# Capítulo 2
# Estruturas Algébricas Básicas

## Sumário

O aprofundar seu estudo de Matemática o estudante frequentemente depara com conceitos como o de grupo, semigrupo, corpo, espaço vetorial, álgebra, anel, módulo, assim como encontra certas estruturas como espaços quociente, produtos tensoriais etc. Nosso objetivo neste capítulo é apresentar definições básicas de tais conceitos acompanhadas, quando possível, de alguns exemplos relevantes. Nossa intenção primária não é de forma alguma a de cobrir completamente esses assuntos e seus resultados mais importantes, mas a de introduzir ao leitor noções dessas estruturas algébricas, de modo que o mesmo possa encontrar aqui referências rápidas às mesmas quando delas necessitar. Vários dos tópicos aqui abordados serão desenvolvidos em capítulos posteriores, de modo que, como no caso do Capítulo 1, o objetivo não é um tratamento extensivo dos diversos assuntos. O estudante já familiar com alguns desses conceitos (os conceitos de grupo e álgebra são populares entre estudantes de Física) encontrará nessa exposição uma visão unificada dos mesmos.

Este capítulo deve ser compreendido como uma continuação do Capítulo 1. O leitor pode achar ser este capítulo uma longa sequência de apenas definições e exemplos, com poucos resultados, o que é parcialmente correto. Seu objetivo, porém, é apresentar várias ideias comuns a várias áreas de um ponto de vista unificado e introduzir construções empregadas ulteriormente.

# 2.1 Estruturas Algébricas Básicas

Ainda atentos ao caráter introdutório apresentaremos aqui definições e exemplos das estruturas algébricas mais comuns.

• **Operações e relações**

Sejam $C$ e $I$ dois conjuntos não vazios e consideremos o produto Cartesiano $C^I$ (o conceito de produto Cartesiano de conjuntos foi definido à página 73). Uma função $f : C^I \to C$ é por vezes dita ser uma *operação* sobre $C$. Se $I$ é um conjunto finito, $f$ é dita ser uma *operação finitária* sobre $C$.

Um conjunto $R \subset C^I$ é dito ser uma relação em $C$. Se $I$ é um conjunto finito, $R$ é dito ser uma *relação finitária* em $C$.

• **Funções finitárias**

Sejam $C$ e $I$ dois conjuntos e consideremos funções $f : C^I \to C$. Se $I$ é um conjunto finito $f : C^I \to C$ é dita ser uma *função finitária* sobre $C$ ou *operação finitária* sobre $C$. Sem perda de generalidade consideraremos aqui funções finitárias do tipo $f : C^n \to C$ para algum $n \in \mathbb{N}$. Se $f$ é uma função finitária para um dado $n$, $f$ é dita ser uma função $n$-ária sobre $C$. Um exemplo de uma função não finitária seria uma função do tipo $f : C^{\mathbb{N}} \to C$ que a cada sequência em $C$ associa um elemento de $C$.

Funções 2-árias serão chamadas aqui de *funções binárias* e funções 1-árias são chamadas de *funções unárias*. Funções unárias e binárias são as de maior relevância.

Por vezes iremos falar também de funções 0-árias sobre $C$, que consistem em funções $f : \{\emptyset\} \to C$. Uma tal função tem por imagem simplesmente um elemento fixo de $C$. Exemplos de funções 0-árias sobre $\mathbb{R}$ seriam $f(\emptyset) = 1$ ou $f(\emptyset) = 0$ ou $f(\emptyset) = \sqrt{2}$. Frequentemente denotamos tais funções pelo elemento de $C$ por ela associado. Nos três exemplos acima, poderíamos denotar as funções por 1, 0 ou $\sqrt{2}$, respectivamente.

• **Magmas**

Um conjunto $C$ dotado de uma relação binária $C \times C \to C$ é dito ser um *magma*. Essa nomenclatura foi introduzida por Bourbaki[1], porém, não é universalmente empregada.

• **Relações finitárias**

Há uma nomenclatura análoga para o caso de relações. Sejam $C$ e $I$ dois conjuntos e consideremos relações $R \subset C^I$. Se $I$ é um conjunto finito $R$ é dita ser uma *relação finitária* sobre $C$. Sem perda de generalidade consideraremos aqui relações finitárias do tipo $R \subset C^n$ para algum $n \in \mathbb{N}$. Se $R$ é uma relação finitária para um dado $n$, $R$ é dita ser uma relação $n$-ária sobre $C$. Para o caso $n = 1$ as relações são também chamadas de unárias e para o caso $n = 2$ são ditas binárias. Relações binárias foram estudadas à página 62.

• **Estruturas**

Seja $C$ um conjunto, $\mathcal{F}$ uma coleção de operações (não necessariamente finitárias) sobre $C$ e seja $\mathcal{R}$ uma coleção de relações (não necessariamente finitárias) em $C$. A tripla $\langle C,\ \mathcal{F},\ \mathcal{R}\rangle$ é dita ser uma *estrutura* sobre $C$. Note-se que tanto $\mathcal{F}$ quanto $\mathcal{R}$ podem ser vazias.

Dado que operações sobre um conjunto $C$ também são relações sobre $C$, a definição de estrutura acima poderia ser simplificada. É porém conveniente mantê-la como está, pois funções são de importância especial.

Uma estrutura $\langle C,\ \mathcal{F}\rangle$ é dita ser uma *estrutura algébrica* e uma estrutura $\langle C,\ \mathcal{R}\rangle$ é dita ser uma *estrutura relacional*.

• **Tipos de operações e de relações**

Ainda um comentário sobre a nomenclatura.

Sejam $C$ e $I$ conjuntos e seja $\alpha : C^I \to C$ uma operação sobre o conjunto $C$. A cardinalidade de $I$ é dita ser o *tipo da operação* $\alpha$. Assim, uma função $n$-ária é também dita ser de tipo $n$. Analogamente, se $R \subset C^I$ é uma relação em $C$ a cardinalidade de $I$ é dita ser o *tipo* da relação $R$.

• **Comentários sobre a notação. Notação mesofixa**

Antes de prosseguirmos, façamos uma observação sobre a notação que é costumeiramente adotada, especialmente quando se trata de funções binárias.

Dado um conjunto $C$ e uma função binária denotada por um símbolo $\phi$, a imagem de um par $(a,\ b) \in C^2$ é comummente denotada por $\phi(a,\ b)$. É muito prático, por vezes, usar uma outra notação e denotar $\phi(a,\ b)$ por $a\,\phi\,b$. Essa notação é denominada *notação mesofixa*. Um exemplo claro desse uso está na função soma de dois números complexos, denotada pelo símbolo $+ : \mathbb{C}^2 \to \mathbb{C}$. Denotamos $+(z,\ w)$ por $z + w$. Outro exemplo está na função produto de dois

[1] *Nicolas Bourbaki*. Nome coletivo adotado por um grupo de importantes matemáticos franceses, surgido por volta de 1935, que teve grande, mas declinante, influência na estruturação e sistematização da Matemática ao longo do século XX. O grupo Bourbaki sofreu diversas críticas pelo seu abstracionismo, considerado em certos círculos como excessivo e mesmo estéril.

números complexos: $\cdot : \mathbb{C}^2 \to \mathbb{C}$. Denotamos $\cdot(z,\ w)$ por $z \cdot w$.

Essa notação será usada adiante para outras funções binárias além das funções soma e produto de números ou matrizes.

Funções unárias também têm por vezes uma notação especial, frequentemente do tipo exponencial. Tal é o caso da operação que associa a cada elemento de um grupo à sua inversa, $g \mapsto g^{-1}$, ou o caso da operação que associa a cada conjunto o seu complementar $A \mapsto A^c$. Ou ainda o caso da transposição de matrizes $M \mapsto M^T$, da conjugação de números complexos $z \mapsto z^*$ para o que usa-se também sabidamente a notação $z \mapsto \overline{z}$.

• **Comutatividade, associatividade e distributividade**

Uma função binária $\chi : C^2 \to C$ é dita ser *comutativa* se para quaisquer $a$ e $b \in C$ valer

$$\chi(a,\ b) \ = \ \chi(b,\ a)\ ,$$

ou seja, na notação mesofixa, se

$$a\chi b \ = \ b\chi a\ .$$

Funções binárias comutativas são frequentemente chamadas de *Abelianas*[2].

Uma função binária $\chi : C^2 \to C$ é dita ser *associativa* se para quaisquer $a$, $b$ e $c \in C$ valer

$$\chi\big(a,\ \chi(b,\ c)\big) \ = \ \chi\big(\chi(a,\ b),\ c\big)\ ,$$

ou seja, na notação mesofixa, se

$$a\chi(b\chi c) \ = \ (a\chi b)\chi c\ .$$

A associatividade permite-nos eliminar os parênteses de expressões como $a\chi(b\chi c)$, que podem ser escritas sem ambiguidade na forma $a\chi b\chi c$.

Dadas duas funções binárias $\chi_1,\ \chi_2 : C^2 \to C$, dizemos que $\chi_1$ é *distributiva* em relação a $\chi_2$ se valer

$$\chi_1\big(a,\ \chi_2(b,\ c)\big) \ = \ \chi_2\big(\chi_1(a,\ b),\ \chi_1(a,\ c)\big) \qquad \text{ou seja,} \qquad a\chi_1(b\chi_2 c) \ = \ (a\chi_1 b)\chi_2(a\chi_1 c)$$

para quaisquer $a,\ b,\ c \in C$.

## 2.1.1 Álgebras Universais

Uma *álgebra universal* é constituída por um conjunto $C$ e uma coleção $\mathcal{F}$ de funções finitárias sobre $C$. A coleção $\mathcal{F}$ não precisa ser finita. Frequentemente denotaremos uma álgebra universal por $\langle C,\ \mathcal{F}\rangle$.

O estudo sistemático das álgebras universais foi iniciado por Withehead[3] e Birkhoff[4], tendo Boole[5], Hamilton[6], De Morgan[7] e Sylvester[8] como precursores. Para uma referência, vide [205]. Vamos a alguns exemplos.

1. Seja $C = \mathbb{R}$ e $\mathcal{F} = \{s,\ m\}$, onde $s$ e $m$ são duas funções binárias dadas por $s : \mathbb{R}^2 \to \mathbb{R}$, $s(x,\ y) = x + y$ e $m : \mathbb{R}^2 \to \mathbb{R}$, $m(x,\ y) = x \cdot y$.

2. Seja $C = \mathrm{Mat}\,(\mathbb{C},\ n)$ (o conjunto das matrizes complexas $n \times n$ para um certo $n \in \mathbb{N}$) e $\mathcal{F} = \{s,\ m\}$, onde $s$ e $m$ são duas funções binárias dadas por $s : C^2 \to C$, $s(A,\ B) = A + B$ e $m : C^2 \to C$, $m(A,\ B) = A \cdot B$.

3. Seja $C$ o conjunto de todas as matrizes complexas $n \times m$ (para $n$ e $m \in \mathbb{N}$) e seja $\mathcal{F} = \{c,\ s,\ t\}$ onde $c : C \to C$ é a função unária dada por $c(A) = \overline{A}$ (a matriz complexo-conjugada de $A$), $s : C^2 \to C$ é a função binária dada por $s(A,\ B) = A + B$ e $t : C^3 \to C$ é a função 3-ária dada por $t(A,\ B,\ C) = AB^TC$, onde $B^T$ é a transposta da matriz $B$.

[2] Niels Henrik Abel (1802–1829).
[3] Alfred North Withehead (1861–1947).
[4] George David Birkhoff (1884–1944).
[5] George Boole (1815–1864).
[6] William Rowan Hamilton (1805–1865).
[7] Augustus De Morgan (1806–1871).
[8] James Joseph Sylvester (1814–1897).

Algumas álgebras universais com propriedades especiais de importância em Matemática recebem denominações próprias e são chamadas de grupos, semigrupos, anéis, corpos etc. Vamos introduzi-las adiante. Em todas elas as funções de $\mathcal{F}$ são 0-árias, unárias ou binárias.

Algumas estruturas frequentemente encontradas, como espaços vetoriais, álgebras e módulos, não se enquadram exatamente no conceito de álgebra universal, mas podem ser encarados como constituídos por pares de álgebras universais dotadas de uma *ação* de uma das álgebras universais sobre a outra. A noção abstrata de ação de uma álgebra universal sobre uma outra álgebra universal será vista mais adiante.

A leitura do restante desta subseção sobre álgebras universais pode ser omitida pois não afetará o que segue.

• **Morfismos entre álgebras universais**

Sejam $\langle A,\ \mathcal{A}\rangle$ e $\langle B,\ \mathcal{B}\rangle$ duas álgebras universais. Uma função $\Delta : \mathcal{A} \to \mathcal{B}$ é dita *preservar o tipo* das operações de $\mathcal{A}$ se para todo $\alpha \in \mathcal{A}$ a operação $\Delta(\alpha) \in \mathcal{B}$ tiver o mesmo tipo que a operação $\alpha$.

Assim, uma aplicação que preserva o tipo leva aplicações unárias em unárias, aplicações binárias em binárias etc.

Um *morfismo* da álgebra universal $\langle A,\ \mathcal{A}\rangle$ na álgebra universal $\langle B,\ \mathcal{B}\rangle$ é um par de aplicações $\langle D,\ \Delta\rangle$ com $D : A \to B$ e $\Delta : \mathcal{A} \to \mathcal{B}$, onde $\Delta$ é uma aplicação que preserva o tipo e de tal forma que para todo $\alpha \in \mathcal{A}$ tenhamos

$$D \circ \alpha \ = \ \Delta(\alpha) \circ D^n$$

como aplicações $A^n \to B$, onde $n$ é o tipo de $\alpha$. Acima, $D^n : A^n \to B^n$ é dada por $D^n(a_1,\ \ldots,\ a_n) := \big(D(a_1),\ \ldots, D(a_n)\big)$. Assim, para todo $\alpha \in \mathcal{A}$ temos

$$D\big(\alpha(a_1,\ \ldots, a_n)\big) \ = \ \Delta(\alpha)\big(D(a_1),\ \ldots, D(a_n)\big)\ ,$$

para toda $(a_1,\ \ldots, a_n) \in A^n$, $n$ sendo o tipo de $\alpha$.

*Exemplo.* Sejam as álgebras universais $\langle \mathbb{R}_+,\ \{\cdot,\ 1\}\rangle$ e $\langle \mathbb{R},\ \{+,\ 0\}\rangle$ com as definições usuais e seja o par $\langle \ln,\ L\rangle$, onde $\ln : \mathbb{R}_+ \to \mathbb{R}$ é o logaritmo Neperiano[9] e $L : \{\cdot,\ 1\} \to \{+,\ 0\}$ dado por $L(\cdot) = +$, $L(1) = 0$. Então, $\langle \ln,\ L\rangle$ é um morfismo de $\langle \mathbb{R}_+,\ \{\cdot,\ 1\}\rangle$ em $\langle \mathbb{R},\ \{+,\ 0\}\rangle$, dado que para todo $a,\ b \in \mathbb{R}_+$ vale

$$\ln(a \cdot b) \ = \ \ln(a) + \ln(b)\ .$$

• **Ações de uma álgebra universal sobre uma outra álgebra universal**

Por razões de completeza apresentaremos aqui a noção geral de *ação* de uma álgebra universal sobre uma outra.

Vamos começar com algumas definições. Sejam $A$ e $B$ dois conjuntos e seja uma função $G : A \times B \to B$. Para todo $n \in \mathbb{N}$ definamos

$$G^{(n,\,1)} : A^n \times B \to B^n \quad \text{tal que} \quad (a_1,\ \ldots, a_n, b) \longmapsto \big(G(a_1,\ b),\ \ldots,\ G(a_n,\ b)\big)$$

com $a_i \in A$, $b \in B$, $i = 1,\ \ldots,\ n$.

Para todo $m \in \mathbb{N}$ definamos

$$G^{(1,\,m)} : A \times B^m \to B^m \quad \text{tal que} \quad (a,\ b_1,\ \ldots, b_m) \longmapsto \big(G(a,\ b_1),\ \ldots,\ G(a,\ b_m)\big)\ ,$$

com $a \in A$, $b_i \in B$, $i = 1,\ \ldots,\ m$.

Para um conjunto $C$ qualquer $\mathrm{id}_C : C \to C$ denota a identidade em $C$: $\mathrm{id}_C(c) = c$, $\forall c \in C$. Fora isso, se $\gamma : C \to C$ é uma aplicação, denotaremos por $\gamma^{(n)} : A^n \to A^n$ a aplicação tal que $\gamma^{(n)}(c_1,\ \ldots,\ c_n) = (\gamma(c_1),\ \ldots,\ \gamma(c_n))$.

Finalmente, para duas aplicações $\alpha : A^n \to A$ e $\beta : B^m \to B$ o par $(\alpha,\ \beta)$ denota a aplicação $A^n \times B^m \to A \times B$ dada por $(\alpha,\ \beta)(a_1,\ \ldots,\ a_n, b_1,\ \ldots,\ b_m) = \big(\alpha(a_1,\ \ldots,\ a_n),\ \beta(b_1,\ \ldots,\ b_m)\big)$.

Com isso podemos formular a definição desejada de ação de uma álgebra universal sobre uma outra.

Sejam $\langle A,\ \mathcal{A}\rangle$ e $\langle B,\ \mathcal{B}\rangle$ duas álgebras universais. Uma *ação* de $\langle A,\ \mathcal{A}\rangle$ sobre $\langle B,\ \mathcal{B}\rangle$ é um par $\langle G,\ \Gamma\rangle$ onde

$$G : A \times B \to B \qquad \text{e} \qquad \Gamma : \mathcal{A} \to \mathcal{B}$$

[9] John Napier (Neper ou Nepair) (1550–1617).

são aplicações tais que $\Gamma$ preserva tipos e as seguintes condições são válidas: Para quaisquer $\alpha \in \mathcal{A}$ e $\beta \in \mathcal{B}$ (cujos tipos serão $n$ e $m$, respectivamente) tem-se que

$$G \circ (\alpha,\ \beta) \ = \ \Gamma(\alpha) \circ G^{(n,\,1)} \circ (\mathrm{id}_{A^n},\ \beta) \ = \ \beta \circ G^{(1,\,m)} \circ (\alpha,\ \mathrm{id}_{B^m}) \tag{2.1}$$

como aplicações $A^n \times B^m \to B$.

De (2.1) segue que

$$G \circ (\alpha,\ \mathrm{id}_B) \ = \ \Gamma(\alpha) \circ G^{(n,\,1)} \circ (\mathrm{id}_{A^n},\ \mathrm{id}_B) \tag{2.2}$$

e

$$G \circ (\mathrm{id}_A,\ \beta) \ = \ \beta \circ G^{(1,\,m)} \circ (\mathrm{id}_A,\ \mathrm{id}_{B^m})\ . \tag{2.3}$$

**E. 2.1** *Exercício.* Mostre isso. ✠

De (2.2) e (2.3) segue que

$$G^{(n,\,1)} \circ (\mathrm{id}_{A^n},\ \beta) \ = \ \Big(\beta \circ G^{(1,\,m)}\Big)^{(n)} \circ j \tag{2.4}$$

e

$$G^{(1,\,m)} \circ (\alpha,\ \mathrm{id}_{B^m}) \ = \ \Big(\Gamma(\alpha) \circ G^{(n,\,1)}\Big)^{(m)} \circ k\ , \tag{2.5}$$

onde $j : A^n \times B^m \to (A \times B^m)^n$ é dada por

$$j(a_1,\ \ldots,\ a_n, b_1,\ \ldots,\ b_m) \ := \ (a_1,\ b_1,\ \ldots,\ b_m, a_2,\ b_1,\ \ldots,\ b_m,\ \ldots,\ a_n,\ b_1,\ \ldots,\ b_m)$$

e $k : A^n \times B^m \to (A^n \times B)^m$ é dada por

$$k(a_1,\ \ldots,\ a_n, b_1,\ \ldots,\ b_m) \ := \ (a_1,\ \ldots,\ a_n,\ b_1,\ a_1,\ \ldots,\ a_n,\ b_2,\ \ldots,\ a_1,\ \ldots,\ a_n,\ b_m)\ .$$

**E. 2.2** *Exercício.* Mostre isso. ✠

Das relações (2.4) e (2.5) segue que a condição (2.1) pode ser escrita como

$$G \circ (\alpha,\ \beta) \ = \ \Gamma(\alpha) \circ \Big(\beta \circ G^{(1,\,m)}\Big)^{(n)} \circ j \ = \ \beta \circ \Big(\Gamma(\alpha) \circ G^{(n,\,1)}\Big)^{(m)} \circ k\ . \tag{2.6}$$

*Observação.* Acima estamos considerando $\mathrm{id}_A$, $\mathrm{id}_B$, como elementos de $\mathcal{A}$, respectivamente de $\mathcal{B}$, o que sempre pode ser feito sem perda de generalidade. ♣

## 2.1.2 Reticulados e Álgebras Booleanas

A noção de *reticulado* é empregada em diversas áreas da Matemática, por exemplo, no estudo de conjuntos parcialmente ordenados, na Teoria de Grafos, na Teoria de Grupos etc. Nestas Notas a noção de reticulado será empregada na demonstração do importante Teorema de Stone-Weierstrass, Teorema 38.16, página 2120, descrito na Seção 38.5, página 2119. Vide para tal o Exemplo 2.3, página 120. Na Física, reticulados desempenham um papel na chamada *Lógica Quântica*, que descreve e estuda os fundamentos lógicos da Física Quântica. Vide para tal Seção 41.4, página 2326. Álgebras Booleanas são um tipo especial de reticulado cujo emprego estende-se a áreas como Lógica, Topologia e Teoria da Medida.

Como referências gerais sobre reticulados, recomendamos [59] e [206]. Para álgebras Booleanas recomendamos [221].

• **Reticulados**

Um *reticulado*[10] é uma álgebra universal constituída por um conjunto não vazio $C$ e duas funções binárias denotadas por $\wedge$ e $\vee$ (lê-se "e" e "ou", respectivamente), dotadas das seguintes propriedades, válidas para todos $a$, $b$ e $c \in C$ (usaremos a notação mesofixa):

[10] Denominado *"lattice"* em Inglês, *"Verband"* em Alemão e *"treillis"* em Francês.

1. Idempotência:
$$a \wedge a \;=\; a\,, \qquad a \vee a \;=\; a\,. \tag{2.7}$$

2. Comutatividade:
$$a \wedge b \;=\; b \wedge a\,, \qquad a \vee b \;=\; b \vee a\,. \tag{2.8}$$

3. Associatividade:
$$a \wedge (b \wedge c) \;=\; (a \wedge b) \wedge c\,, \tag{2.9}$$
$$a \vee (b \vee c) \;=\; (a \vee b) \vee c\,. \tag{2.10}$$

4. Absorvência[11]:
$$a \wedge (a \vee b) \;=\; a\,, \tag{2.11}$$
$$a \vee (a \wedge b) \;=\; a\,. \tag{2.12}$$

Um reticulado em um conjunto $C$ é dito ser um reticulado sobre $C$. Vamos a exemplos de reticulados.

**Exemplo 2.1** Seja $X$ um conjunto não vazio. Afirmamos que $\mathbb{P}(X)$ é um reticulado sob as operações $\wedge$ e $\vee$ definidas para todos $A$, $B \subset X$, por $A \wedge B = A \cap B$, $A \vee B = A \cup B$. Verifique! Mais adiante (Exemplo 2.6, página 125) veremos que esse exemplo, com alguns ingredientes a mais, corresponde a uma álgebra Booleana. ⧫

**Exemplo 2.2** Seja $C = \mathbb{R}$ e sejam as funções binárias $\wedge$ e $\vee$ definidas para todos $a$, $b \in \mathbb{R}$, por
$$a \wedge b \;:=\; \min\{a,\, b\} \;=\; \frac{1}{2}\Big(a + b - \big|a - b\big|\Big)\,,$$
$$a \vee b \;:=\; \max\{a,\, b\} \;=\; \frac{1}{2}\Big(a + b + \big|a - b\big|\Big)\,.$$
Verifique! ⧫

**Exemplo 2.3** Este exemplo generaliza o Exemplo 2.2. Seja $X$ um conjunto não vazio e $C = \mathbb{R}^X$, o conjunto de todas as funções reais definidas em $X$. Para duas funções $f,\ g : X \to \mathbb{R}$ defina-se duas novas funções $f \wedge g$ e $f \vee g$ por
$$(f \wedge g)(x) \;:=\; \min\{f(x),\, g(x)\} \;=\; \frac{1}{2}\Big(f(x) + g(x) - \big|f(x) - g(x)\big|\Big)\,,$$
$$(f \vee g)(x) \;:=\; \max\{f(x),\, g(x)\} \;=\; \frac{1}{2}\Big(f(x) + g(x) + \big|f(x) - g(x)\big|\Big)\,.$$
Esse exemplo de reticulado é relevante na demonstração do Teorema de Stone-Weierstrass, Teorema 38.16, página 2120. ⧫

**Exemplo 2.4** Uma outra generalização do Exemplo 2.2. Seja $C$ um conjunto linearmente ordenado (a definição está à página 80) e sejam as funções binárias $\wedge$ e $\vee$ definidas para todos $a$, $b \in C$, por
$$a \wedge b \;=\; \begin{cases} a, & \text{se } a \preceq b\,, \\ b, & \text{de outra forma}\,, \end{cases} \qquad a \vee b \;=\; \begin{cases} a, & \text{se } a \succeq b\,, \\ b, & \text{de outra forma}\,. \end{cases}$$
⧫

**E. 2.3** *Exercício.* Mostre que cada um dos exemplos acima compõe um reticulado. ✠

[11] Também denominada "Amalgamento". O estudante deve observar que essa é a única propriedade das listadas acima que relaciona ambas as operações $\wedge$ e $\vee$.

• **Reticulados e relações de ordem**

O Exemplo 2.4, acima, mostra-nos que é possível constituir um reticulado a partir de uma relação de ordem total. Reciprocamente, é possível construir uma relação de ordem parcial a partir de um reticulado. Para tratar disso (e para futura referência), enunciemos e provemos o seguinte lema:

**Lema 2.1** *Seja $C$ um conjunto não vazio, o qual constitui um reticulado com duas operações binárias $\wedge$ e $\vee$. Então, dois elementos $x,\ y \in C$ satisfazem a igualdade $x = x \wedge y$ se e somente se satisfizerem também $y = x \vee y$.* □

Prova. Se $x$ e $y \in C$ satisfazem $x = x \wedge y$, então segue que $x \vee y = (x \wedge y) \vee y = y$, sendo que na última igualdade usamos as propriedades de comutatividade e absorvência. Analogamente, se $y = x \vee y$, segue que $x \wedge y = x \wedge (x \vee y) = x$, onde novamente usamos as propriedades de comutatividade e absorvência. ■

Essas observações do Lema 2.1, adicionadas à inspiração do Exemplo 2.4, induzem-nos à seguinte definição de uma relação de ordem parcial em $C$: dizemos que

$$x \preceq y \ \text{ se e somente se } \ x = x \wedge y \ \text{ ou, equivalentemente, se e somente se } \ y = x \vee y \,. \tag{2.13}$$

Precisamos agora justificar que se trata de uma relação de ordem parcial, provando serem válidas as propriedades de reflexividade, transitividade e antissimetria listadas à página 80:

1. Pela propriedade de idempotência, vale $x = x \wedge x$ para todo $x \in C$ e, portanto, $x \preceq x$ para todo $x \in C$. Essa é a propriedade de reflexividade da ordem parcial.
2. Se $x,\ y$ e $z \in C$ satisfazem $x = x \wedge y$ e $y = y \wedge z$, segue que $x = x \wedge y = x \wedge (y \wedge z) \overset{\text{assoc.}}{=} (x \wedge y) \wedge z = x \wedge z$. Logo, provamos que se $x \preceq y$ e $y \preceq z$, então vale $x \preceq z$. Essa é a propriedade de transitividade da ordem parcial.
3. Por fim, se $x = x \wedge y$ e $y = y \wedge x$, a propriedade de comutatividade diz-nos que $x = x \wedge y = y$. Assim, provamos que se $x \preceq y$ e $y \preceq x$ vale $x = y$. Essa é a propriedade de antissimetria da ordem parcial.

**E. 2.4** *Exercício.* Estude as relações de ordem que advêm dos Exemplos 2.1 e 2.3 e constate que são relações de ordem parciais, não totais (exceto no caso em que $C$ tem apenas um elemento). ✠

• **Reticulados limitados superiormente. Reticulados limitados inferiormente**

Um reticulado $C$ é dito ser limitado superiormente se possuir um máximo, ou seja, se existir $\omega \in C$ tal que $x \preceq \omega$ para todo $x \in C$, o que equivale a dizer que $x = x \wedge \omega$ para todo $x \in C$.

Um reticulado $C$ é dito ser limitado inferiormente se possuir um mínimo, ou seja, se existir $\alpha \in C$ tal que $\alpha \preceq x$ para todo $x \in C$, o que equivale a dizer que $x = x \vee \alpha$ para todo $x \in C$.

Essas definições coincidem, como veremos, com as definições de unidade e elemento nulo de um reticulado que apresentaremos adiante.

• **Unidade e elemento nulo de um reticulado**

Caso um reticulado $C$ possua um elemento $e$ tal que $x \wedge e = x$ para todo $x \in C$ o elemento $e$ é dito ser uma *identidade* ou *unidade* do reticulado, e é frequentemente denotado pelo símbolo 1. Pelo Lema 2.1, a relação $x \wedge 1 = x$ é válida se e somente se $1 = x \vee 1$.

Caso um reticulado $C$ possua um elemento $z$ tal que $x \vee z = x$ para todo $x \in C$ o elemento $z$ é dito ser um *elemento nulo* do reticulado, e é frequentemente denotado pelo símbolo 0. Pelo Lema 2.1, a relação $x \vee 0 = x$ é válida se e somente se $0 = x \wedge 0$.

Assim, se existirem unidade e elemento nulo teremos

$$x = x \wedge 1\,, \qquad 1 = x \vee 1\,, \qquad x = x \vee 0 \qquad \text{e} \qquad 0 = x \wedge 0 \tag{2.14}$$

para todo $x \in C$.

A unidade e o elemento nulo, se existirem, são únicos. Se fato, se 1 e $1'$ são unidades de um reticulado $C$ então, por definição, $1 \wedge 1' = 1$, mas também $1' \wedge 1 = 1'$, provando (pela comutatividade) que $1 = 1'$. Analogamente, se 0 e $0'$ são elementos nulos de um reticulado $C$ então, também por definição, $0 \vee 0' = 0$, mas também $0' \vee 0 = 0'$, provando (pela comutatividade) que $0 = 0'$.

Como dissemos acima, podemos associar naturalmente uma relação de ordem parcial $\preceq$ a um reticulado dizendo que $x \preceq y$ se e somente se $x = x \wedge y$ ou, equivalentemente, se $y = y \vee x$.

Se $C$ possui uma unidade 1 teremos $x \preceq 1$ para todo $x \in C$, pois $x = x \wedge 1$. Analogamente, se Se $C$ possui um elemento nulo 0 teremos $0 \preceq x$ para todo $x \in C$, pois $x = x \vee 0$. Vemos com isso que 1 é o máximo e 0 o mínimo do reticulado (se existirem).

• **Reticulados limitados**

Um reticulado que for limitado superiormente e inferiormente é dito ser um *reticulado limitado*. Assim, um reticulado é limitado se possuir uma unidade e um elemento nulo (ou seja, um máximo e um mínimo).

Em um reticulado limitado $C$ vale $0 \preceq x \preceq 1$ para todo $x \in C$. Se em um reticulado $C$ tivermos $0 = 1$, valerá, portanto, $x = 0 = 1$ para todo $x \in C$, ou seja, $C$ possui um único elemento. Um tal caso é totalmente trivial, de forma que sempre consideraremos $0 \neq 1$.

• **Reticulados completos**

Um reticulado é dito ser um *reticulado completo* se todo seu subconjunto não vazio possuir um supremo e um ínfimo (em relação à relação de ordem parcial $\preceq$). Para as definições de supremo e ínfimo, vide página 84 e seguintes. Naturalmente, reticulados completos devem ser limitados.

A coleção de todas as topologias definidas em um conjunto não vazio constitui um reticulado completo. Vide Exercício E. 28.24, página 1535.

• **Elementos complementares**

Seja $C$ um reticulado limitado (ou seja, que possui uma unidade e um elemento nulo). Dizemos que dois elementos $x,\ y \in C$ são complementares se

$$x \wedge y \ = \ 0 \qquad \text{e} \qquad x \vee y \ = \ 1 \, .$$

Em um tal caso dizemos que $x$ é complementar a $y$ e vice-versa. Elementos complementares não são necessariamente únicos, ou seja, se $y$ é complementar a $x$ pode haver $y' \neq y$ que também é complementar a $x$. Como veremos, uma condição suficiente para garantir a unicidade (não a existência!) do complementar de um elemento $x$ é a propriedade distributiva.

Pela definição de unidade e de elemento nulo, valem $0 = 0 \wedge 1$ e $1 = 1 \vee 0$. Essas relações estão dizendo que 0 e 1 são elementos complementares.

Dado um reticulado geral $C$, nem sempre é possível garantir a existência de um elemento complementar para cada um de seus elementos, nem sua unicidade. Se, no entanto valer que cada $x \in C$ possui um elemento complementar único, este é denotado pelo símbolo $\neg x$. Condições suficientes para garantir unicidade (não existência!) serão apresentadas a seguir (distributividade e limitação).

Outros símbolos encontrados na literatura para $\neg x$ são $\complement x$, $x^c$ ou ainda $x^\perp$, esse último empregado no estudo dos chamados reticulados ortocomplementados (Seção 2.1.2.2, página 126).

• **Reticulados complementados**

Um reticulado $C$ no qual todo elemento possui ao menos um complementar é dito ser um *reticulado complementado*.

Se $C$ é complementado e, além disso, para cada $x \in C$ o elemento complementar for único, $\neg x$, então a função $C \ni x \mapsto \neg x \in C$ é uma função unária em $C$.

• **Reticulados distributivos**

Um reticulado sobre um conjunto $C$ é dito ser um *reticulado distributivo* se as operações $\wedge$ e $\vee$ forem distributivas uma em relação à outra, ou seja, se forem satisfeitas as propriedades

$$a \wedge (b \vee c) \ = \ (a \wedge b) \vee (a \wedge c) \tag{2.15}$$

e

$$a \vee (b \wedge c) \;=\; (a \vee b) \wedge (a \vee c)\,. \tag{2.16}$$

para todos $a,\ b$ e $c \in C$.

Em álgebras Booleanas (vide adiante), devido às regras de De Morgan (2.17), as propriedades (2.15) e (2.16) decorrem uma da outra.

**E. 2.5** *Exercício*. Demonstre essa afirmação. ✠

**E. 2.6** *Exercício*. Nos Exemplos 2.1–2.4, acima, quais reticulados são distributivos? Quais não são? ✠

• **Reticulados limitados e distributivos**

Em um reticulado distributivo e limitado $C$, o complementar de um elemento $x \in C$, se existir, é único. De fato, se $y$ e $y' \in C$ são complementares a $x$, teremos $0 = x \wedge y = x \wedge y'$ e $1 = x \vee y = x \vee y'$. Agora,

$$y \;=\; y \wedge 1 \;=\; y \wedge (x \vee y') \;\overset{\text{distrib.}}{=}\; (y \wedge x) \vee (y \wedge y') \;=\; 0 \vee (y \wedge y') \;=\; y \wedge y'$$

e, analogamente,

$$y' \;=\; y' \wedge 1 \;=\; y' \wedge (x \vee y) \;\overset{\text{distrib.}}{=}\; (y' \wedge x) \vee (y' \wedge y) \;=\; 0 \vee (y' \wedge y) \;=\; y' \wedge y\,,$$

provando que $y = y \wedge y' = y'$.

Em um reticulado distributivo e limitado, o complementar (único!) de um elemento $x \in C$, se existir, é denotado pelo símbolo $\complement x$, pelo símbolo $\neg x$ ou ainda pelo símbolo $x^c$. Naturalmente, valem

$$x \wedge (\neg x) \;=\; 0 \qquad \text{e} \qquad x \vee (\neg x) \;=\; 1\,.$$

Se $\neg x$ é o complementar de $x$, é evidente que $\neg x$ tem um complementar, a saber, $x$. Logo, pela unicidade do complementar, $\neg(\neg x) = x$ sempre que $\neg x$ existir. É importante notar também que, pelo comentado acima, valem $\neg 0 = 1$ e $\neg 1 = 0$.

• **Reticulados limitados, complementados e distributivos**

Se além de distributivo e limitado o reticulado for também complementado haverá um complementar único para cada elemento de $C$ e, portanto, haverá uma função unária $\neg : C \to C$ que a cada $x \in C$ associa o seu complementar $\neg x$. Como vimos, vale nesse caso $\neg(\neg x) = x$ para todo $x \in C$, assim como valem as relações $\neg 0 = 1$ e $\neg 1 = 0$.

Um reticulado limitado, complementado e distributivo é dito ser uma *álgebra Booleana*.

### 2.1.2.1 Álgebras Booleanas

Uma *álgebra Booleana*[12] é uma álgebra universal formada por um conjunto $B$ e por uma família $\mathcal{F}$ de cinco funções finitárias: duas binárias, denotadas por $\wedge$ e $\vee$, uma função unária, denotada por $\neg$ ou pelo símbolo $\complement$, e denominada "negação" ou "complemento", e duas funções 0-árias, denotadas genericamente por 0 e 1 (denominadas, obviamente, "zero" e "um"), as quais representam elementos fixos distintos de $B$. As funções acima são supostas satisfazer aos seguintes requisitos:

1. $B$, $\wedge$ e $\vee$ formam um reticulado distributivo.
2. Para todo $a \in B$ vale que $1 \wedge a = a$ e que $0 \vee a = a$ (reticulado limitado).
3. Para todo $a \in B$ vale que $a \wedge (\neg a) = 0$ e que $a \vee (\neg a) = 1$ (reticulado complementado).

[12] George Boole (1815–1864).

Por vezes, denota-se $\neg a$ por $a^{\perp}$ ou ainda por $\complement a$ ou $a^{c}$. Esses dois últimos são de uso mais comum em operações envolvendo conjuntos. Novamente, tem-se pelas definições que $\neg 0 = 1$, $\neg 1 = 0$ e $\neg\,(\neg a) = a$ para todo $a \in B$.

• **Regras de De Morgan**

Em uma álgebra Booleana $B$ valem para todos $a,\ b \in B$ as importantes relações

$$\neg(a \wedge b) \ = \ (\neg a) \vee (\neg b) \qquad \text{e} \qquad \neg(a \vee b) \ = \ (\neg a) \wedge (\neg b)\ , \tag{2.17}$$

as quais são conhecidas como *regras de De Morgan*[13].

A segunda relação em (2.17) é decorrência da primeira, como se vê trocando $a \to \neg a$ e $b \to \neg b$. Por isso, basta provar a primeira, o que significa provar que

$$\Big((\neg a) \vee (\neg b)\Big) \wedge (a \wedge b) \ = \ 0 \qquad \text{e} \qquad \Big((\neg a) \vee (\neg b)\Big) \vee (a \wedge b) \ = \ 1\ . \tag{2.18}$$

Ambas decorrem da comutatividade, da associatividade, da distributividade e das relações (2.14). Para provar a primeira relação em (2.18), temos

$$\begin{aligned}
\Big((\neg a) \vee (\neg b)\Big) \wedge (a \wedge b) \quad &\overset{\text{associat.}}{=} \quad \Big[\Big((\neg a) \vee (\neg b)\Big) \wedge a\Big] \wedge b \\
&\overset{\text{distribut.}}{=} \quad \Big[\Big((\neg a) \wedge a\Big) \vee \Big((\neg b) \wedge a\Big)\Big] \wedge b \\
&= \quad \Big[0 \vee \Big((\neg b) \wedge a\Big)\Big] \wedge b \\
&\overset{(2.14)}{=} \quad \Big((\neg b) \wedge a\Big) \wedge b \ \overset{\text{comutat.}}{=}\ b \wedge \Big((\neg b) \wedge a\Big) \\
&\overset{\text{associat.}}{=} \quad \Big(b \wedge (\neg b)\Big) \wedge a \ = \ 0 \wedge a \ \overset{(2.14)}{=}\ 0\ .
\end{aligned}$$

Para provar a segunda relação em (2.18), temos

$$\begin{aligned}
\Big((\neg a) \vee (\neg b)\Big) \vee (a \wedge b) \quad &\overset{\text{associat.}}{=} \quad (\neg a) \vee \Big((\neg b) \vee (a \wedge b)\Big) \\
&\overset{\text{distribut.}}{=} \quad (\neg a) \vee \Big[\Big((\neg b) \vee a\Big) \wedge \Big((\neg b) \vee b\Big)\Big] \\
&= \quad (\neg a) \vee \Big[\Big((\neg b) \vee a\Big) \wedge 1\Big] \\
&\overset{(2.14)}{=} \quad (\neg a) \vee \Big((\neg b) \vee a\Big) \ \overset{\text{comutat.}}{=}\ (\neg a) \vee \Big(a \vee (\neg b)\Big) \\
&\overset{\text{associat.}}{=} \quad \Big((\neg a) \vee a\Big) \vee (\neg b) \ = \ 1 \vee (\neg b) \ \overset{(2.14)}{=}\ 1\ .
\end{aligned}$$

As regras de De Morgan podem ser válidas em outras estruturas algébricas que não álgebras Booleanas, assim como na Lógica Proposicional. O seguinte exemplo ilustra isso:

**E. 2.7** *Exercício*. Considere-se o conjunto $[0,\ 1] \subset \mathbb{R}$ e nele as operações $\wedge$, $\vee$ e $\neg$ definidas por (aqui, $a,\ b \in [0,\ 1]$)

$$a \wedge b \ := \ ab\ , \qquad a \vee b \ := \ a + b - ab \ = \ 1 - (1-a)(1-b) \qquad \text{e} \qquad \neg a \ := \ 1 - a\ .$$

Verifique que não se trata de um reticulado (quais propriedades definidoras de reticulados não são satisfeitas?), nem as regras de distributividade (2.15)-(2.16) são satisfeitas, mas verifique que as regras de De Morgan (2.17) são satisfeitas. ✠

[13] Augustus De Morgan (1806–1871).

## • Álgebras Booleanas e relação de ordem

**Lema 2.2** *Se $B$ é uma álgebra Booleana e $a,\ b \in B$ satisfazem $a \preceq b$, então $(\neg b) \preceq (\neg a)$. Ou seja, em uma álgebra Booleana a operação de completamento reverte a relação de ordem entre os elementos.* □

Prova. Sejam $a,\ b \in B$ que satisfazem $a \preceq b$. Pela definição de relação de ordem em reticulados (2.13), isso significa que $a = a \wedge b$. Pelo Lema 2.1, página 121, temos também $b = a \vee b$. Usando a segunda regra de De Morgan em (2.17), página 124, segue disso que

$$\neg b \ = \ \neg(a \vee b) \ \overset{(2.17)}{=} \ (\neg a) \wedge (\neg b) \ \overset{\text{simetria}}{=} \ (\neg b) \wedge (\neg a) \ .$$

Agora, a igualdade assim provada $\neg b = (\neg b) \wedge (\neg a)$ é precisamente a afirmação que $(\neg b) \preceq (\neg a)$. ■

## • Exemplos básicos de álgebras Booleanas

**Exemplo 2.5** A menor álgebra Booleana, e talvez uma das mais importantes em aplicações, é composta por dois elementos distintos, denotados por 0 e 1: $B = \{0,\ 1\}$ e as operações $\wedge$, $\vee$ e $\neg$ são dadas por

$$0 \wedge 0 \ = \ 0 \, , \quad 0 \wedge 1 \ = \ 0 \, , \quad 1 \wedge 0 \ = \ 0 \, , \quad 1 \wedge 1 \ = \ 1 \, , \quad 0 \vee 0 \ = \ 0 \, , \quad 0 \vee 1 \ = \ 1 \, , \quad 1 \vee 0 \ = \ 1 \, , \quad 1 \vee 1 \ = \ 1 \, ,$$

e por $\neg 0 = 1$ e $\neg 1 = 0$. É um exercício iluminante verificar que todas as propriedades definidoras de álgebras Booleanas são satisfeitas neste caso. ♦

**Exemplo 2.6** Seja $X$ um conjunto não vazio. Afirmamos que $\mathbb{P}(X)$ é uma álgebra Booleana sob as seguintes definições: para $A,\ B \in \mathbb{P}(X)$ definamos $A \wedge B := A \cap B$, $A \vee B := A \cup B$, $\neg A := \complement A = X \setminus A$, $0 = \emptyset$, $1 = X$.

A idempotência e a comutatividade são evidentes, a associatividade e a distributividade estão expressas em (1.24) e (1.25), página 65, a absorvência decorre das evidentes relações $A \cap (A \cup B) = A$ e $A \cup (A \cap B) = A$. É também claro que $1 \wedge A = X \cap A = A$ e $0 \vee A = \emptyset \cup A = A$. As propriedades de complementaridade são também claras: $A \wedge (\neg A) = A \cap (X \setminus A) = \emptyset = 0$ e $A \vee (\neg A) = A \cup (X \setminus A) = X = 1$. A relação de ordem parcial $A \preceq B \Leftrightarrow A = A \wedge B$ significa $A \preceq B \Leftrightarrow A = A \cap B$, relação essa que significa $A \subset B$. ♦

**Exemplo 2.7** O Exemplo 2.6 tem uma importante generalização. Seja $X$ um conjunto não vazio e seja $\mathcal{M}$ uma $\sigma$-álgebra em $X$. Para a definição e propriedades básicas de $\sigma$-álgebras, vide Seção 1.2.5, página 105 ou Capítulo 28, página 1528. Afirmamos que $\mathcal{M}$ é uma álgebra Booleana sob as mesmas definições do Exemplo 2.6: para $A,\ B \in \mathcal{M}$ definamos $A \wedge B := A \cap B$, $A \vee B := A \cup B$, $\neg A := \complement A = X \setminus A$, $0 = \emptyset$, $1 = X$.

Face ao discutido no Exemplo 2.6, e ao fato que $X \in \mathcal{M}$ e $\emptyset \in \mathcal{M}$ (evidentes pela definição de $\sigma$-álgebra), a única coisa que resta constatar é que as operações $\wedge$, $\vee$ e $\neg$ são, de fato, definidas em $\mathcal{M}$. No entanto, se $A$ e $B$ são elementos de $\mathcal{M}$, sua união também o é (pela definição de $\sigma$-álgebra), assim como sua intersecção (pela Proposição 1.22, página 106). Por fim, se $A \in \mathcal{M}$, então $\neg A := X \setminus A$ é também elemento de $\mathcal{M}$, também pela definição de $\sigma$-álgebra.

Esse exemplo é particularmente importante pois abre a possibilidade de se lidar com álgebras Booleanas nas quais uma *medida de probabilidades* (ou qualquer outro tipo de medida) está definida.

Informamos ainda que a recíproca da afirmação acima não é verdadeira: nem toda álgebra Booleana é isomorfa a uma $\sigma$-álgebra. Vide, *e.g.*, [221]. ♦

**Exemplo 2.8** $B = [0,\ 1] \subset \mathbb{R}$, as operações $\wedge$, $\vee$ são dadas como no Exemplo 2.2, página 120:

$$a \wedge b \ := \ \min\{a,\ b\} \qquad \text{e} \qquad a \vee b \ := \ \max\{a,\ b\}$$

para todos $a,\ b \in [0,\ 1]$ e a operação $\neg$ é dada por $\neg a = 1 - a$ para todo $a \in [0,\ 1]$. Naturalmente, o elemento nulo é o número 0 e a unidade é o número 1. ♦

**Exemplo 2.9** O mesmo que o anterior, mas tomando $B$ como sendo qualquer subconjunto de $[0,\ 1]$ que contenha 0 e 1. ♦

**Exemplo 2.10** Seja $X$ um conjunto não vazio e seja $I$ qualquer subconjunto de $[0,\ 1]$ que contenha 0 e 1. Seja $B = I^X$, a coleção de todas as funções de $X$ em $I$. Como no Exemplo 2.3, página 120, defina-se para cada $x \in X$

$$(f \wedge g)(x) \ = \ \min\{f(x),\ g(x)\} \qquad \text{e} \qquad (f \vee g)(x) \ = \ \max\{f(x),\ g(x)\}$$

e defina-se $(\neg f)(x) = 1 - f(x)$. Tome-se o elemento nulo como sendo a função identicamente nula e a unidade como sendo a função identicamente igual a 1. Esse tipo de reticulado é empregado na demonstração do Teorema de Stone-Weierstrass, Teorema 38.16, página 2120. ♦

**E. 2.8** *Exercício.* Mostre que os sistemas definidos nos exemplos acima formam álgebras Booleanas. ✠

01010101010101010101010101010101010101010101010

A relevância das álgebras Booleanas reside no fato de as mesmas capturarem algebricamente as operações mais importantes da teoria dos conjuntos (como as de união, intersecção, complemento, conjunto vazio) e as da lógica ("e", "ou", "negação", "verdadeiro", "falso"). Os Exemplos 2.6 e 2.5 atestam essa concepção. Fora isso, álgebras Booleanas relacionam-se a espaços topológicos, como pode ser apreciado na discussão sobre os Axiomas de Kuratowski à página 1548, Capítulo 28.

Certas álgebras Booleanas, como a do Exemplo 2.5, são de fácil implementação em Eletrônica e de amplo uso em processamento digital. Um pioneiro na identificação da relevância de álgebras Booleanas no *design* de circuitos lógicos foi Shestakov[14], que teria divulgado suas ideias já em 1935, tendo defendido tese a respeito em 1938 na Universidade Estatal de Moscou. Outro importante pioneiro nessas aplicações de álgebras Booleanas foi Shannon[15], em seu trabalho de Mestrado no MIT *"A Symbolic Analysis of Relay and Switching Circuits"*, de 1937, trabalho fundamental para o *design* de circuitos digitais. Um terceiro pioneiro a ser mencionado foi Zuse[16], que construiu, entre 1936 e 1938, um dos primeiros (segundo alguns, *o* primeiro dos) computadores eletromecânicos programáveis, chamado *Z1*, também baseado em álgebras Booleanas.

### 2.1.2.2 Reticulados Ortocomplementados e Ortomodulares

Tratemos agora de apresentar mais dois tipos de reticulados, os reticulados ortocomplementados e os reticulados ortomodulares, empregados no estudo de aspectos lógicos da Física Quântica. Um exemplo especialmente relevante será discutido na Seção 41.4, página 2326.

• **Reticulados ortocomplementados**

Um reticulado $O$ é dito ser *ortocomplementado* se for um reticulado limitado dotado de uma função unária, denotada por $\perp$ e denominada *ortocomplementação*, com as seguintes propriedades:

1. $(x^\perp)^\perp = x$ para todo $x \in O$ (involução).
2. $x^\perp \vee x = 1$ e $x^\perp \wedge x = 0$ para todo $x \in O$ (complementaridade).
3. Se para $x,\ y \in O$ valer $x \preceq y$ então $y^\perp \preceq x^\perp$ (reversão de ordem).

As propriedades de involução e de complementaridade significam que $\perp$ é uma operação de complementaridade, como a operação $\neg$, acima, mas nessa área é tradicional usar-se o símbolo $\perp$ em lugar de $\neg$, certamente devido ao exemplo discutido da Seção 41.4, página 2326.

A propriedade de reversão de ordem significa, segundo a definição de relação de ordem em reticulados, que se $x = x \wedge y$ então $y^\perp = y^\perp \wedge x^\perp$.

Como se observa comparando-se as definições, toda álgebra Booleana é um reticulado ortocomplementado através da identificação $\perp \equiv \neg$, a reversão de ordem, no caso Booleano, estando afirmada no Lema 2.2, página 125.

[14] Victor Ivanovich Shestakov (1907-1987).
[15] Claude Elwood Shannon (1916–2001).
[16] Konrad Ernst Otto Zuse (1910–1995).

• **Reticulados modulares**

Para um reticulado distributivo, limitado e complementado $B$, ou seja, para uma álgebra Booleana, temos para quaisquer $a,\ b,\ c \in B$,

$$a \vee \big(b \wedge c\big) \ = \ (a \vee b) \wedge (a \vee c) \, .$$

Em particular, se $a \preceq c$, ou seja, se $a \vee c = c$, temos

$$a \vee \big(b \wedge c\big) \ = \ (a \vee b) \wedge c \, .$$

Um reticulado $R$ (que não necessariamente seja distributivo ou limitado) é dito ser um *reticulado modular* se para cada $b \in R$ valer

$$a \preceq c \ \text{ implica } \ a \vee \big(b \wedge c\big) \ = \ (a \vee b) \wedge c \, . \tag{2.19}$$

Essa propriedade é denominada *propriedade modular*, ou *modularidade*. Um reticulado não necessariamente distributivo que satizfaça (2.19) é dito ser um *reticulado modular*. Como vimos, toda álgebra Booleana é um reticulado modular. A propriedade modular é, por assim dizer, uma versão enfraquecida da distributividade.

É relevante notar que se $b = \neg a$, então (2.19) afirma que

$$a \preceq c \ \text{ implica } \ a \vee \big((\neg a) \wedge c\big) \ = \ c \, . \tag{2.20}$$

pois $a \vee \neg a = 1$.

Essa é uma versão ainda mais enfraquecida da distributividade e conduz à definição de *reticulado ortomodular*.

• **Reticulados ortomodulares**

Um reticulado ortocomplementado $R$ é dito ser um *reticulado ortomodular* se para todos $a,\ c \in R$ valer

$$a \preceq c \ \text{ implica } \ c \ = \ a \vee \big(a^{\perp} \wedge c\big) \, . \tag{2.21}$$

Essa identidade é denominada *propriedade ortomodular*, ou *ortomodularidade*.

## 2.1.3 Semigrupos, Monoides e Grupos

Nesta seção introduziremos algumas noções algébricas de grande importância.

• **Quase-grupos e loops**

Um *quase-grupo* é um conjunto $Q$, dotado de uma operação binária $Q \times Q \to Q$, denotada por "$\cdot$", tal que para todo par $a$ e $b \in Q$ existem $x$ e $y \in Q$, únicos, satisfazendo $x \cdot a = b$ e $a \cdot y = b$.

Em palavras, um quase-grupo é uma estrutura onde a "divisão", à esquerda e à direita, é sempre possível.

Um *loop* $L$ é um quase-grupo com elemento neutro, ou seja, é um quase-grupo no qual existe um elemento $e$, denominado *identidade*, tal que $a \cdot e = e \cdot a = a$ para todo $a \in L$.

O elemento neutro de um loop é sempre único, pois se $e'$ é também um elemento neutro, segue que $e' = e' \cdot e = e$.

Em um loop, todo elemento possui uma única *inversa à direita* e uma única *inversa à esquerda* (não necessariamente iguais). Ou seja, para cada $a \in L$ existem um único elemento em $L$ que denotamos por $a_l^{-1}$, denominado *inverso à esquerda de* $a$, tal que $a_l^{-1} \cdot a = e$ e um único elemento em $L$ que denotamos por $a_r^{-1}$, denominado *inverso à direita de* $a$, tal que $a \cdot a_r^{-1} = e$. A existência e unicidade de tais elementos é consequência da propriedade definidora de quase-grupo.

• **Semigrupos**

Um *semigrupo* é um conjunto não vazio $S$ dotado de uma operação binária $S \times S \to S$ denotada por "$\cdot$" e denominada *produto* tal que a seguinte propriedade é satisfeita.

1. *Associatividade.* Para todos $a,\ b$ e $c \in S$ vale $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

• **Monoides**

Um *monoide* é um conjunto não vazio $M$ dotado de uma operação binária $M \times M \to M$ denotada por "$\cdot$" e denominada *produto* tal que as seguintes propriedades são satisfeitas.

1. *Associatividade.* Para todos $a,\ b$ e $c \in M$ vale $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. *Elemento neutro.* Existe um (único!) elemento $e \in M$, denominado elemento neutro, tal que $g \cdot e = e \cdot g = g$ para todo $g \in M$.

*Observação.* A unicidade do elemento neutro é garantida pela observação que se houvesse $e' \in M$ tal que $g \cdot e' = e' \cdot g = g$ para todo $g \in M$ teríamos $e' = e' \cdot e = e$. ♣

• **Grupos**

Uma das noções mais fundamentais de toda a Matemática é a de *grupo*. Um grupo é um conjunto não vazio $G$ dotado de uma operação binária $G \times G \to G$, denotada por "$\cdot$" e denominada *produto*, e de uma operação unária $G \to G$ (bijetora) denominada *inversa*, denotada pelo expoente "$^{-1}$", tais que as seguintes propriedades são satisfeitas.

1. *Associatividade.* Para todos $a,\ b$ e $c \in G$ vale $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. *Elemento neutro.* Existe um (único!) elemento $e \in G$, denominado elemento neutro, tal que $g \cdot e = e \cdot g = g$ para todo $g \in G$.
3. *Inversa.* Para cada $g \in G$ existe um (único!) elemento $h \in G$ tal que $g \cdot h = h \cdot g = e$. Esse elemento é denominado a inversa de $g$ e denotado por $g^{-1}$.

*Observações elementares.*

1. A unicidade do elemento neutro é garantida pela observação que se houvesse $e'$ tal que $g \cdot e' = e' \cdot g = g$ para todo $g \in G$ teríamos $e' = e' \cdot e = e$.
2. Analogamente se estabelece a unicidade da inversa, pois se $g,\ h \in G$ são tais que $h \cdot g = g \cdot h = e$, teremos, usando a associatividade, $g^{-1} = g^{-1} \cdot e = g^{-1} \cdot (g \cdot h) = (g^{-1} \cdot g) \cdot h = e \cdot h = h$.
3. A função $G \ni g \mapsto g^{-1} \in G$, que associa cada elemento de $G$ à sua inversa, é um exemplo de uma função unária.
4. Como $e \cdot e = e$, segue que $e^{-1} = e$.
5. Para todo $g \in G$ vale $\left(g^{-1}\right)^{-1} = g$ pois, usando a associatividade,

$$\left(g^{-1}\right)^{-1} \;=\; \left(\,g^{-1}\right)^{-1} \cdot e \;=\; \left(g^{-1}\right)^{-1} \cdot \left(g^{-1} \cdot g\right) \;=\; \left(\left(g^{-1}\right)^{-1} \cdot g^{-1}\right) \cdot g \;=\; e \cdot g \;=\; g\,.$$

Todo grupo é, trivialmente, um quase-grupo, um loop, um semigrupo e um monoide. ♣

Um grupo $G$ é dito ser *comutativo* ou *Abeliano*[17] se $a \cdot b = b \cdot a$ para todos $a,\ b \in G$. Essa nomenclatura se aplica também a semigrupos e monoides.

Existe uma construção canônica devida a Grothendieck, que discutimos na Seção 2.6.1, página 246, que permite construir um grupo Abeliano a partir de um semigrupo Abeliano dado. Essa construção é importante em várias áreas da Matemática. O leitor interessado poderá passar sem perda à discussão da Seção 2.6.1.

Os primeiros grupos caracterizados foram os chamados *grupos de permutação*, que surgiram provelmente pela primeira vez na obra de Galois[18]. A definição moderna, mais geral, apresentada acima, é devida a Cayley[19].

• **Exemplos simples**

1. O conjunto $S = \{1,\ 2,\ 3,\ \ldots\}$ é um semigrupo em relação à operação de soma usual. O conjunto $M = \{0,\ 1,\ 2,\ 3,\ \ldots\}$ é um monoide em relação à operação de soma usual, sendo o elemento neutro $e = 0$. O conjunto $G = \mathbb{Z} = \{\ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \ldots\}$ é um grupo Abeliano em relação à operação de soma usual, sendo o elemento neutro $e = 0$ e a inversa $n^{-1} = -n$. Esse grupo é comummente denotado por $(\mathbb{Z},\ +)$, para lembrar o conjunto considerado (no caso, $\mathbb{Z}$) e a operação considerada nesse conjunto (no caso, $+$).

[17] Niels Henrik Abel (1802–1829).
[18] Évariste Galois (1811–1832).
[19] Arthur Cayley (1821–1895).

2. $\mathbb{R}$ dotado da operação de multiplicação usual é um monoide onde o elemento neutro é o número 1. Não é um grupo, pois 0 não tem inversa multiplicativa.

3. O conjunto $\mathbb{R}_+ := \{x \in \mathbb{R},\ x > 0\}$ é um semigrupo Abeliano em relação à operação de soma, mas não é um monoide.

4. O conjunto $\mathbb{R}_{0+} := \{x \in \mathbb{R},\ x \geq 0\}$ é um monoide Abeliano em relação à operação de soma mas não um grupo.

5. O conjunto dos números racionais $\mathbb{Q}$ é um grupo Abeliano em relação à operação usual de soma de números racionais. Esse grupo é comummente denotado por $(\mathbb{Q},\ +)$.

6. O conjunto $\mathbb{Q} \setminus \{0\} = \{r \in \mathbb{Q},\ r \neq 0\}$ é um grupo Abeliano em relação à operação usual de produto de números racionais. Esse grupo é comummente denotado por $\big(\mathbb{Q} \setminus \{0\},\ \cdot\big)$.

7. O conjunto dos números reais $\mathbb{R}$ é um grupo Abeliano em relação à operação usual de soma de números reais. Esse grupo é comummente denotado por $(\mathbb{R},\ +)$.

8. O conjunto dos números complexos $\mathbb{C}$ é um grupo Abeliano em relação à operação usual de soma de números complexos. Esse grupo é comummente denotado por $(\mathbb{C},\ +)$.

9. O conjunto $\mathbb{R} \setminus \{0\} = \{x \in \mathbb{R},\ x \neq 0\}$ é um grupo Abeliano em relação à operação usual de produto de números reais. Esse grupo é comummente denotado por $\big(\mathbb{R} \setminus \{0\},\ \cdot\big)$.

10. O conjunto $\mathbb{C} \setminus \{0\} = \{z \in \mathbb{C},\ z \neq 0\}$ é um grupo Abeliano em relação à operação usual de produto de números complexos. Esse grupo é comummente denotado por $\big(\mathbb{C} \setminus \{0\},\ \cdot\big)$.

11. $\mathrm{Mat}\,(\mathbb{C},\ n)$, o conjunto das matrizes complexas $n \times n$ com o produto usual de matrizes é apenas um monoide.

12. $\mathrm{Mat}\,(\mathbb{C},\ n)$, o conjunto das matrizes complexas $n \times n$ é um grupo em relação à operação de soma de matrizes.

13. O conjunto $\mathrm{GL}(n,\ \mathbb{R})$ de todas as matrizes reais $n \times n$ com determinante não nulo (e, portanto, inversíveis) é um grupo em relação à operação de produto usual de matrizes. $\mathrm{GL}(n,\ \mathbb{R})$ é não Abeliano se $n > 1$.

14. O conjunto $\mathrm{GL}(n,\ \mathbb{C})$ de todas as matrizes complexas $n \times n$ com determinante não nulo (e, portanto, inversíveis) é um grupo em relação à operação de produto usual de matrizes. $\mathrm{GL}(n,\ \mathbb{C})$ é não Abeliano se $n > 1$.

15. O conjunto $\mathrm{GL}(n,\ \mathbb{Q})$ de todas as matrizes racionais $n \times n$ com determinante não nulo (e, portanto, inversíveis) é um grupo não Abeliano (se $n > 1$) em relação à operação de produto usual de matrizes. O conjunto $\mathrm{GL}(n,\ \mathbb{Z})$ de todas as matrizes inteiras $n \times n$ com determinante não nulo (e, portanto, inversíveis) é um monoide não Abeliano (se $n > 1$) em relação à operação de produto usual de matrizes. Não é um grupo, pois a inversa de uma matriz inversível com entradas inteiras não é sempre uma matriz com entradas inteiras[20].

16. O conjunto $\mathrm{SL}(n,\ \mathbb{C})$ de todas as matrizes complexas $n \times n$ com determinante igual a 1 (e, portanto, inversíveis) é um grupo não Abeliano (se $n > 1$) em relação à operação de produto usual de matrizes. O mesmo é verdadeiro para $\mathrm{SL}(n,\ \mathbb{R})$, $\mathrm{SL}(n,\ \mathbb{Q})$ e $\mathrm{SL}(n,\ \mathbb{Z})$, as matrizes reais, racionais ou inteiras, respectivamente, com determinante igual a 1.

17. O conjunto de todas as matrizes complexas $n \times n$ cujo determinante tem módulo igual a 1: $\{A \in \mathrm{Mat}\,(\mathbb{C},\ n) |\ |\det(A)| = 1\}$, é um grupo não Abeliano (se $n > 1$) em relação à operação de produto usual de matrizes.

18. Seja $X$ um conjunto não vazio. A coleção $\mathbb{P}(X)$ de todos os subconjuntos de $X$, é um monoide Abeliano com relação à operação de união de conjuntos, o elemento neutro sendo o conjunto vazio. Justifique!

19. Analogamente, a coleção $\mathbb{P}(X) \setminus \{\emptyset\}$ de todos os subconjuntos não vazios de $X$, é um semigrupo Abeliano com relação à operação de união de conjuntos.

20. A coleção $\mathbb{P}(X)$ de todos os subconjuntos de $X$, é um monoide Abeliano com relação à operação de intersecção de conjuntos, o elemento neutro sendo o conjunto $X$. Justifique!

---

[20] Por exemplo, a inversa da matriz $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}(2,\ \mathbb{Z})$ é a matriz $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$ (verifique!), a qual não é elemento de $\mathrm{GL}(2,\ \mathbb{Z})$.

21. Analogamente, a coleção $\mathbb{P}(X) \setminus \{X\}$ de todos os subconjuntos $X$ distintos de $X$, é um semigrupo Abeliano com relação à operação de intersecção de conjuntos.

22. Seja $X$ um conjunto não vazio. Então, $\mathbb{P}(X)$ é um grupo Abeliano em relação à operação de diferença simétrica $A \triangle B := \big(A \cup B\big) \setminus \big(A \cap B\big)$, para $A,\ B \in X$, definida em (1.32), página 66. De fato, a Proposição 1.2, página 67, garante associatividade e comutatividade, o elemento neutro é o conjunto vazio $\emptyset$ e para todo $A \in \mathbb{P}(X)$ tem-se $A^{-1} = A$. Verifique!

    Um grupo onde cada elemento tem a si mesmo como inversa é dito ser um *grupo Booleano*[21].

23. Outro exemplo importante é o seguinte. Seja $C$ um conjunto não vazio e tomemos $S = C^C$, o conjunto de todas as funções de $C$ em $C$. Então, $S$ é um monoide com o produto formado pela *composição* de funções: $f \circ g$, e onde o elemento neutro é a função identidade $\mathrm{id}(s) = s$, $\forall s \in C$. O subconjunto de $C^C$ formado pelas funções bijetoras de $C$ em $C$ é um grupo não Abeliano, onde o produto é a composição de funções, o elemento neutro é a função identidade e o elemento inverso de uma função $f : C \to C$ é a função inversa $f^{-1}$. Esse grupo é denominado *grupo de permutações do conjunto* $C$ e denotado por $\mathrm{Perm}(C)$.

**E. 2.9** *Exercício*. Em caso de dúvida, prove todas as afirmações acima. ✠

**• Exercícios com mais exemplos**

**E. 2.10** *Exercício*. Seja $U$ um espaço vetorial e denote-se por $\mathcal{E}(U)$ a coleção de todos os seus subespaços (incluindo o próprio $U$ e o subespaço nulo $\{0\}$). Podemos definir em $\mathcal{E}(U)$ a operação de soma de subespaços, denotada por "+", da seguinte forma: se $V$ e $W$ são subespaços de $U$ denotamos por $V + W$ o subespaço de $U$ dado por $V \oplus W := \{v + w,\ v \in V,\ w \in W\}$.

Mostre que essa operação é de fato uma operação binária em $\mathcal{E}(U)$, ou seja, que $V + W$ é, de fato, um subespaço de $U$. Mostre que essa operação é associativa, comutativa e que ela possui um elemento neutro: o subespaço nulo $\{0\}$. Conclua que $(\mathcal{E}(U),\ +)$ é um monoide Abeliano. ✠

**E. 2.11** *Exercício*. Considere o conjunto $\mathbb{R}_+ = \{x \in \mathbb{R},\ x > 0\}$ dos reais positivos. Mostre que

$$a * b \ := \ \frac{ab}{a+b}, \qquad a,\ b \in \mathbb{R}_+ \ , \tag{2.22}$$

define uma operação em $\mathbb{R}_+$ e que essa operação é associativa e comutativa, mas que não possui elemento neutro (e, portanto, não apresenta elementos inversos). ✠

**E. 2.12** *Exercício*. Considere o intervalo $(0,\ 1)$. Mostre que

$$a * b \ := \ \frac{ab}{1 - a - b + 2ab} \ , \qquad a,\ b \in (0,\ 1) \ , \tag{2.23}$$

define uma operação no intervalo $(0,\ 1)$ e que essa operação é associativa, comutativa e possui um elemento neutro, que é o número $1/2 \in (0,\ 1)$. Mostre também que a inversa de um elemento $a \in (0,\ 1)$ por essa operação é o elemento $1 - a \in (0,\ 1)$. Dessa forma o intervalo $(0,\ 1)$ munido da operação $*$ é um grupo comutativo.

Esse exemplo será aprofundado quando do tratamento de espaços vetoriais. Vide Exercício E. 2.33, página 142. ✠

### 2.1.3.1 $\mathbb{R}_{0+}$ Estendido

O conjunto $\mathbb{R}_{0+} = \{x \in \mathbb{R},\ x \geq 0\}$ é um monoide Abeliano em relação à operação de soma e em relação à operação de produto e vale ainda a propriedade distributiva $a(b+c) = ab+ac$. Sabidamente, $\mathbb{R}_{0+}$ é também um conjunto linearmente ordenado pela relação de ordem usual.

Vamos abaixo descrever um outro conjunto linearmente ordenado que contém $\mathbb{R}_{0+}$ e é também um monoide Abeliano em relação à operação de soma e em relação à operação de produto e vale ainda a propriedade distributiva.

[21] George Boole (1815–1864).

Definimos um conjunto, que denotaremos por $\mathscr{R}_+$, juntando a $\mathbb{R}_{0+}$ um conjunto formado por um elemento extra, elemento esse que denotaremos provisoriamente por $\omega$, com $\omega \notin \mathbb{R}_{0+}$, para o qual certas relações algébricas serão definidas. Seja $\mathscr{R}_+ := \mathbb{R}_{0+} \cup \{\omega\}$ e definamos as operações de soma e produto em $\mathscr{R}_+$ da seguinte forma: se $a$ e $b$ são elementos de $\mathbb{R}_{0+}$ suas soma $a+b$ e seu produto $ab$ são definidos como usualmente. Fora isso, valem

1. $a + \omega = \omega + a = \omega$, para todo $a \in \mathbb{R}_{0+}$.
2. $\omega + \omega = \omega$.
3. $a\omega = \omega a = \omega$, para todo $a \in \mathbb{R}_{0+}$, $a \neq 0$.
4. $0\omega = \omega 0 = 0$.
5. $\omega\omega = \omega$.

**E. 2.13** *Exercício.* Verifique que $\mathscr{R}_+$ é um monoide Abeliano em relação à operação de soma e em relação à operação de produto definidas acima e que vale ainda a propriedade distributiva. ✣

$\mathscr{R}_+$ é linearmente ordenado tomando-se em $\mathbb{R}_{0+}$ a relação de ordem usual e fixando-se $a < \omega$ para todo $a \in \mathbb{R}_{0+}$.

O conjunto $\mathscr{R}_+$ com as estruturas definidas acima é por vezes denominado *conjunto estendido dos reais não negativos*.

É bastante claro que na definição abstrata acima o objeto representado pelo símbolo $\omega$ desempenha o papel formalmente atribuído a um número infinito positivo. A construção das relações algébricas acima prescinde, porém, dessa noção, pois $\omega$ pode ser qualquer objeto (fora de $\mathbb{R}_{0+}$).

Com um certo abuso de linguagem, é costume, substituir o símbolo $\omega$ pelo símbolo $\infty$, dando a entender que $\omega$ representa algo como um número infinito positivo. É comum também denotar-se $\mathscr{R}_+$ por $[0, \infty]$.

**E. 2.14** *Exercício.* Que problemas surgem quando se tenta estender a construção acima para o conjunto $\mathbb{R}$ de todos os reais? ✣

O conjunto estendido $\mathscr{R}_+$ desempenha um papel na Teoria da Medida e Integração e outras áreas.

### 2.1.3.2 Homomorfismos e Isomorfismos entre Grupos

• **Homomorfismos entre grupos**

Dados dois grupos $G$ e $H$ uma função $\phi : G \to H$ é dita ser um *homomorfismo* ou *morfismo de grupos* se

$$\phi(ab) \;=\; \phi(a)\phi(b) \tag{2.24}$$

para todos $a,\ b \in G$. Sejam $e_G$ e $e_H$ os elementos neutros de $G$ e de $H$, respectivamente. Duas observações são pertinentes sobre um homomorfismo $\phi : G \to H$: 1º $\phi(e_G) = e_H$ e 2º $\phi\big(g^{-1}\big) = \phi(g)^{-1}$ para todo $g \in G$.

O primeiro fato decorre das seguintes relações autoexplicativas, que fazem uso da associatividade dos produtos em $G$ e em $H$ e da propriedade definidora (2.24):

$$\phi(e_G) \;=\; \phi(e_G)e_H \;=\; \phi(e_G)\big(\phi(e_G)\phi(e_G)^{-1}\big) \;=\; \big(\phi(e_G)\phi(e_G)\big)\phi(e_G)^{-1} \;=\; \big(\phi(e_Ge_G)\big)\phi(e_G)^{-1}$$

$$=\; \phi(e_G)\phi(e_G)^{-1} \;=\; e_H\,.$$

A segunda segue de um raciocício similar: para qualquer $g \in G$, tem-se

$$\phi\big(g^{-1}\big) \;=\; \phi\big(g^{-1}\big)e_H \;=\; \phi\big(g^{-1}\big)\big(\phi(g)\phi(g)^{-1}\big) \;=\; \Big(\phi\big(g^{-1}\big)\phi(g)\Big)\phi(g)^{-1} \;=\; \phi(g^{-1}g)\phi(g)^{-1}$$

$$=\; \phi(e_G)\phi(g)^{-1} \;=\; e_H\phi(g)^{-1} \;=\; \phi(g)^{-1}\,.$$

Mais propriedades importantes de homomorfismos de grupos serão estudadas na Seção 2.2.2, página 173 e na Seção 2.2.2.1, página 176. Vide também Seção 2.1.10, página 163.

• **Isomorfismos entre grupos**

Um homomorfismo $\phi : G \to H$ entre dois grupos é dito ser um *isomorfismo* se for bijetor. Cabe aqui observar que se um homomorfismo $\phi : G \to H$ for bijetor, então sua inversa $\phi^{-1} : H \to G$ é também um homomorfismo. De fato, se $h_1,\ h_2 \in H$, então, devido ao fato de $\phi$ ser sobrejetor, existem $g_1,\ g_2 \in G$, únicos (por $\phi$ ser injetivo), tais que $h_1 = \phi(g_1)$ e $h_2 = \phi(g_2)$, ou seja, $g_1 = \phi^{-1}(h_1)$ e $g_2 = \phi^{-1}(h_2)$ e, dessa forma,

$$\phi^{-1}(h_1h_2) \;=\; \phi^{-1}\big(\phi(g_1)\phi(g_2)\big) \;=\; \phi^{-1}\big(\phi(g_1g_2)\big) \;=\; g_1g_2 \;=\; \phi^{-1}(h_1)\phi^{-1}(h_2)\;,$$

onde, na segunda igualdade, usamos o fato de $\phi$ ser um homomorfismo.

Dizemos que dois grupos $G$ e $H$ são isomorfos se houver um isomorfismo $\phi : G \to H$ entre eles. Esse fato é denotado simbolicamente por $G \simeq_\phi H$ (ou simplesmente $G \simeq H$, quando $\phi$ é subentendido).

Moralmente, podemos afirmar que dois grupos isomorfos são o "mesmo" grupo, já que todas as operações realizadas em um grupo podem ser fielmente reproduzidas no outro por via do isomorfismo.

• **Exemplos elementares**

Um exemplo são os grupos $G = (\mathbb{R},\ +)$, o grupo aditivo dos reais, e $H = (\mathbb{R}_+,\ \cdot)$ (aqui $\mathbb{R}_+ \equiv (0,\ \infty)$), o grupo multiplicativo dos reais positivos. Há um isomorfismo entre eles dado pela função exponencial, que a cada $x \in G$ associa o elemento de $H$ dado por $e^x$. De fato, para todos $x,\ y \in \mathbb{R}$ vale, sabidamente, $e^xe^y = e^{x+y}$, o que estabelece que a função exponencial é um homomorfismo de $G$ em $H$. Fora isso, a função exponencial é uma bijeção entre $\mathbb{R}$ e $\mathbb{R}_+$ e, portanto, define um isomorfismo entre os grupos $G = (\mathbb{R},\ +)$ e $H = (\mathbb{R}_+,\ \cdot)$. Esses dois grupos podem ser assim moralmente identificados, já que as operações de soma em $\mathbb{R}$ podem ser fielmente traduzidas em operações de produto[22] em $\mathbb{R}_+$.

Um exemplo relevante de um homomorfismo que não é um isomorfismo se dá entre os grupos $G = \mathrm{GL}(n,\ \mathbb{C})$, $n > 1$, o grupo das matrizes complexas $n \times n$, e o grupo $H = \big(\mathbb{C} \setminus \{0\},\ \cdot\big)$, o grupo multiplicativo dos complexos não nulos. Há um homomorfismo de $G$ em $H$ dado por

$$\phi(A) \;=\; \det(A), \qquad \in \mathrm{GL}(n,\ \mathbb{C})\;.$$

De fato, trata-se de um homomorfismo, pois pela bem conhecida regra do determinante do produto de matrizes (vide Teorema 10.1, página 534) para quaisquer $A,\ B \in \mathrm{GL}(n,\ \mathbb{C})$ tem-se $\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B)$. É fácil ver que $\phi$ é sobrejetora (qualquer número complexo não nulo é o determinante de alguma matriz de $\mathrm{GL}(n,\ \mathbb{C})$), mas não é injetora, pois matrizes distintas de $\mathrm{GL}(n,\ \mathbb{C})$ podem ter o mesmo determinante. Assim, o determinante é um homomorfismo de $\mathrm{GL}(n,\ \mathbb{C})$ em $\big(\mathbb{C} \setminus \{0\},\ \cdot\big)$, mas não um isomorfismo. Comentamos que para $n > 1$ os grupos $\mathrm{GL}(n,\ \mathbb{C})$ e $\big(\mathbb{C} \setminus \{0\},\ \cdot\big)$ não podem ser isomorfos, pois o primeiro não é comutativo, enquanto que o segundo o é.

Outros exemplos relevantes de homomorfismos e isomorfismos entre grupos surgirão no restante do capítulo.

Mais propriedades importantes de isomorfismos de grupos serão estudadas na Seção 2.2.2, página 173 e na Seção 2.2.2.1, página 176. Vide também Seção 2.1.10, página 163.

▲▲▲▲▲▲▲▲▲▲▲▲

A noção de isomorfismo entre grupos é útil no estudo de uma classe de grupos bastante relevante, os chamados grupos $\mathbb{Z}_n$, $n \in \mathbb{N}$, grupos esses de interesse em diversas áreas da Matemática e da Física, tratados na Seção 2.1.3.3.

### 2.1.3.3 Os Grupos $\mathbb{Z}_n$. O Grupo do Círculo

Vamos aqui apresentar três caracterizações diferentes dos chamados *grupos* $\mathbb{Z}_n$, com $n \in \mathbb{N}$ sendo um número natural dado. O caso $\mathbb{Z}_1$ é o grupo trivial, composto de apenas do elemento neutro. Essas caracterizações fazem uso da chamada *Divisão Euclidiana*, que apresentamos na Proposição 2.1. Para apreciarmos essas diferentes caracterizações usaremos a noção de isomorfismo entre grupos.

[22] Esse fato teve uso prático no passado –desde a Idade Média (ao menos) até o advento dos computadores eletrônicos– quando taboas de logaritmos eram empregadas por calculistas para simplificar o cômputo de produtos de números, transformando-os em somas e reduzindo, assim, a quantidade de operações demandadas.

• **A Divisão Euclidiana**

Faremos no que segue uso da seguinte proposição, conhecida como *Divisão Euclidiana*[23]. Vide *e.g.*, [226] para uma outra demonstração.

**Proposição 2.1 (Divisão Euclidiana)** *Seja $n \in \mathbb{N}$, fixo. Então, todo número inteiro $z$ pode ser escrito de maneira única como $z = qn + r$, onde $q \in \mathbb{Z}$ e $r \in \{0,\ 1, \ldots,\ n-1\}$. O número $r$ é denominado* resto da divisão de $z$ por $n$ *e é também denotado por $r = z \bmod n$.* □

*Comentário*. Existem algoritmos para a determinação explícita de $q$ e $r$, como o *Algoritmo de Euclides*, mas eles não nos concernem aqui. ♣

Prova da Proposição 2.1. Seja $n \in \mathbb{N}$, fixo. Considere-se para cada $k \in \mathbb{Z}$ o conjunto $J_k := \{kn,\ \ldots,\ kn + n - 1\}$. Esse conjunto é composto por $n$ elementos sucessivos, sendo o menor deles $\min(J_k) = kn$ e o maior $\max(J_k) = kn + n - 1$. Cabe agora observar que não existe nenhum inteiro $a$ satisfazendo

$$\max(J_k) \ < \ a \ < \ \min(J_{k+1})$$

pois, caso contrário valeria $(k+1)n - 1 < a < (k+1)n$, o que é impossível, pois $(k+1)n - 1$ e $(k+1)n$ são inteiros sucessivos. Assim, o menor elemento de $J_{k+1}$ é o sucessor do maior elemento de $J_k$.

Esses fatos implicam que $J_k$ e $J_{k+1}$ são conjuntos disjuntos, não havendo nenhum inteiro entre ambos. Concluímos facilmente disso que a união de todos os conjuntos $J_k$ é o conjunto $\mathbb{Z}$, a união sendo disjunta:

$$\mathbb{Z} \ = \ \bigcup_{k \in \mathbb{Z}} J_k \ , \qquad J_k \cap J_l = \emptyset \text{ sempre que } \ k \neq l \ .$$

Dessa forma, se $z \in \mathbb{Z}$, podemos afirmar que existe um único $q \in \mathbb{Z}$ tal que $z \in J_q$. Isso está nos dizendo que $z = qn + r$, para algum $r \in \{0,\ 1, \ldots,\ n-1\}$. A unicidade de $r$ é evidente. ■

• **O grupo $\mathbb{Z}_n$**

A *Divisão Euclidiana*, apresentada acima, afirma que, dado $n \in \mathbb{N}$, então todo número inteiro $z$ pode ser escrito de maneira única na forma $z = qn + r$, onde $q \in \mathbb{Z}$ e $r \in \{0,\ 1, \ldots,\ n-1\}$. O número $r$ é denominado *resto da divisão de $z$ por $n$* e é também denotado por $r = z \bmod n$.

Seja $n$ um inteiro positivo maior ou igual a 2 e seja o conjunto $\{0,\ 1,\ \ldots,\ n-1\}$. Vamos definir uma operação binária em $\{0,\ 1,\ \ldots,\ n-1\}$, denominada *soma* e denotada pelo símbolo "+", da seguinte forma:

$$\alpha + \beta = \{\alpha + \beta\} \bmod n$$

para todos $\alpha,\ \beta \in \{0,\ 1,\ \ldots,\ n-1\}$. Acima $\{\alpha + \beta\}$ representa a soma usual de números inteiros em $\mathbb{Z}$.

**E. 2.15** *Exercício*. Prove que a operação de soma definida acima é uma operação binária de $\{0,\ 1,\ \ldots,\ n-1\}$ e mostre que a mesma é associativa, comutativa e tem 0 como elemento neutro. ✠

**E. 2.16** *Exercício*. Para cada $a \in \{0,\ 1,\ \ldots,\ n-1\}$, defina $a^{-1} = \{n - a\} \bmod n$. Mostre que $a^{-1} \in \{0,\ 1,\ \ldots,\ n-1\}$ e que $a + a^{-1} = 0$. ✠

Os dois exercícios acima provam que $\{0,\ 1,\ \ldots,\ n-1\}$ é um grupo Abeliano em relação à operação de soma definida acima. Esse grupo é denominado grupo $\mathbb{Z}_n$.

• **Definindo os grupos $\mathbb{Z}_n$ a partir de uma relação de equivalência**

O grupo $\mathbb{Z}_n$ pode também ser definido de uma maneira alternativa usando relações de equivalência. Fixemos $n \in \mathbb{N}$ e consideremos o conjunto dos números inteiros $\mathbb{Z}$. Estabeleçamos em $\mathbb{Z}$ a seguinte relação de equivalência: dois números $m_1,\ m_2 \in \mathbb{Z}$ são equivalentes, $m_1 \simeq m_2$, se a diferença $m_2 - m_1$ for um múltiplo inteiro de $n$, ou seja $m_2 - m_1 = kn$ para algum $k \in \mathbb{Z}$. Deixamos como exercício (fácil) ao leitor provar que se trata realmente de uma relação de equivalência. As

[23] Euclides de Alexandria (ci. 325 A.C, ci. 265 A.C.).

classes de equivalência de $\mathbb{Z}$ por essa relação são biunivocamente associadas aos elementos do conjunto $\{0,\ 1,\ \ldots,\ n-1\}$, ou seja, o conjunto das classes $\big\{[0],\ [1],\ \ldots,\ [n-1]\ \big\}$, que denotamos por $\mathbb{Z}(n)$, contém <u>todas</u> as classes de equivalência de $\mathbb{Z}$ pela relação acima. Essa afirmação é novamente uma consequência da *Divisão Euclidiana*, Proposição 2.1, página 133, segundo o qual todo $z \in \mathbb{Z}$ é equivalente a algum elemento $r$ do conjunto $\{0,\ 1,\ \ldots,\ n-1\}$. É claro também que dois elementos distintos de $\{0,\ 1,\ \ldots,\ n-1\}$ não podem ser equivalentes (a diferença entre eles é menor que $n$ em valor absoluto).

Assim, as classes de equivalência de $\mathbb{Z}$ são precisamente $[0],\ [1],\ \ldots,\ [n-1]$. Podemos agora introduzir uma operação nessas classes, definindo

$$[a] + [b] \ := \ [a+b]\ .$$

para todos $a,\ b \in \{0,\ 1,\ \ldots,\ n-1\}$. Deixamos ao leitor a tarefa simples de provar que essa definição independe dos representantes tomados nas classes[24], que essa operação é associativa, comutativa e tem a casse $[0]$ como elemento neutro. Além disso, podemos associar a cada $[a]$ um elemento inverso, a saber, a classe $[n-a] = [-a]$.

Esses fatos mostram que a coleção de classes $\mathbb{Z}(n) = \big\{[0],\ [1],\ \ldots,\ [n-1]\ \big\}$ compõe um grupo Abeliano, que é isomorfo ao grupo $\mathbb{Z}_n$ definido anteriormente, com o isomorfismo $h_1 : \mathbb{Z}(n) \to \mathbb{Z}_n$ sendo dado simplesmente por

$$h_1\big([k]\big) \ = \ k, \qquad k \ = \ 0,\ \ldots,\ n-1\ .$$

**E. 2.17** *<u>Exercício</u>.* Mostre que $h_1$ é, de fato, um isomorfismo entre $\mathbb{Z}(n)$ e $\mathbb{Z}_n$. ✠

Vemos assim que, para cada $n \in \mathbb{N}$, os grupos $\mathbb{Z}_n$ e $\mathbb{Z}(n)$ são isomorfos e, portanto, podemos moralmente afirmar que trata-se do mesmo grupo. De fato, alguns textos substituem nossa definição de $\mathbb{Z}_n$ pela de $\mathbb{Z}(n)$. Há ainda uma terceira definição para $\mathbb{Z}_n$, usando raízes $n$-ésimas da unidade.

• **<u>O grupo $\mathbb{Z}_n$ e raízes $n$-ésimas da unidade</u>**

Considere-se o conjunto $\mathbb{F}_n \equiv \Big\{ \exp\big(\frac{2\pi k i}{n}\big),\ k \ = \ 0,\ \ldots,\ n-1 \Big\}$ composto pelas raízes $n$-ésimas de 1, ou seja, por todos os números complexos $z$ satisfazendo $z^n = 1$. Esse conjunto compõe um grupo pela operação usual de multiplicação de números complexos, como pode ser facilmente verificado (faça-o!).

Esse grupo é isomorfo ao grupo $\mathbb{Z}(n)$, definido acima, sendo o isomorfismo $h_2 : \mathbb{Z}(n) \to \mathbb{F}_n$ dado por

$$h_2\big([k]\big) \ = \ \exp\left(\frac{2\pi k i}{n}\right), \qquad k \ = \ 0,\ \ldots,\ n-1\ .$$

**E. 2.18** *<u>Exercício (fácil)</u>.* Mostre que $h_2$ é, de fato, um isomorfismo entre $\mathbb{Z}(n)$ e $\mathbb{F}_n$. ✠

* * *

Vemos assim que, para cada $n \in \mathbb{N}$, os três grupos $\mathbb{Z}_n$, $\mathbb{Z}(n)$ e $\mathbb{F}_n$ são isomorfos e, portanto, podemos moralmente afirmar que trata-se do mesmo grupo. Por isso, cada definição dos três grupos, acima, pode ser apresentada como definição alternativa do grupo $\mathbb{Z}_n$, como pode ser observado em certos textos.

Há ainda mais uma maneira de se definir o grupo $\mathbb{Z}_n$, fazendo uso do chamado *Primeiro Teorema de Isomorfismos*, tal como apresentado no Exercício E. 2.88, página 177.

• **<u>Uma generalização. O grupo do círculo</u>**

As ideias que conduziram à definição dos grupos $\mathbb{Z}_n$ podem ser estendidas a outras situações.

Seja $T > 0$ e considere-se o intervalo semiaberto $[0,\ T)$ de $\mathbb{R}$. Podemos fazer desse intervalo um grupo, procedendo-se da seguinte forma. Primeiramente, observe-se que $\mathbb{R}$ pode ser escrito como a união disjunta de intervalos do tipo $\big[nT,\ (n+1)T\big)$, com $n \in \mathbb{Z}$:

$$\mathbb{R} \ = \ \bigcup_{n \in \mathbb{Z}} \big[nT,\ (n+1)T\big)\ .$$

[24] Entenda-se: se $a \sim a'$ então $[a] = [a']$ e cabe provar que $[a+b] = [a'+b]$ para qualquer $b \in \mathbb{Z}$, o que é deixado como exercício.

Cada intervalo $\big[nT,\ (n+1)T\big)$ é obtido do intervalo $[0,\ T)$ transladando-o de $nT$ unidades. Assim podemos afirmar que cada $x \in \mathbb{R}$ está localizado em um único intervalo $\big[qT,\ (q+1)T\big)$ para algum $q \in \mathbb{Z}$ e, portanto, pode ser escrito de forma <u>única</u> como

$$x \ = \ qT + r$$

com $r \in [0,\ T)$. Escrevemos,

$$r \ = \ x \mod T \, .$$

Podemos agora definir uma operação no intervalo $[0,\ T)$, que denotamos por $\dot{+}_T$, por

$$x \,\dot{+}_T\, y \ := \ (x+y) \mod T \, ,$$

sendo $(x+y)$ a soma usual dos números reais $x$ e $y$. Quando $T$ for subentendido, denotamos essa operação simplesmente por $\dot{+}$.

**E. 2.19** *<u>Exercício</u>*. Seja $T > 0$, fixo. Constate que a operação $\dot{+}$ definida acima é, de fato, uma operação no conjunto $[0,\ T)$, que essa operação é associativa, comutativa, tem $0$ como elemento neutro e cada $x \in [0,\ T)$ tem por inversa o elemento $(T-x) \mod T$ de $[0,\ T)$. ✠

Vemos, assim, que $[0,\ T)$ dotado do produto $\dot{+}$ é um grupo Abeliano, que denotamos por $\mathbb{R}(T)$. Esse grupo é também denotado na literatura por $\mathbb{R}/\{nT,\ n \in \mathbb{Z}\}$.

Há, porém, o seguinte fato importante: todos os grupos $\mathbb{R}(T)$, $T > 0$, são isomorfos.

**E. 2.20** *<u>Exercício</u>*. Sejam $T_1,\ T_2 > 0$. Mostre que a função $\phi : [0,\ T_1) \to [0,\ T_2)$ dada por $\phi(x) = \frac{T_2}{T_1} x$ é um <u>isomorfismo</u> entre $\mathbb{R}(T_1)$ e $\mathbb{R}(T_2)$. ✠

O grupo $\mathbb{R}(2\pi)$ é denominado *grupo do círculo*, pois o intervalo $[0,\ 2\pi)$ pode ser interpretado como o conjunto dos ângulos (em radianos) que descrevem (univocamente!) os pontos do círculo unitário e a operação $\dot{+}$ representa a soma desses ângulos. Veremos no futuro que $\mathbb{R}(2\pi)$ é isomorfo aos grupos $\mathrm{SO}(2)$ e ao grupo $\mathrm{U}(1)$.

Como são isomorfos, cada grupo $\mathbb{R}(T)$, $T > 0$, também é denominado *grupo do círculo*. No caso $T = 1$, o grupo $\mathbb{R}(1)$ é frequentemente denotado por $\mathbb{R}/\mathbb{Z}$ na literatura.

### 2.1.3.4 Subgrupos

Seja $G$ um grupo em relação a uma operação "$\cdot$" e cujo elemento neutro seja $e$. Um subconjunto $H$ de $G$ é dito ser um *subgrupo* de $G$ se for também por si só um grupo em relação à mesma operação, ou seja, se

1. $e \in H$,
2. $h_1 \cdot h_2 \in H$ para todos $h_1 \in H$ e $h_2 \in H$,
3. $h^{-1} \in H$ para todo $h \in H$.

Todo grupo $G$ sempre possui pelo menos dois subgrupos: o próprio $G$ e o subgrupo $\{e\}$ formado apenas pelo elemento neutro de $G$. Esses dois subgrupos são denominados *subgrupos triviais* de $G$. Se um subgrupo $H$ de $G$ não coincidir com nenhum dos subgrupos triviais de $G$, dizemos que $H$ é um *subgrupo próprio* de $G$. Por vezes, na literatura, a simbologia $H < G$ é usada para indicar que $H$ é um subgrupo próprio de $G$, mas evitaremos usar isso.

É fácil verificar que $(\mathbb{Z},\ +)$ e $(\mathbb{Q},\ +)$ são subgrupos de $(\mathbb{R},\ +)$, o grupo aditivo dos reais. O grupo multiplicativo dos reais positivos, $(\mathbb{R}_+,\ \cdot)$, é um subgrupo do grupo multiplicativo dos reais, $\big(\mathbb{R} \setminus \{0\},\ \cdot\big)$.

É fácil ver que $\mathrm{SL}(n,\ \mathbb{R})$, o conjunto de todas as matrizes reais $n \times n$ com determinante igual a 1, é um subgrupo de $\mathrm{GL}(n,\ \mathbb{R})$. Idem para $\mathrm{SL}(n,\ \mathbb{C})$ em relação a $\mathrm{GL}(n,\ \mathbb{C})$.

