-1} \\
&= x^{p-1} + p x^{p-2} + \cdots + p.
\end{aligned}$$

Note-se que

1. $p \nmid 1$
2. $p \mid \binom{p}{k}, \quad k = 1, \ldots, p-1$
3. $p^2 \nmid \binom{p}{1}$,

logo, pelo criterio de Eisenstein, $f(x+1)$ é irredutível e portanto $f(x)$ também o é.

13.2. Factorização em $D[x]$ para um domínio integral D:

O Lema 13.11 e a Proposição 13.12 podem ser generalizados para um domínio integral arbitrário D. Para efeito é necessário substituir $\mathbb{Q}$ pelo corpo de fracções $k = \mathrm{Frac}(D)$. O resultado seguinte pode demonstrar-se usando estas generalizações e o facto de $k[x]$ ser um d.f.u.

Teorema 13.14. *Seja D um* d.f.u.*, então $D[x]$ é um* d.f.u..

Corolário 13.15. *Seja D um* d.f.u.*, então $D[x_1, \ldots, x_n]$ é um* d.f.u..

Demonstração. Segue imediatamente do teorema e do isomorfismo

$$D[x_1, \ldots, x_n] \cong D[x_1, \ldots, x_{n-1}][x_n]. \qquad \square$$

Exercícios

2.13.1. Seja D um domínio integral e $c \in D$ um elemento irredutível. Mostre que o ideal $(x, c) \subset D[x]$ não é principal. Portanto $D[x]$ não é um *d.i.p.*.

2.13.2. Mostre que os seguintes anéis não são *d.i.p.*:
(a) $\mathbb{Z}[x]$;
(b) $k[x_1, \ldots, x_n]$, onde k é um corpo e $n \geq 2$.

2.13.3. Seja $f = \sum a_i x^i \in \mathbb{Z}[x]$ e $p \in \mathbb{Z}$ um primo. Seja $\bar{f} = \sum \overline{a_i} x^i \in \mathbb{Z}_p[x]$.
(a) Mostre que, se f é mónico e $\bar{f}$ é irredutível em $\mathbb{Z}_p[x]$ para algum primo p, então f é irredutível em $\mathbb{Z}[x]$.
(b) Dê um exemplo que mostre que a alínea anterior é falsa se f não for um polinómio mónico.
(c) Generalize a alínea (a) para polinómios com coeficientes num *d.f.u.*.

2.13.4. (a) Seja A um anel comutativo, $b \in A$ e $c \in A^\times$. Mostre que existe um único automorfismo de $A[x]$ tal que $x \mapsto cx + b$ e cuja restrição a A é a identidade id_A. Determine o seu inverso.
(b) Seja D um domíneo integral e seja $\varphi \in \mathrm{Aut}(D[x])$ tal que $\varphi|_D = \mathrm{id}_D$. Mostre que φ é da forma descrita em (a).

2.13.5. Seja k um corpo. Mostre que x e y são coprimos (i.e. $\mathrm{MDC}(x, y) = 1$) em $k[x, y]$, mas $k[x, y] = (1) \supsetneq (x) + (y)$.

Categorias

1. Definição e exemplos

Definição 1.1. *Uma categoria $\mathcal{C}$ é uma classe* $\mathrm{Ob}(\mathcal{C})$ *munida de*

(a) conjuntos disjuntos $\mathrm{Hom}_{\mathcal{C}}(X,Y)$, $\forall\, X,Y \in \mathrm{Ob}(\mathcal{C})$*;*

(b) uma operação

$$\forall\, X,Y,Z \in \mathrm{Ob}(\mathcal{C}), \quad \mathrm{Hom}_{\mathcal{C}}(Y,Z) \times \mathrm{Hom}_{\mathcal{C}}(X,Y) \xrightarrow{\circ} \mathrm{Hom}_{\mathcal{C}}(X,Z)$$

t.q.

1. $\forall\, f \in \mathrm{Hom}_{\mathcal{C}}(Z,W)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y,Z)$, $h \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$

$$(f \circ g) \circ h = f \circ (g \circ h);$$

2. $\forall\, X \in \mathrm{Ob}(\mathcal{C})$ $\exists\, \mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X,X)$:

$$f \circ \mathrm{id}_X = f, \quad \forall\, f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$$
$$\mathrm{id}_X \circ g = g, \quad \forall\, g \in \mathrm{Hom}_{\mathcal{C}}(Y,X)$$

Notação 1.2. Os elementos de $\mathrm{Ob}(\mathcal{C})$ dizem-se *objectos* de $\mathcal{C}$. Os elementos de $\mathrm{Hom}_{\mathcal{C}}(X,Y)$ dizem-se *morfismos* de X em Y. Também se usam as notações $\mathrm{Hom}(X,Y)$ ou $\mathcal{C}(X,Y)$ para denotar os morfismos de X em Y na categoria $\mathcal{C}$. A classe de todos morfismos de $\mathcal{C}$ é denotada $\mathrm{Hom}_{\mathcal{C}}$.

Exemplo 1.3. Set é a categoria cujos objectos são os conjuntos e cujos morfismos são as funções entre conjuntos, com a operação de composição de funções.

Observação 1.4. Como o exemplo anterior mostra, em geral, a classe dos objectos de uma categoria não é um conjunto.

Exemplo 1.5. A classe dos grupos e homomorfismos de grupos com a operação de composição é uma categoria Grp - a *categoria dos grupos*.

Exemplo 1.6. A classe dos anéis (com identidade) e homomorfismos de anéis que preservam a identidade é uma categoria Ring.

Exemplo 1.7. Seja G um grupo. A classe dos conjuntos-G com as funções equivariantes é uma categoria Set_G.

Exemplo 1.8. Seja k um corpo. A classe dos espaços vectoriais sobre k com as transformações lineares-k é uma categoria Vect_k.

Observação 1.9. Em todos os exemplos acima, os objectos são conjuntos com estrutura adicional e os morfismos são funções entre conjuntos que preservam a estrutura. Nem todas as categorias são deste tipo, como veremos a seguir.

Exemplo 1.10. Seja G um grupo. Definimos $\mathcal{C}_G$ como a categoria que tem um só elemento, G, com morfismos $\mathrm{Hom}_{\mathcal{C}_G}(G,G) = G$ e com a composição dada por multiplicação em G.

Exemplo 1.11. Seja $(X, \leq)$ um conjunto parcialmente ordenado. Então $(X, \leq)$ determina uma categoria cujos objectos são os elementos de X e *t.q.*, para $x, y \in X$, $\mathrm{Hom}(x,y)$ tem um elemento se $x \leq y$ e $\mathrm{Hom}(x,y) = \varnothing$, caso contrário.

Observação 1.12. Como este exemplo ilustra, se $X \neq Y$, pode ter-se $\mathrm{Hom}_{\mathcal{C}}(X,Y) = \varnothing$.

Exemplo 1.13. Seja $\mathcal{C}$ uma categoria. Define-se $\mathcal{C}^{op}$ como a categoria que tem os mesmos objectos que $\mathcal{C}$ e cujos morfismos são dados por

$$\mathrm{Hom}_{\mathcal{C}^{op}}(X,Y) \coloneqq \mathrm{Hom}_{\mathcal{C}}(Y,X),$$

e cuja composição é dada por

$$f \circ_{\mathcal{C}^{op}} g \coloneqq g \circ_{\mathcal{C}} f,$$

onde $g \in \mathrm{Hom}_{\mathcal{C}^{op}}(X,Y)$ e $f \in \mathrm{Hom}_{\mathcal{C}^{op}}(Y,Z)$. Diz-se que $\mathcal{C}^{op}$ é a *categoria oposta* de $\mathcal{C}$.

Definição 1.14. *Sejam X, Y objectos de uma categoria $\mathcal{C}$. Se existem $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y,X)$* t.q. *$f \circ g = \mathrm{id}_Y$ e $g \circ f = \mathrm{id}_X$, diz-se que X e Y são* isomorfos *e denota-se $X \cong Y$. Diz-se que f, g são* isomorfismos.

Exemplos 1.15.

1. Em $\mathrm{Grp}, \mathrm{Ring}, \mathrm{Vect}_k$ os isomorfismos coincidem com as definições dadas anteriormente (Exercício 3.1.2).
2. Em $\mathcal{C}_G$ todos os morfismos são isomorfismos.

Definição 1.16. *Seja $\mathcal{C}$ uma categoria e sejam $X, Y \in \mathrm{Ob}(\mathcal{C})$. Diz-se que $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ é* mónico*, ou um* monomorfismo*, se*

$$\forall_{Z \in \mathrm{Ob}(\mathcal{C})} \forall_{g,g' \in \mathrm{Hom}_{\mathcal{C}}(Z,X)} \quad f \circ g = f \circ g' \Rightarrow g = g'.$$

Diz-se que f é epi*, ou um* epimorfismo*, se*

$$\forall_{Z \in \mathrm{Ob}(\mathcal{C})} \forall_{h,h' \in \mathrm{Hom}_{\mathcal{C}}(Y,Z)} \quad h \circ f = h' \circ f \Rightarrow h = h'.$$

Exemplos 1.17. Em Set, Grp e Ring os morfismos mónicos são aqueles que são funções injectivas. Os morfismos epi são os que são funções sobrejectivas em Set e Grp. Mas em Ring há morfismos epi que não funções sobrejectivas, por exemplo, a inclusão $\mathbb{Z} \to \mathbb{Q}$ é epi e claramente não é sobrejectiva.

Exemplo 1.18. Seja Top a categoria dos espaços topológicos com as aplicações contínuas como morfismos. Se $X, Y \in \mathrm{Top}$ e $f \in \mathrm{Hom}_{\mathrm{Top}}(X,Y)$, então f é epi *sse* $\mathrm{im}\, f$ é denso em Y.

Exercícios

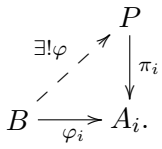
3.1.1. Seja $f : X \to Y$ um isomorfismo na categoria $\mathcal{C}$. Mostre que existe um *único* morfismo $g : Y \to X$ tal que $f \circ g = \mathrm{id}_Y$ e $g \circ f = \mathrm{id}_X$.

3.1.2. Mostre que a Definição 1.14 de isomorfismo nas categorias $\mathrm{Grp}, \mathrm{Ring}, \mathrm{Vect}_k$ coincide com as definições dadas anteriormente. Isto é, mostre que dado um morfismo $f : X \to Y$ na categoria $\mathcal{C}$ tal que existe um morfismo $g : Y \to X$ satisfazendo $f \circ g = \mathrm{id}_Y$ e $g \circ f = \mathrm{id}_X$ *sse* f é uma bijecção, onde $\mathcal{C}$ é uma das categorias $\mathrm{Grp}, \mathrm{Ring}, \mathrm{Vect}_k$.

3.1.3. Mostre que, na categoria $\mathcal{C}_G$ definida no Exemplo 1.10, todos os morfismos são isomorfismos, epimorfismos e monomorfismos.

2. Produtos e coprodutos

Definição 2.1. *Seja $\mathcal{C}$ uma categoria e seja $\{A_i \mid i \in I\}$ uma família de objectos de $\mathcal{C}$. Um* produto *desta família é um objecto $P \in \mathrm{Ob}(\mathcal{C})$ com morfismos $\pi_i \in \mathrm{Hom}_{\mathcal{C}}(P, A_i)$, $i \in I$,* t.q. *dado $B \in \mathrm{Ob}(\mathcal{C})$ e morfismos $\varphi_i \in \mathrm{Hom}_{\mathcal{C}}(B, A_i)$, $i \in I$, existe um único morfismo $\varphi \in \mathrm{Hom}_{\mathcal{C}}(B, P)$ que, para cada $i \in I$, faz comutar o diagrama*



Exemplo 2.2. Em Set o produto é o produto cartesiano.

Exemplo 2.3. Em Grp, dada uma família de grupos $\{G_i \mid i \in I\}$, o produto directo $P = \prod_{i\in I} G_i$, com as projecções $\pi_i \colon P \to G_i$, $i \in I$, é um produto.

Exemplo 2.4. Em Ring, dada uma familia de anéis $\{A_i \mid i \in I\}$, o produto directo de anéis $P = \prod_{i\in I} A_i$ é um produto.

Em geral, o produto pode não existir, como o exemplo seguinte mostra.

Exemplo 2.5. Seja Field a categoria dos corpos e homomorfismos de corpos. Note-se que a existência de um homomorfismo de corpos $k \to k'$ implica $\operatorname{car} k = \operatorname{car} k'$. Concluímos que não existe em Field o produto de $\mathbb{F}_p \coloneqq \mathbb{Z}_p$ e $\mathbb{Q}$.

Teorema 2.6. *Sejam P, Q produtos de uma família de objectos $\{A_i \mid i \in I\}$ numa categoria $\mathcal{C}$. Então $P \cong Q$.*

Demonstração. Sejam $\pi_i \in \mathrm{Hom}_{\mathcal{C}}(P, A_i)$, $\varrho_i \in \mathrm{Hom}_{\mathcal{C}}(Q, A_i)$, $i \in I$, os morfismos de estrutura dos dois produtos. Do facto de P, Q serem produtos em $\mathcal{C}$, obtemos

$$f \in \mathrm{Hom}_{\mathcal{C}}(P, Q), \quad g \in \mathrm{Hom}_{\mathcal{C}}(Q, P)$$

t.q.

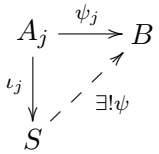
$$\varrho_i \circ f = \pi_i, \quad \pi_i \circ g = \varrho_i,$$

logo $g \circ f \in \mathrm{Hom}_{\mathcal{C}}(P, P)$ satisfaz

$$\pi_i \circ (g \circ f) = \varrho_i \circ f = \pi_i = \pi_i \circ \mathrm{id}_P,$$

o que implica $g \circ f = \mathrm{id}_P$. Da mesma forma se prova $f \circ g = \mathrm{id}_Q$. □

Definição 2.7. *Seja $\{A_j \mid j \in I\}$ uma família de objectos de $\mathcal{C}$. Um* coproduto *desta família é um objecto S conjuntamente com morfismos $\iota_j \in \mathrm{Hom}_{\mathcal{C}}(A_j, S)$, $j \in I$,* t.q.*, dado $B \in \mathrm{Ob}(\mathcal{C})$, e morfismos $\psi_j \in \mathrm{Hom}_{\mathcal{C}}(A_j, B)$ existe um único morfismo $\psi \in \mathrm{Hom}_{\mathcal{C}}(S, B)$ que faz comutar, para cada $j \in I$, o diagrama*



Teorema 2.8. *Sejam $(S, \{\iota_j \mid j \in I\})$ e $(S', \{\iota'_j \mid j \in I\})$ coprodutos de $\{A_j \mid j \in I\}$ em $\mathcal{C}$. Então $S \cong S'$.*

Notação 2.9. Denotamos por $\coprod_{j\in I} A_j$ o coproduto de $\{A_j \mid j \in I\}$, quando este existe.

Exemplo 2.10. Seja $\{A_j \mid j \in I\}$ uma família de grupos abelianos. Recorde-se que a soma directa $\bigoplus_{j\in I} A_j$ é o subgrupo de $\prod_{j\in I} A_j$ dado por:

$$\bigoplus_{j\in I} A_j = \{(a_j)_{j\in I} \mid |\{j \in I \mid a_j \neq 0\}| < \infty\}.$$

Para cada $j \in I$, define-se $\iota_j \colon A_j \to \bigoplus_{i\in I} A_i; a \mapsto (a_i)_{i\in I}$, onde

$$a_i = \begin{cases} a, & i = j \\ 0, & i \neq j. \end{cases}$$

Vejamos que $(\bigoplus_{j\in I} A_j, \{\iota_j \mid j \in I\})$ é um coproduto na categoria Ab.

De facto, dados $\psi_i \in \mathrm{Hom}_{\mathrm{Ab}}(A_i, B)$, definimos

$$\psi\left((a_i)_{i\in I}\right) = \sum_{i\in I} \psi_i(a_i).$$

Note-se que a soma está bem definida porque só um número finito de parcelas são não nulas. Claramente $\psi \in \mathrm{Hom}_{\mathrm{Ab}}\left(\oplus_{i\in I}, B\right)$ e, por construção

$$\psi \circ \iota_j = \psi_j.$$

Exercícios

3.2.1. Seja $(S, \{\iota_j\}_{j\in I})$ um produto da família $\{A_j \mid j \in I\}$ em $\mathcal{C}$. Mostre que $(S, \{\iota_j\}_{j\in I})$ é um coproduto em $\mathcal{C}^{op}$.

3.2.2. Demonstre o Teorema 2.8.

3.2.3. Mostre que, na categoria dos conjuntos Set, qualquer família $\{A_j \mid j \in I\}$ tem um coproduto.
Sugestão: Considere

$$\coprod_{j\in I} A_j \coloneqq \left\{(a, j) \in (\cup_{j\in I} A_i) \times I \mid a \in A_j\right\}$$

com as "inclusões" $\iota_j : A_j \to \coprod_{j\in I} A_j$ dadas por $a \mapsto (a, j)$. O conjunto $\coprod_{j\in I} A_j$ diz-se a *união disjuntas* dos conjunto A_j.

3. Objectos universais

Definição 3.1. *Um objecto I numa categoria $\mathcal{C}$ diz-se* inicial *se*

$$\forall\, C \in \mathrm{Ob}(\mathcal{C})\ |\mathrm{Hom}_{\mathcal{C}}(I, C)| = 1.$$

Um objecto $T \in \mathrm{Ob}(\mathcal{C})$ diz-se terminal *se*

$$\forall\, C \in \mathrm{Ob}(\mathcal{C})\ |\mathrm{Hom}_{\mathcal{C}}(C, T)| = 1.$$

Exemplo 3.2. Em Set, $\varnothing$ é um objecto inicial. Se X é um conjunto *t.q.* $|X| = 1$, então $X \in \mathrm{Set}$ é um objecto terminal.

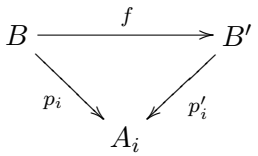
Exemplo 3.3. Na categoria Field não há objectos iniciais nem terminais, pois

$$\mathrm{Hom}_{\mathrm{Field}}(F_1, F_2) \neq \varnothing \Rightarrow \mathrm{car}\, F_1 = \mathrm{car}\, F_2.$$

Teorema 3.4. *Sejam I_1, I_2 objectos iniciais de uma categoria $\mathcal{C}$. Então $I_1 \cong I_2$. O mesmo se verifica para objectos terminais.*

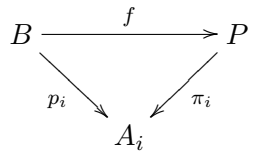
Demonstração. Seja $f\colon I_1 \to I_2$ e $g\colon I_2 \to I_1$ os morfismos cuja existência é garantida pela hipótese do enunciado. Temos, $f \circ g\colon I_2 \to I_2$, logo por unicidade, $f \circ g = \mathrm{id}_{I_2}$. Da mesma forma se prova que $g \circ f = \mathrm{id}_{I_1}$. □

Exemplo 3.5. Sejam A_1, A_2 objectos de uma categoria $\mathcal{C}$. Definimos uma categoria $\mathcal{D}$ cujos objectos são pares $(B, \{p_1, p_2\})$ onde $p_i \in \mathrm{Hom}_{\mathcal{C}}(B, A_i)$. Os morfismos em $\mathcal{D}$, $(B, \{p_1, p_2\}) \to (B', \{p_1', p_2'\})$ são morfismos $f\colon B \to B'$ de $\mathcal{C}$ *t.q.* o diagrama



comuta para $i = 1, 2$.

Um objecto $(P, \{\pi_i\colon P \to A_i\})$ nesta categoria é terminal *sse* $(P, \{\pi_i\colon P \to A_i\})$ é um produto em $\mathcal{C}$: dar $p_i\colon B \to A_i$, $i = 1, 2$, é equivalente a dar um objecto $(B, \{p_i\}) \in \mathrm{Ob}(\mathcal{D})$ e dar $f\colon B \to P$ fazendo comutar, para $i = 1, 2$,



é equivalente a dar um morfismo $(B, \{p_i\}) \to (P, \{\pi_i\})$ em $\mathcal{D}$.

Observação 3.6. O Exemplo 3.5 e o Exercício 3.3.4 podem ser generalizados para o caso de uma família arbitrária de objectos $\{A_i \mid i \in I\}$ em $\mathcal{C}$.

Exercícios

3.3.1. Mostre que o grupo trivial $\{\mathbf{1}\}$ é um objecto final e inicial na categoria Grp.

3.3.2. Mostre que o anel trivial $\{\mathbf{0}\}$ é um objecto terminal e $\mathbb{Z}$ é um objecto inicial na categoria Ring.

3.3.3. Mostre que um objecto T é terminal na categoria $\mathcal{C}$ *sse* T é inicial em $\mathcal{C}^{op}$.

3.3.4. Dada uma categoria $\mathcal{C}$, defina uma categoria $\mathcal{D}$ onde os objectos iniciais de $\mathcal{D}$ correspondem aos coprodutos de $\mathcal{C}$.
Sugestão: Exemplo 3.5.

4. Functores e transformações naturais

Frequentemente estudam-se relações entre várias categorias. Para esse efeito existe uma noção de morfismo entre categorias.

Definição 4.1. *Um* functor (covariante) *entre duas categorias, $\mathcal{C}$, $\mathcal{D}$, é um par de funções (denotadas pelo mesmo símbolo) $T\colon \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ e $T\colon \mathrm{Hom}_{\mathcal{C}} \to \mathrm{Hom}_{\mathcal{D}}$* t.q.

1. $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y) \Rightarrow T(f) \in \mathrm{Hom}_{\mathcal{D}}(TX,TY)$;
2. $T(\mathrm{id}_X) = \mathrm{id}_{TX}$;
3. $T(f \circ g) = T(f) \circ T(g)$.

Definição 4.2. *Substituindo na Definição 4.1 as condições 1. e 3. por*

1'. $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y) \Rightarrow T(f) \in \mathrm{Hom}_{\mathcal{D}}(TY,TX)$;
3'. $T(f \circ g) = T(g) \circ T(f)$

obtém-se a noção de functor contravariante. *Excepto menção em contrário, todos os functores considerados são covariantes.*

Notação 4.3. Utilizamos $T\colon \mathcal{C} \to \mathcal{D}$ para denotar que T é um functor covariante de $\mathcal{C}$ em $\mathcal{D}$.

Exemplo 4.4. A função $T\colon \mathrm{Grp} \to \mathrm{Set}$, que envia um grupo no seu conjunto de suporte (o conjunto dos seus elementos), esquecendo a estrutura de grupo, e que envia um homomorfismo na respectiva função entre conjuntos suporte, é um functor. Designa-se *functor de esquecimento.*

Exemplo 4.5. Da mesma forma, existem functores de esquecimento $\mathrm{Ring} \to \mathrm{Set}$, $\mathrm{Field} \to \mathrm{Set}$, $\mathrm{Set}_G \to \mathrm{Set}$.

Exemplo 4.6. Sejam G, G' grupos e seja $\alpha\colon G \to G'$ um homomorfismo. Então α define um functor $\mathcal{C}_G \to \mathcal{C}_{G'}$.

Exemplo 4.7. Seja G um grupo e seja $i\colon G \to G'$ a função $i(g) = g^{-1}$. Então i define um functor contravariante de $\mathcal{C}_G$ em $\mathcal{C}_G$, pois

$$\forall\, g,h \in G \quad i(g \circ h) = i(gh) = (gh)^{-1} = h^{-1}g^{-1} = i(h) \circ i(g).$$

Exemplo 4.8. As funções

$$\mathrm{Vect}_k \ni V \to V^\star \coloneqq \mathrm{Hom}_{\mathrm{Vect}_k}(V,k)$$
$$\mathrm{Hom}_{\mathrm{Vect}_k}(V,W) \ni f \mapsto (f^\star\colon W^\star \to V^\star; \varphi \mapsto \varphi \circ f)$$

definem um functor contravariante $\mathrm{Vect}_k \to \mathrm{Vect}_k$.

Definição 4.9. *Seja $\mathcal{C}$ uma categoria. Uma* subcategoria *de $\mathcal{C}$ é uma subclasse de objectos $\mathrm{Ob}(\mathcal{C}') \subset \mathrm{Ob}(\mathcal{C})$ munida de subconjuntos $\mathrm{Hom}_{\mathcal{C}'}(X,Y) \subset \mathrm{Hom}_{\mathcal{C}}(X,Y)$, $\forall X,Y \in \mathrm{Ob}(\mathcal{C}')$,* t.q. *$(\mathrm{Ob}(\mathcal{C}'), \mathrm{Hom}_{\mathcal{C}'})$ é uma categoria (com a operação de composição de $\mathcal{C}$).*

Exemplo 4.10. Os grupos abelianos e homomorfismos de grupos abelianos formam uma subcategoria de Grp denotada Ab.

Exemplo 4.11. A categoria Col_k cujos objectos são os espaços vectoriais sobre k da forma k^n, $n \in \mathbb{N}$, e cujos morfismos são as transformações lineares $k^n \to k^n$, é uma subcategoria de Vect_k.

Observação 4.12. Se $\mathcal{C}' \subset \mathcal{C}$ é uma subcategoria, as inclusões $\mathrm{Ob}(\mathcal{C}') \subset \mathrm{Ob}(\mathcal{C})$ e $\mathrm{Hom}_{\mathcal{C}'} \subset \mathrm{Hom}_{\mathcal{C}}$ definem um functor $i\colon \mathcal{C}' \to \mathcal{C}$.

Definição 4.13. *Sejam $\mathcal{C}, \mathcal{D}$ categorias e seja $T\colon \mathcal{C} \to \mathcal{D}$ um functor. Então,*

1. *se $T\colon \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ e $T\colon \mathrm{Hom}_{\mathcal{C}} \to \mathrm{Hom}_{\mathcal{D}}$ são funções bijectivas, T diz-se um* isomorfismo *de categorias e as categorias $\mathcal{C}$ e $\mathcal{D}$ dizem-se isomorfas ou* equivalentes.

2. se

$$\forall_{X,Y\in \mathrm{Ob}(\mathcal{C})}\, \forall_{f,f'\, \mathrm{Hom}_{\mathcal{C}}(X,Y)} \quad T(f) = T(f') \Rightarrow f = f'.$$

diz-se que T é fiel*;*

3. se

$$\forall_{X,Y\in \mathrm{Ob}(\mathcal{C})}\, \forall_{g\in \mathrm{Hom}_{\mathcal{D}}(TX,TY)}\, \exists_{f\in \mathrm{Hom}_{\mathcal{C}}(X,Y)} \quad T(f) = g.$$

diz-se que T é pleno*.*

Observação 4.14. Um functor $T\colon \mathcal{C} \to \mathcal{D}$ é fiel *sse*

$$\forall_{X,Y\in \mathrm{Ob}(\mathcal{C})} \quad T\colon \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{D}}(TX,TY)$$

é injectivo; e é pleno *sse*

$$\forall_{X,Y\in \mathrm{Ob}(\mathcal{C})} \quad T\colon \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{D}}(TX,TY)$$

é sobrejectivo.

Exemplo 4.15. O functor de inclusão $T\colon \mathrm{Ab} \to \mathrm{Grp}$ é fiel e pleno, pois

$$\forall_{G,H\in \mathrm{Ob(Ab)}} \quad \mathrm{Hom}_{\mathrm{Grp}}(G,H) = \mathrm{Hom}_{\mathrm{Ab}}(G,H),$$

mas não é um isomorfismo de categorias pois $T\colon \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ não é sobrejectivo.

Exemplo 4.16. O functor de esquecimento $E\colon \mathrm{Grp} \to \mathrm{Set}$ é fiel mas não é pleno, pois, em geral,

$$\mathrm{Hom}_{\mathrm{Grp}}(G,H) \subsetneq \{f\colon G \to H\} = \mathrm{Hom}_{\mathrm{Set}}(G,H).$$

Definição 4.17. *Uma categoria $\mathcal{C}$ diz-se* concreta *se existe um functor fiel $\sigma\colon \mathcal{C} \to \mathrm{Set}$.*

Muitas categorias têm uma estrutura óbvia de categoria concreta pois os seus objectos são conjuntos com estrutura adicional e os morfismos são funções que preservam essa estrutura. Nesse caso $\sigma\colon \mathcal{C} \to \mathrm{Set}$ é simplesmente o functor de esquecimento.

Exemplos 4.18. Grp, Ring, Field e Set_G são categorias concretas. Neste caso, σ é o functor de esquecimento.

Mesmo que a categoria não seja de forma óbvia uma categoria concreta, pode ser possível definir σ por forma torná-la concreta.

Exemplo 4.19. Se G é um grupo, $\mathcal{C}_G$ é uma categoria concreta: $\sigma\colon \mathcal{C}_G \to \mathrm{Set}$ envia o único objecto no conjunto G e envia cada morfismo $g \in G$ na função $l_g\colon G \to G; h \mapsto gh$.

Há também exemplos de categorias que não podem ser concretizadas, mas estes exemplos saem do âmbito destas notas.

Definição 4.20. *Dados dois functores $S, T : \mathcal{C} \to \mathcal{D}$, uma* transformação natural $\alpha : S \to S$ *é uma função $\alpha : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Hom}_{\mathcal{D}}$ (denotada pela mesma letra) que a cada objecto $C \in \mathrm{Ob}(\mathcal{C})$ faz corresponder um morfismo $\alpha_C \in \mathrm{Hom}_{\mathcal{D}}(S(C),T(C))$ tal que $\forall\, A,B \in \mathrm{Ob}(\mathcal{C})$ e $\forall\, f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ o seguinte diagrama comuta*

$$\begin{array}{ccc} A & & S(A) \xrightarrow{\alpha_A} T(B) \\ {\scriptstyle f}\downarrow & \qquad & {\scriptstyle S(f)}\downarrow \qquad\quad \downarrow{\scriptstyle T(f)} \\ B & & S(B) \xrightarrow[\alpha_B]{} T(B) \end{array}$$

Ou seja, uma transformação natural pode ser vista como um morfismo entre functores.

Exemplo 4.21. Seja A um anel comutativo e $M_n(A)$ o monóide das matrizes $n \times n$ de entradas em A, com o produto. Como $M \in M_n(A)$ é invertível se e só se $\det_A(M) \in A^\times$ e $\det_A(MN) = \det_A(M)\det_A(N)$, o determinante define um homomorfismos de grupos (multiplicativos) $\det_A\colon \mathrm{GL}_n(A) \to A^\times$. Além disso, como a fórmula para calcular o determinante é a "mesma" indepentendemente do anel A, temos que

$$\begin{array}{ccc} \mathrm{GL}_n(A) & \xrightarrow{\det_A} & A^\times \\ {\scriptstyle \mathrm{GL}_n(f)}\downarrow & & \downarrow{\scriptstyle f^\times := f|_{A^\times}} \\ \mathrm{GL}_n(B) & \xrightarrow[\det_B]{} & B^\times \end{array}$$

é um diagrama comutivo, onde $f : A \to B$ é um homomorfismo de anéis qualquer. Ou seja, $\det : \mathrm{GL}_n \to ()^\times$ é uma transformação natural entre os functores $\mathrm{GL}_n : \mathrm{CRing} \to \mathrm{Grp}$ e $()^\times : \mathrm{CRing} \to \mathrm{Grp}$. (CRing é a subcategoria plena de Ring cujos objectos são os anéis comutativos.)

Exercícios

3.4.1. Mostre que dar um functor contravariante de $\mathcal{C}$ em $\mathcal{D}$ é equivalente a dar um functor covariante $T\colon \mathcal{C}^{op} \to \mathcal{D}^{op}$.

3.4.2. Sejam G e H grupos e $f : G \to H$ um homomorfismo de grupos.

(a) Mostre que $C : \mathrm{Grp} \to \mathrm{Grp}$ definido por $G \mapsto [G,G]$ e $f \mapsto f|_{[G,G]}$ é um functor.

(b) Mostre que $Q : \mathrm{Grp} \to \mathrm{Grp}$ dado por $G \mapsto G/[G,G]$, e onde $Q(f) : G/[G,G] \to H/[H,H]$ é o homomorfismo de grupos induzido por f, é um functor.

(c) Mostre que as projecções canónicas $\pi_G : G \to G/[G,G]$ definem uma transformação natural entre o functor identidade $\mathrm{id} : \mathrm{Grp} \to \mathrm{Grp}$ e o functor "quociente pelo comutador" $Q : \mathrm{Grp} \to \mathrm{Grp}$ da alínea anterior.

3.4.3. Mostre que não existe nenhum functor $\mathrm{Grp} \to \mathrm{Ab}$ tal que a cada grupo G faz corresponder o seu centro $Z(G)$.

3.4.4. Seja $\mathrm{Ob}(\mathcal{C})$ o conjunto dos pares (A,S), onde $A \in \mathrm{Ob}(\mathrm{CRing})$ e $S \subset A$ é um conjunto multiplicativo, e

$$\mathrm{Hom}_{\mathcal{C}}((A,S),(B,R)) := \{f \in \mathrm{Hom}_{\mathrm{CRing}}(A,B) \mid f(S) \subset R\}\ .$$

(a) Mostre que $\mathcal{C}$ é uma categoria.

(b) Mostre que $F(A,S) = S^{-1}A$ define um functor $F : \mathcal{C} \to \mathrm{CRing}$.

(c) Seja $E : \mathcal{C} \to \mathrm{CRing}$ o functor de esquecimento definido por $E(A,S) = A$ nos objectos de $\mathcal{C}$. Mostre que os homomorfismos $\varphi_S : A \to S^{-1}A$, $\varphi_S(a) = \frac{a}{\mathbf{1}}$, definem uma transformação natural entre os functores E e F.

Capítulo 4

Módulos

1. Definição e exemplos

Definição 1.1. *Seja A um anel. Um* módulo (à esquerda) *sobre A é um grupo abeliano $(M,+)$ com uma operação $A\times M\to M$ denotada por justaposição $(a,\mathbf{m})\mapsto a\mathbf{m}$* t.q. *para todo $a,b\in A$ e $\mathbf{m},\mathbf{m}'\in M$ se tem*

(a) $(a+b)\mathbf{m}=a\mathbf{m}+b\mathbf{m}$*;*

(b) $a(\mathbf{m}+\mathbf{m}')=a\mathbf{m}+a\mathbf{m}'$*;*

(c) $(ab)\mathbf{m}=a(b\mathbf{m})$*;*

(d) $1_A\mathbf{m}=\mathbf{m}$*.*

De forma análoga, define-se módulo à direita*: é um grupo abeliano $(M,+)$ munido de uma operação $M\times A\to M;(\mathbf{m},a)\to \mathbf{m}a$ satisfazendo as propriedades:*

(a)' $\mathbf{m}(a+b)=\mathbf{m}a+\mathbf{m}b$*;*

(b)' $(\mathbf{m}+\mathbf{m}')a=\mathbf{m}a+\mathbf{m}'a$*;*

(c)' $\mathbf{m}(ab)=(\mathbf{m}a)b$*.*

(d)' $\mathbf{m}1_A=\mathbf{m}$*.*

Notação 1.2. Por vezes designa-se os elementos de A por *escalares* e os elementos M por *vectores*. A operação $A\times M\to M$ (ou $M\times A\to M$, num módulo à direita) é designada por *multiplicação por escalares*.

Observação 1.3. A diferença entre módulo à esquerda e módulo à direita consiste na relação entre o produto em A e o produto de elementos de M por escalares: o resultado de multiplicar $\mathbf{m}\in M$ pelo produto de escalares ab é:

- multiplicar $\mathbf{m}$ primeiro por b e multiplicar o resultado por a – se o módulo é à esquerda;
- multiplicar $\mathbf{m}$ primeiro por a e multiplicar o resultado por b – se o módulo é à direita.

É claro que se A é comutativo, as noções de módulo à esquerda e à direita coincidem.

Notação 1.4.

1. Daqui em diante, todos os módulos considerados serão módulos à esquerda, excepto menção em contrário.
2. Os módulos sobre A são designado módulos-A.

Exemplos 1.5. Seja A um anel.

(a) A é um módulo-A (à esquerda e à direita).

(b) Seja $I \subset A$ um ideal à esquerda (direita), então I é um módulo à esquerda (respectivamente à direita).

(c) A^n tem uma estrutura natural de módulo-A dada pela seguinte operação $A \times A^n \to A^n$:

$$a \cdot (a_1, \ldots, a_n) \coloneqq (aa_1, \ldots, aa_n).$$

(d) Seja $(G, +)$ um grupo abeliano. Então G é um módulo-$\mathbb{Z}$: dado $n \in \mathbb{N}$, define-se

$$n \cdot g \coloneqq \overbrace{g + \cdots + g}^{n \text{ vezes}}$$
$$(-n) \cdot g \coloneqq \underbrace{(-g) + \cdots + (-g)}_{n \text{ vezes}}$$

É imediato verificar que a operação $\mathbb{Z} \times G \to G$ assim definida dá a G uma estrutura de módulo-$\mathbb{Z}$. Reciprocamente, se G é um módulo-$\mathbb{Z}$ então G é um grupo abeliano e dados $n \in \mathbb{N}$, $g \in G$, pela propriedades (a) e (d) da Definição 1.1, tem-se

$$n \cdot g = (\underbrace{1 + \cdots + 1}_{n \text{ vezes}}) \cdot g = \underbrace{g + \cdots + g}_{n \text{ vezes}}.$$

Portanto, a estrutura de módulo-$\mathbb{Z}$ é equivalente à estrutura de grupo abeliano.

(e) Se B é um anel contendo A como um subanel, então B tem uma estrutura natural de módulo-A dada pela restrição da multiplicação $B \times B \to B$ a $A \times B \subset B \times B$.

(f) Seja k um corpo. Um módulo sobre k é um espaço vectorial sobre k. Mais geralmente, se D é um anel de divisão e M é um módulo sobre D, diz-se que M é um *espaço vectorial* sobre D (ou espaço vectorial-D).

(g) Seja X uma varidedade diferenciável e seja $\Omega^k(X)$ o grupo das formas-k diferenciáveis. Então, $\Omega^k(X)$ munido da operação de multiplicação por funções diferenciáveis – denotadas $C^\infty(X)$ – é um módulo-$C^\infty(X)$.

Lema 1.6. *Seja M um módulo-A. Para $a \in A$, $\mathbf{v} \in M$ e $n \in \mathbb{Z}$, temos*

(a) $a \cdot 0_M = 0_M$;

(b) $0_A \cdot \mathbf{v} = 0_M$;

(c) $(-a)\mathbf{v} = -(a\mathbf{v}) = a(-\mathbf{v})$;

(d) $n(a\mathbf{v}) = a(n\mathbf{v})$;

Demonstração. (a) $a \cdot 0_M + a \cdot 0_M = a \cdot (0_M + 0_M) = a \cdot 0_M \Rightarrow a \cdot 0_M = 0_M$;

(b) $0_A \cdot \mathbf{v} + 0_A \cdot \mathbf{v} = (0_A + 0_A) \cdot \mathbf{v} = 0_A \cdot \mathbf{v} \Rightarrow 0_A \cdot \mathbf{v} = 0_M$;

(c) $(-a) \cdot \mathbf{v} + a \cdot \mathbf{v} = (-a + a) \cdot \mathbf{v} = 0_A \cdot \mathbf{v} = 0_M \Rightarrow (-a) \cdot \mathbf{v} = -a \cdot \mathbf{v}$;

(d) Para $n = 0$ segue da definição de $n\mathbf{w}$ e de (a) e (b).
Para $n \in \mathbb{N}$ usamos indução: o caso $n = 1$ segue da definição de $n\mathbf{w}$ e de (d) da Definição 1.1. Supondo a afirmação verdadeira para n, temos

$$(n+1)(a\mathbf{v}) = n(a\mathbf{v}) + 1(a\mathbf{v}) = a(n\mathbf{v}) + a(1\mathbf{v}) = a(n\mathbf{v} + 1\mathbf{v}) = a((n+1)\mathbf{v}) \ ,$$

onde usámos sucessivamente, a definição de $(n+1)(a\mathbf{v})$ no módulo M, a hipótese e a base de indução, a condição (b) na Definição 1.1, a definição de $(n+1)\mathbf{v}$ em M.
Para $-n \in \mathbb{N}$ segue de (c) e do resultado para $n \in \mathbb{N}$. □

2. Homomorfismos e quocientes

Definição 2.1. *Sejam M, N módulos-A. Um* homomorfismo de módulos-A *é um homomorfismos de grupos abelianos $f\colon M \to N$ tal que*

$$\forall a \in A, \forall \mathbf{v} \in M \quad f(a\mathbf{v}) = af(\mathbf{v}).$$

Um submódulo *de M é um módulo-A, $M' \subset M$,* t.q. *a inclusão $i\colon M' \to M$ é um homomorfismo de módulos-A.*

Notação 2.2. Os homomorfismos de módulos-A também se dizem transformações ou aplicações lineares-A. O conjunto das transformações lineares-A de M em N é denotado $\mathrm{Hom}_A(M, N)$.

Definição 2.3. *A classe dos módulos sobre um anel A e respectivos homomorfismos é uma categoria denotada* Mod_A.

Exemplos 2.4. 1. Seja A um anel. Recorde-se que A tem uma estrutura natural de módulo-A à esquerda. Os submódulos desta estrutura são exactamente os ideais esquerdos. Analogamente, os ideais direitos são os submódulos de A quando munido da sua estrutura natural de módulo-A à direita.

2. Seja V um espaço vectorial sobre um corpo k. Os submódulos-k de V são os subespaços vectoriais de V e os morfismos de módulos-k são as aplicações lineares sobre k.
3. Os homomorfismos de grupos abelianos são os morfismos de módulos-$\mathbb{Z}$. Os submódulos-$\mathbb{Z}$ são os subgrupos abelianos.
4. Se $f\colon M \to N$ é um homomorfismo de módulos-A, então

$$\ker f \subset M \quad \text{e} \quad \mathrm{im}\, f \subset N$$

são submódulos-A.

Observação 2.5. O exemplos 2 e 3 acima podem ser refraseados dizendo que a categoria Mod_k é equivalente a Vect_k e que $\mathrm{Mod}_{\mathbb{Z}}$ é equivalente a Ab.

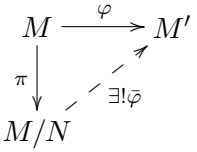
Definição 2.6. *Seja M um módulo-A e seja $N \subset M$ um submódulo. O grupo quociente M/N tem uma estrutura de módulo-A dada por:*

$$\forall\, a \in A, \forall\, \mathbf{v} \in M \quad a(\mathbf{v} + N) \coloneqq a\mathbf{v} + N.$$

Diz-se que M/N é o módulo quociente *de M por N. Com esta estrutura, a projecção canónica $\pi\colon M \to M/N$ é um homomorfismo de módulos-A* t.q. $\ker \pi = N$.

