ELEMENTOS DE MATEMÁTICA

Pedro G. Mattos

ATENÇÃO

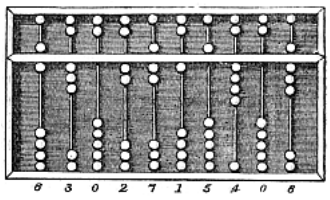
ESTE LIVRO NÃO ESTÁ TERMINADO.
O PROJETO AINDA ESTÁ EM EXECUÇÃO E NÃO HÁ DATA PREVISTA PARA TÉRMINO.

Elementos de Matemática

Pedro G. Mattos

Elementos de Matemática

Uma introdução a Conjuntos, Álgebra, Topologia, Análise e Geometria



Livros & Liberdade

Pedro G. Mattos
pedrogmattos@openmailbox.org
Campinas, SP, Brasil

Arte da capa: *Scuola di Atene* (1511), Raffaello Sanzio.

Versão 0.2.0. Última revisão em 30 de julho de 2017.

Sumário

Parte I

Conjuntos

Capítulo 1

Os Axiomas e as Contruções Essenciais

Conjunto, Pertencimento e os Símbolos da Lógica Formal

A noção de um *conjunto* é uma noção primitiva na matemática. Intuitivamente, um conjunto é um objeto que tem *elementos*. Cada elemento tem para com o conjunto em que está a relação de *pertencimento*. Abstraindo mais essa noção, pensamos que todas as propriedades de um conjunto se resumem aos elementos que a ele pertencem, de modo que um conjunto é, de fato, seus elementos. A *Teoria de Conjuntos* é uma teoria da lógica formal que procura formalizar essas ideias e estudar suas consequências. Neste livro, o tratamento da teoria de conjuntos será um tratamento informal, embora muita ênfase seja dada nos axiomas que constituem uma base para a teoria de conjuntos.

A lógica formal estuda sentenças formadas a partir de símbolos pré-determinados e fixos e as regras que dizem como essas sentenças se relacionam para formar novas sentenças. No tratamento formal da teoria de conjuntos, não há distinção entre conjunto e elemento. Ambos são somente denotados por letras de um alfabeto específico, e a relação de pertencimento é geralmente denotada pelo o símbolo $\in$. Se X e Y são conjuntos, a sentença "o conjunto X pertence ao conjunto Y" ou "o conjunto X é elemento do conjunto Y" é denotada por

$$X \in Y.$$

Para afirmar que um conjunto X não é elemento de um conjunto Y, ou seja, negar $X \in Y$, o símbolo usado é $\notin$ e se denota $X \notin Y$.

As teorias da lógica formal costumam ter axiomas, sentenças assumidas válidas a partir das quais deve-se inferir todas as outras sentenças da teoria. Axiomas, neste livro, serão enunciados, não como sentenças simbólicas, mas como sentenças em português. No entanto, alguns símbolos lógicos frequentemente facilitam e

deixam mais claros os enunciados de sentenças na matemática. Os símbolos

$$\forall \qquad \exists$$

serão usados para substituirem as expressões "para todo" e "existe", respectivamente (desconsiderando possíveis flexões gramaticais). Eles indicam que alguma propriedade vale para todo elemento de um conjunto ou que existem elementos do conjunto para o qual a propriedade vale. O símbolo $\exists!$ significa que existe e é único e o símbolo $\nexists$ que não existe. Além desses, serão usados também os símbolos

$$\Longrightarrow \qquad \Longleftarrow \qquad \Longleftrightarrow$$

para significar a implicação material em cada sentido e a equivalência lógica. Por fim, para os conectivos 'e' e 'ou' são usados os símbolos

$$\text{e} \qquad \text{ou}$$

Esse conectivos indicam, informalmente, que sentenças são ambas verdadeiras, no caso de 'e', ou ao menos uma das duas é, no caso de 'ou'. Os parênteses, que são comumente usados na lógica formal, serao substituidos por espaços, de modo que não haja ambiguidade. Mais detalhes sobre lógica formal e o uso dos símbolos lógicos serão suprimidos. Para aprofundamento em lógica e sistemas dedutivos, um livro indicado é *Introduction to Logic*, de Alfred Tarski.

1.1 Axiomas do Vazio, da Extensão e das Partes

Os conceitos definidos nesta seção são *igualdade* e *contenção* de conjuntos. O primeiro axioma a ser considerado é o que define que existe um conjunto sem nenhum elemento, o *conjunto vazio*. Esse conjunto tem um papel semelhante ao número zero. Ele é, de certo modo, um "objeto neutro" na teoria de conjuntos. Ao decorrer do desenvolvimento da teoria, essa frase sem significado matemática de fato ganhará um significado intuitivo e, em vários casos, uma definição mais precisa.

Axioma 1 (Vazio)**.** Existe o *conjunto vazio*, um conjunto que não possui elementos. Denota-se esse conjunto por $\emptyset$.

Formalmente, o axioma é $\exists x \forall y (y \notin x)$ e um conjunto vazio é um conjunto x que satisfaz $\forall y (y \notin x)$. Como o conjunto vazio não possui elementos, sempre que se conclui que existe um elemento em $\emptyset$, ou seja, que existe $x \in \emptyset$, chega-se em uma contradição e a conclusão é que o que se assumiu para chegar na contradição é falso. Essa é uma forma padrão de se demonstrarem diversas proposições na lógica e na matemática.

O segundo axioma considerado é um axioma baseado em uma dos primeiras propriedades de um conjunto quando pensado intuitivamente: a ideia de que, quando abtrai-se da realidade, um conjunto é totalmente definido pelos elementos a que ele pertencem. Esse axioma se chama axioma da extensão e é a definição de *igualdade* entre conjuntos.

Axioma 2 (Extensão)**.** Sejam X e Y conjuntos. Os conjuntos X e Y são *iguais* se, e somente se,

$$\forall x \in X \; x \in Y \quad \text{e} \quad \forall y \in Y \; y \in X.$$

Denota-se $X = Y$. Caso contrário, denota-se $X \neq Y$.

Formalmente, o axioma é $\forall x \forall y (x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y))$. Quando se consideram conjuntos, é muito útil falar apenas de alguns de seus elementos, um conjunto desses elementos, possivelmente com alguma propriedade específica. Essa noção é a de um subconjunto, um conjunto cujos elementos pertencem todos a um outro conjunto considerado anteriormente. A definição de um subconjunto pode ser dada simplesmente a partir das noções primitivas já fornecidas, pois na ideia de subconjunto só são necessárias as noções de conunto e pertencimento, além dos símbolos lógicos.

Definição 1.1. Seja X um conjunto. Um *subconjunto* (ou uma *parte*) de X é um conjunto Y que satisfaz

$$\forall y \in Y \quad y \in X.$$

Denota-se $Y \subseteq X$. Caso contrário, denota-se $Y \nsubseteq X$. Um subconjunto *próprio* de X é um subconjunto $Y \subseteq X$ tal que $Y \neq X$. Denota-se $Y \subset X$.

Formalmente, a definição é $\forall x \forall y (x \subseteq y \leftrightarrow \forall z (z \in x \rightarrow z \in y))$.

Proposição 1.1. *Seja X um conjunto. Então*

1. $\emptyset \subseteq X$;
2. $X \subseteq \emptyset \implies X = \emptyset$.

Demonstração. Suponha que $\emptyset$ não é subconjunto de X. Então existe $e \in \emptyset$ tal que $e \notin X$. Mas $e \in \emptyset$ é um absurdo, o que mostra que $\emptyset \subseteq X$. ■

O próximo axioma considerado é o que garante que os subconjuntos de um conjunto dado formam um conjunto.

Axioma 3 (Partes)**.** Seja X um conjunto. Então existe o *conjunto das partes* de X, o conjunto que contém todos os subconjuntos de X. Denota-se $\mathcal{P}(X)$.

Proposição 1.2. *Sejam X e Y conjuntos. Então*

$$X \subseteq Y \implies \mathcal{P}(X) \subseteq \mathcal{P}(Y).$$

1.2 Axiomas da Especificação e do Par

A noção intuitiva de subconjunto está diretamente relacionada à ideia de formar, a partir de um conjunto e uma propriedade, o subconjunto dos elementos que têm essa propriedade. A existência desse subconjunto é um axioma, chamado axioma da especificação porque a propriedade dada é um especificação dos elementos do conjunto original.

Axioma 4 (Especificação)**.** Sejam X um conjunto e $\phi(x)$ uma sentença lógica. Existe o conjunto dos elementos de X que satisfazem $\phi(x)$. Denota-se

$$\{x \in X \mid \phi(x)\}.$$

O próximo axioma garante, a partir da existência de dois, a existência de um novo conjunto cujos elementos são os dois conjuntos iniciais. Esse é o axioma do par. Embora a princípio sua necessidade não seja óbvia, esse axioma é importante — ao menos útil — para o desenvolvimento da teoria de conjuntos.

Axioma 5 (Par)**.** Sejam X e Y conjuntos. Existe o *par* de X e Y, o conjunto que tem como únicos elementos X e Y. Denota-se $\{X, Y\}$.

A partir do axioma do par pode-se formar o conjunto que tem como único elemento um conjunto X formando o par de X e X. Esse conjunto é o conjunto unitário com único elemento X.

Definição 1.2. Seja X um conjunto. O *conjunto unitário* de elemento X é o conjunto $\{X, X\}$. Denota-se $\{X\}$.

1.3 Axioma da União

Nesta seção são apresentadas duas das contruções mais importantes da teoria de conjutos: a união e a interseção. A união de um conjunto de conjuntos denotado C é o conjunto cujos elementos pertencem a algum conjunto que pertence C. O axioma da união afirma que esse conjunto existe.

Axioma 6 (União)**.** Seja C um conjunto. Existe a *união* de C, o conjunto dos elementos que pertencem a algum elemento de C. Denota-se $\bigcup C$. A união de um par $\{X, Y\}$ é denotada $X \cup Y$.

Pode-se denotar a conjunto $\bigcup C$ por $\{x \mid \exists X \in C \quad x \in X\}$.

Proposição 1.3. *Sejam X e Y conjuntos. Então*

1. $\bigcup \emptyset = \emptyset$;

2. $X \subseteq Y \implies \bigcup X \subseteq \bigcup Y$.

Demonstração. 1. Suponha que $x \in \bigcup \emptyset$. Então $\exists X \in \emptyset$ tal que $x \in X$, o que é absurdo porque não pode existir $X \in \emptyset$.

2. Seja $x \in \bigcup X$. Então existe $C \in X$ tal que $x \in C$. Como $X \subseteq Y$, segue que $C \in Y$, portanto $x \in \bigcup Y$.

■

A interseção de um conjunto não vazio de conjuntos denotado C é o conjunto cujos elementos pertencem a todos conjuntos que pertencem C. O conjunto interseção existe por consequêcia do axioma da especificação. Como C é não vazio, basta considerar um conjunto $X \in C$ e a sentença lógica dada por

$$\forall Y \in C \quad x \in Y.$$

Desse modo, o conjunto interseção é $\{x \in X \mid \forall Y \in C \quad x \in Y\}$.

Definição 1.3. Seja C um conjunto não vazio. A *interseção* de C é o conjunto dos elementos que pertecem a todos elementos de C. Denota-se $\bigcap C$. A interseção de um par $\{X, Y\}$ é denotada $X \cap Y$.

Pode-se denotar a conjunto $\bigcap C$ por $\{x \mid \forall X \in C \quad x \in X\}$.

Proposição 1.4. *Seja C um conjunto não vazio. Então*

$$\forall X \in C \qquad \bigcap C \subseteq X \subseteq \bigcup C.$$

1.4 Axioma da Escolha

Para que o axioma da escolha seja compreensível, deve-se definir alguns conceitos antes. Essencialmente, o axioma da escolha é sobre produto de conjuntos e sobre funções. O nome escolha, de fato, vem de uma função, a função escolha. Para definir o conceito de função, é necessário primeiro definir o que é um par ordenado de elementos de dois conjuntos e o que é o conjunto de pares ordenados desses conjunto, que é chamado produto dos conjuntos. A partir desse produto de dois conjuntos, definem-se função e, a partir de função, define-se o produto de qualquer conjunto.

Pares Ordenados, Produto de Par e Função

Definição 1.4. Sejam X e Y conjuntos. O *par ordenado* com *primeira coordenada* X e *segunda coordenada* Y é o conjunto

$$(X,Y) \coloneqq \{\{X\},\{X,Y\}\} \in \mathcal{P}\left(\mathcal{P}\left(X \cup Y\right)\right).$$

Proposição 1.5. *Sejam X, Y, Z e W conjuntos. Então*

$$(X,Y) = (Z,W) \iff X = Z \text{ e } Y = W.$$

Definição 1.5. Sejam X e Y conjuntos. O *produto* de X por Y é o conjunto

$$X \times Y \coloneqq \left\{(x,y) \in \mathcal{P}\left(\mathcal{P}\left(X \cup Y\right)\right) \;\middle|\; x \in X \text{ e } y \in Y\right\}.$$

A existência desse conjunto depende da união de pares, do conjunto das partes e do axioma de especificação.

Definição 1.6. Sejam X e Y conjuntos. Uma *função* de X para Y é um conjunto $f \subseteq X \times Y$ que satisfaz

$$\forall x \in X \; \exists! y \in Y \qquad (x,y) \in f.$$

Esse y é a *imagem* de x, denotada por $f(x)$. Denotam-se $f : X \to Y$ e $f(x) \coloneqq y$. Para qualquer conjunto $K \subseteq X$, defini-se a *imagem* de K

$$f(K) = \{y \in Y \mid \exists k \in K \quad y = f(k)\},$$

que é subconjunto de Y. Diz-se que o conjunto $f(X)$ é a *imagem* de f.

Proposição 1.6. *Seja $f : A \to B$.*

1. $A = \emptyset \iff f = \emptyset$.
2. $B = \emptyset \implies A = \emptyset$.

Demonstração. 1. Suponhamos que $A = \emptyset$. Primeiro, notemos que $f = \emptyset$ é uma função de $\emptyset$ em B. Claramente, $f = \emptyset \subseteq \emptyset \times B$. Ainda, se f não fosse função de $\emptyset$ em B, existiria $a \in \emptyset$ tal que não existe único $b \in B$ satisfazendo $(a,b) \in f$. Mas existir $a \in \emptyset$ é um absurdo. Logo f é função. Por fim, se $g : \emptyset \times B$ é uma função, como $\emptyset \times B = \emptyset$, então $g \subseteq \emptyset \times B = \emptyset$, logo $g = \emptyset = f$.

Reciprocamente, suponhamos $f = \emptyset$. Se $A \neq \emptyset$, seja $a \in A$. Como f é função, existe $b \in B$ tal que $(a,b) \in f = \emptyset$, o que é absurdo. Portanto $A = \emptyset$.

2. Suponhamos que $A \neq \emptyset$. Então existe $a \in A$ e, como f é função, existe único $b \in \emptyset$ tal que $(a,b) \in f$. Mas $b \in \emptyset$ é absurdo, o que mostra que $A = \emptyset$.

■

O Axioma da Escolha e Produto de Conjuntos

Definição 1.7. Seja C um conjunto. O *produto* de C é o conjunto

$$\prod C \coloneqq \left\{ f : C \to \bigcup C \;\middle|\; \forall X \in C \quad f(X) \in X \right\}.$$

$$\prod C \coloneqq \left\{ f \in \left(\bigcup C\right)^C \;\middle|\; \forall X \in C \quad f(X) \in X \right\}.$$

Proposição 1.7. *Seja C um conjunto. Então*

1. $C = \emptyset \implies \prod C = \{\emptyset\}$;
2. $\emptyset \in C \implies \prod C = \emptyset$.

Demonstração.

1. Como $C = \emptyset$, então $\bigcup \emptyset = \emptyset$. A função $\emptyset : \emptyset \to \emptyset$ é uma função em $\prod C$, pois satisfaz por vacuidade que $\forall X \in C \quad f(X) \in X$. Se não satisfizesse, existiria $X \in \emptyset$ tal que $f(X) \notin X$, o que é contradição. Isso mostra que $\emptyset \in \prod \emptyset$. Agora, seja $f \in \prod \emptyset$ função de $\emptyset$ em $\emptyset$. Como o domínio de f é $\emptyset$, segue que $f = \emptyset$.

2. Suponha que existe $f \in \prod C$. Então $f : C \to \bigcup C$ satisfaz que $\forall X \in C \quad f(X) \in X$. Como $\emptyset \in C$, existe $f(\emptyset) \in \bigcup C$ e, pela propriedade, $f(\emptyset) \in \emptyset$, contradição. Portanto $\prod C = \emptyset$.

■

Axioma 7 (Escolha)**.** Seja C um conjunto tal que $\emptyset \notin C$. Então $\prod C \neq \emptyset$.

1.5 Axiomas do Infinito e da Fundação

Definição 1.8. Seja X um conjunto. O *sucessor* de X é o conjunto

$$X^+ \coloneqq X \cup \{X\}.$$

Axioma 8. Existe um *conjunto indutivo*, um conjunto que contém $\emptyset$ e contém o sucessor de cada um de seus elementos.

Proposição 1.8. *Seja I um conjunto indutivo e C o conjunto dos subconjuntos de I que são indutivos. Então $\bigcap C$ é um conjunto indutivo.*

1.6 Axioma da Substituição

Os axiomas da especificação e do par são consequência do axioma da substituição.

Propriedades Gerais

Contenção

Proposição 1.9. *Sejam X, Y e Z conjuntos. Então*

1. $X \subseteq X$;
2. $X \subseteq Y \ \ e \ \ Y \subseteq X \iff X = Y$;
3. $X \subseteq Y \ \ e \ \ Y \subseteq Z \implies X \subseteq Z$.

Demonstração. 1. Se $X = \emptyset$, então $\emptyset \subseteq X = \emptyset$. Logo $X \subseteq X$. Caso contrário, seja $x \in X$. Então $x \in X$. Logo $X \subseteq X$.