**E. 2.21** *<u>Exercício</u>*. Seja $D_a = \{a^m,\ m \in \mathbb{Z}\}$ para algum $a > 0$. Mostre que $D_a$ é um subgrupo de $(\mathbb{R}_+,\ \cdot)$, o grupo multiplicativo dos reais positivos. Para $a,\ b > 0$, mostre que $D_{a,\,b} = \{a^m b^n,\ m,\ m \in \mathbb{Z}\}$ é também um subgrupo de $(\mathbb{R}_+,\ \cdot)$. ✠

Um fato relevante é expresso na seguinte proposição:

**Proposição 2.2** *Seja $G$ um grupo e seja $\{H_\lambda,\ \lambda \in \Lambda\}$ uma coleção não vazia arbitrária de subgrupos de $G$. Então, $\bigcap_{\lambda\in\Lambda} H_\lambda$ é um subgrupo de $G$. Consequentemente, $\bigcap_{\lambda\in\Lambda} H_\lambda$ é um subgrupo de cada $H_\lambda$ com $\lambda \in \Lambda$.* □

Prova. É evidente que o elemento neutro de $G$ pertente a $\bigcap_{\lambda\in\Lambda} H_\lambda$, pois pertence a cada $H_\lambda$. Se $h_1$ e $h_2$ são elementos de $\bigcap_{\lambda\in\Lambda} H_\lambda$, então ambos pertencem a cada $H_\lambda$, assim como o produto $h_1h_2$ (pois cada $H_\lambda$ é um subgrupo de $G$). Portanto $h_1h_2 \in \bigcap_{\lambda\in\Lambda} H_\lambda$. Analogamente, se $h \in \bigcap_{\lambda\in\Lambda} H_\lambda$, então $h$ pertence a cada $H_\lambda$, assim como $h^{-1}$ (novamente pois cada $H_\lambda$ é um subgrupo de $G$), implicando que $h^{-1} \in \bigcap_{\lambda\in\Lambda} H_\lambda$. ■

• **Subgrupos gerados por um subconjunto de um grupo**

Se $G$ é um grupo e $A$ é um subconjunto não vazio de $G$ denotamos por $[A]$ o *subgrupo gerado* por $A$ que, por definição, vem a ser a intersecção de todos os subgrupos de $G$ que contêm $A$: $[A] := \bigcap_{H\in\mathcal{A}} H$, onde $\mathcal{A}$ é a coleção de todos os subgrupos de $G$ que contém $A$. Essa coleção nunca é vazia, pois o próprio grupo $G$ contém $A$. É lícito dizer que $[A]$ é o "menor" subgrupo de $G$ que contém o conjunto $A$ pois, pela definição, qualquer outro subgrupo de $G$ que contenha $A$ conterá também $[A]$.

**E. 2.22** *Exercício.* Determine o subgrupo gerado por $\{1\}$ nos grupos $(\mathbb{Z},\ +)$, $(\mathbb{Q},\ +)$, $(\mathbb{R},\ +)$, $(\mathbb{Q}\setminus\{0\},\ \cdot)$ e $(\mathbb{R}\setminus\{0\},\ \cdot)$. ✣

• **Semigrupos cancelativos e não-cancelativos**

Um elemento $a$ de um semigrupo $S$ é dito ser *cancelável à esquerda* se $a\cdot b = a\cdot c$ valer para $b,\ c \in S$ se e somente se $b = c$. Analogamente, um elemento $a$ de um semigrupo $S$ é dito ser *cancelável à direita* se $b\cdot a = c\cdot a$ valer para $b,\ c \in S$ se e somente se $b = c$.

Se todo elemento de um semigrupo $S$ for cancelável à esquerda (à direita), então $S$ é dito ser um *semigrupo cancelativo à esquerda (à direita)*. Se $S$ for cancelativo à esquerda e à direita, então $S$ dito ser um *semigrupo cancelativo*.

Monoides cancelativos (à direita e à esquerda) são definidos analogamente.

**Exemplos 2.11** Vamos a alguns exemplos ilustrativos de semigrupos e de monoides cancelativos ou não.

1. $(\mathbb{N},\ +)$ é um semigrupo Abeliano cancelativo. $(\mathbb{N},\ \cdot)$ é um monoide Abeliano cancelativo.
2. Seja $X$ um conjunto não vazio. A coleção $\mathbb{P}(X)$ de todos os subconjuntos de $X$, é um monoide Abeliano com relação à operação de união de conjuntos, o elemento neutro sendo o conjunto vazio. Esse monoide é não cancelativo, pois se $A,\ B$ e $C$ forem subconjuntos de $X$ tais que $A\cup B = A\cup C$, não segue necessariamente que $B = C$. Justifique!
3. Analogamente, a coleção $\mathbb{P}(X)\setminus\{\emptyset\}$ de todos os subconjuntos não vazios de $X$, é um semigrupo Abeliano não cancelativo com relação à operação de união de conjuntos.
4. Seja $X$ um conjunto não vazio. A coleção $\mathbb{P}(X)$ de todos os subconjuntos de $X$, é um monoide Abeliano com relação à operação de intersecção de conjuntos, o elemento neutro sendo o conjunto $X$. Esse monoide é não cancelativo, pois se $A,\ B$ e $C$ forem subconjuntos de $X$ tais que $A\cap B = A\cap C$, não segue necessariamente que $B = C$. Justifique!
5. Analogamente, a coleção $\mathbb{P}(X)\setminus\{X\}$ de todos os subconjuntos $X$ distintos de $X$, é um semigrupo Abeliano não cancelativo com relação à operação de intersecção de conjuntos.
6. Todo grupo é um semigrupo cancelativo (devido à existência de inversa).
7. $\mathrm{Mat}\,(\mathbb{C},\ n)$, $n > 1$, é um monoide não Abeliano pela multiplicação usual de matrizes e todas as matrizes inversíveis são canceláveis à direita e à esquerda. Como um todo, porém, $\mathrm{Mat}\,(\mathbb{C},\ n)$ não é um monoide cancelativo, pois se $A,\ B$ e $C$ são elementos de $\mathrm{Mat}\,(\mathbb{C},\ n)$ e vale $AB = AC$, não necessariamente segue que $B = C$ caso $A$ seja não inversível.
8. O monoide Abeliano $(\mathcal{E}(U),\ +)$, formado pelos subespaços de um espaço vetorial $U$ (vide Exercício E. 2.10, página 130), não é cancelativo (pois para quaisquer subespaços $V$ e $W$ de $U$ vale $V + U = W + U = U$).
9. O monoide Abeliano $(\mathscr{R}_+,\ +)$ (vide página 130) não é cancelativo (pois $a + \omega = \omega + a = \omega$ para todo $a \in \mathscr{R}_+$). Idem para o monoide Abeliano $(\mathscr{R}_+,\ \cdot)$.

⧫

• **Semigrupos cancelativos Abelianos**

Todo semigrupo Abeliano cancelativo é isomorfo a um semigrupo contido dentro de um grupo, especificamente, do

chamado grupo de Grothendieck associado a esse semigrupo Abeliano. Essa afirmação é demonstrada no Exercício E. 2.149, página 247.

### 2.1.4 Corpos

Um *corpo*[25] é um conjunto não vazio $\mathbb{K}$ dotado de duas operações binárias, denotadas por "+" e "$\cdot$", denominadas *soma* e *produto*, respectivamente, satisfazendo o seguinte :

1. A operação de soma tem as seguintes propriedades:
   (a) Comutatividade: para todos $\alpha,\ \beta \in \mathbb{K}$ vale $\alpha + \beta = \beta + \alpha$.
   (b) Associatividade: para todos $\alpha,\ \beta,\ \gamma \in \mathbb{K}$ vale $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
   (c) Elemento neutro: existe um elemento $0 \in \mathbb{K}$, chamado de *elemento nulo*, ou *zero*, tal que $\alpha + 0 = \alpha$ para todo $\alpha \in \mathbb{K}$.
   (d) Inversa: para cada $\alpha \in \mathbb{K}$ existe um elemento denotado por $\beta$, único, com a propriedade $\alpha + \beta = 0$. Esse elemento é mais comummente denotado por $-\alpha$.
2. A operação de produto tem as seguintes propriedades:
   (a) Comutatividade: para todos $\alpha,\ \beta \in \mathbb{K}$ vale $\alpha \cdot \beta = \beta \cdot \alpha$.
   (b) Associatividade: para todos $\alpha,\ \beta,\ \gamma \in \mathbb{K}$ vale $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.
   (c) Elemento neutro: existe um elemento $1 \in \mathbb{K}$, chamado de *unidade*, tal que $\alpha \cdot 1 = \alpha$ para todo $\alpha \in \mathbb{K}$.
   (d) Inversa: para cada $\alpha \in \mathbb{K}$, $\alpha \neq 0$, existe um único elemento denotado por $\beta$ com a propriedade $\alpha \cdot \beta = 1$. Esse elemento é mais comummente denotado por $\alpha^{-1}$.
3. Distributividade: o produto é distributivo em relação à adição: para todos $\alpha,\ \beta,\ \gamma \in \mathbb{K}$ vale $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Alguns autores consideram conveniente incluir também a hipótese de que o elemento neutro e o elemento nulo são distintos, $1 \neq 0$, pois doutra forma teríamos $\mathbb{K} = \{0\}$ (justifique!), uma situação um tanto trivial.

Note-se que corpos são grupos comutativos em relação à operação de soma e monoides comutativos em relação à operação de produto. Pelo que comentamos anteriormente, isso garante a unicidade do elemento nulo e da unidade de um corpo. A distributividade é a única propriedade listada acima que relaciona as operações de soma e produto.

Os elementos de um corpo são por vezes denominados *escalares*. Por motivos estruturais é importante frisar que um corpo depende em sua definição do conjunto $\mathbb{K}$ e das operações binárias "+" e "$\cdot$" nele definidas e muitas vezes nos referiremos a um corpo como sendo uma tripla $(\mathbb{K},\ +,\ \cdot)$. É frequente omitir-se o símbolo "$\cdot$" de produto por escalares quando nenhuma confusão é possível.

Em um corpo $\mathbb{K}$ sempre vale que $\alpha \cdot 0 = 0$ para todo $\alpha \in \mathbb{K}$. De fato, como $0 = 0 + 0$, segue que

$$\alpha \cdot 0 \ = \ \alpha \cdot (0 + 0) \ = \ \alpha \cdot 0 + \alpha \cdot 0 \, .$$

Somando-se a ambos os lados o elemento inverso $-\alpha \cdot 0$ teremos

$$\alpha \cdot 0 + (-\alpha \cdot 0) \ = \ \alpha \cdot 0 + \alpha \cdot 0 + (-\alpha \cdot 0) \, ,$$

ou seja,

$$0 \ = \ \alpha \cdot 0 + 0 \ = \ \alpha \cdot 0 \, ,$$

como queríamos provar. Pela comutatividade do produto vale também $0 \cdot \alpha = 0$ para todo $\alpha \in \mathbb{K}$.

É fácil verificar que $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos em relação às operações usuais de soma e produto. Esses são os exemplos que inspiraram a definição. Outros exemplos serão discutidos logo abaixo. O conjunto das matrizes $n \times n$ para qualquer $n \geq 2$ com o produto usual de matrizes não é um corpo pois, entre outras razões, o produto não é comutativo.

[25] Em inglês a palavra empregada é *field*. A expressão em português provavelmente provém do francês *corp* ou do alemão *Körper*.

**E. 2.23** *Exercício*. Seja $\mathcal{K}$ um conjunto constituído de dois elementos distintos $a$ e $b$, e considere as seguintes operações, "+" e "$\cdot$", definidas em $\mathcal{K}$:

$$\begin{array}{ll} a+a \,=\, a\,, & a\cdot a \,=\, a\,, \\ b+b \,=\, a\,, & a\cdot b \,=\, b\cdot a \,=\, a\,, \\ a+b \,=\, b+a \,=\, b\,, & b\cdot b \,=\, b\,. \end{array}$$

Mostre que $\mathcal{K}$, munido dessas operações, é um corpo. ✠

• **Os corpos quadráticos**

**E. 2.24** *Exercício*. Um número natural diferente de 0 ou 1 é dito ser um *inteiro sem fator quadrático* se não for múltiplo de um quadrado perfeito. Seja $d$ um inteiro sem fator quadrático e seja $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d},\ a,\ b \in \mathbb{Q}\}$. Mostre que $\mathbb{Q}(\sqrt{d})$ é um corpo, denominado *corpo (real) quadrático*. ✠

Todo número primo inteiro sem fator quadrático é há um interesse particular no caso em que $d$ é um número primo.

**E. 2.25** *Exercício*. Mostre que o conjunto de todos os números reais da forma $a+b\sqrt{2}$, com $a$ e $b$ racionais, é um corpo. Esse corpo é denotado por $\mathbb{Q}(\sqrt{2})$. ✠

**E. 2.26** *Exercício*. Generalizando o exercício anterior, seja $p$ um número primo. Mostre que o conjunto de todos os números reais da forma $a + b\sqrt{p}$, com $a$ e $b$ racionais, é um corpo. Esse corpo é denotado por $\mathbb{Q}(\sqrt{p})$. ✠

**E. 2.27** *Exercício*. Mostre que o conjunto de todos os números reais da forma $a + b\sqrt{2}$ com $a$ e $b$ inteiros **não** é um corpo. ✠

• **Os corpos $\mathbb{Z}_p$, com $p$ primo**

Como observamos na Seção 2.1.3.3, página 132, os conjuntos $\mathbb{Z}_n = \{0,\ 1,\ \ldots,\ n-1\}$, com $n \in \mathbb{N}$, $n \geq 2$, são grupos Abelianos com a soma definida por

$$\alpha + \beta \;=\; [\alpha + \beta] \bmod n\,,$$

para $\alpha,\ \beta \in \mathbb{Z}_n$, onde $[\alpha+\beta]$ denota a soma usual em $\mathbb{Z}$. Podemos também considerar em $\mathbb{Z}_n$ uma operação de produto, definida por,

$$\alpha \cdot \beta \;=\; [\alpha\beta] \bmod n\,,$$

onde $[\alpha\beta]$ denota o produto usual em $\mathbb{Z}$. Podemos nos perguntar: será $\mathbb{Z}_n$ sempre um corpo em relação à essas duas operações? O exercício abaixo mostra que nem sempre a resposta é positiva.

**E. 2.28** *Exercício*. Considere o conjunto $\mathbb{Z}_4 = \{0,\ 1,\ 2,\ 3\}$. Constate que nele o produto do elemento 2 consigo mesmo resulta no elemento nulo. Conclua disso que 2 não pode possuir inversa multiplicativa e constate por inspeção que tal é realmente o caso. ✠

Quando então $\mathbb{Z}_n$ pode ser um corpo? A resposta é dada no seguinte teorema:

**Teorema 2.1** *O conjunto $\mathbb{Z}_n$ é um corpo com as operações acima definidas se e somente se $n$ for um número primo.* □

Prova. As operações de soma e produto definidas acima são comutativas, associativas e distributivas (justifique!). Fora isso sempre vale que $-\alpha = n - \alpha$ para todo $\alpha \in \mathbb{Z}_n$. Resta-nos estudar a existência de elementos inversos $\alpha^{-1}$. Vamos supor que $\mathbb{Z}_n$ seja um corpo. Então, $a \in \{2,\ \ldots,\ n-1\}$ tem uma inversa em $\mathbb{Z}_n$, ou seja, um número $b \in \{1,\ \ldots,\ n-1\}$ tal que $a \cdot b = 1$. Lembrando a definição de produto em $\mathbb{Z}_n$, isso significa que existe um inteiro $r$ tal que $ab = rn + 1$. Mas isso implica

$$b - \frac{1}{a} \;=\; r\left(\frac{n}{a}\right)\,.$$

Como o lado esquerdo não é um número inteiro, o lado direito também não pode ser. Isso diz, então, que $n/a$ não pode ser inteiro para nenhum $a \in \{2,\ \ldots,\ n-1\}$, ou seja, $n$ não tem divisores e é, portanto, um primo. Resta-nos mostrar que $\mathbb{Z}_p$ é efetivamente um corpo quando $p$ é primo, o que agora se reduz a mostrar que para todo $a \in \mathbb{Z}_p$ existe um elemento inverso.

Para apresentar a demonstração, recordemos três conceitos da teoria de números. **1.** Sejam dois números inteiros $f$ e $g$, dizemos que $f$ *divide* $g$ se $g/f \in \mathbb{Z}$. Se $f$ *divide* $g$, denotamos esse fato por $f|g$. **2.** Sejam dois números inteiros $f$ e $g$. O *máximo divisor comum* de $f$ e $g$, denotado $\text{mdc}(f,\ g)$ é o maior inteiro $m$ tal que $m|f$ e $m|g$. **3.** Dois números inteiros $f$ e $g$ são ditos ser *primos entre si* se $\text{mdc}(f,\ g) = 1$.

A demonstração da existência de inverso em $\mathbb{Z}_p$ será apresentada em partes. Vamos primeiro demonstrar a seguinte afirmativa.

**Lema 2.3** *Se $f$ e $g$ são dois números inteiros quaisquer, então existem inteiros $k'$ e $l'$ tais que*

$$mdc(f,\ g) \ = \ k'f + l'g \ .$$

□

Prova. Seja $m = \text{mdc}(f,\ g)$. Seja $M$ o conjunto de todos os números positivos que sejam da forma $kf + lg$ com $k$ e $l$ inteiros. Seja $m'$ o menor elemento de $M$. Note que como os elementos de $M$ são positivos, esse menor elemento existe. Claramente

$$m' \ = \ k'f + l'g \tag{2.25}$$

para algum $k'$ e $l'$. Como, por definição, $m|f$ e $m|g$, segue que $m|m'$, o que só é possível se

$$m' \geq m. \tag{2.26}$$

Vamos agora demonstrar por contradição que $m'|f$. Se isso não fosse verdade, existiriam (pela *Divisão Euclidiana*, Proposição 2.1, página 133) inteiros $\alpha$ e $\beta$ com

$$0 < \beta < m' \tag{2.27}$$

tal que

$$f \ = \ \alpha m' + \beta \ .$$

Usando (2.25) isso diz que

$$\beta \ = \ f - \alpha(k'f + l'g) = (1 - \alpha k')f + (-\alpha l')g \ .$$

Mas, como $\beta > 0$ isso diz que $\beta \in M$. Logo, $\beta \geq m'$, contradizendo (2.27). Logo $m'|f$. De maneira totalmente análoga prova-se que $m'|g$. Portanto $m' \leq \text{mdc}(f,\ g) = m$. Lembrando que havíamos provado (2.26), segue que $m = m'$ e, portanto $m = k'f + l'g$, demonstrando o Lema. ■

**Corolário 2.1** *Se $f$ e $g$ são dois números inteiros primos entre si, então existem inteiros $k'$ e $l'$ tais que*

$$1 \ = \ k'f + l'g \ .$$

□

Prova. Pela definição, como $f$ e $g$ são dois números inteiros primos entre si segue que $\text{mdc}(f,\ g) = 1$. ■

Para finalmente demonstrarmos a existência de inverso em $\mathbb{Z}_p$, com $p$ primo, seja $a \in \{1,\ \ldots,\ p-1\}$. É óbvio que $a$ e $p$ são primos entre si (por quê?). Assim, pelo corolário, existem inteiros $r$ e $s$ com

$$1 \ = \ sa - rp \ .$$

Isso diz que $sa = rp + 1$. Logo, definindo $b \in \mathbb{Z}_p$ como sendo $b = s \mod p$ teremos

$$ba \ = \ (s \mod p)a = (rp + 1) \mod p = 1 \ ,$$

ou seja, $b = a^{-1}$, completando a demonstração do Teorema 2.1. ■

• **Isomorfismos entre corpos**

Dois corpos $\mathbb{K}_1$ e $\mathbb{K}_2$ são ditos isomorfos se existir uma aplicação bijetora $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ que preserve as operações algébricas de $\mathbb{K}_1$ e $\mathbb{K}_2$, ou seja, tal que

$$\phi(a+b) \;=\; \phi(a)+\phi(b)\;, \qquad \phi(ab) \;=\; \phi(a)\phi(b)\;, \qquad \phi(1_{\mathbb{K}_1}) \;=\; 1_{\mathbb{K}_2} \quad \text{e} \quad \phi(0_{\mathbb{K}_1}) \;=\; 0_{\mathbb{K}_2}\;.$$

Acima, $1_{\mathbb{K}_j}$ e $0_{\mathbb{K}_j}$ são a unidade e o elemento nulo, respectivamente, de $\mathbb{K}_j$, $j = 1,\ 2$. É elementar constatar que $\phi(-a) = -\phi(a)$ para todo $a \in \mathbb{K}_1$ e que $\phi(a^{-1}) = \phi(a)^{-1}$ para todo $a \in \mathbb{K}_1$, $a \neq 0_{\mathbb{K}_1}$.

Comentemos que as propriedades $\phi(1_{\mathbb{K}_1}) \;=\; 1_{\mathbb{K}_2}$ $\phi(0_{\mathbb{K}_1}) \;=\; 0_{\mathbb{K}_2}$ são, em verdade, consequências das duas propriedades anteriores: $\phi(a+b) \;=\; \phi(a)+\phi(b)$ e $\phi(ab) \;=\; \phi(a)\phi(b)$, válidas para todos $a,\ b \in \mathbb{K}_1$.

**E. 2.29** *Exercício*. Justifique essa afirmação! ✠

**E. 2.30** *Exercício*. Considere o conjunto $M$ de todas as matrizes reais $2 \times 2$ da forma $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$, com $a,\ b \in \mathbb{R}$. Mostre que esse conjunto é um corpo em relação às operações usuais de soma e produto de matrizes. Mostre que esse corpo é isomorfo ao corpo $\mathbb{C}$ pelo isomorfismo $\phi : \mathbb{C} \to M$ dado por $\phi(a+bi) := \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ para todos $a,\ b \in \mathbb{R}$. ✠

O leitor que apreciou o Exercício E. 2.30 é estimulado a posteriormente estudar a noção de quatérnio, apresentada neste texto na Seção 2.6.3, página 250, pois aquela noção generaliza de diversas formas o conteúdo do exercício.

• **Característica de um corpo**

Seja $\mathbb{K}$ um corpo e 1 sua unidade. Para um número natural $n \in \mathbb{N}$ definimos $n \cdot 1 := \underbrace{1 + \cdots + 1}_{n \text{ vezes}}$.

Um corpo $\mathbb{K}$ é dito ter *característica zero* se não existir $n \in \mathbb{N}$ não nulo tal que $n \cdot 1 = 0$. De outra forma, a *característica* de $\mathbb{K}$ é definida como sendo o menor $n \in \mathbb{N}$ não nulo tal que $n \cdot 1 = 0$.

**Exemplos 2.12** $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{2})$ têm característica zero. Os corpos $\mathbb{Z}_p$, com $p$ primo, têm característica $p$. Mostre isso! ♦

**E. 2.31** *Exercício*. Mostre que a característica de um corpo é ou igual a zero ou é um número primo. Sugestão: Mostre primeiro que $(nm) \cdot 1 = (n \cdot 1)(m \cdot 1)$ para quaisquer números naturais $n$ e $m$. Use, então, o fato que todo natural pode ser decomposto em um produto de fatores primos e use o fato que, em um corpo, se $ab = 0$, segue que ou $a$ ou $b$ ou ambos são zero (ou seja, todo corpo é um anel de integridade: não tem divisores de zero). ✠

## 2.1.5 Espaços Vetoriais

Um espaço vetorial $V$ sobre um corpo $\mathbb{K}$ é um conjunto de elementos chamados *vetores* dotado de uma operação "+": $V \times V \to V$ denominada *soma vetorial* e também de um *produto por escalares* "$\cdot$": $\mathbb{K} \times V \to V$ com as seguintes propriedades:

1. A cada par $u,\ v \in V$ de vetores é associado um elemento $u + v \in V$, denominado *soma* de $u$ e $v$, com as seguintes propriedades:
   (a) A soma é comutativa: $u + v = v + u$ para todos $u,\ v \in V$.
   (b) A soma é associativa: $u + (v + w) = (u + v) + w$ para todos $u,\ v,\ w \in V$.
   (c) Existe um único vetor denotado por 0, denominado *vetor nulo*, tal que $u + 0 = u$ para todo $u \in V$.
   (d) A cada $u \in V$ existe associado um único vetor denotado por $-u$ tal que $u + (-u) = 0$.
2. A cada par $\alpha \in \mathbb{K}$, $u \in V$ existe associado um vetor denotado por $\alpha \cdot u \in V$, denominado *produto de $u$ por $\alpha$*, de forma que
   (a) O produto por escalares é associativo: $\alpha \cdot (\beta \cdot u) = (\alpha\beta) \cdot u$, para todos $\alpha,\ \beta \in \mathbb{K}$ e $u \in V$, onde $\alpha\beta$ é o produto de $\alpha$ por $\beta$ em $\mathbb{K}$.

(b) $1 \cdot u = u$ para todo $u \in V$, onde 1 é a unidade de $\mathbb{K}$.

(c) O produto por escalares é distributivo em relação à soma de vetores: $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$, para todo $\alpha \in \mathbb{K}$ e todos $u,\ v \in V$.

(d) O produto por escalares é distributivo em relação à soma de escalares: $(\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u$, para todos $\alpha,\ \beta \in \mathbb{K}$ e todo $u \in V$.

Note-se que espaços vetoriais são grupos comutativos em relação à operação de soma, fato que, como comentamos anteriormente, garante a unicidade do vetor nulo.

Os elementos de um corpo sobre os quais um espaço vetorial se constitui são frequentemente denominados *escalares*. É frequente omitir-se o símbolo "$\cdot$" de produto por escalares quando nenhuma confusão é possível. É de se notar também que emprega-se o símbolo "+" tanto para a operação de adição do corpo $\mathbb{K}$ quanto para a operação de adição do espaço vetorial $V$, ainda que se trate de operações distintas. Igualmente usamos o mesmo símbolo "0" para designar o vetor nulo de $V$ e o elemento nulo de $\mathbb{K}$. Raramente esses usos são fonte de confusão.

**E. 2.32** *Exercício.* Mostre, usando os postulados acima, que $0 \cdot u = 0$ para todo $u \in V$, onde, permitindo-nos um certo abuso de linguagem, o 0 do lado esquerdo representa o zero do corpo $\mathbb{K}$ e o do lado direito o vetor nulo de $V$. Em seguida, prove que para todo $\alpha \in \mathbb{K}$ e todo $u \in V$ vale $(-\alpha) \cdot u = -(\alpha \cdot u)$, sendo que $-\alpha$ denota a inversa aditiva de $\alpha$ em $\mathbb{K}$ e $-(\alpha \cdot u)$ denota a inversa aditiva de $\alpha \cdot u$ em $V$. ✠

• **Alguns exemplos elementares de espaços vetoriais**

Ao estudante iniciante sugerimos provar com detalhe as afirmações feitas sobre os exemplos que seguem.

1. Se $\mathbb{K}$ é um corpo, então $\mathbb{K}$ é um espaço vetorial sobre $\mathbb{K}$ com as mesmas operações de soma e produto definidas em $\mathbb{K}$.

2. Se $\mathbb{K}$ é um corpo e $\mathbb{L}$ é um subcorpo de $\mathbb{K}$ (ou seja, um subconjunto de $\mathbb{K}$ que é por si só um corpo com as operações definidas em $\mathbb{K}$), então $\mathbb{K}$ é um espaço vetorial sobre $\mathbb{L}$. Por exemplo, $\mathbb{R}$ é um espaço vetorial sobre $\mathbb{Q}$ (esse espaço é curioso, por ser um espaço de dimensão infinita. Vide Seção 2.3.1, página 199 e seguintes).

3. Se $\mathbb{K}$ é um corpo, o produto Cartesiano $\mathbb{K}^n = \{(k_1,\ \ldots,\ k_n),\ k_j \in \mathbb{K},\ j = 1,\ \ldots,\ n\}$ é um espaço vetorial sobre $\mathbb{K}$ com a operação de soma definida por $(k_1,\ \ldots,\ k_n) + (l_1,\ \ldots,\ l_n) = (k_1 + l_1,\ \ldots,\ k_n + l_n)$ e o produto por escalares por $\alpha \cdot (k_1,\ \ldots,\ k_n) = (\alpha k_1,\ \ldots,\ \alpha k_n)$ para todo $\alpha \in \mathbb{K}$. O vetor nulo é o vetor $(0,\ \ldots,\ 0)$.

   Os três exemplos a seguir são casos particulares daquele acima.

4. O produto Cartesiano $\mathbb{R}^n = \{(x_1,\ \ldots,\ x_n),\ x_j \in \mathbb{R},\ j = 1,\ \ldots,\ n\}$ é um espaço vetorial sobre $\mathbb{R}$ com a operação de soma definida por $(x_1,\ \ldots,\ x_n) + (y_1,\ \ldots,\ y_n) = (x_1 + y_1,\ \ldots,\ x_n + y_n)$ e o produto por escalares por $\alpha \cdot (x_1,\ \ldots,\ x_n) = (\alpha x_1,\ \ldots,\ \alpha x_n)$ para todo $\alpha \in \mathbb{R}$. O vetor nulo é o vetor $(0,\ \ldots,\ 0)$.

5. O produto Cartesiano $\mathbb{C}^n = \{(z_1,\ \ldots,\ z_n),\ z_j \in \mathbb{C},\ j = 1,\ \ldots,\ n\}$ é um espaço vetorial sobre $\mathbb{C}$ (sobre $\mathbb{R}$) com a operação de soma definida por $(z_1,\ \ldots,\ z_n) + (w_1,\ \ldots,\ w_n) = (z_1 + w_1,\ \ldots,\ z_n + w_n)$ e o produto por escalares por $\alpha \cdot (z_1,\ \ldots,\ z_n) = (\alpha z_1,\ \ldots,\ \alpha z_n)$ para todo $\alpha \in \mathbb{C}$ (para todo $\alpha \in \mathbb{R}$). O vetor nulo é o vetor $(0,\ \ldots,\ 0)$.

6. Para $p$ primo, o produto Cartesiano $(\mathbb{Z}_p)^n = \{(z_1,\ \ldots,\ z_n),\ z_j \in \mathbb{Z}_p,\ j = 1,\ \ldots,\ n\}$ é um espaço vetorial sobre $\mathbb{Z}_p$ com a operação de soma definida por $(z_1,\ \ldots,\ z_n) + (w_1,\ \ldots,\ w_n) = (z_1 + w_1,\ \ldots,\ z_n + w_n)$ e o produto por escalares por $\alpha \cdot (z_1,\ \ldots,\ z_n) = (\alpha z_1,\ \ldots,\ \alpha z_n)$ para todo $\alpha \in \mathbb{Z}_p$. O vetor nulo é o vetor $(0,\ \ldots,\ 0)$.

   Note que $(\mathbb{Z}_p)^n$ tem um número finito de elementos, a saber $p^n$.

7. Se $\mathbb{K}$ é um corpo, o conjunto $\mathrm{Mat}\,(\mathbb{K},\ m,\ n)$, de todas as matrizes $m \times n$ cujos elementos de matriz pertencem a $\mathbb{K}$, é um espaço vetorial sobre $\mathbb{K}$, com a soma sendo a soma usual de matrizes e o produto por escalares sendo o produto usual de matrizes por números escalares. O vetor nulo é a matriz nula.

8. O conjunto $\mathrm{Mat}\,(\mathbb{R},\ m,\ n)$, de todas as matrizes reais $m \times n$, é um espaço vetorial sobre $\mathbb{R}$, com a soma sendo a soma usual de matrizes e o produto por escalares sendo o produto usual de matrizes por números reais. O vetor nulo é a matriz nula.

9. O conjunto $\mathrm{Mat}\,(\mathbb{C},\ m,\ n)$, de todas as matrizes complexas $m \times n$, é um espaço vetorial sobre $\mathbb{C}$ (sobre $\mathbb{R}$), com a soma sendo a soma usual de matrizes e o produto por escalares sendo o produto usual de matrizes por números complexos (reais). O vetor nulo é a matriz nula.

10. Este exemplo generaliza vários dos anteriores. Sejam $V$ um espaço vetorial sobre um corpo $\mathbb{K}$ e seja $C$ um conjunto não vazio. O conjunto $V^C$ de todas as funções de $C$ em $V$ é um espaço vetorial sobre $\mathbb{K}$ com a soma e o produto por escalares definidos da seguinte forma: se $f$ e $g$ são funções de $C$ em $V$ define-se a soma $f + g$ como sendo a função definida por $(f + g)(c) = f(c) + g(c)$ para todo $c \in C$ e se $\alpha \in \mathbb{K}$, então $\alpha \cdot f$ é a função definida por $(\alpha \cdot f)(c) = \alpha f(c)$ para todo $c \in C$. O vetor nulo é a função identicamente nula.

## • Exemplos "exóticos" podem ser instrutivos

Nos dois próximos exercícios vamos exibir dois exemplos um tanto exóticos de espaços vetoriais, os quais servem para ilustrar o fato de que essa noção é menos trivial do que parece.

**E. 2.33** *Exercício*. Verifique que o intervalo $V = (0,\ 1)$ é um espaço vetorial sobre o corpo dos reais com as operações[26] de soma

$$a \overset{\circ}{+} b \ := \ \frac{ab}{1 - a - b + 2ab}\,, \tag{2.28}$$

para todos $a,\ b \in (0,\ 1)$ (em particular, constate que a operação definida em (2.28) é associativa e comutativa), e com o produto por escalares $\alpha \in \mathbb{R}$ dado por

$$\alpha \cdot a \ := \ \frac{a^\alpha}{a^\alpha + (1-a)^\alpha}\,, \tag{2.29}$$

para todo $a \in V$. Verifique que o vetor nulo é o elemento $1/2 \in (0,\ 1)$ e verifique que a inversa aditiva de $a \in V$ é $\left(\overset{\circ}{-}\ a\right) = 1 - a \in V$.

Este exemplo será estudado com mais profundidade e generalizado na Seção 2.1.11, página 165. ✠

**E. 2.34** *Exercício*. O conjunto $\mathbb{R}^2 = \{\left(\begin{smallmatrix} a_1 \\ a_2 \end{smallmatrix}\right),\ a_1,\ a_2 \in \mathbb{R}\}$, dos pares ordenados de números reais, pode ser feito um espaço vetorial sobre o corpo dos complexos! A operação de soma é definida de modo usual: $\left(\begin{smallmatrix} a_1 \\ a_2 \end{smallmatrix}\right) + \left(\begin{smallmatrix} b_1 \\ b_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a_1+b_1 \\ a_2+b_2 \end{smallmatrix}\right)$. A operação de multiplicação por escalares (complexos!) é definida da seguinte forma. Seja $z = x + iy \in \mathbb{C}$, com $x,\ y \in \mathbb{R}$ sendo sua parte real e imaginária, respectivamente. Defina-se $M(z) := \left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right)$ e defina-se o produto por escalares por

$$z \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \ := \ M(z) \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \ = \ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \ = \ \begin{pmatrix} xa_1 - ya_2 \\ ya_1 + xa_2 \end{pmatrix} \ \in \ \mathbb{R}^2\,. \tag{2.30}$$

Mostre que para dois números complexos quaisquer valem $M(z) + M(w) = M(z + w)$ e $M(z)M(w) = M(zw)$. Conclua disso que (2.30) define um produto de vetores de $\mathbb{R}^2$ por escalares complexos que satisfaz todas as propriedades requeridas na definição de um espaço vetorial sobre o corpo dos complexos:

$$z \cdot \left[\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}\right] \ = \ z \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + z \cdot \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}\,, \quad (z+w) \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \ = \ z \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + w \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \quad \text{e} \quad z \cdot \left[w \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}\right] \ = \ (zw) \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}\,.$$

Se deseja entender como e por que o exemplo acima funciona, constate que

$$M\big(x + iy\big) \ = \ x\mathbb{1} + yJ\,,$$

onde $J$ é a matriz real $J := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, a qual possui a seguinte propriedade sugestiva: $J^2 = -\mathbb{1}$.

Na Seção 3.6, página 304, generalizaremos este exemplo e mostraremos como certos espaços vetoriais *reais* podem ser transformados em espaços vetoriais sobre o corpo dos números *complexos* definindo-se adequadamente o produto dos vetores por escalares. ✠

**E. 2.35** *Exercício*. Aqui vai um exemplo de uma estrutura que não define um espaço vetorial. Tomemos o conjunto dos reais com a operação de soma usual, e tomemos o corpo $\mathbb{Z}_p$ com $p$ primo. Consideremos o produto $\mathbb{Z}_p \times \mathbb{R} \to \mathbb{R}$ denotado por $\alpha \cdot x$ (com $\alpha \in \mathbb{Z}_p$ e $x \in \mathbb{R}$) dado pelo produto usual em $\mathbb{R}$ de $\alpha$ por $x$. Essa estrutura **não** forma um espaço vetorial. Mostre que a regra distributiva $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$ não é satisfeita para todo $\alpha,\ \beta \in \mathbb{Z}_p$. *Sugestão:* veja o que ocorre no caso $\mathbb{Z}_2$ se $\alpha = \beta = 1$. ✠

[26] No lado direito de ambas as expressões (2.28) e (2.29) as diversas operações, como soma, produto, divisão, exponenciação, são as operações usuais de números reais.

Outros exemplos de espaços vetoriais serão encontrados nas seções que seguem, notadamente quando tratarmos das noções de soma direta e produto tensorial de espaços vetoriais.

• **Subespaços. Intersecção de subespaços. O subespaço gerado**

Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K}$ com a operação de soma $+$ e com um vetor nulo 0. Um subconjunto $W \subset V$ que seja por si só um espaço vetorial sobre o mesmo corpo $\mathbb{K}$ com a mesma operação de soma $+$ e com um mesmo vetor nulo 0 é dito ser um *subespaço* de $V$. Um espaço vetorial $V$ sempre possui ao menos dois subespaços: o próprio $V$ e o subespaço nulo $\{0\}$. Esses dois subespaços são denominados *subespaços triviais* de $V$.

Um fato elementar, porém relevante, sobre espaços vetoriais é a seguinte observação. Se $V$ é um espaço vetorial e $V_\lambda$, $\lambda \in \Lambda$, é uma família de subespaços vetoriais de $V$, então $\bigcap_{\lambda\in\Lambda} V_\lambda$ é também uma subespaço vetorial de $V$. Temos que $0 \in \bigcap_{\lambda\in\Lambda} V_\lambda$, pois 0 é um elemento de cada $V_\lambda$. Além disso, se $a$, $b \in \bigcap_{\lambda\in\Lambda} V_\lambda$, segue para todos $\alpha$, $\beta \in \mathbb{K}$ que $\alpha a + \beta b \in V_\lambda$ para cada $\lambda \in \Lambda$ (pois $a$, $b \in V_\lambda$) e, assim, $\alpha a + \beta b \ \in \bigcap_{\lambda\in\Lambda} V_\lambda$.

Esse fato conduz a uma definição. Seja $\mathcal{A}$ um subconjunto de um espaço vetorial $V$ e seja $\Lambda$ a coleção de todos os subespaçoe vetoriais de $V$ que contêm $\mathcal{A}$ ($\Lambda$ é não vazio pois o próprio $V$ contém $\mathcal{A}$ e, portanto, é um elemento de $\Lambda$). Assim, o subconjunto de $V$ formado pela intersecção de todos os elementos de $\Lambda$ é também um subespaço de $V$, o "menor" subespaço de $V$ a conter $\mathcal{A}$. Esse subespaço é denominado *subespaço vetoral gerado pelo conjunto* $\mathcal{A} \subset V$,

*

É quase desnecessário mencionar o quão importantes espaços vetoriais são no contexto da Física, onde, porém, quase somente espaços vetoriais sobre o corpo dos reais ou dos complexos ocorrem.

## 2.1.6 Anéis, Módulos e Álgebras

Introduzimos aqui as importantes noções de anel, módulo e álgebra. Outras seções futuras, como a Seção 2.1.7, página 147, a Seção 2.1.8, página 155 e a Seção 2.4, página 234, tratarão de alguns exemplos e de certos aspectos estruturais das mesmas.

### 2.1.6.1 Anéis

Nesta breve seção limitamo-nos a apresentar a noção de anel para, em seguida, apresentar os conceitos de *módulo* e *álgebra*. Na Seção 2.1.8, página 155, mais propriedades de anéis são estudadas e mais exemplos são apresentados.

• **Anéis não associativos**

Um *anel não associativos* é um conjunto $A$ dotado de duas operações binárias denotadas por "$+$" e "$\cdot$" e denominadas *soma* e *produto*, respectivamente, tais que $A$ é um grupo Abeliano em relação à operação de soma e a operação de produto é distributiva em relação à soma: para quaisquer $a$, $b$ e $c \in A$ valem $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.

Como usual, denotamos por $-a$ a inversa aditiva do elemento $a$ de um anel não associativo.

Se 0 é o elemento neutro de um anel não associativo $A$ em relação à operação de soma, então $a \cdot 0 = 0$ pois, como $0 = 0 + 0$, tem-se pela propriedade distributiva $a \cdot 0 = a \cdot 0 + a \cdot 0$, que implica $0 = a \cdot 0 - (a \cdot 0) = a \cdot 0 + a \cdot 0 - (a \cdot 0) = a \cdot 0$.

**Exemplo 2.13** Seja $\mathrm{Mat}\,(\mathbb{Z},\ n)$ o conjunto das matrizes $n \times n$ cujos elementos de matriz são números inteiros. Para $A,\ B \in \mathrm{Mat}\,(\mathbb{Z},\ n)$ defina o produto $[A,\ B] = AB - BA$, denominado *comutador* de $A$ e $B$ onde $AB$ é o produto usual das matrizes $A$ e $B$. Então, $\mathrm{Mat}\,(\mathbb{Z},\ n)$ com o produto do comutador é um anel não associativo. ♦

Em um anel não associativo, a propriedade de associatividade do produto "$\cdot$" não é requerida. Se ela, porém, for válida, temos a estrutura de um anel.

• **Anéis**

Um *anel* é um conjunto $A$ dotado de duas operações binárias denotadas por "$+$" e "$\cdot$" e denominadas *soma* e *produto*, respectivamente, tais que $A$ é um grupo Abeliano em relação à operação de soma e um semigrupo em relação à operação

de produto (ou seja, o produto é associativo). Por fim, a operação de produto é distributiva em relação à soma: para quaisquer $a,\ b$ e $c \in A$ valem $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(a+b) \cdot c = a \cdot c + b \cdot c$.

Como usual, denotamos por $-a$ a inversa aditiva do elemento $a$ de um anel.

Se 0 é o elemento neutro de um anel $A$ em relação à operação de soma, então $a \cdot 0 = 0$ para todo $a \in A$, pois, como $0 = 0+0$, tem-se pela propriedade distributiva $a \cdot 0 = a \cdot 0 + a \cdot 0$, que implica $0 = a \cdot 0 - (a \cdot 0) = a \cdot 0 + a \cdot 0 - (a \cdot 0) = a \cdot 0$.

Observamos que alguns autores, como Bourbaki, incluem a existência de uma unidade (não nula) na definição de anel. Aqui denominaremos *anéis com unidade* tais anéis. Vide página 155.

### 2.1.6.2 Módulos

Seja $A$ um anel. Um *$A$-módulo à esquerda* é um grupo Abeliano $M$ (cujo produto, seguindo a convenção, denotaremos por "+") dotado de uma função $A \times M \to M$ que a cada par $a \in A$, $m \in M$ associa um elemento de $M$ denotado por $a \cdot m$ com as seguintes propriedades: para todos $a,\ b \in A$ e todos $m,\ n \in M$

1. $a \cdot (m+n) = a \cdot m + a \cdot n$,
2. $(a+b) \cdot m = a \cdot m + b \cdot m$,
3. $a \cdot (b \cdot m) = (ab) \cdot m$,
4. Se $A$ possuir uma identidade $e$ (i.e., um elemento neutro para o produto), então $e \cdot m = m$.

Seja $A$ um anel. Um *$A$-módulo à direita* é um grupo Abeliano $M$ dotado de uma função $M \times A \to M$ que a cada par $a \in A$, $m \in M$ associa um elemento de $M$ denotado por $m \cdot a$ com as seguintes propriedades: para todos $a,\ b \in A$ e todos $m,\ n \in M$

1. $(m+n) \cdot a = m \cdot a + n \cdot a$,
2. $m \cdot (a+b) = m \cdot a + m \cdot b$,
3. $(m \cdot b) \cdot a = m \cdot (ba)$,
4. Se $A$ possuir uma identidade $e$, então $m \cdot e = m$.

Sejam $A$ e $B$ dois anéis. Um *bimódulo* em relação a $A$ e $B$ é um grupo Abeliano $M$ dotado de duas funções $A \times M \to M$ e $M \times B \to M$ que a cada $a \in A$, $b \in B$ e $m \in M$ associam elementos de $M$ denotados por $a \cdot m$ e $m \cdot b$, respectivamente, de modo que $M$ seja um $A$-módulo à esquerda e um $B$-módulo à direita e de modo que valha

1. $a \cdot (m \cdot b) = (a \cdot m) \cdot b$ para todos $a \in A$, $b \in B$, $m \in M$.

Em um certo sentido a noção de módulo generaliza a de espaço vetorial.

### 2.1.6.3 Álgebras

Uma *álgebra* é um espaço vetorial $V$ sobre um corpo $\mathbb{K}$ dotado de uma operação de produto binária "$\cdot$" dita *produto* da álgebra, de modo que as seguintes propriedades são satisfeitas:

**a.** O produto da álgebra é distributivo em relação a soma vetorial: para todos $a,\ b$ e $c \in V$ valem

$$a \cdot (b+c) \ = \ a \cdot b + a \cdot c \quad \text{e} \quad (a+b) \cdot c \ = \ a \cdot c + b \cdot c \, .$$

**b.** O produto por escalares comuta com o produto da álgebra e é distributivo em relação a ele: para todos $a,\ b \in V$ e $\alpha \in \mathbb{K}$ vale

$$\alpha(a \cdot b) \ = \ (\alpha a) \cdot b \ = \ a \cdot (\alpha b) \, .$$

Uma álgebra $V$ é dita ser uma *álgebra comutativa* ou uma *álgebra Abeliana*[27] se para todos $a,\ b \in V$ tivermos

$$a \cdot b \ = \ b \cdot a.$$

Uma álgebra $V$ é dita ser uma *álgebra associativa* se para todos $a,\ b$ e $c \in V$ tivermos

$$a \cdot (b \cdot c) \ = \ (a \cdot b) \cdot c \ .$$

*Notação.* Se $A$ é uma álgebra associativa, podemos sem ambiguidade denotar produtos triplos como $a(bc)$ e $(ab)c$ simplesmente como $abc$. ◀

Uma álgebra que não é comutativa é dita não comutativa, ou não Abeliana, e uma álgebra que não é associativa é dita não associativa. Falaremos um pouco mais sobre álgebras não associativas à página 146.

Devemos dizer que há muitas álgebras importantes encontradas na Física que não são nem comutativas nem associativas. Por exemplo, a álgebra do produto vetorial em $\mathbb{R}^3$ não é nem comutativa nem associativa.

Os seguintes comentários são úteis:

1. Álgebras associativas são anéis. Álgebras não associativas são anéis não associativos.
2. Uma álgebra associativa pode não ser comutativa, um exemplo sendo as álgebras de matrizes complexas $n \times n$ com $n > 1$ (vide adiante).
3. Uma álgebra comutativa pode não ser associativa, um exemplo sendo as álgebras de Jordan não associativas (vide página 150, adiante).

Alguns exemplos elementares de anéis e álgebras:

1. O conjunto $\mathrm{Mat}\,(\mathbb{C},\ n)$ das matrizes complexas $n \times n$ é uma álgebra complexa, associativa e não comutativa (se $n > 1$) em relação à soma e ao produto usuais de matrizes. O conjunto $\mathrm{Mat}\,(\mathbb{Z},\ n)$ das matrizes inteiras $n \times n$ é um anel (não comutativo, se $n > 1$) em relação à soma e ao produto usuais de matrizes.
2. O conjunto $\mathrm{Mat}\,(\mathbb{Q},\ n)$ das matrizes racionais $n \times n$ é um anel (não comutativo, se $n > 1$) em relação à soma e ao produto usuais de matrizes. É também uma álgebra em relação ao corpo dos racionais $\mathbb{Q}$.
3. O conjunto $\mathrm{Pol}(\mathbb{C})$ de todos os polinômios em uma variável complexa com coeficientes complexos é uma álgebra complexa, associativa e Abeliana em relação à soma e ao produto usuais de polinômios. O conjunto $\mathrm{Pol}(\mathbb{Z})$ de todos os polinômios em uma variável complexa com coeficientes inteiros é um anel Abeliano em relação à soma e ao produto usuais de polinômios.
4. O conjunto $\mathrm{Pol}(\mathbb{Q})$ de todos os polinômios em uma variável complexa com coeficientes racionais é um anel Abeliano em relação à soma e ao produto usuais de polinômios. É também uma álgebra associativa e Abeliana em relação ao corpo dos racionais $\mathbb{Q}$.

**E. 2.36** *Exercício*. Em caso de dúvida, justifique as afirmações de acima. ✠

### • Subálgebras. Álgebras geradas, ou envolventes

Se $A$ é uma álgebra sobre um corpo $\mathbb{K}$ e dotada de um produto "$\cdot$" dizemos que um subespaço vetorial $A_0$ de $A$ é uma subálgebra de $A$ se $A_0$ for também uma álgebra com o mesmo produto "$\cdot$", ou seja, se o produto de dois elementos quaisquer de $A_0$ for também um elemento de $A_0$.

Se $A$ é uma álgebra e $\mathcal{F} = \{A_\lambda,\ \lambda \in \Lambda\}$, é uma família de subálgebras de $A$, então $\bigcap_{\lambda\in\Lambda} A_\lambda$ é também uma subálgebra de $A$. De fato, $\bigcap_{\lambda\in\Lambda} A_\lambda$ é um subespaço vetorial de $A$ (vide página 143) e se $a,\ b \in \bigcap_{\lambda\in\Lambda} A_\lambda$, segue que $a \cdot b \in A_\lambda$ para cada $\lambda \in \Lambda$ (pois $a,\ b \in A_\lambda$) e, assim, $a \cdot b \in \bigcap_{\lambda\in\Lambda} A_\lambda$.

[27] Niels Henrik Abel (1802–1829).

**E. 2.37** *Exercício fácil.* Verifique que se as álgebras de uma família $\mathcal{F} = \{A_\lambda,\ \lambda \in \Lambda\}$ forem associativas (ou comutativas, ou de Lie, respectivamente), então $\bigcap_{\lambda\in\Lambda} A_\lambda$ é igualmente associativa (ou comutativa, ou de Lie, respectivamente). ✠

Esses fatos conduzem a uma definição. Seja $C$ um subconjunto de uma álgebra $A$ e seja $\mathcal{F}$ a coleção de todas as subálgebras de $A$ que contêm $C$ ($\mathcal{F}$ é não vazio pois a própria álgebra $A$ contém $C$ e, portanto, é um elemento de $\mathcal{F}$). Assim, o subconjunto de $A$ formado pela intersecção de todos os elementos de $\mathcal{F}$ é também uma subálgebra de $A$, a "menor" subálgebra de $A$ a conter $C$. Essa álgebra é denominada *álgebra associativa envolvente gerada pelo conjunto* $C \subset A$, ou também *álgebra gerada por* $C \subset A$ e é denotada aqui por $C^*$ (essa notação não é universalmente adotada).

A subálgebra gerada por $C$ será composta por todos os elementos de $A$ que possam ser escritos como combinações lineares finitas de produtos finitos de elementos de $C$.

Se $G$ é um subconjunto de uma álgebra $A$ e a subálgebra gerada por $G$ for a própria $A$, então dizemos que $G$ é um *conjunto gerador* de $A$. Se uma álgebra $A$ é gerada por um conjunto $G \subset A$, então todo elemento de $A$ pode ser escrito como uma combinação linear finita de produtos finitos de elementos de $G$.

No caso de álgebras topológicas as definições acima podem ser modificadas para levar em conta o fato de álgebras e subálgebras serem fechadas (topologicamente) ou não. Assim, dizemos que $G$ é um conjunto gerador de uma álgebra $A$ se a menor álgebra que contém $G$ for densa em $A$ (na topologia de $A$). Nesse espírito, dizemos que se uma álgebra $A$ é gerada por um conjunto $G \subset A$, então todo elemento de $A$ pode ser escrito como limite (na topologia de $A$) de combinações lineares finitas de produtos finitos de elementos de $G$.

### • Constantes de estrutura

Seja $A$ uma álgebra de dimensão finita (enquanto espaço vetorial) e seja $B = \{b^1,\ \ldots,\ b^n\}$ uma base em $A$. Então, para cada $i,\ j = 1,\ \ldots,\ n$ o produto $b^i \cdot b^j$ poderá ser escrito como uma combinação linear de elementos de $B$:

$$b^i \cdot b^j \ = \ \sum_{k=1}^{n} {c_k}^{ij}\, b^k \ .$$

As $n^3$ constantes ${c_k}^{ij}$ são denominadas *constantes de estrutura* da álgebra $A$ na base $B$ e elas fixam o produto de todos os elementos de $A$. De fato, se $p,\ q \in A$ são da forma $p = \sum_{i=1}^n \alpha_i b^i$ e $q = \sum_{j=1}^n \beta_j b^j$, então $p \cdot q = \sum_{k=1}^n \gamma_k b^k$, com $\gamma_k = \sum_{i=1}^n \sum_{j=1}^n \alpha_i \beta_j {c_k}^{ij}$. Por essa razão, o conhecimento das constantes de estrutura fornece, em princípio, informações completas sobre álgebras de dimensão finita. É importante enfatizar também que as constantes de estrutura dependem da base escolhida e são transformadas por mudanças de base.

**E. 2.38** *Exercício.* Obtenha a regra de transformação de constantes de estrutura por mudanças de base. ✠

### • Um mínimo sobre álgebras não associativas. Álgebras alternativas

Seja $A$ uma álgebra sobre um corpo $\mathbb{K}$. Definimos o *associador*[28] de três elementos $a,\ b,\ c \in A$ por

$$\big[a,\ b,\ c\big] \ := \ (ab)c - a(bc) \ . \tag{2.31}$$

Trata-se de uma forma trilinear em $A$ com valores em $A$. Uma álgebra é dita ser associativa se $\big[a,\ b,\ c\big] = 0$ para todos $a,\ b,\ c \in A$ e é dita ser não associativa de outra forma.

Uma álgebra $A$ sobre $\mathbb{K}$ é dita ser *alternativa* se valer

$$\big[a,\ a,\ b\big] \ = \ 0 \quad \text{e} \quad \big[b,\ a,\ a\big] \ = \ 0 \tag{2.32}$$

para todos $a,\ b \in A$, ou seja, se valerem

$$(aa)b \ = \ a(ab) \quad \text{e} \quad (ba)a \ = \ b(aa)$$

para todos $a,\ b \in A$.

Naturalmente, toda álgebra associativa é (trivialmente) alternativa. A álgebra dos octônios $\mathbb{O}$ é um exemplo de uma álgebra não associativa que é alternativa. Uma álgebra de Lie $L$ somente é alternativa se $\big[a,\ [a,\ b]\big] = 0$ para todos

[28] Essa nomenclatura segue a da definição de *comutador*.

$a,\ b \in L$ (verifique! Aqui $[\cdot,\ \cdot]$ denota o produto da álgebra de Lie). Tal é o caso, por exemplo, da álgebra de Heisenberg, mas nem toda álgebra de Lie possui essa propriedade.

Vamos provar o seguinte fato: se $A$ é alternativa, vale também

$$\big[a,\ b,\ a\big] \ = \ 0$$

para todos $a,\ b \in A$. De fato, da propriedade $\big[a,\ a,\ b\big] = 0$ segue evidentemente que $\big[a+b,\ a+b,\ c\big] = 0$ para todos $a,\ b,\ c \in A$. Expandindo-se o lado esquerdo, isso significa que

$$\big[a,\ a,\ c\big] + \big[a,\ b,\ c\big] + \big[b,\ a,\ c\big] + \big[b,\ b,\ c\big] \ = \ 0\,.$$

O primeiro e o último termos do lado esquerdo são nulos pela primeira propriedade em (2.32). Assim, provamos que toda álgebra alternativa satisfaz

$$\big[a,\ b,\ c\big] \ = \ -\big[b,\ a,\ c\big]\,, \tag{2.33}$$

para todos $a,\ b,\ c \in A$. Tomando-se, em particular, $c = a$, isso fica

$$\big[a,\ b,\ a\big] \ = \ -\big[b,\ a,\ a\big] \ \overset{(2.32)}{=} \ 0\,,$$

(na última igualdade usamos a segunda propriedade de (2.32)). Isso estabeleceu o que desejávamos provar. Vemos portanto que em uma álgebra alternativa tem-se $\big[a,\ b,\ c\big] = 0$ sempre que dois dos argumentos forem iguais.

*Nota.* A identidade $\big[a,\ b,\ a\big] = 0$ significa $(ab)a = a(ba)$ e é por vezes denominada *propriedade flexível*, ou *flexibilidade*. ♣

Partindo-se do fato que $\big[c,\ a+b,\ a+b\big] = 0$, obtém-se imediatamente (verifique!) que

$$\big[c,\ a,\ b\big] \ = \ -\big[c,\ b,\ a\big] \tag{2.34}$$

para todos $a,\ b,\ c \in A$. Analogamente, de $\big[a+b,\ c,\ a+b\big] = 0$, obtém-se ainda

$$\big[b,\ c,\ a\big] \ = \ -\big[a,\ c,\ b\big] \tag{2.35}$$

também para todos $a,\ b,\ c \in A$. Usando-se repetidamente (2.33), (2.34) e (2.35), obtemos que

$$\big[a,\ b,\ c\big] \ \overset{(2.34)}{=} \ -\big[a,\ c,\ b\big] \ \overset{(2.33)}{=} \ \big[c,\ a,\ b\big] \ \overset{(2.35)}{=} \ -\big[b,\ a,\ c\big] \ \overset{(2.34)}{=} \ \big[b,\ c,\ a\big] \ \overset{(2.33)}{=} \ -\big[c,\ b,\ a\big]\,.$$

Todos os fatos estabelecidos acima sobre álgebras alternativas podem ser resumidos no seguinte: se $A$ é uma álgebra alternativa e $a_1,\ a_2,\ a_3 \in A$, então vale

$$\big[a_i,\ a_j,\ a_k\big] \ = \ \varepsilon_{ijk}\big[a_1,\ a_2,\ a_3\big] \tag{2.36}$$

para quaisquer índices $i,\ j,\ k \in \{1,\ 2,\ 3\}$. Acima, $\varepsilon_{ijk}$ é o símbolo de Levi-Civita. Com isso, podemos dizer que em uma álgebra alternativa o associador é alternante.

A principal motivação da definição de álgebra alternativa é a seguinte. Em uma álgebra não associativa geral, produtos múltiplos de um elemento por si mesmo podem ser distintos, ou seja, podemos ter, por exemplo, $(aa)a \neq a(aa)$ etc. Assim, não é possível definir-se potências como $a^3$, ou, mais geralmente, $a^n$, $n \in \mathbb{N}$, pelo menos não de forma única e não ambígua. No caso de álgebras alternativas, porém, as potências $a^n$, $n \in \mathbb{N}$, podem ser definidas de forma única e vale a lei de potências $a^m a^n = a^{m+n}$ para todos $m,\ n \in \mathbb{N}$.

Defina-se $a^2 := aa$ (o que não sofre de nenhuma ambiguidade). Podemos definir $a^3$ tanto por $a^3 := (a^2)a$ quanto por $a^3 := a(a^2)$, pois, para uma álgebra alternativa $(aa)a = a(aa)$. Analogamente, $a^4$ pode ser definido por $a^2a^2$ ou por $aa^3$ ou ainda por $a^3a$, pois todas essas expressões são idênticas. Não iremos desenvolver esse ponto, encaminhando o leitor à literatura pertinente (e.g., [465]). Mencionamos ainda uma importante generalização desses resultados: um teorema, devido a Artin[29], estabelece que se $A$ é uma álgebra alternativa, então a subálgebra gerada por quaisquer dois de seus elementos é associativa (vide [465]).

## 2.1.7 Exemplos Especiais de Álgebras

Existem inúmeras álgebras de especial interesse em áreas como a Física, a Teoria de Grupos e a Geometria Diferencial. Listaremos alguns poucos exemplos aqui com os quais lidaremos futuramente.

[29] Emil Artin (1889–1962).

### 2.1.7.1 Álgebras de Lie

Uma classe especialmente importante de álgebras é formada pelas chamadas *álgebras de Lie*. Por razões históricas o produto de dois elementos de uma álgebra de Lie é denotado pelo símbolo $[a,\ b]$ em lugar de $a \cdot b$, notação que seguiremos aqui.

Uma álgebra $L$ (sobre um corpo $\mathbb{K}$) é dita ser uma *álgebra de Lie*[30] se seu produto, além das propriedades distributivas gerais dos itens **a** e **b** da página 144, satisfizer também

**a.** Para todo $a \in L$ vale $[a,\ a] = 0$.

**b.** *Identidade de Jacobi*[31]. Para todos $a,\ b$ e $c \in L$ vale

$$\big[a,\ [b,\ c]\big] + \big[c,\ [a,\ b]\big] + \big[b,\ [c,\ a]\big] \ = \ 0\,. \tag{2.37}$$

A primeira propriedade tem uma implicação importante. Como $[a,\ a] = 0$ para todo $a \in L$, vale também que $[a+b,\ a+b] = 0$ para todos $a,\ b \in L$. Expandindo o lado esquerdo teremos que $0 = [a+b,\ a+b] = [a,\ a] + [b,\ b] + [a,\ b] + [b,\ a] = [a,\ b] + [b,\ a]$, ou seja, valerá a importante propriedade de *anticomutatividade*: $[a,\ b] = -[b,\ a]$ para todos $a,\ b \in L$. Reciprocamente, se assumirmos válida a propriedade de anticomutatividade então, tomando $b = a$, a mesma afirmará que $[a,\ a] = -[a,\ a]$ o que implica $[a,\ a] = 0$ *exceto se o corpo* $\mathbb{K}$ *tiver característica igual a* 2.

Assim, para corpos com característica diferente de 2 (como é o caso do corpo dos racionais, dos reais ou dos complexos, que têm característica 0) nossa definição de álgebra de Lie, acima, equivale à seguinte: $L$ é dita ser uma álgebra de Lie se seu produto satisfizer:

**a.** *Anticomutatividade*. Para todos $a,\ b \in L$ vale $[a,\ b] = -[b,\ a]$.

**b.** *Identidade de Jacobi*. Para todos $a,\ b$ e $c \in L$ vale

$$\big[a,\ [b,\ c]\big] + \big[c,\ [a,\ b]\big] + \big[b,\ [c,\ a]\big] \ = \ 0\,. \tag{2.38}$$

É evidente pelas considerações acima que uma álgebra de Lie $L$ só pode ser comutativa se seu produto for trivial $[a,\ b] = 0$ para todos $a,\ b \in L$, um caso que raramente merece consideração especial. Uma álgebra de Lie $L$ também não pode ter uma unidade, pois se $e \in L$ fosse uma identidade, teríamos $e = [e,\ e] = 0$. Logo, para todo $a \in L$ valeria também $a = [a,\ e] = [a,\ 0] = 0$, implicando que $L$ possui apenas o vetor nulo, novamente um caso trivial que não merece consideração. Por fim, se uma álgebra de Lie $L$ for associativa, então a identidade de Jacobi e a anticomutatividade implicam $[a,\ [b,\ c]] = 0$ para todos $a,\ b,\ c \in L$ (prove isso!). Um exemplo de uma álgebra de Lie com tal propriedade é a álgebra de Heisenberg (vide Seção 21.2.2, página 1126). Note que em tal caso a identidade de Jacobi é trivialmente satisfeita.

**E. 2.39** *Exercício*. Para álgebras de Lie de dimensão finita escreva a condição de anticomutatividade e a identidade de Jacobi (2.38) em termos das constantes de estrutura, introduzidas à página 146. ✠

**• Álgebras associativas e álgebras de Lie**

Seja $A$ uma álgebra associativa. Podemos associar a $A$ uma álgebra de Lie definindo o produto $[a,\ b] = ab - ba$, denominado *comutador* de $a$ e $b \in A$. Com essa definição, é claro que $[a,\ a] = 0$ para todo $a \in A$ e a identidade de Jacobi segue do fato que

$$\begin{aligned}
&\big[a,\ [b,\ c]\big] + \big[c,\ [a,\ b]\big] + \big[b,\ [c,\ a]\big] \\
&\qquad = \ a(bc-cb) - (bc-cb)a + c(ab-ba) - (ab-ba)c + b(ca-ac) - (ca-ac)b \\
&\qquad = \ abc - acb - bca + cba + cab - cba - abc + bac + bca - bac - cab + acb \\
&\qquad = \ 0\,,
\end{aligned} \tag{2.39}$$

como facilmente se constata.

[30] Marius Sophus Lie (1842–1899).
[31] Carl Gustav Jacob Jacobi (1804–1851).

**E. 2.40** *Exercício*. Seja $A$ uma álgebra associativa e seja $s \in A$, arbitrário. Defina em $A$ o produto $[a,\ b]_s := asb - bsa$. É óbvio que esse produto satisfaz $[a,\ a]_s = 0$ para todo $a \in A$. Mostre que ele também satisfaz a identidade de Jacobi e, portanto, define uma álgebra de Lie em $A$. ✲

• **Exemplos básicos de álgebras de Lie**

A maioria dos exemplos exibidos nos exercícios abaixo é relevante na teoria dos grupos de Lie.

**E. 2.41** *Exercício*. Mostre que $\mathbb{R}^3$ dotado do produto vetorial usual é uma álgebra de Lie. ✲

**E. 2.42** *Exercício*. Mostre que $\mathrm{Mat}\,(\mathbb{R},\ n)$ (ou $\mathrm{Mat}\,(\mathbb{C},\ n)$), o espaço vetorial de todas as matrizes $n \times n$ reais (complexas) é uma álgebra de Lie com relação ao produto $[A,\ B] := AB - BA$. ✲

**E. 2.43** *Exercício*. Seja $S \in \mathrm{Mat}\,(\mathbb{C},\ n)$. Mostre que $\mathrm{Mat}\,(\mathbb{C},\ n)$ é uma álgebra de Lie com relação ao produto $[A,\ B]_S := ASB - BSA$. ✲

**E. 2.44** *Exercício*. Mostre que o subespaço vetorial de $\mathrm{Mat}\,(\mathbb{R},\ n)$ (ou de $\mathrm{Mat}\,(\mathbb{C},\ n)$) formado pelas matrizes com traço nulo é uma álgebra de Lie real (respectivamente, complexa) com relação ao produto $[A,\ B] = AB - BA$. ✲

**E. 2.45** *Exercício*. Mostre que o subespaço vetorial de $\mathrm{Mat}\,(\mathbb{R},\ n)$ (ou de $\mathrm{Mat}\,(\mathbb{C},\ n)$) formado pelas matrizes antissimétricas, ou seja, tais que $A^T = -A$, é uma álgebra de Lie com relação ao produto $[A,\ B] = AB - BA$. *Sugestão:* mostre que se $A$ e $B$ são antissimétricas, então $[A,\ B]^T = -[A,\ B]$ e, portanto, o comutador de matrizes antissimétricas é também uma matriz antissimétrica.

Um comentário relevante aqui é o seguinte. No espaço vetorial das matrizes reais simétricas (*i.e.*, que satizfazem $A^T = A$) tem-se também que $[A,\ B]^T = -[A,\ B]$. Por essa razão, o comutador sequer define um produto no espaço vetorial das matrizes reais (ou complexas) simétricas, pois o comutador de duas matrizes simétricas **não** é novamente uma matriz simétrica, mas sim uma matriz antissimétrica. ✲

**E. 2.46** *Exercício*. Mostre que o subespaço vetorial real de $\mathrm{Mat}\,(\mathbb{C},\ n)$ formado pelas matrizes antiautoadjuntas, ou seja, tais que $A^* = -A$, é uma álgebra de Lie (sobre o corpo dos reais!) com relação ao produto $[A,\ B] = AB - BA$. ✲

**E. 2.47** *Exercício*. Conclua igualmente que o subespaço vetorial real de $\mathrm{Mat}\,(\mathbb{C},\ n)$ formado pelas matrizes antiautoadjuntas, ou seja, tais que $A^* = -A$, e de traço nulo ($\mathrm{Tr}(A) = 0$) é uma álgebra de Lie (sobre o corpo dos reais!) com relação ao produto $[A,\ B] = AB - BA$. ✲

**E. 2.48** *Exercício*. Fixada uma matriz $M \in \mathrm{Mat}\,(\mathbb{R},\ n)$, mostre que o subconjunto de $\mathrm{Mat}\,(\mathbb{R},\ n)$ formado pelas matrizes $A$ com a propriedade $AM = -MA^T$ é uma álgebra de Lie real com relação ao produto $[A,\ B] = AB - BA$. ✲

**E. 2.49** *Exercício*. Fixada uma matriz $M \in \mathrm{Mat}\,(\mathbb{C},\ n)$, mostre que o subconjunto de $\mathrm{Mat}\,(\mathbb{C},\ n)$ formado pelas matrizes $A$ com a propriedade $AM = -MA^*$ é uma álgebra de Lie *real* com relação ao produto $[A,\ B] = AB - BA$. ✲

Tratemos agora de exibir um exemplo básico de uma álgebra de Lie de dimensão infinita.

• **Colchetes de Poisson**

Sejam $f(p,\ q)$ e $g(p,\ q)$, com $f : \mathbb{R}^2 \to \mathbb{R}$ e $g : \mathbb{R}^2 \to \mathbb{R}$, duas funções reais, infinitamente diferenciáveis, de duas variáveis reais $p$ e $q$. Definimos os *colchetes de Poisson*[32] de $f$ e $g$, denotados por $\{f,\ g\}$, por

$$\{f,\ g\} \ := \ \frac{\partial f}{\partial p}\frac{\partial g}{\partial q} - \frac{\partial f}{\partial q}\frac{\partial g}{\partial p}\,.$$

É claro que $\{f,\ g\}$ é igualmente uma função infinitamente diferenciável de $p$ e $q$.

[32] Siméon Denis Poisson (1781–1840).

Os colchetes de Poisson satisfazem as seguintes propriedades: para quaisquer funções $f,\ g$ e $h$ como acima, valem

**a.** *Linearidade*: $\{f,\ \alpha g + \beta h\} = \alpha\{f,\ g\} + \beta\{f,\ h\}$ para quaisquer $\alpha,\ \beta \in \mathbb{R}$. Analogamente, $\{\alpha f + \beta g,\ h\} = \alpha\{f,\ h\} + \beta\{g,\ h\}$.

**b.** *Antissimetria*: $\{f,\ g\} = -\{g,\ f\}$.

**c.** *Identidade de Jacobi*[33]: $\big\{f,\ \{g,\ h\}\big\} + \big\{h,\ \{f,\ g\}\big\} + \big\{g,\ \{h,\ f\}\big\} = 0$.

**d.** *Identidade de Leibniz*[34]: $\{f,\ gh\} = \{f,\ g\}h + g\{f,\ h\}$.

**E. 2.50** *Exercício importante.* Verifique a validade das quatro propriedades acima. ✠

As propriedades 1 e 2 e 3 indicam que o conjunto das funções $\mathbb{R}^2 \to \mathbb{R}$ infinitamente diferenciáveis é uma álgebra de Lie com o produto definido pelos colchetes de Poisson. Trata-se de uma álgebra de Lie de dimensão infinita.

A definição acima dos colchetes de Poisson pode ser facilmente generalizada para variedades diferenciáveis de dimensão par, mas não trataremos disso aqui por ora. Os colchetes de Poisson desempenham um papel importante na Mecânica Clássica.

**E. 2.51** *Exercício.* Mostre que matrizes $A$, $B$, $C$ de $\mathrm{Mat}\,(\mathbb{R},\ n)$ (ou de $\mathrm{Mat}\,(\mathbb{C},\ n)$) também satisfazem uma identidade de Leibniz: $[A,\ BC] = [A,\ B]C + B[A,\ C]$. Em verdade, essa identidade é válida em qualquer álgebra associativa. Mostre isso também (a prova é idêntica ao caso de matrizes). ✠

### 2.1.7.2 Álgebras de Poisson

O exemplo dos colchetes de Poisson e do Exercício E. 2.51 conduzem à definição das chamadas *álgebras de Poisson*.

Uma *álgebra de Poisson* é um espaço vetorial $\mathcal{P}$ (em relação a um corpo $\mathbb{K}$) dotado de dois produtos, denotados por $*$ e por $\{\cdot,\ \cdot\}$, satisfazendo as seguintes propriedades:

- $\mathcal{P}$ é uma álgebra associativa em relação ao produto $*$.
- $\mathcal{P}$ é uma álgebra de Lie em relação ao produto $\{\cdot,\ \cdot\}$.
- Para todos $a,\ b,\ c \in \mathcal{P}$ vale a *identidade de Leibniz* $\{a,\ b * c\} = \{a,\ b\} * c + b * \{a,\ c\}$.
  Isso significa que o produto $\{\cdot,\ \cdot\}$ age como uma derivação para o produto $*$.

Naturalmente, se $\mathcal{A}$ é uma álgebra associativa com produto $*$ obtemos em $\mathcal{A}$ uma álgebra de Poisson definindo $\{a,\ b\} = a * b - b * a$, como observamos no Exercício E. 2.51. De maior interesse são álgebras de Poisson onde o produto $\{a,\ b\}$ não seja do tipo $a * b - b * a$.

### 2.1.7.3 Álgebras de Jordan

Outra classe de álgebras não associativas de interesse é formada pelas álgebras de Jordan.

Uma álgebra não associativa $J$ sobre um corpo $\mathbb{K}$ é dita ser uma *álgebra de Jordan*[35] se seu produto satisfizer

**a.** *Comutatividade.* Para todos $a,\ b \in J$ vale $a \cdot b = b \cdot a$.

**b.** *Identidade de Jordan.* Para todos $a,\ b \in J$ vale

$$(a \cdot a) \cdot (a \cdot b) \ = \ a \cdot \big((a \cdot a) \cdot b\big)\ . \tag{2.40}$$

[33] Carl Gustav Jacob Jacobi (1804–1851).
[34] Gottfried Wilhelm von Leibniz (1646–1716).
[35] Ernst Pascual Jordan (1902–1980) foi um dos fundadores da Mecânica Quântica.

Como a identidade de Jordan é trivialmente satisfeita por uma álgebra associativa, alguns autores aceitam a inclusão das álgebras associativas dentre as de Jordan (desde que sejam também comutativas, naturalmente). De qualquer forma, dada uma álgebra associativa (não-necessariamente comutativa) é sempre possível definir um produto que faz dela uma álgebra de Jordan.

De fato, se $A$ é uma álgebra associativa (não-necessariamente comutativa) sobre $\mathbb{R}$ ou $\mathbb{C}$[36], cujo produto denotamos por $ab$, o produto

$$a \cdot b \;=\; \frac{1}{2}(ab + ba) \tag{2.41}$$

faz de $A$ uma álgebra de Jordan. Em textos de Física a expressão $ab+ba$ é denominada *anticomutador* e é frequentemente denotada pelo símbolo $\{a,\, b\}$.

**E. 2.52** *Exercício*. Verifique que esse produto é comutativo (trivial) e satisfaz a identidade de Jordan. Verifique também que esse produto não é, em geral, associativo se $A$ não for Abeliana. Esse produto é denominado *produto de Jordan*. ✠

As álgebras de Jordan surgiram da tentativa de definir produtos de observáveis na Mecânica Quântica (representados por operadores autoadjuntos) que definissem novamente observáveis. O seguinte exercício deve tornar isso claro.

**E. 2.53** *Exercício*. Verifique que a coleção das matrizes autoadjuntas de $\mathrm{Mat}\,(\mathbb{C},\, n)$ forma uma álgebra de Jordan para o produto de Jordan acima. ✠

### 2.1.7.4 Álgebras de Grassmann

Álgebras de Grassmann, especialmente em uma de suas formas especiais, as chamadas Álgebras Exteriores (vide Seção 2.5, página 241), são importantes na Topologia Diferencial e na Geometria Diferencial, por exemplo no estudo das chamadas *formas diferenciais*.

Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K}$. Uma *álgebra de Grassmann*[37] sobre $V$ é uma álgebra associativa e unital sobre $\mathbb{K}$, denotada por $\Gamma(V)$, e cujo produto é denotado (por razões históricas) pelo símbolo $\wedge$ (denominado "cunha"), com as seguintes propriedades

**a.** $V$ é um subespaço vetorial de $\Gamma(V)$.

**b.** Para todo $v \in V$ tem-se $v \wedge v = 0$.

A condição de $V$ ser um subespaço de $\Gamma(V)$ é por vezes substituída pela condição de $V$ ser isomorfo a um subespaço de $\Gamma(V)$. Como essa distinção dificilmente possui relevância, vamos ignorá-la aqui.

Como observamos na discussão sobre álgebras de Lie, a condição $v \wedge v = 0$ para todo $v \in V$ implica a condição de anticomutatividade $u \wedge v = -v \wedge u$ para todos $u,\ v \in V$, mas só equivale a essa se a característica de $\mathbb{K}$ não for 2. Fazemos notar também que a condição $v \wedge v = 0$ é assumida apenas para os elementos de $V$, não para todos os elementos de $\Gamma(V)$. Analogamente, fazemos notar que $V$ é suposto ser um subespaço vetorial de $\Gamma(V)$, não necessariamente uma subálgebra de $\Gamma(V)$.

A unidade $e$ de $\Gamma(V)$ não pode ser um elemento de $V$, pois se tal fosse o caso teríamos $e = e \wedge e = 0$, o que implicaria para todo $a \in \Gamma(V)$ que $a = a \wedge e = a \wedge 0 = 0$, o que só faz sentido se $\Gamma(V)$ (e, portanto, $V$) consistir apenas do vetor nulo, um caso desprovido de interesse especial. Assim, nos casos de interesse, $\Gamma(V)$ possui ao menos dois subespaços distintos: o subespaço gerado pela unidade $e$ e o subespaço $V$.

**Proposição 2.3** *Em uma álgebra de Grassmann $\Gamma(V)$ vale a seguinte afirmação: se $v_1,\ \ldots,\ v_m$ são vetores de $V$, então o produto $v_1 \wedge \cdots \wedge v_m$ será nulo se $v_1,\ \ldots,\ v_m$ forem linearmente dependentes.* □

Prova. Vamos supor, sem perda de generalidade, que possamos escrever $v_1$ como combinação linear dos demais: $v_1 = \sum_{k=2}^{m} \alpha_k v_k$. Então, $v_1 \wedge \cdots \wedge v_m = \sum_{k=2}^{m} \alpha_k v_k \wedge \big(v_2 \wedge \cdots \wedge v_m\big)$. Agora, usando a anticomutatividade podemos passar o vetor

[36] Ou, mais genericamente, sobre qualquer corpo que não tenha característica 2.
[37] Hermann Günther Grassmann (1809–1877).

$v_k$ que ocorre no produto $v_2 \wedge \cdots \wedge v_m$ para a primeira posição no mesmo, ganhando um fator $(-1)^{k-2}$. Assim, devido à associatividade, obtemos $v_k \wedge \big(v_2 \wedge \cdots \wedge v_m\big) = (-1)^{k-2} v_k \wedge v_k \wedge \cdots \wedge v_m = 0$, pois $v_k \wedge v_k = 0$. ■

Na Seção 2.5.2, página 243, discutiremos um procedimento geral de construção de uma álgebra de Grassmann a partir de um espaço vetorial $V$ dado. Para aquelas álgebras, as chamadas *álgebras exteriores*, vale a recíproca da Proposição 2.3: um produto $v_1 \wedge \cdots \wedge v_m$ de vetores $v_1, \ \ldots, \ v_m \in V$ será nulo se e somente se $v_1, \ \ldots, \ v_m$ forem linearmente dependentes.

Vamos a alguns exemplos elementares (quiçá triviais) de álgebras de Grassmann. Na Seção 2.5.2, página 243, discutiremos um procedimento geral de construção de uma álgebra de Grassmann a partir de um espaço vetorial $V$ dado, dentro do qual mais exemplos poderão ser construídos.

**Exemplo 2.14** Seja $V$ o espaço vetorial (sobre $\mathbb{C}$) das matrizes $2 \times 2$ da forma $\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right)$, com $b \in \mathbb{C}$. Então, uma álgebra de Grassmann sobre $V$ seria o conjunto das matrizes $2 \times 2$ da forma $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$, com $a, \ b \in \mathbb{C}$, com o produto usual de matrizes. ♦

**Exemplo 2.15** Seja $V$ o espaço vetorial (sobre $\mathbb{C}$) das matrizes $3 \times 3$ da forma $\left(\begin{smallmatrix} 0 & b & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$, com $b, \ c \in \mathbb{C}$. Então, uma álgebra de Grassmann sobre $V$ seria o conjunto das matrizes $3 \times 3$ da forma $\left(\begin{smallmatrix} a & b & c \\ 0 & a & 0 \\ 0 & 0 & a \end{smallmatrix}\right)$, com $a, \ b, \ c \in \mathbb{C}$, com o produto usual de matrizes. Note que nesse caso há uma relação adicional, pois o produto de matrizes da forma $\left(\begin{smallmatrix} 0 & b & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ com matrizes da forma $\left(\begin{smallmatrix} 0 & 0 & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ é nulo. ♦

### 2.1.7.5 Álgebras de Clifford

*Álgebras de Clifford* têm particular relevância na Teoria de Grupos, surgindo também na Geometria Diferencial, na Mecânica Quântica Relativística e na Teoria da Relatividade Geral, contando também com aplicações em Computação Gráfica.

Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K}$ (que suporemos <u>não</u> ter característica 2) e seja $\omega$ uma forma bilinear simétrica em $V$ (para a definição, vide página 263). Uma álgebra de Clifford[38] sobre $V$ e $\omega$, denotada por $\mathrm{Cl}(V, \ \omega)$, é uma álgebra associativa dotada de uma unidade $e \notin V$ com as seguintes propriedades

**a.** Enquanto espaço vetorial sobre $\mathbb{K}$, $\mathrm{Cl}(V, \ \omega)$ é isomorfo a $(\mathbb{K}e) \oplus V$, isto é, $\mathrm{Cl}(V, \ \omega) \simeq (\mathbb{K}e) \oplus V$.

**b.** Para todo $v \in V$ tem-se $v^2 = \omega(v, \ v)e$.

Assim, podemos escrever os elementos de $\mathrm{Cl}(V, \ \omega)$ da forma $\alpha e + u$, com $\alpha \in \mathbb{K}$ e $u \in V$ e temos em $\mathrm{Cl}(V, \ \omega)$

$$\big(\alpha e + u\big)\big(\beta e + v\big) \ = \ \alpha\beta e + (\alpha v + \beta u) + uv \ , \quad \text{com } uv \in \mathrm{Cl}(V, \ \omega) \ ,$$

sendo $\alpha, \ \beta \in \mathbb{K}$ e $u, \ v \in V$. Em particular, caso $u = v$, tem-se pela condição **b**,

$$\big(\alpha e + v\big)\big(\beta e + v\big) \ = \ \big(\alpha\beta + \omega(v, \ v)\big)e + (\alpha + \beta)v \ .$$

Notemos que se $u$ e $v$ são elementos de $V$ então, pela propriedade **b**, acima, vale $(u + v)(u + v) = \omega(u + v, \ u + v)e$. Expandindo ambos os lados e usando que $u^2 = \omega(u, \ u)e$ e $v^2 = \omega(v, \ v)e$, obtemos $uv + vu = 2\omega(u, \ v)e$. Reciprocamente, se supormos que $uv + vu = 2\omega(u, \ v)e$ para todos $u$ e $v \in V$, segue evidentemente que $v^2 = \omega(v, \ v)e$. Assim, a condição **b** equivale a

**b'.** Para todos $u$ e $v \in V$ tem-se $uv + vu = 2\omega(u, \ v)e$.

A definição de álgebra de Clifford para o caso em que $\mathbb{K}$ tem característica 2 é semelhante (ao invés de uma forma bilinear simétrica emprega-se uma forma quadrática[39] sobre $V$), mas como certos resultados gerais não são válidos nesse caso (por exemplo, a condição **b** não equivale à **b'**), não faremos menção a ele aqui e remetemos o estudante à literatura especializada (e.g. [345]).

[38] William Kingdon Clifford (1845–1879). O trabalho original onde a noção surgiu é W. K. Clifford, "Preliminary sketch of bi-quaternions". Proc. London Math. Soc. **4**, 381–395 (1873).

[39] Para a definição, vide Seção 3.1.4, página 274.

• **Álgebras de Clifford e álgebras tensoriais**

Álgebras de Clifford podem ser construídas a partir de dois ingredientes: um espaço vetorial e uma forma bilinear simétrica sobre o mesmo. A construção que apresentaremos é tomada, por alguns autores, como a própria definição de álgebra de Clifford. Vamos aqui considerar apenas o caso do corpo dos reais, mas é evidente que a construção pode ser ainda mais generalizada.

Seja $V$ um espaço vetorial real e $\omega$ uma forma bilinear simétrica sobre $V$. Considere-se a álgebra tensorial (essa noção é detalhada nas Seções 2.5 e 2.5.1, páginas 241 e 242, respectivamente)

$$\mathscr{T}(V) \,:=\, \bigoplus_{n=0}^{\infty} V^{\otimes n} \,,$$

com a convenção $V^{\otimes 0} \equiv \mathbb{R}$ e com o produto definido em (2.172), página 242. Como comentamos na supramencionada Seção, $\mathscr{T}(V)$ é associativa e unital. Por vezes denotaremos essa unidade por $e$.

O conjunto $\mathscr{I}(V,\, \omega)$ obtido por todas as combinações lineares finitas de elementos da forma

$$a \otimes \Big( u \otimes v + v \otimes u - \omega(u,\, v) e \Big) \otimes b$$

para todos $a,\, b \in \mathscr{T}(V)$ e $u,\, v \in V$, é um bi-ideal (ou ideal bilateral) de $\mathscr{T}(V)$ (verifique!). Definimos a álgebra de Clifford $\mathrm{Cl}(V,\, \omega)$ como sendo o quociente

$$\mathrm{Cl}(V,\, \omega) \,:=\, \mathscr{T}(V)/\mathscr{I}(V,\, \omega) \,.$$

(A noção de quociente de uma álgebra associativa por um ideal bilateral é desenvolvida na Seção 2.4.1, página 234). Essa definição corresponde intuitivamenta à imposição que $u \otimes v + v \otimes u = \omega(u,\, v) e$ para todos $u,\, v \in V$.

Com uso das matrizes de Pauli e das matrizes de Dirac é possível construir *representações* de certas álgebras de Clifford, representações essas de relevância na Física Quântica.

• **Álgebras de Clifford e matrizes de Pauli**

As chamadas *matrizes de Pauli*[40] são as matrizes complexas $2 \times 2$ dadas por

$$\sigma_1 \,:=\, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 \,:=\, \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{e} \quad \sigma_3 \,:=\, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} . \tag{2.42}$$

As matrizes de Pauli satisfazem as seguintes relações algébricas: para todos $a,\, b = 1,\, 2,\, 3$ valem

$$[\sigma_a,\, \sigma_b] \,:=\, \sigma_a\sigma_b - \sigma_b\sigma_a \;\; = \;\; 2i \sum_{c=1}^{3} \varepsilon_{abc}\sigma_c \,, \tag{2.43}$$

$$\{\sigma_a,\, \sigma_b\} \,:=\, \sigma_a\sigma_b + \sigma_b\sigma_a \;\; = \;\; 2\delta_{ab}\mathbb{1}_2 \,, \tag{2.44}$$

$$\sigma_a\sigma_b \;\; = \;\; \delta_{ab}\mathbb{1}_2 + i \sum_{c=1}^{3} \varepsilon_{abc}\sigma_c \,. \tag{2.45}$$

Consideremos $V = \mathbb{R}^3$ e a forma bilinear simétrica

$$\omega_E(u,\, v) \,:=\, 2(u_1v_1 + u_2v_2 + u_3v_3) \,=\, 2 \sum_{a,\, b=1}^{3} u_a v_b \delta_{ab} \,,$$

onde $u = (u_1,\, u_2,\, u_3) \in \mathbb{R}^3$, $v = (v_1,\, v_2,\, v_3) \in \mathbb{R}^3$. Temos assim definida a álgebra de Clifford $\mathrm{Cl}(\mathbb{R}^3,\, \omega_E)$.

Seja $\Sigma$ a álgebra gerada pela matriz identidade e por todas as combinações lineares reais finitas de produtos finitos da matriz identidade e das matrizes de Pauli. É bastante claro que $\Sigma$ é uma álgebra de matrizes (é possível mostrar, mas não é relevante aqui, que $\Sigma$ coindice com $\mathrm{Mat}\,(\mathbb{C},\, 2)$, a álgebra de todas as matrizes complexas $2 \times 2$).

[40] Wolfgang Ernst Pauli (1900–1958).

Com uso das matrizes de Pauli podemos encontrar uma representação de $\mathscr{T}(\mathbb{R}^3)$ em $\Sigma$. Ela é dada por

$$\pi(e) \;:=\; \mathbb{1}_2 \;,$$

$$\pi\big(u\big) \;:=\; u\cdot\sigma \;\equiv\; u_1\sigma_1 + u_2\sigma_2 + u_3\sigma_3 \;, \qquad u\in\mathbb{R}^3 \;,$$

e em geral, para $n\in\mathbb{N}$,

$$\pi\big(u^1\otimes\cdots\otimes u^n\big) \;:=\; \big(u^1\cdot\sigma\big)\cdots\big(u^n\cdot\sigma\big) \;=\; \sum_{k_1,\,\ldots,\,k_n=1}^{3} (u^1)_{k_1}\cdots(u^n)_{k_n}\sigma_{k_1}\cdots\sigma_{k_n} \;,$$

com $u^1,\,\ldots,\,u^n\in\mathbb{R}^3$. É subentendido que $\pi$ é linearmente estendida a todo $\mathscr{T}(\mathbb{R}^3)$. Por exemplo, para $m,\,n\in\mathbb{N}$, e $u^1,\,\ldots,\,u^m,\,v^1,\,\ldots,\,v^n\in\mathbb{R}^3$ e $\alpha,\,\beta\in\mathbb{R}$, temos

$$\pi\Big(\alpha u^1\otimes\cdots\otimes u^m + \beta v^1\otimes\cdots\otimes v^n\Big) \;=\; \alpha\pi\big(u^1\otimes\cdots\otimes u^m\big) + \beta\pi\big(v^1\otimes\cdots\otimes v^n\big)$$

$$= \;\alpha\sum_{k_1,\,\ldots,\,k_m=1}^{3} (u^1)_{k_1}\cdots(u^n)_{k_m}\sigma_{k_1}\cdots\sigma_{k_m} + \beta\sum_{l_1,\,\ldots,\,l_n=1}^{3} (v^1)_{l_1}\cdots(v^n)_{l_n}\sigma_{l_1}\cdots\sigma_{l_n} \;.$$

É fácil constatar (faça-o!) que $\pi$ é uma representação da álgebra $\mathscr{T}(\mathbb{R}^3)$ na álgebra $\Sigma$.

O ponto importante é que temos

$$\pi\big(u\otimes v + v\otimes u\big) \;=\; \sum_{a,\,b=1}^{3} u_a v_b\sigma_a\sigma_b + \sum_{a,\,b=1}^{3} v_a u_b\sigma_a\sigma_b \;=\; \sum_{a,\,b=1}^{3} u_a v_b\big(\sigma_a\sigma_b + \sigma_b\sigma_a\big)$$

$$\stackrel{(2.44)}{=} \;2\sum_{a,\,b=1}^{3} u_a v_b\delta_{ab}\mathbb{1}_2 \;=\; \omega_E(u,\,v)\mathbb{1}_2 \;=\; \pi\big(\omega_E(u,\,v)e\big) \;, \quad (2.46)$$

mostrando que $\pi$ anula todos os elementos do ideal $\mathscr{I}(\mathbb{R}^3,\,\omega_E)$ e, portanto, a aplicação $\overline{\pi}:\mathrm{Cl}(\mathbb{R}^3,\,\omega_E)\to\Sigma$ dada por

$$\overline{\pi}\big([a]\big) \;:=\; \pi(a), \qquad a\in\mathscr{T}(\mathbb{R}^3)$$

é uma representação da álgebra de Clifford $\mathrm{Cl}(\mathbb{R}^3,\,\omega_E)$ em $\Sigma$.

• **Álgebras de Clifford e matrizes de Dirac**

Um outro exemplo, importante no contexto da Mecânica Quântica Relativística e das Teorias Quânticas de Campos, concerne as chamadas *matrizes de Dirac*[41]

Nesse caso consideramos $V=\mathbb{R}^4$ (o espaço-tempo de Minkowski[42]) e a forma bilinear $\omega_M$ definida em $V$ é dada por

$$\omega_M(u,\,v) \;=\; \sum_{\mu,\,\nu=0}^{3} u_\mu v_\nu\eta^{\mu\nu} \;=\; u_0v_0 - u_1v_1 - u_2v_2 - u_3v_3 \;,$$

onde $u=(u_0,\,u_1,\,u_2,\,u_3)\in\mathbb{R}^4$, $v=(v_0,\,v_1,\,v_2,\,v_3)\in\mathbb{R}^4$ e onde $\eta^{\mu\nu}$ são os elementos de matriz de $\eta=\begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&-1\end{pmatrix}$ (o chamado tensor métrico de Minkowski).

As chamadas *matrizes de Dirac (na base de Weyl)* são as quatro matrizes $4\times4$ dadas por

$$\gamma^0 \;:=\; \begin{pmatrix}0&\mathbb{1}\\\mathbb{1}&0\end{pmatrix} \;, \qquad \gamma^k \;:=\; \begin{pmatrix}0&-\sigma_k\\\sigma_k&0\end{pmatrix} \;, \quad k=1,\,2,\,3 \;, \quad (2.47)$$

[41] Paul Adrien Maurice Dirac (1902–1984).

[42] Rigorosamente falando, trata-se, em verdade do espaço tangente do espaço-tempo de Minkowski.

onde $\sigma_k$ são as matrizes de Pauli. É relevante constatar (faça-o!) que as mesmas satisfazem as seguintes relações de anticomutação:

$$\gamma^\mu\gamma^\nu + \gamma^\nu\gamma^\mu \;=\; 2\eta^{\mu\nu}\,\mathbb{1}\,, \tag{2.48}$$

para todos $\mu,\ \nu \in \{0,\ 1,\ 2,\ 3\}$.

Em analogia ao que fizemos no caso das matrizes de Pauli, consideramos a álgebra real $\Gamma$ gerada por combinações lineares finitas de produtos finitos da matriz identidade e das matrizes de Dirac. É sabido (vide, *e.g.*, [54]) que $\Gamma$ tem dimensão 16, mas isso não é relevante aqui.

Podemos definir uma representação da álgebra de tensorial $\mathscr{T}(\mathbb{R}^4)$ em $\Gamma$ por

$$\pi(e) \;:=\; \mathbb{1}_4\,,$$

$$\pi\big(a\big) \;=\; \sum_{\mu=0}^{3} a_\mu\gamma^\mu \;=\; a_0\gamma^0 + a_1\gamma^1 + a_2\gamma^2 + a_3\gamma^3\,, \qquad a = (a_0,\ a_1,\ a_2,\ a_3) \in \mathbb{R}^4\,,$$

e, em geral, para $n \in \mathbb{N}$,

$$\pi\big(u^1\otimes\cdots\otimes u^n\big) \;=\; \sum_{\mu_1,\ \ldots,\ \mu_n=0}^{3} (u^1)_{\mu_1}\cdots(u^n)_{\mu_n}\gamma^{\mu_1}\cdots\gamma^{\mu_n}\,,$$

para $u^1,\ \ldots,\ u^n \in V$, com $\pi$ linearmente estendida a todo $\mathscr{T}(\mathbb{R}^4)$.

