Álgebra: notas de estudo

Guilherme Philippi

5 de agosto de 2021

Sumário

1

Introdução

2

Preliminares

2.1 Elementos de Álgebra Abstrata

2.1.1 Relações entre conjuntos

Definição 2.1.1 (Produto cartesiano)**.** Sejam A e B conjuntos. O conjunto

$$A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$$

é o *produto cartesiano de A e B.*

Exemplo 2.1.1. Se $A = \{1, 2, 3\}$ e $B = 3, 4$, então

$$A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}.$$

Definição 2.1.2 (Relação)**.** Uma *relação* entre dois conjuntos A e B é um subconjunto $\mathcal{R} \subset A \times B$. Lê-se $(a, b) \in \mathcal{R}$ como "a está relacionado com b" e escreve-se $a\mathcal{R}b$.

Exemplo 2.1.2 (Relação de igualdade)**.** A realação $=$, chamada *relação de igualdade*, é definida sobre um conjunto S por

$$= \text{ é o subconjunto } \{(x, x) \mid x \in S\} \subset S \times S.$$

Observação 2.1.1. Sempre que uma relação for definida entre um conjunto S e ele mesmo, como no exemplo 2.1.2, diremos que esta é uma relação *sobre S*.

Definição 2.1.3 (Função)**.** Uma *função* φ que mapeia X em Y é uma relação entre X e Y com a propriedade de que cada $x \in X$ só irá aparecer uma única vez, e exatamente uma, em um par ordenado $(x, y) \in \varphi$. Também chamamos φ de *mapa* ou *mapeamento* de X em Y. Escrevemos $\varphi : X \longrightarrow Y$ e expressaremos $(x, y) \in \varphi$ por $\varphi(x) = y$. O *domínio* de φ é o conjunto X e o conjunto Y é dito *contradomínio* de φ. Chama-se de *alcance* de φ o conjunto $\varphi[X] = \{\varphi(x) \mid x \in X\}$.

Definição 2.1.4 (Função injetiva e sobrejetiva)**.** Uma função $\varphi : X \longrightarrow Y$ é *injetiva* se $\varphi(x_1) = \varphi(x_2) \iff x_1 = x_2$. Também, φ é dita *sobrejetiva* se o alcance de φ é Y. Se uma função é injetiva e sobrejetiva, então dizemos que a função é *bijetiva.*

2.1.2 Leis de composição

Definição 2.1.5 (Lei de composição)**.** Uma *lei de composição* sobre um conjunto S é uma função (ou, uma operação binária) $* : S \times S \longrightarrow S$.

Observação 2.1.2 (Notação de operação)**.** Usaremos a notação $*(a,b) = a * b$, para simplificar a escrita de propriedades. Também, quando não houver ambiguidade, suprimiremos o simbolo da lei, fazendo $a * b = ab$.

Definição 2.1.6. Para $a, b, c \in S$, uma lei de composição $*$ é dita

- *Associativa*, se $(a * b) * c = a * (b * c)$;
- *Comutativa*, se $a * b = b * a$.

Proposição 2.1.1. *Seja uma lei associativa dada sobre o conjunto S. Há uma única forma de definir, para todo inteiro n, um produto de n elementos $a_1, \dots, a_n \in S$ (diremos $[a_1 \cdots a_n]$) com as seguintes propriedades:*

1. *o produto $[a_1]$ de um elemento é o próprio elemento;*
2. *o produto $[a_1 a_2]$ de dois elementos é dado pela lei de composição;*
3. *para todo inteiro $1 \leq i \leq n$, $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$.*

Demonstração. A demonstração dessa proposição é feita por indução em n. □

Definição 2.1.7. Dizemos que $e \in S$ é *identidade* para uma lei de composição se $ea = ae = a$ para todo $a \in S$.

Proposição 2.1.2. *O elemento identidade é único.*

Demonstração. Se e, e' são identidades, já que e é identidade, então $ee' = e'$ e, como e' é uma identidade, $ee' = e$. Logo $e = e'$, isto é, a identidade é única. □

Observação 2.1.3. Usaremos $\vec{1}$ para representar a identidade multiplicativa e $\vec{0}$ para denotar a aditiva.

Definição 2.1.8 (Elemento inverso)**.** Seja uma lei de composição que possua uma identidade. Um elemento $a \in S$ é chamado *invertível* se há um outro elemento $b \in S$ tal que $ab = ba = 1$. Desde que b exista, ela é única e a denotaremos por a^{-1} e a chamaremos *inversa de a*.

Proposição 2.1.3. *Se $a, b \in S$ possuem inversa, então a composição $(ab)^{-1} = b^{-1}a^{-1}$.*

Observação 2.1.4 (Potências)**.** Usaremos as seguintes notações:

- $a^n = a^{n-1}a$ é a composição de $a \cdots a$ n vezes;
- a^{-n} é a inversa de a^n;
- $a^0 = \vec{1}$.

Com isso, tem-se que $a^{r+s} = a^r a^s$ e $(a^r)^s = a^{rs}$. (Isso não induz uma notação de fração $\frac{b}{a}$ a menos que seja uma lei comutativa, visto que ba^{-1} pode ser diferente de $a^{-1}b$). Para falar de uma lei de composição aditiva, usaremos $-a$ no lugar de a^{-1} e na no lugar de a^n.

2.1.3 Grupos

Definição 2.1.9 (Grupo)**.** Um *grupo* $(G, *)$ é um conjunto G onde uma lei de composição $*$ é dada sobre G tal que os seguintes axiomas são satisfeitos:

1. *(Associatividade).* Para todo $a, b, c \in G$, tem-se
$$(a * b) * c = a * (b * c);$$
2. *(Existência da identidade).* Existe um elemento $\vec{1} \in G$ tal que, para todo $a \in G$,
$$\vec{1} * a = a * \vec{1} = a;$$
3. *(Existência do inverso).* Para todo $a \in G$ existe um elemento $a' \in G$ tal que
$$a * a' = a' * a = \vec{1}.$$

Observação 2.1.5. É comum abusar da notação e chamar um grupo $(G, *)$ e o conjunto de seus elementos G pelo mesmo simbolo, omitindo a lei de composição na falta de ambiguidade.

Definição 2.1.10 (Grupo abeliano)**.** Um *grupo abeliano* é um grupo com uma lei de composição comutativa. Costuma-se usar a notação aditiva para grupos abelianos.

Proposição 2.1.4 (Lei do cancelamento)**.** *Seja a, b, c elementos de um grupo G. Se $ab = ac$, então $b = c$.*

Subgrupos

Definição 2.1.11 (Subgrupo)**.** Um subconjunto H de um grupo G é chamado de *subgrupo* de G (e escreve-se $H \leq G$) se possuir as seguintes propriedades:

1. *(Fechado).* Se $a, b \in H$, então $ab \in H$;
2. *(Identidade).* $1 \in H$;
3. *(Inversível).* Se $a \in H$, então $a^{-1} \in H$.

Observação 2.1.6 (Lei de composição induzida)**.** Veja que a propriedade 1 necessita de uma lei de composição. Usamos a lei de composição de G para definir uma lei de composição de H, chamada *lei de composição induzida*. Essas propriedades garantem que H é um grupo com respeito a sua lei induzida.

Definição 2.1.12 (Subgrupo apropriado)**.** Todo grupo G possui dois subgrupos triviais: O subgrupo formado por todos os elementos de G e o subgrupo $\{\vec{1}\}$, formado pela identidade de G. Diz-se que um subgrupo é um *subgrupo apropriado* se for diferente desses dois.

Definição 2.1.13 (Centro de um grupo)**.** O *centro* $Z(G)$ de um grupo G é o conjunto de elementos que comutam com todo elemento de G:
$$Z(G) = \{z \in G \mid zx = xz \text{ para todo } x \in G\}.$$

Exemplo 2.1.3. Utilizando da notação multiplicativa, define-se o *subgrupo cíclico* H gerados por um elemento arbitrário x de um grupo G como o conjunto de todas as potências de x: $H = \{\dots, x^{-2}, x^{-1}, \vec{1}, x, x^2, \dots\}$.

Definição 2.1.14. Chama-se *ordem* de um grupo G o número $|G|$ de elementos de G.

Também pode-se definir um subgrupo de um grupo G *gerado por um subconjunto* $U \subset G$. Esse é o menor subgrupo de G que contém U e consiste de todos os elementos de G que podem ser espressos como um produto de uma cadeia de elementos de U e seus inversos.

Exemplo 2.1.4. O *grupo de quaternions* H é o menor subgrupo do conjunto de matrizes 2×2 complexas invertíveis que não é cíclico. Isso consiste nas oito matrizes

$$H = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\},$$

onde

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \ \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \ \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Os dois elementos $\mathbf{i}, \mathbf{j}$ geram H, e o calculo leva as formulas

$$\mathbf{i}^4 = 1, \quad \mathbf{i}^2 = \mathbf{j}^2, \quad \mathbf{ji} = \mathbf{i}^3\mathbf{j}.$$

Homomorfismos e isomorfismos

Definição 2.1.15 (Homomorfismo de grupo)**.** Sejam $(G, *)$ e $(G', \cdot)$ dois grupos. Um *homomorfismo* $\varphi : G \longrightarrow G'$ é um mapeamento tal que

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \ \forall \ a, b \in G. \qquad \text{(propriedade de homomorfismo)}$$

Exemplo 2.1.5 (Inclusão)**.** Seja H o subgrupo de um grupo G. O homomorfismo $i : H \longrightarrow G$ é dito *inclusão* de H em G, definido por $i(x) = x$.

Proposição 2.1.5. *Um homomorfismo $\varphi : G \longrightarrow G'$ mapeia a identidade de G à identidade de G' e transforma as inversas de G nas respectivas inversas em G'. Isto é, as seguintes propriedades valem*

- $\varphi(\vec{1}) = \vec{1}$ *e*
- $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Observação 2.1.7. Por conta da Proposição 2.1.5, dizemos que o mapeamento φ *preserva a estrutura algébrica de grupo.*

Exemplo 2.1.6. Seja $\varphi : G \longrightarrow G'$ um homomorfismo de grupo sobrejetivo de G em G'. Queremos mostrar que, se G é abeliano, então G' deve ser abeliano. Isto é, seja $a', b' \in G'$, queremos mostrar que $a'b' = b'a'$. Como φ é sobrejetiva, existe $a, b \in G$ tal que $\varphi(a) = a'$ e $\varphi(b) = b'$. Pela propriedade de homomorfismo, $a'b' = \varphi(a)\varphi(b) = \varphi(ab)$ e, se G é abeliano, $\varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = b'a'$. Segue que G' deve ser abeliano.

Definição 2.1.16 (Imagem)**.** A *imagem* de um homomorfismo $\varphi : G \longrightarrow G'$ é o subconjunto de G'

$$\text{im}\ \varphi = \{x \in G' \mid x = \varphi(a),\ \text{para algum } a \in G\} = \varphi(G).$$

Proposição 2.1.6. *A imagem de um homomorfismo $\varphi : G \longrightarrow G'$ é um subgrupo de G'.*

Definição 2.1.17 (Núcleo)**.** O *núcleo* do homomorfismo $\varphi : G \longrightarrow G'$ é o subconjunto de G formado pelos elementos que são mapeados pela identidade em G':

$$\text{nu}\ \varphi = \{a \in G \mid \varphi(a) = \vec{1}\} = \varphi^{-1}(\vec{1}).$$

Proposição 2.1.7. *O núcleo de um homomorfismo $\varphi : G \longrightarrow G'$ é um subgrupo de G.*

Definição 2.1.18 (Isomorfismo de grupos)**.** Dois grupos $(G, *)$ e $(G', \cdot)$ são ditos *isomorfos* se possuírem um homomorfismo bijetivo entre si, isto é, há um mapeamento *bijetivo* $\varphi : G \longrightarrow G'$ (chamado *relação de isomorfismo*) que respeita a propriedade de homomorfismo:

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \text{ para todo } a, b \in G.$$

Observação 2.1.8. Usa-se a notação $G \approx G'$ para dizer que G é isomorfo a G'.

Definição 2.1.19 (Classe de isomorfismo)**.** Diz-se que o conjunto de grupos isomórfos a um dado grupo G é a *classe de isomorfismo de G*.

Proposição 2.1.8. *Qualquer dois grupos em uma mesma classe de isomorfismo também são isomorfos entre si.*

Definição 2.1.20 (Automorfismo)**.** Quando uma relação de isomorfismo $\varphi : G \longrightarrow G$ é definida de um grupo G para ele mesmo, chamamos esse tipo de isomorfismo de *automorfismo* de G.

Exemplo 2.1.7 (Conjugação)**.** Seja $b \in G$ um elemento fixo. Então, a *conjugação de G por b* (também chamado *automorfismo interno de G por g*) é o mapeamento φ de G para ele mesmo definido por

$$\varphi_b(x) = bxb^{-1}.$$

Esse é um automorfismo porque:

- é compatível com a propriedade de homomorfismo:

$$\varphi_b(xy) = bxyb^{-1} = bx\vec{1}yb^{-1} = bxb^{-1}byb^{-1} = \varphi_b(x)\varphi_b(y);$$

- é um mapa bijetivo visto que existe a função inversa $\varphi_b^{-1}(x) = b^{-1}xb = \varphi_{b^{-1}}(x)$ (isto é, a conjugação por b^{-1}) que, de forma análoga, também é compatível com a propriedade de homomorfismo.

Observação 2.1.9 (Abelianos)**.** Se o grupo é abeliano possui a conjugação trivial: $bab^{-1} = abb^{-1} = a$ (mapa identidade). Porém, qualquer grupo não comutativo tem alguma conjugação não trivial, isto é, existe ao menos um b que não está no centro do grupo, portanto, ao menos o automorfismo não trivial dado pela conjugação do grupo por b existe.

Definição 2.1.21 (Conjugado)**.** O elemento bab^{-1} é chamado *conjugado de a por b*. Dois elementos $a, a' \in G$ são ditos *conjugados* se existe $b \in G$ tal que $a' = bab^{-1}$.

Observação 2.1.10. O conjugado tem uma interpretação muito útil: Se escrevermos bab^{-1} como a', então

$$ba = a'b.$$

Ou seja, pode-se pensar na conjugação como a mudança em a que resulta de mover b de um lado para o outro na equação.

Proposição 2.1.9. *Seja $\varphi : G \longrightarrow G'$ um homomorfismo. Se $a \in \text{nu}\ \varphi$ e b é qualquer elemento do grupo G, então o conjugado $bab^{-1} \in \text{nu}\ \varphi$.*

Definição 2.1.22 (Subgrupo normal)**.** Um subgrupo N de um grupo G é chamado *subgrupo normal* (escreve-se $N \trianglelefteq G$) se para cada $a \in N$ e $b \in G$, o conjugado $bab^{-1} \in N$.

Observação 2.1.11. Fica claro que o núcleo de um homomorfismo é um subgrupo normal. Além disso, todo subgrupo de um grupo abeliano também é um subgrupo normal, porém, isso não é necessariamente verdade em subgrupos de grupos não abelianos (veja Observação 2.1.9).

Proposição 2.1.10. *O centro de todo grupo é um subgrupo normal do grupo.*

Grupos de Permutação

Definição 2.1.23 (Permutação de um conjunto)**.** Uma permutação de um conjunto A é uma função bijetiva $\varphi : A \longrightarrow A$ do conjunto para ele mesmo.

