Capítulo 1

Grupos

1.1 1ª Aula

1.1.1 Grupos e monóides: definições básicas

Definição 1.1.1. *Uma* operação binária *num conjunto S é uma função*

$$\begin{aligned} S \times S &\to S \\ (x, y) &\mapsto xy \end{aligned}$$

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

$$(xy)z = x(yz).$$

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

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

$$1x = x1 = x, \qquad \forall x \in S.$$

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

Se o 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*

$$xy = yx = 1;$$

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

Exercício 1.1.2. *Seja S um semi-grupo. Mostre que*

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

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

Notação 1.1.3.

1. Se $\star\colon S \times S \to S$ 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 0 para a identidade. Esta notação designa-se por *aditiva.*

3. A notação utilizada na Definição 1.1.1, em que a operação de grupo é representada por justaposição ($(a, b) \mapsto ab$), 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.

Definição 1.1.4. *Se $(G, \cdot)$ é um grupo, define-se*

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

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 1.1.5.

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;

5. $\mathbb{K}^\times := (\mathbb{K} - \{0\}, \cdot)$ 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 $\mathbb{Z}$.

Exercício 1.1.6. *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 $n > 2$. Este grupo designa-se grupo simétrico *de ordem n e denota-se S_n.*

Notação 1.1.7.

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 $\left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{smallmatrix}\right)$;

3. a notação $\sigma = \left(\begin{smallmatrix} i_1 & i_2 & \cdots & i_k \end{smallmatrix}\right)$ 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*. Se $k = 2$, diz-se que σ é uma *transposição*.

Exercício 1.1.8. *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;*

Exercício 1.1.9. *Seja* D_3 *o conjunto das isometrias de um triângulo equilátero (isometrias do plano que deixam o triângulo invariante) munido da operação de composição.*

a. Mostre que $D_3 \cong S_3$.

b. 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*

$$\sigma^i \tau^j, \qquad\qquad i = 0, 1,\ j = 0, 1, 2.$$

1.1.2 Operações definidas por passagem ao quociente

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

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

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

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

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

Proposição 1.1.10. *Seja* R *uma relação de equivalência num semi-grupo* S *tal que*

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

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.*

---

[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] 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.

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

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

$\square$

Exemplo 1.1.11. 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

- $\mathbb{Z}_m = \{\underline{0}, \underline{1}, \ldots, \underline{m-1}\}$ $\qquad$ (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 1.1.12. Diz-se que $\mathbb{Z}_m$ é o *grupo dos inteiros módulo m.*

Observação 1.1.13. 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 1.1.14. $\mathbb{Z}_2 = \{\underline{0}, \underline{1}\}$. A tabela de adição é:

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

Exercício 1.1.15. $\mathbb{Z}_m$ *é um monóide abeliano para a seguinte operação:*

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

e verfica-se a propriedade distributiva*:*

$$\underline{a}(\underline{b} + \underline{c}) = \underline{a}\underline{b} + \underline{a}\underline{c}.$$

1.1.3 Homomorfismos de grupos

Definição 1.1.16. *Sejam G_1, G_2 grupos. Uma função $f\colon G_1 \to G_2$ diz-se um* homomorfismo de grupos *se*

$$\forall x, y \in G_1 \quad f(xy) = f(x)f(y)$$

(ou seja, f preserva produtos).

Se f é um homomorfismo bijectivo, diz-se que é um isomorfismo de grupos.

Exercício 1.1.17. *Se f é um homomorfismo de grupos, tem-se $f(1_{G_1}) = 1_{G_2}$.*

Exemplos 1.1.18.

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 $G = \{z \in \mathbb{C} \mid z^m = 1\} \subset \mathbb{C} - \{0\}$. 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.

Definição 1.1.19. *Seja $f\colon G_1 \to G_2$ um homomorfismo de grupos. Define-se*

- $\ker f \coloneqq \{x \in G_1 \mid f(x) = 1_{G_2}\} \subset G_1$;
- $\operatorname{im} f \coloneqq \{f(x) \mid x \in G_1\} \subset G_2$.

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

Exemplo 1.1.20. 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.*

1.2 2ª Aula

Notação 1.2.1.

1. Os homomorfismos sobrejectivos também são designados *epimorfismos*. Os homomorfismos injectivos são denominados *monomorfismos*.

2. Para denotar que dois grupos, G_1, G_2, são isomorfos, escreve-se $G_1 \cong G_2$.

Exemplo 1.2.2. 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 um monomorfismo,

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

Definição 1.2.3. *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 $H < G$.*

Exercício 1.2.4. *Seja G um grupo e seja $H \subset G$ tal que $H \neq \varnothing$. Mostre que $H < G$* sse *$\forall x, y \in H, xy^{-1} \in H$.*

Exemplo 1.2.5. 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.

Teorema 1.2.6. *Seja $f\colon G \to H$ um homomorfismo de grupos. Temos*

(a) f é um monomorfismo sse *$\ker f = \{1\}$;*

(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 $\{1\} < \ker f$. Temos

$\boxed{\Rightarrow}$ $f(x) = 1 \ \Rightarrow x = 1$ pois f é injectiva.

$\boxed{\Leftarrow}$ $f(x) = f(x') \Rightarrow f(x^{-1}x') = 1 \Rightarrow x^{-1}x' = 1 \Leftrightarrow x' = x$.

(b) Exercício.

□

Exemplo 1.2.7. Seja $G = \mathbb{Z}$, $m \in \mathbb{N}$ e $H = m\mathbb{Z} \subset \mathbb{Z}$. Temos $H < \mathbb{Z}$.

Exercício 1.2.8. *Todos os subgrupos de $\mathbb{Z}$ são desta forma.*

Exemplo 1.2.9. $\mathbb{R}^\times < \mathbb{C}^\times$.

Exemplo 1.2.10. Seja $H = \{\underline{0}, \underline{2}\} \subset \mathbb{Z}_4$. Temos $H < \mathbb{Z}_4$.

Exemplo 1.2.11. 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 1.2.12. Seja $m \in \mathbb{N}$. O subgrupo $m\mathbb{Z} < \mathbb{Z}$ é o núcleo da projecção canónica $\mathbb{Z} \to \mathbb{Z}_m$.

Definição 1.2.13. *Seja $f\colon G \to H$ um homomorfismo de grupos e seja $J < H$. Define-se*

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

Exercício 1.2.14. *Mostre que $f^{-1}(J) < G$.*

Exercício 1.2.15. *Seja G um grupo e sejam $H_i < G$, $i \in I$. Mostre que $\cap_{i\in I} H_i < G$. Mostre que $\cup_{i\in I} H_i$ não é subgrupo em geral.*

Definição 1.2.16. *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 1.2.17. Seja $G = \mathbb{Z}$ e $X = \{m\}$. Temos $\langle X \rangle = m\mathbb{Z}$.

Notação 1.2.18. 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 1.2.19. *Seja G um grupo e seja $X \subset G$, então*

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

Demonstração. Exercício. □

Exemplo 1.2.20. Seja $G = \mathbb{Z}$ e $X = \{2, 3\}$, então $\langle X \rangle = \mathbb{Z}$ pois $1 = 3 - 2 \in \langle X \rangle$.

1.2.1 Grupos cíclicos

Definição 1.2.21. *Um grupo G diz-se* finitamente gerado *se existem $a_1, \dots, a_n \in G$* t.q. *$G = \langle a_1, \dots, a_n \rangle$. Neste caso, $a_1, \dots, a_n$ dizem-se geradores de G. Se se existe $a \in G$* t.q. *$G = \langle a \rangle$, G diz-se cíclico.*

Observação 1.2.22. Os grupos cíclicos são abelianos.

Exemplo 1.2.23. $\mathbb{Z}$, $\mathbb{Z}_m$ são grupos cíclicos.

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

Proposição 1.2.24. *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 um epimorfismo:

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

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 um epimorfismo. Vejamos que é também injectivo:

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

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

Observação 1.2.25.

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 1.2.26. *Seja G um grupo e seja $a \in G$. Define-se* ordem *de a como a cardinalidade de $\langle a \rangle$, e denota-se este número por $|a|$. Ou seja, $|a| = |\langle a \rangle|$.*

Exemplo 1.2.27. Seja $G = \{z \in \mathbb{C} \mid |z| = 1\} < \mathbb{C}^*$ 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 $|a'| = \infty$.

Exercício 1.2.28. *Seja G um grupo e seja $a \in G$. Mostre que se $|a| = \infty$, então*

i. $a^k = 1 \Leftrightarrow k = 0$;

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

Se $|a| = m > 0$, mostre que

i. $m = \min\{k \in \mathbb{N} \mid a^k = 1\}$;

ii. $a^k = 1 \Leftrightarrow m \mid k$;

iii. $a^r = a^s \Leftrightarrow \underline{r} = \underline{s}$ *em* $\mathbb{Z}_m$ i.e., $r \equiv s \mod m$*)*;

iv. $\langle a \rangle = \{1, a, a^2, \ldots, a^{m-1}\}$;

v. $\forall k \in \mathbb{N},\ k \mid m \ \Rightarrow |a^k| = \frac{m}{k}$.

O exercício seguinte mostra que todos os subgrupos de grupos cíclicos são igualmente cíclicos.

Exercício 1.2.29. *Seja G um grupo cíclico, seja $a \in G$ um gerador e seja $H < G$. Mostre que $H = \langle a^m \rangle$ onde $m = \min\{k \in \mathbb{N} \mid a^k \in H\}$.*

Exercício 1.2.30. *Seja G um grupo cíclico de ordem m e seja $k \in \mathbb{N}$* t.q. *$k \mid m$. Mostre que G tem exactamente um subgrupo (cíclico) de ordem k.*

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

Teorema 1.2.31. *Seja $G = \langle a \rangle$ um grupo cíclico. Se $|G| = \infty$ os geradores de G são a e a^{-1}. Se $|G| = m$, os geradores de G são os elementos de $\{a^k \mid (k, m) = 1\}$.*

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 $(k,m)=1 \Leftrightarrow \exists r,s : rk+sm=1$, 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

$$rk \equiv 1 \mod m \Leftrightarrow \exists s : rk+sm=1.$$

$\square$

1.3 3ª Aula

1.3.1 Classes laterais esquerdas, quociente por um subgrupo

Definição 1.3.1. *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 1.3.2. *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

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

(respectivamente, $Ha := \{ha \mid h \in H\}$ 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.*

Demonstração. Exercício. □

Notação 1.3.3. 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 1.3.4. *Seja $H < G$, então as classes laterais esquerdas aH, $a \in G$, formam uma partição de G em conjuntos com o mesmo cardinal;*

Definição 1.3.5. *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 1.3.6. *Se $H < G$, temos*

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

Se $|G| < \infty$, então

- $\forall H < G,\ |H| \mid |G|$, *e*
- $\forall g \in G$, $|g| \mid |G|$.

Demonstração. A partição

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

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

Teorema 1.3.7. *Sejam $K < H < G$, então*

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

Demonstração. Caso G finito:

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

□

Exercício 1.3.8. *Demonstre o teorema no caso de G infinito.*

Exemplo 1.3.9. Seja $G = S_3$ e $H = \langle (12) \rangle$. Então $|S_3| = [G : H]|H|$ e $|H| = 2$, logo $[G : H] = 3$.

Definição 1.3.10. *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 1.3.11. *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

$$\begin{aligned} HK &= (h_1 J \cup \cdots \cup h_n J)\, K \\ &= h_1 K \cup \cdots \cup h_n K \end{aligned}$$

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

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

□

1.3.2 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 1.3.12. *ASCSE* $\equiv$ *as seguintes condições são equivalentes.*

Teorema 1.3.13. *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.

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

$\boxed{b) \Rightarrow c)}$ óbvio;

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

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

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

□

Definição 1.3.14. *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 1.3.15. A propriedade de ser normal é uma propriedade da inclusão $N < G$, não é uma propriedade do grupo N.

Exemplo 1.3.16. Seja $\tau \in D_3$ *t.q.* $\tau^3 = 1$ (*cf.* Exemplo 1.1.9), então $\langle \tau \rangle \lhd G$.

Exercício 1.3.17. *Seja $H < G$* t.q. $[G : H] = 2$*. Mostre que $H \lhd G$.*

A importância dos subgrupos normais decorre do resultado seguinte.

Teorema 1.3.18. *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 epimorfismo 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.*,
$$\begin{aligned}(gN)(g^{-1}N) &= 1N = N \\ (1N)(gN) &= gN = N = (gN)(1N)\end{aligned}$$

3. Por definição do produto em G/N, π é um homomorfismo.

4. $\pi(g) = N \Leftrightarrow gN = 1N \Leftrightarrow g \in N$.

□

Exercício 1.3.19. *Mostre que*

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 1.3.20. *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

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

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

$\square$

Teorema 1.3.21. *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*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

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

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

$\square$

1.3.3 Teoremas de isomorfismo

Teorema 1.3.22 (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 anterior com $N = \ker f$, obtemos $\operatorname{im} \bar{f} = \operatorname{im} f$ e $\ker \bar{f} = \{1\}$, ou seja, $\bar{f}$ é um isomorfismo. □

Corolário 1.3.23 (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 $NK < G$ (Exercício 1.3.19) □

Teorema 1.3.24. *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

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

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

Nota 1.3.25. 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 1.3.26. 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, $\bar{\varphi}\colon \mathbb{R}^\times/\{\pm 1\} \xrightarrow{\cong} (\mathbb{R}^+, \cdot)$.

1.3.4 Produto directo de grupos

Definição 1.3.27. *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 1.3.28. 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 $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2 + y_2)$ 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
$$\mathbb{R}^\times \cong \mathbb{Z}_2 \times \mathbb{R}.$$

Exercício 1.3.29. *Mostre que $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.*

Exemplo 1.3.30. Sejam H, K grupos. No produto directo $G = H \times K$ é habitual identificar H com $H \times \{1_K\}$ e K com $\{1_H\} \times K$. Com estas identificações, temos
$$H \lhd G, \qquad K \lhd G.$$
De facto,
$$(h_1, k)(h_2, 1_K)(h_1^{-1}, k^{-1}) = (h_1h_2h_1^{-1}, k1_Kk^{-1}) \in H,$$
portanto $H \lhd G$. De forma análoga, mostra-se $K \lhd G$.

Observação 1.3.31. Uma propriedade importante do produto directo $G = H \times K$ é o facto de os elementos de H e K comutarem em G.

1.4 4ª Aula

1.4.1 Acções de grupos

Definição 1.4.1. *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. $\forall x \in X \quad 1x = x$;

ii. $\forall g_1, g_2 \in G, \forall x \in X \quad g_1(g_2x) = (g_1g_2)x$.

Diz-se que X é um conjunto-G.

Observação 1.4.2. Também se define acção à direita: é uma função $X \times G \to X; (x, g) \mapsto xg$ *t.q.*

$$(xg_1)g_2 = x(g_1g_2), \qquad \forall g_1, g_2 \in G, \quad \forall x \in X.$$

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

Observação 1.4.3. Seja

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

Com a operação de composição, S_X é um grupo - o grupo das transformações de X. Uma acção de G em X define uma função $T : G \to S_X$ 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 1.4.4. *Dar uma acção de G em X é equivalente a dar um homomorfismo de grupos $T : G \to S_X$.*

Demonstração. Exercício. $\square$

Definição 1.4.5. *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:*

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

Exemplos 1.4.6.

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: $gx = x \Leftrightarrow g = 1$.

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:

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

   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 1.4.7 (Cayley)**.** *Seja G um grupo, então G é isomorfo a um subgrupo do grupo S_G de transformações de G. Em particular, se $|G| = n$, G é isomorfo a um subgrupo do grupo simétrico S_n (Exercício 1.1.6).*

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

Exemplos 1.4.8.

1. Seja G um grupo. G age à esquerda em G por conjugação – $(g, x) \mapsto g \star x := gxg^{-1}$ –, 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. $\mathrm{O}(n, \mathbb{R}) := \{A \in M_n(\mathbb{R}) \mid AA^T = I\}$ 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 $k^n - \{0\}$ por multiplicação.

Definição 1.4.9. *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 1.4.10. 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 1.4.11. *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 1.4.12. A relação

$$x \sim y \Leftrightarrow \exists g \in G : gx = y$$

é uma relação de equivalência:

reflexividade: $1x = x$;

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 1.4.13. *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 1.4.12 ($X/\sim$) e é denotado X/G. Se $|X/G| = 1$, a acção diz-se* transitiva.

Observação 1.4.14.

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 1.4.15. 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 $k^n - \{0\}$ são os subespaços lineares de k^n com dimensão 1. Define-se $\mathbb{P}(k^n) := (k^n - \{0\})/k^\times$.

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 1.4.16, 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

$$J = \begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_k \end{bmatrix}_{n\times n} \qquad \text{e} \qquad J_i = \begin{bmatrix} \lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix}$$

(e $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ são os valores prórios de A). A menos da ordem[3] 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.

Exercício 1.4.16. *Determine as classes de conjugação em S_n.*
Sugestão: Verifique primeiro que $\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$, para qualquer $\sigma \in S_n$ e qualquer ciclo-k $(i_1\ i_2\ \cdots\ i_k) \in S_n$, 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.

Definição 1.4.17. *Seja G um grupo. Define-se* o centro *de G, $C(G)$, como*

$$C(G) = \{g \in G \mid gg' = g'g, \quad \forall g' \in G\} = \{g \in G \mid |\,\mathrm{Cl}(g)| = 1\} < G.$$

Exercício 1.4.18. *Seja G um grupo. Mostre que $C(G) \lhd G$.*

Exercício 1.4.19. *Seja $n \in \mathbb{N}$ t.q. $n > 2$. Mostre que $C(S_n) = \langle 1 \rangle$.*

Exemplo 1.4.20. Seja $H = \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4) \rangle < S_4$. Então $H \cong D_4$ e $C(H) = \{1, (1\ 3)(2\ 4)\} \cong \mathbb{Z}_2$.

[3] 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*.

Definição 1.4.21. *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 1.4.22. *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,

$$\begin{aligned} h \in G_y \Leftrightarrow hy = y \Leftrightarrow hgx = gx \Leftrightarrow g^{-1}hgx = x \Leftrightarrow g^{-1}hg \in G_x \\ \therefore\ g^{-1}G_yg = G_x. \end{aligned}$$

□

Definição 1.4.23. *Se $\forall x \in X$, $G_x = \{1\}$, diz-se que a acção é* livre*.*

Exemplos 1.4.24.

1. A acção de G em G por multiplicação à esquerda (direita) é livre:

$$gx = x \Leftrightarrow g = 1.$$

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, $G_{gH} = gHg^{-1}$.

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

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

Definição 1.4.25. *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 1.4.26. Como $g^ig = g^{i+1} = gg^i$ para quaisquer $i \in \mathbb{Z}$ e $g \in G$, temos $C_G(g) > \langle g \rangle$.

1.5 5ª Aula

1.5.1 Acções de grupos (cont)

Proposição 1.5.1. *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 $1-1$: $gx = g'x \Leftrightarrow g^{-1}g' \in G_x$.

3. ϕ é epi e é equivariante por construção:
$$\phi(g'(gG_x)) = \phi((g'g)G_x) = (g'g)x = g'\phi(gG_x).$$

□

Exemplo 1.5.2. Seja $X = S^2 := \{x \in \mathbb{R}^3 \mid |x| = 1\}$ e sejam $G = O(3)$, $x_0 = e_1 := (0,0,1) \in S^2$. Recorde-se que G age em X por $(A,x) \mapsto Ax$. Temos
$$G_{x_0} = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & B \end{smallmatrix}\right) \mid B \in O(2)\} \cong O(2). \tag{1.5.1}$$
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 1.5.3. *Seja X um conjunto-G finito e seja $X = \bigcup_{i=1}^n \mathcal{O}_{x_i}$ uma partição em órbitas. Então,*
$$|X| = \sum_{i=1}^n [G : G_{x_i}] \tag{1.5.2}$$

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

1.5.2 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

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

$N_G(H)$ é o maior subgrupo G em que H é normal, diz-se o *normalizador de H em G.*

Teorema 1.5.4. *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 $G_{x_i} \neq G$. $\square$

Corolário 1.5.5. *Se* $|G| = p^m$ *(p primo), então*

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

com $k \geq 1$*.*

Demonstração. Como $C(G) < G$, temos apenas que provar $|C(G)| \neq 1$ (ver Corolário 1.3.6). Do Teorema 1.5.4, obtemos,

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

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

Teorema 1.5.6 (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 $X = \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = 1_G\}$. 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:

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

Temos

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

logo $(g_2, \dots, g_p, g_1) \in X$. 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

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

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 1.5.7. *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 1.5.8.

1. $\mathbb{Z}_p$ é um grupo-p finito;

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

Corolário 1.5.9. *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 (1.5.6), $\exists g$ *t.q.* $|g| = q$, logo $q = p$.

□

Definição 1.5.10. *Seja G um grupo finito* t.q. *$|G| = p^n m$, com p primo e $(p, m) = 1$. Um subgrupo-p de expoente n de G diz-se um* subgrupo-p de Sylow *de G.*

Exemplo 1.5.11. 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 Exercício 1.2.30), então $K = \{\underline{0}\} \times \mathbb{Z}_2$ é um subgrupo-2 de G.

Teorema 1.5.12 (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,

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

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

- $p \nmid |C(G)| \Rightarrow \exists i : p \nmid [G : C_G(x_i)] \Rightarrow p^k \mid |C_G(x_i)|$

  Note-se que $C_G(x_i) \neq G$, pois $x_i \notin C(G)$.

  Da hipótese de indução, aplicada a $C_G(x_i)$, segue que $\exists H < C_G(x_i)$ *t.q.* $|H| = p^k$.

- $p \mid |C(G)| \Rightarrow \exists g \in C(G) : |g| = p$ (pelo Teorema 1.5.6).

  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

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

$\square$

1.6 6ª Aula

1.6.1 Teoremas de Sylow (cont.)

Teorema 1.6.1 (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 1.5.4, temos

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

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

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

□

Exemplo 1.6.2. 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:

1º Caso: $G = \mathbb{Z}_6$.

2º Caso: $G \cong D_3$. 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.* 1.1.9).

Neste caso, os subgrupos de Sylow-2 são:

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

Exemplo 1.6.3. Seja A_4 o subgrupo de S_4 das permutações pares (ver Definição 1.8.8). 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 $\sigma \in A_4 \setminus \{1\}$ é um ciclo-3 ou o produto de duas transposições disjunstas.

Seja P um subgrupo-2 de Sylow. Pela observação anterior, se $\sigma \in P \backslash \{1\}$, 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,

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

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:

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

Exercício 1.6.4. *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. [Sugestão: Comece por verificar que $|D_6| = 12 = |A_4|$ e, portanto, o Teorema de Sylow II implica que D_6 tem 1 ou 3 subgrupos-2 de Sylow e tem 1 ou 4 subgrupos-3 de Sylow, tal como no Exemplo1.6.3 anterior.]*

1.6.2 Os Teoremas de Sylow como Teoremas de estrutura: caso abeliano

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 1.6.5. *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 1.6.6. *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:*

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

Observação 1.6.7. 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 1.6.8. *Seja G um grupo abeliano finito. Então existe um isomorfismo*

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

onde $p_1, \dots, p_n$ *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 1.6.9. 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 $P_1, \dots, P_k$ são os subgrupos de Sylow de G, então

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

1.6.3 Os Teoremas de Sylow como Teoremas de estrutura: caso geral

Questão 1.6.10. Será que dado um grupo finito G 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.

Definição 1.6.11. *Seja G um grupo e sejam $G_1, G_2 < G$. Diz-se que G é o* produto directo interno *de G_1 e G_2 se as seguintes condições se verficam*

(i) $G_1 \cap G_2 = \langle 1 \rangle$

(ii) $g_1 g_2 = g_2 g_1, \forall g_1 \in G_1, \forall g_2 \in G_2$

(iii) $G = G_1 G_2$ *(ver Definição 1.3.10)*

Observação 1.6.12. Se G é o produto directo interno de G_1, G_2, tem-se $G_1 \times G_2 \cong G$. O isomorfismo é dado por $(g_1, g_2) \mapsto g_1 g_2$.

Notação 1.6.13. Se $G_1, G_2 < G$, escrevemos $G = G_1 \times G_2$ para denotar que G é o produto directo interno de G_1 e G_2.

Exemplo 1.6.14. Seja $G = O(3) = \{A \in M_3(\mathbb{R}) \mid AA^T = I\}$ e sejam

$$G_1 = SO(3) \coloneqq \{A \in O(3) \mid \det A = 1\}$$
$$G_2 = \{\pm I_3\} \cong \mathbb{Z}_2.$$

Temos

$$O(3) = SO(3) \times \{\pm I_3\}.$$

Exemplo 1.6.15. Seja $G = D_6 = \langle a, b \mid |a| = 6, |b| = 2, bab^{-1} = a^{-1} \rangle$ (ver Exercício 1.6.4) 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 1.6.16. *Seja G um grupo e sejam $G_1, G_2 < G$. Temos $G = G_1 \times G_2$ sse $G_1 \lhd G$, $G_2 \lhd G$, $G_1 \cap G_2 = \langle 1_G \rangle$ e $G = G_1 G_2$.*

Demonstração.