Novamente, temos

$$\pi\big(u\otimes v + v\otimes u\big) \;=\; \sum_{\mu,\ \nu=0}^{3} u_\mu v_\nu\gamma^\mu\gamma^\nu + \sum_{\mu,\ \nu=0}^{3} v_\mu u_\nu\gamma^\mu\gamma^\nu \;=\; \sum_{\mu,\ \nu=0}^{3} u_\mu v_\nu\big(\gamma^\mu\gamma^\nu + \gamma^\nu\gamma^\mu\big)$$

$$\overset{(2.48)}{=}\; 2\sum_{\mu,\ \nu=1}^{3} u_\mu v_\nu\eta^{\mu\nu}\mathbb{1}_2 \;=\; \omega_M(u,\ v)\mathbb{1}_4 \;=\; \pi\big(\omega_M(u,\ v)e\big)\,,$$

mostrando que $\pi$ anula os elementos do ideal $\mathscr{I}(\mathbb{R}^4,\ \omega_M)$ e, portanto, a aplicação $\overline{\pi} : \mathrm{Cl}(\mathbb{R}^4,\ \omega_M) \to \Gamma$ dada por

$$\overline{\pi}\big([a]\big) \;:=\; \pi(a), \qquad a \in \mathscr{T}(\mathbb{R}^4)$$

é uma representação da álgebra de Clifford $\mathrm{Cl}(\mathbb{R}^4,\ \omega_M)$ em $\Gamma$.

• **Álgebras de Clifford e grupos**

Cada álgebra de Clifford $\mathrm{Cl}(V,\ \omega)$ é fortemente associada a representações do grupo de invariância da forma bilinear simétrica $\omega$. Assim, no caso da álgebra de Clifford $\mathrm{Cl}(\mathbb{R}^3,\ \omega_E)$, das matrizes de Pauli, temos o uma relação com o grupo de rotações SO(3) e no caso da álgebra de Clifford $\mathrm{Cl}(\mathbb{R}^4,\ \omega_M)$, das matrizes de Dirac, temos o uma relação com o grupo de Lorentz. Na presente versão destas Notas não iremos explorar essas importantes relações e remetemos o estudante interessado à literatura pertinente (*e.g.*, [345], [181], [551]).

## 2.1.8 Mais sobre Anéis

Apresentaremos em sequência uma série de definições após as quais discutiremos exemplos relevantes.

• **Anéis com unidade**

Um *anel com unidade* é um anel $R$ com a propriedade de existir em $R$ um elemento 1, chamado de *unidade*, com $1 \neq 0$, tal que $a\cdot 1 = 1\cdot a = a$ para todo $a \in R$.

A condição $1 \neq 0$ é necessária para evitar uma situação trivial. Se $1 = 0$, então para qualquer $a \in R$ vale $a = a\cdot 1 = a\cdot 0 = 0$, ou seja, $R$ contém apenas o elemento 0. Como observamos, alguns autores, como Bourbaki, incluem a existência de uma unidade (não nula) na definição de anel.

Uma observação um pouco menos trivial, mas relevante, é que uma unidade, se existir, é sempre única. De fato, se em um anel $R$ com uma unidade 1 existir um outro elemento $1' \in R$ tal que também valha $a \cdot 1' = 1' \cdot a = a$ para todo $a \in R$, teremos, por força das mesmas propriedades, $1' = 1' \cdot 1 = 1$. A mesma observação vale para álgebras com unidade.

• **Anéis sem divisores de zero**

Dado um anel $R$, um elemento não nulo $a \in R$ é dito ser um *divisor de zero* se existir pelo menos um $b \in R$ com $b \neq 0$ tal que $a \cdot b = 0$ ou $b \cdot a = 0$.

Se em um dado anel a relação $a \cdot b = 0$ só for possível se $a = 0$ ou $b = 0$ ou ambos, então esse anel é dito ser um *anel sem divisores de zero*.

**Exemplos 2.16** $\mathbb{C}$ e $\mathbb{R}$ são anéis sem divisores de zero (com os produtos e somas usuais), mas os anéis $\mathrm{Mat}\,(n,\ \mathbb{C})$, $n > 1$, têm divisores de zero (com o produto e soma usuais), pois tem-se, por exemplo, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. ♦

**E. 2.54** *Exercício*. Mostre que em $\mathbb{Z}_4$ tem-se $2 \cdot 2 = 0$, ou seja, 2 é um divisor de zero. Há outros divisores de zero em $\mathbb{Z}_4$? ✠

**E. 2.55** *Exercício*. Mostre que em $\mathbb{Z}_n$ existem divisores de zero caso $n$ não seja um número primo. ✠

• **Anéis de integridade**

Um anel comutativo (ou seja, cujo produto é comutativo), com unidade e sem divisores de zero é dito ser um *anel de integridade* ou também um *domínio de integridade*.

As álgebras $\mathbb{R} \oplus \mathbb{R}$ e $\mathbb{D}$ (dos complexos hiperbólicos), introduzidos na Seção 2.6.3.1, página 250, possuem divisores de zero e, portanto, não são anéis de integridade.

Para a relação entre anéis de integridade e corpos, vide adiante.

• **Anéis de divisão**

Um anel $R$ é dito ser um *anel de divisão* se possuir uma unidade multiplicativa 1, i.e., um elemento tal que para todo $a \in R$ vale $a \cdot 1 = 1 \cdot a = a$ e se para todo $a \in R$, $a \neq 0$, existir uma inversa multiplicativa em $R$, ou seja, um elemento denotado por $a^{-1}$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Em um anel de divisão associativo, a inversa de cada elemento não nulo $a$ é única. De fato, se para um dado $a$ não nulo existir um outro elemento $b$ tal que $a \cdot b = b \cdot a = 1$, teremos $b = b \cdot 1 = b \cdot \left(a \cdot a^{-1}\right) \overset{\text{assoc.}}{=} \left(b \cdot a\right) \cdot a^{-1} = 1 \cdot a^{-1} = a^{-1}$.

**E. 2.56** *Exercício importante*. Mostre que um anel de divisão não pode possuir divisores de zero. Portanto, todo anel de divisão comutativo é também um anel de integridade. ✠

**Exemplos 2.17** Com as definições usuais $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{Q}$ são anéis de divisão mas $\mathbb{Z}$ não o é (falha a existência da inversa multiplicativa). $\mathrm{Mat}\,(n,\ \mathbb{C})$, com $n > 1$, também não é um anel de divisão com as definições usuais pois nem toda a matriz não nula é inversível. ♦

Outro exemplo de anel de divisão (não comutativo!) são os quatérnios, que serão discutidos à página 250.

• **Álgebras de divisão**

Uma álgebra $A$ é dita ser uma *álgebra de divisão* se possuir uma unidade multiplicativa 1, i.e., um elemento tal que para todo $a \in A$ vale $a \cdot 1 = 1 \cdot a = a$ e se para todo $a \in A$, $a \neq 0$, existir uma inversa multiplicativa em $A$, ou seja, um elemento denotado por $a^{-1}$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Como no caso de anéis de divisão associativos, em uma álgebra de divisão associativa, a inversa de cada elemento não nulo é única.

• **Corpos**

Todo anel de divisão cujo produto "$\cdot$" é comutativo é um corpo (verifique!).

• **Corpos não comutativos**

Como a única distinção entre as definições de corpos e de anéis de divisão é que para os primeiros a comutatividade do produto é requerida, diz-se também por vezes que anéis de divisão não comutativos são *corpos não comutativos.*

• **Corpos e anéis de integridade**

É bem claro pelas definições que todo corpo é também um anel de integridade. A recíproca é parcialmente válida:

**Teorema 2.2** *Todo anel de integridade finito é um corpo.* □

Prova. Se $A$ é um anel de integridade, tudo que precisamos é mostrar que todo elemento não nulo de $A$ é inversível. Seja $a$ um elemento de $A \setminus \{0\}$. Definamos a aplicação $\alpha : A \setminus \{0\} \to A$ dada por

$$\alpha(y) \;=\; ay\,.$$

Note que, como $A$ é um anel de integridade o lado direito é não nulo pois nem $a$ nem $y$ o são. Assim, $\alpha$ é, em verdade, uma aplicação de $A \setminus \{0\}$ em $A \setminus \{0\}$ e, como tal, é injetora, pois se $ay = az$, segue que $a(y - z) = 0$, o que só é possível se $y = z$, pois $A$ é um anel de integridade e $a \neq 0$. Agora, uma aplicação injetora de um conjunto finito em si mesmo tem necessariamente que ser sobrejetora (por quê?). Assim, $\alpha$ é uma bijeção de $A \setminus \{0\}$ sobre si mesmo. Como $1 \in A \setminus \{0\}$, segue que existe $y \in A \setminus \{0\}$ tal que $ay = 1$, ou seja, $a$ tem uma inversa. Como $a$ é um elemento arbitrário de $A \setminus \{0\}$, segue que todo elemento de $A \setminus \{0\}$ tem inversa e, portanto, $A$ é um corpo. ■

Anéis de integridade infinitos não são necessariamente corpos:

*Antiexemplo.* Um exemplo de um anel de integridade que não é um corpo é o conjunto de todos os polinômios de $\mathbb{C}$ em $\mathbb{C}$ com o produto e soma usuais. Em verdade, os únicos polinômios que têm inverso multiplicativo são os polinômios constantes não nulos.

• **Anéis de divisão finitos**

O seguinte teorema, originalmente devido a Wedderburn[43], é bastante surpreendente por mostrar uma insuspeita relação entre a cardinalidade de um anel de divisão e a natureza de seu produto

**Teorema 2.3** *Todo anel de divisão finito é comutativo.* □

Assim, pelas observações feitas acima conclui-se:

**Corolário 2.2** *Todo anel de divisão finito é um corpo.* □

A prova do Teorema 2.3 não será apresentada aqui. Uma demonstração elegante, devida a Witt[44], pode ser encontrada na magnífica referência [9].

## 2.1.9 Ações e Representações

No que segue apresentaremos uma série de definições e resultados elementares envolvendo as noções de ação de grupos e representação de grupos e álgebras, temas esses desenvolvidos em outras partes deste texto.

### 2.1.9.1 Ações de Grupos

Seja $M$ um conjunto não vazio e $G$ um grupo. Uma função $\alpha : G \times M \to M$ é dita ser uma *ação à esquerda de $G$ sobre $M$* se as seguintes condições forem satisfeitas:

[43] Joseph Henry Maclagen Wedderburn (1882–1948). O trabalho original de Wedderburn é: J. H. M. Wedderburn, "A theorem on finite algebras", Trans. Amer. Math. Soc. **6**, 349–352 (1905). Esse trabalho contém três demonstrações do Teorema 2.3.

[44] Ernst Witt (1911–1991). O trabalho original de Witt é "Über die Kommutativität endlicher Schiefköerper". Abh. Math. Sem. Univ. Hamburg, **8**, 413 (1931).

1. Para todo $g \in G$ a função $\alpha(g,\ \cdot) : M \to M$ é bijetora[45].
2. Se $e$ for o elemento neutro de $G$, então $\alpha(e,\ \cdot) : M \to M$ é a função identidade: $\alpha(e,\ x) = x$ para todo $x \in M$.
3. Para todos $g,\ h \in G$ e todo $x \in M$ vale

$$\alpha\big(g,\ \alpha(h,\ x)\big) \ = \ \alpha(gh,\ x)\ . \tag{2.49}$$

Uma função $\beta : G \times M \to M$ é dita ser uma *ação à direita de $G$ sobre $M$* se as seguintes condições forem satisfeitas

1. Para todo $g \in G$ a função $\beta(g,\ \cdot) : M \to M$ é bijetora.
2. Se $e$ é o elemento neutro de $G$, então $\beta(e,\ \cdot) : M \to M$ é a função identidade: $\beta(e,\ x) = x$ para todo $x \in M$.
3. Para todos $g,\ h \in G$ e todo $x \in M$ vale

$$\beta\big(g,\ \beta(h,\ x)\big) \ = \ \beta(hg,\ x)\ . \tag{2.50}$$

Note-se que a distinção básica entre (2.49) e (2.50) é a ordem do produto no grupo. Se $G$ é Abeliano não há distinção entre uma ação à direita ou à esquerda.

**E. 2.57** *Exercício.* Seja $\alpha : G \times M \to M$ uma ação à esquerda de um grupo $G$ em um conjunto $M$. Mostre que $\beta : G \times M \to M$ definida por $\beta(g,\ x) = \alpha\big(g^{-1},\ x\big)$ é uma ação à direita de $G$ em $M$. ✠

É frequente encontrar-se outras notações para designar ações de grupos em conjuntos. Uma ação à esquerda $\alpha(g,\ x)$ é frequentemente denotada por $\alpha_g(x)$, de modo que a relação (2.49) fica $\alpha_g\big(\alpha_h(x)\big) = \alpha_{gh}(x)$. Para uma ação à direita, (2.50) fica $\beta_g\big(\beta_h(x)\big) = \beta_{hg}(x)$.

Talvez a notação mais conveniente seja denotar uma ação à esquerda $\alpha(g,\ x)$ simplesmente por $g \cdot x$ ou apenas $gx$. A relação (2.49) fica $g(hx) = (gh)x$. Para uma ação à direita $\beta(g,\ x)$ a notação fica $x \cdot g$, ou apenas $xg$, de modo que (2.50) fica $(xh)g = x(hg)$. Essa notação justifica o uso da nomenclatura *à direita* ou *à esquerda* para classificar as ações.

Seja $\mathcal{F}$ uma coleção de funções bijetoras de um conjunto $M$ em si mesmo. Uma ação $\alpha : G \times M \to M$ é dita ser uma *ação de $G$ em $M$ pela família $\mathcal{F}$* se para todo $g \in G$ as funções $\alpha(g,\ \cdot) : M \to M$ forem elementos do conjunto $\mathcal{F}$.

**E. 2.58** *Exercício.* Seja $G = \mathrm{O}(n)$ o grupo de todas as matrizes reais $n \times n$ ortogonais (ou seja, tais que $R^T = R^{-1}$, onde $R^T$ denota a transposta de $R$). Seja $M$ o conjunto de todas as matrizes reais $n \times n$ simétricas (ou seja, tais que $A^T = A$). Mostre que $\alpha_R(A) := RAR^T$, com $R \in \mathrm{O}(n)$ e $A \in M$, é uma ação à esquerda de $G$ em $M$. Com as mesmas definições, mostre que $\beta_R(A) := R^T AR$ é uma ação à direita de $G$ em $M$.

*Sugestão.* O único ponto que poderia ser difícil para alguns seria mostrar que, para cada $R$ fixo, $\alpha_R$ é bijetora, ou seja, é sobrejetora e injetora. Para mostrar que $\alpha_R$ é sobrejetora, note que se $A$ é uma matriz simétrica qualquer, podemos trivialmente escrever $A = R(R^T AR)R^T$, mostrando que $A = \alpha_R(B)$, onde $B = R^T AR$ é simétrica. Para provar que $\alpha_R$ é injetora note que, se $RA_1R^T = RA_2R^T$, segue facilmente, multiplicando-se por $R^T$ à esquerda e por $R$ à direita, que $A_1 = A_2$.

Observamos, por fim, que poderíamos ter adotado $G = \mathrm{SO}(n)$ nesse exemplo, sem mais modificações. ✠

**E. 2.59** *Exercício.* Seja $G = \mathrm{U}(n)$ o grupo de todas as matrizes complexas $n \times n$ unitárias (ou seja, tais que $U^* = U^{-1}$, onde $U^*$ denota a adjunta de $U$: $U^* = \overline{U^T}$). Seja $M$ o conjunto de todas as matrizes complexas $n \times n$ Hermitianas (ou seja, tais que $A^* = A$). Mostre que $\alpha_U(A) := UAU^*$, com $U \in \mathrm{SU}(n)$ e $A \in M$, é uma ação à esquerda de $G$ em $M$. Com as mesmas definições, mostre que $\beta_U(A) := U^* AU$ é uma ação à direita de $G$ em $M$. Observamos, novamente, que poderíamos ter adotado $G = \mathrm{SU}(n)$ nesse exemplo, sem mais modificações. ✠

Um outro exemplo dos mais interessantes é a ação do grupo $\mathrm{SL}(2,\ \mathbb{C})$ sobre o conjunto das matrizes complexas Hermitianas $2 \times 2$, ação essa que possui uma insuspeita relação com o grupo de Lorentz próprio ortócrono $\mathscr{L}_+^\uparrow$ em $3+1$ dimensões. Esse exemplo, que é relevante na teoria dos spinores, é extensamente desenvolvido na Seção 21.9, página 1239.

[45] Para $g \in G$ fixo, $\alpha(g,\ \cdot) : M \to M$ denota a função $M \ni m \mapsto \alpha(g,\ m) \in M$, ou seja, a função que a cada $m \in M$ associa $\alpha(g,\ m) \in M$.

• **Ações sobre funções em $M$**

Seja $G$ um grupo e $\alpha : G \times M \to M$ uma ação à esquerda de $G$ sobre um conjunto não vazio $M$. Podemos definir uma ação à esquerda $\mathcal{A}$ de $G$ no espaço das funções (assumindo valores complexos, digamos) definidas em $M$ da seguinte forma: se $f : M \to \mathbb{C}$ é uma função de $M$ em $\mathbb{C}$ definimos $\mathcal{A}_g f : M \to \mathbb{C}$ por

$$\big(\mathcal{A}_g f\big)(m) \;:=\; f\big(\alpha_{g^{-1}}(m)\big) \tag{2.51}$$

para todo $g \in G$ e todo $m \in M$. Para constatar que se trata de uma ação à esquerda, observemos primeiramente que para todo $m \in M$ vale

$$\Big(\big(\mathcal{A}_{g_1} \circ \mathcal{A}_{g_2}\big) f\Big)(m) \;=\; \Big(\mathcal{A}_{g_1}\big(\mathcal{A}_{g_2} f\big)\Big)(m) \;=\; \big(\mathcal{A}_{g_2} f\big)\big(\alpha_{g_1^{-1}}(m)\big)$$

$$=\; f\Big(\alpha_{g_2^{-1}}\big(\alpha_{g_1^{-1}}(m)\big)\Big) \;=\; f\Big(\alpha_{g_2^{-1} g_1^{-1}}(m)\Big) \;=\; f\Big(\alpha_{(g_1 g_2)^{-1}}(m)\Big) \;=\; \big(\mathcal{A}_{g_1 g_2} f\big)(m)\;.$$

Isso provou que

$$\mathcal{A}_{g_1} \circ \mathcal{A}_{g_2} \;=\; \mathcal{A}_{g_1 g_2}$$

para todos $g_1,\; g_2 \in G$.

**E. 2.60** *Exercício*. Complete a prova que $\mathcal{A}_g$ define uma ação nas funções definidas em $M$, constatando que $\mathcal{A}_e f = f$ para toda função $f$ ($e$ é o elemento neutro de $G$) e que para cada $g \in G$ a aplicação $\mathcal{A}_g$ é bijetora no espaço de funções. ✠

**Exemplo 2.18** Sejam $M = \mathbb{R}$ e $G = (\mathbb{R},\; +)$, o grupo aditivo dos reais, ou grupo de translações em $\mathbb{R}$. A expressão $\alpha_y(x) = x+y$, com $x \in M$ e $y \in G$, representa uma ação de $G$ sobre $M$, ação essa na qual cada ponto $x \in M$ é transladado de $y$. Se $f : \mathbb{R} \to \mathbb{R}$ for uma função de $M$ nos reais, teremos, segundo a definição geral (2.51), que

$$\big(\mathcal{A}_y f\big)(x) \;:=\; f(x-y)\;.$$

Isso representa uma ação de $G$ sobre as funções definidas em $M$. É fácil perceber seu significado: a ação $\mathcal{A}_y$ translada de $y$ o gráfico de cada função $f$. ⧫

**E. 2.61** *Exercício*. Mostre que se $\alpha : G \times M \to M$ é uma ação à esquerda a aplicação

$$\big(\mathcal{B}_g f\big)(m) \;:=\; f\big(\alpha_g(m)\big) \tag{2.52}$$

define uma ação à direita nas funções definidas em $M$, pois vale neste caso

$$\mathcal{B}_{g_1} \circ \mathcal{B}_{g_2} \;=\; \mathcal{B}_{g_2 g_1}\;.$$

Compare a definição (2.52) com a definição (2.51). ✠

• **Órbita de uma ação**

Seja $G$ um grupo e $\gamma : G \times M \to M$ uma ação (à esquerda ou à direita) de $G$ sobre um conjunto não vazio $M$. Para $m \in M$, definimos a *órbita* de $m$ pela ação $\gamma$ como sendo o conjunto $\mathrm{Orb}_\gamma(m) := \{\gamma_g(m),\; g \in G\} \subset M$.

Claro está que para todo $m \in M$ vale $m \in \mathrm{Orb}_\gamma(m)$.

**E. 2.62** *Exercício*. Mostre que para todo $m \in M$ vale a afirmação que para todo $m' \in \mathrm{Orb}_\gamma(m)$ tem-se $\mathrm{Orb}_\gamma(m') = \mathrm{Orb}_\gamma(m)$. ✠

**E. 2.63** *Exercício*. Conclua que se existe $m \in M$ tal que $\mathrm{Orb}_\gamma(m) = M$, então $\mathrm{Orb}_\gamma(m') = M$ para todo $m' \in M$. ✠

Se $N \subset M$, a união de todas as órbitas de todos os pontos de $N$ é denotada por $GN$, ou seja, $GN := \bigcup_{n \in N} \mathrm{Orb}_\gamma(n)$. Em outras palavras, $GN := \{\gamma_g(n),\; n \in N,\; g \in G\}$.

Na notação $GN$ é subentendida qual a ação $\gamma$ se está considerando. Quando se deseja explicitá-la, denota-se $GN$ por $GN_\gamma$, por $G_\gamma N$ ou ainda por $\gamma(G)N$.

• **Conjuntos invariantes por uma ação**

Seja $G$ um grupo e $\gamma : G \times M \to M$ uma ação (à esquerda ou à direita) de $G$ sobre um conjunto não vazio $M$. Um conjunto não vazio $N \subset M$ é dito ser um *conjunto invariante pela ação* $\gamma$ se para todo $n \in N$ e todo $g \in G$ valer $\gamma_g(n) \in N$, ou seja, se para todo $n \in N$ valer $\mathrm{Orb}_\gamma(n) \subset N$.

Em outras palavras, um conjunto não vazio $N \subset M$ é invariante pela ação $\gamma$ se $GN \subset N$.

É muito fácil ver que se $GN \subset N$, então $GN = N$. De fato, se $GN \subset N$ e $n \in N$, então, evidentemente, $n = \gamma_e(n) \in GN$ (onde $e$ é o elemento neutro de $G$), mostrando que $N \subset GN$.

• **Pontos fixos de uma ação**

Seja $G$ um grupo e $\gamma : G \times M \to M$ uma ação (à esquerda ou à direita) de $G$ sobre um conjunto não vazio $M$.

Dizemos que $p \in M$ é um *ponto fixo de um elemento* $g_0 \in G$ pela ação $\gamma$ se $\gamma_{g_0}(p) = p$.

Dizemos que $p \in M$ é um *ponto fixo da ação* $\gamma$ se $\gamma_g(p) = p$ para todo $g \in G$. Em outras palavras, $p \in M$ é um ponto fixo da ação $\gamma$ se $\mathrm{Orb}_\gamma(p) = \{p\}$.

É evidente pelas definições que todo $m \in M$ é um ponto fixo do elemento neutro $e \in G$.

• **Ações triviais**

Seja $G$ um grupo e $\gamma : G \times M \to M$ uma ação (à esquerda ou à direita) de $G$ sobre um conjunto não vazio $M$.

Dizemos que $\gamma$ é uma ação trivial para um elemento $g_0 \in G$ se $\gamma_{g_0}(m) = m$ para todo $m \in M$. Se $\gamma_{g_0}(m) = m$ para todo $m \in M$, dizemos também que $g_0$ *age trivialmente em* $M$ *por* $\gamma$.

Dizemos que $\gamma$ é uma *ação trivial* se $\gamma_g(m) = m$ para todo $m \in M$ e todo $g \in G$.

À página 175 veremos que o conjunto de todos os elementos de $G$ que agem trivialmente por uma ação $\gamma$ em um conjunto $M$ é um subgrupo normal de $G$.

• **Tipos de ações: ações transitivas, livres ou efetivas**

Seja $G$ um grupo e $\gamma : G \times M \to M$ uma ação (à esquerda ou à direita) de $G$ sobre um conjunto não vazio $M$.

1. Dizemos que $\gamma$ é uma *ação transitiva* em $M$ (ou que $\gamma$ *age transitivamente* em $M$) se existir $m_0 \in M$ tal que $\{\gamma_g(m_0),\ g \in G\} = M$.

   Em outras palavras, $\gamma$ age transitivamente em $M$ se existir pelo menos um elemento $m_0$ de $M$ cuja órbita por $\gamma$ seja todo $M$: $\mathrm{Orb}_\gamma(m_0) = M$. Pelo Exercício E. 2.62, se um elemento de $M$ possui essa propriedade, então todos a possuem.

   Segue que se $\gamma$ age transitivamente em $M$, então para cada par $m,\ n \in M$ existe $g \in G$ (não necessáriamente único!) tal que $\gamma_g(m) = n$.

2. Dizemos que $\gamma$ é uma *ação simplesmente transitiva* em $M$, ou uma *ação regular* em $M$, se para cada par $m,\ n \in M$ existir um <u>único</u> $g \in G$ tal que $\gamma_g(m) = n$. Evidentemente, toda ação simplesmente transitiva é transitiva. Para uma recíproca, vide Proposição 2.4, logo abaixo.

3. Dizemos que $\gamma$ é uma *ação livre* em $M$ (ou que $\gamma$ *age livremente* em $M$) se o elemento neutro $e \in G$ for o único elemento de $G$ que possui pontos fixos pela ação $\gamma$. Em outras palavras, se $\gamma$ for uma ação livre e existir $p \in M$ tal que $\gamma_g(p) = p$ para algum $g$, então $g = e$.

4. Dizemos que $\gamma$ é uma *ação efetiva* em $M$ (ou que $\gamma$ *age efetivamente* em $M$) se o elemento neutro $e \in G$ for o único elemento de $G$ para o qual todo elemento de $M$ é um ponto fixo. Em outras palavras $\gamma$ age efetivamente em $M$ se a igualdade $\gamma_g(m) = m$ for válida para todo $m \in M$ apenas caso $g$ seja o elemento neutro.

   Dizemos, com isso, que se $\gamma$ age efetivamente em $M$, então o elemento neutro $e \in G$ é o único elemento para o qual $\gamma$ age trivialmente.

   Uma ação efetiva é também dita ser uma *ação fiel*.

Sobre a relação entre ações transitivas e simplesmente transitivas temos o seguinte resultado:

**Proposição 2.4** *Seja $G$ um grupo e $\gamma : G \times M \to M$ uma ação (à esquerda ou à direita) de $G$ sobre um conjunto não vazio $M$. Então, $\gamma$ é simplesmente transitiva se e somente se for transitiva e livre.* □

Prova. Seja $e$ o elemento neutro de $G$. Se $\gamma$ for uma ação simplesmente transitiva, então $\gamma$ é evidentemente transitiva. Além disso, se $p \in M$ for tal que $\gamma_g(p) = p$ para algum $g \in G$, então, como também tem-se $\gamma_e(p) = p$, o fato de $\gamma$ ser simplesmente transitiva implica $g = e$, significando que $\gamma$ é livre.

Reciprocamente, seja $\gamma$ uma ação transitiva e livre. Pela transitividade sabemos que para um par de pontos $m,\ n \in M$ existe ao menos um $g \in G$ tal que $\gamma_g(m) = n$. Suponhamos que haja $h \in G$, eventualmente distinto de $g$, para o qual também valha $\gamma_h(m) = n$ Então, se $\gamma$ for uma ação à esquerda, tem-se $\gamma_{g^{-1}h}(m) = \gamma_{g^{-1}}\big(\gamma_h(m)\big) = \gamma_{g^{-1}}(n) = m$, implicando (pelo fato de $\gamma$ ser livre) que $g^{-1}h = e$ e, portanto, que $g = h$. Se $\gamma$ for uma ação à direita, tem-se $\gamma_{g^{-1}h}(n) = \gamma_h\big(\gamma_{g^{-1}}(n)\big) = \gamma_h(m) = n$, implicando também que $g^{-1}h = e$ e, portanto, que $g = h$. Em ambos os casos, concluímos com isso que $\gamma$ é simplesmente transitiva. ■

• **Transitividade e espaços homogêneos**

Se uma ação $\gamma$ (à direita ou à esquerda) for transitiva em $M$ segundo a definição acima, dizemos que $M$ é um *espaço homogêneo* do grupo $G$ pela a ação $\gamma$, ou simplesmente um *espaço homogêneo* do grupo $G$.

Se uma ação $\gamma$ (à direita ou à esquerda) for simplesmente transitiva em $M$ segundo a definição acima, dizemos que $M$ é um *espaço homogêneo principal* do grupo $G$ pela a ação $\gamma$, ou simplesmente um *$G$-torsor*.

• **Ações e relações de equivalência. *"Orbit spaces"***

Dado um grupo $G$ e uma ação $\gamma : G \times M \to M$ (à esquerda ou à direita) de $G$ sobre um conjunto não vazio $M$, podemos definir em $M$ uma relação de equivalência $\sim_\gamma$ da seguinte forma: dizemos que dois pontos $m,\ n \in M$ são equivalentes, $m \sim_\gamma n$ se existir $g \in G$ tal que $\gamma_g(m) = n$.

**E. 2.64** *Exercício (fácil).* Prove que essa definição realmente estabelece uma relação de equivalência em $M$. ✠

É também muito fácil concluir que dois pontos $m,\ n \in M$ são equivalentes no sentido acima se e somente se pertencerem à mesma órbita por $\gamma$, ou seja, se e somente se $\mathrm{Orb}_\gamma(m) = \mathrm{Orb}_\gamma(n)$. Disso segue imediatamente que a coleção das classes de equivalência por essa relação coincide com a coleção das órbitas da ação $\gamma$. Essa coleção é denominada *espaço de órbitas* da ação $\gamma$ em $M$ ou, mais comummente, pelo termo em Inglês "*orbit space*". Muito frequentemente, esse espaço das órbitas é denotado por $M/G$ (dito ser o quociente do espaço $M$ pelo grupo $G$ por meio da ação $\gamma$).

É bastante claro que se uma ação $\gamma$ age transitivamente em $M$, então seu espaço de órbitas coincide com $\{M\}$, um conjunto de um único elemento.

• **Grupos de isotropia, de estabilidade, ou estabilizadores (*"little groups"*)**

Outra noção útil, empregada especialmente no estudo de representações de grupos, é a noção de *grupo de isotropia*, também denominado *grupo estabilizador* ou ainda *grupo estabilidade*.

Seja $G$ um grupo e $\gamma : G \times M \to M$ uma ação (à esquerda ou à direita) de $G$ sobre um conjunto não vazio $M$. Para $m \in M$, defina-se $G_{\gamma,\,m} := \big\{ g \in G \,\big|\, \gamma_g(m) = m \big\}$. É muito fácil constatar que $G_{\gamma,\,m}$ é um subgrupo de $G$: o subgrupo dos elementos de $G$ que mantém $m$ invariante pela ação $\gamma$.

Provaremos isso para ações à esquerda, o outro caso sendo análogo. De fato, 1º é claro que $e \in G_{\gamma,\,m}$; 2º se $g \in G_{\gamma,\,m}$ então $\gamma\big(g^{-1},\ m\big) = \gamma\big(g^{-1},\ \gamma(g,\ m)\big) = \gamma\big(g^{-1}g,\ m\big) = \gamma(e,\ m) = m$, provando que $g^{-1} \in G_{\gamma,\,m}$; por fim, 3º se $g_1,\ g_2 \in G_{\gamma,\,m}$, então $\gamma\big(g_1 g_2,\ m\big) = \gamma\big(g_1,\ \gamma(g_2,\ m)\big) = \gamma\big(g_1,\ m\big) = m$, provando que $g_1 g_2 \in G_{\gamma,\,m}$.

O subgrupo $G_{\gamma,\,m}$ é denominado *grupo de isotropia* de $m$, ou *grupo estabilizador*, ou *grupo de estabilidade* de $m$. Na literatura da Física, ele é dito ser o "*little group*" de $m$. Essa última denominação foi introduzida por Wigner[46] em seu célebre estudo[47] das representações unitárias irredutíveis do chamado *grupo de Poincaré*[48].

[46] Eugene Paul Wigner (1902–1995).

[47] E. Wigner, "On unitary representations of the inhomogeneous Lorentz group", Annals Math. **40**, 149–204 (1939).

[48] Jules Henri Poincaré (1854–1912). O chamado *Grupo de Poincaré*, de fundamental importância na Teoria da Relatividade Especial, é introduzido à página 1209.

Se a ação $\gamma$ for transitiva e $x \neq y$ são elementos distintos de $M$, então $G_{\gamma,\,x}$ e $G_{\gamma,\,y}$ são isomorfos, pois existe $h \in G$ tal que $G_{\gamma,\,x} = h^{-1} G_{\gamma,\,y} h$. No caso de $\gamma$ ser uma ação à esquerda, esse $h$ é um elemento de $G$ tal que $\gamma(h,\ x) = y$ (tal $h$ existe devido à suposta transitividade de $\gamma$). Caso $\gamma$ seja uma ação à direita devemos trocar $h$ por $h^{-1}$.

**E. 2.65** *Exercício*. Prove essas afirmações ✠

**E. 2.66** *Exercício simples.* Prove que uma ação $\gamma : G \times M \to M$ é livre se e somente se todos os grupo de isotropia $G_{\gamma,\,m}$, com $m \in M$ forem triviais, ou seja, se forem compostos apenas pelo elemento neutro $e \in G$. ✠

• **Tipos de ações: continuidade e continuidade forte**

Em se lidando com grupos topológicos agindo em espaços topológicos, outras noções podem ser introduzidas, como a de *ação contínua*, a de *ação fortemente contínua* etc.

A importante noção de *grupo topológico* será apresentada à página 1282 e um tanto discutida na Seção 22.2, página 1284. Vamos a um breve resumo. Seja $G$ um grupo. Para cada $g \in G$ podemos definir uma função $\lambda_g : G \to G$ por $\lambda_g(h) := gh$. Fora isso, tem-se também em $G$ a função $inv : G \to G$ definida por $inv(h) := h^{-1}$. Seja $\tau_G$ uma topologia em $G$. Dizemos que $G$ é um *grupo topológico* em relação a topologia $\tau_G$ se nessa topologia a função $inv$ e todas as funções $\lambda_g$ forem contínuas.

Podemos agora definir noções de continuidade ligadas a ações de grupos topológicos em espaços topológicos.

Seja $M$ um conjunto não vazio dotado de uma topologia $\tau_M$. Uma ação (à esquerda ou à direita) $\gamma : G \times M \to M$ de $G$ sobre $M$ é dita ser

1. *contínua* , se for uma função contínua do espaço topológico $(G \times M,\ \tau_G \times \tau_M)$ no espaço topológico $(M,\ \tau_M)$. Aqui, $\tau_G \times \tau_M$ denota a topologia produto[49] das topologias $\tau_G$ e $\tau_M$.
2. *fortemente contínua*, se para cada $m \in M$ a aplicação de $G$ em $M$ dada por $G \ni g \mapsto \gamma_g(m) \in M$, for contínua em relação às topologias $\tau_G$ e $\tau_M$.

### 2.1.9.2 Representações de Grupos e de Álgebras

• **Representações de grupos**

Uma representação de um grupo é uma ação à esquerda do mesmo em um espaço vetorial pela família das aplicações lineares inversíveis agindo nesse espaço vetorial.

Sejam $G$ um grupo e $V$ um espaço vetorial sobre um corpo $\mathbb{K}$. Uma representação de $G$ em $V$ é uma função $\pi : G \times V \to V$ tal que para todo $g \in G$ as funções $\pi(g,\ \cdot) : V \to V$ sejam lineares e bijetivas e satisfazem $\pi(e,\ v) = v$ e $\pi(g,\ \pi(h,\ v)) = \pi(gh,\ v)$ para todos $g,\ h \in G$ e todo $v \in V$.

Devido à linearidade é conveniente denotar $\pi(g,\ v)$ por $\pi(g)v$. Uma representação satisfaz assim:

1. Para todo $g \in G$, $\pi(g)$ é uma aplicação linear bijetora de $V$ em $V$:

$$\pi(g)(\alpha u + \beta v) \ = \ \alpha \pi(g) u + \beta \pi(g) v$$

   para todos $\alpha,\ \beta \in \mathbb{K}$ e todos $u,\ v \in V$.

2. $\pi(e) = \mathbb{1}$, o operador identidade em $V$.

3. Para todos $g,\ h \in G$ vale

$$\pi(g)\pi(h) \ = \ \pi(gh)\ .$$

A teoria das representações de grupos será desenvolvida no Capítulo, 23, página 1320. A teoria das representações de grupos é de grande importância no tratamento de simetrias na Mecânica Quântica.

[49] A noção geral de topologia produto é introduzida e discutida na Seção 33.5, página 1769.

• **Representações de álgebras**

Seja $A$ uma álgebra sobre um corpo $\mathbb{K}$ e $V$ um espaço vetorial sobre o mesmo corpo. Uma representação de $A$ em $V$ é uma família de funções lineares de $V$ em $V$, $\{\pi(a),\ a \in A\}$, satisfazendo

1. Para todo $a \in A$, $\pi(a) : V \to V$ é uma aplicação linear, ou seja,

$$\pi(a)(\alpha u + \beta v) \ = \ \alpha\pi(a)u + \beta\pi(a)v$$

   para todos $\alpha,\ \beta \in \mathbb{K}$ e todos $u,\ v \in V$.

2. Para todos $\alpha,\ \beta \in \mathbb{K}$ e todos $a,\ b \in A$ vale

$$\pi(\alpha a + \beta b) \ = \ \alpha\pi(a) + \beta\pi(b)\ .$$

3. Para todos $a,\ b \in A$

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

Uma representação $\pi$ de uma álgebra $A$ em um espaço vetorial $V$ é dita ser uma *representação fiel* se $\pi(a) = 0$ só ocorrer para $a = 0$.

Uma representação $\pi$ de uma álgebra $A$ em um espaço vetorial $V$ é dita ser uma *representação não-degenerada* se $\pi(a)v = 0$ para todo $a \in A$ só ocorrer para $v = 0$.

## 2.1.10 Morfismos, Homomorfismos, Epimorfismos, Isomorfismos, Monomorfismos, Endomorfismos e Automorfismos

Dos radicais gregos *hómos:* semelhante, igual; *mónos:* um, sozinho; *epi:* sobre; *ísos:* semelhante, igual; *endon:* para dentro, dentro; *autós:* próprio, mesmo e *morphé:* forma.

Nos limitaremos primeiramente a listar algumas definições básicas que serão usadas e desenvolvidas no restante do texto, onde mais exemplos serão apresentados. A pretensão não é a de desenvolver os assuntos, mas de apresentar as definições para referência futura.

Em termos informais um morfismo entre duas estruturas de um mesmo tipo (dois grupos, dois espaços vetoriais, duas álgebras, dois anéis etc.) é uma função entre as mesmas que respeita as operações lá definidas.

• **Morfismos de grupos**

Dados dois grupos $G$ e $H$, com unidades $e_G$ e $e_H$, respectivamente, uma função $\phi : G \to H$ é dita ser um *homomorfismo* ou *morfismo de grupos* se $\phi(ab) = \phi(a)\phi(b)$ para todos $a,\ b \in G$.

Se $\phi : G \to H$ é um homomorfismo, então vale $\phi(e_G) = e_H$. De fato, para qualquer $a \in G$ tem-se $a = ae_G$ e, portanto, $\phi(a) = \phi(a)\phi(e_G)$. Aplicando-se $\phi(a)^{-1}$ à esquerda, obtemos $e_H = \phi(e_G)$, como desejávamos mostrar. Outro fato verdadeiro para homomorfismos de grupos $\phi : G \to H$ é a relação $\phi\big(a^{-1}\big) = \phi(a)^{-1}$, válida para todo $a \in G$. De fato, como $e_G = a^{-1}a = aa^{-1}$, temos $\phi\big(a^{-1}\big)\phi\big(a\big) = \phi\big(a^{-1}a\big) = \phi(e_G) = e_H = \phi(e_G) = \phi\big(aa^{-1}\big) = \phi\big(a\big)\phi\big(a^{-1}\big)$, para todo $a \in G$, o que estabelece que $\phi\big(a^{-1}\big) = \phi(a)^{-1}$, como desejávamos mostrar.

**Exemplo 2.19** Seja $G \equiv \mathrm{GL}(n,\ \mathbb{C})$, o grupo das matrizes complexas de determinante não nulo e seja $H \equiv (\mathbb{C} \setminus \{0\},\ \cdot)$, o grupo multiplicativo dos números complexos (sem o zero). A aplicação $\phi : G \to H$ dada por $\phi(A) := \det(A)$ é um homomorfismo (pois vale $\det(AB) = \det(A)\det(B)$ para quaisquer $A,\ B \in \mathrm{Mat}\,(\mathbb{C},\ n)$). ♦

Dados dois grupos $G$ e $H$, com unidades $e_G$ e $e_H$, respectivamente, uma função $\phi : G \to H$ é dita ser um *anti-homomorfismo* se $\phi(ab) = \phi(b)\phi(a)$ para todos $a,\ b \in G$. Por exemplo, a aplicação $\phi : G \to G$ tal que $\phi(g) = g^{-1}$ é um anti-homomorfismo (verifique). Se $\phi : G \to H$ é um anti-homomorfismo, é fácil provar, como fizemos no caso de homomorfismos, que $\phi(e_G) = e_H$ e que $\phi\big(a^{-1}\big) = \phi(a)^{-1}$ para todo $a \in G$ (faça-o!).

Um homomorfismo $\phi : G \to H$ entre dois grupos é dito ser um *monomorfismo* se for injetivo.

Um homomorfismo $\phi : G \to H$ entre dois grupos é dito ser um *epimorfismo* se for sobrejetor.

Um homomorfismo $\phi : G \to H$ entre dois grupos é dito ser um *isomorfismo* se for bijetor.

Se $\phi : G \to H$ for um isomorfismo, então a aplicação inversa $\phi^{-1} : H \to G$ é também um isomorfismo. De fato, se $x,\ y \in H$, então, como $\phi$ é bijetor, segue que existem $a,\ b \in G$ (únicos) tais que $x = \phi(a)$ e $y = \phi(b)$. Logo, $\phi^{-1}(xy) = \phi^{-1}\Big(\phi(a)\phi(b)\Big) = \phi^{-1}\big(\phi(ab)\big) = ab = \phi^{-1}(x)\phi^{-1}(y)$. Isso provou que $\phi^{-1} : H \to G$ é também um homomorfismo e, por ser também bijetor, é também um isomorfismo.

Se dois grupos $G$ e $H$ forem tais que exista um isomorfismo $\phi$ entre ambos (o que nem sempre é o caso), dizemos que $G$ e $H$ são *isomorfos (por $\phi$)* e denotamos esse fato por $G \simeq_\phi H$, ou simplesmente por $G \simeq H$.

**Exemplo 2.20** Sejam $G_1 = (\mathbb{R},\ +)$, o grupo dos reais com a operação de soma, e $G_2 = (\mathbb{R}_+,\ \cdot)$, o grupo dos reais positivos com a operação de multiplicação. A função exponencial $\exp : \mathbb{R} \to \mathbb{R}_+$ definida, como usual, por $\mathbb{R} \ni x \mapsto e^x \in \mathbb{R}_+$, é um isomorfismo de $G_1$ em $G_2$, tendo como inversa a função logaritmo $\ln : \mathbb{R}_+ \to \mathbb{R}$ definida, como usual, por $\mathbb{R}_+ \ni x \mapsto \ln(x) \in \mathbb{R}$. Justifique! ♦

**E. 2.67** *Exercício importante.* Mostre que a relação de isomorfia entre grupos é uma relação de equivalência. ✠

Um homomorfismo $\rho$ de um grupo $G$ em si mesmo $\rho : G \to G$ é dito ser um *endomorfismo* de $G$.

**E. 2.68** *Exercício.* Seja o grupo $G \equiv (\mathbb{C} \setminus \{0\},\ \cdot)$, o grupo multiplicativo dos números complexos (sem o zero). Seja a aplicação $\rho : G \to G$ dada por $\rho(z) := z/|z|$, para $z \in \mathbb{C} \setminus \{0\}$. Mostre que $\rho$ é um endomorfismo de $G$. A imagem de $\rho$ é o círculo unitário em $\mathbb{C} \setminus \{0\}$. ✠

**E. 2.69** *Exercício.* Seja $\mathrm{GL}(n,\ \mathbb{C})$, o grupo das matrizes complexas de determinante não nulo. Seja a aplicação $\rho : \mathrm{GL}(n,\ \mathbb{C}) \to \mathrm{GL}(n,\ \mathbb{C})$ dada por $\rho(A) := \det(A)^{-1/n}\, A$, para $A \in \mathrm{GL}(n,\ \mathbb{C})$. Mostre que $\rho$ é um endomorfismo de $G$. A imagem de $\rho$ é $\mathrm{SL}(n,\ \mathbb{C}) \subset \mathrm{GL}(n,\ \mathbb{C})$. *Nota.* Como $\det(A)$ é, em geral, um número complexo, devemos especificar que $\det(A)^{1/n}$ é definida no ramo principal: se $w = |w|e^{i\phi} \in \mathbb{C}$, com $-\pi < \phi \leq \pi$, tomamos $w^{1/n} := |w|^{1/n} e^{i\phi/n}$. ✠

Um isomorfismo $\alpha$ de um grupo $G$ em si mesmo $\alpha : G \to G$ é dito ser um *automorfismo* de $G$.

**E. 2.70** *Exercício.* Um exemplo básico de automorfismo é o seguinte: seja $g \in G$ fixo. Definimos $\alpha_g : G \to G$ por $\alpha_g(a) = g^{-1}ag$ para todo $a \in G$. Mostre que para cada $g \in G$ fixo, $\alpha_g$ é um homomorfismo e que sua inversa é $\alpha_{g^{-1}}$, concluindo que $\alpha_g$ é um automorfismo. ✠

Um automorfismo de um grupo $G$ é dito ser um *automorfismo interno* se for da forma $\alpha_g$, apresentada no Exercício E. 2.70, para algum $g \in G$.

Muitas das definições apresentadas acima têm seus análogos em outras estruturas, como espaços vetoriais, álgebras, anéis, módulos etc. Trataremos de alguns casos.

• **Morfismos de espaços vetoriais**

Sejam $U$ e $V$ dois espaços vetoriais sobre o mesmo corpo $\mathbb{K}$. Uma função $\phi : U \to V$ é dita ser um *homomorfismo* ou *morfismo de espaços vetoriais* se $\phi(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1\phi(u_1) + \alpha_2\phi(u_2)$ para todos $\alpha_1,\ \alpha_2 \in \mathbb{K}$ e todos $u_1,\ u_2 \in U$.

Sejam $U$ e $V$ dois espaços vetoriais sobre o mesmo corpo $\mathbb{K}$. Uma função $\phi : U \to V$ é dita ser um *isomorfismo de espaços vetoriais* se for um morfismo de espaços vetoriais, e se for bijetora.

Se dois espaços vetoriais $U$ e $V$ sobre o mesmo corpo forem tais que exista um isomorfismo $\phi$ entre ambos dizemos que $U$ e $V$ são isomorfos (por $\phi$) e denotamos esse fato por $U \simeq_\phi V$, ou simplesmente por $U \simeq V$.

**E. 2.71** *Exercício importante.* Mostre que a relação de isomorfia entre espaços vetoriais é uma relação de equivalência. ✠

Em espaços vetoriais os conceitos de mono-, endo- e automorfismo não são muito empregados. Em verdade, morfismos de espaços vetoriais são mais frequentemente denominados *operadores lineares* ou *aplicações lineares*, como matrizes, por exemplo.

No caso de espaços vetoriais sobre o corpo dos complexos existem também os conceitos de anti-homomorfismo, anti-isomorfismo etc. Sejam $U$ e $V$ dois espaços vetoriais sobre $\mathbb{C}$. Uma função $\phi : U \to V$ é dita ser um *anti-homomorfismo* ou *antimorfismo de espaços vetoriais* se $\phi(\alpha_1 u_1 + \alpha_2 u_2) = \overline{\alpha_1}\phi(u_1) + \overline{\alpha_2}\phi(u_2)$ para todos $\alpha_1,\ \alpha_2 \in \mathbb{C}$ e todos $u_1,\ u_2 \in U$.

O conceito de anti-isomorfismo é análogo.

• **Morfismos de álgebras**

Sejam $A$ e $B$ duas álgebras (sobre o mesmo corpo $\mathbb{K}$, como espaços vetoriais). Uma função $\phi : A \to B$ é dita ser um *homomorfismo* ou *morfismo de álgebras* se for um morfismo de espaços vetoriais (ou seja $\phi(\alpha_1 a_1 + \alpha_2 a_2) = \alpha_1\phi(a_1) + \alpha_2\phi(a_2)$ para todos $\alpha_1,\ \alpha_2 \in \mathbb{K}$ e todos $a_1,\ a_2 \in A$) e se $\phi(a_1 \cdot a_2) = \phi(a_1) \cdot \phi(a_2)$ para todos $a_1,\ a_2 \in A$.

Sejam $A$ e $B$ duas álgebras sobre o mesmo corpo $\mathbb{K}$. Uma função $\phi : A \to B$ é dita ser um *isomorfismo de álgebras* se for um morfismo de álgebras e se for bijetora.

Se duas álgebras $A$ e $B$ sobre o mesmo corpo forem tais que exista um isomorfismo $\phi$ entre ambos dizemos que $A$ e $B$ são isomorfas (por $\phi$) e denotamos esse fato por $A \simeq_\phi B$, ou simplesmente por $A \simeq B$.

**E. 2.72** *Exercício importante.* Mostre que a relação de isomorfia entre álgebras é uma relação de equivalência. ✠

Um morfismo de álgebra $\rho$ de uma álgebra $A$ em si mesma $\rho : A \to A$ é dito ser um *endomorfismo* de $A$.

## 2.1.11 Induzindo Estruturas Algébricas

Uma construção muito interessante permite induzir a outros conjuntos estruturas de grupo, de espaço vetorial etc., definidas em certos conjuntos. Com ela é possível construir exemplos não-triviais de grupos e espaços vetoriais.

• **Induzindo estruturas de semigrupos e de grupos**

Seja $C$ um conjunto não vazio e seja $S$ um semigrupo, cujo produto denotamos por "$\cdot$". Suponhamos que exista uma função bijetora $f : C \to S$. Então, podemos definir em $C$ um produto $C \times C \to C$, denotado por "$*$", em relação ao qual $C$ é um também um semigrupo: para todos $a,\ b \in C$ definimos

$$a * b \ := \ f^{-1}\big(f(a) \cdot f(b)\big) \, . \tag{2.53}$$

De fato, é fácil ver que para todos $a,\ b$ e $c \in C$ vale

$$a*\big(b*c\big) \ = \ f^{-1}\big(f(a)\cdot f(b*c)\big) \ = \ f^{-1}\Big(f(a)\cdot\big(f(b)\cdot f(c)\big)\Big) \ = \ f^{-1}\Big(\big(f(a)\cdot f(b)\big)\cdot f(c)\Big) \ = \ f^{-1}\Big(f\big(a*b\big)\cdot f(c)\Big) \ = \ \big(a*b\big)*c \, ,$$

provando que o produto $*$ é associativo.

Como acima, seja $C$ um conjunto não vazio e seja $G$ um grupo cujo produto denotamos por "$\cdot$" e cujo elemento neutro é $n$. Então, se existir uma função bijetora $f : C \to G$ o conjunto $C$ é um grupo com o produto $*$ definido acima, seu elemento neutro, denotado por $e$, sendo dado por

$$e \ = \ f^{-1}(n) \tag{2.54}$$

sendo que para cada $a \in C$ sua inversa é dada por

$$a^{-1} \ = \ f^{-1}\big(f(a)^{-1}\big) \, . \tag{2.55}$$

De fato, vale para todo $a \in C$ que

$$a * e \ = \ f^{-1}\big(f(a)\cdot f(e)\big) \ = \ f^{-1}\Big(f(a)\cdot f\big(f^{-1}(n)\big)\Big) \ = \ f^{-1}\big(f(a)\cdot n\big) \ = \ f^{-1}\big(f(a)\big) \ = \ a \, ,$$

provando que $f^{-1}(n)$ é o elemento neutro em $C$. Finalmente, vale para todo $a \in C$ que

$$a * f^{-1}\big(f(a)^{-1}\big) \ = \ f^{-1}\Big(f(a)\cdot f\Big(f^{-1}\big(f(a)^{-1}\big)\Big)\Big) \ = \ f^{-1}\big(f(a)\cdot f(a)^{-1}\big) \ = \ f^{-1}(n) \ = \ e \, ,$$

provando que a inversa de $a$ em $C$ é $f^{-1}\big(f(a)^{-1}\big)$.

Comentamos que, por construção, o grupo formado por $C$ com o produto "$*$" é isomorfo ao grupo formado por $G$ com o produto "$\cdot$", o isomorfismo sendo dado por $f$.

**E. 2.73** *Exercício*. Mostre que se $G$ é um grupo Abeliano, então $C$, com a estrutura acima, também o será. ✠

**Exemplo 2.21** Seja $C = (0,\ 1)$ e $G = \mathbb{R}$, o grupo aditivo dos reais. Seja $f : (0,\ 1) \to \mathbb{R}$ definida por $f(x) := \frac{1}{2}\ln\left(\frac{x}{1-x}\right)$. A função $f$ é bijetora (prove isso!) e sua inversa $f^{-1} : \mathbb{R} \to (0,\ 1)$ é dada por $f^{-1}(y) = \frac{e^{2y}}{1+e^{2y}}$. Então, $(0,\ 1)$ é um grupo com o produto

$$a * b \;=\; \frac{\exp\left[\ln\left(\frac{a}{1-a}\right) + \ln\left(\frac{b}{1-b}\right)\right]}{1+\exp\left[\ln\left(\frac{a}{1-a}\right) + \ln\left(\frac{b}{1-b}\right)\right]} \;=\; \frac{ab}{1-a-b+2ab}\,,$$

para todos $a,\ b \in (0,\ 1)$. O elemento neutro é $f^{-1}(0) = \frac{e^0}{1+e^0} = \frac{1}{2}$ e para cada $a \in (0,\ 1)$ a inversa é

$$a^{-1} \;=\; \frac{e^{-\ln\left(\frac{a}{1-a}\right)}}{1+e^{-\ln\left(\frac{a}{1-a}\right)}} \;=\; 1-a\,.$$

É fácil constatar que esse grupo é Abeliano, como deveríamos esperar. ♦

**E. 2.74** *Exercício*. Encontre outras funções bijetoras entre $C = (0,\ 1)$ e $\mathbb{R}$. Descreva, como acima, as estruturas de grupo induzidas em $C$. ✠

**E. 2.75** *Exercício*. Considere $C = (-1,\ 1)$, o grupo aditivo dos reais $\mathbb{R}$ e a função bijetora $f : C \to \mathbb{R}$ dada por $f(x) = \tan(\pi x/2)$. Descreva, como acima, a estrutura de grupo induzida em $C$. ✠

**E. 2.76** *Exercício*. Considere $C = (-1,\ 1)$, o grupo aditivo dos reais $\mathbb{R}$ e a função bijetora $f : C \to \mathbb{R}$ dada por $f(x) = \operatorname{argtanh}(x) \equiv \tanh^{-1}(x)$. Descreva, como acima, a estrutura de grupo induzida em $C$. ✠

* *

*Nota*. Um teorema devido a Abel[50] e a outros autores afirma que todos os produtos que fazem de $\mathbb{R}$ um grupo Abeliano são da forma $x \overset{\circ}{+} y := f^{-1}\big(f(x)+f(y)\big)$, $x,\ y \in \mathbb{R}$, para alguma $f : \mathbb{R} \to \mathbb{R}$ bijetora. Para uma demonstração, vide [7], Cap. 6.2. O mesmo texto contém diversas generalizações dessa afirmação. ♣

## • Induzindo estruturas de espaços vetoriais

Seja agora $V$ um espaço vetorial sobre um corpo $\mathbb{K}$, sendo 0 seu vetor nulo.

Como acima, seja $C$ um conjunto não vazio e $f : C \to V$ uma função bijetora. Como $V$ é um grupo Abeliano em relação à operação de soma "+", $C$ também o será com relação à operação de "soma" definida por (vide (2.53))

$$a \overset{\circ}{+} b \;:=\; f^{-1}\big(f(a)+f(b)\big)\,.$$

para todo $a,\ b \in C$. O elemento neutro será o "vetor nulo", denotado por $\overset{\circ}{0}$ e dado por $\overset{\circ}{0} := f^{-1}(0)$ (vide (2.54)). A inversa de $a \in C$, denotada por $\overset{\circ}{-}\,a$ é dada por $\overset{\circ}{-}\,a := f^{-1}(-f(a))$ (vide (2.55)).

Contudo, $C$ pode ser transformado em um espaço vetorial sobre o corpo $\mathbb{K}$ definindo, para cada $\alpha \in \mathbb{K}$ e $a \in C$, o produto por escalares, denotado por $\alpha \circ a$, por

$$\alpha \circ a \;:=\; f^{-1}\big(\alpha f(a)\big)\,.$$

Para mostrar que $C$ é, de fato, um espaço vetorial sob estas estruturas precisamos ainda constatar que valem as seguintes propriedades (vide Seção 2.1.5, página 140):

1. Para todos $\alpha,\ \beta \in \mathbb{K}$ e todo $a \in C$ vale $\alpha \circ (\beta \circ a) = (\alpha\beta) \circ a$. De fato, tem-se

$$\alpha \circ (\beta \circ a) \;=\; f^{-1}\big(\alpha f(\beta \circ a)\big) \;=\; f^{-1}\Big(\alpha\big(\beta f(a)\big)\Big) \;=\; f^{-1}\big((\alpha\beta)f(a)\big) \;=\; (\alpha\beta) \circ a\,.$$

[50] Niels Henrik Abel (1802–1829).

2. Para todo $\alpha \in \mathbb{K}$ e todos $a,\ b \in C$ vale $\alpha \circ \Big(a \overset{\circ}{+} b\Big) = (\alpha \circ a) \overset{\circ}{+} (\alpha \circ b)$. De fato, tem-se

$$\alpha \circ \Big(a \overset{\circ}{+} b\Big) \ = \ \alpha \circ \Big(f^{-1}\big(f(a)+f(b)\big)\Big) \ = \ f^{-1}\Big(\alpha f\Big(f^{-1}\big(f(a)+f(b)\big)\Big)\Big) \ = \ f^{-1}\Big(\alpha\big(f(a)+f(b)\big)\Big)$$

$$= \ f^{-1}\big(\alpha f(a)+\alpha f(b)\big) \ = \ f^{-1}\Big(f(\alpha\circ a)+f(\alpha\circ b)\Big) \ = \ (\alpha\circ a) \overset{\circ}{+} (\alpha\circ b)\ .$$

3. Para todos $\alpha,\ \beta \in \mathbb{K}$ e todo $a \in C$ vale $(\alpha+\beta)\circ a = (\alpha\circ a) \overset{\circ}{+} (\beta\circ a)$. De fato, tem-se

$$(\alpha+\beta)\circ a \ = \ f^{-1}\big((\alpha+\beta)f(a)\big) \ = \ f^{-1}\big(\alpha f(a)+\beta f(a)\big) \ = \ f^{-1}\Big(f(\alpha\circ a)+f(\beta\circ a)\Big) \ = \ (\alpha\circ a) \overset{\circ}{+} (\beta\circ a)\ .$$

Novamente, comentamos que, por construção, o espaço vetorial formado por $C$, como descrito acima, é isomorfo ao espaço vetorial $V$, o isomorfismo sendo dado por $f$.

O seguinte exemplo ilustra um espaço vetorial não-trivial sobre os reais que pode ser obtido pela construção acima.

**Exemplo 2.22** Como no Exemplo 2.21, página 166, seja $C = (0,\ 1)$ e $V = \mathbb{R}$, o espaço vetorial dos reais sobre o corpo $\mathbb{R}$. Seja $f : (0,\ 1) \to \mathbb{R}$, definida por $f(x) := \frac{1}{2}\ln\Big(\frac{x}{1-x}\Big)$. A função $f$ é bijetora e sua inversa $f^{-1} : \mathbb{R} \to (0,\ 1)$ é dada por $f^{-1}(y) = \frac{e^{2y}}{1+e^{2y}}$. Então, $C = (0,\ 1)$ é um espaço vetorial com a operação de soma

$$a \overset{\circ}{+} b \ = \ \frac{ab}{1-a-b+2ab}\ ,$$

para todos $a,\ b \in (0,\ 1)$, o vetor nulo é $1/2$, a inversa de $a \in C$ é

$$\Big(\overset{\circ}{-}\ a\Big) \ = \ 1-a$$

e o produto por escalares $\alpha \in \mathbb{R}$ é dado por

$$\alpha \circ a \ = \ \frac{a^\alpha}{a^\alpha + (1-a)^\alpha}\ ,$$

para todo $a \in C$. ♦

**E. 2.77** *Exercício*. Prove todas as afirmações feitas acima. Prove explicitamente que para todos $\alpha,\ \beta \in \mathbb{R}$ e todos $a,\ b \in (0,\ 1)$ valem $\alpha\circ(\beta\circ a) = (\alpha\beta)\circ a$, $\alpha \circ \Big(a \overset{\circ}{+} b\Big) = (\alpha\circ a) \overset{\circ}{+} (\alpha\circ b)$ e $(\alpha+\beta)\circ a = (\alpha\circ a) \overset{\circ}{+} (\beta\circ a)$. ✣

O exercício a seguir mostra que $\mathbb{R}$ também pode adquirir outras estruturas de espaço vetorial real, além da usual.

**E. 2.78** *Exercício*. Seja $C = \mathbb{R}$ e $V = \mathbb{R}$ o espaço vetorial dos reais sobre o corpo $\mathbb{R}$. Seja $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) := x^3$. A função $f$ é bijetora e sua inversa é $f^{-1}(y) = y^{1/3}$. Descreva as operações de soma e multiplicação por escalares definidas em $C$ pela construção acima descrita. ✣

• **Mais exemplos. Símplices como espaços vetoriais reais**

Para $d$ inteiro, $d \geq 1$, seja $\Sigma_d \subset \mathbb{R}^{d+1}$ o *simplex padrão d-dimensional* definido por

$$\Sigma_d \ := \ \left\{ (a_1,\ \ldots,\ a_{d+1}) \in \mathbb{R}^{d+1} \ \text{ com } 0 \leq a_j \leq 1 \text{ para todo } j \text{ e } \sum_{j=1}^{d+1} a_j \ = \ 1 \right\}\ .$$

Seu interior, denotado por $\Sigma_d^0 \subset \mathbb{R}^{d+1}$, é o *simplex padrão aberto d-dimensional*:

$$\Sigma_d^0 \ := \ \left\{ (a_1,\ \ldots,\ a_{d+1}) \in \mathbb{R}^{d+1} \ \text{ com } 0 < a_j < 1 \text{ para todo } j \text{ e } \sum_{j=1}^{d+1} a_j \ = \ 1 \right\}\ .$$

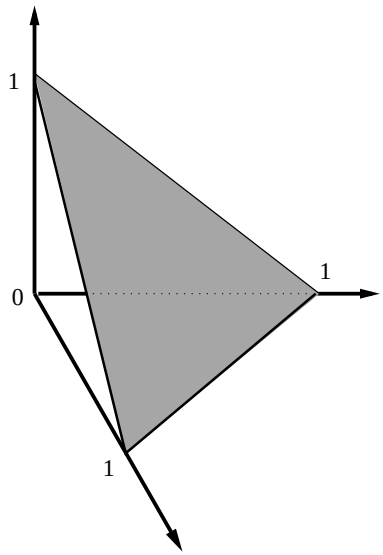


Figura 2.1: O simplex padrão $\Sigma_2$ no espaço tridimensional (área triangular acinzentada, incluindo sua borda). O simplex padrão aberto $\Sigma_2^0$ corresponde apenas à área acinzentada, excluindo sua borda.

Vide Figura 2.1, página 168.

Os dois exemplos a seguir[51] desempenham um papel na análise estatística de *dados composicionais*, uma área desenvolvida, entre outros, por Aitchison[52].

**E. 2.79** *Exercício-exemplo.* A aplicação $f : \Sigma_d^0 \to \mathbb{R}^d$ definida por

$$f(a_1,\, \ldots,\, a_{d+1}) \,:=\, \left(\frac{1}{2}\ln\left(\frac{a_1}{a_{d+1}}\right),\, \ldots,\, \frac{1}{2}\ln\left(\frac{a_d}{a_{d+1}}\right)\right) \tag{2.56}$$

é bijetiva (prove isso!) e sua inversa é (verifique!)

$$f^{-1}(y_1,\, \ldots,\, y_d) \,=\, \left(\frac{e^{2y_1}}{1+e^{2y_1}+\cdots+e^{2y_d}}\,,\, \ldots,\, \frac{e^{2y_d}}{1+e^{2y_1}+\cdots+e^{2y_d}}\,,\, \frac{1}{1+e^{2y_1}+\cdots+e^{2y_d}}\right)\,,$$

a qual é definida para todo $(y_1,\, \ldots,\, y_d) \in \mathbb{R}^d$.

Como $\mathbb{R}^d$ é um espaço vetorial sobre o corpo dos reais, podemos com a função $f$ induzir uma estrutura de espaço vetorial sobre o corpo dos reais em $\Sigma_d^0$, de acordo com as prescrições acima. Mostre que para a soma teremos

$$a \,\mathring{+}\, b \,=\, \left(\frac{a_1 b_1}{a_1 b_1+\cdots+a_{d+1}b_{d+1}}\,,\, \ldots,\, \frac{a_{d+1}b_{d+1}}{a_1 b_1+\cdots+a_{d+1}b_{d+1}}\right)\,, \tag{2.57}$$

com $a,\, b \in \Sigma_d^0$ na forma $a = (a_1,\, \ldots,\, a_{d+1})$ e $b = (b_1,\, \ldots,\, b_{d+1})$. Mostre que para o produto por escalares teremos

$$\alpha \circ a \,=\, \left(\frac{(a_1)^\alpha}{(a_1)^\alpha+\cdots+(a_{d+1})^\alpha}\,,\ldots,\, \frac{(a_{d+1})^\alpha}{(a_1)^\alpha+\cdots+(a_{d+1})^\alpha}\right)\,, \tag{2.58}$$

para todo $\alpha \in \mathbb{R}$ e $a \in \Sigma_d^0$. O vetor nulo $\mathring{0}$ é o elemento de $\Sigma_d^0$ dado por

$$\mathring{0} = \left(\frac{1}{d+1},\, \ldots,\, \frac{1}{d+1}\right)\,. \tag{2.59}$$

✠

[51] Agradecemos a Ricardo Zorzetto Nicoliello Vêncio por chamar-nos a atenção para estes exemplos.
[52] John Aitchison (1926–). Vide J. Aitchison "The Statistical Analysis of Compositional Data". Chapman and Hall, London, (1986).

**E. 2.80** *Exercício-exemplo.* Seja $a = (a_1,\, \ldots,\, a_{d+1}) \in \Sigma_d^0$ e denotemos por $g(a)$ a média geométrica de $a_1,\, \ldots,\, a_{d+1}$:

$$g(a) \,:=\, \big(a_1 \cdots a_{d+1}\big)^{\frac{1}{d+1}} \,.$$

Está claro que $g(a) > 0$ para todo $a \in \Sigma_d^0$. A aplicação $f : \Sigma_d^0 \to \mathbb{R}^d$ definida por

$$f(a_1,\, \ldots,\, a_{d+1}) \,:=\, \left(\ln\left(\frac{a_1}{g(a)}\right),\, \ldots,\, \ln\left(\frac{a_d}{g(a)}\right)\right) \,, \tag{2.60}$$

é bijetiva (prove isso!) e sua inversa é (verifique!)

$$f^{-1}(y_1,\, \ldots,\, y_d)$$

$$= \left(\frac{e^{y_1}}{e^{y_1} + \cdots + e^{y_d} + e^{-(y_1+\cdots+y_d)}} \,,\, \ldots,\, \frac{e^{y_d}}{e^{y_1} + \cdots + e^{y_d} + e^{-(y_1+\cdots+y_d)}} \,,\, \frac{e^{-(y_1+\cdots+y_d)}}{e^{y_1} + \cdots + e^{y_d} + e^{-(y_1+\cdots+y_d)}}\right) \,,$$

a qual é definida para todo $(y_1,\, \ldots,\, y_d) \in \mathbb{R}^d$.

Como $\mathbb{R}^d$ é um espaço vetorial sobre o corpo dos reais, podemos com a função $f$ induzir uma estrutura de espaço vetorial sobre o corpo dos reais em $\Sigma_d^0$, de acordo com as prescrições acima. Mostre que para $a,\, b \in \Sigma_d^0$ a soma $a \mathbin{\mathring{+}} b$ é a mesma que a dada em (2.57), que para $\alpha \in \mathbb{R}$ o produto por escalares $\alpha \circ a$ é o mesmo que o dado em (2.58) e que o vetor nulo é o mesmo dado em (2.59). ✠

Em alguns textos, a função $f$ dada em (2.56) é denotada por $alr$ e a função $f$ dada em (2.60) é denotada por $clr$. É elementar constatar que (2.56) e (2.60) coincidem no caso $d = 1$.

# 2.2 Grupos. Estruturas e Construções Básicas

Nesta seção apresentaremos algumas estruturas e construções básicas da Teoria dos Grupos.

## 2.2.1 Cosets

• **Cosets à esquerda, ou "left cosets"**

Seja $G$ um grupo e $H$ um subgrupo de $G$. Podemos definir em $G$ uma relação de equivalência, que denotaremos por $\sim_l^H$ (o índice "$l$" denotando "left"), dizendo que dois elementos $x$ e $y$ de $G$ são equivalentes se $x^{-1}y \in H$. Representaremos por $x \sim_l^H y$ o fato de $x$ e $y$ serem equivalentes no sentido acima.

**E. 2.81** *Exercício importante.* Verifique que a definição acima corresponde de fato a uma relação de equivalência. ✠

Denotemos por $(G/H)_l$ a coleção das classes de equivalência de $G$ pela relação $\sim_l^H$. O conjunto $(G/H)_l$ é denominado *coset à esquerda* de $G$ por $H$, ou *left coset* de $G$ por $H$.

Seja $[\cdot]_l$ a aplicação $G \to (G/H)_l$ que associa a cada elemento de $G$ a classe de equivalência a qual o elemento pertence. A aplicação $[\cdot]_l$ é denominada *aplicação quociente à esquerda* associada a $H$. Note-se que $[\cdot]_l$ é sobrejetora mas, em geral, não é injetora pois, se $g' \sim_l^H g$, então $[g']_l = [g]_l$. Com isso, os elementos de $(G/H)_l$ poderão ser denotados por $[g]_l$ com $g \in G$, o que frequentemente faremos.

Podemos identificar $[g]_l$ com o conjunto $gH = \{gh,\, h \in H\} \subset G$. De fato, $g' \in gH$ se e somente se existe $h \in H$ tal que $g' = gh$ e, portanto, se e somente se $g^{-1}g' \in H$, ou seja, se e somente se $g \sim_l^H g'$.

Isso nos ensina que se $e$ é o elemento neutro de $G$, então $[e]_l = H$. Assim, o subgrupo $H$ é, ele mesmo, uma classe de equivalência pela relação de equivalência $\sim_l^H$ e, portanto, é um elemento de $(G/H)_l$.

• **Cosets à direita, ou "right cosets"**

Seja $G$ um grupo e $H$ um subgrupo de $G$. Podemos definir em $G$ uma relação de equivalência, que denotaremos por $\sim_r^H$ (o índice "$r$" denotando "right"), dizendo que dois elementos $x$ e $y$ de $G$ são equivalentes se $xy^{-1} \in H$. Representaremos por $x \sim_r^H y$ o fato de $x$ e $y$ serem equivalentes no sentido acima.

**E. 2.82** *Exercício importante.* Verifique que a definição acima corresponde de fato a uma relação de equivalência. ✠

Denotemos por $(G/H)_r$ a coleção das classes de equivalência de $G$ pela relação $\sim_r^H$. O conjunto $(G/H)_r$ é denominado *coset à direita* de $G$ por $H$, ou *right coset* de $G$ por $H$.

Seja $[\cdot]_r$ a aplicação $G \to (G/H)_r$ que associa a cada elemento de $G$ a classe de equivalência a qual o elemento pertence. A aplicação $[\cdot]_r$ é denominada *aplicação quociente à direita* associada a $H$. Note-se que $[\cdot]_r$ é sobrejetora mas, em geral, não é injetora pois, se $g' \sim_r^H g$, então $[g']_r = [g]_r$. Com isso, os elementos de $(G/H)_r$ poderão ser denotados por $[g]_r$ com $g \in G$, o que frequentemente faremos.

Podemos identificar $[g]_r$ com o conjunto $Hg = \{hg,\ h \in H\} \subset G$. De fato, $g' \in Hg$ se e somente se existe $h \in H$ tal que $g' = hg$ e, portanto, se e somente se $g'g^{-1} \in H$, ou seja, se e somente se $g' \sim_r^H g$.

Isso nos ensina que se $e$ é o elemento neutro de $G$, então $[e]_r = H$. Assim, o subgrupo $H$ é, ele mesmo, uma classe de equivalência pela relação de equivalência $\sim_r^H$ e, portanto, é um elemento de $(G/H)_r$.

Doravante, denotaremos $\sim_l^H$ simplesmente por $\sim_l$ e $\sim_r^H$ por $\sim_r$, ficando o subgrupo $H$ subentendido.

• **Ação à esquerda de $G$ sobre $(G/H)_l$**

É sempre possível definir uma ação à esquerda de $G$ sobre o coset à esquerda $(G/H)_l$, a qual age transitivamente em $(G/H)_l$ (vide definição à página 160). Isso faz de $(G/H)_l$ um *espaço homogêneo* de $G$ (vide definição à página 161).

Seja $G$ um grupo, $H$ um subgrupo de $G$ e seja o coset à esquerda $(G/H)_l$, definido acima. Defina

$$\alpha:\ G \times (G/H)_l \ \to\ (G/H)_l \quad \text{tal que} \quad G \times (G/H)_l \ \ni\ \big(g,\ [f]_l\big) \ \longmapsto\ \alpha_g\big([f]_l\big) \ :=\ [gf]_l \ \in\ (G/H)_l\ .$$

Então, $\alpha$ define uma *ação à esquerda* de $G$ sobre $(G/H)_l$. De fato, tem-se que

1. Para cada $g \in G$, $\alpha_g : (G/H)_l \to (G/H)_l$ é bijetora, pois se existem $f_1,\ f_2 \in G$ tais que $[gf_1]_l = [gf_2]_l$, então $gf_1 \sim_l gf_2$, ou seja, $(gf_1)^{-1}(gf_2) \in H$, ou seja, $(f_1)^{-1}f_2 \in H$. Isso estabelece que $f_1 \sim_l f_2$, ou seja, que $[f_1]_l = [f_2]_l$, provando que $\alpha_g : (G/H)_l \to (G/H)_l$ é injetora. Note-se que $\alpha_g : (G/H)_l \to (G/H)_l$ é sobrejetora, pois $\alpha_g\big([g^{-1}f]_l\big) = [f]_l$ e variando $f$ em $G$, $[f]_l$ varre todo $(G/H)_l$.

2. Para a identidade $e \in G$, $\alpha_e\big([f]_l\big) = [ef]_l = [f]_l$ para todo $f \in G$, provando que $\alpha_e : (G/H)_l \to (G/H)_l$ é a aplicação identidade.

3. Para todos $g,\ h \in G$ vale $\alpha_g\Big(\alpha_h\big([f]_l\big)\Big) = \alpha_g\big([hf]_l\big) = [ghf]_l = \alpha_{gh}\big([f]_l\big)$ para qualquer $f \in G$.

Isso provou que $\alpha : G \times (G/H)_l \to (G/H)_l$ é uma ação à esquerda de $G$ em $(G/H)_l$.

Não é difícil ver que a ação $\alpha$ age transitivamente em $(G/H)_l$. De fato, se $e$ é a unidade de $G$, então $\alpha_g\big([e]_l\big) = [g]_l$ e variando $g$ por todo $G$ a imagem $[g]_l$ varre todo $(G/H)_l$.

• **Ação à direita de $G$ sobre $(G/H)_r$**

É sempre possível definir uma ação à direita de $G$ sobre o coset à direita $(G/H)_r$, a qual age transitivamente em $(G/H)_r$ (vide definição à página 160). Isso faz de $(G/H)_r$ um *espaço homogêneo* de $G$ (vide definição à página 161).

Seja $G$ um grupo, $H$ um subgrupo de $G$ e seja o coset à direita $(G/H)_r$, definido acima. Defina

$$\beta:\ G \times (G/H)_r \ \to\ (G/H)_r \quad \text{tal que} \quad G \times (G/H)_r \ \ni\ \big(g,\ [f]_r\big) \ \longmapsto\ \beta_g\big([f]_r\big) \ :=\ [fg]_r \ \in\ (G/H)_r\ .$$

Então, $\beta$ define uma *ação à direita* de $G$ sobre $(G/H)_r$. De fato, tem-se que

1. Para cada $g \in G$, $\beta_g : (G/H)_r \to (G/H)_r$ é bijetora, pois se existem $f_1,\ f_2 \in G$ tais que $[f_1g]_r = [f_2g]_r$, então $f_1g \sim_r f_2g$, ou seja, $(f_1g)(f_2g)^{-1} \in H$, ou seja, $f_1(f_2)^{-1} \in H$. Isso estabelece que $f_1 \sim_r f_2$, ou seja, que $[f_1]_r = [f_2]_r$, provando que $\beta_g : (G/H)_r \to (G/H)_r$ é injetora. Note-se que $\beta_g : (G/H)_r \to (G/H)_r$ é sobrejetora, pois $\beta_g\big([fg^{-1}]_r\big) = [f]_r$ e variando $f$ em $G$, $[f]_r$ varre todo $(G/H)_r$.

2. Para a identidade $e \in G$, $\beta_e\big([f]_r\big) = [fe]_r = [f]_r$ para todo $f \in G$, provando que $\beta_e : (G/H)_r \to (G/H)_r$ é a aplicação identidade.

3. Para todos $g,\ h \in G$ vale $\beta_g\Big(\beta_h\big([f]_r\big)\Big) = \beta_g\big([fh]_r\big) = [fhg]_r = \beta_{hg}\big([f]_r\big)$ para qualquer $f \in G$.

Isso provou que $\beta : G \times (G/H)_r \to (G/H)_r$ é uma ação à direita de $G$ em $(G/H)_r$.

Não é difícil ver que a ação $\beta$ age transitivamente em $(G/H)_r$. De fato, se $e$ é a unidade de $G$, então $\alpha_g\big([e]_r\big) = [g]_r$ e variando $g$ por todo $G$ a imagem $[g]_r$ varre todo $(G/H)_r$.

*

Os cosets $(G/H)_l$ e $(G/H)_r$ podem ser identificados e transformados em grupos se uma certa hipótese for feita sobre o subgrupo $H$ e sua relação com $G$. Esse é nosso assunto na Seção 2.2.2.

### 2.2.1.1 O Teorema de Lagrange

A noção de coset de um grupo por um subgrupo permite obter um elegante, interessante e útil resultado sobre grupos finitos, conhecido como *Teorema de Lagrange*[53], o qual estabelece uma relação entre o número de elementos de um grupo finito e de seus subgrupos. Esse teorema tem consequências tanto para a Teoria de Grupos quanto para a Teoria de Números.

**• Notação e definições preliminares**

Se $G$ é um grupo finito, denotamos por $|G|$ o número de elementos de $G$, também denominada a *ordem* de $G$. Se $H$ é um subgrupo de $G$ denotamos por $\big|(G/H)_l\big|$ (por $\big|(G/H)_r\big|$) o número de elementos do coset $(G/H)_l$ (respectivamente, do coset $(G/H)_r$).

Se $A$ é um subconjunto de um grupo $G$ (não necessariamente finito), e $g \in G$, denotamos por $gA$ o conjunto $\{ga,\ a \in A\}$ e por $Ag$ o conjunto $\{ag,\ a \in A\}$. O conjunto $gA$ (respectivamente, $Ag$) é dito ser o *transladado à esquerda* (à direita) de $A$ por $g$.

Seja $G$ um grupo e sejam $A$ e $B$ dois subconjuntos não vazios (não necessariamente dois subgrupos) de $G$. Denotamos por $|B : A|_l$ o menor conjunto de transladados à esquerda de $A$ que cobrem $B$, ou seja, o menor $n$ tal que $B \subset (g_1A) \cup \cdots \cup (g_nA)$ para algum conjunto $\{g_1,\ \ldots,\ g_n\}$ de elementos distintos de $G$. Caso $B$ não possa ser coberto por uma coleção finita de transladados à esquerda de $A$ dizemos que $|B : A|_l$ vale infinito.

De maneira análoga definimos $|B : A|_r$ como o menor conjunto de transladados à direita de $A$ que cobrem $B$.

Notemos que se $B$ for finito ou compacto e $A$ aberto, então $|B : A|_l$ e $|B : A|_r$ são finitos.

*Comentário*. As quantidades $|B : A|_l$ e $|B : A|_r$, definidas acima, são relevantes na definição da chamada *medida de Haar* de grupos compactos (ou finitos). Vide, *e.g.*, [393]. ♣

**• Resultados preparatórios**

Para demonstrar o Teorema de Lagrange precisamos dos resultados que seguem.

**Lema 2.4** *Seja $H$ um subgrupo de um grupo $G$. Então, existe uma bijeção entre os cosets $(G/H)_l$ e $(G/H)_r$, dada por $\Phi : (G/H)_l \to (G/H)_r$, com $\Phi\big([g]_l\big) := \big[g^{-1}\big]_r$.* □

Prova. Se $g_1$ e $g_2$ são elementos de $G$, então $g_1 \sim_l g_2$ se e somente se $g_2^{-1}g_1 = h \in H$, o que é verdade se e somente se $g_1^{-1}g_2 = h^{-1} \in H$ e, portanto, se e somente se $\big(g_1^{-1}\big)\big(g_2^{-1}\big)^{-1} = h^{-1} \in H$, que é verdade se e somente se $g_1^{-1} \sim_r g_2^{-1}$.

Isso prova que $\Phi : (G/H)_l \to (G/H)_r$, definida por $\Phi\big([g]_l\big) := \big[g^{-1}\big]_r$, está realmente definida nas classes $(G/H)_l$ e é injetora. Mas $\Phi$ é claramente sobrejetora, pois toda classe de $(G/H)_r$ é da forma $\big[g^{-1}\big]_r$ para algum $g \in G$. Portanto, $\Phi$ é bijetora. ■

**Lema 2.5** *Seja $H$ um subgrupo de um grupo $G$ e seja $(G/H)_l$ seu coset à esquerda. Então, existe uma bijeção entre $H$ e cada classe de equivalência que compõe $(G/H)_l$. Portanto, cada classe de equivalência que compõe $(G/H)_l$ possui a mesma cardinalidade de $H$. As mesmas afirmações são válidas para o coset à direita $(G/H)_r$.* □

[53] Joseph-Louis Lagrange (1736–1813).

Prova. Para algum $a \in G$, seja $[a]_l \subset G$ sua classe de equivalência, que é um elemento de $(G/H)_l$. Considere-se a função $\mathsf{L} : H \to [a]_l$ dada por $\mathsf{L}(h) = ah$. Em primeiro lugar, note-se que a imagem dessa função está realmente em $[a]_l$, pois $a^{-1}(ah) = h \in H$, o que mostra que $a \sim_l^H ah$ e, portanto, que $ah \in [a]_l$. Em segundo lugar, observe-se que $\mathsf{L}$ é injetora, pois se $h_1,\ h_2 \in H$ são tais que $\mathsf{L}(h_1) = \mathsf{L}(h_2)$, então $ah_1 = ah_2$, o que claramente implica que $h_1 = h_2$. Finalmente, afirmamos que $\mathsf{L}$ é sobrejetora. De fato, se $b \in [a]_l$, então $a \sim_l^H b$, ou seja, existe $h \in H$ tal que $a^{-1}b = h$. Portanto, $b = ah = \mathsf{L}(h)$, mostrando que a imagem de $\mathsf{L}$ é todo $[a]_l$. Assim, $\mathsf{L} : H \to [a]_l$ é bijetora, o que significa que $H$ e $[a]_l$ têm a mesma cardinalidade. Como $a \in G$ foi escolhido arbitrário, segue que cada elemento de $(G/H)_l$ tem a cardinalidade de $H$.

A prova para o coset à direita $(G/H)_r$ é similar, considerando-se para tal a função $\mathsf{R} : H \to [a]_r$ definida por $\mathsf{R}(h) = ha$. ■

O resultado que segue é válido para grupos finitos, mas pode ser expresso como igualdades entre cardinalidades no caso de grupos não finitos.

**Lema 2.6** *Seja $G$ um grupo finito e $H$ um subgrupo de $G$. Então, $|G : H|_l = \big|(G/H)_l\big|$ e $|G : H|_r = \big|(G/H)_r\big|$. Consequentemente,*

$$|G : H|_l \ = \ \big|(G/H)_l\big| \ = \ \big|(G/H)_r\big| = |G : H|_r \ ,$$

*pelo Lemma 2.4, página 171.* □

Prova. Suponhamos que exista um conjunto $\{g_1,\ \ldots,\ g_n\}$ de $n$ elementos distintos de $G$ tais que $(g_1H) \cup \cdots \cup (g_nH) = G$. Cada $g_kH$ coincide, como ja vimos, com a classe de equivalência $[g_k]_l$ e, portanto, estamos assumindo que $[g_1]_l \cup \cdots \cup [g_n]_l = G$. Evidentemente, podemos assumir que as classes são disjuntas e, assim, fica claro que o menor valor possível de $n$ é $\big|(G/H)_l\big|$, provando que $|G : H|_l = \big|(G/H)_l\big|$. O argumento para as classes à direita é similar. ■

**Definição.** Para grupos finitos, a quantidade

$$|G : H| \ \equiv \ |G : H|_l \ = \ |G : H|_r \ = \ \big|(G/H)_l\big| \ = \ \big|(G/H)_r\big| \ , \tag{2.61}$$

é denominada o *índice* de $H$ em $G$. ♠

• **O Teorema de Lagrange**

Podemos agora enunciar e demonstrar o

**Teorema 2.4 (Teorema de Lagrange)** *Seja $G$ um grupo finito e seja $H$ um subgrupo de $G$. Então, $|G|$ é divisível por $|H|$, ou seja, $|G|/|H| \in \mathbb{N}$. A razão $|G|/|H|$ coincide com o índice de $H$ em $G$, definida em (2.61), que é é o número de elementos dos cosets $(G/H)_l$ ou $(G/H)_r$. Assim, temos*

$$|G| \ = \ |G : H|\,|H| \ ,$$

*onde $|G : H|$, o índice de $H$ em $G$, é definido em (2.61).* □

Prova do Teorema 2.4. O coset $(G/H)_l$ é composto por uma coleção finita de classes de equivalência $[g_1]_l, \ldots,\ [g_p]_l$, disjuntas duas a duas, onde $p \equiv \big|(G/H)_l\big|$. Como sabemos, a união dessas classes é todo $G$ e, pelo Lema 2.5, página 171, todas têm $|H|$ elementos. Logo, $|G| = p|H|$, ou seja, $|G| = \big|(G/H)_l\big|\,|H|$. O restante segue de (2.61). ■

Esse teorema é denominado em honra a Lagrange por este tê-lo demonstrado em uma situação particular, em 1771, estudando a ação do grupo de permutações sobre polinômios de várias variáveis. Generalizações posteriores foram obtidas por Gauss[54], Cauchy[55] e Camille Jordan[56]. Trata-se de mais uma evidência da Lei de Stiegler (pág. 35).

Pelo Teorema de Lagrange concluímos, por exemplo, que um grupo com 10 elementos não pode possuir um subgrupo com 3, 4, 6, 7, 8 ou 9 elementos. Segue também que um grupo cuja ordem é um número primo não pode possuir subgrupos não triviais. Assim, por exemplo, os grupos $\mathbb{Z}_p$, com $p$ primo, não podem possuir subgrupos não triviais.

[54] Johann Carl Friedrich Gauss (1777–1855).
[55] Augustin Louis Cauchy (1789-1857).
[56] Marie Ennemond Camille Jordan (1838–1922).

**E. 2.83** *Exercício (fácil).* Sejam $F$, um grupo finito, $G$, um subgrupo de $F$ e $H$ um subgrupo de $G$ (e, portanto, também de $F$). Mostre que

$$|F : H| \;=\; |F : G|\,|G : H| \,. \tag{2.62}$$

✠

O Teorema de Lagrange aproxima o estudo dos subgrupos de um grupo finito $G$ do problema da decomposição da ordem $|G|$ desse grupo por seus fatores primos. Por exemplo, Teorema de Lagrange levanta a questão de saber quando e se um grupo com $n$ elementos pode possuir um subgrupo cuja ordem é a de um dado divisor de $n$. Exemplos mostram que isso nem sempre é possível, mas há diversos resultados garantindo condições suficientes para tal, alguns dos mais notáveis sendo devidos a Sylow[57]. Vide, *e.g.*, [482] ou [488].

## 2.2.2 Subgrupos Normais e o Grupo Quociente

As noções de subgrupos normais e de grupos quocientes, que apresentamos nesta seção, são de importância central em muitos desenvolvimentos da Teoria de Grupos e permitem expressar certas propriedades estruturais de grupos.

**• Subgrupos normais**

Seja $G$ um grupo. Um subgrupo $N$ de $G$ é dito ser um *subgrupo normal* se $gng^{-1} \in N$ para todo $g \in G$ e todo $n \in N$. Se $N$ é um subgrupo normal de $G$ denotamos esse fato escrevendo $N \lhd G$ ou $G \rhd N$. Observe que todo subgrupo de um grupo Abeliano $G$ é normal.

**E. 2.84** *Exercício importante.* Sejam $G$ e $H$ dois grupos e $\varphi : G \to H$ um homomorfismo. Seja $e_H$ a unidade de $H$.

**I.** Mostre que

$$\mathrm{Ran}\,(\varphi) \;:=\; \Big\{\varphi(g)\Big|\;\; g \in G\Big\} \tag{2.63}$$

é um subgrupo de $H$.

**II.** Mostre que

$$\mathrm{Ker}\,(\varphi) \;:=\; \Big\{g \in G\Big|\;\; \varphi(g) \;=\; e_H\Big\} \tag{2.64}$$

é um subgrupo normal de $G$.

A afirmação II, acima, possui uma recíproca. Vide Exercício E. 2.86, página 175. ✠

*Comentários.* Note-se que $\mathrm{Ran}\,(\varphi)$ é nada mais que a imagem (enquanto função) do homomorfismo $\varphi : G \to H$. O símbolo Ran provém da palavra inglesa "range" (na acepção de "alcance", em Português) e é frequentemente empregado como sinônimo da *imagem* de uma função ou aplicação. O símbolo Ker provém do Alemão "Kern" ("núcleo" ou "caroço", em Português).

O Teorema 2.6, página 177, contém uma importante afirmação sobre a imagem $\mathrm{Ran}\,(\varphi)$ e o núcleo $\mathrm{Ker}\,(\varphi)$ de um homomorfismo entre dois grupos. ♣

**E. 2.85** *Exercício-exemplo.* Seja $\mathrm{GL}(n,\,\mathbb{C})$ o grupo das matrizes complexas $n \times n$ inversíveis e seja $\mathrm{SL}(n,\,\mathbb{C})$ o grupo das matrizes complexas $n \times n$ inversíveis e de determinante 1. Mostre que $\mathrm{SL}(n,\,\mathbb{C}) \lhd \mathrm{GL}(n,\,\mathbb{C})$. Sugestão: é elementar constatar diretamente que $ABA^{-1} \in \mathrm{SL}(n,\,\mathbb{C})$ sempre que $A \in \mathrm{GL}(n,\,\mathbb{C})$ e $B \in \mathrm{SL}(n,\,\mathbb{C})$ mas, equivalentemente, o resultado pode ser também justificado evocando-se o Exercício E. 2.84, recordando para tal que o determinante é um homomorfismo de $\mathrm{GL}(n,\,\mathbb{C})$ no grupo $(\mathbb{C} \setminus \{0\},\,\cdot)$ dos complexos não nulos com o produto definido pela multiplicação. ✠

**• Grupos simples**

Todo grupo $G$ possui ao menos dois subgrupos normais: o próprio grupo $G$ e o subgrupo $\{e_G\}$ formado apenas pelo elemento neutro de $G$. Esses subgrupos são denominados *subgrupos triviais*. Um grupo cujos subgrupos normais sejam apenas os triviais é dito ser um *grupo simples*.

**• Subgrupos normais gerados por um conjunto**

O seguinte resultado sobre grupos normais é muito relevante.

[57] Peter Ludwig Mejdell Sylow (1832–1918).

**Proposição 2.5** *Seja $G$ um grupo e seja $\{N_\lambda,\ \lambda \in \Lambda\}$ uma coleção não vazia arbitrária de subgrupos normais de $G$. Então, $\bigcap_{\lambda\in\Lambda} N_\lambda$ é um subgrupo normal de $G$.* □

Prova. Sabemos pela Proposição 2.2, página 136, que $\bigcap_{\lambda\in\Lambda} N_\lambda$ é um subgrupo de $G$. Se $n \in \bigcap_{\lambda\in\Lambda} N_\lambda$, então $n$ pertence a cada subgrupo normal $N_\lambda$ com $\lambda \in \Lambda$. Logo, para todo $g \in G$ vale $gng^{-1} \in N_\lambda$ para cada cada subgrupo normal $N_\lambda$ e, portanto, $gng^{-1} \in \bigcap_{\lambda\in\Lambda} N_\lambda$. Isso mostra que $\bigcap_{\lambda\in\Lambda} N_\lambda$ é um subgrupo normal de $G$, como desejávamos estabelecer. ■

A Proposição 2.5 suscita a definição de grupo normal gerado por um conjunto:

**Definição. Subgrupo normal gerado por um conjunto.** Seja $S$ um subconjunto não vazio (não necessariamente um subgrupo) de um grupo $G$. O conjunto $S$ pertence ao menos a um subgrupo normal de $G$, a saber, o próprio $G$. Denotamos por $N[S]$ a intersecção de todos os subgrupos normais de $G$ que contém $S$. Pela Proposição 2.5, página 174, $N[S]$ é um subgrupo normal de $G$, e é dito ser o subgrupo normal de $G$ gerado por $S$. Podemos assim dizer que o subgrupo $N[S]$ é o "menor" subgrupo normal de $G$ que contém $S$. ♠

Podemos identificar explicitamente os elementos de $N[S]$.

**Proposição 2.6** *Seja $S$ um subconjunto não vazio (não necessariamente um subgrupo) de um grupo $G$. Então,*

$$N[S] \ = \ \left\{gsg^{-1},\ g \in G,\ s \in S\right\}, \tag{2.65}$$

*com $N[S]$ sendo o subgrupo normal de $G$ gerado por $S$.* □

Prova. Denotemos por $S(G)$ o conjunto definido no lado direito de (2.65). É evidente que $S \subset S(G)$ (tome-se $g = e_G$, o elemento neutro de $G$). É igualmente elementar ver que $S(G)$ é um subgrupo normal de $G$: para todo $h \in G$ e todo $gsg^{-1} \in S(G)$ (com $g \in G$ e $s \in S$), tem-se $h\big(gsg^{-1}\big)h^{-1} = \big(hg\big)s\big(hg\big)^{-1} \in S(G)$. Assim, $S(G)$ é um subgrupo normal de $G$ que contém $S$ e, portanto, $N[S] \subset S(G)$, pois $N[S]$ é a intersecção de todos os subgrupos normais de $G$ que contém $S$.

Por outro lado, $S(G) \subset N[S]$, pois todo elemento de $S(G)$ é da forma $gsg^{-1}$ com $g \in G$ e $s \in S \subset N[S]$. Como $N[S]$ é normal, segue que $gsg^{-1} \in N[S]$. Portanto, $N[S] = S(G)$, como desejávamos provar. ■

O conjunto $S(G) \equiv N[S]$ é também denominado *fecho normal de $S$* ou *subgrupo normal gerado por $S$*.