Proposição 2.1.11 (Multiplicação de permutações)**.** *Seja A um conjunto onde duas permutações τ, σ são dadas. A composição de funções $\tau \circ \sigma$ (chamada* multiplicação de permutações*) é uma lei de composição sobre A.*

Proposição 2.1.12. *Sejam A um conjunto não vazio, S_A o conjunto de todas as permutações de A e $\circ$ uma multiplicação de permutações sobre A. Então, $(S_A, \circ)$ é um grupo.*

Definição 2.1.24 (Grupo simétrico sobre n símbolos)**.** Seja A o conjunto finito $\{1, 2, \ldots, n\}$. O grupo de todas as permutações de A é um *grupo simétrico sobre os n símbolos* $1, 2, \ldots, n$ e é representado por S_n.

Observação 2.1.12. É importante perceber que S_n possui $n!$ elementos, isso é, a quantidade de toda combinação de n elementos.

Exemplo 2.1.8 (Grupos diedrais)**.** O grupo S_3 de $3! = 6$ elementos forma um grupo de simetrias de um triangulo equilátero com vértices 1, 2 e 3. As 6 permutações que formam esse grupo são as 3 rotações e os 3 espelhamentos possíveis sobre os vértices do triangulo. Também chamamos S_3 de D_3, pois D_3 forma o terceiro *grupo diedral*. O n-ésimo grupo diedral D_n é o grupo de simetrias de um polígono regular de n vértices.

Definição 2.1.25 (Restrição da imagem de uma função)**.** Sejam $f : A \longrightarrow B$ uma função e H um subconjunto de A. A *imagem de H por f* é $\{f(h) \mid h \in H\}$ e é representada por $f|_H$.

Lema 2.1.1. *Sejam G e G' grupos e $\varphi : G \longrightarrow G'$ um homomorfismo injetivo. Então, $\varphi|_G$ é um subgrupo de G' e φ provê um isomorfismo de G com $\varphi|_G$.*

Teorema 2.1.1 (Teorema de Cayley)**.** *Todo grupo é isomorfo a um grupo de permutações.*

Relações de Equivalência e Partições

Definição 2.1.26 (Partições)**.** Seja S um conjunto. Uma *partição* P de S é uma subdivisão de S em subconjuntos não vazios e não sobrepostos, isto é, uma união de conjuntos disjuntos.

Exemplo 2.1.9. Pode-se particionar o conjunto dos números inteiros $\mathbb{Z}$ na união de disjuntos $P \cup I$, onde $P = \{z \in \mathbb{Z} \mid z \text{ é par}\}$ e $I = \{z \in \mathbb{Z} \mid z \text{ é impar}\}$.

Definição 2.1.27 (Relações de equivalência)**.** Uma *relação de equivalência* sobre um conjunto S é uma relação que se mantém sobre um subconjunto de elementos de S. Escreve-se $a \sim b$ para representar a equivalência de $a, b \in S$, que precisa respeitar os seguintes axiomas:

1. *(Transitiva).* Se $a \sim b$ e $b \sim c$, então $a \sim c$;
2. *(Simétrica).* Se $a \sim b$, então $b \sim a$;
3. *(Reflexiva).* $a \sim a$.

Observação 2.1.13. A noção de partição em S e a relação de equivalência em S são lógicamente equivalentes: Dada uma partição P sobre S, pode-se definir uma relação de equivalência R tal que, se a e b estão no mesmo subconjunto partição, então $a \sim b$ e, dada uma relação de equivalência R, podemos definir uma partição P tal que o subconjunto que contêm a é o conjunto de todos os elementos b onde $a \sim b$. Esse subconjunto é chamado de *classe de equivalência de a*

$$C_a = \{b \in S \mid a \sim b\}$$

e S é particionado em classes de equivalência.

Proposição 2.1.13. *Sejam C_a e C_b duas classes de equivalência do conjunto S. Se existe d tal que $d \in C_a$ e $d \in C_b$, então $C_a = C_b$.*

Observação 2.1.14 (Representante)**.** Seja um conjunto S. Suponha que exista uma relação de equivalência ou uma partição sobre S. Então, pode-se construir um novo conjunto $\bar{S}$ formado pelas classes de equivalência ou os subconjuntos partições de S. Essa construção induz uma notação muito útil: para $a \in S$, a classe de equivalência de a ou o subconjunto partição que contém a serão denotados como o elemento $\bar{a} \in \bar{S}$. Desta forma, a notação $\bar{a} = \bar{b}$ significa que $a \sim b$ e chamamos $a, b \in S$ de *representantes* das respectivas classes de equivalência $\bar{a}, \bar{b} \in \bar{S}$.

Definição 2.1.28 (Equivalência induzida por aplicação)**.** Seja um mapeamento $\varphi : S \longrightarrow T$. Chama-se de *relação de equivalência determinada por φ* a relação dada por $\varphi(a) = \varphi(b) \Rightarrow a \sim b$. Além disso, para um elemento $t \in T$, o subconjunto de $\varphi^{-1}(t) = \{s \in S \mid \varphi(s) = t\}$ é dito *imagem inversa de t por φ*.

Proposição 2.1.14. *Seja um mapeamento $\varphi : S \longrightarrow T$ e $t \in T$ um elemento qualquer de T. Se a imagem inversa $\varphi^{-1}(t)$ é não vazia, então $t \in \text{im } \varphi$ e $\varphi^{-1}(t)$ forma uma classe de equivalência $\bar{\varphi} \in \bar{S}$ através da relação determinada por φ.*

Definição 2.1.29 (Congruência)**.** Seja $\varphi : G \longrightarrow G'$ um homomorfismo. A relação de equivalência definida por φ é usualmente denotada por $\equiv$ ao invés de $\sim$ e a chamamos de *congruência*:

$$\varphi(a) = \varphi(b) \;\Rightarrow\; a \equiv b, \text{ para } a, b \in G.$$

Proposição 2.1.15. *Seja $\varphi : G \longrightarrow G'$ um homomorfismo e $a, b \in G$. Então as seguintes afirmações são equivalentes:*

- $\varphi(a) = \varphi(b)$
- $b = an$, *para algum* $n \in nu\ \varphi$
- $a^{-1}b \in nu\ \varphi$.

Definição 2.1.30 (classe lateral em relação ao núcleo)**.** Seja $\varphi : G \longrightarrow G'$ um homomorfismo, $a \in G$ e $n \in \text{nu } \varphi$. O conjunto

$$a \text{ nu } \varphi = \{g \in G \mid g = an, \text{ para algum } n \in \text{nu } \varphi\}$$

é dito *classe lateral de nu φ em G.*

Observação 2.1.15. Pode-se particionar o grupo G em *classes de congruência*, formadas pelas classes laterais a nu φ. Estas são imagens inversas do mapeamento φ.

Proposição 2.1.16. *O homomorfismo de grupo $\varphi : G \longrightarrow G'$ é injetivo se, e somente se, seu núcleo é o subgrupo trivial $\{\vec{1}\}$.*

Observação 2.1.16. Esse resultado da uma forma de verificar se um homomorfismo φ é também um isomorfismo: Se nu $\varphi = \{1\}$ e im $\varphi = G'$, então φ é, pelos respectivos motivos, injetiva e sobrejetiva. Então é um isomorfismo.

Orbitas, ciclos e grupos alternados

Definição 2.1.31 (Órbita)**.** Seja σ uma permutação de um conjunto A. Chamamos de *órbitas de σ* a classe de equivalência em A determinada pela relação de equivalência $\sim$:

$$\text{para } a, b \in A,\ a \sim b \iff b = \sigma^n(a), \text{ para algum } n \in \mathbb{Z}.$$

Observação 2.1.17. A relação apresentada na Definição 2.1.31 é, de fato, uma relação de equivalência. Como segue:

- é reflexiva, já que $a = \sigma^0(a) \implies a \sim a$;
- é simétrica pois, se $a \sim b \implies \exists\ n \in \mathbb{Z}$ tal que $b = \sigma^n(a)$, então $a = \sigma^{-n}(b)$. Como $-n \in \mathbb{Z}$, então $b \sim a$;

- é transitiva, visto que $a \sim b \implies b = \sigma^n(a)$ e $b \sim c \implies c = \sigma^m(b)$, para algum $n, m \in \mathbb{Z}$, então $c = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a) \implies a \sim c$.

Exemplo 2.1.10 (Órbita trivial)**.** Já que a permutação identidade i de A leva cada elemento de A para a mesma posição, as órbitas de i são os subconjuntos de apenas um elemento de A.

Definição 2.1.32 (Ciclo)**.** Uma permutação $\sigma \in S_n$ é um *ciclo* se possuir no máximo uma órbita contendo mais que um elemento. O *comprimento* de um ciclo é o número de elementos de sua maior órbita.

Exemplo 2.1.11. Seja a permutação

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix}$$

Como a órbita $(1, 3, 6)$ é a única que contém mais de um elemento, essa permutação sobre o conjunto $\{1, 2, 3, 4, 5, 6, 7, 8\}$ é um ciclo de comprimento 3.

Observação 2.1.18 (Notação de ciclos)**.** Podemos representar um ciclo com a notação de uma única linha, da forma

$$\mu = (1, 3, 6),$$

indicando apenas os elementos da maior órbita do ciclo. Perceba que as demais órbitas não precisam ser representadas pois serão os índices fixos da permutação.

Exemplo 2.1.12 (Produto de ciclos)**.** Pode-se construir uma permutação como um multiplicação de ciclos (veja a definição 2.1.11). Por exemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1, 3, 6)(2, 8)(4, 7, 5).$$

Proposição 2.1.17. *Toda permutação σ de um conjunto finito é um produto de ciclos disjuntos.*

Definição 2.1.33 (Transposição)**.** Um ciclo de comprimento 2 é uma transposição.

Corolário 2.1.1. *Qualquer permutação de um conjunto finito de pelo menos dois elementos é um produto de transposições.*

Definição 2.1.34 (Permutações pares e impares)**.** Uma permutação de um conjunto finito é *par* ou *impar* se pode ser expressa, respectivamente, por um número par ou impar de produtos de transposições.

Proposição 2.1.18. *Uma permutação em S_n pode ser expressa como um produto de um número impar de transposições se e somente se não puder ser expressa como um número par de transposições e vice-versa.*

Proposição 2.1.19. *Seja o grupo simétrico S_n com $n \geq 2$. Então, a coleção de todas as permutações impares de $\{1, \ldots, n\}$ forma um subgrupo de S_n de ordem $\frac{n!}{2}$.*

Definição 2.1.35 (Grupo alternado)**.** O subgrupo de S_n formado pelas permutações impares de n símbolos é chamado *grupo alternado* A_n.

Observação 2.1.19. Os grupos S_n e A_n são muito importantes. O teorema de Cayley mostra que todo grupo finito G é estruturalmente idêntico a algum subgrupo de S_n, para $n = |G|$. Pode-se mostrar que não há formulas envolvendo apenas radicais para solucionar uma equação polinomial de grau $n \geq 5$. Por mais que isso não seja óbvio, esse fato se deve, na verdade, a estrutura de A_n.

Classes laterais

Definimos classe lateral somente em relação ao núcleo de um homomorfismo mas, na verdade, pode-se definir uma classe lateral para qualquer subgrupo H de um grupo G.

Definição 2.1.36 (classe lateral a esquerda)**.** Seja um subgrupo H de um grupo G. O subconjunto da forma

$$aH = \{ah \mid h \in H\}$$

é dito *classe lateral a esquerda de H em G.*

Proposição 2.1.20. *A classe lateral é uma classe de equivalência para a relação de congruência*

$$b = ah \Rightarrow a \equiv b, \text{ para algum } h \in H.$$

Observação 2.1.20. Daí segue que, como classes de equivalência particionam um grupo, classes laterais a esquerda de um subgrupo particionam o grupo.

Definição 2.1.37 (Índice de um subgrupo)**.** O número de classes laterais a esquerda de um subgrupo H em um grupo G chama-se *índice de H em G* e é denotado como $[G : H]$.

Observação 2.1.21. Como há uma bijeção do subgrupo H para a classe lateral aH, a cardinalidade de aH tem de ser a mesma de H. Isto é, as classes laterais de H particionam G em partes de mesma ordem.

Proposição 2.1.21. *Seja aH a classe lateral do subgrupo H no grupo G. Então, a ordem $|G|$ do grupo G é dada por*

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

Proposição 2.1.22 (Teorema de Lagrange)**.** *Seja G um grupo finito e H um subgrupo de G. A ordem de H divide a ordem de G.*

Definição 2.1.38 (Ordem de um elemento)**.** Seja G um grupo. A *ordem de um elemento $a \in G$* é a ordem do grupo cíclico gerado por a.

Proposição 2.1.23. *Seja um grupo G com p elementos tal que p é primo e $a \in G$ diferente da identidade. Então G é o grupo cíclico $\{1, a, \ldots, a^{p-1}\}$ gerado por a.*

Observação 2.1.22. Também podemos obter uma expressão para calcular a ordem de um grupo de homomorfismo. Seja $\varphi : G \longrightarrow G'$ um homomorfismo. Como as classes laterais a esquerda do núcleo de φ são as imagens inversas φ^{-1}, elas estão em uma correspondência biunívoca com a imagem. Daí segue que

$$[G : \text{ nu } \varphi\ ] = |\text{ im } \varphi\ |.$$

Proposição 2.1.24. *Seja $\varphi : G \longrightarrow G'$ um homomorfismo onde G e G' são finitos. Então*
$$|G| = |\ nu\ \varphi\ | \cdot |\ im\ \varphi\ |.$$

Definição 2.1.39 (classes laterais a direita)**.** Os conjuntos da forma

$$Ha = \{ha \mid h \in H\}$$

chamam-se *classes laterais a direita de um subgrupo H*. Esses são classes de equivalência para a relação de congruência a direita

$$b = ha \Rightarrow a \equiv b, \text{ para algum } h \in H.$$

Proposição 2.1.25. *Seja um subgrupo H de um grupo G. As seguintes afirmações são equivalentes:*

- *H é subgrupo normal,*
- *$aH = Ha$ para todo $a \in G$.*

Restrição de um homomorfismo para um subgrupo

Observação 2.1.23. O objetivo dessa seção é apresentar ferramentas para analisar um subgrupo H do grupo G a fim de garantir propriedades do grupo G. No geral, os subgrupos são mais específicos e menos complexos de se trabalhar.

Proposição 2.1.26. *Sejam K e H dois subgrupos do grupo G tal que a interseção $K \cap H$ é um subgrupo de H. Se K é um subgrupo normal de G, então $K \cap H$ é um subgrupo normal de H.*

Exemplo 2.1.13. Com esse resultado, se G é finito pode-se utilizar o Teorema de Lagrange para obter informações sobre a interseção dos dois subgrupos: a interseção divide $|H|$ e $|K|$. Se $|H|$ e $|K|$ não tem o mesmo fator de divisão, então $K \cap H = \{1\}$.

Definição 2.1.40 (Restrição de um homomorfismo para um subgrupo)**.** Sejam o homomorfismo $\varphi : G \longrightarrow G'$ e H um subgrupo de G. Uma *restrição de φ para o subgrupo H* é o homomorfismo $\varphi|_H : H \longrightarrow G'$ definido como

$$\varphi|_H(h) = \varphi(h), \text{ para todo } h \in H.$$

Proposição 2.1.27. *Sejam o homomorfismo $\varphi : G \longrightarrow G'$ e H um subgrupo de G. O núcleo de uma restrição $\varphi|_H$ é a interseção do núcleo de φ e H.*

Proposição 2.1.28. *Sejam $\varphi : G \longrightarrow G'$ um homomorfismo, H' um subgrupo de G' e $\varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}$ a imagem inversa de H'. Então*

- *$\varphi^{-1}(H')$ é um subgrupo de G.*
- *Se H' é um subgrupo normal de G', então $\varphi^{-1}(H')$ é um subgrupo normal de G.*
- *$\varphi^{-1}(H')$ contém o núcleo de φ*
- *A restrição de φ para $\varphi^{-1}(H')$ define um homomorfismo $\varphi^{-1}(H') \longrightarrow H'$, de forma que o núcleo desse homomorfismo é o núcleo de φ.*

Produto de Grupos

Definição 2.1.41 (Produto de grupos)**.** Seja G, G' dois grupos. O *produto* $G \times G'$ é um grupo formado pelo produto das componentes dos grupos G e G', isso é, pela regra

$$(a, a'), (b, b') \mapsto (ab, a'b'),$$

onde $a, b \in G$ e $a', b' \in G'$. O par $(1, 1)$ é uma identidade e $(a, a')^{-1} = (a^{-1}, a'^{-1})$. A propriedade associativa é preservada em $G \times G'$ pois também é em G e G'.