$\boxed{\Rightarrow}$ Temos que provar $G_i \lhd G$. Sejam $g \in G$ e $h \in G_1$. Temos $g = g_1 g_2$, com $g_1 \in G_1$ e $g_2 \in G_2$, logo

$$\begin{aligned} ghg^{-1} &= g_1 g_2 h \left(g_1 g_2\right)^{-1} = g_1 g_2 h g_2^{-1} g_1^{-1} \\ &= g_1 h g_1^{-1} \in G_1, \end{aligned}$$

portanto $G_1 \lhd G$. Da mesma forma segue $G_2 \lhd G$.

$\boxed{\Leftarrow}$ Temos que mostrar que os elementos de G_1 comutam com G_2. De forma equivalente,

$$\forall g_1 \in G_1, g_2 \in G_2 \qquad \underbrace{g_1 g_2 g_1^{-1} g_2^{-1}}_{g} = 1_G.$$

Ora,

$$\begin{gathered} g_2^{-1} \in G_2, \quad g_1 g_2 g_1^{-1} \in G_2 \Rightarrow g \in G_2 \\ g_1 \in G_1, \quad g_2 g_1^{-1} g_2^{-1} \in G_1 \Rightarrow g \in G_1 \\ \therefore g = 1_G. \end{gathered}$$

$\square$

1.7 7ª Aula

1.7.1 Teoria de estrutura de grupos: grupos nilpotentes e grupos resolúveis

Definição 1.7.1. *Seja G um grupo. Define-se*

$$C_1(G) \coloneqq C(G).$$

Para $i \geq 1$, definimos recursivamente

$$C_{i+1}(G) \coloneqq \pi_i^{-1}\left(C(G/C_i(G))\right),$$

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

Exercício 1.7.2. *Mostre que $C_i(G) \lhd G$.*

Obtemos assim uma sucessão ascendente de subgrupos normais de G:

$$\langle 1_G \rangle \lhd C_1(G) \lhd \cdots \lhd C_n(G) \lhd \cdots$$

Definição 1.7.3. *Um grupo G diz-se* nilpotente *se existe $n \in \mathbb{N}$* t.q. $C_n(G) = G$.

Exemplo 1.7.4. Se G é um grupo abeliano, então G é nilpotente, pois $G = C(G) = C_1(G)$.

Teorema 1.7.5. *Os grupos-p finitos são grupos nilpotentes*

Demonstração. Suponhamos que $i \geq 1$ é *t.q.* $C_i(G) \neq G$. Como $C_i(G) \lhd G$, podemos considerar o quociente $G/C_i(G)$, que é um grupo-p finito. Pelo Corolário 1.5.5, obtemos $C(G/C_i(G)) \neq \langle 1_G \rangle$ e portanto $C_{i+1}(G) \supsetneq C_i(G)$. Como $|G| < \infty$, a sucessão $C_i(G)$ tem que terminar eventualmente com $C_i(G) = G$. □

Teorema 1.7.6. *O produto directo de grupos nilpotentes é nilpotente.*

Demonstração. Sejam H, K grupos nilpotentes se seja $G = H \times K$. Vejamos que $C_i(G) = C_i(H) \times C_i(K)$. Para $i = 1$ a igualdade é óbvia:

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

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

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

$$G \xrightarrow{\widetilde{\pi}} \frac{H}{C_i(H)} \times \frac{K}{C_i(K)} \underset{\cong}{\xrightarrow{\psi}} \frac{H \times K}{C_i(H) \times C_i(K)} = \frac{G}{C_i(G)},$$

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 1.7.7 abaixo).

Temos,

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

$\square$

Exercício 1.7.7. *Sejam H, K grupos.*

(a) sejam $H_1 \lhd H$ e $K_1 \lhd K$. Mostre que a expressão $\psi([h],[k]) = [h,k]$ define um isomorfismo $\psi\colon H/H_1 \times K/K_1 \xrightarrow{\cong} \frac{H\times K}{H_1 \times K_1}$;

(b) seja $\widetilde{\pi}\colon H \times K \to H/H_1 \times K/K_1; (h,k) \mapsto ([h],[k])$. Mostre que $\psi \circ \widetilde{\pi}$ é a projecção canónica $H \times K \to \frac{H\times K}{H_1\times K_1}$.

Lema 1.7.8. *Seja $H \subsetneqq G$* t.q. *G é um grupo nilpotente. Então $H \subsetneqq N_G(H)$.*

Demonstração. Definindo $C_0(G) \coloneqq \langle 1_G \rangle$ existe $i \in \mathbb{N}_0$ *t.q.*

1. $C_i(G) < H$;

2. $C_{i+1}(G) \not< H$.

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

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

$$C_{i+1}(G) = \pi^{-1}\left(C\left(G/C_i(G)\right)\right),$$

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

Seja $h \in H$. Temos,

$$\begin{aligned}
&\pi(a)\pi(h) = \pi(h)\pi(a)\\
\Leftrightarrow\, & ahC_i(G) = haC_i(G)\\
\Leftrightarrow\, & h^{-1}a^{-1}ha \in C_i(G)\\
\Rightarrow\, & h^{-1}a^{-1}ha \in H\\
\Leftrightarrow\, & a^{-1}ha \in H\\
\Leftrightarrow\, & a \in N_G(H).
\end{aligned}$$

$$\therefore H \lneq N_G(H).$$

□

Corolário 1.7.9. *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 1.7.8, concluímos que $N_G(P) = G$, ou seja, $P \lhd G$. □

Teorema 1.7.10. *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 1.7.5); 2. o produto directo de grupos nilpotentes é nilpotente (Teorema 1.7.6).

$\boxed{\Rightarrow}$ 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,

$$|G| = |P_1| \cdots |P_k| \quad \text{e} \quad P_i \cap P_j = \langle 1_G \rangle \text{ para } i \neq j.$$

Daqui segue (ver Exercício 1.7.11) $G = P_1 \cdots P_k$. Concluímos que

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

□

Exercício 1.7.11. *Seja G um grupo finito e sejam $G_1, \dots, G_k \lhd G$* t.q.*, para todo i, $G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_k) = \langle 1_G \rangle$ e $|G| = |G_1| \cdots |G_k|$. Mostre que*

(a) G_i comuta com G_j;

(b) $G = G_1 \cdots G_k$ (Definição 1.3.10).

Corolário 1.7.12. *Seja G um grupo nilpotente finito e seja $m \in \mathbb{N}$* t.q. *$m \mid |G|$. Então existe $H < G$* t.q. *$|H| = m$.*

Demonstração. Exercício. □

Exemplo 1.7.13. O grupo simétrico S_n não é nilpotente se $n > 2$, pois:

$$C(S_n) = \langle 1 \rangle$$

(ver Exercício 1.4.19), logo

$$\begin{aligned}
C_1(G) &= \langle 1 \rangle \\
C_2(G) &= \pi^{-1}(C\left(S_n/\langle 1 \rangle\right) = \pi^{-1}(\langle 1 \rangle) \\
&\vdots \\
C_i(G) &= \langle 1 \rangle, \quad \forall i.
\end{aligned}$$

Exemplo 1.7.14. 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 1.5.12;

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

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

Exemplo 1.7.15. 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 $C(\mathbb{H}_8) = \{\pm 1\}$ e $\mathbb{H}_8/C(\mathbb{H}_8)$ tem ordem 4, pelo que $\mathbb{H}_8/C(\mathbb{H}_8) \cong \mathbb{Z}_4$ ou $\mathbb{H}_8/C(\mathbb{H}_8) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Concluímos que $C_2(\mathbb{H}_8) = \mathbb{H}_8$, *i.e.*, $n = 2$.

Definição 1.7.16. *Seja G um grupo. Define-se o* comutador *de $g_1, g_2 \in G$ como*

$$[g_1, g_2] \coloneqq g_1 g_2 g_1^{-1} g_2^{-1} = g_1 g_2 \left(g_2 g_1\right)^{-1} \in G.$$

Proposição 1.7.17. *Sejam $g, g_1, g_2, g_3 \in G$. Então*

(i) $[g_1, g_2]^{-1} = [g_2, g_1]$;

(ii) $[g_1, g_2] = 1_G \Leftrightarrow g_1 g_2 = g_2 g_1$;

(iii) $g[g_1, g_2]g^{-1} = [g g_1 g^{-1}, g g_2 g^{-1}]$;

(iv) $[g_1, g_2 g_3] \cdot [g_2, g_3 g_1] \cdot [g_3, g_1 g_2] = 1_G$;

(v) se H é um grupo e $\phi \in \hom(G, H)$, então

$$\phi([g_1, g_2]) = [\phi(g_1), \phi(g_2)]\,.$$

Demonstração. Óbvio, excepto (iv), que é um cálculo directo. □

Definição 1.7.18. *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 1.7.19. 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 1.7.20. *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 1.7.21. Um grupo G é abeliano *sse* $G^{(1)}$ é trivial.

Exercício 1.7.22. *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 1.1.9). 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 1.7.23. Muitos autores definem o comutador de g_1, g_2 como $g_1^{-1}g_2^{-1}g_1g_2$, o que corresponde na Definição 1.7.20 a $[g_1^{-1}, g_2^{-1}]$. O subgrupo derivado que se obtém com ambas definições é o mesmo.

Proposição 1.7.24 (Propriedades do Derivado)**.** *Sejam* G, G_1, G_2 *grupos. Temos*

(i) $\phi \in \hom(G_1, G_2) \Rightarrow \phi\left(G_1^{(1)}\right) \subset G_2^{(1)}$*;*

(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* $\phi \in \hom(G,A)$ $\exists! \tilde{\phi} \in \hom(G/G^{(1)}, A)$ *que faz comutar*

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & A \\ G/G^{(1)} \arrow[ur, dashed, "\exists! \tilde{\phi}"'] & \end{tikzcd}$$

Demonstração. As asserções (i) e (ii) seguem imediatamente das propriedades dos comutadores. Quanto à asserção (iii): $G/G^{(1)}$ é abeliano, pois de $g_1g_2 = [g_1, g_2]g_2g_1$ vem

$$\pi(g_1)\pi(g_2) = \pi(g_2)\pi(g_1).$$

Quanto ao diagrama:

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

□

Exercício 1.7.25. *Seja* G *um grupo e seja* $H \lhd G$ t.q. G/H *é abeliano. Mostre que* $G^{(1)} < H$*.*

Notação 1.7.26. Diz-se que $G/G^{(1)}$ é o *abelianizado* de G.

Exemplo 1.7.27. Do Exercício 1.7.22 concluimos que o abelianizado de D_3 é $D_3/D_3^{(1)} \cong \mathbb{Z}_2$.

Exemplo 1.7.28. Seja $G = \mathbb{H}_8$. Do Exemplo 1.7.15, sabemos que $\mathbb{H}_8/C(\mathbb{H}_8)$ é abeliano, logo, pelo exercício anterior, temos

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

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

Definição 1.7.29. *Seja G um grupo. Definimos recursivamente o n-*ésimo subgrupo derivado *de G da seguinte forma:*

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

Exercício 1.7.30. *Mostre que $G^{(n)} \lhd G$.*

Observação 1.7.31. 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 1.7.32. *Um grupo G diz-se* resolúvel *se existe $n \in \mathbb{N}$ t.q. $G^{(n)} = \langle 1_G \rangle$.*

1.8 8ª Aula

Proposição 1.8.1. *Seja G um grupo nilpotente, então G é resolúvel.*

Demonstração. Considere-se a sequência crescente de subgrupos

$$\langle 1\rangle =: C_0(G) < C_1(G) < C_2(G) < \cdots < C_n(G) = G.$$

Note-se que $C_i(G)/C_{i-1}(G) \cong C(G/C_{i-1}(G))$ é abeliano, portanto

$$C_i(G)^{(1)} < C_{i-1}(G).$$

Assim,

$$\begin{aligned} & G^{(1)} = C_n(G)^{(1)} < C_{n-1}(G) \\ \Rightarrow\ & G^{(2)} = (C_n(G))^{(2)} < C_{n-1}(G)^{(1)} < C_{n-2}(G) \\ & \quad \vdots \\ \Rightarrow\ & G^{(n)} = (C_n(G))^{(n)} < C_0(G) = \langle 1\rangle. \end{aligned}$$

□

Exemplo 1.8.2. Seja $G = D_6 = \langle a, b \mid |a| = 6, |b| = 2, bab^{-1} = a^{-1}\rangle$. Como $D_6^{(1)} = \langle a^2\rangle \cong Z_3$ é abeliano, então $D_6^{(2)} = \{1\}$, logo D_6 é resolúvel.

Como $C_1(D_6) = C(D_6) = \langle a^3\rangle$ e $D_6/C(D_6) \cong S_3$ (ver 1.6.15), então $C(D_6/C(D_6)) = \{1\}$, logo $C_i(D_6) = \{1\}$, para $i \geq 2$, logo D_6 não é nilpotente.

Teorema 1.8.3. *Sejam G, K grupos. Então*

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

2. *G resolúvel e $f \in \hom(G, K) \Rightarrow f(G)$ 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., G/N é resolúvel.

□

1.8.1 Grupos Simples

Definição 1.8.4. *Um grupo G diz-se* simples *se $H \lhd G$ implica $H = G$ ou $H = \langle 1 \rangle$.*

Exemplo 1.8.5. Se G é abeliano então todos os seus subgrupos são normais, logo G é simples *sse* $G \cong \mathbb{Z}_p$, para algum primo $p \in \mathbb{N}$.

Definição 1.8.6. *Considere-se o homomorfismo $\varphi\colon S_n \to \mathrm{GL}_n(\mathbb{Z})$ dado por*

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

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.

Observação 1.8.7. Como $\det(\varphi(\sigma)) \in \mathbb{Z}^\times$ e $\det\colon \mathrm{GL}_n(\mathbb{Z}) \to \mathbb{Z}^\times$ é um homomorfismo, $\det\circ\varphi\colon S_n \to \mathbb{Z}^\times$ é um homomorfismo.

Definição 1.8.8. *O grupo* alternado *é o seguinte subgrupo de S_n:*

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

Exercício 1.8.9 (ver Exercício 1.1.8)**.** *Seja $\sigma \in S_n$. Mostre que $\sigma \in A_n$* sse

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

Observação 1.8.10. Note-se que $[S_n : A_n] = 2$, logo

$$A_n \lhd S_n.$$

Teorema 1.8.11. *A_n é simples* sse *$n \neq 4$.*

Demonstração. Ver [Hun74, §I.6]. □

Exemplo 1.8.12. Se $n = 3$, então $|A_3| = 3$, logo $A_3 \cong \mathbb{Z}_3$ é simples.

Exemplo 1.8.13. 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.

1.8.2 Séries normais e subnormais

Definição 1.8.14. *Um* série subnormal *de um grupo G é uma cadeia de subgrupos*

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

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

Exemplo 1.8.15. $G^{(n)} < G^{(n-1)} < \cdots < G^{(1)} < G$ é uma série normal. Diz-se a *série derivada* de G.

Exemplo 1.8.16. Seja G nilpotente *t.q.* $G = C_n(G)$, então fazendo $G_i \coloneqq C_{n-i}(G)$, a cadeia

$$G_n = C_0(G) < G_{n-1} = C(G) < \cdots < G_0 = C_n(G) = G$$

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 $N < G$ *t.q.* $N \lhd G_i$ e $G_{i+1} < N$ (se $i < n$) podemos obter uma nova série normal:

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

Definição 1.8.17. *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 1.8.18. *Seja G um grupo. Uma série subnormal $G = G_n < \cdots G_{i+1} < G_i < \cdots G_1 < G_0 = G$ 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 1.8.19. A série derivada $\langle 1 \rangle = G^{(n)} < G^{(n-1)} < \cdots < G^{(1)} < G^{(0)} \coloneqq G$ de um grupo resolúvel é uma série resolúvel.

Teorema 1.8.20. *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 $G_1, \dots, G_i$ escolhidos, prosseguimos escolhendo $G_{i+1} < G_i$ normal maximal. O processo termina com $G_n = \langle 1 \rangle$ 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
$$\{G_{i+1} < N \lhd G_i\} \longleftrightarrow \left\{\tilde{N} \lhd G_i/G_{i+1}\right\}.$$

□

Teorema 1.8.21. *Um grupo G é resolúvel* sse *tem uma série resolúvel.*

Demonstração.

$\boxed{\Rightarrow}$ Óbvio.

$\boxed{\Leftarrow}$ Seja $\langle 1 \rangle = G_n < \cdots < G_1 < G_0 = G$ uma série resolúvel. Temos
$$\begin{aligned}
G/G_1 \text{ abeliano} &\Rightarrow G^{(1)} < G_1 \\
&\Rightarrow G^{(2)} < G_1^{(1)} \\
G_1/G_2 \text{ abeliano} &\Rightarrow G_1^{(1)} < G_2 \Rightarrow G^{(2)} < G_2 \\
&\vdots \\
&\Rightarrow G^{(n)} < G_n = \langle 1 \rangle \\
&\Rightarrow G \text{ é resolúvel.}
\end{aligned}$$

□

Exercício 1.8.22. *Seja D_n o grupo das simetrias de um polígono regular com n lados. Mostre que existem $a, b \in D_n$* t.q. *$a^n = 1 = b^2$, $D_n = \langle a, b\rangle$ e $ba = a^{n-1}b$. Em particular $|D_n| = 2n$.*

Exemplo 1.8.23. O grupo D_n é resolúvel porque

$$\langle 1\rangle < \langle a\rangle < D_n$$

é uma série resolúvel: $D_n/\langle a\rangle \cong \mathbb{Z}_2$.

Definição 1.8.24. *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 1.8.25. A série derivada (logo resolúvel) do grupo D_6 é

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

(ver Exemplo 1.8.2) 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 1.8.23 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 1.8.23 e obter

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

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 1.8.26 (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]. □

Observação 1.8.27. 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 $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Capítulo 2

Anéis

2.1 9ª Aula

Definição 2.1.1. *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 1 ou 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 2.1.2.

1. A identidade de $(A, +)$ é denotada por 0 (ou 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 2.1.3. Na definição de anel dada em [Hun74] não se exige que $(A, \cdot)$ tenha identidade e os anéis aqui considerados são aí designados anéis com identidade.

Observação 2.1.4 (Propriedades básicas da soma e do produto)**.**

1. $\forall x \in A, \quad 0 \cdot x + x = (0+1)x = 1 \cdot x = x \Rightarrow 0 \cdot x = 0;$

2. $\forall x, y \in A, \quad (-x)y + xy = (-x+x)y = 0 \cdot x = 0 \Rightarrow -xy = (-x)y;$

3. para cada $n \in \mathbb{Z}$, temos $n(xy) = (nx)y = x(ny)$;

Definição 2.1.5. $A^\times = (\{x \in A \mid x$ *é invertível em* $(A, \cdot)\}, \cdot)$ *é um grupo que se designa por* grupo das unidades *de* A*.*

Exemplos 2.1.6. 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; $\mathbb{K}^\times = (\mathbb{K} - \{0\}, \cdot)$;

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 $\underline{i} \cdot \underline{j} := \underline{i \cdot j}$ (*cf.* Exercício 1.1.15); tem-se

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

pois

$$xk \equiv 1 \mod m \quad \text{tem solução } sse\ (k, m) = 1.$$

Definição 2.1.7. *Um elemento* $a \in A$ *diz-se um* divisor de zero à esquerda (direita) *se existe* $x \in A - \{0\}$ t.q. $ax = 0$ *(*resp.*)* $xa = 0$*. Se* a *é divisor de zero à esquerda e à direita, diz-se simplesmente que é um* divisor de zero*.*

Exemplo 2.1.8. Em $\mathbb{Z}_6$, $\underline{3}$ é um divisor de zero, pois $\underline{2} \cdot \underline{3} = \underline{3} \cdot \underline{2} = 0$.

Definição 2.1.9. *Se* A *é um anel comutativo sem divisores de zero* t.q. $1 \neq 0$*, diz-se que* A *é um um* domínio integral*. Um anel* D t.q. $1 \neq 0$ *e* $D^\times = D - \{0\}$ *diz-se um* anel de divisão*. Um anel de divisão comutativo diz-se um* corpo*.*

Exemplos 2.1.10 (Domínios integrais, corpos e anéis de divisão)**.**

1. $\mathbb{Z}$ é um domínio integral;

2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ e $\mathbb{F}_p := \mathbb{Z}_p$ (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 2.1.11. 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:

$$\begin{aligned}
\sum_{i=1}^n r_i g_i + 0 \cdot g &= \sum_{i=1}^n r_i g_i, \quad \forall g \in G \\
\sum_{i=1}^n r_i g_i + \sum_{i=1}^n s_i g_i &= \sum_{i=1}^n (r_i + s_i) g_i \\
\sum_{i=1}^n r_i g_i + \sum_{i=n+1}^m r_i g_i &= \sum_{i=1}^m r_i g_i \\
\sum_{i=1}^n r_i g_i \cdot \sum_{j=1}^m s_j h_j &= \sum_{i=1}^n \sum_{j=1}^m r_i s_j g_i h_j
\end{aligned}$$

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

Exercício 2.1.12. *Seja G um grupo. Mostre que $\mathbb{Z}(G)$ é um anel. Dê um exemplo em que $\mathbb{Z}(G)$ tem divisores de zero.*

Exemplo 2.1.13. 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 2.1.14. *Sejam A, B anéis. Uma função $f\colon A \to B$ diz um* homomorfismo de anéis *se*

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

Nota 2.1.15. Tal como referido anteriormente, em [Hun74] consideram-se anéis sem identidade e, por isso, não se exige a condição $f(1_A) = 1_B$ na definição de homomorfismo de anéis.

Exemplos 2.1.16.

1. Se A é um anel, a função $f\colon \mathbb{Z} \to A$ definida por
$$f(n) \coloneqq n \cdot 1_A$$
é um homomorfismo de anéis e é único. Portanto, para todo o anel A $|\hom(\mathbb{Z}, A)| = 1$.

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 2.1.17. *Seja A um anel. Um* subanel *de A é um subconjunto* $B \subset A$ t.q. *a inclusão $B \subset A$ é um homomorfismo de anéis* $(B, +_A, \cdot_A) \to (A, +_A, \cdot_A)$ *. Em particular, tem-se $0_A, 1_A \in B$.*

Exemplos 2.1.18.

1. $\mathbb{Z} \subset \mathbb{Q}$ é um subanel;

2. se A é um anel,
$$C(A) \coloneqq \{x \in A \mid \forall a \in A, xa = ax\}$$
é um subanel de A pois $0_A, 1_A \in C(A)$ e
$$\forall a \in A, \quad \begin{cases} xa = ax \\ ya = ay \end{cases} \Rightarrow \begin{cases} (x \pm y)a = a(x \pm y) \\ (xy)a = (xa)y = a(xy) \end{cases}$$

2.1.1 Ideais

Definição 2.1.19. *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 2.1.20.

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:

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

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

   $$(BA)e_i = B(Ae_i) = 0.$$

   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

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

Exercício 2.1.21. *Dê um exemplo de um anel A e $a \in A$ tais que*

$$\{xay \mid x, y \in A\}$$

não é um ideal.

Exercício 2.1.22. *O conjunto*

$$J_k \coloneqq \left\{A \in M_n(\mathbb{R}) \mid A^T e_i = 0, \text{ para } i \neq k\right\}$$

é um ideal à direita mas não à esquerda.

Definição 2.1.23 (Ideais principais)**.** *Os ideais aA e Aa dizem-se* ideais principais *(resp., esquerdo e direito).*

Exemplo 2.1.24. Em $\mathbb{Z}$ todos os ideais são principais.

Definição 2.1.25. *Um ideal I (à esquerda, direita) diz-se* próprio *se $I \neq A$.*

Observação 2.1.26. Um ideal $I \neq \{0\}$ é próprio *sse* I não contém nenhuma unidade.

Exemplo 2.1.27. 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).

Exercício 2.1.28. *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. $xa \in I$).

Exercício 2.1.29. *Sejam $\{I_k \mid k \in K\}$ ideais (esquerdos, direitos) de um anel. Mostre que $\cap_{k \in I} I_k$ é um ideal (resp. esquerdo, direito).*

Definição 2.1.30. *Seja A um anel e seja $X \subset A$. O* ideal gerado *por X é*

$$(X) \coloneqq \bigcap_{\substack{I \text{ é ideal t.q.} \\ X \subset I}} I.$$

Notação 2.1.31. $(x_1, \ldots, x_n) \coloneqq (\{x_1, \ldots, x_n\})$.

Exercício 2.1.32. $(x) = \{\sum_{i=1}^n a_i x b_i \mid a_i, b_i \in A, n \in \mathbb{N}\}$.

Definição 2.1.33. *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 2.1.34. $aX \coloneqq \{a\}X$, $Xa \coloneqq X\{a\}$, $X^n = \underbrace{X \cdots X}_{n\text{-vezes}}$.