• **Cosets por subgrupos normais**

Chegamos agora à razão de ser da noção de subgrupo normal. A seguinte proposição é fundamental.

**Proposição 2.7** *Seja $G$ um grupo e seja $N$ um subgrupo de $G$. Então, uma condição necessária e suficiente para que possamos identificar $(G/N)_l$ com $(G/N)_r$, ou seja, para que tenhamos $[g]_l = [g]_r$ para todo $g \in G$, é que $N \lhd G$, ou seja, que $N$ seja um subgrupo normal de $G$.* □

Prova. Por definição, $g' \in [g]_l$ se e somente existe $n \in N$ tal que $g^{-1}g' = n$, o que é verdade se e somente se $g'g^{-1} = gng^{-1}$. Mas $g' \in [g]_r$ se e somente se $g'g^{-1} \in N$. Assim $[g]_l = [g]_r$ para todo $g \in G$ se e somente se $gng^{-1} \in N$ para todo $g \in G$ e $n \in N$, o que é verdade se somente se $N$ é um subgrupo normal de $G$. ■

Com isso, caso $N \lhd G$, definimos $[g] \equiv [g]_N := [g]_l = [g]_r$ para todo $g \in G$ e definimos o *coset* de $G$ por $N$ por $G/N := (G/N)_l = (G/N)_r$, ou seja, $G/N = \big\{[g],\ g \in G\big\}$.

**Advertência**. O leitor deve ser advertido aqui que, infelizmente, é comum na literatura denotar o coset à esquerda $(G/H)_l$ por $G/H$, mesmo quando $H$ não é normal (vide, por exemplo, [488] ou [230], entre outros). Evitaremos fazê-lo, pois isso pode levar a uma confusão de conceitos.

• **Ações à direita e à esquerda sobre o coset por um subgrupo normal**

Se $H$ é um subgrupo qualquer de $G$, definimos páginas acima uma ação transitiva à esquerda $\alpha : G \times (G/H)_l \to (G/H)_l$ e uma ação transitiva à direita $\beta : G \times (G/H)_r \to (G/H)_r$. Fica claro pela Proposição 2.7 que se $N \lhd G$, podemos definir tanto

$$\alpha : \; G \times (G/N) \; \to \; G/N \quad \text{tal que} \quad G \times (G/N) \; \ni \; \big(g, \; [f]\big) \; \longmapsto \; \alpha_g\big([f]\big) \; := \; [gf] \; \in \; G/N$$

como uma ação à esquerda de $G$ sobre $G/N$ quanto

$$\beta : \; G \times (G/N) \; \to \; G/N \quad \text{tal que} \quad G \times (G/N) \; \ni \; \big(g, \; [f]\big) \; \longmapsto \; \beta_g\big([f]\big) \; := \; [fg] \; \in \; G/N$$

como uma ação à direita de $G$ sobre $G/N$. Ambas as ações agem transitivamente.

• **O grupo quociente de $G$ por $N$**

Subgrupos normais são importantes, pois com eles podemos fazer da coleção de classes de equivalência $G/N$ um grupo, denominado *grupo quociente de $G$ por $N$*. A construção é a seguinte.

Seja $N \lhd G$. Podemos fazer de $G/N$ um grupo definindo o produto como $[g]_N[h]_N = [gh]_N$. É muito fácil ver que, se esta expressão está bem definida, ela de fato representa um produto associativo na coleção de classes de equivalência $G/N$. O elemento neutro seria a classe $[e]_N$, onde $e$ é a identidade de $G$. Por fim, $[g]_N^{-1} = [g^{-1}]_N$. O ponto não-trivial é mostrar que a definição de produto como $[g]_N[h]_N = [gh]_N$ faz sentido, ou seja, é independente dos elementos tomados nas classes de $g$ e $h$. Para isso precisaremos que $N$ seja normal.

O que temos de fazer é mostrar que se $g' \sim_N g$ e $h' \sim_N h$, então $g'h' \sim_N gh$, ou seja, precisamos mostrar que se $g'g^{-1} \in N$ e $h'h^{-1} \in N$, então $g'h'(gh)^{-1} \in N$. Mas, de fato, tem-se que

$$g'h'(gh)^{-1} \; = \; g'h'h^{-1}g^{-1} \; = \; \big(g'g^{-1}\big)\Big(g\big(h'h^{-1}\big)g^{-1}\Big) \, .$$

Agora, por hipótese, $h'h^{-1} \in N$. Daí, como $N$ é normal (é aqui que essa hipótese entra pela primeira vez), $g(h'h^{-1})g^{-1} \in N$. Como, também pela hipótese, $g'g^{-1} \in N$ e $N$ é um subgrupo, concluímos que $g'h'(gh)^{-1} \in N$, ou seja, $g'h' \sim_N gh$. Assim $[g]_N[h]_N = [gh]_N$ está bem definido e faz das classes $G/N$ um grupo. Esse grupo é denominado de *grupo quociente de $G$ por $N$*.

A noção de grupo quociente é muito importante na teoria de grupos e iremos explorar algumas das aplicações nestas Notas. Adiante usaremo-la para construir a noção de produto tensorial e soma direta de vários objetos, tais como grupos, álgebras etc. A noção de grupo quociente é importante por permitir estudar a relação de certos grupos entre si. Mais adiante (vide Seção 21.8, página 1234) mostraremos, por exemplo, que o grupo SO(3) é isomorfo ao grupo $\mathrm{SU}(2)/\{\mathbb{1}, \, -\mathbb{1}\}$, um resultado de direto interesse físico na Mecânica Quântica. A noção de grupo quociente é também muito importante em problemas combinatórios envolvendo grupos, mas não falaremos disso aqui. Para uma discussão mais ampla, vide [482], [488] ou [394].

**E. 2.86** *Exercício.* Seja $G$ um grupo e seja $N \lhd G$. Mostre que $\varphi : G \to G/N$ dada por $\varphi(g) = [g]_N$ é um homomorfismo e que $\mathrm{Ker}\,(\varphi) = N$. Isso estabelece uma recíproca à afirmação II do Exercício E. 2.84, página 173: todo subgrupo normal de um grupo $G$ é o núcleo de algum homomorfismo de $G$. ✠

• **Ações de um grupo e subgrupos normais**

Vimos no Exercício E. 2.84, página 173, que subgrupos normais surgem quando consideramos homomorfismos entre grupos. Subgrupos normais também aparecem naturalmente quando consideramos ações (à esquerda ou à direita) de um grupo em um conjunto.

Seja $G$ um grupo (cujo elemento neutro é $e_G$), seja $M$ um conjunto não vazio e seja $\gamma : G \times M \to M$ uma ação (à esquerda ou à direita) de $G$ em $M$. Considere-se o subconjunto $N$ de $G$ definido por

$$N \; := \; \Big\{ n \in G \big| \; \gamma_n(m) = m \text{ para todo } m \in M \Big\} \, . \tag{2.66}$$

Note-se que $N$ nunca é vazio, pois sempre vale $e_G \in N$ e note que $N = \{e_G\}$ se e somente se $\gamma$ é uma ação efetiva, ou fiel (para as definições, vide página 160).

Afirmamos que $N$ é um subgrupo normal de $G$. Isso é verdade tanto no caso em que $\gamma$ é uma ação à esquerda quanto à direita. Para sermos objetivos, trataremos do caso de ações à esquerda e o leitor perceberá que, *mutatis mutandis*, tudo o que faremos tem seu análogo para ações à direita.

De fato, $N$ é um subgrupo pelas seguintes razões: *1.* $e_G \in N$; *2.* se $n_1,\ n_2 \in N$, então $\gamma_{n_1 n_2}(m) = \gamma_{n_1}\big(\gamma_{n_2}(m)\big) = \gamma_{n_1}(m) = m$ para todo $m \in M$, estabelecendo que $n_1 n_2 \in N$; *3.* se $n \in N$, então, para todo $m \in M$ vale $\gamma_{n^{-1}}(m) = \gamma_{n^{-1}}\big(\gamma_n(m)\big) = \gamma_{n^{-1}n}(m) = \gamma_{e_G}(m) = m$, o que prova que $n^{-1} \in N$.

Que $N \lhd G$ segue do fato que, para todo $m \in M$, todo $g \in G$ e todo $n \in N$, vale $\gamma_{gng^{-1}}(m) = \gamma_g\Big(\gamma_n\big(\gamma_{g^{-1}}(m)\big)\Big) = \gamma_g\big(\gamma_{g^{-1}}(m)\big) = \gamma_{gg^{-1}}(m) = \gamma_{e_G}(m) = m$, provando que $gng^{-1} \in N$. Na segunda igualdade usamos que $\gamma_n\big(\gamma_{g^{-1}}(m)\big) = \gamma_{g^{-1}}(m)$, pois $n \in N$.

O exercício que segue mostra como podemos obter a partir de $\gamma$ uma ação efetiva, ou fiel, tomando o quociente de $G$ por $N$:

**E. 2.87** *Exercício*. Como antes, seja $M$ um conjunto não vazio, seja $G$ um grupo, seja $\gamma : G \times M \to M$ uma ação (à esquerda ou à direita) de $G$ sobre $M$ e seja $N$ o subgrupo normal de $G$ definido em (2.66). Considere o grupo quociente $G/N$ e defina $\Gamma : (G/N) \times M \to M$ por

$$\Gamma_{[g]}(m) \ := \ \gamma_g(m)\ ,$$

para todos $g \in G$ e $m \in M$.

**I.** Mostre que $\Gamma$, dada acima, faz sentido como função definida nas classes que compõem $G/N$, ou seja, mostre que se $g \sim_N g'$, então, de fato, $\Gamma_{[g]}(m) = \Gamma_{[g']}(m)$ para todo $m \in M$, pois valerá $\gamma_g(m) = \gamma_{g'}(m)$, também para todo $m \in M$.

**II.** Mostre que $\Gamma : (G/N) \times M \to M$ é uma ação (à esquerda ou à direita, dependendo de $\gamma$ o ser) de $G/N$ em $M$.

**III.** Mostre que $\Gamma : (G/N) \times M \to M$ é uma ação efetiva, ou seja, fiel, de $G/N$ em $M$, ou seja, mostre que se valer $\Gamma_{[g]}(m) = m$ para todo $m$, então $[g] = [e_G] = N$, o elemento neutro de $G/N$.

✠

### 2.2.2.1 Alguns Teoremas Sobre Isomorfismos e Homomorfismos de Grupos

Vamos agora apresentar alguns resultados fundamentais sobre homomorfismos de grupos. Historicamente esses resultados originam-se de trabalhos de Noether[58] e van der Waerden[59]. Talvez a maior importância prática dos resultados que obteremos é a de permitir estabelecer que certos grupos são isomorfos, mas esses resultados têm diversas outras consequências estruturais que exploraremos posteriormente.

Se $G$ e $G'$ são dois grupos (com elementos neutros $e_G$ e $e_{G'}$, respectivamente) e $\varphi : G \to G'$ é um homomorfismo, vimos no Exercício E. 2.84, página 173, que $\mathrm{Ran}\,(\varphi)$ (definido em (2.63)) é um subgrupo de $G'$ e que $\mathrm{Ker}\,(\varphi)$ (definido em (2.64)) é um subgrupo normal de $G$.

O teorema que segue é fundamental para todos os resultados que obteremos sobre homomorfismos e isomorfismos de grupos na presente Seção.

**Teorema 2.5 (Teorema Fundamental de Homomorfismos)** *Sejam dois grupos $G$ e $G'$ e um homomorfismo $\varphi : G \to G'$. Seja $N$ um subgrupo normal de $G$ com $N \subset \mathrm{Ker}\,(\varphi)$. Como usual, denotemos por $[g]_N$ a classe do grupo quociente $G/N$ que contém $g \in G$. Então, a aplicação $\Psi : G/N \to G'$, definida por $\Psi\big([g]_N\big) := \varphi(g)$ para cada $g \in G$, é um homomorfismo de $G/N$ em $G'$.*

*Fora isso, $\Psi$ será um epimorfismo (um homomorfismo sobrejetor) se e somente se $\varphi$ o for e $\Psi$ será um monomorfismo (um homomorfismo injetor) se e somente se* $\mathrm{Ker}\,(\varphi) = N$. □

Prova. Definimos $\Psi : G/N \to G'$ por $\Psi\big([g]_N\big) := \varphi(g)$. Primeiramente, provemos que essa expressão está bem definida nas classes $G/N$. Se $g_a,\ g_b \in G$ são tais que $g_a \sim_N g_b$, então existe $n \in N$ tal que $g_a^{-1} g_b = n$. Logo, $\varphi(g_b) = \varphi(g_a n) = \varphi(g_a)\varphi(n) = \varphi(g_a) e_{G'} = \varphi(g_a)$, provando que $\Psi\big([g]_N\big)$ não depende do particular representante tomado em $[g]_N$. Acima, usamos o fato que $\varphi(n) = e_{G'}$, pois supomos que $N \subset \mathrm{Ker}\,(\varphi)$.

[58] Amalie Emmy Noether (1882–1935).
[59] Bartel Leendert van der Waerden (1903–1996).

Vamos agora provar que $\Psi$ é um homomorfismo. Sejam $g_1,\ g_2 \in G$. Temos que $\Psi\big([g_1]_N[g_2]_N\big) = \Psi\big([g_1g_2]_N\big) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \Psi\big([g_1]_N\big)\Psi\big([g_2]_N\big)$.

Temos que $g' \in G'$ está na imagem de $\Psi$ se e somente se existir $g \in G$ tal que $g' = \varphi(g)$. Logo, $\Psi$ é um epimorfismo (um homomorfismo sobrejetor) se e somente se $\varphi$ o for. Resta-nos provar que $\Psi$ é um monomorfismo (um homomorfismo injetor) se e somente se $\mathrm{Ker}\,(\varphi) = N$.

Sejam $g_1,\ g_2 \in G$. Temos que $\Psi\big([g_1]_N\big) = \Psi\big([g_2]_N\big)$ se e somente se $\varphi(g_1) = \varphi(g_2)$ e, portanto, se e somente se $\varphi(g_1^{-1}g_2) = e_{G'}$, ou seja, se e somente se $g_1^{-1}g_2 \in \mathrm{Ker}\,(\varphi)$. Assim, se $N = \mathrm{Ker}\,(\varphi)$ teremos que a igualdade $\Psi\big([g_1]_N\big) = \Psi\big([g_2]_N\big)$ implica que $g_1^{-1}g_2 \in N$, ou seja, $[g_1]_N = [g_2]_N$ e, portanto, $\Psi$ é injetor. Por outro lado, se $\Psi$ for injetor, o raciocínio acima diz-nos que sempre que tivermos $g_1^{-1}g_2 \in \mathrm{Ker}\,(\varphi)$ devemos ter também $[g_1]_N = [g_1]_N$, ou seja, devemos ter $g_1 \sim_N g_2$. Em outras palavras, $g_1^{-1}g_2 \in \mathrm{Ker}\,(\varphi)$ implica que $g_1^{-1}g_2 \in N$. Portanto, se tomarmos, em particular, $g_1 = e_G$ e $g_2 \in \mathrm{Ker}\,(\varphi)$, devemos ter $g_2 \in N$. Assim, estabeleceu-se que $\mathrm{Ker}\,(\varphi) \subset N$, implicando que $\mathrm{Ker}\,(\varphi) = N$. Logo, $\Psi$ será um monomorfismo (um homomorfismo injetivo) se e somente se $\mathrm{Ker}\,(\varphi) = N$. ■

No restante desta seção vamos obter as consequências mais relevantes do Teorema 2.5.

• **O Primeiro Teorema de Isomorfismos**

Sejam $G$ e $H$ dois grupos e $\varphi : G \to H$ um homomorfismo. Já sabemos (Exercício E. 2.84, página 173) que $\mathrm{Ker}\,(\varphi)$ é um subgrupo normal de $G$ e $\mathrm{Ran}\,(\varphi)$ é um subgrupo de $H$. Se tomarmos $N = \mathrm{Ker}\,(\varphi)$ e $G' = \mathrm{Ran}\,(\varphi)$ no Teorema 2.5, obtemos o seguinte corolário importante:

**Teorema 2.6 (Primeiro Teorema de Isomorfismos)** *Sejam $G$ e $H$ dois grupos e $\varphi : G \to H$ um homomorfismo. Então, $G/\mathrm{Ker}\,(\varphi)$ e $\mathrm{Ran}\,(\varphi)$ são grupos isomorfos: $G/\mathrm{Ker}\,(\varphi) \simeq \mathrm{Ran}\,(\varphi)$, com o isomorfismo sendo dado por $\Psi\big([g]_{\mathrm{Ker}\,(\varphi)}\big) = \varphi(g)$, $g \in G$.* □

Prova. Sabemos que $\mathrm{Ker}\,(\varphi) \lhd G$ e que $\mathrm{Ran}\,(\varphi)$ é um subgrupo de $H$. Obviamente, $\varphi$ é sobrejetor em $\mathrm{Ran}\,(\varphi)$. Adotando-se $N = \mathrm{Ker}\,(\varphi)$ e $G' = \mathrm{Ran}\,(\varphi)$ no Teorema 2.5, obtemos a afirmação que $\Psi : G/\mathrm{Ker}\,(\varphi) \to \mathrm{Ran}\,(\varphi)$ dado por $\Psi\big([g]_{\mathrm{Ker}\,(\varphi)}\big) = \varphi(g)$, $g \in G$, é ao mesmo tempo um epimorfismo e um monomorfismo, ou seja, é um isomorfismo. ■

Na Proposição 21.32, página 1237, usaremos o Teorema 2.6 para demonstrar que os grupos $\mathrm{SU}(2)/\{\mathbb{1},\ -\mathbb{1}\}$ e $\mathrm{SO}(3)$ são isomorfos. Os exercícios que seguem exibem algumas aplicações mais simples do Teorema 2.6.

**E. 2.88** *Exercício*. Seja $\mathbb{Z}$ o grupo dos números inteiros com a operação usual de soma. Seja $n \in \mathbb{N}$ com $n \geq 2$, fixo. Denotamos por $n\mathbb{Z}$ o conjunto de todos os múltiplos inteiros de $n$: $n\mathbb{Z} := \big\{nk \,|\, k \in \mathbb{Z}\big\} \subset \mathbb{Z}$. **(a)** Mostre que $n\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$. Como $\mathbb{Z}$ é Abeliano, segue que $n\mathbb{Z}$ é um subgrupo normal de $\mathbb{Z}$. Como $n\mathbb{Z}$ é um subgrupo normal de $\mathbb{Z}$, podemos construir o grupo quociente $\mathbb{Z}/(n\mathbb{Z})$. **(b)** Mostre que $\mathbb{Z}/(n\mathbb{Z})$ é isomorfo ao grupo $\mathbb{Z}_n$ definido à Seção 2.1.3.3, página 132. **(c)** Mostre que a aplicação $\varphi : \mathbb{Z} \to \mathrm{U}(1)$ dada por $\varphi(m) = \exp\big(\frac{2\pi i m}{n}\big)$ é um homomorfismo entre os grupos $\mathbb{Z}$ e $\mathrm{U}(1)$. Mostre que $\mathrm{Ker}\,(\varphi) = n\mathbb{Z}$ e que $\mathrm{Ran}\,(\varphi) = \Big\{\exp\big(\frac{2\pi i m}{n}\big),\ m = 0,\ \ldots,\ n-1\Big\}$. Conclua do Teorema 2.6 que $\mathbb{Z}_n \simeq \mathbb{Z}/(n\mathbb{Z}) \simeq \Big\{\exp\big(\frac{2\pi i m}{n}\big),\ m = 0,\ \ldots,\ n-1\Big\}$. ✣

**E. 2.89** *Exercício*. Seja $\mathrm{GL}(n,\ \mathbb{C})$ o grupo das matrizes complexas $n \times n$ inversíveis (i.e., de determinante não nulo). Seja $\mathrm{SL}(n,\ \mathbb{C}) \subset \mathrm{GL}(n,\ \mathbb{C})$ o subgrupo das matrizes complexas $n \times n$ de determinante igual a 1. Seja $\mathbb{C} \setminus \{0\}$ o grupo multiplicativo dos complexos (sem o elemento zero).

Mostre que a aplicação $\varphi : \mathrm{GL}(n,\ \mathbb{C}) \to \mathbb{C} \setminus \{0\}$ dada por $\mathrm{GL}(n,\ \mathbb{C}) \ni A \mapsto \det(A) \in \mathbb{C} \setminus \{0\}$ é um homomorfismo. *Sugestão:* lembrar que $\det(AB) = \det(A)\det(B)$. Mostre que $\mathrm{Ker}\,(\varphi) = \mathrm{SL}(n,\ \mathbb{C})$ (o que, *en passant*, informa-nos que $\mathrm{SL}(n,\ \mathbb{C})$ é um subgrupo normal de $\mathrm{GL}(n,\ \mathbb{C})$. Vide Exercício E. 2.85, página 173) e mostre que $\mathrm{Ran}\,(\varphi) = \mathbb{C} \setminus \{0\}$. Conclua do Teorema 2.6 que

$$\mathrm{GL}(n,\ \mathbb{C})/\mathrm{SL}(n,\ \mathbb{C}) \ \simeq\ \mathbb{C} \setminus \{0\}\ .$$

✣

**E. 2.90** *Exercício*. Prove analogamente que

$$\mathrm{O}(n)/\mathrm{SO}(n) \ \simeq\ \{-1,\ 1\} \ \simeq\ \mathbb{Z}_2 \qquad \text{e que} \qquad \mathrm{U}(n)/\mathrm{SU}(n) \ \simeq\ \mathrm{U}(1)$$

para todo $n \in \mathbb{N}$. ✣

Na Seção 21.8, página 1234, estabeleceremos a importante relação (Proposição 21.32, página 1237):

$$\mathrm{SO}(3) \ \simeq \ \mathrm{SU}(2)/\{-\mathbb{1},\, \mathbb{1}\}\,,$$

de grande significado na Mecânica Quântica (para a descrição de rotações em estados de partículas com spin 1/2).

Nas Seções 21.9, página 1239, e 21.B, página 1273, estabelecemos que o grupo de Lorentz próprio ortócrono $\mathscr{L}_+^\uparrow$ e o grupo quociente $\mathrm{SL}(2,\,\mathbb{C})/\{-\mathbb{1},\,\mathbb{1}\}$ são também isomorfos. Esse fato é igualmente de grande significado para a Mecânica Quântica Relativista.

• **O Segundo Teorema de Isomorfismos**

O resultado que segue é um corolário do Teorema 2.6, página 177.

**Teorema 2.7 (Segundo Teorema de Isomorfismos)** *Sejam $G$ um grupo, $S$ um subgrupo de $G$ e $N$ um subgrupo normal de $G$. Então, valem as seguintes afirmações:*

1. *$SN := \{sn,\ s \in S,\ n \in N\}$ é um subgrupo de $G$ e $N$ é um subgrupo normal de $SN$.*
2. *$S \cap N$ é um subgrupo normal de $S$.*
3. *$(SN)/N$ e $S/(S \cap N)$ são isomorfos.* □

Prova. Note-se primeiramente que, como $S$ e $N$ são subgrupos de $G$, ambos contêm o elemento neutro. Segue trivialmente desse fato que $SN \supset S \cup N$ e, em particular, que $N \subset SN$. Pela Proposição 2.2, página 136, sabemos que $S \cap N$ é um subgrupo de $G$ e, portanto, é também um subgrupo de $S$ e de $N$.

Se $s_1,\ s_2 \in S$ e $n_1,\ n_2 \in N$, temos que $s_1n_1s_2n_2 = (s_1s_2)\big(s_2^{-1}n_1s_2\big)n_2$. Agora, $s_2^{-1}n_1s_2 \in N$, pois $N$ é um subgrupo normal de $G$ (e $S \subset G$). Logo, $s_1n_1s_2n_2 = s_3n_3$, onde $s_3 = s_1s_2 \in S$ e $n_3 = \big(s_2^{-1}n_2s_2\big)n_2 \in N$. Assim, o produto de dois elementos de $SN$ é um elemento de $SN$. Consideremos agora a operação de inversão. Se $s \in S$ e $n \in N$, então $(sn)^{-1} = n^{-1}s^{-1} = s^{-1}\big(sn^{-1}s^{-1}\big)$. Agora, $sn^{-1}s^{-1} \in N$ pela razão já mencionada. Isso estabeleceu que $SN$ é um subgrupo de $G$, provando o item 1.

É claro que $S \cap N$ é um subgrupo de $S$ e de $N$. Seja $h \in S \cap N$ e seja $s \in S$. Temos que $shs^{-1} \in N$, pois $h \in N$ e $N \lhd G$. Ao mesmo tempo, $shs^{-1} \in S$, pois $h \in S$. Logo, $shs^{-1} \in S \cap N$, provando que $S \cap N$ é um subgrupo normal de $S$, estabelecendo o item 2.

Como $N \lhd G$, tem-se também que $N \lhd SN$, já que $SN$ é um subgrupo de $G$. Assim, o quociente $SN/N$ está definido. Analogamente, o quociente $S/(S \cap N)$ está definido, pois $(S \cap N) \lhd S$. Provemos que esses dois quocientes são isomorfos.

Os elementos de $SN/N$ são classes do tipo $[sn]_N$, com $s \in S$ e $n \in N$. Os elementos de $S/(S \cap N)$ são classes do tipo $[s]_{S\cap N}$, com $s \in S$.

Considere-se a aplicação $\varphi : SN \to S/(S \cap N)$ dada por $\varphi(sn) := [s]_{S\cap N}$. Primeiramente, notemos que essa expressão está bem definida, pois se $s,\ s' \in S$ e $n,\ n' \in N$ são tais que $sn = s'n'$, então $s' = sn''$, onde $n'' = n(n')^{-1}$. Agora, por um lado temos $s^{-1}s' = n'' \in N$ e por outro lado temos $s^{-1}s' \in S$, já que $s$ e $s'$ são elementos de $S$. Isso provou que $s \sim_{S\cap N} s'$ e, portanto, que $[s]_{S\cap N} = [s']_{S\cap N}$.

Vamos agora provar que $\varphi : SN \to S/(S \cap N)$ é um homomorfismo. Isso é simples, pois

$$\varphi\big(s_1n_1s_2n_2\big) \ = \ \varphi\Big(s_1s_2\big(\underbrace{s_2^{-1}n_1s_2n_2}_{\in N}\big)\Big) \ = \ [s_1s_2]_{S\cap N} \ = \ [s_1]_{S\cap N}[s_2]_{S\cap N} \ = \ \varphi\big(s_1n_1\big)\varphi\big(s_2n_2\big)\,.$$

Temos que $\mathrm{Ran}\,(\varphi) = \big\{[s]_{S\cap N},\ s \in S\big\} = S/(S \cap N)$.

Por fim, observemos que $\mathrm{Ker}\,(\varphi) = \big\{sn | s \in S,\ n \in N \ \text{ e } \ [s]_{S\cap N} = [e_G]_{S\cap N}\big\}$. Isso significa que $sn \in \mathrm{Ker}\,(\varphi)$ se e somente se $s \sim_{S\cap N} e_G$, ou seja, se e somente se $se_G \in S \cap N$. Ora, isso é válido se e somente se $s \in S \cap N$. Logo, $sn \in N$ e, portanto, $\mathrm{Ker}\,(\varphi) = N$.

Evocando-se agora o Teorema 2.6, página 177, temos que $(SN)/\mathrm{Ker}\,(\varphi) \simeq \mathrm{Ran}\,(\varphi)$, ou seja, $(SN)/N \simeq S/(S \cap N)$. completando a prova. ■

• **O Terceiro Teorema de Isomorfismos**

O resultado que segue é mais um corolário do Teorema 2.6, página 177.

**Teorema 2.8 (Terceiro Teorema de Isomorfismos)** *Seja $G$ um grupo e sejam $N_1$ e $N_2$ dois subgrupos normais de $G$ tais que $N_1 \subset N_2$. Então, $N_1 \lhd N_2$ e valem*

1. $(N_2/N_1) \lhd (G/N_1)$.
2. $(G/N_1)/(N_2/N_1)$ *é isomorfo a* $G/N_2$. □

Prova. Que $N_1 \lhd N_2$ é evidente, pois $N_1 \lhd G$ e $N_2$ é um subgrupo de $G$.

Temos $G/N_1 = \big\{[g]_{N_1},\ g \in G\big\}$ e $N_2/N_1 = \big\{[n_2]_{N_1},\ n_2 \in N_2\big\}$. É claro que $N_2/N_1$ é um subgrupo de $G/N_1$. Agora, $[g]_{N_1}[n_2]_{N_1}[g]_{N_1}^{-1} = \big[gn_2g^{-1}\big]_{N_1}$. Mas $gn_2g^{-1} \in N_2$, já que $N_2 \lhd G$. Logo, $[g]_{N_1}[n_2]_{N_1}[g]_{N_1}^{-1} \in N_2/N_1$, provando que $(N_2/N_1) \lhd (G/N_1)$ e provando o item 1.

Pelo item 1, o quociente $(G/N_1)/(N_2/N_1)$ está bem definido. Seja $\varphi : G/N_1 \to G/N_2$ definido por $\varphi\big([g]_{N_1}\big) := [g]_{N_2}$.

Primeiramente, notemos que $\varphi$ está bem definida pois, se $g' \sim_{N_1} g$, então $g^{-1}g' \in N_1$. Logo, $g^{-1}g' \in N_2$, pois $N_1 \subset N_2$, implicando que $[g']_{N_2} = [g]_{N_2}$. Vamos provar que $\varphi$ é um homomorfismo. Temos que

$$\varphi\big([g_1]_{N_1}[g_2]_{N_1}\big) \ = \ \varphi\big([g_1g_2]_{N_1}\big) \ = \ [g_1g_2]_{N_2} \ = \ [g_1]_{N_2}[g_2]_{N_2} \ = \ \varphi\big([g_1]_{N_1}\big)\varphi\big([g_2]_{N_1}\big) \ .$$

Temos ainda que $\mathrm{Ran}\,(\varphi) = \Big\{[g]_{N_2},\ g \in G\Big\} = G/N_2$. Além disso, $\mathrm{Ker}\,(\varphi) = \Big\{[g]_{N_1} |\ [g]_{N_2} = [e_G]_{N_2}\Big\}$. Agora, $[g]_{N_2} = [e_G]_{N_2}$ se e somente se $ge_G \in N_2$, ou seja, se e somente se $g \in N_2$. Logo, $\mathrm{Ker}\,(\varphi) = \Big\{[n_2]_{N_1} |\ n_2 \in N_2\Big\} = N_2/N_1$.

Evocando-se agora o Teorema 2.6, página 177, temos que $(G/N_1)/\mathrm{Ker}\,(\varphi) \simeq \mathrm{Ran}\,(\varphi)$, ou seja, $(G/N_1)/(N_2/N_1) \simeq G/N_2$, completando a prova. ■

### 2.2.2.2 O Centro de um Grupo. Centralizadores e Normalizadores

• **O centro de um grupo**

Seja $G$ um grupo. O conjunto dos elementos de $G$ que têm a propriedade de comutarem com todos os elementos de $G$ é denominado o *centro do grupo* $G$ e é frequentemente denotado por $\mathbf{Z}(G)$. Em símbolos[60]:

$$\mathbf{Z}(G) \ := \ \Big\{h \in G |\ hg \,=\, gh \text{ para todo } g \in G\Big\} \ .$$

Note que $\mathbf{Z}(G)$ nunca é um conjunto vazio, pois o elemento neutro de $G$ sempre pertence a $\mathbf{Z}(G)$. Em alguns grupos, porém, esse pode ser o único elemento de $\mathbf{Z}(G)$. Esse é o caso, por exemplo, do grupo de permutações de $n$ elementos (por quê?).

**E. 2.91** *Exercício*. Mostre que $\mathbf{Z}(G)$ é sempre um subgrupo Abeliano de $G$. É igualmente elementar constatar que se $G$ é Abeliano se e somente se $\mathbf{Z}(G) = G$. ✠

*Comentário relevante*. Façamos alguns comentários para evitar-se confusões frequentes. Se um grupo $G_2$ é subgrupo de um grupo $G_1$, então é certo que os elementos de $\mathbf{Z}(G_1)$ comutam com todos os elementos de $G_2$. Mas isso não implica que $\mathbf{Z}(G_1)$ contenha $\mathbf{Z}(G_2)$, pois pode haver elementos em $\mathbf{Z}(G_2)$ que não comutam com certos elementos de $G_1$. Lembrar que $\mathbf{Z}(G_2)$ é composto por elementos de $G_2$ apenas, e não contém elementos de $G_1 \setminus G_2$.

O fato de um grupo $G_2$ ser subgrupo de um grupo $G_1$ não necessariamente implica que $\mathbf{Z}(G_2)$ seja subgrupo de $\mathbf{Z}(G_1)$, ou vice-versa. Há exemplos nos dois sentidos: tem-se $\mathbf{Z}\big(\mathrm{O}(2)\big) = \{\mathbb{1}_2,\ -\mathbb{1}_2\} \subset \mathrm{SO}(2) = \mathbf{Z}\big(\mathrm{SO}(2)\big)$ mas, por outro lado, $\mathbf{Z}\big(\mathrm{SO(n)}\big) \subset \mathbf{Z}\big(\mathrm{O(n)}\big)$ para todo $n > 2$. De fato, $\mathbf{Z}\big(\mathrm{O(n)}\big) = \{\mathbb{1}_n,\ -\mathbb{1}_n\}$ para todo $n > 2$, enquanto que $\mathbf{Z}\big(\mathrm{SO(n)}\big) = \{\mathbb{1}_n,\ -\mathbb{1}_n\}$ caso $n > 2$ seja par, e $\mathbf{Z}\big(\mathrm{SO(n)}\big) = \{\mathbb{1}_n\}$ para $n > 2$ ímpar. Vide Seção 2.2.2.3, página 180, em particular, vide a Proposição 2.12, página 182. ♣

[60] O emprego da letra **Z** provavelmente deriva da palavra alemã *"Zentrum"*.

• **Grupos projetivos**

É elementar constatar que para qualquer grupo $G$, seu centro $\mathbf{Z}(G)$ é um subgrupo normal de $G$. O grupo quociente $\mathrm{P}(G) := G/\mathbf{Z}(G)$ é denominado *grupo projetivo associado a* $G$. Exemplos desses grupos dentre grupos matriciais serão estudados na Seção 21.2.1.1, página 1124.

• **Centralizadores e normalizadores**

Seja $G$ um grupo e $F$ um subconjunto (não necessariamente um subgrupo) não vazio de $G$. O chamado *centralizador* de $F$ em $G$, denotado por $\mathbf{C}(F,\ G)$ (ou simplesmente por $\mathbf{C}(F)$, quando $G$ for subentendido), é o conjunto de todos os elementos de $G$ que comutam com todos os elementos de $F$:

$$\mathbf{C}(F,\ G)\ :=\ \Big\{g\in G|\ gf=fg \text{ para todo } f\in F\Big\}\ .$$

Seja $G$ um grupo e $F$ um subconjunto (não necessariamente um subgrupo) não vazio de $G$. Dado um elemento $h\in G$, denotamos por $hFh^{-1}$ o conjunto de todos os elementos de $G$ que sejam da forma $hfh^{-1}$ para algum $f\in F$, ou seja, $hFh^{-1}:=\{hfh^{-1},\ f\in F\}$.

O chamado *normalizador* de $F$ em $G$, denotado por $\mathbf{N}(F,\ G)$ (ou simplesmente por $\mathbf{N}(F)$, quando $G$ for subentendido), é o conjunto de todos os elementos $g\in G$ tais que $gFg^{-1}=F$:

$$\mathbf{N}(F,\ G)\ :=\ \Big\{g\in G|\ gFg^{-1}\ =\ F\Big\}\ .$$

**E. 2.92** *Exercício.* Com as definições acima, com $G$ sendo um grupo e $F\subset G$, $F$ sendo não vazio:

1. Constate que $\mathbf{C}(F,\ G)\subset\mathbf{N}(F,\ G)$ e que $\mathbf{Z}(G)=\mathbf{C}(G,\ G)$.
2. Mostre que $\mathbf{C}(F,\ G)$ e $\mathbf{N}(F,\ G)$ são subgrupos de $G$ e que $\mathbf{C}(F,\ G)\lhd\mathbf{N}(F,\ G)$.
3. Mostre que se $F$ for um subgrupo de $G$, então $F\lhd\mathbf{N}(F,\ G)$.
4. Mostre que se $F$ e $H$ forem subgrupos de $G$ e $F\lhd H$, então $H\subset\mathbf{N}(F,\ G)$ e, portanto, $\mathbf{N}(F,\ G)$ é o maior subgrupo de $G$ em relação ao qual $F$ é normal.

✠

### 2.2.2.3 O Centro de Alguns Grupos de Interesse

Vamos na corrente seção determinar o centro de alguns grupos de interesse. Faremos uso de definições e resultados do Capítulo 21, página 1114, e utilizaremos preferencialmente recursos elementares de Álgebra Linear, ainda que alguns dos resultados possam ser provados como consequência de teoremas mais profundos da Álgebra de Operadores.

Um resultado básico que empregaremos é o seguinte:

**Proposição 2.8** *Seja* $A\in\mathrm{Mat}\,(\mathbb{C},\ n)$ *(ou* $A\in\mathrm{Mat}\,(\mathbb{R},\ n)$*) uma matriz que comuta com todas as matrizes de* $\mathrm{Mat}\,(\mathbb{C},\ n)$ *(de* $\mathrm{Mat}\,(\mathbb{R},\ n)$*). Então,* $A=\lambda\mathbb{1}_n$ *com* $\lambda\in\mathbb{C}$ *(ou* $\lambda\in\mathbb{R}$*). Aqui,* $\mathbb{1}_n$ *é a matriz identidade* $n\times n$*.* □

Prova. Tomemos o caso de matrizes complexas pois o caso real é tratado analogamente. Se $A$ comuta com todas os elementos de $\mathrm{Mat}\,(\mathbb{C},\ n)$, então, em particular, comuta com as matrizes unitais $E^{a,\,b}$, com $a,\ b\in\{1,\ \ldots,\ n\}$, definidas da seguinte forma: $E^{a,\,b}$ é a matriz cujo elemento $ij$ é nulo a menos que $i=a$ e que $j=b$, em cujo caso $(E^{a,\,b})_{ij}=1$. Em símbolos,

$$\left(E^{a,\,b}\right)_{ij}\ =\ \delta_{ia}\delta_{jb}\ . \tag{2.67}$$

Pela regra de produto de matrizes, temos para os elementos de matriz de $AE^{a,\,b}$ e de $E^{a,\,b}A$,

$$(AE^{a,\,b})_{ij}\ =\ \sum_{k=1}^{n}A_{ik}(E^{a,\,b})_{kj}\ =\ \sum_{k=1}^{n}A_{ik}\delta_{ka}\delta_{jb}\ =\ A_{ia}\delta_{jb}\ , \tag{2.68}$$

$$(E^{a,\,b}A)_{ij}\ =\ \sum_{k=1}^{n}(E^{a,\,b})_{ik}A_{kj}\ =\ \sum_{k=1}^{n}\delta_{ia}\delta_{kb}A_{kj}\ =\ A_{bj}\delta_{ia}\ . \tag{2.69}$$

Assim, a condição $AE^{a,\,b} = E^{a,\,b}A$ implica que para todos $a,\ b,\ i,\ j \in \{1,\ \ldots,\ n\}$ vale

$$A_{ia}\delta_{jb} \;=\; A_{bj}\delta_{ia}\;.$$

Tomando-se $j = b$, concluímos $A_{ia} = A_{bb}\delta_{ia}$. Para $i = a$ isso diz que $A_{aa} = A_{bb}$ e, como $a$ e $b$ são arbitrários, concluímos dessa igualdade que $A_{bb} = \lambda$, constante independente de $b$. Daí, $A_{ia} = \lambda\delta_{ia}$, o que significa que $A = \lambda\mathbb{1}$. ■

• **O centro de** $\mathrm{GL}(n,\ \mathbb{C})$ **e de** $\mathrm{GL}(n,\ \mathbb{R})$

Como exercício vamos determinar o centro de $\mathrm{GL}(n,\ \mathbb{C})$. Se $A \in \mathbf{Z}\big(\mathrm{GL}(n,\ \mathbb{C})\big)$, então $AB = BA$ para toda $B \in \mathrm{GL}(n,\ \mathbb{C})$. Tomemos, em particular, uma matriz $B$ da forma $B = \mathbb{1} + E^{a,\,b}$, com $a,\ b \in \{1,\ \ldots,\ n\}$, onde $E^{a,\,b}$ são as matrizes unitais definidas em (2.67).

Antes de prosseguir, convença-se que $\mathbb{1} + E^{a,\,b} \in \mathrm{GL}(n,\ \mathbb{C})$, notando que $\det(\mathbb{1} + E^{a,\,b}) \neq 0$. Mais especificamente, notando que $\det(\mathbb{1} + E^{a,\,b}) = 2$, caso $a = b$ e $\det(\mathbb{1} + E^{a,\,b}) = 1$, caso $a \neq b$.

Agora, como supostamente $AB = BA$, segue que $AE^{a,\,b} = E^{a,\,b}A$ para todos $a,\ b \in \{1,\ \ldots,\ n\}$. Pela Proposição 2.8, página 180, isso implica que $A$ é um múltiplo da matriz identidade.

Afora isso, é evidente que toda matriz que seja um múltiplo não nulo da matriz identidade é um elemento de $\mathrm{GL}(n,\ \mathbb{C})$ e comuta com todo elemento de $\mathrm{GL}(n,\ \mathbb{C})$. Para futura referência expressamos nossas conclusões na forma de uma proposição:

**Proposição 2.9** *O centro do grupo* $\mathrm{GL}(n,\ \mathbb{C})$*, ou seja,* $\mathbf{Z}\big(\mathrm{GL}(n,\ \mathbb{C})\big)$*, coincide com o conjunto de todas as matrizes da forma* $\lambda\mathbb{1}$*, com* $\lambda \in \mathbb{C}$ *e* $\lambda \neq 0$*, ou seja, é o conjunto das matrizes não nulas que são múltiplos complexos da unidade. Em símbolos,*

$$\mathbf{Z}\big(\mathrm{GL}(n,\ \mathbb{C})\big) \;=\; \Big\{\lambda\mathbb{1},\ \lambda \in \mathbb{C},\ \lambda \neq 0\Big\} \;\simeq\; \big(\mathbb{C} \setminus \{0\},\ \cdot\big)\;,$$

*onde* $\big(\mathbb{C} \setminus \{0\},\ \cdot\big)$ *é o grupo multiplicativo dos complexos não nulos.* □

Para o caso de matrizes inversíveis reais, a mesma demonstração de acima conduz ao seguinte resultado:

**Proposição 2.10** *O centro do grupo* $\mathrm{GL}(n,\ \mathbb{R})$*, ou seja,* $\mathbf{Z}\big(\mathrm{GL}(n,\ \mathbb{R})\big)$*, coincide com o conjunto de todas as matrizes da forma* $\lambda\mathbb{1}$*, com* $\lambda \in \mathbb{R}$ *e* $\lambda \neq 0$*, ou seja, é o conjunto das matrizes não nulas que são múltiplos reais da unidade. Em símbolos,*

$$\mathbf{Z}\big(\mathrm{GL}(n,\ \mathbb{R})\big) \;=\; \Big\{\lambda\mathbb{1},\ \lambda \in \mathbb{R},\ \lambda \neq 0\Big\} \;\simeq\; \big(\mathbb{R} \setminus \{0\},\ \cdot\big)\;,$$

*onde* $\big(\mathbb{R} \setminus \{0\},\ \cdot\big)$ *é o grupo multiplicativo dos reais não nulos.* □

• **O centro de** $\mathrm{SL}(n,\ \mathbb{C})$ **e de** $\mathrm{SL}(n,\ \mathbb{R})$

Os exercícios a seguir fornecem os centros de $\mathrm{SL}(n,\ \mathbb{C})$ e de $\mathrm{SL}(n,\ \mathbb{R})$.

**E. 2.93** *Exercício.* Mostre que o centro de $\mathrm{SL}(n,\ \mathbb{C})$ é o conjunto de todas as matrizes da forma $\lambda\mathbb{1}$, com $\lambda \in \mathbb{C}$ satisfazendo $\lambda^n = 1$. Mostre que esse grupo é isomorfo ao grupo $\mathbb{Z}_n$. *Sugestão:* lembre-se que toda matriz de $\mathrm{SL}(n,\ \mathbb{C})$ é um múltiplo de uma matriz de $\mathrm{GL}(n,\ \mathbb{C})$ e use a Proposição 2.9, página 181. ✠

**E. 2.94** *Exercício.* Mostre que o centro de $\mathrm{SL}(n,\ \mathbb{R})$ é o conjunto de todas as matrizes da forma $\lambda\mathbb{1}$, com $\lambda \in \mathbb{R}$ satisfazendo $\lambda^n = 1$. Esse grupo é $\{\mathbb{1}\}$ quando $n$ é ímpar e $\{\mathbb{1},\ -\mathbb{1}\}$ quando $n$ é par. (Lembre-se que $\mathrm{SL}(n,\ \mathbb{R})$ é formado apenas por matrizes reais). *Sugestão:* adapte a sugestão do Exercício E. 2.93. ✠

• **O centro dos grupos** $\mathrm{SO}(n)$ **e** $\mathrm{O}(n)$

Como antes, $E^{a,\,b} \in \mathrm{Mat}\,(\mathbb{R},\ n)$, com $a,\ b \in \{1,\ \ldots,\ n\}$, denota a matriz cujo elemento $ij$ é nulo a menos que $i = a$ e que $j = b$, em cujo caso $(E^{a,\,b})_{ij} = 1$. Em símbolos, $(E^{a,\,b})_{ij} = \delta_{ia}\delta_{jb}$.

Para obtermos o centro dos grupos $\mathrm{SO}(n)$ necessitamos da seguinte proposição:

**Proposição 2.11** *Seja $A \in \mathrm{Mat}\,(\mathbb{R},\ n)$ uma matriz que comuta com todas as matrizes antissimétricas $n \times n$. Se $n = 2$, então $A$ é da forma $A = \alpha \mathbb{1}_2 + \beta M$, com $\alpha,\ \beta \in \mathbb{R}$ e onde $M := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Para $n > 2$, $A$ é um múltiplo da matriz identidade, ou seja, é da forma $A = \alpha \mathbb{1}_n$, com $\alpha \in \mathbb{R}$.* □

Prova. Se $A$ comuta com todas as matrizes antissimétricas $n \times n$, então $A$ comuta com todas as matrizes da forma $E^{a,\,b} - E^{b,\,a}$, com $a,\ b \in \{1,\ \ldots,\ n\}$. Segundo (2.68) e (2.69), temos para os elementos de matriz

$$\big(A(E^{a,\,b} - E^{b,\,a})\big)_{ij} \;=\; A_{ia}\delta_{jb} - A_{ib}\delta_{ja}\ , \tag{2.70}$$

$$\big((E^{a,\,b} - E^{b,\,a})A\big)_{ij} \;=\; A_{bj}\delta_{ia} - A_{aj}\delta_{ib}\ . \tag{2.71}$$

Assim, temos para todos $a,\ b,\ i,\ j \in \{1,\ \ldots,\ n\}$ que

$$A_{ia}\delta_{jb} - A_{ib}\delta_{ja} \;=\; A_{bj}\delta_{ia} - A_{aj}\delta_{ib}\ . \tag{2.72}$$

Fazendo $i = a$ e $j = b$ em (2.72), obtemos

$$A_{aa}\delta_{bb} - A_{ab}\delta_{ba} \;=\; A_{bb}\delta_{aa} - A_{ab}\delta_{ab}\ ,$$

ou seja, $A_{aa} = A_{bb}$. Como $a$ e $b$ são arbitrários, isso diz-nos que os elementos da diagonal de $A$ são todos iguais.

A relação (2.72) também diz-nos que para $i = j = a$, temos

$$A_{aa}\delta_{ab} - A_{ab}\delta_{aa} \;=\; A_{ba}\delta_{aa} - A_{aa}\delta_{ab}$$

o que implica

$$A_{ab} + A_{ba} \;=\; 2A_{aa}\delta_{ab}\ .$$

Essa relação nada traz se novo caso $a = b$, mas para $a \neq b$, ela diz-nos que

$$A_{ab} \;=\; -A_{ba} \qquad (\text{para } a \neq b)\ .$$

Assim, os elementos fora da diagonal de $A$ são antissimétricos.

Os resultados obtidos até agora dizem que $A$ é da forma $A = \alpha \mathbb{1}_n + J$, onde $J \in \mathrm{Mat}\,(\mathbb{R},\ n)$ é antissimétrica e $\alpha \in \mathbb{R}$.

Há agora dois casos a considerar:

1. **Caso** $n = 2$. Nesse caso, todas as matrizes antissimétricas são da forma $\beta \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ para algum $\beta \in \mathbb{R}$. Assim, toda matriz $A \in \mathrm{Mat}\,(\mathbb{R},\ 2)$ da forma $A = \alpha \mathbb{1}_2 + J$ com $J$ antissimétrica comuta com toda matriz antissimétrica $2 \times 2$.
2. **Caso** $n > 2$. Fazendo em (2.72) $a \neq b$, $j \neq a$, $j \neq b$ e $i = a$ (essas condições simultâneas são impossíveis caso $n = 2$, mas não o são caso $n > 2$), obtemos $A_{bj} = 0$. Como $j \neq b$, isso afirma que os elementos fora da diagonal de $A$ são nulos, ou seja, $J = 0$.

Essas considerações completam a demonstração. ■

O corolário que segue é agora evidente e dispensa demonstração:

**Corolário 2.3** *Se $A \in \mathrm{Mat}\,(\mathbb{R},\ n)$, com $n > 2$, é uma matriz antissimétrica que comuta com <u>todas</u> as matrizes antissimétricas $n \times n$, então $A = 0$.* □

Chegamos agora ao ponto que nos interessa: o centro dos grupos $\mathrm{SO}(n)$ e $\mathrm{O}(n)$, com $n \geq 2$, $n \in \mathbb{N}$:

**Proposição 2.12**

$$\mathbf{Z}\big(\mathrm{SO}(n)\big) \;=\; \begin{cases} \mathrm{SO}(2)\ , & \text{caso } n = 2\ , \\ \{\mathbb{1}_n,\ -\mathbb{1}_n\} \;\simeq\; \mathbb{Z}_2\ , & \text{caso } n > 2 \text{ e } n \text{ é par}\ , \\ \{\mathbb{1}_n\}\ , & \text{caso } n > 2 \text{ e } n \text{ é ímpar}\ . \end{cases} \tag{2.73}$$

*Além disso, para todo $n \geq 2$, $n \in \mathbb{N}$ tem-se*

$$\mathbf{Z}\big(\mathrm{O}(n)\big) \;=\; \{\mathbb{1}_n,\ -\mathbb{1}_n\} \;\simeq\; \mathbb{Z}_2\ . \tag{2.74}$$

*Acima, $\mathbb{1}_n$ é a matriz identidade $n \times n$.* □

Prova. Temos $\mathbf{Z}\big(\mathrm{SO}(2)\big) = \mathrm{SO}(2)$, pois $\mathrm{SO}(2)$ é Abeliano. Tomemos $n > 2$. Se $A \in \mathbf{Z}\big(\mathrm{SO}(n)\big)$, então $Ae^{\alpha B} = e^{\alpha B}A$ para toda matriz antissimétrica $B \in \mathrm{Mat}\,(\mathbb{R},\ n)$ e todo $\alpha \in \mathbb{R}$ (para tal, vide, por exemplo, Proposição 21.21, página 1192). Derivando-se em relação a $\alpha$ e tomando-se $\alpha = 0$, concluímos que $AB = BA$ para toda matriz antissimétrica $B \in \mathrm{Mat}\,(\mathbb{R},\ n)$. Pela Proposição 2.11, página 182, $A = \lambda\mathbb{1}_n$, com $\lambda \in \mathbb{R}$. Como $A \in \mathrm{SO}(n)$, seu determinante deve ser igual a 1, o que implica $\lambda = 1$, caso $n$ seja ímpar e $\lambda = \pm 1$, caso $n$ seja par. Isso estabeleceu que $\mathbf{Z}\big(\mathrm{SO}(n)\big) = \{\mathbb{1}_n,\ -\mathbb{1}_n\} \simeq \mathbb{Z}_2$ se $n > 2$ for par e que $\mathbf{Z}\big(\mathrm{SO}(n)\big) = \{\mathbb{1}_n\}$ para $n > 2$, ímpar.

Tomemos novamente $n \geq 2$. Como $\mathrm{SO}(n) \subset \mathrm{O}(n)$, os elementos de $\mathbf{Z}\big(\mathrm{O}(n)\big)$ são em primeiro lugar matrizes que comutam com todos os elementos de $\mathrm{SO}(n)$. Já sabemos que tais matrizes comutam com todas as matrizes reais antissimétricas e, pela Proposição 2.11, página 182, elas são da forma $\alpha\mathbb{1}_2 + \beta \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $\alpha,\ \beta \in \mathbb{R}$, caso $n = 2$, ou da forma $\alpha\mathbb{1}_n$, $\alpha \in \mathbb{R}$, caso $n > 2$.

1. Caso $n = 2$. As matrizes $\alpha\mathbb{1}_2 + \beta \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha & \beta \\ -\beta & \alpha \end{smallmatrix}\right)$ são ortogonais se e somente se $\alpha^2 + \beta^2 = 1$, ou seja, se e somente se forem elementos de $\mathrm{SO}(2)$. As matrizes de $\mathrm{O}(2)$ que não são elementos de $\mathrm{SO}(2)$ são da forma $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) R$, com $R \in \mathrm{SO}(2)$. Assim, se $A \in \mathbf{Z}\big(\mathrm{O}(2)\big)$, $A$ deve ser um elemento de $\mathrm{SO}(2)$ que comuta com $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. A condição é $A = \left(\begin{smallmatrix} \alpha & \beta \\ -\beta & \alpha \end{smallmatrix}\right)$ com $\alpha^2 + \beta^2 = 1$ e
$$\left(\begin{smallmatrix} \alpha & \beta \\ -\beta & \alpha \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \left(\begin{smallmatrix} \alpha & \beta \\ -\beta & \alpha \end{smallmatrix}\right) ,$$
o que implica $\beta = 0$. A condição $\alpha^2 + \beta^2 = 1$ implica, portanto, $\alpha = \pm 1$ e concluímos que $\mathbf{Z}\big(\mathrm{O}(2)\big)$ é composto apenas pelas matrizes $\pm\mathbb{1}_2$.
2. Caso $n > 2$. As matrizes da forma $\alpha\mathbb{1}_n$, $\alpha \in \mathbb{R}$, são elementos de $\mathrm{O}(n)$ se e somente se $\alpha^2 = 1$, ou seja, se e somente se $\alpha = \pm 1$. Concluímos que também nesse caso $\mathbf{Z}\big(\mathrm{O}(n)\big)$ é composto apenas pelas matrizes $\pm\mathbb{1}_n$. ■

• **O centro dos grupos** $\mathrm{SU}(n)$ **e** $\mathrm{U}(n)$

Para obtermos o centro dos grupos $\mathrm{SU}(n)$ necessitamos da seguinte proposição:

**Proposição 2.13** *Seja $A \in \mathrm{Mat}\,(\mathbb{C},\ n)$ uma matriz que comuta com todas as matrizes autoadjuntas $n \times n$. Então, $A$ é da forma $A = \lambda\mathbb{1}_n$, com $\lambda \in \mathbb{C}$.* □

Prova. Seja $A \in \mathrm{Mat}\,(\mathbb{C},\ n)$ uma matriz que comuta com todas as matrizes autoadjuntas $n \times n$. Isso implica que $A$ comuta com todos os elementos de $\mathrm{Mat}\,(\mathbb{C},\ n)$, pois se $M \in \mathrm{Mat}\,(\mathbb{C},\ n)$, então podemos escrever $M = \frac{1}{2}\Big[\big(M + M^*\big) + i\big((M - M^*)/i\big)\Big]$, que é uma combinação linear de duas matrizes autoadjuntas: $M + M^*$ e $(M - M^*)/i$. Assim, $A$ comuta com todos os elementos de $\mathrm{Mat}\,(\mathbb{C},\ n)$ e, pela Proposição 2.8, página 180, $A$ é um múltiplo da unidade. ■

**Proposição 2.14** *Para $n \in \mathbb{N}$ tem-se $\mathbf{Z}\big(\mathrm{SU}(n)\big) = \big\{\lambda\mathbb{1}_n \big|\ \lambda \in \mathbb{C},\ \text{com } \lambda^n = 1\big\} \simeq \mathbb{Z}_n$ e $\mathbf{Z}\big(\mathrm{U}(n)\big) = \big\{\lambda\mathbb{1}_n \big|\ \lambda \in \mathbb{C}\ \text{com } |\lambda| = 1\big\} \simeq \mathrm{U}(1)$. Aqui, $\mathbb{1}_n$ é a matriz identidade $n \times n$.* □

Prova. O caso $n = 1$ é trivial. Tomemos $n \geq 2$. Se $A \in \mathbf{Z}\big(\mathrm{SU}(n)\big)$, então $Ae^{\alpha iB} = e^{\alpha iB}A$ para toda matriz autoadjunta $B \in \mathrm{Mat}\,(\mathbb{C},\ n)$ e todo $\alpha \in \mathbb{R}$ (para tal, vide, por exemplo, Proposição 21.19, página 1188). Derivando-se em relação a $\alpha$ e tomando-se $\alpha = 0$, concluímos que $AB = BA$ para toda matriz autoadjunta $B \in \mathrm{Mat}\,(\mathbb{C},\ n)$. Pela Proposição 2.13, página 183, $A = \lambda\mathbb{1}_n$, com $\lambda \in \mathbb{R}$. Como $A \in \mathrm{SU}(n)$, seu determinante deve ser igual a 1, o que implica $\lambda^n = 1$.

Como $\mathrm{SU}(n) \subset \mathrm{U}(n)$, temos que os elementos de $\mathbf{Z}\big(\mathrm{U}(n)\big)$ são, em primeiro lugar, elementos de $\mathrm{Mat}\,(\mathbb{C},\ n)$ que comutam com todas as matrizes de $\mathrm{SU}(n)$. Vimos que tais matrizes devem comutar com todas as matrizes autoadjuntas e, portanto, pelos nossos resultados anteriores, são da forma $\lambda\mathbb{1}_n$ com $\lambda \in \mathbb{C}$. Matrizes desse tipo obviamente comutam com os elementos de $\mathrm{U}(n)$ e são elas mesmas unitárias se e somente se $|\lambda| = 1$. Concluímos que $\mathbf{Z}\big(\mathrm{U}(n)\big) = \big\{\lambda\mathbb{1}_n \big|\ \lambda \in \mathbb{C}\ \text{com } |\lambda| = 1\big\} \simeq \mathrm{U}(1)$. ■

### 2.2.3 Grupos Gerados por Conjuntos. Grupos Gerados por Relações

• **Suporte de uma função**

Seja $f : X \to G$ uma função de um conjunto não vazio $X$ em um grupo $G$. O *suporte* de $f$, denotado por $\text{supp}\,(f)$, é o conjunto de todos os pontos $x \in X$ tais que $f(x) \neq e$, onde $e$ é a unidade de $G$: $\text{supp}\,(f) := \{x \in X |\ f(x) \neq e\}$. Uma função $f : X \to G$ é dita ser de *suporte finito* se seu suporte for um conjunto finito.

• **Grupo Abeliano livremente gerado por um conjunto**

Uma noção importante que usaremos adiante é a de *grupo Abeliano livremente gerado por um conjunto* $X$. Seja $X$ um conjunto não vazio. Seja $\mathsf{F}(X)$ a coleção de todas as funções de suporte finito de $X$ em $\mathbb{Z}$. É fácil ver que $\mathsf{F}(X)$ tem naturalmente uma estrutura de grupo Abeliano, definindo, para $f$, $f' \in \mathsf{F}(X)$ o produto de $f$ e $f'$ como sendo o elemento $ff' = (f + f')$ de $\mathsf{F}(X)$ dado por

$$(f + f')(x) = f(x) + f'(x)\ , \tag{2.75}$$

para todo $x \in X$. É claro que esse $(f + f')$ tem suporte finito. O elemento neutro $e$ de $\mathsf{F}(X)$ é claramente a função identicamente nula e a inversa de cada $f$ é $-f$. Pelo fato de $\mathsf{F}(X)$ ter essa estrutura natural de grupo $\mathsf{F}(X)$ é denominado grupo Abeliano livremente gerado pelo conjunto $X$.

Para $x \in X$ vamos denotar por $\delta_x$ a função característica de $x$:

$$\delta_x(y) \ := \ \begin{cases} 1, & \text{se } y = x\ , \\ 0, & \text{se } y \neq x\ . \end{cases} \tag{2.76}$$

Claramente $\delta_x \in \mathsf{F}(X)$. Dado que cada $f \in \mathsf{F}(X)$ tem suporte finito, pode-se escrevê-la da forma

$$f \ = \ \sum_{n=1}^{N} a_n\, \delta_{x_n}\ , \tag{2.77}$$

para valores de $N \in \mathbb{N}$ e dos $a_n$'s dependentes de $f$, com $\{x_1, \ldots, x_N\} = \text{supp}\ (f)$ e com $a_i \in \mathbb{Z}$ para $i = 1, \ldots, N$.

Com um flagrante abuso de linguagem é costume escrever (2.77) da forma

$$f \ = \ \sum_{n=1}^{N} a_n\, x_n\ , \tag{2.78}$$

onde fica, por assim dizer, subentendido que aqui os $x_n$'s representam não os elementos de $X$ mas sim suas funções características ($X$ pode ser um conjunto qualquer, de modo que operações como soma de elementos de $X$ ou multiplicação de elementos de $X$ por um inteiro podem não serem sequer definidas).

É fácil verificar que $\mathsf{F}(X)$ é um grupo Abeliano livre (daí seu nome), o que quer dizer que não há em $\mathsf{F}(X)$ nenhuma relação não-trivial entre seus elementos, a não ser aquela que lhe confere Abelianidade: $ff'f^{-1}f'^{-1} = e$.

• **Relações e grupos gerados módulo relações**

Vamos passar agora a uma construção muito importante, a de grupo Abeliano livremente gerado por um conjunto módulo relações. Vamos apresentar essa construção de forma bem geral.

Seja $J$ um conjunto (em princípio arbitrário) de índices e seja, para cada $j \in J$, um elemento de $\mathsf{F}(X)$ dado por

$$r_j \ := \ \sum_{i=1}^{n(j)} \alpha_{j,\,i}\, x_{j,\,i}\ \ , \tag{2.79}$$

onde, para cada $j \in J$, $n(j) \in \mathbb{N}$ e, para todo $j \in J$ e $i \in \{1, \ldots, n(j)\}$, tem-se $\alpha_{j,\,i} \in \mathbb{Z}$ e $x_{j,\,i} \in X$ com $x_{j,\,i} \neq x_{j,\,i'}$ se $i \neq i'$. Denotamos $\mathcal{R} := \{r_j,\ j \in J\}$. Os elementos de $\mathcal{R}$ serão chamados "relações".

Seja $\mathsf{R}(\mathcal{R})$ o subgrupo de $\mathsf{F}(X)$ formado por todos os elementos de $\mathsf{F}(X)$ que são combinações lineares finitas de $r_j$'s com coeficientes em $\mathbb{Z}$:

$$s \in \mathsf{R} \Leftrightarrow s \ = \ s_1 r_{j_1} + \cdots + s_m r_{j_m}\ , \tag{2.80}$$

para certos $s_i \in \mathbb{Z}$ e $m \in \mathbb{N}$, que dependem de $s$. $\mathsf{R}(\mathcal{R})$ é dito ser o subgrupo de $\mathsf{F}(X)$ gerado pelas relações de $\mathcal{R}$.

Por ser um subgrupo de um grupo Abeliano, $\mathsf{R}(\mathcal{R})$ é normal. Assim, podemos definir o *grupo Abeliano livremente gerado por $X$, módulo as relações $\mathcal{R}$* como sendo o grupo $\mathsf{F}(X)/\mathsf{R}(\mathcal{R})$. Note-se que $[a]_R = e$ para todo $a \in \mathsf{R}(\mathcal{R})$, o que equivale a dizer que os elementos de $\mathcal{R}$ são identificados como zero (daí serem chamados de "relações", pois refletem identidades que não existiam em $\mathsf{F}(X)$ e que estão sendo agora impostas em $\mathsf{F}(X)/\mathsf{R}(\mathcal{R})$).

*

Mais adiante vamos usar as definições e construções acima nas definições de produto tensorial de grupos Abelianos e de espaços vetoriais.

## 2.2.4 O Produto Direto e o Produto Semidireto de Grupos. O Produto Tensorial de Grupos Abelianos

Vamos aqui descrever alguns procedimentos importantes que permitem construir um novo grupo a partir de outros grupos dados: o produto direto e o produto semidireto de grupos. Para o caso de grupos Abelianos descreveremos também o chamado produto tensorial, de importância na definição de produtos tensoriais de espaços vetoriais.

### 2.2.4.1 O Produto Direto (ou Soma Direta) de Grupos

• **O produto direto de dois grupos**

Se $G$ e $H$ são dois grupos, cujas identidades são $e_G$ e $e_H$, respectivamente é por vezes muito importante fazer do produto Cartesiano $G \times H$ um grupo. A maneira mais fácil é definir o produto de dois pares ordenados $(g_1,\ h_1)$, $(g_2,\ h_2)$, com $g_1,\ g_2 \in G$ e $h_1,\ h_2 \in H$, por

$$(g_1,\ h_1) \cdot (g_2,\ h_2) \ := \ (g_1 g_2,\ h_1 h_2)\ .$$

O leitor pode facilmente se convencer que esse produto é associativo, que $(e_G,\ e_H)$ é o elemento neutro e que $(g,\ h)^{-1} = (g^{-1},\ h^{-1})$.

Isso faz de $G \times H$ um grupo, denominado *produto direto* de $G$ e $H$ e denotado também por $G \times H$ (vide comentário sobre a notação adiante). Alternativamente, esse grupo pode ser chamado também de *soma direta* de $G$ e $H$ e denotado por $G \oplus H$. No caso de haver uma família finita de grupos envolvida não há distinção entre a noção de produto direto e de soma direta. Vide adiante.

**E. 2.95** *Exercício*. Mostre que os produtos diretos $G \oplus H$ e $H \oplus G$ são grupos isomorfos. ✠

**E. 2.96** *Exercício*. Sejam $G$ e $H$ dois grupos e seja a soma direta $G \oplus H$.

**I.** Mostre que o conjunto $\widetilde{G} := \big\{(g,\ e_H),\ g \in G\big\}$ é um subgrupo de $G \oplus H$ que é isomorfo a $G$. Mostre que $\widetilde{G}$ é um subgrupo normal de $G \oplus H$. Mostre que $\big(G \oplus H\big)/\widetilde{G}$ é isomorfo a $H$.

**II.** Mostre que o conjunto $\widetilde{H} := \Big\{(e_G,\ h),\ h \in H\Big\}$ é um subgrupo de $G \oplus H$ que é isomorfo a $H$. Mostre que $\widetilde{H}$ é um subgrupo normal de $G \oplus H$. Mostre que $\big(G \oplus H\big)/\widetilde{H}$ é isomorfo a $G$.

Acima, $e_G$ e $e_H$ são as unidades de $G$ e $H$, respectivamente. ✠

• **Produto direto e soma direta de coleções arbitrárias de grupos**

As ideias acima podem ser generalizadas com as definições de produtos diretos e somas diretas de coleções arbitrárias de grupos (não necessariamente Abelianos).

Seja $J$ um conjunto arbitrário de índices e $\mathcal{G} := \{G_j,\ j \in J\}$ uma coleção de grupos. Seja o produto Cartesiano[61] $\mathfrak{G} := \bigtimes\limits_{j \in J} G_j$. Podemos fazer de $\mathfrak{G}$ um grupo definindo o produto de dois elementos $\mathfrak{G} \ni \underline{g} = \bigtimes\limits_{j \in J} \big(g_j\big)$, $\mathfrak{G} \ni \underline{h} = \bigtimes\limits_{j \in J} \big(h_j\big)$

[61] Para a notação, vide página 73.

como $\underline{g}\cdot\underline{h} = \bigtimes_{j\in J}\big(g_j h_j\big)$. Com essa estrutura $\mathfrak{G}$ é dito ser o *produto direto* dos grupos $G_j$, $j\in J$, e será denotado por $\mathfrak{G}_p = \bigtimes_{j\in J} G_j$ ou por $\mathfrak{G}_p = \prod_{j\in J} G_j$. Vide comentário sobre notação, adiante.

O produto direto $\mathfrak{G}_p$ possui um subgrupo importante, aquele formado por elementos $\bigtimes_{j\in J} g_j \in \mathfrak{G}_p$ onde apenas um número finito de $g_j$'s é distinto da identidade $e_j$ do respectivo grupo $G_j$. Esse subgrupo é dito ser a *soma direta* dos grupos $G_j$ , $j\in J$, e é denotado por $\mathfrak{G}_s = \bigoplus_{j\in J} G_j$.

*Comentário sobre a notação.* O uso dos símbolos $\bigtimes_{j\in J} G_j$ ou $\prod_{j\in J} G_j$ para denotar o produto direto da família de grupos $\{G_j,\ j\in J\}$ não é universal. Muitos autores, especialmente em textos mais antigos, usam o símbolo $\bigotimes_{j\in J} G_j$. Evitamos fazê-lo, pois o símbolo $\otimes$ é mais frequentemente empregado para denotar *produtos tensoriais de grupos Abelianos*, uma noção que introduziremos na Seção 2.2.4.3, página 190. É importante observar também que no caso de $J$ ser um conjunto finito não há distinção entre o produto direto e a soma direta: $\prod_{j\in J} G_j = \bigoplus_{j\in J} G_j$ (se $J$ for finito). ♣

Neste ponto devemos gastar algumas palavras sobre a questão da associatividade das construções acima. Dados três grupos $G_1$, $G_2$ e $G_3$, podemos, repetindo o procedimento de construção da soma direta de dois grupos, construir os grupos $G_1\oplus(G_2\oplus G_3)$ e $(G_1\oplus G_2)\oplus G_3$, assim como podemos construir diretamente o grupo $G_1\oplus G_2\oplus G_3$. A distinção entre esses três objetos, enquanto conjuntos, muito se assemelha à distinção entre produtos Cartesianos de três conjuntos que fizemos à página 73 e é conveniente ignorá-la na grande maioria das situações. É de se notar também que se trata de três grupos isomorfos, pois

$$\varphi_1 : G_1\oplus(G_2\oplus G_3)\to G_1\oplus G_2\oplus G_3\ ,\quad \varphi_1\big(a_1\oplus(a_2\oplus a_3)\big) \ := \ a_1\oplus a_2\oplus a_3$$

$$\varphi_2 : (G_1\oplus G_2)\oplus G_3\to G_1\oplus G_2\oplus G_3\ ,\quad \varphi_2\big((a_1\oplus a_2)\oplus a_3\big) \ := \ a_1\oplus a_2\oplus a_3$$

são dois isomorfismos de grupo, como facilmente se constata, os quais são denominados *isomorfismos canônicos.*

### 2.2.4.2 O Produto Semidireto de Grupos

**• O produto semidireto de dois grupos**

Dados dois grupos $G$ e $H$ há uma outra maneira de fazer de $G\times H$ um grupo além do produto direto. Para tal é necessário que exista uma ação de $G$ em $H$ por automorfismos de $H$. Expliquemos melhor isso.

Lembremos que um *automorfismo* de um grupo $H$ é um isomorfismo de $H$ em si mesmo. Uma ação (à esquerda) de $G$ sobre $H$ por automorfismos é um função $\alpha : G\times H\to H$ tal que a cada par $(g,\ h)\in G\times H$ associa um elemento denotado por $\alpha_g(h)$ de $H$ de tal forma que as seguintes condições sejam satisfeitas:

1. Para todo $g\in G$, a função $\alpha_g(\cdot) : H\to H$ é um automorfismo de $H$, ou seja, $\alpha_g(h)\alpha_g(h') = \alpha_g(hh')$, sendo que $\alpha_g(\cdot) : H\to H$ é bijetora com $(\alpha_g)^{-1} = \alpha_{g^{-1}}$.
2. Para todo $h\in H$ vale $\alpha_{e_G}(h) = h$.
3. Para todo $h\in H$ vale $\alpha_g\big(\alpha_{g'}(h)\big) = \alpha_{gg'}(h)$ para quaisquer $g,\ g'\in G$.

Acima $e_G$ e $e_H$ são as unidades de $G$ e $H$, respectivamente.

**E. 2.97** *Exercício-exemplo.* Um exemplo importante é o seguinte. Seja $N\lhd G$. Então, com $n\in N$, $\alpha_g(n) := gng^{-1}$ define uma ação (à esquerda) de $G$ sobre $N$ por automorfismos. Verifique! ✣

Pela definição geral, tem-se pelas propriedades *1, 2* e *3* acima que para quaisquer $g\in G$ e $h\in H$

$$\alpha_g(e_H)h \ = \ \alpha_g(e_H)\alpha_g\big(\alpha_{g^{-1}}(h)\big) \ = \ \alpha_g\big(e_H\alpha_{g^{-1}}(h)\big) \ = \ \alpha_g\big(\alpha_{g^{-1}}(h)\big) \ = \ h\ ,$$

o que implica $\alpha_g(e_H) = e_H$ para todo $g \in G$.

Se $G$ e $H$ são grupos e $\alpha : G \times H \to H$ é uma ação à esquerda de $G$ sobre $H$ por automorfismos, então podemos definir em $G \times H$ um produto de dois pares ordenados $(g_1,\ h_1)$, $(g_2,\ h_2)$, com $g_1,\ g_2 \in G$ e $h_1,\ h_2 \in H$, por

$$(g_1,\ h_1) \cdot (g_2,\ h_2) \ := \ \big(g_1 g_2,\ h_1 \alpha_{g_1}(h_2)\big) \ .$$

**E. 2.98** *Exercício importante.* Mostre que esse produto é associativo, que $(e_G,\ e_H)$ é a unidade e que

$$(g,\ h)^{-1} \ = \ \Big(g^{-1},\ \alpha_{g^{-1}}\big(h^{-1}\big)\Big) \tag{2.81}$$

para quaisquer $g \in G$, $h \in H$. ✠

Com isso, $G \times H$ adquire a estrutura de um grupo, denominado *produto semidireto de $G$ por $H$ pelo automorfismo* $\alpha : G \times H \to H$, ou simplesmente *produto semidireto de $G$ por $H$* quando um automorfismo $\alpha : G \times H \to H$ específico é subentendido. Na literatura, o produto semidireto de $G$ por $H$ é denotado por $G \circledS_\alpha H$ ou por $G \rtimes_\alpha H$ (ou simplesmente $G \circledS H$ ou $G \rtimes H$ quando um automorfismo $\alpha : G \times H \to H$ específico é subentendido). Mais raramente encontra-se também as notações $G \times_\alpha H$ ou $G \otimes_\alpha H$ para designar produtos semidiretos.

Comenta-se que o símbolo $\rtimes$ foi inventado como uma combinação gráfica do símbolo $\times$, de produto Cartesiano, com o símbolo $\lhd$, que indica um subgrupo normal. Vide exemplo (2.82), abaixo.

É relevante observar que no caso em que $\alpha$ é a aplicação identidade (isto é, vale $\alpha_g(h) = h$ para todo $g \in G$ e todo $h \in H$) o grupo $G \circledS H$ coincide com a soma direta $G \oplus H$.

• **Exemplos**

**I.** Seja $G$ um grupo e $N \lhd G$. Então, para $g_1,\ g_2 \in G$ e $n_1,\ n_2 \in N$ o produto

$$(g_1,\ n_1) \cdot (g_2,\ n_2) \ := \ \big(g_1 g_2,\ n_1 g_1 n_2 g_1^{-1}\big) \tag{2.82}$$

define o grupo $G \circledS N$, ou $G \rtimes N$, o produto semidireto de um grupo $G$ por um subgrupo normal $N$ pelo automorfismo natural.

**II.** Considere o grupo $G$, formado por todos os números reais não nulos com o produto dado pela multiplicação usual e o grupo $H$, formado por todos os reais com o produto dado pela soma: $G = (\mathbb{R} \setminus \{0\},\ \cdot)$ e $H = (\mathbb{R},\ +)$.

Para todo $a \in \mathbb{R} \setminus \{0\}$ e $x \in \mathbb{R}$ definimos $\alpha : G \times H \to H$ por $\alpha_a(x) := ax$. Para cada $a \in G$, tem-se que $\alpha_a$ é bijetora, com inversa dada por $\alpha_{1/a}$. Fora isso, $\alpha_a(x) + \alpha_a(y) = ax + ay = a(x+y) = \alpha_a(x+y)$. Assim, $\alpha_a$ é um automorfismo (condição 1. da definição acima). Fora isso, para todo $x \in H$, $\alpha_1(x) = x$ (condição 2.). Por fim, para todo $x \in H$, $\alpha_a(\alpha_b(x)) = abx = \alpha_{ab}(x)$, para quaisquer $a,\ b \in G$ (condição 3.). Concluímos que $\alpha$ é uma ação à esquerda de $G$ sobre $H$ por automorfismos.

Assim, fazemos de $G \times H$ um grupo $G \circledS_\alpha H$ com o produto

$$(a,\ x) \cdot (b,\ y) \ := \ (ab,\ x + ay) \ .$$

O elemento neutro é o par $(1,\ 0)$ e $(a,\ x)^{-1} = (1/a,\ -x/a)$.

Para interpretar o que esse grupo $G \circledS_\alpha H$ significa, vamos definir uma ação[62] $\Gamma$ de $G \circledS_\alpha H$ sobre o conjunto $\mathbb{R}$ da seguinte forma. Para $(a,\ x) \in G \circledS_\alpha H$ e $z \in \mathbb{R}$, definimos

$$\Gamma\big((a,\ x),\ z\big) \ := \ az + x \ .$$

Para verificar que isso é uma ação notemos as seguintes propriedades: *i.* para cada $(a,\ x)$ fixo $\Gamma\big((a,\ x),\ z\big)$ é uma função bijetora de $\mathbb{R}$ em $\mathbb{R}$ (lembre-se que $a \neq 0$). *ii.* Para todo $z \in \mathbb{R}$, $\Gamma\big((1,\ 0),\ z\big) = z$.

$$\textit{iii.} \qquad \Gamma\Big((a,\ x),\ \Gamma((b,\ y),\ z)\Big) \ = \ \Gamma\big((a,\ x),\ bz + y\big) \ = \ a(bz+y) + x \ = \ abz + (x + ay)$$

$$= \ \Gamma\big((ab,\ x + ay),\ z\big) \ = \ \Gamma\big((a,\ x) \cdot (b,\ y),\ z\big) \ .$$

[62] O conceito de ação de um grupo em um conjunto foi definido na Seção 2.1.9.1, página 157.

Isso mostrou que $\Gamma$ é uma ação de $G\circledS_\alpha H$ sobre o conjunto $\mathbb{R}$. Como vemos, a ação de um elemento $(a,\ x)$ consiste em uma combinação de uma multiplicação por $a \neq 0$ seguida por uma translação por $x \in \mathbb{R}$. Isso exibe o significado geométrico do grupo $G\circledS_\alpha H$. Vamos a um outro exemplo semelhante.

**III. Grupos de homotetias.** Seja $V$ um espaço vetorial (e, como tal, um grupo Abeliano em relação à soma de vetores) e seja $D = (\mathbb{R}_+,\ \cdot)$ o grupo multiplicativo dos reais positivos (grupo de dilatações). O chamado *grupo de homotetias* de $V$ é o produto semidireto $D\circledS_\alpha V$ com $\alpha$ dado por $\alpha_\lambda(v) = \lambda v$, $\lambda \in D$, $v \in V$. O produto nesse grupo é, portanto, $(\lambda_1,\ v_1)(\lambda_2,\ v_2) = \big(\lambda_1\lambda_2,\ v_1 + \lambda_1 v_2\big)$.

Esse grupo possui uma ação em $V$ dada por $A_{(\lambda,\ v)}(x) = \lambda x + v$, que envolve uma multiplicação de um vetor $x \in V$ por $\lambda > 0$ e uma translação por $v$. Tais transformações são denominadas *homotetias*[63]. Como, para qualquer $a \in V$, vale $\lambda x + v = \lambda(x - a) + u$, com $u = v + \lambda a$, vemos que toda homotetia pode ser considerara como uma dilatação a partir de um centro $a$ acompanhado de uma translação.

**IV. Grupos Euclidianos.** Considere o conjunto de todas as operações do espaço tridimensional que envolvem rotações e translações. Por exemplo, considere-se a operação na qual cada vetor $\vec{x}$ é primeiramente rodado por uma matriz de rotação $R \in \mathrm{SO}(3)$ e em seguida é transladado por um vetor $\vec{x}_0$:

$$\vec{x} \ \mapsto \ R\vec{x} + \vec{x}_0. \tag{2.83}$$

A composição de duas de tais operações conduz à transformação $\vec{x} \mapsto R'\big(R\vec{x} + \vec{x}_0\big) + \vec{x}'_0$, ou seja,

$$\vec{x} \ \longmapsto \ \big(R'R\big)\vec{x} + \vec{x}'_0 + R'\vec{x}_0\ . \tag{2.84}$$

O espaço vetorial $\mathbb{R}^3$ é naturalmente um grupo Abeliano em relação à adição de vetores. Se $R \in \mathrm{SO}(3)$, $\alpha_R(\vec{x}_0) := R\vec{x}_0$ define uma ação por automorfismos de $\mathrm{SO}(3)$ sobre $\mathbb{R}^3$. A expressão (2.84) inspira a definição do produto semidireto $\mathrm{SO}(3)\circledS_\alpha\mathbb{R}^3$ por

$$\big(R',\ \vec{x}'_0\big)\cdot\big(R,\ \vec{x}_0\big) \ = \ \Big(R'R,\ \vec{x}'_0 + R'\vec{x}_0\Big)\ .$$

**E. 2.99** *Exercício.* Verifique que a transformação (2.83) define uma ação à esquerda do grupo $\mathrm{SO}(3)\circledS_\alpha\mathbb{R}^3$ sobre $\mathbb{R}^3$. ✠

**Definição. Grupos Euclidianos.** Os grupos $\mathbf{E}_n := \mathrm{O}(n)\circledS_\alpha\mathbb{R}^n$ são denominados *grupos Euclidianos em dimensão* $n$. Os grupos $\mathbf{SE}_n := \mathrm{SO}(n)\circledS_\alpha\mathbb{R}^n$ são denominados *grupos Euclidianos especiais em dimensão* $n$. ♠

Mais material sobre os grupos Euclidianos, incluindo representações matriciais, geradores etc., pode ser encontrado na Seção 21.5, página 1196.

**V. Grupos afins.** Seja $V$ um espaço vetorial (e, como tal, um grupo Abeliano em relação à soma de vetores) e seja $\mathrm{Aut}(V)$ a coleção de todas as aplicações lineares bijetoras de $V$ em $V$.

Por exemplo $V = \mathbb{R}^n$ e $\mathrm{Aut}(\mathbb{R}^n)$ é o conjunto de todas as matrizes reais $n \times n$ inversíveis.

Então, fazemos de $\mathrm{Aut}(V) \times V$ um grupo, definindo

$$(A,\ v)\cdot(B,\ u) \ := \ (AB,\ v + Au)\ .$$

Esse grupo é por vezes denominado *grupo afim* do espaço vetorial $V$. Mais sobres grupos afins na Seção 21.5, página 1196.

*Observação.* O caso $V = \mathbb{R}$ corresponde exatamente ao exemplo **II**, acima. ♣

No Teorema de Mazur-Ulam, Teorema 3.8, página 297, mostramos que o grupo de isometrias de um espaço vetorial real e normado sobre si mesmo é um grupo afim que compõe isometrias lineares com translações.

###

Mencionamos, por fim, que o *grupo de Poincaré*, introduzido à página 1209, é também um exemplo de um grupo definido como um produto semidireto de dois grupos, a saber, o produto semidireto do grupo das transformações de Lorentz com o grupo das translações no espaço-tempo.

[63] Do grego *"homo"* (similar) e *"tetia"* (posição). O termo foi cunhado por Michel Chasles (1793–1880).

• **Mais sobre $G\circledS_\alpha H$**

O exercício a seguir estabelece alguns fatos fundamentais sobre produtos semidiretos de dois grupos $G$ e $H$. Especificamente, ele apresenta relações estruturais entre $G\circledS_\alpha H$ e os grupos $G$ e $H$.

**E. 2.100** *Exercício*. Sejam $G$ e $H$ dois grupos e seja o produto semidireto $G\circledS_\alpha H$, onde $\alpha : G\times H\to H$ é uma ação (à esquerda) de $G$ sobre $H$ por automorfismos, como descrito acima. Sejam $e_G$ e $e_H$ as unidades de $G$ e $H$, respectivamente.

**I.** Mostre que o conjunto $\widetilde{G} := \Big\{(g,\, e_H),\ g\in G\Big\}$ é um subgrupo de $G\circledS_\alpha H$ e que $\widetilde{G}$ é isomorfo a $G$.

**II.** Mostre que o conjunto $\widetilde{H} := \Big\{(e_G,\, h),\ h\in H\Big\}$ é um subgrupo de $G\circledS_\alpha H$ e que $\widetilde{H}$ é isomorfo a $H$.

**III.** Mostre que $\widetilde{H}$ é um subgrupo normal de $G\circledS_\alpha H$.

**IV.** Considere as classes de equivalência que compõem o grupo quociente $\big(G\circledS_\alpha H\big)/\widetilde{H}$. Mostre que $(g,\, h)\sim_{\widetilde{H}}(g',\, h')$ se e somente se $g=g'$. Conclua que $\big[(g,\, h)\big] = \Big\{(g,\, h'),\ h'\in H\Big\}$ e conclua que $\big[(g,\, h)\big] = \big[(g,\, e_H)\big]$.

**V.** Mostre que o grupo quociente $\big(G\circledS_\alpha H\big)/\widetilde{H}$ é isomorfo a $G$.

Por fim, explicite qual condição $\alpha$ deve satisfazer para que $\widetilde{G}$ seja também um subgrupo normal de $G\circledS_\alpha H$. Em tal caso, prove que $\big(G\circledS_\alpha H\big)/\widetilde{G}$ é isomorfo a $H$. Compare com as afirmativas do Exercício E. 2.96, página 185. ✠

• **Ações de $G\circledS_\alpha H$ em $H$**

Sejam, como acima, $G$ e $H$ dois grupos e seja $\alpha$ uma ação de $G$ em $H$ por automorfismos de $H$, de sorte que com esses ingredientes possamos definir o produto semidireto $G\circledS_\alpha H$.

Com esses ingredientes, podemos definir uma ação (à esquerda) de $G\circledS_\alpha H$ em $H$, que denotaremos por, $A : \big(G\circledS_\alpha H\big)\times H\to H$, por

$$A_{(g,\,h)}(h') \;:=\; h\alpha_g(h')\;. \tag{2.85}$$

Para ver que se trata de uma ação de $G\circledS_\alpha H$ em $H$, observe-se que, de acordo com essa definição, temos

$$\begin{aligned} A_{(g_1,\,h_1)}\Big(A_{(g_2,\,h_2)}(h')\Big) \;&=\; A_{(g_1,\,h_1)}\big(h_2\alpha_{g_2}(h')\big) \;=\; h_1\alpha_{g_1}\big(h_2\alpha_{g_2}(h')\big) \;=\; \big(h_1\alpha_{g_1}(h_2)\big)\alpha_{g_1g_2}(h') \\ &=\; A_{\left(g_1g_2,\,h_1\alpha_{g_1}(h_2)\right)}(h') \;=\; A_{(g_1,\,h_1)(g_2,\,h_2)}(h')\;, \end{aligned}$$

ou seja,

$$A_{(g_1,\,h_1)}\circ A_{(g_2,\,h_2)} \;=\; A_{(g_1,\,h_1)(g_2,\,h_2)}\;. \tag{2.86}$$

Para demonstrar que $A$ é de fato uma ação (à esquerda) de $G\circledS_\alpha H$ em $H$, resta apenas constatar que $A_{(e_G,\,e_H)}(h')=h'$ para todo $h'\in H$ e que para cada $g\in G$, $h\in H$, aplicação $A_{(g,\,h)}(\cdot)$ é uma bijeção de $H$ em $H$. Provar isso é elementar e é deixado ao leitor como exercício.

• **Ações de $G\circledS_\alpha H$ em funções definidas em $H$**

Com uso da ação (2.85) podemos também definir uma ação (à esquerda) de $G\circledS_\alpha H$ no espaço das funções definidas em $H$ (assumindo valores nos complexos, digamos).

Seja $f : H\to\mathbb{C}$ uma função definida em $H$ com valores nos complexos. Seguindo (2.51), página 159, defina-se uma nova função $\mathcal{A}_{(g,\,h)}f$ por

$$\Big(\mathcal{A}_{(g,\,h)}f\Big)(h') \;:=\; f\Big(A_{(g,\,h)^{-1}}(h')\Big)\;. \tag{2.87}$$

Pelos comentários gerais da página 159 $\mathcal{A}_{(g,\,h)}$ define uma ação à esquerda de $G\circledS_\alpha H$ em funções definidas em $H$ e, portanto, vale

$$\Big(\Big(\mathcal{A}_{(g_1,\,h_1)}\circ\mathcal{A}_{(g_2,\,h_2)}\Big)f\Big)(h') \;=\; \big(\mathcal{A}_{(g_1,\,h_1)(g_2,\,h_2)}f\big)(h')$$

ou seja,

$$\mathcal{A}_{(g_1,\,h_1)}\circ\mathcal{A}_{(g_2,\,h_2)} \;=\; \mathcal{A}_{(g_1,\,h_1)(g_2,\,h_2)}\;.$$

Note-se que nesse caso

$$\Big(\mathcal{A}_{(g,\,h)}f\Big)(h') \;:=\; f\Big(A_{(g,\,h)^{-1}}(h')\Big) \overset{(2.81)}{=} f\Big(A_{\left(g^{-1},\,\alpha_{g^{-1}}(h^{-1})\right)}(h')\Big) \overset{(2.85)}{=} f\Big(\alpha_{g^{-1}}(h^{-1})\alpha_{g^{-1}}(h')\Big) \;=\; f\Big(\alpha_{g^{-1}}(h^{-1}h')\Big)\,.$$

Em resumo, vale

$$\Big(\mathcal{A}_{(g,\,h)}f\Big)(h') \;=\; f\Big(\alpha_{g^{-1}}(h^{-1}h')\Big)\,. \tag{2.88}$$

Segundo (2.52), página 159, uma ação à direita de $G\circledS_\alpha H$ nas funções definidas em $H$ é obtida por

$$\Big(\mathcal{B}_{(g,\,h)}f\Big)(h') \;:=\; f\Big(A_{(g,\,h)}(h')\Big) \;=\; f\Big(h\alpha_g(h')\Big)\,. \tag{2.89}$$

**Exemplo 2.23** Vamos a um exemplo relevante. Considere-se o grupo Euclidiano $\mathbf{SE}_3 := \mathrm{SO}(3)\circledS_\alpha\mathbb{R}^3$ com $\alpha_R(\vec{y}) = R\vec{y}$ para todo $R \in \mathrm{SO}(3)$ e todo $\vec{y} \in \mathbb{R}^3$, como acima. A ação à esquerda de $\mathbf{SE}_3$ no grupo aditivo $\mathbb{R}^3$ é

$$A_{(R,\,\vec{x})}(\vec{y}) \;:=\; \vec{x} + R\vec{y}\,,$$

o que representa uma rotação por $R$ do vetor $\vec{y}$ seguida de uma translação por $\vec{x}$. A ação à esquerda de $\mathbf{SE}_3$ nas funções definidas em $\mathbb{R}^3$ (com valores complexos, digamos) é dada por

$$\Big(\mathcal{A}_{(R,\,\vec{x})}f\Big)(\vec{y}) \;:=\; f\Big(A_{(R,\,\vec{x})^{-1}}(\vec{y})\Big) \;=\; f\Big(A_{(R^{-1},\,-R^{-1}\vec{x})}(\vec{y})\Big) \;=\; f\Big(-R^{-1}\vec{x} + R^{-1}\vec{y}\Big)\,,$$

ou seja,

$$\Big(\mathcal{A}_{(R,\,\vec{x})}f\Big)(\vec{y}) \;=\; f\Big(R^{-1}(\vec{y}-\vec{x})\Big)\,, \tag{2.90}$$

tal como em (2.88), o que significa que fazemos primeiro uma translação por $-\vec{x}$ no argumento e depois uma rotação por $R^{-1}$ do que resulta.

A ação à direita (2.89) de $\mathbf{SE}_3$ nas funções definidas em $\mathbb{R}^3$ é dada aqui concretamente por

$$\Big(\mathcal{B}_{(R,\,\vec{x})}f\Big)(\vec{y}) \;=\; f\Big(R\vec{y}+\vec{x}\Big)\,. \tag{2.91}$$

Compare com (2.90). ⧫

**Exemplo 2.24** Um segundo exemplo relevante é aquele no qual temos dois grupos $G$ e $N$ com $N \lhd G$. Em $G\circledS N$ temos o produto (2.82), sendo $\alpha_g(n) = gng^{-1}$. A correspondente ação à esquerda (2.85) de $G\circledS N$ em $N$ é dada por

$$A_{(g,\,n)}(n') \;=\; ngn'g^{-1}\,.$$

A correspondente ação $\mathcal{A}_{(g,\,n)}$ de $G\circledS N$ nas funções definidas em $N$ é, de acordo com (2.88),

$$\Big(\mathcal{A}_{(g,\,n)}f\Big)(n') \;=\; f\Big(g^{-1}n^{-1}n'g\Big)\,.$$

A ação à direita (2.89) de $G\circledS N$ nas funções definidas em $N$ é dada aqui por

$$\Big(\mathcal{B}_{(g,\,n)}f\Big)(n') \;=\; f\Big(ngn'g^{-1}\Big)\,.$$

⧫

### 2.2.4.3 Produtos Tensoriais de Grupos Abelianos

Uma outra construção muito importante que podemos fazer com grupos é a do seu *produto tensorial*. Aqui trataremos especificamente de produtos tensoriais de grupos Abelianos. Com essa construção podemos definir produtos tensoriais de espaços vetoriais, um objeto de grande importância na Teoria de Grupos, na Álgebra, na Geometria Diferencial, na Topologia Algébrica, na Mecânica Clássica, na Mecânica Quântica e na Teoria da Relatividade Geral.

Começamos exibindo um exemplo-protótipo que ilustra as características definidoras dessa estrutura para passarmos, em seguida, à sua construção geral, primeiro no caso de dois grupos Abelianos e, depois, no caso de uma coleção finita

de grupos Abelianos. A importante construção de produtos tensoriais de espaços vetoriais será realizada na Seção 2.3.5, página 214, tendo por base o que apresentaremos na seção corrente.

Observamos também *en passant* que é possível definir produtos tensoriais de grupos não Abelianos[64], mas não trataremos desse tema na versão corrente destas Notas. Outra generalização importante, da qual também não trataremos aqui, é a de produtos tensoriais envolvendo uma coleção infinita de fatores. Esse último tema é particularmente sutil no contexto de espaços vetoriais topológicos.