Proposição 2.1.29. *A ordem de $G \times G'$ é o produto das ordens de G e G'.*

Observação 2.1.24 (Projeções)**.** O produto de grupos é composto pelos homomorfismos:

$$i : G \longrightarrow G \times G', \quad i' : G' \longrightarrow G \times G', \quad p : G \times G' \longrightarrow G, \quad p' : G \times G' \longrightarrow G',$$

definidos como

$$i(x) = (x, 1), \quad i'(x') = (1, x'), \quad p(x, x') = x, \quad , p'(x, x') = x'.$$

Os mapeamentos i, i' são injetivos, já os mapeamentos p, p' são sobrejetivos, onde nu $p = 1 \times G'$ e nu $p' = G \times 1$. Esses mapeamentos são chamados de *projeções*. Já que são núcleos, $G \times 1$ e $1 \times G'$ são subgrupos normais de $G \times G'$.

Proposição 2.1.30 (Propriedades de Mapeamento dos Produtos)**.** *Seja H um grupo qualquer. O homomorfismo $\Phi : H \longrightarrow G \times G'$ tem correspondência biunívoca com o par $\Phi(h) = (\varphi(h), \varphi'(h))$ de homomorfismos*

$$\varphi : H \longrightarrow G, \quad \varphi' : H \longrightarrow G'.$$

O núcleo de Φ é a interseção $(nu\ \varphi) \cap (\ nu\ \varphi')$.

Observação 2.1.25. É extremamente desejável encontrar uma relação isomorfa entre um grupo G e um produto de outros dois grupos $H \times H'$. Quando isso acontece, e infelizmente não são muitas as vezes, trabalhar com os grupos H e H' costumam ser mais simples que G.

Proposição 2.1.31. *Sejam $r, s \in \mathbb{Z}$ não divisíveis entre si. Um grupo cíclico de ordem rs é isomorfo ao produto dos grupos cíclicos de ordem r e s.*

Observação 2.1.26. Em contrapartida, um grupo cíclico de ordem par 4, por exemplo, não é isomorfo ao produto de dois grupos cíclicos de ordem 2. Também não podemos afirmar nada com base no resultado anterior sobre grupos não cíclicos.

Definição 2.1.42 (Conjunto de produtos)**.** Sejam dois subgrupos A, B de um grupo G. Chamamos o *conjunto de produtos de elementos de A e B* por

$$AB = \{x \in G \mid x = ab \text{ para algum } a \in A \text{ e } b \in B\}.$$

Proposição 2.1.32. *Sejam H e K subgrupos de um grupo G.*

- *Se $H \cap K = \{1\}$, o mapeamento de produto $p : H \times K \longrightarrow G$ definido por $p(h, k) = hk$ é injetivo e sua imagem é o subconjunto HK;*
- *Se um dos subgrupos H ou K é um subgrupo normal de G, então os conjuntos de produtos HK e KH são iguais e HK é subgrupo de G;*
- *Se ambos H e K são subgrupos normais, $H \cap K = \{1\}$ e $HK = G$, então G é isomorfo ao grupo de produto $H \times K$.*

Aritmética Modular

Definição 2.1.43 (Congruente modulo n)**.** Seja $n \in \mathbb{N}$. Dizemos que dois inteiros a, b são *congruentes modulo* n, e escrevemos

$$a \equiv b \pmod{n},$$

se n divide $b - a$, ou se $b = a + nk$ para algum inteiro k. Chamamos as classes de equivalência definidas por essa relação de *classes de equivalência módulo* n, ou *classes de resíduo módulo* n.

Exemplo 2.1.14. A classe de congruência de 0 é o subgrupo $\bar{0}$ de todos os múltiplos de n

$$\bar{0} = n\mathbb{Z} = \{\dots, -n, 0, n, 2n, \dots\}.$$

Proposição 2.1.33. *Há n classes de congruência módulo n (denotamos esse conjunto por $\mathbb{Z}/n\mathbb{Z}$), isto é, o índice $[\mathbb{Z} : n\mathbb{Z}]$ é n. São elas*

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Definição 2.1.44 (Soma e produto)**.** Seja $\bar{a}$ e $\bar{b}$ as classes de congruência representadas pelos inteiros a e b. Define-se a *soma* como a classe de congruência de $a + b$ e o *produto* pela classe de congruência ab, isto é,

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{e} \quad \bar{a}\bar{b} = \overline{ab}.$$

Proposição 2.1.34. *Se $a' \equiv b'$ $(mod\ n)$ e $a \equiv b$ $(mod\ n)$, então $a' + b' \equiv a + b$ $(mod\ n)$ e $a'b' \equiv ab$ $(mod\ n)$.*

Observação 2.1.27. Além disso, a soma e produto também continuam respeitando as propriedades associativas, comutativas e distributivas, desde que o mesmo se mantém para soma e multiplicação de inteiros.

Exemplo 2.1.15. Seja $n = 13$, então

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{12}\}.$$

Com isso,

$$(\bar{7} + \bar{9})(1\bar{1} + \bar{6}) \;=\; \bar{3} \cdot \bar{4} \;=\; 1\bar{2}.$$

Estrutura de grupos abelianos finitamente gerados

Teorema 2.1.2 (Teorema fundamental dos grupos abelianos finitamente gerados)**.** *Todo grupo abeliano finitamente gerado G é isomorfo a um produto de grupos cíclicos na forma*

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

onde os p_i são primos, não necessariamente distintos, os r_i são inteiros positivos e o conjunto $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. O produto é único, exceto por possíveis rearranjos dos fatores; isso é, o número (chamado número Betti *de G) de fatores $\mathbb{Z}$ é único e as potências de primos $(p_i)^{r_i}$ são únicas.*

Exemplo 2.1.16. Queremos encontrar todos os grupos abelianos de ordem 360, *a menos de isomorfismos*. Dizer *a menos de isomorfismo* significa que qualquer grupo abeliano de ordem 360 deve ser estruturalmente idêntico — isto é, isomorfo — a algum presente no conjunto solução.

Solução. Já qe nossos grupos são da ordem finita 360, não aparecerão $\mathbb{Z}$ no produto. Primeiro, vamos expressar 360 como um produto de potências de primos: $360 = 2^3 3^2 5$. Então, pelo Teorema 2.1.2, temos as seguintes possibilidades

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
2. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
4. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
5. $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
6. $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Então, esses são os seis diferentes grupos abelianos (a menos de isomorfismos) de ordem 360. △

Definição 2.1.45 (Grupo decomponível e indecomponível)**.** Um grupo é dito *decomponível* se ele é isomorfo a um produto direto de dois subgrupos não triviais. Do contrário, é dito *indecomponível.*

Proposição 2.1.35. *Os grupos abelianos finitos indecomponível são exatamente os grupos cíclicos que possuem a ordem de uma potência prima.*

Proposição 2.1.36. *Se m divide a ordem de um grupo abeliano finito G, então G tem um subgrupo de ordem m.*

Proposição 2.1.37. *Se m é um* quadrado inteiro livre*, isto é, m não é divisível por nenhum quadrado de primo, então todo grupo abeliano de ordem m é cíclico.*

Grupos Quociente

Definição 2.1.46 (Produto de classes laterais)**.** Sejam $N \trianglelefteq G$ e as classes laterais $\bar{a} = aN$ e $\bar{b} = bN$, para $a, b \in G$. Chamamos de *produto das classes laterais $\bar{a}$ e $\bar{b}$* a classe lateral $\bar{a}\bar{b} = abN$, isto é, a classe lateral que contém ab.

Proposição 2.1.38. *Sejam G um grupo e S um conjunto qualquer com uma lei de composição. Seja também $\varphi : G \longrightarrow S$ um mapeamento sobrejetivo tal que $\varphi(a)\varphi(b) = \varphi(ab)$ para todo a, $b \in G$. Então S é um grupo.*

Definição 2.1.47 (Operação induzida por bijeção)**.** Seja um grupo G e um conjunto S com a mesma cardinalidade de G. Por conta disso, há uma correspondência injetiva $\leftrightarrow$ entre S e G. Podemos definir uma *operação binária sobre S induzida pela relação com os elementos de G*, da forma

$$\text{se } x \leftrightarrow g_1,\ y \leftrightarrow g_2 \text{ e } z \leftrightarrow g_1 g_2 \text{ então } xy = z,$$

onde $x, y, z \in S$ e $g_1 g_2 \in G$. Também, a direção $\to$ da correspondência biunívoca $s \leftrightarrow g$ define uma função bijetiva $\mho : S \longrightarrow G$, isto é

$$\text{se } \mho(x) = g_1,\ \mho(y) = g_2 \text{ e } \mho(z) = g_1 g_2 \text{ então } xy = z.$$

Assim, como $\mho(xy) = \mho(z) = g_1 g_2 = \mho(x)\mho(y)$, a Proposição 2.1.38 garante que S é um grupo e, além disso, $\mho$ representa um isomorfismo que mapeia o grupo S no grupo G.

Teorema 2.1.3 (Grupo quociente). *Seja $\phi : G \longrightarrow G'$ um homomorfismo de grupos com núcleo H. O conjunto de todas as classes laterais de H formam o chamado* grupo de quociente *G/H (lê-se G sobre H, não confundir com G dividido por H), onde $(aH)(bH) = (ab)H$, para todo $a, b \in G$. Também, o mapa $\mho : G/H \longrightarrow \phi[G]$ definido por $\mho(aH) = \phi(a)$ é um isomorfismo. Tanto a multiplicação de classes laterais como $\mho$ estão bem definidos, isto é, independem das escolhas de a e b.*

Proposição 2.1.39. *Seja H um subgrupo de um grupo G. Então, a multiplicação da classe lateral a esquerda é bem definida pela equação*

$$(aH)(bH) = (ab)H$$

se e somente se H é um subgrupo normal de G.

Corolário 2.1.2. *Se $N \trianglelefteq G$, então as classes laterais de N formam um grupo G/N sobre a operação binária $(aN)(bN) = (ab)N$.*

Definição 2.1.48 (Grupo quociente). O grupo G/H no corolário 2.1.2 se chama *grupo quociente* (ou, *grupo fator*) de G por H.

Exemplo 2.1.17. Como $\mathbb{Z}$ é um grupo abeliano, $n\mathbb{Z}$ é um subgrupo normal. O corolário 2.1.2 permite a construção do grupo quociente $\mathbb{Z}/n\mathbb{Z}$ sem citar um homomorfismo.

Proposição 2.1.40 (Homomorfismo induzido por grupo quociente). *Seja $H \trianglelefteq G$. Então $\gamma : G \longrightarrow G/H$ dado por $\gamma(x) = xH$ é um homomorfismo com núcleo H.*

Corolário 2.1.3. *Todo subgrupo normal de um grupo G é o núcleo de um homomorfismo.*

Teorema 2.1.4 (Teorema fundamental do homomorfismo). *Seja $\phi : G \longrightarrow G'$ um homomorfismo de grupo com núcleo H. Então $\phi[G]$ é um grupo e $\mu : G/H \longrightarrow \phi[G]$ dado por $\mu(gH) = \phi(g)$ é um isomorfismo. Se $\gamma : G \longrightarrow G/H$ é o homomorfismo dado por $\gamma(g) = gH$, então $\phi(g) = \mu\gamma(g)$ para cada $g \in G$.*

2.1.4 Anéis e Corpos

Definição 2.1.49 (Anel). Um *anel* $(R, +, \cdot)$ é um conjunto R acompanhado de duas operações binárias $+$ e $\cdot$ definidas sobre R tais que os seguintes axiomas são satisfeitos:

1. $(R, +)$ é um grupo abeliano.

2. A operação $\cdot$ é associativa.

3. Para todo $a, b, c \in R$ vale a *lei da distributividade à esquerda* e a *lei de distributividade à direita*, respectivamente,

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

Exemplo 2.1.18. Todo subconjunto dos números complexos que é fechado para a adição e multiplicação usual dos complexos é um anel. Por exemplo, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são todos anéis. Outro exemplo interessante é de um anel contendo apenas o elemento 0. Chamamos esse de *anel trivial*.

Observação 2.1.28 (Notação)**.** Da mesma forma que com os grupos, costuma-se denotar o anel $(R, +, \cdot)$ apenas por seu conjunto R. Também, para um anel $(R, +, \cdot)$, chama-se sua primeira operação + de *adição do anel* e sua segunda operação $\cdot$ de *multiplicação do anel*. O grupo $(R, +)$ é chamado *grupo aditivo de R*.

Proposição 2.1.41. *Se R é um anel com identidade aditiva $\vec{0}$, então, $\forall a \in R$,*

$$\vec{0} \cdot a = a \cdot \vec{0} = \vec{0}.$$

Demonstração. Pelas propriedades do grupo $(R, +)$,

$$a\vec{0} + a\vec{0} = a(\vec{0} + \vec{0}) = a\vec{0} = \vec{0} + a\vec{0}.$$

E, pela lei de cancelamento do grupo,

$$a\vec{0} + a\vec{0} = \vec{0} + a\vec{0} \implies a\vec{0} = \vec{0}.$$

De forma semelhante,

$$\vec{0}a + \vec{0}a = (\vec{0} + \vec{0})a = \vec{0}a = \vec{0} + \vec{0}a \implies \vec{0}a = \vec{0}.$$

Daí, segue que $a\vec{0} = \vec{0}a = \vec{0}$. □

Proposição 2.1.42. *Se R é um anel, então, para todo $a, b \in R$ vale*

- $a(-b) = (-a)b = -(ab)$ *e*
- $(-a)(-b) = ab$.

Definição 2.1.50 (Anel associativo)**.**

Definição 2.1.51 (Anel comutativo)**.**

Definição 2.1.52 (Anel com identidade)**.**

Definição 2.1.53 (subanel)**.** Um subconjunto S de um anel R é um subanel de R (escreve-se $S \leq R$) se, e somente se, valem os seguintes axiomas:

1. *(Existência do elemento nulo).* $0 \in S$;
2. *(Subtração fechada).* $a - b \in S$, para todo $a, b \in S$;
3. *(Produto fechado).* $ab \in S$, para todo $a, b \in S$.

Proposição 2.1.43. *Seja $(S, +, \cdot)$ um subanel de $(R, +, \cdot)$. Então $(S, +, \cdot)$ é um anel.*

Definição 2.1.54 (Divisor de zero)**.** pag 2 hazenwinkel;

Definição 2.1.55 (Domínio de integridade)**.** Um anel R é chamado *domínio de integridade* se $ab \neq 0$ para todo elemento não-nulo $a, b \in R$. Isto é, se R não possuir divisores de zero.

Definição 2.1.56 (Unidade)**.**

Proposição 2.1.44 (Grupo multiplicativo)**.** *O conjunto das unidades R^* de um anel R formam um grupo com respeito a multiplicação. Chamamos $(R^*, \cdot)$ de* grupo multiplicativo*.*

Definição 2.1.57 (Elemento idempotente)**.** Um elemento e de um anel R é chamado *idempotente* se $e^2 = e$. Além disso, dois elementos idempotentes e, f são ditos *ortogonais* se $ef = fe = 0$.