2. $X \subseteq Y$ e $Y \subseteq X$ se, e somente se, $\forall x \in X \ x \in Y$ e $\forall y \in Y \ y \in X$, o que é equivalente a $X = Y$ pelo axioma da extensão.

3. Se $X = \emptyset$, então $X \subseteq Z$. Caso contrário, seja $x \in X$. Então, como $X \subseteq Y$, $x \in Y$ e, como $Y \subseteq Z$, $x \in Z$. Logo $X \subseteq Z$.

■

União e Interseção

Proposição 1.10. *Sejam X, Y e Z conjuntos. Então*

1. $X \cup \emptyset = X$;
2. $X \cup Y = Y \cup X$;
3. $(X \cup Y) \cup Z = X \cup (Y \cup Z)$;
4. $X \cup X = X$;
5. $X \subseteq Y \iff X \cup Y = Y$.

Proposição 1.11. *Sejam X, Y e Z conjuntos. Então*

1. $X \cap \emptyset = \emptyset$;
2. $X \cap Y = Y \cap X$;
3. $(X \cap Y) \cap Z = X \cap (Y \cap Z)$;
4. $X \cap X = X$;
5. $X \subseteq Y \iff X \cap Y = X$.

Proposição 1.12. *Sejam X, Y e Z conjuntos. Então*

1. $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$;
2. $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$.

Capítulo 2

Famílias e Propriedades de Conjuntos

2.1 Famílias e Indexações

Os axiomas já foram todos enunciados no capítulo anterior e as bases da teoria de conjuntos clássica está construída. Sendo assim, é necessário mudar a linguagem com que muitas das operações sobre conjuntos são tratadas, entre elas a união, a interseção e o produto. O conceito de uma família será definido nesta seção. Embora inicialmente a notação do capítulo anterior seja mais simples, eventualmente a notação de famílias com índices será necessária, por dois motivos principais. O primeiro é que esse conceito facilitará muito os enunciados de várias propriedades e teoremas na matemática eventualmente. O segundo é que tradicionalmente os matemáticos usam famílias e índices para denotar uniões, interseções, produtos e muitas outras noções. A ideia básica de uma família é a seguinte. Quando se define a união de um conjunto C na teoria de conjuntos, a ideia intuitiva por trás da definição é que se estão unindo os conjuntos que são elementos de C. A união de um par $\{X, Y\}$ é denotada $X \cup Y$ não por acaso, essa notação indica um conjunto que está sendo formado com os elementos de X e Y, não com os elementos dos elementos de C, como no caso de $\bigcup C$.

Generalizando essa ideia, a união de três conjuntos X_1, X_2, X_3 pode ser denotada $X_1 \cup X_2 \cup X_3$ e o mesmo pode ser feito para qualquer quantidade finita de conjuntos. Mas para fazer o mesmo para uma quantidade qualquer de conjuntos, não é possível escrever esses conjuntos numa lista. Por isso surgiu a ideia de *indexar* os conjuntos de C que se pretende unir, usando a notação $(X_i)_{i \in I}$, sendo que cada X_i é um elemento de C e i seu índice. Em seguida, indica-se na parte inferior do símbolo de união que os conjuntos indexados estão sendo unidos, de modo que

$\bigcup C$ é denotado

$$\bigcup_{i \in C} X_i.$$

Essa notação tem a vantagem de estar mais próxima da intuição e também permite trabalhar com duplas uniões mais facilmente. As mesmas ideias são aplicadas para interseções e produtos. No entanto, ainda resta um problema, o problema principal. Tendo já especificada qual é a notação que pretende-se aplicar, ainda falta definir o que é uma família somente a partir dos conceitos da teoria de conjuntos. Essa definição vem a seguir.

Definição 2.1. Sejam C e I conjuntos não vazios. Uma *família* de elementos de X indexados por I é uma função $F : I \to C$. O conjunto I é o *conjunto de índices* da família. Denota-se isso por

$$(F_i)_{i \in I} \subseteq C$$

e a imagem de $i \in I$ por F é denotada F_i e chamada de *i-ésimo membro* da família. Uma *sequência* é uma família em que $I = \mathbb{N}$, e uma *sequência finita* é uma família em que $I \in \mathbb{N}$ (ou seja, $I = \{0, \ldots, n\}$ para algum $n \in \mathbb{N}$, e nesse caso diz-se n-sequência).

Vale notar que uma família é vazia se, e somente se, $I = \emptyset$. Uma família é uma função e, portanto, quando se afirma que uma família, afirma-se que uma função é vazia, ou que é a função vazia. Mas isso ocorre se, e somente se, seu domínio, no caso o conjunto de índices, é vazio.

Definição 2.2. Seja X um conjunto não vazio. Uma *indexação* de X é uma família bijetiva $(x_i)_{i \in I}$ de elementos de X. Nesse caso, X é um conjunto indexado por I e denota-se $X = \{x_i\}_{i \in I}$.

A noção de uma família é, de fato, mais motivada por notação do que por um conceito teórico, já que uma família é simplesmennte uma função sem nenhuma restrição além disso, e a única diferença entre uma família é uma função é o contexto de utilização. Uma pergunta relevante, ainda, é se todo conjunto pode ser indexado por meio de uma família. Essa pergunta tem uma resposta óbvia e uma não óbvia, e ambas afirmam que sim. A resposta óbvia é que, para se indexar um conjunto C basta considerar a função $F : C \to C$ definida para todo $X \in C$ por $F(X) = X$. Desse modo, essa é uma indexação do conjunto X. Mas essa resposta não satisfaz a tradição de indexar um quantidade finita de conjuntos $\{X, Y\}$ com números naturais. A resposta menos óbvia é que todo conjunto pode ser bem ordenado e, dessa forma, existe uma função de um número ordinal para o conjunto, logo uma indexação desse conjunto por um número ordinal. Os números naturais são os números ordinais finitos, o que significa que essa resposta menos óbvia condiz com a idexação que se faz usualmente de uma quantidade finita de conjuntos. Esse tópicos, no entanto, não serão abordados nesse capítulo.

2.2 Propriedades de União e Interseção

A partir da definição de família, pode-se definir a união e a interseção de uma família de conjuntos a partir da imagem do conjunto de índices I pela função C, o conjunto $C(I) = \{C_i \mid i \in I\}$. No entanto, um problema teórico se manifesta para se definir uma família de conjuntos. Se uma família é uma função de um conjunto de índices em um conjunto de elementos, para se definir uma família de conjuntos deveria existir um conjunto de todos conjuntos para fazer o papel de contradomínio de uma família. Esse conjunto, no entanto, não existe na teoria de conjuntos abordada neste livro, o que sugere que a definição de uma família de conjuntos depende, de fato, de um conjunto cujos elementos são os conjuntos da família de conjuntos. A existência desse conjunto de conjuntos é suposta, mas ele não é o conjunto de todos os conjuntos. Sendo assim, sempre que se enunciar uma família de conjuntos, essas ressalvas serão assumidas.

Definição 2.3. A *união* de uma família $(C_i)_{i\in I}$ é o conjunto

$$\bigcup_{i\in I} C_i \coloneqq \bigcup C(I).$$

A *interseção* de uma família não vazia $(C_i)_{i\in I}$ é o conjunto

$$\bigcap_{i\in I} C_i \coloneqq \bigcap C(I).$$

Quando I for finito, pode-se denotar

$$C_1 \cup \cdots \cup C_n \coloneqq \bigcup_{i\in I} C_i \qquad \text{e} \qquad C_1 \cap \cdots \cap C_n \coloneqq \bigcap_{i\in I} C_i.$$

Proposição 2.1. *Seja $(C_i)_{i\in I}$ uma família de conjuntos. Então*

1. $\forall i \in I \quad C_i = \emptyset \qquad \Leftrightarrow \qquad \bigcup_{i\in I} C_i = \emptyset.$
2. $\exists i \in I \quad C_i = \emptyset \qquad \Rightarrow \qquad \bigcap_{i\in I} C_i = \emptyset.$

Proposição 2.2. *Seja $(C_i)_{i\in I}$ uma família não vazia de conjuntos. Então*

1. $\left(\bigcap_{i\in I} C_i\right)^{\complement} = \bigcup_{i\in I} (C_i)^{\complement}$
2. $\left(\bigcup_{i\in I} C_i\right)^{\complement} = \bigcap_{i\in I} (C_i)^{\complement}$

Demonstração. 1. Para isso, basta notar que $c \in \left(\bigcap_{i\in I} C_i\right)^{\complement}$ se, e somente se, $c \notin \bigcap_{i\in I} C_i$. Mas isso ocorre se, e somente se, existe $i \in I$ tal que $c \notin C_i$. Essa afirmação é equivalente a $c \in (C_i)^{\complement}$ que, por sua vez, é equivalente a $c \in \bigcup_{i\in I}(C_i)^{\complement}$.

2. Como, para todo conjunto C, $(C^{\complement})^{\complement} = C$, segue do item anterior que

$$\left(\bigcup_{i\in I} C_i\right)^{\complement} = \left(\bigcup_{i\in I}((C_i)^{\complement})^{\complement}\right)^{\complement} = \left(\left(\bigcap_{i\in I}(C_i)^{\complement}\right)^{\complement}\right)^{\complement} = \bigcap_{i\in I}(C_i)^{\complement}.$$

■

Proposição 2.3. *Seja (C_{ij}) uma família não vazia de conjuntos. Então*

$$\bigcup_{i\in I}\left(\bigcap_{j\in J} C_{ij}\right) \subseteq \bigcap_{j\in J}\left(\bigcup_{i\in I} C_{ij}\right)$$

Proposição 2.4. *Seja (C_{ij}) uma família não vazia de conjuntos. Então*

1. $\bigcap_{i\in I} \mathcal{P}(C_i) = \mathcal{P}\left(\bigcap_{i\in I} C_i\right)$;
2. $\bigcup_{i\in I} \mathcal{P}(C_i) \subseteq \mathcal{P}\left(\bigcup_{i\in I} C_i\right)$.

2.3 Produto de Conjuntos

Definição 2.4. Seja $(C_i)_{i\in I}$ uma família de conjuntos. O *produto* de $(C_i)_{i\in I}$ é o conjunto

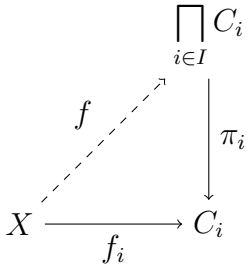
$$\prod_{i\in I} C_i \coloneqq \{(c_i)_{i\in I} \mid \forall i \in I \quad c_i \in C_i\}.$$

As famílias $(c_i)_{i\in I}$ são de elementos em $\bigcup_{i\in I} C_i$.

Definição 2.5. Seja $(C_i)_{i\in I}$ uma família de conjuntos e $i \in I$. A *projeção canônica* de $\prod_{i\in I} C_i$ em C_i é a função

$$\begin{aligned} \pi_i : \prod_{i\in I} C_i &\to C_i \\ (c_i)_{i\in I} &\mapsto c_i. \end{aligned}$$

Proposição 2.5 (Propriedade Universal)**.** *Sejam $(C_i)_{i\in I}$ uma família de conjuntos, X um conjunto e, para todo $i \in I$, $f_i : X \to C_i$ uma função. Então existe única função $f : X \to \prod_{i\in I} C_i$ tal que, para todo $i \in I$, $\pi_i \circ f = f_i$ (o diagrama comuta).*



Demonstração. Defina a função

$$\begin{aligned} f : X &\to \prod_{i\in I} C_i \\ x &\mapsto (f_i(x))_{i\in I}. \end{aligned}$$

Para todo $x \in X$ e para todo $i \in I$,

$$\pi_i \circ f(x) = \pi_i(f(x)) = \pi_i((f_i(x))_{i\in I}) = f_i(x).$$

Portanto $\pi_i \circ f = f_i$. Isso mostra a existência da f. Para a unicidade, seja $\overline{f} : X \to \prod_{i\in I} C_i$ função tal que, para todo $i \in I$, $\pi_i \circ \overline{f} = f_i$. Seja $x \in X$. Como $\overline{f}(x) \in \prod_{i\in I} C_i$, $\overline{f}(x) = (x_i)_{i\in I}$. Da propriedade comutativa de $\overline{f}$, segue que, para todo $i \in I$,

$$x_i = \pi_i \circ \overline{f}(x) = f_i(x).$$

Como $f(x) = (f_i(x))_{i\in I}$, isso mostra que $\overline{f}(x) = f(x)$. Portanto $\overline{f} = f$. ∎

2.4 Coproduto de Conjuntos

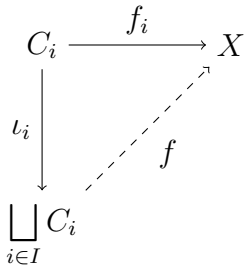
Definição 2.6. Seja $(C_i)_{i\in I}$ uma família não vazia de conjuntos. O *coproduto* de $(C_i)_{i\in I}$ é o conjunto

$$\bigsqcup_{i\in I} C_i \coloneqq \{(i,c) \mid i \in I \text{ e } c \in C_i\}.$$

Definição 2.7. Seja $(C_i)_{i\in I}$ uma família de conjuntos e $i \in I$. A *inclusão canônica* de C_i em $\bigsqcup_{i\in I} C_i$ é a função

$$\begin{aligned} \iota_i : C_i &\to \bigsqcup_{i\in I} C_i \\ c &\mapsto (i,c). \end{aligned}$$

Proposição 2.6 (Propriedade Universal)**.** *Sejam $(C_i)_{i\in I}$ uma família de conjuntos, X um conjunto e, para todo $i \in I$, $f_i : C_i \to X$ uma função. Então existe única função $f : \bigsqcup_{i\in I} C_i \to X$ tal que, para todo $i \in I$, $f \circ \iota_i = f_i$ (o diagrama comuta).*



Demonstração. Defina a função

$$\begin{aligned} f : \bigsqcup_{i\in I} C_i &\to X \\ (i,c) &\mapsto f_i(c). \end{aligned}$$

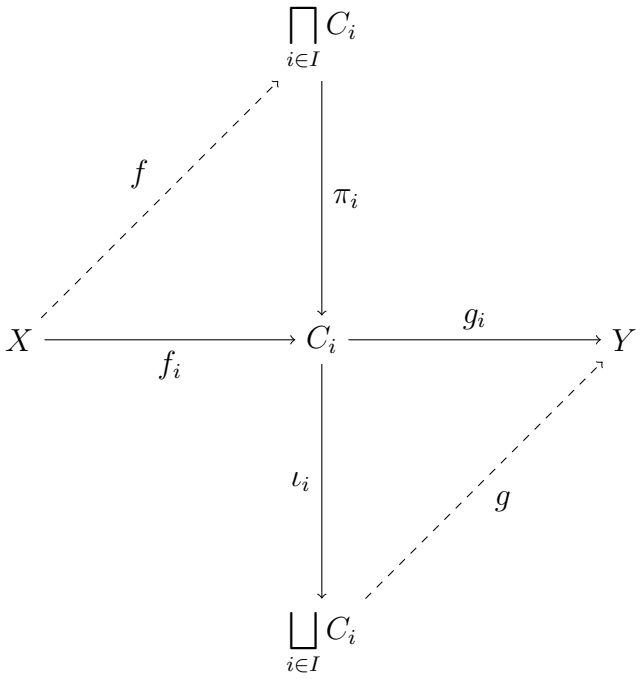
Seja $i \in I$ e $c \in C_i$. Então

$$f \circ \iota_i(c) = f(\iota_i(c)) = f(i,c) = f_i(c).$$

Portanto $f \circ \iota_i = f_i$. Isso mostra a existência da f. Para a unicidade, seja $\overline{f} : \bigsqcup_{i\in I} C_i \to X$ função tal que, para todo $i \in I$, $\overline{f} \circ \iota_i = f_i$. Seja $x \in \bigsqcup_{i\in I} C_i$. Existem $i \in I$ e $c \in C_i$ tais que $x = (i,c)$. Da propriedade comutativa de $\overline{f}$, segue que

$$\overline{f}(x) = \overline{f}(i,c) = \overline{f}(\iota_i(x)) = \overline{f} \circ \iota_i(c) = f_i(c) = f(i,c) = f(x).$$

Isso mostra que $\overline{f} = f$. ■



Os diagramas comutativos do
produto e do coproduto de conjuntos.

Propriedades Gerais

Proposição 2.7. *Seja $(C_{ij})_{(i,j)\in I\times J}$ uma família de conjuntos. Então*

1. $\bigcup_{j\in J}\left(\bigcap_{i\in I} C_{ij}\right) \subseteq \bigcap_{i\in I}\left(\bigcup_{j\in J} C_{ij}\right)$;

2. $\bigcap_{j\in J}\left(\bigcap_{i\in I} C_{ij}\right) = \bigcap_{i\in I}\left(\bigcap_{j\in J} C_{ij}\right)$.

Demonstração. 1.

$$\begin{aligned} c \in \bigcup_{j\in J}\left(\bigcap_{i\in I} C_{ij}\right) &\Rightarrow \exists j \in J \qquad c \in \bigcap_{i\in I} C_{ij} \\ &\Rightarrow \exists j \in J\ \forall i \in I \qquad c_i \in C_{ij} \\ &\Rightarrow \forall i \in I \qquad c \in \bigcup_{j\in J} C_{ij} \\ &\Rightarrow c \in \bigcap_{i\in I}\left(\bigcup_{j\in J} C_{ij}\right). \end{aligned}$$

2.

$$\begin{aligned} c \in \bigcap_{j\in J}\left(\bigcap_{i\in I} C_{ij}\right) &\Leftrightarrow \forall j \in J \qquad c \in \bigcap_{i\in I} C_{ij} \\ &\Leftrightarrow \forall j \in J\ \forall i \in I \qquad c_i \in C_{ij} \\ &\Leftrightarrow \forall i \in I\ \forall j \in J \qquad c_i \in C_{ij} \\ &\Leftrightarrow \forall i \in I \qquad c_i \in \bigcup_{j\in J} C_{ij} \\ &\Leftrightarrow c \in \bigcap_{i\in I}\left(\bigcap_{j\in J} C_{ij}\right). \end{aligned}$$

■

Notemos que a inclusão contrária no primeiro item nao vale. Suponhamos que para um $j_0 \in J$, todos os C_{ij_0} são vazios, mas para todos outros $j \in J$, os C_{ij} não são vazios. Então o produto desses C_{ij} será sempre vazio, pois sempre tem um dos elementos do produto vazio, e então a união desses produtos será vazia; no entanto, a união desses C_{ij} não será nenhuma vazia e, então, o produto não seráa vazio (pelo axioma da escolha).