Nota histórica. Aparentemente a noção de produto tensorial de espaços vetoriais foi introduzida por Gibbs[65], primeiramente para o espaço vetorial $\mathbb{R}^3$, em cerca de 1884[66], em um estudo sobre corpos deformáveis, e posteriormente generalizada por ele mesmo para espaços vetoriais de dimensão finita arbitrária[67]. Gibbs denominava seu produto o "produto indeterminado" de vetores. O termo *tensor* foi cunhado por Voigt[68][69]. O uso de tensores na Geometria Diferencial foi iniciado por Ricci[70] e por Levi-Civita[71]. Os trabalhos de ambos influenciaram Einstein[72] que introduziu de forma central a noção de tensor na Teoria da Relatividade Geral. A versão que aqui apresentamos da construção de produtos vetoriais de grupos Abelianos e de módulos origina-se nos livros de Álgebra de Bourbaki [71]. ♣

## • Um exemplo-protótipo de um produto tensorial de grupos Abelianos

Sejam $A$ e $B$ dois conjuntos não vazios e sejam $\mathcal{A} := \mathbb{Z}^A$ e $\mathcal{B} := \mathbb{Z}^B$ as coleções de todas as funções definidas em $A$ e em $B$, respectivamente, e assumindo valores em $\mathbb{Z}$, ou seja, $\mathcal{A} := \{f : A \to \mathbb{Z}\}$ e $\mathcal{B} := \{g : B \to \mathbb{Z}\}$.

É claro que tanto $\mathcal{A}$ quanto $\mathcal{B}$ são grupos Abelianos com relação à operação de soma de funções: $(f+g)(x) := f(x)+g(x)$, com o elemento neutro sendo a função identicamente nula e a inversa de uma função $f$ sendo a função $-f$, dada por $(-f)(x) := -f(x)$.

Vamos denotar por $f \otimes g : A \times B \to \mathbb{Z}$ a função produto de $f$ com $g$, ou seja, a função definida em $A \times B$ que a cada par $(a,\ b) \in A \times B$ associa o valor $f(a)g(b) \in \mathbb{Z}$:

$$\big(f \otimes g\big)(a,\ b) \ := \ f(a)g(b)\ .$$

A função $f \otimes g$ assim definida é um exemplo de um elemento de $\mathbb{Z}^{A\times B}$: a coleção de todas as funções definidas em $A \times B$ assumindo valores em $\mathbb{Z}$, ou seja, $\mathbb{Z}^{A\times B} := \{F : A \times B \to \mathbb{Z}\}$. Dentro de $\mathbb{Z}^{A\times B}$, que também é um grupo Abeliano de funções, vamos destacar um subgrupo específico: o das funções que podem ser escritas como uma soma **finita** de funções do tipo $f \otimes g$ com $f \in \mathcal{A}$ e $g \in \mathcal{B}$. Esse subgrupo é denotado por $\mathcal{A} \otimes \mathcal{B}$ e é denominado o *produto tensorial (algébrico)* dos grupos Abelianos $\mathcal{A}$ e $\mathcal{B}$.

$\mathcal{A} \otimes \mathcal{B}$ é o conjunto de todas as funções definidas em $A \times B$ com valores em $\mathbb{Z}$ e que sejam da forma $\displaystyle\sum_{k=1}^{N} f_k(a)g_k(b)$, para algum $N \in \mathbb{N}$, arbitrário, e funções $f_k \in \mathcal{A}$ e $g_k \in \mathcal{B}$, também arbitrárias. As $N$ funções $f_1,\ \ldots,\ f_N$ não precisam ser todas distintas, nem as $N$ funções $g_1,\ \ldots,\ g_N$. Assim, com esse entendimento, escrevemos

$$\mathcal{A} \otimes \mathcal{B} \ := \ \left\{ \sum_{k=1}^{N} f_k \otimes g_k, \ \text{ com } N \in \mathbb{N}, \text{ arbitrário e } f_k \in \mathcal{A},\ g_k \in \mathcal{B}, \text{ arbitrárias} \right\} .$$

É claro que $\mathcal{A} \otimes \mathcal{B}$ compõe um grupo Abeliano (um subgrupo de $\mathbb{Z}^{A\times B}$), pois a soma de dois elementos de $\mathcal{A} \otimes \mathcal{B}$ é novamente um elemento de $\mathcal{A} \otimes \mathcal{B}$ (por ser novamente uma soma finita de produtos de funções).

Sobre essas operações de soma e produto em $\mathcal{A} \otimes \mathcal{B}$ vale fazer algumas observações muito importantes. Para produtos de funções em $\mathbb{Z}$ valem as bem-conhecidas regras de fatoração

$$f(a)g_1(b) + f(a)g_2(b) \ = \ f(a)\big(g_1(b) + g_2(b)\big) \qquad \text{e} \qquad f_1(a)g(b) + f_2(a)g(b) \ = \ \big(f_1(a) + f_2(a)\big)g(b)\ .$$

[64] O trabalho original sobre o assunto é: Ronald Brown and Jean-Louis Loday *"Van Kampen theorems for diagrams of spaces"*, Topology, **26**, Number 3, 311–335 (1987).

[65] Josiah Willard Gibbs (1839–1903).

[66] J. W. Gibbs, "Elements of Vector Analysis Arranged for the Use of Students in Physics", Tuttle, Morehouse & Taylor, New Haven, 1884.

[67] J. W. Gibbs, "On Multiple Algebra", Proceedings of the American Association for the Advancement of Science, 35 (1886). Disponível em http://archive.org/details/onmultiplealgeb00gibbgoog

[68] Woldemar Voigt (1850–1919).

[69] W. Voigt, "Die fundamentalen physikalischen Eigenschaften der Krystalle in elementarer Darstellung" Verlag von Veit & Comp., Leipzig, 1898

[70] Gregorio Ricci Curbastro (1853–1925).

[71] Tullio Levi-Civita (1873–1941).

[72] Albert Einstein (1879–1955).

Em notação de produto tensorial, elas ficam

$$f \otimes g_1 + f \otimes g_2 \;=\; f \otimes (g_1 + g_2)\,, \tag{2.92}$$

$$f_1 \otimes g + f_2 \otimes g \;=\; (f_1 + f_2) \otimes g\,. \tag{2.93}$$

A ideia central da construção do produto tensorial de dois grupos Abelianos quaisquer é produzir um novo grupo que satisfaça as mesmas regras do grupo de funções $\mathcal{A} \otimes \mathcal{B}$, em especial, as regras (2.92)–(2.93).

• **A noção "intuitiva" de produto tensorial de dois grupos**

Para efeito de comparação, recordemos a noção de soma direta de dois grupos Abelianos, introduzida na Seção 2.2.4.1, página 185. Sejam $A$ e $B$ dois grupos Abelianos, cujos elementos neutros denotaremos por identidades $0_A$ e $0_B$, respectivamente, e cujas operações de produto denotaremos ambas pelo mesmo símbolo: "+". Desejamos encontrar uma maneira de fazer do produto Cartesiano $A \times B$ um grupo também. Uma maneira de fazer isso é definir a "soma" de dois pares ordenados $(a,\ b)$, $(a',\ b') \in A \times B$ por

$$\big(a,\ b\big) + \big(a',\ b'\big) \;:=\; \big(a + a',\ b + b'\big)\,. \tag{2.94}$$

O leitor pode facilmente constatar que essa operação é uma operação binária de $A \times B$ em si mesmo, que ela é associativa, que tem por elemento neutro o par $(0_A,\ 0_B)$ e que para cada $(a,\ b) \in A \times B$ a inversa é $(a,\ b)^{-1} = (-a,\ -b)$, onde $-a$ é o elemento inverso de $a$ em $A$, e analogamente para $-b$. Portanto, com esse produto, $A \times B$ é um grupo Abeliano, denominado *soma direta de $A$ e $B$* ou *produto direto de $A$ e $B$*[73] e denotado pelo símbolo $A \oplus B$. Com essa estrutura de grupo em mente, os pares ordenados $(a,\ b)$ são frequentemente denotados pelo símbolo $a \oplus b$.

A definição de produto tensorial de dois grupos Abelianos $A$ e $B$, que denotaremos por $A \otimes B$, é distinta da de soma direta. O ponto de partida é o mesmo: o produto Cartesiano $A \times B$, mas a regra de produto a ser construída é muito diferente daquela dada em (2.94). Em primeiro lugar, os elementos de $A \otimes B$ são somas formais finitas de pares ordenados de $A \times B$, como $(a,\ b) + (a',\ b')$, mas não impomos a relação (2.94). O que realmente entendemos por "soma formal" será precisado adiante, fazendo uso do conceito de grupo Abeliano livremente gerado por um conjunto, uma noção introduzida na Seção 2.2.3, página 184. Por ora fiquemos apenas com a noção intuitiva. Para dar a $A \otimes B$ uma estrutura de grupo, desejamos impor algumas condições às somas formais acima. Primeiramente impomos que

$$(a,\ b) + (a',\ b') \;=\; (a',\ b') + (a,\ b)\,,$$

para todos $a,\ a' \in A$, $b,\ b' \in B$. Em segundo lugar impomos, sob a inspiração de (2.92)–(2.93), que valham

$$(a + a',\ b) \;=\; (a,\ b) + (a',\ b) \qquad \text{e} \qquad (a,\ b + b') \;=\; (a,\ b) + (a,\ b')$$

para todos $a,\ a' \in A$, $b,\ b' \in B$. O estudante deve notar que essas imposições são distintas daquelas de (2.94).

**E. 2.101** *Exercício*. Mostre que com as regras de soma dadas acima todos os pares $(0_A,\ b)$ e $(a,\ 0_B)$ são identificados entre si e com o elemento neutro da operação de soma de pares ordenados. Fora isso, o elemento inverso de um par $(a,\ b)$ é $(-a,\ b) = (a,\ -b)$. Mostre que, com isso, $A \otimes B$ é um grupo Abeliano, denominado *Produto Tensorial dos Grupos Abelianos* $A$ e $B$. ✠

Com essa estrutura de grupo em mente, os pares ordenados $(a,\ b)$ são frequentemente denotados pelo símbolo $a \otimes b$.

Passemos agora à formalização dessas ideias. A definição geral abstrata de produtos tensoriais de uma coleção finita de grupos Abelianos faz uso do conceito de grupo livremente gerado por um conjunto, noção discutida na Seção 2.2.3, página 184. Usaremos a notação lá empregada. Comecemos com o caso de dois grupos Abelianos para passarmos depois ao caso de uma coleção finita de grupos Abelianos.

• **O produto tensorial de dois grupos Abelianos**

Aqui faremos uso da construção do grupo Abeliano livremente gerado por um conjunto módulo relações, introduzida à página 184.

Sejam $A_1$ e $A_2$ dois grupos Abelianos cujos elementos neutros são $0_1$ e $0_2$, respectivamente, e cujos produtos de grupo denotaremos aditivamente: com o símbolo $+$. Seja $X = A_1 \times A_2$ e seja $\mathsf{F}(X) = \mathsf{F}(A_1 \times A_2)$ o grupo Abeliano livremente

[73] A distinção entre produto direto e soma direta só se faz quando uma coleção não finita de grupos é envolvida. Vide Seção 2.2.4.1, página 185.

gerado por $X = A_1 \times A_2$ (a noção de grupo Abeliano livremente gerado por um conjunto foi apresentada na Seção 2.2.3, página 184). Seja em $\mathsf{F}(X)$ o conjunto $\mathcal{R}$ de relações, dado por

$$\mathcal{R} \;:=\; \Big\{ r \in \mathsf{F}(X) \Big| \; r = (a_1 + a_1',\, a_2) - (a_1,\, a_2) - (a_1',\, a_2) \\ \text{ou } r \;=\; (a_1,\, a_2 + a_2') - (a_1,\, a_2) - (a_1,\, a_2') \;,\; \text{com } a_1,\, a_1' \in A_1 \text{ e } a_2,\, a_2' \in A_2 \Big\} \;. \tag{2.95}$$

Seja $\mathsf{R}(\mathcal{R})$ o subgrupo do grupo Abeliano $\mathsf{F}(A_1 \times A_2)$ composto por todas as combinações lineares finitas com coeficientes inteiros de elementos de $\mathcal{R}$. Como $\mathsf{R}(\mathcal{R}) \lhd \mathsf{F}(A_1 \times A_2)$, chegamos à definição do grupo Abeliano $A_1 \otimes A_2$, o *produto tensorial (algébrico)* dos grupos Abelianos $A_1$ e $A_2$:

$$A_1 \otimes A_2 \;:=\; \mathsf{F}(A_1 \times A_2)/\mathsf{R}(\mathcal{R}) \;.$$

*Notação.* Para $a_1 \in A_1$ e $a_2 \in A_2$ denotaremos por $a_1 \otimes a_2$ o elemento de $A_1 \otimes A_2$ que corresponde (na notação discutida acima) à função $\delta_{(a_1,\, a_2)}$. Ou seja, $a_1 \otimes a_2$ denota a classe de equivalência $[\delta_{(a_1,\, a_2)}]$ para as relações de equivalência definidas pelo subgrupo $\mathsf{R}(\mathcal{R})$. ◀

Pela definição do grupo livremente gerado $\mathsf{F}(A_1 \times A_2)$, pela construção do quociente $\mathsf{F}(A_1 \times A_2)/\mathsf{R}(\mathcal{R})$ e com uso dessa notação, um elemento geral de $A_1 \otimes A_2 := \mathsf{F}(A_1 \times A_2)/\mathsf{R}(\mathcal{R})$ é dado por uma combinação linear finita, com coeficientes inteiros, de elementos do tipo $a_1 \otimes a_2$, ou seja, um elemento de $A_1 \otimes A_2$ é da forma

$$\sum_{i=1}^{N} c_i \, a_1^{(i)} \otimes a_2^{(i)} \;, \tag{2.96}$$

com $N \in \mathbb{N}$ arbitrário, com $c_i \in \mathbb{Z}$ para cada $i = 1,\, \ldots,\, N$ e com $a_1^{(1)},\, \ldots,\, a_1^{(N)}$ elementos de $A_1$ e $a_2^{(1)},\, \ldots,\, a_2^{(N)}$ elementos de $A_2$.

Também com essa mesma notação, valem pela construção as seguintes regras:

$$(a_1 + a_1') \otimes a_2 \;=\; a_1 \otimes a_2 + a_1' \otimes a_2 \qquad \text{e} \qquad a_1 \otimes (a_2 + a_2') \;=\; a_1 \otimes a_2 + a_1 \otimes a_2' \;,$$

para todos $a_1,\, a_1' \in A_1$ e todos $a_2,\, a_2' \in A_2$.

É importante que façamos alguns comentários sobre o elemento neutro de $A_1 \otimes A_2 := \mathsf{F}(A_1 \times A_2)/\mathsf{R}(\mathcal{R})$. Seja $0_1$ o elemento neutro de $A_1$ e $0_2$ o elemento neutro de $A_2$. Afirmamos primeiramente que todos os elementos da forma $a_1 \otimes 0_2$ são idênticos. De fato, vale que $(a_1,\, a_2) - (a_1,\, a_2) = 0$ para quaisquer $a_1 \in A_1$, $a_2 \in A_2$, pois o lado esquerdo representa a função $\delta_{(a_1,\, a_2)} - \delta_{(a_1,\, a_2)}$, que é trivialmente nula. Assim, podemos escrever $(a_1,\, 0_2) = (a_1,\, 0_2) + (a_1,\, a_2) - (a_1,\, a_2) = (a_1,\, 0_2) + (a_1,\, a_2) - (a_1,\, 0_2 + a_2)$. Agora, o lado direito é claramente um elemento de $\mathsf{R}(\mathcal{R})$ e, portanto, estabelecemos que $(a_1,\, 0_2) \in \mathsf{R}(\mathcal{R})$ para qualquer $a_1 \in A_1$. Assim, todos os elementos da forma $(a_1,\, 0_2)$ pertencem à mesma classe de equivalência e, consequentemente, temos $a_1 \otimes 0_2 = a_1' \otimes 0_2$ para quaisquer $a_1,\, a_1' \in A_1$. Em particular, vale $a_1 \otimes 0_2 = 0_1 \otimes 0_2$ para qualquer $a_1 \in A_1$.

De forma totalmente análoga pode-se provar que $0_1 \otimes a_2 = 0_1 \otimes a_2'$ para quaisquer $a_2,\, a_2' \in A_2$. Em particular, vale $0_1 \otimes a_2 = 0_1 \otimes 0_2$ para qualquer $a_2 \in A_2$. Com isso, estabelecemos que $0_1 \otimes a_2 = 0_1 \otimes 0_2 = a_1 \otimes 0_2$ para quaisquer $a_1 \in A_1$, $a_2 \in A_2$.

É fácil agora ver que $0_1 \otimes 0_2$ é o elemento neutro de $A_1 \otimes A_2$. De fato, tomemos um elemento de $A_1 \otimes A_2$ da forma $a_1 \otimes a_2$. Temos que

$$a_1 \otimes a_2 + 0_1 \otimes 0_2 \;=\; a_1 \otimes a_2 + 0_1 \otimes a_2 \;=\; (a_1 + 0_1) \otimes a_2 \;=\; a_1 \otimes a_2 \;.$$

(Acima, na primeira igualdade, usamos a identificação $0_1 \otimes 0_2 = 0_1 \otimes a_2$ estabelecida acima). Como um elemento geral de $A_1 \otimes A_2$ é uma soma finita de elementos do tipo $a_1 \otimes a_2$, concluímos que $0_1 \otimes 0_2$ é o elemento neutro de $A_1 \otimes A_2$.

Tratemos agora da inversa de um elemento do tipo $a_1 \otimes a_2 \in A_1 \otimes A_2$. Afirmamos que essa inversa, que denotamos por $-(a_1 \otimes a_2)$ é dada por $(-a_1) \otimes a_2$ ou por $a_1 \otimes (-a_2)$, as quais são elementos idênticos de $A_1 \otimes A_2$.

De fato, temos

$$a_1 \otimes a_2 + (-a_1) \otimes a_2 \;=\; \big(a_1 + (-a_1)\big) \otimes a_2 \;=\; 0_1 \otimes a_2 \;=\; 0_1 \otimes 0_2$$

e, analogamente,

$$a_1 \otimes a_2 + a_1 \otimes (-a_2) \;=\; a_1 \otimes \big(a_2 + (-a_2)\big) \;=\; a_1 \otimes 0_2 \;=\; 0_1 \otimes 0_2 \;.$$

Isso estabelece que tanto $(-a_1)\otimes a_2$ quanto $a_1\otimes(-a_2)$ são o elemento inverso de $a_1\otimes a_2$ e, consequentemente, pela unicidade do elemento inverso em um grupo, temos *a fortiori* $(-a_1)\otimes a_2 = a_1\otimes(-a_2)$ para quaisquer $a_1\in A_1$, $a_2\in A_2$.

**E. 2.102** *Exercício.* Prove a identidade $(-a_1)\otimes a_2 = a_1\otimes(-a_2)$ mostrando que $(-a_1,\ a_2)-(a_1,\ -a_2)$ é um elemento de R. Escreva,

$$(-a_1,\ a_2)-(a_1,\ -a_2) \;=\; \Big[(-a_1,\ a_2)+(a_1,\ a_2)-(0_1,\ a_2)\Big]-\Big[(a_1,\ a_2)+(a_1,\ -a_2)-(a_1,\ 0_2)\Big]$$
$$+(0_1,\ a_2)-(0_1,\ 0_2)+(0_1,\ 0_2)-(a_1,\ 0_2)\,,$$

constate que os termos entre colchetes são elementos de $\mathcal{R}$ e use o fato provado acima que $(0_1,\ a_2)$, $(0_1,\ 0_2)$ e $(a_1,\ 0_2)$ são também elementos de R($\mathcal{R}$). ✠

Comentemos, por fim, que podemos convencionar uma simplificação ligeira para a representação (2.96) de um elemento geral de $A_1\otimes A_2$. Usando as regras acima expostas podemos escrever,

$$n\big(a_1\otimes a_2\big) \;=\; (na_1)\otimes a_2 \;=\; a_1\otimes(na_2)\,,$$

para $n\in\mathbb{Z}$, $a_1\in A_1$ e $a_2\in A_2$, onde, como sempre, se faz em um grupo Abeliano $na_k := \pm(\underbrace{a_k+\cdots+a_k}_{|n|\text{ vezes}})$ para $n\neq 0$, com $\pm$ sendo o sinal de $n$, e $na_k = 0_k$ caso $n=0$. Tendo isso em mente, um elemento geral de $A_1\otimes A_2$ pode ser sempre escrito na forma de uma soma finita do tipo

$$\sum_{i=1}^{N} a_1^{(i)}\otimes a_2^{(i)}\,, \tag{2.97}$$

para algum $N\in\mathbb{N}$ e alguns $a_1^{(i)}\in A_1$, $a_2^{(i)}\in A_2$, ao invés da representação (2.96), absorvendo, portanto, os coeficientes inteiros $c_i$ nos produtos tensoriais $a_1^{(i)}\otimes a_2^{(i)}$.

*

Em resumo, temos o seguinte quadro: se $A_1$ e $A_2$ são grupos Abelianos com elementos neutros $0_1$ e $0_2$, respectivamente, então:

1. $A_1\otimes A_2$ é um grupo Abeliano cujos elementos são somas finitas da forma $\displaystyle\sum_{i=1}^{N} a_1^{(i)}\otimes a_2^{(i)}$, com $N\in\mathbb{N}$, arbitrário, sendo $a_1^{(1)},\ \ldots,\ a_1^{(N)}$ elementos arbitrários de $A_1$ e $a_2^{(1)},\ \ldots,\ a_2^{(N)}$ sendo elementos arbitrários de $A_2$.
2. Valem as regras
$$(a_1+a_1')\otimes a_2 \;=\; a_1\otimes a_2 + a_1'\otimes a_2 \qquad\text{e}\qquad a_1\otimes(a_2+a_2') \;=\; a_1\otimes a_2 + a_1\otimes a_2'$$
para todos $a_1,\ a_1'\in A_1$ e todos $a_2,\ a_2'\in A_2$.
3. O elemento neutro de $A_1\otimes A_2$ é $0_1\otimes 0_2$ e valem as identificações $0_1\otimes a_2 = 0_1\otimes 0_2 = a_1\otimes 0_2$ para quaisquer $a_1\in A_1$, $a_2\in A_2$.
4. A inversa de um elemento $a_1\otimes a_2$ é $(-a_1)\otimes a_2 = a_1\otimes(-a_2)$. A inversa de um elemento geral $\displaystyle\sum_{i=1}^{N} a_1^{(i)}\otimes a_2^{(i)}$ é $\displaystyle\sum_{i=1}^{N}\big(-a_1^{(i)}\big)\otimes a_2^{(i)} = \sum_{i=1}^{N} a_1^{(i)}\otimes\big(-a_2^{(i)}\big)$.

• **O produto tensorial de uma coleção finita de grupos Abelianos**

A construção acima pode agora ser facilmente generalizada para o caso de uma coleção finita $A_1,\ \ldots,\ A_n$ de grupos Abelianos. Vamos listar os fatos principais, cujas demonstrações são idênticas às do caso do produto tensorial de dois grupos, como apresentado acima.

Como acima, consideramos $X = A_1 \times \cdots \times A_n$. Seja em $\mathsf{F}(X) = \mathsf{F}(A_1 \times \cdots \times A_n)$ o conjunto $\mathcal{R}$ de relações dado por $\mathcal{R} = \bigcup_{k=1}^{n} \mathcal{R}_k$, onde

$$\mathcal{R}_k \;:=\; \Big\{ r \in \mathsf{F}(X) |\; r = (a_1,\, \ldots,\, a_{k-1},\, a_k + a'_k,\, a_{k+1},\, \ldots,\, a_n)$$

$$- (a_1,\, \ldots,\, a_{k-1},\, a_k,\, a_{k+1},\, \ldots,\, a_n) - (a_1,\, \ldots,\, a_{k-1},\, a'_k,\, a_{k+1},\, \ldots,\, a_n)\,,$$

$$\text{com } a_j \in A_j \text{ para todo } j = 1,\, \ldots,\, n \text{ e } a'_k \in A_k \Big\}\,.$$

Seja $\mathsf{R}(\mathcal{R})$ o subgrupo de $\mathsf{F}(A_1 \times \cdots \times A_n)$ composto por todas as combinações lineares finitas com coeficientes inteiros de elementos de $\mathcal{R}$. Como antes, temos que $\mathsf{R}(\mathcal{R})$ é um subgrupo normal de $\mathsf{F}(A_1 \times \cdots \times A_n)$, já que este é Abeliano. Chegamos assim à definição do grupo Abeliano $A_1 \otimes \cdots \otimes A_n$, o *produto tensorial* de $A_1,\, \ldots,\, A_n$, que é definido como

$$A_1 \otimes \cdots \otimes A_n \;:=\; \mathsf{F}(A_1 \times \cdots \times A_n)/\mathsf{R}(\mathcal{R})\,.$$

Denotamos por $a_1 \otimes \cdots \otimes a_n$ a classe de equivalência de $\delta_{(a_1,\, \ldots,\, a_n)}$, com $a_k \in A_k$ para cada $k$. Os elementos de $A_1 \otimes \cdots \otimes A_n$ são somas finitas de elementos como $a_1 \otimes \cdots \otimes a_n$, com $a_k \in A_k$ para cada $k$. Valem as regras

$$\begin{array}{ccccc}
a_1 \otimes a_2 \otimes \cdots \otimes a_{n-1} \otimes a_n & + & a'_1 \otimes a_2 \otimes \cdots \otimes a_{n-1} \otimes a_n & = & (a_1 + a'_1) \otimes a_2 \otimes \cdots \otimes a_{n-1} \otimes a_n\,, \\
\vdots & & \vdots & & \\
\vdots & & \vdots & & \\
a_1 \otimes a_2 \otimes \cdots \otimes a_{n-1} \otimes a_n & + & a_1 \otimes a_2 \otimes \cdots \otimes a_{n-1} \otimes a'_n & = & a_1 \otimes a_2 \otimes \cdots \otimes a_{n-1} \otimes (a_n + a'_n)\,,
\end{array}$$

para todos $a_k,\, a'_k \in A_k$, $k = 1,\, \ldots,\, n$.

O elemento neutro de $A_1 \otimes \cdots \otimes A_n$ é da forma $0_1 \otimes \cdots \otimes 0_n$, onde para cada $k$, $0_k$ é o elemento neutro de $A_k$, sendo ainda que vale a igualdade

$$0_1 \otimes \cdots \otimes 0_n \;=\; 0_1 \otimes a_2 \otimes \cdots \otimes a_n \;=\; \cdots \;=\; a_1 \otimes \cdots \otimes a_{n-1} \otimes 0_n\,, \tag{2.98}$$

com cada $a_k$ sendo um elemento arbitrário de $A_k$, para todo $k$. Isso se vê do fato que valem

$$\begin{array}{ccccccc}
a_1 \otimes a_2 \otimes \cdots \otimes a_n + 0_1 \otimes a_2 \otimes \cdots \otimes a_n & = & (a_1 + 0_1) \otimes a_2 \otimes \cdots \otimes a_n & = & a_1 \otimes a_2 \otimes \cdots \otimes a_n\,, \\
\vdots & \vdots & \vdots & \vdots & \vdots & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & & \\
a_1 \otimes a_2 \otimes \cdots \otimes a_n + a_1 \otimes a_2 \otimes \cdots \otimes 0_n & = & a_1 \otimes a_2 \otimes \cdots \otimes (a_n + 0_n) & = & a_1 \otimes a_2 \otimes \cdots \otimes a_n\,.
\end{array}$$

As igualdades em (2.98) seguem da unicidade do elemento neutro de um grupo. Como facilmente se constata, a inversa de um elemento da forma $a_1 \otimes a_2 \otimes \cdots \otimes a_n$ é

$$-\big(a_1 \otimes a_2 \otimes \cdots \otimes a_n\big) \;=\; (-a_1) \otimes a_2 \otimes \cdots \otimes a_n \;=\; \cdots \;=\; a_1 \otimes \cdots \otimes a_{n-1} \otimes (-a_n)\,,$$

onde $-a_k$ é a inversa de $a_k$ em $A_k$. Novamente, as igualdades acima seguem da unicidade da inversa em um grupo.

Como discutimos no caso de somas diretas, os grupos $A_1 \otimes (A_2 \otimes A_3)$, $(A_1 \otimes A_2) \otimes A_3$ e $A_1 \otimes A_2 \otimes A_3$ são isomorfos, com os isomorfismos canônicos definidos por

$$\varphi_1 : A_1 \otimes (A_2 \otimes A_3) \;\to\; A_1 \otimes A_2 \otimes A_3\,, \qquad \varphi_1\left(\sum_k \alpha_k\, a_1^k \otimes \big(a_2^k \otimes a_3^k\big)\right) \;:=\; \sum_k \alpha_k\, a_1^k \otimes a_2^k \otimes a_3^k\,,$$

$$\varphi_2 : (A_1 \otimes A_2) \otimes A_3 \;\to\; A_1 \otimes A_2 \otimes A_3\,, \qquad \varphi_2\left(\sum_k \alpha_k\, \big(a_1^k \otimes a_2^k\big) \otimes a_3^k\right) \;:=\; \sum_k \alpha_k\, a_1^k \otimes a_2^k \otimes a_3^k\,,$$

e analogamente para o caso em que se tem uma coleção maior de fatores. Acima, $\alpha_k \in \mathbb{Z}$ e $a_i^k \in A_i$ para todo $i$ e $k$, as somas em $k$ sendo, naturalmente, finitas.

**E. 2.103** *Exercício*. Mostre que $\varphi_1$ e $\varphi_2$, definidos acima, são, de fato, isomorfismos de grupo. ✠

**E. 2.104** *Exercício*. Sejam $A$ e $B$ grupos Abelianos. Mostre que $A \otimes B$ e $B \otimes A$ são grupos isomorfos, com o isomorfismo $\varphi : A \otimes B \to B \otimes A$ dado por $\varphi\big(a \otimes b\big) := \big(b \otimes a\big)^{-1} = -b \otimes a$. ✠

**E. 2.105** *Exercício (desafio).* Mostre que para quaisquer $m,\ n \in \mathbb{N}$ os grupos $\mathbb{Z}_m \otimes \mathbb{Z}_n$ e $\mathbb{Z}_{\mathrm{mdc}(m,\,n)}$ são isomorfos. Aqui, $\mathrm{mdc}(m,\,n)$ é o máximo divisor comum entre $m$ e $n$. ✠

**E. 2.106** *Exercício*. Sejam $A$, $B$ e $C$ grupos Abelianos. Demonstre a validade da propriedade distributiva $A \otimes (B \oplus C) = \big(A \oplus B\big) \otimes \big(A \oplus C\big)$. Mostre que essa propriedade se estende para somas diretas arbitrárias de grupos Abelianos: $A \otimes \Big(\oplus_{\lambda \in \Lambda} B_\Lambda\Big) = \oplus_{\lambda \in \Lambda} \big(A \otimes B_\Lambda\big)$. ✠

## 2.2.5 O Produto Livre de Grupos. Amálgamas

Vamos aqui apresentar mais duas construção possíveis de serem feitas com dois grupos arbitrários, o chamado *produto livre* e o chamado *amálgama de dois grupos por homomorfismos*. As definições que apresentaremos podem ser estendidas a qualquer coleção finita de grupos. As noções de produto livre e amálgamas de grupos são úteis, por exemplo, na Topologia Algébrica, como no estudo de grupos de homotopia de espaços topológicos [526].

• **O produto livre de dois grupos**

Sejam $G$ e $H$ dois grupos (não necessariamente Abelianos) com elementos neutros $e_G$ e $e_H$, respectivamente. Uma *palavra* de comprimento $n \in \mathbb{N}_0$ gerada por $G$ e $H$ vem a ser uma sequência finita $(x_1,\ \ldots,\ x_n)$ na união disjunta $G \sqcup H$, com as seguintes propriedades:

1. A palavra de comprimento $n = 0$ é vazia e denotada por $()$.
2. Para $n \in \mathbb{N}$, os elementos sucessivos de $(x_1,\ \ldots,\ x_n)$ pertencem a grupos diferentes. Assim, para $j \in \{1,\ \ldots,\ n-1\}$, se $x_j \in G$ tem-se $x_{j+1} \in H$ e vice-versa: se $x_j \in H$ tem-se $x_{j+1} \in G$.
3. Nenhum elemento de $(x_1,\ \ldots,\ x_n)$ é igual aos elementos neutros $e_G$ ou $e_H$.

Denotamos por $\mathscr{F}_n(G,\ H)$ a coleção de todas as palavras de comprimento $n \in \mathbb{N}_0$ geradas por $G$ e $H$. Denotamos por $\mathscr{F}(G,\ H)$ a coleção de todas as palavras geradas por $G$ e $H$, ou seja, $\mathscr{F}(G,\ H) = \bigcup\limits_{n \in \mathbb{N}_0} \mathscr{F}_n(G,\ H)$.

**E. 2.107** *Exercício simples.* Constate que $\mathscr{F}(G,\ H)$ é idêntico a $\mathscr{F}(H,\ G)$ ✠

Podemos definir um produto em $\mathscr{F}(G,\ H)$ por meio das seguintes regras:

1. Para a palavra vazia tem-se $() \cdot () := ()$.
2. Para todo $n \in \mathbb{N}$ vale $() \cdot (x_1,\ \ldots,\ x_n) = (x_1,\ \ldots,\ x_n) \cdot () := (x_1,\ \ldots,\ x_n)$.
3. Para duas palavras de comprimento 1, tem-se

$$(x_1) \cdot (y_1) \ := \ \begin{cases} (x_1,\ y_1), & \text{caso } x_1 \text{ e } y_1 \text{ pertençam a grupos distintos.} \\ (x_1 y_1), & \text{caso } x_1 \text{ e } y_1 \text{ pertençam ao mesmo grupo e } x_1 \neq y_1^{-1}. \\ (), & \text{caso } x_1 \text{ e } y_1 \text{ pertençam ao mesmo grupo e } x_1 = y_1^{-1}. \end{cases}$$

4. Para os demais casos com $n \in \mathbb{N}$ e $m \in \mathbb{N}$ tem-se

$$(x_1,\, \ldots,\, x_n) \cdot (y_1,\, \ldots,\, y_m) \,:=$$

$$\begin{cases} (x_1,\, \ldots,\, x_n,\, y_1,\, \ldots,\, y_m), & \text{caso } x_n \text{ e } y_1 \text{ pertençam a grupos distintos.} \\ (x_1,\, \ldots,\, x_n y_1,\, \ldots,\, y_m), & \text{caso } x_n \text{ e } y_1 \text{ pertençam ao mesmo grupo e } x_n \neq y_1^{-1}. \\ (x_1,\, \ldots,\, x_{n-1},\, y_2\, \ldots,\, y_m), & \text{caso } x_n \text{ e } y_1 \text{ pertençam ao mesmo grupo e } x_n = y_1^{-1}. \end{cases}$$

Observe que em todos os casos resulta do produto um elemento de $\mathscr{F}(G,\, H)$, pois dois elementos sucessivos da sequência resultante sempre pertencem a grupos distintos e nela os elementos neutros $e_G$ ou $e_H$ nunca comparecem.

Observe também que o produto de um elemento de $\mathscr{F}_n(G,\, H)$ por um elemento de $\mathscr{F}_m(G,\, H)$ pode ser um elemento de $\mathscr{F}_{n+m}(G,\, H)$, de $\mathscr{F}_{n+m-1}(G,\, H)$ ou de $\mathscr{F}_{n+m-2}(G,\, H)$, dependendo do caso.

O produto assim definido é por vezes denominado *concatenação de palavras geradas por $G$ e $H$*.

**E. 2.108** *Exercício simples.* Verifique que o produto acima definido em $\mathscr{F}(G,\, H)$ é associativo, possui a palavra vazia () como elemento neutro e cada palavra não nula $(x_1,\, \ldots,\, x_n)$ tem como elemento inverso a palavra $\left(x_n^{-1},\, \ldots,\, x_1^{-1}\right)$. ✠

Dessa forma, o conjunto $\mathscr{F}(G,\, H)$ é um grupo com relação ao produto dado pela concatenação de palavras, acima definida. Esse grupo é dito ser o *produto livre dos grupos $G$ e $H$*, ou ainda o *produto livremente gerado pelos grupos $G$ e $H$*. O produto livre de $G$ e $H$ é também denotado por $G * H$, notação que passaremos a empregar.

**E. 2.109** *Exercício*. O grupo $G * H$ não é Abeliano (e é infinito), exceto se $G$ ou $H$ forem triviais e o outro for Abeliano (finito). Justifique essas afirmações. ✠

**E. 2.110** *Exercício (fácil).* Mostre que os subconjuntos de $G * H$ dados por

$$\tilde{G} \,:=\, \{()\} \cup \big\{(g),\, g \in G,\, g \neq e_G\big\} \qquad \text{e} \qquad \tilde{H} \,:=\, \{()\} \cup \big\{(h),\, h \in H,\, h \neq e_H\big\} \tag{2.99}$$

são subgrupos de $G * H$ e que esses subgrupos são isomorfos a $G$ e a $H$, respectivamente. ✠

**• Comentário sobre a notação**

Na literatura é frequente adotar-se uma notação diferente para as palavras e para o produto em $G * H$. Palavras como $(x_1,\, \ldots,\, x_n)$ são denotadas simplesmente por $x_1 \cdots x_n$, como se fossem um produto formal sucessivo dos elementos de $x_1$ a $x_n$. Esse produto é formal pois elementos sucessivos não pertencem ao mesmo grupo. O produto de duas palavras $(x_1,\, \ldots,\, x_n)$ e $(y_1,\, \ldots,\, y_m)$ fica $x_1 \cdots x_n y_1 \cdots y_m$, sendo que, caso $x_n$ e $y_1$ pertençam ao mesmo grupo, o fator $x_n y_1$ deve ser entendido como o produto de ambos nesse grupo e, caso $x_n y_1$ for o elemento neutro desse grupo, o fator $x_n y_1$ deve ser eliminado.

Evitamos usar essa notação pois há uma situação na qual ela pode ser ambígua: quando $G$ e $H$ forem o mesmo grupo ou forem subgrupos de um grupo maior. Nesse caso a expressão $x_1 \cdots x_n$ pode ser entendida como o produto em $G * H$ ou como o produto no grupo que lhes é comum.

**• Um exemplo: o grupo livremente gerado por dois elementos**

Seja $A$ um grupo com unidade $e_A$ dotado da seguinte propriedade: existe $a \in A$ tal que para nenhum $n \in \mathbb{N}$ vale $a^n = e_A$. É fácil checar que $A_1 := \{a^n,\, n \in \mathbb{Z}\}$ (convencionamos que $a^0 = e_A$) é um subgrupo de $A$ que é Abeliano, tem infinitos elementos e é isomorfo ao grupo $(\mathbb{Z},\, +)$. Verifique! Um grupo como $A_1$ é denominado *grupo cíclico infinito de um elemento gerado por $a \in A$*.

É um exercício muito fácil provar que todos os grupos cíclico infinitos gerados por um elemento são isomorfos.

Seja $B$ um outro grupo dotado de um outro grupo cíclico infinito de um elemento$B_1 := \{b^n,\, n \in \mathbb{Z}\}$. Nesse caso $A_1 * B_1$ é o grupo constituído por todas as palavras finitas formadas apenas pelas letras $a$ e $b$ e suas potências, tais como $a$, $b$, $a^5$, $b^{-7}$, $a^{-1}b$, $ba$, $ab^{-5}$, $b^3a^3$, $b^2a^{-2}b^7$ etc. O grupo $A_1 * B_1$ assim constituído é denominado *grupo livremente gerado por dois elementos*.

É um exercício muito fácil provar que todos os grupos livremente gerados por dois elementos são isomorfos. Tais grupos são por vezes denotados por $\mathsf{F}_2$. O primeiro grupo de homotopia do espaço composto por $\mathbb{R}^2$ menos dois pontos distintos quaisquer é isomorfo a um grupo livremente gerado por dois elementos, $\mathsf{F}_2$.

• **Extensão do produto livre para mais de dois grupos**

A construção acima do produto livre de dois grupos pode ser facilmente estendida para uma coleção finita de grupos. Se possuirmos três grupos $F$, $G$ e $H$, por exemplo, definimos palavras como sequências finitas $(x_1,\ \ldots,\ x_n)$ com cada $x_k$ pertencendo a um dos três grupos, onde dois elementos sucessivos nunca pertencem ao mesmo grupo e nunca comparecem os elementos neutros de $F$, $G$ e $H$. O produto de palavras é definido similarmente ao caso de dois grupos (e é também associativo), o elemento neutro é a sequência vazia () e a inversa de $(x_1,\ \ldots,\ x_n)$ é $\left(x_n^{-1},\ \ldots,\ x_1^{-1}\right)$.

• **Amálgamas de dois grupos por homomorfismos**

Sejam $G$ e $H$ dois grupos para os quais definimos o produto livre $G * H$, como acima. Vamos considerar que exista um terceiro grupo $U$, com elemento neutro $e_U$, e dois homomorfismos $\phi : U \to G$ e $\psi : U \to H$.

Considere-se agora o subconjunto de $G * H$ dado por $S_{\phi,\,\psi} := \left\{\left(\phi(u),\ \psi(u)^{-1}\right),\ u \in U,\ u \neq e_U\right\}$ e considere-se o subgrupo normal $N[S_{\phi,\,\psi}]$ de $G * H$ gerado por $S_{\phi,\,\psi}$ (para a definição de subgrupo normal gerado por um conjunto, vide página 174).

**Definição. Amálgama de dois grupos por homomorfismos.** O *amálgama dos grupos $G$ e $H$ pelos homomorfismos $\phi$ e $\psi$* é definido como o grupo quociente $(G * H)/N[S_{\phi,\,\psi}]$. ♠

O significado intuitivo de $(G * H)/N[S_{\phi,\,\psi}]$ é que trata-se de um grupo onde identificamos $N[S_{\phi,\,\psi}]$ com o elemento neutro, como se estivéssemos impondo as relações $\phi(u)\psi(u)^{-1} = e$, ou seja, $\phi(u) = \psi(u)$ para todo $u \in U$. Note-se que $\phi(u)$ e $\psi(u)$ pertencem a grupos distintos ($G$ e $H$), respectivamente.

A noção de amálgama de dois grupos por homomorfismos é relevante na Topologia Algébrica, como no estudo de grupos de homotopia de espaços topológicos [526].

A seguinte observação é relevante:

**Proposição 2.15** *Se $\phi : U \to G$ e $\psi : U \to H$ forem homomorfismos injetores, então os grupos $G$ e $H$ são isomorfos a dois subgrupos de $(G * H)/N[S_{\phi,\,\psi}]$.* □

Prova. Considere o subgrupo $\tilde{G}$ de $G * H$ definido em (2.99). Afirmamos que se $g_1$, $g_2$ são elementos de $G$, então $(g_1) \cdot (g_2)^{-1} = \left(g_1 g_2^{-1}\right)$ não é elemento de $N[S_{\phi,\,\psi}]$ caso $g_1 g_2^{-1} \neq e_G$, o que significa que $(g_1)$ e $(g_2)$ não pertencem à mesma classe de equivalência em $(G * H)/N[S_{\phi,\,\psi}]$.

Para provar a afirmação, observe que pela Proposição 2.6, página 174, os elementos de $N[S_{\phi,\,\psi}]$ são da forma $\left(x_1,\ \ldots,\ x_n\right) \cdot \left(\phi(u),\ \psi(u)^{-1}\right) \cdot \left(x_n^{-1},\ \ldots,\ x_1^{-1}\right)$.

Agora, $\left(g_1 g_2^{-1}\right)$ não pode ser da forma $\left(x_1,\ \ldots,\ x_n\right) \cdot \left(\phi(u),\ \psi(u)^{-1}\right) \cdot \left(x_n^{-1},\ \ldots,\ x_1^{-1}\right)$ caso $n \geq 2$, simplesmente pois essas palavras sempre têm comprimento maior que 1. Para $n = 1$, porém, temos elementos de $N[S_{\phi,\,\psi}]$ na forma $\left(x_1\right) \cdot \left(\phi(u),\ \psi(u)^{-1}\right) \cdot \left(x_1^{-1}\right)$. Como $\phi(u)$ e $\psi(u)$ pertencem a grupos diferentes, tais elementos só poderão estar em $\tilde{G}$ se $x_1 \in G$ e $\psi(u) = e_H$. Mas isso implica que $u = e_U$ (pela injetividade dos homomorfismos), implicando $\phi(u) = e_g$ (idem). Assim, os elementos $\left(x_1\right) \cdot \left(\phi(u),\ \psi(u)^{-1}\right) \cdot \left(x_1^{-1}\right)$ são forçosamente da forma $\left(x_1\right) \cdot () \cdot \left(x_1^{-1}\right) = ()$, não podendo, consequentemente, ser iguais a $\left(g_1 g_2^{-1}\right)$ caso $g_1 g_2^{-1} \neq e_G$.

O argumento para o subgrupo $\tilde{H}$ de $G * H$ é similar. Vemos assim imediatamente que $G$ e $H$ são isomorfos aos grupos das classes de equivalência $\{[(g)],\ g \in G\}$ e $\{[(h)],\ h \in H\}$, respectivamente. ■

# 2.3 Espaços Vetoriais. Estruturas e Construções Básicas

Nesta seção apresentaremos algumas estruturas e construções básicas da teoria dos espaços vetoriais. Discutiremos a noção de espaço quociente e apresentaremos duas maneiras distintas de construir espaços vetoriais a partir de uma coleção

dada de espaços vetoriais (sobre um mesmo corpo), a chamada *soma direta de espaços vetoriais* e o chamado *produto tensorial de espaços vetoriais*. Um comentário pertinente (destinado aos estudantes mais avançados) é que as construções que apresentaremos adiante correspondem às noções de soma direta e produto tensorial *algébricos*. Isso significa que outras estruturas, como uma topologia, ou propriedades, como completeza, não são necessariamente herdadas pela construção. Assim, por exemplo, o produto tensorial algébrico de dois espaços de Banach não é necessariamente um espaço de Banach. Para tal é necessário introduzir um completamento extra, que pode não ser único.

## 2.3.1 Bases Algébricas de um Espaço Vetorial

• **Dependência linear**

Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K}$. Um conjunto finito $u_1,\, \ldots,\, u_n \in V$ de vetores é dito ser *linearmente dependente* se existir um conjunto de escalares $\alpha_1,\, \ldots,\, \alpha_n \in \mathbb{K}$, nem todos nulos, tais que

$$\alpha_1 u_1 + \cdots + \alpha_n u_n \;=\; 0\,.$$

Um conjunto arbitrário de vetores é dito ser *linearmente independente* se não possuir nenhum subconjunto finito que seja linearmente dependente.

• **Combinações lineares**

Para um conjunto finito de vetores $\{u_1,\, \ldots,\, u_n\} \subset V$ e de escalares $\{\alpha_1,\, \ldots,\, \alpha_n\} \subset \mathbb{K}$, uma expressão como

$$\alpha_1 u_1 + \cdots + \alpha_n u_n$$

é dita ser uma *combinação linear* dos vetores $u_1,\, \ldots,\, u_n$.

• **Varredura linear**

Seja $C \subset V$ um conjunto de vetores. A *varredura linear* ("linear span") de $C$, denotado por span $(C)$ é o conjunto de todos os vetores de $V$ que podem ser escritos como uma combinação linear finita de elementos de $C$.

• **Bases algébricas em espaços vetoriais**

Aqui $I$ designa um conjunto arbitrário não vazio de índices.

Uma *base algébrica*, também denominada *base de Hamel*[74], em um espaço vetorial $V$ é um conjunto $B = \{b_i,\, i \in I\}$ de vetores linearmente independentes tais que span $(B) = V$ e tais que qualquer vetor $u$ de $V$ pode ser escrito de modo único como uma combinação linear finita de elementos de $B$.

Se $B$ é uma base algébrica, então para cada $u \in V$ existem univocamente definidos $\alpha_1,\, \ldots,\, \alpha_n \in \mathbb{K}$ e $i_1,\, \ldots,\, i_n \in I$ tais que:

$$u \;=\; \alpha_1 b_{i_1} + \cdots + \alpha_n b_{i_n}\,.$$

Os seguintes teoremas podem ser demonstrados com uso do Lema de Zorn (omitiremos as demonstrações aqui. Vide, por exemplo, [241]).

**Teorema 2.9** *Todo espaço vetorial $V$ possui uma base algébrica, exceto o espaço vetorial trivial $V = \{0\}$.* □

**Teorema 2.10** *Dado um espaço vetorial $V$ (não-trivial), todas as bases algébricas em $V$ têm a mesma cardinalidade.* □

• **Isomorfismos**

Dois espaços vetoriais $U$ e $V$ sobre o mesmo corpo $\mathbb{K}$ são ditos *isomorfos* se houver uma bijeção linear $\phi : U \to V$ entre ambos. A aplicação $\phi$ com tais propriedades é dita ser um isomorfismo de $U$ em $V$. Denota-se fato de dois espaços

[74] Georg Hamel (1877-1954). A referência original é G. Hamel, *"Eine Basis aller Zahlen und die unstetigen Lösungen der Funktionalgleichung $f(x+y) = f(x) + f(y)$"*. Math. Annalen, **60**, 459–462 (1905).

vetoriais $U$ e $V$ sobre o mesmo corpo $\mathbb{K}$ serem isomorfos por

$$U \simeq V .$$

Os fatos descritos no exercício seguinte são propriedades elementares importantes de isomorfismo.

**E. 2.111** *Exercício*. Demonstre as seguintes afirmações:

1. Sejam $U$ e $V$ dois espaços vetoriais sobre o mesmo corpo $\mathbb{K}$ e seja $\phi : U \to V$ um isomorfismo. Então $\phi^{-1} : V \to U$ é também um isomorfismo.
2. Sejam $U_1$, $U_2$ e $U_3$ espaços vetoriais sobre o mesmo corpo $\mathbb{K}$ e sejam $\phi_{12} : U_1 \to U_2$ e $\phi_{23} : U_2 \to U_3$ isomorfismos. Então $\phi_{23} \circ \phi_{12} : U_1 \to U_3$ é também um isomorfismo.

É evidente que todo espaço vetorial é isomorfo a si mesmo (o isomorfismo sendo a identidade). Esse fato e os resultados acima permitem ver que, dado um conjunto de espaços vetoriais sobre um mesmo corpo, então a relação de isomorfia é uma relação de equivalência nesse conjunto. Prove isso também. ✠

Para muitos propósitos, dois espaços isomorfos podem ser identificados. Esse tipo de identificação é recorrentemente empregada na literatura, muitas vezes sem maiores comentários.

### • Dimensão algébrica

Um espaço vetorial é dito ser de *dimensão algébrica finita* se possuir uma base algébrica finita. Se um espaço vetorial $V$ tem dimensão algébrica finita, sua *dimensão algébrica*, ou simplesmente *dimensão* é definida como sendo o número de elementos de sua base.

Nem todo espaço vetorial tem uma base algébrica finita (vide exemplos abaixo). A *dimensão algébrica* de um espaço vetorial é definida como sendo a cardinalidade de suas bases algébricas (pelo Teorema 2.10, acima, são todas iguais).

*Exemplo 1.* $V = \mathbb{C}^n$ sobre o corpo dos complexos ou $V = \mathbb{R}^n$ sobre o corpo dos reais. Tais são bem conhecidos exemplos-protótipo de espaços vetoriais de dimensão finita ($= n$).

Seja $\mathcal{P}$ = conjunto de todos os polinômios de uma variável real com coeficientes complexos: $P_n(t) \in \mathcal{P}$,

$$P_n(t) \;=\; a_n t^n + \cdots + a_1 t + a_0$$

com $t \in \mathbb{R}$, $a_i \in \mathbb{C}$, é dito ser um polinômio de grau $n$ se $a_n \neq 0$.

*Exemplo 2.* $V = \mathcal{P}$ sobre o corpo dos complexos. Este é claramente um espaço vetorial de dimensão infinita. $V$ possui uma base algébrica, a saber, o conjunto de todos os polinômios da forma $b_n = t^n$, $n = 0,\ 1,\ 2,\ \ldots$.

*Exemplo 3.* $V = \mathbb{R}$ sobre o corpo dos reais. O conjunto dos reais sobre o corpo dos reais é também um espaço vetorial de dimensão 1, a saber, uma possível base é formada pelo elemento 1: $B = \{1\}$, já que, obviamente, qualquer elemento $x \in \mathbb{R}$ pode ser escrito como $x = x \cdot 1$, com $x$ no corpo dos reais.

Esse exemplo pode parecer banal, e de fato o é, mas leva a um antiexemplo curioso que mostra que a dimensão algébrica de um espaço vetorial é também fortemente dependente do corpo de escalares utilizado.

*Exemplo 4.* $V = \mathbb{R}$ sobre o corpo dos racionais.

A surpresa aqui é que este **não** é um espaço vetorial de dimensão algébrica finita: não existe um conjunto finito $\{x_1,\ \ldots,\ x_m\}$ de números reais tais que todo $x \in \mathbb{R}$ possa ser escrito como

$$x \;=\; r_1 x_1 + \cdots + r_m x_m \ ,$$

onde os números $r_i$ são racionais. A razão é que, como $\mathbb{Q}$ é um conjunto contável, a coleção de números que se deixam escrever como o lado direito é uma coleção contável (tem a mesma cardinalidade de $\mathbb{Q}^m$). O conjunto $\mathbb{R}$, porém, não é contável.

Um resultado um tanto surpreendente diz, porém, que esse espaço vetorial possui uma base algébrica, ou seja, existe um conjunto $H \subset \mathbb{R}$ tal que para cada $x \in \mathbb{R}$ existe um conjunto finito $h_1,\ \ldots,\ h_n$ de elementos de $H$ e um conjunto finito de racionais $r_1,\ \ldots,\ r_n$ tais que $x = r_1 h_1 + \cdots + r_n h_n$. A demonstração da existência de uma tal base faz uso do Lema de Zorn e pode ser encontrada em [85] ou [100]. Essa base é denominada *base de Hamel* de $\mathbb{R}$.

Uma consequência curiosa da existência de bases de Hamel em $\mathbb{R}$ será discutida no tópico que se inicia à página 201.

Outros exemplos menos dramáticos que mostram a dependência da dimensão com o corpo utilizado são os seguintes: sejam $V_1 = \mathbb{C}$ sobre o corpo dos complexos e $V_2 = \mathbb{C}$ sobre o corpo dos reais. $V_1$ tem dimensão 1, mas $V_2$ tem dimensão 2.

Mais adiante faremos uso do seguinte resultado:

**Teorema 2.11** *Se em um espaço vetorial $V$ existir um conjunto $\{v_1, \ldots, v_n\}$ de $n$ vetores linearmente independentes, então a dimensão algébrica de $V$ é maior ou igual a $n$.* □

Prova. A demonstração é feita por absurdo. Suponhamos que haja uma base $B = \{b_1, \ldots, b_k\}$ em $V$ com $k < n$. Então, podemos escrever

$$v_1 \;=\; \alpha_1 b_1 + \cdots + \alpha_k b_k \; .$$

pois $B$ é uma base. Nem todos os $\alpha_i$ podem ser nulos. Supondo que $\alpha_k$ seja um elemento não nulo, podemos escrever

$$b_k \;=\; (\alpha_k)^{-1}\big(v_1 - \alpha_1 b_1 - \cdots - \alpha_{k-1} b_{k-1}\big) \; . \tag{2.100}$$

Analogamente, temos que

$$v_2 = \beta_1 b_1 + \cdots + \beta_k b_k$$

e, usando (2.100), podemos escrever

$$v_2 \;=\; \gamma_1 b_1 + \cdots + \gamma_{k-1} b_{k-1} + \lambda_1 v_1 \; .$$

Os $\gamma_i$ não podem ser todos nulos, pois de outra forma teríamos $v_2 = \lambda_1 v_1$, contrariando a hipótese de os $v_i$'s serem linearmente independentes. Suponhamos que $\gamma_{k-1}$ seja o elemento não nulo, podemos escrever $b_{k-1}$ como uma combinação linear envolvendo $\{b_1, \ldots, b_{k-2}\}$ e os vetores $v_1$ e $v_2$. Prosseguindo, concluiremos após $k$ passos que

$$v_{k+1} \;=\; \lambda'_1 v_1 + \cdots + \lambda'_k v_k \; ,$$

contrariando a hipótese de que os $v_i$'s são linearmente independentes. ■

• **Automorfismos descontínuos do grupo** $(\mathbb{R}, +)$ *Nota para os estudantes mais avançados.*

Neste tópico usaremos as bases de Hamel da reta real para ilustrar uma "patologia" cuja existência é por vezes mencionada na teoria de grupos, a saber, a existência de automorfismos descontínuos do grupo $(\mathbb{R}, +)$.

Considere-se a equação $f(x+y) = f(x) + f(y)$ para todo $x,\ y \in \mathbb{R}$. Podemos nos perguntar: que funções $f : \mathbb{R} \to \mathbb{R}$ podem satisfazê-la[75]? É bastante claro que funções do tipo $f(x) = cx$, com $c$ constante real, satisfazem $f(x+y) = f(x) + f(y)$ para todo $x,\ y \in \mathbb{R}$. Fora isso, $f(x) = cx$ são contínuas e são bijeções de $\mathbb{R}$ em $\mathbb{R}$ (a menos que $c = 0$).

Serão essas as únicas funções com a propriedade $f(x+y) = f(x) + f(y)$ para todo $x,\ y \in \mathbb{R}$? Haverá outras funções com essa propriedade e que não sejam contínuas? Será que há outras funções com essa propriedade, não-contínuas, e que também sejam bijeções de $\mathbb{R}$ em $\mathbb{R}$? A resposta a essa última pergunta é muito curiosa e conduz a uma classe de funções cuja existência ilustra algumas dificuldades encontradas na teoria de grupos. Provemos em primeiro lugar a seguinte afirmação (historicamente esse pequeno resultado é devido a Cauchy[76]):

**Proposição 2.16** *Se $f : \mathbb{R} \to \mathbb{R}$ satisfizer $f(x+y) = f(x) + f(y)$ para todo $x,\ y \in \mathbb{R}$ e $f$ for contínua em toda reta real $\mathbb{R}$, então $f$ é da forma $f(x) = cx$ para algum $c$, constante real.* □

Prova. Seja $f$ contínua satisfazendo $f(x+y) = f(x) + f(y)$ para todo $x,\ y \in \mathbb{R}$ e $f : \mathbb{R} \to \mathbb{R}$. É claro que, tomando $x = y = 0$ tem-se $f(0) = f(0+0) = 2f(0)$ e, portanto, $f(0) = 0$. Segue facilmente daí que $0 = f(0) = f(x + (-x)) = f(x) + f(-x)$ e, portanto, $f(-x) = -f(x)$ para todo $x \in \mathbb{R}$.

Seja agora $p$ inteiro positivo e $x$ real, ambos arbitrários. Teremos que $f(px) = f\big((p-1)x + x\big) = f\big((p-1)x\big) + f(x) = f\big((p-2)x\big) + 2f(x)$ etc. Repetindo $p$ vezes esse proceder, concluímos que $f(px) = pf(x)$. Como $f(-x) = -f(x)$, essa relação vale para $p$ negativo também. Seja agora $q$ inteiro, não nulo. Então, pelo que acabamos de provar, $f(1) =$

[75] Para um tratamento extenso de equações funcionais como essa, vide [7].
[76] Augustin Louis Cauchy (1789-1857).

$f(q/q) = qf(1/q)$ e concluímos que $f(1/q) = f(1)/q$. Se, então, tivermos um número racional $r$ da forma $r = p/q$, com $p$ inteiro e $q$ inteiro não nulo, teremos que $f(r) = f(p/q) = pf(1/q) = (p/q)f(1) = rf(1)$. Finalizamos a prova evocando a continuidade de $f$ e o fato que todo $x$ real pode ser aproximado por um número racional: seja $x \in \mathbb{R}$ e $r_n$, $n \in \mathbb{N}$, uma sequência de números racionais que converge a $x$, i.e., $x = \lim_{n\to\infty} r_n$. Então, $f(x) = f\big(\lim_{n\to\infty} r_n\big) = \lim_{n\to\infty} f(r_n) = (\lim_{n\to\infty} r_n)\, f(1) = xf(1)$. Na segunda igualdade usamos a hipótese (crucial!) que $f$ é contínua em toda parte. Denotando $f(1) = c$ a afirmação está provada. ■

Com esse resultado em mãos podemos nos perguntar: haverá funções não-contínuas que satisfazem $f(x + y) = f(x) + f(y)$? Talvez surpreendentemente, a resposta é positiva. Não só há funções não contínuas com essa propriedade, mas há dentre elas funções bijetoras de $\mathbb{R}$ em $\mathbb{R}$. Funções com tais características um tanto patológicas podem ser construídas com o uso das assim chamadas *bases de Hamel* da reta real, seguindo uma construção concebida por esse autor[77]. Detalhemos.

Seja o espaço vetorial $V$ dos números reais sob o corpo dos racionais. Como consideramos páginas acima, esse espaço vetorial tem dimensão algébrica infinita, mas existe uma base $H \subset \mathbb{R}$ de $V$, não-contável, denominada *base de Hamel*, tal que todo elemento $x$ de $\mathbb{R}$ pode ser escrito como combinação linear finita (única!) por racionais de elementos de $H$, ou seja, para todo $x \in \mathbb{R}$ existe um $n$ (que depende de $x$), racionais $r_1, \ldots, r_n$ (que dependem de $x$) e elementos $h_1, \ldots, h_n$ de $H$ (que também dependem de $x$) tais que $x$ pode ser escrita (de forma única!) como $x = r_1h_1 + \cdots + r_nh_n$. Denominaremos essa expressão a decomposição de $x$ em $H$.

Notemos que se $x$ e $y$ são números reais e $x = r_1h_1 + \cdots + r_nh_n$ e $y = r'_1h'_1 + \cdots + r'_mh'_m$ são suas decomposições em $H$, então a decomposição de $x + y$ é $r_1h_1 + \cdots + r_nh_n + r'_1h'_1 + \cdots + r'_mh'_m$.

Vamos definir uma função $f : \mathbb{R} \to \mathbb{R}$, da seguinte forma. Primeiramente fixamos seus valores nos elementos de $H$ tomando, para cada $h \in H$, $f(h) := f_h \in \mathbb{R}$, onde os números $f_h$ são escolhidos arbitrariamente. Em segundo lugar, para qualquer $x \in \mathbb{R}$, e cuja decomposição em $H$ seja $x = r_1h_1 + \cdots + r_nh_n$, definimos $f(x) := r_1f(h_1) + \cdots + r_nf(h_n) = r_1f_{h_1} + \cdots + r_nf_{h_n}$. Assim, se $x$ e $y$ são números reais e $x = r_1h_1 + \cdots + r_nh_n$ e $y = r'_1h'_1 + \cdots + r'_mh'_m$ são suas decomposições em $H$, teremos $f(x + y) = r_1f_{h_1} + \cdots + r_nf_{h_n} + r'_1f_{h'_1} + \cdots + r'_mf_{h'_m} = f(x) + f(y)$.

O leitor pode convencer-se que há, para cada base de Hamel $H$, infinitas funções desse tipo (devido à arbitrariedade da escolha dos $f_h$'s) e que todas são descontínuas, exceto se escolhermos $f_h = ch$ para todo $h \in H$, com uma constante $c$ fixa.

Espertamente, podemos tomar $f$ como uma bijeção de $H$ em $H$, ou seja, podemos escolher[78] $f_h \in H$ para todo $h \in H$ e de modo que para todo $h \in H$ exista um $g \in H$ único tal que $f_g = h$. Uma situação trivial dessas é aquela na qual $f$ é a identidade quando restrita a $H$: $f_h = h$ para todo $h \in H$, mas outras escolhas são também possíveis. Se $f$ for uma bijeção de $H$ em $H$, é fácil de se ver que imagem de $f$ no domínio $\mathbb{R}$ é toda a reta real $\mathbb{R}$ (mostre isso)!

Além disso, uma tal $f$, bijetora enquanto função de $H$ em $H$, é igualmente bijetora como função de $\mathbb{R}$ em $\mathbb{R}$. Mostremos isso. Sejam $x$ e $y \in \mathbb{R}$ com decomposições $x = r_1h_1 + \cdots + r_nh_n$ e $y = s_1g_1 + \cdots + s_mg_m$ com $r_j,\ s_k \in \mathbb{Q}$ e $h_j,\ g_k \in H$ e suponhamos que $f(x) = f(y)$. Isso significa que $r_1f_{h_1} + \cdots + r_nf_{h_n} = s_1f_{g_1} + \cdots + s_mf_{g_m}$. Como cada $f_{h_j}$ e cada $f_{g_k}$ é elemento de $H$, essa igualdade só é possível se $m = n$, se $f_{h_j} = f_{g_{\pi(j)}}$ e se $r_j = s_{\pi(j)}$ para todo $j = 1, \ldots, n$, onde $\pi$ é um elemento do grupo de permutações de $n$ elementos (ou seja, é uma bijeção de $\{1, \ldots, n\}$ em si mesmo). Como $f$ é uma bijeção de $H$ em si mesmo, segue que $h_j = g_{\pi(j)}$ para todo $j = 1, \ldots, n$. Assim,

$$x \;=\; \sum_{j=1}^{n} r_jh_j \;=\; \sum_{j=1}^{n} s_{\pi(j)}g_{\pi(j)} \;=\; \sum_{j=1}^{n} s_jg_j \;=\; y$$

e, portanto, $f : \mathbb{R} \to \mathbb{R}$ é bijetora.

Uma função que satisfaça $f(x + y) = f(x) + f(y)$ para todo $x,\ y \in \mathbb{R}$ e $f : \mathbb{R} \to \mathbb{R}$ representa um endomorfismo do grupo $(\mathbb{R},\ +)$. O que aprendemos no último parágrafo pode ser expresso na linguagem da teoria de grupos como a afirmação que existem automorfismos de $(\mathbb{R},\ +)$ que não são contínuos. Esse fato ilustra algumas situações patológicas que são por vezes encontradas ou mencionadas no estudo de grupos contínuos. Com o uso de funções $f$ desse tipo é possível, por exemplo, construir subgrupos uniparamétricos não-contínuos de um grupo de Lie dado ou representações não-contínuas de tais subgrupos.

[77] Georg Hamel (1877-1954). A referência original é G. Hamel, *"Eine Basis aller Zahlen und die unstetigen Lösungen der Funktionalgleichung $f(x + y) = f(x) + f(y)$"*. Math. Annalen, **60**, 459–462 (1905).

[78] Que tal é possível é garantido pelo *Axioma da Escolha* ⟶ Exercício.

Assim, por exemplo, se $A$ é uma matriz real $n \times n$ antissimétrica, então $O(t) = \exp(tA)$, $t \in \mathbb{R}$ é um subgrupo uniparamétrico contínuo de $\mathrm{SO}(n)$, pois $O(0) = \mathbb{1}$ e $O(t)O(t') = O(t+t')$ para todos $t,\ t' \in \mathbb{R}$, sendo os elementos de matriz de $O(t)$ funções contínuas de $t$. Se agora definirmos $P(t) = \exp\big(f(t)A\big)$, $t \in \mathbb{R}$, para uma função $f : \mathbb{R} \to \mathbb{R}$, patológica como acima (ou seja, satisfazendo $f(x+y) = f(x) + f(y)$ para todo $x,\ y \in \mathbb{R}$, bijetora mas descontínua), ainda teremos $P(0) = \mathbb{1}$ e $P(t)P(t') = P(t+t')$ para todos $t,\ t' \in \mathbb{R}$, mas os elementos de matriz de $P(t)$ não são funções contínuas de $t$.

• **Bases topológicas em espaços vetoriais** *Nota para os estudantes mais avançados.*

O conceito de base algébrica não deve ser confundido com o de *base topológica*, conceito esse pertencente ao contexto dos espaços vetoriais topológicos:

Uma *base topológica* em um espaço vetorial topológico $V$ é um conjunto $B = \{b_i,\ i \in I\}$ de vetores linearmente independentes tais que span $(B)$ é um conjunto denso em $V$, ou seja, o fecho de span $(B)$ é $V$.

Uma base topológica é dita ser *base topológica completa* se não possuir nenhum subconjunto próprio que também seja uma base topológica.

A *dimensão topológica* de um espaço vetorial é, então, definida como sendo a cardinalidade das bases topológicas completas de $V$.

Para ilustrar como os conceitos de base algébrica e base topológica são diferentes, consideremos novamente o seguinte Exemplo 4 acima:

*Exemplo 5.* $V = \mathbb{R}$ sobre o corpo dos racionais, com a topologia usual sobre $\mathbb{R}$, tem uma base topológica completa de dimensão finita: $B = \{1\}$. De fato, o conjunto $\{r \cdot 1,\ r \in \mathbb{Q}\}$ é denso em $\mathbb{R}$. Esse espaço vetorial possui, portanto, uma dimensão topológica igual a um.

**Definição. Espaço vetorial separável.** Um espaço vetorial topológico sobre o corpo dos reais ou dos complexos é dito ser separável se possuir uma base topológica contável. ♠

## 2.3.2 O Dual Algébrico de um Espaço Vetorial

Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K}$ (por exemplo, o corpo $\mathbb{C}$). Uma aplicação $l : V \to \mathbb{K}$, definida sobre todo $V$, é dita ser um *funcional linear* se

$$l(\alpha x + \beta y) \ = \ \alpha l(x) + \beta l(y)$$

para todo $x,\ y \in V$ e todo $\alpha,\ \beta \in \mathbb{K}$.

**E. 2.112** *Exercício.* Mostre que, de acordo com a definição acima, vale para qualquer funcional linear $l$ que $l(0) = 0$. ✠

O conjunto de todos os funcionais lineares de $V$ em $\mathbb{K}$ é denominado espaço *dual algébrico* de $V$ e denotado $V'$. O conjunto $V'$ é feito um espaço vetorial (sobre $\mathbb{K}$), por meio da seguinte relação:

$$(\alpha l + \beta m)(x) \ := \ l(\alpha x) + m(\beta x)\ ,$$

para todo $l$ e $m \in V'$ ; $\alpha,\ \beta \in \mathbb{K}$ e todo $x \in V$. O vetor nulo de $V'$ é o funcional linear que associa trivialmente todo vetor de $V$ a zero: $l(x) = 0,\ \forall x \in V$.

O seguinte teorema é verdadeiro e será implicitamente usado várias vezes no que segue. Sua demonstração é, como veremos, elementar mas instrutiva.

**Teorema 2.12** *Seja um espaço vetorial $V$ sobre um corpo $\mathbb{K}$. Se um vetor $v$ tem a propriedade que $l(v) = 0$ para todo $l \in V'$, então $v = 0$.* □

Prova. Seja $B$ uma base algébrica em $V$. Para cada elemento $b \in B$ podemos associar um funcional linear $l_b$, definido da seguinte forma. Como todo $w \in V$ pode ser escrito como uma combinação linear finita de elementos de $B$, podemos sempre escrever

$$w = w_b b + w'\ ,$$

onde $w'$ é uma combinação linear finita de elementos de $B \setminus \{b\}$ e $w_b \in \mathbb{K}$. (É claro que $w_b = 0$ caso $b$ não compareça na decomposição de $w$ em uma soma finita de elementos de $B$). Definimos, então

$$l_b(w) \;:=\; w_b \;,$$

para todo vetor $w \in V$. É um exercício simples mostrar que, para cada $b \in B$, a aplicação $l_b : V \to \mathbb{K}$ dada acima é um funcional linear.

**E. 2.113** *Exercício*. Mostre isso. ✣

Seja, então, $v$ um vetor como no enunciado do teorema. Se $l(v) = 0$ para todo $l \in V'$, vale obviamente que $l_b(v) = 0$ para todo $b \in B$. Isso, porém, trivialmente implica que $v = 0$, completando a demonstração. ■

Se $A$ e $B$ são espaços vetoriais e $A \subset B$, então $B' \subset A'$.

**E. 2.114** *Exercício*. Justifique essa última afirmativa. ✣

• **Notação**

Para $x \in V$ e $l \in V'$ é frequente usar-se a notação $\langle l,\ x\rangle$ em lugar de $l(x)$. A expressão $\langle l,\ x\rangle$ é muitas vezes dita ser o "pairing", ou "emparelhamento", entre $l \in V'$ e $x \in V$. Essa notação é graficamente conveniente por expressar a igualdade de status entre $V$ e $V'$. Uma inconveniência se dá em casos em que pode haver confusão com a notação de produto escalar.

Com essa notação, as propriedades de linearidade expressam-se como

$$\langle \alpha_1 l_1 + \alpha_2 l_2,\ x\rangle \;=\; \alpha_1\langle l_1,\ x\rangle + \alpha_2\langle l_2,\ x\rangle \qquad \text{e} \qquad \langle l,\ \alpha_1 x_1 + \alpha_2 x_2\rangle \;=\; \alpha_1\langle l,\ x_1\rangle + \alpha_2\langle l,\ x_2\rangle \;,$$

válidas para todos $l,\ l_1,\ l_2 \in V'$, $x,\ x_1,\ x_2 \in V$ e $\alpha_1,\ \alpha_2 \in \mathbb{K}$.

• **Base dual canônica**

Seja $U$ um espaço vetorial sobre um corpo $\mathbb{K}$ e suponhamos que $U$ tenha dimensão finita, ou seja, que $U$ possua uma base finita $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_n\}$, $n \in \mathbb{N}$. Todo elemento de $u \in U$ pode ser escrito na forma $\displaystyle\sum_{i=1}^{n} u^i \mathbf{e}_i$ com $u^i \in \mathbb{K}$. Para $j = 1,\ \ldots,\ n$ definamos $\mathbf{e}^j : U \to \mathbb{K}$ por[79]

$$\mathbf{e}^j(u) \;:=\; u^j \;.$$

É elementar provar que cada $\mathbf{e}^j$ é um funcional linear em $U$ e, portanto, um elemento de $U'$. Pela definição, vale

$$\mathbf{e}^j\big(\mathbf{e}_i\big) \;=\; \delta_{ij} \;,$$

para todos $i,\ j = 1,\ \ldots,\ n$, ou seja, na notação de emparelhamento,

$$\langle \mathbf{e}^j,\ \mathbf{e}_i\rangle \;=\; \delta_{ij} \;.$$

Em verdade o conjunto $\{\mathbf{e}^1,\ \ldots,\ \mathbf{e}^n\}$ forma uma base em $U'$, denominada *base dual canônica* da base $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_n\}$. De fato, se $\ell \in U'$ teremos

$$\ell(u) \;=\; \ell\left(\sum_{i=1}^{n} u^i \mathbf{e}_i\right) \;=\; \sum_{i=1}^{n} u^i \ell\big(\mathbf{e}_i\big) \;=\; \sum_{i=1}^{n} \ell\big(\mathbf{e}_i\big)\mathbf{e}^i(u) \;,$$

para todo $u \in U$, provando que

$$\ell \;=\; \sum_{i=1}^{n} \ell\big(\mathbf{e}_i\big)\mathbf{e}^i \;,$$

[79] Como veremos, a distinção notacional que doravante faremos entre índices superiores e inferiores, ainda que não possua nenhum significado profundo em si, é muito conveniente e muito empregada em textos de Física.

o que estabelece que todo elemento de $U'$ é uma combinação linear de $\{\mathbf{e}^1,\ \ldots,\ \mathbf{e}^n\}$. Os elementos de $\{\mathbf{e}^1,\ \ldots,\ \mathbf{e}^n\}$ são linearmente independentes, pois se $\sum_{i=1}^n \alpha_i \mathbf{e}^i = 0$ isso significa que para todo $\mathbf{e}_j$, $j = 1,\ \ldots,\ n$, valerá $0 = \sum_{i=1}^n \alpha_i \mathbf{e}^i(\mathbf{e}_j) = \alpha_j$.

É relevante comentar que a base dual de $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_n\}$ é única. De fato, se $\{\mathbf{e}^1,\ \ldots,\ \mathbf{e}^n\}$ e $\{\ell^1,\ \ldots,\ \ell^n\}$ satisfazem $\langle \mathbf{e}^j,\ \mathbf{e}_i\rangle = \delta_{ij}$ e $\langle \ell^j,\ \mathbf{e}_i\rangle = \delta_{ij}$ para todos $i,\ j$, então $\langle \ell^j - \mathbf{e}^j,\ \mathbf{e}_i\rangle = 0$ para todos $i,\ j$, o que implica que, para cada $j$ e para todo $u \in U$, vale $\langle \ell^j - \mathbf{e}^j,\ u\rangle = 0$, donde conclui-se que $\ell^j = \mathbf{e}^j$ para todo $j$.

### • O dual topológico de um espaço vetorial

Seja $V$ um espaço vetorial topológico. O conjunto de todos os funcionais lineares contínuos sobre $V$ é dito ser o *dual topológico* de $V$. O dual topológico será denotado neste texto por $V^\dagger$. Note-se que $V^\dagger \subset V'$.

### • Exemplos de funcionais lineares

*Exemplo 1.* Seja $V = \mathbb{C}^n$, sobre o corpo dos complexos. Seja $a_1,\ \ldots,\ a_n$ um conjunto fixo de números complexos. Para qualquer vetor $z = (z_1,\ \ldots,\ z_n) \in \mathbb{C}^n$ defina-se $l(z) = \overline{a_1} z_1 + \cdots + \overline{a_n} z_n$. Então, $l$ é um funcional linear em $\mathbb{C}^n$.

**E. 2.115** *Exercício.* Verifique. ✠

Em verdade, é possível demonstrar a recíproca: em $\mathbb{C}^n$ todo funcional linear é da forma acima para algum conjunto $\{a_1,\ \ldots,\ a_n\}$. Essa afirmativa é um caso particular de um teorema importante conhecido como "Teorema da Representação de Riesz", um resultado válido para espaços de Hilbert, dos quais $\mathbb{C}^n$ é um exemplo, e que será demonstrado na Seção 41.2.2.1,

Seja $\mathcal{P}$ o conjunto de todos os polinômios de uma variável real com coeficientes complexos: $P_n(t) \in \mathcal{P}$,

$$P_n(t) \ = \ a_n t^n + \cdots + a_1 t + a_0 \ ,$$

com $t \in \mathbb{R}$, $a_i \in \mathbb{C}$, é dito ser um polinômio de grau $n$ se $a_n \neq 0$. O conjunto $\mathcal{P}$ é claramente um espaço vetorial sobre os complexos.

*Exemplo 2.* Para cada $t_0 \in \mathbb{R}$ e $p \in \mathcal{P}$, $l(p) = p(t_0)$ é um funcional linear em $\mathcal{P}$.

**E. 2.116** *Exercício.* Verifique. ✠

Esse exemplo pode ser generalizado:

*Exemplo 3.* Sejam $t_1,\ \ldots,\ t_n \in \mathbb{R}$, distintos, e $a_1,\ \ldots,\ a_n$ números complexos. Para todo $p \in \mathcal{P}$, definamos

$$l(p) \ = \ a_1 p(t_1) + \cdots + a_n p(t_n) \ .$$

Então, $l$ é um funcional linear em $\mathcal{P}$.

**E. 2.117** *Exercício.* Verifique. ✠

O último exemplo pode ser fortemente generalizado nos dois exemplos que seguem.

*Exemplo 3.* Seja $(a,\ b)$ um intervalo finito de $\mathbb{R}$ e $h$ uma função complexa integrável nesse intervalo (ou seja, $\int_a^b |h(t)|dt \leq \infty$). Então,

$$l(p) \ = \ \int_a^b \overline{h(t)}\, p(t)\ dt$$

está definida para todo $p \in \mathcal{P}$ e define um funcional linear em $\mathcal{P}$.

**E. 2.118** *Exercício.* Justifique as duas últimas afirmativas. ✠

*Exemplo 4.* Seja a função $g(x) = e^{-x^2}$. Então,

$$l(p) \ = \ \int_{-\infty}^{\infty} g(t)\, p(t)\ dt$$

está definida para todo $p \in \mathcal{P}$ e define um funcional linear em $\mathcal{P}$.

**E. 2.119** *Exercício*. Justifique as duas últimas afirmativas. ✠

• **A relação entre $V$ e $V'$**

Vamos aqui discutir o fato que sempre existe uma maneira (não canônica, vide abaixo) de associar vetores de um espaço vetorial $V$ com elementos de seu dual algébrico $V'$.

Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K}$ e $B \subset V$ uma base algébrica em $V$. Seja $\mathcal{F}_B \equiv \mathbb{K}^B$ a coleção de todas as funções de $B$ em $\mathbb{K}$. Afirmamos que existe uma bijeção de $\mathcal{F}_B$ sobre $V'$, ou seja, esses dois conjuntos podem ser identificados nesse sentido.

Para tal, seja $f \in \mathcal{F}_B$. Definimos uma aplicação $I : \mathcal{F}_B \to V'$ da seguinte forma. Como todo $x \in V$ pode ser escrito como uma combinação linear finita de elementos de $B$, digamos, $x = \alpha_1 b_{i_1} + \cdots + \alpha_n b_{i_n}$, escrevemos

$$I(f)(x) \;:=\; \alpha_1 f(b_{i_1}) + \cdots + \alpha_n f(b_{i_n}) \,.$$

$I(f)$ é um funcional linear pois, se escrevemos $y = \alpha_{n+1} b_{i_{n+1}} + \cdots + \alpha_{n+m} b_{i_{n+m}}$, teremos

$$\begin{aligned} I(f)(x+y) &= \alpha_1 f(b_{i_1}) + \cdots + \alpha_{n+m} f(b_{i_{n+m}}) \\ &= \alpha_1 f(b_{i_1}) + \cdots + \alpha_n f(b_{i_n}) + \alpha_{n+1} f(b_{i_{n+1}}) + \cdots + \alpha_{n+m} f(b_{i_{n+m}}) \\ &= I(f)(x) + I(f)(y) \,. \end{aligned} \tag{2.101}$$

Isso mostrou que $I(f)$ é de fato um elemento de $V'$ para cada $f \in \mathcal{F}_B$. Vamos mostrar o reverso: que a cada elemento $l$ de $V'$ há um elemento $g_l$ de $\mathcal{F}_B$ associado e que $I(g_l) = l$. Seja novamente $x = \alpha_1 b_{i_1} + \cdots + \alpha_n b_{i_n} \in V$ e seja $l$ um elemento de $V'$. Tem-se

$$l(x) \;=\; \alpha_1 l(b_{i_1}) + \cdots + \alpha_n l(b_{i_n}) \,.$$

Definimos $g_l : B \to \mathbb{K}$ por

$$g_l(b) \;:=\; l(b)$$

para todo $b \in B$. Pela definição

$$I(g_l)(x) \;=\; \alpha_1 g_l(b_{i_1}) + \cdots + \alpha_n g_l(b_{i_n}) \;=\; \alpha_1 l(b_{i_1}) + \cdots + \alpha_n l(b_{i_n}) \;=\; l(x) \tag{2.102}$$

para todo $x \in V$. Logo $I(g_l) = l$ como queríamos. Isso provou que $I$ é injetora.

$I$ é também sobrejetora, pois é evidente que se $l : V \to \mathbb{K}$ for um elemento de $V'$, então a restrição de $l$ a $B$ é um elemento de $\mathcal{F}_B$ e vale $I(l \restriction B) = l$. De fato, para qualquer $x = \alpha_1 b_{i_1} + \cdots + \alpha_n b_{i_n}$, temos $I(l \restriction B)(x) = \alpha_1 l(b_{i_1}) + \cdots + \alpha_n l(b_{i_n}) = l\big(\alpha_1 b_{i_1} + \cdots + \alpha_n b_{i_n}\big) = l(x)$.

A aplicação $I : \mathcal{F}_B \to V'$ é, portanto, uma bijeção entre esses dois conjuntos. Notemos, porém, que essa bijeção não é canônica no sentido que a mesma depende da base adotada. Se trocarmos $B$ por outra base a bijeção altera-se.

De posse desses fatos podemos entender a relação entre $V$ e $V'$ da seguinte forma. Seja o subconjunto $\mathcal{G}_B$ de $\mathcal{F}_B$ formado por todas as funções de suporte finito em $B$, ou seja, pelas funções que assumem valores não nulos (no corpo $\mathbb{K}$) apenas para um subconjunto finito de $B$. Para $g \in \mathcal{G}_B$ existe um conjunto finito $B_g = \{b_1, \ldots, b_n\} \subset B$ tal que $g$ é não nula nos elementos de $B_g$, mas é nula em $B \setminus B_g$.

Os conjuntos $\mathcal{G}_B$ e $V$ podem ser identificados no seguinte sentido: existe uma bijeção $J : \mathcal{G}_B \to V$. Tal é fácil de ver se lembrarmos que os elementos de $V$ podem ser escritos como uma combinação linear finita de elementos de $B$. Para cada $g \in \mathcal{G}_B$ definimos

$$J(g) \;:=\; g(b_1) b_1 + \cdots + g(b_n) b_n \in V \,,$$

onde $\{b_1, \ldots, b_n\} = B_g$. Se $x = \alpha_1 b_{i_1} + \cdots + \alpha_n b_{i_n} \in V$, definimos $g_x \in \mathcal{G}_B$ por

$$g_x(b_{i_a}) \;=\; \alpha_a, \quad a = 1, \ldots, n \qquad \text{e} \qquad g_x(b) \;= 0 \quad \text{se} \quad b \notin \{b_{i_1}, \ldots, b_{i_n}\} \,.$$

É fácil ver, então, que

$$J(g_x) \;=\; g(b_{i_1}) b_{i_1} + \cdots + g(b_{i_n}) b_{i_n} \;=\; \alpha_1 b_{i_1} + \cdots + \alpha_n b_{i_n} \;=\; x \,, \tag{2.103}$$

o que mostra que $J$ é sobrejetora. Que $J$ é injetora, segue do fato que se $f \in \mathcal{G}_B$ é tal que $\{b'_1,\ \ldots,\ b'_m\} = B_f$ e $J(g) = J(f)$, então teremos $g(b_1)b_1 + \cdots + g(b_n)b_n = f(b'_1)b'_1 + \cdots + f(b'_n)b'_n$, o que implica que $n = m$, que $b_i = b'_i$ e que $g(b_i) = f(b_i)$ para todo $i \in \{1,\ \ldots,\ n\}$, ou seja, que $f = g$.

Notemos novamente que essa bijeção $J$ também não é canônica, no sentido que a mesma depende da base adotada. Se trocarmos $B$ por outra base a bijeção altera-se.

**E. 2.120** *Exercício importante.* Mostre agora que $J^{-1} : V \to \mathcal{G}_b$ é linear, ou seja, $J^{-1}(\alpha x + \beta y) = \alpha J^{-1}(x) + \beta J^{-1}(y)$ para todos $x,\ y \in V$ e todos $\alpha,\ \beta \in \mathbb{K}$. ✠

Juntando o discutido acima, concluímos que $\phi := I \circ J^{-1}$ é uma aplicação linear injetora de $V$ em $V'$. A mesma, porém, não é "natural", pois depende da base algébrica $B$ escolhida.

No caso em que $V$ é um espaço de dimensão finita, $\mathcal{F}_b$ e $\mathcal{G}_b$ coincidem e, portanto, $\phi = I \circ J^{-1}$ é uma aplicação linear bijetora de $V$ em $V'$. Concluímos, portanto, que se $V$ é um espaço vetorial de dimensão finita, então ele é isomorfo a seu dual $V'$. Esse isomorfismo não é canônico: depende de uma escolha de base.

Para futura referência, colocamos esses resultados na forma de uma proposição:

**Proposição 2.17** *Seja $V$ um espaço vetorial. Então, existe ao menos uma aplicação linear injetora (não canônica) de $V$ em $V'$, que denotamos por $\phi : V \to V'$. O espaço $V$, portanto, é isomorfo a sua imagem por $\phi$ em $V'$: $V \simeq \phi(V) \subset V'$.*

*Se a dimensão de $V$ for finita, então $\phi$ é também sobrejetora e, portanto, $V \simeq V'$. Portanto, $\phi$ define um isomorfismo (não canônica) entre $V$ e $V'$.* ■

Assim, fixada uma base $B$ em $V$ há uma maneira de associar todos os elementos de $V$ com elementos do seu dual algébrico. Notemos porém que no caso de espaços de dimensão infinita pode haver elementos de $V'$ aos quais não correspondem tais identificações, ou seja, a imagem de $\phi = I \circ J^{-1}$ é tipicamente um subconjunto próprio de $V'$.

**E. 2.121** *Exercício-Exemplo.* Seja $\mathcal{P}$ o espaço vetorial dos polinômios em $\mathbb{R}$ definido acima. Seja $T = \{t_i \in \mathbb{R},\ i \in \mathbb{N}\}$, um conjunto contável de pontos distintos da reta real e seja $q(t) = q_0 + q_1 t + \cdots + q_n t^n$, um polinômio. Definamos $l_q \in V'$ por

$$l_q(p) \ := \ q_0 p(t_0) + q_1 p(t_1) + \cdots + q_n p(t_n) \ .$$

Mostre que a aplicação $\mathcal{P} \ni q \mapsto l_q \in V'$ é linear e injetora.

Será que com o conjunto $T$ fixado todo elemento de $V'$ seria da forma $l_q$ para algum $q$? Pense. Inspire-se nos exemplos 3 e 4 da página 205. O que acontece para conjuntos $T$ diferentes? ✠

Antes de sairmos desse tema mencionemos um resultado elementar que será evocado adiante.

**Proposição 2.18** *Se $U$ e $V$ são espaços vetoriais sobre um mesmo corpo e ambos tem dimensão finita, então $U \simeq V$ se e somente se $U' \simeq V'$.* ■

Prova. Como vimos na Proposição 2.17, $U \simeq U'$ e $V \simeq V'$. Logo, devido à transitividade da relação de isomorfia, $U \simeq V$ se e somente se $U' \simeq V'$. ■

### • O bidual algébrico de um espaço vetorial

Mais interessante que a relação entre $V$ e $V'$, é a relação de $V$ com o *dual algébrico* de $V'$, o chamado bidual algébrico de $V$ e denotado por $(V')'$, assunto que discutiremos agora. A razão é que, ao contrário do que tipicamente ocorre entre $V$ e $V'$, há sempre uma aplicação linear injetora entre $V$ e $(V')'$ que é natural, ou seja, independente de escolhas de bases.

Outro interesse na relação entre $V$ e $(V')'$ reside no fato que a mesma revela-nos, como veremos, uma distinção aguda entre espaços vetoriais de dimensão finita e infinita.

Se $V$ é um espaço vetorial sobre um corpo $\mathbb{K}$ já observamos que $V'$ é também um espaço vetorial sobre o mesmo corpo. Assim, $V'$ tem também seu dual algébrico, que é denominado *bidual algébrico* de $V$.

O bidual algébrico de um espaço vetorial $V$ é o espaço $(V')'$. Como vimos nas páginas anteriores, existe pelo menos uma aplicação linear injetiva de $V$ em $V'$. Chamemos esta aplicação de $\phi_1$. Analogamente, existe pelo menos uma aplicação linear injetiva $\phi_2$ de $V'$ em $(V')'$. A composição $\phi_2 \circ \phi_1$ fornece uma aplicação linear injetiva de $V$ em $(V')'$. Como $\phi_1$ e $\phi_2$ dependem de escolhas de base, a composição $\phi_2 \circ \phi_1$ também depende, não sendo, assim, natural.

Ao contrário do que ocorre na relação entre $V$ e $V'$, podemos sempre encontrar uma aplicação linear injetiva de $V$ em $(V')'$ que é natural, *i.e.*, independente de base. Vamos denotá-la por $\boldsymbol{\Lambda}$. Definimos $\boldsymbol{\Lambda} : V \to (V')'$ da seguinte forma: para $x \in V$, $\boldsymbol{\Lambda}(x)$ é o elemento de $(V')'$ que associa a cada $l \in V'$ o valor $l(x)$:

$$\boldsymbol{\Lambda}(x)(l) \;:=\; l(x)\;, \tag{2.104}$$

ou seja,

$$\big\langle \boldsymbol{\Lambda}(x),\, l \big\rangle \;:=\; \big\langle l,\, x \big\rangle\;. \tag{2.105}$$

**E. 2.122** *Exercício.* Mostre que $\boldsymbol{\Lambda} : V \to (V')'$ é linear. Mostre que $\boldsymbol{\Lambda} : V \to (V')'$ é injetora. Sugestão: use o Teorema 2.12, enunciado e demonstrado na página 203. ✤

É transparente pela definição de $\boldsymbol{\Lambda}$ que a mesma é independente de bases e, portanto, "natural". A relação entre $x \in V$ e um elemento de $(V')'$ mostrada acima é tão direta que quase poderíamos dizer que $V$ é um subconjunto de $(V')'$: $V \subset (V')'$. Alguns autores, abusando um pouco da linguagem, chegam mesmo a escrever uma tal relação de inclusão. Mais correta, no entanto, é a relação $\boldsymbol{\Lambda}(V) \subset (V')'$. Analogamente, a definição (2.104)–(2.105) permite-nos identificar $\boldsymbol{\Lambda}(x) \equiv x$ para todo $x \in V$. Faremos isso frequentemente, ainda que essa identificação seja imprecisa.

Poderíamos nesse momento nos perguntar: quando podemos eventualmente ter $\boldsymbol{\Lambda}(V) = (V')'$? Para o caso de espaços vetoriais sobre o corpo dos reais ou dos complexos a resposta é simples e, um tanto surpreendentemente, e se expressa no seguinte teorema.

**Teorema 2.13** *Seja $V$ um espaço vetorial sobre o corpo dos reais ou dos complexos. Então, $\boldsymbol{\Lambda}(V) = (V')'$ se e somente se $V$ for um espaço vetorial de dimensão finita. Como $\boldsymbol{\Lambda}$ é linear e injetora, isso diz-nos que $V$ e $(V')'$ são espaços vetoriais isomorfos se e somente se $V$ for de dimensão finita.* □

Este teorema revela uma importante distinção entre espaços de dimensão finita e infinita. Em dimensão finita todos os funcionais lineares do dual algébrico de $V'$ são da forma $\boldsymbol{\Lambda}(x)$ para algum vetor $x$. Em dimensão infinita, porém, há certamente elementos em $(V')'$ que não são dessa forma. Assim, ao tomarmos duais duplos em dimensão infinita sempre obtemos espaços vetoriais "maiores", o que não ocorre em dimensão finita.

Prova do Teorema 2.13. Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K} = \mathbb{C}$ ou $\mathbb{R}$.

*Caso de dimensão finita.* Vamos, em primeiro lugar, supor que $V$ seja de dimensão finita e denotemos por $\dim V$ sua dimensão. Seja também $B = \{b_1, \ldots, b_n\}$ uma base de $V$. É claro que o número de elementos de $B$ é $n = \dim V$.

É fácil mostrar que o conjunto $\{\boldsymbol{\Lambda}(b_1), \ldots, \boldsymbol{\Lambda}(b_n)\}$ é linearmente independente em $(V')'$. De fato, se existirem escalares $\alpha^i$ tais que $\alpha^1\boldsymbol{\Lambda}(b_1) + \cdots + \alpha^n\boldsymbol{\Lambda}(b_n) = 0$, ou seja, $\boldsymbol{\Lambda}(\alpha^1 b_1 + \cdots + \alpha^n b_n) = 0$, teríamos $\boldsymbol{\Lambda}(w)(l) = l(w) = 0$ para todo $l \in V'$, onde $w = \alpha^1 b_1 + \cdots + \alpha^1 b_n$. Isso, porém, implica $w = 0$ (pelo Teorema 2.12, página 203), o que implica $\alpha^1 = \cdots = \alpha^n = 0$.

Isso afirma que $\dim (V')' \geq \dim V$. Afirmamos que a igualdade só se dá se $\boldsymbol{\Lambda}(V) = (V')'$. De fato, se $\boldsymbol{\Lambda}(V) = (V')'$, então todo elemento de $(V')'$ é da forma

$$\boldsymbol{\Lambda}\big(\alpha^1 b_1 + \cdots + \alpha^n b_n\big) \;=\; \alpha^1\boldsymbol{\Lambda}(b_1) + \cdots + \alpha^n\boldsymbol{\Lambda}(b_n)\;,$$

com $\alpha^k \in \mathbb{K}$ para todo $k$ e, portanto, $\{\boldsymbol{\Lambda}(b_1), \ldots, \boldsymbol{\Lambda}(b_n)\}$ é uma base em $(V')'$ e $\dim (V')' = \dim V$. Se, por outro lado, $\boldsymbol{\Lambda}(V)$ é um subconjunto próprio de $(V')'$, existem elementos $v'' \in (V')'$ tais que $v'' - \alpha^1\boldsymbol{\Lambda}(b_1) - \cdots - \alpha^n\boldsymbol{\Lambda}(b_n) \neq 0$ para todos $\alpha^i \in \mathbb{K}$. Portanto, $\{v'', \boldsymbol{\Lambda}(b_1), \ldots, \boldsymbol{\Lambda}(b_n)\}$ é um conjunto de $n+1$ vetores linearmente independentes. Logo $\dim (V')' > n = \dim V$, pelo Teorema 2.11, página 201.