Exemplo 2.7. Seja $I \subset A$ um ideal esquerdo. Então o quociente A/I tem uma estrutura natural de módulo-A e a projecção $\pi\colon A \to A/I$ é linear-A.

Proposição 2.8. *Seja $M \in \mathrm{Mod}_A$ e seja $N \subset M$ um submódulo-A. Então o módulo quociente M/N tem a seguinte propriedade universal: dados $M' \in \mathrm{Mod}_A$ e $\varphi \in \mathrm{Hom}_A(M, M')$* t.q. *$N \subset \ker \varphi$, existe um único $\bar{\varphi} \in \mathrm{Hom}_A(M/N, M')$* t.q.



Temos $\mathrm{im}\, \bar{\varphi} = \mathrm{im}\, \varphi$ e $\ker \bar{\varphi} = \pi(\ker \varphi)$.

Demonstração. Segue do resultado análogo para grupos abelianos, notando que $\bar{\varphi}$ satisfaz:

$$\bar{\varphi}(a\pi(\mathbf{v})) = \bar{\varphi}(\pi(a\mathbf{v})) = \varphi(a\mathbf{v}) = a\varphi(\mathbf{v}) = a\bar{\varphi}(\pi(\mathbf{v}))\ . \qquad \square$$

Observação 2.9. Tal como no caso dos homomorfismos de grupos abelianos, um morfismo φ de módulos-A é injectivo *sse* $\ker \varphi = \{0\}$.

Teorema 2.10 (Teoremas de Isomorfismo)**.** *Sejam M, N módulos-A. Então,*

(a) dado $\varphi \in \mathrm{Hom}_A(M,N)$, tem-se

$$M/\ker\varphi \cong \mathrm{im}\,\varphi;$$

(b) se $N_1, N_2 \subset M$ são submódulos-A, então N_1+N_2, $N_1 \cap N_2$ são submódulos de M e tem-se

$$\frac{N_1+N_2}{N_2} \cong \frac{N_1}{N_1\cap N_2};$$

(c) se $N_2 \subset N_1$ são submódulos-A de M, tem-se

$$\frac{M/N_2}{N_1/N_2} \cong \frac{M}{N_1}.$$

(d) Mais, a correspondência

$$P \mapsto P/N_1$$

estabelece uma bijecção entre os submódulos de M contendo N_1 e os submódulos de M/N_1.

Demonstração. Todos os homomorfismos de grupos utilizados na demonstração do resultado análogo para grupos são homomorfismos de módulos. □

Observação 2.11. Seja M um módulo-A seja $\{N_i\}_{i\in I}$ uma família de submódulos, então $\cap_{i\in I} N_i \subset M$ é um submódulo-A.

Definição 2.12. *Seja M um módulo-A e seja $S \subset M$. Define-se o* submódulo gerado por S *como o submódulo de M dado por*

$$\langle S\rangle \coloneqq \bigcap_{\substack{N\subset M \text{ é submódulo}\\ N\supset S}} N.$$

Assim, $\langle S\rangle$ é o menor submódulo de M que contém S.

Notação 2.13. $\langle \mathbf{v}_1,\dots,\mathbf{v}_n\rangle \coloneqq \langle\{\mathbf{v}_1,\dots,\mathbf{v}_n\}\rangle$.

Exemplo 2.14. Seja M um módulo-A e sejam $\mathbf{v}_1,\dots,\mathbf{v}_n \in M$. Então

$$\langle \mathbf{v}_1,\dots,\mathbf{v}_n\rangle = \left\{ \sum_{i=1}^{n} a_i\mathbf{v}_i \mid a_i \in A \right\}.$$

Definição 2.15. *Um módulo-A que é gerado por um elemento diz-se um módulo* cíclico*.*

Exemplo 2.16. Seja $I \subset A$ um ideal esquerdo e seja $\pi\colon A \to A/I$ a projecção canónica. Então A/I é cíclico, pois $A/I = \langle 1_{A/I}\rangle$.

Exemplo 2.17. Seja M um módulo-A, seja $\{N_i\}_{i\in I}$ uma família de submódulos e seja $S = \cup_{i\in I} N_i$. Então

$$\langle S\rangle = \Big\{ \sum_{j\in J} \mathbf{v}_j \mid J \subset I : |J| < \infty, \mathbf{v}_j \in N_j \Big\}.$$

Exercícios

4.2.1. Na categoria Mod_A temos as noções de isomorfismo, epimorfismo e monomorfismo – ver Definições 1.14 e 1.16 do Capítulo 3. Dado $f \in \mathrm{Hom}_A(M,N)$, mostre que:

(a) f é um isomorfismo *sse* f é bijectivo;

(b) f é um monomorfismo *sse* f é injectivo;
Sugestão para ($\Rightarrow$): considere a inclusão $g\colon \ker f \to M$ e a aplicação nula para g'.

(c) f é um epimorfismo *sse* f é sobrejectivo.
Sugestão para ($\Rightarrow$): considere a projecção canónica $h\colon N \to N/\mathrm{im}\, f$ e a aplicação nula para h'.

4.2.2. Seja M um módulo-A cíclico. Mostre que existe um ideal esquerdo $I \subset A$ *t.q.* $M \cong A/I$.

4.2.3. Um módulo-A, $M \neq \{0\}$, diz-se *simples* se os únicos submódulos são $\{0\}$ e M. Prove as seguintes afirmações:
(a) Qualquer módulo simples é cíclico.
(b) Se M é simples, então qualquer endomorfismo[1] de M ou é nulo ou é um isomorfismo.

4.2.4. (a) Sejam M_i módulos-A, com $i \in \mathbb{N}$, tais que $M_i \subset M_{i+1}$, e seja $M = \cup_{i\in\mathbb{N}} M_i$. Mostre que M é um módulo-A.
(b) Dê um exemplo de uma anel A e módulos-A M_1 e M_2 tais que $M_1 \cup M_2$ não é um módulo.

4.2.5. Sejam M e N módulos-A. Mostre que:
(a) $\mathrm{Hom}_A(M,N)$ é um grupo abeliano para a soma $f+g$ definida por $(f+g)(\mathbf{v}) = f(\mathbf{v}) + g(\mathbf{v})\ \forall\, \mathbf{v} \in M$;
(b) $\mathrm{End}_A(M) \coloneqq \mathrm{Hom}_A(M,M)$ é um anel (com identidade) com o produto dado pela composição de funções;
(c) M é um módulo à esquerda sobre o anel dos endomorfismos[1] $\mathrm{End}_A(M)$, onde $f \cdot \mathbf{v} = f(\mathbf{v})$, para $\mathbf{v} \in M$ e $f \in \mathrm{End}_A(M)$.

4.2.6. Seja A um *d.i.p.*, M um módulo-A e $b \in A$. Seja

$$bM \coloneqq \{b\mathbf{v} \mid \mathbf{v} \in M\} \qquad \text{e} \qquad M[b] \coloneqq \{\mathbf{v} \in M \mid b\mathbf{v} = 0\}\ .$$

Se $p \in A$ é um elemento primo, mostre que
(a) $A/(p)$ é um corpo;
(b) pM e $M[p]$ são submódulos de M;
(c) M/pM é um espaço vectorial sobre $A/(p)$ com o seguinte produto de escalares

$$(a+(p))(\mathbf{v}+pM) = a\mathbf{v} + pM \qquad \forall\, a \in A, \mathbf{v} \in M\ ;$$

(d) $M[p]$ é um espaço vectorial sobre $A/(p)$ com o produto por escalares dado por

$$(a+(p))\mathbf{v} = a\mathbf{v} \qquad \forall\, a \in A, \mathbf{v} \in M\ .$$

[1] Tal como no caso dos grupos e anéis, um endomorfismo de um módulo M é um homomorfismo $f\colon M \to M$.

3. Produto directo e soma directa

Definição 3.1. *Seja $\{M_i\}_{i\in I}$ uma família de módulos-A. Define-se*

(a) o produto directo $\prod_{i\in I} M_i$ *como o produto directo de grupos abelianos munido da operação*

$$\forall\, a \in A, \forall\, (\mathbf{v}_i)_{i\in I} \in \prod_{i\in I} M_i \quad a(\mathbf{v}_i)_{i\in I} \coloneqq (a\mathbf{v}_i)_{i\in I}; \tag{3.1}$$

(b) a soma directa $\bigoplus_{i\in I} M_i$ *como a soma directa de grupos abelianos munida da operação* (3.1).

Tal como no caso dos grupos abelianos definem-se $\pi_k\colon \prod_{i\in I} M_i \to M_k$ *e* $\iota_k\colon M_k \to \bigoplus_{i\in I} M_i$ t.q. $\pi_k\left((\mathbf{v}_i)_{i\in I}\right) = \mathbf{v}_k$ *e*

$$\iota_k(\mathbf{v}) = (\mathbf{v}_i)_{i\in I}, \quad \mathbf{v}_i = \begin{cases} \mathbf{v} & i = k \\ 0, & i \neq k \end{cases}$$

Observação 3.2. Se $|I| < \infty$, então o produto e a soma directa coincidem.

Exemplos 3.3.

1. $\bigoplus_{i=1}^{n} A = \prod_{i=1}^{n} A = A^n$;
2. $\bigoplus_{i=1}^{\infty} A \cong A[x]$ como módulos-A;
3. $\prod_{i=1}^{\infty} A \cong A[[x]]$ como módulos-A.

Proposição 3.4. *O produto directo de módulos-A (munido das respectivas projecções) é um produto na categoria* Mod_A.

Demonstração. Como para grupos abelianos. □

Proposição 3.5. *A soma directa de módulos-A (equipada com as respectivas inclusões) é um coproduto na categoria* Mod_A.

Demonstração. Como para grupos abelianos. □

Corolário 3.6. *Produtos directos e somas directas de módulos são únicos a menos de isomorfismos e são descritos pelas respectivas propriedades universais.*

4. Soma directa interna e somandos directos

Definição 4.1. *Seja $\{N_i\}_{i\in I}$ uma família de submódulos de um módulo-A M. Se o homomorfismo induzido pelas inclusões $\iota_i\colon N_i \hookrightarrow M$*

$$\bigoplus_{i\in I} N_i \to M; (\mathbf{v}_i)_{i\in I} \mapsto \sum_{i\in I} \mathbf{v}_i$$

é um isomorfismo, diz-se que M é uma soma directa interna *dos submódulos $\{N_i\}_{i\in I}$ e escreve-se*

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

Proposição 4.2. *Seja $\{N_i\}_{i\in I}$ uma família de submódulos de M. Então $M = \bigoplus_{i\in I} N_i$* sse

(a) $M = \sum_{i\in I} N_i$;
(b) $\forall j \in I$, $N_j \cap \sum_{i\in I\setminus\{j\}} N_i = \{0\}$.

Demonstração. Seja $\varphi\colon \bigoplus_{i\in I} N_i \to M; (\mathbf{v}_i)_{i\in I} \mapsto \sum_{i\in I} \mathbf{v}_i$. Temos: φ é epi *sse* (a) se verifica; φ é mono *sse* (b) se verifica. De facto:

$$\ker\varphi \neq 0 \Leftrightarrow \exists\, i_1, \ldots, i_k \in I,\, \exists\, (\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k}) \in N_{i_1} \times \cdots \times N_{i_k} \setminus \{0\} \text{ t.q. } \mathbf{v}_{i_1} + \cdots + \mathbf{v}_{i_k} = 0,$$

e

$$\mathbf{v}_{i_1} + \cdots + \mathbf{v}_{i_k} = 0 \Leftrightarrow \underbrace{\mathbf{v}_{i_1}}_{\in N_{i_1}} = \underbrace{-(\mathbf{v}_{i_2} + \ldots + \mathbf{v}_{i_k})}_{\in N_{i_2}+\cdots+N_{i_k}}. \qquad \square$$

Definição 4.3. *Sejam M um módulo-A e N_1 um submódulo de M. Diz-se que N_1 é um* somando directo *de M se existe um submódulo $N_2 \subset M$* t.q.

$$M = N_1 \oplus N_2.$$

Nestas condições, diz-se que N_2 é um complemento *de N_1.*

Exemplos 4.4. Seja $A = \mathbb{Z}$ nos próximos dois exemplos.

1. Seja $M = \mathbb{Z}^2$ e $N_1 = \langle (1,1) \rangle \subset M$. Vejamos que N_1 é um somando directo de M: seja $N_2 = \langle (1,0) \rangle$, temos
   - $N_1 \cap N_2 = \{0\}$, pois $(a,a) = (b,0) \Leftrightarrow a = b = 0$;
   - $M = N_1 + N_2$, pois $(a,b) = (b,b) + (a-b,0)$.

   Pela Proposição 4.2, $M = N_1 \oplus N_2$ e portanto N_1 é um somando directo de M. Note que o complemento de N_1 não é único, por exemplo, $N_3 = \langle (0,1) \rangle$ também satisfaz $M = N_1 \oplus N_3$.
2. Seja $M = \mathbb{Z}$ e $N_1 = \langle 2 \rangle$. Vejamos que N_1 não é um somando directo de M. Se fosse, existiria $N_2 < M$ *t.q.* $\mathbb{Z} = N_1 \oplus N_2$ e portanto ter-se-ia
   $$\frac{M}{N_1} = \frac{N_1 + N_2}{N_1} \cong \frac{N_2}{N_1 \cap N_2} = N_2.$$
   No entanto,
   $$\frac{M}{N_1} = \frac{\mathbb{Z}}{\langle 2 \rangle} = \mathbb{Z}_2,$$
   e não podemos ter $\mathbb{Z}_2 \cong N_2 \subset M$, pois os elementos não nulos de M têm ordem infinita.

Definição 4.5. *Sejam M_n módulos-A e sejam $f_n \in \mathrm{Hom}_A(M_n, M_{n+1})$. Diz-se que a sucessão*

$$\cdots \longrightarrow M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots$$

é exacta *em M_n se* $\ker f_n = \mathrm{im}\, f_{n-1}$ *(em particular, temos $f_n \circ f_{n-1} = 0$). Se a sucessão é exacta em M_n, para todo o n, diz-se que a sucessão é* exacta.

Exemplo 4.6. Sejam $i\colon N \hookrightarrow M$ a inclusão de um submódulo e $\pi\colon M \to M/N$ a projecção canónica. A sucessão

$$0 \to N \xrightarrow{i} M \xrightarrow{\pi} M/N \to 0$$

é:

1. exacta em N *sse* i é mono;
2. exacta em M/N *sse* π é epi;
3. exacta em M *sse* $\ker \pi = \mathrm{im}\, i \cong N$.

Exemplo 4.7. A sucessão

$$0 \to \mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_m \to 0$$

é exacta onde $\times m$ denota o homomorfismo $\mathbb{Z} \to \mathbb{Z}; k \mapsto km$.

Notação 4.8. Uma sucessão exacta da forma

$$0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$$

diz-se uma sucessão *curta exacta*.

Definição 4.9. *Diz-se que a sucessão curta exacta de módulos-A*

$$0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$$

se cinde *se* $\mathrm{im}\, f_1$ *é um somando directo de M_2.*

Observação 4.10. Se a sucessão se cinde, seja $N \subset M_2$ um complemento de $\operatorname{im} f_1$, i.e., $M_2 = \operatorname{im} f \oplus N$. Temos

$$N \cong \frac{M_2}{\operatorname{im} f_1} = \frac{M_2}{\ker f_2} \xrightarrow[\cong]{f_2} M_3,$$

logo

$$\boxed{M_2 \cong M_1 \oplus M_3}$$

Exemplo 4.11. Sejam M_1, M_2 módulos-A. A sucessão

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

cinde-se, pois $\iota_2(M_2) \subset M_1 \oplus M_2$ é um complemento de $\iota_1(M_1)$ e portanto $\iota_1(M_1)$ é um somando directo de $M_1 \oplus M_2$.

Definição 4.12. *Um isomorfismo entre duas sucessões curtas exactas* $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ *e* $0 \to N_1 \xrightarrow{g_1} N_2 \xrightarrow{g_2} N_3 \to 0$ *é um triplo de isomorfismos* $\alpha_1 \colon M_1 \to N_1$, $\alpha_2 \colon M_2 \to N_2$ *e* $\alpha_3 \colon M_3 \to N_3$ t.q. *o diagrama*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \longrightarrow & 0 \end{array}$$

comuta.

Proposição 4.13. *Seja* $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ *uma sucessão exacta de módulos-A. ASCSE:*

(a) A sucessão cinde-se;

(b) $\exists\, r \in \operatorname{Hom}_A(M_3, M_2)$ t.q. $f_2 \circ r = \mathrm{id}_{M_3}$*;*

(c) $\exists\, l \in \operatorname{Hom}_A(M_2, M_1)$ t.q. $l \circ f_1 = \mathrm{id}_{M_1}$.

Exemplo 4.14. Sejam M_1, M_2 módulos-A. Então a sucessão

$$0 \longrightarrow M_1 \underset{l}{\overset{\iota_1}{\rightleftarrows}} M_1 \oplus M_2 \underset{r}{\overset{\pi_2}{\rightleftarrows}} M_2 \longrightarrow 0$$

cinde-se. Os homomorfismos r e l a que se refere a Proposição 4.13 são $r = \iota_2$ e $l = \pi_1$:

$$\begin{aligned} \pi_2 \circ r = \pi_2 \circ \iota_2 &= \mathrm{id}_{M_2} \\ l \circ \iota_1 = \pi_1 \circ \iota_1 &= \mathrm{id}_{M_1}. \end{aligned}$$

Observação 4.15. No exemplo anterior, os homomorfismos r e l da Proposição 4.13 são obtidos a partir de ι_1, π_2 e do complemento M_2 para $M_1 = \operatorname{im} \iota_1$ da seguinte forma:

$$\begin{aligned} r(\mathbf{v}_2) = \iota_2(\mathbf{v}_2) = (0, \mathbf{v}_2) &= (\pi_2|_{M_2})^{-1}(\mathbf{v}_2); \\ l\overbrace{(\mathbf{v}_1, \mathbf{v}_2)}^{\mathbf{v}} = \mathbf{v}_1 &= \iota_1^{-1}(\mathbf{v}_1, 0) \\ &= \iota_1^{-1}(\mathbf{v} - \iota_2(\pi_2(\mathbf{v}))) \\ &= \iota_1^{-1}(\mathbf{v} - r(\pi_2(\mathbf{v}))). \end{aligned}$$

Demonstração da Proposição 4.13.

$\boxed{(a) \Rightarrow (b)}$ Seja N um complemento de $\operatorname{im} f_1$. Defina-se $r \coloneqq (f_2|_N)^{-1}$. Note-se que r está bem definido, pois $N \cap \ker f_2 = \{0\}$ e

$$f_2 \circ r = f_2 \circ (f_2|_N)^{-1} = \mathrm{id}_{M_3}.$$

$\boxed{(b) \Rightarrow (c)}$ Seja r como em (b). Define-se $l\colon M_2 \to M_1$ pela fórmula

$$l(\mathbf{x}) \coloneqq f_1^{-1}(\mathbf{x} - r(f_2(\mathbf{x}))).$$

Temos:

- l está bem definida:
$$f_2(\mathbf{x} - r(f_2(\mathbf{x}))) = f_2(\mathbf{x}) - f_2(\mathbf{x}) = 0 \Rightarrow \mathbf{x} - r(f_2(\mathbf{x})) \in \operatorname{im} f_1.$$
- $l \circ f_1 = \mathrm{id}_{M_1}$:
$$l(f_1(\mathbf{x})) = f_1^{-1}(f_1(\mathbf{x}) - r(f_2(f_1(\mathbf{x})))) = f_1^{-1}(f_1(\mathbf{x})) = \mathbf{x}.$$

$\boxed{(c) \Rightarrow (a)}$ Seja l como no enunciado. Defina-se $N \coloneqq \ker l$. Temos

- $N \cap \operatorname{im} f_1 = \{0\}$, pois:
$$\begin{aligned} \mathbf{x} \in N \cap \operatorname{im} f_1 &\Leftrightarrow l(\mathbf{x}) = 0 \wedge \exists \mathbf{y} : \mathbf{x} = f_1(\mathbf{y}) \\ &\Rightarrow l(f_1(\mathbf{y})) = 0 \Leftrightarrow \mathbf{y} = 0 \\ &\Rightarrow \mathbf{x} = 0. \end{aligned}$$
- $M_2 = N + \operatorname{im} f_1$, pois:
$$\mathbf{x} = \underbrace{\mathbf{x} - f_1(l(\mathbf{x}))}_{\in \ker l} + \underbrace{f_1(l(\mathbf{x}))}_{\in \operatorname{im} f_1}.$$

Concluímos que $M_2 = N \oplus \operatorname{im} f_1$. □

Exercícios

4.4.1. Sejam M_i, para $i \in I$, e N módulos-A. Mostre que:
(a) $\mathrm{Hom}_A(\bigoplus_{i\in I} M_i, N) \cong \prod_{i\in I} \mathrm{Hom}_A(M_i, N)$;
(b) $\mathrm{Hom}_A(N, \prod_{i\in I} M_i) \cong \prod_{i\in I} \mathrm{Hom}_A(N, M_i)$;
(c) $\mathrm{Hom}_A(N, \bigoplus_{i\in I} M_i) \subset \prod_{i\in I} \mathrm{Hom}_A(N, M_i)$;
(d) A inclusão na alínea anterior pode não ser uma igualdade.

4.4.2. Seja $f\colon M \to M$ um homomorfismo de módulos-A tal que $f \circ f = f$. Mostre que $M = \ker f \oplus \operatorname{im} f$.

4.4.3. Mostre que uma sucessão curta exacta de módulos-A, $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ cinde-se *sse* é isomorfa a
$$0 \to M_1 \xrightarrow{\iota_1} M_1 \oplus M_3 \xrightarrow{\pi_2} M_3 \to 0.$$

4.4.4. (Lema dos Cinco.) Considere o seguinte diagrama comutativo de módulos-A
$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \downarrow{\scriptstyle h_3} & & \downarrow{\scriptstyle h_4} & & \downarrow{\scriptstyle h_5} \\ N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \xrightarrow{g_3} & N_4 & \xrightarrow{g_4} & N_5 \end{array}$$
onde as linhas são sucessões exactas. Mostre que:
(a) se h_1 é sobrejectivo e h_2, h_4 são injectivos, então h_3 é injectivo;
(b) se h_5 é injectivo e h_2, h_4 são sobrejectivos, então h_3 é sobrejectivo;
(c) se h_1, h_2, h_4, h_5 são isomorfismos, então h_3 também é um isomorfismo.

4.4.5. (a) Dadas duas sucessões curtas exactas de módulos-A
$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0 \quad \text{e} \quad 0 \longrightarrow M_3 \xrightarrow{f_3} M_4 \xrightarrow{f_4} M_5 \longrightarrow 0 \ ,$$

mostre que

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_3 \circ f_2} M_4 \xrightarrow{f_4} M_5 \xrightarrow{f_5} 0$$

é uma sucessão exacta.

(b) Mostre que qualquer sucessão exacta de módulos-A pode ser obtida combinando sucessões curtas exactas como em (a).

4.4.6. Define-se sucessão exacta na categoria dos grupos de maneira análoga ao que se definiu para módulos, ou seja, na Definição 4.5 consideramos grupos e homomorfismos de grupos. Dada a seguinte sucessão curta exacta de grupos

$$\{\mathbf{1}\} \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow \{\mathbf{1}\} \ ,$$

mostre que as seguintes afirmações são equivalentes:

(a) $G = N' \rtimes H' \cong N \rtimes H$, onde $N' = \operatorname{im} \alpha$, para algum subgrupo $H' < G$ (ver Exercício 1.8.5);

(b) Existe um homomorfismo de grupos $r \colon H \to G$ tal que $\beta \circ r = \mathrm{id}_H$;

(c) Existe um homomorfismo de grupos $l \colon G \to N$ tal que $l \circ \alpha = \mathrm{id}_N$.

Em particular, caso alguma destas (logo todas) condições se verifique, o grupo G não é necessariamente isomorfo à soma directa $N \oplus H$, como acontece na categoria dos módulos-A – compare com a Proposição 4.13.

5. Módulos livres

Definição 5.1. *Seja M um módulo-A. Diz-se que $S \subset M$ é* linearmente independente (*l.i.*) *se para todos $\mathbf{v}_1, \ldots, \mathbf{v}_n \in S$, distintos, se tem*

$$\forall\, a_1, \ldots, a_n \in A \quad \sum_{i=1}^{n} a_i \mathbf{v}_i = 0 \Rightarrow a_1 = a_2 = \cdots = a_n = 0.$$

Caso contrário, S diz-se linearmente dependente.

Exemplo 5.2. Se M é um espaço vectorial-k, a noção de independência linear aqui definida coincide com a habitual.

Definição 5.3. *Seja M um módulo-A.*

- *Um subconjunto $S \subset M$ diz-se um* conjunto gerador *de M se $\langle S \rangle = M$.*
- *Se M tem um subconjunto gerador finito, diz-se que M é* finitamente gerado *ou que M é de* tipo finito.
- *Diz-se que $S \subset M$ é uma* base *se S é* l.i., *e $M = \langle S \rangle$.*
- *Se M tem uma base, diz-se que M é um* módulo livre.

Exemplos 5.4.

1. Seja k um corpo. Então os módulos-k (espaços vectoriais-k) são todos livres. Mais à frente revemos alguns resultados básicos de álgebra linear que generalizamos para o caso dos espaços vectoriais sobre anéis de divisão.
2. $\mathbb{Z}^n$ é um módulo livre com base $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, onde $\mathbf{e}_i$ denota o i-ésimo elemento da base canónica: $\mathbf{e}_i \coloneqq (\delta_{ki})_{k=1,\ldots,n} \in \mathbb{Z}^n$.
3. Um anel A é um módulo-A livre com base $\{1\}$.
4. Seja $I \subset A$ um ideal esquerdo. Então o módulo-A A/I é gerado por $1 + I$, mas $\{1+\mathrm{I}\}$ não é uma base: $a \in I \Rightarrow a(1 + I) = 0 \Rightarrow \{1 + I\}$ não é *l.i.* se $I \neq \{0\}$. Na realidade, este módulo não é livre – Exercício 4.5.1.
5. Seja X um conjunto. Denotamos por $F(X)$ o módulo-A livre gerado por X:

$$F(X) \coloneqq \left\{ f \colon X \to A \mid |f^{-1}(A \setminus \{0\})| < \infty \right\}.$$

   As operações de adição e multiplicação por escalares em $F(X)$ são definidas ponto a ponto, usando as operações existentes em A: $(f_1 + f_2)(x) \coloneqq f_1(x) + f_2(x)$, $(a \cdot f_1)(x) \coloneqq a \cdot (f_1(x))$.
   Exercício: Justifique que $f_1 + f_2 \in F(X)$ e $a \cdot f_1 \in F(X)$.
   Para cada $x \in X$, definimos

$$\mathbf{e}_x \in F(X) \quad t.q. \quad \mathbf{e}_x(y) = \begin{cases} 1_A, & x = y \\ 0_A, & x \neq y \end{cases}.$$

   Então $\{\mathbf{e}_x \mid x \in X\}$ é uma base de $F(X)$ (justifique!) e portanto $F(X)$ é livre.

Notação 5.5. Se for necessário enfatizar o anel de escalares A, denotamos $F(X)$ por $F_A(X)$. Dizemos que $\{\mathbf{e}_x \mid x \in X\}$ é a *base canónica* de $F(X)$.

Proposição 5.6. *Seja M um módulo-A livre e seja $B \subset M$ uma base. Se M' é outro módulo-A e $\varphi \colon M \to M'$ é um isomorfismo, então $\varphi(B)$ é uma base de M'.*

Proposição 5.7. *Seja $M \in \mathrm{Mod}_A$ livre com base $\{\mathbf{v}\}$. Então $M \cong A$.*

Seja $(\mathcal{C}, \sigma \colon \mathcal{C} \to \mathrm{Set})$ uma categoria concreta. Dados $X, Y \in \mathcal{C}$, simplificamos notação identificando $\sigma X, \sigma Y$ com X, Y e $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ como um subconjunto de $\mathrm{Hom}_{\mathrm{Set}}(X, Y)$.

Definição 5.8. *Seja $\mathcal{C}$ uma categoria concreta. Sejam $F \in \mathcal{C}$, $X \in \mathrm{Set}$ e $i \colon X \to F$ uma função em* Set. *Diz-se que F é* livremente gerado por (X, i) *se*

$$\forall\, C \in \mathcal{C}\, \forall\, f \in \mathrm{Hom}_{\mathrm{Set}}(X, C)\ \exists!\, \bar{f} \in \mathrm{Hom}_{\mathcal{C}}(F, C) : \bar{f} \circ i = f \in \mathrm{Hom}_{\mathrm{Set}}(X, C).$$

Exercícios

4.5.1. Mostre que, se $I \neq \{0\}$ é um ideal bilateral do anel A, então A/I não é livre como módulo-A.

4.5.2. (a) Seja A um anel comutativo, portanto A é um módulo-A livre e qualquer ideal I é um submódulo de A. Mostre que se o ideal $I \neq \{0\}$ é um módulo livre então I é principal.
Sugestão: Mostre que qualquer subconjunto de I com pelo menos dois elementos é linearmente dependente.

(b) Dê um exemplo de um anel comutativo A e de um ideal principal $I \neq \{0\}$ de A tais que I não é um módulo-A livre.

4.5.3. Mostre que, se $A \neq \{0\}$ é um anel comutativo tal que qualquer submódulo de um módulo-A livre é livre, então A é um *d.i.p.*.

4.5.4. Demonstre a Proposição 5.6.

4.5.5. Demonstre a Proposição 5.7.

4.5.6. Seja B um anel e seja F um módulo-B livre com uma base numerável $\{\mathbf{e}_i \mid i \in \mathbb{N}\}$. Considere o anel $A = \mathrm{End}_B(F)$ – ver Exercício 4.2.5.

(a) Sejam $f_1, f_2 \colon F \to F$ definidas por

$$\begin{cases} f_1(\mathbf{e}_{2i-1}) = \mathbf{e}_i \\ f_1(\mathbf{e}_{2i}) = 0 \end{cases} \quad \text{e} \quad \begin{cases} f_2(\mathbf{e}_{2i-1}) = 0 \\ f_2(\mathbf{e}_{2i}) = \mathbf{e}_i \ . \end{cases}$$

Mostre que $\{f_1, f_2\}$ é uma base de A e conclua que $A \cong A^2$ como módulos-A.

(b) Conclua que $A \cong A^n$, para qualquer $n \in \mathbb{N}$.

4.5.7. Seja M um módulo-A e seja X um conjunto. Então $M \cong F(X)$ *sse* existe uma função $i \colon X \to M$ *t.q.* M é um objecto livre gerado por (X, i) em Mod_A.

6. Caracterização dos módulos livres; espaços vectoriais

Lema 6.1. *Seja M um módulo-A. Então existe um módulo-A livre F e um epimorfismo de módulos-A $h\colon F \to M$.*

Demonstração. Seja $X \subset M$ *t.q.* $M = \langle X\rangle$ (*e.g.*, $X = M$). Seja $F = F(X)$ e seja $h\colon F \to M$ determinado pela inclusão $i\colon X \hookrightarrow M$. □

Proposição 6.2. *Seja M um módulo-A. ASCSE*

(a) M é livre;

(b) existem submódulos $N_i \subset M$, $i \in I$, t.q. *$N_i \cong A$ e $M = \bigoplus_{i\in I} N_i$;*

(c) $M \cong F(X)$ para algum conjunto X.

Demonstração. $\boxed{(a)\Rightarrow(b)}$ Seja $B = \{\mathbf{v}_i \mid i \in I\}$ uma base e seja $N_i = \langle \mathbf{v}_i\rangle$. Por definição de base, $M = \bigoplus_{i\in I} N_i$, e $N_i \cong A$ pela Proposição 5.7.

$\boxed{(b)\Rightarrow(a)}$ Como $N_i \cong A$ e $\{1_A\}$ é uma base de A, existe $\mathbf{v}_i$ *t.q.* $N_i = \langle \mathbf{v}_i\rangle$ (ver Proposição 5.6). Então $\{\mathbf{v}_i \mid i \in I\}$ é uma base de M .

$\boxed{(a)\Rightarrow(c)}$ Se $B = \{\mathbf{v}_i \mid i \in I\}$ é uma base de M, então $F(I) \cong M$ (o isomorfismo $\bar{f}\colon F(I) \to M$ é induzido pela função $f\colon I \to M; i \mapsto \mathbf{v}_i$).

$\boxed{(c)\Rightarrow(a)}$ Seja $\varphi\colon F(X) \to M$ um isomorfismo. Como o conjunto $\{\mathbf{e}_x \mid x \in X\}$ é uma base de $F(X)$, então $\varphi(\{\mathbf{e}_x \mid x \in X\})$ é uma base de M (ver Proposição 5.6). □

Observação 6.3. 1. Combinando a equivalência (a)⇔(c) da proposição anterior com o Exercício 4.5.7, obtém-se que M é um módulo-A livre *sse* M é um objecto livre na categoria Mod_A.

2. Em particular, pondo $A = \mathbb{Z}$ definimos *grupo abeliano livre* como sendo um objecto livre na categoria $\mathrm{Ab} \cong \mathrm{Mod}_{\mathbb{Z}}$. A proposição anterior diz-nos que G é um grupo abeliano livre *sse* $G \cong \oplus_{i\in I}\mathbb{Z}$.

Teorema 6.4. *Seja V um espaço vectorial sobre um anel de divisão D. Então V tem uma base e portanto é livre.*

Demonstração. Demonstramos que um subconjunto de V que seja maximal entre os subconjuntos *l.i.* é uma base.

Seja $\mathbf{v} \in V \setminus \{0\}$, então $\forall a \in D^\times$, $a\mathbf{v} \neq 0$. Portanto $\{\mathbf{v}\}$ é *l.i.*.

Seja $\mathcal{L} \coloneqq \{S \subset V \mid S \text{ é } l.i.\}$. Temos $\mathcal{L} \neq \varnothing$ e $\mathcal{L}$ é parcialmente ordenado pela relação de inclusão. Seja S_i, $i \in I$, uma cadeia em $\mathcal{L}$. Então $S = \cup_{i\in I} S_i$ é *l.i.*: se $\mathbf{v}_1, \ldots, \mathbf{v}_n \in S$, então existe $i \in I$ *t.q.* $\mathbf{v}_1, \ldots, \mathbf{v}_n \in S_i$. Como S_i é *l.i.*,

$$a_1\mathbf{v}_1 + \ldots + a_n\mathbf{v}_n = 0 \Rightarrow a_1 = \cdots = a_n = 0.$$

Portanto, a cadeia $\{S_i\}_{i\in I}$ é majorada. Pelo Lema de Zorn, $\mathcal{L}$ tem um elemento maximal S.

Suponhamos que existe $\mathbf{v} \in V \setminus \langle S\rangle$. Por maximalidade de S, existem

$$\mathbf{v}_1, \ldots, \mathbf{v}_n \in S, \qquad a, a_1, \ldots, a_n \in D \text{ não todos nulos.}$$

t.q. $a\mathbf{v} + a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = 0$. Mas, então $a \neq 0$ (caso contrário $a_1 = \cdots = a_n = 0$ por independência linear de S) e

$$\mathbf{v} = -a^{-1}a_1\mathbf{v}_1 - \cdots - a^{-1}a_n\mathbf{v}_n,$$

o que contraria a hipótese $\mathbf{v} \notin \langle S\rangle$. Concluímos que $\langle S\rangle = V$ e portanto S é uma base de V. □

Corolário 6.5. *Seja V um espaço vectorial sobre um anel de divisão D. Seja $S \subset V$ um conjunto* l.i. *maximal. Então S é uma base de V. Mais geralmente, se $S' \subset V$ é um conjunto* l.i.*, então existe $S \subset V$* t.q. *$S' \subset S$ e S é uma base de V.*

Em particular, a última afirmação deste corolário é equivalente a dizer que se pode completar qualquer conjunto linearmente independente para se obter uma base de V.

7. Anéis de matrizes

Sejam $U_1, \ldots, U_n$ módulos-A e seja $M = U_1 \oplus \cdots \oplus U_n$. Queremos estudar o anel $\mathrm{End}_A(M)$.

Recordem-se as projecções $\pi_i \colon M \to U_i$ e as inclusões $\iota_i \colon U_i \hookrightarrow M$. Temos,

$$\boxed{\sum_{i=1}^{n} \iota_i \circ \pi_i = \mathrm{id}_M,} \qquad \boxed{\pi_i \circ \iota_j = \delta_{ij}\, \mathrm{id}_{U_j}\,.}$$

Exemplo 7.1 (Caso $n = 2$)**.** Temos,

$$\begin{aligned}(\iota_1 \circ \pi_1 + \iota_2 \circ \pi_2)\,(x,y) &= \iota_1 \circ \pi_1(x,y) + \iota_2 \circ \pi_2(x,y) = (x,0) + (0,y) = (x,y);\\ \pi_1 \circ \iota_1(x) &= \pi_1(x,0) = x;\\ \pi_1 \circ \iota_2(y) &= \pi_1(0,y) = 0.\end{aligned}$$

Seja $f \in \mathrm{End}_A(M) = \mathrm{End}_A(U_1 \oplus U_2)$. Definimos

$$\begin{aligned}f_{11} &= \pi_1 \circ f \circ \iota_1 \in \mathrm{Hom}_A(U_1, U_1)\\ f_{12} &= \pi_1 \circ f \circ \iota_2 \in \mathrm{Hom}_A(U_2, U_1)\\ f_{21} &= \pi_2 \circ f \circ \iota_1 \in \mathrm{Hom}_A(U_1, U_2)\\ f_{22} &= \pi_2 \circ f \circ \iota_2 \in \mathrm{Hom}_A(U_2, U_2).\end{aligned}$$

Obtemos assim 4 homomorfismos que podemos escrever na forma matricial:

$$\begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix}, \qquad f_{ij} \in \mathrm{Hom}_A(U_j, U_i).$$

Reciprocamente, dada uma matriz de homomorfismos $\left[\begin{smallmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{smallmatrix}\right]$ tal que $\alpha_{ij} \colon U_j \to U_i$, definimos $\alpha \in \mathrm{End}_A(M)$ por

$$\alpha = \sum_{i,j=1}^{2} \iota_i \circ \alpha_{ij} \circ \pi_j \colon M \to M.$$

Obtemos assim correspondências inversas, pois temos:

$$\begin{aligned}f \mapsto [\pi_i \circ f \circ \iota_j]_{i,j} \mapsto \sum_{i,j} \iota_i \circ \pi_i \circ f \circ \iota_j \circ \pi_j &= \sum_{j=1}^{2} \Big(\sum_{i=1}^{2} (\iota_i \circ \pi_i) \Big) \circ f \circ (\iota_j \circ \pi_j)\\ = \sum_{j=1}^{2} \mathrm{id}_M \circ f \circ (\iota_j \circ \pi_j) = \mathrm{id}_M \circ f \circ \Big(\sum_{j=1}^{2} \iota_j \circ \pi_j \Big) &= \mathrm{id}_M \circ f \circ \mathrm{id}_M = f\ .\end{aligned}$$

e

$$\begin{aligned}[\alpha_{ij}]_{i,j} \mapsto \sum_{r,s} \iota_r \circ \alpha_{rs} \circ \pi_s \mapsto \Big[\pi_i \circ \Big(\sum_{r,s} \iota_r \circ \alpha_{rs} \circ \pi_s \Big) \circ \iota_j \Big]_{i,j}&\\ = \Big[\sum_{r,s} (\pi_i \circ \iota_r) \circ \alpha_{rs} \circ (\pi_s \circ \iota_j) \Big]_{i,j} = \big[\mathrm{id}_{M_i} \circ \alpha_{ij} \circ \mathrm{id}_{M_j}\big]_{i,j} &= [\alpha_{ij}]_{i,j}\ .\end{aligned}$$

A composta

$$(f\circ g)_{ij}=\pi_i\circ f\circ g\circ\iota_j=\pi_i\circ f\circ\Big(\sum_{k=1}^{2}\iota_k\circ\pi_k\Big)\circ g\circ\iota_j$$
$$=\sum_k(\pi_i\circ f\circ\iota_k)\circ(\pi_k\circ g\circ\iota_j)=\sum_k f_{ik}\circ g_{kj}$$

corresponde ao produto de matrizes de homomorfismos:

$$\begin{bmatrix}f_{11}&f_{12}\\f_{21}&f_{22}\end{bmatrix}\cdot\begin{bmatrix}g_{11}&g_{12}\\g_{21}&g_{22}\end{bmatrix}\coloneqq\begin{bmatrix}f_{11}\circ g_{11}+f_{12}\circ g_{21}&f_{11}\circ g_{12}+f_{12}\circ g_{22}\\f_{21}\circ g_{11}+f_{22}\circ g_{21}&f_{21}\circ g_{12}+f_{22}\circ g_{22}\end{bmatrix}.\tag{7.1}$$

Teorema 7.2. *Seja $M=U_1\oplus\cdots\oplus U_n$, então as correspondências*

$$f\mapsto\big[f_{ij}\big];\quad f_{ij}=\pi_i\circ f\circ\iota_j,$$

e

$$\big[f_{ij}\big]\mapsto\alpha=\sum_{i,j}\iota_i\circ\alpha_{ij}\circ\pi_j,$$

estabelecem um isomorfismo de anéis entre $\mathrm{End}_A(M)$ *e o anel de matrizes $n\times n$, com entradas $\alpha_{ij}\in\mathrm{Hom}_A(U_j,U_i)$, munido do produto descrito em* (7.1)*, no caso $n=2$.*

Demonstração. Como no caso $n=2$. □

Corolário 7.3. *Seja U um módulo-A. Então, existe um isomorfismo de anéis*

$$\mathrm{End}_A(U^n)\cong M_n(\mathrm{End}_A(U)).$$

Exemplo 7.4. Consideremos o caso $U=A$, visto como um módulo-A à esquerda e seja $f\in\mathrm{End}_A(A)$. Seja $b=f(1_A)$. Temos

$$\forall a\in A,\quad f(a)=af(1_A)=ab.$$

Se $g\in\mathrm{End}_A(A)$ e $c=g(1_A)$, temos

$$(f\circ g)(1_A)=f(g(1_A))=f(c)=cf(1_A)=cb.$$

Portanto, $\mathrm{End}_A(A)\cong A^{op}$, onde A^{op} denota o anel $(A,+,\star)$ com a mesma soma de A e produto dado por

$$\boxed{b\star c\coloneqq cb.}$$

Corolário 7.5. *Seja A um anel. Então, existe um isomorfismo de anéis*

$$\boxed{\mathrm{End}_A\left(A^n\right)\cong M_n\left(A^{op}\right).}$$

Exemplos 7.6.