Exercício 2.1.35. *Sejam $X, Y, Z \subset A$ ideais (esquerdos, direitos). Mostre que*

(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) $(X + Y)Z = X + YZ$*.*

Teorema 2.1.36 (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 $f \in \hom(A, B)$* t.q. *$I \subset \ker f$ existe um único $\bar{f} \in \hom(A/I, B)$ que faz comutar o diagrama seguinte*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ A/I \arrow[ur, "\exists! \bar{f}"] & \end{tikzcd}$$

Tem-se

$$\ker \bar{f} = \pi(\ker f), \qquad \operatorname{im} \bar{f} = \operatorname{im} f.$$

Demonstração.

1. O produto está bem definido:

$$\begin{aligned} \pi(a) = \pi(a') \ \wedge \ \pi(b) = \pi(b') \ &\Leftrightarrow \ a - a', b - b' \in I. \\ &\Rightarrow a'b' = ab + \underbrace{(a' - a)b}_{\in I} + \underbrace{a'(b' - b)}_{\in I} \\ &\Rightarrow \pi(a'b') = \pi(ab). \end{aligned}$$

A identidade em A/I é $\pi(1_A)$: $\pi(a)\pi(1_A) = \pi(a1_A)\pi(a) = \pi(1_A a) = \pi(1_a)\pi(a)$.

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 epimorfismo *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:

$$\bar{f}(\pi(a))\bar{f}(\pi(b)) = f(a)f(b) = f(ab) = \bar{f}(\pi(ab)) = \bar{f}(\pi(a)\pi(b)),$$
$$\bar{f}(\pi(1_A)) = f(1_A) = 1_B.$$

□

Exemplo 2.1.37. 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 $f \in \hom(\mathbb{Z}, A)$ *t.q.* $(m) \subset \ker f$. O único homomorfismo $\mathbb{Z} \to A$ é dado por $1 \mapsto 1_A$, portanto há um homomorfismo $\mathbb{Z}_m \to A$ se $m \cdot 1_A = 0$. Neste caso, o homomorfismo é dado por $\bar{i} \mapsto i \cdot 1_A$. Se $m \cdot 1_A \neq 0$, $\hom(\mathbb{Z}_m, A) = \varnothing$.

2.2 10ª Aula

Definição 2.2.1. *Seja A um anel. Define-se a* característica *de A como*

$$\operatorname{car} A = \min \{m \in \mathbb{N} \mid m \cdot 1_A = 0\},$$

se o mínimo existir. Caso contrário, define-se $\operatorname{car} A = 0$.

Exemplos 2.2.2.

1. $\operatorname{car}(\mathbb{Z}_m) = m$;

2. $\operatorname{car}(\mathbb{Z}) = 0$;

3. $\operatorname{car}(\mathbb{Q}) = \operatorname{car}(\mathbb{R}) = \operatorname{car}(\mathbb{C}) = 0$;

4. $\operatorname{car} M_n(A) = \operatorname{car}(A)$.

Proposição 2.2.3. *Seja A um anel* t.q. $\operatorname{car}(A) = m > 0$. *Então o homomorfismo $\varphi\colon \mathbb{Z}_m \to A; \bar{i} \to i \cdot 1_A$ é injectivo.*

*Se A não tem divisores de zero (*e.g.*, A é um domínio integral), então* $\operatorname{car} A = 0$ *ou* $\operatorname{car} A$ *é primo.*

Demonstração. A primeira asserção segue de

$$\varphi(\bar{i}) = 0 \Leftrightarrow i \cdot 1_A = 0 \Leftrightarrow i \in \{k \in \mathbb{N} \mid k \cdot 1_A = 0\} \Rightarrow i \geq m,$$

se $i > 0$. Suponhamos que A não tem divisores de zero e seja $m = d_1 d_2 > 0$ com $d_i > 0$. Então

$$0 = m{\cdot}1_A = (d_1{\cdot}1_A)(d_2{\cdot}1_A) = (d_2{\cdot}1_A)(d_1{\cdot}1_A) \Rightarrow d_1{\cdot}1_A = 0 \vee d_2{\cdot}1_A = 0 \Rightarrow m = d_1 \vee m = d_2.$$

□

Corolário 2.2.4 (Teoremas de Isomorfismo)**.**

1. *$f \in \hom(A, B)$ induz um isomorfismo*

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

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 2.2.5. *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 2.2.6. *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 2.2.7. *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 2.2.8. *Seja A um anel.*

(a) Se A é comutativo e $I \subset A$ é um ideal, então I é primo sse

$$\forall a, b \in A \quad ab \in I \Rightarrow a \in I \ \vee\ b \in I. \tag{2.2.1}$$

(b) *Se A é não comutativo, então a condição* (2.2.1) *é suficiente para que I seja primo (mas não necessária - ver exercícios).*

Demonstração.

$\boxed{\Leftarrow}$ Sejam J, K ideais *t.q.* $JK \subset I$. Suponhamos $K \not\subset I$. Seja $y \in K \setminus I$. Temos

$$\begin{aligned} \forall x \in J \quad xy \in I \Rightarrow x \in I \\ \therefore J \subset I. \end{aligned}$$

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

$$\begin{aligned} & (a) \subset I \quad \vee \quad (b) \subset I \\ \Leftrightarrow \quad & a \in I \quad \vee \quad b \in I. \end{aligned}$$ □

Exemplos 2.2.9.

1. Seja A um domínio integral. Então (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

$$\begin{aligned} & \forall a, b \in \mathbb{Z} \quad ab \in (m) \Rightarrow a \in (m) \vee b \in (m) \\ \Leftrightarrow \quad & \forall a, b \in \mathbb{Z} \quad m \mid ab \Rightarrow m \mid a \vee m \mid b. \end{aligned}$$

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 2.2.10. *Seja A um anel. Um ideal $I \subset A$ diz-se* maximal *se $I \neq A$ e*

$$\forall_{ideal\ J \subset A} \quad J \supset I \Rightarrow J = A \vee J = I.$$

De forma análoga, define-se ideal esquerdo maximal *e* ideal direito maximal.

Exemplos 2.2.11.

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

$$\begin{aligned} J \supsetneq I &\Rightarrow \exists a \in \mathbb{R} - \{0\} : a \in J \\ &\Rightarrow J \supset (a, x, y) = A, \end{aligned}$$

logo I é maximal.

Teorema 2.2.12. *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.*

$$\pi(a)\pi(b) = 1_{A/M} = \pi(1_A),$$

logo $ab - 1_A \in M$ e portanto $1_A \in I$, ou seja, $I = A$. □

2.2.1 Conjuntos parcialmente ordenados: lema de Zorn

Definição 2.2.13. *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 2.2.14.

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 2.2.15. 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 2.2.16. $(\mathbb{R}, \leq)$ é um conjunto totalmente ordenado.

Definição 2.2.17. *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 2.2.18 (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 2.2.19. *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

$$aJ \subset J \wedge Ja \subset J, \qquad \text{(resp. } aJ \subset J,\ Ja \subset J\text{)}$$

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 $1_A \notin K$, $\forall K \in Y$ e assim $1_A \notin J$. 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 $M \supset I$. □

Teorema 2.2.20 (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

   $$\begin{aligned} &a \equiv x \equiv a_j \mod I_j, \quad j = 2, \ldots, n \\ &a \equiv a_1 \mod I_1. \end{aligned}$$

3. Provamos a unicidade de a:

   $$\begin{aligned} &a \equiv a_j \equiv a' \mod I_j, j = 1, \ldots, n \\ \Rightarrow\, &a - a' \in I_1 \cap \cdots \cap I_n \\ \Leftrightarrow\, &a \equiv a' \mod I_1 \cap \cdots \cap I_n. \end{aligned}$$

$\square$

2.3 11ª Aula

Definição 2.3.1. *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 2.3.2. 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.*

$$a_i = \begin{cases} a, & i = k \\ 0, & i \neq k \end{cases}$$

não é um homomorfismo de anéis, pois $i_k(1_{A_k}) \neq 1$.

Teorema 2.3.3 (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*

$$\begin{tikzcd} & \prod_{i\in I} A_i \arrow[d, "\pi_k"] \\ B \arrow[ur, "\exists! f"] \arrow[r, "f_k"'] & A_k \end{tikzcd}$$

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 2.3.4. 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 $f_i\colon B \to A_i$, $i \in I$.

Exemplo 2.3.5. 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 2.2.20), 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 2.3.6. Sejam $m_1, \ldots, m_r \in \mathbb{N}$ *t.q.* $(m_i, m_j) = 1$, $i \neq j$, 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

$$\mathbb{Z}_m \cong \prod_{j=1}^{r} \frac{\mathbb{Z}/(m)}{(m_j)/(m)} \cong \prod_{j=1}^{r} \frac{\mathbb{Z}}{(m_j)} = \prod_{j=1}^{r} \mathbb{Z}_{m_j}.$$

2.3.1 Anéis Comutativos

Nesta Secção A denota um *anel comutativo*. Recorde-se (2.2.1) que um ideal $P \subset A$ é primo *sse*

$$ab \in P \Rightarrow a \in P \quad \vee \quad b \in P.$$

Teorema 2.3.7. *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*

$$\forall a, b \in A \quad \pi(a)\pi(b) = 0 \Rightarrow \pi(a) = 0 \vee \pi(b) = 0.$$

Ou seja,

$$ab \in P \Rightarrow a \in P \vee b \in P.$$

□

Corolário 2.3.8. *O ideal* (0) *é primo* sse *A é um domínio integral.*

Teorema 2.3.9. *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 2.2.12).

$\boxed{\Rightarrow}$ Seja $\pi\colon A \to A/M$ a projecção canónica e seja $a \in A$ *t.q.* $\pi(a) \neq 0$. Como $a \notin M$ e M, por hipótese, é maximal, temos

$$1_A \in (a) + M \Rightarrow \exists b \in A : ab - 1_A \in M \Rightarrow \pi(a)\pi(b) = \pi(ab) = \pi(1_A) = 1_{A/M}.$$

□

Corolário 2.3.10. *Seja $M \subset A$ um ideal maximal. Então M é primo.*

Corolário 2.3.11. *A é um corpo* sse *(0) é maximal*

Demonstração. $A/(0) \cong A$. □

Corolário 2.3.12. *A é um corpo* sse *não tem ideais próprios não nulos.*

Demonstração. A não tem ideais próprios não nulos *sse* (0) é maximal. □

Corolário 2.3.13. *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 $\ker f = (0)$ 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 $\ker \pi = (0)$. O resultado segue do corolário anterior.

□

2.3.2 Factorização em anéis comutativos

Definição 2.3.14. *Seja A um anel comutativo e sejam $a, b \in A$. Se $a \neq 0$, 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 2.3.15. *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 2.1.5)* 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 $a \neq 0$ e $b \neq 0$ porque $a \sim b$), então

$$b = bcc' \Rightarrow cc' = 1_A \Rightarrow c, c' \in A^\times.$$

□

Definição 2.3.16. *Seja A um anel comutativo. Diz-se que*

1. *$c \in A - \{0\}$ 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. *$p \in A - \{0\}$ 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 2.3.17. *Um domínio integral D diz-se um* domínio de factorização única (d.f.u.) *se*

(i) $\forall d \in D \setminus (D^\times \cup \{0\})\ \exists c_1, \dots, c_n$ *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. *$c_i \sim c'_{\sigma(i)}$, $i = 1, \dots, n$.*

Exemplos 2.3.18.

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 anel

$$\mathbb{Z}[\sqrt{-5}] := \{m + n\sqrt{-5} \mid m, n \in \mathbb{Z}\}$$

não é um *d.f.u.*, pois

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

são duas factorizações não equivalentes em irredutíveis (Exercício 2.3.21).

Exemplos 2.3.19.

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

$$\underline{2} = \underline{4} \cdot \underline{2} = \underline{8},$$

   mas $\underline{4}, \underline{2} \notin \mathbb{Z}_6^\times$.

Teorema 2.3.20. *Seja D um domínio integral e sejam $a, p, c \in D - \{0\}$.*

1. *p é primo* sse *(p) é primo e $(p) \neq (0)$;*

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 2.3.15, 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

$$\begin{aligned} p = ab &\Rightarrow p = pa'b \\ &\Leftrightarrow p(1 - a'b) = 0 \\ &\Leftrightarrow a'b = 1 \\ &\Rightarrow b \in D^{\times}. \end{aligned}$$

4. $(p) = (a) \Rightarrow (a)$ primo $\neq (0) \Rightarrow a$ primo;

5. $(c) = (a) \Rightarrow (a)$ maximal entre ideais principais;

6. $a \mid c \Leftrightarrow (a) \supset (c)$, logo $(a) = D$ ou $(a) = (c)$.

$\square$

Exercício 2.3.21. *Mesmo num domínio integral, nem sempre os irredutíveis são primos. Considere o subanel $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ definido por*

$$\mathbb{Z}[\sqrt{-5}] \coloneqq \left\{ n + m\sqrt{-5} \mid m, n \in \mathbb{Z} \right\}.$$

Em $\mathbb{Z}[\sqrt{-5}]$ temos,

$$3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

portanto

$$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$$

Mostre que $3 \nmid (2 \pm \sqrt{-5})$ e que 3 é irredutível em $\mathbb{Z}[\sqrt{-5}]$. Conclua que 3 é um elemento irredutível que não é primo.

Exercício 2.3.22. *Determine os elementos primos e os elementos irredutíveis de $\mathbb{Z}_{15}$.*

2.4 12ª Aula

2.4.1 Factorização em domínios integrais

Teorema 2.4.1. *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 2.4.2. *Um domínio integral cujos ideais são principais diz-se um* domínio de ideais principais (*d.i.p.*).

Exemplos 2.4.3. 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 2.4.4. *Seja D um* d.i.p.*, então D é um* d.f.u..

Demonstração. Vejamos que se verificam as duas condições do Teorema 2.4.1.

(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 2.4.1.

$\boxed{\Leftarrow}$ Suponhamos que D satisfaz as condições (a) e (b) do enunciado.

1. Seja $d \in D \setminus (D^\times \cup \{0\})$. 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).

□

2.4.2 Domínios Euclidianos

Definição 2.4.5. *Um anel comutativo A diz-se um* anel euclidiano *se existe* $\varphi\colon A-\{0\}\to\mathbb{N}_0$ t.q.

(i) $ab\neq 0\Rightarrow \varphi(a)\leq\varphi(ab)$*;*

(ii) $a\in A$, $b\in A-\{0\}\Rightarrow\exists q,r\in A$, 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 2.4.6. Com a função $\varphi(n)\coloneqq|n|$, $\mathbb{Z}$ é um domínio euclidiano.

Exemplo 2.4.7. Seja k um corpo. Então $k[x]$ é um domínio euclidiano com $\varphi(f(x))\coloneqq\deg(f(x))$, como veremos mais tarde.

Exercício 2.4.8. *Mostre que* $\mathbb{Z}[i]\coloneqq\{m+n\mathrm{i}\mid m,n\in\mathbb{Z}\}\subset\mathbb{C}$ *é um domínio euclidiano com* $\varphi(m+n\mathrm{i})=m^2+n^2$.

Teorema 2.4.9. *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 ($I=\{0\}$ é principal) e seja $b\in I-\{0\}$ *t.q.*
$$\varphi(b)=\min\{\varphi(a)\mid a\in I-\{0\}\}$$
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 $I=(b)$. $\square$

Definição 2.4.10. *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 2.4.11. O máximo divisor comum pode existir ou não e, se existir, não é em geral único.

Exemplo 2.4.12. 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,

$$(m, n) = \bigcap_{\substack{I \text{ ideal} \\ I \supset (m),(n)}} I = \bigcap_{x|m,\, x|n} (x) = (d). \tag{2.4.1}$$

Em $\mathbb{Z}$, podemos usar a igualdade (2.4.1) para definir o máximo divisor comum. O mesmo pode ser feito num *d.i.p.* arbitrário.

Teorema 2.4.13. *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 $(d) = (d')$. □

2.4.3 Localização

Definição 2.4.14. *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) $1_A \in S$;

(ii) $\forall_{s_1, s_2 \in S} \quad s_1 \cdot s_2 \in S$.

Definição 2.4.15. *Seja A um anel comutativo e seja $S \subset A$ um subconjunto multiplicativo. Consideremos a seguinte relação de equivalência em $A \times S$*

$$(a, s) \sim (a', s') \Leftrightarrow \exists_{s'' \in S} : s''(as' - a's) = 0.$$

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 $\frac{1}{1}$ e o zero é $\frac{0}{1}$.

Exercício 2.4.16. *Nas condições da Definição 2.4.15*

(a) As operações em $S^{-1}A$ estão bem definidas;

(b) $(S^{-1}A, +, \cdot)$ é um anel com identidade $\frac{1}{1}$ e zero $\frac{0}{1}$

Exemplo 2.4.17. Consideremos o subconjunto multiplicativo $S = \mathbb{Z} - \{0\}$ do anel $\mathbb{Z}$. Denotamos por $[n, m]$ a classe de equivalência de $(n, m) \in \mathbb{Z} \times S$. Definimos

$$f\colon S^{-1}\mathbb{Z} \to \mathbb{Q}; [n, m] \mapsto \frac{n}{m}.$$

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

$$f\colon S^{-1}\mathbb{Z} \xrightarrow{\cong} \mathbb{Q}.$$

Definição 2.4.18. *Seja A um anel comutativo e seja $S \subset A$ multiplicativo. O homomorfismo $\varphi_S\colon A \to S^{-1}A$ é definido por*

$$\varphi_S(a) := \frac{a}{1}.$$

Observação 2.4.19. 1. Se $s \in S$, então $\varphi_S(s) = \frac{s}{1}$ tem inverso $\frac{1}{s}$;

2. $\ker \varphi_S = \{a \in A \mid \exists_{s \in S} : as = 0\}$. De facto,

$$\varphi_S(a) = \frac{0}{1} \Leftrightarrow \frac{a}{1} = \frac{0}{1} \Leftrightarrow \exists_{s'' \in S} : s''(a \cdot 1 - 0 \cdot 1) = 0 \Leftrightarrow \exists_{s'' \in S} : a \cdot s'' = 0.$$

3. Se S é tal que $0 \in S$ então $S^{-1}A$ é o anel trivial.

Proposição 2.4.20. *Seja A um domínio integral e seja $S \subset A$ um subconjunto multiplicativo* t.q. $0 \notin S$. *Então $S^{-1}A$ é um domínio integral que contém uma cópia de A (φ_S é injectivo).*

Demonstração.

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{0}{1} \Leftrightarrow \exists_{s \in S} : s(a_1 a_2) = 0 \Leftrightarrow a_1 a_2 = 0 \Leftrightarrow a_1 = 0 \vee a_2 = 0$$
$$\Rightarrow \frac{a_1}{s_1} = \frac{0}{1} \vee \frac{a_2}{s_2} = \frac{0}{1} \ .$$

□

Exemplo 2.4.21. $\varphi_{\mathbb{Z}-\{0\}} : \mathbb{Z} \to (\mathbb{Z}-\{0\})^{-1}\mathbb{Z} \cong \mathbb{Q}$ é um monomorfismo.

Teorema 2.4.22. *Seja A um domínio integral e seja $S = A - \{0\}$. Então* $\mathrm{Frac}(A) := S^{-1}A$ *é um corpo.*

Demonstração. S é um conjunto multiplicativo pois A não contém divisores de zero. Além disso, temos:

$$\frac{a}{s} \neq \frac{0}{1} \Leftrightarrow a \in S \Rightarrow \frac{a}{s} \cdot \frac{s}{a} = \frac{1}{1}. \qquad \square$$

Definição 2.4.23. *Nas condições do Teorema 2.4.22, diz-se que* $\mathrm{Frac}(A)$ *é o corpo de fracções de A.*

Exemplo 2.4.24. Seja $A = \mathbb{R}[x]$ e $S = \mathbb{R}[x] - \{0\}$. Temos,

$$\mathrm{Frac}(\mathbb{R}[x]) = \mathbb{R}(x) := \left\{ \frac{p(x)}{q(x)} \mid p(x), q(x) \in \mathbb{R}[x], q(x) \neq 0 \right\}.$$

2.5 13ª Aula

2.5.1 Ideais de $S^{-1}A$:

Seja $I \subset A$ um ideal, define-se

$$S^{-1}I := \left\{ \frac{a}{s} \in S^{-1}A \mid a \in I \right\} \subset S^{-1}A.$$

Exercício 2.5.1. *Mostre que $S^{-1}I \subset S^{-1}A$ é um ideal.*

Obtemos assim correspondências entre ideais de A e de $S^{-1}A$ dadas por:

$$\begin{aligned} A \supset I &\mapsto S^{-1}I \subset S^{-1}A \\ \varphi_S^{-1}(J) &\leftarrow\!\shortmid J \subset S^{-1}A. \end{aligned}$$

Exercício 2.5.2. *Sejam $I, J \subset A$ ideais. Mostre que*

(a) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$;

(b) $S^{-1}(IJ) = S^{-1}I \cdot S^{-1}J$;

(c) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.

Exercício 2.5.3. *Seja A um anel comutativo de seja $S \subset A$ um subconjunto multiplicativo. Mostre que dado um ideal $K \subset S^{-1}A$ existe um ideal $I \subset A$* t.q. *$K = S^{-1}I$.*

O exercício seguinte mostra que quando restringidas a certos ideais estas correspondências são bijectivas. Em geral isto não se passa (*cf.* Exemplo 2.5.7).

Exercício 2.5.4. *Nas condições do exercício anterior. Mostre que as correspondências $I \mapsto S^{-1}I$ e $K \mapsto \varphi_S^{-1}(K)$ estabelece um 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 2.5.5. Seja A um anel comutativo e seja $P \subset A$ um ideal primo. Então $S = A \setminus P$ é multiplicativo, pois $1_A \in S$

$$a, b \in S \Rightarrow ab \in S,$$

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 2.5.6. *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 2.5.7. Seja $A = \mathbb{Z}$ e $P = (p)$, com $p \in \mathbb{N}$ primo. Temos
$$\mathbb{Z}_{(p)} := A_P = \left\{\frac{r}{s} \in \mathbb{Q} \mid r, s \in \mathbb{Z}, p \nmid s\right\} \subset \mathbb{Q}.$$
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 2.5.8. 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 2.5.9. *Um anel comutativo A diz-se um* anel local *se contém um único ideal maximal.*

Pela obervação anterior, a localizaccão A_P de A num ideal primo $P \subset A$ é um anel local.

Proposição 2.5.10. *Um anel comutativo A é local se e só se $A \setminus A^\times$ é um ideal.*

Demonstração. Exercício. $\square$

2.5.2 Anéis de polinómios

Exemplo 2.5.11. $\mathbb{R}[x]$ 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

$$\begin{aligned} f(x) + g(x) &= c_r x^r + \cdots + c_0 \\ &\Rightarrow \boxed{c_k = a_k + b_k} \end{aligned} \tag{2.5.1}$$

$$\begin{aligned} f(x) \cdot g(x) &= d_s x^s + \cdots + d_0 \\ &\Rightarrow \boxed{d_k = \sum_{i+j=k} a_i b_j} \end{aligned} \tag{2.5.2}$$

De seguida pretendemos definir polinómios com coeficientes num anel arbitrário.

Exemplo 2.5.12. 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 2.5.13. *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:

$$(a+b)(n) \coloneqq a(n) + b(n) \tag{2.5.3}$$

$$(a \cdot b)(n) \coloneqq \sum_{i+j=n} a(i)b(j) \tag{2.5.4}$$

Notação 2.5.14. 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 2.5.15.

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.* $a(n) \in C(A)$, $\forall n \in \mathbb{N}_0$, segue que $a \in C(A[x])$.

Proposição 2.5.16. *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

$$f(x) + g(x) = \sum_{i=0}^{n+m} (a_i + b_i) x^i \tag{2.5.5}$$

$$f(x)g(x) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_i b_{i-j} \right) x^i. \tag{2.5.6}$$

Com esta estrutura $A[x]$ é um anel t.q. $x \in C(A[x])$. *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 2.5.17. $\mathbb{Z}_2[x]$ é um anel comutativo com caraterística 2 e $|\mathbb{Z}_2[x]| = |\mathbb{N}|$.

Definição 2.5.18 (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*

$$\mathrm{eval}_c \left(\sum_{i=0}^{n} a_i x^i \right) \coloneqq \sum_{i=0}^{n} a_i c^i \in A.$$

Exercício 2.5.19. *Mostre que* eval_c *é um homomorfismo de anéis.*

Notação 2.5.20. Dado $f(x) \in A[x]$ é habitual usar $f(c)$ para denotar $\mathrm{eval}_c(f(x))$.