Vamos, então, mostrar que obrigatoriamente tem-se que $\dim (V')' = \dim V$, provando o teorema.

Como vimos quando discutimos a relação entre $V$ e $V'$ à página 206, $V'$ é equivalente ao conjunto $\mathcal{F}_B$ de todas as funções de $B$ em $\mathbb{K}$, enquanto que $V$ é equivalente ao conjunto $\mathcal{G}_B$ formado por todas as funções que assumem valores

não nulos (no corpo $\mathbb{K}$) apenas para um conjunto finito de $B$. Como $B$ tem um número finito de elementos, sucede $\mathcal{G}_B = \mathcal{F}_B$. Logo, $V$ e $V'$ são equivalentes: existe uma bijeção linear $\varphi_1$ entre ambos.

A aplicação $\varphi_1$ leva a base $B$ em uma base $\varphi_1(B)$ em $V'$. Para ver isso, notemos que todo elemento $l \in V'$ é da forma $l = \varphi_1(v)$, para algum $v \in V$. Como todo $v \in V$ é da forma $v = \alpha^1 b_1 + \cdots + \alpha^n b_n$, segue que todo elemento $l \in V'$ é da forma $\alpha^1\varphi_1(b_1) + \cdots + \alpha^n\varphi_1(b_n)$. Como $\varphi_1$ é bijetora, $\{\varphi_1(b_1), \ldots, \varphi_1(b_n)\}$ é um conjunto de vetores linearmente independentes pois se existirem escalares $\beta^1, \ldots, \beta^n$ tais que

$$\beta^1\varphi_1(b_1) + \cdots + \beta^n\varphi_1(b_n) \;=\; 0$$

teríamos $\varphi_1(\beta^1 b_1 + \cdots + \beta^n b_n) = 0$, o que implica $\beta^1 b_1 + \cdots + \beta^n b_n = 0$, pois $\varphi_1$ é bijetora. Isso, porém, implica $\beta^1 = \cdots = \beta^n = 0$, pois $\{b_1, \ \ldots, b_n\}$ é uma base. Assim, $\varphi_1(B) = \{\varphi_1(b_1), \ldots, \varphi_1(b_n)\}$ é uma base em $V'$ e, portanto, $\dim V' = n = \dim V$.

Analogamente, tem-se que $V'$ e $(V')'$ são equivalentes e, portanto, existe uma bijeção linear $\varphi_2$ entre ambos que leva a base $\varphi_1(B)$ em uma base $\varphi_2 \circ \varphi_1(B)$ em $(V')'$. Portanto, $\dim V' = \dim (V')'$. Logo $\dim V = \dim V' = \dim (V')'$, como queríamos provar.

*Caso de dimensão infinita.* No caso de dimensão infinita desejamos mostrar que sempre há elementos em $(V')'$ que não são da forma $\mathbf{\Lambda}(x)$ para algum $x \in V$. Abaixo $\mathbb{K}$ é o corpo dos reais ou dos complexos.

Vamos primeiro delinear a estratégia a ser seguida. Seja $B$ uma base em $V$ (fixa daqui por diante). Como sabemos, existe uma aplicação linear bijetora $\phi : \mathcal{F}_B \to V'$. Uma função $s : B \to \mathbb{K}$, $s \in \mathcal{F}_B$ é dita ser *limitada* se existir um $M > 0$ tal que $|s(b)| < M$ para todo $b \in B$. Seja $\mathcal{L}_B$ o conjunto de todas as funções limitadas de $B$ em $\mathbb{K}$. É claro que $\mathcal{L}_B \subset \mathcal{F}_B$.

Vamos mostrar o seguinte: não existe nenhum vetor não nulo $v \in V$ com a propriedade que $\mathbf{\Lambda}(v)(\beta) = 0$ para todo $\beta \in \phi(\mathcal{L}_B)$. Seja $v = \alpha^1 b_1 + \cdots + \alpha^m b_m$ um tal vetor para o qual $\mathbf{\Lambda}(v)(\beta) = 0$. Isso significa que para todo $\beta \in \phi(\mathcal{L}_B)$

$$0 \;=\; \mathbf{\Lambda}(v)(\beta) \;=\; \beta(v) = \alpha^1\beta(b_1) + \cdots + \alpha^m\beta(b_m)\;.$$

Para cada $i \in \{1, \ \ldots, \ m\}$ tomemos os funcionais lineares $\beta^i$ definidos nos elementos $b$ de $B$ por

$$\beta^i(b) \;:=\; \begin{cases} 1, & \text{se } b = b_i\;, \\ 0, & \text{de outra forma.} \end{cases}$$

Como todo $\beta^i$ é um elemento de $\phi(\mathcal{L}_B)$ (por quê?), teríamos $0 = \beta^i(v) = \alpha^i$ para todo $i$, o que implica $v = 0$.

A conclusão é que nenhum elemento de $(V')'$ que seja da forma $\mathbf{\Lambda}(v)$ para algum $v \in V$ não nulo pode anular todos os elementos de $\phi(\mathcal{L}_B) \subset V'$. A estratégia que seguiremos será a de exibir um elemento de $(V')'$ que tem precisamente a propriedade de anular todos os elementos de $\phi(\mathcal{L}_B)$. Um tal elemento não pode pertencer, portanto, a $\mathbf{\Lambda}(V)$, o que mostra que $\mathbf{\Lambda}(V)$ é um subconjunto próprio de $(V')'$ no caso de dimensão infinita.

Seja $u \in V' \setminus \phi(\mathcal{L}_B)$ e $U$ o subespaço de $V'$ gerado por $u$. Todo elemento $l \in V'$ pode ser escrito de modo único na forma $l = au + y$, onde $a \in \mathbb{K}$ e $y$ pertence ao subespaço complementar de $U$. Definamos $\alpha(l) = a$. É claro que $\alpha \in (V')'$ e que $\alpha$ aniquila todo elemento de $\phi(\mathcal{L}_B)$, pois estes pertencem ao subespaço complementar de $U$ (por quê?). Assim, $\alpha \in (V')'$ mas $\alpha \notin \mathbf{\Lambda}(V)$. ■

• **"Pullbacks"**

Sejam $U$ e $V$ dois espaços vetoriais (não necessariamente de dimensão finita) sobre um mesmo corpo $\mathbb{K}$ e seja $\psi : U \to V$ uma aplicação linear entre ambos. A aplicação $\psi$ induz uma aplicação linear denotada por $\psi^* : V' \to U'$, do espaço dual $V'$ no espaço dual $U'$, a qual é definida de forma que, para todos $\ell \in V'$ e $u \in U$ valha

$$\big\langle \psi^*(\ell), u \big\rangle \;:=\; \big\langle \ell, \psi(u) \big\rangle\;.$$

A aplicação $\psi^*$ é dita ser o *pullback* de $\psi$. É elementar constatar que $\psi^* : V' \to U'$ é uma aplicação linear entre esses espaços.

**E. 2.123** *Exercício*. Prove essa afirmação! ✠

**E. 2.124** *Exercício*. Sejam $U_1$, $U_2$ e $U_3$ três espaços vetoriais sobre o mesmo corpo $\mathbb{K}$. Sejam $\psi_{12} : U_1 \to U_2$ e $\psi_{23} : U_2 \to U_3$ aplicações lineares. Mostre que $\big(\psi_{23} \circ \psi_{12}\big)^* = \big(\psi_{12}\big)^* \circ \big(\psi_{23}\big)^*$. ✠

**E. 2.125** *Exercício*. Seja $U$ um espaço vetorial e $\mathbf{id}_U : U \to U$ o operador identidade (ou seja, tal que $\mathbf{id}_U(u) = u$ para todo $u \in U$). Mostre que $(\mathbf{id}_U)^* = \mathbf{id}_{U'}$. ✠

Esses últimos exercícios preparam a seguinte proposição relevante:

**Proposição 2.19** *Sejam $U$ e $V$ dois espaços vetoriais sobre um mesmo corpo $\mathbb{K}$ e seja $\psi : U \to V$ um isomorfismo de $U$ em $V$. Então o* pullback $\psi^* : V' \to U'$ *é também um isomorfismo de $V'$ em $U'$ e vale $\big(\psi^*\big)^{-1} = \big(\psi^{-1}\big)^*$.* □

Prova. Provemos que $\psi^*$ é sobrejetora. Seja $j \in U'$, para todo $u \in U$ temos

$$\langle j,\, u\rangle \;=\; \big\langle j,\, \psi^{-1} \circ \psi(u)\big\rangle \;=\; \Big\langle \psi^* \circ \big(\psi^{-1}\big)^*(j),\, u\Big\rangle\,,$$

provando que $j = \psi^* \circ (\psi^{-1})^*(j)$ e, portanto, que $j$ está na imagem de $\psi^*$. Como $j \in U'$ é arbitrário, provou-se que $\psi^* : V' \to U'$ é sobrejetora.

Provemos que $\psi^*$ é injetora. Sejam $\ell_1,\ \ell_2 \in V'$ tais que $\psi^*(\ell_1) = \psi^*(\ell_2)$. Teríamos, para todo $u \in U$,

$$\langle \ell_1 - \ell_2,\, \psi(u)\rangle \;=\; \big\langle \psi^*(\ell_1) - \psi^*(\ell_2),\, u\big\rangle \;=\; 0\,.$$

Como a imagem de $\psi$ é sobrejetora e $u \in U$ é arbitrário, isso implica que $\ell_1 = \ell_2$, estabelecendo a injetividade de $\psi^*$.

Assim, $\psi^*$ é inversível. Disso segue que

$$\mathbf{id}_{U'} \;=\; \mathbf{id}_U^* \;=\; \big(\psi^{-1} \circ \psi\big)^* \;=\; \psi^* \circ \big(\psi^{-1}\big)^* \qquad \text{e que} \qquad \mathbf{id}_{V'} \;=\; \mathbf{id}_V^* \;=\; \big(\psi \circ \psi^{-1}\big)^* \;=\; \big(\psi^{-1}\big)^* \circ \psi^*\,,$$

o que prova que $\big(\psi^*\big)^{-1} = \big(\psi^{-1}\big)^*$. ■

## 2.3.3 Subespaços e Espaços Quocientes

• **Subespaços**

Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K}$. Um subconjunto $W$ de $V$ é dito ser um subespaço de $V$ (sobre o mesmo corpo $\mathbb{K}$) se para todo $\alpha,\ \beta \in \mathbb{K}$ e todo $u,\ v \in W$ valer que $\alpha u + \beta v \in W$. É evidente que um subespaço de um espaço vetorial é por si só um espaço vetorial.

**Proposição 2.20** *Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K}$ e seja $\{W_\lambda \subset V,\ \lambda \in\ \Lambda\}$ uma família (não vazia) de subespaços de $V$. Então, $\bigcap_{\lambda\in\Lambda} W_\lambda$ é também um subespaço de $V$.* □

Prova. Se $u$ e $v$ são elementos de $\bigcap_{\lambda\in\Lambda} W_\lambda$ então ambos pertencem a cada $W_\lambda$ com $\lambda \in \Lambda$. Como cada $W_\lambda$ é um subespaço de $V$, conclui-se que toda combinação linear $\alpha u + \beta v$, com $\alpha,\ \beta \in \mathbb{K}$, é um elemento de $W_\lambda$. Como isso se dá para cada $W_\lambda$ com $\lambda \in \Lambda$, concluímos que $(\alpha u + \beta v) \in \bigcap_{\lambda\in\Lambda} W_\lambda$. Isso completa a prova. ■

• **Subespaços gerados por um conjunto**

Seja $V$ um espaço vetorial sobre um corpo $\mathbb{K}$ e seja $A$ um subconjunto não vazio de $A$. Seja $\{W_\lambda(A) \subset V,\ \lambda \in\ \lambda\}$ a coleção de todos os subespaços de $V$ que contém o conjunto $A$, ou seja, a coleção de todos os subespaços $W_\lambda(A)$ de $V$ tais que $A \subset W_\lambda(A)$. Essa família é não vazia, pois, evidentemente contém o espaço $V$. Define-se o *subespaço gerado* por $A$ por

$$[\![A]\!] \;:=\; \bigcap_{\lambda\in\Lambda} W_\lambda(A)\,.$$

Que se trata de um subespaço é evidente pela Proposição 2.20. Interpretando-se a definição pode-se dizer que $[\![A]\!]$ é o menor subespaço de $V$ que contém $A$. Justifique esse palavreado.

• **Quocientes**

Se $W$ é um subespaço de um espaço vetorial $V$ sobre um corpo $\mathbb{K}$, então é possível definir em $V$ uma relação de equivalência $E_W \subset V \times V$ da seguinte forma: dizemos que $(u,\ v) \in V \times V$ pertence a $E_W$ se $u - v \in W$.

**E. 2.126** *Exercício*. Mostre que isso de fato define uma relação de equivalência em $V$. ✠

Seguindo a notação usual denotaremos também essa relação de equivalência pelo símbolo $\sim_W$: $u \sim_W v$ se $u - v \in W$.

Denotemos por $V/W$ o conjunto das classes de equivalência de $V$ pela relação $E_W$. Denotaremos por $[u] \in V/W$ a classe de equivalência que contém o vetor $u \in V$.

Com esses ingredientes podemos transformar $V/W$ em um espaço vetorial sobre $\mathbb{K}$. Isso se dá definindo em $V/W$ uma soma e um produto por escalares. O vetor nulo será a classe de equivalência $[0]$ que contém o vetor 0. Como subconjunto de $V$, a classe $[0]$, aliás, vem a ser o conjunto $W$ (por quê?).

Se $[u]$ e $[v]$ são as classes de equivalência que contêm os elementos $u$ e $v$, respectivamente, de $V$, então definimos

$$[u] + [v] \ = \ [u + v] \ .$$

**E. 2.127** *Exercício*. Mostre que essa definição é coerente, no sentido que independe dos representantes ($u$ e $v$) escolhidos nas classes. Mostre que essa operação de soma é comutativa e associativa. Mostre que $[u] + [0] = [u]$ para todo $u \in V$. ✠

Analogamente, a operação de multiplicação por escalares é definida por

$$\alpha[u] \ := \ [\alpha u] \ ,$$

para todo $u \in V$.

**E. 2.128** *Exercício*. Mostre que essa definição é coerente, no sentido que independe do representante $u$ escolhido na classe. Mostre que o conjunto $V/W$ é, portanto, um espaço vetorial sobre o corpo $\mathbb{K}$ com as operações definidas acima. ✠

O espaço vetorial $V/W$ assim obtido é denominado *espaço quociente* de $V$ por $W$.

## 2.3.4 Somas Diretas de Espaços Vetoriais

• **A soma direta de uma coleção finita de espaços vetoriais**

Sejam $V_1$ e $V_2$ dois espaços vetoriais (sobre um mesmo corpo $\mathbb{K}$, sendo doravante $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$). Como $V_1$ e $V_2$ são dois grupos Abelianos, o grupo Abeliano obtido pela soma direta $V_1 \oplus V_2$ está definido pelo procedimento geral descrito na Seção 2.2.4, página 185. Isso, entretanto, ainda não faz de $V_1 \oplus V_2$ um espaço vetorial.

Para isso, é preciso definir o produto de um elemento de $V_1 \oplus V_2$ por um escalar (um elemento de $\mathbb{K}$). Definimos o produto de $v_1 \oplus v_2 \in V_1 \oplus V_2$ por $\alpha \in \mathbb{K}$ como sendo o elemento $(\alpha v_1) \oplus (\alpha v_2)$, ou seja,

$$\alpha(v_1 \oplus v_2) \ := \ (\alpha v_1) \oplus (\alpha v_2) \ . \tag{2.106}$$

É fácil constatar que, com essa definição, $V_1 \oplus V_2$ torna-se um espaço vetorial (vide a definição formal de espaço vetorial à página 140), que denotaremos por $V_1 \oplus_{\mathbb{K}} V_2$. O assim definido espaço vetorial $V_1 \oplus_{\mathbb{K}} V_2$ é dito ser a *soma direta dos espaços vetoriais* $V_1$ e $V_2$ sobre o corpo $\mathbb{K}$.

Se tivermos uma coleção finita de espaços vetoriais $V_1,\ \ldots,\ V_n$ (sobre um mesmo corpo $\mathbb{K}$) procedemos analogamente, primeiro definindo o grupo Abeliano $V_1 \oplus \cdots \oplus V_n$ e depois definindo a multiplicação por escalares por

$$\alpha(v_1 \oplus \cdots \oplus v_n) \ := \ (\alpha v_1) \oplus \cdots \oplus (\alpha v_n) \ ,$$

com $\alpha \in \mathbb{K}$ e $v_1 \oplus \cdots \oplus v_n \in V_1 \oplus \cdots \oplus V_n$. O espaço vetorial (sobre $\mathbb{K}$) assim definido é denotado por $V_1 \oplus_{\mathbb{K}} \cdots \oplus_{\mathbb{K}} V_n$.

• **Soma direta de coleções arbitrárias de espaços vetoriais**

Se $\{V_i,\ i \in J\}$ é uma coleção de espaços vetoriais que, em particular, são grupos Abelianos, cai definida, pelo apresentado na subseção anterior, a soma direta $\mathbb{V}_s := \bigoplus_{i\in J} V_i$, definida primeiramente como grupo Abeliano. $\mathbb{V}_s$ pode ser feito um espaço vetorial definindo-se, para um escalar genérico $\alpha \in \mathbb{K}$,

$$\alpha \cdot \left( \bigtimes_{a\in J} (v_a) \right) := \bigtimes_{a\in J} (\alpha v_a) \,, \tag{2.107}$$

para todo $\bigtimes_{a\in J} (v_a) \in \mathbb{V}_s$ (para a notação de produtos Cartesianos gerais, vide página 73). É um exercício elementar (faça-o!) mostrar que, com essas estruturas, $\mathbb{V}_s$ é de fato um espaço vetorial, satisfazendo a definição apresentada na Seção 2.1.5, página 140.

• **Representações de grupos em somas diretas de espaços vetoriais**

Sejam $U$ e $V$ dois espaços vetoriais sobre um mesmo corpo $\mathbb{K}$ (que omitiremos doravante). Seja $G$ um grupo e sejam $\pi^U$ e $\pi^V$ representações de $G$ em $U$ e $V$, respectivamente. As representações $\pi^U$ e $\pi^V$ permitem definir uma representação de $G$ em $U \oplus V$ denominada *representação soma direta* e denotada por $\pi^U \oplus \pi^V$, ou por $\pi^{U\oplus V}$, a qual é definida como segue. Para $g \in G$, define-se $\Big(\pi^U \oplus \pi^V\Big)(g)$ por

$$\Big(\pi^U \oplus \pi^V\Big)(g)\ (u \oplus v) \ := \ \Big(\pi^U(g)u\Big) \oplus \Big(\pi^V(g)v\Big) \,, \tag{2.108}$$

para todos $u \in U$ e $v \in V$. A generalização para somas diretas arbitrárias de espaços vetoriais é imediata.

### 2.3.4.1 Formas Multilineares

Para $n \in \mathbb{N}$, considere-se uma coleção finita de espaços vetoriais $V_1,\ \ldots,\ V_n$ (sobre um mesmo corpo $\mathbb{K}$) e seja sua soma direta $V_1 \oplus \cdots \oplus V_n$. Uma *forma $n$-linear* em $V_1 \oplus \cdots \oplus V_n$ é uma aplicação $\omega : V_1 \oplus \cdots \oplus V_n \to \mathbb{K}$ tal que para $\alpha,\ \beta \in \mathbb{K}$ e $v_j,\ v'_j \in V_j$, $j = 1,\ \ldots,\ n$, valem as relações

$$\begin{aligned} &\omega\Big(v_1 \oplus \cdots \oplus v_{i-1} \oplus (\alpha v_i + \beta v'_i) \oplus v_{i+1} \oplus \cdots \oplus v_n\Big) \\ &\qquad = \ \alpha\omega\Big(v_1 \oplus \cdots \oplus v_{i-1} \oplus v_i \oplus v_{i+1} \oplus \cdots \oplus v_n\Big) + \beta\omega\Big(v_1 \oplus \cdots \oplus v_{i-1} \oplus v'_i \oplus v_{i+1} \oplus \cdots \oplus v_n\Big) \end{aligned} \tag{2.109}$$

para cada $i = 1,\ \ldots,\ n$.

É elementar constatar-se pela definição que se $\omega : V_1 \oplus \cdots \oplus V_n \to \mathbb{K}$ é uma forma $n$-linear, então

$$\omega\Big(v_1 \oplus \cdots \oplus v_{i-1} \oplus 0 \oplus v_{i+1} \oplus \cdots \oplus v_n\Big) \ = \ 0$$

para todo $i$, ou seja, se um dos argumentos é o vetor nulo a forma se anula (prova: tome-se $\alpha = \beta = 0$ em (2.109)).

Vamos denotar por $\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ o conjunto de todas as $n$-formas lineares em $V_1 \oplus \cdots \oplus V_n$. O conjunto $\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ é também um espaço vetorial sobre $\mathbb{K}$. Para duas $n$-formas lineares $\omega_1$ e $\omega_2$ e dois escalares $\alpha_1,\ \alpha_2 \in \mathbb{K}$ define-se a combinação linear $\alpha_1\omega_1 + \alpha_2\omega_2$ como sendo a $n$-forma linear que a todo $v_1 \oplus \cdots \oplus v_n \in V_1 \oplus \cdots \oplus V_n$ associa

$$(\alpha_1\omega_1 + \alpha_2\omega_2)(v_1 \oplus \cdots \oplus v_n) \ := \ \alpha_1\omega_1(v_1 \oplus \cdots \oplus v_n) + \alpha_2\omega_2(v_1 \oplus \cdots \oplus v_n) \,.$$

Formas $n$-lineares são também genericamente denominadas *formas multilineares*. A noção de forma multilinear possui uma estreita relação com a noção de produto tensorial, como discutiremos mais adiante.

• **Base em $\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ no caso de dimensão finita**

Sejam $V_k$, $k = 1,\ \ldots,\ n$ espaços de dimensão finita sobre o corpo $\mathbb{K}$ (aqui, $\mathbb{R}$ ou $\mathbb{C}$). Seja $m_k = \dim V_k$, a dimensão do espaço $V_k$ e seja $\Big\{\mathbf{e}^{(k)}{}_1,\ \ldots,\ \mathbf{e}^{(k)}{}_{m_k}\Big\}$ uma base em $V_k$ e $\Big\{\mathbf{e}^{(k)1},\ \ldots,\ \mathbf{e}^{(k)m_k}\Big\}$ sua correspondente base dual canônica.

Cada vetor $v_k \in V_k$ pode ser escrito na forma $v_k = \sum_{a=1}^{m_k} (v_k)^a \mathbf{e}^{(k)}{}_a$, onde $\big\{(v_k)^1, \ldots,\ (v_k)^{m_k}\big\}$ são as componentes de $v_k$ na base $\Big\{\mathbf{e}^{(k)}{}_1,\ \ldots,\ \mathbf{e}^{(k)}{}_{m_k}\Big\}$.

Defina-se $\mathbf{m}^{a_1\cdots a_n} \in \mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ (com $1 \leq a_1 \leq m_1,\ \ldots,\ 1 \leq a_n \leq m_n$) por

$$\mathbf{m}^{a_1\cdots a_n}(v_1 \oplus \cdots \oplus v_n) \;=\; \mathbf{m}^{a_1\cdots a_n}\left(\sum_{b_1=1}^{m_1} (v_1)^{b_1}\mathbf{e}^{(1)}{}_{b_1} \;\oplus\; \ldots \;\oplus\; \sum_{b_n=1}^{m_n} (v_n)^{b_n}\mathbf{e}^{(n)}{}_{b_n}\right) \;:=\; (v_1)^{a_1}\cdots\,(v_n)^{a_n}\;. \tag{2.110}$$

É elementar constatar que, de fato, $\mathbf{m}^{a_1\cdots a_n}$ é uma forma multilinear, ou seja, $\mathbf{m}^{a_1\cdots a_n} \in \mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$. Claro está por (2.110) que

$$\mathbf{m}^{a_1\cdots a_n}\Big(\mathbf{e}^{(1)}{}_{b_1} \;\oplus\; \ldots \;\oplus\; \mathbf{e}^{(n)}{}_{b_n}\Big) \;=\; \delta^{a_1}{}_{b_1}\cdots\delta^{a_n}{}_{b_n}\;. \tag{2.111}$$

É fácil constatar que $\Big\{\mathbf{m}^{a_1\cdots a_n},\ 1 \leq a_1 \leq m_1,\ \ldots,\ 1 \leq a_n \leq m_n\Big\}$ forma uma base em $\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ (associada às bases $\Big\{\mathbf{e}^{(k)}{}_1,\ \ldots,\ \mathbf{e}^{(k)}{}_{m_k}\Big\}$ de $V_k$, $k = 1,\ \ldots,\ n$). De fato, para cada $\omega \in \mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ tem-se

$$\begin{aligned}
\omega\big(v_1 \oplus \cdots \oplus v_n\big) \;&=\; \omega\left(\sum_{a_1=1}^{m_1} (v_1)^{a_1}\mathbf{e}^{(1)}{}_{a_1} \;\oplus\; \ldots \;\oplus\; \sum_{a_n=1}^{m_n} (v_n)^{a_n}\mathbf{e}^{(n)}{}_{a_n}\right)\\
&=\; \sum_{a_1=1}^{m_1}\cdots\sum_{a_n=1}^{m_n} (v_1)^{a_1}\cdots\,(v_n)^{a_n}\omega\left(\mathbf{e}^{(1)}{}_{a_1} \;\oplus\; \ldots \;\oplus\; \mathbf{e}^{(n)}{}_{a_n}\right)\\
&=\; \sum_{a_1=1}^{m_1}\cdots\sum_{a_n=1}^{m_n} \omega\left(\mathbf{e}^{(1)}{}_{a_1} \;\oplus\; \ldots \;\oplus\; \mathbf{e}^{(n)}{}_{a_n}\right)\mathbf{m}^{a_1\cdots a_n}(v_1 \oplus \cdots \oplus v_n)\;,
\end{aligned}$$

mostrando que

$$\omega \;=\; \sum_{a_1=1}^{m_1}\cdots\sum_{a_n=1}^{m_n} \omega\left(\mathbf{e}^{(1)}{}_{a_1} \;\oplus\; \ldots \;\oplus\; \mathbf{e}^{(n)}{}_{a_n}\right)\mathbf{m}^{a_1\cdots a_n}\;, \tag{2.112}$$

como desejávamos.

Para o espaço dual $\Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)'$ temos a base dual canônica $\Big\{\mathbf{m}_{b_1\cdots b_n},\ \ 1 \leq b_j \leq m_j,\ j = 1,\ \ldots,\ n\Big\}$, onde $\mathbf{m}_{b_1\cdots b_n}$ são tais que

$$\Big\langle \mathbf{m}_{b_1\cdots b_n},\ \mathbf{m}^{a_1\cdots a_n}\Big\rangle \;=\; \delta_{b_1}{}^{a_1}\cdots\delta_{b_n}{}^{a_n}\;. \tag{2.113}$$

Segue disso e de (2.112) que

$$\begin{aligned}
\Big\langle \mathbf{m}_{b_1\cdots b_n},\ \omega\Big\rangle \;&=\; \left\langle \mathbf{m}_{b_1\cdots b_n},\ \sum_{a_1=1}^{m_1}\cdots\sum_{a_n=1}^{m_n} \omega\left(\mathbf{e}^{(1)}{}_{a_1} \;\oplus\; \ldots \;\oplus\; \mathbf{e}^{(n)}{}_{a_n}\right)\mathbf{m}^{a_1\cdots a_n}\right\rangle\\
&=\; \sum_{a_1=1}^{m_1}\cdots\sum_{a_n=1}^{m_n} \omega\left(\mathbf{e}^{(1)}{}_{a_1} \;\oplus\; \ldots \;\oplus\; \mathbf{e}^{(n)}{}_{a_n}\right)\Big\langle \mathbf{m}_{b_1\cdots b_n},\ \mathbf{m}^{a_1\cdots a_n}\Big\rangle \;\overset{(2.113)}{=}\; \omega\left(\mathbf{e}^{(1)}{}_{b_1} \;\oplus\; \ldots \;\oplus\; \mathbf{e}^{(n)}{}_{b_n}\right)\;.
\end{aligned}$$

Sobre essa igualdade

$$\omega\left(\mathbf{e}^{(1)}{}_{b_1} \;\oplus\; \ldots \;\oplus\; \mathbf{e}^{(n)}{}_{b_n}\right) \;=\; \Big\langle \mathbf{m}_{b_1\cdots b_n},\ \omega\Big\rangle \tag{2.114}$$

comentaremos mais adiante.

### 2.3.5 Produtos Tensoriais de Espaços Vetoriais

A noção de produto tensorial de espaços vetoriais é relevante em áreas como a Geometria Diferencial, a Física Relativística, a Teoria dos Corpos Deformáveis[80], a Mecânica Clássica, a Mecânica Quântica etc. Vide nota histórica sobre a noção de tensor à página 191.

Vamos começar nossa definição da noção de produto tensorial de espaços vetoriais discutindo um exemplo-protótipo de uma tal estrutura.

• **Um exemplo-protótipo de um produto tensorial de espaços vetoriais**

Sejam $A$ e $B$ dois conjuntos não vazios e sejam $\mathcal{A} := \mathbb{R}^A$ e $\mathcal{B} := \mathbb{R}^B$ as coleções de todas as funções definidas em $A$ e em $B$, respectivamente, e assumindo valores em $\mathbb{R}$, ou seja, $\mathcal{A} := \{f :\ A \to \mathbb{R}\}$ e $\mathcal{B} := \{g :\ B \to \mathbb{R}\}$. É claro que tanto $\mathcal{A}$ quanto $\mathcal{B}$ são espaços vetoriais reais.

Vamos denotar por $f \otimes_{\mathbb{R}} g : A \times B \to \mathbb{R}$ a função produto de $f$ com $g$, ou seja, a função definida em $A \times B$ que a cada par $(a,\ b) \in A \times B$ associa o valor $f(a)g(b) \in \mathbb{R}$:

$$\big(f \otimes_{\mathbb{R}} g\big)(a,\ b) \ := \ f(a)g(b)\ .$$

A função $f \otimes_{\mathbb{R}} g$ assim definida é um exemplo de um elemento de $\mathbb{R}^{A\times B}$, a coleção de todas as funções definidas em $A \times B$ assumindo valores em $\mathbb{R}$, ou seja, $\mathbb{R}^{A\times B} := \{F :\ A \times B \to \mathbb{R}\}$. Dentro de $\mathbb{R}^{A\times B}$, que também é um espaço vetorial real, vamos destacar um subespaço específico: o das funções que podem ser escritas como uma soma **finita** de funções do tipo $f \otimes_{\mathbb{R}} g$ com $f \in \mathcal{A}$ e $g \in \mathcal{B}$. Esse subespaço é denotado por $\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$ e é denominado o *produto tensorial (algébrico)* dos espaços $\mathcal{A}$ e $\mathcal{B}$.

$\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$ é o conjunto de todas as funções reais definidas em $A \times B$ que sejam da forma $\displaystyle\sum_{k=1}^{N} f_k(a)g_k(b)$, para algum $N \in \mathbb{N}$, arbitrário, e funções $f_k \in \mathcal{A}$ e $g_k \in \mathcal{B}$, também arbitrárias. As $N$ funções $f_1,\ \ldots,\ f_N$ não precisam ser todas distintas, nem as $N$ funções $g_1,\ \ldots,\ g_N$. Assim, com esse entendimento, escrevemos

$$\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B} \ := \ \left\{ \sum_{k=1}^{N} f_k \otimes_{\mathbb{R}} g_k, \ \text{ com } N \in \mathbb{N},\ \text{arbitrário e } f_k \in \mathcal{A},\ g_k \in \mathcal{B},\ \text{arbitrárias} \right\}\ .$$

É muito claro que $\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$ compõe um espaço vetorial real (um subespaço de $\mathbb{R}^{A\times B}$). Primeiramente, pois a soma de dois elementos de $\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$ é novamente um elemento de $\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$ (por ser novamente uma soma finita de produtos de funções). Segundamente, pois o produto de um elemento de $\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$ por um escalar real é novamente um elemento de $\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$.

Sobre essas operações de soma e multiplicação por escalares em $\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$ vale fazer algumas observações muito importantes. Para produtos de funções valem as bem-conhecidas regras de fatoração

$$f(a)g_1(b) + f(a)g_2(b) \ = \ f(a)\big(g_1(b) + g_2(b)\big) \qquad \text{e} \qquad f_1(a)g(b) + f_2(a)g(b) \ = \ \big(f_1(a) + f_2(a)\big)g(b)\ .$$

Para a multiplicação por um escalar real $\alpha$, vale a regra $\alpha\big(f(a)g(b)\big) = \big(\alpha f(a)\big)g(b) = f(a)\big(\alpha g(b)\big)$. Em notação de produto tensorial, elas ficam

$$f \otimes_{\mathbb{R}} g_1 + f \otimes_{\mathbb{R}} g_2 \ = \ f \otimes_{\mathbb{R}} (g_1 + g_2)\ , \tag{2.115}$$

$$f_1 \otimes_{\mathbb{R}} g + f_2 \otimes_{\mathbb{R}} g \ = \ (f_1 + f_2) \otimes_{\mathbb{R}} g \tag{2.116}$$

e

$$\alpha\big(f \otimes_{\mathbb{R}} g\big) \ = \ \big(\alpha f\big) \otimes_{\mathbb{R}} g \ = \ f \otimes_{\mathbb{R}} \big(\alpha g\big)\ . \tag{2.117}$$

Essa última se estende a um elemento qualquer de $\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$ da seguinte forma evidente:

$$\alpha\left(\sum_{k=1}^{N} f_k \otimes_{\mathbb{R}} g_k\right) \ = \ \sum_{k=1}^{N} \big(\alpha f_k\big) \otimes_{\mathbb{R}} g_k \ = \ \sum_{k=1}^{N} f_k \otimes_{\mathbb{R}} \big(\alpha g_k\big)\ . \tag{2.118}$$

[80] Para esse tema, vide *e.g.*, [324] e [497].

• **Ainda sobre a noção "intuitiva" de produto tensorial de dois espaços vetoriais**

As regras (2.115)–(2.118) têm grande importância, nem tanto pelo que são no contexto acima, mas pelo que sugerem. Dados dois espaços vetoriais $U$ e $V$ sobre um mesmo corpo $\mathbb{K}$, a ideia por trás da construção de um produto tensorial $U \otimes_{\mathbb{K}} V$ desses dois espaços é reproduzir, ou imitar, as propriedades do espaço vetorial $\mathcal{A} \otimes_{\mathbb{R}} \mathcal{B}$, acima, composto de somas finitas de produtos de funções. Assim, $U \otimes_{\mathbb{K}} V$ deve ser composto por somas finitas de produtos tensoriais de vetores de $U$ e de $V$ e devem respeitar regras como (2.115)–(2.118) de soma e multiplicação por escalares. Como isso é efetivamente implementado é algo que começaremos agora a apresentar.

Sejam $U$ e $V$ dois espaços vetoriais em relação a um mesmo corpo, digamos, $\mathbb{C}$. Os espaços $U$ e $V$ são grupos Abelianos em relação às respectivas operações de soma de vetores. Assim, podemos, como discutido na Seção 2.2.4.3, página 190, definir o grupo Abeliano $U \otimes V$, o produto tensorial dos grupos Abelianos $U$ e $V$. Naquela construção estão definidos produtos tensoriais como $u \otimes v$, com $u \in U$ e $v \in V$, e os elementos gerais de $U \otimes V$ são somas finitas de produtos tensoriais desse tipo. Além disso, valem por construção as relações

$$u \otimes v_1 + u \otimes v_2 \;=\; u \otimes (v_1 + v_2)\,,$$

$$u_1 \otimes v + u_2 \otimes v \;=\; (u_1 + u_2) \otimes v$$

para todos $u,\ u_1,\ u_2 \in U$ e todos $v,\ v_1,\ v_2 \in V$.

Esse grupo Abeliano $U \otimes V$ ainda não tem uma estrutura de espaço vetorial (sobre os complexos), pois não dissemos como definir o produto de um elemento de $U \otimes V$ por um escalar $\alpha \in \mathbb{C}$. Isso é feito da seguinte forma, para $u \in U$, $v \in V$, define-se $\alpha(u \otimes v)$ impondo (como essa "imposição" é feita é algo que será formalizado adiante)

$$\alpha(u \otimes v) \;:=\; (\alpha u) \otimes v \;=\; u \otimes (\alpha v)\,. \tag{2.119}$$

O estudante deve comparar essa regra de produto por escalares com a regra (2.106). Para elementos de $U \otimes V$ que sejam somas finitas, como por exemplo $u \otimes v + u' \otimes v'$, impomos

$$\begin{aligned} \alpha\left(u \otimes v + u' \otimes v'\right) \;&:=\; \alpha\left(u \otimes v\right) + \alpha\left(u' \otimes v'\right) \\ &=\; (\alpha u) \otimes v + (\alpha u') \otimes v' \;=\; u \otimes (\alpha v) + u' \otimes (\alpha v')\,. \end{aligned}$$

**E. 2.129** *Exercício*. Constate que, com essa definição, $U \otimes V$ torna-se um espaço vetorial, ou seja, verifique que são válidos os postulados da definição formal de espaço vetorial dados à página 140. ✠

Esse espaço vetorial, que denotaremos por $U \otimes_{\mathbb{C}} V$, é denominado *produto tensorial* dos espaços $U$ e $V$. O subíndice $\mathbb{C}$ aposto ao símbolo $\otimes$ é por vezes dispensado, e serve apenas para recordar que um escalar (ou seja, um elemento de $\mathbb{C}$, nesse caso) pode ser passado de um lado para outro do símbolo $\otimes$, tal como na última igualdade em (2.119). Passemos agora à formalização dessas ideias.

• **O produto tensorial de dois espaços vetoriais**

Sejam $U$ e $V$ dois espaços vetoriais sobre um mesmo corpo $\mathbb{K}$ (que assumiremos, por simplicidade, tendo característica zero, como $\mathbb{C}$ ou $\mathbb{R}$). Como $U$ e $V$ são dois grupos Abelianos, o grupo Abeliano $U \otimes V$ está definido pelo procedimento descrito na Seção 2.2.4.3, página 190. Isso, entretanto, ainda não faz de $U \otimes V$ um espaço vetorial. Para isso tomemos $X = U \otimes V$ e consideremos em $\mathsf{F}(X)$ (o grupo livremente gerado por $X$) o subconjunto definido por

$$\mathcal{R} \;:=\; \left\{ r \in \mathsf{F}(U \otimes V) |\; r \;=\; (\alpha u) \otimes v - u \otimes (\alpha v),\ \text{com } \alpha \in \mathbb{K},\ u \in U,\ v \in V \right\}. \tag{2.120}$$

Como antes, seja $\mathsf{R}(\mathcal{R})$ o subgrupo composto por todas as combinações lineares finitas com coeficientes inteiros de $\mathcal{R}$. Definimos, então, um novo grupo Abeliano $U \otimes_{\mathbb{K}} V$ como $U \otimes_{\mathbb{K}} V := \mathsf{F}(U \otimes V)/\mathsf{R}(\mathcal{R})$.

$U \otimes_{\mathbb{K}} V$ é por ora apenas mais um grupo Abeliano, mas podemos adicionar-lhe uma estrutura de espaço vetorial da seguinte forma. Primeiramente é preciso definir o produto de um escalar por um elemento de $U \otimes_{\mathbb{K}} V$. Para elementos da forma $u \otimes_{\mathbb{K}} v$ com $u \in U$ e $v \in V$, definimos o produto $\alpha(u \otimes_{\mathbb{K}} v)$, para $\alpha \in \mathbb{K}$ por

$$\alpha(u \otimes_{\mathbb{K}} v) \;:=\; (\alpha u) \otimes_{\mathbb{K}} v = u \otimes_{\mathbb{K}} (\alpha v)\,. \tag{2.121}$$

A última igualdade segue da definição de $U \otimes_{\mathbb{K}} V$. Os demais elementos de $U \otimes_{\mathbb{K}} V$ são da forma de somas finitas de elementos como $u \otimes_{\mathbb{K}} v$, ou seja, são da forma

$$\sum_{k=1}^{N} u_k \otimes_{\mathbb{K}} v_k$$

para algum $N \in \mathbb{N}$. Para os mesmos, definimos

$$\alpha \left( \sum_{k=1}^{N} u_k \ \otimes_{\mathbb{K}} v_k \right) \ := \ \sum_{k=1}^{N} (\alpha u_k) \ \otimes_{\mathbb{K}} v_k \ = \ \sum_{k=1}^{N} u_k \ \otimes_{\mathbb{K}} (\alpha v_k) \ ,$$

com $\alpha \in \mathbb{K}$.

É fácil constatar (faça-o!) que, com essa definição, $U \otimes_{\mathbb{K}} V$ torna-se um espaço vetorial (vide a definição formal de espaço vetorial na Seção 2.1.5, página 140), que também denotaremos por $U \otimes_{\mathbb{K}} V$. O assim definido espaço vetorial $U \otimes_{\mathbb{K}} V$ é denominado *produto tensorial dos espaços vetoriais $U$ e $V$ sobre o corpo* $\mathbb{K}$. O subíndice $\mathbb{K}$ aposto ao símbolo $\otimes$ é por vezes dispensado, e serve apenas para recordar que um escalar (ou seja, um elemento de $\mathbb{K}$) pode ser passado de um lado para outro do símbolo $\otimes$, tal como na última igualdade em (2.121).

Mais adiante (Seção 2.3.5.1, página 221) comentaremos sobre uma segunda definição equivalente de produtos tensoriais como espaços duais de formas multilineares. Essa segunda definição e sua equivalência com a anterior, porém, é restrita a produtos de espaços vetoriais de dimensão finita.

Os elementos de $U \otimes_{\mathbb{K}} V$ são genericamente denominados *tensores de ordem* 2 (ou "rank" 2). Em seguida, discutiremos como definir tensores de ordem maior.

• **O produto tensorial de uma coleção finita de espaços vetoriais**

As ideias acima podem ser generalizadas para o caso de uma coleção finita de espaços vetoriais. Sejam $U^1, \ldots, U^n$ uma coleção finita de espaços vetoriais sobre um mesmo corpo $\mathbb{K}$ (que assumiremos, por simplicidade, tendo característica zero, como $\mathbb{C}$ ou $\mathbb{R}$). Como cada $U^a$ é um grupo Abeliano, o grupo Abeliano $U^1 \otimes \cdots \otimes U^n$ está definido pelo procedimento descrito anteriormente. Isso, entretanto, ainda não faz de $U^1 \otimes \cdots \otimes U^n$ um espaço vetorial. Para isso, tomemos $X = U^1 \otimes \cdots \otimes U^n$ e consideremos o subconjunto $\mathcal{R}$ de $\mathsf{F}(X)$ definido por $\mathcal{R} := \bigcup_{\substack{i,\, j=1 \\ i \neq j}}^{n} \mathcal{R}_{ij}$, com

$$\mathcal{R}_{ij} \ := \ \Big\{ r \in \mathsf{F}(X) \Big| \ \ r \ = \ \left( u^1 \otimes \cdots \otimes u^{i-1} \otimes \left( \alpha u^i \right) \otimes u^{i+1} \otimes \cdots \otimes u^n \right) - \left( u^1 \otimes \cdots \otimes u^{j-1} \otimes \left( \alpha u^j \right) \otimes u^{j+1} \otimes \cdots \otimes u^n \right)$$

$$\text{com } \alpha \in \mathbb{K},\ u^k \in U^k \text{ para todo } k = 1, \ldots, n \Big\} \, .$$

Como antes, seja $\mathsf{R}(\mathcal{R})$ o subgrupo composto por todas as combinações lineares finitas com coeficientes inteiros de elementos de $\mathcal{R}$. Definimos, assim, um novo grupo Abeliano $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$ como

$$U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n \ := \ \mathsf{F}(U^1 \otimes \cdots \otimes U^n) / \mathsf{R}(\mathcal{R}) \, .$$

$U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$ é por ora apenas mais um grupo Abeliano, mas podemos adicionar-lhe uma estrutura de espaço vetorial definindo o produto de um escalar por um elemento de $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$. Para elementos da forma $u^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u^n$ com $u^k \in U^k$ para todo $k = 1, \ldots, n$, definimos o produto $\alpha(u^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u^n)$, para $\alpha \in \mathbb{K}$, por

$$\alpha(u^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u^n) \ := \ u^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u^{j-1} \otimes_{\mathbb{K}} \left( \alpha u^j \right) \otimes_{\mathbb{K}} u^{j+1} \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u^n$$

para qualquer $j = 1, \ldots, n$. Que o lado direito independe do particular $j$ adotado segue da definição de $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$. Os demais elementos de $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$ são da forma de somas finitas de elementos como $u^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u^n$, ou seja, são da forma

$$\sum_{k=1}^{N} u_k^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u_k^n \tag{2.122}$$

para algum $N \in \mathbb{N}$. Para os mesmos, definimos

$$\alpha \left( \sum_{k=1}^{N} u_k^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u_k^n \right) := \sum_{k=1}^{N} \alpha \left( u_k^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u_k^n \right) = \sum_{k=1}^{N} u_k^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u_k^{j-1} \otimes_{\mathbb{K}} \left( \alpha u_k^j \right) \otimes_{\mathbb{K}} u_k^{j+1} \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u_k^n \, ,$$

$\alpha \in \mathbb{K}$, onde, como anteriormente mencionado, a última igualdade é válida para qualquer $j$ adotado.

É fácil constatar (faça-o!) que, com essa definição, $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$ torna-se um espaço vetorial (vide a definição formal de espaço vetorial na Seção 2.1.5, página 140), que também denotaremos por $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$. O assim definido espaço vetorial $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$ é denominado *produto tensorial algébrico dos espaços vetoriais* $U^k$, $k = 1, \ldots, n$, *sobre o corpo* $\mathbb{K}$, ou simplesmente *produto tensorial dos espaços vetoriais* $U^k$.

• **Alguns comentários**

Observe-se que, com a construção acima, vale, para $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$,

$$\left( \alpha_1 u^1 \right) \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} \left( \alpha_n u^n \right) = \left( \alpha_1 \cdots \alpha_n \right) \left( u^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u^n \right) \, .$$

Esse fato limita a construção de produtos tensoriais que expusemos acima a produtos tensoriais envolvendo apenas uma coleção finita de espaços $U^k$, pois para coleções não finitas o produto de infinitos escalares $\alpha_k$ pode não estar definido.

Uma outra observação que fazemos é que a construção do produto tensorial, acima, é puramente algébrica: se os espaços vetoriais $U^k$ forem espaços vetoriais topológicos nenhuma topologia é naturalmente transmitida para esse produto tensorial. A construção de produtos tensoriais topológicos requer elaborações adicionais que estão fora do nosso modesto escopo.

*Notação.* Quando não houver motivo de confusão denotaremos $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$ simplesmente por $U^1 \otimes \cdots \otimes U^n$. Frequentemente usaremos a notação $U^{\otimes_{\mathbb{K}} n}$, ou simplesmente $U^{\otimes n}$, para denotar $\underbrace{U \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U}_{n \text{ vezes}}$. É também conveniente definir $U^{\otimes_{\mathbb{K}} n}$ para $n = 0$ como sendo o corpo $\mathbb{K}$. ◀

Os elementos de $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$ são genericamente denominados *tensores de ordem* $n$ (ou "rank" $n$).

Mais adiante (Seção 2.3.5.1, página 221) comentaremos sobre uma segunda definição de produtos tensoriais como espaços duais de formas multilineares. Essa segunda definição, porém, é restrita a produtos de espaços vetoriais de dimensão finita.

• **Resumo das conclusões**

Em resumo, temos o seguinte quadro: se $U^1, \ldots, U^n$ são espaços vetoriais sobre um mesmo corpo $\mathbb{K}$, cujos vetores nulos denotamos todos pelo símbolo 0, então:

1. $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$ é um espaço vetorial sobre $\mathbb{K}$ cujos elementos são somas finitas da forma $\displaystyle\sum_{k=1}^{N} u_k^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u_k^n$, com $N \in \mathbb{N}$, arbitrário, sendo $u_1^k, \ldots, u_N^k$ elementos arbitrários de $U^k$, para cada $k = 1, \ldots, n$.
2. Valem as regras

$$\begin{array}{ccccc} u^1 \otimes u^2 \otimes \cdots \otimes u^{n-1} \otimes u^n & + & u^{1'} \otimes u^2 \otimes \cdots \otimes u^{n-1} \otimes u^n & = & \left( u^1 + u^{1'} \right) \otimes u^2 \otimes \cdots \otimes u^{n-1} \otimes u^n \, , \\ \vdots & & \vdots & & \vdots \\ u^1 \otimes u^2 \otimes \cdots \otimes u^{n-1} \otimes u^n & + & u^1 \otimes u^2 \otimes \cdots \otimes u^{n-1} \otimes u^{n'} & = & u^1 \otimes u^2 \otimes \cdots \otimes u^{n-1} \otimes \left( u^n + u^{n'} \right) \, , \end{array}$$

   para todos $u^k, \, u^{k'} \in U^k$, $k = 1, \ldots, n$.
3. O vetor nulo de $U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n$ é $0 \otimes \cdots \otimes 0$ e valem as identificações

$$0 \otimes \cdots \otimes 0 = 0 \otimes u^2 \otimes \cdots \otimes u^{n-1} \otimes u^n = \cdots = u^1 \otimes u^2 \otimes \cdots \otimes u^{n-1} \otimes 0$$

   para quaisquer $u^k \in U^k$, $k = 1, \ldots . n$.

4. Vale a regra de produto por escalares ($\alpha \in \mathbb{K}$),

$$\alpha\left(\sum_{k=1}^{N} u_k^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u_k^n\right) := \sum_{k=1}^{N} (\alpha u_k^1) \otimes_{\mathbb{K}} u_k^2 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u_k^{n-1} \otimes_{\mathbb{K}} u_k^n = \cdots = \sum_{k=1}^{N} u_k^1 \otimes_{\mathbb{K}} u_k^2 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u_k^{n-1} \otimes_{\mathbb{K}} (\alpha u_k^n) .$$

**• Produto tensorial com um corpo**

Seja $U$ um espaço vetorial sobre $\mathbb{K}$. Como todo corpo $\mathbb{K}$ é também, naturalmente, um espaço vetorial sobre $\mathbb{K}$, o produto tensorial $\mathbb{K} \otimes_{\mathbb{K}} U$ está igualmente definido. É, porém, natural nesse contexto identificar-se $\mathbb{K} \otimes_{\mathbb{K}} U$ com $U$ por meio do isomorfismo $\alpha \otimes_{\mathbb{K}} u \mapsto \alpha u$, para todos $\alpha \in \mathbb{K}$ e $u \in U$. Doravante essa identificação será feita silentemente, salvo menção em contrário. O dito acima repete-se para o produto $U \otimes_{\mathbb{K}} \mathbb{K}$.

**• O isomorfismo canônico**

Dadas duas coleções finitas $V^1, \ldots, V^m$ e $U^1, \ldots, U^n$ de espaços vetoriais sobre o mesmo corpo $\mathbb{K}$ podemos, pela construção descrita acima, definir os espaços vetoriais produto

$$\mathfrak{A} = \left(V^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} V^m\right) \otimes_{\mathbb{K}} \left(U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n\right) \qquad \text{e} \qquad \mathfrak{B} = V^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} V^m \otimes_{\mathbb{K}} U^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U^n .$$

Esses dois espaços são isomorfos, com o isomorfismo $\mathcal{C} : \mathfrak{A} \to \mathfrak{B}$ dado por

$$\mathcal{C}\left(\left(v^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} v^m\right) \otimes_{\mathbb{K}} \left(u^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u^n\right)\right) := v^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} v^m \otimes_{\mathbb{K}} u^1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} u^n , \tag{2.123}$$

sendo estendido linearmente para os demais elementos. Esse isomorfismo é denominado *isomorfismo canônico* entre $\mathfrak{A}$ e $\mathfrak{B}$. O isomorfismo canônico é relevante na definição da chamada *álgebra tensorial*, tal como descrito na Seção 2.5.1, página 242.

**E. 2.130** *Exercício.* Mostre que $\mathcal{C} : \mathfrak{A} \to \mathfrak{B}$, definido acima, é, de fato, um isomorfismo entre espaços vetoriais. ✻

Se $U$ é um espaço vetorial sobre um corpo $\mathbb{K}$, vimos acima que $U^{\otimes_{\mathbb{K}} m} \otimes_{\mathbb{K}} U^{\otimes_{\mathbb{K}} n}$ e $U^{\otimes_{\mathbb{K}}(m+n)}$ são canonicamente isomorfos. Observe que isso faz sentido mesmo quando $m = 0$ (ou $n = 0$, ou ambos), pois nesse caso $U^{\otimes_{\mathbb{K}} m} = \mathbb{K}$, por convenção.

**• Bases em produtos tensoriais**

Sejam $U$ e $V$ dois espaços vetoriais de dimensão finita sobre um mesmo corpo $\mathbb{K}$ (que omitiremos doravante), dotados de bases $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ e $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$, respectivamente. Afirmamos que a coleção de vetores $\{\mathbf{e}_i \otimes \mathbf{f}_j,\ i = 1, \ldots, m,\ j = 1, \ldots, n\}$ forma uma base em $U \otimes V$. De fato, se $u \in U$ e $v \in V$ são da forma $u = \sum_{i=1}^{m} u^i \mathbf{e}_i$ e $v = \sum_{j=1}^{n} v^j \mathbf{f}_j$, então $u \otimes v = \sum_{i=1}^{m} \sum_{j=1}^{n} u^i v^j\, \mathbf{e}_i \otimes \mathbf{f}_j$. Como todos os elementos de $U \otimes V$ são obtidos como combinação linear finita de elementos da forma $u \otimes v$ com $u \in U$ e $v \in V$, concluímos imediatamente que os mesmos podem ser escritos como combinação linear dos elementos $\mathbf{e}_i \otimes \mathbf{f}_j$, como queríamos. Isso estabeleceu também que a dimensão de $U \otimes V$ é o produto da dimensão de $U$ pela de $V$: $\dim(U \otimes V) = \dim U \dim V$.

As considerações acima estendem-se sem maiores surpresas para produtos tensoriais de mais de dois espaços vetoriais sobre um mesmo corpo. Para $n \in \mathbb{N}$, sejam $V_j$, $j = 1, \ldots, n$ espaços de dimensão finita sobre o corpo $\mathbb{K}$ (aqui, $\mathbb{R}$ ou $\mathbb{C}$). Seja $m_j = \dim V_j$, a dimensão do espaço $V_j$ e seja $\left\{\mathbf{e}^{(j)}{}_1, \ldots, \mathbf{e}^{(j)}{}_{m_j}\right\}$ uma base em $V_j$. Assim, um vetor $v_j \in V_j$ se deixa escrever na forma $v_j = \sum_{a=1}^{m_j} (v_j)^a \mathbf{e}^{(j)}{}_a$, onde $\{(v_j)^1, \ldots, (v_j)^{m_j}\}$ são as componentes de $v_j$ na base $\left\{\mathbf{e}^{(j)}{}_1, \ldots, \mathbf{e}^{(j)}{}_{m_j}\right\}$. Um elemento geral de $V_1 \otimes \cdots \otimes V_n$ da forma (2.122) pode ser escrito com auxílio da base acima como

$$\sum_{k=1}^{N} u_k^1 \otimes \cdots \otimes u_k^n = \sum_{a_1=1}^{m_1} \cdots \sum_{a_n=1}^{m_n} \left(\sum_{k=1}^{N} \left(u_k^1\right)^{a_1} \cdots \left(u_k^n\right)^{a_n}\right) \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n} . \tag{2.124}$$

É evidente, portanto, que o conjunto $\mathcal{B} := \left\{\mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n},\ 1 \leq a_j \leq m_j \text{ para todo } j = 1, \ldots, n\right\}$ é uma base em $V_1 \otimes \cdots \otimes V_n$ e que esse espaço possui dimensão $m_1 \cdots m_n$. Assim, de forma geral, um tensor arbitrário $T \in V_1 \otimes \cdots \otimes V_n$

pode ser escrito nessa base $\mathcal{B}$ na forma

$$T \;=\; \sum_{a_1=1}^{m_1} \cdots \sum_{a_n=1}^{m_n} T^{a_1 \cdots a_n}\; \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n} \;. \tag{2.125}$$

As constantes $T^{a_1 \cdots a_n}$ são denominadas *componentes do tensor $T$ na base $\mathcal{B}$*.

• **A convenção de Einstein**

A representação (2.125) de um tensor $T$ é frequentemente escrita na forma simplificada

$$T \;=\; T^{a_1 \cdots a_n}\; \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n} \;, \tag{2.126}$$

com a deliberada omissão dos símbolos de somatória, sob o entendimento implícito de que índices de componentes de tensores, se repetidos, são somados em seu domínio (no caso acima, cada $a_k$ é somado de 1 a $m_k$). Essa convenção útil poupa muitas expressões de complicações notacionais e é denominada *convenção de Einstein*[81], ou *notação de Einstein*. A convenção de Einstein é muito usada em textos de Física e passaremos a fazer uso cada vez mais frequente da mesma.

• **Alguns exemplos**

**Exemplo 2.25** Seja $C(\mathbb{R})$, o espaço vetorial das funções reais e contínuas definidas em $\mathbb{R}$. O produto tensorial $C(\mathbb{R}) \otimes C(\mathbb{R})$ é o espaço de todas as funções $F$ de duas variáveis $x,\ y \in \mathbb{R}$ da forma

$$F(x,\ y) \;=\; \sum_{k=1}^{N} f_k(x) g_k(y) \;,$$

para algum $N \in \mathbb{N}$ e com $f_k,\ g_k \in C(\mathbb{R})$. Note-se que $C(\mathbb{R}) \otimes C(\mathbb{R})$ é um subconjunto próprio de $C(\mathbb{R}^2)$, a coleção de todas as funções contínuas definidas em $\mathbb{R}^2$, pois nem toda função contínua de duas variáveis reais pode ser escrita na forma de uma soma finita de produtos de funções contínuas de uma variável. Exemplos são as funções $G(x,\ y) := 1/\big(1+x^2+y^2\big)$ e $H(x,\ y) := \exp(xy)$. ♦

**Exemplo 2.26** Seja $\mathcal{P}(\mathbb{R})$ o espaço vetorial de todos os polinômios reais em uma variável real. Há em $V$ uma base, a saber, aquela composta pelos monômios $e_j(x) = x^j$, $j \in \mathbb{N}_0$. O produto tensorial $\mathcal{P}(\mathbb{R}) \otimes \mathcal{P}(\mathbb{R})$ é composto por funções da forma

$$P(x,\ y) \;=\; \sum_{k=1}^{N} p_k(x) q_k(y) \;,$$

onde os $p_k$'s e os $q_k$'s são polinômios em uma variável e $N \in \mathbb{N}$. Expandindo-se os $p_k$'s e os $q_k$'s nos monômios $e_j$, é claro que podemos escrever a expressão resultante na forma

$$P(x,\ y) \;=\; \sum_{a=0}^{n} \sum_{b=0}^{m} C_{ab}\, x^a y^b \;,$$

com $C_{ab} \in \mathbb{R}$ e com $n,\ m \in \mathbb{N}_0$.

Note-se que neste exemplo, em contraste com o Exemplo 2.25, vale $\mathcal{P}(\mathbb{R}) \otimes \mathcal{P}(\mathbb{R}) = \mathcal{P}(\mathbb{R}^2)$, onde $\mathcal{P}(\mathbb{R}^2)$ é o espaço vetorial de todos os polinômios reais em duas variáveis reais. ♦

• **Representações tensoriais de grupos**

Sejam $U$ e $V$ dois espaços vetoriais de dimensão finita ($m$ e $n$, respectivamente) sobre um mesmo corpo $\mathbb{K}$ (que omitiremos doravante), dotados de bases $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_m\}$ e $\{\mathbf{f}_1,\ \ldots,\ \mathbf{f}_n\}$, respectivamente. Seja $G$ um grupo e sejam $\pi^U$ e $\pi^V$ representações de $G$ em $U$ e $V$, respectivamente. As representações $\pi^U$ e $\pi^V$ permitem definir uma representação de $G$ em $U \otimes V$ denominada *representação produto tensorial* e denotada por $\pi^U \otimes \pi^V$ ou por $\pi^{U \otimes V}$, a qual é definida como segue. Para $g \in G$, define-se $\big(\pi^U \otimes \pi^V\big)(g)$ por

$$\Big(\pi^U \otimes \pi^V\Big)(g)\ \big(u \otimes v\big) \;:=\; \Big(\pi^U(g)u\Big) \otimes \Big(\pi^V(g)v\Big) \;,$$

[81] Albert Einstein (1879–1955).

para $u \in U$ e $v \in V$, sendo $\pi^U \otimes \pi^V$ estendido linearmente para os demais elementos de $U \otimes V$.

Um elemento $t$ de $U \otimes V$ pode ser escrito da forma $t = \sum_{i=1}^{m} \sum_{j=1}^{n} t^{ij}\, \mathbf{e}_i \otimes \mathbf{f}_j$, com $t^{ij}$ sendo as componentes de $t$. Para $g \in G$, a ação de $\pi^U \otimes \pi^V$ sobre $t \in U \otimes V$ é dada por

$$\Big(\pi^U \otimes \pi^V\Big)(g)t \;:=\; \sum_{i=1}^{m} \sum_{j=1}^{n} t^{ij} \Big(\pi^U(g)\mathbf{e}_i\Big) \otimes \Big(\pi^V(g)\mathbf{f}_j\Big)\,.$$

Escrevendo, em notação matricial para $\pi^U(g)$ e $\pi^V(g)$,

$$\pi^U(g)\mathbf{e}_i \;=\; \sum_{a=1}^{m} \pi^U(g)^a{}_i\, \mathbf{e}_a \qquad \text{e} \qquad \pi^V(g)\mathbf{f}_j \;=\; \sum_{b=1}^{n} \pi^V(g)^b{}_j\, \mathbf{f}_b\,,$$

obtém-se

$$\Big(\pi^U \otimes \pi^V\Big)(g)t \;:=\; \sum_{a=1}^{m} \sum_{b=1}^{n} t'^{ab}\, \mathbf{e}_a \otimes \mathbf{f}_b\,,$$

onde, para todos $1 \leq a \leq m$ e $1 \leq b \leq n$,

$$t'^{ab} \;:=\; \sum_{i=1}^{m} \sum_{j=1}^{n} \pi^U(g)^a{}_i\, \pi^V(g)^b{}_j\, t^{ij}\,. \tag{2.127}$$

As grandezas $t'_{ab}$ são as novas componentes de $t$ após a transformação produzida por $\pi^U \otimes \pi^V$. É frequente em livros de Física definir-se a noção de tensor (de rank 2, no caso) como sendo uma quantidade que se transforma segundo (2.127) por uma transformação induzida por um grupo (por exemplo, pelo grupo de rotações ou pelo grupo de Lorentz). Estritamente falando, um tensor não pode ser *definido* dessa forma, pois (2.127) é uma propriedade derivada, requerendo uma definição prévia da noção de produto tensorial de espaços vetoriais, tal como apresentamos acima. Ainda assim, no que concerne ao interesse da Física, a transformação de componentes expressa em (2.127) captura em muitos casos o aspecto mais importante da noção de tensor.

• **Distributividade entre produtos tensoriais e somas diretas**

Se $U$, $V$ e $W$ são espaços vetoriais sobre um mesmo corpo $\mathbb{K}$, então os espaços vetoriais $\mathfrak{C} = U \otimes_{\mathbb{K}} \Big(V \oplus_{\mathbb{K}} W\Big)$ e $\mathfrak{D} = \Big(U \otimes_{\mathbb{K}} V\Big) \oplus_{\mathbb{K}} \Big(U \otimes_{\mathbb{K}} W\Big)$ são isomorfos. Esse fato será importante na definição da álgebra tensorial, Seção 2.5.1, página 242. O isomorfismo $\mathcal{N} : \mathfrak{C} \to \mathfrak{D}$ é definido por

$$\mathcal{N}\left(\sum_{a=1}^{n} u_a \otimes_{\mathbb{K}} \Big(v_a \oplus_{\mathbb{K}} w_a\Big)\right) \;:=\; \left(\sum_{b=1}^{n} u_b \otimes_{\mathbb{K}} v_b\right) \oplus_{\mathbb{K}} \left(\sum_{c=1}^{n} u_c \otimes_{\mathbb{K}} w_c\right)\,,$$

para todo $n \in \mathbb{N}$ e para todos $u_a \in U$, $v_a \in V$ e $w_a \in W$, $a = 1,\, \ldots,\, n$.

**E. 2.131** *Exercício*. Mostre que $\mathcal{N} : \mathfrak{C} \to \mathfrak{D}$, definida acima, é, de fato, um isomorfismo de espaços vetoriais. Para tal é necessário e suficiente provar que $\mathcal{N}$ é linear, sobrejetor e que $\mathcal{N}(\kappa) = 0$ se e somente se $\kappa = 0$. Para provar que $\mathcal{N}$ é sobrejetor, observe que todo elemento de $\mathfrak{D}$ é da forma $\left(\sum_{b=1}^{n'} u'_b \otimes_{\mathbb{K}} v'_b\right) \oplus_{\mathbb{K}} \left(\sum_{c=1}^{n''} u''_c \otimes_{\mathbb{K}} w''_c\right)$. Definindo $n \equiv n' + n''$ e

$$u_k \equiv \begin{cases} u'_k\,, & k = 1,\, \ldots,\, n', \\ u''_{k-n'}\,, & k = n'+1,\, \ldots,\, n\,, \end{cases} \qquad v_k \equiv \begin{cases} v'_k\,, & k = 1,\, \ldots,\, n', \\ 0\,, & k = n'+1,\, \ldots,\, n\,, \end{cases} \qquad w_k \equiv \begin{cases} 0\,, & k = 1,\, \ldots,\, n', \\ w''_{k-n'}\,, & k = n'+1,\, \ldots,\, n\,, \end{cases}$$

para cada $k = 1,\, \ldots,\, n$, teremos

$$\left(\sum_{b=1}^{n'} u'_b \otimes_{\mathbb{K}} v'_b\right) \oplus_{\mathbb{K}} \left(\sum_{c=1}^{n''} u''_c \otimes_{\mathbb{K}} w''_c\right) \;:=\; \left(\sum_{b=1}^{n} u_b \otimes_{\mathbb{K}} v_b\right) \oplus_{\mathbb{K}} \left(\sum_{c=1}^{n} u_c \otimes_{\mathbb{K}} w_c\right)$$

(verifique!) que é, evidentemente, um elemento da imagem de $\mathcal{N}$. Determine $\mathcal{N}^{-1}$. ✠

Devido ao fato de $U \otimes_{\mathbb{K}} \left( V \oplus_{\mathbb{K}} W \right)$ e $\left( U \otimes_{\mathbb{K}} V \right) \oplus_{\mathbb{K}} \left( U \otimes_{\mathbb{K}} W \right)$ serem isomorfos, iremos por vezes identificá-los como sendo o mesmo espaço. Evidentemente, há nisso um abuso de linguagem. Essa identificação permite-nos pictoricamente dizer que o produto tensorial é distributivo em relação à soma direta.

Observemos, por fim, que o exposto acima estende-se para somas diretas finitas, como formulado no seguinte exercício:

**E. 2.132** *Exercício*. Sejam $U$ e $V^j$, $j = 1, \ldots, m$, com $m \in \mathbb{N}$, espaços vetoriais sobre o mesmo corpo $\mathbb{K}$. Mostre que

$$U \otimes_{\mathbb{K}} \left( \bigoplus_{j=1}^{m} V^j \right) \simeq \bigoplus_{j=1}^{m} \left( U \otimes_{\mathbb{K}} V^j \right),$$

sendo que o símbolo $\simeq$ denota a relação de isomorfismo entre espaços vetoriais. O isomorfismo é dado por

$$\mathcal{N} \left( \sum_{a=1}^{n} u_a \otimes_{\mathbb{K}} \left( \bigoplus_{j=1}^{m} v_a^j \right) \right) := \bigoplus_{j=1}^{m} \left( \sum_{a=1}^{n} u_a \otimes_{\mathbb{K}} v_a^j \right),$$

para todo $n \in \mathbb{N}$ e para todos $u_a \in U$, $v_a^j \in V^j$, $a = 1, \ldots, n$, $j = 1, \ldots, m$.

Analogamente, mostre que

$$\left( \bigoplus_{j=1}^{m} V^j \right) \otimes_{\mathbb{K}} U \simeq \bigoplus_{j=1}^{m} \left( V^j \otimes_{\mathbb{K}} U \right),$$

com o isomorfismo dado por

$$\mathcal{N} \left( \sum_{a=1}^{n} \left( \bigoplus_{j=1}^{m} v_a^j \right) \otimes_{\mathbb{K}} u_a \right) := \bigoplus_{j=1}^{m} \left( \sum_{a=1}^{n} v_a^j \otimes_{\mathbb{K}} u_a \right),$$

para todo $n \in \mathbb{N}$ e para todos $u_a \in U$, $v_a^j \in V^j$, $a = 1, \ldots, n$, $j = 1, \ldots, m$. ✠

### 2.3.5.1 Produtos Tensoriais, Duais Algébricos e Formas Multilineares

Nesta seção, os espaços vetoriais considerados o são sobre um mesmo corpo $\mathbb{K}$, que tomaremos por simplicidade como sendo $\mathbb{R}$ ou $\mathbb{C}$. Aqui discutiremos a relação entre o espaço dual de produtos tensoriais com o produto tensorial de espaços duais. O resultado de maior significado que obteremos, porém, é a equivalência entre produtos tensoriais e o dual de formas multilineares. Comentaremos que esse resultado permite uma definição alternativa da noção de produto tensorial de espaços vetoriais, válida no caso de dimensão finita.

• **Isomorfismo natural entre $(U \otimes V)'$ e $(U') \otimes (V')$ no caso de dimensão finita**

Sejam $U$ e $V$ dois espaços vetoriais de dimensão finita sobre um mesmo corpo $\mathbb{K}$ e sejam $U'$, respectivamente, $V'$ seus espaços duais. Sabemos da discussão da Seção 2.3.2, página 203, que por serem de dimensão finita, $U$ e $V$ são não-canonicamente isomorfos a seus duais $U'$ e $V'$, respectivamente, e que $U \otimes V$ é isomorfo a seu dual $(U \otimes V)'$. Segue disso que $(U \otimes V)'$ e $(U') \otimes (V')$ são igualmente isomorfos. Tal como discutido na Seção 2.3.2, esses isomorfismos, porém, não são naturais: dependem de escolhas de base. Há, porém, um isomorfismo natural entre $(U \otimes V)'$ e $(U') \otimes (V')$ que desejamos discutir aqui.

Se $\ell \in U'$ e $\mu \in V'$, podemos definir um funcional linear em $U \otimes V \equiv U \otimes_{\mathbb{K}} V$, que denotaremos como $\ell \times \mu$, por

$$(\ell \times \mu) \left( \sum_{a=1}^{N} u_a \otimes v_a \right) := \sum_{a=1}^{N} \ell(u_a) \mu(v_a) \tag{2.128}$$

para todos $\sum_{a=1}^{N} u_a \otimes v_a \in U \otimes V$. Que $\ell \times \mu$ é um funcional linear em $U \otimes V$ é um fato de demonstração elementar, deixado como exercício.

Se considerarmos agora elementos gerais de $U' \otimes V'$ da forma $\sum_{a=1}^{M} \ell_a \otimes \mu_a$ a aplicação $\Phi : U' \otimes V' \to (U \otimes V)'$ dada por

$$\Phi \left( \sum_{a=1}^{M} \ell_a \otimes \mu_a \right) := \sum_{a=1}^{M} \ell_a \times \mu_a \tag{2.129}$$

define uma aplicação linear de $U' \otimes V'$ em $(U \otimes V)'$ e que é injetora e sobrejetora. Essa $\Phi$ é o isomorfismo canônico a que nos referimos acima.

Para provarmos que $\Phi$ é sobrejetora, seja $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ uma base em $U$ e $\{\mathbf{e}^1, \ldots, \mathbf{e}^m\}$ sua base dual canônica e, respectivamente, seja $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ uma base em $V$ e $\{\mathbf{f}^1, \ldots, \mathbf{f}^n\}$ sua base dual canônica. Seja $\omega \in (U \otimes V)'$. Todo elemento de $U \otimes V$ é da forma $\alpha^{ij}\mathbf{e}_i \otimes \mathbf{f}_j$ (com a adoção da já mencionada *convenção de Einstein* de soma sobre índices repetidos) e, portanto, $\omega\left(\alpha^{ij}\mathbf{e}_i \otimes \mathbf{f}_j\right) = \alpha^{ij}\omega\left(\mathbf{e}_i \otimes \mathbf{f}_j\right)$. Ao mesmo tempo, vale $\left(\mathbf{e}^a \times \mathbf{f}^b\right)\left(\alpha^{ij}\mathbf{e}_i \otimes \mathbf{f}_j\right) = \alpha^{ij}\mathbf{e}^a\left(\mathbf{e}_i\right)\mathbf{f}^b\left(\mathbf{f}_j\right) = \alpha^{ij}\delta_{ia}\delta_{jb} = \alpha^{ab}$ e, portanto,

$$\omega\left(\alpha^{ij}\mathbf{e}_i \otimes \mathbf{f}_j\right) \;=\; \omega\left(\mathbf{e}_k \otimes \mathbf{f}_l\right)\Big(\left(\mathbf{e}^k \times \mathbf{f}^l\right)\left(\alpha^{ij}\mathbf{e}_i \otimes \mathbf{f}_j\right)\Big)\,,$$

implicando

$$\omega \;=\; \omega\left(\mathbf{e}_k \otimes \mathbf{f}_l\right)\left(\mathbf{e}^k \times \mathbf{f}^l\right) \;=\; \Phi\left(\omega\left(\mathbf{e}_k \otimes \mathbf{f}_l\right)\mathbf{e}^k \otimes \mathbf{f}^l\right)$$

para todo $\omega \in (U \otimes V)'$, provando a sobrejetividade de $\Phi$.

Observe-se agora que se $\Phi\left(\mu_{ij}\mathbf{e}^i \otimes \mathbf{f}^j\right) = \Phi\left(\nu_{ij}\mathbf{e}^i \otimes \mathbf{f}^j\right)$, teremos $\mu_{ij}\left(\mathbf{e}^i \times \mathbf{f}^j\right) = \nu_{ij}\left(\mathbf{e}^i \times \mathbf{f}^j\right)$ e, calculando ambos os lados em $\mathbf{e}_a \otimes \mathbf{f}_b$, obtém-se $\mu_{ab} = \nu_{ab}$ para cada $a = 1, \ldots, m$ e $b = 1, \ldots, n$, provando a injetividade de $\Phi$.

Estabelecemos com isso que os espaços vetoriais $(U \otimes V)'$ e $(U') \otimes (V')$ são naturalmente isomorfos caso $U$ e $V$ sejam de dimensão finita.

**• Generalizando para produtos tensoriais finitos arbitrários**

As considerações acima se deixam generalizar para produtos tensoriais finitos de espaços de dimensão finita sobre um mesmo corpo. Assim, se $V_i$, $i = 1, \ldots, n$, são espaços vetoriais sobre um mesmo corpo $\mathbb{K}$, teremos que $(V_1') \otimes \cdots \otimes (V_n')$ e $(V_1 \otimes \cdots \otimes V_n)'$ são espaços vetoriais naturalmente isomorfos.

Nesse mesmo caso, como $V_1 \otimes \cdots \otimes V_n$ é um espaço vetorial de dimensão finita sobre $\mathbb{R}$ ou $\mathbb{C}$, existe um isomorfismo natural entre $V_1 \otimes \cdots \otimes V_n$ e seu bidual $\Big(\big(V_1 \otimes \cdots \otimes V_n\big)'\Big)'$ (vide Teorema 2.13, página 208, e a discussão que lhe antecede). Disso concluímos que existe um isomorfismo natural entre $V_1 \otimes \cdots \otimes V_n$ e $\Big((V_1') \otimes \cdots \otimes (V_n')\Big)'$.

Sejam $V_k$, $k = 1, \ldots, n$ espaços de dimensão finita sobre o corpo $\mathbb{K}$ (aqui, $\mathbb{R}$ ou $\mathbb{C}$). Seja $m_k = \dim V_k$, a dimensão do espaço $V_k$ e seja $\left\{\mathbf{e}^{(k)}{}_1, \ldots, \mathbf{e}^{(k)}{}_{m_k}\right\}$ uma base em $V_k$ e $\left\{\mathbf{e}^{(k)1}, \ldots, \mathbf{e}^{(k)m_k}\right\}$ sua correspondente base dual canônica em $(V_k)'$.

Seguindo a convenção de Einstein, vamos escrever os elementos de $V_1 \otimes \cdots \otimes V_n$ na forma

$$A \;=\; A^{a_1\cdots a_n}\,\mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n}$$

e os elementos de $(V_1') \otimes \cdots \otimes (V_n')$ na forma

$$B \;=\; B_{b_1\cdots b_n}\,\mathbf{e}^{(1)b_1} \otimes \cdots \otimes \mathbf{e}^{(n)b_n}\,.$$

Denominemos, como acima, por $\Phi : (V_1') \otimes \cdots \otimes (V_n') \to (V_1 \otimes \cdots \otimes V_n)'$ o isomorfismo entre $(V_1') \otimes \cdots \otimes (V_n')$ e $(V_1 \otimes \cdots \otimes V_n)'$. Por definição, $\Phi$ satisfaz

$$\begin{aligned}
\Big\langle \Phi(B),\, A\Big\rangle \;&=\; \Big\langle \Phi\left(B_{b_1\cdots b_n}\,\mathbf{e}^{(1)b_1} \otimes \cdots \otimes \mathbf{e}^{(n)b_n}\right),\quad A^{a_1\cdots a_n}\,\mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n}\Big\rangle \\
&=\; B_{b_1\cdots b_n}\,A^{a_1\cdots a_n}\,\Big\langle \Phi\left(\mathbf{e}^{(1)b_1} \otimes \cdots \otimes \mathbf{e}^{(n)b_n}\right),\quad \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n}\Big\rangle \\
&:=\; B_{b_1\cdots b_n}\,A^{a_1\cdots a_n}\,\underbrace{\Big\langle \mathbf{e}^{(1)b_1},\, \mathbf{e}^{(1)}{}_{a_1}\Big\rangle}_{=\,\delta^{b_1}{}_{a_1}} \cdots \underbrace{\Big\langle \mathbf{e}^{(n)b_n},\, \mathbf{e}^{(n)}{}_{a_n}\Big\rangle}_{=\,\delta^{b_n}{}_{a_n}} \;=\; B_{c_1\cdots c_n}\,A^{c_1\cdots c_n}\,. \qquad (2.130)
\end{aligned}$$

Para futuro uso, resumimos os fatos acima na seguinte proposição:

**Proposição 2.21** *Se $V_1$, ..., $V_n$, $n \in \mathbb{N}$, são espaços vetoriais de dimensão finita sobre o mesmo corpo, então*

$$V_1' \otimes \cdots \otimes V_n' \simeq \big(V_1 \otimes \cdots \otimes V_n\big)' , \tag{2.131}$$

*ou seja, $V_1' \otimes \cdots \otimes V_n'$ e $\big(V_1 \otimes \cdots \otimes V_n\big)'$ são espaços vetoriais canonicamente isomorfos. Por força do Teorema 2.13, página 208, isso implica, também em dimensão finita, a relação canônica de isomorfia expressa em*

$$V_1 \otimes \cdots \otimes V_n \simeq \big(V_1' \otimes \cdots \otimes V_n'\big)' , \tag{2.132}$$

*relação essa que se obtém de (2.131) substituindo-se $V_k$ por $V_k'$, para cada $k$.* □

• **Mais convenções e identificações**

Além da convenção de Einstein, há uma outra convenção frequentemente adotada na literatura. Como $\Phi$, definida acima é um isomorfismo, é comum identificar-se um tensor $B_{b_1\cdots b_n}\ \mathbf{e}^{(1)b_1} \otimes \cdots \otimes \mathbf{e}^{(n)b_n} \in (V_1') \otimes \cdots \otimes (V_n')$ com sua imagem por $\Phi$. Isso corresponde a identificar-se $(V_1') \otimes \cdots \otimes (V_n')$ com o espaço vetorial dual $(V_1 \otimes \cdots \otimes V_n)'$. Com essas convenções e identificações, (2.130) pode ser apresentada simplesmente na forma

$$\Big\langle B,\ A \Big\rangle = \Big\langle B_{b_1\cdots b_n}\ \mathbf{e}^{(1)b_1} \otimes \cdots \otimes \mathbf{e}^{(n)b_n},\quad A^{a_1\cdots a_n}\ \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n} \Big\rangle = B_{c_1\cdots c_n}\ A^{c_1\cdots c_n} , \tag{2.133}$$

com $A \in V_1 \otimes \cdots \otimes V_n$ e $B \in (V_1') \otimes \cdots \otimes (V_n')$.

De forma totalmente análoga permitimo-nos, no caso de dimensão finita, identificar $V_1 \otimes \cdots \otimes V_n$ com o espaço vetorial dual $\Big((V_1') \otimes \cdots \otimes (V_n')\Big)'$, escrevendo

$$\Big\langle A^{a_1\cdots a_n}\ \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n},\quad B_{b_1\cdots b_n}\ \mathbf{e}^{(1)b_1} \otimes \cdots \otimes \mathbf{e}^{(n)b_n} \Big\rangle = A^{c_1\cdots c_n}\ B_{c_1\cdots c_n} . \tag{2.134}$$

• **Produtos tensoriais e formas multilineares**

Vamos agora discutir a relação entre produtos tensoriais de espaços vetoriais de dimensão finita e o dual de formas multilineares. A saber, estabeleceremos que o espaço vetorial $V_1 \otimes \cdots \otimes V_n$ é isomorfo ao espaço dual de $\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ (o espaço vetorial das as formas $n$-lineares sobre $V_1 \oplus \cdots \oplus V_n$, noção introduzida na Seção 2.3.4.1, página 212).

Considere-se a aplicação $\mathbf{\Psi} : V_1 \otimes \cdots \otimes V_n \to \Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)'$ definida de sorte que para todo elemento geral de $V_1 \otimes \cdots \otimes V_n$ da forma $\sum_{k=1}^{N} v_1^k \otimes \cdots \otimes v_n^k$ tenhamos

$$\left\langle \mathbf{\Psi}\left(\sum_{k=1}^{N} v_1^k \otimes \cdots \otimes v_n^k\right),\quad \omega \right\rangle := \sum_{k=1}^{N} \omega\Big(v_1^k \oplus \cdots \oplus v_n^k\Big) , \tag{2.135}$$

para todo funcional multilinear $\omega \in \mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$. Note-se que essa definição é natural: independe de escolhas de base. Vamos mostrar que se trata realmente de um isomorfismo de espaços vetoriais.

A prova da linearidade de $\mathbf{\Psi}$ é elementar e é deixada como exercício. A definição (2.135) diz-nos também que

$$\Big\langle \mathbf{\Psi}\Big(\mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n}\Big),\quad \omega \Big\rangle = \omega\Big(\mathbf{e}^{(1)}{}_{a_1} \oplus \cdots \oplus \mathbf{e}^{(n)}{}_{a_n}\Big)$$

e que para todo elemento geral de $V_1 \otimes \cdots \otimes V_n$ da forma $T^{a_1\cdots a_n}\mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n}$ tem-se

$$\Big\langle \mathbf{\Psi}\Big(T^{a_1\cdots a_n}\ \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n}\Big),\quad \omega \Big\rangle = T^{a_1\cdots a_n}\ \omega\Big(\mathbf{e}^{(1)}{}_{a_1} \oplus \cdots \oplus \mathbf{e}^{(n)}{}_{a_n}\Big) . \tag{2.136}$$

É evidente dessa expressão que valerá a igualdade

$$\Big\langle \mathbf{\Psi}\Big(T^{a_1\cdots a_n}\ \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n}\Big),\quad \omega \Big\rangle = 0$$

para todo $\omega \in \mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ se e somente se $T^{a_1 \cdots a_n} = 0$ para todos os índices $a_1, \ \ldots, \ a_n$ (para ver isso, adote-se $\omega = \mathbf{m}^{b_1 \cdots b_n}$ em (2.136), com $\mathbf{m}^{b_1 \cdots b_n}$ definido em (2.110), página 213). Assim, concluímos que $\mathbf{\Psi}$ é injetora.

Como vimos, todo $\omega \in \mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ pode ser escrito na forma (2.112). Assim, se $\Omega \in \Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)'$, teremos

$$\Big\langle \Omega, \ \omega \Big\rangle \ = \ \omega \left( {\mathbf{e}^{(1)}}_{a_1} \oplus \cdots \oplus {\mathbf{e}^{(n)}}_{a_n} \right) \Big\langle \Omega, \ \mathbf{m}^{a_1 \cdots a_n} \Big\rangle \, .$$

Logo, por (2.136), vemos que $\Omega = \mathbf{\Psi}(W)$, onde

$$W \ = \ \Big\langle \Omega, \ \mathbf{m}^{a_1 \cdots a_n} \Big\rangle \, {\mathbf{e}^{(1)}}_{a_1} \otimes \cdots \otimes {\mathbf{e}^{(n)}}_{a_n} \ \in \ V_1 \otimes \cdots \otimes V_n \, .$$

Isso provou que $\mathbf{\Psi}$ é sobrejetora e estabeleceu o isomorfismo de espaços vetoriais

$$V_1 \otimes \cdots \otimes V_n \ \simeq \ \Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)' \, . \tag{2.137}$$

Note-se ainda que, por (2.136) e por (2.114) temos

$$\Big\langle \mathbf{\Psi} \left( T^{a_1 \cdots a_n} \, {\mathbf{e}^{(1)}}_{a_1} \otimes \cdots \otimes {\mathbf{e}^{(n)}}_{a_n} \right), \ \ \omega \Big\rangle \ = \ T^{a_1 \cdots a_n} \Big\langle \mathbf{m}_{a_1 \cdots a_n}, \ \omega \Big\rangle \ = \ \Big\langle T^{a_1 \cdots a_n} \mathbf{m}_{a_1 \cdots a_n}, \ \omega \Big\rangle$$

para todo $\omega \in \mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$ ($\mathbf{m}_{a_1 \cdots a_n}$ foram definidos em (2.113), página 213) e, portanto, vale

$$\mathbf{\Psi} \left( T^{a_1 \cdots a_n} {\mathbf{e}^{(1)}}_{a_1} \otimes \cdots \otimes {\mathbf{e}^{(n)}}_{a_n} \right) \ = \ T^{a_1 \cdots a_n} \mathbf{m}_{a_1 \cdots a_n} \, . \tag{2.138}$$

Para futura referência, resumimos os importantes fatos estabelecidos acima na seguinte proposição:

**Proposição 2.22** *Se $V_1, \ \ldots, \ V_n$, $n \in \mathbb{N}$, são espaços vetoriais de dimensão finita sobre o mesmo corpo, então*

$$V_1 \otimes \cdots \otimes V_n \ \simeq \ \Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)' \, , \tag{2.139}$$

*ou seja, o produto tensorial $V_1 \otimes \cdots \otimes V_n$ e o dual espaço dos funcionais $n$-lineares, ou seja, $\Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)'$, são espaços vetoriais canonicamente isomorfos.* □

Reunindo nossos resultados das Proposições 2.21 e 2.22, temos:

**Proposição 2.23** *Se $V_1, \ \ldots, \ V_n$, $n \in \mathbb{N}$, são espaços vetoriais de dimensão finita sobre o mesmo corpo, então*

$$V_1 \otimes \cdots \otimes V_n \ \simeq \ \Big((V_1)' \otimes \cdots \otimes (V_n)'\Big)' \ \simeq \ \Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)' \, . \tag{2.140}$$

*Pela Proposição 2.18, página 207, e pelo Teorema 2.13, página 208, segue de (2.140) (tomando-se o dual) que*

$$\big(V_1 \otimes \cdots \otimes V_n\big)' \ \simeq \ (V_1)' \otimes \cdots \otimes (V_n)' \ \simeq \ \mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big) \, . \tag{2.141}$$

*Essa relação também será evocada adiante.* □

• **Uma alternativa à definição de produto tensorial de espaços vetoriais**

A expressão (2.139) diz-nos que podemos, para todos os efeitos, identificar $V_1 \otimes \cdots \otimes V_n$ e o dual de $\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$, as formas $n$-lineares em $V_1 \oplus \cdots \oplus V_n$. Por isso, a igualdade (2.139) pode ser tomada como *definição* da noção de produto tensorial de espaços vetoriais, o que é feito por alguns autores. Note-se, porém, que essa segunda definição da noção de produto tensorial é restrita ao produto tensorial de espaços de dimensão finita. Nossa primeira definição de produto tensorial de espaços vetoriais (Seção 2.3.5, página 214) é mais geral, e se aplica mesmo ao caso de espaços de dimensão infinita.

Nenhuma das duas definições é "elementar" ou "simples" e pode-se adotar uma ou outra de acordo com a conveniência. A maioria dos textos sobre Topologia Diferencial ou Geometria Diferencial, por exemplo, prefere a segunda definição (2.137) (espaços tangentes e cotangentes a variedades de dimensão finita são espaços vetoriais de dimensão finita. Vide Seção 34, página 1802).

• **Novamente, identificações e convenções**

Como $\mathbf{\Psi} : V_1 \otimes \cdots \otimes V_n \to \Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)'$ é um isomorfismo, convenciona-se também identificar (sempre em dimensão finita) os espaços $V_1 \otimes \cdots \otimes V_n$ e $\Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)'$, ou seja, convenciona-se identificar um tensor $T^{a_1 \cdots a_n}\, \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n}$ com sua imagem por $\mathbf{\Psi}$. Com a mesma, (2.138) fica simplesmente

$$T^{a_1 \cdots a_n}\, \mathbf{e}^{(1)}{}_{a_1} \otimes \cdots \otimes \mathbf{e}^{(n)}{}_{a_n} \;\equiv\; T^{a_1 \cdots a_n} \mathbf{m}_{a_1 \cdots a_n}\,, \tag{2.142}$$

que identifica um tensor com o dual de uma forma multilinear ($\mathbf{m}_{a_1 \cdots a_n}$ foram definidos em (2.113), página 213).

Devido a (2.140) temos (sempre em dimensão finita) as identificações de $V_1 \otimes \cdots \otimes V_n$ com $\Big((V_1') \otimes \cdots \otimes (V_n')\Big)'$ e com $\Big(\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)\Big)'$. Evocaremos essas identificações no futuro, por vezes, sem maiores comentários.

Comentamos, por fim, que também adotaremos a convenção de identificar

$$T_{a_1 \cdots a_n}\, \mathbf{e}^{(1)a_1} \otimes \cdots \otimes \mathbf{e}^{(n)a_n} \;\equiv\; T_{a_1 \cdots a_n} \mathbf{m}^{a_1 \cdots a_n}\,, \tag{2.143}$$

assim como identificaremos $\Big(V_1 \otimes \cdots \otimes V_n\Big)'$ com $(V_1)' \otimes \cdots \otimes (V_n)'$ e com $\mathcal{M}\big(V_1 \oplus \cdots \oplus V_n\big)$, devido a (2.141).

## 2.3.6 Produtos Tensoriais de um Espaço Vetorial com seu Dual

Seja $V$ um espaço vetorial de dimensão finita. Adotaremos sua dimensão como sendo $m \in \mathbb{N}$ e consideraremos $V$ como sendo um espaço real. Em aplicações como à Geometria Diferencial e à Teoria da Relatividade (Especial e Geral), estamos muitas vezes interessados em tensores que sejam elementos de produtos tensoriais envolvendo $p$ fatores $V$ e $q$ fatores $V'$, como $\underbrace{V \otimes \cdots \otimes V}_{p \text{ vezes}} \otimes \underbrace{V' \otimes \cdots \otimes V'}_{q \text{ vezes}}$. Os elementos de tais espaços são denominados *tensores de tipo (ou posto)* $(p,\, q)$.

Outros ordenamentos também podem ocorrer no produto tensorial, tais como $V \otimes V' \otimes V$.

### 2.3.6.1 Tensores Associados a Formas Bilineares Simétricas Não Degeneradas. Métricas

Vamos tratar de um caso de particular importância na Física Relativística e na Geometria Diferencial: o caso de tensores de ordem dois associados a formas bilineares não-degeneradas e simétricas.

Com uso de uma forma bilinear não-degenerada e simétrica podemos constituir um isomorfismo entre $V$ e seu dual $V'$, assim como entre produtos tensoriais de $\underbrace{V \otimes \cdots \otimes V}_{p \text{ vezes}} \otimes \underbrace{V' \otimes \cdots \otimes V'}_{q \text{ vezes}}$ com seu espaço dual $\underbrace{V' \otimes \cdots \otimes V'}_{p \text{ vezes}} \otimes \underbrace{V \otimes \cdots \otimes V}_{q \text{ vezes}}$.

Esses isomorfismos estão relacionados às operações de "subir e abaixar índices" de tensores, bem conhecidas daqueles familiarizados com a Teoria da Relatividade. Aqui descreveremos o significado matemático dessas operações.

Uma nomenclatura que por vezes utilizaremos é a de chamar os elementos de $V'$ de *covetores*. Covetores são, portanto, duais de vetores.

• **Delta de Krönecker**

Se $i$, $j$ pertencem a algum conjunto discreto, definimos

$$\delta_{ij} \;\equiv\; \delta_i{}^j \;\equiv\; \delta^i{}_j \;\equiv\; \delta^{ij} \;:=\; \begin{cases} 1\,, & \text{se } i = j\,, \\ 0\,, & \text{se } i \neq j\,. \end{cases}$$

O símbolo $\delta$ assim definido é denominado *delta de Krönecker*[82].

[82] Leopold Krönecker (1823–1891).

• **Mais sobre bases duais. Mudanças de base**

Se $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_m\}$ é uma base em $V$, sua correspondente base dual canônica (para a definição, vide página 204) em $V'$ será aqui denotada por $\{\mathbf{e}^1,\ \ldots,\ \mathbf{e}^m\}$. Com isso, tem-se, por definição,

$$\Big\langle \mathbf{e}^i,\ \mathbf{e}_j \Big\rangle \ = \ \delta^i{}_j$$

para todos $i,\ j \in \{1,\ \ldots,\ m\}$. Vamos considerar uma nova base $\{\mathbf{f}_1,\ \ldots,\ \mathbf{f}_m\}$ em $V$ com $\mathbf{f}_k \ = \ \sum_{l=1}^{m} E_k{}^l \mathbf{e}_l$ ou, adotando a *convenção de Einstein*,

$$\mathbf{f}_k \ = \ E_k{}^l \mathbf{e}_l \tag{2.144}$$

com certos coeficientes reais $E_k{}^l$. Para que a nova base seja composta por vetores linearmente independentes a matriz de mudança de base $S$, cujos elementos são dados por $S_{ij} \equiv E_i{}^j$, deve ser inversível. Vamos denotar os elementos $(S^{-1})_{ij}$ da matriz inversa $S^{-1}$ por $E^i{}_j \equiv (S^{-1})_{ji}$. Naturalmente, $S^{-1}S = \mathbb{1}$ e $SS^{-1} = \mathbb{1}$, ou seja, $\sum_{k=1}^{m}(S^{-1})_{ik}S_{kj} = \delta_{ij}$ e $\sum_{k=1}^{m} S_{ik}(S^{-1})_{kj} = \delta_{ij}$. Com a notação acima, essas duas relações ficam (também na convenção de Einstein),

$$E^k{}_i E_k{}^j \ = \ \delta_i{}^j \ , \tag{2.145}$$

$$E_i{}^k E^j{}_k \ = \ \delta_i{}^j \ . \tag{2.146}$$

Definamos agora uma nova base $\{\mathbf{f}^1,\ \ldots,\ \mathbf{f}^m\}$ no espaço dual $V'$ por

$$\mathbf{f}^k \ = \ E^k{}_l \, \mathbf{e}^l \ . \tag{2.147}$$

Teremos,

$$\Big\langle \mathbf{f}^a,\ \mathbf{f}_b \Big\rangle \ = \ E^a{}_c E_b{}^d \underbrace{\Big\langle \mathbf{e}^c,\ \mathbf{e}_d \Big\rangle}_{=\delta^c{}_d} \ = \ E^a{}_c E_b{}^c \ \overset{(2.146)}{=} \ \delta^a{}_b \ ,$$

mostrando que as bases $\{\mathbf{f}^1,\ \ldots,\ \mathbf{f}^m\}$ e $\{\mathbf{f}_1,\ \ldots,\ \mathbf{f}_m\}$ são duais. É de se lembrar (vide comentário à página 205) que a base dual de $\{\mathbf{f}_1,\ \ldots,\ \mathbf{f}_m\}$ é única.