1. Dado $f\in\mathrm{End}_A(A^n)$ a correspondência do Teorema 7.2 é $f\mapsto\big[f_{ij}\big]$ *t.q.* f_{ij} é a i-ésima componente de $f(\mathbf{e}_j)$, (e o elemento $\mathbf{e}_i$ é o i-ésimo elemento da base canónica de A^n: $\mathbf{e}_i=(\delta_{ij}\cdot 1_A)_{j=1,\dots,n}$). Se $g\in\mathrm{End}_A(A^n)$ é representado pela matriz $\big[g_{ij}\big]$, temos $f\circ g=\big[h_{ij}\big]$ com
$$h_{ij}=\sum_k f_{ik}\star g_{kj}=\sum_k g_{kj}f_{ik}.$$
2. Mais geralmente, $\mathrm{Hom}_A(A^m,A^n)$ é um grupo abeliano cujos elementos podem ser representados matrizes da $n\times m$ seguinte maneira $f\mapsto\big[f_{ij}\big]$, com
$$f_{ij}=(\pi_i\circ f\circ\iota_j)\ (1_A)\in A.$$
Com esta representação , se $g\in\mathrm{Hom}_A(A^p,A^m)$ então a composta $h=f\circ g\in\mathrm{Hom}_A(A^p,A^n)$ é representada pela matriz $\big[h_{ij}\big]$ dada por
$$h_{ij}=\sum_k f_{ik}\star g_{kj}=\sum_k g_{kj}f_{ik}.\tag{7.2}$$

Ou seja,

$$\boxed{\mathrm{Hom}_A(A^m, A^n) \cong M_{n\times m}(A^{op})}$$

e, através deste isomorfismo, o produto de matrizes

$$M_{n\times m}(A^{op}) \times M_{m\times p}(A^{op}) \to M_{n\times p}(A^{op}),$$

descrito em (7.2), corresponde à composição

$$\mathrm{Hom}_A(A^m, A^n) \times \mathrm{Hom}_A(A^p, A^m) \to \mathrm{Hom}_A(A^p, A^n).$$

3. Se A é um anel comutativo, então $A \cong A^{op}$ e portanto,

$$\boxed{\mathrm{Hom}_A(A^m, A^n) \cong M_{n\times m}(A).}$$

8. Invariância dimensional

Definição 8.1. *Diz-se que um anel A tem a* propriedade da invariância dimensional (*p.i.d.*) *se para todo o módulo-A livre, M, todas as bases de M têm a mesma cardinalidade.*

Se A tem a p.i.d. *e M é um módulo-A livre chama-se* dimensão de M *à cardinalidade de uma sua base e denota-se* $\dim_A M$.

Exemplo 8.2. Os corpos têm a *p.i.d.*. De seguida veremos que os anéis de divisão também têm a *p.i.d.*.

Exemplo 8.3. Se F é um módulo-A livre com uma base numerável, o anel $\mathrm{End}_A(F)$ não tem a *p.i.d.*– ver Exercício 4.5.6.

Proposição 8.4. *Se A tem a* p.i.d. *e M, N são módulos livres sobre A, tem-se $M \cong N$* sse $\dim_A M = \dim_A N$.

Demonstração. $\boxed{\Rightarrow}$ Se $f\colon M \to N$ é um isomorfismo e $S \subset M$ é uma base, então $f(S)$ é uma base de N, pela Proposição 5.6, logo $\dim_A M = \dim_A N$.

$\boxed{\Leftarrow}$ Como M, N são módulos livres então são objectos livres em Mod_A gerados pelas inclusões $i\colon \mathcal{B}_M \to M$ e $j\colon \mathcal{B}_N \to N$, onde $\mathcal{B}_M$ e $\mathcal{B}_N$ são bases de M e N, respectivamente. Como $\dim_A M = \dim_A N$, existe uma bijecção $k : \mathcal{B}_M \to \mathcal{B}_N$. Pela definição de objecto livre aplicada a M e à função $j \circ k\colon \mathcal{B}_M \to N$, existe um único homorfismo $f\colon M \to N$ tal que $f \circ i = j \circ k$. Fazendo o mesmo a N e à função $i \circ k^{-1} : \mathcal{B}_N \to M$, obtemos um único homomorfismo $g\colon N \to M$ tal que $g \circ j = i \circ k^{-1}$. Portanto

$$f \circ (g \circ j) = f \circ i \circ k^{-1} = (j \circ k) \circ k^{-1} = j \ ,$$

ou seja, $(f \circ g)|_{\mathcal{B}_N} = \mathrm{id}_{\mathcal{B}_N}$, donde se conclui que $f \circ g = \mathrm{id}_N$ pois $\mathcal{B}_N$ é um conjunto gerador de N. Analogamente também se verifica que $g \circ f = \mathrm{id}_M$, logo $M \cong N$. □

Exemplo 8.5. Dois espaços vectoriais sobre um anel de divisão são isomorfos *sse* têm a mesma dimensão.

Proposição 8.6. *Seja A um anel. Seja $M \in \mathrm{Mod}_A$* t.q. *M tem uma base infinita. Então todas as bases de M têm a mesma cardinalidade.*

Demonstração. Seja $M \in \mathrm{Mod}_A$ livre com base $\{\mathbf{v}_i\}_{i\in I}$ *t.q.* I é infinito. Seja $\{\mathbf{w}_j\}_{j\in J}$ outra base. Então

$$\forall_{j\in J}\, \exists_{I_j \subset I} : |I_j| < \infty \wedge \mathbf{w}_j \in \langle\{\mathbf{v}_i \mid i \in I_j\}\rangle.$$

Vejamos que $I = \cup_{j\in J} I_j$. De facto,

$$i \notin \cup_{j\in J} I_j \Rightarrow \mathbf{v}_i \in \langle\{\mathbf{v}_s \mid s \in I \setminus \{i\}\}\rangle,$$

pois $\langle\{\mathbf{w}_j \mid j \in J\}\rangle = M$. Obtemos assim uma contradição, pois $\{\mathbf{v}_i\}_{i\in I}$ é *l.i.*, logo $I = \cup_{j\in J} I_j$.

Em particular, J é infinito, pois $|I_j| < \infty$, $\forall j \in J$. Da igualdade $I = \cup_{j\in J} I_j$ vem também

$$|I| = |\cup_{j\in J} I_j| \leq |J \times \mathbb{N}| = |J|,$$

pois J é infinito. E, uma vez que J é infinito, trocando os papéis de I e J, obtém-se também que $|J| \leq |I|$. □

Teorema 8.7. *As bases de um espaço vectorial sobre um anel de divisão têm todas a mesma cardinalidade.*

Demonstração. Sejam S, S' bases de um espaço vectorial V sobre um anel de divisão D. Se S ou S' são infinitos, então o resultado segue da Proposição 8.6. Suponhamos que $S = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ e $S' = \{\mathbf{y}_1, \ldots, \mathbf{y}_m\}$, com $n \leq m$. Temos

$$\mathbf{y}_1 = a_1\mathbf{x}_1 + \cdots + a_n\mathbf{x}_n, \qquad a_i \in D.$$

Seja i_1 *t.q.* $a_{i_1} \neq 0$ (existe tal i_1 pois $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ é *l.i.* e $\mathbf{y}_1 \neq 0$), então

$$\mathbf{x}_{i_1} = a_{i_1}^{-1}\Big(\mathbf{y}_1 - \sum_{i \neq i_1} a_i\mathbf{x}_i\Big),$$

logo o conjunto $\{\mathbf{y}_1\} \cup \{\mathbf{x}_i \mid i \neq i_1\}$ gera V. Temos

$$\mathbf{y}_2 = \sum_{i \neq i_1} b_i\mathbf{x}_i + c_1\mathbf{y}_1.$$

Seja i_2 *t.q.* $b_{i_2} \neq 0$, então

$$\mathbf{x}_{i_2} = b_{i_2}^{-1}\Big(\mathbf{y}_2 - c_1\mathbf{y}_1 - \sum_{i \neq i_1, i_2} b_i\mathbf{x}_i\Big),$$

logo $\{\mathbf{y}_1, \mathbf{y}_2\} \cup \{\mathbf{x}_i \mid i \neq i_1, i_2\}$ gera V. Prosseguindo com este procedimento de eliminação conclui-se que $\langle \mathbf{y}_1, \ldots, \mathbf{y}_n \rangle = V$ e portanto $n = m$ visto que S' é *l.i.*. □

Proposição 8.8. *Seja A um anel. ASCSE*

(a) A tem a p.i.d.*;*

(b) $\forall_{m,n \in \mathbb{N}} \quad A^n \cong A^m \Rightarrow n = m$*;*

(c) $\forall_{m,n \in \mathbb{N}} \forall_{X \in M_{n\times m}(A^{op})} \forall_{Y \in M_{m\times n}(A^{op})} : \quad XY = I_n \wedge YX = I_m \Rightarrow m = n.$

Demonstração. $\boxed{(a) \Rightarrow (b)}$ Óbvio.

$\boxed{(b) \Rightarrow (a)}$ Segue do facto de todas as bases infinitas terem a mesma cardinalidade pela Proposição 8.6.

$\boxed{(b) \Leftrightarrow (c)}$ Segue de

$$\mathrm{Hom}_A(A^m, A^n) \cong M_{n\times m}(A^{op}) \quad \text{e} \quad \mathrm{Hom}_A(A^n, A^m) \cong M_{m\times n}(A^{op}).$$ □

Corolário 8.9. *Sejam A, B anéis* t.q. $\mathrm{Hom}_{\mathrm{Ring}}(A, B) \neq \varnothing$*. Se B tem a* p.i.d. *então A tem a* p.i.d.*.*

Demonstração. Sejam $X \in M_{n\times m}(A^{op})$ e $Y \in M_{m\times n}(A^{op})$ *t.q.* $XY = I_n$ e $YX = I_m$. Denotamos por $f(X) \in M_{n\times m}(B^{op})$, $f(Y) \in M_{m\times n}(B^{op})$ as matrizes que resultam de aplicar o homomorfismo f às entradas de X e Y. Temos $f(X)f(Y) = I_n$ e $f(Y)f(X) = I_m$, logo $n = m$. □

Corolário 8.10. *Seja A um anel comutativo, então A tem a* p.i.d.*.*

Demonstração. Seja $\mathcal{M} \subset A$ um ideal maximal então a projecção canónica $\pi\colon A \to A/\mathcal{M}$ é um homomorfismo para um corpo que, como já vimos, tem a *p.i.d.*. Segue do Corolário anterior que A tem a *p.i.d.*. □

Se D é um anel de divisão, os módulos-D são os espaços vectoriais-D e são livres. Em particular, os submódulos (i.e. os subespaços) de um espaço vectorial são livres. Mas esta propriedade não é válida em geral para módulos-A, mesmo quando o anel A tem a *p.i.d.*, como mostra o seguinte exemplo.

Exemplo 8.11. Seja $A = k[x, y]$, onde k é um corpo. O anel A é comutativo, logo tem a *p.i.d.* e, claro, A é um módulo-A livre de dimensão 1. O ideal $I = (x, y)$ é um submódulo de A mas não é livre, pois não é um ideal principal – ver Exercício 4.5.2.

Exercícios

4.8.1. (a) Mostre que $\dim_{\mathbb{R}} \mathbb{C} = 2$ e $\dim_{\mathbb{R}} \mathbb{R} = 1$.
(b) Mostre que não existe nenhum corpo k tal que $\mathbb{R} \subsetneq k \subsetneq \mathbb{C}$.

4.8.2. Sejam V e W espaços vectoriais sobre um anel de divisão D e seja $f : V \to W$ uma transformação linear. Mostre que $\dim_D V = \dim_D(\ker f) + \dim_D(\operatorname{im} f)$.

4.8.3. (a) Sejam V e W espaços vectoriais, de dimensão finita, sobre um anel de divisão D *t.q.* $\dim_D V = \dim_D W$ e seja $f \colon V \to W$ uma transformação linear. Prove que as seguintes afirmações são equivalentes:
(i) f é um isomorfismo;
(ii) f é sobrejectiva;
(iii) f é injectiva.
(b) Através de exemplos, mostre que a alínea anterior pode ser falsa se V e W têm dimensão infinita.

4.8.4. Seja V um espaço vectorial sobre um anel de divisão D e seja $W \subset V$ um subespaço. Mostre que:
(a) $\dim_D W \leq \dim_D V$;
(b) $\dim_D W = \dim_D V < \infty \Rightarrow W = V$;
(c) $\dim_D V = \dim_D W + \dim_D(V/W)$.

4.8.5. Considere o espaço vectorial real $V = \mathbb{R}[x]$ e seja $W = \{f(x) \in V \mid f(0) = 0\}$. Mostre que W é um subespaço de V e que $W \neq V$. Determine uma base para W e outra para V e conclua que $\dim_{\mathbb{R}} W = \dim_{\mathbb{R}} V$. Portanto, a alínea (b) do exercício anterior pode ser falsa no caso de espaços vectoriais de dimensão infinita.

9. Módulos projectivos

Definição 9.1. *Um módulo-A, P, diz-se* projectivo *se para todo o diagrama em* Mod_A

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{g} & N & \longrightarrow & 0 \end{array}$$

t.q. *a linha inferior é exacta (*i.e., *g é epi), existe $h\colon P \to M$ que faz comutar:*

$$\begin{array}{ccccc} & & P & & \\ & \overset{\exists h}{\swarrow} & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{g} & N & \longrightarrow & 0 \end{array}$$

Teorema 9.2. *Se $F \in \mathrm{Mod}_A$ é livre, então F é projectivo.*

Demonstração. Seja $B = \{\mathbf{v}_i \mid i \in I\}$ uma base de F e sejam f, g como no diagrama

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{g} & N & \longrightarrow & 0, \end{array}$$

onde g é epi. Para cada $i \in I$, seja $\mathbf{m}_i \in M$ *t.q.* $g(\mathbf{m}_i) = f(\mathbf{v}_i)$. O homomorfismo $h\colon F \to M$ *t.q.* $h(\mathbf{v}_i) = \mathbf{m}_i$ faz comutar o diagrama. □

Exemplo 9.3. Seja k um corpo. Em $\mathrm{Mod}_k = \mathrm{Vect}_k$ todos os módulos são livres e portanto são projectivos.

Exemplo 9.4. $\mathbb{Z}_2$ é um módulo-$\mathbb{Z}$ não projectivo: no diagrama

$$\begin{array}{ccccc} & & \mathbb{Z}_2 & & \\ & \overset{\nexists h}{\swarrow} & \downarrow{\scriptstyle \mathrm{id}} & & \\ \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}_2 & \longrightarrow & 0, \end{array}$$

onde π é a projecção canónica, não existe h como indicado, pois $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) = 0$.

Corolário 9.5. *Seja $M \in \mathrm{Mod}_A$, então existe um módulo projectivo P e um epimorfismo $h\colon P \to M$.*

Demonstração. Pode tomar-se P livre. □

Teorema 9.6. *Seja $P \in \mathrm{Mod}_A$. ASCSE*

(i) P é projectivo;

(ii) toda a sucessão exacta de módulos-A da forma

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

cinde-se;

(iii) P é somando directo de um módulo livre, i.e., *existe $F \in \mathrm{Mod}_A$ livre e $K \in \mathrm{Mod}_A$* t.q. *$K, P \subset F$ são submódulos, e $F = K \oplus P$.*

Demonstração. $\boxed{(i) \Rightarrow (ii)}$ Seja r como no seguinte diagrama comutativo

$$\begin{array}{ccccc} & & P & & \\ & \overset{\exists r}{\swarrow} & \downarrow{\scriptstyle \mathrm{id}_P} & & \\ N & \xrightarrow{g} & P & \longrightarrow & 0, \end{array}$$

que existe porque P é projectivo. Então, $g \circ r = \mathrm{id}_P$, logo a sucessão cinde-se.

$\boxed{(ii) \Rightarrow (iii)}$ Seja $g\colon F \to P$ um epimorfismo com F livre. Seja $i\colon \ker g \to F$ a inclusão. A sucessão

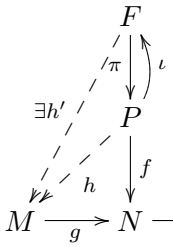
$$0 \to \ker g \xrightarrow{i} F \xrightarrow{g} P \to 0$$

é exacta. Por (i), a sucessão cinde-se, logo $F \cong \ker g \oplus P$.

$\boxed{(iii) \Rightarrow (i)}$ Seja

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow[g]{} & N & \longrightarrow & 0 \end{array}$$

t.q. g é epi. Sejam F, K *t.q.* F é livre e $F \cong K \oplus P$. Consideremos a projecção $\pi\colon F \to P$ e seja h' um homomorfismo que faz comutar o triângulo exterior do diagrama seguinte (h' existe porque F é projectivo)



onde $\iota\colon P \to K \oplus P$ é a inclusão e $h \coloneqq h' \circ \iota$. Então

$$g \circ h = g \circ h' \circ \iota = f \circ \pi \circ \iota = f \circ \mathrm{id}_P = f.$$

Concluímos que P é projectivo. □

Exemplo 9.7. Consideremos o anel $\mathbb{Z}_6$. Temos dois ideais

$$I \coloneqq \{\underline{0}, \underline{3}\} = (\underline{3}) \subset \mathbb{Z}_6 \quad \text{e} \quad J \coloneqq \{\underline{0}, \underline{2}, \underline{4}\} = (\underline{2}) \subset \mathbb{Z}_6$$

que são, portanto, submódulos-$\mathbb{Z}_6$ de $\mathbb{Z}_6$. Temos $\mathbb{Z}_6 = I \oplus J$, logo I, J são projectivos. No entanto, I, J não são livres, pois não têm subconjuntos linearmente independentes: $\underline{2} \times \underline{3} = \underline{0}$.

Exercícios

4.9.1. Dado um anel comutativo A, A^n tem uma estrutura de módulo-$M_n(A)$ identificando os vectores em A^n com as matrizes coluna e o produto por escalares $M_n(A) \times A^n \to A^n$ dado por multiplicação de matrizes $(X, \mathbf{v}) \mapsto X\mathbf{v}$.
   (a) Mostre que A^n não é um módulo-$M_n(A)$ livre.
   Sugestão: Verifique que $\{\mathbf{v}\}$ é linearmente dependente sobre $M_n(A)$ para qualquer $\mathbf{v} \in A^n$.
   (b) Mostre que A^n é um módulo-$M_n(A)$ projectivo.
   Sugestão: Identifique A^n com um submódulo N de $M_n(A)$ e mostre que N é um somando directo de $M_n(A)$.

4.9.2. Seja A um anel. Um elemento $e \in A$ diz-se *idempotente* se $e^2 = e$. Mostre que, se $e \in A$ é idempotente, Ae é um módulo-A projectivo.

4.9.3. Sejam $P_i \in \mathrm{Mod}_A$, $i \in I$. Mostre que $\bigoplus_{i \in I} P_i$ é projectivo *sse* P_i é projectivo $\forall i \in I$.

4.9.4. Mostre que $\mathbb{Q}$ não é um módulo-$\mathbb{Z}$ projectivo.

4.9.5. Seja A um anel comutativo. Dados dois módulos-A, P e M, o conjunto $\mathrm{Hom}_A(P, M)$ tem uma estrutura de módulo-A definida por

$$(f+g)(\mathbf{v}) = f(\mathbf{v}) + g(\mathbf{v}) \qquad \text{e} \qquad (af)(\mathbf{v}) = af(\mathbf{v}) \quad \forall\, \mathbf{v} \in P \ ,$$

com $f, g \in \mathrm{Hom}_A(P, M)$ e $a \in A$.

(a) Dado um homomorfismo de módulos-A, $g : M \to N$, define-se

$$g_* : \mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N)$$

por $g_*(\varphi) \coloneqq g \circ \varphi$. Mostre que a aplicação g_* é um homomorfismo de módulos-A.

(b) Seja

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

uma sucessão curta exacta de módulos-A.

(i) Se P é um módulo-A qualquer, mostre que

$$0 \longrightarrow \mathrm{Hom}_A(P, L) \xrightarrow{f_*} \mathrm{Hom}_A(P, M) \xrightarrow{g_*} \mathrm{Hom}_A(P, N)$$

é uma sucessão exacta.

(ii) Mostre que g_* é sobrejectivo se e só se P é um módulo-A projectivo.

10. Módulos injectivos

Consideremos o diagrama dual do que define módulo projectivo:

Definição 10.1. *Um módulo-A, I, diz-se* injectivo *se para todo o diagrama*

$$\begin{array}{ccccc} 0 & \longrightarrow & N & \xrightarrow{i} & M \\ & & {\scriptstyle f}\downarrow & & \\ & & I & & \end{array}$$

t.q. *a linha superior é exacta (*i.e., *i é injectivo), existe $h\colon M \to I$ que faz comutar o diagrama*

$$\begin{array}{ccccc} 0 & \longrightarrow & N & \xrightarrow{i} & M \\ & & {\scriptstyle f}\downarrow & \swarrow_{\exists h} & \\ & & I. & & \end{array}$$

Consideramos o caso particular de $A = \mathbb{Z}$.

Definição 10.2. *Um grupo abeliano D diz-se* divisível *se $\forall y \in D$ e $\forall n \in \mathbb{Z} \setminus \{0\}$ a equação*

$$nx = y$$

tem solução $x \in D$.

Exemplo 10.3. $(\mathbb{Q}, +)$ é um grupo divisível.

Proposição 10.4. *Um módulo $I \in \mathrm{Mod}_A$ é injectivo* sse *para todo o ideal esquerdo $L \subset A$ e todo $f\colon L \to I$ existe $h\colon A \to I$ que faz comutar o diagrama seguinte*

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \xrightarrow{i} & A \\ & & {\scriptstyle f}\downarrow & \swarrow_{\exists h} & \\ & & I, & & \end{array}$$

onde $i\colon L \to A$ é o homomorfismo inclusão.

Teorema 10.5. *Um grupo abeliano D é divisível* sse *D é um módulo-$\mathbb{Z}$ injectivo.*

Demonstração. $\boxed{\Leftarrow}$ Suponhamos que D é injectivo. Seja $y \in D$ e $n \in \mathbb{Z} \setminus \{0\}$. Consideremos o diagrama

$$\begin{array}{ccccc} 0 & \longrightarrow & n\mathbb{Z} & \xrightarrow{i} & \mathbb{Z} \\ & & {\scriptstyle f}\downarrow & \swarrow_{h} & \\ & & D, & & \end{array}$$

onde $f(n) = y$ – note que $n\mathbb{Z}$ é um módulo-$\mathbb{Z}$ livre com base $\{n\}$. Temos $nh(1) = h(n) = h(i(n)) = f(n) = y$ e podemos tomar $x = h(1)$.

$\boxed{\Rightarrow}$ Sejam f, i como no diagrama seguinte

$$\begin{array}{ccccc} 0 & \longrightarrow & N & \xrightarrow{i} & M \\ & & {\scriptstyle f}\downarrow & & \\ & & D & & \end{array}$$

Seja

$$\mathcal{S} \coloneqq \left\{ g\colon M' \to D \mid i(N) < M' < M \ \wedge\ g \circ i = f \right\}.$$

Temos $\mathcal{S} \neq \varnothing$ pois

$$\left(f \circ i^{-1}\colon i(N) \to D\right) \in \mathcal{S}.$$

O conjunto $\mathcal{S}$ é parcialmente ordenado pela relação:

$$\left(g_1\colon M_1' \to D\right) \leq \left(g_2\colon M_2' \to D\right) \Leftrightarrow M_1' \subset M_2' \ \wedge\ g_2|_{M_1'} = g_1.$$

Seja $\{g_j\colon M_j' \to D \mid j \in J\}$ uma cadeia em $\mathcal{S}$. Defina-se $M' \coloneqq \cup_{j\in I} M_j'$ e $g\colon M' \to D$ *t.q.* $g|_{M_j'} = g_j$. Temos $g \circ i = g_j \circ i = f$, $\forall j$, logo $g\colon M' \to D$ é majorante.

Pelo lema de Zorn, existe um elemento maximal $h\colon M' \to D$ de $\mathcal{S}$. Seja $\mathbf{y} \in M \setminus M'$ e $M'' \coloneqq M' + \langle \mathbf{y} \rangle$. Se $M' \cap \langle \mathbf{y} \rangle = \{0\}$, temos $M'' = M' \oplus \langle \mathbf{y} \rangle$ e h pode ser prolongado fazendo $\bar{h}|_{\langle \mathbf{y} \rangle} \coloneqq 0$.

Se $M' \cap \langle \mathbf{y} \rangle \neq \{0\}$, então $I = \{m \in \mathbb{Z} \mid m\mathbf{y} \in M' \cap \langle \mathbf{y} \rangle\}$ é um ideal não nulo de $\mathbb{Z}$, logo $I = \langle n \rangle$, para algum $n \in \mathbb{Z} \setminus \{0\}$. Seja $x \in D$ *t.q.* $h(n\mathbf{y}) = nx$. Defina-se $\bar{h}\colon M'' \to D$ *t.q.* $\bar{h}|_{M'} = h$ e $\bar{h}(\mathbf{y}) = x$, i.e., $\bar{h}(\mathbf{v} + m\mathbf{y}) \coloneqq h(\mathbf{v}) + mx$ onde $\mathbf{v} \in M$ e $m \in \mathbb{Z}$. $\bar{h}$ está bem definido pois, se $\mathbf{v}_1 + m_1\mathbf{y} = \mathbf{v}_2 + m_2\mathbf{y}$, com $\mathbf{v}_i \in M'$ e $m_i \in \mathbb{Z}$, então

$$\begin{aligned} \mathbf{v}_1 - \mathbf{v}_2 = m_2\mathbf{y} - m_1\mathbf{y} = (m_2 - m_1)\mathbf{y} &\in M' \cap \langle \mathbf{y} \rangle \\ \Rightarrow m_2 - m_1 \in I &\Leftrightarrow m_2 - m_2 = mn \end{aligned}$$

para algum $m \in \mathbb{Z}$ e, portanto,

$$\begin{aligned} h(\mathbf{v}_1) - h(\mathbf{v}_2) = h(\mathbf{v}_1 - \mathbf{v}_2) &= h((m_2 - m_1)\mathbf{y}) \\ &= h(mn\mathbf{y}) = mh(n\mathbf{y}) = mnx = m_2x - m_1x\ . \end{aligned}$$

Obtemos assim uma contradição, pois $\bar{h}$ prolonga h. Concluímos que $M' = M$. □

Exemplo 10.6. $(\mathbb{Q}, +)$ é um grupo abeliano injectivo.

Exercícios

4.10.1. Demonstre a Proposição 10.4.

4.10.2. Mostre que as seguintes afirmações são equivalentes:
- (i) qualquer módulo-A é projectivo;
- (ii) qualquer sucessão curta exacta de módulos-A cinde-se;
- (iii) qualque módulo-A é injectivo.

4.10.3. Mostre que qualquer espaço vectorial sobre um anel de divisão D é projectivo e injectivo.

4.10.4. Prove as seguintes afirmações:
- (a) nenhum grupo abeliano finito, não trivial, é divisível;
- (b) nenhum grupo abeliano livre[2], não trivial, é divisível.

4.10.5. Mostre que o grupo $\mathbb{Z}(p^\infty)$, onde $p \in \mathbb{N}$ é um primo, é divisível.

4.10.6. Seja D um grupo abeliano livre de torção[3] divisível.
- (a) Dados $n \in \mathbb{Z} \setminus \{0\}$ e $a \in D$, seja $b \in D$ tal que $nb = a$. Mostre que $\frac{1}{n} \cdot a \coloneqq b$ induz um produto por escalares $\mathbb{Q} \times D \to D$ que, juntamente com a soma em D, define uma estrutura de espaço vectorial-$\mathbb{Q}$ em D.
- (b) Conclua que $D \cong \oplus_{i\in I}\mathbb{Q}$.

[2] Recorde que um grupo abeliano G diz-se *livre* se for livre como módulo-$\mathbb{Z}$ – ver Observação 6.3.

[3] Um grupo abeliano G diz-se *livre de torção* se o subgrupo $\mathrm{Tor}(G) \coloneqq \{g \in G \mid |g| \text{ é finita}\}$ é o grupo trivial $\{0\}$ – ver Exercício 1.4.11.

11. Produto tensorial

Definição 11.1. *Sejam $M_1, M_2, N \in \mathrm{Mod}_A$ e seja $\varphi\colon M_1 \times M_2 \to N$. Diz-se que φ é* bilinear-A *se para todo $a, a' \in A$ e todo $\mathbf{v}, \mathbf{v}' \in M_1$, $\mathbf{w}, \mathbf{w}' \in M_2$ se tem*

(i) $\varphi(a\mathbf{v} + a'\mathbf{v}', \mathbf{w}) = a\varphi(\mathbf{v}, \mathbf{w}) + a'\varphi(\mathbf{v}', \mathbf{w})$;

(ii) $\varphi(\mathbf{v}, a\mathbf{w} + a'\mathbf{w}') = a\varphi(\mathbf{v}, \mathbf{w}) + a'\varphi(\mathbf{v}, \mathbf{w})$

i.e., *φ é bilinear-A se é linear-A separadamente em cada uma das variáveis.*

Observação 11.2. De forma análoga define-se aplicação multilinear-A:

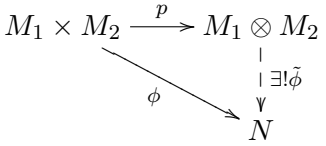
$$\varphi\colon M_1 \times \cdots \times M_r \to N.$$

Exemplos 11.3. 1. Seja V um espaço vectorial-$\mathbb{R}$ e seja $(\cdot\,,\cdot) : V \times V \to \mathbb{R}$ um produto interno. A aplicação $(\cdot\,,\cdot)$ é bilinear-$\mathbb{R}$.

2. Se A é um anel comutativo, o produto $A \times A \to A$, $(a, b) \mapsto ab$, é bilinear-A.
3. Seja M um módulo sobre um anel comutativo A. O produto por escalares $A \times M \to M$, $(a, \mathbf{v}) \mapsto a\mathbf{v}$, é bilinear-$A$.
4. O determinante $\det : M_n(\mathbb{R}) \to \mathbb{R}$ é multilinear nas colunas (ou linhas) de uma matriz $n \times n$.

No resto desta secção, A é um anel comutativo.

Teorema 11.4. *Sejam $M_1, M_2 \in \mathrm{Mod}_A$. Então existe um módulo-A, $M_1 \otimes M_2$, com uma aplicação bilinear-A, $p\colon M_1 \times M_2 \to M_1 \otimes M_2$, que é universal para aplicações bilineares-A a partir de $M_1 \times M_2$,* i.e., *dado $N \in \mathrm{Mod}_A$ e uma aplicação bilinear-A $\phi\colon M_1 \times M_2 \to N$, $\exists!\, \tilde{\phi} \in \mathrm{Hom}_A(M_1 \otimes M_2, N)$ que faz comutar o diagrama seguinte:*



Demonstração. Seja L o módulo-A livre gerado $M_1 \times M_2$: $L \coloneqq F(M_1 \times M_2)$; os seus elementos escrevem-se unicamente na forma

$$\sum_{i=1}^{n} a_i \mathbf{e}_{(\mathbf{v}_i, \mathbf{w}_i)},$$

com $a_i \in A$, $\mathbf{v}_i \in M_1$, $\mathbf{w}_i \in M_2$. Seja $R \subset L$ o submódulo gerado pelos elementos da seguinte forma:

$$\begin{aligned}
&\mathbf{e}_{(\mathbf{v}+\mathbf{v}', \mathbf{w})} - \mathbf{e}_{(\mathbf{v}, \mathbf{w})} - \mathbf{e}_{(\mathbf{v}', \mathbf{w})} \\
&\mathbf{e}_{(\mathbf{v}, \mathbf{w}+\mathbf{w}')} - \mathbf{e}_{(\mathbf{v}, \mathbf{w})} - \mathbf{e}_{(\mathbf{v}, \mathbf{w}')} \\
&\mathbf{e}_{(a\mathbf{v}, \mathbf{w})} - a\mathbf{e}_{(\mathbf{v}, \mathbf{w})} \\
&\mathbf{e}_{(\mathbf{v}, a\mathbf{w})} - a\mathbf{e}_{(\mathbf{v}, \mathbf{w})}.
\end{aligned}$$

onde $\mathbf{v}, \mathbf{v}' \in M_1$, $\mathbf{w}, \mathbf{w}' \in M_2$ e $a \in A$.

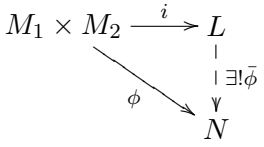
Defina-se $M_1 \otimes M_2 \coloneqq L/R$, seja $\pi\colon L \to M_1 \otimes M_2$ a projecção canónica e seja $p\colon M_1 \times M_2 \to M_1 \otimes M_2$ a composta

$$\begin{aligned}
p\colon M_1 \times M_2 &\hookrightarrow L \xrightarrow{\pi} M_1 \otimes M_2 \\
(\mathbf{v}, \mathbf{w}) &\longmapsto \mathbf{e}_{(\mathbf{v}, \mathbf{w})} \longmapsto \pi(\mathbf{e}_{(\mathbf{v}, \mathbf{w})}).
\end{aligned}$$

Por definição de R, p é bilinear-A:

$$\mathbf{e}_{(\mathbf{v}+\mathbf{v}', \mathbf{w})} - \mathbf{e}_{(\mathbf{v}, \mathbf{w})} - \mathbf{e}_{(\mathbf{v}', \mathbf{w})} \in R \Leftrightarrow p(\mathbf{v} + \mathbf{v}', \mathbf{w}) = p(\mathbf{v}, \mathbf{w}) + p(\mathbf{v}', \mathbf{w}).$$

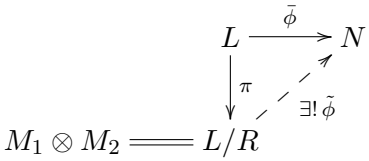
Falta apenas provar que p é universal. Seja $\phi\colon M_1 \times M_2 \to N$ uma aplicação bilinear-A. Seja $\bar{\phi}\colon L \to N$ o homomorfismo determinado por ϕ:



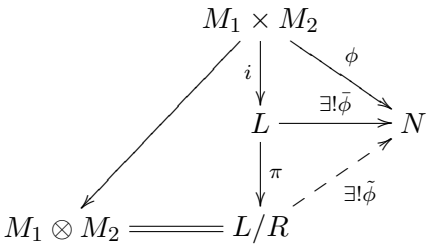
Ou seja, $\bar{\phi}$ é a extensão linear de ϕ. Temos

$$\phi \text{ bilinear-}A \Leftrightarrow R \subset \ker \bar{\phi},$$

logo $\exists!\, \tilde{\phi}\colon L/R \to N$ que faz comutar



Juntando os dois diagramas acima, obtemos o diagrama pretendido:



□

Observação 11.5. A propriedade universal do produto tensorial determina-o a menos de isomorfismo tal como acontece com outros objectos universais: quociente, soma directa (coproduto), produto directo (produto).

Notação 11.6. Dados $\mathbf{v} \in M_1$ e $\mathbf{w} \in M_2$ denotamos por $\mathbf{v} \otimes \mathbf{w}$ o elemento $p(\mathbf{v}, \mathbf{w})$ do produto tensorial $V \otimes W$:

$$\boxed{\mathbf{v} \otimes \mathbf{w} \coloneqq p(\mathbf{v}, \mathbf{w})}$$

Observação 11.7.

1. Da bilinearidade de $p\colon M_1 \times M_2 \to M_1 \otimes M_2$, seguem as seguintes igualdades em $M_1 \otimes M_2$

$$a(\mathbf{v} \otimes \mathbf{w}) = (a\mathbf{v}) \otimes \mathbf{w} = \mathbf{v} \otimes (a\mathbf{w})$$
$$(\mathbf{v} + \mathbf{v}') \otimes \mathbf{w} = \mathbf{v} \otimes \mathbf{w} + \mathbf{v}' \otimes \mathbf{w}.$$

   Ambas igualdades são usadas com frequência.

2. A função

$$\begin{aligned} p\colon M_1 \times M_2 &\longrightarrow M_1 \otimes M_2 \\ (\mathbf{v}, \mathbf{w}) &\longmapsto \mathbf{v} \otimes \mathbf{w} \end{aligned}$$

   não é sobrejectiva em geral, no entanto, dado $\mathbf{x} \in M_1 \otimes M_2$ existem $\mathbf{v}_1, \ldots, \mathbf{v}_n \in M_1$, $\mathbf{w}_1, \ldots, \mathbf{w}_n \in M_2$ *t.q.*

$$\boxed{\mathbf{x} = \sum_{i=1}^{n} \mathbf{v}_i \otimes \mathbf{w}_i}$$

pois

$$\mathbf{x} = \pi\Big(\sum_{i=1}^{n} a_i \mathbf{e}_{(\mathbf{v}'_i, \mathbf{w}'_i)}\Big) \Leftrightarrow \mathbf{x} = \sum_{i=1}^{n} a_i \left(\mathbf{v}'_i \otimes \mathbf{w}'_i\right) = \sum_{i=1}^{n} \underbrace{\left(a_i \mathbf{v}'_i\right)}_{\mathbf{v}_i} \otimes \underbrace{\mathbf{w}'_i}_{\mathbf{w}_i}.$$

3. Da propriedade universal do produto tensorial (ou de 2. acima) segue que dois homomorfismos $f, g\colon M_1 \otimes M_2 \to N$ são iguais *sse*

$$\forall_{\mathbf{v}\in M_1}\, \forall_{\mathbf{w}\in M_2} \quad f(\mathbf{v}\otimes\mathbf{w}) = g(\mathbf{v}\otimes\mathbf{w}).$$

Exemplos 11.8. 1. Se $A = \mathbb{R}$ e $V = W = \mathbb{R}^n$, então

$$V \otimes W = T^{0,2}(\mathbb{R}^n)$$

são os tensores-2 covariantes. Se $V = W = (\mathbb{R}^n)^* \coloneqq \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$, então $V \otimes W = T^{2,0}(\mathbb{R}^n)$, *e.g.*, o produto interno usual $(\cdot\,,\cdot) \in T^{2,0}(\mathbb{R}^n)$.

2. Sejam $A = \mathbb{Z}$, $M_1 = \mathbb{Z}_2$ e $M_2 = \mathbb{Z}_3$. Temos

$$\forall_{m,n\in\mathbb{Z}} \quad \underline{m} \otimes \underline{n} = \underline{m} \otimes 4\underline{n} = 2(\underline{m} \otimes (2\underline{n})) = (2\underline{m}) \otimes (2\underline{n}) = 0.$$

Concluímos que $\mathbb{Z}_2 \otimes \mathbb{Z}_3 = \{0\}$.

Observação 11.9. No Exemplo 11.8.2. usámos o seguinte facto: da bilinearidade de $p\colon M_1 \times M_2 \to M_1 \otimes M_2$ segue

$$\forall_{\mathbf{v}\in M_1}\, \forall_{\mathbf{w}\in M_2} \quad \mathbf{v}\otimes 0_{M_2} = 0_{M_1} \otimes \mathbf{w} = 0_{M_1\otimes M_2}.$$

De facto,

$$p(\mathbf{v}, 0_{M_2}) = p(\mathbf{v}, 0_A \cdot 0_{M_2}) = 0_{M_1\otimes M_2} = p(0_A \cdot 0_{M_1}, \mathbf{w}) = p(0_{M_1}, \mathbf{w}).$$

Notação 11.10. Também se escreve $M_1 \otimes_A M_2$ para enfatizar que se trata do *produto tensorial como módulos-A.*

Teorema 11.11. *Dados $M_1, \ldots, M_n \in \mathrm{Mod}_A$ existe um módulo-A, $\bigotimes_{i=1}^n M_i$, com uma aplicação multiplinear $p\colon \prod_{i=1}^n M_i \to \bigotimes_{i=1}^n M_i$ que é universal entre as aplicações multilineares para módulos-A. Esta propriedade determina o módulo $\bigotimes_{i=1}^n M_i$ a menos de isomorfismo.*

Notação 11.12. $\boxed{\mathbf{v}_1 \otimes \cdots \otimes \mathbf{v}_n \coloneqq p(\mathbf{v}_1, \ldots, \mathbf{v}_n)}$

Proposição 11.13 (Propriedades do Produto Tensorial)**.** *Sejam M, M_1, M_2, M_3, N, M_i (para $i \in I$) módulos-A. Temos os seguintes isomorfismos naturais*

(a) $M_1 \otimes (M_2 \otimes M_3) \cong (M_1 \otimes M_2) \otimes M_3 \cong M_1 \otimes M_2 \otimes M_3$*;*

(b) $M_1 \otimes M_2 \cong M_2 \otimes M_1$ *com isomorfismos induzidos por* $\mathbf{v}\otimes\mathbf{w} \leftrightarrow \mathbf{w}\otimes\mathbf{v}$*;*

(c) $\left(\bigoplus_{i\in I} M_i\right) \otimes N \cong \bigoplus_{i\in I}(M_i \otimes N)$ *com isomorfismos induzidos por* $(\mathbf{v}_i)_{i\in I}\otimes\mathbf{w} \leftrightarrow (\mathbf{v}_i\otimes\mathbf{w})_{i\in I}$*;*

(d) $M \otimes_A A \cong A \otimes_A M \cong M$ *com isomorfismos induzidos por* $\mathbf{v}\otimes a \leftrightarrow a\otimes\mathbf{v} \leftrightarrow a\mathbf{v}$*.*

Demonstração.

(a) Exercício.