Exemplo 2.1.19. Seja um anel R com identidade. Então $0, 1 \in R$ são elementos idempotentes e ortogonais.

Definição 2.1.58 (Anel de divisão)**.** Um *anel de divisão D* é um anel não trivial onde todos os elementos não-nulos de D formam um grupo sobre a multiplicação.

Proposição 2.1.45. *Um anel não trivial D é anel de divisão se, e somente se, todo elemento não-nulo de D é uma unidade.*

Homomorfismos de anéis

Definição 2.1.59 (Homomorfismo de anéis)**.** Sejam dois anéis $(R, +, \cdot)$ e $(R', +', \cdot')$. Um mapa $\phi : R \longrightarrow R'$ é um *homomorfismo* se a *propriedade de homomorfismo* vale para ambas as operações, isso é, se, para todo $a, b \in R$,

$$\phi(a + b) = \phi(a) +' \phi(b) \quad \text{e} \quad \phi(a \cdot b) = \phi(a) \cdot' \phi(b).$$

Exemplo 2.1.20 (Homomorfismo trivial)**.** Sejam os anéis R, R' e o elemento neutro $\vec{0}$ da adição do anel R'. A aplicação $\phi : R \longrightarrow R'$ definida por $\phi(a) = \vec{0}$, para todo $a \in R$, é um homomorfismo de anéis porque

$$\phi(a + b) = \vec{0} = \vec{0} \ +' \vec{0} = f(a) +' f(b) \quad \text{e} \quad f(a \cdot b) = \vec{0} = \vec{0} \ \cdot' \vec{0} = f(a) \ \cdot' f(b).$$

A essa aplicação dá-se o nome *homomorfismo trivial de anéis.*

Definição 2.1.60 (Homomorfismo injetivo e sobrejetivo)**.** Chama-se de *homomorfismo injetivo* e *homomorfismo sobrejetivo* um homomorfismo de anéis definido, respectivamente, por uma função injetiva ou uma função sobrejetiva.

Exemplo 2.1.21. Seja o homomorfismo de anéis $\phi : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ tal que $\phi(n) = (n, 0)$, para todo $n \in \mathbb{Z}$. Perceba que, para cada $(n, 0) \in \mathbb{Z} \times \mathbb{Z}$ tem-se um único $n \in \mathbb{Z}$ tal que $\phi(n) = (n, 0)$, daí, ϕ é injetiva e esse é um homomorfismo injetivo. Também, seja $\mu : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ o homomorfismo tal que $\mu(n, m) = n$ para todo $(n, m) \in \mathbb{Z} \times \mathbb{Z}$. É fácil perceber que para todo $z \in \mathbb{Z}$, existirá $(z, 0) \in \mathbb{Z} \times \mathbb{Z}$, donde μ é um homomorfismo sobrejetivo.

Proposição 2.1.46. *Se $\phi : R \longrightarrow R'$ é um homomorfismo de anéis, então, para todo $a, b \in A$,*

- $\phi(0_R) = 0_{R'}$,
- $\phi(-a) = -\phi(a)$ *e*
- $\phi(a-b) = \phi(a) - \phi(b)$.

Demonstração. Como $\phi(a) = \phi(a + 0_R) = \phi(a) + \phi(0_R)$, pela propriedade de homomorfismo, então,

$$\phi(a) = \phi(a) + \phi(0_R) \implies -\phi(a) + \phi(a) = -\phi(a) + \phi(a) + \phi(0_R),$$

isto é, $0_{R'} = \phi(0_R)$.

Daí segue que,

$$0_{R'} = \phi(0_R) = \phi(a-a) = \phi(a) + \phi(-a),$$

e como $0_{R'} = \phi(a) + \phi(-a)$,

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

Fica evidente que

$$\phi(a-b) = \phi(a) + \phi(-b) = \phi(a) - \phi(b).$$

□

Proposição 2.1.47. *Seja $\phi : R \longleftarrow R'$ um homomorfismo de anéis onde $1_R \in R$ é identidade do produto de R. Então*

- *R' possui identidade multiplicativa $1_{R'}$ e $\phi(1_R) = 1_{R'}$;*
- *se $a \in R$ possui inversa multiplicativa a^{-1}, então $\phi(a)^{-1} = \phi(a^{-1})$.*

Definição 2.1.61 (Imagem de homomorfismo de anéis)**.** A *imagem* de um homomorfismo de anéis $\phi : R \longrightarrow R'$ é o subconjunto de R'

$$\text{im } \phi = \{x \in R' \mid x = \phi(a), \text{ para algum } a \in R\} = \phi(R).$$

Proposição 2.1.48. *Seja um homomorfismo de anéis $\phi : R \longrightarrow R'$, então a imagem $\phi(R) \leq R'$ e, além disso, se $S \leq R$ então $\phi(S) \leq R'$.*

Demonstração. Como S é um subanel de R, então $0_R \in S$ e $\phi(0_R) = 0_{R'}$ implica que $0_{R'} \in \phi(S)$. Além disso, sejam $a, b \in \phi(S)$, então existem $s_1, s_2 \in S$ tais que $\phi(s_1) = a$, $\phi(s_2) = b$ e, como S é anel, $s_1 - s_2 \in S$ e segue que $\phi(s_1 - s_2) \in \phi(S)$. Como $\phi(s_1 - s_2) = \phi(s_1) - \phi(s_2) = a - b$, $a - b \in \phi(S)$. De forma semelhante para o produto, $a, b \in \phi(S) \implies s_1 s_2 \in S \implies ab \in \phi(S)$. □

Proposição 2.1.49. *Sejam $\phi : R \longrightarrow T$ e $\mu : T \longrightarrow R'$ homomorfismos de anéis. Então, $\mu \circ \phi : R \longrightarrow R'$ também é um homomorfismo de anéis.*

Demonstração. Sejam $a, b \in R$. Como ϕ é homomorfismo, segue que

$$\phi(a+b) = \phi(a) + \phi(b) \text{ e } \phi(ab) = \phi(a)\phi(b).$$

Portanto, aplicando μ,

$$\mu \circ \phi(a+b) = \mu(\phi(a) + \phi(b)) \text{ e } \mu \circ \phi(ab) = \mu(\phi(a)\phi(b)),$$

Mas como μ também respeita a propriedade de homomorfismo, segue que

$$\mu(\phi(a)+\phi(b)) = \mu(\phi(a)) + \mu(\phi(b)) = \mu\circ\phi(a) + \mu\circ\phi(b) \text{ e}$$

$$\mu(\phi(a)\phi(b)) = \mu(\phi(a))\mu(\phi(b)) = \mu\circ\phi(a)\mu\circ\phi(b).$$

□

Definição 2.1.62 (Núcleo)**.** O *núcleo* do homomorfismo de anéis $\phi : R \longrightarrow R'$ é o subconjunto de R formado pelos elementos que são mapeados pelo elemento nulo em R':

$$\text{nu}\ \phi = \{a \in R \mid \phi(a) = 0\}.$$

Exemplo 2.1.22. Seja $\phi : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $\phi(a,b) = a$. Então ϕ é um homomorfismo de anéis e

$$\text{nu}\ \phi = \{(a,b) \in \mathbb{Z}\times\mathbb{Z} \mid a = 0\}.$$

Proposição 2.1.50. *Seja um homomorfismo $\phi : R \longrightarrow R'$ com núcleo* nu ϕ *e seja 0_R o elemento nulo de R. Então $0_R \in$* nu ϕ.

Proposição 2.1.51. *Seja $\phi : R \longrightarrow R'$ um homomorfismo de anéis. Então*

- *nu $\phi \le R$;*
- *ϕ é injetor se, e somente se, nu $\phi = \{0_R\}$.*

Definição 2.1.63 (Isomorfismo de anéis)**.**

Corpos

Definição 2.1.64 (Corpo)**.** Um *corpo* $(F,+,\cdot)$ é um anel de divisão comutativo.

Exemplo 2.1.23. $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos clássicos de corpos sobre suas respectivas adições e multiplicações usuais. Note que $\mathbb{Z}$ não é corpo, visto que suas únicas unidades são 1 e -1. No entanto, $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ é o menor corpo possível (a menos de isomorfismos).

Proposição 2.1.52. *Todo domínio de integridade finito é um corpo.*

Proposição 2.1.53. *Em um corpo $(F,+,\cdot)$, $(F\setminus\{0\},\cdot)$ é um grupo abeliano.*

Definição 2.1.65 (Subcorpo)**.** Seja um corpo F. Um corpo $K \le F$ é dito *subcorpo* de F e F é dito *extensão* de K.

Definição 2.1.66 (Elemento algébrico e transcendente)**.** Sejam um corpo K e sua extensão F. Um elemento α de F é dito *algébrico sobre* K se existe algum polinômio não-nulo $f(x) \in K[x]$ tal que $f(\alpha) = 0$. Se $\alpha \in F$ não é algébrico sobre K, então α é *transcendente sobre* K.

Definição 2.1.67 (Extensão algébrica)**.** Um corpo de extensão E de um corpo F é uma *extensão algébrica de* F se todo elemento em E é algébrico sobre F.

2.1.5 Módulos, Espaços Vetoriais e Álgebras

Definição 2.1.68 (Módulo)**.** Seja $(R, +, \cdot)$ um anel. Um grupo abeliano $(M, \oplus)$ é chamado de *módulo sobre um anel R* (ou, simplesmente R-módulo) se existir uma aplicação

$$\begin{array}{ccc} R \times M & \longrightarrow & M \\ (r, m) & \mapsto & rm \end{array},$$

chamada *multiplicação por escalar*, tal que para todo $r, r' \in R$ e $m, m' \in M$ valham

1. $0_R m = 0_M$;
2. se R tem identidade 1, então $1m = m$;
3. $(r + r')m = (rm) \oplus (r'm)$;
4. $r(m \oplus m') = (rm) \oplus (rm')$;
5. $(r \cdot r')m = r(r'm)$.

Observação 2.1.29 (Notação)**.** Na falta de ambiguidades, costuma-se usar 0 para se referir tanto a identidade aditiva 0_R de R quanto a 0_M de M. De forma semelhante, usa-se o simbolo de adição + tanto para $\oplus$ de M quanto + de R.

Exemplo 2.1.24 ($\mathbb{Z}$-módulo)**.** Seja o anel $(\mathbb{Z}, +, \cdot)$. Podemos fazer qualquer grupo abeliano $(A, +)$ virar um $\mathbb{Z}$-módulo através do seguinte produto escalar: para $n \in \mathbb{Z}$ e $a \in A$,

$$na = \begin{cases} a + a + \cdots + a \quad (n \text{ vezes}), & \text{se } n > 0 \\ 0, & \text{se } n = 0 \\ -a - a - \cdots - a \quad (-n \text{ vezes}), & \text{se } n < 0 \end{cases}.$$

Proposição 2.1.54. *Seja M um grupo. M é um $\mathbb{Z}$-módulo se, e somente se, M é um grupo abeliano.*

Definição 2.1.69 (Submódulo)**.** Sejam R um anel e M um R-módulo. Um *R-submódulo* de M é um subgrupo N de M que é fechado sob a ação dos elementos do anel, i.e., para todo $r \in R$ e $n \in N$, $rn \in N$.

Proposição 2.1.55 (Critério de submódulo)**.** *Sejam R um anel e M um R-módulo. Um subconjunto N de M é um submódulo de M se, e somente se,*

1. *$N \neq \varnothing$;*
2. *para todo $r \in R$ e $x, y \in N$, $x + ry \in N$.*

Definição 2.1.70 (Produto direto)**.** Seja $M_1, \ldots, M_k$ uma coleção de R-módulos. A coleção de k-tuplas $(m_1, m_2, \ldots, m_k)$, onde $m_i \in M_i$, com adição e ação de R definidos componente a componente, é chamado de *produto direto de* $M_1, \ldots, M_k$ e é denotado por $M_1 \times \cdots \times M_k$.

Definição 2.1.71 (Módulo livre, base e grau)**.** Um R-módulo L é dito *livre* no subconjunto A de L se, para todo elemento não-nulo $x \in L$, existirem únicos elementos não-nulos $r_1, r_2, \ldots, r_n \in R$ e únicos $a_1, a_2, \ldots, a_n \in A$ tais que

$$x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n, \text{ para algum } n \in \mathbb{Z}^+.$$

Nesse caso, dizemos que A é uma *base* ou *conjunto de geradores livres* para L. Se R é um anel comutativo, a cardinalidade de A é chamada de *grau* de L.

Álgebras

Definição 2.1.72 (R-álgebra)**.** Seja R um anel comutativo com identidade. Uma *R-álgebra* é um anel A com identidade onde existe um homomorfismo $f : R \longrightarrow A$ levando 1_R para 1_A, tal que o subanel $f(R) \leq A$ está contido no centro de A.

Exemplo 2.1.25. Todo anel A com identidade é uma $\mathbb{Z}$-álgebra.

Proposição 2.1.56. *Se o anel $(A, +, \cdot)$ é uma R-álgebra pelo homomorfismo $f : R \longrightarrow A$, então A tem um R-módulo através da multiplicação por escalar induzida por f, i.e., $r \cdot a = a \cdot r = f(r)a$, onde $r \in R$ e $a \in A$.*

Proposição 2.1.57. *Sejam R um anel comutativo com identidade e $(A, +, \cdot)$ um anel com identidade. Então, A é uma R-álgebra se e somente se A é um R-módulo satisfazendo*

$$r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$$

para todo $r \in R$ e $a, b \in A$.

Espaços Vetoriais

Definição 2.1.73 (Espaço vetorial)**.** Seja o grupo abeliano E um K-módulo. Se K é um corpo, dizemos que E é um *espaço vetorial sobre o corpo K*. Também, passamos a nos referenciar aos elementos de K por *escalares* e aos de E por *vetores*.

Exemplo 2.1.26 (n-espaço afim sobre um corpo)**.** Sejam K um corpo e $n \in \mathbb{Z}^+$ um inteiro positivo. Seja o conjunto

$$K^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in K, \text{ para todo } 1 \leq i \leq n\}.$$

Tornamos K^n em um espaço vetorial ao definirmos sua adição e uma multiplicação escalar componente a componente, como segue:

$$\begin{aligned} (a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) &= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \\ \alpha(a_1, \ldots, a_n) &= (\alpha a_1, \ldots, \alpha a_n), \qquad \alpha \in K. \end{aligned}$$

Chamamos K^n de *n-espaço afim sobre K*. Por exemplo, chamamos o n-espaço afim $\mathbb{R}^n$ sobre $\mathbb{R}$ de *n-espaço Euclidiano*, que é um espaço vetorial sobre K.

Definição 2.1.74 (Subespaço)**.** Um submódulo de um espaço vetorial é chamado de *subespaço*.

Definição 2.1.75 (Independência linear)**.** Seja V um espaço vetorial sobre K. Um subconjunto S de V é chamado de conjunto de *vetores linearmente independentes* se uma equação

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

com $\alpha_i \in K$ e $v_i \in S$, para todo $1 \leq i \leq n$, implicar que

$$\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0.$$

Um conjunto ordenado de vetores linearmente independentes que geram V formam uma *base* do espaço vetorial V.

Proposição 2.1.58. *Qualquer espaço vetorial sobre K finitamente gerado é um K-módulo livre.*

Definição 2.1.76 (Dimensão)**.** Seja E um espaço vetorial. Se E é um K-módulo livre em um subconjunto $A \subset E$, então o grau de E é chamado de *dimensão de E*. Senão, diz-se que E tem dimensão infinita.

Definição 2.1.77 (Extensão finita)**.** Se um corpo de extensão E de um corpo F é de dimensão finita n como um espaço vetorial sobre F, então E é uma *extensão finita de grau n sobre F*. Denotaremos por $[E : F]$ o grau n de E sobre F.