É importante frisar que para quaisquer $u \in V'$, $v \in V$, o pareamento $\langle u,\ v\rangle$ é invariante pelas mudanças de bases (2.144) e (2.147). Esse importante fato é um tanto evidente, mas recomendamos ao leitor incrédulo provar essa afirmação, como exercício.

**E. 2.133** *Exercício*. Com as convenções e definições acima, constate que os vetores de base $\mathbf{e}_i \in V$ e $\mathbf{e}^i \in V'$, $i = 1,\ \ldots,\ m$, podem ser obtidos a partir dos vetores de base $\mathbf{f}_k \in V$ e $\mathbf{f}^k \in V'$, $k = 1,\ \ldots,\ m$, respectivamente, pelas transformações

$$\mathbf{e}_i \ = \ E^k{}_i \mathbf{f}_k \qquad \text{e} \qquad \mathbf{e}^i \ = \ E^i{}_k \mathbf{f}^k \ ,$$

sendo $i = 1,\ \ldots,\ m$. ✠

• **Formas bilineares simétricas. Formas bilineares simétricas não-degeneradas**

Como antes, denotemos por $\mathcal{M}(V \oplus V)$ o espaço das formas bilineares em $V$. Uma forma bilinear $\omega : V \oplus V \to \mathbb{R}$ é dita ser uma *forma bilinear simétrica* se valer $\omega(u \oplus v) = \omega(v \oplus u)$ para todos $u,\ v \in V$. Uma forma bilinear simétrica $\omega : V \oplus V \to \mathbb{R}$ é dita ser uma *forma bilinear simétrica não-degenerada* se satisfizer a seguinte condição: $\omega(u \oplus v) = 0$ para todo $v \in V$ se e somente se $u = 0$.

• **Métricas e formas bilineares**

Seja $g \in \mathcal{M}(V \oplus V)$ uma forma bilinear simétrica e não-degenerada em $V$: $g : V \oplus V \ni (a \oplus b) \mapsto g(a \oplus b) \in \mathbb{R}$. Em uma base $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_m\}$ de $V$ podemos escrever um vetor $a \in V$ como $a = a^i \mathbf{e}_i$. Assim, teremos

$$g(a \oplus b) \ = \ g\Big(\big(a^i \mathbf{e}_i\big) \oplus \big(b^j \mathbf{e}_j\big)\Big) \ = \ g\left(\mathbf{e}_i \oplus \mathbf{e}_j\right) a^i b^j \ = \ g_{ij} a^i b^j \ ,$$

onde definimos

$$g_{ij} \ := \ g\left(\mathbf{e}_i \oplus \mathbf{e}_j\right) \ ,$$

as componentes (ditas "covariantes") de $g$ na base $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_m\}$ de $V$, e escrevemos $g = g_{ij}\mathbf{m}^{ij}$ ($\mathbf{m}^{ij}$ foi definido em (2.110)–(2.111), página 213). Recordemos que convencionamos identificar formas bilineares em $V \oplus V$ com tensores em $V' \otimes V'$ e, assim, temos

$$g \;=\; g_{ij}\mathbf{m}^{ij} \;=\; g_{ij}\mathbf{e}^i \otimes \mathbf{e}^j \;.$$

Vide (2.143). Com essas identificações, temos o pareamento

$$\big\langle g,\, a\otimes b\big\rangle \;=\; \Big\langle g_{ij}\mathbf{e}^i\otimes\mathbf{e}^j,\ \big(a^k\mathbf{e}_k\big)\otimes\big(b^l\mathbf{e}_l\big)\Big\rangle \;=\; g_{ij}a^kb^l\big\langle \mathbf{e}^i\otimes\mathbf{e}^j,\ \mathbf{e}_k\otimes\mathbf{e}_l\big\rangle$$

$$= g_{ij}a^kb^l\underbrace{\big\langle \mathbf{e}^i,\ \mathbf{e}_k\big\rangle}_{=\delta^i_k}\underbrace{\big\langle \mathbf{e}^j,\ \mathbf{e}_l\big\rangle}_{=\delta^j_l} \;=\; g_{ij}a^ib^j \;=\; g(a\oplus b)\;,$$

como esperado.

A condição de simetria implica que $g_{ij} = g_{ji}$ para todos os índices $i,\ j \in \{1,\ \ldots,\ m\}$. Assim, a forma bilinear simétrica $g$ possui $m(m+1)/2$ componentes independentes. Mais adiante exploraremos as implicações de supor $g$ como não-degenerada. Agora necessitamos saber como as componentes de $g$ transformam-se por mudança de base em $V$.

• **Comentários sobre a nomenclatura**

Uma forma bilinear simétrica e não-degenerada $g$ é também denominada *tensor pseudométrico*, *tensor métrico* ou simplesmente *pseudométrica* ou *métrica*, em $V$.

O leitor não deve confundir esse conceito de métrica com o conceito de métrica empregado em Topologia (uma generalização da noção de distância entre pontos), estudado no Capítulo 25, página 1410. Ainda que circunstancialmente haja uma certa relação entre essas noções em casos especiais (na Geometria Riemanniana, um tensor métrico pode sob hipóteses induzir uma métrica topológica em uma variedade), trata-se de uma coincidência de nomenclatura um tanto infeliz.

Outro ponto infeliz da nomenclatura comum refere-se à partícula "pseudo". Normalmente, uma forma simétrica e não-degenerada deveria ser denominada *tensor métrico* ou *métrica* se for também positivo. Uma forma simétrica, não-degenerada e não-positiva deveria ser denominada *tensor pseudométrico* ou *pseudométrica*. No entanto, na Teoria da Relatividade, é costume não empregar a partícula "pseudo", ainda que lá se lide com formas simétricas, não-degeneradas e não positivas.

• **Transformação das componentes de uma métrica por mudança de base**

Em uma nova base $\{\mathbf{f}_1,\ \ldots,\ \mathbf{f}_m\}$ em $V$ dada em termos da base $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_m\}$ por (2.144), as componentes de $g$ serão

$$g'_{ij} \;:=\; g\big(\mathbf{f}_i\oplus\mathbf{f}_j\big) \;=\; g\Big(E_i{}^k\mathbf{e}_k\oplus E_j{}^l\mathbf{e}_l\Big) \;=\; E_i{}^kE_j{}^l\,g\,(\mathbf{e}_k\oplus\mathbf{e}_l) \;=\; E_i{}^kE_j{}^lg_{kl}\;.$$

Assim,

$$g \;=\; g_{ij}\mathbf{e}^i\otimes\mathbf{e}^j \;=\; g'_{ij}\mathbf{f}^i\otimes\mathbf{f}^j\;,$$

com

$$g'_{ij} \;=\; E_i{}^kE_j{}^l\;g_{kl}\;. \tag{2.148}$$

A expressão (2.148) mostra como obter as componentes de $g$ na base $\{\mathbf{f}_1,\ \ldots,\ \mathbf{f}_m\}$ a partir das componentes de $g$ na base $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_m\}$.

• **A "inversa" de um tensor métrico**

A condição de não-degenerescência do tensor métrico implica que, em cada base $\{\mathbf{e}_1,\ \ldots,\ \mathbf{e}_m\}$ de $V$, a matriz $G$ com elementos $g_{ij}$, possui uma inversa. Os elementos de matriz dessa inversa $G^{-1}$ são denotados por $g^{ij}$, com índices superiores. Como veremos, essa distinção notacional de índices superiores e inferiores, ainda que não possua nenhum significado profundo em si, é muito conveniente e muito empregada em textos de Física. Observe-se que como $G$ é uma matriz simétrica, $G^{-1}$ também o é e vale a relação simetria $g^{ij} = g^{ji}$ para todos os índices $i,\ j$.

Naturalmente, $G^{-1}G = \mathbb{1}$ e $GG^{-1} = \mathbb{1}$, o que se escreve na forma

$$g^{ij}g_{jk} \;=\; \delta^i{}_k \qquad \text{e} \qquad g_{ij}g^{jk} \;=\; \delta_i{}^k\;. \tag{2.149}$$

Por uma mudança de sistema de coordenadas $G$ transforma-se segundo $G' = SGS^T$ com $S_{ab} = E_a{}^b$ (vide (2.148)). Logo, $G^{-1}$ transforma-se como $G'^{-1} = \big(S^{-1}\big)^T G^{-1} S^{-1}$. Os elementos de matriz de $S^{-1}$ são $\big(S^{-1}\big)_{ab} = E^b{}_a$ (vide (2.145)–(2.146)). Logo, a transformação dos elementos $g^{ij}$ é

$$g'^{ij} \;=\; E^i{}_k E^j{}_l g^{kl} \;. \tag{2.150}$$

**E. 2.134** *Exercício.* Verifique isso e constate que essa expressão respeita as relações (2.149), como esperado. ✠

Com os elementos $g^{ij}$ é possível definir uma forma bilinear $g^\sharp \in \mathcal{M}\big(V' \otimes V'\big)$, $g^\sharp : V' \oplus V' \to \mathbb{R}$, definida numa base $\{\mathbf{e}^1, \ldots, \mathbf{e}^m\}$ por

$$g^\sharp\Big(\big(a_i \mathbf{e}^i\big) \oplus \big(b_j \mathbf{e}^j\big)\Big) \;:=\; g^{ij} a_i b_j \;. \tag{2.151}$$

Observe-se que

$$g^\sharp\big(\mathbf{e}^i \oplus \mathbf{e}^j\big) \;=\; g^{ij} \;. \tag{2.152}$$

Como um tensor de tipo (0, 2), temos

$$g^\sharp \;=\; g^{ij} \mathbf{e}_i \otimes \mathbf{e}_j \;. \tag{2.153}$$

É importante notar que as expressões (2.151) e (2.153) são invariantes por mudanças de base. É suficiente provar essa afirmação para (2.153). De fato,

$$g'^\sharp \;=\; g'^{ij} \mathbf{f}_i \otimes \mathbf{f}_j \overset{(2.150)}{=} E^i{}_k E^j{}_l g^{kl} \Big(E_i{}^a \mathbf{e}_a\Big) \otimes \Big(E_j{}^b \mathbf{e}_b\Big) \;=\; \underbrace{E^i{}_k E_i{}^a}_{=\delta_k{}^a} \underbrace{E^j{}_l E_j{}^b}_{=\delta_l{}^b} g^{kl} \mathbf{e}_a \otimes \mathbf{e}_b \;=\; g^{kl} \mathbf{e}_k \otimes \mathbf{e}_l \;=\; g^\sharp \;,$$

como queríamos mostrar. Isso prova que $g^\sharp$ tem uma existência intrínseca, independente da base adotada.

Agora, um pouco da nomenclatura adotada em textos de Física. As componentes $g_{ij}$ do tensor métrico são também denominadas *componentes covariantes do tensor métrico*. As componentes de $g^\sharp$ em uma base são (por definição) $g^{ij}$ e são denominadas *componentes contravariantes do tensor métrico*. O tensor $g$ é também denominado *tensor métrico covariante* e o tensor $g^\sharp$ é também denominado *tensor métrico contravariante*.

• **Mapeando $V$ em $V'$ com os tensores métricos**

Por uma questão de simetria, vamos aqui denotar o tensor métrico $g$ por $g_\sharp$. Temos, portanto, em bases $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ e $\{\mathbf{e}^1, \ldots, \mathbf{e}^m\}$ de $V$ e $V'$, respectivamente,

$$g_\sharp \;=\; g_{ij}\, \mathbf{e}^i \otimes \mathbf{e}^j \qquad \text{e} \qquad g^\sharp \;=\; g^{ij}\, \mathbf{e}_i \otimes \mathbf{e}_j \;.$$

Os tensores $g_\sharp$ e $g^\sharp$ permitem-nos definir dois isomorfismos lineares entre os espaços $V$ em $V'$, os quais, por economia e similaridade, também denotamos por $\boldsymbol{g}_\sharp$ e $\boldsymbol{g}^\sharp$:

- Definimos $\boldsymbol{g}_\sharp : V \to V'$ como sendo a aplicação linear que a cada $a \in V$ associa um elemento $\boldsymbol{g}_\sharp(a) \in V'$ de forma que
$$\big\langle \boldsymbol{g}_\sharp(a),\, b\big\rangle \;=\; g_\sharp(a \oplus b) \tag{2.154}$$
seja válida para todo $b \in V$. Em uma base, escrevendo $a = a^i \mathbf{e}_i \in V$, $b = b^j \mathbf{e}_j \in V$, a definição (2.154) fica $(\boldsymbol{g}_\sharp(a))_j b^j \;=\; g_{ij} a^i b^j$, mostrando que $\boldsymbol{g}_\sharp(a) = \big(\boldsymbol{g}_\sharp(a)\big)_j \mathbf{e}^j \in V'$, com as componentes dadas por
$$\big(\boldsymbol{g}_\sharp(a)\big)_j \;=\; g_{ji} a^i \;.$$

- Definimos $\boldsymbol{g}^\sharp : V' \to V$ como sendo a aplicação linear que a cada $d \in V'$ associa um elemento $\boldsymbol{g}^\sharp(d) \in V$ de forma que
$$\big\langle c,\, \boldsymbol{g}^\sharp(d)\big\rangle \;=\; g^\sharp(c \oplus d) \tag{2.155}$$
seja válida para todo $c \in V'$. Em uma base, escrevendo $c = c_i \mathbf{e}^i \in V'$, $d = d_j \mathbf{e}^j \in V'$, a definição (2.155) fica $c_j (\boldsymbol{g}^\sharp(d))^j \;=\; g^{ij} c_j d_i$, mostrando que $\boldsymbol{g}^\sharp(d) = \big(\boldsymbol{g}^\sharp(d)\big)^j \mathbf{e}_j \in V$, com as componentes dadas por
$$\big(\boldsymbol{g}^\sharp(d)\big)^j \;=\; g^{ji} d_i \;.$$

Como $g_{ij}$ e $g^{ij}$ são matrizes inversíveis, é imediato que $\boldsymbol{g}_\sharp : V \to V'$ e $\boldsymbol{g}^\sharp : V' \to V$ são isomorfismos. Como é de se esperar, $\boldsymbol{g}^\sharp$ e $\boldsymbol{g}_\sharp$ são a inversa uma da outra. De fato, para todo $d = d_i \mathbf{e}^i \in V'$ tem-se

$$\boldsymbol{g}_\sharp\Big(\boldsymbol{g}^\sharp(d)\Big) \;=\; \boldsymbol{g}_\sharp\Big(\boldsymbol{g}^\sharp\big(d_i\mathbf{e}^i\big)\Big) \;=\; \boldsymbol{g}_\sharp\Big((g^{ji}d_i)\mathbf{e}_j\Big) \;=\; \underbrace{g_{kj}g^{ji}}_{=\delta_k{}^i}\, d_i\mathbf{e}^k \;=\; d_i\,\mathbf{e}^i \;=\; d\,,$$

ou seja, $\boldsymbol{g}_\sharp \circ \boldsymbol{g}^\sharp = \mathbf{id}_{V'}$. De maneira totalmente análoga demonstra-se que $\boldsymbol{g}^\sharp \circ \boldsymbol{g}_\sharp = \mathbf{id}_V$.

**E. 2.135** *Exercício.* Mostre que

$$\langle u,\, v\rangle \;=\; g_\sharp\Big(\boldsymbol{g}^\sharp(u)\oplus v\Big) \;=\; g^\sharp\Big(u\oplus \boldsymbol{g}_\sharp(v)\Big) \;=\; \langle \boldsymbol{g}_\sharp(v),\, \boldsymbol{g}^\sharp(u)\rangle\,, \tag{2.156}$$

para todos $u \in V'$ e $v \in V$. ✣

• **Subindo e abaixando índices vetores, covetores e tensores em geral**

Como vimos acima, a aplicação que leva um vetor $v \in V$ ao covetor $\boldsymbol{g}_\sharp(v) \in V'$ corresponde, no que concerne às suas componentes em uma base de coordenadas, a transformar as componentes $v^i$ nas componentes $\big(\boldsymbol{g}_\sharp(v)\big)_j = g_{ji}v^i$. Analogamente, a aplicação que leva um covetor $u \in V'$ ao vetor $\boldsymbol{g}^\sharp(u) \in V$ corresponde, no que concerne às suas componentes em uma base de coordenadas, a transformar as componentes $u_j$ nas componentes $\big(\boldsymbol{g}^\sharp(u)\big)^i = g^{ij}u_j$.

Como $\boldsymbol{g}_\sharp$ e $\boldsymbol{g}^\sharp$ são isomorfismos, é costume em textos de Física tratar $v \in V$ e $\boldsymbol{g}_\sharp(v) \in V'$ em pé de igualdade, assim como $u \in V'$ e $\boldsymbol{g}^\sharp(u) \in V$.

As componentes $v^i$ de $v \in V$ em uma base $\{\mathbf{e}_1,\, \ldots,\, \mathbf{e}_m\}$ são denominadas *componentes contravariantes* de $v$, enquanto que as componentes $\big(\boldsymbol{g}_\sharp(v)\big)_j$ de $\big(\boldsymbol{g}_\sharp(v)\big) \in V'$ na base dual $\{\mathbf{e}^1,\, \ldots,\, \mathbf{e}^m\}$ são denotadas simplesmente por $v_j$ e são denominadas *componentes covariantes* de $v$.

Analogamente, as componentes $u_j$ de $u \in V'$ na base dual $\{\mathbf{e}^1,\, \ldots,\, \mathbf{e}^m\}$ são denominadas *componentes covariantes* de $u$, enquanto que as componentes $\big(\boldsymbol{g}^\sharp(u)\big)^i$ de $\boldsymbol{g}^\sharp(u) \in V$ na base $\{\mathbf{e}_1,\, \ldots,\, \mathbf{e}_m\}$ são denotadas simplesmente por $u^j$ e são denominadas *componentes contravariantes* de $u$.

Com essas identificações

$$\big(\boldsymbol{g}_\sharp(v)\big)_j \;\equiv\; v_j \qquad \text{e} \qquad \big(\boldsymbol{g}^\sharp(u)\big)^i \;\equiv\; u^j$$

podemos escrever expressões como

$$u_jv^j \;=\; g_{ij}u^iv^j \;=\; g^{ij}u_iv_j \;=\; u^jv_j \tag{2.157}$$

como representações em componentes da igualdade (2.156).

**E. 2.136** *Exercício importante.* Verifique que, de fato, (2.157) expressa (2.156) em coordenadas nas bases $\{\mathbf{e}_1,\, \ldots,\, \mathbf{e}_m\}$ e $\{\mathbf{e}^1,\, \ldots,\, \mathbf{e}^m\}$. ✣

Esse tipo de notação, muito mais prática, é encontrada amiúde em livros sobre a Teoria da Relatividade Geral. Assim, de um ponto de vista notacional, no que concerne às componentes, a passagem de $v \in V$ a $\boldsymbol{g}_\sharp(v) \in V'$ e de $u \in V'$ a $\boldsymbol{g}^\sharp(u) \in V$ consiste em abaixar e, respectivamente, elevar os índices, transformações essas definidas pelas contrações $v_j = g_{ij}v^i$ e $u^i = g^{ij}u_j$, respectivamente, com as componentes dos tensores $g_\sharp$ e $g^\sharp$. Essas operações são inversas uma da outra, pois $\boldsymbol{g}_\sharp$ e $\boldsymbol{g}^\sharp$ são operações inversas, como já comentamos. Componentes de vetores, com índices em cima, são frequentemente denominadas *componentes contravariantes* e componentes de covetores, com índices em baixo, são frequentemente denominadas *componentes covariantes*.

Com tensores que sejam elementos de produtos tensoriais dos espaços $V$ e $V'$, as aplicações $\boldsymbol{g}_\sharp$ e $\boldsymbol{g}^\sharp$ estendem-se também de maneira óbvia, permitindo, analogamente, definir as operações de elevar e abaixar índices tensoriais. Assim, definimos

$$\underbrace{\boldsymbol{g}^\sharp\otimes\cdots\otimes\boldsymbol{g}^\sharp}_{p\text{ vezes}}\otimes\underbrace{\boldsymbol{g}_\sharp\otimes\cdots\otimes\boldsymbol{g}_\sharp}_{q\text{ vezes}}:\quad \underbrace{V'\otimes\cdots\otimes V'}_{p\text{ vezes}}\otimes\underbrace{V\otimes\cdots\otimes V}_{q\text{ vezes}} \;\longrightarrow\; \underbrace{V\otimes\cdots\otimes V}_{p\text{ vezes}}\otimes\underbrace{V'\otimes\cdots\otimes V'}_{q\text{ vezes}}$$

como a aplicação linear que leva o tensor

$$T_{i_1\cdots i_p}{}^{j_1\cdots j_q}\;\mathbf{e}^{i_1}\otimes\cdots\otimes\mathbf{e}^{i_p}\otimes\mathbf{e}_{j_1}\otimes\cdots\otimes\mathbf{e}_{j_q} \qquad \text{no tensor "dual"} \qquad T^{i_1\cdots i_p}{}_{j_1\cdots j_q}\;\mathbf{e}_{i_1}\otimes\cdots\otimes\mathbf{e}_{i_p}\otimes\mathbf{e}^{j_1}\otimes\cdots\otimes\mathbf{e}^{j_q}\,,$$

onde

$$T^{i_1\cdots i_p}{}_{j_1\cdots j_q} \;:=\; g^{i_1\,k_1}\cdots g^{i_p\,k_p}\; g_{j_1\,l_1}\cdots g_{j_q\,l_q}\; T_{k_1\cdots k_p}{}^{l_1\cdots l_q}\;.$$

Com essas operações de subida e abaixamento de índices em componentes de tensores gerais podemos constituir grandezas invariantes por mudanças de base, tais como $U^{i_1\cdots i_p}{}_{j_1\cdots j_q}\,V_{i_1\cdots i_p}{}^{j_1\cdots j_q}$.

### 2.3.7 Produtos Tensoriais de um mesmo Espaço Vetorial. Os Espaços Simétrico e Antissimétrico

Seja $U$ um espaço vetorial, não necessariamente de dimensão finita, sobre um corpo $\mathbb{K}$ (que suporemos, por simplicidade, tendo característica 0). Considere-se para cada $n \in \mathbb{N}$ o produto tensorial $U^{\otimes_{\mathbb{K}} n} \equiv \underbrace{U \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} U}_{n \text{ vezes}}$, que passaremos a denotar por $U^{\otimes n}$, omitindo o subíndice $\mathbb{K}$ dos símbolos $\otimes$ e $\oplus$. Adotamos por convenção que $U^{\otimes 0} = \mathbb{K}$ e $U^{\otimes 1} = U$.

Para $n \geq 2$ podemos definir uma representação $\mathcal{P}_n$ do grupo de permutações de $n$ elementos, $S_n$, em $U^{\otimes n}$, da seguinte forma: se $\pi$ é um elemento de $S_n$, definimos $\mathcal{P}_n(\pi) : U^{\otimes n} \to U^{\otimes n}$ como sendo o operador linear que a cada vetor da forma $u_1 \otimes \cdots \otimes u_n$ associa o vetor $u_{\pi(1)} \otimes \cdots \otimes u_{\pi(n)}$. Isso significa que $\mathcal{P}_n(\pi)$ age em vetores gerais de $U^{\otimes n}$ da forma

$$\mathcal{P}_n(\pi)\left(\sum_{k=1}^{l} \alpha_k\, u_1^k \otimes \cdots \otimes u_n^k\right) \;=\; \sum_{k=1}^{l} \alpha_k\, \mathcal{P}_n(\pi)\left(u_1^k \otimes \cdots \otimes u_n^k\right) \;=\; \sum_{k=1}^{l} \alpha_k\, u_{\pi(1)}^k \otimes \cdots \otimes u_{\pi(n)}^k\;,$$

onde os $\alpha_k$'s são elementos de $\mathbb{K}$. É elementar constatar que $\mathcal{P}_n(\pi)\mathcal{P}_n(\pi') = \mathcal{P}_n(\pi\pi')$ para todos $\pi,\ \pi' \in S_n$ e que $\mathcal{P}_n(\mathbf{id}\,) = \mathbb{1}$, $\mathbf{id}$ sendo a identidade (elemento neutro) de $S_n$. Isso confirma que $\mathcal{P}_n$ é uma representação de $S_n$ em $U^{\otimes n}$.

Para $n = 0$ e $n = 1$ convencionamos que $S_n$ é o grupo trivial (contendo apenas a identidade) e que em ambos os casos $\mathcal{P}_n(\mathbf{id}\,) = \mathbb{1}$, o operador identidade.

Definimos o *operador de simetrização* $\mathcal{S}_n : U^{\otimes n} \to U^{\otimes n}$ e o *operador de antissimetrização* $\mathcal{A}_n : U^{\otimes n} \to U^{\otimes n}$, para $n \geq 2$, por

$$\mathcal{S}_n \;:=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathcal{P}_n(\pi) \qquad \text{e} \qquad \mathcal{A}_n \;:=\; \frac{1}{n!}\sum_{\pi\in S_n} \text{sinal}\,(\pi)\,\mathcal{P}_n(\pi)\;, \tag{2.158}$$

respectivamente, onde $\text{sinal}\,(\pi)$ é o sinal, ou paridade, de $\pi \in S_n$. Para $n = 0$ e $n = 1$ definimos $\mathcal{S}_0 = \mathcal{A}_0 = \mathbb{1}$ e $\mathcal{S}_1 = \mathcal{A}_1 = \mathbb{1}$, o operador identidade.

A seguinte proposição contém as propriedades algébricas mais relevantes dos operadores $\mathcal{S}_n$ e $\mathcal{A}_n$.

**Proposição 2.24** *Com as definições e convenções acima, valem as seguintes afirmações:*

1. $\mathcal{S}_n\mathcal{P}_n(\pi) = \mathcal{P}_n(\pi)\mathcal{S}_n = \mathcal{S}_n$ *para todo* $n \geq 0$ *e todo* $\pi \in S_n$.
2. *Para todo* $n \geq 0$ *e todo* $\pi \in S_n$ *vale*

$$\mathcal{A}_n\mathcal{P}_n(\pi) \;=\; \mathcal{P}_n(\pi)\mathcal{A}_n \;=\; \text{sinal}\,(\pi)\mathcal{A}_n\;. \tag{2.159}$$

3. $\mathcal{S}_n^2 \;=\; \mathcal{S}_n$ *para todo* $n \geq 0$.
4. $\mathcal{A}_n^2 \;=\; \mathcal{A}_n$ *para todo* $n \geq 0$.
5. $\mathcal{S}_n\mathcal{A}_n = \mathcal{A}_n\mathcal{S}_n = 0$ *para todo* $n \geq 2$. *Para* $n = 0$ *e* $n = 1$ *valem* $\mathcal{S}_n\mathcal{A}_n = \mathcal{A}_n\mathcal{S}_n = \mathbb{1}$.

*Os fatos que* $\mathcal{S}_n^2 = \mathcal{S}_n$ *e* $\mathcal{A}_n^2 = \mathcal{A}_n$ *dizem-nos que* $\mathcal{S}_n$ *e* $\mathcal{A}_n$ *são projetores.* □

Prova. Que $\mathcal{S}_n\mathcal{P}_n(\pi) = \mathcal{P}_n(\pi)\mathcal{S}_n = \mathcal{S}_n$ vale para $n = 0$ e $n = 1$ é evidente. Seja $n \geq 2$. Teremos,

$$\mathcal{S}_n\mathcal{P}_n(\pi') \;=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathcal{P}_n(\pi)\,\mathcal{P}_n(\pi') \;=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathcal{P}_n(\pi\pi') \;\overset{\pi''=\pi\pi'}{=}\; \frac{1}{n!}\sum_{\pi''\in S_n} \mathcal{P}_n(\pi'') \;=\; \mathcal{S}_n\;.$$

Na terceira igualdade acima usamos o fato que, para cada $\pi'$ a aplicação $\pi \mapsto \pi\pi' \equiv \pi''$ é bijetora em $S_n$ e, portanto, somar sobre todo $\pi \in S_n$ equivale a somar sobre todo $\pi'' \in S_n$. A prova de que $\mathcal{P}_n(\pi')\mathcal{S}_n = \mathcal{S}_n$ é análoga.

Que $\mathcal{A}_n\mathcal{P}_n(\pi) = \mathcal{P}_n(\pi)\mathcal{A}_n = \mathcal{A}_n$ vale para $n = 0$ e $n = 1$ é evidente. Seja $n \geq 2$. Teremos,

$$\mathcal{A}_n\mathcal{P}_n(\pi') \;=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi)\mathcal{P}_n(\pi)\,\mathcal{P}_n(\pi') \;=\; \mathrm{sinal}\,(\pi')\frac{1}{n!}\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi\pi')\mathcal{P}_n(\pi\pi')$$

$$\stackrel{\pi''=\pi\pi'}{=} \frac{\mathrm{sinal}\,(\pi')}{n!}\sum_{\pi''\in S_n} \mathrm{sinal}\,(\pi'')\mathcal{P}_n(\pi'') \;=\; \mathrm{sinal}\,(\pi')\mathcal{A}_n\;.$$

Na segunda igualdade acima usamos o fato que, $\mathrm{sinal}\,(\pi\pi') = \mathrm{sinal}\,(\pi)\mathrm{sinal}\,(\pi')$. A prova de que $\mathcal{P}_n(\pi')\mathcal{A}_n = \mathrm{sinal}\,(\pi')\mathcal{A}_n$ é análoga.

Que $\mathcal{S}_n^2 = \mathcal{S}_n$ para $n = 0$ e $n = 1$ é evidente, pela definição. Para $n \geq 2$, segue das definições e do obtido acima que

$$\mathcal{S}_n^2 \;=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathcal{S}_n\mathcal{P}_n(\pi) \;=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathcal{S}_n \;=\; \left(\frac{1}{n!}\sum_{\pi\in S_n} 1\right)\mathcal{S}_n \;=\; \mathcal{S}_n\;,$$

pois $S_n$ possui $n!$ elementos.

Que $\mathcal{A}_n^2 = \mathcal{A}_n$ para $n = 0$ e $n = 1$ é evidente pela definição. Para $n \geq 2$, segue as definições e do obtido acima que

$$\mathcal{A}_n^2 \;=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi)\mathcal{A}_n\mathcal{P}_n(\pi) \;=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathcal{A}_n \;=\; \left(\frac{1}{n!}\sum_{\pi\in S_n} 1\right)\mathcal{A}_n \;=\; \mathcal{A}_n\;.$$

Que para $n = 0$ e $n = 1$ valem $\mathcal{S}_n\mathcal{A}_n = \mathcal{A}_n\mathcal{S}_n = \mathbb{1}$ é evidente pela definição. Para $n \geq 2$ provemos que $\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi) = 0$. De fato,

$$\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi) \;\stackrel{\pi=\pi'\pi''}{=}\; \sum_{\pi''\in S_n} \mathrm{sinal}\,(\pi'\pi'') \;=\; \mathrm{sinal}\,(\pi')\sum_{\pi''\in S_n} \mathrm{sinal}\,(\pi'') \;=\; \mathrm{sinal}\,(\pi')\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi)\;.$$

Na primeira igualdade escolhemos $\pi' \in S_n$ e definimos $\pi'' := (\pi')^{-1}\pi$. A aplicação $\pi \to (\pi')^{-1}\pi \equiv \pi''$ é bijetora e, portanto, somar sobre todo $\pi \in S_n$ equivale a somar sobre todo $\pi'' \in S_n$. Escolhendo $\pi'$ de forma que $\mathrm{sinal}\,(\pi') = -1$ (isso sempre é possível se $n \geq 2$) obtemos na última igualdade que $\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi) = 0$.

Assim, para $n \geq 2$, segue das definições e do obtido acima que

$$\mathcal{S}_n\mathcal{A}_n \;=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi)\mathcal{S}_n\mathcal{P}_n(\pi) \;=\; \frac{1}{n!}\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi)\mathcal{S}_n \;=\; \left(\frac{1}{n!}\sum_{\pi\in S_n} \mathrm{sinal}\,(\pi)\right)\mathcal{S}_n \;=\; 0\;.$$

A prova que $\mathcal{A}_n\mathcal{S}_n = 0$ para $n \geq 2$ é análoga. ■

As imagens dos projetores $\mathcal{S}_n$ e $\mathcal{A}_n$ são dois subespaços de $U^{\otimes n}$ denotados por $(U^{\otimes n})_S$ e $(U^{\otimes n})_A$, respectivamente, e denominados *subespaço simétrico* e *subespaço antissimétrico*, respectivamente. Para $n = 0$ e para $n = 1$ os subespaços simétrico e antissimétrico coincidem com $\mathbb{K}$ e $U$, respectivamente. Como $\mathcal{S}_n$ e $\mathcal{A}_n$ são projetores, os elementos de $(U^{\otimes n})_S$ são invariantes pela ação de $\mathcal{S}_n$ e os elementos de $(U^{\otimes n})_A$ são invariantes pela ação de $\mathcal{A}_n$. Os elementos de $(U^{\otimes n})_S$ são denominados *vetores simétricos* e os de $(U^{\otimes n})_A$ são denominados *vetores antissimétricos*.

Notação. A imagem por $n!\mathcal{A}_n$ de elementos da forma $u_1 \otimes \cdots \otimes u_n$, com $u_k \in U$ para todo $k$, será denotada por $u_1 \wedge_{\mathbb{K}} \cdots \wedge_{\mathbb{K}} u_n$, ou simplesmente por $u_1 \wedge \cdots \wedge u_n$:

$$u_1 \wedge \cdots \wedge u_n \;:=\; n!\,\mathcal{A}_n\big(u_1 \otimes \cdots \otimes u_n\big) \;=\; \sum_{\pi\in S_n} \mathrm{sinal}\,(\pi)\, u_{\pi(1)} \otimes \cdots \otimes u_{\pi(n)}\;. \tag{2.160}$$

Os elementos de $(U^{\otimes n})_A$ são, portanto, combinações lineares finitas de elementos da forma $u_1 \wedge \cdots \wedge u_n$. ◀

Exemplificamos. Para $n = 2$, $\mathcal{S}_2\big(u_1 \otimes u_2\big) = \frac{1}{2}\big(u_1 \otimes u_2 + u_2 \otimes u_1\big)$ é um elemento do subespaço simétrico $\big(U^{\otimes 2}\big)_S$ e $u_1 \wedge u_2 := 2!\,\mathcal{A}_2\big(u_1 \otimes u_2\big) = u_1 \otimes u_2 - u_2 \otimes u_1$ é um elemento do subespaço antissimétrico $\big(U^{\otimes 2}\big)_A$. Para $n = 3$,

$$\mathcal{S}_3\big(u_1 \otimes u_2 \otimes u_3\big) \;=\; \frac{1}{3!}\Big(u_1 \otimes u_2 \otimes u_3 + u_3 \otimes u_1 \otimes u_2 + u_2 \otimes u_3 \otimes u_1 + u_1 \otimes u_3 \otimes u_2 + u_2 \otimes u_1 \otimes u_3 + u_3 \otimes u_2 \otimes u_1\Big)$$

é um elemento do espaço simétrico $\big(U^{\otimes 3}\big)_S$, enquanto que

$$u_1 \wedge u_2 \wedge u_3 \;:=\; 3!\,\mathcal{A}_3\big(u_1 \otimes u_2 \otimes u_3\big) \;=\; u_1 \otimes u_2 \otimes u_3 + u_3 \otimes u_1 \otimes u_2 + u_2 \otimes u_3 \otimes u_1 - u_1 \otimes u_3 \otimes u_2 - u_2 \otimes u_1 \otimes u_3 - u_3 \otimes u_2 \otimes u_1$$

é um elemento do espaço antissimétrico $\big(U^{\otimes 3}\big)_A$. Acima, os $u_k$'s são elementos de $U$.

**E. 2.137** *Exercício.* Mostre que

$$u_1 \wedge \cdots \wedge u_n \;=\; \operatorname{sinal}(\pi) u_{\pi(1)} \wedge \cdots \wedge u_{\pi(n)} \;. \tag{2.161}$$

*Sugestão:* use que $\mathcal{A}_n \mathcal{P}_n(\pi) = \operatorname{sinal}(\pi)\mathcal{A}_n$.

Conclua que se dois dos vetores de $u_1, \ldots, u_n$ forem iguais, então $u_1 \wedge \cdots \wedge u_n = 0$. Conclua disso que se os vetores $u_1, \ldots, u_n$ não forem linearmente independentes, então $u_1 \wedge \cdots \wedge u_n = 0$. ✠

O exercício que segue indica algumas das consequências dos resultados do Exercício E. 2.137 no caso em que $U$ tem dimensão finita.

**E. 2.138** *Exercício.* Justifique as afirmações que seguem. Se $U$ é um espaço de dimensão finita $m$, então segue do exposto no Exercício E. 2.137 que $u_1 \wedge \cdots \wedge u_n = 0$ sempre que $n > m$ e que, portanto, $\big(U^{\otimes n}\big)_A = \{0\}$, o espaço vetorial trivial, sempre que $n > m$.

Se $m$ é a dimensão de $U$ e $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ uma base em $U$, então todo elemento $a \in U$ se escreve na forma $a = \sum_{k=1}^{m} \alpha^k \mathbf{e}_k$. Como todos os elementos de $\big(U^{\otimes l}\big)_A$, $l = 0, \ldots, m$, são combinações lineares finitas de elementos da forma $a_1 \wedge \cdots \wedge a_l$, com $a_j \in U$, $\forall j \in \{1, \ldots, l\}$, concluímos que os elementos da forma $\mathbf{e}_{k_1} \wedge \cdots \wedge \mathbf{e}_{k_l}$ com $k_1 < \ldots < k_l$ compõem uma base em $\big(U^{\otimes l}\big)_A$.

Um simples argumento combinatório demonstra que há $\binom{m}{l}$ $l$-uplas $(k_1, \ldots, k_l)$ com $k_j \in \{1, \ldots, m\}$ para todo $j$ e com $k_1 < \cdots < k_l$ e, portanto, $\big(U^{\otimes l}\big)_A$ tem dimensão $\binom{m}{l} = \frac{m!}{l!(m-l)!}$. Assim, todo elemento $\alpha$ de $\big(U^{\otimes l}\big)_A$ pode ser escrito na forma

$$\alpha \;=\; \sum_{1 \le k_1 < \ldots < k_l \le m} \alpha_{k_1 \cdots k_l}\, \mathbf{e}_{k_1} \wedge \cdots \wedge \mathbf{e}_{k_l} \;=\; \sum_{k_1=1}^{m} \cdots \sum_{k_l=1}^{m} \frac{\alpha_{k_1 \cdots k_l}}{l!}\, \mathbf{e}_{k_1} \wedge \cdots \wedge \mathbf{e}_{k_l} \;,$$

com $\alpha_{k_1 \cdots k_l} \in \mathbb{K}$, sendo que na última igualdade assumimos que as quantidades $\alpha_{k_1 \cdots k_l}$ são antissimétricas por permutações de seus índices, ou seja, satisfazem $\alpha_{k_{\pi(1)} \cdots k_{\pi(l)}} = \operatorname{sinal}(\pi)\alpha_{k_1 \cdots k_l}$ para todo $\pi \in S_l$ e todos $k_1, \ldots, k_l \in \{1, \ldots, m\}$. ✠

Um fato relevante das considerações acima é que $\big(U^{\otimes l}\big)_A$ e $\big(U^{\otimes m-l}\big)_A$ têm a mesma dimensão, $\binom{m}{l} = \frac{m!}{l!(m-l)!}$, sendo, portanto (não-canonicamente) isomorfos. Esse isomorfismo pode ser explorado quando da presença de formas bilineares não-degeneradas em $U$, conduzindo a uma estrutura de dualidade, a chamada *dualidade de Hodge*[83] entre os espaços $\big(U^{\otimes l}\big)_A$.

A discussão sobre produtos tensoriais de espaços vetoriais será continuada na Seção 2.5, página 241.

## 2.3.8 O Produto Tensorial de Módulos. Derivações

**• O produto tensorial de dois módulos sobre uma álgebra associativa**

Vamos aqui a uma definição que nos será importante. Sejam $M$ e $N$ dois bimódulos sobre uma álgebra associativa $A$, ambos supostos serem espaços vetoriais sobre o corpo dos complexos. Com os métodos expostos anteriormente de construção de produtos tensoriais de espaços vetoriais, podemos definir o espaço vetorial $M \otimes_{\mathbb{C}} N$. Entretanto, em certas aplicações desejamos definir um outro tipo de produto tensorial entre $M$ e $N$ que seja também um módulo sobre a mesma álgebra $A$.

Para tal, consideremos em $M \otimes_{\mathbb{C}} N$ e o conjunto de relações

$$\mathcal{R} \;:=\; \Big\{ r \in M \otimes_{\mathbb{C}} N \,\Big|\, r \;=\; (ma) \otimes_{\mathbb{C}} n - m \otimes_{\mathbb{C}} (an),\ \text{com } a \in A,\ m \in M,\ n \in N \Big\} \;. \tag{2.162}$$

[83] Sir William Vallance Douglas Hodge (1903–1975).

Definamos, então, $\mathsf{R}(\mathcal{R})$ como sendo o subespaço de $M \otimes_{\mathbb{C}} N$ composto por todas as combinações lineares finitas com coeficientes no corpo $\mathbb{C}$ de elementos de $\mathcal{R}$. Como $\mathsf{R}(\mathcal{R})$ é um subespaço de $M \otimes_{\mathbb{C}} N$, queda definido um novo produto tensorial, que denotamos por $M \otimes_A N$, dado pelo quociente de espaços vetoriais

$$M \otimes_A N \;:=\; \big(M \otimes_{\mathbb{C}} N\big)/\mathsf{R}(\mathcal{R})\,. \tag{2.163}$$

Podemos fazer de $M \otimes_A N$ um módulo, digamos à direita, sobre $A$ tomando o produto

$$a \cdot (m \otimes_A n) \;:=\; (ma) \otimes_A n = m \otimes_A (an)\,, \tag{2.164}$$

para todo $a \in A$ e todos $m \in M$, $n \in N$. Em verdade, esse produto deve ser linearmente estendido a todo $M \otimes_A N$, por

$$a \cdot \left( \sum_{j=1}^{k} m_j \otimes_A n_j \right) \;:=\; \sum_{j=1}^{k} (am_j) \otimes_A n_j \;=\; \sum_{j=1}^{k} m_j \otimes_A (an_j)\,,$$

para todo $k \in \mathbb{N}$ e todos $a \in A$, $m_j \in M$, $n_j \in N$, $j = 1,\, \ldots,\, k$.

**E. 2.139** *Exercício*. Verifique que essa expressão faz de $M \otimes_A N$, de fato, um módulo sobre $A$. ✠

O subíndice $A$ aposto ao símbolo $\otimes$ serve para recordar que um elemento da álgebra associativa $A$ pode ser passado de um lado para outro do símbolo $\otimes_A$, tal como na última igualdade em (2.164). Essa propriedade não é satisfeita pelo produto tensorial original $M \otimes_{\mathbb{C}} N$.

Faremos uso do assim definido produto tensorial $M \otimes_A N$ adiante. O mais importante para nós será a identidade $(ma) \otimes_A n = m \otimes_A (an)$ válida em todo $M \otimes_A N$ para todo $a \in A$. Uma outra construção que também irá interessar-nos é a seguinte. Seja $M$ um bimódulo sobre uma álgebra associativa $A$ e tomemos $V_n = M^{\otimes_A n} \equiv \underbrace{M \otimes_A \cdots \otimes_A M}_{n \text{ vezes}}$. Com os conceitos apresentados anteriormente temos definida a soma direta $\bigoplus_{n \in \mathbb{N}} M^{\otimes_A n}$.

• **Derivações**

Seja $A$ uma álgebra associativa sobre $\mathbb{C}$ com identidade $e$ e seja $\mathcal{M}$ um bimódulo sobre $A$. Uma aplicação linear $\delta :\, A \to \mathcal{M}$ é dita ser uma *derivação* de $A$ em $\mathcal{M}$ se satisfaz a regra de Leibniz[84]:

$$\delta(ab) \;=\; a\delta(b) + \delta(a)b\,, \tag{2.165}$$

para todos $a,\, b \in A$.

Vamos a alguns exemplos.

*Exemplo 1.* Seja $A$ uma álgebra sobre $\mathbb{C}$ com unidade $e$ e $\mathcal{M} = A \otimes_{\mathbb{C}} A$ com os seguintes produtos de bimódulo:

$$a \cdot (b \otimes c) \;:=\; (ab) \otimes c\,, \tag{2.166}$$

$$(b \otimes c) \cdot a \;:=\; b \otimes (ca)\,. \tag{2.167}$$

Deixa-se ao leitor verificar a associatividade dos produtos de bimódulo nesse caso. Defina-se

$$\delta(a) \;:=\; a \otimes e - e \otimes a\,. \tag{2.168}$$

Deixa-se ao leitor verificar a validade da regra de Leibniz nesse exemplo. Note-se também que, por essa definição, $\delta(e) = 0$.

*Exemplo 2.* Seja $A$ uma álgebra associativa sobre $\mathbb{C}$, com unidade $e$ e $\mathcal{M} = A \otimes_{\mathbb{C}} A$, com os seguintes produtos de bimódulo:

$$a \cdot (b \otimes c) \;:=\; (ab) \otimes c\,, \tag{2.169}$$

$$(b \otimes c) \cdot a \;:=\; b \otimes (ca) - (bc) \otimes a\,. \tag{2.170}$$

[84] Gottfried Wilhelm von Leibniz (1646–1716).

Deixa-se ao leitor verificar a associatividade dos produtos de bimódulo nesse caso. Defina-se

$$\delta(a) \;:=\; e \otimes a \;. \tag{2.171}$$

Deixa-se ao leitor verificar a validade da regra de Leibniz nesse exemplo. Note-se também que, por essa definição, $\delta(e) = e \otimes e \neq 0$.

*Exemplo 3.* Exemplo importante de derivações pode ser visto em álgebras de Lie. Seja $\mathcal{A}$ uma álgebra de Lie vista como um bimódulo sobre si mesma. Seja $z$ um elemento fixo da álgebra e seja a aplicação $d_z : \mathcal{A} \to \mathcal{A}$ dada por $d_z(a) = [z,\, a]$. É fácil verificar (faça!) usando a identidade de Jacobi (2.37) que

$$d_z\big([a,\, b]\big) \;=\; \big[d_z(a),\, b\big] + \big[a,\, d_z(b)\big]$$

para todo $a,\, b \in \mathcal{A}$. Assim, tem-se que a cada $z \in \mathcal{A}$ é associada uma derivação $d_z$.

# 2.4 Anéis e Álgebras. Estruturas e Construções Básicas

## 2.4.1 Ideais em Anéis e Álgebras Associativas

A noção de ideal, introduzida por Dedekind[85] e depois aprofundada e generalizada por Hilbert[86] e Noether[87], desempenha um papel central no estudo de álgebras e anéis. Apesar de algumas definições gerais que seguem aplicarem-se tanto para anéis quanto para anéis não associativos vamos nos restringir, por simplicidade, aos primeiros.

### 2.4.1.1 Ideais em Anéis

• **Subgrupo gerado por um subconjunto de um anel (e alguma notação)**

Seja $A$ um anel e, como tal, dotado de uma operação de produto "$\cdot$" (símbolo esse que, por simplicidade, omitiremos no que segue) e de uma operação de soma "+" em relação à qual é um grupo Abeliano, segundo as definições da Seção 2.1.6.1, página 143.

Se $B \subset A$ é um subconjunto não vazio de $A$, o conjunto $\mathscr{G}[B] \subset A$ definido por

$$\mathscr{G}[B] \;:=\; \Big\{ m_1 b_1 + \cdots + m_n b_n \;,\quad n \in \mathbb{N} \;,\;\; m_k \in \mathbb{Z} \;\text{ e }\; b_k \in B \;\text{ para todo } k = 1,\, \ldots,\, n \Big\} \;,$$

formado por todas as somas finitas de múltiplos inteiros de elementos de $B$, é o menor subgrupo de $A$ que contém $B$, o chamado *subgrupo gerado pelo subconjunto $B$ de $A$*.

É de se observar que se $B$ e $C$ são subconjuntos não vazios de $A$, então $\mathscr{G}[B \cup C]$ contém $\mathscr{G}[B]$ e $\mathscr{G}[C]$ como subgrupos.

Se $B$ e $C$ são subconjuntos não vazios de $A$ denotamos por $BC$ o conjunto de todos os elementos de $A$ que são da forma $bc$ com $b \in B$ e $c \in C$:

$$BC \;:=\; \Big\{ bc \;,\;\; \text{com } b \in B \;\text{ e }\; c \in C \Big\} \;.$$

Com isso, é fácil ver que $\mathscr{G}[B]\mathscr{G}[C] \subset \mathscr{G}[BC]$.

Se $B$, $C$ e $D$ são subconjuntos não vazios de $A$ denotamos por $BCD$ os conjuntos $(BC)D = B(CD)$ (essa igualdade dando-se em função da assumida associatividade de $A$):

$$BCD \;:=\; \Big\{ bcd \;,\;\; \text{com } b \in B \;,\; c \in C \;\text{ e }\; d \in D \Big\} \;.$$

• **Ideais à esquerda, à direita e bilaterais em anéis**

Seja $A$ um anel. Um subconjunto $L$ de $A$ que seja um subgrupo de $A$ em relação à operação "+" é dito ser um *ideal à esquerda* de $A$ se $al \in L$ para todo $a \in A$ e todo $l \in L$. Um subconjunto $R$ de $A$ que seja um subgrupo de $A$ em relação

[85] Julius Wilhelm Richard Dedekind (1831–1916).
[86] David Hilbert (1862–1943).
[87] Amalie Emmy Noether (1882–1935).

à operação "+" é dito ser um *ideal à direita* de $A$ se $ra \in R$ para todo $a \in A$ e todo $r \in R$. Um subconjunto $B$ de $A$ é dito ser um *bi-ideal* de $A$, ou um *ideal bilateral* de $A$, se for simultaneamente um ideal à direita e um ideal à esquerda de $A$.

Naturalmente, se $A$ é um anel, $A$ é um ideal bilateral de si mesmo, assim como $\{0\}$ é um ideal bilateral (trivial) de $A$.

É claro também que se $L$ é um ideal à esquerda de um anel $A$, então $L$ é um módulo à esquerda sobre $A$ e analogamente para ideais à direita e ideais bilaterais.

• **Homomorfismos e ideais bilaterais**

Sejam $A$ e $B$ dois anéis e seja $\phi : A \to B$ um homomorfismo. Então, $\mathrm{Ker}(\phi) = \{a \in A |\ \phi(a) = 0\}$ é um ideal bilateral de $A$. De fato, $0 \in \mathrm{Ker}(\phi)$, se $a,\ a' \in \mathrm{Ker}(\phi)$, então $\phi(a + a') = \phi(a) + \phi(a') = 0$ e se $a \in \mathrm{Ker}(\phi)$, então $-a \in \mathrm{Ker}(\phi)$, pois $\phi(-a) = -\phi(a) = 0$, provando que $\mathrm{Ker}(\phi)$ é um subgrupo de $A$. Fora isso, se $b \in \mathrm{Ker}(\phi)$, então para todo $a \in A$ vale $\phi(ab) = \phi(a)\phi(b) = \phi(a)0 = 0$ e, analogamente, para todo $c \in A$ vale $\phi(bc) = \phi(b)\phi(c) = 0\phi(c) = 0$.

A afirmação feita acima, que $\mathrm{Ker}(\phi)$ é um ideal bilateral, apesar de elementar, tem aplicações e consequências em diversas áreas.

• **Intersecções de ideais**

Seja $A$ um anel e sejam $L_\lambda$ com $\lambda \in \Lambda$ ($\Lambda$ sendo um conjunto arbitrário de índices) uma família de ideais à esquerda de $A$. É muito fácil verificar pelas definições (faça-o!) que $\bigcap_{\lambda\in\Lambda} L_\lambda$ é também um ideal à esquerda de $A$. Afirmação análoga vale para ideais à direita e ideais bilaterais.

• **Ideais gerados por subconjuntos de um anel**

Seja $C \subset A$ um subconjunto não vazio de um anel $A$. Então, a intersecção de todos os ideais à esquerda de $A$ que contêm $C$ é também um ideal à esquerda, que é dito ser o *ideal à esquerda gerado pelo conjunto* $C$. Definições análogas valem para ideais à direita e ideais bilaterais.

Denotaremos por $\mathscr{I}_E[A,\ C]$ (ou simplesmente por $\mathscr{I}_E[C]$, quando o anel $A$ for subentendido) o ideal à esquerda gerado por $C \subset A$. Analogamente, denotamos por $\mathscr{I}_D[A,\ C]$ (ou simplesmente por $\mathscr{I}_D[C]$) e por $\mathscr{I}_B[A,\ C]$ (ou simplesmente por $\mathscr{I}_B[C]$) os ideais à direita e bilaterais, respectivamente, gerados por $C \subset A$.

No caso de anéis associativos é possível explicitar mais os elementos de ideais gerados por conjuntos.

**Proposição 2.25** *Seja $C \subset A$ um subconjunto não vazio de um anel associativo $A$. Tem-se que:*

1. $\mathscr{I}_E\big[A,\ C\big] = \mathscr{G}\big[(AC) \cup C\big]$*, ou seja, o ideal à esquerda gerado por* $C$*,* $\mathscr{I}_E\big[A,\ C\big]$*, consiste em todos os elementos de* $A$ *formados por somas finitas de produtos de elementos de* $A$ *com elementos de* $C$ *(nessa ordem) mais somas finitas de elementos de* $C$ *com coeficientes inteiros. Naturalmente, se* $A$ *é unital, então* $\mathscr{I}_E\big[A,\ C\big] = \mathscr{G}\big[AC\big]$*.*
2. $\mathscr{I}_D\big[A,\ C\big] = \mathscr{G}\big[(CA) \cup C\big]$*, ou seja, o ideal à direita gerado por* $C$*,* $\mathscr{I}_D\big[A,\ C\big]$*, consiste em todos os elementos de* $A$ *formados por somas finitas de produtos de elementos de* $C$ *com elementos de* $A$ *(nessa ordem) mais somas finitas de elementos de* $C$ *com coeficientes inteiros. Naturalmente, se* $A$ *é unital, então* $\mathscr{I}_E\big[A,\ C\big] = \mathscr{G}\big[CA\big]$*.*
3. $\mathscr{I}_B\big[A,\ C\big] = \mathscr{G}\big[(ACA) \cup (AC) \cup (CA) \cup C\big]$*. Naturalmente, se* $A$ *é unital, então* $\mathscr{I}_E[A,\ C] = \mathscr{G}[ACA]$*.* □

Prova. É evidente que $\mathscr{G}\big[(AC) \cup C\big]$ é um ideal à esquerda de $A$ e que contém $C$ e, portanto, $\mathscr{I}_E\big[A,\ C\big] \subset \mathscr{G}\big[(AC) \cup C\big]$. Por outro lado, $\mathscr{I}_E\big[A,\ C\big]$, por ser um ideal à esquerda de $A$ que contém $C$, necessariamente contém todos os elementos de $AC$ e de $C$ e o subgrupo gerado por tais elementos (um ideal de $A$ é um subgrupo de $A$), ou seja, $\mathscr{I}_E[A,\ C]$ deve conter todos os elementos de $\mathscr{G}\big[(AC) \cup C\big]$. Isso estabelece que $\mathscr{I}_E\big[A,\ C\big]$ e $\mathscr{G}\big[(AC) \cup C\big]$ são iguais. Os dois outros casos são análogos. ■

**E. 2.140** *Exercício*. Complete os detalhes faltantes da demonstração acima. ✠

• **Ideais principais**

Se $A$ é um anel e $a \in A$, os ideais gerados pelo conjunto de um elemento $C = \{a\}$ são denominados por alguns autores os *ideais principais* gerados por $a$.

Denotamos por $aA$ o conjunto $aA := \{aa' |\ a' \in A\}$ e por $Aa$ o conjunto $Aa := \{a'a |\ a' \in A\}$. É muito fácil constatar que $\mathscr{I}_E[\{a\}]$, o ideal principal à esquerda gerado por $a$, coincide com $Aa$ e que $\mathscr{I}_D[\{a\}]$, o ideal principal à direita gerado por $a$, coincide com $aA$.

Observe-se que o conjunto $AaA := \{a'aa'' |\ a',\ a'' \in A\}$ **não** é um ideal de $A$, por não ser um subgrupo de $A$.

• **Somas de ideais**

Se $L_1$ e $L_2$ são dois ideais à esquerda de um anel $A$, então sua soma, definida por $L_1+L_2 := \{l_1+l_2\ ,\ \ l_1 \in L_1 \text{ e } l_2 \in L_2\}$ é também, como facilmente se verifica, um ideal à esquerda de $A$. Esse ideal é dito ser a *soma* dos ideais $L_1$ e $L_2$. Afirmação análoga vale tanto para somas de dois ideais à direita quanto para somas de ideais bilaterais.

• **Estrutura de reticulado em anéis**

Seja $A$ um anel. Para dois ideais à esquerda $L_1$ e $L_2$ de $A$ defina-se as operações $L_1 \wedge L_2 := L_1 \cap L_2$ e $L_1 \vee L_2 := L_1 + L_2$. A coleção de todos os ideais à esquerda de $A$ é um *reticulado* (para a definição, vide página 119 e seguintes) em relação a essas duas operações. Afirmação análoga vale tanto para a coleção de todos os ideais à direita de $A$ quanto para a coleção de todos os ideais bilaterais de $A$.

**E. 2.141** *Exercício*. Prove as afirmações acima. ✠

• **Produtos de ideais**

Seja $B$ um subconjunto não vazio de $A$. Se $L$ é um ideal à esquerda de $A$ o conjunto $\mathscr{G}\big[LB\big]$ é igualmente um ideal à esquerda de $A$, denominado o ideal produto de $L$ por $B$. Analogamente, se $R$ é um ideal à direita de $A$ o conjunto $\mathscr{G}\big[BR\big]$ é igualmente um ideal à direita de $A$, denominado o ideal produto de $B$ por $R$. Por fim, se $L$ é um ideal à esquerda de $A$ e $R$ é um ideal à direita de $A$, então $\mathscr{G}\big[LR\big]$ é um ideal bilateral de $A$, denominado o bi-ideal produto de $L$ por $R$.

• **Quocientes de anéis por ideais bilaterais**

Vamos agora a uma das mais importantes construções ligadas à noção de anel: a de anel quociente de um anel por um seu ideal bilateral. Essa construção guarda forte semelhança à de grupo quociente, introduzida na Seção 2.2.2, página 173.

Seja $A$ um anel e $B$ um ideal bilateral de $A$. Podemos definir em $A$ uma relação de equivalência declarando $a \sim a'$ se $a - a' \in B$ para $a,\ a' \in A$.

Por essa definição é evidente que $a \sim a$ para todo $a \in A$. É também evidente que, se $a \sim a'$, então $a' \sim a$ para todos $a,\ a' \in A$. Por fim, se $a \sim a'$ e $a' \sim a''$, então $a - a'' = (a - a') + (a' - a'') \in B$, pois $a - a' \in B$, $a' - a'' \in B$ e $B$ é um subgrupo de $A$, provando que $a \sim a''$. Isso estabeleceu que "$\sim$", definida acima, é, de fato, uma relação de equivalência em $A$. Assim, $A$ particiona-se em classes de equivalência por essa relação de equivalência. Seja $[a]$ a classe de equivalência de um elemento $a \in A$. Podemos fazer da coleção das classes de equivalência, que denotaremos por $A/B$, um anel definindo

$$[a_1] + [a_2] \ := \ [a_1 + a_2] \qquad \text{e} \qquad [a_1]\,[a_2] \ := \ [a_1 a_2]\ ,$$

$a_1,\ a_2 \in A$. Antes de mostrar que essas operações fazem de $A/B$ um anel, é preciso provar que elas estão bem definidas enquanto operações entre classes. Mas, de fato, se $a_1,\ a_2 \in A$ e $b_1,\ b_2 \in B$, tem-se $(a_1+b_1)+(a_2+b_2) = a_1+a_2+(b_1+b_2)$, e como $b_1 + b_2 \in B$, segue que a soma $[a_1]+[a_2]$ não depende do particular representante tomado das classes $[a_1]$ e $[a_2]$, o resultado sendo sempre um elemento da classe $[a_1 + a_2]$. Analogamente, $(a_1 + b_1)(a_2 + b_2) = a_1a_2 + (a_1b_2 + b_1a_2 + b_1b_2)$. Como $a_1b_2 + b_1a_2 + b_1b_2 \in B$ (note que a propriedade de **bi**-lateralidade do ideal $B$ é usada aqui), segue que o produto $[a_1][a_2]$ não depende do particular representante tomado das classes $[a_1]$ e $[a_2]$, o resultado sendo sempre um elemento da classe $[a_1a_2]$.

É evidente pelas definições que $[a_1] + [a_2] = [a_2] + [a_1]$ para todos $[a_1],\ [a_2] \in A/B$. É também fácil ver que $[0] = B$. Logo, $[0]$ é o elemento neutro de $A/B$ pela operação de soma. Cada $[a] \in A/B$, tem no elemento $[-a]$ seu inverso aditivo, pois $[a] + [-a] = [a - a] = [0]$. Logo $A/B$ é um grupo comutativo para a operação "+". Agora, para todos $[a_1]$, $[a_2]$ e

$[a_3] \in A/B$ vale $\big([a_1][a_2]\big)[a_3] = [a_1a_2][a_3] = [a_1a_2a_3] = [a_1]\big([a_2][a_3]\big)$, provando que o produto é associativo. Por fim,

$$[a_1]\big([a_2]+[a_3]\big) \;=\; [a_1][a_2+a_3] \;=\; \big[a_1(a_2+a_3)\big] \;=\; \big[a_1a_2+a_1a_3\big] \;=\; [a_1a_2]+[a_1a_3] \;=\; [a_1][a_2]+[a_1][a_3]$$

e

$$\big([a_2]+[a_3]\big)[a_1] \;=\; [a_2+a_3][a_1] \;=\; \big[(a_2+a_3)a_1\big] \;=\; \big[a_2a_1+a_3a_1\big] \;=\; [a_2a_1]+[a_3a_1] \;=\; [a_2][a_1]+[a_3][a_1] \;,$$

estabelecendo a distributividade do produto na soma. Isso demonstrou que $A/B$ é um anel.

O anel $A/B$ é denominado *anel quociente* de $A$ pelo ideal bilateral $B$, ou *anel fator* de $A$ por $B$. Diversas estruturas algébricas importantes são construídas na forma de quocientes de anéis por ideais bilaterais e teremos a oportunidade de apresentar algumas.

Notemos, por fim, que se $A$ possui uma identidade 1, então $[1]$ é a identidade de $A/B$, pois, para todo $[a] \in A/B$ vale $[a][1] = [a1] = [a]$. Fora isso, se $A$ é comutativo, $A/B$ também o é, pois $[a][b] = [ab] = [ba] = [b][a]$ para todos $a,\ b \in A$. A recíproca não é necessariamente verdadeira: $A/B$ pode ser comutativo sem que $A$ o seja.

### • Anéis gerados por relações

Seja $A$ um anel. É por vezes muito importante construir um novo anel a partir de $A$ identificando alguns elementos selecionados de $A$. Se, por exemplo, $a$ e $b$ são elementos distintos de $A$ pode ser de nosso interesse impor que valha uma relação como $a = b$, ou como $a^2 = b$, ou ainda como $aba = b^3$, ou várias delas simultaneamente. Isso equivale a impor que alguns elementos de $A$ (como os elementos $a - b$, ou $a^2 - b$ ou ainda $aba - b^3$, nos exemplos acima) sejam nulos. Combinando alguns ingredientes apresentados acima uma tal construção é possível.

Seja $A$ um anel e seja $C$ um subconjunto não vazio de $A$. Seja $\mathscr{I}_B[A,\ C] \equiv \mathscr{I}_B[C]$ o ideal bilateral gerado por $C$ e seja o anel $A/\mathscr{I}_B[C]$. Pela construção, se $x \in \mathscr{I}_B[C]$, então $[x] = [0]$. Como $C \subset \mathscr{I}_B[C]$, segue que se $c \in C$, vale $[c] = [0]$. Como se vê, essa construção permite o efeito desejado se impor a nulidade de certos elementos de $A$, a saber os de $C$ (e todos os demais de $\mathscr{I}_B[C]$, os quais são da forma de somas finitas de elementos como $c$ ou $aca'$, com $a,\ a' \in A$ e $c \in C$).

O anel $A/\mathscr{I}_B[C]$ é dito ser o *anel gerado* pelo subconjunto $C \subset A$, ou o *anel gerado* pelo conjunto de relações $C \subset A$. O anel $A/\mathscr{I}_B[C]$ será por vezes denotado por $\mathscr{R}[A,\ C]$ ou simplesmente por $\mathscr{R}[C]$, quando $A$ for subentendido.

Um exemplo relevante de uma tal construção é o seguinte. Seja $A$ um anel não comutativo. Podemos construir um anel comutativo a partir de $A$ considerando o conjunto $C = \{ab - ba,\ \text{com}\ a,\ b \in A\}$ e construindo o anel $\mathscr{R}[A,\ C] = A/\mathscr{I}_B[C]$. Os elementos de $\mathscr{R}[A,\ C]$ são classes $[a]$ com $a \in A$. Para todos $a,\ b \in A$ teremos que $[a][b] - [b][a] = [ab - ba] = [0]$, pois $ab - ba \in C \subset \mathscr{I}_B[C]$, que é a classe do elemento 0. Com isso, vê-se que $\mathscr{R}[A,\ C]$ é um anel comutativo, por vezes denominado a *Abelianização* do anel $A$.

**E. 2.142** *Exercício*. Seja o anel $\mathbb{Z}$, formado pelos inteiros, com as operações usuais de soma e produto. Seja $C = \{n\}$, com $n$ um inteiro positivo. Mostre que $\mathscr{R}[\mathbb{Z},\ \{n\}]$ coincide com $\mathbb{Z}_n$. ✻

Construções como a do anel gerado por um subconjunto $C$ são particularmente potentes quando combinadas à construção da álgebra tensorial de espaços vetoriais, que introduziremos na Seção 2.5, página 241.

### • Ideais próprios, primos e maximais e algumas de suas propriedades

Vamos agora a algumas definições úteis. Seja $A$ um anel.

Um ideal $I$ de $A$ é dito ser um *ideal próprio* se $I$ for um subconjunto próprio de $A$. É fácil constatar que se $A$ é um anel com identidade 1, então um ideal $I$ é próprio se e somente se $1 \notin I$. Essa observação elementar tem consequências diversas sobre propriedades estruturais de ideais, como veremos adiante.

Um ideal próprio de $I$ de $A$ é dito ser um *ideal primo* se para todos $a$ e $b \in A$ para os quais valha $ab \in I$ tem-se ou que $a \in I$ ou que $b \in I$ (ou ambos).

Um ideal próprio $M$ de $A$ é dito ser um *ideal maximal* se não houver em $A$ nenhum outro ideal próprio que contém $M$.

**Proposição 2.26** *Se $A$ é um anel comutativo com uma unidade* 1*, então todo ideal maximal de $A$ é um ideal primo.* □

Prova. Como $A$ é comutativo, todo ideal de $A$ é bilateral. Sejam $a,\ b \in A$ tais que $ab \in M$. Se $a \in M$ a prova está completa. Vamos, então, supor que $a \notin M$. O conjunto $Aa$ é um ideal, pois para todo $a' \in A$ vale $a'ab \in a'M \subset M$. Fora isso, $Aa$ não é um subconjunto de $M$ pois, como $A$ é unital, $Aa$ contém o elemento $1a = a \notin M$. Assim, a soma $Aa + M$ é um ideal bilateral de $A$ que contém $M$ como subconjunto próprio e que deve conter a unidade, pois se assim não fosse seria um ideal próprio de $A$ que contém $M$ propriamente, contrariando a maximalidade de $M$. Logo, existem $a' \in A$ e $m \in M$ tais que $a'a + m = 1$. Logo, $a'ab + mb = b$. Agora, $a'ab \in M$ e $mb = bm \in M$. Logo, $b \in M$. ■

As proposições que seguem contém informações importantes sobre a relação entre ideais primos, ideais maximais e quocientes.

**Proposição 2.27** *Seja $A$ um anel comutativo com unidade e $P$ um ideal primo em $A$. Então, $A/P$ é um anel de integridade.* □

Prova. Vimos acima que a comutatividade de $A$ implica a comutatividade de $A/P$ e que $A/P$ é unital, pois $A$ o é, a unidade sendo [1]. Tudo o que precisamos é provar que $A/P$ não tem divisores de zero. Suponhamos que $A/P$ tenha divisores de zero, ou seja, que existam $[a] \neq [0]$ e $[b] \neq [0]$ tais que $[a][b] = [0]$. Isso significa que $[ab] = [0]$, ou seja, que $ab \in I$. Pela hipótese, isso significa ou que $a \in I$ (o que implica $[a] = [0]$) ou que $b \in I$ (o que implica $[b] = [0]$) ou ambos. Isso é uma contradição e com ela completa-se a demonstração. ■

A seguinte proposição é empregada na teoria dos anéis e álgebras comutativas e na topologia algébrica.

**Proposição 2.28** *Seja $A$ um anel comutativo com unidade e $M$ um ideal maximal em $A$. Então, $A/M$ é um corpo.* □

Prova. Vimos acima que a comutatividade de $A$ implica a comutatividade de $A/M$ e que $A/M$ é unital, pois $A$ o é, a unidade sendo [1]. Vimos também (Proposição 2.26) que $M$ é um anel primo e, portanto, $A/M$ é um anel de integridade (Proposição 2.27). Tudo o que precisamos é provar que todo elemento não nulo $[a]$ de $A/M$ tem uma inversa.

Primeiramente, notemos que se $a \in A$ tem uma inversa $a^{-1}$, então $[a^{-1}]$ é a inversa de $[a]$, pois $[a][a^{-1}] = [aa^{-1}] = [1]$. Vamos, então, considerar elementos $a \in A$ que não tenham inversa em $A$. A condição que $[a]$ seja um elemento não nulo de $A/M$ significa que $a \notin M$.

Fixado um tal $a$, consideremos o conjunto $aA$. O fato de $a$ não ter inversa em $A$ equivale a dizer que $1 \notin aA$. O conjunto $aA$ é um ideal à direita, mas também um ideal à esquerda, pois, devido à comutatividade de $A$, vale $aA = Aa$. Assim, $aA$ é um ideal bilateral que não contém 1. Notemos também que $aA$ não é um subconjunto de $M$ pois, como $A$ é unital, $aA$ contém o elemento $a1 = a \notin M$.

A soma $M + aA$ é igualmente um ideal bilateral de $A$, mas $M + aA$ contém o elemento 1 pois, se assim não fosse, $M + aA$ seria um ideal bilateral próprio de $A$ que contém $M$ propriamente (já que $aA$ não é um subconjunto de $M$), contrariando a hipótese que $M$ é maximal. Assim $1 \in M + aA$, o que significa que existem $m \in M$ e $a' \in A$ tais que $m + aa' = 1$, ou seja, $aa' = 1 - m$, o que implica $[aa'] = [1]$ e, portanto, $[a][a'] = [1]$. Isso prova que $[a]$ tem uma inversa multiplicativa, a saber, $[a]^{-1} = [a']$. ■

### 2.4.1.2 Ideais em Álgebras Associativas

As definições e construções acima, sobre ideais em anéis, podem ser estendidas para o contexto de álgebras associativas. Lembrando que toda álgebra associativa é um anel, um ponto relevante a considerar é a estrutura linear introduzida pelo corpo de escalares $\mathbb{K}$ com os quais podemos multiplicar os vetores da álgebra em questão. Aqui não repetiremos todas as construções acima no mesmo nível de detalhe, por tal ser claramente dispensável, e nos ateremos apenas aos fatos mais importantes para os desenvolvimentos ulteriores. Vamos primeiramente às definições adequadas de ideais em álgebras.

• **Subespaço gerado por subconjunto de uma álgebra associativa e alguma notação**

Seja $A$ uma álgebra associativa sobre um corpo $\mathbb{K}$. Como tal, $A$ é dotada de uma operação associativa de produto "$\cdot$" (símbolo esse que, por simplicidade, omitiremos no que segue) e de uma operação de soma "+" em relação à qual é um grupo Abeliano, sendo também um espaço vetorial sobre $\mathbb{K}$.

Se $B \subset A$ é um subconjunto não vazio de $A$, o conjunto $\mathscr{E}[B] \subset A$ definido por

$$\mathscr{E}[B] := \left\{ \alpha_1 b_1 + \cdots + \alpha_n b_n \, , \quad n \in \mathbb{N} \, , \ \alpha_k \in \mathbb{K} \ \text{ e } \ b_k \in B \ \text{ para todo } k = 1, \, \ldots, \, n \right\} ,$$

e formado por todas as combinações lineares finitas de elementos de $B$ com coeficientes em $\mathbb{K}$, é o menor subespaço de $A$ que contém $B$, o chamado *subespaço gerado pelo subconjunto $B$ de $A$*.

É de se observar que se $B$ e $C$ são subconjuntos não vazios de $A$, então $\mathscr{E}[B \cup C]$ contém $\mathscr{E}[B]$ e $\mathscr{E}[C]$ como subespaços.

Analogamente ao caso de anéis, se $B$ e $C$ são subconjuntos não vazios de $A$ denotamos por $BC$ o conjunto de todos os elementos de $A$ que são da forma $bc$ com $b \in B$ e $c \in C$: $BC := \left\{ bc, \ \text{ com } b \in B \text{ e } c \in C \right\}$. Com isso, é fácil ver que $\mathscr{E}[B]\mathscr{E}[C] \subset \mathscr{E}[BC]$. Se $B$, $C$ e $D$ são subconjuntos não vazios de $A$ também denotamos por $BCD$ os conjuntos $(BC)D = B(CD)$ (essa igualdade dando-se em função da assumida associatividade de $A$): $BCD := \left\{ bcd, \ \text{ com } b \in B, \ c \in C \text{ e } \ d \in D \right\}$.

**• Ideais à esquerda, à direita e bilaterais em álgebras associativas**

Seja $A$ uma álgebra associativa sobre um corpo $\mathbb{K}$. Um subconjunto $L$ de $A$ que seja um subespaço vetorial sobre $\mathbb{K}$ de $A$ é dito ser um *ideal algébrico à esquerda* de $A$ se $al \in L$ para todo $a \in A$ e todo $l \in L$. Um subconjunto $R$ de $A$ que seja um subespaço vetorial sobre $\mathbb{K}$ de $A$ é dito ser um *ideal algébrico à direita* de $A$ (ou simplesmente um *ideal à direita* de $A$) se $ra \in L$ para todo $a \in A$ e todo $r \in R$. Um subconjunto $B$ de $A$ é dito ser um *bi-ideal algébrico* ou um *ideal bilateral algébrico* de $A$ for simultaneamente um ideal à direita e um ideal à esquerda de $A$. Por vezes omitiremos o qualificativo "algébrico" e falaremos apenas de ideais à esquerda ou à direita ou bilaterais, tal como no caso de anéis.

**• Homomorfismos e ideais algébricos bilaterais**

Sejam $A$ e $B$ duas álgebras associativas e seja $\phi : A \to B$ um homomorfismo algébrico. Então, $\mathrm{Ker}(\phi) = \{a \in A |\ \phi(a) = 0\}$ é um ideal bilateral algébrico de $A$. A prova dessa importante afirmação é análoga à do caso de anéis e os detalhes são deixados como exercício.

**• Intersecções de ideais**

Seja $A$ uma álgebra associativa e sejam $L_\lambda$ com $\lambda \in \Lambda$ ($\Lambda$ sendo um conjunto arbitrário de índices) uma família de anéis algébricos à esquerda de $A$. É muito fácil verificar pelas definições (faça-o!) que $\bigcap_{\lambda \in \Lambda} L_\lambda$ é também um ideal algébrico à esquerda de $A$. Afirmação análoga vale para ideais algébricos à direita e ideais algébricos bilaterais.

**• Ideais algébricos gerados por subconjuntos de uma álgebra associativa**

Assim como no caso de anéis, a noção de ideais algébricos gerados por subconjuntos de uma álgebra associativa permite construções de grande relevância.

Seja $C \subset A$ um subconjunto não vazio de uma álgebra associativa $A$. Então, a intersecção de todos os ideais algébricos à esquerda de $A$ que contém $C$ é também um ideal algébrico à esquerda, que é dito ser o *ideal algébricos à esquerda gerado pelo conjunto $C$*. Definições análogas valem para ideais algébricos à direita e ideais algébricos bilaterais.

Denotaremos por $\mathscr{I}_E[A, \, C]$ (ou simplesmente por $\mathscr{I}_E[C]$, quando a álgebra $A$ for subentendida) o ideal algébrico à esquerda gerado por $C \subset A$. Analogamente, denotamos por $\mathscr{I}_D[A, \, C]$ (ou simplesmente por $\mathscr{I}_D[C]$) e por $\mathscr{I}_B[A, \, C]$ (ou simplesmente por $\mathscr{I}_B[C]$) os ideais algébricos à direita e bilaterais, respectivamente, gerados por $C \subset A$.

No caso de álgebras associativas é possível explicitar mais os elementos de ideais algébricos gerados por conjuntos.

**Proposição 2.29** *Seja $C \subset A$ um subconjunto não vazio de uma álgebra associativa $A$. Tem-se que:*

1. *$\mathscr{I}_E\big[A, \, C\big] = \mathscr{E}\big[(AC) \cup C\big]$, ou seja, o ideal algébrico à esquerda gerado por $C$, $\mathscr{I}_E\big[A, \, C\big]$, consiste em todos os elementos de $A$ formados por combinações lineares finitas com coeficientes em $\mathbb{K}$ de produtos de elementos de $A$ com elementos de $C$ (nessa ordem) mais combinações lineares finitas com coeficientes em $\mathbb{K}$ de elementos de $C$. Naturalmente, se $A$ é unital, então $\mathscr{I}_E\big[A, \, C\big] = \mathscr{E}\big[AC\big]$.*

2. *$\mathscr{I}_D\big[A, \, C\big] = \mathscr{E}\big[(CA) \cup C\big]$, ou seja, o ideal algébrico à direita gerado por $C$, $\mathscr{I}_D\big[A, \, C\big]$, consiste em todos os elementos de $A$ formados por combinações lineares finitas com coeficientes em $\mathbb{K}$ de produtos de elementos de $C$*

*com elementos de $A$ (nessa ordem) mais combinações lineares finitas com coeficientes em $\mathbb{K}$ de elementos de $C$. Naturalmente, se $A$ é unital, então $\mathscr{I}_E\big[A,\,C\big] = \mathscr{E}\big[CA\big]$.*

3. *$\mathscr{I}_B\big[A,\,C\big] = \mathscr{E}\big[(ACA)\cup(AC)\cup(CA)\cup C\big]$. Naturalmente, se $A$ é unital, então $\mathscr{I}_E[A,\,C] = \mathscr{E}[ACA]$.* □

A prova é análoga ao caso de anéis e deixada como exercício.

• **Somas de ideais algébricos**

Se $L_1$ e $L_2$ são dois ideais algébricos à esquerda de uma álgebra associativa $A$, então sua soma, definida por $L_1+L_2 := \{l_1+l_2\ ,\ \ l_1\in L_1 \text{ e } l_2\in L_2\}$ é também, como facilmente se verifica, um ideal algébrico à esquerda de $A$. Esse ideal é dito ser a *soma* dos ideais algébricos $L_1$ e $L_2$. Afirmação análoga vale tanto para somas de dois ideais algébricos à direita quanto para somas de ideais algébricos bilaterais.

• **Estrutura de reticulado**

Seja $A$ uma álgebra associativa. Para dois ideais algébricos à esquerda $L_1$ e $L_2$ de $A$ defina-se as operações $L_1\wedge L_2 := L_1\cap L_2$ e $L_1\vee L_2 := L_1+L_2$. A coleção de todos os ideais algébricos à esquerda de $A$ é um *reticulado* (para a definição, vide página 119 e seguintes) em relação a essas duas operações. Afirmação análoga vale tanto para a coleção de todos os ideais algébricos à direita de $A$ quanto para a coleção de todos os ideais algébricos bilaterais de $A$.

**E. 2.143** *Exercício*. Prove as afirmações acima. ✠

• **Produtos de ideais algébricos**

Se $L$ é um ideal algébrico à esquerda de $A$ o conjunto $\mathscr{E}\big[LC\big]$ é igualmente um ideal algébrico à esquerda de $A$, denominado o ideal algébrico produto de $L$ por $C$. Analogamente, se $R$ é um ideal algébrico à direita de $A$ o conjunto $\mathscr{E}\big[BR\big]$ é igualmente um ideal algébrico à direita de $A$, denominado o ideal algébrico produto de $B$ por $R$. Por fim, se $L$ é um ideal algébrico à esquerda de $A$ e $R$ é um ideal algébrico à direita de $A$, então $\mathscr{E}\big[LR\big]$ é um ideal algébrico bilateral de $A$, denominado o bi-ideal algébrico produto de $L$ por $R$.

• **Quocientes de álgebras associativas por ideais bilaterais**

É bastante claro ao leitor que com as definições acima podemos reproduzir as construções que realizamos no caso de anéis, pois álgebras associativas são anéis e subespaços de álgebras são também subgrupos das mesmas em relação à operação de adição. De particular importância é a construção de quocientes. Se $A$ é uma álgebra associativa e $B$ é um ideal bilateral algébrico de $A$, então nossas construções prévias permitem definir o anel $A/B$ composto das classes características $[a]$, com $a\in A$, sendo a relação de equivalência em $A$ dada por $a\sim a'$ se $a-a'\in B$. Podemos fazer de $A/B$ uma álgebra por meio da estrutura linear

$$\alpha_1[a_1]+\alpha_2[a_2] \ :=\ [\alpha_1a_1+\alpha_2a_2]\ ,$$

definida para todos $\alpha_1,\ \alpha_2\in\mathbb{K}$ e todos $a_1,\ a_2\in A$. Primeiramente precisamos provar que a expressão acima está bem definida enquanto operação entre classes. Porém, se $a_1,\ a_2\in A$ e $b_1,\ b_2\in B$, então $\alpha_1(a_1+b_1)+\alpha_2(a_2+b_2) = \alpha_1a_1+\alpha_2a_2+(\alpha_1b_1+\alpha_2b_2)$. Como $\alpha_1b_1+\alpha_2b_2\in B$ (pois $B$ é um subespaço de $A$), segue que $\alpha_1[a_1]+\alpha_2[a_2]$ não depende do particular representante adotado das classes $[a_1]$ e $[a_2]$, fornecendo sempre a classe $[\alpha_1a_1+\alpha_2a_2]$.

Isso estabelece que o anel $A/B$ é uma álgebra associativa em relação sobre o corpo $\mathbb{K}$, denominada *álgebra quociente* da álgebra associativa $A$ com o ideal bilateral algébrico $B$, ou *álgebra fator* de $A$ por $B$.

• **Álgebras geradas por relações**

Seja $A$ uma álgebra associativa. É por vezes muito importante construir um nova álgebra associativa a partir de $A$ identificando alguns elementos selecionados de $A$. Se, por exemplo, $a$ e $b$ são elementos distintos de $A$ pode ser de nosso interesse impor que valha uma relação como $a=b$, ou como $a^2=b$, ou ainda como $aba=b^3$, ou várias delas simultaneamente. Isso equivale a impor que alguns elementos de $A$ (como os elementos $a-b$, ou $a^2-b$ ou ainda $aba-b^3$, nos exemplos acima) sejam nulos. Combinando alguns ingredientes apresentados acima uma tal construção é possível.

Seja $A$ uma álgebra associativa e seja $C$ um subconjunto não vazio de $A$. Seja $\mathscr{I}_B[A,\ C] \equiv \mathscr{I}_B[C]$ o ideal algébrico bilateral gerado por $C$ e seja a álgebra associativa $A/\mathscr{I}_B[C]$. Pela construção, se $x \in A/\mathscr{I}_B[C]$, então $[x] = [0]$. Como $C \subset \mathscr{I}_B[C]$, segue que se $c \in C$, vale $[c] = [0]$. Como se vê, essa construção permite o efeito desejado se impor serem nulos certos elementos de $A$, a saber os de $C$ (e todos os demais de $\mathscr{I}_B[C]$, os quais são da forma de somas finitas de elementos como $c$ ou $aca'$, com $a,\ a' \in A$ e $c \in C$).

A álgebra associativa $A/\mathscr{I}_B[C]$ é dito ser a *álgebra gerada* pelo subconjunto $C \subset A$, ou a *álgebra gerada* pelo conjunto de relações $C \subset A$. A álgebra associativa $A/\mathscr{I}_B[C]$ será por vezes denotado por $\mathscr{A}[A,\ C]$ ou simplesmente por $\mathscr{A}[C]$, quando $A$ for subentendido.

Um exemplo relevante de uma tal construção é o seguinte. Seja $A$ uma álgebra associativa não comutativa. Podemos construir uma álgebra associativa comutativa a partir de $A$ considerando o conjunto $C = \{ab - ba,\ \text{com}\ a,\ b \in A\}$ e construindo a álgebra $\mathscr{A}[A,\ C] = A/\mathscr{I}_B[C]$. Os elementos de $\mathscr{A}[A,\ C]$ são classes $[a]$ com $a \in A$. Para todos $a,\ b \in A$ teremos que $[a][b] - [b][a] = [ab - ba] = [0]$, pois $ab - ba \in C \subset \mathscr{I}_B[C]$, que é a classe do elemento 0. Com isso, vê-se que $\mathscr{A}[A,\ C]$ é uma álgebra associativa e comutativa, por vezes denominado a *Abelianização* da álgebra associativa $A$.

Construções como a da álgebra gerada por um subconjunto $C$ são particularmente potentes quando combinadas à construção da álgebra tensorial de espaços vetoriais, que introduziremos na Seção 2.5, página 241. Na Seção 2.1.7.5, página 152, mostramos como quocientes por certos ideais em álgebras tensoriais podem ser empregadas na definição das chamadas Álgebras de Clifford, de relevância na Física Quântica.

# 2.5 Espaços de Fock, Álgebras Tensoriais e Álgebras Exteriores

Começamos nossa discussão sobre álgebras tensoriais apresentando a noção de espaço de Fock associado a um espaço vetorial, uma construção muito importante na Mecânica Quântica, na Teoria Quântica de Campos e na Mecânica Estatística Quântica, sendo também relevante em certas áreas da Matemática, como na Teoria dos Grupos de Lie e outras.

• **O espaço de Fock**

Seja $U$ um espaço vetorial (não necessariamente de dimensão finita) sobre um corpo $\mathbb{K}$. Na Seção 2.3.5, página 214, definimos o produto tensorial $U^{\otimes_{\mathbb{K}} n}$ que aqui iremos denotar simplificadamente por $U^{\otimes n}$ (doravante omitiremos o subíndice $\mathbb{K}$ dos símbolos $\otimes$ e $\oplus$). Pela convenção adotada naquela seção, temos $U^{\otimes n} = \mathbb{K}$ quando $n = 0$. Agregando a isso a definição de somas diretas de coleções arbitrárias de espaços vetoriais, apresentada na Seção 2.3.4, página 211, podemos definir o espaço vetorial

$$\mathscr{T}(U) \ := \ \bigoplus_{n=0}^{\infty} U^{\otimes n} \ .$$

O espaço $\mathscr{T}(U)$ é denominado o *espaço de Fock*[88] associado[89] ao espaço vetorial $U$.

Na Seção 2.3.7, página 230, definimos também os espaços simétrico e antissimétrico $(U^{\otimes n})_S$ e $(U^{\otimes n})_A$, respectivamente. Com eles, podemos analogamente definir os espaços

$$\mathscr{T}_S(U) \ := \ \bigoplus_{n=0}^{\infty} \left(U^{\otimes n}\right)_S \qquad \text{e} \qquad \mathscr{T}_A(U) \ := \ \bigoplus_{n=0}^{\infty} \left(U^{\otimes n}\right)_A$$

que são os subespaços simétrico e antissimétrico de $\mathscr{T}(U)$, respectivamente. Acima, para $n = 0$ convencionamos que $\left(U^{\otimes 0}\right)_S = \left(U^{\otimes 0}\right)_A = \mathbb{K}$ e para $n = 1$ convencionamos que $\left(U^{\otimes 1}\right)_S = \left(U^{\otimes 1}\right)_A = U$.

Os espaços $\mathscr{T}_S(U)$ e $\mathscr{T}_A(U)$ são denominados o *espaço de Fock simétrico* e o *espaço de Fock antissimétrico*, respectivamente, associados ao espaço vetorial $U$.

Antes de prosseguirmos, comentemos que as construções de $\mathscr{T}(U)$, $\mathscr{T}_S(U)$ e $\mathscr{T}_A(U)$, acima, são puramente algébricas. Em diversos casos é possível introduzir topologias nelas caso $U$ seja também um espaço vetorial topológico. Isso se dá

[88] Vladimir Aleksandrovich Fock (1898–1974).

[89] Os espaços de Fock foram introduzidos em V. Fock, "*Konfigurationsraum und zweite Quantelung*", Z. Phys. **75**, 622–647 (1932).

no importante caso em que $U$ é um espaço de Hilbert. Vide para tal Seção 41.3, página 2316. Por ora, não entraremos no estudo geral de espaços de Fock topológicos.

### 2.5.1 Álgebras Tensoriais

Lembremos que, de acordo com a definição de soma direta, cada vetor $\underline{v}$ de $\mathscr{T}(U)$ é da forma $v_0 \oplus v_1 \oplus v_2 \oplus \cdots$, com $v_k \in U^{\otimes n}$ para todo $k$, mas somente um número finito de $v_k$'s é não nulo. É função disso, é possível definir em $\mathscr{T}(U)$ um produto que o transforma em uma álgebra associativa: para $\underline{a} \in \bigoplus_{n=0}^{\infty} U^{\otimes n}$ e $\underline{b} \in \bigoplus_{n=0}^{\infty} U^{\otimes n}$ da forma $\underline{a} = \sum_k \alpha_k\, a_0^k \oplus a_1^k \oplus a_2^k \oplus \cdots$ e $\underline{b} = \sum_l \beta_l\, b_0^l \oplus b_1^l \oplus b_2^l \oplus \cdots$, as duas somas sendo finitas, com $\alpha_k \in \mathbb{K}$ e $\beta_l \in \mathbb{K}$ e com $a_i^k \in U^{\otimes i}$, $b_j^l \in U^{\otimes j}$ para todos $k,\, l,\, i$ e $j$, definimos um produto, que denotamos por $\underline{a} \otimes \underline{b}$, por

$$\begin{aligned}\left(\sum_k \alpha_k\, a_0^k \oplus a_1^k \oplus a_2^k \oplus \cdots\right) \otimes \left(\sum_l \beta_l\, b_0^l \oplus b_1^l \oplus b_2^l \oplus \cdots\right) &:= \sum_{k,\,l} \alpha_k \beta_l \left(a_0^k \oplus a_1^k \oplus a_2^k \oplus \cdots\right) \otimes \left(b_0^l \oplus b_1^l \oplus b_2^l \oplus \cdots\right) \\ &= \sum_{k,\,l} \alpha_k \beta_l \bigoplus_{p=0}^{\infty} \left[\sum_{q=0}^{p} a_q^k \otimes b_{p-q}^l\right] \\ &= \bigoplus_{p=0}^{\infty} \left[\sum_{q=0}^{p} \left(\sum_k \alpha_k\, a_q^k\right) \otimes \left(\sum_l \beta_l\, b_{p-q}^l\right)\right], \qquad (2.172)\end{aligned}$$

Acima, usamos diversas vezes as propriedades de distributividade estabelecidas no Exercício E. 2.132, página 221. Os elementos $a_q^k \otimes b_{p-q}^l$ são definidos pelo isomorfismo canônico: se

$$\underline{x} \,=\, \sum_r \chi_r\, x_1^r \otimes \cdots \otimes x_m^r \in U^{\otimes m} \qquad \text{e} \qquad \underline{y} \,=\, \sum_s \xi_s\, y_1^s \otimes \cdots \otimes y_n^s \in U^{\otimes n}$$

com as somas sendo finitas e $\chi_r,\, \xi_s \in \mathbb{K}$ para todos $r,\, s$, então

$$\underline{x} \otimes \underline{y} \,\equiv\, \sum_r \sum_s \chi_r \xi_s\, x_1^r \otimes \cdots \otimes x_m^r \otimes y_1^s \otimes \cdots \otimes y_n^s \in U^{\otimes(m+n)}\,.$$

Aqui, usamos o isomorfismo canônico $U^{\otimes m} \otimes U^{\otimes n} \to U^{\otimes(m+n)}$ (vide (2.123)) para identificar $\left(x_1^r \otimes \cdots \otimes x_m^r\right) \otimes \left(y_1^s \otimes \cdots \otimes y_n^s\right)$ e $x_1^r \otimes \cdots \otimes x_m^r \otimes y_1^s \otimes \cdots \otimes y_n^s$.

Observe-se que, devido ao fato de que apenas uma coleção finita de componentes $a_i^k$ e $b_j^l$ ser não nula, então apenas uma coleção finita de elementos da forma $\sum_{q=0}^{p} a_q^k \otimes b_{p-q}^l$, com $p = 0,\, \ldots,\, \infty$, será não nula também (Exercício E. 2.144), provando que o produto acima realmente resulta em elementos de $\mathscr{T}(U)$ e, portanto, define um produto em $\mathscr{T}(U)$.

**E. 2.144** *Exercício*. Sejam $a_i \in U^{\otimes i}$ e $b_j \in U^{\otimes j}$ para todos $i,\, j = 0,\, 1,\, \ldots,\, \infty$. Mostre que se $a_i = 0$ para todo $i > M$ e $b_j = 0$ para todo $j > N$, então $\sum_{q=0}^{p} a_q \otimes b_{p-q} = 0$ para todo com $p > M + N$. ✠

O espaço vetorial $\mathscr{T}(U)$ torna-se, assim, uma álgebra, denominada *álgebra tensorial* de $U$. Essa álgebra é associativa e unital, como se vê nos próximos exercícios.

**E. 2.145** *Exercício*. Mostre que o produto definido acima é associativo. Para tal, observe que, para $\underline{x} = x_1 \otimes \cdots \otimes x_m$, $\underline{y} = y_1 \otimes \cdots \otimes y_n$ e $\underline{z} = z_1 \otimes \cdots \otimes z_o$ o isomorfismo canônico mapeia $\left(\underline{x} \otimes \underline{y}\right) \otimes \underline{z}$ e $\underline{x} \otimes \left(\underline{y} \otimes \underline{z}\right)$ em $\underline{x} \otimes \underline{y} \otimes \underline{z}$. ✠

**E. 2.146** *Exercício*. Seja $\underline{e} \in \mathscr{T}(U)$ da forma $\underline{e} := 1 \oplus 0 \oplus 0 \oplus \cdots$, onde $1$ é a unidade do corpo $\mathbb{K}$. Mostre, usando a definição de produto dada acima, que $\underline{1}\,\underline{b} = \underline{b}$ para todo $\underline{b} \in \mathscr{T}(U)$. ✠

Álgebras tensoriais são objetos de enorme importância e diversos outros tipos de álgebra podem ser construídas a partir da mesma ou de modo semelhante à mesma.