(b) Seja $\varphi\colon M_1 \times M_2 \to M_2 \otimes M_1$, dado por $\varphi(\mathbf{v}, \mathbf{w}) = \mathbf{w}\otimes\mathbf{v}$ e $\psi\colon M_2 \times M_1 \to M_1 \otimes M_2$ dado por $\psi(\mathbf{w}, \mathbf{v}) = \mathbf{v}\otimes\mathbf{w}$. Vejamos que φ e ψ são bilineares:

$$\begin{aligned}\varphi(a\mathbf{v} + a'\mathbf{v}', \mathbf{w}) &= \mathbf{w} \otimes (a\mathbf{v} + a'\mathbf{v}') \\ &= a(\mathbf{w}\otimes\mathbf{v}) + a'(\mathbf{w}\otimes\mathbf{v}') \\ &= a\varphi(\mathbf{v}, \mathbf{w}) + a'\varphi(\mathbf{v}', \mathbf{w}).\end{aligned}$$

As restantes condições relativas à bilinearidade seguem de forma análoga. Pela propriedade universal do produto tensorial, concluí-se que existe $\tilde{\varphi} \in \mathrm{Hom}_A(M_1 \otimes M_2, M_2 \otimes M_1)$ e $\tilde{\psi} \in \mathrm{Hom}_A(M_2 \otimes M_1, M_1 \otimes M_2)$ *t.q.*

$$\begin{aligned}\tilde{\varphi}(\mathbf{v} \otimes \mathbf{w}) &= \mathbf{w} \otimes \mathbf{v}\\ \tilde{\psi}(\mathbf{w} \otimes \mathbf{v}) &= \mathbf{v} \otimes \mathbf{w},\end{aligned}$$

logo

$$\tilde{\psi} \circ \tilde{\varphi}(\mathbf{v} \otimes \mathbf{w}) = \tilde{\psi}(\mathbf{w} \otimes \mathbf{v}) = \mathbf{v} \otimes \mathbf{w} = \mathrm{id}_{M_1 \otimes M_2}(\mathbf{v} \otimes \mathbf{w}).$$

Portanto $\tilde{\psi} \circ \tilde{\varphi} = \mathrm{id}_{M_1 \otimes M_2}$. Da mesma forma, $\tilde{\varphi} \circ \tilde{\psi} = \mathrm{id}_{M_2 \otimes M_1}$.

(c) Vamos verificar que $\bigoplus_{i \in I}(M_i \otimes N)$ satisfaz a propriedade universal do produto tensorial $\left(\bigoplus_{i \in I} M_i\right) \otimes N$. Seja

$$q : \Big(\bigoplus_{i \in I} M_i\Big) \times N \to \bigoplus_{i \in I}(M_i \otimes N)$$

a aplicação dada por $q((\mathbf{v}_i)_{i \in I}, \mathbf{w}) = (\mathbf{v}_i \otimes \mathbf{w})_{i \in I}$.

(1º) q é bilinear-A pois

$$\begin{aligned}q(a(\mathbf{u}_i)_{i \in I} + b(\mathbf{v}_i)_{i \in I}, \mathbf{w}) &= q((a\mathbf{u}_i + b\mathbf{v}_i)_{i \in I}, \mathbf{w}) = ((a\mathbf{u}_i + b\mathbf{v}_i) \otimes \mathbf{w})_{i \in I}\\ &= (a(\mathbf{u}_i \otimes \mathbf{w}) + b(\mathbf{v}_i \otimes \mathbf{w}))_{i \in I}\\ &= a(\mathbf{u}_i \otimes \mathbf{w})_{i \in I} + b(\mathbf{v}_i \otimes \mathbf{w})_{i \in I}\\ &= aq((\mathbf{u}_i)_{i \in I}, \mathbf{w}) + bq((\mathbf{v}_i)_{i \in I}, \mathbf{w}) \ ,\end{aligned}$$

onde $(\mathbf{u}_i)_{i \in I}, (\mathbf{v}_i)_{i \in I} \in \bigoplus_{i \in I} M_i$, $\mathbf{w} \in N$ e $a, b \in A$, e

$$\begin{aligned}q((\mathbf{u}_i)_{i \in I}, a\mathbf{w} + b\mathbf{w}') &= (\mathbf{u}_i \otimes (a\mathbf{w} + b\mathbf{w}'))_{i \in I}\\ &= (a(\mathbf{u}_i \otimes \mathbf{w}) + b(\mathbf{u}_i \otimes \mathbf{w}'))_{i \in I}\\ &= aq((\mathbf{u}_i)_{i \in I}, \mathbf{w}) + bq((\mathbf{u}_i)_{i \in I}, \mathbf{w}') \ ,\end{aligned}$$

onde $(\mathbf{u}_i)_{i \in I} \in \bigoplus_{i \in I} M_i$, $\mathbf{w}, \mathbf{w}' \in N$ e $a, b \in A$.

(2º) $\bigoplus_{i \in I}(M_i \otimes N)$ e q verificam a propriedade universal do produto tensorial:

Seja L um módulo-A e $\varphi : \left(\bigoplus_{i \in I} M_i\right) \times N \to L$ uma aplicação bilinear-A. Queremos mostrar que existe um único homomorfismo $\tilde{\varphi}$ que faz o seguinte diagrama comutar

$$\begin{array}{ccc}\left(\bigoplus_{i \in I} M_i\right) \times N & \xrightarrow{\ q\ } & \bigoplus_{i \in I}(M_i \otimes N)\\ & \searrow^{\varphi} & \downarrow{\scriptstyle \tilde{\varphi}}\\ & & L\end{array}$$

Para cada $i \in I$, seja $\varphi_i : M_i \times N \to L$ a aplicação dada por $\varphi_i(\mathbf{v}_i, \mathbf{w}) = \varphi(\iota_i(\mathbf{v}_i), \mathbf{w})$, onde $\iota_i : M_i \to \bigoplus_{i \in I} M_i$ são as aplicações de estrutura da soma directa. Como φ_i é bilinear (verifique!), existe um único homomorfismo $\tilde{\varphi}_i : M_i \otimes N \to L$ tal que

$$\tilde{\varphi}_i(\mathbf{v}_i \otimes \mathbf{w}) = \varphi(\iota_i(\mathbf{v}_i), \mathbf{w}) = \varphi(\iota_i(\mathbf{v}_i), \mathbf{w}) \ . \tag{11.1}$$

Pela propriedade universal da soma directa, a colecção de homomorfismos $\{\tilde{\varphi}_i : M_i \otimes N \to L\}$ define um único homomorfismo $\tilde{\varphi} : \bigoplus_{i \in I}(M_i \otimes N) \to L$ tal que

$$\tilde{\varphi}((\mathbf{u}_i)_{i \in I}) = \sum_{i \in I} \tilde{\varphi}(\mathbf{u}_i) \ . \tag{11.2}$$

(Note que a soma é finita pois $\{i \in I \mid \mathbf{u}_i \neq 0\}$ é um conjunto finito porque se trata de uma soma directa.)

Este homomorfismo φ faz o diagrama acima comutar pois:

$$\begin{aligned}
\tilde{\varphi}(q((\mathbf{v}_i)_{i\in I}, \mathbf{w})) &= \tilde{\varphi}((\mathbf{v}_i \otimes \mathbf{w})_{i\in I}) && \text{por definição de } q \\
&= \sum_{i\in I} \tilde{\varphi}(\mathbf{v}_i \otimes \mathbf{w}) && \text{por (11.2)} \\
&= \sum_{i\in I} \varphi(\iota_i(\mathbf{v}_i), \mathbf{w}) && \text{por (11.1)} \\
&= \varphi\Big(\sum_{i\in I} \iota_i(\mathbf{v}_i), \mathbf{w}\Big) && \text{porque } \varphi \text{ é bilinear} \\
&= \varphi((\mathbf{v}_i)_{i\in I}, \mathbf{w}) \ ,
\end{aligned}$$

onde $(\mathbf{v}_i)_{i\in I} \in \bigoplus_{i\in I} M_i$ e $\mathbf{w} \in N$, portanto $\tilde{\varphi} \circ q = \varphi$.

(d) Seja $\varphi\colon A \otimes_A M \to M$ o homomorfismo definido por $\varphi(a \otimes \mathbf{v}) \coloneqq a\mathbf{v}$ (φ está bem definido porque a expressão que a define é bilinear) e seja $\psi\colon M \to A \otimes_A M$ definido por $\psi(\mathbf{v}) \coloneqq 1_A \otimes \mathbf{v}$. Temos

$$\begin{aligned}
\psi \circ \varphi(a \otimes \mathbf{v}) = \psi(a\mathbf{v}) = 1_A \otimes (a\mathbf{v}) = a(1_A \otimes \mathbf{v}) = a \otimes \mathbf{v} \\
\varphi \circ \psi(\mathbf{v}) = \varphi(1_A \otimes \mathbf{v}) = 1_A \cdot \mathbf{v} = \mathbf{v}.
\end{aligned}$$

□

Definição 11.14. *Dados $f_1 \operatorname{Hom}_A(M_1, N_1)$, $f_2 \in \operatorname{Hom}_A(M_2, N_2)$, a função*

$$\begin{aligned}
M_1 \times M_2 &\to N_1 \otimes N_2 \\
(\mathbf{v}, \mathbf{w}) &\mapsto f_1(\mathbf{v}) \otimes f_2(\mathbf{w})
\end{aligned}$$

é bilinear, portanto induz um homomorfismo $M_1 \otimes M_2 \to N_1 \otimes N_2$ que denotamos por $T(f_1, f_2)$ ou por $f_1 \otimes f_2$.

Definição 11.15. *Denotamos por $(\operatorname{Mod}_A)^2$, ou por $\operatorname{Mod}_A \times Mod_A$, a categoria dos pares de módulos-A e pares de homomorfismos de módulos-A.*

Proposição 11.16. *A correspondência $(M, N) \mapsto M \otimes N$ define um functor $(\operatorname{Mod}_A)^2 \to \operatorname{Mod}_A$. Em particular, dado um módulo-A, N, as correspondências*

$$\begin{aligned}
f &\mapsto T(f, \mathrm{id}_N) \qquad e \qquad & f &\mapsto T(\mathrm{id}_N, f) \\
M &\mapsto M \otimes N & M &\mapsto N \otimes M
\end{aligned}$$

são functores $\operatorname{Mod}_A \to \operatorname{Mod}_A$.

Corolário 11.17. *Sejam $M, N \in \operatorname{Mod}_A$ livres com bases $\{\mathbf{m}_i\}_{i\in I}$ e $\{\mathbf{n}_j\}_{j\in J}$. Então $M \otimes N \in \operatorname{Mod}_A$ é livre com base $\{\mathbf{m}_i \otimes \mathbf{n}_j\}_{(i,j)\in I\times J}$. Em particular,*

$$\dim_A(M \otimes N) = \dim_A(M) \dim_A(N).$$

Demonstração. Sejam $\varphi\colon \bigoplus_{i\in I} A \xrightarrow{\cong} M$ e $\psi\colon \bigoplus_{j\in J} A \xrightarrow{\cong} N$ os isomorfismos dados por

$$\varphi\,(a_i)_{i\in I} \coloneqq \sum_{i\in I} a_i \mathbf{m}_i \quad \text{e} \quad \psi\,(b_j)_{j\in J} \coloneqq \sum_{j\in J} b_j \mathbf{n}_j.$$

Temos

$$\big(\bigoplus_{i\in I} A\big) \otimes \big(\bigoplus_{j\in J} A\big) \xrightarrow[\cong]{T(\varphi,\psi)} M \otimes N$$

pois $(\varphi, \psi) \in \operatorname{Hom}_{(\operatorname{Mod}_A)^2}$ é um isomorfismo. Por outro lado,

$$\begin{aligned}
\bigoplus_{(i,j)\in I\times J} A \otimes_A A \quad &\xrightarrow{\cong} \quad \bigoplus_{(i,j)\in I\times J} A \\
(a_i \otimes b_j)_{i,j} \quad &\longmapsto \quad (a_i b_j)_{i,j} \ ,
\end{aligned}$$

logo o resultado segue. □

Exemplo 11.18. $A[x]$ e $A[y]$ são módulos-A livres com bases $\{1, x, x^2, \ldots\}$ e $\{1, y, y^2, \ldots\}$, respectivamente, logo, pelo Corolário 11.17, $A[x] \otimes_A A[y]$ é livre com base $\{x^i \otimes y^j \mid i, j \in \mathbb{N}_0\}$ e $x^i \otimes y^j \mapsto x^i y^j$ define um isomorfismo de módulos-A $A[x] \otimes_A A[y] \to A[x, y]$.

Exemplo 11.19. Identificando vectores com matizes coluna, a aplicação

$$B : \mathbb{R}^n \times \mathbb{R}^n \to M_n(\mathbb{R})$$
$$(\mathbf{v}, \mathbf{w}) \mapsto \mathbf{v}\mathbf{w}^T$$

é bilinear-$\mathbb{R}$, portanto induz uma aplicação linear-$\mathbb{R}$

$$\beta : \mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{R}^n \to M_n(\mathbb{R})$$
$$\mathbf{v} \otimes \mathbf{w} \mapsto \mathbf{v}\mathbf{w}^T$$

onde $\mathbf{w}^T$ designa a transposta da matriz $\mathbf{w}$. Seja $\{\mathbf{e}_i\}_{i\in\{1,\ldots,n\}}$ a base canónica de $\mathbb{R}^n$ e seja $E_{i,j} \in M_n(\mathbb{R})$ a matriz cuja entrada (i, j) é 1 e as restantes entradas são nulas . Então $\{\mathbf{e}_i \otimes \mathbf{e}_j\}_{i,j\in\{1,\ldots,n\}}$ é uma base[4] de $\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{R}^n$. Como $\beta(\mathbf{e}_i \otimes \mathbf{e}_j) = E_{ij}$ e como $\{E_{ij}\}_{i,j\in\{1,\ldots,n\}}$ é uma base de $M_n(\mathbb{R})$, concluímos que β é um isomorfismo.

Exercícios

4.11.1. (a) Seja G um grupo abeliano. Mostre que $G \otimes \mathbb{Z}_m \cong G/mG, \forall\, m > 0$.
(b) Mostre que $\mathbb{Z}_m \otimes \mathbb{Z}_n \cong \mathbb{Z}_d$, onde $d = \text{MDC}(m, n)$.
(c) Seja G um grupo abeliano de torção.[5] Mostre que $G \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.
(d) Mostre que $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$.

4.11.2. Sejam M e N módulos sobre um anel comutativo A e sejam $M' \subset M$ e $N' \subset N$ submódulos. Mostre que

$$M/M' \otimes_A N/N' \cong (M \otimes_A N)/H\ ,$$

onde H é o submódulo de $M \otimes N$ gerado por $\mathbf{v}' \otimes \mathbf{w}$ e $\mathbf{v} \otimes \mathbf{w}'$ para $\mathbf{v}' \in M'$, $\mathbf{v} \in M$, $\mathbf{w}' \in N'$ e $\mathbf{w} \in N$.

4.11.3. Sejam I e J ideais de um anel comutativo A, seja M um módulo-A. Mostre que:
(a) $A/I \otimes_A M \cong M/IM$, como módulos-$A$, onde $IM = \langle a\mathbf{v} \mid a \in I, \mathbf{v} \in M\rangle$ é um submódulo de M;
(b) $A/I \otimes_A A/J \cong A/(I + J)$, como módulos-$A$.

4.11.4. A inclusão $\iota : \mathbb{Z}_2 \to \mathbb{Z}_4$ é um homomorfismo de grupos abelianos, pois $\mathbb{Z}_2 < \mathbb{Z}_4$. Mostre que $\text{id} \otimes \iota \colon \mathbb{Z}_2 \otimes \mathbb{Z}_2 \to \mathbb{Z}_2 \otimes \mathbb{Z}_4$ é a aplicação nula, no entanto $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \neq 0$ e $\mathbb{Z}_2 \otimes \mathbb{Z}_4 \neq 0$.

4.11.5. Dê exemplos de um anel comutativo A e módulos-A M e N tais que:
(a) $M \otimes_A N \ncong M \otimes_{\mathbb{Z}} N$;
(b) $\exists\, \mathbf{u} \in M \otimes_A N$ *t.q.* $\forall\, \mathbf{v} \in M, \forall\, \mathbf{w} \in N \quad \mathbf{u} \neq \mathbf{v} \otimes \mathbf{w}$;
(c) $\exists\, \mathbf{v}, \mathbf{v}' \in M, \mathbf{w}, \mathbf{w}' \in N$ *t.q.* $\mathbf{v} \neq \mathbf{v}', \mathbf{w} \neq \mathbf{w}'$ e $\mathbf{v} \otimes \mathbf{w} = \mathbf{v}' \otimes \mathbf{w}'$.

4.11.6. Determine $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$ e $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$.

4.11.7. Demonstre a Proposição 11.16.

[4] Uma vez que o anel dos escalares é um corpo, já sabemos que os módulos são livres, mas o Corolário 11.17 permite-nos identificar uma base para o produto tensorial à custa de uma de $\mathbb{R}^n$.

[5] Um grupo abeliano G diz-se de *torção* se $G = \text{Tor}(G)$ – ver Exercício 1.4.11.

12. Propriedades adicionais do produto tensorial

Teorema 12.1. *Seja A um anel comutativo, seja N um módulo-A e seja*

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

uma sucessão exacta de módulos-A. Então

$$M_1 \otimes N \xrightarrow{f\otimes \mathrm{id}} M_2 \otimes N \xrightarrow{g\otimes \mathrm{id}} M_3 \otimes N \longrightarrow 0$$

é uma sucessão exacta.

Demonstração. 1. $g\otimes \mathrm{id}$ é sobrejectivo: Dado $\mathbf{v} \in M_3$ e $\mathbf{w} \in N$, seja $\mathbf{u} \in M_2$ tal que $g(\mathbf{u}) = \mathbf{v}$ (g é sobrejectivo por hipótese). Temos

$$\mathbf{v} \otimes \mathbf{w} = g(\mathbf{u}) \otimes \mathbf{w} = (g \otimes \mathrm{id})(\mathbf{u} \otimes \mathbf{w}) \in \mathrm{im}(g \otimes \mathrm{id})$$

e, como os elementos $\mathbf{v} \otimes \mathbf{w}$ geram $M_3 \otimes N$, concluímos que $g \otimes \mathrm{id}$ é sobrejectivo.

2. $\ker(g \otimes \mathrm{id}) \subset \mathrm{im}(f \otimes \mathrm{id})$:

$$\mathrm{im}\, f = \ker g \Rightarrow g \circ f = 0 \Rightarrow (g \otimes \mathrm{id}) \circ (f \otimes \mathrm{id}) = (g \circ f) \otimes \mathrm{id} = 0.$$

3. $\mathrm{im}(f \otimes \mathrm{id}) \subset \ker(g \otimes \mathrm{id})$: Por 2. e pela propriedade universal do quociente de módulos (Proposição 2.8), a aplicação

$$\varphi : \frac{M_2 \otimes N}{\mathrm{im}(f \otimes \mathrm{id})} \longrightarrow M_3 \otimes N$$

induzida por $g \otimes \mathrm{id}$, i.e, tal que $\varphi(\underline{\mathbf{u} \otimes \mathbf{w}}) = g(\mathbf{u}) \otimes \mathbf{w}$, é um homomorfismo de módulos-A.

Como $\mathrm{im}(f \otimes \mathrm{id}) = \ker(g \otimes \mathrm{id})$ *sse* φ é injectiva, vamos mostrar que φ é injectiva. Para isso basta ver que φ tem inverso à esquerda.

Seja então $\psi : M_3 \times N \to \frac{M_2 \otimes N}{\mathrm{im}(f\otimes \mathrm{id})}$ dada por $\psi(\mathbf{v}, \mathbf{w}) = \underline{\mathbf{u} \otimes \mathbf{w}}$, onde $\mathbf{u} \in M_2$ é tal que $g(\mathbf{u}) = \mathbf{v}$.

ψ está bem definida: seja $\mathbf{u}' \in M_2$ tal que $\mathbf{v} = g(\mathbf{u}) = g(\mathbf{u}')$, então

$$\mathbf{u}' - \mathbf{u} \in \ker g = \mathrm{im}\, f \Rightarrow (\mathbf{u}' - \mathbf{u}) \otimes \mathbf{w} \in \mathrm{im}(f \otimes \mathrm{id}) \quad \forall_{\mathbf{w}\in N}$$

e portanto

$$\psi(g(\mathbf{u}) \otimes \mathbf{w}) = \underline{\mathbf{u} \otimes \mathbf{w}} = \underline{\mathbf{u} \otimes \mathbf{w}} + \underline{(\mathbf{u}' - \mathbf{u}) \otimes \mathbf{w}} = \underline{\mathbf{u}' \otimes \mathbf{w}} = \psi(g(\mathbf{u}') \otimes \mathbf{w}).$$

Como ψ é claramente bilinear, exite um homomorfismo

$$\tilde{\psi} : M_3 \otimes N \longrightarrow \frac{M_2 \otimes N}{\mathrm{im}(f \otimes \mathrm{id})}$$

tal que $\tilde{\psi}(\mathbf{v} \otimes \mathbf{u}) = \psi(\mathbf{v}, \mathbf{u})$. Logo

$$\tilde{\psi} \circ \varphi(\underline{\mathbf{u} \otimes \mathbf{w}}) = \tilde{\psi}(g(\mathbf{u}) \otimes \mathbf{w}) = \underline{\mathbf{u} \otimes \mathbf{w}} \qquad \forall\, \mathbf{u} \in_2 \forall\, \mathbf{w} \in N$$

donde concluímos que $\tilde{\psi} \circ \varphi = \mathrm{id}$. □

Observação 12.2. Recorde que $T : (\mathrm{Mod}_A)^2 \to \mathrm{Mod}_A$ com $T(M, N) = M \otimes_A N$ e $T(f, g) = f \otimes g$ é um functor. Se fixarmos o módulo N e $g = \mathrm{id}_N$, obtemos um novo functor (Proposição 11.16)

$$T_N : \mathrm{Mod}_A \to \mathrm{Mod}_A$$

definido por $T_N(M) = M \otimes_A N$, nos objectos, e $T_N(f) = f \otimes \mathrm{id}$, nos morfismos. O teorema anterior, diz-nos que T_N preserva o lado direito de uma sucessão curta exacta. Um functor que satisfaz esta propriedade diz-se *exacto à direita*.

Teorema 12.3. *Seja A um anel comutativo e sejam $M, N, K \in \mathrm{Mod}_A$. Então existe um isomorfismo de módulos-A*

$$\alpha\colon \mathrm{Hom}_A(M \otimes_A N, K) \xrightarrow{\cong} \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, K))$$

dado por

$$\forall_{\mathbf{v}\in M}\, \forall_{\mathbf{w}\in N} \quad [\alpha(f)(\mathbf{v})]\,(\mathbf{w}) \coloneqq f(\mathbf{v}\otimes\mathbf{w}).$$

Demonstração. Verificamos que α está bem definido e tem inverso:

1. $\alpha(f)(\mathbf{v}) \in \mathrm{Hom}_A(N, K)$:
$$\begin{aligned}\alpha(f)(\mathbf{v})(a\mathbf{w} + a'\mathbf{w}') &= f(\mathbf{v}\otimes(a\mathbf{w}+b\mathbf{w}')) = af(\mathbf{v}\otimes\mathbf{w}) + a'f(\mathbf{v}\otimes\mathbf{w}')\\ &= a\,[\alpha(f)(\mathbf{v})]\,(\mathbf{w}) + a'\,[\alpha(f)(\mathbf{v})]\,(\mathbf{w}').\end{aligned}$$
2. $\alpha f \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, K))$: temos
$$\begin{aligned}\big(\alpha(f)(a\mathbf{v}+a'\mathbf{v}')\big)\,(\mathbf{w}) &= f\left((a\mathbf{v})\otimes\mathbf{w} + (a'\mathbf{v}')\otimes\mathbf{w}\right)\\ &= (a\alpha(f)(\mathbf{v}))\,(\mathbf{w}) + \big(a'\alpha(f)(\mathbf{v}')\big)\,(\mathbf{w}),\end{aligned}$$
   logo,
$$\alpha(f)(a\mathbf{v}+a'\mathbf{v}') = a\alpha(f)(\mathbf{v}) + a'\alpha(f)(\mathbf{v}').$$
3. $\alpha(af + a'f') = a\alpha(f) + a'\alpha(f')$.
4. α tem um inverso β definido por
$$\beta(g)(\mathbf{v}\otimes\mathbf{w}) = g(\mathbf{v})(\mathbf{w}),$$
   onde $g \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, K))$. Note-se que $\beta(g)$ está bem definida pois a a expressão acima é bilinear-A em $\mathbf{v}, \mathbf{w}$.

Onde se tomou sempre $a, a' \in A$, $f, f' \in \mathrm{Hom}_A(M \otimes_A N, K)$, $\mathbf{v}, \mathbf{v}' \in M$ e $\mathbf{w}, \mathbf{w}' \in N$. □

Observação 12.4. 1. Dado um módulo-A, N, a correspondência $M \mapsto \mathrm{Hom}_A(N, M)$ define um functor
$$H_N : \mathrm{Mod}_A \to \mathrm{Mod}_A \ .$$
   O teorema anterior, diz-nos que
$$\mathrm{Hom}_A(T_N(M), K) \cong \mathrm{Hom}_A(M, H_N(K)) \qquad \forall_{M,K\in\mathrm{Mod}_A}\ .$$
   Nestas condições, T_N e H_N dizem-se *functores adjuntos.*

2. Outro exemplo de um par de functores adjuntos já encontrado:
   F : Set $\to$ Mod_A dado por $X \mapsto F(X)$, onde $F(X)$ é o módulo-A livre gerado pelo conjunto X, é un functor (exercício). Como $F(X)$ também é um objecto livre na categoria Mod_A então, pela Definição 5.8,
$$\mathrm{Hom}_{\mathrm{Mod}_A}(F(X), M) \cong \mathrm{Hom}_{\mathrm{Set}}(X, E(M)) \qquad \forall_{X\in\mathrm{Set}}\forall_{M\in\mathrm{Mod}_A}\ ,$$
   onde $E : \mathrm{Mod}_A \to \mathrm{Set}$ é o functor esquecimento. Ou seja, F e E são functores adjuntos.

Exercícios

Nestes exercícios, A é um anel comutativo.

4.12.1. Seja N um módulo-A e considere a seguinte sucessão curta exacta de módulos-A

$$(*) \qquad 0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$$

Mostre que

$$0 \longrightarrow N \otimes_A M_1 \xrightarrow{\mathrm{id}\otimes f_1} N \otimes_A M_2 \xrightarrow{\mathrm{id}\otimes f_2} N \otimes_A M_3 \longrightarrow 0$$

é uma sucessão curta exacta de módulos-A se
(a) a sucessão $(*)$ cinde-se; ou
(b) N é um módulo-A livre; ou
(c) N é um módulo-A projectivo.

4.12.2. Seja M um módulo-A. Define-se o *dual* de M por

$$M^* := \mathrm{Hom}_A(M, A).$$

Mostre que M^* é um módulo-A com a soma $f + g$ e o produto por um escalar[6] af definidos respectivamente por

$$\begin{aligned} (f+g)(\mathbf{v}) &= f(\mathbf{v}) + g(\mathbf{v}) \\ (af)(\mathbf{v}) &= af(\mathbf{v}) \qquad\qquad \forall\, \mathbf{v} \in M\ , \end{aligned}$$

onde $f, g \in M^*$ e $a \in A$.

4.12.3. Seja M um módulo-A livre com uma base $\{\mathbf{e}_i\}_{i\in I}$. Seja $\mathbf{e}_i^* \in M^*$ (ver Exercício 4.12.2) definido por $\mathbf{e}_i^*(\mathbf{e}_j) = \delta_{ij}$, i.e., $\mathbf{e}_i^*(\mathbf{e}_j) = 1$ se $j = i$ e $\mathbf{e}_i^*(\mathbf{e}_j) = 0$ caso contrário.
(a) Mostre que $\{\mathbf{e}_i^*\}_{i\in I}$ é um conjunto linearmente independente em M^*.
(b) Mostre que, se I é finito, então $\{\mathbf{e}_i^*\}_{i\in I}$ é uma base de M^*.
(c) Através de um exemplo, mostre que $\{\mathbf{e}_i^*\}_{i\in I}$ pode não ser uma base de M^*, se I for um conjunto infinito.

4.12.4. Sejam M e N módulos-A. Mostre que $(M \otimes_A N)^* \cong \mathrm{Hom}_A(M, N^*)$ (ver exercício 4.12.2).

4.12.5. Sejam M e N módulos-A.
(a) Seja $\varphi \in M^*$ (ver exercício 4.12.2) e $\mathbf{w} \in N$. Mostre que $\alpha_{\varphi,\mathbf{w}} \colon M \to N$, dada por $\mathbf{v} \mapsto \varphi(\mathbf{v})\mathbf{w}$, é uma aplicação linear-A.
(b) Mostre que $\alpha \colon M^* \otimes_A N \to \mathrm{Hom}_A(M, N)$ dada por $\varphi \otimes \mathbf{w} \mapsto \alpha_{\varphi,\mathbf{w}}$ é uma aplicação linear-A.
(c) Mostre que, se M e N são módulos livres finitamente gerados, então a aplicação α da alínea anterior é um isomorfismo.
(d) Conclua que $(A^n)^* \otimes_A A^n \cong \mathrm{End}_A(A^n) \cong M_n(A)$. (Compare com o exemplo 11.19.)

[6] Se A não é um anel comutativo, o dual M^* de um módulo-A esquerdo M tem uma estrutura de módulo-A direito com o produto de $f \in M^*$ por um escalar $a \in A$ dado por $(fa)(\mathbf{v}) = f(\mathbf{v})a$. Recorde que, no caso comutativo, as noções de módulos esquerdos e direitos coincidem.

13. Extensão de escalares

Seja $\alpha\colon A \to B$ um homomorfismo de anéis comutativos. Então B admite uma estrutura de módulo-A, $A \times B \to B$, dada por $(a, b) \mapsto \alpha(a) \cdot b$. Um caso particular é considerar A um subanel de B e α a inclusão de A em B.

Definição 13.1. *Seja M um módulo-A. Define-se*

$$M_B \coloneqq B \otimes_A M,$$

com a estrutura de módulo-B dada por

$$(b', b \otimes \mathbf{v}) \mapsto (b'b) \otimes \mathbf{v}, \quad \forall\, b, b' \in B \quad \forall\, \mathbf{v} \in M.$$

Diz-se que M_B se obtém de M por extensão de escalares.

Proposição 13.2. *Se M é livre, então M_B é um módulo-B livre com dimensão* $\dim_B M_B = \dim_A M$. *Se $\{\mathbf{e}_i\}_{i\in I}$ é uma base de M, então $\{1_B \otimes \mathbf{e}_i\}_{i\in I}$ é uma base de M_B.*

Demonstração.

$$M \xrightarrow[\cong]{f} \bigoplus_{i\in I} A \Rightarrow M_B \xrightarrow[\cong]{T(\mathrm{id}_B, f)} B \otimes_A \Big(\bigoplus_{i\in I} A\Big) \cong \bigoplus_{i\in I} \big(B \otimes_A A\big) \cong \bigoplus_{i\in I} B. \qquad \square$$

Exemplo 13.3. Seja $A = \mathbb{R}$, $B = \mathbb{C}$, $\alpha\colon \mathbb{R} \to \mathbb{C}$ a inclusão e $M = \mathbb{R}[x]$. Como $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R} \cong \mathbb{C}$ e $\mathbb{R}[x] \cong \bigoplus_{i=0}^{\infty} \mathbb{R}$, temos

$$M_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[x] \cong \mathbb{C} \otimes_{\mathbb{R}} \Big(\bigoplus_{i=0}^{\infty} \mathbb{R}\Big) \cong \bigoplus_{i=0}^{\infty} \big(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}\big) \cong \bigoplus_{i=0}^{\infty} \mathbb{C} \cong \mathbb{C}[x].$$

Exemplo 13.4. O homomorfismo α não tem de ser injectivo. Seja $A = \mathbb{Z}$, $B = \mathbb{Z}_n$ e seja $\alpha\colon \mathbb{Z} \to \mathbb{Z}_n$ a projecção canónica. Então

$$M = \mathbb{Z}[x] \Rightarrow M_{\mathbb{Z}_n} \cong \mathbb{Z}_n[x].$$

Exercícios

4.13.1. (Duas mudanças de escalares.) Sejam A, B, C anéis comutativos e $\alpha\colon A \to B$, $\beta : B \to C$ homomorfismos de anéis. Se M é um módulo-A, mostre que $C \otimes_B (B \otimes_A M) \cong C \otimes_A M$ como módulos-C, i.e., $(M_B)_C \cong M_C$, onde a estrutura de módulo-B é induzida por α e as estruturas de de módulo-C são induzidas por β em M_B e por $\beta \circ \alpha$ em M.

4.13.2. (Restrição de escalares.) Sejam A, B anéis comutativos e $\alpha : A \to B$ um homomorfismo de anéis.

(a) Seja N um módulo-B. Mostre que $a \cdot \mathbf{v} \coloneqq \alpha(a)\mathbf{v}$, juntamente com a soma em N, define uma estrutura de módulo-A em N. Este módulo-A denota-se por $\mathrm{Res}_A^B N$.

(b) Mostre que

$$\mathrm{Hom}_B(B \otimes_A M, N) \cong \mathrm{Hom}_A(M, \mathrm{Res}_A^B N)$$

como módulos-B.

4.13.3. (Localização de módulos.) Seja A um anel comutativo e $S \subset A$ um subconjunto multiplicativo e considere o anel $S^{-1}A$. Dado um módulo-A M define-se

$$(\mathbf{v}, s) \sim (\mathbf{w}, r) \Leftrightarrow \exists\, x \in S \text{ tal que } x(s\mathbf{w} - r\mathbf{v}) = 0,$$

onde $(\mathbf{v}, s), (\mathbf{w}, r) \in M \times S$.

(a) Mostre que $\sim$ é uma relação de equivalência em $M \times S$.

(b) Denotamos por $\frac{\mathbf{v}}{s}$ a classe de equivalência de $(\mathbf{v}, s) \in M \times S$ e por $S^{-1}M$ o conjunto das classes de equivalência. Mostre que $S^{-1}M$ é um módulo-$S^{-1}A$ com as seguintes operações:

$$\frac{\mathbf{v}}{s} + \frac{\mathbf{w}}{r} := \frac{r\mathbf{v} + s\mathbf{w}}{sr} \qquad \text{e} \qquad \frac{a}{t} \cdot \frac{\mathbf{v}}{s} := \frac{a\mathbf{v}}{ts} \ ,$$

onde $\frac{\mathbf{v}}{s}, \frac{\mathbf{w}}{r} \in S^{-1}M$ e $\frac{a}{t} \in S^{-1}A$. (Em particular, não se esqueça de mostrar que as operações acima estão bem definidas.)

(c) Como $\varphi_S : A \to S^{-1}A$, $a \mapsto \frac{a}{1}$, é um homomorfismo de anés, $S^{-1}M$ tem também uma estrutura natural de módulo-A. Mostre que

$$\begin{aligned} \psi_S : M &\to S^{-1}M \\ \mathbf{v} &\mapsto \frac{\mathbf{v}}{1} \end{aligned}$$

é um homomorfismo de módulos-A tal que $\varphi_S(a)\psi_S(\mathbf{v}) = \psi_S(a\mathbf{v})$. Este homomorfismo ψ_S é o homomorfismo canónico da localização $S^{-1}M$.

4.13.4. Seja A um anel comutativo, $S \subset A$ um conjunto multiplicativo e M um módulo-A. Considere a localização $S^{-1}A$ de A e $S^{-1}M$ de M, e os respectivos homomorfismos canónicos $\varphi_S : A \to S^{-1}A$ e $\psi_S : M \to S^{-1}M$ – ver Exercício 4.13.3.

(a) Mostre que

$$\begin{aligned} \alpha : S^{-1}A \otimes_A M &\to S^{-1}M \\ \frac{a}{s} \otimes \mathbf{v} &\mapsto \frac{a\mathbf{v}}{s} \end{aligned}$$

está bem definido e é um isomorfismo de módulos-$S^{-1}A$.

(b) Seja

$$\begin{aligned} \phi_{S^{-1}A,M} : M &\to S^{-1}A \otimes_A M \\ \mathbf{v} &\mapsto \varphi_S(1) \otimes \mathbf{v} = \frac{1}{1} \otimes \mathbf{v} \ , \end{aligned}$$

o homomorfismo associado à extensão de escalares induzida por φ_S. Mostre que $\alpha \circ \phi_{S^{-1}A,M} = \psi_S$.

14. Módulos sobre domínios integrais

No que se segue D é um domínio integral.

Proposição 14.1. *Seja M um módulo-D. Então*

$$\operatorname{Tor} M \coloneqq \{\mathbf{v} \in M \mid \exists\, a \in D \setminus \{0\} : a\mathbf{v} = 0\}$$

é um submódulo de M.

Demonstração. Sejam $\mathbf{v}, \mathbf{v}' \in \operatorname{Tor} M$ e $d, d' \in D \setminus \{0\}$ *t.q.*

$$d\mathbf{v} = d'\mathbf{v}' = 0.$$

Temos $dd' \neq 0$ e $dd'(\mathbf{v} - \mathbf{v}') = d'(d\mathbf{v}) - d(d'\mathbf{v}') = 0$, portanto $\operatorname{Tor} M$ é um subgrupo de M. Dado $d'' \in D$ temos $d''\mathbf{v} \in \operatorname{Tor} M$, pois $(d''d)\mathbf{v} = 0$. Concluímos que $\operatorname{Tor} M$ é um submódulo de M. □

Exemplos 14.2.

1. Se $D = k$ é um corpo e $M \in \operatorname{Vect}_k$, então $\operatorname{Tor} M = \{0\}$;
2. se $D = \mathbb{Z}$ e $M = \mathbb{Z}_n$, então $\operatorname{Tor} M = \mathbb{Z}_n$;
3. se $D = \mathbb{Z}$ e $M = \mathbb{Z}^n$, então $\operatorname{Tor} M = \{0\}$;
4. se $D = \mathbb{Z}$ e $M = \mathbb{Q}$, então $\operatorname{Tor} M = \{0\}$;
5. se $D = k[x]$, $M = V \in \operatorname{Vect}_k$ e $T \in \operatorname{End}_k(V) \coloneqq \operatorname{Hom}_k(V, V)$, então V tem uma estrutura de módulo-D dada por:

$$f(x) \cdot \mathbf{v} \coloneqq \sum_{i=0}^{n} a_i T^i \mathbf{v},$$

onde $f(x) = \sum_{i=0}^{n} a_i x^i$. Se $\dim_k V$ é finita, temos $V = \operatorname{Tor}_{k[x]} V$ – Exercício 4.14.1.

Definição 14.3. *Se $M \in \operatorname{Mod}_D$ é* t.q. $\operatorname{Tor} M = M$*, diz-se que M é um* módulo de torção*. Se $\operatorname{Tor} M = \{0\}$, diz-se que M é um módulo* livre de torção*.*

Exemplo 14.4. Seja G um grupo abeliano, i.e., um módulo-$\mathbb{Z}$. Então

$$g \in \operatorname{Tor} G \Leftrightarrow \exists\, n \in \mathbb{Z} \setminus \{0\} \text{ tal que } ng = 0 \Leftrightarrow n \mid |g|.$$

Ou seja, $\operatorname{Tor} G = \{g \in G \,|\, |g| \text{ é finita}\}$. Portanto

- G é um grupo abeliano livre de torção sse qualquer elemento não nulo tem ordem infinita;
- G é um grupo abeliano de torção sse todos os elementos têm ordem finita.

Observação 14.5. Um módulo pode ser livre de torção sem ser livre: $\mathbb{Q}$ é um módulo-$\mathbb{Z}$ livre de torção e não é livre, pois, para todo $p, q \in \mathbb{Q}$, o conjunto $\{p, q\}$ é linearmente dependente.

Proposição 14.6.

(a) Seja $\phi \in \operatorname{Hom}_D(M_1, M_2)$, então

$$\phi(\operatorname{Tor} M_1) \subset \operatorname{Tor} M_2.$$

Se ϕ é injectiva, então $\phi(\operatorname{Tor} M_1) = (\operatorname{Tor} M_2) \cap \operatorname{im} \phi$. Se ϕ é sobrejectiva e $\ker \phi \subset \operatorname{Tor} M_1$, então $\phi(\operatorname{Tor} M_1) = \operatorname{Tor} M_2$.

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

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

$$\operatorname{Tor}\Big(\bigoplus_{i \in I} M_i\Big) = \bigoplus_{i \in I} \operatorname{Tor} M_i.$$

Demonstração. (a) Temos

$$a\mathbf{v} = 0 \Rightarrow a\phi(\mathbf{v}) = 0,$$

logo $\phi(\operatorname{Tor} M_1) \subset \operatorname{Tor} M_2$.

Se ϕ é injectiva e $\mathbf{w} = \phi(\mathbf{v})$, $a\mathbf{w} = 0$, então

$$a\mathbf{w} = \phi(a\mathbf{v}) = 0 \Rightarrow a\mathbf{v} = 0 \Rightarrow \mathbf{v} \in \operatorname{Tor} M_1.$$

Se ϕ é sobrejectiva e $\ker\phi \subset \operatorname{Tor} M_1$, e $\mathbf{w} \in \operatorname{Tor} M_2$ é *t.q.* $a\mathbf{w} = 0$ e $\mathbf{w} = \phi(\mathbf{v})$, então:

$$\begin{aligned}\phi(a\mathbf{v}) = 0 &\Rightarrow a\mathbf{v} \in \operatorname{Tor} M_1\\ &\Rightarrow \exists\, b \in D \setminus \{0\} \text{ tal que } ba\mathbf{v} = 0\\ &\Rightarrow \mathbf{v} \in \operatorname{Tor} M_1 \quad (\text{pois } ba \neq 0).\end{aligned}$$

(b) Como $\pi\colon M \to M/\operatorname{Tor} M$ é sobrejectiva e $\ker\pi = \operatorname{Tor} M$, temos, por (a),

$$\operatorname{Tor}\left(\frac{M}{\operatorname{Tor} M}\right) = \pi(\operatorname{Tor} M) = \{0\}.$$

(c) Segue directamente da definição de Tor e da soma directa – Exercício 4.14.2. □

Definição 14.7. *Seja $K = \operatorname{Frac}(D)$ o corpo de fracções de D. Note-se que K é um módulo-D. Dado $M \in Mod_D$, definimos*

$$M_K \coloneqq K \otimes_D M \in \operatorname{Vect}_K .$$

Ou seja, M_K é o módulo-K obtido de M por extensão de escalares. Denotamos por $\phi_{K,M}$ (ou simplesmente ϕ, se não houver risco de confusão) o homomorfismo natural de módulo-D dado por

$$\phi\colon M \to M_K; \mathbf{v} \mapsto 1 \otimes \mathbf{v}.$$

Exemplo 14.8. Sejam $D = \mathbb{Z}$ e $M = \mathbb{Z}^n$, então $M_{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \mathbb{Q}^n$.