Proposição 2.8. *Sejam C_i conjuntos*

$$f^{-1}\left(\prod_{i\in I} C_i\right) = \bigcap f_i^{-1}(C_i).$$

Capítulo 3

Relações e Funções

3.1 Relações

Definição 3.1. Sejam X e Y conjuntos. Uma *relação* R de X para Y é um subconjunto de $X \times Y$. Os conjuntos X e Y são, respectivamente, o *domínio* e o *contradomínio* de R. Denota-se $x\ R\ y$ para $(x, y) \in R$.

Definição 3.2. Seja R uma relação de X em Y. A *relação inversa* de R é a relação R^{-1} de Y em X definida por

$$\forall x \in X\ \forall y \in Y \qquad x\ R\ y \Leftrightarrow y\ R^{-1}\ x.$$

3.2 Funções

Definição 3.3. Sejam X e Y conjuntos. Uma *função* de X para Y é uma relação f de X para Y que satisfaz

$$\forall x \in X\ \exists! y \in Y \qquad (x, y) \in f.$$

Esse y é a *imagem* de x. Denotam-se $y = f(x)$ e

$$\begin{aligned} f : X &\to Y \\ x &\mapsto f(y) \end{aligned}$$

Para qualquer conjunto $K \subseteq X$, definimos a *imagem* de K

$$f(K) = \{y \in Y \mid \exists k \in K \quad y = f(k)\},$$

que é subconjunto de Y. Diz-se que o conjunto $f(X)$ é a *imagem* de f.

Proposição 3.1. *Seja $f : A \to B$.*

1. *$A = \emptyset$ se, e somente se, $f = \emptyset$.*

2. *Se $B = \emptyset$, então $A = \emptyset$.*

Demonstração. 1. Suponhamos que $A = \emptyset$. Primeiro, notemos que $f = \emptyset$ é uma função de $\emptyset$ em B. Claramente, $f = \emptyset \subseteq \emptyset \times B$. Ainda, se f não fosse função de $\emptyset$ em B, existiria $a \in \emptyset$ tal que não existe único $b \in B$ satisfazendo $(a, b) \in f$. Mas existir $a \in \emptyset$ é um absurdo. Logo f é função. Por fim, se $g : \emptyset \times B$ é uma função, como $\emptyset \times B = \emptyset$, então $g \subseteq \emptyset \times B = \emptyset$, logo $g = \emptyset = f$.

   Reciprocamente, suponhamos $f = \emptyset$. Se $A \neq \emptyset$, seja $a \in A$. Como f é função, existe $b \in B$ tal que $(a, b) \in f = \emptyset$, o que é absurdo. Portanto $A = \emptyset$.

2. Suponhamos que $A \neq \emptyset$. Então existe $a \in A$ e, como f é função, existe único $b \in \emptyset$ tal que $(a, b) \in f$. Mas $b \in \emptyset$ é absurdo, o que mostra que $A = \emptyset$.

■

Proposição 3.2. *Sejam $f : A \to B$ e $g : A' \to B'$. Então $f = g$ se, e somente se, $A = A'$ e, para todo $a \in A$, $f(a) = g(a)$.*

Demonstração. Suponhamos que $f = g$. Se $A = \emptyset$, então $f = \emptyset$ e $g = f = \emptyset$, o que implica $A' = \emptyset$. Ainda, para todo $a \in A$, $f(a) = g(a)$ pois, se isso fosse falso, existiria $a \in \emptyset$ tal que $f(a) \neq g(a)$, mas existir $a \in \emptyset$ é absurdo. Se $A \neq \emptyset$, seja $a \in A$. Então existe $b \in B$ tal que $(a, b) \in f$ e, como $f = g$, $(a, b) \in g$. Isso implica $a \in A'$ e concluímos que $A \subseteq A'$. Por outro lado, seja $a \in A'$. Então existe $b \in B'$ tal que $(a, b) \in g$ e, como $f = g$, $(a, b) \in f$. Isso implica $a \in A$ e concluímos que $A' \subseteq A$. Portanto $A = A'$. Agora, seja $a \in A$. Então existem $f(a) \in B$ e $g(a) \in B'$. Como $(a, f(a)) \in f$ e $f = g$, então $(a, f(a)) \in g$. Como f é função, existe único $b \in B$ tal que $(a, b) \in f$, o que implica $f(a) = g(a)$.

Reciprocamente, suponhamos que $A = A'$ e que, para todo $a \in A$, $f(a) = g(a)$. Se $A = \emptyset$, então $f = \emptyset$ e $g = \emptyset$, logo $f = g$. Se $A \neq \emptyset$, então seja $p \in f$. Existe $a \in A$ tal que $p = (a, f(a))$. Como $f(a) = g(a)$, então $p = (a, g(a))$; mas $(a, g(a)) \in g$, o que implica $p \in g$ e, portanto, $f \subseteq g$. Agora, seja $p \in g$. Existe $a \in A'$ tal que $p = (a, g(a))$. Como $f(a) = g(a)$, então $p = (a, f(a))$; mas $(a, f(a)) \in f$, o que implica $p \in f$ e, portanto, $f \subseteq g$. Assim, concluímos que $f = g$. ■

Proposição 3.3. *Seja $f : A \to B$. Então $f : A \to f(A)$.*

Definição 3.4. Sejam $f : A \to B$ uma função e $A' \subseteq A$ um conjunto. A *restrição* de f a A' é a função

$$\begin{aligned} f|_{A'} : A' &\to B \\ a &\mapsto f(a). \end{aligned}$$

Proposição 3.4. *Sejam $f : A \to B$, $A' \subseteq A$ e $B' \subseteq B$. Então a restrição $f|_{A'}$ é uma função de A' em B' se, e somente se, $f(A') \subseteq B'$.*

Demonstração. Se que $f|_{A'}$ é uma função de A' em B', então o contradomínio de $f_{A'}$ é B', o que significa que, para todo $a \in A'$, $f(a) = f|_{A'}(a) \in B'$, logo $f(A') \subseteq B$. Reciprocamente, se, para todo $a \in A'$, $f(a) \in B'$, então $f|_{A'}$ é uma função de A' em B'. ■

3.2.1 Composição de Funções

Definição 3.5. Sejam $f : A \to B'$ e $g : B \to C$ funções tais que $B' \subseteq B$. A *função composta* de g com f, denotada $g \circ f$, é a função

$$\begin{aligned} g \circ f : A &\to C \\ a &\mapsto g(f(a)). \end{aligned}$$

Proposição 3.5. *Sejam $f : A \to B'$, $g : B \to C'$ e $h : C \to D$ funções tais que $B' \subseteq B$ e $C' \subseteq C$. Então*

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

Demonstração. Primeiro, notemos que $g \circ f$ é uma função de A em C', o que implica que $h \circ (g \circ f)$ é uma função de A em D. Anda, notemos que $h \circ g$ é uma função de B em D, o que implica que $(h \circ g) \circ f$ é uma função de A em D. Logo os domínios de $h \circ (g \circ f)$ e $(h \circ g) \circ f$ são iguais. Se $A = \emptyset$, então $h \circ (g \circ f) = (h \circ g) \circ f = \emptyset$. Suponhamos, então, que $A \neq \emptyset$ e seja $a \in A$. Então

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))) = (h \circ g)(f(a)) = ((h \circ g) \circ f)(a),$$

o que mostra que $h \circ (g \circ f) = (h \circ g) \circ f$. ■

Proposição 3.6. *Seja $f : A \to B$. Então*

1. *$f \circ \emptyset = \emptyset$;*
2. *$\emptyset \circ f = \emptyset$.*

Demonstração. Para a primeira igualdade, notemos que $f \circ \emptyset$ é uma função de $\emptyset$ em B e, portanto, $f \circ \emptyset = \emptyset$. Para a segunda igualdade, notemos que $\emptyset \circ f$ é uma função de A em $\emptyset$ e, portanto, $A = \emptyset$, o que é equivalente a $\emptyset \circ f = \emptyset$. ■

Definição 3.6. Seja A um conjunto não vazio. A *função identidade* em A é a função

$$\begin{aligned} id_A : A &\to A \\ a &\mapsto a. \end{aligned}$$

Proposição 3.7. *Seja $f : A \to B$ uma função. Então*

$$f \circ id_A = f \quad e \quad id_B \circ f = f.$$

Demonstração. Primeiro, notemos que $f \circ id_A$ e $id_B \circ f$ são funções de A em B e, portanto, têm o mesmo domínio de f. Se $A = \emptyset$, então $f : \emptyset \to B$ e, portanto, $f = \emptyset$. Notemos que $id_\emptyset = \emptyset$. De fato, $\emptyset$ é função e, se não fosse identidade de $\emptyset$ em $\emptyset$, existiria $a \in \emptyset$ tal que $f(a) \neq a$; mas $a \in \emptyset$ é absurdo. Assim, $f \circ id_A$ é uma função de $\emptyset$ em B e, portanto, $f \circ id_A = \emptyset = f$. Ainda, $id_B \circ f$ é uma função de $\emptyset$ em B e, portanto, $id_B \circ f = \emptyset = f$. Se $A \neq \emptyset$, seja $a \in A$. Então $(f \circ id_A)(a) = f(id_A(a)) = f(a) = id_B(f(a)) = (id_B \circ f)(a)$. ■

3.2.2 Função Inversa, Injetividade e Sobrejetividade

Definição 3.7. Seja $f : A \to B$ uma função. Uma *função inversa* de f é uma função $g : B \to A$ tal que

$$g \circ f = id_A \quad \text{e} \quad f \circ g = id_B.$$

Definição 3.8. Uma *função injetiva* (ou *injeção*) é uma função $f : A \to B$ que satisfaz

$$\forall a_1, a_2 \in A \qquad f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

Definição 3.9. Uma *função sobrejetiva* sobre um conjunto B é uma função $f : A \to B$ que satisfaz $f(A) = B$.

Definição 3.10. Sejam A e B conjunto. Uma *bijeção* entre A e B é uma função injetiva $f : A \to B$ que é sobrejetiva sobre B.

Proposição 3.8. *Seja $f : A \to B$. Então f é injetiva se, e somente se, existe $g : B \to A$ tal que $g \circ f = id_A$.*

Demonstração. Suponhamos que f é injetiva. Se $A = \emptyset$. Então $f = \emptyset$ e, portanto, tomando $g = id_B$, temos que $g \circ f = id_B \circ \emptyset = id_\emptyset = \emptyset$. Se $A \neq \emptyset$, seja $a \in A$.

■

Proposição 3.9. *Seja $f : A \to B$. Então f é sobrejetiva sobre B se, e somente se, existe $g : B \to A$ tal que $f \circ g = id_B$.*

Demonstração. Suponhamos que f é sobrejetiva sobre B. Então $B = f(A)$; ou seja, para todo $b \in B$, existe $a \in A$ tal que $f(a) = b$ e, portanto, definimos a função $g : B \to A$ para cada elemento de B como $g(b) \coloneqq a$. Assim, segue que $g \circ f = id_B$. ■

Proposição 3.10. *Seja $f : A \to B$. Se $g : B \to A$ e $g' : B \to A$ são funções inversas de f, então $g = g'$.*

Demonstração. Primeiro, notemos que os domínios de g e g' são os mesmos. Agora, se $A = \emptyset$, então $f = \emptyset$. Mas isso significa que $id_A = \emptyset$ e, como g e g' são inversas de f, segue que g (NÃO SEI SE ROLA COM A=0).

Se $A \neq \emptyset$, seja $a \in A$. Então $g \circ f = id_B$ ■

Proposição 3.11. *Sejam $f : A \to B'$ e $g : B \to C$ funções tais que $B' \subseteq B$. Se f e g são funções injetivas, então $g \circ f$ é uma função injetiva.*

Demonstração. Sejam $a_1, a_2 \in A$ tais que $g \circ f(a_1) = g \circ f(a_2)$. Então $g(f(a_1)) = g(f(a_2))$. Como g é injetiva, então $f(a_1) = f(a_2)$ e, como f é injetiva, então $a_1 = a_2$. Portanto $g \circ f$ é injetiva. ■

Proposição 3.12. *Sejam $f : A \to B$ e $g : B \to C$ funções. Se f e g são funções sobrejetivas, então $g \circ f$ é uma função sobrejetiva.*

Demonstração. Como f é sobrejetiva, então $f(A) = B$. Ainda, como g é sobrejetiva, então $g(B) = C$. Então $g \circ f(A) = g(f(A)) = g(B) = C$. Portanto $g \circ f$ é sobrejetiva. ■

Proposição 3.13. *Sejam $f : D \to C$ uma função, $X \subseteq D$ e $Y \subseteq C$. Então*

1. *$X \subseteq f^{-1}(f(X))$.*
2. *$X = f^{-1}(f(X))$ se f é injetiva.*
3. *$f(f^{-1}(Y)) \subseteq Y$.*
4. *$f(f^{-1}(Y)) = Y$ se f é sobrejetiva.*

Demonstração.

1. Seja $x \in X$. Então $f(x) \in f(X)$, o que implica que $x \in f^{-1}(f(X))$.
2. Seja $x \in f^{-1}(f(X))$. Então $f(x) \in f(X)$. Portanto existe $x' \in X$ tal que $f(x) = f(x')$. Da injetividade, segue que $x = x' \in X$.

3. Seja $y \in f(f^{-1}(Y))$. Então existe $x \in f^{-1}(Y)$ tal que $f(x) = y$. Mas então $f(x) \in Y$, portanto $y \in Y$.

4. Seja $y \in Y$. Da sobrejetividade, existe $x \in X$ tal que $f(x) = y \in Y$. Isso implica que $x \in f^{-1}(Y)$ e, portanto, $y = f(x) = f(f^{-1}(Y))$.

■

3.2.3 Conjunto Potência (Conjunto de Funções)

Definição 3.11. Sejam X e Y conjuntos não vazios. O *conjunto de todas as funções de X em Y* é o conjunto

$$Y^X \coloneqq \{f \ : \ f : X \to Y\}.$$

3.3 Imagem Inversa de Função e Propriedades

Definição 3.12. Seja $f : A \to B$ uma função e $B' \subseteq B$. A *imagem inversa* de B sob f é o conjunto

$$f^{-1}(B') \coloneqq \{a \in A \mid f(a) \in B'\}.$$

Proposição 3.14. *Seja $f : A \to B$ uma função, $B' \subseteq B$ e $(B_i)_{i\in I} \subseteq \mathcal{P}(B)$ uma família de subconjuntos de B. Então*

1. $f^{-1}(\emptyset) = \emptyset$;
2. $f^{-1}(B) = A$;
3. $f^{-1}\left((B')^{\complement}\right) = (f^{-1}(B'))^{\complement}$;
4. $f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i)$;
5. $f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i)$.

Demonstração. 1. Suponha, por absudo, que existe $a \in f^{-1}(\emptyset)$. Então $f(a) \in \emptyset$, o que é absurdo, e conclui-se $f^{-1}(\emptyset) = \emptyset$.

2. Seja $a \in A$. Como f é função de A em B, então existe $b \in B$ tal que $f(a) = b$, o que implica $a \in f^{-1}(B)$ e, então, $a \subseteq A$. Como a inclusão contrária vale por definição, então$f^{-1}(B) = A$.

3. Seja $a \in f^{-1}((B')^{\complement})$. Então $f(a) \in (B')^{\complement}$. Mas isso implica $a \notin f^{-1}(B')$, pois, caso contrário, seguiria que $f(a) \in B'$, o que contradiz a hipótese. Portanto $a \in (f^{-1}(B'))^{\complement}$; ou seja, $f^{-1}((B')^{\complement}) \subseteq (f^{-1}(B'))^{\complement}$. Reciprocamente, seja $a \in (f^{-1}(B'))^{\complement}$. Se, por absurdo, $f(a) \in B'$, então $a \notin f^{-1}(B')$, o que contradiz a hipótese. Portanto $f(a) \in (B')^{\complement}$, o que implica $a \in f^{-1}((B')^{\complement})$. Assim conclui-se que $(f^{-1}(B'))^{\complement} \subseteq f^{-1}((B')^{\complement})$ e, portanto, $f^{-1}((B')^{\complement}) = (f^{-1}(B'))^{\complement}$.

4. Seja $a \in f^{-1}(\bigcup_{i\in I} B_i)$. Então $f(a) \in \bigcup_{i\in I} B_i$. Isso significa que exite $i \in I$ tal que $f(a) \in B_i$. Portanto $a \in f^{-1}(B_i)$, e segue que $a \in \bigcup_{i\in I} f^{-1}(B_i)$; ou seja, $f^{-1}(\bigcup_{i\in I} B_i) \subseteq \bigcup_{i\in I} f^{-1}(B_i)$. Reciprocamente, seja $a \in \bigcup_{i\in I} f^{-1}(B_i)$. Então existe $i \in I$ tal que $a \in f^{-1}(B_i)$. Então $f(a) \in B_i$. Mas isso implica que $f(a) \in \bigcup_{i\in I} B_i$. Portanto $a \in f^{-1}(\bigcup_{i\in I} B_i)$; ou seja, $\bigcup_{i\in I} f^{-1}(B_i) \subseteq f^{-1}(\bigcup_{i\in I} B_i)$. Assim, conclui-se que $f^{-1}(\bigcup_{i\in I} B_i) = \bigcup_{i\in I} f^{-1}(B_i)$.