Exemplo 2.5.21. 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 2.5.22. *Consideremos o conjunto*

$$A[x_1, \ldots, x_n] := \{a\colon \mathbb{N}_0^n \to A \mid \exists N : k_i > N, i = 1, \ldots, n \Rightarrow a(k_1, \ldots, k_n) = 0\}.$$

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*

$$\begin{aligned}(a + b)(K) &= a(K) + b(K)\\ (ab)(K) &= \sum_{I+J=K} a(I)b(J).\end{aligned}$$

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 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:

$$f(x_1, \ldots, x_n) = \sum_{0 \leq i_1,\ldots,i_n \leq N} a_{i_1\cdots i_n} x_1^{i_1} \cdots x_n^{i_n}. \tag{2.5.7}$$

Notação 2.5.23. Dado $I = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ denotamos $x^I := x_1^{i_1} \cdots x_n^{i_n}$.

Com esta notação a fórmula (2.5.7) escreve-se na seguinte forma:

$$f(x_1, \ldots, x_n) = \sum_{I \in \mathbb{N}_0^n} a_I x^I.$$

Observação 2.5.24. $x_i \in C\left(A[x_1, \ldots, x_n]\right)$.

Exemplo 2.5.25. Seja $f(x, y) = \underline{1} + xy$, $g(x, y) = x + y$ elementos de $\mathbb{Z}_2[x, y]$. Temos

$$f(x, y)g(x, y) = (\underline{1} + xy)(x + y) = x + y + x^2y + xy^2.$$

Homomorfismos a partir de anéis de polinómios:

Sejam A e B anéis comutativos. Recorde-se que $A \subset A[x_1, \dots, x_n]$, portanto dado um homomorfismo $\varphi\colon A[x_1, \dots, x_n] \to B$, obtemos um homomorfismo por restrição $f \coloneqq \varphi|_A\colon A \to B$. Seja $b_i = \varphi(x_i)$, $i = 1, \dots, n$. Então φ é determinado por f e por $b_1, \dots, b_n$:

$$\begin{aligned}\varphi\left(\sum_I a_I x^I\right) &= \sum_I \varphi(a_I x^I) = \sum_I \varphi(a_I)\varphi(x^I)\\ &= \sum_I f(a_I)\varphi(x_1^{i_1} \cdots x_n^{i_n}) = \sum_I f(a_I)\varphi(x_1)^{i_1} \cdots \varphi(x_n)^{i_n}\\ &= \sum_I f(a_I) b_1^{i_1} \cdots b_n^{i_n} \end{aligned} \tag{2.5.8}$$

Proposição 2.5.26. *Dar um homomorfismo $\varphi\colon A[x_1, \dots, x_n] \to B$ é equivalente a dar um homomorfismo $f\colon A \to B$ e n elementos $b_1, \dots, b_n \in B$. O homorfismo φ determinado por f, $b_1, \dots, b_n \in B$ é dado por* (2.5.8)*.*

Para o caso em que A ou B não é comutativo, ver exercícios.

Observação 2.5.27. O anel $A[x_1, \dots, x_n]$ 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 $C \cong A[x_1, \dots, x_n]$.

Proposição 2.5.28. $A[x_1, \dots, x_{n+k}] \cong (A[x_1, \dots, x_n])\,[x_{n+1}, \dots, x_{n+k}]$.

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 2.5.29. 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

$$\varphi(f(x, y)) = \left(3x^2\right) y + (5x + 1) \cdot 1 \in \mathbb{Z}[x][y].$$

2.6 14ª Aula

2.6.1 Séries formais

Definição 2.6.1. *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:

$$(a+b)(n) \coloneqq a(n) + b(n) \tag{2.6.1}$$

$$(a\cdot b)(n) \coloneqq \sum_{i+j=n} a(i)b(j) \tag{2.6.2}$$

$A[[x]]$ diz-se o anel das séries formais de coeficientes em A.

Observação 2.6.2. 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 2.6.3. 1. x designa o elemento de $A[[x]]$ cujo valor em $n \in \mathbb{N}_0$ é

$$x(n) \coloneqq \begin{cases} 1, & n = 1 \\ 0, & n \neq 1 \end{cases}$$

2. $\sum_{n=0}^{\infty} a_n x^n$ denota o elemento de $A[[x]]$ correspondente à sucessão $(a_n)_{n\in\mathbb{N}_0}$.

Observação 2.6.4. 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 2.6.5. *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:

$$\begin{aligned} b_0 a_0 = 1 &\Leftrightarrow b_0 = a_0^{-1} \\ b_1 a_0 + b_0 a_1 = 0 &\Leftrightarrow b_1 = -b_0 a_1 a_0^{-1} = -a_0 a_1 a_0^{-1} \\ &\vdots \\ b_n a_0 + \cdots + b_0 a_n = 0 &\Leftrightarrow b_n = -\left(b_{n-1} a_1 + \cdots + b_0 a_n\right) a_0^{-1}. \end{aligned}$$

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 2.6.6. 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,

$$(1-x)\sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} x^n - \sum_{n=0}^{\infty} x^{n+1} = \sum_{n=0}^{\infty} x^n - \sum_{n=1}^{\infty} x^n = 1.$$

Exemplo 2.6.7. Se k é um corpo, então $k[[x]]$ é um anel local.

2.6.2 Factorização em anéis de polinómios

Definição 2.6.8. *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 2.6.9 (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)
$$\begin{array}{lcl} c_k b_n & = & a_m \\ c_{k-1} b_n + c_k b_{n-1} & = & a_{m-1} \\ & \vdots & \\ c_0 b_n + c_1 b_{n-1} + \cdots + c_k b_{n-k} & = & a_{m-k} = a_n \end{array} \tag{2.6.3}$$

(iii) $r = f - qg$.

O sistema (2.6.3) 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 2.6.10. *Se k é um corpo, então $k[x]$ é um domínio euclidiano com $\varphi\colon A[x] - \{0\} \to \mathbb{N}_0; f \mapsto \deg f$. Em particular, $k[x]$ é um* d.i.p. *(e portanto um* d.f.u.*).*

Definição 2.6.11. *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 2.6.12. *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 2.6.13. *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 $q_m(x) \in D[x] - \{0\}$, logo $m \leq n = \deg f$. □

Exemplos 2.6.14. 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 2.6.15. 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

$$(x - c)(x - \bar{c}) = (x^2 - 2\,\mathrm{Re}(c)x + |c|^2) \mid f(x) \quad \text{em } \mathbb{R}[x],$$

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.

Factorização em $\mathbb{Z}[x]$

Lema 2.6.16. *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 $\mathbb{Z}[x]$. $\square$

Proposição 2.6.17 (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

$$\begin{array}{rcll} a_1 & = & b_0c_1 + b_1c_0 & \Rightarrow p \mid b_1 \\ a_2 & = & b_0c_2 + b_1c_1 + b_2c_0 & \Rightarrow p \mid b_2 \\ & \vdots & & \\ a_r & = & b_0c_r + \cdots + b_rc_0 & \Rightarrow p \mid b_r \Rightarrow p \mid a_m. \quad \text{Contradição!} \end{array}$$

$\square$

Exemplo 2.6.18. 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
$$\begin{aligned} f(x+1) &= \frac{1}{x+1-1}((x+1)^p - 1) \\ &= \frac{1}{x}\sum_{k=1}^{p}\binom{p}{k}x^k \\ &= \sum_{k=1}^{p}\binom{p}{k}x^{k-1} \\ &= x^{p-1} + px^{p-2} + \cdots + p. \end{aligned}$$
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.

Factorização em $D[x]$ para um domínio integral D:

O Lemma 2.6.16 e a Proposição 2.6.17 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 2.6.19. *Seja D um* d.f.u.*, então $D[x]$ é um* d.f.u..

Corolário 2.6.20. *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
$$D[x_1, \ldots, x_n] \cong D[x_1, \ldots, x_{n-1}][x_n].$$
□

Capítulo 3

Categorias

3.1 15ª Aula

3.1.1 Definição e exemplos

Definição 3.1.1. *Uma categoria é uma classe* $\mathcal{C}$ *munida de*

(a) conjuntos disjuntos $\hom_{\mathcal{C}}(X,Y)$, $\forall\, X,Y \in \mathcal{C}$*;*

(b) uma operação

$$\forall\, X,Y,Z \in \mathcal{C}, \quad \hom_{\mathcal{C}}(Y,Z) \times \hom_{\mathcal{C}}(X,Y) \xrightarrow{\circ} \hom_{\mathcal{C}}(X,Z)$$

t.q.

1. $\forall\, f \in \hom_{\mathcal{C}}(Z,W)$, $g \in \hom_{\mathcal{C}}(Y,Z)$, $h \in \hom_{\mathcal{C}}(X,Y)$

$$(f \circ g) \circ h = f \circ (g \circ h);$$

2. $\forall\, X \in \mathcal{C} \exists\, \mathrm{id}_X \in \hom_{\mathcal{C}}(X,X)$:

$$f \circ \mathrm{id}_X = f, \quad \forall\, f \in \hom_{\mathcal{C}}(X,Y)$$
$$\mathrm{id}_X \circ g = g, \quad \forall\, g \in \hom_{\mathcal{C}}(Y,X)$$

Notação 3.1.2. Os elementos de $\mathcal{C}$ dizem-se *objectos* de $\mathcal{C}$. Os elementos de $\hom_{\mathcal{C}}(X,Y)$ dizem-se *morfismos* de X em Y. Também se usam as notações $\hom(X,Y)$ 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 $\hom_{\mathcal{C}}$.

Exemplo 3.1.3. 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 3.1.4. Como o exemplo anterior mostra, em geral, a classe dos objectos de uma categoria não é um conjunto.

Exemplo 3.1.5. A classe dos grupos e homomorfismos de grupos com a operação de composição é uma categoria Grp - a *categoria dos grupos*.

Exemplo 3.1.6. A classe dos anéis (com identidade) e homomorfismos de anéis que preservam a identidade é uma categoria Ring.

Exemplo 3.1.7. Seja G um grupo. A classe dos conjuntos-G com as funções equivariantes é uma categoria Set_G.

Exemplo 3.1.8. Seja k um corpo. A classe dos espaços vectoriais sobre k com as transformações lineares-k é uma categoria Vect_k.

Observação 3.1.9. 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 3.1.10. Seja G um grupo. Definimos $\mathcal{C}_G$ como a categoria que tem um só elemento, G, com morfismos $\hom_{\mathcal{C}_G}(G, G) = G$ e com a composição dada por multiplicação em G.

Exemplo 3.1.11. Seja $(X, \leq)$ um conjunto parcialmente ordenado. Então $(X, \leq)$ determina uma categoria cujos objectos são os elementos de X e *t.q.*, para $x, y \in X$, $\hom(x, y)$ tem um elemento se $x \leq y$ e $\hom(x, y) = \varnothing$, caso contrário.

Observação 3.1.12. Como este exemplo ilustra, se $X \neq Y$, pode ter-se $\hom_{\mathcal{C}}(X, Y) = \varnothing$.

Exemplo 3.1.13. 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

$$\hom_{\mathcal{C}^{op}}(X, Y) := \hom_{\mathcal{C}}(Y, X),$$

e cuja composição é dada por

$$f \circ_{\mathcal{C}^{op}} g \coloneqq g \circ_{\mathcal{C}} f,$$

onde $g \in \hom_{\mathcal{C}^{op}}(X, Y)$ e $f \in \hom_{\mathcal{C}^{op}}(Y, Z)$. Diz-se que $\mathcal{C}^{op}$ é a *categoria oposta* de $\mathcal{C}$.

Definição 3.1.14. *Sejam X, Y objectos de uma categoria $\mathcal{C}$. Se existem $f \in \hom_{\mathcal{C}}(X, Y)$, $g \in \hom_{\mathcal{C}}(Y, X)$* 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 3.1.15.

1. Em $\mathrm{Grp}, \mathrm{Ring}, \mathrm{Vect}_k$ os isomorfismos coincidem com as definições dadas anteriormente (exercício).

2. Em $\mathcal{C}_G$ todos os morfismos são isomorfismos.

Definição 3.1.16. *Seja $\mathcal{C}$ uma categoria e sejam $X, Y \in \mathcal{C}$. Diz-se que $f \in \hom_{\mathcal{C}}(X, Y)$ é* mónico *se*

$$\forall_{Z \in \mathcal{C}} \forall_{g, g' \in \hom_{\mathcal{C}}(Z, X)} \quad f \circ g = f \circ g' \Rightarrow g = g'.$$

Diz-se que f é epi *se*

$$\forall_{Z \in \mathcal{C}} \forall_{h, h' \in \hom_{\mathcal{C}}(Y, Z)} \quad h \circ f = h' \circ f \Rightarrow h = h'.$$

Exemplos 3.1.17. Em Set, Grp, 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 3.1.18. Seja Top a categoria dos espaços topológicos com as aplicações contínuas como morfismos. Se $X, Y \in \mathrm{Top}$ e $f \in \hom_{\mathrm{Top}}(X, Y)$, então f é epi *sse* $\operatorname{im} f$ é denso em Y.

3.1.2 Produtos e coprodutos

Definição 3.1.19. *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 $P \in \mathcal{C}$ com morfismos $\pi_i \in \hom_{\mathcal{C}}(P, A_i)$, $i \in I$,* t.q. *dado $B \in \mathcal{C}$ e morfismos $\varphi_i \in \hom_{\mathcal{C}}(B, A_i)$,*

$i \in I$, existe um único morfismo $\varphi \in \hom_{\mathcal{C}}(B, P)$ que, para cada $i \in I$, faz comutar o diagrama

$$\begin{tikzcd} & P \arrow[d, "\pi_i"] \\ B \arrow[ur, dashed, "\exists!\varphi"] \arrow[r, "\varphi_i"'] & A_i. \end{tikzcd}$$

Exemplo 3.1.20. Em Set o produto é o produto cartesiano.

Exemplo 3.1.21. 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 3.1.22. 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 3.1.23. 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 $\mathbb{F}_p := \mathbb{Z}_p$ e $\mathbb{Q}$.

Teorema 3.1.24. *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 $\pi_i \in \hom_{\mathcal{C}}(P, A_i)$, $\varrho_i \in \hom_{\mathcal{C}}(Q, A_i)$, $i \in I$, os morfismos de estrutura dos dois produtos. Do facto de P, Q serem produtos em $\mathcal{C}$, obtemos

$$f \in \hom_{\mathcal{C}}(P, Q), \quad g \in \hom_{\mathcal{C}}(Q, P)$$

t.q.

$$\varrho_i \circ f = \pi_i, \quad \pi_i \circ g = \varrho_i,$$

logo $g \circ f \in \hom_{\mathcal{C}}(P, P)$ 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 3.1.25. *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 $\iota_j \in \hom_{\mathcal{C}}(A_j, S)$, $j \in I$,* t.q., *dado $B \in \mathcal{C}$, e morfismos $\psi_j \in \hom_{\mathcal{C}}(A_j, B)$ existe um único morfismo $\psi \in \hom_{\mathcal{C}}(S, B)$ que faz comutar, para cada $j \in I$, o diagrama*

$$\begin{tikzcd} A_j \arrow[r, "\psi_j"] \arrow[d, "\iota_j"'] & B \\ S \arrow[ur, dashed, "\exists!\psi"'] & \end{tikzcd}$$

Exercício 3.1.26. *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 $\mathcal{C}^{op}$.*

Teorema 3.1.27. *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 $S \cong S'$.*

Demonstração. Exercício. □

Notação 3.1.28. Denotamos por $\coprod_{j\in I} A_j$ o coproduto de $\{A_j \mid j \in I\}$, quando este existe.

Exemplo 3.1.29. 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 $\psi_i \in \hom_{\mathrm{Ab}}(A_i, B)$, 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 $\psi \in \hom_{\mathrm{Ab}}\left(\oplus_{i\in I}, B\right)$ e, por construção

$$\psi \circ \iota_j = \psi_j.$$

3.2 16ª Aula

3.2.1 Objectos universais

Definição 3.2.1. *Um objecto I numa categoria $\mathcal{C}$ diz-se* inicial *se*

$$\forall\, C \in \mathcal{C}\ |\hom_{\mathcal{C}}(I, C)| = 1.$$

Um objecto $T \in \mathcal{C}$ diz-se terminal *se*

$$\forall\, C \in \mathcal{C}\ |\hom_{\mathcal{C}}(C, T)| = 1.$$

Exemplo 3.2.2. Em Set, $\varnothing$ é um objecto inicial. Se X é um conjunto *t.q.* $|X| = 1$, então $X \in$ Set é um objecto terminal.

Exercício 3.2.3. *Um objecto $T \in \mathcal{C}$ é terminal* sse *$T \in \mathcal{C}^{op}$ é inicial.*

Exemplo 3.2.4. O grupo trivial $\langle 1 \rangle$ é um objecto final e inicial na categoria Grp.

Exemplo 3.2.5. Na categoria Ring, o anel trivial $\{0\}$ é um objecto terminal e $\mathbb{Z}$ é um objecto inicial.

Exemplo 3.2.6. Na categoria Field não há objectos iniciais nem terminais, pois

$$\hom_{\text{Field}}(F_1, F_2) \neq \varnothing \Rightarrow \operatorname{car} F_1 = \operatorname{car} F_2.$$

Teorema 3.2.7. *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 3.2.8. 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 $p_i \in \hom_{\mathcal{C}}(B, A_i)$. 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

$$\begin{tikzcd} B \arrow[rr, "f"] \arrow[dr, "p_i"'] & & B' \arrow[dl, "p_i'"] \\ & A_i & \end{tikzcd}$$

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 $(B, \{p_i\}) \in \mathcal{D}$ e dar $f \colon B \to P$ fazendo comutar, para $i = 1, 2$,

$$\begin{tikzcd} B \arrow[rr, "f"] \arrow[dr, "p_i"'] & & P \arrow[dl, "\pi_i"] \\ & A_i & \end{tikzcd}$$

é equivalente a dar um morfismo $(B, \{p_i\}) \to (P, \{\pi_i\})$ em $\mathcal{D}$.

Exercício 3.2.9. *Defina uma categoria onde os objectos iniciais de uma categoria $\mathcal{C}$ correspondem aos coprodutos de $\mathcal{C}$.*

Observação 3.2.10. O Exemplo 3.2.8 e o Exercício 3.2.9 podem ser generalizados para o caso de uma família arbitrária de objectos $\{A_i \mid i \in I\}$ em $\mathcal{C}$.

3.2.2 Functores

Frequentemente estudam-se relações entre várias categorias. Para esse efeito existe uma noção de morfismo entre categorias.

Definição 3.2.11. *Um* functor (covariante) *entre duas categorias, $\mathcal{C}$, $\mathcal{D}$, é um par de funções (denotadas pelo mesmo símbolo) $T \colon \mathcal{C} \to \mathcal{D}$ e $T \colon \hom_{\mathcal{C}} \to \hom_{\mathcal{D}}$* t.q.

1. $f \in \hom_{\mathcal{C}}(X, Y) \Rightarrow T(f) \in \hom_{\mathcal{D}}(TX, TY)$;

2. $T(\mathrm{id}_X) = \mathrm{id}_{TX}$;

3. $T(f \circ g) = T(f) \circ T(g)$.

Definição 3.2.12. *Substituindo na Definição 3.2.11 as condições 1. e 3. por*

1'. $f \in \hom_{\mathcal{C}}(X, Y) \Rightarrow T(f) \in \hom_{\mathcal{D}}(TY, TX)$;

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 3.2.13. Utilizamos $T\colon \mathcal{C} \to \mathcal{D}$ para denotar que T é um functor covariante de $\mathcal{C}$ em $\mathcal{D}$.

Exercício 3.2.14. *Sejam $\mathcal{C}$, $\mathcal{D}$ categorias. Mostre que dar um functor contravariante de $\mathcal{C}$ em $\mathcal{D}$ é equivalente a dar um functor covariante $T\colon \mathcal{C}^{op} \to \mathcal{D}^{op}$.*

Exemplo 3.2.15. A função $T\colon$ Grp $\to$ 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 3.2.16. Da mesma forma, existem functores de esquecimento Ring $\to$ Set, Field $\to$ Set, $\mathrm{Set}_G \to$ Set.

Exemplo 3.2.17. Sejam G e H grupos e $f : G \to H$ um homofismo de grupos. Então C : Grp $\to$ Grp definido por $G \mapsto [G, G]$ e $f \mapsto f|_{[G,G]}$ é um functor, pois $f([G, G]) \subset [H, H]$. Passando ao quociente pelo grupo comutador, obtém-se um outro functor Q : Grp $\to$ Grp dado por $G \mapsto G/[G, G]$ e $Q(f) : G/[G, G] \to H/[H, H]$ é o homomorfismo de grupos induzido por f.

Exercício 3.2.18. *Mostre que não existe nenhum functor* Grp $\to$ Ab *tal que a cada grupo G faz corresponder o seu centro $C(G)$.*

Exemplo 3.2.19. 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 3.2.20. 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 3.2.21. As funções

$$\mathrm{Vect}_k \ni V \longmapsto V^\star := \hom_{\mathrm{Vect}_k}(V, k)$$

$$\hom_{\mathrm{Vect}_k}(V, W) \ni f \longmapsto f^\star\colon W^\star \to V^\star; \varphi \mapsto \varphi \circ f$$

definem um functor contravariante $\mathrm{Vect}_k \to \mathrm{Vect}_k$.

Definição 3.2.22. *Seja $\mathcal{C}$ uma categoria. Uma* subcategoria *de $\mathcal{C}$ é uma subclasse de objectos $\mathcal{C}' \subset \mathcal{C}$ munida de subconjuntos* $\hom_{\mathcal{C}'}(X, Y) \subset \hom_{\mathcal{C}}(X, Y)$*,* $\forall X, Y \in \mathcal{C}'$*,* t.q. $(\mathcal{C}', \hom_{\mathcal{C}'})$ *é uma categoria (com a operação de composição de $\mathcal{C}$).*

Exemplo 3.2.23. Os grupos abelianos e homomorfismos de grupos abelianos formam uma subcategoria de Grp denotada Ab.

Exemplo 3.2.24. 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 3.2.25. Se $\mathcal{C}' \subset \mathcal{C}$ é uma subcategoria, as inclusões $\mathrm{Ob}_{\mathcal{C}'} \subset \mathrm{Ob}_{\mathcal{C}}$ e $\hom_{\mathcal{C}'} \subset \hom_{\mathcal{C}}$ definem um functor $i\colon \mathcal{C}' \to \mathcal{C}$.

Definição 3.2.26. *Sejam $\mathcal{C}, \mathcal{D}$ categorias e seja $T\colon \mathcal{C} \to \mathcal{D}$ um functor. Então,*

1. *se*
$$\forall_{X,Y\in\mathcal{C}}\,\forall_{f,f'\,\hom_{\mathcal{C}}(X,Y)} \quad T(f) = T(f') \Rightarrow f = f'.$$
diz-se que T é fiel*;*

2. *se*
$$\forall_{X,Y\in\mathcal{C}}\,\forall_{g\in\hom_{\mathcal{D}}(TX,TY)}\,\exists_{f\in\hom_{\mathcal{C}}(X,Y)} : T(f) = g.$$
diz-se que T é pleno*.*

Observação 3.2.27. Um functor $T\colon \mathcal{C} \to \mathcal{D}$ é fiel *sse*

$$\forall_{X,Y\in\mathcal{C}} \quad T\colon\ \hom_{\mathcal{C}}(X,Y) \to \hom_{\mathcal{D}}(TX,TY)$$

é injectivo; e é pleno *sse*

$$\forall_{X,Y\in\mathcal{C}} \quad T\colon\ \hom_{\mathcal{C}}(X,Y) \to \hom_{\mathcal{D}}(TX,TY)$$

é sobrejectivo.

Exemplo 3.2.28. O functor de inclusão $T\colon$ Ab $\to$ Grp é fiel e pleno, pois

$$\forall\, G, H \in \mathrm{Ab} \quad \hom_{\mathrm{Grp}}(G,H) = \hom_{\mathrm{Ab}}(G,H).$$

Exemplo 3.2.29. O functor de esquecimento $E\colon \mathrm{Grp} \to \mathrm{Set}$ é fiel mas não é pleno, pois, em geral,

$$\hom_{\mathrm{Grp}}(G,H) \subsetneq \{f\colon G \to H\} = \hom_{\mathrm{Set}}(G,H).$$

Definição 3.2.30. *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 3.2.31. 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 3.2.32. 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.

3.2.3 Transformações naturais

Definição 3.2.33. *Dados dois functores $S, T : \mathcal{C} \to \mathcal{D}$, uma* transformação natural *$\alpha : S \to S$ é uma função $\alpha : \mathrm{Ob}_{\mathcal{C}} \to \hom_{\mathcal{D}}$ (denotada pela mesma letra) que a cada objecto $C \in \mathrm{Ob}_{\mathcal{C}}$ faz corresponder um morfismo $\alpha_C \in \hom_{\mathcal{D}}(S(C), T(C))$ tal que $\forall\, A, B \in \mathrm{Ob}_{\mathcal{C}}$ e $\forall\, f \in \hom_{\mathcal{C}}(A,B)$ o seguinte diagrama comuta*

$$\begin{tikzcd} A \arrow[d, "f"'] \\ B \end{tikzcd} \qquad \begin{tikzcd} S(A) \arrow[r, "\alpha_A"] \arrow[d, "S(f)"'] & T(B) \arrow[d, "T(f)"] \\ S(B) \arrow[r, "\alpha_B"'] & T(B) \end{tikzcd}$$

Ou seja, uma tranformação natural pode ser vista como um morfismo entre functores.