Proposição 14.9. *Seja $M \in \operatorname{Mod}_D$. Então*

(a) $K \otimes_D \operatorname{Tor} M = 0$;

(b) $K \otimes_D (M/\operatorname{Tor} M) \cong K \otimes_D M$;

(c) Se $N \subset M$ é um submódulo tal que M/N é um módulo de torção, então $K \otimes_D N \cong K \otimes_D M$

Demonstração. (a) Exercício.

(b) Seja $\pi : M \to M/\operatorname{Tor} M$ a projecção canónica e $i : \operatorname{Tor} M \to M$ a inclusão. Então

$$0 \longrightarrow \operatorname{Tor} M \xrightarrow{\ i\ } M \xrightarrow{\ \pi\ } M/\operatorname{Tor} M \longrightarrow 0$$

é uma sucessão exacta, logo

$$K \otimes_D \operatorname{Tor} M \xrightarrow{\mathrm{id}\otimes i} K \otimes_D M \xrightarrow{\mathrm{id}\otimes\pi} K \otimes_D (M/\operatorname{Tor} M) \longrightarrow 0$$

também é uma sucessão exacta de módulos-D, pelo Teorema 12.1. Como $K \otimes_D \operatorname{Tor} M = 0$, por (a), concluimos que $\mathrm{id}\otimes\pi$ é um isomorfismo de módulos-D.

(c) Seja $i : N \to M$ a inclusão. Então $\alpha = \mathrm{id}\otimes i : K \otimes_D N \to K \otimes_D M$ é um homomorfismo de módulos-D. Para mostrar que α é um isomorfismo, construimos o seu inverso. Seja $\beta' : K \times M \to K \otimes_D N$ dado por

$$\beta'(x, \mathbf{m}) = \frac{x}{a} \otimes a\mathbf{m}$$

onde $a \in D \setminus \{0\}$ é tal que $a\mathbf{m} \in N$ – existe um elemento a nestas condições pois M/N é um módulo de torção. Verifique que $\beta'(x, \mathbf{m})$ não depende da escolha de a e que β' é uma aplicação bilinear. Portanto, existe um homomorfismo $\beta : K \otimes_D M \to K \otimes_D N$ tal que $\beta(x \otimes \mathbf{m}) = \beta'(x, \mathbf{m})$. Temos que $\alpha \circ \beta = \mathrm{id}_{K\otimes_D M}$ e $\beta \circ \alpha = \mathrm{id}_{K\otimes_D N}$, donde concluimos que α é um isomorfismo. □

Exemplo 14.10. Seja $D = \mathbb{Z}[\sqrt{10}]$ e considere o ideal $I = (2, \sqrt{10})$. Portanto I é um submódulo do módulo D, cujo quociente D/I é um módulo de torção porque

$$2(a + b\sqrt{10} + I) = I = 0_{D/I} \quad \forall\, a, b \in \mathbb{Z}$$

e $2 \in \mathbb{Z} \setminus \{0\}$. Pela Proposição 14.9(c), temos que $K \otimes_D I \cong K \otimes_D D \cong K$. Note, no entanto, que $I \ncong D$, pois I não é um módulo-D livre.

A proposição anterior usa apenas a estrutura de módulo-D dada pela construção do produto tensorial. Na próxima proposição já se explora a estrutura adicional de M_K como espaço vectorial sobre K.

Proposição 14.11. *Seja $M \in \mathrm{Mod}_D$ e seja $\phi = \phi_{K,M} \colon M \to M_K$. Então, temos:*

(a) $\forall\, \mathbf{w} \in M_K \,\exists\, d \in D \,\exists\, \mathbf{v} \in M : \mathbf{w} = \frac{1}{d}\phi(\mathbf{v})$;

(b) $\ker \phi = \mathrm{Tor}\, M$.

Demonstração. (a)

$$\begin{aligned}
\mathbf{w} = \sum_{i=1}^{n} \frac{a_i}{b_i} \otimes \mathbf{v}_i &= \frac{1}{b_1 \cdots b_n} \sum_{i=1}^{n} \Big(a_i \prod_{j \neq i} b_j \Big) \otimes \mathbf{v}_i \\
&= \frac{1}{b_1 \cdots b_n} \sum_{i=1}^{n} 1 \otimes \Big(\Big(a_i \prod_{j \neq i} b_j \Big) \mathbf{v}_i \Big) \\
&= \frac{1}{b_1 \cdots b_n} \Big(1 \otimes \Big(\sum_{i=1}^{n} \Big(a_i \prod_{j \neq i} b_j \Big) \mathbf{v}_i \Big) \Big) \in \frac{1}{b_1 \cdots b_n}\, \phi(M).
\end{aligned}$$

(b) A inclusão $\mathrm{Tor}\, M \subset \ker \phi$ é óbvia: se $b \in D \setminus \{0\}$ é *t.q.* $b\mathbf{v} = 0$, então

$$\phi(\mathbf{v}) = 1 \otimes \mathbf{v} = b(b^{-1} \otimes \mathbf{v}) = b^{-1} \otimes (b\mathbf{v}) = 0.$$

Para a inclusão inversa, ver o Exercício 4.14.7. □

Definição 14.12. *Seja $M \in \mathrm{Mod}_D$ e seja $S \subset M$ um subconjunto. Define-se a* característica *de S como* $\dim_K \langle \phi(S) \rangle$. *Em particular, a* característica *de M é* $\mathrm{rank}\, M := \dim_K M_K$.

Observação 14.13. Se M é finitamente gerado, então M tem característica finita, pois

$$\dim_K \langle \phi(S) \rangle \leq |S| \ .$$

Exemplos 14.14. 1. $\mathbb{Z}_n$ é um módulo-$\mathbb{Z}$ de característica zero.

2. Mais geralmente, se M é um módulo-D de torção, então M tem característica zero.

3. $\mathbb{Q}$ é um módulo-$\mathbb{Z}$ de característica 1: $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ (ver Exercício 4.11.1). No entanto, $\mathbb{Q}$ não é finitamente gerado como grupo abeliano.

Lema 14.15. *Seja $M \in \mathrm{Mod}_D$, então $\{\mathbf{e}_i\}_{i \in I} \subset M$ é* l.i. sse *$\{1 \otimes \mathbf{e}_i\}_{i \in I} \subset M_K$ é* l.i..

Demonstração. Seja $\psi \colon \bigoplus_{i \in I} D \to M; \psi\left((a_i)_{i \in I}\right) = \sum_{i \in I} a_i \mathbf{e}_i$. Consideremos a composta

$$\bigoplus_{i \in I} D \xrightarrow{\psi} M \xrightarrow{\phi} M_K.$$

Temos

1. $\{1 \otimes \mathbf{e}_i\}_{i \in I}$ é *l.i. sse* $\phi \circ \psi$ é mono:

$$\sum_i \frac{a_i}{b_i}(1 \otimes \mathbf{e}_i)) = 0 \Leftrightarrow \frac{1}{b} \sum_i a_i'(1 \otimes \mathbf{e}_i) = 0 \Leftrightarrow \frac{1}{b}\, \phi \circ \psi \left((a_i')_{i \in I} \right) = 0,$$

onde $b = b_1 \cdots b_n$ e $a_i' = a_i \prod_{j \neq i} b_j$.

2. $\phi \circ \psi$ é mono *sse*:

$$\begin{aligned} \psi \text{ é mono} \wedge \Big(\operatorname{im}\psi \cap \underbrace{\ker \phi}_{\operatorname{Tor} M} = \{0\} \Big) \quad &\Leftrightarrow \quad \psi \text{ é mono} \wedge \Big(\operatorname{Tor}\Big(\bigoplus_{i\in I} D \Big) = \{0\} \Big) \\ &\Leftrightarrow \quad \psi \text{ é mono} \\ &\Leftrightarrow \quad \{\mathbf{e}_i\}_{i\in I} \text{ é } \textit{l.i.} \end{aligned}$$

onde $\ker \phi = \operatorname{Tor} M$ pela Proposição 14.11. □

Exercícios

4.14.1. Seja k um corpo, $V \in \operatorname{Vect}_k$ e $T \in \operatorname{End}_k(V)$. Considere a estrutura de módulo-$k[x]$ em V descrita no Exemplo 14.2.5, i.e., com o produto por escalres de $k[x]$ induzido por $x \cdot \mathbf{v} \coloneqq T(\mathbf{v})$, para $\mathbf{v} \in V$. Se $\dim_k V = n$ é finita, mostre que $\operatorname{Tor}_{k[x]} V = V$.
Sugestão: Considere os vectores $\mathbf{v}, T(\mathbf{v}), \ldots, T^n(\mathbf{v})$.

4.14.2. Demosntre a Proposição 14.6(c), i.e., se $\{M_i\}_{i\in I}$ é uma família de módulos-D, mostre que $\operatorname{Tor}\Big(\bigoplus_{i\in I} M_i \Big) = \bigoplus_{i\in I} \operatorname{Tor} M_i$.

4.14.3. Sejam M_i módulos-D, $i \in I$.
(a) Mostre que $\operatorname{Tor}\big(\prod_{i\in I} M_i \big) \subset \prod_{i\in I} \operatorname{Tor}(M_i)$.
(b) Será sempre verdade que $\operatorname{Tor}\big(\prod_{i\in I} M_i \big) = \prod_{i\in I} \operatorname{Tor}(M_i)$?

4.14.4. Considere a seguinte sucessão curta exacta em Mod_D

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0 \ .$$

(a) Mostre que

$$0 \longrightarrow \operatorname{Tor} M \xrightarrow{f|_{\operatorname{Tor} M}} \operatorname{Tor} N \xrightarrow{g|_{\operatorname{Tor} N}} \operatorname{Tor} P$$

é uma sucessão exacta.
(b) Dê um exemplo de um homomorfismo sobrejectivo $g : M \to P$ tal que a restrição $g|_{\operatorname{Tor} N} : \operatorname{Tor} N \to \operatorname{Tor} P$ não é sobrejectiva.

4.14.5. Demonstre a Proposição 14.9(a).

4.14.6. Seja D um domínio integral e seja M um módulo-D livre. Mostre que M é livre de torção. Através de um contra-exemplo, mostre que o recíproco é falso.

4.14.7. Seja D um domínio integral com corpo de fracções $K = \operatorname{Frac}(D)$ e seja M um módulo-D. Recorde que $\operatorname{Frac}(D) = S^{-1}D$ com $S = D \setminus \{0\}$, e considere o espaço vectorial-K $N = S^{-1}M$ – ver Exercício 4.13.3.
(a) Seja $\psi_S : M \to S^{-1}M$ o homomorfismo canónico dado por $\mathbf{v} \mapsto \frac{\mathbf{v}}{1}$. Mostre que $\ker \psi_S = \operatorname{Tor} M$.
(b) Conclua que $\ker \phi = \operatorname{Tor} M$, onde $\phi = \phi_{K,M} \colon M \to K \otimes_D M; \mathbf{v} \to 1 \otimes \mathbf{v}$.
Sugestão: Exercício 4.13.4.

15. Módulos sobre um *d.i.p.*

No que se segue D é um *d.i.p.*.

15.1. Matrizes com entradas num *d.i.p.*

Seja $A \in M_{m\times n}(D)$ e considere as seguintes operações elementares representadas por matrizes invertíveis:

- (i) trocar as colunas (linhas) i, j;
- (ii) multiplicar uma coluna (linha) por uma unidade;
- (iii) somar um múltiplo de uma coluna (linha) a outra;
- (iv) substituir as colunas (linhas) a_i e a_j pelas novas colunas[7] (resp. linhas) a'_i e a'_j *t.q.* $a'_{1i} = \mathrm{MDC}(a_{1i}, a_{1j})$ e $a'_{1j} = 0$ (resp. $a'_{i1} = \mathrm{MDC}(a_{i1}, a_{j1})$ e $a'_{j1} = 0$).[8]

Para mostrar que é possível efectuar a operação (iv), basta considerar o caso ilustrado no exemplo seguinte.

Exemplo 15.1. Sejam $A = \begin{bmatrix} a & b \end{bmatrix}$, $d = \mathrm{MDC}(a, b)$, r, s, a', b' *t.q.*

$$d = ar + bs, \quad a' = a/d, \quad b' = b/d.$$

Em particular, $1 = a'r + b's$, logo

$$Q = \begin{bmatrix} r & -b' \\ s & a' \end{bmatrix} \in GL_2(D)$$

pois $\det Q = a'r + b's \in D^\times$. Temos

$$AQ = \begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} r & -b' \\ s & a' \end{bmatrix} = \begin{bmatrix} d & d(a'b' - b'a') \end{bmatrix} = \begin{bmatrix} d & 0 \end{bmatrix}.$$

Definição 15.2. *Seja $d \in D \setminus \{0\}$, definimos $\delta(d) \in \mathbb{N}$ como o número de factores primos de uma factorização de d em irredutíveis, contado com multiplicidade, se $d \notin D^\times$; e definimos $\delta(d) = 0$, se $d \in D^\times$.*

Observação 15.3. Se $a, d \in D$ são *t.q.* $d \mid a$ e $a \nsim d$, então $\delta(d) < \delta(a)$.

Exemplo 15.4. Seja $D = \mathbb{Z}$. Seja

$$A = \begin{bmatrix} 4 & 6 \\ 6 & 13 \end{bmatrix}.$$

Aplicando a operação (iv) às colunas de A e, usando a matriz Q do exemplo anterior, fica

$$Q = \begin{bmatrix} -1 & -3 \\ 1 & 2 \end{bmatrix} \qquad \text{e} \qquad B \coloneqq AQ = \begin{bmatrix} 2 & 0 \\ 7 & 8 \end{bmatrix}.$$

Aplicando agora a operação (iv) às linhas de B, temos que

$$d = 1\,, \quad a' = a/d = 2\,, \quad b' = b/d = 7\,, \quad (-3)2 + 7 = 1 \Rightarrow r = -3 \text{ e } s = 1$$

donde

$$P = \begin{bmatrix} r & s \\ -b' & a' \end{bmatrix} = \begin{bmatrix} -3 & 1 \\ -7 & 2 \end{bmatrix} \qquad \text{e} \qquad PB \coloneqq PAQ = \begin{bmatrix} 1 & 8 \\ 0 & 16 \end{bmatrix}.$$

Note que a entrada $(1, 2)$ de B é zero como resultado da operação (iv) aplicada às colunas, mas após a aplicação de (iv) nas linhas, essa entrada deixou de ser nula.

Note também que, na entrada $(1, 1)$ foi-se obtendo sucessivamente $4 \mapsto 2 \mapsto 1$ e que $\delta(4) = 2 > \delta(2) = 1 > \delta(1) = 0$.

[7] obtidas por combinação linear de a_i e a_j

[8] as restantes colunas (linhas) permanecem inalteradas.

Observação 15.5. Anteriormente, apenas se definiu o símbolo $a \mid b$ num anel comutativo A para $a, b \in A \setminus \{0\}$. Uma vez que $a0 = 0$ para todo o $a \in D$, por convenção, vamos escrever $a \mid 0$ e, em particular, $0 \mid 0$.

Proposição 15.6. *Seja $A \in M_{m\times n}(D)$, então existem $P \in M_m(D)$ e $Q \in M_n(D)$, invertíveis,* t.q. *PAQ é diagonal:*

$$PAQ = \operatorname{diag}(d_1, \cdots, d_r) = \sum_{i=1}^{r} d_i E_{ii},$$

onde $d_1 \mid \cdots \mid d_r$ e E_{ii} é a matriz $(\delta_{ti}\delta_{si})_{1\le t\le m, 1\le s\le n}$ e $r = \min\{n, m\}$.

Demonstração. Basta demonstrar que se pode obter uma matriz diagonal a partir de A com as operações elementares (i) a (iv) definidas anteriormente.

Descrevemos de seguida um procedimento iterativo para diagonalizar A.

Passo 1. Pôr um elemento não nulo na entrada $(1, 1)$ de A (pode ser feito aplicando a operação (i) para linhas e colunas) se $A \neq 0$, e terminar o algoritmo se $A = 0$;

Passo 2. Usar a operação (iv) até que, para todo o k, $a_{11} \mid a_{1k}$ e $a_{11} \mid a_{k1}$.
NOTA: cada vez que a_{11} muda em resultado da aplicação da operação (iv), $\delta(a_{11})$ diminui. Logo, ao fim de um número finito de aplicações da operação (iv) obtém-se uma matriz cuja entrada a_{11} satisfaz $a_{11} \mid a_{1k}$ e $a_{11} \mid a_{k1}$.

Passo 3. Usar as operações (ii) e (iii) para obter uma matriz da forma

$$\begin{bmatrix} d_1^1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{bmatrix},$$

onde A_1 é uma matriz $(m-1)\times(n-1)$. De seguida podemos aplicar o mesmo procedimento à matriz A_1. Assim, aplicando sucessivamente os passos acima, obtemos uma matriz da forma

$$\begin{bmatrix} d_1^1 & 0 & \cdots & 0 \\ 0 & d_2^1 & 0 & \cdots \\ \vdots & 0 & \ddots & \end{bmatrix} = \operatorname{diag}(d_1^1, \ldots, d_1^r),$$

onde as entradas nulas d_i^1, se as houver, aparecem no fim da lista – consequência do Passo 1.

Falta apenas satisfazer a condição $d_1^1 \mid d_2^1 \mid \cdots \mid d_r^1$. Consideremos a seguinte sequência de operações elementares[9]:

$$\begin{bmatrix} d_1^1 & 0 & \cdots & 0 \\ 0 & d_2^1 & 0 & \cdots \\ \vdots & 0 & \ddots & \end{bmatrix} \xrightarrow{(iii)} \begin{bmatrix} d_1^1 & d_2^1 & \cdots & 0 \\ 0 & d_2^1 & 0 & \cdots \\ \vdots & 0 & \ddots & \end{bmatrix} \xrightarrow{(iv)+(iii)} \begin{bmatrix} d_1^2 & 0 & \cdots & 0 \\ 0 & d_2^2 & 0 & \cdots \\ \vdots & 0 & \ddots & \end{bmatrix}$$

Obtemos $d_1^2 \mid d_2^2$. De seguida, aplicando o mesmo procedimento às linhas 1 e 3, obtemos uma matriz diagonal $\operatorname{diag}(d_1^3, d_2^3, d_3^3, \cdots)$ *t.q.* $d_1^3 \mid d_2^3$ e $d_1^3 \mid d_3^3$. Prosseguindo, obtemos uma matriz $\operatorname{diag}(d_1^r, \ldots, d_r^r)$ *t.q.* $d_1^r \mid d_i^r$, para todo o i. Definimos $d_1 \coloneqq d_1^r$. De seguida, consideramos a matriz $\operatorname{diag}(d_2^r, \cdots, d_r^r)$ e aplicamos o mesmo algoritmo. O processo termina com uma matriz diagonal $\operatorname{diag}(d_1, \ldots, d_r)$ *t.q.* $d_1 \mid d_2 \mid \cdots \mid d_r$. □

Definição 15.7. *Seja $A \in M_{m\times n}(D)$ e seja* $\operatorname{diag}(d_1, \ldots, d_r)$ *uma matriz obtida por diagonalização de A, como acima, diz-se que $d_1, \ldots, d_r$ são* factores invariantes *de A.*

Pode mostrar-se que os factores invariantes são únicos a menos de multiplicação por unidades e que duas matrizes são semelhantes *sse* têm os mesmos factores invariantes.

[9] Faça os passos intermédios e determine expressões para d_1^2 e d_2^2 à custa de d_1^1 e d_2^1 – Exercício 4.15.1. Essas expressões vão permitir justificar que $d_1^2 \mid d_2^2$ e todas as relações de divisibilidade no resto desta demonstração.

Corolário 15.8. *Seja $f \in \mathrm{Hom}_D(D^n, D^m)$. Então existem bases de D^n e de D^m em relação às quais f é representada por uma matriz diagonal.*

Demonstração. Recorde-se que $\mathrm{Hom}_D(D^n, D^m) \cong M_{m\times n}(D^{op})$. Seja $A \in M_{m\times n}(D^{op})$ a matriz que representa f relativamente às bases canónicas de D^m e D^n. Sejam $P \in \mathrm{GL}_m(D)$ e $Q \in \mathrm{GL}_n(D)$ como na Proposição 15.6 e sejam $\mathcal{B} \subset D^n$, $\mathcal{B}' \subset D^m$ os conjuntos de vectores colunas de Q^{-1} e P, respectivamente. Então, relativamente às bases $\mathcal{B}$ e $\mathcal{B}'$ o homomorfismo f é representado por PAQ. □

Exemplo 15.9. Pretendemos diagonalizar a matriz

$$A = \begin{bmatrix} 2 & -1 \\ 1 & 2 \\ 1 & 1 \end{bmatrix} \in M_{3\times 2}(\mathbb{Z}),$$

o que pode ser conseguido aplicando as operações elementares:

$$\begin{bmatrix} 2 & -1 \\ 1 & 2 \\ 1 & 1 \end{bmatrix} \xrightarrow{L1\leftrightarrow L2} \begin{bmatrix} 1 & 2 \\ 2 & -1 \\ 1 & 1 \end{bmatrix} \xrightarrow{C2-2C1} \begin{bmatrix} 1 & 0 \\ 2 & -5 \\ 1 & -1 \end{bmatrix}$$

$$\xrightarrow[L3-L1]{L2-2L1} \begin{bmatrix} 1 & 0 \\ 0 & -5 \\ 0 & -1 \end{bmatrix} \xrightarrow{L2\leftrightarrow L3} \begin{bmatrix} 1 & 0 \\ 0 & -1 \\ 0 & -5 \end{bmatrix} \xrightarrow{L3-5L2} \begin{bmatrix} 1 & 0 \\ 0 & -1 \\ 0 & 0 \end{bmatrix},$$

onde usámos a seguinte notação para legendar as operações:

$Li \leftrightarrow Lj$ = trocar as linhas i e j;

$Ci \leftrightarrow Cj$ = trocar as colunas i e j;

$Li + \lambda Lj$ = somar à linha i λ vezes a linha j;

$Ci + \lambda Cj$ = somar à coluna i λ vezes a coluna j.

As matrizes P, Q da Proposição 15.6 são:

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -5 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 3 & -5 \end{bmatrix} \quad \text{e} \quad Q = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}.$$

Obtivemos assim uma matriz diagonal

$$PAQ = \begin{bmatrix} 1 & 0 \\ 0 & -1 \\ 0 & 0 \end{bmatrix},$$

equivalente a A.

Exemplo 15.10. Pretendemos diagonalizar a matriz

$$A = \begin{bmatrix} (t-2)(t-1) & t-2 \\ (t-1)^3 & (t-2)(t-1) \end{bmatrix} \in M_2(\mathbb{R}[t]),$$

o que pode ser conseguido realizando a seguinte sequência de operações elementares:

$$A \xrightarrow{C2\leftrightarrow C1} \begin{bmatrix} t-2 & (t-2)(t-1) \\ (t-2)(t-1) & (t-1)^3 \end{bmatrix} \xrightarrow{L2-(t-1)L1} \begin{bmatrix} t-2 & (t-2)(t-1) \\ 0 & (t-1)^2 \end{bmatrix}$$

$$\xrightarrow{C2-(t-1)C1} \begin{bmatrix} t-2 & 0 \\ 0 & (t-1)^2 \end{bmatrix} \xrightarrow{L1+L2} \begin{bmatrix} t-2 & (t-1)^2 \\ 0 & (t-1)^2 \end{bmatrix}$$

$$\xrightarrow{C2-tC1} \begin{bmatrix} t-2 & 1 \\ 0 & (t-1)^2 \end{bmatrix} \xrightarrow{C1\leftrightarrow C2} \begin{bmatrix} 1 & t-2 \\ (t-1)^2 & 0 \end{bmatrix}$$

$$\xrightarrow{L2-(t-1)^2L1} \begin{bmatrix} 1 & t-2 \\ 0 & -(t-2)(t-1)^2 \end{bmatrix} \xrightarrow{C2-(t-2)C1} \begin{bmatrix} 1 & 0 \\ 0 & -(t-2)(t-1)^2 \end{bmatrix}.$$

Teorema 15.11. *Sejam D um* d.i.p.*, $N \in \mathrm{Mod}_D$ livre e $M \subset N$ um submódulo. Então M é livre e satisfaz $\dim_D M \leq \dim_D N$ (convencionamos que o módulo trivial $\{0\}$ é livre de dimensão zero).*

Demonstração. Demonstramos apenas o caso em que N é finitamente gerado. Podemos supor $N = D^n$. Seja $\pi_i \colon D^n \to D$ a i-ésima projecção e seja $p_i \coloneqq \pi_i|_M$. Então $\ker p_i \subset \ker \pi_i = D^{n-1}$. Demonstramos o resultado por indução em n:

- se $n = 0$, não há nada a provar;
- suponhamos que o teorema é válido para $n-1$. A sucessão

$$0 \to \ker p_n \to M \to \operatorname{im} p_n \to 0 \tag{15.1}$$

é exacta. Como $\operatorname{im} p_n \subset D$ é um submódulo, existe $d \in D$ *t.q.* $\operatorname{im} p_n = (d)$. Se $d = 0$, temos $(d) = (0)$ e $M \cong \ker p_n \subset D^{n-1}$, logo M é livre. Se $d \neq 0$, então $(d) \cong D$, logo (15.1) cinde-se e temos

$$M \cong \ker p_n \oplus \operatorname{im} p_n \cong \ker p_n \oplus D.$$

Por hipótese, $\ker p_n$ é livre e $\dim_D \ker p_n \leq n-1$, donde o resultado segue. □

Corolário 15.12. *Seja M um módulo-D finitamente gerado. Então existe uma sucessão curta exacta da seguinte forma:*

$$0 \longrightarrow D^n \xrightarrow{f} D^m \xrightarrow{g} M \longrightarrow 0.$$

Demonstração. Seja $g \colon D^m \to M$ um epimorfismo. Temos $\ker g \subset D^m$, logo $\ker g \cong D^n$ para algum n. □

Definição 15.13. *Seja $g \colon D^m \to M$ um epimorfismo. Diz-se que $(D^m, \ker g)$ é uma* apresentação *de M.*

Note-se que $M \cong D^m / \ker g$. O Corolário 15.12 garante a existência de uma apresentação livre (*i.e.*, tal que $\ker g$ é livre).

Exercícios

4.15.1. Considere as seguintes operações elementares

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \xrightarrow{(iii)} \begin{bmatrix} a & b \\ 0 & b \end{bmatrix} \xrightarrow{(iv)+(iii)} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$$

onde (iv) é aplicado às colunas. Obtenha expressões para c, d à custa de a, b e conclua que $c \mid d$. Repita o exercício para matrizes diagonais 3×3.

4.15.2. Determine os factores invariantes das seguintes matrizes de entradas em $\mathbb{Z}$:

$$A = \begin{bmatrix} 12 & 0 & 0 & 0 \\ 0 & 20 & 0 & 0 \\ 0 & 0 & 150 & 0 \\ 0 & 0 & 0 & 18 \end{bmatrix} \qquad \text{e} \qquad B = \begin{bmatrix} 4 & 2 & -2 \\ 2 & -10 & 6 \end{bmatrix}$$

4.15.3. Demonstre o Teorema 15.11 no caso geral, i.e., quando N não é necessariamente finitamente gerado.

16. Classificação de módulos finitamente gerados sobre *d.i.p.*

Antes de prosseguir o estudo dos módulos sobre *d.i.p.*, necessitamos da seguinte definição geral sobre módulos.

Definição 16.1. *Sejam A um anel, $M \in \mathrm{Mod}_A$ e seja $\mathbf{v} \in M$. Define-se o* aniquilador *de $\mathbf{v}$ por*

$$\mathrm{ann}(\mathbf{v}) \coloneqq \{a \in A \mid a\mathbf{v} = 0\}.$$

Então $\mathrm{ann}(\mathbf{v}) \subset A$ *é um ideal esquerdo* t.q. $A/\mathrm{ann}(\mathbf{v}) \cong \langle \mathbf{v} \rangle$.

Teorema 16.2. *Seja D um* d.i.p. *e seja M um módulo-D* finitamente gerado. *Então, existem $d_1, \ldots, d_m \in D$* t.q.

$$M \cong \frac{D}{(d_1)} \oplus \cdots \oplus \frac{D}{(d_m)},$$

e $(d_1) \supset (d_2) \supset \cdots \supset (d_m)$. Os ideais $(d_1), \ldots, (d_m)$ são unicamente determinados por M.

Demonstração. Podemos supor $M = D^m/\mathrm{im}(f)$, onde $f\colon D^n \to D^m$, $m \geq n$, é representado por uma matriz $A = \mathrm{diag}(d_1, \ldots, d_n)$ *t.q.* $d_1 \mid d_2 \mid \cdots \mid d_n$ (Corolário 15.12 e Proposição 15.6) e seja $d_i = 0$ para $i > n$.

Seja $\pi\colon D^m \to M$ a projecção e seja

$$\mathbf{v}_i \coloneqq \pi(\mathbf{e}_i),$$

onde $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ é a base canónica de D^m. Mostramos de seguida que $\langle \mathbf{v}_i \rangle \cong D/(d_i)$ e $M = \bigoplus_{i=1}^m \langle \mathbf{v}_i \rangle$:

1. $\langle \mathbf{v}_i \rangle \cong D/\mathrm{ann}(\mathbf{v}_i)$ e
$$a \in \mathrm{ann}(\mathbf{v}_i) \Leftrightarrow a\mathbf{v}_i = 0 \Leftrightarrow \pi(a\mathbf{e}_i) \Leftrightarrow a\mathbf{e}_i \in \mathrm{im}(f)$$
Para $i \leq n$, temos $a\mathbf{e}_i \in \mathrm{im}(f)$ *sse* $d_i \mid a$. Para $i > n$, temos $a\mathbf{e}_i \in \mathrm{im}(f)$ *sse* $a = 0 = d_i$. Em ambos os casos, $\mathrm{ann}(\mathbf{v}_i) = (d_i)$;
2. $\sum_{i=1}^m \langle \mathbf{v}_i \rangle = M$ pois $\langle \{\mathbf{e}_i \mid i = 1, \ldots, m\} \rangle = D^m$ e π é epi;
3.
$$\mathbf{v} \in \langle \mathbf{v}_i \rangle \cap \sum_{j \neq i} \langle \mathbf{v}_j \rangle \Leftrightarrow \exists_{a_1, \ldots, a_m} : \mathbf{v} = a_i\mathbf{v}_i = \sum_{j \neq i} a_j \mathbf{v}_j$$
$$\Rightarrow a_i\mathbf{e}_i - \sum_{i \neq j} a_j \mathbf{e}_j \in \mathrm{im}(f) \Rightarrow a_i \in \mathrm{ann}(\mathbf{v}_i) \Rightarrow \mathbf{v} = a_i\mathbf{v}_i = 0.$$

Resta apenas mostrar a unicidade de $(d_1), \ldots, (d_m)$, o que faremos mais adiante. □

Corolário 16.3. *Seja $M \in \mathrm{Mod}_D$* finitamente gerado. *Então*

$$M = \mathrm{Tor}\, M \oplus L,$$

onde L é livre e $\dim L = \mathrm{rank}\, M$. Em particular, M é livre sse *M é livre de torção. Mais precisamente, temos*

$$M \cong \Big(\bigoplus_{i=1}^{n} D/(d_i) \Big) \oplus D^k, \tag{16.1}$$

tal que $d_1 \mid d_2 \mid \cdots \mid d_n \neq 0$ e $k = \mathrm{rank}\, M$.

Demonstração. Podemos supor $M = \bigoplus_{i=1}^m D/(d_i)$ com $(d_i) \supset (d_{i+1})$. Seja $s = \max\{i \mid d_i \neq 0\}$. Temos

$$\mathrm{Tor}\, M = \bigoplus_{i=1}^{s} \mathrm{Tor}\,(D/(d_i)) = \bigoplus_{i=1}^{s} D/(d_i).$$

Seja $L = \bigoplus_{i=s+1}^{m} D/(d_i) = \bigoplus_{i=s+1}^{m} D$. Temos

$$M = \operatorname{Tor} M \oplus L,$$

e

$$M_K = K \otimes_D M \cong K \otimes_D L \cong K^{m-s},$$

logo $\operatorname{rank} M = \dim_K M_K = m - s = \dim_D L$.

Se M é livre de torção, então $M = L$, logo M é livre. □

Observação 16.4. A condição de M ser finitamente gerado não pode ser removida: se $D = \mathbb{Z}$ e $M = \mathbb{Q}$, temos $\operatorname{Tor} M = \{0\}$, mas M não é livre como módulo-$\mathbb{Z}$.

Definição 16.5. *Diz-se que* (16.1) *é a decomposição em* factores cíclicos invariantes. *Os elementos d_i da decomposição* (16.1) *dizem-se* factores invariantes *de M.*

Observação 16.6. Os factores invariantes estão determinados a menos de multiplicação por unidades (ou em alternativa, os ideais correspondentes, (d_i), estão unicamente determinados).

Exemplo 16.7. No caso em que $D = \mathbb{Z}$, o corolário anterior diz que todo o grupo abeliano *finitamente gerado* G é da forma

$$G \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n} \oplus \mathbb{Z}^k,$$

com $d_1 \mid d_2 \mid \cdots \mid d_n \neq 0$ e $k \geq 0$.

Exemplo 16.8. Seja G o grupo abeliano gerado pelos elementos x, y, z satisfazendo as relações $2x + 4y = 0$ e $x + y + 3z = 0$. Pelos resultados anteriores, sabemos que G é a soma directa de grupos cíclicos. Seja $L = \mathbb{Z}x \oplus \mathbb{Z}y \oplus \mathbb{Z}z$ o grupo abeliano livre no conjunto $\{x, y, z\}$ e seja $R = \langle 2x + 4y, x + y + 3z \rangle < L$. Então $G \cong L/R$, ou seja,

$$G \cong \mathbb{Z}^3 / \operatorname{im} f$$

onde $f : \mathbb{Z}^3 \to \mathbb{Z}^2$ é representada pela matriz

$$A = \begin{bmatrix} 1 & 1 & 3 \\ 2 & 4 & 0 \end{bmatrix} \in M_{2\times 3}(\mathbb{Z}) \ .$$

Portanto, para determinar uma decomposição de G numa soma directa de grupos cíclicos, basta calcular os factores invariantes da matriz A. Aplicando sucessivamente operações elementares à matriz A obtemos

$$A = \begin{bmatrix} 1 & 1 & 3 \\ 2 & 4 & 0 \end{bmatrix} \xrightarrow{P_1\times} \begin{bmatrix} 1 & 1 & 3 \\ 0 & 2 & -6 \end{bmatrix} \xrightarrow{\times Q_1} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & -6 \end{bmatrix} \xrightarrow{\times Q_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} = B.$$

onde

$$P_1 = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \quad , \quad Q_1 = \begin{bmatrix} 1 & -1 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{e} \quad Q_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix}$$

são as matrizes correspondentes às operações efectuadas. Portanto $d_1 = 1$, $d_2 = 2$ e $k = 1$ (na notação do Corolário 16.3), ou seja,

$$G \cong \mathbb{Z}_1 \oplus \mathbb{Z}_2 \oplus \mathbb{Z} \cong \mathbb{Z}_2 \oplus \mathbb{Z} \ .$$

Recorrendo às matrizes P_i e Q_j podemos ainda obter explicitamente um isomorfismo da seguinte maneira. Sejam $a = 2x + 4y$ e $b = x + y + 3z$ os geradores de R, portanto

$$A \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \ .$$

Pondo $P = P_1$ e $Q = Q_1 Q_2$, temos que $PAQ = B$ e

$$PAQ\Big(Q^{-1} \begin{bmatrix} x \\ y \\ z \end{bmatrix}\Big) = P \begin{bmatrix} a \\ b \end{bmatrix} \qquad \text{ou seja} \qquad B \begin{bmatrix} x + y + 3z \\ y - 3z \\ z \end{bmatrix} = \begin{bmatrix} a \\ b - 2a \end{bmatrix} \ ,$$

donde $x' = x + y + 3z, y' = y - 3z, z' = z$ geram G e $a' = a, b' = b - 2a$ geram R, e ainda $a' = x', b' = 2y'$, logo

$$y' \mapsto (\underline{1}, 0) \in \mathbb{Z}_2 \oplus \mathbb{Z} \quad \text{e} \quad z' \mapsto (\underline{0}, 1) \in \mathbb{Z}_2 \oplus \mathbb{Z}$$

determina um isomorfismo $G \to \mathbb{Z}_2 \oplus \mathbb{Z}$.

Corolário 16.9. *Dois módulos-D finitamente gerados são isomorfos* sse *têm os mesmos factores invariantes e a mesma característica.*

Demonstração. Segue da unicidade dos factores invariantes (que ainda não demonstrámos). □

Notação 16.10. Diz-se que os factores invariantes e a característica constituem um conjunto *completo* de invariantes dos módulos-D de tipo finito.

Exercícios

4.16.1. (a) Seja D um *d.i.p.* e M um módulo-D de torção finitamente gerado. Mostre que $I = \{d \in D \mid dM = 0\}$ é um ideal não nulo de D. Um elemento $a \in I$ diz-se o *aniquilador mínimo* de M.

(b) Dê um exemplo de um grupo abeliano finito M com aniquilador mínimo $m \in \mathbb{Z}$ e de um subgrupo cíclico N com ordem $n \in \mathbb{N}$ satisfazendo $n \mid m$ e $n \neq \pm 1$, $n \neq \pm m$ tais que N não é um somando directo de M.

4.16.2. Seja M o módulo sobre $\mathbb{Z}[i]$ gerado por elementos x, y cujas relações são determinadas por $(1+i)x+(2-i)y = 0$ e $3x+5y = 0$. Escreva M como uma soma directa de módulos cíclicos.

4.16.3. Seja G um grupo abeliano gerado por elementos x, y, z cujas relações são geradas por

$$\begin{aligned} 6x + 4y &= 0 \\ 4x + 4y + 12z &= 0 \\ 8x + 8y + 36z &= 0\ . \end{aligned}$$

Determine os factores invariantes de G.

4.16.4. Seja D um *d.i.p.* e seja M um módulo-D cíclico de ordem[10] $a \in D$. Mostre que:

(a) Dado $b \in D$ tal que a e b são coprimos, então $bM = M$ e $M[b] = 0$. (Ver Exercício 4.2.6 para a definição de $M[b]$.)

(b) Se $b \mid a$ em D, i.e., se $bc = a$ para algum $c \in D$, então $bM \cong D/(c)$ e $M[b] \cong D/(b)$.

4.16.5. Seja D um *d.i.p.* e seja M um módulo-D cíclico de ordem[10] $a \in D$. Mostre que:

(a) Qualquer submódulo de M é cíclico e tem ordem um divisor de a.

(b) Para cada ideal $(b) \supset (a)$, M contém exactamente um submódulo cíclico de ordem b.

4.16.6. Seja D um *d.i.p.* e sejam M e N módulos-D com ordens[10] $a \neq 0$ e $b \neq 0$, respectivamente, *t.q.* a e b não são coprimas. Mostre que os factores invariantes de $M \oplus N$ são $\mathrm{MDC}(a, b)$ e $\mathrm{MMC}(a, b)$.

[10] O módulo-D cíclico $M = \langle \mathbf{v} \rangle$ tem *ordem* $a \in D$ se $\mathrm{ann}(\mathbf{v}) = (a) \subset D$.

17. Decomposição em factores cíclicos primários

Seja $d = p_1^{m_1} \cdots p_r^{m_r}$ uma factorização de $d \in D$ em factores primos (distintos, não associados). Então, pelo Teorema Chinês dos Restos 4.5 do Capítulo 2:

$$D/(d) \cong D/(p_1^{m_1}) \oplus \cdots \oplus D/(p_r^{m_r}).$$

Definição 17.1. *Um módulo-D da forma $D/(p^m)$, com $p \in D$ primo, diz-se um módulo* cíclico primário.

Teorema 17.2 (Decomposição em factores cíclicos primários)**.** *Seja M um módulo-D de tipo finito. Então*

$$M \cong D/(p_1^{m_1}) \oplus \cdots \oplus D/(p_s^{m_s}) \oplus L, \tag{17.1}$$

onde L é livre de dimensão $\operatorname{rank} M$ *e $p_1, \ldots, p_n \in D$ são primos (não necessariamente distintos). Os ideais $(p_i^{m_i})$ são unicamente determinados por M.*

Demonstração. A existência segue da decomposição (16.1) e do Teorema Chinês dos restos: se $q_1^{n_1} \cdots q_r^{n_r}$ é uma decomposição de $d \in D$ em potências de primos (distintos), $q_i \in D$, então

$$D/(d) \cong D/(q_1^{n_1}) \oplus \cdots \oplus D/(q_r^{n_r}).$$

A unicidade da decomposição será demonstrada mais adiante. □

Definição 17.3. *Diz-se que* (17.1) *é a decomposição* cíclica primária *de M. Os elementos $p_i^{m_i} \in D$ dizem-se* divisores elementares *de M.*

Corolário 17.4. *O tipo de isomorfismo de um módulo-D de tipo finito é completamente determinado pela característica* $\operatorname{rank} M$ *e pelos seus divisores elementares.*

Notação 17.5. Diz-se que os divisores elementares e a característica constituem um conjunto *completo* de invariantes dos módulos-D de tipo finito.

Exemplo 17.6. Quantos grupos abelianos de ordem 30000 é que existem? Seja G um grupo abeliano de ordem $|G| = 30000 = 3 \cdot 2^4 \cdot 5^4$. Considerando as possíveis decomposições cíclicas primárias, temos $G \cong \mathbb{Z}_3 \oplus G_1 \oplus G_2$, com $|G_1| = 2^4$ e $|G_2| = 5^4$. Basta portanto determinar quantos grupos abelianos existem com ordem p^4, $p \in \mathbb{N}$ primo. A decomposição cíclica primária de um destes grupo é da forma

$$\mathbb{Z}_{p^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_r}}$$

com $m_1 + \cdots + m_r = 4$, e podemos supor que $m_1 \leq \cdots \leq m_r$. Portanto, temos que contar as partições de 4:

$$\begin{aligned} 4 &= 1+1+1+1 \\ 4 &= 1+1+2 \\ 4 &= 2+2 \\ 4 &= 1+3 \\ 4 &= 4 \end{aligned}$$

Concluimos que, a menos de isomorfismos, há 5 grupos abelianos de ordem p^4, logo existem 25 grupos abelianos de ordem 30000.