5. Seja $a \in f^{-1}(\bigcap_{i\in I} B_i)$. Então $f(a) \in \bigcap_{i\in I} B_i$. Isso significa que, para todo $i \in I$, $f(a) \in B_i$. Portanto, para todo $i \in I$, $a \in f^{-1}(B_i)$, e segue que $a \in \bigcap_{i\in I} f^{-1}(B_i)$; ou seja, $f^{-1}(\bigcap_{i\in I} B_i) \subseteq \bigcap_{i\in I} f^{-1}(B_i)$. Reciprocamente, seja $a \in \bigcap_{i\in I} f^{-1}(B_i)$. Então, para todo $i \in I$, $a \in f^{-1}(B_i)$. Então, para todo $i \in I$, $f(a) \in B_i$, o que implica que $f(a) \in \bigcap_{i\in I} B_i$. Portanto $a \in f^{-1}(\bigcap_{i\in I} B_i)$; ou seja, $\bigcap_{i\in I} f^{-1}(B_i) \subseteq f^{-1}(\bigcap_{i\in I} B_i)$. Assim, conclui-se que $f^{-1}(\bigcap_{i\in I} B_i) = \bigcap_{i\in I} f^{-1}(B_i)$. ■

3.4 Propriedades de Imagem e Imagem Inversa

Proposição 3.15. *Sejam $f : D \to C$ uma função e $(C_i)_{i\in I}$ uma família de subconjuntos de C. Então*

1. $f(\emptyset) = \emptyset$;
2. $f(D) \subseteq C$;
3. $f\left(\bigcup_{i\in I} C_i\right) = \bigcup_{i\in I} f(C_i)$;

Demonstração. 1. Suponha, por absurdo, que existe $c \in f(\emptyset)$. Nesse caso, existe $d \in \emptyset$ tal que $f(d) = c$, o que é absurdo. Logo $f(\emptyset) = \emptyset$.

2. Se$f(D) = \emptyset$, então vale a proposição. Caso contrário, seja $c \in f(D)$. Então existe $d \in D$ tal que $f(d) = c \in C$.

3. Se $f\left(\bigcup_{i\in I} C_i\right) = \emptyset$, então $\bigcup_{i\in I} C_i = \emptyset$. Assim, segue que, para todo $i \in I$, $C_i = \emptyset$ e temos que $f(C_i) = \emptyset$. Portanto $\bigcup_{i\in I} f(C_i) = \emptyset$. Caso contrário,

seja $d \in f\left(\bigcup_{i\in I} C_i\right)$. Então existe $c \in \bigcup_{i\in I} C_i$ tal que $f(c) = d$ e, consequentemente, existe $i \in I$ tal que $c \in C_i$. Assim, segue que $d = f(c) \in f(C_i) \subseteq \bigcup_{i\in I} f(C_i)$.

Reciprocamente, se $\bigcup_{i\in I} f(C_i) = \emptyset$, então, para todo $i \in I$, $f(C_i) = \emptyset$, o que implica $C_i = \emptyset$. Assim, segue que $\bigcup_{i\in I} C_i = \emptyset$ e, portanto, $f\left(\bigcup_{i\in I} C_i\right) = \emptyset$. Caso contrário, seja $d \in \bigcup_{i\in I} f(C_i)$. Então existe $i \in I$ tal que $d \in f(C_i)$ e, consequentemente, existe $c \in C_i$ tal que $f(c) = d$. Assim, segue que $c \in \bigcup_{i\in I} C_i$ e, portanto, que $d \in f\left(\bigcup_{i\in I} C_i\right)$.

■

Capítulo 4

Relações Binárias

Definição 4.1. Seja A um conjunto não vazio. Uma *relação binária* R em A é uma relação R de A em A.

Definição 4.2. Seja A um conjunto não vazio e R uma relação binária em A. Definem-se as seguintes propriedades de R:

1. (Reflexividade) $\forall a \in A \qquad aRa$;
2. (Irreflexividade) $\nexists a \in A \qquad aRa$;
3. (Simetria) $\forall a_1, a_2 \in A \qquad a_1Ra_2 \Leftrightarrow a_2Ra_1$;
4. (Antissimetria) $\forall a_1, a_2 \in A \qquad a_1Ra_2 \text{ e } a_2Ra_1 \Rightarrow a_1 = a_2$;
5. (Transitividade) $\forall a_1, a_2, a_3 \in A \qquad a_1Ra_2 \text{ e } a_2Ra_3 \Rightarrow a_1Ra_3$;
6. (Totalidade) $\forall a_1, a_2 \in A \qquad a_1Ra_2 \text{ ou } a_2Ra_1$.

Uma relação que satisfaz as propriedades acima é, respectivamente, reflexiva, simétrica, antissimátrica, transitiva e total.

4.1 Relações de Equivalência

Definição 4.3. Seja A um conjunto não vazio. Uma *relação de equivalência* $\sim$ em A é uma relação binária que é reflexiva, simétrica e transitiva.

Costumamos denotar uma relação de equivalência com símbolos $\sim, \simeq, \approx, \equiv$ ou outros símbolos semelhantes.

Definição 4.4. Seja A um conjunto não vazio e $\sim$ uma relação de equivalência em A. A *classe de equivalência* de $a \in A$ é o conjunto

$$[a] \coloneqq \{b \in A \mid b \sim a\}.$$

O *conjunto quociente* de A por $\sim$ é o conjunto

$$A/\sim \coloneqq \{[a] \mid a \in A\}.$$

Teorema 4.1 (Teorema Fundamental das Relações de Equivalência)**.** *Seja A um conjunto não vazio. Se $\sim$ é uma relação de equivalência em A, então $A/\sim$ é uma partição de A. Reciprocamente, se P é uma partição de A, então existe uma relação de equivalência $\sim$ em A tal que $P = A/\sim$.*

Demonstração. Seja $\sim$ uma relação de equivalência em A e $P \coloneqq A/\sim$. Claramete, $\emptyset \notin P$. Ainda, para todo $a \in A$, como $a \sim a$, então $a \in [a]$. Logo

$$\bigcup_{[a]\in P} [a] = A.$$

Por fim, sejam $[a_1], [a_2] \in P$ tais que $[a_1] \neq [a_2]$. Se existir $a \in [a_1] \cap [a_2]$, então, para todo $b \in [a_1]$, $b \sim a_1$ e $a_1 \sim a$, o que implica $b \sim a$. Ainda, $a \sim a_2$. Então $b \in [a_2]$; ou seja, $[a_1] \subseteq [a_2]$. Por outro lado, $b \sim a_2 \sim a \sim a_1$, o que implica $[a_2] \subseteq [a_1]$. Isso implica $[a_1] = [a_2]$, absurdo. Logo $[a_1] \cap [a_2] = \emptyset$. Assim, concluímos que P é uma partição de A.

Seja P uma partição de A. A relação binária $\sim$ em A, definida por

$$\forall a_1, a_2 \in A \qquad a_1 \sim a_2 \Leftrightarrow \exists Q \in P \quad a_1, a_2 \in Q,$$

é uma relação de equivalência. Claramente, para todo $a \in A$, existe $Q \in P$ tal que $a \in Q$, pois $\bigcup_{R\in P} R = A$. Então $a \sim a$, o que mostra a reflexividade. Ainda, a simetria é trivial pela definição da relação $\sim$. Por fim, para $a_1, a_2, a_3 \in A$, se $a_1 \sim a_2$ e $a_2 \sim a_3$, existem conjuntos $Q, R \in P$ tais que $a_1, a_2 \in Q$ e $a_2, a_3 \in R$. Como $a_2 \in Q \cap R$, pela definição de partição $Q = R$. Então $a_1 \sim a_3$, o que mostra a transitividade. Logo $\sim$ é uma relação de equivalência em A. ■

4.2 Relações de Ordem

4.2.1 Ordens Parciais, Estritas e Totais

Definição 4.5. Seja X um conjunto não vazio. Uma *ordem parcial* $\leq$ em X é uma relação binária que é reflexiva, antissimétrica e transitiva. Uma *ordem total* é uma relação de ordem parcial que é total.

Costumamos denotar uma relação de ordem com símbolos $\leq, \preceq, \subseteq, \trianglelefteq$ ou outros símbolos semelhantes.

Exemplo 4.1. Seja A um conjunto. Então a relação $\subseteq$ entre elementos de $\mathcal{P}(A)$ é uma relação de ordem parcial em $\mathcal{P}(A)$.

Exemplo 4.2. Seja $\mathbb{N}$ o conjunto dos naturais. Então a relação divide $|$, definida por

$$a|b \Leftrightarrow \exists n \in \mathbb{N} \qquad an = b$$

é uma relação de ordem parcial nos naturais.

Proposição 4.2. *Seja X um conjunto não vazio e $\leq$ uma ordem parcial em X. Então a relação binária $\geq$ em X, definida para todos $x_1, x_2 \in X$ por*

$$x_1 \geq x_2 \Leftrightarrow x_2 \leq x_1,$$

é uma ordem parcial em X.

Demonstração. Vamos mostrar que valem as três propriedades de ordem parcial. Sejam $x_1, x_2, x_2 \in X$. Como $x_1 \leq x_1$, então $x_1 \geq x_1$. Agora suponha que $x_1 \geq x_2$. Por definição, temos $x_2 \leq x_1$, o que implica $x_1 \leq x_2$, que por sua vez implica $x_2 \geq x_1$. Por fim, suponha $x_1 \geq x_2$ e $x_2 \geq x_3$. Então $x_2 \leq x_1$ e $x_3 \leq x_2$, o que implica $x_3 \leq x_1$ e, portanto, $x_1 \geq x_3$. ■

Definição 4.6. Seja X um conjunto não vazio e $\leq$ uma ordem parcial em X. A *ordem dual de* $\leq$ é a ordem parcial $\geq$ em X, definida para todos $x_1, x_2 \in X$ por

$$x_1 \geq x_2 \Leftrightarrow x_2 \leq x_1.$$

O conceito de dualidade é um conceito importante na teoria de ordem. De fato, toda definição ou teorema tem uma definição ou teorema dual, que consiste em trocar a ordem parcial $\leq$ por sua ordem dual $\geq$.

Definição 4.7. Seja X um conjunto não vazio. Uma *ordem estrita* $<$ em X é uma relação binária que é irreflexiva e transitiva.

Costumamos denotar uma relação de ordem estrita com símbolos $<, \prec, \subset, \triangleleft$ ou outros símbolos semelhantes.

Exemplo 4.3. Seja A um conjunto. Então a relação $\subset$ entre elementos de $\mathcal{P}(A)$ é uma relação de ordem estrita em $\mathcal{P}(A)$.

Proposição 4.3. *Seja X um conjunto não vazio e $\leq$ uma ordem parcial em X. Então a relação binária $<$ em X, definida para todos $x_1, x_2 \in X$ por*

$$x_1 < x_2 \Leftrightarrow x_1 \leq x_2 \quad e \quad x_1 \neq x_2,$$

é uma ordem estrita em X.

Demonstração. Sejam $x_1, x_2, x_3 \in X$. Claramente, $<$ é irreflexiva por definição pois, se $x_1 < x_2$, então $x_1 \neq x_2$. Consideremos agora a transitividade de $<$. Se $x_1 < x_2$ e $x_2 < x_3$, então $x_1 \leq x_2$ e $x_2 \leq x_3$, e também $x_1 \neq x_2$ e $x_2 \neq x_3$. Pela transitividade de $\leq$, temos $x_1 \leq x_3$. Ainda, $x_1 = x_3$ implica $x_1 \leq x_2$ e $x_2 \leq x_1$ e, da antissimetria de $\leq$, temos $x_1 = x_2$, absurdo. Concluímos que $x_1 \neq x_3$ e, portanto, $x_1 < x_3$. ■

Definição 4.8. Seja X um conjunto não vazio e $\leq$ uma ordem parcial em X. A *ordem estrita associada a* $\leq$ é a ordem estrita $<$ em X, definida para todos $x_1, x_2 \in X$ por

$$x_1 < x_2 \Leftrightarrow x_1 \leq x_2 \text{ e } x_1 \neq x_2.$$

Proposição 4.4. *Seja X um conjunto não vazio e $<$ uma ordem estrita em X. Então a relação binária $\leq$ em X, definida para todos $x_1, x_2 \in X$ por*

$$x_1 \leq x_2 \Leftrightarrow x_1 < x_2 \text{ ou } x_1 = x_2,$$

é uma ordem parcial em X.

Demonstração. A demonstração é análoga à demonstração da proposição anterior. ■

Definição 4.9. Seja X um conjunto não vazio e $<$ uma ordem estrita em X. A *ordem parcial associada a* $<$ é a ordem parcial $<$ em X, definida para todos $x_1, x_2 \in X$ por

$$x_1 \leq x_2 \Leftrightarrow x_1 < x_2 \text{ ou } x_1 = x_2.$$

4.2.2 Conjuntos Parcialmente Ordenados

Definição 4.10. Um *conjunto parcialmente ordenado* é um par $(X, \leq)$ em que X é um conjunto não vazio e $\leq$ é uma relação de ordem parcial em X.

Definição 4.11 (Maior e menor elementos)**.** Sejam $(X, \leq)$ um conjunto parcialmente ordenado e $Y \subseteq X$. Um *maior elemento* de Y é um elemento $m \in Y$ que satisfaz

$$\forall y \in Y \qquad y \leq m.$$

Dualmente, um *menor elemento* de Y é um elemento $m \in Y$ que satisfaz

$$\forall y \in Y \qquad m \leq y.$$

Proposição 4.5. *Seja $(X, \leq)$ um conjunto parcialmente ordenado e $Y \subseteq X$. Se existe maior elemento de Y, ele é único. Dualmente, se existe menor elemento de Y, ele é único.*

Demonstração. Seja m um maior elemento de Y. Então, se $n \in Y$ é um maior elemento de Y, então $m \leq n$. Mas, como m é um maior elemento de Y, então $n \leq m$ e, como $\leq$ é antissimétrica, $m = n$. A mesma demonstração vale para um menor elemento de Y, considerando a ordem parcial $\geq$, dual de $\leq$. ■

Notação. Sejam $(X, \leq)$ um conjunto parcialmente ordenado e $Y \subseteq X$. Se existirem, o maior e menor elementos de Y são denotados $\max Y$ e $\min Y$, respectivamente.

Proposição 4.6. *Seja $(X, \leq)$ um conjunto parcialmente ordenado. Então*

1. *$\emptyset$ não tem maior nem menor elemento.*
2. $\forall x \in X \qquad \min\{x\} = \max\{x\} = x.$

Proposição 4.7. *Sejam $(X, \leq)$ um conjunto parcialmente ordenado e Y e Z conjuntos tais que $Z \subseteq Y \subseteq X$. Então, se Y e Z têm maior elemento,*

$$\max Y = \max(\{\max Z\} \cup (Y \setminus Z)).$$

Dualmente, se Y e Z têm menor elemento,

$$\min Y = \min(\{\min Z\} \cup (Y \setminus Z)).$$

Demonstração. Vamos mostrar que $\max Y \in \{\max Z\} \cup (Y \setminus Z)$. Como $\max Y \in Y$, $\max Y \notin (Y \setminus Z)$ implica que $\max Y \in Z$. Portanto $\max Y \leq \max Z$; por outro lado, como $Z \subseteq Y$, então $\max Z \leq \max Y$, o que implica $\max Y = \max Z$ e, assim, concluímos que $\max Y \in \{\max Z\} \cup (Y \setminus Z)$. Agora vamos mostrar que $\{\max Z\} \cup (Y \setminus Z)$ tem maior elemento $\max Y$. Seja $y \in \{\max Z\} \cup (Y \setminus Z)$. Se $y = \max Z$, como $Z \subseteq Y$, então $y \leq \max Y$. Se $y \in (Y \setminus Z)$, como $(Y \setminus Z) \in Y$, então $y \leq \max Y$. Portanto $\max Y = \max(\{\max Z\} \cup (Y \setminus Z))$. ■

Definição 4.12 (Elementos maximal e minimal)**.** Seja $(X, \leq)$ um conjunto parcialmente ordenado e $Y \subseteq X$ um conjunto não vazio. Um *elemento maximal* de Y é um elemento $m \in Y$ que satisfaz

$$\nexists y \in Y \qquad m < y.$$

Dualmente, um *elemento minimal* de Y é um elemento $m \in Y$ que satisfaz

$$\nexists y \in Y \qquad y < m.$$

Proposição 4.8. *Seja $(X, \leq)$ um conjunto parcialmente ordenado e $Y \subseteq X$ um conjunto não vazio. Se Y tem maior elemento, então ele é o único elemento maximal de Y. Dualmente, se Y tem menor elemento, então ele é o único elemento minimal de Y.*

Demonstração. Se Y tem maior elemento, então, para todo $y \in Y$, vale $y \leq \max Y$. Como $\max Y$ é único, não existe elemento $y \in Y$ tal que $y \neq \max$ e $\max Y \leq y$. Portanto $\max Y$ é um elemento maximal de Y. Agora, se existisse outro elemento maximal m de Y, teríamos $m \leq \max Y$, pois $\max Y$ é o maior elemento de Y, o que contradiz a maximalidade de m. Logo $\max Y$ é o único elemento maximal de Y. ■

Definição 4.13 (Limitantes superior e inferior)**.** Seja $(X, \leq)$ um conjunto parcialmente ordenado e $Y \subseteq X$. Um *limitante superior* de Y é um elemento $l \in X$ que satisfaz

$$\forall y \in Y \qquad y \leq l.$$

Dualmente, um *limitante inferior* de Y é um elemento $l \in X$ que satisfaz

$$\forall y \in Y \qquad l \leq y.$$

Um conjunto *limitado por cima* é um conjunto que possui limitante superior. Um conjunto *limitado por baixo* é um conjunto que possui limitante inferior. Um conjunto *limitado* é um conjunto limitado por cima e por baixo.