Exemplo 3.2.34. 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 *sse* $\det_A(M) \in A^\times$ e $\det_A(MN) = \det_A(M)\det_A(N)$, o determinante define um homomorfismos de grupos (multiplicativos) $\det_A : \mathrm{GL}_n(A) \to A^\times$. Além disso, como a fórmula para calcular o determinante é a "mesma" independentemente do anel A, temos que

$$\begin{tikzcd}
\mathrm{GL}_n(A) \arrow[r, "\det_A"] \arrow[d, "\mathrm{GL}_n(f)"'] & A^\times \arrow[d, "f^\times := f|_{A^\times}"] \\
\mathrm{GL}_n(B) \arrow[r, "\det_B"'] & B^\times
\end{tikzcd}$$

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.)

Exercício 3.2.35. *Mostre que as projeccões 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"* $Q : \mathrm{Grp} \to \mathrm{Grp}$, *definido no Exemplo 3.2.17*

Capítulo 4

Módulos

4.1 17ª Aula

4.1.1 Definição exemplos

Definição 4.1.1. *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 4.1.2. 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 4.1.3. 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 4.1.4.

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 4.1.5. 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 $A \times A^n \to A^n$:
$$a \cdot (a_1, \dots, a_n) := (aa_1, \dots, aa_n).$$

(d) Seja $(G, +)$ um grupo abeliano. Então G é um módulo-$\mathbb{Z}$: dado $n \in \mathbb{N}$, define-se
$$\begin{aligned} n \cdot g &:= \overbrace{g + \cdots + g}^{n\text{-vezes}} \\ (-n) \cdot g &:= \underbrace{(-g) + \cdots + (-g)}_{n\text{-vezes}} \end{aligned}$$

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 4.1.1, 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 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 4.1.6. *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. (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) $(-a) \cdot \mathbf{v} + a \cdot \mathbf{v} = (-a + a) \cdot \mathbf{v} = 0_A \cdot \mathbf{v} = 0_M \Rightarrow (-a) \cdot \mathbf{v} = -a \cdot \mathbf{v}$.

□

4.1.2 Homomorfismos e quocientes

Definição 4.1.7. *Sejam M, N módulos-A. Um* homomorfismo de módulos-A *é um homomorfismos de grupos abelianos $f : M \to N$ que é linear-A,* i.e.,

$$\forall a \in A, \forall \mathbf{v} \in M \quad f(a\mathbf{v}) = af(\mathbf{v}).$$

Um submódulo *de M é um módulo-A, $M' \subset M$,* t.q. *a inclusão $i : M' \to M$ é um homomorfismo de módulos-A.*

Notação 4.1.8. Os homomorfismos de módulos-A também se dizem transformações lineares-A. O conjunto das transformações lineares-A de M em N é denotado $\hom_A(M, N)$.

Definição 4.1.9. *A classe dos módulos sobre um anel A e respectivos homomorfismos é uma categoria denotada* Mod_A.

Exercício 4.1.10. *Na categoria* Mod_A *temos as noções de isomorfismo, epimorfismo e monomorfismo – ver Definições 3.1.14 e 3.1.16. Dado $f \in \hom_A(M, N)$, mostre que:*

(a) f é um isomorfismo sse *f é bijectivo;*

(b) f é um monomorfismo sse *f é injectivo;*

(c) f é um epimorfismo sse *f é sobrejectivo.*

Exemplos 4.1.11.

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

$$\ker f \subset M \quad \text{e} \quad \operatorname{im} f \subset N$$

são submódulos-A.

Observação 4.1.12. 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 4.1.13. *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 4.1.14. 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.

Definição 4.1.15. *Seja $f\colon M \to N$ um homomorfismo de módulos-A. Define-se*

$$\operatorname{coker} f \coloneqq \frac{N}{\operatorname{im} f} \ .$$

Proposição 4.1.16. *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 $\varphi \in \hom_A(M, M')$* t.q. *$N \subset \ker\varphi$, existe um único $\bar\varphi \in \hom_A(M/N, M')$* t.q.

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\pi"'] & M' \\ M/N \arrow[ur, dashed, "\exists!\bar\varphi"'] & \end{tikzcd}$$

Temos $\operatorname{im}\bar\varphi = \operatorname{im}\varphi$ *e* $\ker\bar\varphi = \pi(\ker\varphi)$.

Demonstração. Segue do resultado análogo para grupos abelianos, notando que $\bar\varphi$ é linear-A:

$$\bar\varphi(a\pi(\mathbf{v})) = \bar\varphi(\pi(a\mathbf{v})) = \varphi(a\mathbf{v}) = a\varphi(\mathbf{v}) = a\bar\varphi(\pi(\mathbf{v})) \ . \qquad \square$$

Observação 4.1.17. Tal como no caso dos homomorfismos de grupos abelianos, um morfismo φ de módulos-A é injectivo *sse* $\ker\varphi = \{0\}$.

Teorema 4.1.18 (Teoremas de Isomorfismo)**.** *Sejam M, N módulos-A. Então,*

(a) dado $\varphi \in \hom_A(M, N)$, tem-se

$$M/\ker\varphi \cong \operatorname{im}\varphi;$$

(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

$$\frac{M/N_2}{N_1/N_2} \cong \frac{M}{N_1}.$$

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 4.1.19. 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 4.1.20. *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 4.1.21. $\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle \coloneqq \langle \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \rangle$.

Exemplo 4.1.22. Seja M um módulo-A e sejam $\mathbf{v}_1, \ldots, \mathbf{v}_n \in M$. Então

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle = \left\{ \sum_{i=1}^{n} a_i \mathbf{v}_i \mid a_i \in A \right\}.$$

Definição 4.1.23. *Um módulo-A que é gerado por um elemento diz-se um módulo* cíclico*.*

Exemplo 4.1.24. Seja $I \subset A$ um ideal esquerdo e seja $\pi\colon A \to A/I$ a projecção canónica. Então A/I é cíclico, pois $A/I = \langle 1_{A/I} \rangle$.

Exercício 4.1.25. *Seja M um módulo-A cíclico. Mostre que existe um ideal esquerdo $I \subset A$* t.q. *$M \cong A/I$.*

Exemplo 4.1.26. 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

$$\langle S \rangle = \left\{ \sum_{j\in J} \mathbf{v}_j \mid J \subset I : |J| < \infty, \mathbf{v}_j \in N_j \right\}.$$

4.1.3 Produto directo e soma directa

Definição 4.1.27. *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*

$$\forall_{a\in A}, \forall_{(\mathbf{v}_i)_{i\in I} \in \prod_{i\in I} M_i} \quad a(\mathbf{v}_i)_{i\in I} \coloneqq (a\mathbf{v}_i)_{i\in I}; \tag{4.1.1}$$

(b) a soma directa *$\bigoplus_{i\in I} M_i$ como a soma directa de grupos abelianos munida da operação* (4.1.1)*.*

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 4.1.28. Se $|I| < \infty$, então o produto e a soma directa coincidem.

Exemplos 4.1.29.

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 4.1.30. *O produto directo de módulos-A (munido das respectivas projecções) é um produto na categoria* Mod_A.

Demonstração. Como para grupos abelianos. $\square$

Proposição 4.1.31. *A soma directa de módulos-A (equipada com as respectivas inclusões) é um coproduto na categoria* Mod_A.

Demonstração. Como para grupos abelianos. $\square$

4.2 18ª Aula

4.2.1 Soma directa interna e somandos directos

Definição 4.2.1. *Seja* $\{N_i\}_{i\in I}$ *uma família de submódulos de um módulo-A* M*. Se o homomofismo 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 4.2.2. *Seja* $\{N_i\}_{i\in I}$ *uma família de submódulos de* M*. Então* $M = \oplus_{i\in I} N_i$ 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:

$$\ker\varphi \neq 0 \Leftrightarrow \exists_{i_1,\ldots,i_k\in I}\, \exists_{(\mathbf{v}_{i_1},\ldots,\mathbf{v}_{i_k})\in N_{i_1}\times\cdots\times N_{i_k}-\{0\}} : \mathbf{v}_{i_1} + \cdots + \mathbf{v}_{i_k} = 0,$$

e

$$\mathbf{v}_{i_1} + \cdots + \mathbf{v}_{i_k} = 0 \Leftrightarrow \underbrace{\mathbf{v}_{i_1}}_{\in N_{i_1}} = \underbrace{-(\mathbf{v}_{i_2} + \ldots + \mathbf{v}_{i_k})}_{\in N_{i_2}+\cdots+N_{i_k}}.$$

□

Definição 4.2.3. *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 4.2.4. 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 4.2.2, $M = N_1 \oplus N_2$ 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, existira $N_2 < M$ *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 de M têm ordem infinita.

Definição 4.2.5. *Sejam M_n módulos-A e sejam $f_n \in \hom_A(M_n, M_{n+1})$. 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 $\ker f_n = \operatorname{im} f_{n-1}$ (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 4.2.6. 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* $\ker \pi = \operatorname{im} i \cong N$.

Exemplo 4.2.7. 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 4.2.8. 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 *exacta curta*.

Definição 4.2.9. *Diz-se que a sucessão exacta curta de módulos-A*

$$0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$$

se cinde *se* $\operatorname{im} f_1$ *é um somando directo de* M_2*.*

Observação 4.2.10. Se a sucessão se cinde, seja $N \subset M_2$ um complemento de $\operatorname{im} f_1$. Temos

$$N \cong \frac{M_2}{\operatorname{im} f_1} = \frac{M_2}{\ker f_2} \underset{\cong}{\xrightarrow{f_2}} M_3,$$

logo

$$\boxed{M_2 \cong M_1 \oplus M_3}$$

Exemplo 4.2.11. 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 4.2.12. *Um isomorfismo entre duas sucessões exactas curtas* $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ *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*

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r, "f_1"] \arrow[d, "\alpha_1"] & M_2 \arrow[r, "f_2"] \arrow[d, "\alpha_2"] & M_3 \arrow[r] \arrow[d, "\alpha_3"] & 0 \\
0 \arrow[r] & N_1 \arrow[r, "g_1"] & N_2 \arrow[r, "g_2"] & N_3 \arrow[r] & 0
\end{tikzcd}$$

comuta.

Exercício 4.2.13. *Mostre que uma sucessão 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*

$$0 \to M_1 \xrightarrow{\iota_1} M_1 \oplus M_3 \xrightarrow{\pi_2} M_3 \to 0.$$

Proposição 4.2.14. *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) $\exists\, r \in \hom_A(M_3, M_2) : f_2 \circ r = \mathrm{id}_{M_3}$*;*

(c) $\exists\, l \in \hom_A(M_2, M_1) : l \circ f_1 = \mathrm{id}_{M_1}$*.*

Exemplo 4.2.15. Sejam M_1, M_2 módulos-A. Então a sucessão

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, shift left, "\iota_1"] & M_1 \oplus M_2 \arrow[l, dotted, shift left, "l"] \arrow[r, shift left, "\pi_2"] & M_2 \arrow[l, dotted, shift left, "r"] \arrow[r] & 0 \end{tikzcd}$$

cinde-se. os homomorfismos r e l a que se refere a Proposição 4.2.14 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 4.2.16. No exemplo anterior, os homomorfismos r e l a que se refere a Proposição 4.2.14 são obtidos a partir de ι_1, π_2 e do complemento M_2 para $M_1 = \operatorname{im} \iota_1$ da seguinte forma:

$$\begin{aligned} r(\mathbf{v}_2) &= \iota_2(\mathbf{v}_2) = (0, \mathbf{v}_2) = \left(\pi_2|_{M_2}\right)^{-1}(\mathbf{v}_2); \\ l\,\overbrace{(\mathbf{v}_1, \mathbf{v}_2)}^{\mathbf{v}} &= \mathbf{v}_1 = \iota_1^{-1}(\mathbf{v}_1, 0) \\ &= \iota_1^{-1}(\mathbf{v} - \iota_2(\pi_2(\mathbf{v}))) \\ &= \iota_1^{-1}(\mathbf{v} - r(\pi_2(\mathbf{v}))). \end{aligned}$$

Demonstração da Proposição 4.2.14.
$\boxed{(a) \Rightarrow (b)}$ Seja N um complemento de $\operatorname{im} f_1$. Defina-se $r := \left(f_2|_N\right)^{-1}$. Note-se que r está bem definido, pois $N \cap \ker f_2 = \{0\}$ e

$$f_2 \circ r = f_2 \circ \left(f_2|_N\right)^{-1} = \mathrm{id}_{M_3}.$$

$\boxed{(b) \Rightarrow (c)}$ 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:

$$f_2(\mathbf{x} - r(f_2(\mathbf{x}))) = f_2(\mathbf{x}) - f_2(\mathbf{x}) = 0 \Rightarrow \mathbf{x} - r(f_2(\mathbf{x})) \in im f_1.$$

- $l \circ f_1 = \mathrm{id}_{M_1}$:

$$l(f_1(\mathbf{x})) = f_1^{-1}(f_1(\mathbf{x}) - r(f_2(f_1(\mathbf{x})))) = f_1^{-1}(f_1(\mathbf{x})) = \mathbf{x}.$$

$\boxed{(c) \Rightarrow (a)}$ Seja l como no enunciado. Defina-se $N \coloneqq \ker l$. Temos

- $N \cap \mathrm{im}\, f_1 = \{0\}$, pois:

$$\begin{aligned} \mathbf{x} \in N \cap \mathrm{im}\, f_1 &\Leftrightarrow l(\mathbf{x}) = 0 \wedge \exists \mathbf{y} : \mathbf{x} = f_1(\mathbf{y}) \\ &\Rightarrow l(f_1(\mathbf{y})) = 0 \\ &\Leftrightarrow \mathbf{y} = 0 \\ &\Rightarrow \mathbf{x} = 0. \end{aligned}$$

- $M_2 = N + \mathrm{im}\, f_1$, pois:

$$\mathbf{x} = \underbrace{\mathbf{x} - f_1(l(\mathbf{x}))}_{\in \ker l} + \underbrace{f_1(l(\mathbf{x}))}_{\in \mathrm{im}\, f_1}.$$

Concluímos que $M_2 = N \oplus \mathrm{im}\, f_1$. □

4.2.2 Módulos livres

Definição 4.2.17. *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 4.2.18. Se M é um espaço vectorial-k, a noção de independência linear aqui definida coincide a habitual.

Definição 4.2.19. *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:*

(a) S é l.i.*, e*

(b) $M = \langle S\rangle$.

Se M tem uma base, diz-se que M é livre*.*

Exemplos 4.2.20.

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 $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$, onde $\mathbf{e}_i$ denota o i-ésimo elemento da base canónica: $\mathbf{e}_i \coloneqq (\delta_{ki})_{k=1,\dots,n} \in \mathbb{Z}^n$.

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+T} não é uma base: $a \in I \Rightarrow a(1+I) = 0 \Rightarrow \{1+I\}$ não é *l.i.* se $I \neq (0)$.

   Exercício: Se $I \neq (0)$ é um ideal bilateral, então A/I não é livre.

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 $f_1 + f_2 \in F$ e $a \cdot f_1 \in F$.

   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 $F(X)$ e portanto $F(X)$ é livre.

Exercício 4.2.21. *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'.*

Exercício 4.2.22. *Seja $M \in \mathrm{Mod}_A$ livre com base $\{\mathbf{v}\}$. Mostre que $M \cong A$.*

Notação 4.2.23. 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 $F(X)$.

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 $\hom_{\mathcal{C}}(X, Y)$ como um subconjunto $\hom_{\mathrm{Set}}(X, Y)$.

Definição 4.2.24. *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*

$$\forall\, C \in \mathcal{C}\, \forall\, f \in \hom_{\mathrm{Set}}(X, C)\ \exists!\, \bar{f} \in \hom_{\mathcal{C}}(F, C) : \bar{f} \circ i = f \in \hom_{\mathrm{Set}}(X, C).$$

Exercício 4.2.25. *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.

4.3 19ª Aula

4.3.1 Caracterização dos módulos livres; espaços vectoriais

Lema 4.3.1. *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 4.3.2. *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 $N_i \cong A$ pelo Exercício 4.2.22.

$\boxed{(b) \Rightarrow (a)}$ Seja $\mathbf{v}_i$ *t.q.* $N_i = \langle \mathbf{v}_i \rangle$, então $\{\mathbf{v}_i \mid i \in I\}$ é uma base de M (ver Exercício 4.2.21).

$\boxed{(a) \Rightarrow (c)}$ 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 (*cf.* Exercício 4.2.21).

□

Teorema 4.3.3. *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 $\mathbf{v} \in V - \{0\}$, 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. $\square$

Corolário 4.3.4. *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.*

4.3.2 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 4.3.5 (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 $f \in \operatorname{End}_A(M) = \operatorname{End}_A(U_1 \oplus U_2)$. Definimos

$$\begin{aligned}
f_{11} &= \pi_1 \circ f \circ \iota_1 \in \hom_A(U_1, U_1)\\
f_{12} &= \pi_1 \circ f \circ \iota_2 \in \hom_A(U_2, U_1)\\
f_{21} &= \pi_2 \circ f \circ \iota_1 \in \hom_A(U_1, U_2)\\
f_{22} &= \pi_2 \circ f \circ \iota_2 \in \hom_A(U_2, U_2).
\end{aligned}$$

Obtemos assim 4 homomorfismos que podemos escrever na forma matricial:

$$\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix}, \qquad f_{ij} \in \hom_A(U_j, U_i).$$

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 $\alpha \in \operatorname{End}_A(M)$ 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:

$$\begin{aligned}
f \mapsto (\pi_i \circ f \circ \iota_j)_{i,j} &\mapsto \sum_{i,j} \iota_i \circ \pi_i \circ f \circ \iota_j \circ \pi_j = \sum_{j=1}^{2} \sum_{i=1}^{2} (\iota_i \circ \pi_i) \circ f \circ (\iota_j \circ \pi_j)\\
&= \sum_{j=1}^{2} \mathrm{id}_M \circ f \circ (\iota_j \circ \pi_j) = \mathrm{id}_M \circ f \circ \mathrm{id}_M = f.
\end{aligned}$$

e

$$\begin{aligned}
(\alpha_{ij})_{i,j} \mapsto \sum_{r,s} \iota_r \circ \alpha_{rs} \circ \pi_s &\mapsto \Big(\pi_i \circ \sum_{r,s} \iota_r \circ \alpha_{rs} \circ \pi_s \circ \iota_j\Big)_{i,j}\\
&= \Big(\sum_{r,s} (\pi_i \circ \iota_r) \circ \alpha_{rs} \circ (\pi_s \circ \iota_j)\Big)_{i,j} = \big(\mathrm{id}_{M_i} \circ \alpha_{ij} \circ \mathrm{id}_{M_j}\big)_{i,j} = (\alpha_{ij})_{i,j} \ .
\end{aligned}$$

A composta

$$\begin{aligned}
\{f \circ g\}_{ij} = \pi_i \circ f \circ g \circ \iota_j &= \pi_i \circ f \circ \left(\sum_{k=1}^{2} \iota_k \circ \pi_k\right) \circ g \circ \iota_j\\
&= \sum_k (\pi_i \circ f \circ \iota_k) \circ (\pi_k \circ g \circ \iota_j) = \sum_k f_{ik} \circ g_{kj}
\end{aligned}$$

corresponde ao produto de matrizes de homomorfismos:

$$\begin{aligned}\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \cdot \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} &:= \\ &= \begin{pmatrix} f_{11} \circ g_{11} + f_{12} \circ g_{21} & f_{11} \circ g_{12} + f_{12} \circ g_{22} \\ f_{21} \circ g_{11} + f_{22} \circ g_{21} & f_{21} \circ g_{12} + f_{22} \circ g_{22}. \end{pmatrix}\end{aligned} \tag{4.3.1}$$

Teorema 4.3.6. *Seja $M = U_1 \oplus \cdots \oplus U_n$, então as correspondências*

$$f \mapsto \left(f_{ij}\right); \quad f_{ij} = \pi_i \circ f \circ \iota_j,$$

e

$$\left(f_{ij}\right) \mapsto \alpha = \sum_{i,j} \iota_i \circ \alpha_{ij} \circ \pi_j,$$

estabelecem um isomorfismo de anéis entre $\operatorname{End}_A(M)$ *e o anel de matrizes* $n \times n$*, com entradas* $\alpha_{ij} \in \hom_A(U_j, U_i)$*, munido do produto descrito em* (4.3.1)*, no caso* $n = 2$.

Demonstração. Como no caso $n = 2$. □

Corolário 4.3.7. *Seja U um módulo-A. Então, existe um isomorfismo de anéis*

$$\operatorname{End}_A(U^n) \cong M_n(\operatorname{End}_A(U)).$$

Exemplo 4.3.8. Consideremos o caso $U = A$, visto como um módulo-A à esquerda e seja $f \in \operatorname{End}_A(A)$. Seja $b = f(1_A)$. Temos

$$\forall a \in A, \quad f(a) = af(1_A) = ab.$$

Se $g \in \operatorname{End}_A(A)$ e $c = g(1_A)$, temos

$$(f \circ g)(1_A) = f(g(1_A)) = f(c) = cf(1_A) = cb.$$

Portanto, $\operatorname{End}_A(A) \cong A^{op}$, onde A^{op} denota o anel $(A, +, \star)$ *t.q.*

$$\boxed{b \star c := cb}$$

Corolário 4.3.9. *Seja A um anel. Então, existe um isomorfismo de anéis*

$$\boxed{\operatorname{End}_A\left(A^n\right) \cong M_n\left(A^{op}\right)}$$

Exemplos 4.3.10.

1. Dado $f \in \mathrm{End}_A(A^n)$ a correspondência do Teorema 4.3.6 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, $\hom_A(A^m, A^n)$ 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 $g \in \hom_A(A^p, A^m)$ então a composta $h = f \circ g \in \hom_A(A^p, A^n)$ é representada pela matriz $\big(h_{ij}\big)$ dada por
$$h_{ij} = \sum_k f_{ik} \star g_{kj} = \sum_k g_{kj} f_{ik}. \tag{4.3.2}$$
Ou seja,
$$\boxed{\hom_A(A^m, A^n) \cong M_{n\times m}(A^{op})}$$
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 (4.3.2), corresponde à composição
$$\hom_A(A^m, A^n) \times \hom_A(A^p, A^m) \to \hom_A(A^p, A^n).$$

3. Se A é um anel comutativo, então $A \cong A^{op}$ e portanto,
$$\boxed{\hom_A(A^m, A^n) \cong M_{n\times m}(A)}$$

4.3.3 Invariância Dimensional

Definição 4.3.11. *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 4.3.12. Os corpos têm a *p.i.d.*. De seguida veremos que os anéis de divisão também têm a *p.i.d.*.

Proposição 4.3.13. *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. Como M, N são objectos livres em Mod_A gerados por bases, se $\dim_A M = \dim_A N$ então existe uma bijecção entre as bases de M e N e essa bijecção induz um isomorfismo entre M e N. Reciprocamente, se $f\colon M \to N$ é um isomorfismo e $S \subset M$ é uma base, então $f(S)$ é uma base de N, logo $\dim_A M = \dim_A N$. $\square$

Exemplo 4.3.14. Dois espaços vectoriais sobre um anel de divisão são isomorfos *sse* têm a mesma dimensão.

Proposição 4.3.15. *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, otém-se também que $|J| \leq |I|$. $\square$

4.4 20ª Aula

4.4.1 Invariância dimensional (cont.)

Teorema 4.4.1. *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 4.3.15. 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.* $a_{i_1} \neq 0$, então

$$\mathbf{x}_{i_1} = a_{i_1}^{-1}\left(\mathbf{y}_1 - \sum_{i \neq i_1} a_i\mathbf{x}_i\right),$$

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

$$\mathbf{x}_{i_2} = b_{i_2}^{-1}\left(\mathbf{y}_2 - c_1\mathbf{y}_1 - \sum_{i \neq i_1, i_2} b_i\mathbf{x}_i\right),$$

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 concluí-se que $\langle \mathbf{y}_1, \ldots, \mathbf{y}_n \rangle = V$ e portanto $n = m$ visto que S' é *l.i.*. □

Proposição 4.4.2. *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 (Proposição 4.3.15).