18. Relação entre factores invariantes e elementares

Descrevemos de seguida um algoritmo para determinar os factores invariantes a partir dos divisores elementares: sejam $p_1, \ldots, p_s \in D$ primos não associados representantes das classes

(para a relação de associado) que surgem na decomposição (17.1). Ordenamos as potências dos p_i que ocorrem em (17.1) da seguinte forma

$$\begin{matrix} p_1^{m_{11}} & \cdots & p_s^{m_{1s}} \\ \vdots & & \vdots \\ p_1^{m_{t1}} & \cdots & p_s^{m_{ts}} \end{matrix}$$

t.q., para todo o j, $m_{1j} \leq m_{2j} \leq \cdots \leq m_{tj}$ e acrescentamos potências triviais p_i^0 de forma a que todos os p_i ocorrem o mesmo número de vezes. Fazendo $d_i = p_1^{m_{i1}} \cdots p_s^{m_{is}}$ vem

$$D/(d_i) \cong D/(p_1^{m_{i1}}) \oplus \cdots \oplus D/(p_s^{m_{is}})$$

e $d_i \mid d_{i+1}$. É fácil de ver que partindo da decomposição invariante e aplicando o Teorema Chinês do restos para obter uma decomposição cíclica primária, e depois aplicando este algoritmo, recuperamos a decomposição invariante inicial.

Exemplo 18.1. Consideremos o grupo abeliano $\mathbb{Z}_2 \oplus \mathbb{Z}_{12}$. A correspondente decomposição cíclica primária é $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$. Temos assim, $p_1 = 2$ e $p_2 = 3$ e portanto

$$\begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \Rightarrow \begin{cases} d_1 = 2^1 \cdot 3^0 = 2 \\ d_2 = 2^2 \cdot 3^1 = 12 \end{cases}.$$

Recuperámos assim a decomposição em factores cíclicos invariantes a partir da decomposição em factores cíclicos primários.

Pode mostrar-se que os processos de obtenção da decomposição cíclica primária a partir da em factores invariantes e desta a partir da decomposição cíclica primária são inversos um do outro. Portanto a unicidade dos dois tipos de decomposição é equivalente.

Exercícios

4.18.1. Seja $G = \mathbb{Z}^3/\operatorname{im} f$, onde $f\colon \mathbb{Z}^3 \to \mathbb{Z}^3$ é dado por $f(x,y,z) = (2x+y+z, 3x, x+y)$. Determine a decomposição de G em factores cíclicos primários.

4.18.2. Quantos subgrupos de ordem p^2 é que o grupo abeliano $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$ contém?

4.18.3. (a) Quais os divisores elementares do grupo abeliano $\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{15}$? Quais são os factores invariantes deste grupo?
(b) Repetir a alínea anterior para $\mathbb{Z}_{42} \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}_{200} \oplus \mathbb{Z}_{1000}$.

4.18.4. A menos de isomorfismos, determine todos os grupos abelianos de ordem 32 e 72.

4.18.5. A menos de isomorfismos, determine todos os grupos abelianos de ordem n para $n \leq 20$.

4.18.6. Seja $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$. Mostre que os factores invariantes do grupo abeliano G são $\mathrm{MDC}(m,n)$ e $\mathrm{MMC}(m,n)$, se $\mathrm{MDC}(m,n) > 1$, e apenas mn, se $\mathrm{MDC}(m,n) = 1$.

4.18.7. Seja G um grupo abeliano finito e $H < G$. Mostre que G contém um subgrupo isomorfo a G/H.

19. Unicidade da decomposição em factores cíclicos primários

Definição 19.1. *Seja $M \in \mathrm{Mod}_D$ e seja $p \in D$ um primo. Diz-se que o submódulo*

$$M(p) \coloneqq \{\mathbf{v} \in M \mid \exists k \in \mathbb{N} : p^k \mathbf{v} = 0\}$$

é a componente p-primária *de M.*

Observação 19.2. Se $\varphi\colon M \to N$ é um isomorfismo, então $\varphi|_{M(p)}\colon M(p) \xrightarrow{\cong} N(p)$. Assim, a componente p-primária de um módulo é preservada por isomorfismos (diz-se que é um invariante).

Proposição 19.3. *Seja D um d.i.p. e sejam M_i módulos-D, para $i \in I$. Então*

$$M = \bigoplus_{i \in I} M_i \quad \Rightarrow \quad M(p) = \bigoplus_{i \in I} M_i(p) \ .$$

Exemplo 19.4. Seja $M = D/(p_1^{m_1}) \oplus \cdots \oplus D/(p_s^{m_s}) \oplus D^k$, onde $p_i \in D$ são primos. Dado um primo $p \in D$, pela proposição anterior e pelo Exercício 4.19.2 (b) e (c) temos

$$M(p) = \bigoplus_{\{i \mid p_i \sim p\}} D/(p_i^{m_i}) \ .$$

O exemplo anterior mostra que para demonstrar a unicidade da decomposição em factores cíclicos primários basta considerar o caso de módulos de torção com uma só componente primária.

Proposição 19.5. *Seja $p \in D$ um primo e sejam $m_1, \ldots, m_r, n_1, \ldots, n_s \in \mathbb{N}$ t.q. $m_1 \leq \cdots \leq m_r$, $n_1 \leq \cdots \leq n_s$, e*

$$D/(p^{m_1}) \oplus \cdots \oplus D/(p^{m_r}) \cong D/(p^{n_1}) \oplus \cdots \oplus D/(p^{n_s}).$$

Então $r = s$ e $m_i = n_i$, $i = 1, \ldots, r$.

Demonstração. Seja $l \in \mathbb{N}_0$, pelo Exercício 4.19.2 (d), temos

$$p^l \left(D/(p^m)\right) \cong \begin{cases} D/(p^{m-l}), & l < m \\ 0, & l \geq m \end{cases}$$

e daí segue

$$\frac{p^l \left(D/(p^m)\right)}{p^{l+1} \left(D/(p^m)\right)} \cong \begin{cases} D/(p), & l < m \\ 0, & l \geq m \end{cases}.$$

Seja $M = D/(p^{m_1}) \oplus \cdots \oplus D/(p^{m_r}) \cong D/(p^{n_1}) \oplus \cdots \oplus D/(p^{n_s})$. Juntando os dois factos acima, obtemos

$$\forall_l \quad \frac{p^l M}{p^{l+1} M} \cong \bigoplus_{\{i \mid m_i > l\}} D/(p) \cong \bigoplus_{\{i \mid n_i > l\}} D/(p),$$

considerando a estrutura de espaço vectorial sobre o corpo $D/(p)$ (pois p é um primo no *d.i.p.* D) e comparando dimensões sobre $D/(p)$, obtemos

$$\forall_l \quad \#\{i \mid m_i > l\} = \#\{i \mid n_i > l\},$$

donde

$$r = s \quad \wedge \quad n_i = m_i, \ i = 1, \ldots, r. \qquad \square$$

Exemplo 19.6. Vejamos que $p^l\mathbb{Z}_{p^m}/p^{l+1}\mathbb{Z}_{p^m} \cong \mathbb{Z}_p$ para todo $l < m$. Note-se que

$$\frac{p^l\mathbb{Z}/p^m\mathbb{Z}}{p^{l+1}\mathbb{Z}/p^m\mathbb{Z}} \cong \frac{p^l\mathbb{Z}}{p^{l+1}\mathbb{Z}}.$$

Seja $\pi\colon p^l\mathbb{Z} \to p^l\mathbb{Z}/p^{l+1}\mathbb{Z}$ a projecção canónica. Seja $\psi : \mathbb{Z} \to \mathbb{Z}$ a aplicação dada por $\psi(n) = p^l n$. Como ψ é um homomorfismo de módulos-$\mathbb{Z}$ com imagem $\operatorname{im}\psi = p^l\mathbb{Z}$, a composta

$$\varphi \coloneqq \pi \circ \psi : \mathbb{Z} \to \frac{p^l\mathbb{Z}}{p^{l+1}\mathbb{Z}} \ ; \quad n \mapsto \pi(p^l n)$$

é um homomorfismo sobrejectivo. Temos

$$\varphi(n) = 0 \Leftrightarrow p^l n \equiv 0 \mod p^{l+1} \Leftrightarrow n \equiv 0 \mod p \Leftrightarrow n \in p\mathbb{Z} \ ,$$

ou seja, $\ker(\varphi) = p\mathbb{Z}$, donde concluimos que φ induz um isomorfismo

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \frac{p^l\mathbb{Z}}{p^{l+1}\mathbb{Z}} \ .$$

Exercícios

4.19.1. Demonstre a Proposição 19.3.

4.19.2. Sejam $p, q \in D$ elementos primos. Recorde a definição de $M[b]$ do Exercício 4.2.6 e mostre que
(a) $M(p) = \bigcup_{n\in\mathbb{N}} M[p^n]$;
(b) $D(p) = \{0\}$;
(c) $\big(D/(q^m)\big)(p) \neq \{0\}$ se e só se $q \sim p$, onde $m \in \mathbb{N}$;
(d) $p^l\big(D/(p^m)\big) \cong D/(p^{l-m})$, para $l < m$, e $p^l\big(D/(p^m)\big) = \{0\}$, para $l \geq m$.
Sugestão: Use os resultados do Exercício 4.16.4.

20. Formas canónicas racionais

Seja k um corpo e seja V um espaço vectorial-k de *dimensão finita*. Recorde-se que existe uma bijecção

$$\boxed{\mathrm{End}_k(V) \leftrightarrow \text{estruturas de módulo-}k[x] \text{ em } V,}$$

que é obtida da seguinte forma: dada $T \in \mathrm{End}_k(V)$, a respectiva estrutura de módulo-$k[x]$ é definida por

$$\Big(\sum_i a_i x^i\Big) \cdot \mathbf{v} \coloneqq \sum_i a_i T^i \mathbf{v}, \qquad \forall \textstyle\sum_i a_i x^i \in k[x], \quad \forall\, \mathbf{v} \in V\ .$$

A correspondência inversa envia uma estrutura de módulo-$k[x]$ em V na transformação linear $T\colon V \to V$ dada por

$$T\mathbf{v} \coloneqq x \cdot \mathbf{v}, \qquad \forall \mathbf{v} \in V.$$

Consideremos agora fixada a estrutura de módulo-$k[x]$ em V associada à transformação $T \in \mathrm{End}_k(V)$. Em particular, V é um módulo-$k[x]$ de torção finitamente gerado (Exercício 4.14.1) pois $\dim_k V$ é finita. Dado um subespaço-k $W \subset V$, temos

$$\boxed{W \subset V \text{ é um submódulo-}k[x] \textit{ sse } W \text{ é um subespaço invariante para } T}$$

Lema 20.1. *Nas condições acima, sejam $V_i \subset V$, $i = 1, \ldots, r$, subespaços-k. Então*

$$V = V_1 \oplus \cdots \oplus V_r \textit{ em } \mathrm{Mod}_{k[x]}$$

sse $V_1 \oplus \cdots \oplus V_r$ *em* Vect_k *e V_i é um espaço invariante para T, $i = 1, \ldots, r$.*

Tendo em conta o lema anterior e a classificação de módulos finitamente gerados sobre o d.i.p. $k[x]$ (Teorema 16.2 ou Corolário 16.3), basta estudar os submódulos-$k[x]$ cíclicos de V.

Lema 20.2. *Nas condições acima, se um subespaço-k $W \subset V$ é um submódulo-$k[x]$ cíclico então W tem uma base sobre k da forma $\{T^i\mathbf{v} \mid i = 0, \ldots, m-1\}$ para algum $\mathbf{v} \in W$ e $m \in \mathbb{N}$.*

Demonstração. Sejam $W \subset V$ um submódulo-$k[x]$ cíclico , $\mathbf{v} \in W$ um gerador e $f \in k[x]$ um gerador de $\mathrm{ann}(f) \subset k[x]$. Sem perda de generalidade, podemos supor que f é mónico. Seja $m = \deg f$. Temos,

$$\varphi_{\mathbf{v}}\colon k[x]/(f) \xrightarrow{\cong} W;\ p + (f) \mapsto p \cdot \mathbf{v}.$$

Como $\{\underline{1}, \underline{x}, \ldots, \underline{x}^{m-1}\}$ é uma base para $k[x]/(f)$ enquanto espaço vectorial-k, o conjunto

$$\varphi_{\mathbf{v}}\{\underline{1}, \underline{x}, \ldots, \underline{x}^{m-1}\} = \{\mathbf{v}, T\mathbf{v}, \ldots, T^{m-1}\mathbf{v}\}$$

é uma base para W. □

Sejam $\mathbf{v}$, f como na demonstração do lema anterior: $f = x^m + \sum_{i=0}^{m-1} a_i x^i$. Seja $\mathbf{w}_i \coloneqq T^i\mathbf{v}$, $i = 0, \ldots, m-1$. Calculamos a matriz que representa a transformação $T|_W : W \to W$ na base $\mathcal{B} = \{\mathbf{w}_0, \ldots, \mathbf{w}_{m-1}\}$:

$$\begin{aligned} T\mathbf{w}_0 &= T\mathbf{v} = \mathbf{w}_1 \\ &\vdots \\ T\mathbf{w}_{m-2} &= T^{m-1}\mathbf{v} = \mathbf{w}_{m-1} \\ T\mathbf{w}_{m-1} &= T^m\mathbf{v} = -a_0\mathbf{w}_0 - a_1\mathbf{w}_1 - \cdots - a_{m-1}\mathbf{w}_{m-1}, \end{aligned}$$

onde usámos a igualdade

$$0 = f \cdot \mathbf{v} = a_0\mathbf{v} + a_1 T\mathbf{v} + \cdots + a_{m-1}T^{m-1}\mathbf{v} + T^m\mathbf{v}.$$

Concluímos que a matriz de T na base $\mathcal{B}$ é

$$R = \begin{bmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & -a_{m-1} \end{bmatrix} \tag{20.1}$$

Corolário 20.3. *Seja V um espaço-k de dimensão finita e seja $T \in \mathrm{End}_k(V)$. Então existem subsespaços $V_1, \ldots, V_s \subset V$ invariantes para T* t.q.

$$V = V_1 \oplus \cdots \oplus V_s$$

e cada V_i tem uma base da forma $\mathcal{B}_i = \{T^j \mathbf{v}_i \mid j = 0, \ldots, m_i - 1\}$, para algum $\mathbf{v}_i \in V_i$ e $m_i \in \mathbb{N}$. A matriz de T na $\mathcal{B}_1, \ldots, \mathcal{B}_s$ é da forma

$$R = \begin{bmatrix} R_1 & \cdots & 0 \\ & \ddots & \\ 0 & \cdots & R_s \end{bmatrix} \tag{20.2}$$

onde, se $m_i > 1$, R_i é da forma

$$R_i = \begin{bmatrix} 0 & \cdots & 0 & -a_{0,i} \\ 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & -a_{m_i-1,i} \end{bmatrix}$$

i.e., *R_i é da forma* (20.1). *Se $m_i = 1$, R_i é uma matriz 1×1, $R_i = [-a_{0,i}]$.*

Uma matriz da forma (20.2) *diz-se uma* forma racional *para T.*

Observação 20.4. No Corolário 20.3, temos

$$\mathrm{ann}(\mathbf{v}_i) = (a_{0,i} + a_{1,i}x + \cdots + a_{m_i-1,i}x^{m_i-1} + x^m).$$

Observação 20.5. As formas canónicas racionais são obtidas a partir da decomposição de V em soma directa de módulos-$k[x]$ cíclicos. Como tal, não é única, pois há várias decomposições.

Exemplo 20.6. Seja $V = \mathbb{R}^4$ e $T : \mathbb{R}^4 \to \mathbb{R}^4$ a aplicação linear dada por $T(x_1, x_2, x_3, x_4) = (4x_4, x_1, x_2, x_3)$ para qualquer $\mathbf{v} = (x_1, x_2, x_3, x_4) \in \mathbb{R}^4$. Como $T^4 = 4I$ e $\dim V = 4$, temos $V \cong \mathbb{R}[x]/(x^4 - 4)$ em $\mathrm{Mod}_{\mathbb{R}[x]}$. Podemos factorizar $x^4 - 4$ das seguintes maneiras

$$x^4 - 4 = (x^2 - 2)(x^2 + 2) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)\ .$$

A cada uma das factorizações corresponde uma decomposição em módulos-$\mathbb{R}[x]$ cíclicos (por aplicação do Teorema Chinês dos Restos):

$$V \cong \frac{\mathbb{R}[x]}{(x^4 - 4)} \cong \frac{\mathbb{R}[x]}{(x^2 - 2)} \oplus \frac{\mathbb{R}[x]}{(x^2 + 2)} \cong \frac{\mathbb{R}[x]}{(x - \sqrt{2})} \oplus \frac{\mathbb{R}[x]}{(x + \sqrt{2})} \oplus \frac{\mathbb{R}[x]}{(x^2 + 2)}$$

A cada decomposição corresponde uma forma canónica racional:

$$\begin{bmatrix} 0 & 0 & 0 & 4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{ou} \quad \begin{bmatrix} 0 & 2 & & \\ 1 & 0 & & \\ & & 0 & -2 \\ & & 1 & 0 \end{bmatrix} \quad \text{ou} \quad \begin{bmatrix} \sqrt{2} & & & \\ & -\sqrt{2} & & \\ & & 0 & -2 \\ & & 1 & 0 \end{bmatrix}\ .$$

21. Forma canónica de Jordan

Suponhamos agora que k é um corpo algebricamente fechado. Então (a menos de multiplicação por unidades) os únicos primos do anel $k[x]$ são da forma

$$f(x) = x - \lambda, \qquad \lambda \in k.$$

Portanto, os módulos cíclicos primários sobre $k[x]$ são da forma

$$\frac{k[x]}{((x-\lambda)^m)}, \qquad \lambda \in k, m \in \mathbb{N}.$$

Note-se que o conjunto $\mathcal{B}_{\lambda,m} = \{\underline{1}, \underline{x-\lambda}, \ldots, \underline{(x-\lambda)}^{m-1}\}$ é uma base para este espaço vectorial sobre k.

De novo, consideramos um espaço vectorial $V \in \mathrm{Vect}_k$ de dimensão finita com a estrutura de módulo-$k[x]$ fornecida por uma aplicação linear-k, $T\colon V \to V$. Suponhamos que $W \subset V$ é um submódulo cíclico primário sobre $k[x]$ e suponhamos que $\mathbf{v} \in W$ é um gerador. Então existem $\lambda \in k$, $m \in \mathbb{N}$ *t.q.* $\mathrm{ann}(\mathbf{v}) = ((x-\lambda)^m)$, portanto a aplicação

$$\varphi_{\mathbf{v}}\colon \frac{k[x]}{((x-\lambda)^m)} \to W;\ f(x) + ((x-\lambda)^m) \mapsto f(x)\cdot\mathbf{v},$$

é um isomorfismo de módulos-$k[x]$. Em particular, é um isomorfismo de espaços vectoriais-k. Portanto,

$$\varphi_{\mathbf{v}}\left(\mathcal{B}_{\lambda,m}\right) = \left\{\mathbf{v}, (T-\lambda)\mathbf{v}, \ldots, (T-\lambda)^{m-1}\mathbf{v}\right\}$$

é uma base para W como espaço-k. Defina-se

$$\mathbf{w}_i \coloneqq (T-\lambda)^{m-i}\mathbf{v}, \qquad i = 1, \ldots, m.$$

Temos

$$T\mathbf{w}_i = (T-\lambda)\mathbf{w}_i + \lambda\mathbf{w}_i = \underbrace{(T-\lambda)^{m-(i-1)}\mathbf{v}}_{\mathbf{w}_{i-1}} + \underbrace{\lambda(T-\lambda)^{m-i}\mathbf{v}}_{\lambda\mathbf{w}_i}$$
$$= \begin{cases} \mathbf{w}_{i-1} + \lambda\mathbf{w}_i, & i = 2, \ldots, m \\ \lambda\mathbf{w}_1, & i = 1. \end{cases}$$

Concluímos que $\{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ é uma base de W relativamente à qual T é representada pela matriz

$$J = \begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}.$$

Corolário 21.1. *Sejam k um corpo* algebraicamente fechado*, V um espaço vectorial-k de dimensão finita, e $T\colon V \to V$ uma transformação linear. Então existem subsespaços $V_1, \cdots, V_s$, invariantes para T* t.q. *$V = \bigoplus_{i=1}^{s} V_i$, e cada V_i tem uma base $\mathcal{B}_i$ em T é representada por uma matriz da forma*

$$J_i = \begin{bmatrix} \lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix},$$

se $\dim V_i > 1$*, e* $J_i = \left[\lambda_i\right]$*, se* $\dim V_i = 1$.

As matrizes $J_1, \ldots, J_s$ *dizem-se* blocos de Jordan *e*

$$J = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_s \end{bmatrix}$$

diz-se uma forma canónica de Jordan *de* T. *J representa T na base $\mathcal{B} = \cup_i \mathcal{B}_i$ e é única a menos de reordenação dos blocos.*

21.1. Método para calcular a forma canónica de Jordan e respectivas bases

1. Calcular os valores próprios $\lambda_1, \cdots, \lambda_l$;
2. Para cada valor próprio $\lambda \in \{\lambda_1, \ldots, \lambda_l\}$, determinar o espaço próprio $\ker(T-\lambda)$; se $g \coloneqq \dim \ker(T-\lambda)$ é igual à multiplicidade algébrica de λ, a, como raiz de $p(x) = \det(T-x)$, então há g blocos de Jordan correspondentes a λ, todos com dimensão 1; um para cada elemento de uma base de $\ker(T-\lambda)$.
3. Se $g < a$, determinar o menor $M \in \mathbb{N}$ tal que $(T-\lambda)^M = (T-\lambda)^{M+1}$. Pôr $E_i \coloneqq \ker(T-\lambda)^i$ e $r_i \coloneqq \dim E_i$, para $i = 1, \ldots, M$. Então

$$g = r_1 < r_2 < \cdots < r_M = a \ .$$

Defina-se

$$\begin{cases} s_1 &= r_1 \\ s_2 &= r_2 - r_1 \\ &\vdots \\ s_M &= r_M - r_{M-1} \end{cases} \quad \text{e} \quad \begin{cases} t_1 &= s_1 - s_2 \\ &\vdots \\ t_{M-1} &= s_{M-1} - s_M \\ t_M &= s_M \end{cases} .$$

Então t_i é o número[11] de blocos de Jordan $i \times i$. Sejam $m_1 = M > m_2 > \cdots > m_L$ os índices m tais que $t_m \neq 0$. Ou seja, T tem precisamente t_{m_i} blocos de Jordan $m_i \times m_i$ e daqui já podemos escrever a forma canónica de Jordan para T. Os restantes passos descrevem como obter uma base correspondente, começando pelos blocos maiores.

4. Seja $N_1 \coloneqq \operatorname{im}(T-\lambda)^{m_1-1} \cap \ker(T-\lambda) \neq \{0\}$. Determinar uma base $\mathcal{B}_1$ para N_1. Para cada elemento de $\mathbf{w} \in \mathcal{B}_1$ resolver iterativamente as equações

$$(*) \qquad \begin{aligned} \mathbf{w}_1 &= \mathbf{w} \\ (T-\lambda)\mathbf{w}_2 &= \mathbf{w}_1 \\ (T-\lambda)\mathbf{w}_3 &= \mathbf{w}_2 \\ &\vdots \\ (T-\lambda)\mathbf{w}_{m_1} &= \mathbf{w}_{m_1-1} \end{aligned}$$

O conjunto $\{\mathbf{w}_i \mid i = 1, \ldots, m_1\}$ é uma base para o espaço próprio generalizado correspondente ao vector próprio $\mathbf{w}$. A este espaço próprio corresponde um bloco de Jordan com dimensão m_1 e com λ na diagonal principal. Aplicar o mesmo procedimento aos outros elementos de $\mathcal{B}_1$.

5. Se $L > 1$, seja $N_2 \coloneqq \operatorname{im}(T-\lambda)^{m_2-1} \cap \ker(T-\lambda) \supsetneq N_1$. Determinar $\mathcal{B}_2$ *t.q.* $\mathcal{B}_2 \cup \mathcal{B}_1$ é uma base para N_2. Aplicar a $\mathcal{B}_2$ o procedimento iterativo $(*)$ do Passo 4, até obter m_2 vectores para cada $\mathbf{w} \in \mathcal{B}_2$.
6. Voltar a aplicar o Passo 5 para cada m_i, com $i \leq L$. No final obtemos espaços próprios generalizados cujas dimensões somam a.

[11] E s_i é o número de blocos de Jordan com dimensão pelo menos i.

Exemplo 21.2. Para ilustrar o algoritmo anterior, vamos aplicá-lo a uma matriz já na sua forma canónica de Jordan. Considere

$$A = \begin{bmatrix} 2 & & & & & & & & & \\ & 2 & & & & & & & & \\ & & 2 & 1 & & & & & & \\ & & 0 & 2 & & & & & & \\ & & & & 2 & 1 & & & & \\ & & & & 0 & 2 & & & & \\ & & & & & & 2 & 1 & 0 & 0 \\ & & & & & & 0 & 2 & 1 & 0 \\ & & & & & & 0 & 0 & 2 & 1 \\ & & & & & & 0 & 0 & 0 & 2 \end{bmatrix}.$$

Passo 1: $\lambda = 2$ é o único valor próprio. (Também sabemos que há dois blocos de Jordan 1×1, dois blocos 2×2 e um bloco 4×4, mas não vamos usar esta informação no resto do exemplo.)

Passo 2: Escrevendo $A - 2$ obtém-se directamente que $r_1 = \dim \ker(A-2) = 5$, donde concluimos que há cinco blocos de Jordan, alguns dos quais de tamanho maior do que um.

Passo 3: Calculamos as potências sucessivas de $A - 2$ até obtermos a mesma matriz (neste caso será a matriz nula pois A só tem um valor próprio):

$$(A-2)^2 = \begin{bmatrix} 0 & & & & & & & & & \\ & 0 & & & & & & & & \\ & & 0 & 0 & & & & & & \\ & & 0 & 0 & & & & & & \\ & & & & 0 & 0 & & & & \\ & & & & 0 & 0 & & & & \\ & & & & & & 0 & 0 & 1 & 0 \\ & & & & & & 0 & 0 & 0 & 1 \\ & & & & & & 0 & 0 & 0 & 0 \\ & & & & & & 0 & 0 & 0 & 0 \end{bmatrix},$$

$(A-2)^3$ tem uma única entrada não nula, um 1, na posição $(7, 10)$, e $(A-2)^4 = 0$. Concluimos que $m_1 = 4$, $m_2 = 2$ e $m_3 = 1$ são os únicos tamanhos dos blocos de Jordan, pois

$$\begin{aligned} r_1 = 5, r_2 = 8, r_3 = 9, r_4 = 10 &\Rightarrow s_1 = 5, s_2 = 3, s_3 = 1, s_4 = 1 \\ &\Rightarrow t_1 = 2, t_2 = 2, t_3 = 0, t_4 = 1. \end{aligned}$$

Passo 4: Como $E_1 \coloneqq \ker(A-2) = \langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_5, \mathbf{e}_7 \rangle$, então

$$N_1 \coloneqq \operatorname{im}(A-2)^{m_1-1} \cap E_1 = \langle \mathbf{e}_7 \rangle \cap E_1 = \langle \mathbf{e}_7 \rangle .$$

Calculamos os vectores própios generalizados a partir de $\mathbf{w} = \mathbf{w}_1 = \mathbf{e}_7$ e obtemos como possíveis soluções:

$$\begin{array}{lll} (A-2)\mathbf{w}_2 = \mathbf{e}_7 & \Leftrightarrow \mathbf{w}_2 \in \mathbf{e}_8 + E_1 & \text{seja } \mathbf{w}_2 = \mathbf{e}_8; \\ (A-2)\mathbf{w}_3 = \mathbf{e}_8 & \Leftrightarrow \mathbf{w}_3 \in \mathbf{e}_9 + E_1 & \text{seja } \mathbf{w}_3 = \mathbf{e}_9 + \mathbf{e}_7; \\ (A-2)\mathbf{w}_4 = \mathbf{e}_9 + \mathbf{e}_7 & \Leftrightarrow \mathbf{w}_4 \in \mathbf{e}_{10} + \mathbf{e}_8 + E_1 & \text{seja } \mathbf{w}_4 = \mathbf{e}_{10} + \mathbf{e}_8 + 4\mathbf{e}_3. \end{array}$$

Passo 5: Como $m_2 = 2$ fica

$$N_2 \coloneqq \operatorname{im}(A-2) \cap E_1 = \langle \mathbf{e}_3, \mathbf{e}_5, \mathbf{e}_7, \mathbf{e}_8, \mathbf{e}_9 \rangle \cap E_1 = \langle \mathbf{e}_3, \mathbf{e}_5, \mathbf{e}_7 \rangle .$$

A escolha "óbvia" para completar $\mathcal{B}_1 = \{\mathbf{e}_7\}$ seria $\{\mathbf{e}_3, \mathbf{e}_5\}$, mas vamos antes escolher $\mathcal{B}_2 = \{\mathbf{u}, \mathbf{v}\}$ com $\mathbf{u} = \mathbf{e}_3 + \mathbf{e}_5$ e $\mathbf{v} = \mathbf{e}_5 - \mathbf{e}_3 + 6\mathbf{e}_7$.

Cálculo de um vector próprio generalizado para $\mathbf{u}_1 = \mathbf{u}$:

$$(A-2)\mathbf{u}_2 = \mathbf{u}_1 \qquad \Leftrightarrow \mathbf{u}_2 \in \mathbf{e}_4 + \mathbf{e}_6 + E_1, \qquad \text{seja } \mathbf{u}_2 = \mathbf{e}_4 + \mathbf{e}_6 + 3\mathbf{e}_3 + 2\mathbf{e}_7.$$

Cálculo de um vector próprio generalizado para $\mathbf{v}_1 = \mathbf{v}$:

$$(A-2)\mathbf{v}_2 = \mathbf{v}_1 \qquad \Leftrightarrow \mathbf{v}_2 \in \mathbf{e}_6 - \mathbf{e}_4 + 6\mathbf{e}_8 + E_1, \qquad \text{seja } \mathbf{v}_2 = \mathbf{e}_6 - \mathbf{e}_4 + 6\mathbf{e}_8 - \mathbf{e}_1.$$

Passo 6: Fazemos mais uma iteração do Passo 4 com $m_3 = 1$:

$$N_3 \coloneqq \operatorname{im}(A-2)^0 \cap E_1 = E_1$$

e temos apenas de completar $\mathcal{B}_2$ para uma base de E_1. Por exemplo, podemos tomar $\mathcal{B}_3 = \{\mathbf{x}, \mathbf{y}\}$ com $\mathbf{x} = e_1 + 2\mathbf{e}_3 - 4\mathbf{e}_7$ e $\mathbf{y} = e_2 + e_1$.

Em resumo, a base que obtemos é $\mathcal{B} = \{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3, \mathbf{w}_4, \mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_1, \mathbf{v}_2, \mathbf{x}, \mathbf{y}\}$, a que corresponde a matriz mudança de base

$$P = \begin{bmatrix} | & | & | & | & | & | & | & | & | & | \\ \mathbf{w}_1 & \mathbf{w}_2 & \mathbf{w}_3 & \mathbf{w}_4 & \mathbf{u}_1 & \mathbf{u}_2 & \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{x} & \mathbf{y} \\ | & | & | & | & | & | & | & | & | & | \end{bmatrix}$$

e obtem-se[12]

$$J = P^{-1}AP = \begin{bmatrix} J_4 & & & & \\ & J_2 & & & \\ & & J_2 & & \\ & & & 2 & \\ & & & & 2 \end{bmatrix},$$

onde J_i é um bloco de Jordan $i \times i$, pois escrevemos primeiros os vectores próprios generalizados para o bloco maior, depois para os dois blocos 2×2 e finalmente para os 1×1.

Exemplo 21.3. Calcular a forma canónica de Jordan de

$$A = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 0 & 1 \\ 2 & -4 & 4 \end{bmatrix} \in M_3(\mathbb{C})$$

e uma matriz mudança de base.

Passo 1: Cálculo dos valores próprios:

$$\det(A - \lambda I) = (2-\lambda)^3 = 0 \Leftrightarrow \lambda = 2$$

com múltiplicadade algébrica 3.

Passo 2: Cálculo dos vectores próprios:

$$A - 2I = \begin{bmatrix} 0 & 0 & 0 \\ 1 & -2 & 1 \\ 2 & -4 & 2 \end{bmatrix} \to \begin{bmatrix} 0 & 0 & 0 \\ 1 & -2 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \tag{21.1}$$

portanto $E_1 = \ker(A-2I) = \{(2a-b, a, b) \mid a, b \in \mathbb{C}\}$ tem dimensão 2, donde A tem dois blocos de Jordan.

Passo 3: Como a matriz tem três colunas e dois blocos de Jordan, temos necessariamente um bloco 1×1 e um bloco 2×2, logo $m_1 = 2$ e $m_2 = 1$.

Passo 4: De (21.1), temos $\operatorname{im}(A-2I) = \langle (0,1,2) \rangle \subset E_1$, logo $N_1 = \operatorname{im}(A-2I)$ e podemos escolher $\mathbf{w}_1 = (0,1,2)$. Resolvendo o sistema

$$(A-2I)\mathbf{w}_2 = \mathbf{w}_1 \Leftrightarrow \mathbf{w}_2 \in (1,0,0) + N_1 \ ,$$

podemos escolher $\mathbf{w}_2 = (1,0,0)$.

[12] Não é necessário calcular a inversa P^{-1} nem o produto $P^{-1}AP$, pois o resultado é consequência do que foi feito anteriormente. Mas poderá querer de facto verificar (usando um programa de computador adequado) estes cálculos, dada a escolha "menos óbvia" dos vectores da base $\mathcal{B}$.

Passo 5: Como $m_2 = 1$, basta escolher $\mathbf{v} \in E_1$ tal que $\{\mathbf{v}, \mathbf{w}_1\}$ é uma base de E_1. Por exemplo, pondo $a = 0$ e $b = 1$ na expressão dos vectores de E_1 determinada no Passo 2, fica $\mathbf{v} \coloneqq (-1, 0, 1)$.

Obtemos então a seguinte matriz mudança de base

$$P \coloneqq \begin{bmatrix} | & | & | \\ \mathbf{w}_1 & \mathbf{w}_2 & \mathbf{v} \\ | & | & | \end{bmatrix} = \begin{bmatrix} 0 & 1 & -1 \\ 1 & 0 & 0 \\ 2 & 0 & 1 \end{bmatrix},$$

a que corresponde a forma canónica de Jordan

$$J = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

21.2. Método para calcular a forma canónica de Jordan sem a base correspondente

Suponhamos que $T \in \mathrm{End}_k(k^n)$ é representada na base canónica pela matriz $A \in M_n(k)$. Recorde-se que os blocos de Jordan A correspondem aos divisores elementares do módulo-$k[x]$ determinado por T. Para os calcular, temos de determinar um homomorfismo

$$f\colon (k[x])^m \to (k[x])^n \quad t.q. \quad k^n \cong (k[x])^n / \operatorname{im}(f)$$

e diagonalizar a matriz que representa f – ver Corolário 15.12 e início da demonstração do Teorema 16.2. Ora,

$$\begin{aligned} k^n &\cong k[x] \otimes_{k[x]} k^n \\ &\cong k[x] \otimes_k k^n / \langle \{x \otimes \mathbf{v} - 1 \otimes T\mathbf{v} \mid \mathbf{v} \in k^n\} \rangle \\ &= k[x] \otimes_k k^n / \langle \{x \otimes \mathbf{e}_i - 1 \otimes T\mathbf{e}_i \mid i = 1, \ldots, n\} \rangle \\ &\cong (k[x])^n / \langle \{x\mathbf{e}_i - T\mathbf{e}_i \mid i = 1, \ldots, n\} \rangle \\ &= (k[x])^n / \operatorname{im}(f), \end{aligned}$$

onde f é o homomorfismo $(k[x])^n \to (k[x])^n$ dado por

$$f(\mathbf{e}_i) = x\mathbf{e}_i - T\mathbf{e}_i.$$

Ou seja, é representada na base canónica de $(k[x])^n$ pela matriz

$$xI_n - A \in M_n(k[x]).$$

Exemplo 21.4. Calcular a forma canónica de Jordan de

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

Começamos por diagonalizar a matriz $x - A$:

$$x - A = \begin{bmatrix} x-2 & 0 & 0 \\ -1 & x & -1 \\ -2 & 4 & x-4 \end{bmatrix} \xrightarrow{L1 \leftrightarrow L2} \begin{bmatrix} -1 & x & -1 \\ x-2 & 0 & 0 \\ -2 & 4 & x-4 \end{bmatrix}$$

$$\xrightarrow[L2+(x-2)L1]{L3-2L1} \begin{bmatrix} -1 & x & -1 \\ 0 & x(x-2) & 2-x \\ 0 & 4-2x & x-2 \end{bmatrix} \xrightarrow[C3-C1]{C2+xC1} \begin{bmatrix} -1 & 0 & 0 \\ 0 & x(x-2) & 2-x \\ 0 & 4-2x & x-2 \end{bmatrix}$$

$$\xrightarrow{L2\leftrightarrow L3} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 4-2x & x-2 \\ 0 & x(x-2) & 2-x \end{bmatrix} \xrightarrow{C2\leftrightarrow C3} \begin{bmatrix} -1 & 0 & 0 \\ 0 & x-2 & 4-2x \\ 0 & 2-x & x(x-2) \end{bmatrix}$$

$$\xrightarrow{L3+L2} \begin{bmatrix} -1 & 0 & 0 \\ 0 & x-2 & 4-2x \\ 0 & 0 & x(x-2)+4-2x \end{bmatrix} \xrightarrow[-1L1]{C3+2C2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)^2 \end{bmatrix}$$

Obtemos assim a seguinte decomposição de $\mathbb{C}^3$ (com a estrutura de módulo sobre $\mathbb{C}[x]$ determinada por A) em soma de módulos cíclicos primários sobre o anel $\mathbb{C}[x]$:

$$\mathbb{C}^3 \cong \mathbb{C}[x]/(1) \oplus \mathbb{C}[x]/(x-2) \oplus \mathbb{C}[x]/\left((x-2)^2\right) \cong \mathbb{C}[x]/(x-2) \oplus \mathbb{C}[x]/\left((x-2)^2\right).$$

Portanto, a forma canónica de Jordan de A é:

$$J = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}.$$

Exercícios

4.21.1. Demonstre o Lema 20.1.

4.21.2. Seja k um corpo, V um espaço vectorial-k e $T \in \mathrm{End}_k(V)$. Considere a habitual estrutura de módulo-$k[x]$ em V induzida por $x\mathbf{v} \coloneqq T(\mathbf{v})$. Mostre que

$$k[x] \otimes_{k[x]} V \cong k[x] \otimes_k V / \langle \{x \otimes \mathbf{v} - 1 \otimes T\mathbf{v} \mid \mathbf{v} \in V\} \rangle$$

como módulos-$k[x]$.

4.21.3. Determine a forma canónica de Jordan das seguintes matrizes em $M_4(\mathbb{C})$:

$$A = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 4 & 1 & 1 & -1 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 0 \\ 1 & 1 & 2 & 2 \end{bmatrix} \quad \text{e} \quad C = \begin{bmatrix} 4 & -1 & 0 & -1 \\ 0 & 3 & 0 & 0 \\ -1 & 1 & 3 & 2 \\ 1 & -1 & 0 & 2 \end{bmatrix}.$$

4.21.4. Seja $A \in M_n(\mathbb{R})$. Mostre que A é conjugada a uma matriz da forma

$$\begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_k \end{bmatrix},$$

onde cada B_j ou é um bloco de Jordan para um valor próprio $\lambda_j \in \mathbb{R}$, ou é da forma

$$B_j = \begin{bmatrix} A_j & I & & \\ & A_j & \ddots & \\ & & \ddots & I \\ & & & A_j \end{bmatrix},$$

com $A_j = \begin{bmatrix} a_j & -b_j \\ b_j & a_j \end{bmatrix}$, $a_j, b_j \in \mathbb{R}$ e $b_j \neq 0$, e $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Sugestão: Considere a inclusão $M_n(\mathbb{R}) \subset M_n(\mathbb{C})$, e determine uma base apropriada para $\mathbb{R}^n$ à custa de uma base de $\mathbb{C}^n$ que transforme A na sua forma canónica de Jordan $J \in M_n(\mathbb{C})$. Para isso, considere casos separados para os valores próprios em $\mathbb{R}$ e em $\mathbb{C} \setminus \mathbb{R}$.

22. Aplicações das formas canónicas e dos factores invariantes e elementares

Recorde que um grupo G age à esquerda em si próprio por conjugação (Exemplo 9.8 do Capítulo 1). No caso particular de $G = GL_n(k)$, onde k é um corpo, podemos recorrer às formas canónicas racionais ou de Jordan para identificar as órbitas desta acção, i.e., as classes de conjugação do grupo $GL_n(k)$.

Considere o espaço vectorial-k $V = k^n$ com a estrutura de módulo-$k[x]$ induzida por $A \in GL_n(k)$. Então

$$k^n \cong \frac{k[x]}{(d_1(x))} \oplus \cdots \oplus \frac{k[x]}{(d_n(x))} \ , \tag{22.1}$$

como módulo-$k[x]$, onde $d_1(x) \mid \cdots \mid d_n(x) \neq 0$ são os factores invariantes (portanto únicos a menos do produto por unidades) da matriz $xI - A \in M_n(k[x])$. Podemos supor que os $d_i(x)$ são polinómios mónicos, pois $k^\times = k \setminus \{0\}$. Como $\dim_k V = n$, temos

$$\deg(d_1(x)) + \cdots + \deg(d_n(x)) = n \tag{22.2}$$

e, portanto, basta considerar as várias possibilidades para cada $d_i(x) \in k[x]$, tendo em conta as suas factorizações[13] em polinómios irredutíveis em $k[x]$.

Exemplo 22.1. Seja $n = 2$ e k um corpo qualquer. Seja $A \in GL_2(k)$ e sejam $d_1(x), d_2(x)$ os factores invariantes mónicos de $x - A$. Por (22.2), temos $\deg(d_1) = 0$ e $\deg(d_2) = 2$, ou $\deg(d_1) = \deg(d_2) = 1$.

Se $\deg(d_1) = \deg(d_2) = 1$, como $d_1 \mid d_2$ e ambos são mónicos, temos necessariamente $d_1(x) = d_2(x) = x - \lambda$, para algum $\lambda \in k$.

Se $\deg(d_1) = 0$ e $\deg(d_2) = 2$, temos $d_1(x) = 1$ e $d_2(x)$ ou é irredutível ou é da forma $d_2(x) = (x - \lambda)^2$ ou $d_2(x) = (x - \lambda)(x - \mu)$, com $\lambda \neq \mu$.