Proposição 2.1.59. *Se o grau de uma extensão $[E : F]$ é n, então para qualquer elemento $a \in E$, os elementos $1, \alpha, \ldots, \alpha^n$ são linearmente dependentes sobre F e, portanto, α é uma raiz de algum polinômio $f(x) \in F[x]$.*

Proposição 2.1.60. *Um corpo de extensão finito E sobre um corpo F é uma extensão algébrica de F.*

Proposição 2.1.61. *Se E é um corpo de extensão finito de um corpo F e K é um corpo de extensão finito de E, então K é um corpo de extensão finita de F e*

$$[K : F] = [K : E][E : F].$$

2.2 Álgebra Geométrica

Neste capitulo iremos introduzir o estudo da *Álgebra Geométrica* — nome definido por William Kingdon Clifford (1845-1879), o que eventualmente fez com que essa área também fosse chamada de Álgebra de Clifford [1]. Para isso, começaremos com alguns conceitos da *Teoria da Expansão* (ou, em alemão, *Ausdehnungslehre* [2]), introduzidos por Hermann Günther Grassmann (1809-1877), precursor do que hoje entendemos como a Álgebra Linear.

> *"Until recently I was unacquainted with the Ausdehnungsleh, and knew only so much of it as is contained in the author's geometrical papers (...). I may, perhaps, therefore be permitted to express miy profound admiration of that extraordinary work, and my conviction that its principles will exercise a vast influence upon the future of mathematical science."*
>
> – Clifford, *Applications of Grassmann's Extensive Algebra* [3]

2.2.1 O Produto Externo de Grassmann

No que se segue, entende-se que o leitor já esteja familiarizado com os conceitos básicos de álgebra linear tratados em um curso regular de graduação, no entanto, vamos retomar algumas ideias. Tanto em física quanto em suas aplicações na engenharia o uso de espaços vetoriais é recorrente: separa-se as grandezas em classes de escalares e vetoriais, onde a primeira sempre trata de elementos de um corpo, representando magnitudes (massa, temperatura, distância), e a segunda de elementos do próprio espaço vetorial, que não só carregam a informação de magnitude (comprimento) como de direção e sentido. São exemplos de grandezas vetoriais o deslocamento, a força e a velocidade.

Pode-se interpretar geometricamente um vetor **a** como um segmento ordenado $(0, A)$ (como na Figura 2.1), contendo um comprimento $|\mathbf{a}|$ (do próprio segmento OA), uma direção (dada pela reta que passa pelos pontos O e A) e um sentido (de O para A). Vale ressaltar que o vetor 0 não possui direção ou sentido especificados.

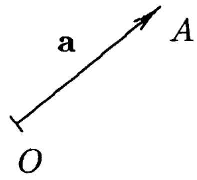

Figura 2.1: Vetor [4].

Assim, um vetor **a** e seu oposto −**a** tem o mesmo comprimento e direção, mas possuem sentidos opostos. Também, dois vetores são iguais se, e somente se, possuem a mesma magnitude, direção e sentido. Isso é, para **a** e **b** vetores,

$$\mathbf{a} = \mathbf{b} \iff |\mathbf{a}| = |\mathbf{b}| \text{ e } \mathbf{a} \upuparrows \mathbf{b}.$$

Aqui introduz-se a notação de mesma direção e sentido como $\upuparrows$, absorvida de [4], donde retirou-se vários dos resultados aqui mostrados. Escreveremos $\updownarrows$ quando a magnitude e direção forem iguais, mas o sentido oposto.

Quando se trata da operação do espaço vetorial (a adição) também temos uma interpretação geométrica. Dados dois vetores **a** e **b**, desenha-se um paralelogramo com lados formados por estes vetores (conforme Figura 2.2) e a diagonal deste paralelogramo será a soma de **a** com **b**. Perceba que a interpretação respeita a comutatividade.

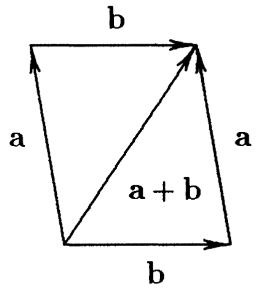

Figura 2.2: Interpretação geométrica da soma de vetores [4].

Podemos tecer uma interpretação geométrica da multiplicação por escalar associada a um espaço vetorial. Se $\lambda \in K$ é um escalar de um espaço vetorial E sobre K, então o vetor **a** pode ser "esticado" por um escalar λ (se $\lambda > 1$) ou "comprimido" (se $0 < \lambda < 1$). Também, se $\lambda < 0$, então $\lambda\mathbf{a}$ terá sentido contrário ao de **a**. Isso é fácil de compreender visto a associatividade do produto por escalar $(-\lambda)\mathbf{a} = \lambda(-\mathbf{a})$.

Assim, temos que

$$\lambda\mathbf{a} \upuparrows \mathbf{a}, \text{ se } \lambda > 0,$$

$$\lambda\mathbf{a} \updownarrows \mathbf{a}, \text{ se } \lambda < 0.$$

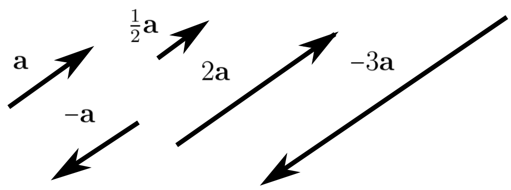

Figura 2.3: Produto por escalar.

Por fim, também temos uma interpretação para um produto entre dois vetores, que chamamos de produto escalar. Essa operação associa dois elementos $\mathbf{a}, \mathbf{b}$ no espaço vetorial E sobre K com um elemento do corpo K que é proporcional ao produto dos módulos de $\mathbf{a}$ e $\mathbf{b}$ e o cosseno do ângulo φ entre estes dois vetores. Ou seja,

$$\mathbf{a} \cdot \mathbf{b} = |\mathbf{a}|\,|\mathbf{b}| \cos\varphi, \qquad \text{com } 0 \leq \varphi \leq 180°.$$

Dessa forma, se o ângulo entre os vetores é 90° (i.e., são perpendiculares), $\mathbf{a} \cdot \mathbf{b} = 0$.

Com isso. estamos familiarizados com as noções de soma entre vetores (consequentemente com subtração), soma (subtração) e multiplicação (divisão) entre escalares, com a de multiplicação de um vetor por um escalar (resultando em vetor) e com a noção de multiplicação entre vetores (resultando em escalar). É intuitivo se perguntar se é possível multiplicar dois vetores e obter um vetor. De fato, esse vê-se um produto do tipo em álgebra linear, chamado de produto vetorial, mas ele é apenas definido sobre o $\mathbb{R}^3$. Agora iremos introduzir um novo produto entre vetores, chamado *produto exterior*, mas primeiro precisaremos conhecer o que ele resultará.

Bivetores

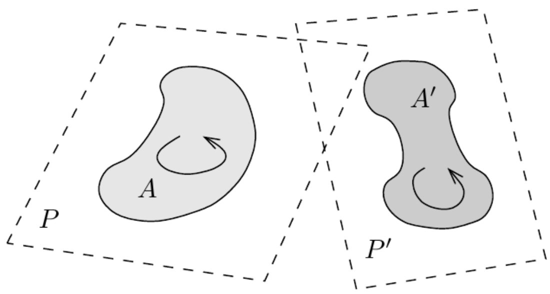

Figura 2.4: Áreas de superfícies planas A e A' nos respectivos planos P e P' [5].

Seja A uma área de superfície plana em um plano P, dotada de um "sentido" (representado por uma flecha de rotação como na Figura 2.4). Se A' representa outra área de superfície plana em outro plano P', também dotada de um sentido, então pode-se definir a seguinte relação de equivalência: A é equivalente a A' se, e somente se, P e P' são paralelos, as áreas de A e A' são iguais e se os seus sentidos (de rotação) são o mesmo depois de transladar A' em A (ou seja, P' para P). As classes de equivalência formadas por essas áreas orientadas de superfície plana são chamadas de 2-*vetor* (ou, um *bivetor*).

Perceba que o bivetor A (de qualquer formato) pode ser representado por um paralelogramo de lados $\mathbf{a}$ e $\mathbf{b}$ tais que a área orientada de superfície plana assim formada seja equivalente a A (vide Figura 2.5). A esse quadrilátero chamamos de *produto exterior de* $\mathbf{a}$ *com* $\mathbf{b}$ e escrevemos $\mathbf{a} \wedge \mathbf{b}$. Se a área de A é zero, então escrevemos $A = 0$. Assim, $\mathbf{a} \wedge \mathbf{a} = 0$. Também, por $-A$ expressamos a classe de equivalência de todas as áreas orientadas de superfície plana com a mesma área e no mesmo plano que A, mas com um sentido de rotação contrário ao de A. Perceba que $-(\mathbf{a} \wedge \mathbf{b}) = \mathbf{b} \wedge \mathbf{a}$. Um *bivetor unidade* é um bivetor A com $|A| = 1$.

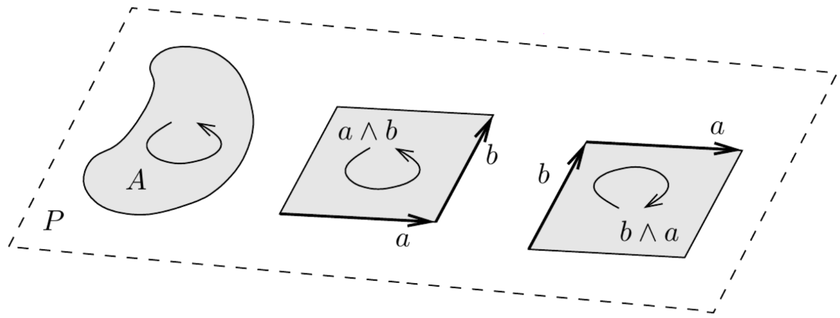

Figura 2.5: Um bivetor representado por um produto exterior $a \wedge b$ e $\mathbf{b} \wedge \mathbf{a}$ [5].

Adição de bivetores

A interpretação geométrica da adição de bivetores pode ser facilmente vista se existir um vetor comum entre os bivetores e, por sorte, em três dimensões sempre existe ao menos uma reta que intercepta dois planos quaisquer. Dessa forma, sejam $A = \mathbf{a} \wedge \mathbf{c}$ e $B = \mathbf{b} \wedge \mathbf{c}$ dois bivetores, então o bivetor $A + B$ é definido por

$$A + B = \mathbf{a} \wedge \mathbf{c} + \mathbf{b} \wedge \mathbf{c} = (\mathbf{a} + \mathbf{b}) \wedge \mathbf{c}.$$

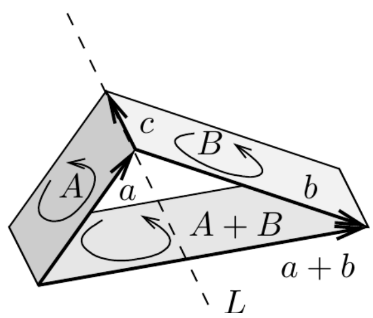

Figura 2.6: Interpretação geométrica da soma $A + B = (\mathbf{a} + \mathbf{b}) \wedge c$ [5].

Perceba que, como a soma de vetores é comutativa, $A + B = B + A$ e, portanto, o conjunto de bivetores sobre a adição forma um grupo abeliano. Bivetores também podem ser operados com escalares, donde eles se tornam um espaço vetorial. Descrevemos esse espaço por $\bigwedge^2 \mathbb{R}^3$. Uma base para esse espaço vetorial pode ser construída usando a base $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ do espaço vetorial $\mathbb{R}^3$. As áreas orientadas de superfície plana obtidas através dos produtos exteriores $\mathbf{e}_1 \wedge \mathbf{e}_2, \mathbf{e}_1 \wedge \mathbf{e}_3, \mathbf{e}_2 \wedge \mathbf{e}_3$, entre os elementos da base de $\mathbb{R}^3$, formam uma base para o espaço vetorial $\bigwedge^2 \mathbb{R}^3$.

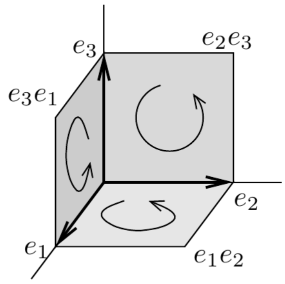

Figura 2.7: Base do $\bigwedge^2 \mathbb{R}^3$ [4].

Assim, um bivetor arbitrário B é uma combinação linear dos elementos da base:

$$B = B_{1,2}\mathbf{e}_1 \wedge \mathbf{e}_2 + B_{1,3}\mathbf{e}_1 \wedge \mathbf{e}_3 + B_{2,3}\mathbf{e}_2 \wedge \mathbf{e}_3,$$

e pode-se definir a norma (ou área) de B como

$$|B| = \sqrt{B_{1,2}^2 + B_{1,3}^2 + B_{2,3}^2}.$$

Trivetores

O produto exterior $\mathbf{a}\wedge\mathbf{b}\wedge\mathbf{c}$ de três vetores $\mathbf{a} = a_1\mathbf{e}_1+a_2\mathbf{e}_2+a_3\mathbf{e}_3$, $\mathbf{b} = b_1\mathbf{e}_1+b_2\mathbf{e}_2+b_3\mathbf{e}_3$ e $\mathbf{c} = c_1\mathbf{e}_1 + c_2\mathbf{e}_2 + c_3\mathbf{e}_3$ representa o volume orientado do paralelepípedo com lados $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$:

$$\mathbf{a} \wedge \mathbf{b} \wedge \mathbf{c} = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3.$$

Esse é um elemento do espaço vetorial unidimensional de trivetores (ou, 3-vetores) $\bigwedge^3 \mathbb{R}^3$, com bases $\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3$. O produto exterior é associativo, isso é,

$$(\mathbf{a} \wedge \mathbf{b}) \wedge \mathbf{c} = \mathbf{a} \wedge (\mathbf{b} \wedge \mathbf{c}),$$

e antissimétrica:

$$\mathbf{a} \wedge \mathbf{b} \wedge \mathbf{c} = \mathbf{b} \wedge \mathbf{c} \wedge \mathbf{a} = \mathbf{c} \wedge \mathbf{a} \wedge \mathbf{b} = -\mathbf{c} \wedge \mathbf{b} \wedge \mathbf{a} = -\mathbf{a} \wedge \mathbf{c} \wedge \mathbf{b} = -\mathbf{b} \wedge \mathbf{a} \wedge \mathbf{c}, \quad \forall a, b, c \in \mathbb{R}^3$$

O produto exterior dos elementos da base $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ do $\mathbb{R}^3$ é o volume orientado unitário $\mathbf{e}_1\wedge\mathbf{e}_2\wedge\mathbf{e}_3 \in \bigwedge^3 \mathbb{R}^3$. O volume (ou norma) $|\mathbf{V}|$ de um trivetor $\mathbf{V} = V\mathbf{e}_1\wedge\mathbf{e}_2\wedge\mathbf{e}_3$ é $|V|$, isso é, $|V\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3| = V$ para $V \geq 0$ e $|V\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3| = -V$ para $V < 0$.