$\boxed{(b) \Leftrightarrow (c)}$ Segue de

$$\hom_A(A^m, A^n) \cong M_{n\times m}(A^{op}) \quad \text{e} \quad \hom_A(A^n, A^m) \cong M_{m\times n}(A^{op}).$$

□

Corolário 4.4.3. *Sejam A, B anéis* t.q. $\hom_{\mathrm{Ring}}(A, B) \neq \varnothing$. *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 4.4.4. *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.*. □

Exercício 4.4.5. *Seja V um espaço vectorial sobre um anel de divisão D e seja $W \subset V$ um subespaço. Então*

(i) $\dim_D W \leq \dim_D V$

(ii) $\dim_D W = \dim_D V < \infty \Rightarrow W = V$

(iii) $\dim_D V = \dim_D W + \dim_D(V/W)$

4.4.2 Módulos Projectivos

Definição 4.4.6. *Um módulo-A, P, diz-se* projectivo *se para todo o diagrama em* Mod_A

$$\begin{tikzcd} & P \arrow[d, "f"] & \\ M \arrow[r, "g"] & N \arrow[r] & 0 \end{tikzcd}$$

t.q. *a linha inferior é exacta (*i.e., *g é epi), existe* $h\colon P \to M$ *que faz comutar:*

$$\begin{tikzcd} & P \arrow[dl, dashed, "\exists h"'] \arrow[d, "f"] & \\ M \arrow[r, "g"] & N \arrow[r] & 0 \end{tikzcd}$$

Teorema 4.4.7. *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

$$\begin{tikzcd} & F \arrow[d, "f"] & \\ M \arrow[r, "g"] & N \arrow[r] & 0, \end{tikzcd}$$

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 4.4.8. Seja k um corpo. Em $\mathrm{Mod}_k = \mathrm{Vect}_k$ todos os módulos são livres e portanto são projectivos.

Exemplo 4.4.9. $\mathbb{Z}_2$ é um módulo-$\mathbb{Z}$ não projectivo: no diagrama

$$\begin{tikzcd} & \mathbb{Z}_2 \arrow[dl, dashed, "\nexists h"'] \arrow[d, "\mathrm{id}"] & \\ \mathbb{Z} \arrow[r, "\pi"] & \mathbb{Z}_2 \arrow[r] & 0, \end{tikzcd}$$

onde π é a projecção canónica, não existe h como indicado, pois $\hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) = 0$.

Corolário 4.4.10. *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 4.4.11. *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

$$\begin{tikzcd}
& P \arrow[dl, dashed, "\exists r"'] \arrow[d, "\mathrm{id}_P"] & \\
N \arrow[r, "g"] & P \arrow[r] & 0,
\end{tikzcd}$$

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

$$\begin{tikzcd}
& P \arrow[d, "f"] & \\
M \arrow[r, "g"'] & N \arrow[r] & 0
\end{tikzcd}$$

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)

$$\begin{tikzcd}
& F \arrow[ddl, dashed, "\exists h'"'] \arrow[d, "\pi"'] & \\
& P \arrow[u, bend right, "\iota"'] \arrow[dl, dashed, "h"] \arrow[d, "f"] & \\
M \arrow[r, "g"'] & N \arrow[r] & 0,
\end{tikzcd}$$

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.

$\square$

Exemplo 4.4.12. Consideremos o anel $\mathbb{Z}_6$. Temos dois ideais

$$I \coloneqq \{\bar{0}, \bar{3}\} = (\bar{3}) \subset \mathbb{Z}_6 \quad \text{e} \quad J \coloneqq \{\bar{0}, \bar{2}, \bar{4}\} = (\bar{2}) \subset \mathbb{Z}_6$$

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: $\underline{2} \times \underline{3} = \underline{0}$.

Exercício 4.4.13. *Sejam $P_i \in \mathrm{Mod}_R$, $i \in I$. Mostre que $\bigoplus_{i\in I} P_i$ é projectivo sse P_i é projectivo $\forall i \in I$.*

4.4.3 Módulos Injectivos

Consideremos o diagrama dual do que define módulo projectivo:

$$\begin{tikzcd} & P \\ M \arrow[ur, dashed, "\exists h"] & N \arrow[l, "g"'] \arrow[u, "f"'] & 0 \arrow[l] \end{tikzcd}$$

Definição 4.4.14. *Um módulo-A, I, diz-se* injectivo *se para todo o diagrama*

$$\begin{tikzcd} & I \\ M & N \arrow[l, "i"'] \arrow[u, "f"'] & 0 \arrow[l] \end{tikzcd}$$

t.q. *a linha inferior é exacta (*i.e., *i é injectivo), existe $h\colon M \to I$ que faz comutar o diagrama*

$$\begin{tikzcd} & I \\ M \arrow[ur, dashed, "\exists h"] & N \arrow[l, "i"'] \arrow[u, "f"'] & 0. \arrow[l] \end{tikzcd}$$

Consideramos o caso particular de $A = \mathbb{Z}$.

Definição 4.4.15. *Um grupo abeliano D diz-se* divisível *se $\forall y \in D$ e $\forall n \in \mathbb{Z} - \{0\}$ a equação*

$$nx = y$$

tem solução $x \in D$.

Exemplo 4.4.16. $(\mathbb{Q}, +)$ é um grupo divisível.

Exercício 4.4.17. *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*

$$\begin{tikzcd} & I & \\ A \arrow[ur, dashed, "\exists h"] & L \arrow[l, "i"'] \arrow[u, "f"'] & 0. \arrow[l] \end{tikzcd}$$

Teorema 4.4.18. *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 $n \in \mathbb{Z} - \{0\}$. Consideremos o diagrama

$$\begin{tikzcd} & \langle y \rangle & \\ \mathbb{Z} \arrow[ur, dashed, "h"] & n\mathbb{Z} \arrow[l, "i"'] \arrow[u, "f"'] & 0, \arrow[l] \end{tikzcd}$$

onde $f(n) = y$. Temos $nh(1) = h(n) = h(i(n)) = f(n) = y$.

$\boxed{\Rightarrow}$ Sejam f, i como no diagrama seguinte

$$\begin{tikzcd} & D & \\ M & N \arrow[l, "i"'] \arrow[u, "f"'] & 0. \arrow[l] \end{tikzcd}$$

Seja

$$\mathcal{S} := \{g\colon M' \to D \mid i(N) < M' < M \wedge g \circ i = f\}.$$

Temos $S \neq \varnothing$ pois

$$\big(f \circ i^{-1}\colon i(N) \to D\big) \in \mathcal{S}.$$

O conjunto $\mathcal{S}$ é parcialmente ordenado pela relação:

$$(g_1\colon M_1' \to D) \leq (g_2\colon M_2' \to D) \Leftrightarrow M_1' \subset M_2' \wedge g_2|_{M_1'} = g_1.$$

Seja $\{g_j\colon M_j' \to D \mid j \in J\}$ uma cadeia em $\mathcal{S}$. Defina-se $M' := \cup_{j\in I} M_j'$ 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 $h\colon M' \to N$ de $\mathcal{S}$. Seja $y \in M \setminus M'$ e $M'' := M' + \langle y\rangle$. Se $M' \cap \langle y\rangle = \{0\}$, temos $M'' = M' \oplus \langle y\rangle$ e h pode ser estendido fazendo $\bar{h}|_{\langle y\rangle} := 0$.

Se $M' \cap \langle y\rangle \neq \{0\}$, então $I = \{m \in \mathbb{Z} \mid my \in M' \cap \langle y\rangle\}$ 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.* $h(ny) = nx$. Defina-se $\bar{h}\colon M'' \to D$ *t.q.* $\bar{h}|_{M'} = h$ e $\bar{h}(y) = x$, i.e., $\bar{h}(v+my) := h(v)+mx$ onde $v \in M$ e $m \in \mathbb{Z}$. $\bar{h}$ está bem definido pois, se $v_1 + m_1 y = v_2 + m_2 y$, com $v_i \in M'$ e $m_i \in \mathbb{Z}$, então

$$\begin{aligned} v_1 - v_2 = m_2 y - m_1 y = (m_2 - m_1)y \in M' \cap \langle y\rangle \\ \Rightarrow m_2 - m_1 \in I \Leftrightarrow m_2 - m_2 = mn \end{aligned}$$

para algum $m \in \mathbb{Z}$ e, portanto,

$$\begin{aligned} h(v_1) - h(v_2) &= h(v_1 - v_2) = h((m_2 - m_1)y) \\ &= h(mny) = mh(ny) = mnx = m_2 x - m_1 x\ . \end{aligned}$$

Obtemos assim uma contradição, pois $\bar{h}$ estende h. Concluímos que $M' = M$.

$\square$

Exemplo 4.4.19. $(\mathbb{Q}, +)$ é um grupo abeliano injectivo.

4.5 21ª Aula

4.5.1 Produto Tensorial

Seja A um *anel comutativo.*

Definição 4.5.1. *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* $\mathbf{m}_1, \mathbf{m}'_1 \in M_1$, $\mathbf{m}_2, \mathbf{m}'_2 \in M_2$ *se tem*

(i) $\varphi(a\mathbf{m}_1 + a'\mathbf{m}'_1, \mathbf{m}_2) = a\varphi(\mathbf{m}_1, \mathbf{m}_2) + a'\varphi(\mathbf{m}'_1, \mathbf{m}_2)$;

(ii) $\varphi(\mathbf{m}_1, a\mathbf{m}_2 + a'\mathbf{m}'_2) = a\varphi(\mathbf{m}_1, \mathbf{m}_2) + a'\varphi(\mathbf{m}_1, \mathbf{m}'_2)$

i.e., φ *é bilinear-*A *se é linear-*A *separadamente em cada uma das variáveis.*

Observação 4.5.2. De forma análoga define-se aplicação multilinear-A:

$$\varphi\colon M_1 \times \cdots \times M_r \to N.$$

Exemplo 4.5.3. 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$-\mathbb{R}$.

Teorema 4.5.4. *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 $\phi\colon M_1 \times M_2 \to N$, $\exists!\, \tilde{\phi} \in \hom_A(M_1 \otimes M_2, N)$ *que faz comutar o diagrama seguinte:*

$$\begin{tikzcd} M_1 \times M_2 \arrow[r, "p"] \arrow[dr, "\phi"'] & M_1 \otimes M_2 \arrow[d, dashed, "\exists!\tilde{\phi}"] \\ & N \end{tikzcd}$$

Demonstração. Seja L o módulo-A livre gerado $M_1 \times M_2$: $L := F(M_1 \times M_2)$; os seus elementos escrevem-se unicamente na forma

$$\sum_{i=1}^{n} a_i \mathbf{e}_{(v_i, w_i)},$$

com $a_i \in A$, $v_i \in M_1$, $w_i \in M_2$. Seja $R \subset L$ o submódulo gerado pelos elementos da seguinte forma:

$$\begin{aligned}
&\mathbf{e}_{(v+v',w)} - \mathbf{e}_{(v,w)} - \mathbf{e}_{(v',w)}\\
&\mathbf{e}_{(v,w+w')} - \mathbf{e}_{(v,w)} - \mathbf{e}_{(v,w')}\\
&\mathbf{e}_{(av,w)} - a\mathbf{e}_{(v,w)}\\
&\mathbf{e}_{(v,aw)} - a\mathbf{e}_{(v,w)}.
\end{aligned}$$

onde $v, v' \in M_1$, $w, w' \in M_2$ 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

$$\begin{tikzcd}
p\colon M_1 \times M_2 \arrow[r, hook] & L \arrow[r, "\pi"] & M_1 \otimes M_2 \\
(v,w) \arrow[r, mapsto] & \mathbf{e}_{(v,w)} \arrow[r, mapsto] & \pi(\mathbf{e}_{(v,w)}).
\end{tikzcd}$$

Por definição de R, p é bilinear-A:

$$\mathbf{e}_{(v+v',w)} - \mathbf{e}_{(v,w)} - \mathbf{e}_{(v',w)} \in R \Leftrightarrow p(v+v',w) = p(v,w) + p(v',w).$$

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:

$$\begin{tikzcd}
M_1 \times M_2 \arrow[r, "i"] \arrow[dr, "\phi"'] & L \arrow[d, dashed, "\exists! \bar{\phi}"] \\
& N
\end{tikzcd}$$

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

$$\begin{tikzcd}
& L \arrow[r, "\bar{\phi}"] \arrow[d, "\pi"] & N \\
M_1 \otimes M_2 \arrow[r, equal] & L/R \arrow[ur, dashed, "\exists!\, \tilde{\phi}"'] &
\end{tikzcd}$$

Juntando os dois diagramas acima, obtemos o diagrama pretendido:

$$\begin{tikzcd}
& M_1 \times M_2 \arrow[ddl] \arrow[d, "i"] \arrow[dr, "\phi"] & \\
& L \arrow[r, "\exists!\bar{\phi}"] \arrow[d, "\pi"] & N \\
M_1 \otimes M_2 \arrow[r, equal] & L/R \arrow[ur, dashed, "\exists!\tilde{\phi}"'] &
\end{tikzcd}$$

□

Observação 4.5.5. 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 4.5.6. Dados $\mathbf{v} \in M_1$ e $\mathbf{w} \in M_2$ denotamos por $v \otimes w$ o elemento $p(v, w)$ do produto tensorial $V \otimes W$:

$$\boxed{\mathbf{v} \otimes \mathbf{w} := p(\mathbf{v}, \mathbf{w})}$$

Observação 4.5.7.

1. Da bilinearidade de $p\colon M_1 \times M_2 \to M_1 \otimes M_2$, seguem as seguintes igualdades em $M_1 \otimes M_2$

$$\begin{aligned} a(\mathbf{v} \otimes \mathbf{w}) &= (a\mathbf{v}) \otimes \mathbf{w} = \mathbf{v} \otimes (a\mathbf{w}) \\ (\mathbf{v} + \mathbf{v}') \otimes \mathbf{w} &= \mathbf{v} \otimes \mathbf{w} + \mathbf{v}' \otimes \mathbf{w}. \end{aligned}$$

   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

$$\mathbf{x} = \pi\left(\sum_{i=1}^{n} a_i \mathbf{e}_{(\mathbf{v}'_i,\mathbf{w}'_i)}\right) \Leftrightarrow \mathbf{x} = \sum_{i=1}^{n} a_i \left(\mathbf{v}'_i \otimes \mathbf{w}'_i\right) = \sum_{i=1}^{n} \underbrace{(a_i \mathbf{v}'_i)}_{\mathbf{v}_i} \otimes \underbrace{\mathbf{w}'_i}_{\mathbf{w}_i}.$$

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 4.5.8.

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 $V = W = (\mathbb{R}^n)^\star := \hom_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$, então $V \otimes W = T^{2,0}(\mathbb{R}^n)$, *e.g.*, o produto interno usual $(\cdot\,,\cdot) \in T^{2,0}(\mathbb{R}^n)$ (voltaremos a este exemplo mais adiante).

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 4.5.9. No Exemplo 4.5.8.2. usámos o seguinte facto: da bilinearidade de $p\colon M_1 \times M_2 \to M_1 \otimes M_2$ segue

$$\forall_{\mathbf{v}\in M_1} \forall_{\mathbf{w}\in M_2} \quad \mathbf{v} \otimes 0_W = 0_V \otimes \mathbf{w} = 0_{V\otimes W}.$$

De facto,

$$p(\mathbf{v}, 0) = p(\mathbf{v}, 0_A \cdot 0_W) = 0_{V\otimes W} = p(0_A \cdot 0_V, \mathbf{w}).$$

Exercício 4.5.10. *Determine* $r \in \mathbb{N}$ t.q. $\mathbb{Z}_m \otimes \mathbb{Z}_n \cong \mathbb{Z}_r$.

Notação 4.5.11. Também se escreve $M_1 \otimes_A M_2$ para enfatizar que se trata do *produto tensorial como módulos-A.*

Teorema 4.5.12. *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 multiplineares para módulos-A. Esta propriedade determina o módulo* $\bigotimes_{i=1}^n M_i$ *a menos de isomorfismo.*

Notação 4.5.13. $\boxed{\mathbf{v}_1 \otimes \cdots \otimes \mathbf{v}_n := p(\mathbf{v}_1, \ldots, \mathbf{v}_n)}$

Proposição 4.5.14 (Propriedades do Produto Tensorial)**.** *Sejam M, M_1, M_2, M_3, N, N_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* $v_1 \otimes v_2 \leftrightarrow v_2 \otimes v_1$*;*

(c) $\left(\bigoplus_{i\in I} N_i\right) \otimes N \cong \left(\bigoplus_{i \in I} N_i \otimes N\right)$ *com isomorfismos induzidos por* $(v_i)_{i\in I} \otimes w \leftrightarrow (v_i \otimes w)_{i \in I}$*;*

(d) $M \otimes_A A \cong A \otimes_A M \cong M$ *com isomorfismos indizidos por* $v \otimes a \leftrightarrow a \otimes v \leftrightarrow av$*.*

Demonstração.

(b) Seja $\varphi\colon M_1 \times M_2 \to M_2 \otimes M_1$, dado por $\varphi(\mathbf{v}_1, \mathbf{v}_2) = \mathbf{v}_2 \otimes \mathbf{v}_1$ e $\psi\colon M_2 \times M_1 \to M_1 \otimes M_2$ dado por $\psi(\mathbf{v}_2, \mathbf{v}_1) = \mathbf{v}_1 \otimes \mathbf{v}_2$. Vejamos que φ e ψ são bilineares:

$$\begin{aligned} \varphi(a\mathbf{v}_1 + a'\mathbf{v}_1', \mathbf{v}_2) &= \mathbf{v}_2 \otimes (a\mathbf{v}_1 + a'\mathbf{v}_1') \\ &= a(\mathbf{v}_2 \otimes \mathbf{v}_1) + a'(\mathbf{v}_2 \otimes \mathbf{v}_1') \\ &= a\varphi(\mathbf{v}_1, \mathbf{v}_2) + a'\varphi(\mathbf{v}_1', \mathbf{v}_2). \end{aligned}$$

As restantes condições relativas à bilinearidade seguem de forma análoga. Pela propriedade universal do produto tensorial, concluí-se que existe $\tilde{\varphi} \in \hom_A(M_1 \otimes M_2, M_2 \otimes M_1)$ e $\tilde{\psi} \in \hom_A(M_2 \otimes M_1, M_1 \otimes M_2)$ *t.q.*

$$\begin{aligned} \tilde{\varphi}(\mathbf{v}_1 \otimes \mathbf{v}_2) &= \mathbf{v}_2 \otimes \mathbf{v}_1 \\ \tilde{\psi}(\mathbf{v}_2 \otimes \mathbf{v}_1) &= \mathbf{v}_1 \otimes \mathbf{v}_2, \end{aligned}$$

logo

$$\tilde{\psi}\tilde{\varphi}(\mathbf{v}_1 \otimes \mathbf{v}_2) = \tilde{\psi}(\mathbf{v}_2 \otimes \mathbf{v}_1) = \mathbf{v}_1 \otimes \mathbf{v}_2 = \mathrm{id}_{M_1 \otimes M_2}(\mathbf{v}_1 \otimes \mathbf{v}_2).$$

Portanto $\tilde{\psi}\tilde{\varphi} = \mathrm{id}_{M_1 \otimes M_2}$. Da mesma forma, $\tilde{\varphi}\tilde{\psi} = \mathrm{id}_{M_2 \otimes M_1}$.

(*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

$$\begin{aligned}\psi\varphi(a\otimes\mathbf{v}) &= \psi(a\mathbf{v}) = 1_A\otimes(a\mathbf{v}) = a(1_A\otimes\mathbf{v}) = a\otimes\mathbf{v}\\ \varphi\psi(\mathbf{v}) &= \varphi(1_A\otimes\mathbf{v}) = 1_A\cdot\mathbf{v} = \mathbf{v}.\end{aligned}$$ □

Definição 4.5.15. *Dados $f_1 \hom_A(M_1,N_1)$, $f_2\in\hom_A(M_2,N_2)$, a função*

$$\begin{aligned} M_1\times M_2 &\longrightarrow N_1\otimes N_2\\ (\mathbf{v},\mathbf{w}) &\longmapsto f_1(\mathbf{v})\otimes f_2(\mathbf{w})\end{aligned}$$

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 4.5.16. *Denotamos por $(\mathrm{Mod}_A)^2$, ou por $\mathrm{Mod}_A \times Mod_A$ a categoria dos pares de módulos-A e pares de homomorfismos de módulos-A.*

Proposição 4.5.17. *A correspondência $(M,N)\mapsto M\otimes N$ define um functor $(\mathrm{Mod}_A)^2\to\mathrm{Mod}_A$. Em particular, dado um módulo-A, N, as correspondências*

$$\underset{f\mapsto T(f,\mathrm{id}_N)}{M\to M\otimes N} \quad e \quad \underset{f\mapsto T(\mathrm{id}_N,f)}{M\mapsto N\otimes M}$$

são functores $\mathrm{Mod}_A\to\mathrm{Mod}_A$.

Demonstração. Exercício. □

Corolário 4.5.18. *Sejam $M,N\in\mathrm{Mod}_A$ livres com bases $\{\mathbf{m}_i\}_{i\in I}$ e $\{\mathbf{n}_j\}_{j\in J}$. Então $M\otimes N\in\mathrm{Mod}_A$ 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

$$\varphi\left(a_i\right)_{i\in I} \coloneqq \sum_{i\in I} a_i\mathbf{m}_i \quad \text{e} \quad \psi\left(b_j\right)_{j\in J} \coloneqq \sum_{j\in J} b_j\mathbf{n}_j.$$

Temos

$$\left(\bigoplus_{i\in I} A\right)\otimes\left(\bigoplus_{j\in J} A\right)\xrightarrow[\cong]{T(\varphi,\psi)} M\otimes N$$

pois $(\varphi, \psi) \in \hom_{(\mathrm{Mod}_A)^2}$ é um isomorfismo. Por outro lado,

$$\begin{array}{ccc} \bigoplus\limits_{(i,j)\in I\times J} A \otimes_A A & \xrightarrow{\cong} & \bigoplus\limits_{(i,j)\in I\times J} A \\ \Cup & & \Cup \\ (a_i \otimes b_j)_{i,j} & \longmapsto & (a_i b_j)_{i,j}\,, \end{array}$$

logo o resultado segue. □

Produto tensorial de módulos sobre um anel não comutativo

Se A é um anel não comutativo pode definir-se o produto tensorial entre um módulo-A *à direita*, M_1, e um módulo-A *à esquerda*, M_2: define-se $M_1 \otimes_A M_2$ como um *grupo abeliano* munido de uma aplicação *biaditiva* (*i.e.*, bilinear sobre $\mathbb{Z}$) $p\colon M_1 \times M_2 \to M_1 \otimes_A M_2$ que satisfaz

$$\forall_{a\in A}\,\forall_{\mathbf{v}\in M_1}\,\forall_{\mathbf{w}\in M_2} \quad p(\mathbf{v}a, \mathbf{w}) = p(\mathbf{v}, a\mathbf{w}),$$

ou seja,

$$(\mathbf{v}a) \otimes \mathbf{w} = \mathbf{v} \otimes (a\mathbf{w}).$$

Para que se possa definir em $M_1 \otimes_A M_2$ uma estrutura natural de módulo-A é necessário que M_1 ou M_2 sejam *bimódulos-A*.

4.6 22ª Aula

4.6.1 Propriedades adicionais do produto tensorial

Teorema 4.6.1. *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

$$M_1 \otimes N \xrightarrow{f\otimes Id} M_2 \otimes N \xrightarrow{g\otimes Id} M_3 \otimes N \longrightarrow 0$$

é uma sucessão exacta.

Demonstração. 1. $g \otimes Id$ é sobrejectivo: Dado $v \in M_3$ e $w \in N$, seja $u \in M_2$ tal que $g(u) = v$ (g é sobrejectivo por hipótese). Temos

$$v \otimes w = g(u) \otimes w = (g \otimes Id)(u \otimes w) \in \operatorname{im}(g \otimes Id)$$

e, como os elementos $v \otimes w$ geram $M_3 \otimes N$, concluímos que $g \otimes Id$ é sobrejectivo.

2. $\ker(g \otimes Id) \subset \operatorname{im}(f \otimes Id)$:

$$\operatorname{im} f = \ker g \Rightarrow g \circ f = 0 \Rightarrow (g \otimes Id) \circ (f \otimes Id) = (g \circ f) \otimes Id = 0.$$

3. $\operatorname{im}(f\otimes Id) \subset \ker(g\otimes Id)$: Por 2. e pela propriedade universal do quociente de módulos (Proposição 4.1.16), a aplicação

$$\varphi : \frac{M_2 \otimes N}{\operatorname{im}(f \otimes Id)} \longrightarrow M_3 \otimes N$$

induzida por $g\otimes Id$, i.e, tal que $\varphi(\underline{u \otimes w}) = g(u)\otimes w$, é um homomorfismo de módulos-A.

Como $\operatorname{im}(f \otimes Id) = \ker(g \otimes Id)$ *sse* φ é injectiva, vamos mostrar que φ é injectiva. Para isso basta ver que φ tem inverso à esquerda.

Seja então $\psi : M_3 \times N \to \frac{M_2\otimes N}{\operatorname{im}(f\otimes Id)}$ dada por $\psi(v, w) = \underline{u \otimes w}$, onde $u \in M_2$ é tal que $g(u) = v$.