Obtemos os seguintes quatro tipos de formas racionais para a matriz A

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} , \quad \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} , \quad \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 0 & -a_0 \\ 1 & -a_1 \end{bmatrix} , \tag{22.3}$$

onde $\lambda, \mu \in k^\times$, $\lambda \neq \mu$ e $x^2 - a_1 x - a_0$ é irredutível em $k[x]$. No caso de k ser um corpo algebricamente fechado, nunca obtemos o último tipo. Note que as matrizes em (22.3) não são conjugadas entre si, pois correspondem a estruturas distintas de k^2 como módulo-$k[x]$, i.e., a decomposições (22.1) distintas.

Exemplo 22.2. Continuando o exemplo anterior com $n = 2$, seja agora $k = \mathbb{Z}_p$, com $p \in \mathbb{N}$ um primo. Logo há apenas um número finito de escolhas para λ, μ e polinómios irredutíveis $x^2 - a_1 x - a_0 \in \mathbb{Z}_p[x]$, portanto, não só temos um número finito de tipos de classes de conjugação, como temos mesmo um número total finito de classes.

No caso particular de $\mathbb{Z}_3 = \{0, 1, 2\}$, como $x^2 + 1$, $x^2 + x + 2$ e $x^2 + 2x + 2$ são os únicos polinómios mónicos, irredutíveis, de grau dois em $\mathbb{Z}_3[x]$, obtemos oito classes de conjugação em $GL_2(\mathbb{Z}_3)$, identificadas pelas seguintes formas canónicas racionais:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \text{ e } \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Seja k um corpo e $f(x) \in k[x]$ um polinómio não nulo de grau m. Recorde que o quociente $M = k[x]/(f(x))$ é um módulo-$k[x]$ com uma estrutura natural de espaço vectorial sobre k de dimensão $m = \deg(f)$ e

$$\mathcal{B}_M = \{\underline{1}, \underline{x}, \ldots, \underline{x}^{m-1}\}$$

[13] únicas pois $k[x]$ é um d.i.p., logo um d.f.u.

é uma base-k de M. Seja $g(x) \in k[x]$ um polinómio de grau n e considere $N = k[x]/(g(x))$. Portanto $V = M \otimes_k N$ é um espaço vectorial-k de dimensão $m+n$ e, tal como anteriormente, podemos dar-lhe uma estrutura de módulo-$k[x]$ através de uma aplicação linear-k, $T \in \mathrm{End}_k(V)$, pondo $x\mathbf{v} \coloneqq T(\mathbf{v})$. E podemos determinar a decomposição cíclica invariante ou primária à custa dos factores invariantes de $x - A \in M_{m+n}(k[x])$, onde $A \in M_{m+n}(k)$ é uma representação matricial de T, nalguma base-k de V. Por exemplo, como

$$\mathcal{B}_N = \{\underline{1}, \underline{x}, \ldots, \underline{x}^{n-1}\}$$

é uma base-k de N então, pelo Corolário 11.17,

$$\mathcal{B}_N \otimes \mathcal{B}_M \coloneqq \{\underline{x}^i \otimes \underline{x}^j \mid i = 0, \ldots, m-1,\ j = 0, \ldots, n-1\}$$

é uma base-k de V.

Exemplo 22.3. Sejam $f(x) = x^2 - 3$ e $g(x) = x^2 - 2x - 2$, sejam $M = \mathbb{Q}[x]/(f(x))$ e $N = \mathbb{Q}[x]/(g(x))$, seja $V = M \otimes_{\mathbb{Q}} N$ com a estrutura de módulo-$\mathbb{Q}[x]$ induzida por $T \in \mathrm{End}_k(M \otimes_{\mathbb{Q}} N)$, onde

$$T(\underline{a(x)} \otimes \underline{b(x)}) = \underline{xa(x)} \otimes \underline{xb(x)} \qquad \text{i.e.} \quad x(\underline{a(x)} \otimes \underline{b(x)}) \coloneqq \underline{xa(x)} \otimes \underline{xb(x)}\ .$$

Considere a base

$$\mathcal{B} = \{\mathbf{e}_1 = \underline{1} \otimes \underline{1}, \mathbf{e}_2 = \underline{1} \otimes \underline{x}, \mathbf{e}_3 = \underline{x} \otimes \underline{1}, \mathbf{e}_4 = \underline{x} \otimes \underline{x}\}\ .$$

Então

$$\begin{aligned}
T(\mathbf{e}_1) &= \underline{x} \otimes \underline{x} = \mathbf{e}_4\ , \\
T(\mathbf{e}_2) &= \underline{x} \otimes \underline{x}^2 = \underline{x} \otimes \underline{2x+2} = \underline{x} \otimes \underline{2x} + \underline{x} \otimes \underline{2} = 2\mathbf{e}_4 + 2\mathbf{e}_3\ , \\
T(\mathbf{e}_3) &= \underline{x}^2 \otimes \underline{x} = \underline{3} \otimes \underline{x} = 3\mathbf{e}_2\ , \\
T(\mathbf{e}_4) &= \underline{x}^2 \otimes \underline{x}^2 = \underline{3} \otimes \underline{2x+2} = \underline{3} \otimes \underline{2x} + \underline{3} \otimes \underline{2} = 6\mathbf{e}_2 + 6\mathbf{e}_1\ ,
\end{aligned}$$

donde

$$A = \begin{bmatrix} 0 & 0 & 0 & 6 \\ 0 & 0 & 3 & 6 \\ 0 & 2 & 0 & 0 \\ 1 & 2 & 0 & 0 \end{bmatrix}$$

é a matriz que representa T na base $\mathcal{B}$. Diagonalizando a matriz $x - A$:

$$x - A = \begin{bmatrix} x & 0 & 0 & -6 \\ 0 & x & -3 & -6 \\ 0 & -2 & x & 0 \\ -1 & -2 & 0 & x \end{bmatrix} \xrightarrow[L_2 \leftrightarrow L_3]{L_1 \leftrightarrow L_4} \begin{bmatrix} -1 & -2 & 0 & x \\ 0 & -2 & x & 0 \\ 0 & x & -3 & -6 \\ x & 0 & 0 & -6 \end{bmatrix}$$

$$\xrightarrow[L_3 - \frac{x}{2}L_2]{L_4 + xL_1} \begin{bmatrix} -1 & -2 & 0 & x \\ 0 & -2 & x & 0 \\ 0 & 0 & \frac{x^2}{2} - 3 & -6 \\ 0 & -2x & 0 & x^2 - 6 \end{bmatrix} \xrightarrow[C_4 + xC_1]{C_2 - 2C_1} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & x & 0 \\ 0 & 0 & \frac{x^2}{2} - 3 & -6 \\ 0 & -2x & 0 & x^2 - 6 \end{bmatrix}$$

$$\xrightarrow[L_4 - xL_2]{2L_3} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & x & 0 \\ 0 & 0 & x^2 - 6 & -12 \\ 0 & 0 & -x^2 & x^2 - 6 \end{bmatrix} \xrightarrow[L_4 + \frac{x^2-6}{12}L_3]{C_3 + \frac{1}{2}C_2} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & x^2 - 6 & -12 \\ 0 & 0 & -x^2 + \frac{(x^2-6)^2}{12} & 0 \end{bmatrix}$$

$$\xrightarrow{C_3 + \frac{x^2-6}{12}C_4} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & -12 \\ 0 & 0 & \frac{x^4 - 24x^2 + 36}{12} & 0 \end{bmatrix} \xrightarrow[C_3 \leftrightarrow C_4]{12L_4} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -12 & 0 \\ 0 & 0 & 0 & x^4 - 24x^2 + 36 \end{bmatrix},$$

obtemos que

$$V \cong \frac{\mathbb{Q}[x]}{(x^4 - 24x^2 + 36)}$$

é a decomposição invariante de V como módulo sobre $\mathbb{Q}[x]$.

Observação 22.4. Quando $T \in \mathrm{End}_k(M \otimes_k N)$ é obtido por $T = T_M \otimes T_N$, com $T_M \in \mathrm{End}_k(M)$ e $T_N \in \mathrm{End}_k(N)$ (recorde que $\otimes_k : \mathrm{Vect}_k \times \mathrm{Vect}_k \to \mathrm{Vect}_k$ é um functor), a matriz A para T na base $\mathcal{B} = \mathcal{B}_M \otimes \mathcal{B}_N$ é dada pelo chamado *produto de Kronecker* das matrizes A_M e A_N que representam T_M e T_N nas bases $\mathcal{B}_M$ e $\mathcal{B}_N$, respectivamente.

No exemplo anterior, A é o produto de Kronecker das matrizes

$$A_M = \begin{bmatrix} 0 & 3 \\ 1 & 0 \end{bmatrix} \quad \text{e} \quad A_N = \begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}$$

que são as formas racionais associadas ao produto pelo escalar x em M e N, respectivamente.

Exercícios

4.22.1. Determine as classes de conjugação dos grupos
(a) $GL_3(\mathbb{C})$;
(b) $GL_3(\mathbb{Z}_2)$;
(c) $GL_4(\mathbb{R})$.
Na alínea (b), indique explicitamente um representante de cada classe.

4.22.2. Decida se os seguintes pares de matrizes são conjugadas nos grupos indicados:

(a) $\begin{bmatrix} 0 & 0 & 0 & 4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ e $\begin{bmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ em $GL_4(\mathbb{Q})$;

(b) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$ e $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ em $GL_3(\mathbb{Z}_5)$;

(c) $\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ e $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ em $GL_4(\mathbb{Z}_2)$.

4.22.3. Considere o espaço vectorial-k (onde k é um corpo)

$$V = \frac{k[x]}{(f(x))} \otimes_k \frac{k[x]}{(g(x))}$$

com a estrutura de módulo-$k[x]$ induzida por $T \in \mathrm{End}_k(V)$ definido por

$$T\big(\underline{a(x)} \otimes \underline{b(x)}\big) = \underline{xa(x)} \otimes \underline{xb(x)} \ ,$$

para $a(x), b(x) \in k[x]$. Determine as decomposições cíclicas invariante e primária de V como módulo-$k[x]$ quando
(a) $f(x) = g(x) = x^2 - 3$ e $k = \mathbb{Q}$;
(b) $f(x) = (x-3)^2$, $g(x) = x^2 - 1$ e $k = \mathbb{C}$.

23. Módulos Noetherianos a Artinianos

Seja A um anel.

Definição 23.1. *Diz-se que $M \in \mathrm{Mod}_A$ é* Noetheriano *se toda a cadeia ascendente de submódulos de M:*

$$M_1 \subset M_2 \subset M_3 \subset \cdots M_n \subset \cdots$$

termina, i.e.*, existe $N \in \mathbb{N}$ tal que $M_n = M_N$, para $n \geq N$.*

Diz-se que M é Artiniano *se toda a cadeia descendente de submódulos de M:*

$$M_1 \supset M_2 \supset \cdots \supset M_n \cdots$$

termina, i.e.*, existe $N \in \mathbb{N}$ tal que $M_n = M_N$, para $n \geq N$.*

Exemplo 23.2. Seja $A = D$ um anel de divisão e seja $V \in \mathrm{Vect}_D$. Então as cadeias de submódulos são cadeias de subespaços-D, logo V é noetheriano *sse* V é Artiniano *sse* $\dim_D V$ é finita.

Exemplo 23.3. Seja $A = \mathbb{Z}$ e $M = \mathbb{Z}$, então M é Noetheriano: as cadeias de submódulos são cadeias de ideais. Temos

$$(k_1) \subset (k_2) \subset \cdots \subset (k_n) \subset \cdots$$

sse $k_n \mid k_{n-1} \mid \cdots \mid k_2 \mid k_1$, portanto o número de inclusões próprias é limitado pelo número de factores primos de k_1. No entanto, M não é Artiniano pois a cadeia

$$(2) \supset (4) \supset \cdots \supset (2^n) \supset \cdots$$

não termina.

Proposição 23.4. *$M \in \mathrm{Mod}_A$ é Noetheriano* sse *todos os submódulos de M são finitamente gerados.*

Demonstração. $\boxed{\Rightarrow}$ Seja $N \subset M$ um submódulo. Se N não é finitamente gerado, existe uma sucessão $\{\mathbf{v}_n\}_{n\in\mathbb{N}} \subset N$ tal que $\mathbf{v}_{n+1} \notin \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$, logo

$$\langle \mathbf{v}_1 \rangle \subset \langle \mathbf{v}_1, \mathbf{v}_2 \rangle \subset \cdots \subset \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle \subset \cdots$$

não termina.

$\boxed{\Leftarrow}$ Seja

$$M_1 \subset \cdots \subset M_n \subset \cdots$$

uma cadeia ascendente de módulos-A. Sejam $\mathbf{v}_1, \ldots, \mathbf{v}_r$ geradores de $\cup_n M_n$. Seja $k \in \mathbb{N}$ tal que $\mathbf{v}_1, \ldots, \mathbf{v}_r \in M_k$. Temos $M_n = M_k$, para $n \geq k$. □

Definição 23.5. *Seja A um anel. Se A é Noetheriano como um módulo-A esquerdo (direito), diz-se que A é* Noetheriano à esquerda (resp. direita)*. Se A é Noetheriano à esquerda e à direita, diz-se que é* Noetheriano*.*

Se A é Artiniano como módulo-R esquerdo (direito), diz-se que R é Artiniano à esquerda (resp. direita)*. Se R é Artiniano à esquerda e à direita, diz-se que é* Artiniano*.*

Observação 23.6. Um anel A é Artiniano (Noetheriano) à esquerda *sse* as cadeias descendentes (resp. ascendentes) de ideais esquerdos terminam.

Teorema 23.7. *Seja A um anel Artiniano (Noetheriano) à esquerda. Então todo o módulo-R finitamente gerado é Artiniano (resp. Noetheriano).*

Demonstração. Começamos por considerar o caso de módulos com um gerador. Se $M \in \mathrm{Mod}_A$ é cíclico, temos $M \cong A/I$, para algum ideal esquerdo $I \subset A$. Os submódulos $N \subset M$ são da forma $N = J/I$, onde $J \supset I$ é um ideal. Portanto, se A é Artiniano (Noetheriano) segue que M é Artiniano (resp. Noetheriano).

Prosseguimos a demonstração por indução no número de geradores. Suponhamos que o resultado é válido para módulos com $n-1$ geradores ou menos.

Seja M um módulo com n geradores: $M = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$. Consideremos a sucessão exacta

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

onde $M' = \langle \mathbf{v}_1, \ldots, \mathbf{v}_{n-1} \rangle$ e $M'' = M/M' = \langle \pi(\mathbf{v}_n) \rangle$ Por hipótese, os módulos M', M'' são Artinianos. Consideremos uma cadeia descendente

$$M_1 \supset M_2 \supset \cdots \supset M_k \supset \cdots \supset M_n \supset \cdots$$

Seja $k \in \mathbb{N}$ tal que, para $n \geq k$, $M_n \cap M' = M_k \cap M'$ e $\pi(M_n) = \pi(M_k)$. Temos o morfismo de sucessões exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_n \cap M' & \longrightarrow & M_n & \xrightarrow{\pi} & \pi(M_n) & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle i} & & \| & & \\ 0 & \longrightarrow & M_k \cap M' & \longrightarrow & M_k & \xrightarrow{\pi} & \pi(M_k) & \longrightarrow & 0, \end{array}$$

onde i é a inclusão. Pelo Lema dos Cinco (Exercício 4.4.4), segue $M_n = M_k$, para $n \geq k$. □

Corolário 23.8. *Se A é um* d.i.p. *e se $M \in \mathrm{Mod}_A$ é finitamente gerado, então M é Noetheriano.*

Demonstração. Nas condições do enunciado, A é Noetheriano pois todos os seus ideais sendo principais são finitamente gerados. O resultado segue do Teorema 23.7. □

24. Módulos semi-simples

Definição 24.1. *Seja M um módulo-A não trivial. Diz-se que M é* simples *se M não tem submódulos próprios não triviais. Se $M = \bigoplus_\alpha M_\alpha$, onde cada M_α é simples, diz-se que M é* semi-simples.

Exemplos 24.2.

1. Se $A = \mathbb{Z}$ os módulos-A simples são os grupos abelianos simples, *i.e.*, são isomorfos a $\mathbb{Z}_p$, com p primo.
2. Se $A = \mathbb{Z}$, $M = \mathbb{Z}_6$ é um módulo-A semi-simples, pois $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$.
3. Se $A = D$ é um anel de divisão, então $V \in \mathrm{Mod}_A = \mathrm{Vect}_D$ é simples *sse* $\dim_D M = 1$. Todo o espaço vectorial-D é semi-simples.

Lema 24.3. *Seja $M \in \mathrm{Mod}_A$ tal que existem $M_\alpha \subset M$, $\alpha \in I$, submódulos simples, satisfazendo $M = \sum_{\alpha \in I} M_\alpha$ (soma não necessariamente directa). Seja $N \subsetneq M$ um submódulo, então existe $J \subset I$ tal que*

$$M = N \oplus \Big(\bigoplus_{\alpha \in J} M_\alpha \Big).$$

Em particular, existe $J \subset I$ tal que $M = \bigoplus_{\alpha \in J} M_\alpha$.

Demonstração. Seja $\mathcal{F} = \{K \subset I \mid N + \sum_{\alpha \in K} M_\alpha \text{ é soma directa}^{14}\}$. Para cada $\alpha \in I$, como M_α é simples, temos

$$M_\alpha \cap N = \{0\} \quad \text{ou} \quad M_\alpha \cap N = M_\alpha.$$

Logo $\mathcal{F} \neq \varnothing$, pois, por hipótese, existe α tal que $M_\alpha \not\subset N$, e portanto $N + M_\alpha$ é uma soma directa.

[14] Ou seja, $N + \sum_{\alpha \in K} M_\alpha$ é a soma directa interna de N e $\{M_\alpha\}_{\alpha \in K}$

Dado $K \subset I$, temos $K \in \mathcal{F}$ se e só se

$$\forall_{K_0 \subset K} |K_0| < \infty \Rightarrow N \cap \sum_{\alpha \in K_0} M_\alpha = \{0\} \wedge \sum_{\alpha \in K_0} M_\alpha \text{ é soma directa.}$$

Daqui segue facilmente que $\mathcal{F}$ é parcialmente ordenado pela relação de inclusão e, com esta relação, se $\{K_t\}$ é uma cadeia em $\mathcal{F}$, o conjunto $K = \cup_t K_t \in \mathcal{F}$ é um majorante de $\{K_t\}$. Pelo Lema de Zorn, existe $J \in \mathcal{F}$ maximal. Como cada M_β é simples, temos

$$\forall_{\beta \in I \setminus J} \quad M_\beta \cap \Big(N + \sum_{\alpha \in J} M_\alpha\Big) = \{0\} \quad \text{ou} \quad M_\beta,$$

e por maximalidade de J, temos $M_\beta \cap \big(N + \sum_{\alpha \in J} M_\alpha\big) = M_\beta$, logo

$$M = \sum_{\beta \in I} M_\beta \subset N + \sum_{\alpha \in J} M_\alpha,$$

donde

$$M = N \oplus \Big(\bigoplus_{\alpha \in J} M_\alpha\Big). \qquad \square$$

Teorema 24.4. *Seja A um anel e seja $M \in \mathrm{Mod}_A$. ASCSE*

(a) $\exists \{M_\alpha\}_{\alpha \in I} : M_\alpha \subset M$ é submódulo simples e $M = \sum_{\alpha \in I} M_\alpha$;

(b) M é semi-simples;

(c) todo o submódulo $N \subset M$ é um somando directo.

Demonstração. $\boxed{(a) \Rightarrow (b)}$ Segue do Lema 24.3 (caso $N = \{0\}$).

$\boxed{(b) \Rightarrow (c)}$ Segue do Lema 24.3, pois, por definição, se M é semi-simples, M é soma de submódulos simples.

$\boxed{(c) \Rightarrow (a)}$ Seja $S = \{\sum_\alpha M_\alpha \mid M_\alpha \subset M \text{ é submódulo simples}\}$. Então $S \subset M$ é um submódulo, logo existe um submódulo $N \subset M$ tal que $M = S \oplus N$. Suponhamos $N \neq \{0\}$. Seja $C \subset N$ um submódulo cíclico tal que $C \neq \{0\}$. Seja $C' \subset C$ um submódulo próprio maximal (*cf.* Exercício 24.5). Por maximalidade de C', C/C' é simples e, por (c), existe um submódulo $C'' \subset C$ tal que

$$C = C' \oplus C''.$$

Daqui segue que $C'' \cong C/C'$ é um submódulo simples, o que contraria a definição de N. Concluímos que $M = S$. $\square$

Exercício 24.5. *Seja N um módulo-A finitamente gerado, não nulo. Mostre que existe um submódulo próprio maximal $N' \subset N$.*

Corolário 24.6. *Seja $M \in \mathrm{Mod}_A$ semi-simples, $M = \bigoplus_{\alpha \in I} M_\alpha$, com M_α simples. Então, dado um submódulo $N \subset M$ existem $J, K \subset I$ tais que*

$$N \cong \bigoplus_{\alpha \in K} M_\alpha \quad e \quad M = N \oplus \Big(\bigoplus_{\alpha \in J} M_\alpha\Big).$$

Demonstração. O subconjunto $J \subset I$ pode ser escolhido como no Lema 24.3. Temos

$$M = N \oplus \Big(\bigoplus_{\alpha \in J} M_\alpha\Big) = \Big(\bigoplus_{\alpha \in I \setminus J} M_\alpha\Big) \oplus \Big(\bigoplus_{\alpha \in J} M_\alpha\Big),$$

logo

$$N \cong M/\bigoplus_{\alpha \in J} M_\alpha \cong \bigoplus_{\alpha \in I \setminus J} M_\alpha.$$

Portanto, podemos escolher $K = I \setminus J$. $\square$

Corolário 24.7. *Seja $M \in \mathrm{Mod}_A$ semi-simples e seja $N \subset M$ um submódulo. Então N e M/N são semi-simples.*

Lema 24.8 (Schur)**.** *Sejam S, M módulos-A tais que S é simples e seja $\varphi \in \mathrm{Hom}_A(S, M)$. Então $\varphi(S) = \{0\}$ ou $\varphi(S) \cong S$. Em particular, $\mathrm{End}_A(S)$ é um anel de divisão.*

Demonstração. Seja $\varphi \in \mathrm{Hom}_A(S, M)$, temos $\ker\varphi = \{0\}$ ou $\ker\varphi = S$. Se $\varphi \in \mathrm{End}_A(M)$ é tal que $\varphi \neq 0$, temos $\ker\varphi = 0$ e $\mathrm{im}\,\varphi = M$. Concluímos que φ é um isomorfismo, logo tem um inverso como elemento de $\mathrm{End}_A(S)$. □

Corolário 24.9. *Sejam $M, M' \in \mathrm{Mod}_A$ tais que $M = \bigoplus_{\alpha\in I} M_\alpha$, $M' = \bigoplus_{\beta\in J} M'_\beta$ com M_α, M'_β módulos simples (portanto M, M' são semi-simples) e $\forall_{\alpha,\beta}\ M_\alpha \ncong M'_\beta$. Então* $\mathrm{Hom}_A(M, M') = 0$.

Demonstração. Pelo Exercício 4.4.1 temos

$$\mathrm{Hom}_A(M, M') \cong \prod_{\alpha} \mathrm{Hom}_A(M_\alpha, M') \subset \prod_{\alpha,\beta} \mathrm{Hom}_A(M_\alpha, M'_\beta) = 0. \qquad \square$$

Proposição 24.10. *Sejam $H_1, \ldots, H_r$ módulos-A semi-simples tais que, para cada i, H_i é da forma $N_i^{n_i}$, com N_i simples e $N_i \ncong N_j$, se $i \neq j$. Seja $N \cong \oplus_{i=1}^r H_i$. Então*

$$\mathrm{End}_A(N) \cong \prod_{i=1}^{r} \mathrm{End}_A(H_i) \cong \prod_{i=1}^{r} M_{n_i}\big(\mathrm{End}_A(N_i)\big).$$

Demonstração. Seja $f \in \mathrm{End}_A(M)$. Pelo Corolário 24.9, temos $f(H_i) \subset H_i$. O último isomorfismo é consequência dos resultados sobre homomorfismos e matrizes. □

Capítulo 5

Teoria de estrutura de anéis

1. Anéis simples Artinianos: 1º Teorema de Wedderburn

Definição 1.1. *Um anel A diz-se* simples *se $A \neq 0$ e A não tem ideais próprios. Diz-se que A é semi-simples à esquerda (direita) se A é semi-simples como módulo-A à esquerda (resp. direita).*

Exemplo 1.2. De acordo com o Exercício 2.2.9, se D é um anel de divisão $M_n(D)$ é simples.

Observação 1.3. Um anel A pode ser simples sem ser semi-simples à esquerda (direita). De facto vamos ver que

$$A \text{ semi-simples à esquerda} \Rightarrow A \text{ semi-simples à direita e Artiniano e Noetheriano,}$$

mas há anéis simples que não são Artinianos nem Noetherianos.

Exercício 1.4. *Seja $\mathbb{R}^\infty \coloneqq \bigoplus_{n=1}^{\infty} \mathbb{R}$. Consideremos o anel $A = \mathrm{End}_{\mathbb{R}}(\mathbb{R}^\infty)$ e o ideal $I = \{f \in A \mid \dim_{\mathbb{R}} \mathrm{im}\, f < \infty\}$.*

(a) Seja $f \in A \setminus I$. Mostre que existem $l, r \in A$ tais que $lfr = 1_A$. Conclua que A/I é simples.

(b) Seja $\{\mathbf{v}_{ij} \mid i, j \in \mathbb{N}\}$ uma base de $\mathbb{R}^\infty$ e seja $J_n = \{f \in R \mid \forall_{i \geq n} f(\mathbf{v}_{ij}) = 0\}$. Mostre que

$$J_1 + I \supsetneq J_2 + I \supsetneq \cdots \supsetneq J_n + I \supsetneq \cdots$$

é uma cadeia descendente de ideais esquerdos de A/I que não termina.

Observação 1.5. 1. Um ideal esquerdo $I \subset A$ diz-se *minimal* se $I \neq 0$ e

$$\forall_{J \text{ ideal}}\, J \subset I \Rightarrow J = I \vee J = 0.$$

Os submódulos esquerdos simples de A são exactamente os ideais esquerdos minimais.

2. Se A é um anel Artiniano à esquerda, então A tem um ideal minimal esquerdo: basta tomar $I_0 = R$ e construir uma cadeia de ideais esquerdos

$$I_0 \supsetneq I_1 \supsetneq I_2 \supsetneq \cdots \supsetneq I_n$$

até que a cadeia não admita extensões. O ideal I_n é minimal.

Exemplo 1.6. Seja D um anel de divisão. Recorde-se os elementos $E_{ij} = (\delta_{ij} \cdot 1_D) \in M_n(D)$. Os elementos do ideal esquerdo $I \coloneqq M_n(D) \cdot E_{11}$ são da forma $\begin{bmatrix} \mathbf{v} & \mathbf{0} \end{bmatrix}$ tal que $\mathbf{v} \in D^n$.

Vejamos que I é minimal. Sejam $J \subset I$ e $A = \begin{bmatrix} \mathbf{v} & \mathbf{0} \end{bmatrix} \in J$ tal que $v_j \neq 0$. Então $E_{11} = v_j^{-1} E_{1j} A$, logo $J = I$.

Teorema 1.7 (1º Teorema de Wedderburn)**.** *Seja A um anel. ASCSE*

(a) A é simples e Artiniano à esquerda;

(b) A é um anel não trivial, semi-simples à esquerda tal que todos os módulos-A simples são isomorfos;

(c) $A \cong M_n(D)$ para algum $n \in \mathbb{N}$ e algum anel de divisão D.

Em (c) o número n é unicamente determinado por A, e D é unicamente determinado a menos de isomorfismo.

Observação 1.8. A versão do 1º Teorema de Wedderburn para módulos à direita também é válida.

Demonstração. $\boxed{(a) \Rightarrow (b)}$ Seja $I \neq 0$ um ideal esquerdo minimal. Por minimalidade de I, temos

$$\forall_{c \in I \setminus (0)} \quad I = Ac.$$

Fixemos $c \in I \setminus (0)$. Por A ser simples, vem

$$A = AcA = \sum_{a \in A} Aca.$$

Consideremos o homomorfismo

$$\varphi \colon I = Ac \to Aca;\ bc \mapsto bca.$$

Claramente φ é um epimorfismo, logo temos $Aca \cong Ac = I$, se $\ker \varphi = 0$, ou, se $\ker \varphi = I$, é $Aca = 0$. Concluímos que A é uma soma de módulos simples (isomorfos a I) e portanto A é semi-simples à esquerda.

Seja M um módulo-A simples. Como M é cíclico, existe um ideal esquerdo $J \subset A$ tal que $M \cong R/J$. Pelo Lema 24.3 do Capítulo 4, existe $B \subset A$ tal que

$$A = J \oplus \Big(\bigoplus_{a \in B} Aca \Big),$$

logo

$$A/J \cong \bigoplus_{a \in B} Aca \cong \bigoplus_{a \in B} I.$$

Portanto $|B| = 1$ e $M \cong I$.

$\boxed{(b) \Rightarrow (c)}$ Note-se que A é um módulo-A finitamente gerado, pois $A = \langle 1 \rangle$. Logo, se A é semi-simples à esquerda, temos

$$A = \bigoplus_{i=1}^{n} I_i,$$

onde $I_1, \ldots, I_n$ são ideais esquerdos minimais. Por hipótese, $I_1, \ldots, I_n$ são isomorfos a um módulo-A comum, digamos, $I_i \cong U$. Portanto,

$$A \cong U^n$$

Pelo Lema de Schur, $D' \coloneqq \mathrm{End}_A(U)$ é um anel de divisão. Temos

$$\mathrm{End}_A(U^n) \cong M_n(\mathrm{End}_A(U)) \cong M_n(D').$$

Por outro lado,

$$\mathrm{End}_A(U^n) \cong \mathrm{End}_A(A) \cong A^{op},$$

logo

$$A \cong M_n(D')^{op} \cong M_n(D'^{op}),$$

onde o último isomorfismo é dado por transposição de matrizes: $X \mapsto X^T$. Concluímos que

$$A \cong M_n(D),$$

onde D é o anel de divisão D'^{op}.

O Exercício 1.9 mostra que n é determinado pelo tipo de isomorfismo A. O tipo de isomorfismo de U é determinado por A: se $U' \in \mathrm{Mod}_A$ é simples e $U' \ncong U$, temos

$$\mathrm{Hom}_A(U', A) \cong \big(\mathrm{Hom}_A(U', U)\big)^n \cong 0 \ncong \mathrm{Hom}_A(U, A) \cong (\mathrm{End}_A(U))^n.$$

Como $D \cong \big(\mathrm{End}_A(U)\big)^{op}\big)$, o tipo de isomorfismo de D é determinado pelo por A.

$\boxed{(c) \Rightarrow (a)}$ Note-se que $M_n(D)$ é um espaço vectorial-D de dimensão finita e os ideais de $M_n(D)$ são subsespaços-D, logo $M_n(D)$ é Artiniano à esquerda. Por último, notamos que $M_n(D)$ é simples (Exercício 2.2.9). □

Exercício 1.9. *Seja D um anel de divisão. Mostre que*

(a) se $V \subset D^n$ é um subespaço-D, ${}_VI \coloneqq \{X \in M_n(D) \mid XV = 0\}$ é um ideal esquerdo de $M_n(D)$;

(b) se, para cada ideal esquerdo $I \subset M_n(D)$, definirmos o subsespaço-D

$$ {}_IV \coloneqq \bigcap_{X \in I} \ker X,$$

então as correspondências $V \mapsto {}_VI$ e $I \mapsto {}_IV$ são inversas uma da outra e invertem inclusões; $V \subset W \Rightarrow {}_WI \subset {}_VI$ e $I \subset J \Rightarrow {}_JV \subset {}_IV$;

(c) n é o comprimento máximo das cadeias de ideais esquerdos de $M_n(D)$, i.e.*, n é o máximo $k \in \mathbb{N}$ tal que existe uma cadeia*

$$\{0\} \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_k,$$

de ideais esquerdos de $M_n(D)$. Em particular, o tipo de isomorfismo de $A = M_n(D)$ determina n.

Definição 1.10. *Seja K um anel comutativo. Define-se uma* álgebra sobre K *como um anel A com uma estrutura de módulo-K tal que a multiplicação em A é bilinear,* i.e.*,*

$$\forall_{x,y \in A} \forall_{\alpha \in K} \quad \alpha(xy) = (\alpha x)y = x(\alpha y).$$

Exemplos 1.11. 1. Todo o anel A é uma álgebra-$\mathbb{Z}$;

2. $\mathbb{R}[x]$ é uma álgebra-$\mathbb{R}$;

3. $M_n(K)$ é uma álgebra-K, para qualquer anel comutativo K;

4. se D é um anel de divisão, então $k \coloneqq Z(D) = \{d \in D \mid \forall_{d' \in D} dd' = d'd\}$ é um corpo e D é uma álgebra sobre k;

5. $M_n(D)$ é uma uma álgebra-k.

Corolário 1.12. *Seja A um anel simples e Artiniano à esquerda. Então A é uma álgebra sobre um corpo.*

2. Anéis semi-simples: 2º Teorema de Wedderburn

Teorema 2.1 (2º Teorema de Wedderburn)**.** *Seja A um anel semi-simples à esquerda. Então*

$$A \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r), \tag{2.1}$$

onde $D_1, \ldots, D_r$ são anéis de divisão determinados por A a menos de isomorfismo e $n_1, \ldots, n_r \in \mathbb{N}$ são determinados por A. Reciprocamente, se A é um anel como em (2.1)*, então A é semi-simples à esquerda.*

Em particular, se A é um anel semi-simples à esquerda, então A é semi-simples à direita e é Artiniano (à esquerda e à direita).

Demonstração. Seja A um anel semi-simples à esquerda. Como A é um módulo-A finitamente gerado, temos

$$A = H_1 \oplus \cdots \oplus H_r,$$

onde $H_i \cong I_i^{n_i}$, para algum ideal esquerdo minimal $I_i \subset A$ e, $H_i \ncong H_j$, para $i \neq j$.

Pelo Lema de Schur, $\mathrm{End}_A(I_i) = D_i^{op}$ é um anel de divisão. Temos

$$\mathrm{End}_A(H_i) \cong M_{n_i}(D_i^{op})$$

e

$$A^{op} \cong \mathrm{End}_A(A) \cong \prod_{i=1}^{r} \mathrm{End}_A(H_i) \cong \prod_{i=1}^{r} M_{n_i}(D_i^{op}),$$

logo

$$A \cong \prod_{i=1}^{r} M_{n_i}(D_i),$$

onde (pelo Teorema 1.7) n_i, e o tipo de isomorfismo de D_i são determinados pelo tipo de isomorfismo de H_i, que é determinado por A.

Reciprocamente, se D_i é um anel de divisão, temos $M_{n_i}(D_i) \cong I_i^{n_i}$, onde I_i é o ideal esquerdo minimal $M_{n_i}(D_i) \cdot E_{11}$. Daqui segue que

$$A \cong \prod_{i=1}^{r} M_{n_i}(D_i) \cong \bigoplus_{i=1}^{r} I_i^{n_i}$$

é semi-simples à esquerda, pois cada I_i é um módulo-A simples (por ser um módulo-$M_{n_i}(D_i)$ simples).

É fácil de ver que A é Artiniano à esquerda porque cada $M_{n_i}(D_i)$ o é.

Aplicando transposição de matrizes a $A = \prod_i M_{n_i}(D_i)$ segue que A é também semi-simples à direita e artiniano à direita, pois esta operação induz uma bijecção entre ideais esquerdos e ideais direitos. □

Capítulo 6

Teoria de representação de grupos

1. Representações

Recorde que uma acção de um grupo G num conjunto X é uma aplicação $G \times X \to X$, $(g, x) \mapsto g \cdot x$, tal que $\mathbf{1}_G \cdot x = x$ e $g \cdot (h \cdot x) = (gh) \cdot x$ para todo o $x \in X$ e $g, h \in G$. Recorde ainda que dar uma acção de G em X é equivalente a dar um homomorfismo de grupos $G \to S_X$.

Definição 1.1. *Seja G um grupo e k um corpo. Uma* representação *de G sobre k é um espaço vectorial $V \in \mathrm{Vect}_k$ com uma acção $G \times V \to V$ tal que, para cada $g \in G$, a aplicação bijectiva $V \to V, v \mapsto g \cdot v$, é linear-$k$. A dimensão $\dim_k V$ diz-se a* dimensão da representação V.

Ou seja, em termos do homomorfismo $\rho\colon G \to S_V$ associado à acção, a sua imagem está contida em $\mathrm{Aut}_k(V)$, por isso, passamos a escrever $\rho\colon G \to \mathrm{Aut}_k(V)$. Se $\dim_k V = n$ é finita, então $Aut_k(V) \cong GL_n(k)$ (isomorfismo dado fixando uma base para V) e também escrevemos $\rho\colon G \to GL_n(k)$.

Notação 1.2. Denotamos por (V, ρ), ou apenas por V, uma representação-k de G.

Definição 1.3. *Duas representações (V_1, ρ_1) e (V_2, ρ_2) do grupo G dizem-se* equivalentes *ou* isomorfas *se existe um isomorfismo $f \in \mathrm{Hom}_k(V_1, V_2)$ tal que f é equivariante-G, i.e.,*

$$f(\rho_1(g)(\mathbf{v})) = \rho_2(g)(f(\mathbf{v})) \quad \forall\, \mathbf{v} \in V_1 \ .$$

Definição 1.4.

- *Quando a acção de G em V é trivial, i.e., quando $g \cdot \mathbf{v} = \mathbf{v}$ para qualquer $g \in G$ e $\mathbf{v} \in V$, o que é equivalente a $\rho(g) = \mathrm{id}_V$ para qualque $g \in G$, V diz-se uma* representação trivial.
- *Seja $\mathcal{B} = \{e_i \mid i \in I\}$ uma base-k de V. Se a acção permuta os elementos de $\mathcal{B}$, i.e., para cada $g \in G$ tem-se $\rho(g)(\mathcal{B}) = \mathcal{B}$, V diz-se uma* representação de permutação.

Exemplo 1.5. Seja $G = S_3$ e $V = k^3$ com base canónica $\{\mathbf{e}_i\}_{i \in \{1,2,3\}}$. Seja $\rho\colon S_3 \to GL_3(k)$ dado por

$$\rho(12) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \text{e} \qquad \rho(123) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \ .$$

Como (12) e (123) geram S_3, $\rho(12)$ e $\rho(123)$ são matrizes de ordens 2 e 3, respectivamente, e $\rho(12)\rho(123)\rho(12) = \rho(132)$ (recorde que $S_3 \cong D_3$), então ρ está bem definida e é um homomorfismo de grupos. Note ainda que a acção de cada $\sigma \in S_3$ em k^3 é precisamente $\rho(\sigma)(\mathbf{e}_i) = \mathbf{e}_{\sigma(i)}$, portanto (k^3, ρ) é uma representação de permutação de S_3.

Compondo o homomorfismo ρ com o determinante $\det\colon GL_3(k) \to k^\times = GL_1(k)$ obtemos uma representação de S_3 de dimensão 1

$$\operatorname{sgn}\colon S_3 \to k^\times\,, \quad \sigma \mapsto \operatorname{sgn}(\sigma)$$

a que chamamos *representação sinal* de S_3.

O exemplo 3.16 do Capítulo 1 generaliza o exemplo anterior para S_n, $n \geq 2$.

Exemplo 1.6. Seja G um grupo cíclico de ordem 2, i.e., $G = \{\mathbf{1}_G, a\}$ com $a^2 = \mathbf{1}_G$, e k um corpo. Seja (k, ρ) uma representação de G de dimensão 1. Então $\rho(a)$ é a multiplicação por um escalar[1] $x \in k$ tal que $x^2 = 1$, i.e., uma raiz do polinómio $x^2 - 1 \in k[x]$.

Se a característica de k não é 2, i.e., se $-1 \neq 1$, então G tem duas representações de dimensão 1: a trivial, que corresponde a escolher $\rho(a) = 1$, e a *representação sinal*, que corresponde a escolher $\rho(a) = -1$.

Se a característica de k é 2 (por exemplo, $k = \mathbb{Z}_2$), i.e., se $-1 = 1$, então G tem apenas uma representações de dimensão 1: a trivial.

Exemplo 1.7. Seja G um grupo cíclico de ordem $n \in \mathbb{N}$, i.e., $G = \langle a \mid |a| = n\rangle$. Seja $\rho\colon G \to GL_2(\mathbb{R})$ dado por

$$\rho(a) = \begin{bmatrix} \cos(\frac{2\pi}{n}) & -\operatorname{sen}(\frac{2\pi}{n}) \\ \operatorname{sen}(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{bmatrix}\,.$$

Como $\rho(a)$ é uma matriz invertível de ordem n, ρ é um homomorfismo de grupos bem definido e $(\mathbb{R}^2, \rho)$ é uma representação de G. Note que $\rho(a)$ é a rotação do plano $\mathbb{R}^2$, de centro na origem, de um ângulo $2\pi/n$.

Exemplo 1.8. Seja $G = D_n = \langle a, b \mid |a| = n, |b| = 2, bab^{-1} = a^{-1}\rangle$, e seja $\rho : G \to GL_2(\mathbb{R})$ dado por $\rho(a)$ do exemplo anterior (afinal $\langle a\rangle$ é o subgrupo das rotações de D_n) e

$$\rho(b) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\,.$$

Então $\mathbb{R}^2$ com esta acção é uma representação de D_n. Note que $\rho(b)$ é a reflexão do plano em relação ao eixo vertical.

Proposição 1.9. *Seja G um grupo. Há uma bijecção entre representações de dimensão 1 de G e de $G/[G,G]$*

Demonstração. Seja V uma representação de G de dimensão 1 e seja $\rho\colon G \to GL_1(k)$ o homomorfismo de grupo associado à acção de G em V. Como $GL_1(k) \cong k^\times$ é um grupo abeliano, pela Proposição 12.22 do Capítulo 1, temos $\ker\rho > [G,G]$ e portanto, pela propriedade universal do quociente $G/[G,G]$, existe um único homomorfismo de grupos $\bar\rho\colon G/[G,G] \to GL_1(k)$ tal que $\rho = \bar\rho \circ \pi$, onde $\pi : G \to G/[G,G]$ é a projecção canónica.