Na Seção 2.1.7.5, página 152, mostramos como álgebras tensoriais podem ser empregadas na denifição das chamadas Álgebras de Clifford, de relevância na Física Quântica.

## 2.5.2 Álgebras Exteriores

Álgebras exteriores são um tipo especial de álgebras de Grassmann (apresentadas na Seção 2.1.7.4, página 151) e ocorrem de forma importante na Topologia Diferencial e na Geometria Diferencial, especialmente no estudo das chamadas *formas diferenciais*, introduzidas por Élie Cartan[90]. O tratamento que faremos aqui é geral e não se especializa a estruturas diferenciáveis.

Na Seção 2.3.7, página 230, definimos o espaço $(U^{\otimes n})_A$ como o subespaço de $U^{\otimes n}$ constituído pela imagem do operador de antissimetrização $\mathcal{A}_n$. Sejam $p,\ q \in \mathbb{N}_0$. Se $x \in (U^{\otimes p})_A$ e $y \in (U^{\otimes q})_A$, então $x$ e $y$ são (evidentemente) elementos de $U^{\otimes p}$ e $U^{\otimes q}$, respectivamente, e, portanto, o produto tensorial $x \otimes y$ (como introduzido acima) define um elemento de $U^{\otimes(p+q)}$. Para $x \in (U^{\otimes p})_A$ e $y \in (U^{\otimes q})_A$, defina-se o produto $\wedge_{p,\,q} : (U^{\otimes p})_A \times (U^{\otimes q})_A \to \big(U^{\otimes(p+q)}\big)_A$ por

$$x \wedge_{p,\,q} y \ := \ \frac{(p+q)!}{p!q!}\,\mathcal{A}_{p+q}\big(x \otimes y\big)\ . \tag{2.173}$$

Note-se que, por essa definição, valerá no caso $p = 0$ que $x \in \mathbb{K}$ e, portanto, $x \wedge_{0,\,q} y := \mathcal{A}_q\big(x \otimes y\big) = \mathcal{A}_q\big(xy\big) = x\mathcal{A}_q\big(y\big) = xy$. Analogamente, no caso $q = 0$ teremos $y \in \mathbb{K}$ e, portanto, $x \wedge_{p,\,0} y := \mathcal{A}_p\big(x \otimes y\big) = \mathcal{A}_p\big(yx\big) = y\mathcal{A}_p\big(x\big) = yx$.

De acordo com (2.159), página 230, vale

$$\mathcal{A}_{p+q}\Big(x_{\pi(1)} \otimes \cdots \otimes x_{\pi(p)} \otimes y_{\sigma(1)} \otimes \cdots \otimes y_{\sigma(q)}\Big) \ = \ \mathrm{sinal}\,(\pi)\mathrm{sinal}\,(\sigma)\mathcal{A}_{p+q}\Big(x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes y_q\Big) \tag{2.174}$$

para todos $\pi \in S_p$, $\sigma \in S_q$. Assim, se $x$ e $y$ são da forma $x = x_1 \wedge \cdots \wedge x_p$ e $y = y_1 \wedge \cdots \wedge y_q$, então, usando também (2.160) e (2.161), segue que

$$\begin{aligned}
\big(x_1 \wedge \cdots \wedge x_p\big) \wedge_{p,\,q} \big(y_1 \wedge \cdots \wedge y_q\big) \ &= \ \frac{(p+q)!}{p!q!} \sum_{\pi\in S_p}\sum_{\sigma\in S_q} \mathrm{sinal}\,(\pi)\mathrm{sinal}\,(\sigma)\ \mathcal{A}_{p+q}\Big(x_{\pi(1)} \otimes \cdots \otimes x_{\pi(p)} \otimes y_{\sigma(1)} \otimes \cdots \otimes y_{\sigma(q)}\Big) \\
&= \ \frac{(p+q)!}{p!q!} \sum_{\pi\in S_p}\sum_{\sigma\in S_q} \mathcal{A}_{p+q}\Big(x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes y_q\Big) \\
&= \ (p+q)!\ \mathcal{A}_{p+q}\Big(x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes y_q\Big) \\
&= \ x_1 \wedge \cdots \wedge x_p \wedge y_1 \wedge \cdots \wedge y_q\ .
\end{aligned} \tag{2.175}$$

Essa igualdade torna evidente que para $x$, $y$ e $z$ da forma $x = x_1 \wedge \cdots \wedge x_p \in (U^{\otimes p})_A$, $y = y_1 \wedge \cdots \wedge y_q \in (U^{\otimes q})_A$ e $z = z_1 \wedge \cdots \wedge z_r \in (U^{\otimes r})_A$, vale

$$\big(x \wedge_{p,\,q} y\big) \wedge_{p+q,\,r} z \ = \ x \wedge_{p,\,q+r} \big(y \wedge_{q,\,r} z\big)\ . \tag{2.176}$$

Devido à linearidade dos produtos $\wedge_{p,\,q}$ (vide (2.173)), a relação (2.176) estende-se para todos $x \in (U^{\otimes p})_A$, $y \in (U^{\otimes q})_A$ e $z \in (U^{\otimes r})_A$.

Para $x \in (U^{\otimes p})_A$, $y \in (U^{\otimes q})_A$ é importante compararmos $x \wedge_{p,\,q} y$ e $y \wedge_{q,\,p} x$, ambos elementos de $(U^{\otimes(p+q)})_A$. Por

[90] Élie Joseph Cartan (1869–1951).

(2.175), temos que

$$\begin{aligned}\big(x_1\wedge\cdots\wedge x_p\big)\wedge_{p,\,q}\big(y_1\wedge\cdots\wedge y_q\big) &= x_1\wedge\cdots\wedge x_p\wedge y_1\wedge\cdots\wedge y_q\\ &= (-1)^{pq}y_1\wedge\cdots\wedge y_q\wedge x_1\wedge\cdots\wedge x_p\\ &= (-1)^{pq}\big(y_1\wedge\cdots\wedge y_q\big)\wedge_{q,\,p}\big(x_1\wedge\cdots\wedge x_p\big)\,.\end{aligned}$$

Consequentemente, vale

$$x\wedge_{p,\,q}y \;=\; (-1)^{pq}\,y\wedge_{q,\,p}x \tag{2.177}$$

para todos $x\in(U^{\otimes p})_A$ e $y\in(U^{\otimes q})_A$. É evidente por essa relação que se $p$ for ímpar, teremos $x\wedge_{p,\,p}x=0$ para todo $x\in(U^{\otimes p})_A$. Isso não é necessariamente verdade para $p$ par. Porém, segue de (2.175) e do comentado no Exercício E. 2.137, página 232, que $\big(x_1\wedge\cdots\wedge x_p\big)\wedge_{p,\,p}\big(x_1\wedge\cdots\wedge x_p\big)=x_1\wedge\cdots\wedge x_p\wedge x_1\wedge\cdots\wedge x_p=0$ para todo $p\in\mathbb{N}$.

Para futura referência, resumindo nossos resultados, temos

**Proposição 2.30** *Com as definições acima valem,*

1. *O produto $\wedge_{p,\,q}:(U^{\otimes p})_A\times(U^{\otimes q})_A\to(U^{\otimes(p+q)})_A$ é bilinear, ou seja, satisfaz*

   $$\big(\alpha_1x_1+\alpha_2x_2\big)\wedge_{p,\,q}y \;=\; \alpha_1x_1\wedge_{p,\,q}y+\alpha_2x_2\wedge_{p,\,q}y \quad\text{ e }\quad x\wedge_{p,\,q}\big(\alpha_1y_1+\alpha_2y_2\big) \;=\; \alpha_1x\wedge_{p,\,q}y_1+\alpha_2x\wedge_{p,\,q}y_2\,,$$

   *para todos $\alpha_1,\ \alpha_2\in\mathbb{R}$, $x_1,\ x_2\in(U^{\otimes p})_A$ e $y_1,\ y_2\in(U^{\otimes q})_A$.*

2. *O produto $\wedge_{p,\,q}:(U^{\otimes p})_A\times(U^{\otimes q})_A\to(U^{\otimes(p+q)})_A$ satisfaz*

   $$\big(x\wedge_{p,\,q}y\big)\wedge_{p+q,\,r}z \;=\; x\wedge_{p,\,q+r}\big(y\wedge_{q,\,r}z\big)\,. \tag{2.178}$$

   *para todos $x\in(U^{\otimes p})_A$, $y\in(U^{\otimes q})_A$ e $z\in(U^{\otimes r})_A$. Essa propriedade é por vezes denominada* pré-associatividade.

3. *Para todos $x\in(U^{\otimes p})_A$ e $y\in(U^{\otimes q})_A$ vale*

   $$x\wedge_{p,\,q}y \;=\; (-1)^{pq}\,y\wedge_{q,\,p}x\,. \tag{2.179}$$

   *Essa propriedade é por vezes denominada* comutatividade graduada. *Caso $p$ seja ímpar, isso implica que $x\wedge_{p,\,p}x=0$. Para $p$ par isso não é necessariamente verdade. Porém, para $x_1,\ \ldots,\ x_p\in U$, vale*

   $$\big(x_1\wedge\cdots\wedge x_p\big)\wedge_{p,\,p}\big(x_1\wedge\cdots\wedge x_p\big)=x_1\wedge\cdots\wedge x_p\wedge x_1\wedge\cdots\wedge x_p \;=\; 0$$

   *para <u>todo</u> $p\in\mathbb{N}$.* □

• **<u>A álgebra exterior de $U$</u>**

Podemos agora proceder de forma análoga à que empregamos ao transformarmos $\mathscr{T}(U)$ em uma álgebra associativa e unital, usando os produtos $\wedge_{p,\,q}$ para fazer também de $\mathscr{T}_A(U)$ uma álgebra associativa. Para $\underline{a}\in\displaystyle\bigoplus_{n=0}^{\infty}(U^{\otimes n})_A$ e $\underline{b}\in\displaystyle\bigoplus_{n=0}^{\infty}(U^{\otimes n})_A$ da forma $\underline{a}=\displaystyle\sum_k\alpha_k\,a_0^k\oplus a_1^k\oplus a_2^k\oplus\cdots$ e $\underline{b}=\displaystyle\sum_l\beta_l\,b_0^l\oplus b_1^l\oplus b_2^l\oplus\cdots$, as duas somas sendo finitas, com $\alpha_k\in\mathbb{K}$ e $\beta_l\in\mathbb{K}$ e com $a_i^k\in(U^{\otimes i})_A$, $b_j^l\in(U^{\otimes j})_A$ para todos $k,\ l,\ i$ e $j$, definimos o produto $\underline{a}\wedge\underline{b}$ por

$$\begin{aligned}\left(\sum_k\alpha_k\,a_0^k\oplus a_1^k\oplus a_2^k\oplus\cdots\right)\wedge\left(\sum_l\beta_l\,b_0^l\oplus b_1^l\oplus b_2^l\oplus\cdots\right) &:= \sum_{k,\,l}\alpha_k\beta_l\,\Big(a_0^k\oplus a_1^k\oplus a_2^k\oplus\cdots\Big)\wedge\Big(b_0^l\oplus b_1^l\oplus b_2^l\oplus\cdots\Big)\\ &= \sum_{k,\,l}\alpha_k\beta_l\,\bigoplus_{p=0}^{\infty}\left[\sum_{q=0}^{p}a_q^k\wedge_{q,\,p-q}b_{p-q}^l\right]\\ &= \bigoplus_{p=0}^{\infty}\left[\sum_{q=0}^{p}\left(\sum_k\alpha_k\,a_q^k\right)\wedge_{q,\,p-q}\left(\sum_l\beta_l\,b_{p-q}^l\right)\right]\,.\end{aligned} \tag{2.180}$$

A associatividade do produto assim definido decorre diretamente de (2.176) e sua demonstração é deixada como exercício. O espaço vetorial $\mathscr{T}_A(U)$ torna-se, assim, uma álgebra associativa denominada *álgebra exterior* de $U$. Essa álgebra é unital, como se depreende do próximo exercício.

**E. 2.147** *Exercício.* Seja $\underline{e} \in \mathscr{T}_A(U)$ da forma $\underline{e} := 1 \oplus 0 \oplus 0 \oplus \cdots$, onde $1$ é a unidade do corpo $\mathbb{K}$. Mostre, usando a definição de produto dada acima, que $\underline{1} \wedge \underline{b} = \underline{b}$ para todo $\underline{b} \in \mathscr{T}_A(U)$. ✠

É importante também reconhecer que $U$ é isomorfo ao subespaço de $\mathscr{T}_A(U)$ definido por $0 \oplus U \oplus 0 \oplus 0 \oplus \cdots$ e que para esse subespaço temos $\big(0 \oplus u \oplus 0 \oplus \cdots\big) \wedge \big(0 \oplus u \oplus 0 \oplus 0 \oplus \cdots\big) = 0 \oplus 0 \oplus (u \wedge_{1,\,1} u) \oplus 0 \oplus 0 \oplus \cdots = 0$, pois $u \wedge_{1,\,1} u = u \wedge u = 0$ para todo $u \in U$. Decorre disso que $\mathscr{T}_A(U)$ é uma *álgebra de Grassmann* (vide definição na Seção 2.1.7.4, página 151).

• **O caso de espaços de dimensão finita**

De particular importância para a Topologia Diferencial e para a Geometria Diferencial é o caso em que $U$ é um espaço de dimensão finita $m$. Seja $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ uma base em $U$. Pelo comentado no Exercício E. 2.138, página 232, vale aqui para o espaço $\mathscr{T}_A(U)$ de todos os tensores antissimétricos,

$$\mathscr{T}_A(U) \;=\; \mathbb{K} \oplus U \oplus \big(U^{\otimes 2}\big)_A \oplus \cdots \oplus \big(U^{\otimes m}\big)_A \;, \tag{2.181}$$

pois $(U^{\otimes n})_A = \{0\}$, o espaço vetorial trivial, sempre que $n > m$. Pelo mesmo Exercício E. 2.138, cada espaço $\big(U^{\otimes l}\big)_A$ tem uma base composta por vetores da forma $\mathbf{e}_{k_1} \wedge \cdots \wedge \mathbf{e}_{k_l}$ com $k_j \in \{1, \ldots, m\}$ para todo $j$ e com $k_1 < \ldots < k_l$ e, consequentemente, $\big(U^{\otimes l}\big)_A$ tem dimensão $\binom{m}{l} = \frac{m!}{l!(m-l)!}$. Portanto, $\mathscr{T}_A(U)$ tem dimensão $\sum_{l=0}^{m} \frac{m!}{l!(m-l)!} = 2^m$.

• **O produto interior**

Há também um outro produto útil que pode ser definido entre espaços $\big(U^{\otimes n}\big)_A$, o chamado *produto interior*. Para $u \in U'$ define-se $I_u^n : \big(U^{\otimes n}\big)_A \to \big(U^{\otimes (n-1)}\big)_A$, $1 \leq n \leq m$, da seguinte forma: para cada $\omega \in \big(U^{\otimes n}\big)_A$ define-se $I_u^n \omega$ como sendo o elemento de $\big(U^{\otimes (n-1)}\big)_A$ tal que para todos $v_1, \ldots, v_{r-1} \in U'$ vale

$$\big\langle v_1 \oplus \cdots \oplus v_{r-1},\; I_u^n \omega \big\rangle \;=\; \big\langle u \oplus v_1 \oplus \cdots \oplus v_{r-1},\; \omega \big\rangle \;. \tag{2.182}$$

Honorificamente define-se também $I_u^0 \equiv 0$.

**E. 2.148** *Exercício.* Demonstre as seguintes propriedades do produto interior:

$$I_u^n I_u^{n+1} \;=\; 0 \,, \quad 0 \,\leq\, n \,\leq\, m-1 \,. \tag{2.183}$$

$$I_u^{n_1+n_2}\big(\omega_1 \wedge_{n_1,\,n_2} \omega_2\big) \;=\; \big(I_u^{n_1}\omega_1\big) \wedge_{n_1-1,\,n_2} \omega_2 + (-1)^{n_1} \omega_1 \wedge_{n_1,\,n_2-1} I_u^{n_2}\big(\omega_2\big) \,, \tag{2.184}$$

para todos $\omega_1 \in \big(U^{\otimes n_1}\big)_A$ e $\omega_2 \in \big(U^{\otimes n_2}\big)_A$. Observe-se que a propriedade (2.184) é similar à regra de Leibniz para derivadas, exceto pelo fator $(-1)^{n_1}$ do lado direito. ✠

O produto interior pode ser estendido a todo $\mathscr{T}_A(U) = \bigoplus_{n=0}^{m} \big(U^{\otimes n}\big)_A$ pelo operador linear $I_u : \mathscr{T}_A(U) \to \mathscr{T}_A(U)$ definido por

$$I_u \bigoplus_{a=0}^{m} \omega^a \;:=\; \bigoplus_{a=0}^{m} \big(I_u^a \omega^a\big) \;=\; \bigoplus_{a=1}^{m} \big(I_u^a \omega^a\big) \,, \tag{2.185}$$

onde $\omega^a \in \big(U^{\otimes a}\big)_A$ para cada $a = 0, \ldots, m$. Observe-se que a imagem de $I_u$ é o subespaço $\bigoplus_{n=0}^{m-1} \big(U^{\otimes n}\big)_A$ de $\mathscr{T}_A(U) = \bigoplus_{n=0}^{m} \big(U^{\otimes n}\big)_A$. Por (2.183), vale

$$\big(I_u\big)^2 \bigoplus_{a=0}^{m} \omega^a \;=\; \bigoplus_{a=1}^{m} \big(I_u^{a-1} I_u^a \omega^a\big) \;\overset{(2.183)}{=}\; 0 \,,$$

provando que $\big(I_u\big)^2 = 0$ e, portanto, que $I_u$ é nilpotente.

Sejam

$$\omega_1 \;:=\; \sum_k \alpha_k a_0^k \oplus a_1^k \oplus \cdots \oplus a_m^k \qquad \text{e} \qquad \omega_2 \;:=\; \sum_l \beta_l b_0^l \oplus b_1^l \oplus \cdots \oplus b_m^l$$

elementos de $\mathscr{T}_A(U)$. Então, vale

$$I_u\Big(\omega_1 \wedge \omega_2\Big) \;=\; \big(I_u\omega_1\big) \wedge \omega_2 + \big(G\omega_1\big) \wedge \big(I_u\omega_2\big) \;, \tag{2.186}$$

onde $G : \mathscr{T}_A(U) \to \mathscr{T}_A(U)$, o chamado *operador de graduação*, é o operador linear definido por

$$G\bigoplus_{j=0}^{m} a_j \;:=\; \bigoplus_{j=0}^{m}(-1)^j a_j \;.$$

Por exemplo, no caso $m = 5$, $G\Big(a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5\Big) = a_0 \oplus (-a_1) \oplus a_2 \oplus (-a_3) \oplus a_4 \oplus (-a_5)$. A demonstração de (2.186) é apresentada no Apêndice 2.A, página 261.

# 2.6 Tópicos Especiais

Esta seção é formada por alguns assuntos independentes que, embora relevantes, não se enquadram na exposição que pretendíamos ter nas seções anteriores.

## 2.6.1 O Grupo de Grothendieck

Vamos aqui descrever uma construção que permite obter um grupo Abeliano a partir de um semigrupo Abeliano dado. Um grupo construído por esse procedimento é chamado de grupo de Grothendieck[91] associado ao semigrupo Abeliano em questão. Grupos de Grothendieck desempenham um papel importante em várias áreas da Matemática, como por exemplo na chamada K-teoria.

Seja um semigrupo Abeliano $S$ (não necessariamente dotado de um elemento neutro) cujo produto denotamos pelo símbolo $+$.

Consideremos em primeiro lugar o produto Cartesiano $S \times S$ e vamos introduzir lá uma relação de equivalência da seguinte forma: dois pares $(a,\ b)$ e $(a',\ b') \in S \times S$ são equivalentes, $(a,\ b) \sim (a',\ b')$, se existir pelo menos um elemento $p \in S$ tal que[92]

$$a + b' + p \;=\; a' + b + p \;. \tag{2.187}$$

Vamos mostrar que isso define de fato uma relação de equivalência. Em primeiro lugar é claro que $(a,\ b) \sim (a,\ b)$ para qualquer par $(a,\ b) \in S^2 = S \times S$, dado que aqui, para verificar (2.187), basta tomar qualquer elemento $p \in S$. Em segundo lugar é evidente que, se $(a,\ b) \sim (a',\ b')$, então $(a',\ b') \sim (a,\ b)$. Finalmente, vamos mostrar que se $(a,\ b) \sim (c,\ d)$ e $(c,\ d) \sim (e,\ f)$, então $(a,\ b) \sim (e,\ f)$. Por hipótese existem $p$ e $p' \in S$ tais que

$$a + d + p \;=\; b + c + p \qquad \text{e} \qquad c + f + p' \;=\; d + e + p' \;.$$

Daqui extraímos que

$$\big(a + d + p\big) + \big(c + f + p'\big) \;=\; \big(b + c + p\big) + \big(d + e + p'\big) \;,$$

ou seja, que

$$a + f + p'' \;=\; b + e + p'' \;,$$

onde $p'' = d + c + p + p'$. Essa relação diz precisamente que $(a,\ b) \sim (e,\ f)$, completando a prova de que temos assim uma relação de equivalência em $S^2$.

Vamos considerar agora o conjunto $\mathsf{K}(S) := S^2/\sim$ de todas as classes de equivalência definidas acima. Como é usual, denotaremos por $[(a,\ b)]$ a classe à qual pertence o par $(a,\ b) \in S^2$. Vamos construir em $\mathsf{K}(S)$ uma estrutura de grupo Abeliano, cujo produto também denotaremos por $+$. Dadas duas classes $[(a,\ b)]$ e $[(c,\ d)]$ definimos

$$\big[(a,\ b)\big] + \big[(c,\ d)\big] \;:=\; \big[(a + c,\ b + d)\big] \;. \tag{2.188}$$

[91] Alexander Grothendieck (1928–2014).

[92] Comentemos, antes de prosseguirmos, que não supomos necessariamente que $S$ seja um semigrupo cancelativo. Assim, não necessariamente inferimos de (2.187) que $a+b' = a'+b$. A definição de semigrupo cancelativo, assim como exemplos de semigrupos cancelativo e não-cancelativos (Abelianos ou não) encontra-se à página 136 (vide Exemplos 2.11, página 136).

Note-se que por essa definição tem-se (verifique!)

$$\big[(a,\ b)\big] + \big[(c,\ d)\big] \ = \ \big[(c,\ d)\big] + \big[(a,\ b)\big]$$

para todo $a,\ b,\ c,\ d \in S$, pelo fato de a operação de soma ser Abeliana em $S$.

A primeira coisa a fazer é mostrar que essa definição independe dos elementos tomados nas classes. Para isto basta provar que se $(a',\ b') \sim (a,\ b)$, então $(a+c,\ b+d) \sim (a'+c,\ b'+d)$. Se $(a',\ b') \sim (a,\ b)$, então existe $p \in S$ tal que

$$a + b' + p \ = \ a' + b + p\ .$$

Somando-se $c+d$ a ambos os lados tiramos

$$\big(a+c\big) + \big(b'+d\big) + p \ = \ \big(a'+c\big) + \big(b+d\big) + p$$

que é precisamente a afirmativa que $(a+c,\ b+d) \sim (a'+c,\ b'+d)$.

É igualmente fácil verificar que para quaisquer $x,\ y \in S$ tem-se que $(x,\ x) \sim (y,\ y)$ e que, portanto, $[(x,\ x)] = [(y,\ y)]$. Vamos provar que há em $\mathsf{K}(S)$ um elemento neutro. Este é precisamente a classe $\underline{e} := [(x,\ x)]$ com $x \in S$ arbitrário. Note-se que, para qualquer par $(a,\ b) \in S^2$ teremos

$$\big[(a,\ b)\big] + \big[(x,\ x)\big] \ = \ \big[(a+x,\ b+x)\big] \ = \ \big[(a,\ b)\big]\ ,$$

pois $(a+x+b)+p = (b+x+a)+p$ para qualquer $p \in S$.

Falta-nos provar a associatividade do produto e a existência de uma inversa para cada elemento de $\mathsf{K}(S)$. Para a associatividade, notemos que

$$\big[(a,\ b)\big] + \Big(\big[(c,\ d)\big] + \big[(e,\ f)\big]\Big) \ := \ \big[(a,\ b)\big] + \big[(c+e,\ d+f)\big] \ = \ \big[(a+c+e,\ b+d+f)\big]\ ,$$

$$\Big(\big[(a,\ b)\big] + \big[(c,\ d)\big]\Big) + \big[(e,\ f)\big] \ := \ \big[(a+c,\ b+d)\big] + \big[(e,\ f)\big] \ = \ \big[(a+c+e,\ b+d+f)\big]\ .$$

Para provar a existência de inversa notemos que para cada par $(a,\ b) \in S^2$ podemos tomar $[(a,\ b)]^{-1} := [(b,\ a)]$ pois

$$\big[(a,\ b)\big] + \big[(a,\ b)\big]^{-1} \ = \ \big[(a,\ b)\big] + \big[(b,\ a)\big] \ = \ \big[(a+b,\ a+b)\big] \ = \ \underline{e}\ .$$

Isso mostrou que $\mathsf{K}(S)$ tem uma estrutura de grupo Abeliano. Este é o chamado *grupo de Grothendieck* associado ao semigrupo Abeliano $S$.

Como de costume, denotaremos $\big[(a,\ b)\big]^{-1}$ por $-\big[(a,\ b)\big]$. Assim, $-\big[(a,\ b)\big] = \big[(b,\ a)\big]$.

Todo semigrupo Abeliano cancelativo é isomorfo a um semigrupo contido dentro de um grupo, a saber, de seu grupo de Grothendieck. A prova dessa afirmação é o conteúdo do exercício que segue.

**E. 2.149** *Exercício.* **I.** Mostre que $(a+f,\ f) \sim (a+g,\ g)$ para quaisquer $a,\ f,\ g \in S$. **II.** Mostre que $\mathsf{S}(S) := \Big\{ \big[(a+f,\ f)\big],\ a \in S \Big\}$ é um semigrupo em $\mathsf{K}(S)$ com relação à mesma operação definida em (2.188). **III.** Mostre que a aplicação $\varphi : S \to \mathsf{S}(S)$ definida por $S \ni a \mapsto \varphi(a) := \big[(a+f,\ f)\big] \in \mathsf{S}(S)$ (com $f \in S$, arbitrário) é um homomorfismo do semigrupo $S$ no semigrupo $\mathsf{S}(S)$.

**IV.** Mostre que todo elemento $\big[(a,\ b)\big]$ de $\mathsf{K}(S)$ pode ser escrito da forma $\big[(a,\ b)\big] = \varphi(a) - \varphi(b)$ e que $\varphi(a) - \varphi(b) = \varphi(a') - \varphi(b')$ se e somente se existir $p \in S$ com $a + b' + p = a' + b + p$.

**V.** Suponha que $S$ possua a seguinte propriedade: se para $a,\ a' \in S$ existir $p \in S$ tal que $a+p = a'+p$, então $a = a'$ (nesse caso $S$ é dito ser um semigrupo Abeliano cancelativo. Vide página 136). Mostre que nesse caso $\varphi : S \to \mathsf{S}(S)$ é um isomorfismo do semigrupo $S$ no semigrupo $\mathsf{S}(S)$. Nessa situação, teríamos, em um certo sentido, que o grupo $\mathsf{K}(S)$ contém uma cópia do semigrupo $S$ dentro de si (a saber $\mathsf{S}(S)$), sendo, portanto, uma espécie de extensão do semigrupo $S$. ✠

**E. 2.150** *Exercício.* Seja o semigrupo Abeliano $(\mathbb{N},\ +)$, dos números naturais com a soma usual. Mostre que $\mathsf{K}(\mathbb{N}) \simeq (\mathbb{Z},\ +)$, o grupo dos números inteiros com a operação de soma usual. ✠

O exercício acima indica a possibilidade de se definir os números inteiros a partir dos naturais. Os inteiros seriam, por definição, o grupo de Grothendieck do monoide Abeliano dos naturais com a operação de soma usual. Modernamente, no estudo dos Fundamentos da Matemática é dessa forma, aliás, que os números inteiros são definidos.

**E. 2.151** *Exercício*. Seja o monoide Abeliano $(\mathbb{N},\ \cdot)$, dos números naturais (sem o zero), com o produto dado pela multiplicação usual. Mostre que $\mathsf{K}(\mathbb{N}) \simeq (\mathbb{Q}_+,\ \cdot)$, o grupo dos racionais positivos (sem o zero) com o produto dado pela multiplicação usual. ✠

O exercício acima indica a possibilidade de se definir os números racionais positivos a partir dos naturais. Os racionais seriam, por definição, o grupo de Grothendieck do monoide Abeliano dos naturais com a operação de produto usual. Modernamente, no estudo dos Fundamentos da Matemática é dessa forma, aliás, que os números racionais são definidos.

**E. 2.152** *Exercício*. Aplique a construção de Grothendieck para o semigrupo $\mathscr{R}_+$, definido à página 130. Mostre que o grupo assim obtido possui apenas um elemento (ou seja, é o grupo trivial). ✠

**E. 2.153** *Exercício*. Seja $X$ um conjunto não vazio e considere o semigrupo Abeliano (e não cancelativo) composto pela a coleção $\mathbb{P}(X) \setminus \{\emptyset\}$ (de todos os subconjuntos não vazios de $X$) com relação à operação de união de conjuntos. Mostre que o grupo de Grothendieck correspondente é trivial. ✠

**E. 2.154** *Exercício*. Seja $X$ um conjunto não vazio e considere o semigrupo Abeliano (e não cancelativo) composto pela a coleção $\mathbb{P}(X) \setminus \{X\}$ (de todos os subconjuntos de $X$ distintos de $X$) com relação à operação de união de conjuntos. Mostre que o grupo de Grothendieck correspondente é trivial. ✠

## 2.6.2 Grupóides

Um *grupóide* é definido da seguinte forma. É dado um conjunto $C$ e um subconjunto $C_0 \subset C$, o qual é a imagem de duas funções unárias $p$ e $c$ (chamadas de "partida" e "chegada"), ou seja, $p : C \to C_0$, $c : C \to C_0$. Os elementos de $C_0$ são pontos fixos de $p$ e de $c$, ou seja,

$$c(\alpha) \ = \ \alpha \qquad \text{e} \qquad p(\alpha) \ = \ \alpha$$

para todo $\alpha \in C_0$ (aqui denotaremos os elementos de $C$ por letras gregas).

Define-se em $C \times C$ um subconjunto (ou seja, uma relação em $C$), que denotaremos por $R_C$, da seguinte forma:

$$R_C \ := \ \Big\{(\alpha, \beta) \in C^2 |\ \ p(\alpha) \ = \ c(\beta)\Big\} \, .$$

É também dada uma função binária $R_C \to C$, que denotaremos por "$\cdot$" e que denominaremos "produto", a qual satisfaz as seguintes hipóteses:

1. Associatividade: $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ sempre que os produtos estejam definidos, ou seja, se $(\beta,\ \gamma)$, $(\alpha,\ \beta \cdot \gamma)$, $(\alpha,\ \beta)$ e $(\alpha \cdot \beta,\ \gamma)$ forem todos elementos de $R_C$
2. Para todo $(\alpha,\ \beta) \in R_C$ temos $p(\alpha \cdot \beta) = p(\beta)$.
3. Para todo $(\alpha,\ \beta) \in R_C$ temos $c(\alpha \cdot \beta) = c(\alpha)$.
4. Para todo $\alpha \in C$ temos $\alpha \cdot p(\alpha) = \alpha$.
5. Para todo $\alpha \in C$ temos $c(\alpha) \cdot \alpha = \alpha$.

Fora isso, existe para cada $\alpha \in C$ uma assim chamada *inversa bilateral* $\alpha^{-1} \in C$, a qual satisfaz $\alpha \cdot \alpha^{-1} = c(\alpha)$ e $\alpha^{-1} \cdot \alpha = p(\alpha)$. Note que, por essa definição, tem-se que, para todo $\alpha_0 \in C_0$, $\alpha_0 \cdot \alpha_0^{-1} = \alpha_0^{-1} \cdot \alpha_0 = \alpha_0$.

Estes ingredientes definem um grupóide. Note-se que um grupóide não necessariamente contém um "elemento neutro" (vide exemplos).

• **Exemplo: grupos**

O exemplo mais elementar (e um tanto trivial) de um grupóide é um grupo. Seja $G$ um grupo com $e$ sendo seu elemento neutro. Defina-se $G_0 = \{e\}$, $p(g) = e$ e $c(g) = e$ para todos $g \in G$. Claro está que $e \in G$ é ponto fixo de $p$ e de $c$. O conjunto $R_G$ coincide com $G^2$: $R_G = \{(g,\ h),\ g,\ h \in G\}$. O produto $R_G \to G$ é definido como o produto em $G$: $g \cdot h = gh$, para todos $(g,\ h) \in G^2$. A inversa bilateral de um elemento $g$ é $g^{-1}$, sua inversa em $G$.

Deixamos ao leitor a simples tarefa de verificar que as propriedades 1–5, página 248, da definição de grupóide são trivialmente satisfeitas neste caso.

• **Exemplo de grupóide: caminhos**

Este exemplo é um protótipo da definição de grupóide acima, ou seja, aquela possivelmente foi criada tendo o mesmo como exemplo-guia.

Seja $I$ o intervalo fechado $[0,\ 1]$ e vamos considerar o conjunto $\mathcal{C}$ de todas as funções contínuas de $I$ em um espaço topológico Hausdorff qualquer (por exemplo, $\mathbb{R}^2$). Um elemento $\gamma$ de $C$ é uma curva orientada contínua em $\mathbb{R}^2$ que tem um ponto de partida $\gamma(0)$ e um ponto de chegada $\gamma(1)$.

Podemos introduzir uma relação de equivalência em $\mathcal{C}$ da seguinte forma: duas curvas $\alpha$ e $\beta \in \mathcal{C}$ são equivalentes ($\alpha \sim \beta$) se existir uma bijeção contínua $b : I \to I$ com $b(0) = 0$, $b(1) = 1$, tal que $\alpha = \beta \circ b$. Vamos denominar por $C$ as classes de equivalência de $\mathcal{C}$ pela relação de equivalência acima: $C := \mathcal{C}/\sim$.

O conjunto $C_0$ é o subconjunto de $C$ formado pelas classes de equivalência de curvas constantes: $[\alpha] \in C_0 \Leftrightarrow \alpha(t) = \alpha(t'),\ \forall t,\ t' \in I$.

Definimos as funções unárias $p$ e $c$ da seguinte forma: $p([\gamma])$ é a classe de equivalência da curva constante que a todo $t \in I$ associa o ponto $\gamma(0)$ de $\mathbb{R}^2$, o ponto de partida de $\gamma$; $c([\gamma])$ é a classe de equivalência da curva constante que a todo $t \in I$ associa o ponto $\gamma(1)$ de $\mathbb{R}^2$, o ponto de chegada de $\gamma$.

Dados dois elementos em $C$ queremos agora definir o seu produto. A ideia a ser seguida é que o produto de duas curvas é definido apenas quando o ponto de chegada da primeira coincide com o ponto de partida da segunda e resulta em uma curva única unindo o ponto de partida da primeira com o ponto de chegada da última. Matematicamente isso é feito definindo-se o produto $[\beta] \cdot [\alpha]$ como sendo a classe de equivalência da curva $\beta * \alpha$ definida pela composição

$$\beta * \alpha(t) \ := \begin{cases} \alpha(2t), & \text{para } 0 \le t \le 1/2\ , \\ \\ \beta(2t-1), & \text{para } 1/2 < t \le 1\ . \end{cases}$$

Claramente $\beta * \alpha$ só é um elemento de $C$ (ou seja, uma curva contínua) se $\alpha(1) = \beta(0)$.

Por fim a inversa bilateral de $[\alpha]$ é definida como sendo a classe $[\alpha^{-1}]$, onde $\alpha^{-1}(t) = \alpha(1-t)$.

Deixamos para o leitor como exercício mostrar que a estrutura definida acima é a de um grupóide.

Notemos que para a composição $*$ acima não vale a associatividade: $(\alpha * \beta) * \gamma \neq \alpha * (\beta * \gamma)$, se ambos os lados estiverem definidos (por quê?). No entanto, as curvas $(\alpha * \beta) * \gamma$ e $\alpha * (\beta * \gamma)$ são equivalentes no sentido da definição acima e de tal forma que para o produto "$\cdot$" definido nas classes $C$ vale a associatividade $[\alpha] \cdot ([\beta] \cdot [\gamma]) = ([\alpha] \cdot [\beta]) \cdot [\gamma]$, se ambos os lados estiverem definidos (por quê?). Essa é a razão de termos feito a construção nas classes $C$ e não diretamente em $\mathcal{C}$. Esse fato já deve ser familiar ao leitor que conheça o conceito de *grupo de homotopia* de espaços topológicos. O grupóide apresentado acima e o grupo de homotopia são, aliás, fortemente aparentados e ao leitor sugere-se pensar sobre qual a conexão entre ambos.

• **Exemplo de grupóide: relações de equivalência**

Seja $K$ um conjunto no qual haja uma relação de equivalência $R \subset K \times K$. Tomamos $C = R$ e $C_0 = \big\{(x,\ x),\ x \in K\big\} \subset R$. Definimos

1. $p\big((x,\ y)\big) := (x,\ x),\ \forall x,\ y \in K$ com $x \sim y$.
2. $c\big((x,\ y)\big) := (y,\ y),\ \forall x,\ y \in K$ com $x \sim y$.
3. Produto: $(x,\ y) \cdot (y,\ z) := (x,\ z),\ \forall x,\ y,\ z \in K$ com $x \sim y \sim z$.
4. Inversa bilateral: $(x,\ y)^{-1} := (y,\ x)$.

É fácil verificar (faça-o!) que a estrutura assim definida é a de um grupóide.

• **Exemplo de grupóide: uniões disjuntas de grupos**

Considere-se a união disjunta

$$\mathcal{G} \,=\, \bigsqcup_{n\in\mathbb{N}} G_n \,=\, \bigcup_{n\in\mathbb{N}} (n,\, G_n) \,=\, \bigcup_{n\in\mathbb{N}} \bigcup_{g_n\in G_n} (n,\, g_n)\,,$$

onde, $G_n$ é, para cada $n \in \mathbb{N}$, um grupo[93]. Os elementos de $\mathcal{G}$ são, assim, pares ordenados $(n,\ g_n)$, onde $n \in \mathbb{N}$ e $g_n \in G_n$. O primeiro elemento de um par $(n,\ g_n)$ é denominado *índice*.

Definimos $\mathcal{G}_0 \subset \mathcal{G}$ por $\mathcal{G}_0 = \bigcup_{n\in\mathbb{N}}(n,\ e_n)$, onde $e_n$ é o elemento neutro de $G_n$. Definimos também $p : \mathcal{G} \to \mathcal{G}_0$ e $c : \mathcal{G} \to \mathcal{G}_0$ por $p\big((n,\ g_n)\big) := (n,\, e_n)$ e $c\big((n,\ g_n)\big) := (n,\ e_n)$. Está claro que para $(n,\, e_n) \in \mathcal{G}_0$ valem $p\big((n,\, e_n)\big) = (n,\, e_n) = c\big((n,\, e_n)\big)$ e, assim, os elementos de $C_0$ são pontos fixos de $p$ e de $c$.

Segundo a definição, $R_{\mathcal{G}} \subset \mathcal{G} \times \mathcal{G}$ é definido por

$$\begin{aligned} R_{\mathcal{G}} \,&=\, \Big\{\big((n,\, g_n),\, (m,\, h_m)\big) \,\in\, \mathcal{G}^2 \big| p\big((n,\, g_n)\big) \,=\, c\big((m,\, h_m)\big)\Big\} \\ &=\, \Big\{\big((n,\, g_n),\, (m,\, h_m)\big) \,\in\, \mathcal{G}^2 \big| (n,\, e_n) \,=\, (m,\, e_m)\Big\} \\ &=\, \Big\{\big((n,\, g_n),\, (n,\, h_n)\big) \big| n \in \mathbb{N} \text{ e } g_n,\, h_n \in G_n\Big\}\,. \end{aligned} \tag{2.189}$$

O produto em $R_{\mathcal{G}}$ é, assim, definido apenas para elementos com o mesmo índice:

$$(n,\, g_n)\cdot(n,\, h_n) \,:=\, (n,\, g_n h_n)\,, \qquad n \in \mathbb{N}\,.$$

A inversa bilateral do elemento $(n,\ g_n)$ é $(n,\ g_n^{-1})$ e é fácil ver que $(n,\ g_n)\cdot(n,\ g_n^{-1}) = (n,\ e_n) = c\big((n,\ g_n)\big)$ e que $(n,\, g_n^{-1})\cdot(n,\, g_n) = (n,\, e_n) = p\big((n,\, g_n)\big)$, como desejado.

Deixamos ao diligente leitor a simples tarefa de verificar que as propriedades 1–5, página 248, da definição de grupóide são satisfeitas neste caso.

## 2.6.3 Quatérnios, Números Complexos e outros Amigos

Vamos nesta seção tratar brevemente de um tipo de álgebra que possui algumas aplicações interessantes na Teoria de Grupos e outros lugares, a chamada álgebra dos *quatérnios*. Esta se apresenta como uma espécie de extensão a $\mathbb{R}^4$ das álgebras dos complexos e do produto vetorial em $\mathbb{R}^3$. Como preaquecimento, apresentaremos ambas de um ponto de vista mais fundamental.

Para textos sobre Álgebra Clássica e Abstrata, com notas históricas, vide [369, 370].

### 2.6.3.1 Álgebras Comutativas e Associativas em $\mathbb{R}^2$. A Álgebra dos Complexos

• **A álgebra $\mathbb{R}\oplus\mathbb{R}$**

Dado um espaço vetorial como $\mathbb{R}^2$ há várias maneiras de definir no mesmo um produto de modo a fazer do mesmo uma álgebra. Por exemplo, podemos definir em $\mathbb{R}^2$ o produto

$$(x_1,\, x_2)\cdot(y_1,\, y_2) \,=\, (x_1 y_1,\, x_2 y_2)\,, \tag{2.190}$$

que é associativo e comutativo. O produto (2.190) faz de $\mathbb{R}^2$ uma álgebra isomorfa a $\mathbb{R}\oplus\mathbb{R}$, ou seja, a duas cópias da álgebra usual dos números reais e vamos também denotá-la por $\mathbb{R}\oplus\mathbb{R}$.

A álgebra $\mathbb{R}\oplus\mathbb{R}$ tem uma unidade, o elemento $\mathbf{e} \equiv (1,\ 1)$. Um elemento da forma $(a,\ b)$ possui uma inversa multiplicativa se e somente se $a \neq 0$ e $b \neq 0$, sendo essa inversa $(1/a,\ 1/b)$. Os elementos $(1,\ 0)$ e $(0,\ 1)$ são idempotentes:

[93] É permitido que haja repetição dos grupos, ou seja, que haja $n,\ m \in \mathbb{N}$ com $n \neq m$ mas $G_n = G_m$.

satisfazem $(1,\ 0)\cdot(1,\ 0) = (1,\ 0)$ e $(0,\ 1)\cdot(0,\ 1) = (0,\ 1)$, sendo que também vale $(1,\ 0)\cdot(0,\ 1) = (0,\ 0)$, o vetor nulo de $\mathbb{R}\oplus\mathbb{R}$.

O fato de valer $(1,\ 0)\cdot(0,\ 1) = (0,\ 0)$ significa que $\mathbb{R}\oplus\mathbb{R}$ possui divisores de zero e, portanto, não é um anel de integridade. Vide página 156 e seguintes. O fato de existirem elementos não nulos em $\mathbb{R}\oplus\mathbb{R}$ sem inversa multiplicativa significa que $\mathbb{R}\oplus\mathbb{R}$ não é uma álgebra de divisão. Vide página 156.

Por fim, vale comentar que a álgebra $\mathbb{R}\oplus\mathbb{R}$ possui uma involução, ou seja, uma aplicação unária de $\mathbb{R}\oplus\mathbb{R}$ cujo quadrado é a identidade e que é um homomorfismo. Ela é dada por $\mathbb{R}\oplus\mathbb{R}\ni(a,\ b)\mapsto\overline{(a,\ b)} := (b,\ a)\in\mathbb{R}\oplus\mathbb{R}$. É elementar verificar que

$$\overline{\overline{(a,\ b)}} \;=\; (a,\ b) \qquad \text{e que} \qquad \overline{(a,\ b)\cdot(c,\ d)} \;=\; \overline{(a,\ b)}\cdot\overline{(c,\ d)}$$

para todos $(a,\ b),\ (c,\ d)\in\mathbb{R}\oplus\mathbb{R}$.

Para $(x,\ y)\in\mathbb{R}\oplus\mathbb{R}$ temos

$$\overline{(x,\ y)}\cdot(x,\ y) \;=\; (yx,\ xy) \;=\; xy\mathbf{e}\,.$$

Assim, podemos definir $N:\mathbb{R}\oplus\mathbb{R}\to\mathbb{R}$ por

$$N\big((x,\ y)\big) \;:=\; \overline{(x,\ y)}\cdot(x,\ y) \;\equiv\; xy\,,$$

identificando $a\mathbf{e}\in\mathbb{R}\oplus\mathbb{R}$ com $a\in\mathbb{R}$. É fácil ver que

$$N\big((a,\ b)\cdot(c,\ d)\big) \;=\; N\big((a,\ b)\big)N\big((c,\ d)\big) \qquad \text{e} \qquad N\Big(\overline{(a,\ b)}\Big) \;=\; N\big((a,\ b)\big)$$

para todos $(a,\ b),\ (c,\ d)\in\mathbb{R}\oplus\mathbb{R}$.

Uma função $N$ com as propriedade a acima é dita ser uma *norma algébrica*, noção que não deve ser confundida com a de norma em um espaço vetorial.

Vale comentar que $(x,\ y)\in\mathbb{R}\oplus\mathbb{R}$ possui inversa multiplicativa se e somente se $N\big((x,\ y)\big)\neq 0$ e essa inversa é

$$(x,\ y)^{-1} \;=\; \frac{1}{N\big((x,\ y)\big)}\overline{(x,\ y)} \;=\; (1/x,\ 1/y)\,.$$

Encontraremos similaridades entre as diversas estruturas algébricas de $\mathbb{R}\oplus\mathbb{R}$, apresentadas acima, com outras da álgebra dos números complexos e, especialmente, da álgebra dos números complexos *hiperbólicos*, das quais trataremos em seguida. Como veremos, a álgebra dos números complexos hiperbólicos é isomorfa a álgebra $\mathbb{R}\oplus\mathbb{R}$.

• **A álgebra dos números complexos**

Bem mais interessante que o produto (2.190) é o produto

$$(x_1,\ x_2)\cdot(y_1,\ y_2) \;=\; (x_1y_1 - x_2y_2,\ x_1y_2 + x_2y_1)\,, \tag{2.191}$$

também definido em $\mathbb{R}^2$, e que é igualmente associativo e comutativo.

**E. 2.155** *Exercício.* Verifique a validade dessas afirmações! ✠

O espaço vetorial $\mathbb{R}^2$ com esse produto é denominado *álgebra dos números complexos*, denotada por $\mathbb{C}$. Os elementos da álgebra $\mathbb{C}$ são denominados *números complexos*, ainda que, como conjunto, $\mathbb{C}$ seja idêntico a $\mathbb{R}^2$.

Definindo-se os vetores $\mathbf{e} := (1,\ 0)$ e $\mathbf{i} := (0,\ 1)$, podemos escrever todo $(x,\ y)\in\mathbb{R}^2$ da forma $(x,\ y) = x\mathbf{e} + y\mathbf{i}$, sendo que (2.191) indica que $\mathbf{e}$ é a unidade da álgebra (pois $(x_1,\ x_2)\cdot\mathbf{e} = \mathbf{e}\cdot(x_1,\ x_2) = (x_1,\ x_2)$) para todo $(x_1,\ x_2)\in\mathbb{R}^2$) e

$$\mathbf{i}^2 \;\equiv\; \mathbf{i}\cdot\mathbf{i} \;=\; -\mathbf{e}\,,$$

indicando que $\mathbf{i}$ pode ser interpretado como a "raiz quadrada" de menos a unidade, tal como no tratamento informal dos números complexos.

A conjugação complexa é a operação unária que associa cada par $(x,\ y)\in\mathbb{R}^2$ ao par $(x,\ -y)\in\mathbb{R}^2$, ou seja, associa $z\equiv x\mathbf{e} + y\mathbf{i}$ a $\overline{z} := x\mathbf{e} - y\mathbf{i}$. É evidente que se trata de uma involução, pois $\overline{(\overline{z})} = z$ para todo $z\in\mathbb{R}^2$. É também claro que $\overline{\mathbf{e}} = \mathbf{e}$ e $\overline{\mathbf{i}} = -\mathbf{i}$. É também um exercício fácil (faça-o!) constatar que

$$\overline{z\cdot w} \;=\; \overline{z}\cdot\overline{w} \tag{2.192}$$

para quaisquer números complexos $z$ e $w$.

Se $z \equiv x\mathbf{e} + y\mathbf{i}$, vale

$$\overline{z} \cdot z \;=\; x^2 + y^2 \;=\; \big\|(x,\, y)\big\|^2 \,,$$

onde $\|\cdot\|$ denota a norma Euclidiana usual em $\mathbb{R}^2$. Assim, podemos definir $|z| := \sqrt{\overline{z}\cdot z} = \sqrt{x^2+y^2} = \|z\|$ como aplicação de $\mathbb{C}$ em $[0,\, \infty)$. A expressão $|z|$ é denominada *módulo* do número complexo $z$. Observe-se que $|z| = 0$ se e somente se $z = 0$. É um exercício fácil (faça-o!) constatar que, devido a (2.192) e à comutatividade do produto dos números complexos,

$$|z \cdot w| \;=\; |z|\,|w|$$

para quaisquer números complexos $z$ e $w$.

É fácil constatar que $N(z) := \overline{z}\cdot z = |z|^2$ é uma *norma algébrica* em $\mathbb{C}$.

Todo número complexo não nulo possui uma inversa multiplicativa, a qual é dada por

$$z^{-1} \;=\; \frac{1}{N(z)}\overline{z} \;=\; \frac{1}{|z|^2}\overline{z}\,.$$

Verifique!

Para $z = x\mathbf{e} + y\mathbf{i} \neq 0$ definimos $\cos(\theta) := x/|z|$ e $\operatorname{sen}(\theta) := y/|z|$ e podemos trivialmente escrever

$$z \;=\; |z|\big(\cos(\theta)\mathbf{e} + \operatorname{sen}(\theta)\mathbf{i}\big)\,, \tag{2.193}$$

que é denominada *forma polar*, ou *representação polar*, do número complexo $z$ (essa expressão vale trivialmente quando $z = 0$, em cujo caso $\theta$ não está definido, pois $|z| = 0$).

Por fim, vale comentar que é prática corrente denotar-se um número complexo $x\mathbf{e} + y\mathbf{i}$ com a notação simplificada $x + iy$, omitindo-se a unidade $\mathbf{e}$ e adotando formalmente a identificação $\mathbf{i} \equiv i := \sqrt{-1}$.

**E. 2.156** *Exercício*. Mostre que os únicos elementos idempotentes de $\mathbb{C}$, ou seja, que satizfazem $z\cdot z = z$, são $0$ e a unidade $\mathbf{e}$. ✠

• **Fórmula de Euler**

Inspirados na expansão em série de Taylor da função exponencial, definamos

$$e^{\theta\mathbf{i}} \;:=\; \mathbf{e} + \sum_{n=1}^{\infty} \frac{\theta^n}{n!}\mathbf{i}^n\,. \tag{2.194}$$

Tem-se

$$e^{\theta\mathbf{i}} \;=\; \cos(\theta)\mathbf{e} + \operatorname{sen}(\theta)\mathbf{i}\,, \tag{2.195}$$

relação esta por vezes denominada *fórmula de Euler*.

**E. 2.157** *Exercício*. Justifique as expressões acima. A convergência da série em (2.194) é demonstrada munindo $\mathbb{C}$ da topologia métrica associada à norma Euclidiana $\|\cdot\|$ de $\mathbb{R}^2$. Para provar (2.195) deve-se separar a soma em $n$ em termos com $n$ par e $n$ ímpar e usar os fatos que $\mathbf{i}^{2m} = (-1)^m\mathbf{e}$ e $\mathbf{i}^{2m+1} = (-1)^m\mathbf{i}$, para todos $m \in \mathbb{N}_0$. ✠

Vê-se, então, que podemos escrever (2.193) na forma

$$z \;=\; |z|e^{\theta\mathbf{i}}\,,$$

que também é denominada *representação polar* de $z \in \mathbb{C}$.

### 2.6.3.2 A Álgebra dos Números Complexos Hiperbólicos

O espaço vetorial $\mathbb{R}^2$ também pode ser feito uma álgebra comutativa e associativa por meio de um outro produto, dito *produto hiperbólico*. Para $(x_1,\, x_2)$, $(y_1,\, y_2) \in \mathbb{R}^2$ defina-se o produto hiperbólico por

$$(x_1,\, x_2)\cdot(y_1,\, y_2) \;=\; (x_1y_1 + x_2y_2,\; x_1y_2 + x_2y_1)\,. \tag{2.196}$$

Compare-se essa definição a (2.191), página 251. É fácil constatar que esse produto é comutativo (pois $(x_1,\, x_2)\cdot(y_1,\, y_2) = (y_1,\, y_2)\cdot(x_1,\, x_2)$ para todos $(x_1,\, x_2)$, $(y_1,\, y_2) \in \mathbb{R}^2$) e associativo.

**E. 2.158** *Exercício*. Verifique a validade dessas afirmações! ✠

O espaço vetorial $\mathbb{R}^2$ com esse produto é denominado *álgebra dos números complexos hiperbólicos*, denotada por $\mathbb{D}$ (uma notação que, advertimos, não é universalmente adotada).

Similarmente ao que fizemos no caso dos números complexos, definamos $\mathbf{e} := (1,\ 0)$ e $\mathbf{j} := (0,\ 1)$. Podemos escrever todo $(x,\ y) \in \mathbb{R}^2$ da forma $(x,\ y) = x\mathbf{e} + y\mathbf{j}$, sendo que (2.191) indica que $\mathbf{e}$ é a unidade da álgebra (pois $(x_1,\ x_2)\cdot\mathbf{e} = \mathbf{e}\cdot(x_1,\ x_2) = (x_1,\ x_2)$) para todo $(x_1,\ x_2) \in \mathbb{R}^2$) e

$$\mathbf{j}^2 \ \equiv\ \mathbf{j}\cdot\mathbf{j} \ =\ +\mathbf{e}\,.$$

Assim, $\mathbf{j}$ tem a interpretação de "raiz quadrada" da unidade (não de menos a unidade, como no caso dos números complexos). Como elementos de $\mathbb{R}^2$, $\mathbf{j}$ e $\mathbf{i}$ coincidem, mas suas propriedades algébricas são diferentes.

A conjugação complexa é a operação unária que associa cada par $(x,\ y) \in \mathbb{R}^2$ ao par $(x,\ -y) \in \mathbb{R}^2$, ou seja, associa $z \equiv x\mathbf{e} + y\mathbf{j}$ a $\overline{z} := x\mathbf{e} + y\mathbf{j}$. É evidente que se trata de uma involução, pois $\overline{(\overline{z})} = z$ para todo $z \in \mathbb{R}^2$. É também claro que $\overline{\mathbf{e}} = \mathbf{e}$ e $\overline{\mathbf{j}} = \mathbf{j}$. Igualmente fácil é verificar a propriedade

$$\overline{z\cdot w} \ =\ \overline{z}\cdot\overline{w}\,, \tag{2.197}$$

válida para todo $z,\ w$. Se $z \equiv x\mathbf{e} + y\mathbf{j}$ vale

$$\overline{z}\cdot z \ =\ x^2 - y^2\,.$$

Verifique! Definindo-se $N : \mathbb{R}^2 \to \mathbb{R}$ por $N(z) := \overline{z}\cdot z$, segue facilmente da comutatividade e de (2.197) que

$$N(z\cdot w) \ =\ N(z)N(w)\,,$$

também para todo $z$ e $w$, assim como segue que $N\big(\overline{z}\big) = N(z)$, para todo $z$. A função $N$ é, portanto, uma forma quadrática em $\mathbb{R}^2$, mas que não é positiva, em contraste com o que ocorre com números complexos. A função $N$ é uma *norma algébrica* em $\mathbb{D}$.

Afirmamos que $z$ possui inversa se e somente se $N(z) \neq 0$, em cujo caso vale

$$z^{-1} \ =\ \frac{1}{N(z)}\,\overline{z}\,.$$

De fato, se $N(z) \neq 0$, temos pela expressão acima $z\cdot\frac{\overline{z}}{N(z)} = \frac{z\cdot\overline{z}}{N(z)} = \mathbf{e}$. Por outro lado, se $N(z) = 0$ e existisse a inversa $b = z^{-1}$, teríamos $\mathbf{e} = b\cdot z$, o que implica, multiplicando-se à direita por $\overline{z}$ e usando-se a associatividade,

$$\overline{z} \ =\ \big(b\cdot z\big)\cdot\overline{z} \ =\ b\cdot\big(z\cdot\overline{z}\big) \ =\ b\cdot N(z) \ =\ 0\,,$$

o que implica $\overline{z} = 0$ e, portanto, $z = 0$.

É fácil constatar que $N\big(\mathbf{e}\pm\mathbf{j}\big) = 0$. Consequentemente, $\mathbf{e}\pm\mathbf{j}$ não possuem inversa. Se definirmos

$$\mathbf{d}_\pm \ :=\ \frac{1}{2}\big(\mathbf{e}\pm\mathbf{j}\big) \quad \text{é fácil constatar (faça-o!) que} \quad \mathbf{d}_\pm\cdot\mathbf{d}_\pm \ =\ \mathbf{d}_\pm\,.$$

Assim, $\mathbf{d}_\pm$ são elementos idempotentes de $\mathbb{D}$. Além disso, vale $\mathbf{d}_+\cdot\mathbf{d}_- = 0 = \mathbf{d}_-\cdot\mathbf{d}_+$ e $\overline{(\mathbf{d}_\pm)} = \mathbf{d}_\mp$.

O fato de valer $\mathbf{d}_+\cdot\mathbf{d}_- = 0$ significa que $\mathbb{D}$ possui divisores de zero e, portanto, não é um anel de integridade. Vide páginas 156 e seguintes. O fato de existirem elementos não nulos em $\mathbb{D}$ sem inversa multiplicativa significa que $\mathbb{D}$ não é uma álgebra de divisão. Vide página 156.

Como $\mathbf{e} = \mathbf{d}_+ + \mathbf{d}_-$ e $\mathbf{j} = \mathbf{d}_+ - \mathbf{d}_-$, todo $z \in \mathbb{D}$ pode ser representado na forma

$$z \ =\ x\mathbf{e} + y\mathbf{j} \ =\ (x+y)\mathbf{d}_+ + (x-y)\mathbf{d}_-\,.$$

Com isso, é fácil verificar que para as combinações lineares de $\mathbf{d}_+$ e $\mathbf{d}_-$ valem as relações

$$\big(a_1\mathbf{d}_+ + a_2\mathbf{d}_-\big)\cdot\big(b_1\mathbf{d}_+ + b_2\mathbf{d}_-\big) \ =\ (a_1b_1)\mathbf{d}_+ + (a_2b_2)\mathbf{d}_-$$

para todos $a_1,\ a_2,\ b_1,\ .b_2 \in \mathbb{R}$. Concluímos com isso que $\mathbb{D}$ é isomorfa à álgebra $\mathbb{R}\oplus\mathbb{R}$, com o isomorfismo $\Phi : \mathbb{D} \to \mathbb{R}\oplus\mathbb{R}$ dado por

$$\Phi\big(x\mathbf{e} + y\mathbf{e}\big) \ =\ \Phi\big((x+y)\mathbf{d}_+ + (x-y)\mathbf{d}_-\big) \ =\ (x+y,\ x-y)\,.$$

**E. 2.159** *Exercício*. Constate que $\Phi : \mathbb{D} \to \mathbb{R} \oplus \mathbb{R}$ dada acima é bijetora e a aplicação inversa $\Phi^{-1} : \mathbb{R} \oplus \mathbb{R} \to \mathbb{D}$ é dada por $\Phi^{-1}(x,\, y) = x\mathbf{d}_+ + y\mathbf{d}_- = \frac{1}{2}(x+y)\mathbf{e} + \frac{1}{2}(x-y)\mathbf{j}$. Constate que para quaisquer $z,\, w \in \mathbb{D}$ valem $\Phi(z \cdot w) = \Phi(z) \cdot \Phi(w)$, o que mostra que $\Phi$ é, de fato, um homomorfismo. Constate também que $\Phi\big(\overline{z}\big) = \overline{\Phi(z)}$ e $\Phi(\mathbf{e}) = (1,\, 1)$, confirmando que $\Phi$ mapeia a unidade de $\mathbb{D}$ na unidade de $\mathbb{R} \oplus \mathbb{R}$. Constate que $\Phi(\mathbf{d}_+) = (1,\, 0)$ e $\Phi(\mathbf{d}_-) = (0,\, 1)$, o que significa que $\Phi$ mapeia os elementos idempotentes de $\mathbb{D}$ nos elementos idempotentes de $\mathbb{R} \oplus \mathbb{R}$. Por fim, no que concerne à relação entre as normas algébricas de $\mathbb{D}$ e $\mathbb{R} \oplus \mathbb{R}$, verifique que $N\Big(\Phi\big(x\mathbf{e} + y\mathbf{e}\big)\Big) = N\big((x+y,\, x-y)\big) = x^2 - y^2 = N\big(x\mathbf{e} + y\mathbf{e}\big)$. ✣

• **Fórmula de Euler**

Inspirados na expansão em série de Taylor da função exponencial, definamos

$$e^{\theta\mathbf{j}} \;:=\; \mathbf{e} + \sum_{n=1}^{\infty} \frac{\theta^n}{n!}\mathbf{j}^n \;. \tag{2.198}$$

Tem-se

$$e^{\theta\mathbf{j}} \;=\; \cosh(\theta)\mathbf{e} + \operatorname{senh}(\theta)\mathbf{j} \;. \tag{2.199}$$

**E. 2.160** *Exercício*. Justifique as expressões acima. A convergência da série em (2.198) é demonstrada munindo $\mathbb{D}$ da topologia métrica associada à norma Euclidiana $\|\cdot\|$ de $\mathbb{R}^2$. Para provar (2.199) deve-se separar a soma em $n$ em termos com $n$ par e $n$ ímpar e usar os fatos que $\mathbf{j}^{2m} = \mathbf{e}$ e $\mathbf{j}^{2m+1} = \mathbf{j}$, para todos $m \in \mathbb{N}_0$. ✣

△▽△▽△▽△▽△▽△▽△▽△▽△▽△▽△▽△▽△▽△▽△▽△▽△▽△▽△

A álgebra dos complexos hiperbólicos teria sido inventada por Cockle[94] em cerca de 1848. Já a álgebra dos números complexos tem raízes bem mais profundas, que remontam à Idade Mèdia, tendo sido talvez criada por Cardano[95] em cerca de 1545, e especialmente por Bombelli[96], em 1572. Como é bem sabido, a motivação original teria sido a de dar sentido a raízes de certos polinômios. Aparentemente, porém, foram Gauss[97] e Hamilton[98] os primeiros a sistematizar a noção de número complexo em termos mais próximos à modernidade. O nome de Hamilton aparecerá adiante na apresentação dos chamados *quatérnios*. O uso da letra $i$ para designar $\sqrt{-1}$ nasce com Euler[99] - uma de suas incontáveis contribuições notacionais à Matemática - e foi difundido por Gauss. Este último foi o primeiro a denominar os números complexos por esse nome.

Para textos com notas históricas sobre Álgebra Clássica e Abstrata, vide [369, 370].

### 2.6.3.3 Álgebras em $\mathbb{R}^3$. A Álgebra do Produto Vetorial

Em $\mathbb{R}^3$ podemos definir igualmente vários tipos de produtos, tais como o produto

$$(x_1,\, x_2,\, x_3) \cdot (y_1,\, y_2,\, y_3) \;=\; (x_1y_1,\, x_2y_2,\, x_3y_3) \;, \tag{2.200}$$

que é igualmente associativo e comutativo; o produto

$$(x_1,\, x_2,\, x_3) \cdot (y_1,\, y_2,\, y_3) \;=\; (x_1y_1,\, x_2y_2 - x_3y_3,\, x_2y_3 + x_3y_2) \;, \tag{2.201}$$

também associativo e comutativo ou ainda um produto como

$$(x_1,\, x_2,\, x_3) \cdot (y_1,\, y_2,\, y_3) \;=\; (x_2y_3 - x_3y_2,\, x_3y_1 - x_1y_3,\, x_1y_2 - x_2y_1) \;, \tag{2.202}$$

que não é nem associativo nem comutativo. O produto (2.200) faz de $\mathbb{R}^3$ uma álgebra isomorfa a $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$ (três cópias da álgebra dos reais). O produto (2.201) faz de $\mathbb{R}^3$ uma álgebra isomorfa a $\mathbb{R} \oplus \mathbb{C}$ e o produto (2.202) é o bem conhecido produto vetorial, muitas vezes denotado pelo símbolo $\times$ (ou, mais raramente, por $\wedge$).

O produto vetorial faz de $\mathbb{R}^3$ uma álgebra que, no entanto, não é comutativa nem associativa. Em vez disso, o produto vetorial satisfaz

[94] Sir James Cockle (1819–1895).
[95] Gerolamo Cardano (1501–1576).
[96] Rafael Bombelli (1526–1572).
[97] Johann Carl Friedrich Gauss (1777–1855).
[98] William Rowan Hamilton (1805–1865).
[99] Leonhard Euler (1707–1783).

1. *Anticomutatividade* (ou *antissimetria*):
$$(x_1,\, x_2,\, x_3) \times (y_1,\, y_2,\, y_3) \;=\; -(y_1,\, y_2,\, y_3) \times (x_1,\, x_2,\, x_3)$$
para todos $(x_1,\, x_2,\, x_3)$, $(y_1,\, y_2,\, y_3) \in \mathbb{R}^3$;
2. *Identidade de Jacobi*[100]:
$$\big((x_1,\, x_2,\, x_3) \times (y_1,\, y_2,\, y_3)\big) \times (z_1,\, z_2,\, z_3) + \big((z_1,\, z_2,\, z_3) \times (x_1,\, x_2,\, x_3)\big) \times (y_1,\, y_2,\, y_3) + \big((y_1,\, y_2,\, y_3) \times (z_1,\, z_2,\, z_3)\big) \times (x_1,\, x_2,\, x_3) \;=\; 0 \quad (2.203)$$
para todos $(x_1,\, x_2,\, x_3)$, $(y_1,\, y_2,\, y_3)$, $(z_1,\, z_2,\, z_3) \in \mathbb{R}^3$.

Observem-se as permutações cíclicas que ocorrem em (2.203).

**E. 2.161** *Exercício importante*. Usando a definição do produto vetorial em (2.202), verifique essas afirmações. ✠

**E. 2.162** *Exercício*. Usando as propriedades acima verifique que a álgebra $\mathbb{R}^3$ com o produto vetorial dado em (2.202) não possui uma unidade. ✠

### 2.6.3.4 Quatérnios

Inspirados na discussão anterior, o que se poderia, então, fazer para tornar $\mathbb{R}^4$ em uma álgebra? Naturalmente poder-se-ia definir em $\mathbb{R}^4$ várias álgebras imitando o que fizemos acima. Por exemplo, com o produto
$$(x_1,\, x_2,\, x_3,\, x_4) \cdot (y_1,\, y_2,\, y_3,\, y_4) \;=\; (x_1y_1,\, x_2y_2,\, x_3y_3,\, x_4y_4)\,, \quad (2.204)$$
$\mathbb{R}^4$ torna-se uma álgebra associativa e comutativa isomorfa a $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$. Com o produto
$$\big(x_1,\, x_2,\, x_3,\, x_4\big) \cdot \big(y_1,\, y_2,\, y_3,\, y_4\big) \;=\; \big(x_1y_1 - x_2y_2,\, x_1y_2 + x_2y_1,\, x_3y_3 - x_4y_4,\, x_3y_4 + x_4y_3\big)\,, \quad (2.205)$$
$\mathbb{R}^4$ torna-se uma álgebra associativa e comutativa isomorfa a $\mathbb{C} \oplus \mathbb{C}$. Com o produto
$$\big(x_1,\, x_2,\, x_3,\, x_4\big) \cdot \big(y_1,\, y_2,\, y_3,\, y_4\big) \;=\; \big(x_2y_3 - x_3y_2,\, x_3y_1 - x_1y_3,\, x_1y_2 - x_2y_1,\, x_4y_4\big) \quad (2.206)$$
$\mathbb{R}^4$ torna-se uma álgebra não associativa e não comutativa isomorfa a $\mathbb{R}^3 \oplus \mathbb{R}$, com o produto vetorial na componente $\mathbb{R}^3$.

Há também outros produtos que são meras variantes das listadas acima (ache algumas). Existe, porém, um produto não-trivial, denominado *produto quaterniônico*, que faz de $\mathbb{R}^4$ uma álgebra associativa, com unidade, mas não comutativa. Esse produto foi descoberto (ou inventado) por W. R. Hamilton[101]. A história da descoberta desse produto em $\mathbb{R}^4$, ocorrida em 16 de outubro 1843, numa tentativa de generalizar a álgebra dos números complexos para mais que duas dimensões, é bastante pitoresca (vide adiante) e representou um marco na história da Álgebra por ser o primeiro exemplo de uma álgebra associativa mas não comutativa (a descoberta de Hamilton antecede a introdução da álgebra das matrizes e a introdução do produto vetorial). Esse produto é o seguinte:
$$(x_0,\, x_1,\, x_2,\, x_3) \cdot (y_0,\, y_1,\, y_2,\, y_3) \;:=\; \big(x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3,\, x_0y_1 + y_0x_1 + x_2y_3 - x_3y_2,\, x_0y_2 + y_0x_2 + x_3y_1 - x_1y_3,\, x_0y_3 + y_0x_3 + x_1y_2 - x_2y_1\big)\,. \quad (2.207)$$

[100] Carl Gustav Jacob Jacobi (1804–1851).
[101] William Rowan Hamilton (1805–1865). W. R. Hamilton foi também o inventor do chamado formalismo Hamiltoniano da Mecânica Clássica.

**E. 2.163** *Exercício*. Mostre que o produto acima é associativo. *Sugestão:* paciência. ✠

O espaço vetorial $\mathbb{R}^4$ dotado do produto acima é denominado *álgebra dos quatérnios* ou *álgebra quaterniônica* e é denotada frequentemente por $\mathbb{H}$ (em honra a Hamilton). A álgebra $\mathbb{H}$ é associativa mas não é comutativa. $\mathbb{H}$ tem uma unidade, a saber, o vetor $(1,\ 0,\ 0,\ 0) \in \mathbb{R}^4$.

**E. 2.164** *Exercício*. Mostre que $\mathbb{H}$ não é uma álgebra comutativa. ✠

**E. 2.165** *Exercício*. Mostre que $(1,\ 0,\ 0,\ 0)$ é a unidade de $\mathbb{H}$. ✠

Há uma maneira melhor de representar o produto quaterniônico que a expressão (2.207). Vamos escrever os vetores da base canônica de $\mathbb{R}^4$ como

$$e_0 \ = \ (1,\ 0,\ 0,\ 0)\,, \qquad e_1 \ = \ (0,\ 1,\ 0,\ 0)\,, \qquad e_2 \ = \ (0,\ 0,\ 1,\ 0)\,, \qquad e_3 \ = \ (0,\ 0,\ 0,\ 1)\,,$$

de modo que todo $x \in \mathbb{R}^4$ pode ser escrito na forma $x = x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3$. O produto quaterniônico pode, portanto, ser definido pelo produto dos elementos da base canônica, que segue as seguintes regras:

$$\begin{aligned} &1.\quad e_0 \text{ é a unidade da álgebra: } x \cdot e_0 \ = \ e_0 \cdot x \ = \ x \text{ para todo } x \in \mathbb{R}^4\,. \\ &2.\quad (e_1)^2 \ = \ (e_2)^2 \ = \ (e_3)^2 \ = \ -e_0\,. \\ &3.\quad e_ae_b = -e_be_a \text{ para todo } a \neq b \text{ com } a,\ b = 1,\ 2,\ 3\,. \\ &4.\quad e_1e_2 = e_3,\ \ e_2e_3 = e_1 \ \text{ e } \ e_3e_1 = e_2\,. \end{aligned} \tag{2.208}$$

Essas foram as regras do produto quaterniônico tal como formuladas originalmente por Hamilton.

**E. 2.166** *Exercício*. Verifique que as regras (2.208) reproduzem perfeitamente o produto quaterniônico (2.207). ✠

*Comentário histórico*. Hamilton fora o primeiro, em 1835, a encarar a álgebra dos complexos da forma semelhante à que expomos acima: como o espaço vetorial $\mathbb{R}^2$ com o produto definido em (2.191). Tendo atingido esse entendimento, Hamilton iniciou uma série de tentativas de generalizar essas ideias para o espaço tridimensional $\mathbb{R}^3$. Mais especificamente, e usando linguagem atual, Hamilton procurou por uma álgebra de divisão normada em $\mathbb{R}^3$. Hamilton dedicou-se por um longo tempo, de forma intensiva e obstinada, a essa procura. Em carta escrita muitos anos depois a um de seus filhos, Hamilton relata: *"Every morning in the early part of the above-cited month, on my coming down to breakfast, your (then) little brother William Edwin, and yourself, used to ask me: 'Well, Papa, can you multiply triplets?' Whereto I was always obliged to reply, with a sad shake of the head: 'No, I can only add and subtract them'"*.

Hamilton falhou nessa tentativa pois, como é hoje entendido, tais álgebras não existem no caso tridimensional. Instintivamente, porém, Hamilton começou a procurar por uma solução para seu problema tornando-o mais difícil (um "método" não raramente empregado nas Ciências, ademais) e começou a pensar no caso quadridimensional.

As regras de produto de quatérnios (em versão próxima àquelas expressas em (2.208)) teriam subitamente ocorrido a Hamilton, após inúmeras e obstinadas tentativas de sua parte, quando o mesmo caminhava na manhã do dia 16 de outubro 1843 com sua esposa ao longo do *Royal Canal*, em Dublin, Irlanda. Hamilton dirigia-se à Real Academia Irlandesa para presidir uma sessão. Segundo seu relato, *"I then and there felt the galvanic circuit of thought* close*; and the sparks which fell from it were the fundamental equations between i, j, k; exactly such as I have used them ever since"*.

Entusiasmado com seu achado, e temendo esquecer suas relações, Hamilton teria imediatamente talhado com seu canivete as expressões que definem o produto de quatérnios na ponte Brougham (também denominada "Broom Bridge"), sobre o mesmo canal. O entalhe original de Hamilton não sobreviveu, se realmente existiu, mas certo é que até o presente existe uma placa comemorativa posterior sobre a mesma ponte. Vide Figura 2.2, página 257.

Como se vê, usa-se na Figura 2.2 uma notação que se relaciona à nossa pelas identificações $1 \equiv e_0$, $i \equiv e_1$, $j \equiv e_2$, $k \equiv e_3$. O termo "quatérnio" foi cunhado por Hamilton. Sua primeira publicação a respeito foi a carta: *"On quaternions, or on a new system of imaginaries in algebra"*, Edinburgh and Dublin Philosophical Magazine and Journal of Science, vol. XXV, 489–495 (1844).

Hamilton sempre acreditou que a álgebra dos quatérnios teria um grande impacto na Física e fez diversas tentativas de formular as leis da Mecânica Clássica e do Eletromagnetismo usando quatérnios. Sua influência estendeu-se, entre outros, a Maxwell[102], que originalmente formulou as equações básicas do Eletromagnetismo, que levam seu nome, em termos de quatérnios (vide [356]). Essas primeiras tentativas, porém, acabaram eclipsadas pelo advento da Análise Vetorial, sob a influência de Helmholtz[103], Gibbs[104] e Heaviside[105]. Hoje em dia, quatérnios encontram aplicações relevantes até mesmo em Computação Gráfica, devido à sua relação com o grupo de rotações. ♣

[102] James Clerk Maxwell (1831–1879).
[103] Hermann Ludwig Ferdinand von Helmholtz (1821–1894).
[104] Josiah Willard Gibbs (1839–1903).
[105] Oliver Heaviside (1850–1925).

Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication
$i^2 = j^2 = k^2 = ijk = -1$
& cut it on a stone of this bridge


Figura 2.2: Placa comemorativa à descoberta de Hamilton na Brougham Bridge, Dublin.

• **Subálgebras Abelianas**

A álgebra dos quatérnios $\mathbb{H}$ possui algumas subálgebras Abelianas de interesse, como mostram os exercícios a seguir.

**E. 2.167** *Exercício*. Mostre que $\mathbb{H}_a := \{x \in \mathbb{R}^4,\ x = x_0 e_0 + x_1 e_1 = (x_0,\ x_1,\ 0,\ 0)\}$ é uma subálgebra Abeliana de $\mathbb{H}$ que é isomorfa à álgebra $\mathbb{C}$ dos complexos. ✠

**E. 2.168** *Exercício*. Mostre o mesmo para $\mathbb{H}_b := \{x \in \mathbb{R}^4,\ x = x_0 e_0 + x_2 e_2 = (x_0,\ 0,\ x_2,\ 0)\}$ e $\mathbb{H}_c := \{x \in \mathbb{R}^4,\ x = x_0 e_0 + x_3 e_3 = (x_0,\ 0,\ 0,\ x_3)\}$. ✠

**E. 2.169** *Exercício*. Será possível fazer de $\mathbb{R}^4$ um espaço vetorial complexo? Seja $\alpha \in \mathbb{C}$ e considere para $x \in \mathbb{R}^4$ o produto do escalar $\alpha$ pelo vetor $x$ definido por

$$\alpha \cdot x \ = \ \big(\mathsf{Re}(\alpha) e_0 + \mathsf{Im}(\alpha) e_1\big) \cdot x \ ,$$

onde o produto do lado direito é o produto quaterniônico. Mostre que isso faz de $\mathbb{R}^4$ um espaço vetorial sobre o corpo dos complexos. Para isto verifique as propriedades definidoras de um espaço vetorial listadas à página 140. ✠

**E. 2.170** *Exercício*. No exercício anterior há outros produtos do escalar $\alpha$ pelo vetor $x$ que podem ser considerados:

$$\alpha \cdot x \ = \ \big(\mathsf{Re}(\alpha) e_0 + \mathsf{Im}(\alpha) e_2\big) \cdot x \ ,$$

ou

$$\alpha \cdot x \ = \ \big(\mathsf{Re}(\alpha) e_0 + \mathsf{Im}(\alpha) e_3\big) \cdot x \ ,$$

ou mesmo

$$\alpha \cdot x \ = \ x \cdot \big(\mathsf{Re}(\alpha) e_0 + \mathsf{Im}(\alpha) e_1\big)$$

etc. Mostre que todos esses seis produtos de escalares $\alpha \in \mathbb{C}$ por vetores $x \in \mathbb{R}^4$ fazem de $\mathbb{R}^4$ um espaço vetorial sobre o corpo dos complexos. ✠

• **Quatérnios e álgebras de matrizes $2 \times 2$**

Além de ser de manipulação mais simples, as regras (2.208) permitem representar a álgebra quaterniônica de um modo talvez mais familiar, a saber, em termos de certas matrizes complexas $2 \times 2$.

Sejam $a$ e $b$ dois números complexos e seja $M(a,\ b)$ a matriz

$$M(a,\ b) \ := \ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \ ,$$

onde $\overline{z}$ é o complexo conjugado de $z \in \mathbb{C}$. É fácil de se ver que o conjunto de todas as matrizes dessa forma é uma álgebra

sobre os reais com o produto usual de matrizes, pois vale

$$M(a,\ b)M(c,\ d)\ =\ M\big(ac-b\overline{d},\ ad+b\overline{c}\big)\ .$$

**E. 2.171** *Exercício.* Verifique! ✠

Existe um isomorfismo entre a álgebra dos quatérnios e essa álgebra de matrizes $2\times 2$. Ele associa (bijetivamente!) a cada quádrupla $(x_0,\ x_1,\ x_2,\ x_3)\in\mathbb{H}$ a matriz $M\big(x_0-ix_3,\ x_2+ix_1\big)\in \mathrm{Mat}\,(\mathbb{C},\ 2)$:

$$x\ =\ \big(x_0,\ x_1,\ x_2,\ x_3\big)\ \longleftrightarrow\ \begin{pmatrix} x_0-ix_3 & x_2+ix_1 \\ -x_2+ix_1 & x_0+ix_3 \end{pmatrix}\ =:\ \mathsf{M}(x)\ . \tag{2.209}$$

É fácil verificar (faça!) que o produto quaterniônico é respeitado por essa associação:

$$\mathsf{M}(x)\mathsf{M}(y)\ =\ \mathsf{M}\big(x\cdot y\big)\ ,$$

onde, acima, $x\cdot y$ é o produto quaterniônico de $x$ e $y\in\mathbb{R}^4$.

Note-se que por essa associação tem-se

$$\mathsf{M}(x)\ =\ \mathsf{M}(x_0e_0+x_1e_1+x_2e_2+x_3e_3)\ =\ x_0\mathsf{M}(e_0)+x_1\mathsf{M}(e_1)+x_2\mathsf{M}(e_2)+x_3\mathsf{M}(e_3)\ ,$$

com

$$\mathsf{M}(e_0)\ =\ \mathbb{1}\ ,\qquad \mathsf{M}(e_1)\ =\ i\sigma_1\ ,\qquad \mathsf{M}(e_2)\ =\ i\sigma_2\ ,\qquad \mathsf{M}(e_3)\ =\ -i\sigma_3\ ,$$

onde

$$\mathbb{1}\ =\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\ ,\qquad \sigma_1=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\ ,\qquad \sigma_2=\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\quad\text{e}\quad \sigma_3=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\ , \tag{2.210}$$

as três matrizes últimas sendo as chamadas *matrizes de Pauli*[106], que satisfazem

1. $(\sigma_1)^2=(\sigma_2)^2=(\sigma_3)^2=\mathbb{1}$,
2. $\sigma_i\sigma_j=-\sigma_j\sigma_i$ para todo $i\neq j$ e
3. $\sigma_1\sigma_2=i\sigma_3$, $\sigma_2\sigma_3=i\sigma_1$, $\sigma_3\sigma_1=i\sigma_2$.

**E. 2.172** *Exercício.* Verifique essas propriedades. ✠

O aparecimento das matrizes de Pauli, acima, aponta para a existência de uma íntima relação entre quatérnios e o grupo SU(2), como veremos mais adiante.

• **O conjugado quaterniônico, ou involução quaterniônica**

Definimos o *conjugado quaterniônico* de $x=x_0e_0+x_1e_1+x_2e_2+x_3e_3\in\mathbb{H}$ por

$$\overline{x}\ =\ x_0e_0-x_1e_1-x_2e_2-x_3e_3\ \in\ \mathbb{H}\ .$$

A aplicação $\mathbb{H}\ni x\longmapsto\overline{x}\in\mathbb{H}$ é também denominada *involução quaterniônica*. Note-se que $\overline{\overline{x}}=x$ para todo $x\in\mathbb{H}$.

É fácil constatar (faça-o!) que

$$\overline{x}\cdot x\ =\ \Big((x_0)^2+(x_1)^2+(x_2)^2+(x_3)^2\Big)\ e_0\ . \tag{2.211}$$

• **Norma quaterniônica**

Em uma álgebra $\mathcal{A}$ uma função $N:\mathcal{A}\to\mathbb{R}_+$ que satisfaça $N(a\cdot b)=N(a)N(b)$ para todos $a,\ b\in\mathcal{A}$, com $N(a)=0\Leftrightarrow a=0$, é dita ser uma *norma algébrica*. Em $\mathbb{R}$ e $\mathbb{C}$ tem-se a norma algébrica $N(z)=|z|$, o módulo ou valor

[106] Wolfgang Ernst Pauli (1900–1958).

absoluto de $z$. No caso dos complexos, essa norma também satisfaz $\left|\overline{z}\right| = |z|$. O conjunto dos quatérnios $\mathbb{H}$ também possui uma norma algébrica, como agora veremos.

A raiz quadrada do préfator que multiplica $e_0$ na expressão (2.211) é denotado por $\|x\|_{\mathbb{H}}$, ou simplesmente por $\|x\|$, e é denominado *norma quaterniônica* de $x \in \mathbb{H}$:

$$\|x\|_{\mathbb{H}} \equiv \|x\| := \sqrt{(x_0)^2 + (x_1)^2 + (x_2)^2 + (x_3)^2} \quad \in [0, \infty) , \tag{2.212}$$

de sorte que podemos escrever $\overline{x} \cdot x = \|x\|^2 e_0$. Note-se que $\|x\| = 0 \Leftrightarrow x = 0$ e que

$$\|x + y\|_{\mathbb{H}} \leq \|x\|_{\mathbb{H}} + \|y\|_{\mathbb{H}}$$

para todos $x,\ y \in \mathbb{H}$.

**E. 2.173** *Exercício*. Verifique que a norma $\|\cdot\|_{\mathbb{H}}$ satisfaz

$$\|x \cdot y\|_{\mathbb{H}} = \|x\|_{\mathbb{H}} \|y\|_{\mathbb{H}} , \tag{2.213}$$

para todos $x,\ y \in \mathbb{H}$. Essa propriedade faz de $\|\cdot\|_{\mathbb{H}}$ o que se denomina ser uma *norma operatorial*, ou *algébrica*. ✠

Vale também, como é fácil ver,

$$\left\|\overline{x}\right\|_{\mathbb{H}} = \|x\|_{\mathbb{H}} , \tag{2.214}$$

para todo $x \in \mathbb{H}$.

• **$\mathbb{H}$ é um anel de divisão**

É fácil ver que a álgebra dos quatérnios é um anel de divisão (vide página 156), ou seja, todo $x \in \mathbb{R}^4$, $x \neq 0$, tem uma inversa em relação ao produto quaterniônico. Do isomorfismo $\mathsf{M}$ definido em (2.209) acima vê-se que

$$\det\big(\mathsf{M}(x)\big) = \det\big(\mathsf{M}(x_0 + ix_1, x_2 + ix_3)\big) = (x_0)^2 + (x_1)^2 + (x_2)^2 + (x_3)^2 = \|x\|_{\mathbb{H}}^2$$

e, portanto, $\mathsf{M}(x)$ tem uma matriz inversa sempre que $x \neq 0$.

De fato, é fácil ver que para $x \neq 0$ tem-se a inversa multiplicativa quaterniônica

$$x^{-1} := \frac{1}{\|x\|_{\mathbb{H}}^2}\, \overline{x} \quad \in \mathbb{H} , \tag{2.215}$$

pois vale $x^{-1} \cdot x = x \cdot x^{-1} = e_0$.

**E. 2.174** *Exercício*. Verifique! ✠

Note-se que, por $\mathbb{H}$ ser um anel de divisão, $\mathbb{H}$ não tem divisores de zero: $x \cdot y = 0$ se e somente se $x = 0$ ou $y = 0$. Como $\mathbb{H}$ é uma álgebra (real), é comum dizer-se que $\mathbb{H}$ é uma álgebra de divisão.

Há um teorema devido a Hurwitz[107] que afirma que há apenas quatro álgebras que são álgebras de divisão[108] e possuem uma norma algébrica: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ e a chamada álgebra dos octônios, da qual não falaremos aqui. Esta última, por sinal, não é associativa.

• **O conjunto dos quatérnios não nulos $\mathbb{H} \setminus \{0\}$ é um grupo**

Comentemos que as considerações acima dizem-nos também que $\mathbb{H} \setminus \{0\}$, o conjunto dos quatérnios não nulos, é também um grupo não Abeliano para a operação (associativa) de produto de quatérnios. O elemento neutro é $e_0$ e a inversa é aquela dada em (2.215).

O grupo quaterniônico $\mathbb{H} \setminus \{0\}$ possui, como veremos, alguns subgrupos de interesse.

• **O grupo quaterniônico $\mathbb{Q}_8$**

O conjunto de oito elementos

$$\mathbb{Q}_8 = \big\{ \pm e_0,\ \pm e_1,\ \pm e_2,\ \pm e_3 \big\} \tag{2.216}$$

é um subgrupo não Abeliano finito de $\mathbb{H} \setminus \{0\}$ e é denominado *grupo quaterniônico*.

[107] Adolf Hurwitz (1859–1919).
[108] Vide definição à página 156.

**E. 2.175** *Exercício*. Verifique que $\mathbb{Q}_8$ é um grupo para o produto quaterniônico. Use para tal as regras de produto para os elementos $e_k$, $k = 0,\ 1,\ 2,\ 3$, dadas em (2.208). ✠

• **O grupo dos quatérnios unitários $\mathbb{H}_1$ e o grupo SU(2)**

Um quatérnio $x \in \mathbb{H}$ é dito ser um *quatérnio unitário* se $\|x\|_{\mathbb{H}} = 1$.

Como já comentamos, $\mathbb{H} \setminus \{0\}$ é um grupo em relação ao produto quaterniônico. Devido à propriedade (2.213), é evidente que o produto de dois quatérnios unitários é igualmente um quatérnio unitário. Devido a (2.215) e a (2.214), é também elementar constatar que o elemento inverso de um quatérnio unitário é igualmente um quatérnio unitário (a saber, se $x \in \mathbb{H}$ é um quatérnio unitário, então $x^{-1} = \overline{x}$). Concluímos disso que

$$\mathbb{H}_1 \ := \ \Big\{ x \ = \ x_0 e_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 \ \in \ \mathbb{H}, \ \ \|x\|_{\mathbb{H}} \ = \ 1 \Big\} \tag{2.217}$$

é um grupo (não Abeliano) com relação ao produto quaterniônico, denominado *grupo dos quatérnios unitários*. O grupo finito $\mathbb{Q}_8$, definido em (2.216), é um subgrupo de $\mathbb{H}_1$ o qual, por sua vez, é um subgrupo de $\mathbb{H} \setminus \{0\}$.

A condição $\|x\|_{\mathbb{H}} = 1$ em (2.217) significa que $(x_0)^2 + (x_1)^2 + (x_2)^2 + (x_3)^2 \ = \ 1$. Assim, podemos identificar o conjunto $\mathbb{H}_1$ com $S^3$: a superfície da esfera de raio 1 em $\mathbb{R}^4$. (Lembremos que para todo inteiro $n \geq 1$, o conjunto de pontos $S^n := \big\{(x_1,\ \ldots,\ x_{n+1}) \in \mathbb{R}^{n+1} \text{ com } x_1^2 + \cdots + x_{n+1}^2 = 1\big\} \ \subset \ \mathbb{R}^{n+1}$ designa a superfície da esfera unitária de $\mathbb{R}^{n+1}$).

Como a aplicação $\mathsf{M}$ definida em (2.209) é um isomorfismo, concluímos que a coleção de matrizes $\big\{\mathsf{M}(x),\ x \in \mathbb{H}_1\big\}$ é um grupo (pelo produto matricial usual) e que esse grupo é isomorfo ao grupo $\mathbb{H}_1$. De forma mais explícita, esse é o grupo das matrizes

$$\left\{ \begin{pmatrix} x_0 - ix_3 & x_2 + ix_1 \\ -x_2 + ix_1 & x_0 + ix_3 \end{pmatrix} \ \text{ com } x_0,\ x_1,\ x_2,\ x_3 \in \mathbb{R} \text{ tais que } (x_0)^2 + (x_1)^2 + (x_2)^2 + (x_3)^2 \ = \ 1 \right\} .$$

Como veremos na Seção 21.3.4, página 1177, (vide particularmente a expressão (21.169)), esse grupo de matrizes é idêntico ao grupo SU(2), o grupo das matrizes unitárias $2 \times 2$ de determinante 1. Concluímos disso que o grupo $\mathbb{H}_1$ e o grupo SU(2) são isomorfos, com o isomorfismo definido em (2.209).

* ** *** ** *

A álgebra $\mathbb{H}$ possui várias outras propriedades interessantes, mas vamos encerrar aqui nossa exposição introdutória. O leitor interessado poderá encontrar mais sobre $\mathbb{H}$ nos bons livros sobre Álgebra. Para mais detalhes sobre a relação entre quatérnios e os grupos SU(2) e SO(3), vide, e.g., [488].

# Apêndices

## 2.A Prova de (2.186)

Neste apêndice demonstramos a relação (2.186), página 246, e sua versão para o contexto de variedades diferenciáveis, a relação (36.12).

Sejam $\omega_1 := \sum_k \alpha_k a_0^k \oplus a_1^k \oplus \cdots \oplus a_m^k$ e $\omega_2 := \sum_l \beta_l b_0^l \oplus b_1^l \oplus \cdots \oplus b_m^l$ elementos de $\mathscr{T}_A(U)$. Pelas definições, tem-se

$$
\begin{aligned}
I_u\Big(\omega_1 \wedge \omega_2\Big) &\overset{(2.180)}{=} \bigoplus_{q=0}^{m} \sum_{r=0}^{q} I_u^q \left[ \left( \sum_k \alpha_k a_r^k \right) \wedge_{r,\,q-r} \left( \sum_l \beta_l b_{q-r}^l \right) \right] \\
&\overset{(2.184)}{=} \bigoplus_{q=0}^{m} \sum_{r=0}^{q} \left[ I_u^r \left( \sum_k \alpha_k a_r^k \right) \wedge_{r,\,q-r} \left( \sum_l \beta_l b_{q-r}^l \right) \right. \\
&\qquad \left. + (-1)^r \left( \sum_k \alpha_k a_r^k \right) \wedge_{r,\,q-r} I_u^{q-r} \left( \sum_l \beta_l b_{q-r}^l \right) \right] \\
&= \sum_k \sum_l \alpha_k \beta_l \left\{ \left[ \bigoplus_{q=0}^{m} I_u^q \left( a_q^k \right) \right] \wedge \left[ \bigoplus_{q=0}^{m} \left( b_q^l \right) \right] + \left[ \bigoplus_{q=0}^{m} \left( (-1)^r a_r^k \right) \right] \wedge \left[ \bigoplus_{q=0}^{m} I_u^q \left( b_q^l \right) \right] \right\} . \\
&= I_u \left[ \sum_k \alpha_k \bigoplus_{q=0}^{m} a_q^k \right] \wedge \left[ \sum_l \beta_l \bigoplus_{q=0}^{m} b_q^l \right] + \left[ \sum_k \alpha_k \bigoplus_{q=0}^{m} (-1)^k a_q^k \right] \wedge \left[ \sum_l \beta_l \bigoplus_{q=0}^{m} b_q^l \right] \\
&= \big(I_u \omega_1\big) \wedge \omega_2 + \big(G\omega_1\big) \wedge \big(I_u \omega_2\big) ,
\end{aligned}
$$

onde $G : \mathscr{T}_A(U) \to \mathscr{T}_A(U)$, o chamado *operador de graduação*, é o operador linear definido por

$$
G \bigoplus_{j=0}^{m} a_j \;:=\; \bigoplus_{j=0}^{m} (-1)^j a_j \; .
$$

Por exemplo, no caso $m = 5$, $G\Big(a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5\Big) = a_0 \oplus (-a_1) \oplus a_2 \oplus (-a_3) \oplus a_4 \oplus (-a_5)$.