ψ está bem definida: seja $u' \in M_2$ tal que $v = g(u) = g(u')$, então

$$u' - u \in \ker g = \operatorname{im} f \Rightarrow (u' - u) \otimes w \in \operatorname{im}(f \otimes Id) \quad \forall_{w\in N}$$

e portanto

$$\psi(g(u)\otimes w) = \underline{u\otimes w} = \underline{u\otimes w} + \underline{(u'-u)\otimes w} = \underline{u'\otimes w} = \psi(g(u')\otimes w).$$

Como ψ é claramente bilinear, exite um homomorfismo

$$\tilde{\psi} : M_3 \otimes N \longrightarrow \frac{M_2\otimes N}{\mathrm{im}(f\otimes Id)}$$

tal que $\tilde{\psi}(v\otimes u) = \psi(v,u)$. Logo

$$\tilde{\psi}\circ\varphi(\underline{u\otimes w}) = \tilde{\psi}(g(u)\otimes w) = \underline{u\otimes w} \qquad \forall_{u\in_2}\forall_{w\in N}$$

donde concluímos que $\tilde{\psi}\circ\varphi = Id$. □

Observação 4.6.2. 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 $g = Id_N$, obtemos um novo functor (Proposição 4.5.17)

$$T_N : \mathrm{Mod}_A \to \mathrm{Mod}_A$$

definido por $T_N(M) = M\otimes_A N$, nos objectos, e $T_N(f) = f\otimes Id$, 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 4.6.3. *Seja A um anel comutativo e sejam $M, N, K \in \mathrm{Mod}_A$. Então existe um isomorfismo de módulos-A*

$$\alpha\colon\ \hom_A(M\otimes_A N, K) \xrightarrow{\cong} \hom_A(M, \hom_A(N,K))$$

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. Verficamos que α está bem definido e tem inverso:

1. $\alpha(f)(\mathbf{v}) \in \hom_A(N,K)$:

$$\begin{aligned}\alpha(f)(\mathbf{v})(a\mathbf{w}+a'\mathbf{w}') &= f(\mathbf{v}\otimes(a\mathbf{w}+b\mathbf{w}')) = af(\mathbf{v}\otimes\mathbf{w}) + a'f(\mathbf{v}\otimes\mathbf{w}') \\ &= a\,[\alpha(f)(\mathbf{v})]\,(\mathbf{w}) + a'\,[\alpha(f)(\mathbf{v})]\,(\mathbf{w}').\end{aligned}$$

2. $\alpha f \in \hom_A(M, \hom_A(N, K))$: temos

$$\begin{aligned}(\alpha(f)(a\mathbf{v} + a'\mathbf{v}'))(\mathbf{w}) &= f((a\mathbf{v}) \otimes \mathbf{w} + (a'\mathbf{v}') \otimes \mathbf{w}) \\ &= (a\alpha(f)(\mathbf{v}))(\mathbf{w}) + (a'\alpha(f)(\mathbf{v}'))(\mathbf{w}),\end{aligned}$$

   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 $g \in \hom_A(M, \hom_A(N, K))$. 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 $a, a' \in A$, $f, f' \in \hom_A(M \otimes_A N, K)$, $v, v' \in M$ e $w, w' \in N$. □

Observação 4.6.4. 1. Dado um módulo-A, N, a correspondência $M \mapsto \hom_A(N, M)$ define um functor

$$H_N : \mathrm{Mod}_A \to \mathrm{Mod}_A \ .$$

   O teorema anterior, diz-nos que

$$\hom_A(T_N(M), K) \cong \hom_A(M, H_N(K)) \qquad \forall_{M,K \in \mathrm{Mod}_A} \ .$$

   Nestas condições, T_N e H_N dizem-se *functores adjuntos.*

2. Outro exemplo de um par de funcotres adjuntos já encontrado:

   $F : \mathrm{Set} \to \mathrm{Mod}_A$ 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 Definiccão 4.2.24,

$$\hom_{\mathrm{Mod}_A}(F(X), M) \cong \hom_{\mathrm{Set}}(X, E(M)) \qquad \forall_{X \in \mathrm{Set}} \forall_{M \in \mathrm{Mod}_A} \ ,$$

   onde $E : \mathrm{Mod}_A \to \mathrm{Set}$ é o functor esquecimento. Ou seja, F e E são functores adjuntos.

4.6.2 Extensão de escalares

Seja $\phi\colon A \to B$ um homomorfismo de anéis comutativos. Então B admite uma estrutura de módulo-A, $A \times B \to B$, dada por $(a,b) \mapsto \phi(a) \cdot_B b$.

Definição 4.6.5. *Seja M um módulo-A. Define-se*

$$M_B \coloneqq B \otimes_A M,$$

com a estrutura de módulo-B dada por

$$(b', b \otimes \mathbf{v}) \mapsto (b'b) \otimes \mathbf{v}, \quad \forall_{b,b' \in B} \forall_{\mathbf{v} \in M}.$$

Diz-se que M_B se obtém de M por extensão de escalares.

Proposição 4.6.6. *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.

$$M \underset{\cong}{\xrightarrow{f}} \bigoplus_{i \in I} A \Rightarrow M_B \underset{\cong}{\xrightarrow{T(\mathrm{id}_B, f)}} B \otimes_A \bigoplus_{i \in I} A \cong \bigoplus_{i \in I} B \otimes_A A \cong \bigoplus_{i \in I} B. \qquad \square$$

Exemplo 4.6.7. Seja $A = \mathbb{R}$, $B = \mathbb{C}$ e seja $\phi\colon \mathbb{R} \to \mathbb{C}$ a inclusão. Então

$$M = \mathbb{R}[x] \Rightarrow M_{\mathbb{C}} \cong \mathbb{C}[x].$$

Exemplo 4.6.8. O homomorfismo ϕ não tem de ser injectivo. Seja $A = \mathbb{Z}$, $B = \mathbb{Z}_n$ e seja $\phi\colon \mathbb{Z} \to \mathbb{Z}_n$ a projecção canónica. Então

$$M = \mathbb{Z}[x] \Rightarrow M_{\mathbb{Z}_n} \cong \mathbb{Z}_n[x].$$

4.7 23ª Aula

4.7.1 Módulos sobre Domínios Integrais

No que se segue D é um domínio integral.

Proposição 4.7.1. *Seja M um módulo-D. Então*

$$\operatorname{Torc} M := \{\mathbf{v} \in M \mid \exists\, a \in D - \{0\} : a\mathbf{v} = 0\}$$

é um submódulo de M.

Demonstração. Sejam $\mathbf{v}, \mathbf{v}' \in \operatorname{Torc} M$ e $d, d' \in D - \{0\}$ *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 $\operatorname{Torc} M$ é um subgrupo de M. Dado $d'' \in D$ temos $d''\mathbf{v} \in \operatorname{Torc} M$, pois $(d''d)\mathbf{v} = 0$. Concluímos que $\operatorname{Torc} M$ é um submódulo de M. □

Exemplos 4.7.2.

1. Se $D = k$ é um corpo e $M \in \mathrm{Vect}_k$, então $\operatorname{Torc} M = \{0\}$;
2. se $D = \mathbb{Z}$ e $M = \mathbb{Z}_n$, então $\operatorname{Torc} M = \mathbb{Z}_n$;
3. se $D = \mathbb{Z}$ e $M = \mathbb{Z}^n$, então $\operatorname{Torc} M = \{0\}$;
4. se $D = \mathbb{Z}$ e $M = \mathbb{Q}$, então $\operatorname{Torc} M = \{0\}$;
5. se $D = k[x]$, $M = V \in \mathrm{Vect}_k$ e $T \in \hom_k(V, V)$, então V tem uma estrutura de módulo-D dada por:
$$f(x) \cdot \mathbf{v} := \sum_{i=0}^{n} a_i T^i \mathbf{v},$$
onde $f(x) = \sum_{i=0}^{n} a_i x^i$. Temos
$$V = \operatorname{Torc}_{k[x]} V.$$

Definição 4.7.3. *Se $M \in \mathrm{Mod}_D$ é* t.q. $\operatorname{Torc} M = M$*, diz-se que M é um* módulo de torção. *Se* $\operatorname{Torc} M = \{0\}$*, diz-se que M é um módulo* livre de torção.

Exemplo 4.7.4. Seja G um grupo abeliano, i.e., um módulo-$\mathbb{Z}$. Então

$$g \in \operatorname{Torc} G \Leftrightarrow \exists\, n \in \mathbb{Z} \setminus \{0\} \text{ t.q. } ng = 0 \Leftrightarrow n \mid |g|.$$

Ou seja, $\operatorname{Torc} G = \{g \in G \mid |g| \text{ é finita}\}$. 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 4.7.5. 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.

Exercício 4.7.6. *Seja M um módulo-D livre. Mostre que M é livre de torção.*

Proposição 4.7.7.

(a) Seja $\phi \in \hom_D(M_1, M_2)$, então

$$\phi(\operatorname{Torc} M_1) \subset \operatorname{Torc} M_2.$$

Se ϕ é mono, então $\phi(\operatorname{Torc} M_1) = (\operatorname{Torc} M_2) \cap \operatorname{im} \phi$. Se ϕ é epi e $\ker \phi \subset \operatorname{Torc} M_1$, então $\phi(\operatorname{Torc} M_1) = \operatorname{Torc} M_2$.

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

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

$$\operatorname{Torc}\left(\bigoplus_{i \in I} M_i\right) = \bigoplus_{i \in I} \operatorname{Torc} M_i.$$

Demonstração.

(a) Temos

$$a\mathbf{v} = 0 \Rightarrow a\phi(\mathbf{v}) = 0,$$

logo $\phi(\operatorname{Torc} M_1) \subset \operatorname{Torc} M_2$.

Se ϕ é mono e $\mathbf{w} = \phi(\mathbf{v})$, $a\mathbf{w} = 0$, então

$$a\mathbf{w} = \phi(a\mathbf{v}) = 0 \Rightarrow a\mathbf{v} = 0 \Rightarrow \mathbf{v} \in \operatorname{Torc} M_1.$$

Se ϕ é epi e $\ker\phi \subset \operatorname{Torc} M_1$, e $\mathbf{w} \in \operatorname{Torc} M_2$ é *t.q.* $a\mathbf{w} = 0$ e $\mathbf{w} = \phi(\mathbf{v})$, então:

$$\begin{aligned}\phi(a\mathbf{v}) = 0 &\Rightarrow a\mathbf{v} \in \operatorname{Torc} M_1\\ &\Rightarrow \exists_{a' \in D - \{0\}} : a'a\mathbf{v} = 0\\ &\Rightarrow \mathbf{v} \in \operatorname{Torc} M_1 \quad (\text{pois } a'a \neq 0).\end{aligned}$$

(b) Como $\pi\colon M \to M/\operatorname{Torc} M$ é epi e $\ker\pi = \operatorname{Torc} M$, temos, por (a),

$$\operatorname{Torc}\left(\frac{M}{\operatorname{Torc} M}\right) = \pi(\operatorname{Torc} M) = \{0\}.$$

(c) Segue directamente da definição de Torc e da soma directa. □

Definição 4.7.8. *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*

$$M_K := K \otimes_D M \in \operatorname{Vect}_K.$$

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 4.7.9. 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 4.7.10. *Seja $M \in \operatorname{Mod}_D$. Então*

(a) $K \otimes_D \operatorname{Torc} M = 0$;

(b) $K \otimes_D (M/\operatorname{Torc} M) \cong K \otimes_D M$;

(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 $\pi : M \to M/\operatorname{Torc} M$ a projecção canónica e $i : \operatorname{Torc} M \to M$ a inclusão. Então

$$0 \longrightarrow \operatorname{Torc} M \xrightarrow{i} M \xrightarrow{\pi} M/\operatorname{Torc} M \longrightarrow 0$$

é uma sucessão exacta, logo

$$K \otimes_D \operatorname{Torc} M \xrightarrow{Id \otimes i} K \otimes_D M \xrightarrow{Id \otimes \pi} K \otimes_D (M/\operatorname{Torc} M) \longrightarrow 0$$

também é uma sucessão exacta de módulos-D, pelo Teorema 4.6.1. Como $K \otimes_D \operatorname{Torc} M = 0$, por (a), concluimos que $Id \otimes \pi$ é um isomosfismo de módulos-D.

(c) Seja $i : N \to M$ a inclusão. Então $\alpha = Id \otimes i : K \otimes_D N \to K \otimes_D M$ 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

$$\beta'(x, m) = \frac{x}{a} \otimes am$$

onde $a \in D \setminus \{0\}$ é tal que $am \in N$ – existe um elemensto a nestas condições pois M/N é um módulo de torção. Verifique que $\beta'(x, m)$ 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 $\beta(x \otimes m) = \beta'(x, m)$. Temos que $\alpha \circ \beta = Id_{K \otimes_D M}$ e $\beta \circ \alpha = Id_{K \otimes_D N}$, donde concluimos que α é um isomorfismo. $\square$

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 4.7.11. *Seja $M \in \operatorname{Mod}_D$ e seja $\phi = \phi_{K,M} : M \to M_K$. 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) $\ker \phi = \operatorname{Torc} M$.

Demonstração. (a)

$$\begin{aligned}\mathbf{w} = \sum_{i=1}^{n} \frac{a_i}{b_i} \otimes \mathbf{v}_i &= \frac{1}{b_1 \cdots b_n} \sum_{i=1}^{n} \Big(a_i \prod_{j \neq i} b_j \Big) \otimes \mathbf{v}_i \\ &= \frac{1}{b_1 \cdots b_n} \sum_{i=1}^{n} 1 \otimes \Big(\Big(a_i \prod_{j \neq i} b_j \Big) \mathbf{v}_i \Big) \in \frac{1}{b_1 \cdots b_n} \phi(M) \\ &= \frac{1}{b_1 \cdots b_n} 1 \otimes \Big(\sum_{i=1}^{n} \Big(a_i \prod_{j \neq i} b_j \Big) \mathbf{v}_i \Big) \in \frac{1}{b_1 \cdots b_n} \phi(M).\end{aligned}$$

(b) A inclusão $\operatorname{Torc} M \subset \ker \phi$ é óbvia: se $b \in D - \{0\}$ 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 4.7.12. □

Exercício 4.7.12. *Seja D um domínio integral com corpo de fracções $K = \operatorname{Frac}(D)$ e seja M um módulo-D. Seja N o quociente de $M \times (D - \{0\})$ pela seguinte relação de equivalência:*

$$(\mathbf{v}, d) \sim (\mathbf{v}', d') \Leftrightarrow \exists\, d'' \in D - \{0\} : d''(d\mathbf{v}' - d'\mathbf{v}) = 0.$$

Designando a classe de equivalência de $(\mathbf{v}, d)$ por $[\mathbf{v}, d]$, definem-se as seguintes operações $N \times N \to N$ e $K \times N \to N$:

$$\begin{gathered}[\mathbf{v}_1, d_1] + [\mathbf{v}_2, d_2] := [d_2\mathbf{v}_1 + d_1\mathbf{v}_2, d_1 d_2]; \\ \tfrac{a}{b}[\mathbf{v}_1, d_1] := [a\mathbf{v}_1, bd_1];\end{gathered}$$

onde $\mathbf{v}_i \in M, d_i \in D - \{0\}, a/b \in K$.

(a) Mostre que as operações acima estão bem definidas e definem uma estrutura de espaço vectorial sobre K em N;

(b) Mostre que o núcleo do homomorfismo-D $\varphi\colon M \to N$ definido por $\varphi(\mathbf{v}) = [\mathbf{v}, 1]$ é $\operatorname{Torc} M$;

(c) Mostre que existe um isomorfismo $N \to K \otimes_D M$ que transforma φ no homomorfismo $\phi = \phi_{K,M}\colon M \to K \otimes_D M; \mathbf{v} \to 1 \otimes \mathbf{v}$. Conclua que $\ker \phi = \operatorname{Torc} M$.

Definição 4.7.13. *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* $\operatorname{rank} M := \dim_K M_K$.

Observação 4.7.14. Se M é finitamente gerado, então M tem característica finita, pois $\dim_K \langle \phi(S) \rangle \leq |S|$.

Exemplos 4.7.15. 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: $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ (exercício). No entanto, $\mathbb{Q}$ não é finitamente gerado como grupo abeliano.

Lema 4.7.16. *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 $\psi\colon \oplus_{i \in I} D \to M; \psi\left((a_i)_{i \in I}\right) = \sum_{i \in I} a_i \mathbf{e}_i$. 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* $\phi\psi$ é mono:

$$\sum_i \frac{a_i}{b_i}(1 \otimes \mathbf{e}_i)) = 0 \Leftrightarrow \frac{1}{b} \sum_i a_i'(1 \otimes \mathbf{e}_i) = 0 \Leftrightarrow \frac{1}{b}\, \phi\psi\left((a_i')_{i \in I}\right) = 0,$$

   onde $b = b_1 \cdots b_n$ e $a_i' = a_i \prod_{j \neq i} b_j$.

2. $\phi\psi$ é mono *sse*:

$$\begin{aligned} & \psi \text{ é mono} \wedge \Big(\operatorname{im} \psi \cap \underbrace{\ker \phi}_{\operatorname{Torc} M} = \{0\}\Big) \\ \Leftrightarrow \quad & \psi \text{ é mono} \wedge \Big(\operatorname{Torc}\Big(\bigoplus_{i \in I} D\Big) = \{0\}\Big) \\ \Leftrightarrow \quad & \psi \text{ é mono} \\ \Leftrightarrow \quad & \{\mathbf{e}_i\}_{i \in I} \text{ é } \textit{l.i.} \end{aligned}$$

   onde $\ker \phi = \operatorname{Torc} M$ pela Proposição 4.7.11. □

4.8 24ª Aula

4.8.1 Módulos sobre um *d.i.p.*

No que se segue D é um *d.i.p.*.

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 (resp. linhas) a'_i e a'_j [1] *t.q.* $a'_{1i} = mdc(a_{1i}, a_{1j})$ e $a'_{1j} = 0$ (resp. $a'_{i1} = mdc(a_{i1}, a_{j1})$ e $a'_{j1} = 0$). [2]

Para mostrar que é possível efectuar a operação (iv), basta considerar o caso ilustrado no exemplo seguinte.

Exemplo 4.8.1. Sejam $A = \begin{bmatrix} a & b \end{bmatrix}$, $d = mdc(a, b)$, 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 4.8.2. *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 $d \in D^\times$.*

[1] obtidas por combinação linear de a_i e a_j

[2] as restantes colunas (linhas) permanecem inalteradas.

Observação 4.8.3. Se $a, d \in D$ são *t.q.* $d \mid a$ e $a \nsim d$, então $\delta(d) < \delta(a)$.

Exemplo 4.8.4. 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

$$Q = \begin{bmatrix} -1 & 3 \\ 1 & 2 \end{bmatrix} \qquad \text{e} \qquad B := AQ = \begin{bmatrix} 2 & 0 \\ 7 & 8 \end{bmatrix} .$$

Aplicando agora a operação (iv) às linhas de B, temos que

$$d = 1 \ , \quad a' = a/d = 2 \ , \quad b' = b/d = 7 \ , \quad (-3)2 + 7 = 1 \Rightarrow r = -1 \text{ e } s = 1$$

donde

$$P = \begin{bmatrix} r & s \\ -b' & a' \end{bmatrix} = \begin{bmatrix} -3 & 1 \\ -7 & 2 \end{bmatrix} \qquad \text{e} \qquad PB := PAQ = \begin{bmatrix} 1 & 8 \\ 0 & 16 \end{bmatrix} .$$

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 $\delta(4) = 2 > \delta(2) = 1 > \delta(1) = 0$.

Proposição 4.8.5. *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* $(\delta_{ti}\delta_{si})_{1\leq t\leq m, 1\leq s\leq n}$ *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

$$\begin{bmatrix} d_1^1 & 0 & \cdots & 0 \\ 0 & d_2^1 & 0 & \cdots \\ \vdots & 0 & \ddots & \end{bmatrix} = \operatorname{diag}(d_1^1, \ldots, d_r^1) ,$$

onde as entradas nulas d_i^1, se as houver, aparecem no fim da lista – consequência do Passo 1.

Uma vez que $a0 = 0$ para todo o $a \in D$, por convenção[3], vamos escrever $a \mid 0$ e, em particular, $0 \mid 0$.

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[4]:

$$\begin{bmatrix} d_1^1 & 0 & \cdots & 0 \\ 0 & d_2^1 & 0 & \cdots \\ \vdots & 0 & \ddots & \end{bmatrix} \xrightarrow{(iii)} \begin{bmatrix} d_1^1 & d_2^1 & \cdots & 0 \\ 0 & d_2^1 & 0 & \cdots \\ \vdots & 0 & \ddots & \end{bmatrix} \xrightarrow{(iv)+(iii)} \begin{bmatrix} d_1^2 & 0 & \cdots & 0 \\ 0 & d_2^2 & 0 & \cdots \\ \vdots & 0 & \ddots & \end{bmatrix}$$

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 $d_1^3 \mid d_3^3$.

[3] Anteriormente, apenas se definiu o símbolo $a \mid b$ num anel comutativo A para $a, b \in A \setminus \{0\}$. Atenção: Não confundir a notação $a|0$ com a noção de divisor de zero no anel A.

[4] Faça os passos intermédios e determine expressões para d_1^2 e d_2^2 à custa de d_1^1 e d_2^2. Essas expressões vão permitir justificar que $d_1^2 \mid d_2^2$ e todas as relações de divisibilidade no resto desta demonstração.

Prosseguindo, obtemos uma matriz $\operatorname{diag}(d_1^r, \dots, d_r^r)$ *t.q.* $d_1^r \mid d_i^r$, para todo o i. Definimos $d_1 := d_1^r$. 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 $\operatorname{diag}(d_1, \dots, d_r)$ *t.q.* $d_1 \mid d_2 \mid \cdots \mid d_r$. $\square$

Definição 4.8.6. *Seja $A \in M_{m\times n}(D)$ e seja* $\operatorname{diag}(d_1, \dots, d_r)$ *uma matriz obtida por diagonalização de A, como acima, diz-se que $d_1, \dots, d_r$ 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.

Corolário 4.8.7. *Seja $f \in \hom_D(D^n, D^m)$. 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 $\hom_D(D^n, D^m) \cong M_{m\times n}(D^{op})$. 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 4.8.5 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 $\mathcal{B}, \mathcal{B}'$ o homomorfismo f é representado por PAQ. $\square$

Exemplo 4.8.8. Pretendemos diagonalizar a matriz

$$\begin{bmatrix} 2 & -1 \\ 1 & 2 \\ 1 & 1 \end{bmatrix} \in M_{3\times 2}(\mathbb{Z}),$$

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 4.8.5 são:

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -5 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 3 & -5 \end{bmatrix}$$

$$Q = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}.$$

Obtivemos assim uma matriz diagonal

$$PAQ = \begin{bmatrix} 1 & 0 \\ 0 & -1 \\ 0 & 0 \end{bmatrix},$$

equivalente a A.

Exemplo 4.8.9. Pretendemos diagonalizar a matriz

$$\begin{bmatrix} (t-2)(t-1) & t-2 \\ (t-1)^3 & (t-2)(t-1) \end{bmatrix} \in M_2(\mathbb{R}[t]),$$

o que pode ser conseguido realizando a seguinte sequência de operações elementares:

$$\begin{bmatrix} (t-2)(t-1) & t-2 \\ (t-1)^3 & (t-2)(t-1) \end{bmatrix} \xrightarrow{C2 \leftrightarrow C1} \begin{bmatrix} t-2 & (t-2)(t-1) \\ (t-2)(t-1) & (t-1)^3 \end{bmatrix}$$

$$\xrightarrow{L2-(t-1)L1} \begin{bmatrix} t-2 & (t-2)(t-1) \\ 0 & (t-1)^2 \end{bmatrix} \xrightarrow{C2-(t-1)C1} \begin{bmatrix} t-2 & 0 \\ 0 & (t-1)^2 \end{bmatrix}$$

$$\xrightarrow{L1+L2} \begin{bmatrix} t-2 & (t-1)^2 \\ 0 & (t-1)^2 \end{bmatrix} \xrightarrow{C2-tC1} \begin{bmatrix} t-2 & 1 \\ 0 & (t-1)^2 \end{bmatrix} \xrightarrow{C1 \leftrightarrow C2} \begin{bmatrix} 1 & t-2 \\ (t-1)^2 & 0 \end{bmatrix}$$

$$\xrightarrow{L2-(t-1)^2 L1} \begin{bmatrix} 1 & t-2 \\ 0 & -(t-2)(t-1)^2 \end{bmatrix} \xrightarrow{C2-(t-2)C1} \begin{bmatrix} 1 & 0 \\ 0 & -(t-2)(t-1)^2 \end{bmatrix}.$$

Teorema 4.8.10. *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 $\pi_i : D^n \to D$ a i-ésima projecção e seja $p_i := \pi_i|_M$. 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
$$0 \to \ker p_n \to M \to \operatorname{im} p_n \to 0 \tag{4.8.1}$$
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 (4.8.1) 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. $\square$

Exercício 4.8.11. *Demonstre o Teorema 4.8.10 no caso geral.*

Corolário 4.8.12. *Seja $M \in \mathrm{Mod}_D$ finitamente gerado. Então existe uma sucessão exacta curta da seguinte forma:*
$$0 \to D^n \xrightarrow{f} D^m \xrightarrow{g} M \to 0.$$

Demonstração. Seja $g : D^m \to M$ um epimorfismo. Temos $\ker g \subset D^m$, logo $\ker g \cong D^n$ para algum n. $\square$

Definição 4.8.13. *Seja $g : D^m \to M$ 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 4.8.12 garante a existência de uma apresentação livre (*i.e.*, *t.q.* $\ker g$ é livre).