Reciprocamente, dada uma representação (k, σ) de dimensão 1 de $G/[G,G]$, então a composta $\sigma \circ \pi\colon G \to GL_1(k)$ define uma representação de G.

Como estas correspondências são a inversa uma da outra, obtemos a bijeção pretendida. □

Exemplo 1.10. Seja $G = S_3$ e $k = \mathbb{R}$. Como $[S_3, S_3] = A_3$ e S_3/A_3 é cíclico de ordem 2, pelo Exemplo 1.6 e pelo lema anterior, concluímos que S_3 tem duas representações de dimensão 1: a trivial e a representação sinal do Exemplo 1.5.

[1] $\operatorname{Aut}_k(k) = GL_1(k) = k^\times$

O exemplo anterior generaliza-se para qualquer S_n, com $n \geq 2$, pois $[S_n, S_n] = A_n$.

Definição 1.11. *Sejam (V_1, ρ_1) e (V_2, ρ_2) duas representações-k do grupo G.*

- $V_1 \oplus V_2 \in \mathrm{Vect}_k$ *com a acção $\rho_1 \oplus \rho_2$ definida por*

$$g \cdot (\mathbf{v}_1, \mathbf{v}_2) = (\rho_1(g)(\mathbf{v}_1), \rho_2(g)(\mathbf{v}_2)) \qquad \forall\, g \in G \quad \forall\, \mathbf{v}_i \in V_i$$

  diz-se a representação soma directa.

- $V_1 \otimes V_2 \in \mathrm{Vect}_k$ *com a acção $\rho_1 \otimes \rho_2$ definida por*

$$g \cdot (\mathbf{v}_1 \otimes \mathbf{v}_2) = (\rho_1(g)(\mathbf{v}_1)) \otimes (\rho_2(g)(\mathbf{v}_2)) \qquad \forall\, g \in G \quad \forall\, \mathbf{v}_i \in V_i$$

  diz-se a representação produto tensorial.

Exemplo 1.12. A soma directa de representações triviais é trivial.

Proposição 1.13. *Sejam (V_1, ρ_1) e (V_2, ρ_2) representações de G, de dimensões finitas $\dim_k V_1 = n$ e $\dim_k V_2 = m$. Sejam $\{\mathbf{e}_1 \ldots, \mathbf{e}_n\}$ e $\{\mathbf{f}_1 \ldots, \mathbf{f}_m\}$ bases de V_1 e V_2, respectivamente, e sejam $A(g) = [a_{rs}]$ e $B(g) = [b_{rs}]$ as matrizes de $\rho_1(g)$ e $\rho_2(g)$ nesssas bases. Então*

(a)

$$A(g) \oplus B(g) \coloneqq \begin{bmatrix} A(g) & 0 \\ 0 & B(g) \end{bmatrix} \in GL_{n+m}(k)$$

é a matriz de $(\rho_1 \oplus \rho_2)(g)$ na base $\{\mathbf{e}_1, \ldots, \mathbf{e}_n, \mathbf{f}_1, \ldots, \mathbf{f}_m\}$ de $V_1 \oplus V_2$;

(b)

$$A(g) \otimes B(g) \coloneqq \begin{bmatrix} a_{11}B(g) & a_{12}B(g) & \cdots & a_{1n}B(g) \\ \vdots & \vdots & & \vdots \\ a_{n1}B(g) & a_{n2}B(g) & \cdots & a_{nn}B(g) \end{bmatrix} \in GL_{nm}(k)$$

é a matriz de $(\rho_1 \otimes \rho_2)(g)$ na base $\{\mathbf{e}_i \otimes \mathbf{f}_j \mid i = 1, \ldots, n, j = 1, \ldots, m\}$ de $V_1 \otimes V_2$.

Demonstração. (a) Óbvio.

(b) Pelo Corolário 11.17 do Capítulo 4 temos que $\mathcal{B} \coloneqq \{\mathbf{e}_i \otimes \mathbf{f}_j \mid i = 1, \ldots, n, j = 1, \ldots, m\}$ é uma base-k de $V_1 \otimes V_2$. Portanto basta escrever $(\rho_1 \otimes \rho_2)(\mathbf{e}_i \otimes \mathbf{f}_j)$ como uma combinação linear dos elementos em $\mathcal{B}$ com coeficiente em k. Temos

$$(\rho_1 \otimes \rho_2)(\mathbf{e}_i \otimes \mathbf{f}_j) = (\rho_1)(\mathbf{e}_i) \otimes (\rho_2)(\mathbf{f}_j) = \Big(\sum_{r=1}^{n} a_{ri}\mathbf{e}_r\Big) \otimes \Big(\sum_{s=1}^{m} b_{sj}\mathbf{f}_s\Big)$$

$$(*) \qquad = \sum_{r=1}^{n} a_{ri}\Big(\sum_{j=1}^{m} b_{sj}(\mathbf{e}_r \otimes \mathbf{f}_s)\Big)$$

Por outro lado, a coluna de $A(g) \otimes B(g)$ correspondente a $\mathbf{e}_i \otimes \mathbf{f}_j$ tem entradas

$$(\underbrace{a_{1i}b_{1j}, a_{1i}b_{2j}, \ldots, a_{1i}b_{mj}}_{m}, \underbrace{a_{2i}b_{1j}, a_{2i}b_{2j}, \ldots, a_{2i}b_{mj}}_{m}, \ldots, \underbrace{a_{ni}b_{1j}, a_{ni}b_{2j}, \ldots, a_{ni}b_{mj}}_{m})$$

o que corresponde a $(*)$ ordenando $\mathcal{B}$ por ordem lexicográfica nos índices (i, j). □

Exemplo 1.14. Considere o anel de grupo (Exemplo 1.12 do Capítulo 2 com $A = k$)

$$k(G) = \Big\{ \sum_{i=1}^{n} a_i g_i \mid n \in \mathbb{N}, a_i \in k, g_i \in G \Big\} .$$

Se identificarmos $a \in k$ com $a\mathbf{1}_G \in k(G)$, k é um subanel de $k(G)$, $k(G)$ tem uma estrutura natural de espaço vectorial sobre k e G é uma base-k. O produto no anel $k(G)$ também define,

por restrição, uma acção de G em $k(G)$:

$$G \times k(G) \to k(G)$$
$$\Big(g, \sum_{i=1}^{n} a_i g_i\Big) \mapsto \sum_{i=1}^{n} a_i (g g_i) \ .$$

$k(G)$, com esta acção, diz-se a *representação regular* de G. Como $\rho(g)(g_i) = g g_i$, ou seja, para cada $g \in G$ fixo $\rho(g)$ permuta os elementos da base G de $k(G)$, concluímos que a representação regular é uma representação de permutação.

Lema 1.15. *(a) Um espaço vectorial $V \in \mathrm{Vect}_k$ é uma representação de G se e só se V é um módulo-$k(G)$.*

(b) Duas representações de G, V_1 e V_2, são equivalentes se e só se V_1 e V_2 são isomorfas como módulos-$k(G)$.

Definição 1.16. *Seja (V, ρ) uma representação de G.*

- *Um subespaço $W \subset V$ diz-se uma* subrepresentação *ou um* subespaço invariante-G *de V se W é invariante por $\rho(g)$, i.e., se $\rho(g)(W) \subset W$, para todo o $g \in G$.*
- *Se W é uma subrepresentação de V, dizemos que W tem um complemento em V se existe uma subrepresentação W' tal que $V = W \oplus W'$ e, neste caso, W' diz-se um* complemento *de W.*
- *V diz-se uma* representação irredutível *se $\{0\}$ e V são os únicos subespaços invariantes-G. Caso contrário, V diz-se* redutível.
- *V diz-se* completamente redutível *se for a soma directa de representações irredutíveis.*

Lema 1.17. *Dada uma representação V de G e um subespaço $W \subset V$, então*

(a) W é uma subrepresentação de V se e só se W é um submódulo-$k(G)$ de V;

(b) V é irredutível se e só se V é um módulo-$k(G)$ simples;

(c) V é completamente redutível se e só se V é um módulo-$k(G)$ semi-simples.

Exemplo 1.18. Qualquer representação V de dimensão 1 é irredutível, pois $V \cong k$ como espaços vectoriais-k, logo os únicos subespaços são V e $\{0\}$ (e estes subespaços são sempre invariantes).

Exemplo 1.19. Seja G um grupo finito e consideremos a representação regular $k(G)$. Seja $\bar{g} = \sum_{g \in G} g$. Então $W = \langle \bar{g} \rangle$ é um subespaço invariante-G de $k(G)$ e G age trivialmente em W, ou seja, W é uma subrepresentação trivial de $k(G)$ – Exercício 6.1.3. Portanto, se $G \neq \{\mathbf{1}\}$, a representação regular nunca é irredutível.

Exemplo 1.20. Se V é uma representação de dimensão 2, então V é redutível se e só se

$$\exists\, \mathbf{v} \in V \setminus \{0\} \quad \forall\, g \in G \quad \text{tal que} \quad g \cdot \mathbf{v} \in \langle \mathbf{v} \rangle = \{a\mathbf{v} \mid a \in k\} \ ,$$

pois, neste caso, $\langle \mathbf{v} \rangle$ é uma subrepresentação de dimensão 1, e os únicos subespaços $\neq \{0\}$ e $\neq V$ candidatos a subrepresentações de V têm dimensão 1.

Observação 1.21. Se W é uma subrepresentação de V, temos em particular que W é subespaço-k de V e, portanto, existe sempre[2] um subespaço-k $W' \subset V$ tal que $V = W \oplus W'$ em Vect_k. Mas W' apenas é um complemento para W, no sentido das representações, se for invariante-G, o que nem sempre acontece – ver Exercícios 6.1.5 e 6.1.6.

Um dos objectivos da Teoria de Representação de Grupos é determinar a decomposição da representação regular em soma directa de representações irredutíveis, se possível.

[2]Podemos, por exemplo, completar uma base de W até obter uma base $\mathcal{B}$ para V e definimos W' como o espaço-k gerado por $\mathcal{B} \setminus W$.

Notação 1.22. Se V e W são representações, denotamos por $\mathrm{Hom}_k(V,W)$ o conjunto dos homomorfismos entre V e W como espaços vectoriais-k, como temos feito sempre, e denotamos por $\mathrm{Hom}_G(V,W)$ o subconjunto de $\mathrm{Hom}_k(V,W)$ das aplicações equivariantes-G, i.e., de acordo com o Lemma 1.17, $\mathrm{Hom}_G(V,W) \coloneqq \mathrm{Hom}_{k(G)}(V,W)$. Analogamente, definimos $\mathrm{End}_G(V) \coloneqq \mathrm{End}_{k(G)}(V)$.

Temos, portanto, que $\mathrm{Hom}_G(V,W)$ é um grupo abeliano para a soma usual de funções, e que $\mathrm{End}_G(V)$ é um anel com o produto dado pela composição de funções.

Lema 1.23 (Schur)**.** *Sejam V e W duas representações irredutíveis. Então*

(a) se $f \in \mathrm{Hom}_G(V,W)$, $f = 0$ ou f é um isomorfismo;

(b) o anel $\mathrm{End}_G(V)$ é uma álgebra de divisão;

(c) se k é um corpo algebricamente fechado, $\mathrm{End}_G(V) \cong k$, mais precisamente, qualquer $f \in \mathrm{End}_G(V)$ é da forma $f = \lambda \,\mathrm{id}_V$ para algum escalar $\lambda \in k$.

Demonstração. (a) Seja $f \in \mathrm{Hom}_G(V,W)$. Portanto $\ker(f)$ é um submódulo-$k(G)$ de V e $\mathrm{im}(f)$ é um submódulo-$k(G)$ de W. Como V e W são irredutíveis, temos $\ker(f) = V$ ou $\{0\}$, e $\mathrm{im}(f) = W$ ou $\mathrm{im}\, f = \{0\}$. Portanto, f é a aplicação nula, se $\ker(f) = V$ ou $\mathrm{im}(f) = \{0\}$, ou f é um isomorfismo, se $\ker(f) = \{0\}$ e $\mathrm{im}(f) = W$.

(b) Por (a) qualquer $f \in \mathrm{End}_G(V) \setminus \{0\}$ é um isomorfismo, logo tem um inverso em $\mathrm{End}_G(V)$.

(c) Seja $f \in \mathrm{End}_G(V) \setminus \{0\}$. Como $V \cong k^n$, por (b) podemos assumir que $f \in GL_n(k)$ e, como k é algebricamente fechado, a matriz f tem um valor próprio $\lambda \in k$. Como $\lambda \,\mathrm{id}_V \in \mathrm{End}_G(V)$, também temos que $f - \lambda \,\mathrm{id}_V \in \mathrm{End}_G(V)$ e $\ker(f - \lambda \,\mathrm{id}_V) \neq \{0\}$ (porque λ é valor próprio), logo, por (a), $f = \lambda \,\mathrm{id}_V$. □

Usando o Lema de Zorn e o lema anterior, prova-se[3] o seguinte corolário.

Corolário 1.24. *Seja V uma representação de G. Então V é completamente redutível se e só se qualquer subrepresentação $W \subset V$ tem um complemento.*

Observação 1.25. Se G é finito, $|G| \in \mathbb{N}$ e identificamos o inteiro $|G|$ com $|G|1_k \in k$. Dizemos que $|G|$ é invertível em k e escrevemos $|G| \in k^\times$ se $|G|1_k$ é invertível. Portanto, se k tem característica zero, $|G|$ é sempre invertível em k. Se a característica de k é o primo[4] p, $|G| \in k^\times$ se e só $p \nmid |G|$.

Teorema 1.26 (Maschke)**.** *Seja G um grupo finito tal que $|G|$ é invertível em k. Então*

(a) qualquer representação de G é completamente redutível;

(b) existe apenas um número finito de representações de G irredutíveis $V_1, \ldots, V_r$ e

$$k(G) = V_1^{n_1} \oplus \cdots \oplus V_r^{n_r} \ ,$$

com $n_i \in \mathbb{N}$.

Demonstração. (a) Seja W uma subrepresentação de V. Pelo Corolário 1.24, temos que ver que W tem um complemento, i.e., que existe uma subrepresentação W' tal que $V = W \oplus W'$. Suponhamos que $W \neq \{0\}$ e $W \neq V$, caso contrário nada há a provar.

Seja W_0 um subespaço-k de V tal que $V = W \oplus W_0$ como espaços vectoriais-k. Seja $\pi : V \to W$ a projecção e $\iota : W \to V$ a inclusão. Portanto π e ι são aplicações lineares-k e a

[3]Pode-se fazer uma demonstração mais elementar considererando apenas representações de dimensão finita. Para o caso geral compare o seguinte corolário com o Lema 24.3 do Capítulo 4. O Lema de Schur também já foi abordado no Capítulo 4, Lema 24.8, que voltámos a repetir numa versão enunciada na linguagem das representações.

[4]Recorde que a característica de um corpo ou é 0 ou é um primo $p \in \mathbb{N}$.

composta $\varphi = \iota \circ \pi$ também é linear-k e ainda $\ker(\varphi) = W_0$ e $\mathrm{im}(\varphi) = W$. Seja $f : V \to V$ a aplicação definida por

$$f(\mathbf{v}) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot \varphi(g \cdot \mathbf{v}) \ .$$

Como f é uma combinação linear de aplicações lineares-k, f é linear-k. Temos ainda que $\mathrm{im}(f) \subset W$ pois $\mathrm{im}(\varphi) = W$ e W é invariante-G.

(1º) f é equivariante-G: sejam $h \in G$ e $\mathbf{v} \in V$ quaisquer. Então

$$\begin{aligned} f(h \cdot \mathbf{v}) &= \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot \varphi(g \cdot (h \cdot \mathbf{v})) \\ &= \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot \varphi((gh) \cdot \mathbf{v}) && \text{por definição de acção} \\ &= \frac{1}{|G|} \sum_{g' \in G} (g'h^{-1})^{-1} \cdot \varphi(g' \cdot \mathbf{v}) && \text{porque } g' = gh \text{ também percorre } G \\ &= h \cdot \Big(\frac{1}{|G|} \sum_{g' \in G} (g')^{-1} \cdot \varphi(g' \cdot \mathbf{v}) \Big) \\ &= h \cdot f(\mathbf{v}) \ . \end{aligned}$$

(2º) $f^2 = f$: seja $\mathbf{w} \in W$ qualquer, então $g \cdot \mathbf{w} \in W$ para todo o $g \in G$ porque W é invariante-G, logo $\pi(g \cdot \mathbf{w}) = g \cdot \mathbf{w}$, por definição da projeção π, e $\varphi(g \cdot \mathbf{w}) = g \cdot \mathbf{w}$. Temos

$$f(\mathbf{w}) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot \varphi(g \cdot \mathbf{w}) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot (g \cdot \mathbf{w}) = \mathbf{w} \qquad \forall\, \mathbf{w} \in W \ , \tag{1.1}$$

portanto

$$f^2(\mathbf{v}) = f(f(\mathbf{v})) = f(\mathbf{v}) \qquad \forall\, \mathbf{v} \in V \ ,$$

pois $f(\mathbf{v}) \in W$.

(3º) $\mathrm{im}(f) = W$: por construção $f(V) \subset W$, por (1.1) do ponto anterior $f(\mathbf{w}) = \mathbf{w}$ para qualquer $\mathbf{w} \in W$.

Dos três pontos acima, concluímos que $V = \mathrm{im}(f) \oplus \ker(f) = W \oplus \ker(f)$ como módulos-$k(G)$, portanto $W' = \ker(f)$ é um complemento de W – na primeira igualdade usámos o Exercício 4.4.2.

(b) Seja V uma representação irredutível de G. Pelo Exercício 6.1.7, sabemos que V é equivalente a $k(G)/I$ para algum ideal esquerdo maximal $I \subset k(G)$, portanto I é um submódulo-$k(G)$ de $k(G)$, o que é ainda equivalente a dizer que I é uma subrepresentação de $k(G)$. Por (a) temos que existe um complemento J de I, i.e., $k(G) = I \oplus J$ como módulos-$k(G)$. Portanto $J \cong k(G)/I \cong V$ é uma subrepresentação de $k(G)$.

Como $k(G)$ é completamente redutível, temos que $k(G)$ é a soma directa de representações irredutíveis V_i, i.e., $k(G) = \bigoplus_{i=1}^{n} V_i$, onde o número de somandos é finito pois $\dim_k k(G) = |G|$ é finita. Por outro lado, acabámos de ver que qualquer representação irredutível V é subrepresentação de $k(G)$, logo $V = V_i$ para algum i. Agrupando os somandos V_i isomorfos entre si, obtemos o resultado pretendido. □

O resultado anterior é falso sem a hipótese de $|G| \in k^\times$ – ver Exercício 6.1.6.

Exercícios

6.1.1. (a) Determine as representações reais (sobre $\mathbb{R}$) de dimensão 1 do grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$.
(b) Determine as representações reais de dimensão 1 do grupo D_4.
Sugestão: Calcule $[D_4, D_4]$ e verifique que $D_4/[D_4, D_4] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

6.1.2. Demonstre os Lemas 1.15 e 1.17.

6.1.3. Seja G um grupo finito, e seja $\bar{g} = \sum_{g \in G} g \in k(G)$. Seja $W = \langle \bar{g} \rangle = \{a\bar{g} \in k(G) \mid a \in k\}$. Mostre que W é uma subrepresentação da representação regular $k(G)$ e é trivial.

6.1.4. (a) Seja G um grupo abeliano finito e k um corpo algebricamente fechado. Mostre que qualquer representação irredutível de G tem dimensão 1.
(b) Seja G um grupo cíclico de ordem 4 com gerador a. Considere a seguinte representação real V com acção $\rho : G \to GL_2(\mathbb{R})$ definida por

$$\rho(a) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} .$$

Mostre que V é irredutível sobre $\mathbb{R}$.

6.1.5. Seja $G = \{\mathbf{1}_G, a\}$ o grupo cíclico de ordem 2 e considere a representação regular $\mathbb{R}(G)$. Seja

$$V_1 = \{x\mathbf{1}_G + xa \in \mathbb{R}(G) \mid x \in \mathbb{R}\} \qquad \text{e} \qquad V_2 = \{x\mathbf{1}_G - xa \in \mathbb{R}(G) \mid x \in \mathbb{R}\} .$$

(a) Mostre que V_1 e V_2 são subrepresentações da representação regular $\mathbb{R}(G)$. Quais as suas dimensões?
(b) Mostre que V_1 é uma representaçao trivial e V_2 é equivalente à representação sinal.
(c) Mostre que $\mathbb{R}(G) = V_1 \oplus V_2$.

6.1.6. Seja $G = \{\mathbf{1}_G, a\}$ o grupo cíclico de ordem 2 e considere a representação regular $\mathbb{Z}_2(G)$. Seja

$$V = \{x\mathbf{1}_G + xa \in \mathbb{Z}_2(G) \mid x \in \mathbb{Z}_2\} .$$

Mostre que V é uma subrepresentação da representação regular $\mathbb{Z}_2(G)$ que não tem um complemento. (Compare com o exercício anterior.)

6.1.7. Seja $V \neq \{0\}$ uma representação irredutível de G. Mostre que existe um ideal esquerdo maximal I do anel $k(G)$ tal que $V \cong k(G)/I$ como módulos-$k(G)$.
Sugestão: Use o Lema de Schur 1.23.

2. Caracteres

Definição 2.1. *Seja V uma representação de G, de dimensão n, com acção dada por $\rho\colon G \to GL_n(k)$. O* caracter *associado a V é a aplicação $\chi_V\colon G \to k$, $\chi_V(g) = \mathrm{Tr}(\rho(g))$, onde* Tr *designa o traço de uma matriz.*

Exemplo 2.2. Seja V a representação trivial de dimensão n. Então $\rho(g) = I$ (a matriz identidade $n \times n$) para todo o $g \in G$ e, portanto o caracter χ_V é a aplicação constante $\chi_V = n$.

Exemplo 2.3. Seja $V = k(G)$ a representação regular do grupo G de ordem n finita. Então $G = \{g_1, \ldots, g_n\}$ é uma base de V e $\rho(g)(g_i) = gg_i$. Logo

$$\chi_V(g) = \#\{i \mid gg_i = g_i\} = \begin{cases} |G| & \text{se } g = \mathbf{1}_G, \\ 0 & \text{se } g \neq \mathbf{1}_G. \end{cases}$$

Nos próximos exemplos introduz-se algumas construções a partir de representações que iremos usar nalguns resultados no resto desta secção.

Exemplo 2.4. (Representação dual.) Seja (V, ρ) uma representação de G. O espaço dual $V^* = \mathrm{Hom}_k(V, k)$ tem a seguinte acção de G dada por $\rho^*(g) = \rho(g^{-1})^T$:

$$(\rho^*(g)f)(\mathbf{v}) \coloneqq f(\rho(g^{-1})(\mathbf{v})) \qquad \forall\, \mathbf{v} \in V \ ,$$

onde $g \in G$ e $f \in V^*$.

Exemplo 2.5. (Pontos fixos.) Seja (V, ρ) uma representação de G. Seja V^G o conjunto dos pontos fixos de V pela acção, ou seja,

$$V^G \coloneqq \{\mathbf{v} \in V \mid \rho(g)(\mathbf{v}) = \mathbf{v},\, \forall\, g \in G\} \ .$$

Então V^G é um subespaço invariante-G de V com acção trivial, ou seja, V^G é a maior subrepresentação trivial de V.

Exemplo 2.6. (Representação "homomorfismos".) Sejam (V, ρ_1) e (W, ρ_2) duas representações de G, então $\mathrm{Hom}_k(V, W)$ é uma representação de G com a seguinte acção dada por ρ:

$$(\rho(g)f)(\mathbf{v}) \coloneqq \rho_2(g)f(\rho_1(g^{-1})(\mathbf{v})) \qquad \forall\, \mathbf{v} \in V \ ,$$

onde $g \in G$ e $f \in \mathrm{Hom}_k(V, W)$.

Observação 2.7. A representação dual corresponde a considerar a representação trivial $W = k$ no exemplo anterior.

A partir de agora consideramos apenas representações complexas, i.e., sobre $k = \mathbb{C}$ (um corpo algebricamente fechado de característica zero), de dimensão finita de um grupo finito G.

Recorde que $\mathbb{C}^n$ tem um produto interno hermítico dado por

$$\langle \mathbf{z}, \mathbf{w} \rangle = \sum_{i=1}^{n} z_i \overline{w}_i \ ,$$

onde $\mathbf{z} = (z_1, \ldots, z_n)$ e $\mathbf{w} = (w_1, \ldots, w_n)$, tal que é linear-$\mathbb{C}$ na primeira variável e $\langle \mathbf{w}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{w} \rangle}$. Portanto

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)} \in \mathbb{C} \ . \tag{2.1}$$

define uma produto interno no espaço $\mathbb{C}^G \coloneqq \{G \to \mathbb{C}\}$ das funções complexas definidas em G.

Recorde ainda que $A \in M_n(\mathbb{C})$ diz-se uma matriz unitária se $A\bar{A}^T = I$, em particular

$$U_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid A\bar{A}^T = I\}$$

é um subgrupo de $GL_n(\mathbb{C})$.

Definição 2.8. *Dizemos que* (V,ρ) *é uma* representação unitária *se* $\operatorname{im}\rho \subset U_n(\mathbb{C})$.

Lema 2.9. *Qualquer representação complexa é equivalente a uma representação unitária.*

Demonstração. Ver [**Ser77**]. □

Tendo em conta o lema anterior, podemos assumir que as representações complexas são unitárias.

Proposição 2.10. *Sejam* V, W *representações do grupo* G. *Então*

(a) $\chi_V(\mathbf{1}) = \dim V$;
(b) $\chi_V(hgh^{-1}) = \chi_V(g)$ *para qualquer* $g, h \in G$;
(c) $\chi_{V\oplus W} = \chi_V + \chi_W$;
(d) $\chi_{V\otimes W} = \chi_V \cdot \chi_W$;
(e) $\chi_{V^*}(g) = \chi_V(g^{-1}) = \overline{\chi_V(g)}$ *para todo o* $g \in G$.

Demonstração. (a) $\chi_V(\mathbf{1}_G) = \operatorname{Tr}(\rho(\mathbf{1}_G)) = \operatorname{Tr}(I) = \dim V$.
(b) Segue de $\operatorname{Tr}(S^{-1}AS) = \operatorname{Tr}(A)$, com $S \in GL_n(\mathbb{C})$.
(c), (d) Consequência imediata da Proposição 1.13.

(e) Assumindo que V é unitária, temos $\rho(g^{-1}) = \rho(g)^{-1} = \overline{\rho(g)}^T$ e, calculando traços, obtemos $\chi_V(g^{-1}) = \overline{\chi_V(g)}$, pois $\operatorname{Tr}(A) = \operatorname{Tr}(A^T)$ para qualquer matriz $n \times n$ A. A primeira igualdade é consequência da definição da representação dual. □

A alínea (b) da proposição anterior sugere a seguinte definição.

Definição 2.11. $f : G \to \mathbb{C}$ *diz-se uma* função de classe *se* f *é constante em cada classe de conjugação de* G, *i.e., se*

$$f(hgh^{-1}) = f(g) \quad \forall\, g, h \in G \ .$$

Exemplo 2.12. O caracter de uma representação é uma função de classe.

Observação 2.13. Como dar uma função de classe é equivalente a escolher um número complexo para cada classe de conjugação, o conjunto das funções de classe é um espaço vectorial-$\mathbb{C}$ com dimensão igual ao número de classes de conjugação em G.

Proposição 2.14. *Seja* (V,ρ) *uma representação de* G. *Seja* $e_V : V \to V$ *dada por*

$$e_V \coloneqq \frac{1}{|G|}\sum_{g\in G}\rho(g) \ .$$

Então (i) $e_V \in \operatorname{End}_G(V)$; *(ii)* $e_V^2 = e_V$; *(iii)* $\operatorname{im} e_V = V^G$ *e (iv)* $e_V|_{V^G} = \operatorname{id}_{V^G}$.

Demonstração. (1º) $e_V \in \operatorname{End}_k(V)$, porque $\rho(g) \in \operatorname{End}_k(V)$ para qualquer $g \in G$, e e_V é equivariante pois, para todo o $h \in G$,

$$e_V(h\cdot\mathbf{v}) = \frac{1}{|G|}\sum_{g\in G}(g\cdot(h\cdot\mathbf{v})) = h\frac{1}{|G|}\sum_{g\in G}(h^{-1}gh)\cdot\mathbf{v} = h\frac{1}{|G|}\sum_{g'=h^{-1}gh\in G}(g')\cdot\mathbf{v} = h\cdot e_V(\mathbf{v}) \ .$$

(2º) $\operatorname{im} e_V \subset V^G$ pois

$$h\cdot e_V(\mathbf{v}) = \frac{1}{|G|}\sum_{g\in G}(hg)\cdot\mathbf{v} = \frac{1}{|G|}\sum_{g'=gh\in G} g'\cdot\mathbf{v} = e_V(\mathbf{v}) \quad \forall\,\mathbf{v}\in V \ .$$

(3º) Se $\mathbf{v} \in V^G$ então

$$e_V(\mathbf{v}) = \frac{1}{|G|}\sum_{g\in G} g\cdot\mathbf{v} = \frac{1}{|G|}\sum_{g\in G}\mathbf{v} = \mathbf{v} \ ,$$

portanto $V^G \subset \operatorname{im} e_V$ e $e_V|_{V^G} = \mathrm{id}_V$.
(4º) Como $\operatorname{im} e_V = V^G$ e $e_V|_{V^G} = \mathrm{id}_V$, temos $e_V^2(\mathbf{v}) = e_V(e_V(\mathbf{v})) = e_V(\mathbf{v})$, para todo o $\mathbf{v} \in V$, pois $e_V(\mathbf{v}) \in \operatorname{im} e_V$. □

Corolário 2.15. *Seja V uma representação de G. Então*

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \ .$$

Demonstração. Pela proposição anterior: $V^G = \operatorname{im} e_V$ e $\ker e_V$ são subrepresentações de V (pontos (i) e (iii)) e $V = V^G \oplus \ker e_V$ (ponto (ii)), portanto,

$$\operatorname{Tr}(e_V) = \operatorname{Tr}(e_V|_{V^G}) = \dim V^G \ ,$$

onde se usou o ponto (iv) na última igualdade. Por outro lado, directamente da definição de e_V, temos

$$\operatorname{Tr}(e_V) = \frac{1}{|G|} \sum_{g \in G} \operatorname{Tr}(\rho(g)) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \ . \qquad \square$$

Pelo Teorema de Maschke 1.26, uma vez que $\mathbb{C}$ tem característica zero, sabemos que qualquer grupo finito tem apenas um número finito de representações irredutíveis $V_1, \ldots, V_r$. Ainda pelo Teorema de Maschke, como cada representação V de G é completamente redutível, temos

$$V = V_1^{m_1} \oplus \cdots \oplus V_r^{m_r} \ , \tag{2.2}$$

onde $m_i \in \mathbb{N}_0$ ($m_i = 0$ significa que V_i não é subrepresentação de V).

Definição 2.16. *1. A m_i na igualdade* (2.2) *chamamos* multiplicidade *de V_i em V.*
2. Seja $\chi_i = \chi_{V_i}$. A $\chi_1, \ldots, \chi_r$ chamamos os caracteres irredutíveis *de G.*

Teorema 2.17. *Sejam $\chi_1, \ldots, chi_r$ os caracteres irredutíveis do grupo G. Então*

$$\langle \chi_i, \chi_j \rangle = \begin{cases} 1 & \text{se } i = j, \\ 0 & \text{se } i \neq j \ . \end{cases}$$

Demonstração. Seja $U = \operatorname{Hom}_k(V, W)$ a representação "homomorfismos" do Exemplo 2.6. Pelo Exercício 4.12.5 temos[5] que $\operatorname{Hom}_k(V, W) \cong V^* \otimes W$, portanto, pela Proposição 2.10

$$\chi_U = \chi_{V^* \otimes W} = (\chi_{V^*})(\chi_W) = \overline{\chi_V} \chi_W$$

e pelo Corolário 2.15 e Exercício 6.2.1

$$\dim \big(\operatorname{Hom}_G(V, W) \big) = \dim \big(U^G \big) = \frac{1}{|G|} \sum_{g \in G} \chi_W \overline{\chi_V} = \langle \chi_W, \chi_V \rangle \ . \tag{2.3}$$

Pelo Lema de Schur 1.23, temos que $\operatorname{Hom}_G(V_i, V_j) = \{0\}$, se $i \neq j$ (pois $V_i \ncong V_j$ neste caso) e que $\operatorname{Hom}_G(V_i, V_i) \cong \mathbb{C}$, portanto o resultado segue da igualdade (2.3) pondo $V = V_j$ e $W = V_i$. □

Corolário 2.18. *Seja V uma representações de G.*

(a) A multiplicidade de V_i em V é $\langle \chi_V, \chi_i \rangle$.
(b) Seja W outra representação. Então $\chi_W = \chi_V$ se e só se W é equivalente a V.

Demonstração. (a) Da igualdade (2.2), aplicando a Proposição 2.10(c) e o Teorema 2.17, obtemos

$$\langle \chi_V, \chi_i \rangle = \sum_{j=1}^{r} m_j \langle \chi_j, \chi_i \rangle = m_i$$

(b) Segue directamente de (a) pois cada V_i tem a mesma multiplicidade em V e W. □

[5] O exercício apenas dá um isomorfismo de espaços vectoriais-k, mas verifica-se que o isomorfismo definido também é equivariante-G.

Corolário 2.19. *Sejam $V_1, \ldots, V_r$ as representações irredutíveis de G e seja $n_i = \dim V_i$. Então*
(a) $\mathbb{C}(G) = V_1^{n_1} \oplus \cdots \oplus V_r^{n_r}$;
(b) $|G| = \sum_{i=1}^{r} n_i^2$;

Demonstração. (a) Seja m_i a multiplicidade de V_i em $\mathbb{C}(G)$. Então

$$\begin{aligned} m_i &= \langle \chi_{\mathbb{C}(G)}, \chi_i \rangle && \text{por (a) do corolário anterior} \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{\mathbb{C}(G)}(g)\overline{\chi_i(g)} && \text{por definição de } \langle -, - \rangle \\ &= \frac{1}{|G|}\big(|G|\overline{\chi_i(\mathbf{1}_G)}\big) && \text{pelo Exemplo 2.3} \\ &= \dim V_i && \text{pela Proposição 2.10(a).} \end{aligned}$$

O resultado segue do Teorema de Maschke 1.26.
(b) Por (a) e novamente pela Proposição 2.10, temos

$$|G| = \chi_{\mathbb{C}(G)}(\mathbf{1}_G) = \sum_{i=1}^{r} n_i \chi_i(\mathbf{1}_G) = \sum_{i=1}^{r} n_i^2 \, . \qquad \square$$

Observação 2.20. Note que (a) do teorema anterior diz que a multiplicidade de cada V_i na representação regular é a dimensão $\dim V_i$.

Teorema 2.21. *Os caracteres irredutíveis formam uma base do espaço das funções de classe.*

Demonstração. Uma vez que os caracteres irredutíveis são ortonormados, estes são linearmente independentes. Para mostrar que formam um conjunto gerador, ver a Proposição 6 e o Teorema 6, página 19, de [**Ser77**]. $\square$

Corolário 2.22. *O número r de representações irredutíveis de G é igual ao número de classes de conjugação de G.*

Demonstração. Segue do teorema anterior e da Observação 2.13. $\square$

Observação 2.23. Alternativamente, aplicando o Teorema 2.1 do Capítulo 5 ao anel de grupo[6] $\mathbb{C}(G)$, neste caso temos $D_i = \mathrm{End}_G(V_i)$, portanto $D_i \cong \mathbb{C}$ pelo Lema de Schur 1.23, logo

$$\mathbb{C}(G) \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}) \, ,$$

onde r é o número de representações irredutíveis e $n_i = dim V_i$. O centro de cada anel $M_{n_i}(\mathbb{C})$ é $Z(M_{n_i}(\mathbb{C})) = \{\lambda I \mid \lambda \in \mathbb{C}\} \cong \mathbb{C}$, logo $\dim Z(\mathbb{C}(G)) = r$. Por outro lado, pelo próximo Lema 2.24, obtemos que $\dim(\mathbb{C}(G))$ é o número de classes de conjugação.

Lema 2.24. *Seja k um corpo qualquer e seja G um grupo finito. Sejam $C_1, \ldots, C_c$ as classes de conjugação (distintas entre si) de G e defina-se $z_i = \sum_{g \in C_i} g$. Então $\{z_1, \ldots, z_c\}$ é uma base-k do centro $Z(k(G))$, logo $\dim Z(k(G)) = c$.*

Demonstração. Como k é comutativo, dado $a \in k(G)$ então $a \in Z(k(G))$ se e só se $hah^{-1} = a$ para todo o $h \in G$. Portanto, cada $z_i \in Z(k(G))$ pois

$$hz_ih^{-1} = \sum_{g \in C_i} hgh^{-1} = \sum_{g' = hgh^{-1} \in C_i} g' = z_i \, .$$

Por outro lado, pondo

$$a = \sum_{g \in G} a_g g \in Z(k(G)) \, ,$$

[6] $k(G)$ é um módulo-$k(G)$ semi-simples pelo Teorema de Maschke, se $|G| \in k^\times$, portanto é um anel semi-simples à esquerda.

com $a_g \in k$, fica

$$hah^{-1} = \sum_{g\in G} a_g hgh^{-1} = \sum_{g'=hgh^{-1}\in G} a_{h^{-1}g'h} g'$$

e como G é uma base-k de $k(G)$, obtemos $hah^{-1} = a$ para todo o $h \in G$ se e só se

$$a_g = a_{h^{-1}gh} \quad \forall g, h \in G$$

ou seja, $a_g = a_{g'}$ se g e g' estão na mesma classe de conjugação, obtemos assim a como combinação linear de $z_1, \ldots, z_c$.

Concluímos portanto que $\{z_1, \ldots, z_c\}$ gera $Z(k(G))$. A independência linear é consequência de as classes de conjugação serem disjuntas duas a duas (são classes de equivalência de uma relação de equivalência) e de G ser um conjunto linearmente independente sobre k. □

2.1. Tabela de caracteres

Dado um grupo finito G, seja c o número de classes de conjugação de G, sejam $g_1, \ldots, g_c$ representantes de cada uma das classes e sejam $\chi_1, \ldots, \chi_c$ os caracteres irredutíveis. Então $[\chi_i(g_j)]$ é uma matriz quadrada $c \times c$ a que chamamos *tabela de caracteres* de G.

Exemplo 2.25. $G = S_3$ tem três classes de conjugação representadas por $\mathbf{1}$, (12) e (123) – ver Exercício 1.9.2. Portanto, pelo corolário 2.22, sabemos que há três representações irredutíveis. Do Exemplo 1.10, temos duas representações de dimensão um, logo irredutíveis: a representação trivial e a representação sinal. Do Corolário 2.19, $6 = 1+1+n_3^2$, pois $n_1 = n_2 = 1$, logo $n_3 = 2$. Obtemos portanto

g_i	$\mathbf{1}$	(12)	(123)
$\lvert C_i\rvert$	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	a	b

Para determinar a e b usamos as relações de ortogonalidade do Teorema 2.17:

$$\begin{cases} \langle \chi_3, \chi_1\rangle = 0 \\ \langle \chi_3, \chi_1\rangle = 0 \end{cases} \Leftrightarrow \begin{cases} \frac{1}{6}(2+3a+2b) = 0 \\ \frac{1}{6}(2-3a+2b) = 0 \end{cases} \Leftrightarrow a = 0\,, b = -1\ .$$

Exemplo 2.26. Como $S_3 \cong D_3$ e $\mathbb{R} \subset \mathbb{C}$, o Exemplo 1.8 dá-nos a seguinte representação $V = \mathbb{C}^2$ com acção definida por

$$\rho(12) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{e} \qquad \rho(123) = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

Como $\chi_V(\mathbf{1}) = 2$, $\chi_V(12) = 0$ e $\chi_V(123) = -1$, temos $\chi_V = \chi_3$ logo, pelo Corolário 2.18, concluímos que $V_3 \cong V$.

Exemplo 2.27. Considere a representação V de S_3 do Exemplo 1.5 com $k = \mathbb{C}$. Uma vez que $\dim V = 3$, pelo Exemplo 2.25 sabemos que V não é irredutível. Como $\chi_V(\mathbf{1}) = 3$, $\chi_V(12) = 1$ e $\chi_V(123) = 0$, as multiplicidades m_i de V_i do Exemplo 2.25 em V são

$$m_1 = \langle \chi_V, \chi_1\rangle = \frac{1}{6}(3 + 3\cdot 1 + 0) = 1$$

$$m_2 = \langle \chi_V, \chi_2\rangle = \frac{1}{6}(3 - 3\cdot 1 + 0) = 0$$

$$m_3 = \langle \chi_V, \chi_3\rangle = \frac{1}{6}(3\cdot 2 + 0 + 0) = 1$$

donde conluímos que $V \cong V_1 \oplus V_3$.

Exercícios

6.2.1. Sejam V e W duas representações de G e considere a representação "homomorfismos" $U = \mathrm{Hom}_k(V, W)$ do Exemplo 2.6. Mostre que $U^G = \mathrm{Hom}_G(V, W)$.

6.2.2. Mostre que uma representação complexa V é irredutível se e só se $\langle \chi_V, \chi_V \rangle = 1$.

6.2.3. Determine se as representações dos Exemplos 1.7 e 1.8 são irredutíveis sobre $\mathbb{C}$. Em caso negativo, determine a sua decomposição em soma directa de representações irredutíveis.

6.2.4. Determine as representações complexas irredutíveis dos seguintes grupos:
(a) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} < \mathbb{H}^\times$;
(b) D_4;
(c) D_5.

6.2.5. Determine a tabela de caracteres de A_4 e S_4.

6.2.6. (a) Se V é uma representação de dimensão 1 e W é uma representações irredutível, mostre que $V \otimes W$ é irredutível.
(b) Dê um exemplo de um grupo G e duas representações irredutíveis V, W de G tais que $V \otimes W$ não é irredutível.

6.2.7. Seja V uma representação de dimensão finita. Mostre que V é irredutível se e só se V^* é irredutível.

Bibliografia

[Hun74] T.W. Hungerford, *Algebra*, Graduate texts in mathematics, vol.73, 1980, Springer-Verlag.

[FR04] R.L. Fernandes e Manuel Ricou, *Introdução à Álgebra*, 2004, IST Press.

[Ser77] J.-P. Serre, *Linear Representations of Finite Groups*, Graduate texts in mathematics, vol.42, 1977, Springer-Verlag.