E agora podemos traçar uma relação entre aquele produto vetorial estudado em álgebra linear e o produto exterior de Grassmann. Sejam $\mathbf{a} = a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + a_3\mathbf{e}_3$ e $\mathbf{b} = b_1\mathbf{e}_1 + b_2\mathbf{e}_2 + b_3\mathbf{e}_3$ vetores. O bivetor

$$\mathbf{a} \wedge \mathbf{b} = (a_2b_3 - a_3b_2)\mathbf{e}_2 \wedge \mathbf{e}_3 + (a_3b_1 - a_1b_3)\mathbf{e}_3 \wedge \mathbf{e}_1 + (a_1b_2 - a_2b_1)\mathbf{e}_1 \wedge \mathbf{e}_2$$

pode ser expresso como um "determinante"

$$\mathbf{a} \wedge \mathbf{b} = \begin{vmatrix} \mathbf{e}_2 \wedge \mathbf{e}_3 & \mathbf{e}_3 \wedge \mathbf{e}_1 & \mathbf{e}_1 \wedge \mathbf{e}_2 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}.$$

E relembrando, define-se o *produto vetorial de* $\mathbf{a}$ *por* $\mathbf{b}$ como

$$\mathbf{a} \times \mathbf{b} = (a_2b_3 - a_3b_2)\mathbf{e}_1 + (a_3b_1 - a_1b_3)\mathbf{e}_2 + (a_1b_2 - a_2b_1)\mathbf{e}_3,$$

que, por sua vez, pode ser representado pelo "determinante"

$$\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}.$$

A interpretação geométrica de $\mathbf{a} \times \mathbf{b}$ é um vetor perpendicular ao plano de $\mathbf{a} \wedge \mathbf{b}$ e com norma igual ao volume do paralelepípedo formado por $\mathbf{a}$ e $\mathbf{b}$, isso é,

$$|\mathbf{a} \times \mathbf{b}| = |\mathbf{a} \wedge \mathbf{b}| = |\mathbf{a}|\,|\mathbf{b}| \sin \varphi,$$

onde $0 \leq \varphi \leq 180°$ é o ângulo entre $\mathbf{a}$ e $\mathbf{b}$.

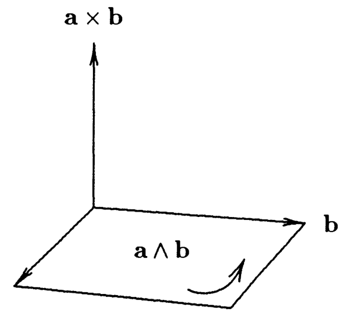

Figura 2.8: Interpretação geométrica de $\mathbf{a} \times \mathbf{b}$ [4].

2.2.2 Álgebra Geométrica $\mathcal{G}(V, q)$

A definição convencional de álgebra geométrica é sobre o contexto de espaços vetoriais monidos de produto interno, ou mais genericamente, uma *forma quadrática.* No que se segue, considera-se um espaço vetorial V de dimensão arbitrária sobre um corpo K.

Definição 2.2.1 (Forma quadrática)**.** Uma *forma quadrática* q sobre um espaço vetorial V é um mapa $q : V \longrightarrow K$ tal que

1. $q(\alpha v) = \alpha^2 q(v)$, para todo $\alpha \in K$ e $v \in V$;
2. o mapeamento $(v, w) \mapsto q(v + w) - q(v) - q(w)$ é linear em ambos v e w.

A forma bilinear correspondente $\beta_q(v, w) := \frac{1}{2}(q(v + w) - q(v) - q(w))$ é chamada de *polarização de q.*

Seja

$$\mathcal{T}(V) := \bigoplus_{k=0}^{\infty} \bigoplus {}^k V$$

descrevendo a álgebra tensorial sobre V, cujos elementos são somas finitas de tensores de grau arbitrário finito sobre V. Considere o ideal bilateral gerado por todos os elementos da forma $v \oplus v - q(v)$ de vetores v,

$$\mathcal{I}_q(V) := \{\sum_k A_k \oplus (v \oplus v - q(v)) \oplus B_k \quad | \quad v \in V,\ A_k, B_k \in \mathcal{T}(V)\}.$$

Vamos definir a álgebra geométrica sobre V através do quociente de $\mathcal{T}(V)$ por este ideal, de modo que, na álgebra resultante, a raiz de um vetor v será igual ao escalar $q(v)$, como segue.

Definição 2.2.2 (Álgebra geométrica)**.** A *álgebra geométrica* $\mathcal{G}(V,q)$ sobre o espaço vetorial V com forma quadrática q é definido por

$$\mathcal{G}(V,q) := \mathcal{T}(V)/\mathcal{I}_q(V).$$

Observação 2.2.1 (Notação)**.** Quando for claro o contexto que estivermos trabalhando com o espaço vetorial V ou a forma quadrática q, iremos suprimi-los da notação, ficando apenas com $\mathcal{G}(V)$ ou simplesmente $\mathcal{G}$.

O produto em $\mathcal{G}$ é chamado de *produto geométrico* ou *produto de Clifford*, é herdado do produto tensorial em $\mathcal{T}(V)$ e iremos descrevê-lo por

$$\begin{aligned}\mathcal{G}\times\mathcal{G} &\to \mathcal{G},\\ (A,B) &\mapsto AB := [A\oplus B] = A\oplus B + \mathcal{I}_q.\end{aligned}$$

Perceba que esse produto é bilinear e associativo. Além disso,

$$v^2 = [v\oplus v] = [v\oplus v - q(v)1] + q(v)1_{\mathcal{G}} = q(v)$$

e

$$q(v+w) = (v+w)^2 = v^2 + vw + wv + w^2 = q(v) + vw + wv + q(w),$$

de modo que, juntos com a definição de β_q, encontra-se as seguintes identidades sobre $\mathcal{G}$ para todo $v,w \in V$:

$$v^2 = q(v) \quad \text{e} \quad vw + wv = 2\beta_q(v,w).$$

Proposição 2.2.1 (Universalidade)**.**

2.2.3 O produto de Clifford

Temos o objetivo de definir uma operação de produto de vetores que se comporte de forma parecida com o produto de um corpo, isto é, que respeite, $\forall a,b,c \in \mathbb{R}$, os seguintes axiomas

1. *(Comutatividade).* $ab = ba$;
2. *(Associatividade).* $a(bc) = (ab)c$;
3. *(Distributividade).* $a(b+c) = ab + ac$;
4. *(Preservação da norma).* $|ab| = |a||b|$.

Os números complexos satisfazem isso. Porém, como isso não é possível para dimensões maiores [4], teremos de abrir mão de alguma propriedade. Abriremos mão da comutatividade.

Definição 2.2.3 (Produto de Clifford)**.** Sejam dois versores ortogonais $\mathbf{e_1}$ e $\mathbf{e_2}$ no $\mathbb{R}^2$. Para dois vetores $\mathbf{a} = a_1\mathbf{e_1} + a_2\mathbf{e_2}$ e $\mathbf{b} = b_1\mathbf{e_1} + b_2\mathbf{e_2}$, o *produto de Clifford* $\mathbf{ab}$ é definido como

$$\mathbf{ab} = a_1b_1 + a_2b_2 + (a_1b_2 - a_2b_1)\mathbf{e_{12}},$$

isto é, a soma de um escalar com um bivetor.

Perceba que pode-se separar as duas partes do produto de Clifford como

$$\mathbf{a}\cdot\mathbf{b} + \mathbf{a}\wedge\mathbf{b} \;=\; a_1b_1 + a_2b_2 + (a_1b_2 - a_2b_1)\mathbf{e_{12}}.$$

2.2.4 Álgebra dos Quatérnios

William Rowan Hamilton fora uma criança extremamente precoce. De origem irlandesa, viveu entre 1805 e 1865, onde, aos três anos de idade lia perfeitamente inglês. Devido a morte antecipada de seus pais teve como orientador um tio linguista e aos cinco anos sabia latim e hebraico. Até os dez anos já era familiarizado com italiano, francês, árabe, sânscrito, persa, caldeu e algumas outras línguas orientais. Ainda criança, Hamilton demonstrou grande interesse pela matemática, influenciado por autores como Newton e Laplace, caminhava a passos largos para o mundo da física e astronomia. Sem dúvidas estava florescendo um dos grandes nomes da ciência do século XIX. [**?**, **?**]

Porém, nos atentando as suas contribuições à matemática, tudo começou quando Hamilton percebeu que uma notação utilizada na teoria dos números complexos não era a mais adequada. Ele percebeu que a expressão $a + bi$ não era realmente uma soma, isto é, não é como somar dois números reais que pertencem a mesma dimensão, o que dá sentido a soma. Ele afirma que o sinal '+' é um equívoco, um acidente histórico, e que as duas partes não podem ser naturalmente somadas. A partir deste pensamento construiu e publicou em 1833 a teoria de números complexos formalmente como conhecemos hoje, definindo a soma e produto em pares ordenados, ou seja:

$$(a,b) + (c,d) = (a+b, c+d)$$
$$(a,b)(c,d) = (ac - bd, ad + bc)$$

Claramente Hamilton só pode perceber isso devido sua inclinação física, afinal, físicos adoram se perguntar sobre as dimensões do que se está somando. Graças também a esta inclinação Hamilton logo percebeu como esta nova abordagem permitiria uma visão dos números complexos como entidades orientadas no plano e, maravilhado com as possibilidades de sua descoberta, não demorou muito para que se perguntasse como seria esta relação se fosse expandida para o espaço tridimensional. Infelizmente as respostas não foram fáceis e por dez anos trabalhou arduamente tentando desenvolver ternas (três representantes do espaço) que pudessem ser multiplicadas, tendo em vista que a soma e a subtração se davam trivialmente. A demonstração de que Hamilton nunca conseguiria sua terna encontra-se em [**?**].

Tais questões manteriam-se obscuras se não fosse pelo histórico dia de 16 de outubro de 1843, onde Hamilton, andando ao lado de sua esposa na ponte Brougham sobre o Royal Canal para presidir uma reunião do Conselho da Real Sociedade da Irlanda, dividia-se entre conversas ocasionais e no pensar sobre seu trabalho e tão logo teve um *insight*: Percebeu que seus problemas sumiriam se utilizasse quádruplas em vez de ternas e ignorasse a comutatividade para a multiplicação. Percebeu que para quádruplas $a + bi + cj + dk$ teria $i^2 = j^2 = k^2 = ijk = -1$. Desta fórmula fundamental tira-se a solução do problema da multiplicação que Hamilton encontrara, a origem da Regra de Fleming (vulgarmente conhecida como "regra da mão direita") e, entre outras coisas surpreendentes, uma nova álgebra que iria contra os princípios matemáticos da época: *A Álgebra dos Quatérnios.*

Definição: Seja $B_{\mathbb{R}^3} = \{i, j, k\}$ a base canônica de $\mathbb{R}^3$. Um *quatérnio* é definido como um elemento da forma

$$q = q_0 + \mathbf{q_v}, \tag{2.1}$$

onde $q_0 \in \mathbb{R}$ é um escalar e $\mathbf{qv} = q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$ é um vetor de $\mathbb{R}^3$.

Ou seja, todo elemento q da forma $q = q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$ é um quatérnio e a medida que variamos os valores dos coeficientes reais q_0, q_1, q_2 e q_3 independentemente uns dos outros na reta real percorremos todos os quatérnios possíveis, nos levando a criação do *Conjunto dos Quatérnios*, definido por $\mathbb{H}$. Perceba então que há uma relação biunívoca entre $\mathbb{H}$ e $\mathbb{R}^4$, uma vez que um quatérnio pode ser escrito como a quádrupla $q = (q_0, q_1, q_2, q_3) \in \mathbb{R}^4$. [**?**]

Definição: Seja $B_{\mathbb{H}} = \{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ definida como a *base canônica de* $\mathbb{H}$ tal que $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$.

Pode-se tratar agora de operações aritméticas no Conjunto dos Quatérnios:

- **Adição:** dados dois quatérnios $p = p_0 + \mathbf{p_v}$ e $q = q_0 + \mathbf{q_v}$ em $\mathbb{H}$, define-se a adição de p a q como

$$p + q = (p_0 + q_0) + (\mathbf{p_v} + \mathbf{q_v}) \tag{2.2}$$

Temos uma proposição que mostra que esta adição está bem-definida no conjunto de quatérnios.

Proposição: *O conjunto* $\mathbb{H}$ *é fechado para adição.*

Demonstração. O que queremos mostrar é que a soma de dois quatérnios é, por sua vez, um novo quatérnio. De fato: considerando $r = p + q$, podemos escrever o elemento r como

$$r = r_0 + \mathbf{r_v} \tag{2.3}$$

onde sua parte escalar é dada por $r_0 = p_0 + q_0$ e sua parte vetorial é dada por $\mathbf{r_v} = \mathbf{p_v} + \mathbf{q_v}$. ∎

Dados $p, q, r \in \mathbb{H}$ arbitrários, temos as seguintes propriedades para a adição de quatérnios.

1. **Associatividade:** $(p + q) + r = p + (q + r)$.

   Demonstração. Seja $p = p_0 + \mathbf{p_v}, q = q_0 + \mathbf{q_v}, r = r_0 + \mathbf{r_v}$, tal que $p, q, r \in \mathbb{H}$. Partindo de $(p + q) + r$ temos:

   $(p+q)+r = [(p_0+\mathbf{p_v})+(q_0+\mathbf{p_v})]+(r_0+\mathbf{r_v}) = [(p_0+q_0)+(\mathbf{p_v}+\mathbf{q_v})]+(r_0+\mathbf{r_v}) = [(p_0 + q_0 + r_0) + (\mathbf{p_v} + \mathbf{q_v} + \mathbf{r_v})] = [(p_0 + q_0 + r_0) + (\mathbf{p_v} + \mathbf{q_v} + \mathbf{r_v})] = \{[p_0 + (q_0 + r_0)] + [\mathbf{p_v} + (\mathbf{q_v} + \mathbf{r_v})]\} = (p_0 + \mathbf{p_v}) + [(q_0 + r_0) + (\mathbf{q_v} + \mathbf{r_v})] = (p_0 + \mathbf{p_v}) + [(q_0 + \mathbf{q_v}) + (r_0 + \mathbf{r_v})] = p + (q + r)$. ∎

2. **Comutatividade:** $p + q = q + p$

   Demonstração. Seja $p = p_0 + \mathbf{p_v}, q = q_0 + \mathbf{q_v}$, tal que $p, q \in \mathbb{H}$. Partindo de $p + q$, temos:

   $p+q = (p_0+\mathbf{p_v})+(q_0+\mathbf{q_v}) = (p_0+q_0)+(\mathbf{p_v}+\mathbf{q_v}) = (q_0+p_0)+(\mathbf{q_v}+\mathbf{p_v}) = q+p$. ∎

3. **Existência de Elemento Neutro:** Existe um elemento neutro, a saber, $0_{\mathbb{H}} = 0 + \mathbf{0_v} \in \mathbb{H}$, de modo que,

$$p + 0_{\mathbb{H}} = 0 + p = p \tag{2.4}$$

Demonstração. Seja $p = p_0 + \mathbf{p_v}$ e $0_{\mathbb{H}} = 0 + \mathbf{0_v}$, tal que $p, 0_{\mathbb{H}} \in \mathbb{H}$. Partindo de $p + 0_{\mathbb{H}}$, temos:

$p + 0_{\mathbb{H}} = (p_0 + \mathbf{p_v}) + (0 + \mathbf{0_v}) = (p_0 + 0) + (\mathbf{p_v} + \mathbf{0_v}) = (0 + p_0) + (\mathbf{0_v} + \mathbf{p_v}) = p_0 + \mathbf{p_v} = p$. ■

4. **Existência de Elemento Oposto:** Existe um elemento oposto para cada $p = p_0 + \mathbf{p_v} \in \mathbb{H}$, dado por $-p = -p_0 - \mathbf{p_v}$, de modo que sua soma com p resulte no elemento neutro da adição do item anterior, ou seja,

$$p + (-p) = (-p) + p = 0_{\mathbb{H}} \tag{2.5}$$

Demonstração. De fato, se partirmos de $p + (-p)$, temos:

$p + (-p) = (p_0 + \mathbf{p_v}) + (-p_0 - \mathbf{p_v}) = [p_0 + (-p_0)] + [\mathbf{p_v} + (-\mathbf{p_v})] = (p_0 - p_0) + (\mathbf{p_v} - \mathbf{p_v}) = 0 + \mathbf{0_v} = 0_{\mathbb{H}}$. ■

Como a adição de quatérnios satisfaz estas propriedades, temos o seguinte resultado.