4.9 25ª Aula

4.9.1 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 4.9.1. *Sejam A um anel, $M \in \mathrm{Mod}_A$ e seja $\mathbf{v} \in M$. Define-se*

$$\mathrm{ann}(\mathbf{v}) \coloneqq \{a \in A \mid a\mathbf{v} = 0\}.$$

Então $\mathrm{ann}(\mathbf{v}) \subset A$ *é um ideal esquerdo* t.q. $A/\mathrm{ann}(\mathbf{v}) \cong \langle \mathbf{v} \rangle$.

Teorema 4.9.2. *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.* $d_1 \mid d_2 \mid \cdots \mid d_n$ (Proposição 4.8.5) 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.

$$\begin{aligned}
\mathbf{v} \in \langle \mathbf{v}_i \rangle \cap \sum_{j\neq i} \langle \mathbf{v}_j \rangle &\Leftrightarrow \exists_{a_1,\ldots,a_m} : \mathbf{v} = a_i\mathbf{v}_i = \sum_{j\neq i} a_j \mathbf{v}_j \\
&\Rightarrow a_i\mathbf{v}_i - \sum_{i\neq j} a_j\mathbf{v}_j \in \operatorname{im}(f) \\
&\Rightarrow a_i \in \operatorname{ann}(v_i) \Rightarrow v = a_i\mathbf{v}_i = 0.
\end{aligned}$$

Resta apenas mostrar a unicidade de $(d_1), \ldots, (d_m)$, o que faremos mais adiante. □

Corolário 4.9.3. *Seja $M \in \operatorname{Mod}_D$ finitamente gerado. Então*

$$M = \operatorname{Torc} M \oplus L,$$

onde L é livre e $\dim L = \operatorname{rank} M$. Em particular, M é livre sse *M é livre de torção. Mais precisamente, temos*

$$M \cong \Big(\bigoplus_{i=1}^{n} D/(d_i)\Big) \oplus D^k, \tag{4.9.1}$$

t.q. $d_1 \mid d_2 \mid \cdots \mid d_n \neq 0$ *e* $k = \operatorname{rank} M$.

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

$$\operatorname{Torc} M = \bigoplus_{i=1}^{s} \operatorname{Torc}(D/(d_i)) = \bigoplus_{i=1}^{s} D/(d_i).$$

Seja $L = \bigoplus_{i=s+1}^m D/(d_i) = \bigoplus_{i=s+1}^m D$. Temos

$$M = \operatorname{Torc} M \oplus L,$$

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 4.9.4. A condição de M ser finitamente gerado não pode ser removida: se $D = \mathbb{Z}$ e $M = \mathbb{Q}$, temos $\operatorname{Torc} M = \{0\}$, mas M não é livre como módulo-$\mathbb{Z}$.

Exemplo 4.9.5. 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 $k \geq 0$.

Definição 4.9.6. *Diz-se que* (4.9.1) *é a decomposição em* factores cíclicos invariantes*. Os elementos d_i da decomposição* (4.9.1) *dizem-se* factores invariantes *de M.*

Observação 4.9.7. Os factores invariantes estão determinados a menos de multiplicação por unidades (ou em alternativa, os ideais correspondentes, (d_i), estão unicamente determinados).

Corolário 4.9.8. *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 4.9.9. Diz-se que os divisores invariantes e a característica constituem um conjunto *completo* de invariantes dos módulos-D de tipo finito.

4.9.2 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 2.2.20:

$$D/(d) \cong D/(p_1^{m_1}) \oplus \cdots \oplus D/(p_r^{m_r}).$$

Definição 4.9.10. *Um módulo-D da forma $D/(p^m)$, com $p \in D$ primo, diz-se um módulo* cíclico primário*.*

Teorema 4.9.11 (Decomposição em factores cíclicos primários)**.** *Seja M um módulo-D de tipo finito. Então*

$$M \cong D/(p_1^{m_1}) \oplus \cdots \oplus D/(p_s^{m_s}) \oplus L, \tag{4.9.2}$$

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 (4.9.1) 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 4.9.12. *Diz-se que* (4.9.2) *é a decomposição* cíclica primária *de* M*. Os elementos* $p_i^{m_i} \in D$ *dizem-se* divisores elementares *de* M*.*

Corolário 4.9.13. *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 4.9.14. Diz-se que os divisores elementares e a característica constituem um conjunto *completo* de invariantes dos módulos-D de tipo finito.

Exemplo 4.9.15. 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.

4.9.3 Relação entre divisores invariantes e elementares

Descrevemos de seguida um algoritmo para determinar os divisores invariantes a partir dos divisores elementares: sejam $p_1, \dots, p_s \in D$ primos não associados representantes das classes (para a relação de associado) que surgem na decomposição (4.9.2). Ordenamos as potências dos p_i que ocorrem em (4.9.2) da seguinte forma

$$\begin{array}{ccc} p_1^{m_{11}} & \cdots & p_s^{m_{1s}} \\ \vdots & & \vdots \\ p_1^{m_{t1}} & \cdots & p_s^{m_{ts}} \end{array}$$

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 4.9.16. 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

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \Rightarrow \begin{cases} d_1 = 2^1 \cdot 3^0 = 2 \\ d_2 = 2^2 \cdot 3^1 = 12 \end{cases}.$$

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.

4.9.4 Unicidade da decomposição em factores cíclicos primários

Definição 4.9.17. *Seja $M \in \mathrm{Mod}_D$ de tipo finito 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 4.9.18. 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).

Exercício 4.9.19. *Seja $M = \bigoplus_{i\in I} M_i$. Mostre que $M(p) = \bigoplus_{i\in I} M_i(p)$.*

Exemplo 4.9.20. 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. Então, dado um primo $p \in D$, temos

$$M(p) = \bigoplus_{\{i|p_i \sim p\}} D/(p_i^{m_i}) \ .$$

(*cf.* [Hun74, Exercício IV.6.3] (Ficha 10)).

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 4.9.21. *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 $t \in \mathbb{N}_0$, pelo Exercício IV.6.3 de Hungerford (Ficha 10), temos

$$p^t\left(D/(p^m)\right) \cong \begin{cases} D/(p^{m-t}), & t < m \\ 0, & t \geq m \end{cases}$$

e daí segue

$$\frac{p^t\left(D/(p^m)\right)}{p^{t+1}\left(D/(p^m)\right)} \cong \begin{cases} D/(p), & t < m \\ 0, & t \geq m \end{cases} .$$

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

$$\forall_t \quad \frac{p^t M}{p^{t+1} M} \cong \bigoplus_{\{i \mid m_i > t\}} D/(p) \cong \bigoplus_{\{i \mid n_i > t\}} D/(p),$$

logo

$$\forall_t \quad \#\{i \mid m_i > t\} = \#\{i \mid n_i > t\},$$

donde

$$r = s \quad \wedge \quad n_i = m_i, \; i = 1, \ldots, r.$$ □

Exemplo 4.9.22. Vejamos que $p^t \mathbb{Z}_{p^m} / p^{t+1} \mathbb{Z}_{p^m} \cong \mathbb{Z}_p$ para todo $t < m$. Note-se que

$$\frac{p^t \mathbb{Z} / p^m \mathbb{Z}}{p^{t+1} \mathbb{Z} / p^m \mathbb{Z}} \cong \frac{p^t \mathbb{Z}}{p^{t+1} \mathbb{Z}}.$$

Seja $\pi \colon p^t \mathbb{Z} \to p^t \mathbb{Z} / p^{t+1} \mathbb{Z}$ a projecção. Consideremos o homomorfismo

$$\varphi \colon \frac{\mathbb{Z}}{p\mathbb{Z}} \to \frac{p^t \mathbb{Z}}{p^{t+1} \mathbb{Z}} \; ; \quad \underline{n} \mapsto \pi(p^t n).$$

Por construção φ é epi. Temos

$$\varphi(\underline{n}) = 0 \Leftrightarrow n p^t \equiv 0 \mod p^{t+1} \Leftrightarrow n \equiv 0 \mod p.$$

Concluímos que φ é um isomorfismo.

4.10 26ª Aula

4.10.1 Formas canónicas racionais

Seja k um corpo e seja V um espaço vectorial-k de *dimensão finita*. Recorde-se que existe uma bijecção

$$\boxed{\hom_k(V,V) \leftrightarrow \text{estruturas de módulo-}k[x]\text{ em } V,}$$

que é obtida da seguinte forma: dada $T \in \hom_k(V,V)$, a respectiva estrutura de módulo-$k[x]$ é definida por

$$\Big(\sum_i a_i x^i\Big) \cdot \mathbf{v} := \sum_i a_i T^i \mathbf{v}, \qquad \forall_{\sum_i a_i x^i \in k[x]}, \forall_{\mathbf{v}\in V}.$$

A correspondência inversa envia uma estrutura de módulo-$k[x]$ em V na transformação linear $T\colon V \to V$ dada por

$$T\mathbf{v} := x \cdot \mathbf{v}, \qquad \forall \mathbf{v} \in V.$$

Consideremos agora fixada a estrutura de módulo-$k[x]$ em V associada à transformação $T \in \hom_k(V,V)$. Dado um subespaço-k $W \subset V$, temos

$$\boxed{W \subset V \text{ é um submódulo-}k[x] \textit{ sse } W \text{ é um subespaço invariante para } T}$$

Exercício 4.10.1. *Nas condições acima, sejam $V_i \subset V$, $i = 1, \ldots, r$, subespaços-k. Mostre que*

$$V = V_1 \oplus \cdots \oplus V_r \textit{ em } \mathrm{Mod}_{k[x]}$$

sse $V_1 \oplus \cdots \oplus V_r$ *em* Vect_k *e V_i é um espaço invariante para T, $i = 1, \ldots, r$.*

Lema 4.10.2. *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 $\operatorname{ann}(f) \subset k[x]$. Sem perda de generalidade, podemos supôr 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. $\square$

Sejam $\mathbf{v}$, f como na demonstração do lema anterior: $f = x^m + \sum_{i=0}^{m-1} a_i x^i$. Seja $\mathbf{w}_i := T^i\mathbf{v}$, $i = 0, \ldots, m-1$. 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

$$R = \begin{bmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & -a_{m-1} \end{bmatrix} \tag{4.10.1}$$

Corolário 4.10.3. *Seja V um espaço-k de dimensão finita e seja $T \in \hom_k(V,V)$. 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

$$R = \begin{bmatrix} R_1 & \cdots & 0 \\ & \ddots & \\ 0 & \cdots & R_s \end{bmatrix} \tag{4.10.2}$$

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* (4.10.1). *Se $m_i = 1$, R_i é uma matriz 1×1, $R_i = [-a_{0,i}]$.*

Uma matriz da forma (4.10.2) *diz-se uma* forma racional *para T.*

Observação 4.10.4. No Corolário 4.10.3, temos

$$\operatorname{ann}(\mathbf{v}_i) = (a_{0,i} + a_{1,i}x + \cdots + a_{m_i-1,i}x^{m_i-1} + x^m).$$

Observação 4.10.5. 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 4.10.6. 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 $v = (x_1, x_2, x_3, x_4) \in \mathbb{R}^4$. 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:

$$\begin{bmatrix} 0 & 0 & 0 & 4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{ou} \quad \begin{bmatrix} 0 & 2 & & \\ 1 & 0 & & \\ & & 0 & -2 \\ & & 1 & 0 \end{bmatrix} \quad \text{ou} \quad \begin{bmatrix} \sqrt{2} & & & \\ & \sqrt{-2} & & \\ & & 0 & -2 \\ & & 1 & 0 \end{bmatrix}.$$

4.10.2 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 espaço vectoriais-k. Portanto,

$$\varphi_{\mathbf{v}}\left(\mathcal{B}_{\lambda,m}\right) = \left\{\mathbf{v}, (T-\lambda)\mathbf{v}, \dots, (T-\lambda)^{m-1}\mathbf{v}\right\}$$

é uma base para W como espaço-k. Defina-se

$$\mathbf{w}_i \coloneqq (T-\lambda)^{m-i}\mathbf{v}, \qquad i = 1, \dots, m.$$

Temos

$$\begin{aligned} T\mathbf{w}_i &= (T-\lambda)\mathbf{w}_i + \lambda\mathbf{w}_i = \underbrace{(T-\lambda)^{m-(i-1)}\mathbf{v}}_{\mathbf{w}_{i-1}} + \underbrace{\lambda(T-\lambda)^{m-i}\mathbf{v}}_{\lambda\mathbf{w}_i} \\ &= \begin{cases} \mathbf{w}_{i-1} + \lambda\mathbf{w}_i, & i = 2, \dots, m \\ \lambda\mathbf{w}_1, & i = 1. \end{cases} \end{aligned}$$

Concluímos que $\{\mathbf{w}_1, \dots, \mathbf{w}_m\}$ 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 4.10.7. *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. *$V = \oplus_{i=1}^s V_i$, 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.*

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 $g := \dim \ker(T - \lambda)$ 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 $E_i := \ker(T - \lambda)^i$ e $r_i := \dim E_i$, para $i = 1, \ldots, M$. Então

$$g = r_1 < r_2 < \cdots < r_M = a \ .$$

Defina-se

$$\begin{cases} s_1 & = r_1 \\ s_2 & = r_2 - r_1 \\ & \vdots \\ s_M & = r_M - r_{M-1} \end{cases} \qquad \text{e} \qquad \begin{cases} t_1 & = s_1 - s_2 \\ & \vdots \\ t_{M-1} & = s_{M-1} - s_M \\ t_M & = s_M \end{cases} .$$

Então t_i é o número[5] 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.

[5]E s_i é o número de blocos de Jordan com dimensão pelo menos i.

4. Seja $N_1 := \operatorname{im}(T-\lambda)^{m_1-1} \cap \ker(T-\lambda) \neq \{0\}$. Determinar uma base $\mathcal{B}_1$ para N_1. Para cada elemento de $\mathbf{w} \in \mathcal{B}_1$ resolver iterativamente as equações

$$\begin{aligned} \mathbf{w}_1 &= \mathbf{w} \\ (T-\lambda)\mathbf{w}_2 &= \mathbf{w}_1 \\ (T-\lambda)\mathbf{w}_3 &= \mathbf{w}_2 \\ &\vdots \\ (T-\lambda)\mathbf{w}_{m_1} &= \mathbf{w}_{m_1-1} \end{aligned} \tag{$*$}$$

   O conjunto $\{\mathbf{w}_i \mid i = 1, \dots, m_1\}$ 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 $N_2 := \operatorname{im}(T-\lambda)^{m_2-1} \cap \ker(T-\lambda) \supsetneq N_1$. 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.

Exemplo 4.10.8. 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 $E_1 := \ker(A-2) = \langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_5, \mathbf{e}_7 \rangle$, então

$$N_1 := \operatorname{im}(A-2)^{m_1-1} \cap E_1 = \langle \mathbf{e}_7 \rangle \cap E_1 = \langle \mathbf{e}_7 \rangle \ .$$

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

$$N_2 := \operatorname{im}(A-2) \cap E_1 = \langle \mathbf{e}_3, \mathbf{e}_5, \mathbf{e}_7, \mathbf{e}_8, \mathbf{e}_9 \rangle \cap E_1 = \langle \mathbf{e}_3, \mathbf{e}_5, \mathbf{e}_7 \rangle \ .$$

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 $\mathbf{u}_1 = \mathbf{u}$:

$$(A-2)\mathbf{u}_2 = \mathbf{u}_1 \quad \Leftrightarrow \mathbf{u}_2 \in \mathbf{e}_4 + \mathbf{e}_6 + E_1, \quad \text{seja } \mathbf{u}_2 = \mathbf{e}_4 + \mathbf{e}_6 + 3\mathbf{e}_3 + 2\mathbf{e}_7.$$

Cálculo de um vector próprio generalizado para $\mathbf{v}_1 = \mathbf{v}$:

$$(A-2)\mathbf{v}_2 = \mathbf{v}_1 \quad \Leftrightarrow \mathbf{v}_2 \in \mathbf{e}_6 - \mathbf{e}_4 + 6\mathbf{e}_8 + E_1, \quad \text{seja } \mathbf{v}_2 = \mathbf{e}_6 - \mathbf{e}_4 + 6\mathbf{e}_8 - \mathbf{e}_1.$$

Passo 6: Fazemos mais uma iteração do Passo 4 com $m_3 = 1$:

$$N_3 := \operatorname{im}(A-2)^0 \cap E_1 = E_1$$

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[6]

$$J = P^{-1}AP = \begin{bmatrix} J_4 & & & & \\ & J_2 & & & \\ & & J_2 & & \\ & & & 2 & \\ & & & & 2 \end{bmatrix},$$

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 4.10.9. Calcular a forma canónica de Jordan de

$$A = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 0 & 1 \\ 2 & -4 & 4 \end{bmatrix} \in M_3(\mathbb{C})$$

[6]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 $\mathcal{B}$.

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:

$$A - 2I = \begin{bmatrix} 0 & 0 & 0 \\ 1 & -2 & 1 \\ 2 & -4 & 2 \end{bmatrix} \to \begin{bmatrix} 0 & 0 & 0 \\ 1 & -2 & 1 \\ 0 & 0 & 0 \end{bmatrix} , \tag{4.10.3}$$

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 (4.10.3), temos $\mathrm{im}(A - 2I) = \langle (0, 1, 2) \rangle \subset E_1$, logo $N_1 = \mathrm{im}(A - 2I)$ 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 $\mathbf{w}_2 = (1, 0, 0)$.

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 $\mathbf{v} := (-1, 0, 1)$.

Obtemos então a seguinte matriz mudança de base

$$P := \begin{bmatrix} | & | & | \\ \mathbf{w}_1 & \mathbf{w}_2 & \mathbf{v} \\ | & | & | \end{bmatrix} = \begin{bmatrix} 0 & 1 & -1 \\ 1 & 0 & 0 \\ 2 & 0 & 1 \end{bmatrix} ,$$

a que corresponde a forma canónica de Jordan

$$J = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} .$$

Método para calcular a forma canónica de Jordan sem a base correspondente

Suponhamos que $T \in \hom_k(k^n, k^n)$ 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

$$f\colon\ (k[x])^m \to (k[x])^n \quad t.q. \quad k^n \cong (k[x])^n \,/\, \mathrm{im}(f)$$

e diagonalizar a matriz que representa f – ver Corolário 4.8.12 e início da demonstração do Teorema 4.9.2.

Ora,

$$\begin{aligned} k^n &\cong k[x] \otimes_{k[x]} k^n \cong k[x] \otimes_k k^n / \langle \{x \otimes \mathbf{v} - 1 \otimes T\mathbf{v} \mid \mathbf{v} \in k^n\} \rangle \\ &= k[x] \otimes_k k^n / \langle \{x \otimes \mathbf{e}_i - 1 \otimes T\mathbf{e}_i \mid i = 1, \ldots, n\} \rangle \\ &\cong (k[x])^n / \langle \{x\mathbf{e}_i - T\mathbf{e}_i \mid i = 1, \ldots, n\} \rangle = (k[x])^n \,/\, \mathrm{im}(f), \end{aligned}$$

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 4.10.10. 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 $\mathbb{C}[x]$:

$$\begin{aligned}\mathbb{C}^3 &\cong \mathbb{C}[x]/(1) \oplus \mathbb{C}[x]/(x-2) \oplus \mathbb{C}[x]/\big((x-2)^2\big)\\ &\cong \mathbb{C}[x]/(x-2) \oplus \mathbb{C}[x]/\big((x-2)^2\big).\end{aligned}$$

Portanto, a forma canónica de Jordan de A é:

$$J = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}.$$

4.11 27ª Aula

4.11.1 Aplicações das formas canónicas e dos factores invariantes e elementares

Recorde que um grupo G age à esquerda em si próprio por conjugação (Exemplo 1.4.8). 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

$$k^n \cong \frac{k[x]}{(d_1(x))} \oplus \cdots \oplus \frac{k[x]}{(d_n(x))} \ , \tag{4.11.1}$$

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

$$\deg(d_1(x)) + \cdots + \deg(d_n(x)) = n \tag{4.11.2}$$

e, portanto, basta considerar as várias possibilidades para cada $d_i(x) \in k[x]$, tendo em conta as suas factorizações[7] em polinómios irredutíveis em $k[x]$.

Exemplo 4.11.1. 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 (4.11.2), 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

$$\begin{bmatrix} \lambda & \\ & \lambda \end{bmatrix} \ , \quad \begin{bmatrix} \lambda & 1 \\ & \lambda \end{bmatrix} \ , \quad \begin{bmatrix} \lambda & \\ & \mu \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 0 & -a_0 \\ 1 & -a_1 \end{bmatrix} \ , \tag{4.11.3}$$

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

[7] únicas pois $k[x]$ é um d.i.p., logo um d.f.u.

que as matrizes em (4.11.3) não são conjugadas entre si, pois correspondem a estruturas distintas de k^2 como módulo-$k[x]$, i.e., a decomposições (4.11.1) distintas.

Exemplo 4.11.2. 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 $x^2 - a_1x - a_0 \in \mathbb{Z}_p[x]$, 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:

$$\begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} 2 & \\ & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ & 2 \end{bmatrix}, \begin{bmatrix} 1 & \\ & 2 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \text{ e } \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Exercício 4.11.3. *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.

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

$$\mathcal{B}_M = \{\underline{1}, \underline{x}, \dots, \underline{x}^{m-1}\}$$

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 $x\mathbf{v} := T(\mathbf{v})$. 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

$$\mathcal{B}_N = \{\underline{1}, \underline{x}, \dots, \underline{x}^{n-1}\}$$

é uma base-k de N então, pelo Corolário 4.5.18,

$$\mathcal{B}_N \otimes \mathcal{B}_M := \{\underline{x}^i \otimes \underline{x}^j \mid i = 0, \ldots, m-i,\ j = 0, \ldots, n-1\}$$

é uma base-k de V.

Exemplo 4.11.4. 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

$$T(\underline{a(x)} \otimes \underline{b(x)}) = \underline{xa(x)} \otimes \underline{xb(x)} \qquad \text{i.e.} \quad x(\underline{a(x)} \otimes \underline{b(x)}) := \underline{xa(x)} \otimes \underline{xb(x)}\ .$$

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 $x - A$:

$$x - A = \begin{bmatrix} x & 0 & 0 & -6 \\ 0 & x & -3 & -6 \\ 0 & -2 & x & 0 \\ -1 & -2 & 0 & x \end{bmatrix} \xrightarrow[L_2 \leftrightarrow L_3]{L_1 \leftrightarrow L_4} \begin{bmatrix} -1 & -2 & 0 & x \\ 0 & -2 & x & 0 \\ 0 & x & -3 & -6 \\ x & 0 & 0 & -6 \end{bmatrix}$$

$$\xrightarrow[L_3 - \frac{x}{2} L_2]{L_4 + xL_1} \begin{bmatrix} -1 & -2 & 0 & x \\ 0 & -2 & x & 0 \\ 0 & 0 & \frac{x^2}{2} - 3 & -6 \\ 0 & -2x & 0 & x^2 - 6 \end{bmatrix} \xrightarrow[C_4 + xC_1]{C_2 - 2C_1} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & x & 0 \\ 0 & 0 & \frac{x^2}{2} - 3 & -6 \\ 0 & -2x & 0 & x^2 - 6 \end{bmatrix}$$

$$\xrightarrow[L_4 - xL_2]{2L_3} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & x & 0 \\ 0 & 0 & x^2 - 6 & -12 \\ 0 & 0 & -x^2 & x^2 - 6 \end{bmatrix} \xrightarrow[L_4 + \frac{x^2 - 6}{12} L_3]{C_3 + \frac{1}{2} C_2} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & x^2 - 6 & -12 \\ 0 & 0 & -x^2 + \frac{(x^2 - 6)^2}{12} & 0 \end{bmatrix}$$

$$\xrightarrow{C_3 + \frac{x^2 - 6}{12} C_4} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & -12 \\ 0 & 0 & \frac{x^4 - 24x^2 + 36}{12} & 0 \end{bmatrix} \xrightarrow[C_3 \leftrightarrow C_4]{12L_4} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -12 & \\ 0 & 0 & 0 & x^4 - 24x^2 + 36 \end{bmatrix}\ ,$$

obtemos que

$$V \cong \frac{\mathbb{Q}[x]}{(x^4 - 24x + 36)}$$

é a decomposição invariante de V como módulo sobre $\mathbb{Q}[x]$.

Observação 4.11.5. 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 Kroneker* das matrizes A_M e A_N que representam T_M e T_N nas bases $\mathcal{B}_M$ e $\mathcal{B}_N$, respectimvamente.

No exemplo anterior, A é o produto de Kroneker 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.

Bibliografia

[Hun74] Hungerford

[FR04] R.L. Fernandes, M. Ricou

.