Proposição 4.9. *Sejam $(X, \leq)$ um conjunto parcialmente ordenado e Y e Z conjuntos tais que $Z \subseteq Y \subseteq X$. Então, se L_Z é o conjunto dos limitantes superiores de Z*

...

Definição 4.14 (Supremo e ínfimo)**.** Seja $(X, \leq)$ um conjunto parcialmente ordenado e $Y \subseteq X$. O *supremo* de Y, denotado $\sup Y$, é o menor elemento do conjunto de limitantes superiores de Y. Dualmente, o *ínfimo* de Y, denotado $\inf Y$, é o maior elemento do conjunto de limitantes inferiores de Y.

Proposição 4.10. *Sejam $(X, \leq)$ um conjunto parcialmente ordenado e Y e Z conjuntos tais que $Z \subseteq Y \subseteq X$. Então, se Y e Z têm supremo,*

$$\sup Y = \sup(\{\sup Z\} \cup (Y \setminus Z)).$$

Dualmente, se Y e Z têm ínfimo,

$$\inf Y = \inf(\{\inf Z\} \cup (Y \setminus Z)).$$

Demonstração. Seja $y \in \{\sup Z\} \cup (Y \setminus Z)$. Se $y = \sup Z$, como $Z \subseteq Y$, então $\sup Z \leq \sup Y$; ■

4.2.3 Funções Monótonas

Definição 4.15. Sejam $\boldsymbol{X} = (X, \leq)$ e $\boldsymbol{Y} = (Y, \preceq)$ conjuntos parcialmente ordenados. Uma *função monótona* de $\boldsymbol{X}$ em $\boldsymbol{Y}$ é uma função $\phi : X \to Y$ que satisfaz

$$\forall x_1, x_2 \in X \qquad x_1 \leq x_2 \Rightarrow \phi(x_1) \preceq \phi(x_2).$$

4.2.4 Cadeias e Lema de Zorn

Definição 4.16. Seja $(X, \leq)$ um conjunto parcialmente ordenado. Uma *cadeia* de X é um conjunto $Y \subseteq X$ que satisfaz

$$\forall y_1, y_2 \in Y \qquad y_1 \leq y_2 \text{ ou } y_2 \leq y_1.$$

Proposição 4.11. *Seja $(X, \leq)$ um conjunto totalmente ordenado e $Y \subseteq X$ um conjunto não vazio. Então Y é uma cadeia de X.*

Demonstração. ... ■

Lema 4.12 (Lema de Zorn)**.** *Seja $(X, \leq)$ um conjunto parcialmente ordenado. Se toda cadeia de X possui limitante superior, então X tem elemento maximal.*

4.2.5 Reticulados

Definição 4.17. Um *reticulado* é um conjunto parcialmente ordenado $(X, \leq)$ em que, para todos $x_1, x_1 \in X$, o conjunto $\{x_1, x_2\}$ tem supremo e ínfimo, denotados, respectivamente, $x_1 \vee x_2$ e $x_1 \wedge x_2$.

Proposição 4.13. *Seja $(X, \leq)$ um reticulado e $Y \subseteq X$ um conjunto finito. Então Y tem supremo e ínfimo.*

Capítulo 5

Cardinalidade de Conjuntos

5.1 Igualdade de Cardinais

Definição 5.1. Sejam X e Y conjuntos. Diz-se que $|X| = |Y|$ (a *cardinalidade de X é igual à cardinalidade de Y*) se, e somente se, existe uma bijeção C entre X e Y. Caso contrário, diz-se que $|X| \neq |Y|$ (a *cardinalidade de X é diferente da cardinalidade de Y*).

As cardinalidades dos números naturais e dos números reais são denotadas, respectivamente

$$|\mathbb{N}| \coloneqq \aleph_0 \quad \text{e} \quad |\mathbb{R}| \coloneqq \mathfrak{c}.$$

Proposição 5.1. *Sejam X, Y e Z conjuntos não vazios. Então*

1. $|X| = |X|$;
2. $|X| = |Y| \Rightarrow |Y| = |X|$;
3. $|X| = |Y| \quad e \quad |Y| = |Z| \Rightarrow |X| = |Z|$.

Demonstração.

1. Claramente, a função identidade em X é uma bijeção entre X e X e, portanto, $|X| = |X|$.
2. Se $|X| = |Y|$, então existe bijeção $C : X \to Y$. Mas então $C^{-1} : Y \to X$ é uma bijeção de Y em X e, portanto, $|Y| = |X|$.
3. Se $|X| = |Y|$ e $|Y| \quad \text{e} \quad |Y|$, então esistem bijeções $C_1 : X \to Y$ e $C_2 : Y \to Z$. Mas então $C_2 \circ C_1 : X \to Z$ é uma bijeção de X em Y e, portanto, $|X| = |Z|$. ■

De certa forma, essa proposição mostra que a noção de cardinalidades iguais se comporta como uma relação de equivalência. Não podemos dizer que $=$ é, de fato,

uma relação de equivalência porque nao existe um conjunto de todos os conjuntos no qual defini-la. Todas proposições sobre cardinalidades são, na verdade, proposições sobre funções entre conjutos e convém saber que as propriedades acima valem.

5.2 Ordenação de Cardinais

Definição 5.2. Sejam X e Y conjuntos não vazios.

1. Diz-se que $|X| \leq |Y|$ (a *cardinalidade de X é menor ou igual à cardinalidade de Y*) se, e somente se, existe função injetiva $C : X \to Y$.

   Diz-se que $|X| \geq |Y|$ (a *cardinalidade de X é maior ou igual à cardinalidade de Y*) se, e somente se, existe função sobrejetiva $C : X \to Y$.

2. Diz-se que $|X| < |Y|$ (a *cardinalidade de X é menor que a cardinalidade de Y*) se, e somente se, $|X| \leq |Y|$ e $|X| \neq |Y|$.

   Diz-se que $|X| > |Y|$ (a *cardinalidade de X é maior que a cardinalidade de Y*) se, e somente se, $|X| \geq |Y|$ e $|X| \neq |Y|$.

Definição 5.3. Um conjunto *enumerável* (ou *contável*) é um conjunto X tal que $\#X \leq \aleph_0$. Uma função injetiva $E : X \to \mathbb{N}$ é uma *enumeração* de X.

Definição 5.4. Um conjunto *finito* é um conjunto X tal que $\#X < \aleph_0$. Um conjunto *infinito* é um conjunto que não é finito.

A seguir, demonstraremos algumas proposições para mostrar que o símbolo $\leq$ se comporta como uma relação de ordem total. Novamente, não podemos dizer formalmente que $\leq$ é uma relação, pois não existe o conjunto de todos os conjuntos no qual defini-la. No entanto, as propriedades acima são bem úteis de se ter em mente e serão usadas na demonstração de outras proposições. As propriedades análogas à reflexividade e transitividade de uma relação de ordem são bem triviais. A antissimetria, por outro lado, é bem difícil, tanto que é um conhecido teorema, o Teorema de Cantor-Schröder-Bernstein. Ainda, é possível demonstrar que $\leq$ se comporta como uma relação total; ou seja, todo conjunto pode ser comparado. Vamos demonstrar primeiro as propriedades triviais. Em seguida, demonstraremos separadamente as outras duas.

Proposição 5.2. *Sejam X, Y e Z conjuntos não vazios. Então*

1. $|X| \leq |X|$;
2. $|X| \leq |Y| \quad e \quad |Y| \leq |X| \Rightarrow |X| = |Y|$;

3. $|X| \leq |Y| \quad e \quad |Y| \leq |Z| \Rightarrow |X| \leq |Z|$*;*

4. $|X| \leq |Y| \quad ou \quad |Y| \leq |X|$.

Demonstração. 1. Claramente, a função identidade é uma bijeção de X em X, logo é uma injeção de X em X e, portanto, $|X| \leq |X|$.

2. Teorema de Cantor-Schröder-Bernstein.

3. $|X| \leq |Y|$ e $|Y| \leq |Z|$, então existem funções injetivas $C_1 : X \to Y$ e $C_2 : Y \to Z$. Mas então $C_2 \circ C_1 : X \to Z$ é uma função injetiva de X em Z e, portanto, $|X| \leq |Z|$.

■

MOSTRAR QUE INFITO EQUIVALE A
X tal que $|X| \geq \aleph_0$.

5.3 Operações com Cardinais

Definição 5.5. Sejam X e Y conjuntos não vazios. Definimos as seguintes "operações"entre cardinais:

1. $|X| + |Y| \coloneqq |X + Y|$;
2. $|X| \times |Y| \coloneqq |X \times Y|$;
3. $|X|^{|Y|} \coloneqq \left|X^Y\right|$.

5.4 Cardinalidade de Soma (ou União Disjunta)

Proposição 5.3. *Seja $(C_i)_{i\in I}$ uma família não vazia de conjuntos disjuntos dois a dois. Então*

$$\left|\bigsqcup_{i\in I} C_i\right| = \left|\bigcup_{i\in I} C_i\right|.$$

Demonstração. Consideremos a função

$$\begin{aligned} f : \bigsqcup_{i\in I} C_i &\to \bigcup_{i\in I} C_i \\ (c, i) &\mapsto c. \end{aligned}$$

Mostremos que f é bijeção. (Injetividade) Sejam $(c_1, i_1), (c_2, i_2) \in \bigsqcup_{i\in I} C_i$ tais que $c_1 = c_2$. Como os C_i são disjuntos dois a dois, existe único $i \in I$ tal que $c_1 = c_2 \in C_i$. Logo $i_1 = i_2 = i$ e, portanto, $(c_1, i_1) = (c_2, i_2)$. (Sobrejetividade) Seja $c \in \bigcup_{i\in I} C_i$. Então existe $i \in I$ tal que $c \in C_i$. ■

Proposição 5.4. *Seja $(C_i)_{i\in I}$ uma família não vazia de conjuntos de mesma cardinalidade. Então*

$$\left|\bigsqcup_{i\in I} C_i\right| = |I| \times |C|$$

para algum C de $(C_i)_{i\in I}$.

Demonstração. Como $I \neq \emptyset$, seja $j \in I$ e defina $C \coloneqq C_j$. Como todos os conjuntos de $(C_i)_{i\in I}$ têm a mesma cardinalidade, para todo $i \in I$, seja $f_i : C_i \to C$ bijeção. Considere a função

$$\begin{aligned} f : \bigsqcup_{i\in I} C_i &\to I \times C \\ (c, i) &\mapsto (i, f_i(c)). \end{aligned}$$

Mostremos que f é bijeção. (Injetividade) Sejam $(c_1, i_1), (c_2, i_2) \in \bigsqcup_{i\in I} C_i$ tais que $(i_1, f_{i_1}(c_1)) = (i_2, f_{i_2}(c_2))$. Então $i_1 = i_2$ e $f_{i_1}(c_1) = f_{i_2}(c_2)$, o que implica que $f_{i_1} = f_{i_2}$ e, portanto, $c_1 = c_2$, já que f_{i_1} é injetiva. Logo $(c_1, i_1) = (c_2, i_2)$. (Sobrejetividade) Seja $(i, c) \in I \times C$. Como f_i é sobrejetiva, existe $c' \in C_i$ tal que $f_i(c') = c$. Portanto $f(c', i) = (i, f_i(c')) = (i, c)$.

Da sobrejetividade de f e da definição de produto de cardinais, segue que

$$\left|\bigsqcup_{i\in I} C_i\right| = |I \times C| = |I| \times |C|\,.$$

■

Teorema 5.5. *Seja $(C_i)_{i\in I}$ uma família não vazia de conjuntos. Se existem $\min_{i\in I} |C_i|$ e $\max_{i\in I} |C_i|$, então*

$$|I| \times \min_{i\in I} |C_i| \leq \left|\bigsqcup_{i\in I} C_i\right| \leq |I| \times \max_{i\in I} |C_i|.$$

Demonstração. Mostremos a primeira desigualdade. Seja $j \in I$ tal que $|C_j| \coloneqq \min_{i\in I} |C_i|$ e $C \coloneqq C_j$. Para cada $i \in I$, existe função injetiva $f_i : C \to C_i$. Considere a função

$$\begin{aligned} f : I \times C &\to \bigsqcup_{i\in I} C_i \\ (i, c) &\mapsto (f_i(c), i). \end{aligned}$$

Mostremos que f é injetiva. Sejam $(i_1, c_1), (i_2, c_2) \in I \times C$ tais que $(f_{i_1}(c_1), i_1) = (f_{i_2}(c_2), i_2)$. Então $i_1 = i_2$ e $f_{i_1} = f_{i_2}$. Como f_{i_1} é injetiva, temos que $c_1 = c_2$, logo $(i_1, c_1) = (i_2, c_2)$.

Mostremos agora a segunda desigualdade. Seja $j \in I$ tal que $|C_j| \coloneqq \max_{i \in I} |C_i|$ e $C \coloneqq C_j$. Para cada $i \in I$, existe função sobrejetiva $f_i : C_i \to C$. Considere a função

$$\begin{aligned} f : \bigsqcup_{i \in I} C_i &\to I \times C \\ (c, i) &\mapsto (i, f_i(c)). \end{aligned}$$

Mostremos que f é sobrejetiva. Seja $(i, c) \in I \times C$. Como f_i é sobrejetiva, existe $c' \in C_i$ tal que $f_i(c') = c$. Portanto $f(c', i) = (i, f_i(c')) = (i, c)$. ■

Capítulo 6

Conjuntos Numéricos

6.1 Números Naturais

Definição 6.1. Um *modelo de números naturais* é uma tripla $\boldsymbol{N} = (N, 0, s)$ em que

1. N é um conjunto, o *conjunto de números naturais*;
2. $0 \in N$, o *zero* de $\boldsymbol{N}$;
3. $s : N \to N$ é uma função injetiva tal que $s^{-1}(\{0\}) = \emptyset$, a função *sucessor*;
4. (Axioma da Indução) Para todo conjunto $I \subseteq N$, se $0 \in I$ e $s(n) \in I$ para todo $n \in I$, então $I = N$.
5. (Axioma da Indução)' Para todo conjunto $I \subseteq N$, se $0 \in I$ e $s(I) \subseteq I$, então $I = N$.

O *um* de $\boldsymbol{N}$ é o elemento $1 \coloneqq s(0)$.

Pela teoria de conjuntos, é possível definir um conjunto infinito $\boldsymbol{N}$ que satisfaz os axiomas de um modelo de números naturais. A construção considera $0 \coloneqq \emptyset$, $1 \coloneqq \{0\}$, e, de modo geral, $s(n) \coloneqq n \cup \{n\} = \{0, 1, \cdots, n\}$. Claramente a construção é feita com mais cuidado, mas a partir dessa construção podemos realmente achar um modelo de números naturais. A partir de agora, consideraremos que esse conjunto existe.

Proposição 6.1. *Seja $\boldsymbol{N}$ um modelo de números naturais. Então, para todo $n \in N \setminus \{0\}$, existe $m \in N$ tal que $n = s(m)$.*

Demonstração. Seja $I \coloneqq \{n \in N : n = 0 \text{ ou } \exists m \in N \quad n = s(m)\}$. Primeiro, notemos que $0 \in I$. Agora, seja $n \in I$. Então $s(n) \in I$, pois $n \in N$ e $s(n) = s(n)$. Logo $I = N$. Assim, se $n \in N \setminus \{0\}$, segue que existe $m \in N$ tal que $n = s(n)$. ■

Essa proposição mostra que s é sobrejetiva em $N \setminus \{0\}$ e, portanto, que s é uma bijeção entre N e $N \setminus \{0\}$, o que mostra que N é um conjunto infinito. No entanto, vale lembrar que a definição de conjunto infinito depende do conjunto dos números naturais.

6.1.1 Adição

Teorema 6.2. *Seja* $\boldsymbol{N}$ *um modelo de números naturais. Existe uma única função*

$$\begin{aligned} + : N \times N &\to N \\ (n_1, n_2) &\mapsto n_1 + n_2 \end{aligned}$$

que satisfaz

1. *(A1)* $\forall n \in N \qquad n + 0 = n$;
2. *(A2)* $\forall n_1, n_2 \in N \qquad n_1 + s(n_2) = s(n_1 + n_2)$.

Demonstração. Primeiro mostraremos que essa função $+$ está bem definida. Para isso, devemos mostrar que, para todo $n_1, n_2 \in N$, existe único $n_3 \in N$ tal que $n_1 + n_2 = n_3$ satisfazendo $(A_1), (A_2)$. Consideremos o conjunto $I \coloneqq \{n \in N : \exists! n_3 \in N \quad n_1 + n = n_3\}$. Primeiro, notemos que $0 \in I$, pois $n + 0 = n$ e, portanto, n_3 é único. Agora, seja $n \in I$. Então existe único $n_3 \in N$ tal que $n_1 + n = n_3$ e, como s é função, $s(n_3) = s(n_1 + n) \in N$ é único e tomando $n_1 + s(n) = s(n_1 + n)$, concluímos que $s(n) \in I$ e, portanto, $I = N$. Logo $+$ está bem definida. Agora, mostremos que $+$ é única. Sejam $+_1, +_2 : N \times N \to N$ funções satisfazendo $(A_1), (A_2)$, $n_1 \in N$ e $I \coloneqq \{n \in N : n_1 +_1 n = n_1 +_2 n\}$. Primeiro, notemos que $0 \in I$, pois $n_1 +_1 0 = n = n_1 +_2 0$. Agora, seja $n \in I$. Então

$$n_1 +_1 s(n) = s(n_1 +_1 n) = s(n_1 +_2 n) = n_1 +_2 s(n),$$

o que implica que $s(n) \in I$ e, portanto, que $I = N$. Logo $+_1 = +_2$. ■

Definição 6.2. Seja $\boldsymbol{N}$ um modelo de números naturais. A função $+$ é a *adição nos números naturais* e, dados $n_1, n_2 \in N$, o número $n_1 + n_2 \in N$ é a *soma de* n_1 *e* n_2.