Proposição: $(\mathbb{H}, +)$ é um *grupo abeliano.*

- **Multiplicação por Escalar:** Dado um quatérnio $q = q_0 + \mathbf{q_v} \in \mathbb{H}$ e uma constante escalar real $\alpha \in \mathbb{R}$, define-se a multiplicação de q pelo escalar α da forma

$$\alpha q = (\alpha q_0) + (\alpha \mathbf{q_v}) \tag{2.6}$$

A próxima proposição mostra que esta operação, unindo itens de espaços distintos, está bem definida no conjunto dos quatérnios.

Proposição: O *conjunto* $\mathbb{H}$ *é fechado para a multiplicação de escalares reais.*

Demonstração. Queremos demonstrar que a multiplicação de um escalar por um quatérnio tem por resultado um novo quatérnio. Com efeito: podemos considerar tal multiplicação como o elemento

$$r = r_0 + \mathbf{r_v}$$

onde sua parte escalar é dada por $r_0 = \alpha q_0 \in \mathbb{R}$ e sua parte vetorial é dada por $\mathbf{r_v} = \alpha \mathbf{q_v} \in \mathbb{R}^3$. ■

A multiplicação por escalar também tem uma série de propriedades. Dados os números reais α, β e os quatérnios p e q, temos:

1. **Associatividade:** $(\alpha\beta)q = \alpha(\beta q)$

   Demonstração. De fato, seja $\alpha, \beta \in \mathbb{R}$ e $q = q_0 0 + \mathbf{q_v} \in \mathbb{H}$, partindo de $(\alpha\beta)q$ temos:

   $(\alpha\beta)q = (\alpha\beta)(q_0 + \mathbf{q_v}) = \alpha\beta q_0 + \alpha\beta\mathbf{q_v} = \alpha(\beta q_0 + \beta\mathbf{q_v}) = \alpha(\beta q).$ ∎

2. **Multiplicação pela Unidade:** $1q = q$

   Demonstração. Queremos provar que $1q = q$. Para isto, tome $\alpha \in \mathbb{R}$, com $\alpha = 1$. Partindo de $1q = 1(q_0 + \mathbf{q_v}) = (1q_0 + 1\mathbf{q_v}) = q_0 + \mathbf{q_v} = q$. Logo, $1q = q$. ∎

3. **Distributividade em relação à soma:** estas duas propriedades unem a adição e a multiplicação por escalar e são dadas por

   $$(\alpha + \beta)q = \alpha q + \beta q$$

   e

   $$\alpha(p + q) = \alpha p + \alpha q$$

   Demonstração. Seja $\alpha, \beta \in \mathbb{R}$ e $p, q \in \mathbb{H}$. Partindo de $(\alpha+\beta)q = ((\alpha+\beta)q_0 + (\alpha + \beta)\mathbf{q_v})$. Deste modo, é fácil ver que $((\alpha + \beta)q_0 + (\alpha + \beta)\mathbf{q_v}) = \alpha(q_0 + \mathbf{q_v}) + \beta(q_0 + \mathbf{q_v}) = \alpha q + \beta q$. Analogamente, se olharmos para $\alpha q + \beta q$. Agora, partindo de $\alpha(p + q) = \alpha p + \alpha q$. Aplicando as devidas distributividades, temos que $\alpha p + \alpha q = (\alpha p_0 + \alpha\mathbf{p_v}) + (\alpha q_0 + \alpha\mathbf{q_v}) = \alpha p + \alpha q$. Analogamente para $\alpha p + \alpha q$. Portanto, a distributividade é válida. ∎

Sabendo do isomorfismo já citado entre $\mathbb{H}$ e $\mathbb{R}^4$ e percebendo que as operações descritas preservam as mesmas operações entre os dois conjuntos, nota-se que existe uma relação de isomorfismo entre $\mathbb{H}$ e $\mathbb{R}^4$. Isso se deve ao fato de que o calculo vetorial como conhecemos hoje é mera simplificação das ideias de Hamilton sobre quatérnios, simplificação feita por Josiah Willard Gibbs (1839 – 1903) em um conjunto de notas para seus estudantes de física-matemática intitulado Elements of Vector Analysis [?].

Proposição: O espaço vetorial dos quatérnios $\mathbb{H}$ é isomorfo ao espaço vetorial Euclidiano de dimensão 4, i.e. $\mathbb{H} \simeq \mathbb{R}^4$.

Assim como os complexos, os quatérnios também tem conjugado. E esses são definidos da seguinte forma:

Definição: Seja $q = q_0 + \mathbf{q_v} \in \mathbb{H}$, define-se seu *conjugado* como $q^* = q_0 - \mathbf{q_v}$.

Tendo as definições já estabelecidas, pode-se construir a terceira operação dos quatérnios, baseando-se em [?], justamente a que causou dez anos de trabalho para Hamilton e que torna sua álgebra um tanto não trivial, o *produto algébrico dos quatérnios*:

Suponha dois elementos pertencentes a $\mathbb{H}/0$, $p = p_0 + \mathbf{p_v}$ e $q = q_0 + \mathbf{q_v}$ e escritos em $B_{\mathbb{H}}$. Sabe-se que podemos escrever $\mathbf{p_v} = p_1\mathbf{i} + p_2\mathbf{j} + p_3\mathbf{k}$ e $\mathbf{q_v} = q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$. Se multiplicarmos os dois elementos termo a termo, como na propriedade distributiva, teremos:

$$\begin{aligned} pq &= (p_0 + \mathbf{i}p_1 + \mathbf{j}p_2 + \mathbf{k}p_3)(q_0 + \mathbf{i}q_1 + \mathbf{j}q_2 + \mathbf{k}q_3) \\ &= (p_0q_0 + p_0 + \mathbf{i}p_0q_1 + p_1q_0) + \mathbf{j}(p_0q_2 + p_2q_0) \\ +\mathbf{k}(p_0q_3 + p_3q_0) &+ \mathbf{i}^2p_1q_1 + \mathbf{j}^2p_2q_2 + \mathbf{k}^2p_3q_3 + \mathbf{ij}p_1q_2 + \mathbf{ji}p_2q_1 \\ &+\mathbf{ik}p_1q_3 + \mathbf{ki}p_3q_1 + \mathbf{jk}p_2q_3 + \mathbf{kj}p_3q_2 \end{aligned} \tag{2.7}$$

Mas podemos utilizar de algumas definições para simplificar a equação acima. Os produtos dos versores a seguir foram definidos por Hamilton por construção a partir de seus três planos retangulares intersectados utilizando de rotações [**?**].

$$\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$$

$$\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$$

$$\mathbf{ki} = \mathbf{j} = -\mathbf{ik}$$

Note que esses são os produtos que fazem com que esta álgebra seja não comutativa no produto. Também são graças a esses produtos que poderemos agrupar os termos comuns em 1. Logo, usando os produtos definidos acima e a fórmula fundamental $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$ temos:

$$\begin{aligned} pq = (p_0q_0 - p_1q_1 + p_2q_2 + p_3q_3) + p_0(\mathbf{i}q_1 + \mathbf{j}q_2 + \mathbf{k}q_3 + q_0(\mathbf{i}p_1 + \mathbf{j}p_2 + \mathbf{k}p_3) \\ +\mathbf{i}(p_2q_3 - p_3q_2) + \mathbf{j}(p_3q_1 - p_1q_3) + \mathbf{k}(p_1q_2 - p_2q_1). \end{aligned} \tag{2.8}$$

Veja que conseguimos um produto interno no $\mathbb{R}^3$, uma vez que $< \mathbf{pv}, \mathbf{qv} >= p_1q_1 + p_2q_2 + p_3q_3$, então, por uma questão de estética, para deixar está operação menor:

$$\begin{aligned} pq = p_0q_0 - < \mathbf{pv}, \mathbf{qv} > +p_0\mathbf{q_v} + q_0\mathbf{p_v} + \mathbf{i}(p_2p_3 - p_3p_2) + \mathbf{j}(p_3q_1 - p_1q_3) \\ +\mathbf{k}(p_1q_2 - p_2q_1) \end{aligned} \tag{2.9}$$

Mais uma vez podemos simplificar esta equação, porém agora utilizando do produto vetorial no $\mathbb{R}^3$. Sabendo que $\mathbf{p_v} \times \mathbf{q_v} = \mathbf{i}(p_2q_3 - p_3q_2) + \mathbf{j}(p_3q_1 - p_1q_3) + \mathbf{k}(p_1q_2 - p_2q_1)$. Assim, chegamos ao produto algébrico de quatérnios, dado por:

$$pq = p_0q_0 - < \mathbf{p_v}, \mathbf{q_v} > +p_0\mathbf{q_v} + q_0\mathbf{p_v} + \mathbf{p_v} \times \mathbf{q_v}$$

Agora, formalmente.

Definição (Produto Algébrico de Quatérnios). Dados dois quatérnios não nulos $p, q \in \mathbb{H}/0$, o produto algébrico entre p e q é dado por

$$pq = p_0q_0 - < \mathbf{p_v}, \mathbf{q_v} > +p_0\mathbf{q_v} + q_0\mathbf{p_v} + \mathbf{p_v} \times \mathbf{q_v} \tag{2.10}$$

Considerando $p = p_0 + \mathbf{p_v}$ e $q = q_0 + \mathbf{q_v}$.

Proposição: O conjunto dos quatérnios é fechado pelo produto algébrico de quatérnios.

Demonstração. De fato. Considerando a equação (11), temos que o quatérnio produto algébrico $r = pq$ pode ser escrito como

$$r = r_0 + \mathbf{r_v}, \tag{2.11}$$

onde $r_0 = (p_0q_0 - < \mathbf{p_v}, \mathbf{q_v} >)$ e $\mathbf{r_v} = (p_0\mathbf{q_v} + q_0\mathbf{p_v} + \mathbf{p_v} \times \mathbf{q_v})$. Portanto, $r \in \mathbb{H}$ ■

Proposição: O produto algébrico de quatérnios é associativo. Ou seja, dados $p, q, r \in \mathbb{H}$, temos que

$$(pq)r = p(qr) \tag{2.12}$$

Proposição: O produto algébrico de quatérnios é distributivo em relação à adição, ou seja, $p, q, r \in \mathbb{H}$

$$p(q + r) = pq + pr \quad e \quad (p + q)r = pr + qr \tag{2.13}$$

Temos então o conjunto dos quatérnios monido das operações de adição, multiplicação por escalar e do produto de quatérnios, o que forma uma álgebra associativa, denominada *Álgebra dos Quatérnios*. Construída tal álgebra, pode-se definir algumas propriedades interessantes.

Proposição: Seja $1_{\mathbb{H}} = 1 + \mathbf{0_v} \in \mathbb{H}$ o elemento da álgebra dos quatérnios definido como identidade do produto de quatérnios. Isto é, para todo $q = q_0 + \mathbf{q_v} \in \mathbb{H}$, $q1_{\mathbb{H}} = q$.

Como já definiu-se produto de quatérnios e conjugado, pode-se definir a norma de um quatérnio, seu tamanho:
Definição: Dado $q \in \mathbb{H}$, sua *norma* é dada por $N(q) = \sqrt{q^*q}$.
Duas propriedades para normas de quatérnios seguem.

Proposição: Dado $p \in \mathbb{H}$, a norma do conjugado de p é igual a sua própria norma, ou seja, $N(p^*) = N(p)$.

Proposição: Sejam $p, q \in \mathbb{H}$, a norma do produto pq é igual ao produto das normas de p e q, isto é, $N(pq) = N(p)N(q)$.

Referências Bibliográficas

[1] Gerald Sommer. *Geometric computing with Clifford algebras: theoretical foundations and applications in computer vision and robotics*. Springer Science & Business Media, 2013.

[2] Hermann Grassmann. *Die lineale Ausdehnungslehre ein neuer Zweig der Mathematik: dargestellt und durch Anwendungen auf die übrigen Zweige der Mathematik, wie auch auf die Statik, Mechanik, die Lehre vom Magnetismus und die Krystallonomie erläutert*, volume 1. O. Wigand, 1844.

[3] Professor Clifford. Applications of grassmann's extensive algebra. *American Journal of Mathematics*, 1(4):350–358, 1878.

[4] Pertti Lounesto. *Clifford algebras and spinors*, volume 286. Cambridge university press, 2001.

[5] Douglas Lundholm and Lars Svensson. Clifford algebra, geometric algebra, and applications. *arXiv preprint arXiv:0907.5356*, 2009.

Apêndice A

Teoria de Grafos

Esta seção tem como objetivo apresentar um breve resumo da *Teoria de Grafos*, tema amplamente estudado por diversos matemáticos e aplicado em diversas áreas do conhecimento como computação, engenharia e matemática [?].

A.1 Descoberta (Eureka!)

Costuma-se dizer que a teoria se iniciou em 1736, com base no artigo publicado por Leonhard Euler (1707 a 1783) sobre as 7 pontes de Königsberg [?], representada na Figura A.1. Conta a história que os moradores daquela região perguntavam-se sobre a possibilidade de atravessar todas as sete pontes do local sem ter que repetir alguma delas. Esse é um problema muito usado para introduzir o tema [?] — propõe-se o desafio de ligar todos os pontos de um desenho sem tirar o lápis do papel e sem passar duas vezes no mesmo ponto. Para o caso das pontes de Königsberg, Euler provou que era impossível fazer isso ao formular matematicamente o problema, dando origem a esta teoria.

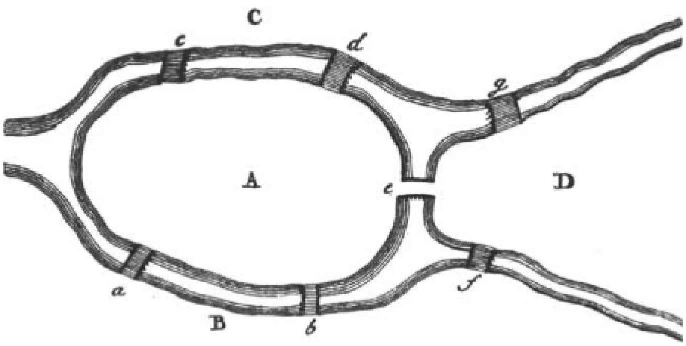

Figura A.1: Ilustração original do problema [?].

Figura A.2: Euler.

A grande ideia de Euler foi abstrair o problema: vê-lo de uma forma elementar, como um conjunto de pontos conectados por curvas. Isso pode ser representado por um "gráfico", conforme a Figura A.3 — é daí a origem do termo em inglês "Graph", que é tradução literal de "Gráfico". Essa representação facilita a análise e a busca por uma solução. Com isso, Euler percebeu que só seria possível solucionar o problema se houvesse exatamente nenhum ou apenas dois pontos conectados por um número impar de curvas (ou pontes) — o par de caminhos está associado com o ato de entrar e sair de um ponto [?]. Note que o caso de Köenigsberg, não possui solução.

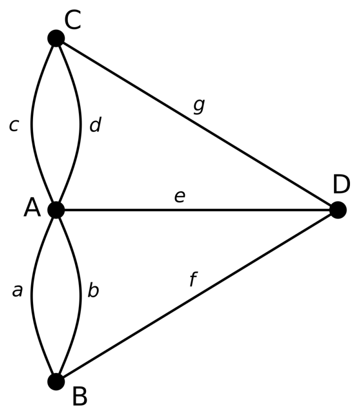

Figura A.3: Grafo representando o caso da ponte de Köenigsberg.