Teorema 6.3 (Associatividade da adição)**.** *Seja* $\boldsymbol{N}$ *um modelo de números naturais. Então*

$$\forall n_1, n_2, n_3 \in N \qquad (n_1 + n_2) + n_3 = n_1 + (n_2 + n_3).$$

Demonstração. Sejam $n_1, n_2 \in N$ e $I \coloneqq \{n_3 \in N : (n_1+n_2)+n_3 = n_1+(n_2+n_3)\}$. Notemos que $0 \in I$, pois

$$\begin{aligned} &\text{(A1)} && (n_1 + n_2) + 0 = n_1 + n_2 \\ &\text{(A1)} && = n_1 + (n_2 + 0). \end{aligned}$$

Agora, seja $n \in I$. Então

$$\begin{aligned} &\text{(A2)} && (n_1 + n_2) + s(n) = s((n_1 + n_2) + n) \\ &(n \in I) && = s(n_1 + (n_2 + n)) \\ &\text{(A2)} && = n_1 + s(n_2 + n) \\ &\text{(A2)} && = n_1 + (n_2 + s(n)), \end{aligned}$$

o que implica $s(n) \in I$. Logo $I = N$. ■

Teorema 6.4. *Seja* $\boldsymbol{N}$ *um modelo de números naturais. Então*

$$\forall n \in N \qquad s(n) = n + 1.$$

Demonstração. Seja $n \in N$. Então

$$s(n) = s(n + 0) = n + s(0) = n + 1.$$

■

Lema 6.5. *Seja* $\boldsymbol{N}$ *um modelo de números naturais. Então*

1. $\forall n \in N \qquad 0 + n = n;$
2. $\forall n \in N \qquad 1 + n = n + 1.$

Demonstração. Demonstraremos ambas afirmações por indução em n.

1. Seja $I \coloneqq \{n \in N : 0 + n = n\}$. Primeiro notemos que $0 \in I$, pois $0 + 0 = 0$. Agora, seja $n \in I$. Então

   $$0 + s(n) = 0 + (n + 1) = (0 + n) + 1 = n + 1 = s(n),$$

   o que implica que $s(n) \in I$ e, portanto, $I = N$.

2. Seja $I \coloneqq \{n \in N : 1 + n = n + 1\}$. Primeiro notemos que $0 \in I$, pois $1 + 0 = 1 = 0 + 1$. Agora, seja $n \in I$. Então

   $$1 + s(n) = 1 + (n + 1) = (1 + n) + 1 = (n + 1) + 1 = s(n) + 1,$$

   o que implica que $s(n) \in I$ e, portanto, $I = N$.

■

Teorema 6.6 (Comutatividade da adição)**.** *Seja* $\mathbf{N}$ *um modelo de números naturais. Então*

$$\forall n_1, n_2 \in N \qquad n_1 + n_2 = n_2 + n_1.$$

Demonstração. Demonstraremos a afirmação por indução. Seja $n_1 \in N$ e $I \coloneqq \{n \in N : n_1 + n = n + n_1\}$. Primeiro notemos que $0 \in I$, pois

$$n_1 + 0 = n_1 = 0 + n_1.$$

Agora, seja $n \in I$. Então

$$\begin{aligned} n_1 + s(n) &= n_1 + (n + 1) \\ &= (n_1 + n) + 1 \\ &= (n + n_1) + 1 \\ &= n + (n_1 + 1) \\ &= n + (1 + n_1) \\ &= (n + 1) + n_1 \\ &= s(n) + n_1, \end{aligned}$$

o que implica que $s(n) \in I$ e, portanto, $I = N$. ■

6.1.2 Multiplicação

Teorema 6.7. *Seja* $\mathbf{N}$ *um modelo de números naturais. Existe uma única função*

$$\begin{aligned} \times : N \times N &\to N \\ (n_1, n_2) &\mapsto n_1 \times n_2 \end{aligned}$$

que satisfaz

1. *(M1)* $\forall n \in N \qquad n \times 0 = 0$*;*
2. *(M2)* $\forall n_1, n_2 \in N \qquad n_1 \times s(n_2) = (n_1 \times n_2) + n_1.$

Demonstração. Primeiro devemos mostrar que a função $\times$ está bem definida. Para isso, devemos mostrar que, para todo $n_1, n_2 \in N$, existe único $n_3 \in N$ tal que $n_1 \times n_2 = n_3$. Consideremos $I \coloneqq \{n \in N : \exists! n_3 \in N \quad n_1 \times n = n_3\}$. Primeiro, notemos que $0 \in I$, pois $n_1 \times 0 = 0$ e, portanto, n_3 esxite e é único. Agora, seja $n \in I$. Então existe único $n_3 \in N$ tal que $n_1 \times n = n_3$ e, como $+$ é função, $n_3 + n_1 = n_1 \times n + n$ é único e tomando $n_1 \times s(n) = n_1 \times n + n_1$, concluímos que

$s(n) \in I$ e, portanto, $I = N$. Logo $\times$ está bem definida. Agora, devemos mostrar que $\times$ é única. Sejam $\times_1, \times_2 : N \times N \to N$ funções satisfazendo $(M_1), (M_2)$, $n_1 \in N$ e $I \coloneqq \{n \in N : n_1 \times_1 n = n_1 \times_2 n\}$. Primeiro, notemos que $0 \in I$, pois $n_1 \times_1 0 = 0 = n_1 \times_2 0$. Agora, seja $n \in I$. Então

$$n_1 \times_1 s(n) = n_1 \times_1 n + n_1 = n_1 \times_2 n + n_1 = n_1 \times_2 s(n),$$

o que implica que $s(n) \in I$ e, portanto, que $I = N$. Logo $\times_1 = \times_2$. ■

Definição 6.3. Seja $\boldsymbol{N}$ um modelo de números naturais. A função $\times$ é a *multiplicação nos números naturais* e, dados $n_1, n_2 \in N$, o número $n_1 \times n_2 \in N$ é o *produto de* n_1 *e* n_2.

Teorema 6.8 (Distributividade)**.** *Seja* $\boldsymbol{N}$ *um modelo de números naturais. Então*

1. $\forall n, m, k \in N \qquad n \times (m + k) = (n \times m) + (n \times k)$;
2. $\forall n, m, k \in N \qquad (n + m) \times k = (n \times k) + (m \times k)$.

Demonstração. 1. Sejam $n, m \in N$ e $I \coloneqq \{k \in N : n \times (m + k) = (n \times m) + (n \times k)\}$. Primeiro, notemos que $0 \in I$, pois

$$\begin{aligned}
&(A_1) && n \times (m + 0) = n \times m \\
&(A_1) && = n \times m + 0 \\
&(M_1) && = (n \times m) + (n \times 0).
\end{aligned}$$

Agora, seja $k \in I$. Então

$$\begin{aligned}
&(A_2) && n \times (m + s(k)) = n \times s(m + k) \\
&(M_2) && = (n \times (m + k)) + n \\
&(k \in I) && = ((n \times m) + (n \times k)) + n \\
&(6.3) && = (n \times m) + ((n \times k) + n) \\
&(M_2) && = (n \times m) + (n \times s(k)),
\end{aligned}$$

o que implica que $s(k) \in I$ e, portanto, que $I = N$.

2. Sejam $n, m \in N$ e $I \coloneqq \{k \in N : (n+m) \times k = (n \times k) + (m \times k)\}$. Primeiro, notemos que $0 \in I$, pois

$$\begin{aligned}
&(M_1) && (n + m) \times 0 = 0 \\
&(A_1) && = 0 + 0 \\
&(M_1) && = (n \times 0) + (m \times 0).
\end{aligned}$$

Agora, seja $k \in I$. Então

$$\begin{aligned}
(M_2) \qquad (n+m) \times s(k) &= ((n+m) \times k) + (n+m) \\
(k \in I) \qquad &= ((n \times k) + (m \times k)) + (n+m) \\
(6.3) \qquad &= ((n \times k) + n) + ((m \times k) + m) \\
(M_2) \qquad &= (n \times s(k)) + (m \times s(k)),
\end{aligned}$$

o que implica que $s(k) \in I$ e, portanto, que $I = N$.

■

Teorema 6.9 (Associatividade da multiplicação)**.** *Seja* $\mathbf{N}$ *um modelo de números naturais. Então*

$$\forall n, m, k \in N \qquad (n \times m) \times k = n \times (m \times k).$$

Demonstração. Sejam $n, m \in N$ e $I \coloneqq \{k \in N : (n \times m) \times k = n \times (m \times k)\}$. Primeiro, notemos que $0 \in I$, pois

$$(M_1) \qquad (n \times m) \times 0 = 0 = n \times 0 = n \times (m \times 0)$$

Agora, seja $k \in I$. Então

$$\begin{aligned}
(M_2) \qquad (n \times m) \times s(k) &= ((n \times m) \times k) + (n \times m) \\
(k \in I) \qquad &= (n \times (m \times k)) + (n \times m) \\
(6.8) \qquad &= n \times ((m \times k) + m) \\
(M_2) \qquad &= n \times (m \times s(k)),
\end{aligned}$$

o que implica que $s(k) \in I$ e, portanto, que $I = N$. ■

Lema 6.10. *Seja* $\mathbf{N}$ *um modelo de números naturais. Então*

1. $\forall n \in N \qquad 0 \times n = 0$;
2. $\forall n \in N \qquad n \times 1 = n = 1 \times n$.

Demonstração. 1. Vamos mostrar por indução em n. Seja $I \coloneqq \{n \in N : 0 \times n = 0\}$. Primeiro, notemos que $0 \in I$, pois $0 \times 0 = 0$. Agora, seja $n \in I$. Então

$$0 \times s(n) = (0 \times n) + 0 = 0 + 0 = 0,$$

o que mostra que $s(n) \in N$ e, portanto, $I = N$.

2. Seja $n \in N$. Então

$$n \times 1 = (n \times 0) + n = 0 + n = n.$$

Mostraremos a segunda igualdade por indução em n. Seja $I \coloneqq \{n \in N : 1 \times n = n\}$. Primeiro, notemos que $0 \in I$, pois $1 \times 0 = 0$. Agora, seja $n \in I$. Então

$$1 \times s(n) = (1 \times n) + 1 = n + 1 = s(n),$$

o que implica que $s(n) \in I$ e, portanto, que $I = N$.

■

Teorema 6.11. *Seja $\boldsymbol{N}$ um modelo de números naturais. Então*

$$\forall n, m \in N \qquad n \times m = m \times n.$$

Demonstração. Sejam $n \in N$ e $I \coloneqq \{m \in N : n \times m = m \times n\}$. Primeiro, notemos que $0 \in I$, pois

$$\begin{aligned} (M_1) \qquad & n \times 0 = 0 \\ (6.10) \qquad & = 0 \times n. \end{aligned}$$

Agora, seja $m \in I$. Então

$$\begin{aligned} (M_2) \qquad & n \times s(m) = (n \times m) + n \\ (m \in I) \qquad & = (m \times n) + n \\ (6.10) \qquad & = (m \times n) + (1 \times n) \\ (6.8) \qquad & = (m + 1) \times n \\ (6.4) \qquad & = s(m) \times n, \end{aligned}$$

o que implica que $s(m) \in I$ e, portanto, que $I = N$. ■

6.1.3 Ordenação

Lema 6.12. *Seja $\boldsymbol{N}$ um modelo de números naturais. Então*

1. $\forall n, m, k \in N \qquad n + k = m + k \implies n = m;$
2. $\forall n, m \in N \qquad n + m = 0 \implies n = m = 0.$

Demonstração. 1. Seja $I \coloneqq \{k \in N : \forall n, m \in N \quad n + k = m + k \implies n = m\}$. Primeiro, notemos que $0 \in I$, pois, para todos $n, m \in N$, se $n + 0 = m + 0$, então $n = m$. Agora, seja $k \in I$ e $n, m \in N$. Se $n + s(k) = m + s(k)$, então $s(n + k) = s(m + k)$ e, como s é injetiva, $n + k = m + k$, o que implica que $n = m$ e, assim, temos que $s(k) \in I$ e, portanto, $I = N$.

2. Suponhamos, por absurdo, que $n \neq 0$ ou $m \neq 0$. Notemos que $n+m = m+n$; então, sem perda de generalidade, seja $m \neq 0$. Então existe $k \in N$ tal que $m = s(k)$ e segue que $n + m = n + s(k) = s(n + k) = 0$, o que é absurdo, pois $s^{-1}(\{0\}) = \emptyset$. Logo $n = m = 0$.

■

Definição 6.4. Seja $\boldsymbol{N}$ um modelo dos números naturais. A relação binária $\leq$ em N é definida por

$$n \leq m \qquad \Longleftrightarrow \qquad \exists d \in N \quad n + d = m.$$

Proposição 6.13. *Seja $\boldsymbol{N}$ um modelo dos números naturais. A relação binária $\leq$ em N é uma relação de ordem total.*

Demonstração. Primeiro, notemos que $\leq$ é reflexiva, pois, pra todo $n \in N$, $n+0 = n$, o que implica que $n \leq n$. Segundo, notemos que $\leq$ é antissimétrica. Sejam $n, m \in N$ tais que $n \leq m$ e $m \leq n$; então existem $d_1, d_2 \in N$ tais que $n + d_1 = m$ e $m + d_2 = n$ e, portanto, que $n + m = n + m + d_1 + d_2$, o que implica $d_1 + d_2 = 0$ e, portanto, que $d_1 = d_2 = 0$. Assim $n = m$. Terceiro, mostremos que $\leq$ é transitiva. Sejam $m, n, k \in N$ tais que $n \leq m$ e $m \leq k$. Então existem $d_1, d_2 \in N$ tais que $n + d_1 = m$ e $m + d_2 = k$. Assim, $n + d_1 + d_2 = k$, logo $n \leq k$. Isso termina a demonstração de que $\leq$ é uma ordem parcial. Por fim, devemos mostrar que a ordem parcial $\leq$ é total. Sejam $n \in N$ e $I \coloneqq \{m \in N : n \leq m \text{ ou } m \leq n\}$. Primeiro, notemos que $0 \in I$, pois $0 + n = n$, logo $0 \leq n$. Agora, seja $m \in I$. Se $nleqm$, existe $d \in N$ tal que $n+d = m$, e segue que, como $n+d+1 = m+1 = s(m)$, $n \leq s(m)$. Se $m \leq n$, existe $d \in N$ tal que $m + d = n$. Consideramos dois casos: se $d = 0$, então $n + 1 = m + 1 = s(m)$, logo $n \leq s(m)$; se $d \neq 0$, existe $k \in N$ tal que $d = s(k) = k+1$, o que implica $n = m+d = m+k+1 = m+1+k = s(m)+k$ e, portanto, $s(m) \leq n$. Assim, concluímos que $s(m) \in I$ e, portanto, que $I = N$. Assim, fica provado que $\leq$ é uma ordem total. ■

Dessa forma, a relação binária $<$ fica definida como a ordem estrita associada a $\leq$.

Teorema 6.14 (Boa ordenação)**.** *Seja $\boldsymbol{N}$ um modelo de números naturais. Então $(\boldsymbol{N}, \leq)$ é bem ordenado.*

Demonstração. Seja $C \subseteq N$ um conjunto que não tem menor elemento. Devemos mostrar que $C = \emptyset$. Notemos que $0 \notin C$ porque, para todo $n \in C$, $0 \leq n$, o que implicaria que $0 = \min C$. Consideremos $I \coloneqq \{m \in N : \forall n \in C \quad m < n\}$. Inicialmente, ressaltemos que $C \cap I = \emptyset$, pois, se existe $m \in I \cap C$, então, como $m \in I$, para todo $n \in C$, $m < n$ e, como $m \in C$, segue que $m < m$, o que é absurdo. Então notemos que $0 \in I$, pois $0 \leq n$ para todo $n \in C$ e $0 \notin C$. Agora,

seja $m \in I$. Então, para todo $n \in C$, $m < n$, o que implica que existe $d \in N \setminus \{0\}$ tal que $m + d = n$. Então segue que existe $k \in N$ tal que $d = s(k) = k + 1$ e segue que $s(m) + k = m + k + 1 = n$; ou seja, $s(m) \leq n$. Agora notemos que $s(m) \notin C$, pois, caso contrário, $s(m) = \min C$. Portanto, para todo $n \in C$, $s(m) < n$, o que mostra que $s(m) \in I$ e, por sua vez, que $I = N$. Como $C \subseteq N$, segue que $C \cap N = C$. Mas então $\emptyset = C \cap I = C \cap N = C$. ■

Teorema 6.15 (Indução completa)**.** *Seja* $\boldsymbol{N}$ *um modelo de números naturais. Para todo conjunto* $I \subseteq N$*, se* $0 \in I$ *e*

$$\{m \in N : m < n\} \subseteq I \quad \Longrightarrow \quad s(n) \in I,$$

então $I = N$*.*

Demonstração. Seja $I \subseteq N$ e suponha que $0 \in I$ e $\{m \in N : m < n\} \subseteq I \implies s(n) \in I$. Então ■

Lema 6.16. *Seja* $\boldsymbol{N}$ *um modelo de números naturais. Então*

$$\forall n_1, n_2, m_1, m_2 \in N \qquad \begin{cases} n_1 \leq m_1 \\ n_2 \leq m_2 \end{cases} \quad \Longrightarrow \quad \begin{cases} n_1 + n_2 \leq m_1 + m_2 \\ n_1 \times n_2 \leq m_1 \times m_2. \end{cases}$$

Demonstração. Para $i \in \{1, 2\}$, como $n_i \leq m_i$, existe $d_i \in N$ tal que $n_i + d_i = m_i$. Assim, segue que $n_1 + d_1 + n_2 + d_2 = m_1 + m_2$ e, portanto, $n_1 + n_2 \leq m_1 + m_2$. Ainda, segue que

$$m_1 \times m_2 = (n_1 + d_1) \times (n_2 + d_2) = (n_1 \times n_2) + (n_1 \times d_2) + (d_1 \times n_1) + (d_1 \times d_2)$$

e, portanto, $n_1 \times n_2 \leq m_1 \times m_2$. ■

6.2 Números Inteiros

Proposição 6.17. *Seja* $\boldsymbol{N}$ *um modelo de números naturais. A relação binária* $\sim$ *em* $N \times N$ *definida por*

$$\forall n_1, n_2, m_1, m_2 \qquad (n_1, n_2) \sim (m_1, m_2) \quad \Longleftrightarrow \quad n_1 + m_2 = n_2 + m_1$$

é uma relação de equivalência.

Demonstração. Sejam $(n_1, n_2), (m_1, m_2), (k_1, k_2) \in N \times N$. Primeiro, notemos que $n_1 + n_2 = n_2 + n_1$, o que mostra que $(n_1, n_2) \sim (n_1, n_2)$. Segundo, notemos que, se $(n_1, n_2) \sim (m_1, m_2)$, então $n_1 + m_2 = n_2 + m_1$, o que implica que $m_1 + n_2 = m_2 + n_1$ e, portanto, que $(m_1, m_2) \sim (n_1, n_2)$. Terceiro, notemos que, se $(n_1, n_2) \sim (m_1, m_2)$ e $(m_1, m_2) \sim (k_1, k_2)$, então $n_1 + m_2 = n_2 + m_1$ e $m_1 + k_2 = m_2 + k_1$, o que implica que $n_1 + m_2 + m_1 + k_2 = n_2 + m_1 + m_2 + k_1$ e, portanto, que $n_1 + k_2 = n_2 + k_1$, logo $(n_1, n_2) \sim (k_1, k_2)$. ■

Definição 6.5. Seja $\boldsymbol{N}$ um modelo de números naturais com a equivalência $\sim$. O *modelo de números inteiros* associado a $\boldsymbol{N}$ é o par $\boldsymbol{Z} = (\boldsymbol{N}, Z)$, em que Z é o conjunto

$$Z \coloneqq N \times N \Big/ \sim,$$

o *conjunto dos números inteiros.*

Proposição 6.18. *Seja $\boldsymbol{Z}$ um modelo de números inteiros. Para todo $z \in Z$, existe único $d \in N$ tal que $z = [(n + d, n)]$ ou $z = [(n, n + d)]$.*

Demonstração. Seja $z \in Z$. Então $z = [(n_1, n_2)]$. Notemos que $n_1 \leq n_2$ ou $n_1 \geq n_2$. Agora, devemos notar que isso está bem definido para qualquer representante de z. Sejam $(n_1, n_2), (n_1', n_2') \in z$. Então $n_1 + n_2' = n_2 + n_1'$. Sem perda de generalidade, cosideremos que $n_1 \geq n_2$. Nesse caso, existe $d \in N$ tal que $n_1 = n_2 + d$. Mas isso implica que $n_2 + d + n_2' = n_2 + n_1'$ e, portanto, que $n_1' = n_2' + d$ e, então $n_1' \geq n_2'$. Do mesmo modo, supondo $n_1' \geq n_2'$ achamos que $n_1 \geq n_2$. Ainda, o valor d é o mesmo em ambos os casos. Assim, se $n_1 \geq n_2$, temos que $z = [(n+d, n)]$ e, caso contrário, que $z = [(n, n + d)]$. A unicidade de d é óbvia pois, se existem d_1, d_2 tais que $n_1 = n_2 + d_1$ e $n_1 = n_2 + d_2$, então segue que $n_2 + d_1 = n_2 + d_2$ e, portanto, que $d_1 = d_2$. ■

Pela proposição anterior, um número inteiro de $\boldsymbol{Z}$ é unicamente representado pelo elemento $d \in N$ e sua posição no par ordenado. Por isso, se $z = [(n + d, n)]$, identificamos z com d e, se $z = [(n, n + d)]$, identificamos z com $-d$.

6.2.1 Adição e Subtração

Definição 6.6. Seja $\boldsymbol{Z}$ um modelo de números inteiros. O *zero* de $\boldsymbol{Z}$ é o elemento $0 \coloneqq [(n, n)]$.

Definição 6.7. Seja $\boldsymbol{Z}$ um modelo de números inteiros. A *adição nos números inteiros* é a função

$$\begin{gathered} + : Z \times Z \to Z \\ ([(n_1, n_2)], [(m_1, m_2)]) \mapsto [(n_1 + m_1, n_2 + m_2)]. \end{gathered}$$

Dados $n, m \in Z$, o número $n + m$ é a *soma de n e m.*

Teorema 6.19. *Seja $\boldsymbol{Z}$ um modelo de números inteiros. A função $+$ está bem definida.*

Demonstração. Sejam $n, m \in Z$ e $(n_1, n_2), (n_1', n_2') \in n$, $(m_1, m_2), (m_1', m_2') \in m$. Então $n + m$ pode ser calculado por

$$[(n_1, n_2)] + [(m_1, m_2)] = [(n_1 + m_1, n_2 + m_2)]$$
$$[(n_1', n_2')] + [(m_1', m_2')] = [(n_1' + m_1', n_2' + m_2')].$$

Como $n_1 + n_2' = n_2 + n_1'$ e $m_1 + m_2' = m_2 + m_1'$, segue que

$$n_1 + n_2' + m_1 + m_2' = n_2 + n_1' + m_2 + m_1'$$

e, portanto, $(n_1 + m_1, n_2 + m_2) \sim (n_1' + m_1', n_2' + m_2')$, o que mostra que a soma $n + m$ está bem definida. ■

Proposição 6.20. *Seja $\boldsymbol{Z}$ um modelo de números inteiros. Então*

1. $\forall n \in Z \qquad n + 0 = n$;
2. $\forall n, m, k \in Z \qquad (n + m) + k = n + (m + k)$;
3. $\forall n, m \in Z \qquad n + m = m + n$.

Demonstração. Sejam $n, m, k \in Z$ e $(n_1, n_2) \in n, (m_1, m_2) \in m, (k_1, k_2) \in k$.

1. Como $(0, 0) \in 0$, então $(n_1, n_2) + (0, 0) = (n_1, n_2)$, logo $n + 0 = n$.
2. Notemos que
$$\begin{aligned}((n_1, n_2) + (m_1, m_2)) + (k_1, k_2) &= (n_1 + m_1, n_2 + m_2) + (k_1, k_2) \\ &= (n_1 + m_1 + k_1, n_2 + m_2 + k_2) \\ &= (n_1, n_2) + (m_1 + k_1, m_2 + k_2) \\ &= (n_1, n_2) + ((m_1, m_2) + (k_1, k_2)),\end{aligned}$$
logo $(n + m) + k = n + (m + k)$.
3. Notemos que
$$\begin{aligned}(n_1, n_2) + (m_1, m_2) &= (n_1 + m_1, n_2 + m_2) \\ &= (m_1 + n_1, m_2 + n_2) \\ &= (m_1, m_2) + (n_1, n_2),\end{aligned}$$
logo $n + m = m + n$.

■

Definição 6.8. Seja $\boldsymbol{Z}$ um modelo de números inteiros. A função *negativo* em $\boldsymbol{Z}$ é a função

$$-: Z \to Z$$
$$[(n_1, n_2)] \mapsto [(n_2, n_1)].$$

6.2.2 Multiplicação

A partir desta seção, usaremos a notação nm em vez de $n \times m$ para facilitar os cálculos.

Definição 6.9. Seja $\boldsymbol{Z}$ um modelo de números inteiros. O *um* de $\boldsymbol{Z}$ é o elemento $1 \coloneqq [(n+1, n)]$.

Definição 6.10. Seja $\boldsymbol{Z}$ um modelo de números inteiros. A *multiplicação nos números inteiros* é a função

$$\begin{gathered} \times : Z \times Z \to Z \\ ([(n_1, n_2)], [(m_1, m_2)]) \mapsto [(n_1 m_1 + n_2 m_2, n_2 m_1 + n_1 m_2)]. \end{gathered}$$

Dados $n, m \in Z$, o número $n \times m$ é o *produto de n e m*.

Teorema 6.21. *Seja $\boldsymbol{Z}$ um modelo de números inteiros. A função $\times$ está bem definida.*

Demonstração. Sejam $n, m \in Z$ e $(n_1, n_2), (n_1', n_2') \in n$, $(m_1, m_2), (m_1', m_2') \in m$. Então $n \times m$ pode ser calculado por

$$\begin{aligned} [(n_1, n_2)] \times [(m_1, m_2)] &= [(n_1 m_1 + n_2 m_2, n_2 m_1 + n_1 m_2)] \\ [(n_1', n_2')] \times [(m_1', m_2')] &= [(n_1' m_1' + n_2' m_2', n_2' m_1' + n_1' m_2')]. \end{aligned}$$

Como $n_1 + n_2' = n_2 + n_1'$ e $m_1 + m_2' = m_2 + m_1'$, segue que

$$\begin{aligned} &(n_1 m_1 + n_2 m_2 + n_2' m_1' + n_1' m_2') + (n_1 m_2' + n_2 m_1' + n_1 m_1' + n_2 m_2') \\ &= n_1(m_1 + m_2') + n_2(m_2 + m_1') + (n_2' + n_1) m_1' + (n_1' + n_2) m_2' \\ &= n_1(m_1' + m_2) + n_2(m_2' + m_1) + (n_2 + n_1') m_1' + (n_1 + n_2') m_2' \\ &= (n_2 m_1 + n_1 m_2 + n_1' m_1' + n_2' m_2') + (n_1 m_2' + n_2 m_1' + n_1 m_1' + n_2 m_2'), \end{aligned}$$

o que implica que

$$n_1 m_1 + n_2 m_2 + n_2' m_1' + n_1' m_2' = n_2 m_1 + n_1 m_2 + n_1' m_1' + n_2' m_2'$$

e, portanto, $(n_1 m_1 + n_2 m_2, n_2 m_1 + n_1 m_2) \sim (n_1' m_1' + n_2' m_2', n_2' m_1' + n_1' m_2')$, o que mostra que o produto $n \times m$ está bem definido. ■

6.2.3 Ordenação

Definição 6.11. Seja $\boldsymbol{Z}$ um modelo de números inteiros. A relação binária $\leq$ em N é definida por

$$[(n_1, n_2)] \leq [(m_1, m_2)] \quad \iff \quad n_1 + m_2 \leq n_2 + m_1.$$

Proposição 6.22. *Seja $\boldsymbol{Z}$ um modelo de números inteiros. A relação binária $\leq$ em N está bem definida e é uma relação de ordem total.*

6.3 Números Racionais

6.3.1 Adição e Subtração

6.3.2 Multiplicação e Divisão

6.3.3 Ordenação

6.4 Números Reais

6.4.1 Adição e Subtração

6.4.2 Multiplicação e Divisão

6.4.3 Ordenação

6.4.4 Completude

Capítulo 7

Resto temporário

7.1 Complementares e Diferença Simétrica

Definição 7.1. Sejam X e Y conjuntos. O *complementar relativo* de Y em X é o conjunto

$$X \setminus Y \coloneqq \{x \in X \mid x \notin Y\}.$$

Definição 7.2. Sejam U um conjunto e X um subconjunto de U. O *complementar* de X em U é o conjunto

$$X^{\complement} \coloneqq U \setminus X.$$

Definição 7.3. Sejam X e Y conjuntos. A *diferença simétrica* de X e Y é o conjunto

$$X \triangle Y \coloneqq (X \setminus Y) \cup (Y \setminus X).$$

7.1.1 Propriedades

Proposição 7.1. *Sejam X, Y subconjuntos de U. Então*

1. $(X^{\complement})^{\complement} = X$;
2. $\emptyset^{\complement} = U$ *e* $U^{\complement} = \emptyset$;
3. $X \cap X^{\complement} = \emptyset$ *e* $X \cup X^{\complement} = U$;
4. $X \subseteq Y \iff Y^{\complement} \subseteq X^{\complement}$.
5. $(X \cup Y)^{\complement} = X^{\complement} \cap Y^{\complement}$ *e* $(X \cap Y)^{\complement} = X^{\complement} \cup Y^{\complement}$.

7.2 Outras definições

Definição 7.4. Seja X um conjunto não vazio. Uma *partição* de X é um conjunto $P \subseteq \mathcal{P}(X)$ de subconjuntos de X que satisfaz

1. $\emptyset \notin P$;
2. $\bigcup P = X$;
3. $\forall A, B \in P \qquad A \neq B \implies A \cap B = \emptyset$.

7.3 Limites de Conjuntos

Definição 7.5. Sejam X um conjunto e $(A_n)_{n\in\mathbb{N}}$ uma sequência de subconjuntos de X. O *limite inferior* de $(A_n)_{n\in\mathbb{N}}$ é o conjunto

$$\liminf A_n \coloneqq \bigcup_{m=0}^{\infty} \left(\bigcap_{n=m}^{\infty} A_n \right).$$

Esse conjunto é o conjuto dos pontos que não pertencem todos menos finitos conjuntos A_n. O *limite superior* de $(A_n)_{n\in\mathbb{N}}$ é o conjunto

$$\limsup A_n \coloneqq \bigcap_{m=0}^{\infty} \left(\bigcup_{n=m}^{\infty} A_n \right).$$

Esse conjunto é o conjunto dos pontos que pertencem a infinitos conjuntos A_n.

Proposição 7.2. *Sejam X um conjunto e $(A_n)_{n\in\mathbb{N}}$ uma sequência de subconjuntos de X. Então*

$$\emptyset \subseteq \liminf A_n \subseteq \limsup A_n \subseteq X.$$

Proposição 7.3. *Sejam X um conjunto e $(A_n)_{n\in\mathbb{N}}$ uma sequência de subconjuntos de X. Então*

1. *Se $(A_n)_{n\in\mathbb{N}}$ é monótona cresente,*

$$\liminf A_n = \bigcup_{n=0}^{\infty} A_n = \limsup A_n.$$

2. *Se $(A_n)_{n\in\mathbb{N}}$ é monótona decresente,*

$$\liminf A_n = \bigcap_{n=0}^{\infty} A_n = \limsup A_n.$$

Definição 7.6. Sejam X um conjunto e $(A_n)_{n\in\mathbb{N}}$ uma sequência de subconjuntos de X. Um *limite* de $(A_n)_{n\in\mathbb{N}}$ é um conjunto $\lim A_n$ tal que

$$\lim A_n = \liminf A_n = \limsup A_n.$$

Parte II

Álgebra

Capítulo 8

Operações Binárias, Magmas, Semigrupos e Monoides

A *Álgebra* estuda objetos matemáticos conhecidos como *estruturas algébricas*. As definições desse objeto variam e podem ser tomadas de modo a serem mais ou menos gerais. No entanto, esse objetivos sempre são n-listas em que as entradas são conjuntos e funções. Uma das definições que podem ser tomadas é a de que essas estruturas são listas em que a primeira entrada é um conjunto e as demais são funções. Em geral, essas funções são *operações n-árias*, funções da n-ésima potência de um conjunto nele mesmo. Não definiremos aqui esses objetos com detalhes, nos restringindo somente a casos específicos. Ao leitor fica a oportunidade de perceber as semelhanças entre as definições e generalizá-las, ou mesmo de procurar mais a respeito.

8.1 Operações Binárias

Definição 8.1. Seja X um conjunto não vazio. Uma *operação binária* em X é uma função

$$\begin{aligned} * : X \times X &\to X \\ (x_1, x_2) &\mapsto x_1 * x_2 \end{aligned}$$

Proposição 8.1 (Propriedade de fecho)**.** *Sejam X e Y conjuntos não vazios tais que $Y \subseteq X$ e $*$ uma operação binária em X. Então a restrição $*|_{Y\times Y}$ da operação binária $*$ a $Y \times Y$ é uma operação binária em Y se, e somente se,*

$$\forall y_1, y_2 \in Y \qquad y_1 * y_2 \in Y.$$

Demonstração. Basta notar que, como $Y \subseteq X$, então $Y \times Y \subseteq X \times X$, e a proposição segue da proposição 3.4. ■

Denotamos $*|_{Y\times Y}$ por $*$ quando não há ambiguidade.

Definição 8.2. Seja X um conjunto. Uma operação binária *associativa* é uma operação binária $* : X \times X \to X$ que satisfaz

$$\forall x_1, x_2, x_3 \in X \quad (x_1 * x_2) * x_3 = x_1 * (x_2 * x_3).$$

Uma operação binária *comutativa* é uma operação binária $* : X \times X \to X$ que satisfaz

$$\forall x_1, x_2 \in X \quad x_1 * x_2 = x_2 * x_1.$$

Definição 8.3. Sejam X um conjunto e $+$ uma operação binária em X. Uma operação binária *distributiva* sobre $+$ é uma operação binária $*$ em X que satisfaz

$$\forall x_1, x_2, x_3 \in X \quad x_1 * (x_2 + x_3) = (x_1 * x_2) + (x_1 * x_3).$$

8.2 Magma

Definição 8.4. Um *magma* é um par $\boldsymbol{X} = (X, *)$ em que X é um conjunto não vazio e $*$ é uma operação binária em X.

Definição 8.5. Seja $\boldsymbol{X} = (X, *)$ um magma. Um *elemento neutro* de $\boldsymbol{X}$ é um elemento $e \in X$ que satisfaz

$$\forall x_1 \in X \quad e * x_1 = x_1 = x_1 * e.$$

Pode-se distinguir *elemento neutro à esquerda* e *elemento neutro à direita*, que seria o caso de e se só satisfizesse, respectivamente, as iguadades da esquerda e da direita acima, mas não adotaremos essa distinção neste livro.

Definição 8.6. Seja $\boldsymbol{X} = (X, *)$ um magma com elemento neutro e e $x_1 \in X$. Um *inverso* de x_1 em $\boldsymbol{X}$ é um elemento $x_2 \in X$ que satisfaz

$$x_2 * x_1 = e = x_1 * x_2.$$

Pode-se distinguir *inverso à esquerda* e *inverso à direita*, que seria o caso de x_2 se só satisfizesse, respectivamente, as iguadades da esquerda e da direita acima, mas não adotaremos essa distinção neste livro.