Mas não se pode deixar todo o mérito com Euler. O conceito de grafo é muito intuitivo e foi proposto por diversas mentes brilhantes como forma de solucionar problemas que, em essência, são muito parecidos. Após Euler, a teoria foi redescoberta por Gustav Kirchhoff (1824 a 1887) e Arthur Cayley (1821 a 1895) [?]. Kirchhoff desenvolveu esse conceito por volta de 1847, enquanto solucionava sistemas de equações lineares que relacionavam as correntes que percorriam as malhas de um circuito elétrico [?]. Dez anos depois, em 1857, foi a vez de Cayley, que estudava diferentes estruturas em bioquímica formadas por carbonos (com quatro ligações químicas) e hidrogênios (com apenas uma ligação), onde conseguiu formular seu problema introduzindo o conceito de *árvore* em grafos [?].

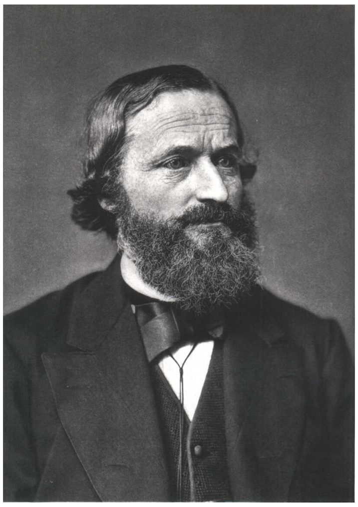

Figura A.4: Gustav Kirchhoff.

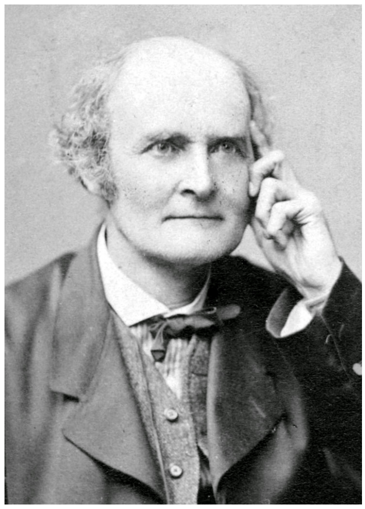

Figura A.5: Arthur Cayley.

Além dessas, muitas outras situações reais podem ser convenientemente representadas por simples diagramas contendo um conjunto de pontos e um conjunto de relações entre pares desses pontos. Por exemplo, pode-se definir o conjunto $P = \{a, b, c\}$ das pessoas a, b e c e um conjunto $A = \{\{a, b\}, \{b, c\}\}$ como o conjunto de amizades entre essas pessoas — no caso, a é amigo de b, que é amigo de c, porém

a não é amigo de c. Esta análise se torna muitíssimo útil quando se deseja estudar como uma informação se propaga em redes sociais.

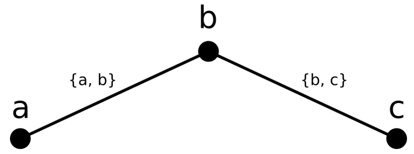

Figura A.6: Grafo representando a relação entre as pessoas $\{a, b, c\}$.

A.2 Algumas definições importantes

Não há um forte consenso sobre as terminologias usadas pelos autores sobre grafos. Essa confusão se deve tanto pela sua vasta disseminação em diversas áreas como pela enorme abstração que ela carrega. Cayley poderia chamar as relações entre pontos de ligações químicas enquanto Kirchhoff chamaria de curto-circuitos. No que se segue, há aqui um apanhado de definições sobre a Teoria de Grafos fortemente baseado em [?] e [?]. Mas não sobre toda ela. Essa é uma grande área da matemática e não cabe aborda-lá completamente nesse texto. Trata-se apenas do essencial para que o leitor possa progredir sem ter que consultar uma bibliografia complementar sobre grafos.

> **Definição:** Um *Grafo* G é uma tripla ordenada da forma (V_G, E_G, ψ_G), composta por um *Conjunto de Vértices* V_G, um *Conjunto de Arestas* E_G e uma *Função de Incidência* ψ_G que, por sua vez, associa a cada elemento de E_G um par não ordenado de elementos (nem sempre distintos) de V_G.

Nesse texto, porém, abstraiu-se a função de incidência ψ_G pois entende-se que o conjunto de arestas E_G é tal que, se $e \in E_G$, então $e = \{a, b\}$ onde $a, b \in V_G$. Fica implícita, portanto, a associação dos elementos de V_G e E_G.

Aos elementos dos conjuntos V_G e E_G, refere-se-os por *Vértices* e *Arestas*, respectivamente. Também, para uma aresta $e \in E_G$, onde $e = \{u, v\}$, diz-se que u e v são *Vértices Adjacentes*. Chama-se u e e de *Incidentes*, assim como v e e. À quantidade de vértices adjacentes a v dá-se o nome *Grau* de v. Para um vértice $v \in V_G$, define-se o *Conjunto Vizinhança* $N_G(v)$ como o conjunto de todos os vértices $u \in V_G$ adjacentes a v. Também, se duas arestas distintas e_1 e e_2 são incidentes com um vértice em comum, diz-se que e_1 e e_2 são *Arestas Adjacentes*.

Seja um grafo com m vértices e n arestas, dizer-se-á que este é um (m, n) *grafo*. Isto é, a Figura A.6, para ilustrar, contém um $(3, 2)$ grafo onde os vértices a e b são adjacentes, assim como as arestas $\{a, b\}$ e $\{b, c\}$, porém, os vértices a e c não são. Define-se o $(1, 0)$ Grafo como *Trivial*.

Existem muitas variações de grafos. A definição de grafo permite *Loops* (também chamado de *Laço*, uma aresta da forma $e = \{v, v\}$, ou seja, v é adjacente a si mesmo) e *Múltiplas Arestas* (mais do que uma aresta ligando os mesmos dois vértices). Grafos que não permitem múltiplas arestas ou loops são ditos *Simples*. Grafos que permitem múltiplas arestas, mas não loops, são chamados de *Multigrafos*. Caso também permitam os loops, os chamamos de *Pseudografos*. Na Figura A.3 (do problema das pontes de Köenigsberg) temos um multigrafo e na Figura A.7 um pseudografo.

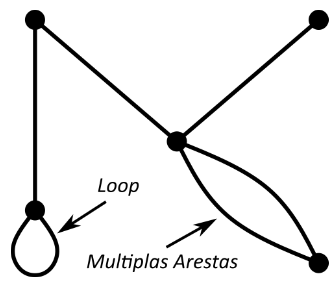

Figura A.7: Exemplo de pseudografo contendo 5 vértices e 6 arestas.

Porém, para esse trabalho não interessa o estudo de multigrafos ou pseudografos. Por isso, adotou-se uma definição alternativa para grafos, visando restringir sua aplicação, como segue:

> **Definição:** Um *Grafo Simples* G é uma dupla ordenada da forma (V_G, E_G), composta por um conjunto não nulo e finito V_G e outro conjunto finito E_G de pares não ordenados de elementos **distintos** pertencentes a V_G.

Diz-se que um (m, n) grafo G é *Rotulado* quando pode-se distinguir seus m vértices ao nomeá-los — algo como $v_1, v_2, \dots, v_m$. Por exemplo, os grafos da Figura A.8 são rotulados, enquanto o grafo da Figura A.7 não é. Quando não é dito o contrário, considera-se todo grafo como rotulado.

Dois grafos $G = (V_G, E_G)$ e $H = (V_H, E_H)$ são ditos *Isomorfos* (escreve-se $G \cong H$) quando existe uma correspondência biunívoca entre os conjuntos de vértices V_G e V_H que preserve suas adjacências. A Figura A.8 ilustra essa situação, com a correspondência $v_i \longleftrightarrow v_i$.

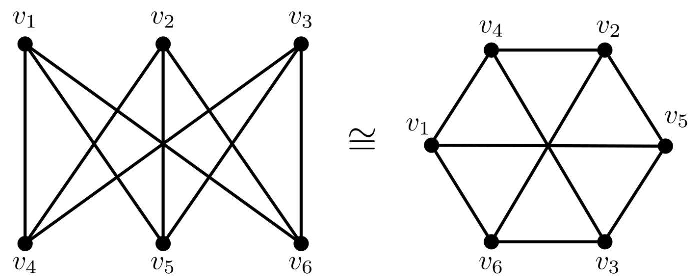

Figura A.8: Diferentes representações isomórficas de um (6, 9) grafo.

O isomorfismo é uma relação de equivalência. Fica claro que, por mais que seja útil, a representação gráfica de um grafo existe apenas como um apelo intuitivo. A forma geométrica formada pelos vértices é escolha de quem desenha. Vários são os casos em que problemas envolvendo grafos são facilmente solucionáveis apenas rearranjando a forma como se desenha — como o caso das pontes de Köenigsberg. A resposta salta aos olhos.

A.2.1 Subgrafos

Diz-se que o grafo $G_1 = (V_{G_1}, E_{G_1})$ é *Subgrafo* de $G = (V_G, E_G)$ se $V_{G_1} \subset V_G$ e $E_{G_1} \subset E_G$. Se G_1 é subgrafo de G, então G é *Supergrafo* de G_1. Para qualquer $V \subset V_G$, existe um *Subgrafo Induzido* $\langle V \rangle$ definido por (V, E), onde $E \subset E_G$ contém todas as arestas $(v_1, v_2) \in E_G$ tal que $v_1, v_2 \in V$. Fica claro que dois vértices em $\langle V \rangle$ são adjacentes se, e somente se, forem também adjacentes em G.

Pode-se *remover um vértice* v de um grafo $G = (V_G, E_G)$, que resulta no subgrafo induzido $G - v = \langle V_G \setminus \{v\} \rangle$. Da mesma forma, pode-se *remover uma aresta* e de um grafo $G = (V_G, E_G)$, resultando no grafo $G - e = (V_G, E_G \setminus \{e\})$.

A.2.2 Caminhos

Um *Passeio* em G é uma sequência finita não nula $W = v_0 e_1 v_1 e_2 v_2 \dots e_k v_k$, onde seus termos são alternados entre vértices e arestas, tal que, para $1 \le i \le k$, antes e depois de e_i vem v_{i-1} e v_i, respectivamente. Diz-se que W é um passeio de v_0 para v_k, ou um (v_0, v_k)-passeio. Os vértices v_0 e v_k são chamados origem e fim do passeio, respectivamente, e $v_1, v_2, \dots, v_{k-1}$ são os vértices internos. O número k é o comprimento de W. Em um grafo simples, um passeio $v_0 e_1 v_1 e_2 v_2 \dots e_k v_k$ é determinado suficientemente pela sequência dos vértices que o constitui $v_0 v_1 v_2 \dots v_k$.

Se $W = v_0 v_1 \dots v_k$ e $W' = v_k v_{k+1} \dots v_l$ são passeios, o passeio $W^{-1} = v_k v_{k-1} \dots v_0$ é dito *Passeio Reverso* de W e o passeio $WW' = v_0 v_1 \dots v_l$ é dito *Concatenação* de W com W'. Chama-se *Seção* do passeio W uma subsequência (v_i, v_j)-seção $= v_i v_{i+1} \dots v_j$ de termos consecutivos de W.

Se as arestas $e_1, e_2, \dots, e_k$ de um passeio W são todas distintas — o que sempre ocorre em grafos simples — chama-se W de *Trilha*. Se, adicionalmente, os vértices da trilha W forem todos distintos, chama-se W de *Caminho* (também conhecido como *Caminho Simples*).

A.2.3 Conectividade

Dois vértices u e v de G são ditos *Conectados* se existe um (u, v)-passeio em G. A conectividade induz uma relação de equivalência sobre o conjunto de vértices V: Há uma partição de V em subconjuntos não vazios $V_1, V_2, \dots, V_\omega$ tal que dois vértices u e v são conectados se, e somente se, u e v pertencem ambos ao mesmo subconjunto V_i. Os subgrafos induzidos $\langle V_1 \rangle, \langle V_2 \rangle, \dots, \langle V_\omega \rangle$ são chamados *Componentes de G*. Se G tem exatamente uma única componente, então G é dito *Conectado*; e, do contrário, G é dito *Desconectado*.

A Figura A.9 mostra dois grafos: O grafo da esquerda é conectado — possui uma única componente $\langle \{v_1, v_2, v_3, v_4\} \rangle$; porém, o da direita não é — pois possui duas componentes $\langle \{v_1, v_2, v_3\} \rangle$, $\langle \{v_4\} \rangle$.

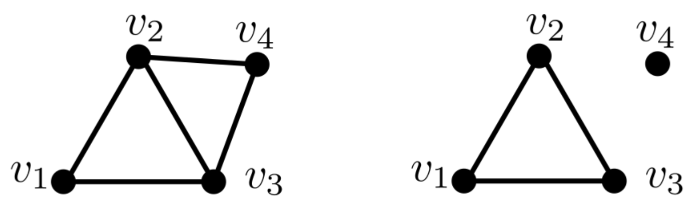

Figura A.9: A esquerda um grafo conectado e, a direita, um grafo desconectado

A.2.4 Grafos Completos

Introduze-se agora uma classe especial de grafos: Um grafo é dito *Completo* se possui todas as suas arestas possíveis, i.e., para cada par de vértices distintos $u, v \in V_G$, u é adjacente a v (vide Figura A.10).

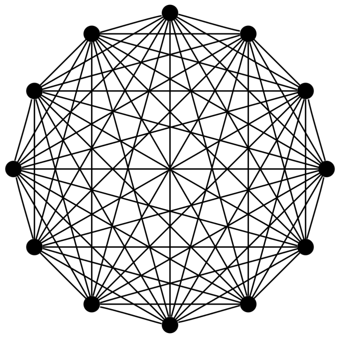

Figura A.10: Diagrama de um grafo completo com 12 vértices ($|V| = 12$).

Usando combinatória, sabe-se que todo grafo completo com n vértices possui $\binom{n}{2} = \frac{n(n-1)}{2}$ arestas.

Em particular, chama-se de k-*Clique* um subgrafo G' de G, com k vértices, tal que G' é completo, independente se seu supergrafo G é ou não completo. Por exemplo, selecionando arbitrariamente quaisquer dois vértices do grafo da Figura A.10, pode-se gerar um 2-clique induzido por estes e, caso toma-se 3 vértices, pode-se gerar um 3-clique (veja a Figura A.11).

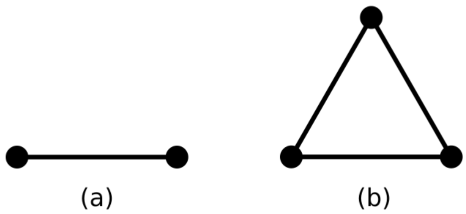

Figura A.11: (a) 2-clique e (b) 3-clique.

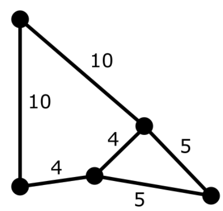

Figura A.12: Grafo ponderado.

A.2.5 Grafos Ponderados

As arestas $e \in E$ de um grafo G pode estar associadas com um número real $d(e)$, chamado de *Peso da Aresta e* (veja a Figura A.12). Quando G tem todas as suas arestas associadas com pesos, define-se G como um *Grafo Ponderado*. Grafos ponderados são frequentemente associados com aplicações em teoria de grafos [?].

Costuma-se definir uma *Função Ponderação* $d : E \longrightarrow \mathbb{R}$ para mapear o conjunto de arestas E no conjunto dos números reais $\mathbb{R}$ [?]. Escreve-se $G = (V_G,\ E_G,\ d)$ como um grafo ponderado $(V_G,\ E_G)$ e função ponderação d.