Proposição 8.2. *Seja $\boldsymbol{X} = (X, *)$ um magma. Se existe elemento neutro de $\boldsymbol{X}$, ele é único.*

Demonstração. Suponha que existam dois elementos neutros de $\boldsymbol{X}$, e_1 e e_2. Então

$$e_1 = e_1 * e_2 = e_2.$$

■

Definição 8.7. Seja $\boldsymbol{X}$ um magma, $Y \subseteq X$ e $x \in X$. Definimos

$$x * Y \coloneqq \{x * y : y \in Y\} \quad \text{e} \quad Y * x \coloneqq \{y * x : y \in Y\}.$$

8.3 Semigrupo

Definição 8.8. Um *semigrupo* é um magma $\boldsymbol{X} = (X, *)$ em que $*$ é associativa. Um semigrupo *comutativo* é um semigrupo em que $*$ é comutativa.

Definição 8.9. Seja $\boldsymbol{X} = (X, *)$ um semigrupo e $x_1, \ldots, x_n \in X$. Definimos a operação $*$ entre esses n elementos recursivamente como

$$\overset{n}{\underset{i=1}{\ast}} x_i \coloneqq \begin{cases} x_1 & n = 1 \\ \left(\overset{n-1}{\underset{i=1}{\ast}} x_i \right) * x_n & n > 1. \end{cases}$$

Usualmente, os símbolos usados são o somatório $\bigplus$ para a adição e o produtório $\bigtimes$ para a multiplicação.

Proposição 8.3. *Sejam $\boldsymbol{X} = (X, *)$ um semigrupo, m, n naturais não nulos e $x_1, \cdots, x_{m+n}$ elementos de X. Então*

$$\overset{m}{\underset{i=1}{\ast}} x_i * \overset{n}{\underset{i=1}{\ast}} x_{m+i} = \overset{m+n}{\underset{i=1}{\ast}} x_i.$$

Demonstração. A demonstração será por indução em n. Se $n = 1$, temos que

$$\overset{m}{\underset{i=1}{\ast}} x_i * \overset{1}{\underset{i=1}{\ast}} x_{m+i} = \overset{m}{\underset{i=1}{\ast}} x_i * x_{m+1} = \overset{m+1}{\underset{i=1}{\ast}} x_i.$$

Considere agora que vale a igualdade para n. Então

$$\begin{aligned} \overset{m}{\underset{i=1}{\ast}} x_i * \overset{n+1}{\underset{i=1}{\ast}} x_{m+i} &= \overset{m}{\underset{i=1}{\ast}} x_i * \left(\overset{n}{\underset{i=1}{\ast}} x_{m+i} * x_n \right) \\ &= \left(\overset{m}{\underset{i=1}{\ast}} x_i * \overset{n}{\underset{i=1}{\ast}} x_{m+i} \right) * x_n \\ &= \overset{m+n}{\underset{i=1}{\ast}} x_i * x_n \\ &= \overset{m+n+1}{\underset{i=1}{\ast}} x_i. \end{aligned}$$

■

Essa proposição diz, basicamente, que podemos colocar os parêntesses como quisermos que o resultado será o mesmo.

Notação. Costumamos denotar essa operação por $x_1 * \cdots * x_n$.

Definição 8.10. Seja $\boldsymbol{X} = (X, *)$ um semigrupo comutativo, n um número natural não nulo e ψ uma bijeção do conjunto $\{1, \ldots, n\}$ em si mesmo. Então

$$\overset{n}{\underset{i=1}{\ast}} x_{\psi(i)} = \overset{n}{\underset{i=1}{\ast}} x_i.$$

Demonstração. Usaremos o fato de que $*$ é associativa. A demonstração será por indução em n. Se $n = 1$, a afirmação é óbvia. Considere que vale para n. Seja k um inteiro tal que $\psi(k) = n$. Então

$$\begin{aligned}\overset{n}{\underset{i=1}{\ast}} x_{\psi(i)} &= \overset{k-1}{\underset{i=1}{\ast}} x_{\psi(i)} * x_{\psi(k)} * \overset{n}{\underset{i=k+1}{\ast}} x_{\psi(i)} \\ &= \overset{k-1}{\underset{i=1}{\ast}} x_{\psi(i)} * \overset{n}{\underset{i=k+1}{\ast}} x_{\psi(i)} * x_{\psi(k)}.\end{aligned}$$

Agora, defininamos uma bijeção ϕ do conjunto $\{1, \ldots, n-1\}$ em si mesmo, dada por

$$\phi(m) = \begin{cases} \psi(m) & m < k \\ \psi(m+1) & m > k. \end{cases}$$

Então temos

$$\begin{aligned}\overset{n}{\underset{i=1}{\ast}} x_{\psi(i)} &= \overset{k-1}{\underset{i=1}{\ast}} x_{\psi(i)} * \overset{n}{\underset{i=k+1}{\ast}} x_{\psi(i)} * x_{\psi(k)} \\ &= \overset{n-1}{\underset{i=1}{\ast}} x_{\phi(i)} * x_n \\ &= \overset{n-1}{\underset{i=1}{\ast}} x_i * x_n \\ &= \overset{n}{\underset{i=1}{\ast}} x_i.\end{aligned}$$

■

8.4 Homomorfismo de Semigrupos

Definição 8.11. Sejam $\boldsymbol{X} = (X, *)$ e $\boldsymbol{Y} = (Y, \cdot)$ semigrupos. Um *homomorfismo de semigrupos* de $\boldsymbol{X}$ em $\boldsymbol{Y}$ é uma função $h : X \to Y$ que satisfaz

$$\forall x_1, x_2 \in X \qquad h(x_1 * x_2) = h(x_1) \cdot h(x_2).$$

Denotamo-lo por $h : \boldsymbol{X} \to \boldsymbol{Y}$.

Proposição 8.4 (Composição de homomorfismos é homomorfismo)**.** *Sejam* $\boldsymbol{X}_1 = (X, *_1)$*,* $\boldsymbol{X}_2 = (X_2, *_2)$ *e* $\boldsymbol{X}_3 = (X_3, *_3)$ *semigrupos e* $h_1 : \boldsymbol{X}_1 \to \boldsymbol{X}_2$ *e* $h_2 : \boldsymbol{X}_2 \to \boldsymbol{X}_3$ *homomorfismos de semigrupos. Então* $h_2 \circ h_1 : \boldsymbol{X}_1 \to \boldsymbol{X}_3$ *é homomorfismo de semigrupos.*

Demonstração. Sejam $x_1, x_2 \in X_1$. Então

$$\begin{aligned}(h_2 \circ h_1)(x_1 *_1 x_2) &= h_2(h_1(x_1 *_1 x_2)) \\ &= h_2(h_1(x_1) *_2 h_1(x_2)) \\ &= h_2(h_1(x_1)) *_3 h_2(h_1(x_2)) \\ &= (h_2 \circ h_1)(x_1) *_3 (h_2 \circ h_1)(x_2).\end{aligned}$$

■

8.5 Monoide

Definição 8.12. Um *monoide* é um semigrupo $\boldsymbol{M} = (M, *)$ que tem elemento neutro. Um monoide *comutativo* é um monoide em que $*$ é comutativa.

Notação. Costumamos denotar o elemento neutro de um monoide $\boldsymbol{M}$ por e_M. Quando não há ambiguidade, denotamos o elemento neutro por e. Ainda, como existe elemento neutro, definimos $\ast_{i=1}^{n} x_i = e$ quando $n \leq 0$.

Exemplo 8.1. O conjunto $\mathbb{N}$ com a função

$$\begin{aligned}\max : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (m, n) &\mapsto \begin{cases} m & m \geq n \\ n & m < n \end{cases}\end{aligned}$$

formam um monoide comutativo com elemento neutro 0.

Proposição 8.5. *Seja* $(M, *)$ *um monoide com elemento neutro* e*. Se* $m \in M$ *tem inverso sob* $*$*, ele é único.*

Demonstração. Suponha que existam dois inversos n_1 e n_2 de m. Então

$$n_1 = n_1 * e = n_1 * (m * n_2) = (n_1 * m) * n_2 = e * n_2 = n_2.$$

■

Notação. Isso nos permite denotar o inverso de um elemento $x \in X$ por $\overline{x}$. Em geral, a notação do inverso pode ser outra. Quando a operação binária é a adição $(+)$, denotamos o inverso por $-m$. Quando é a multiplicação $(\cdot)$, denotamo-lo por m^{-1}.

Proposição 8.6. *Seja $(M, *)$ um monoide com elemento neutro e. Se $m \in M$ tem inverso sob $*$, então*

$$(m^{-1})^{-1} = m.$$

Demonstração.

$$\begin{aligned}(m^{-1})^{-1} &= (m^{-1})^{-1} * e \\ &= (m^{-1})^{-1} * (m^{-1} * m) \\ &= ((m^{-1})^{-1} * m^{-1}) * m \\ &= e * m \\ &= m.\end{aligned}$$

■

Definição 8.13. Seja $\boldsymbol{M} = (M, *)$ um monoide. Um *submonoide* de $\boldsymbol{M}$ é um monoide $\boldsymbol{S} = (S, *_S)$ em que $S \subseteq M$ e $*_S = *|_{S\times S}$. Denota-se $\boldsymbol{S} \leq \boldsymbol{S}$. Um submonoide *próprio* de $\boldsymbol{M}$ é um monoide $\boldsymbol{S} \leq \boldsymbol{M}$ em que M é um subconjunto próprio de M ($S \subset M$). Denota-se $\boldsymbol{S} < \boldsymbol{M}$.

Proposição 8.7. *Sejam $\boldsymbol{M} = (M, *)$ um monoide e $S \subseteq M$. Então $\boldsymbol{S} = (S, *|_{S\times S})$ é um monoide com $e \in S$ se, e somente se,*

1. *(Identidade) $e \in S$.*
2. *(Fechamento) $\forall\ s_1, s_2 \in S \quad s_1 * s_2 \in S$;*

Ainda, se $\boldsymbol{M}$ é comutativo, então $\boldsymbol{S}$ é comutativo.

Demonstração. Por simplicidade, definamos $\star := *_{S\times S}$.

($\Rightarrow$) Suponhamos que $\boldsymbol{S}$ é um monoide com $e \in S$. (Identidade) Então vale a identidade. (Fechamento) Como $\boldsymbol{S}$ é um monoide, $\star$ é uma operação binária, portanto segue que a propriedade de fechamento (8.1).

($\Leftarrow$) Suponhamos que valem as propriedades listadas. (Operação binária) Pela identidade, segue que $S \neq \emptyset$, e disso e do fechamento, segue que $\star$ é uma operação binária (8.1). (Associatividade) Sejam $s_1, s_2, s_3 \in S$. Da associatividade de $*$ segue que

$$(s_1 \star s_2) \star s_3 = (s_1 * s_2) * s_3 = s_1 * (s_2 * s_3) = s_1 \star (s_2 \star s_3).$$

Logo $\star$ é associativa. (Identidade) Seja $s \in S$. Como $e \in S$, da identidade de $*$ segue que

$$e \star s = e * s = s = s * e = s \star e.$$

Logo e é identidade de $\boldsymbol{S}$.

Por fim, suponhamos que $\boldsymbol{M}$ é um monoide comutativo. Sejam $s_1, s_2 \in S$. Como $*$ é comutativa, então

$$s_1 \star s_2 = s_1 * s_2 = s_2 * s_1 = s_2 \star s_1.$$

Logo $\star$ é comutativa. ■

Vale observar que, somente sabendo que $\boldsymbol{S}$ é um monoide, isto é, que um subconjunto S de um monoide $\boldsymbol{M}$ com a operação do monoide restrita a esse subconjunto formam um monoide, não podemos garantir que o elemento neutro de $\boldsymbol{S}$ é o mesmo que o de $\boldsymbol{M}$.

8.6 Homomorfismos de Monoides

Definição 8.14. Sejam $\boldsymbol{M} = (M, *)$ e $\boldsymbol{N} = (N, \cdot)$ monoides com elementos neutros e_M e e_N, respectivamente. Um *homomorfismo de monoides* de $\boldsymbol{M}$ em $\boldsymbol{N}$ é uma função $h : M \to N$ que satisfaz

1. h é um homomorfismo de semigrupos de $\boldsymbol{M}$ em $\boldsymbol{N}$:

   (a) $\forall m_1, m_2 \in X \qquad h(m_1 * m_2) = h(m_1) \cdot h(m_2)$;

2. $h(e_M) = e_N$.

Denotamo-lo por $h : \boldsymbol{M} \to \boldsymbol{N}$.

Podemos notar que precisamos garantir que a função h leve o elemento neutro de um monoide no elemento neutro de outro, já que isso não seria verdade se função fosse somente um homomorfismo de semigrupos. No entanto, mesmo sem a segunda propriedade, um homomorfismo de semigrupos entre grupos garante que a imagem do elemento neutro do primeiro seja um elemento neutro do conjunto imagem. Veremos mais adiante que um homomorfismo de grupos é simplesmente um homomorfismo de semigrupos, pois ele é suficiente para preservar a estrutura algébrica de grupos.

Proposição 8.8 (Composição de homomorfismos é homomorfismo)**.** *Sejam $\boldsymbol{M}_1 = (M_1, *_1)$, $\boldsymbol{M}_2 = (M_2, *_2)$ e $\boldsymbol{M}_3 = (M_3, *_3)$ monoides e $h_1 : \boldsymbol{M}_1 \to \boldsymbol{M}_2$ e $h_2 : \boldsymbol{M}_2 \to \boldsymbol{M}_3$ homomorfismos de monoides. Então $h_2 \circ h_1 : \boldsymbol{M}_1 \to \boldsymbol{M}_3$ é homomorfismo de monoides.*

Demonstração. 1. Como homomorfismos de monoides são homomorfismos de semigrupos, o resultado segue da proposição na seção de semigrupos que afirma que composição de homomorfismos é homomorfismo (8.4).

2. Sejam e_1, e_2 e e_3 os elementos neutros de $\boldsymbol{M}_1$, $\boldsymbol{M}_2$ e $\boldsymbol{M}_3$, respectivamente. Então
$$(h_2 \circ h_1)(e_1) = h_2(h_1(e_1)) = h_2(e_2) = e_3.$$

■

Capítulo 9

Grupos

9.1 Grupo

Definição 9.1. Um *grupo* é um par $\boldsymbol{G} = (G, *)$ em que G é um conjunto e $* : G \times G \to G$ é uma operação binária que satisfaz

(Associatividade)	$\forall g_1, g_2, g_3 \in G$	$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$
(Identidade)	$\exists e \in G \ \forall g \in G$	$e * g = g = g * e$
(Invertibilidade)	$\forall g \in G \ \exists g^{-1} \in G$	$g^{-1} * g = e = g * g^{-1}$

Um grupo *comutaivo* é um grupo que satisfaz

(Comutatividade)	$\forall g_1, g_2 \in G$	$g_1 * g_2 = g_2 * g_1$

Notação. Denotaremos o inverso de $g \in G$ por g^{-1} e $g_1 * g_2$ por $g_1 g_2$. Quando o grupo é comutativo, podemos usar $+$ para denotar sua operação binária. Nesse caso, o inverso de $g \in G$ é denotado por $-g$.

Em vista das definições introdutórias do capítulo anterior, um grupo é um monoide $\boldsymbol{G} = (G, *)$ em que todos elementos de G têm inverso sob $*$, e um grupo comutaivo é um grupo em que $*$ é comutativa.

Definição 9.2. Seja $\boldsymbol{G} = (G, *)$ um grupo, $g \in G$ e $n \in \mathbb{N}$. Definimos

$$g^n \coloneqq \overset{n}{\underset{i=1}{\ast}} g \quad \text{e} \quad g^{-n} \coloneqq \overset{n}{\underset{i=1}{\ast}} g^{-1}.$$

Proposição 9.1 (Lei do corte em grupos)**.** *Seja $\boldsymbol{G}$ um grupo. Então*

1. $\forall g, g_1.g_2 \in G \qquad gg_1 = gg_2 \quad \Rightarrow \quad g_1 = g_2.$

2. $\forall g, g_1.g_2 \in G \qquad g_1 g = g_2 g \quad \Rightarrow \quad g_1 = g_2.$

3. $\forall g_1, \ldots, g_n \in G \qquad (g_1 \cdots g_n)^{-1} = g_n^{-1} \cdots g_1^{-1}.$

Demonstração. Se $gg_1 = gg_2$, então

$$g_1 = (g^{-1}g)g_1 = g^{-1}(gg_1) = g^{-1}(gg_2) = (g^{-1}g)g_2 = g_2.$$

A demonstração da segunda implicação é análoga. ■

9.2 Subgrupo

Definição 9.3. Seja $\boldsymbol{G} = (G, *)$ um grupo. Um *subgrupo* de $\boldsymbol{G}$ é um grupo $\boldsymbol{S} = (S, \star)$ em que $S \subseteq G$ e $\star = *|_{S\times S}$. Denota-se $\boldsymbol{S} \leq \boldsymbol{G}$. Um subgrupo *próprio* de $\boldsymbol{G}$ é um subgrupo $\boldsymbol{S} \leq \boldsymbol{G}$ em que S é um conjunto próprio de G ($S \subset G$). Denota-se $\boldsymbol{S} < \boldsymbol{G}$.

Proposição 9.2. *Sejam $\boldsymbol{G}$ um grupo e $S \subseteq G$. Então $\boldsymbol{S} = (S, *|_{S\times S})$ é um grupo se, e somente se, S satisfaz*

(Não-vacuidade)	$S \neq \emptyset$	
(Fechamento da multiplicação)	$\forall\ s_1, s_2 \in S$	$s_1 s_2 \in S$
(Fechamento da inversão)	$\forall\ s \in S$	$s^{-1} \in S$

Ainda, se $\boldsymbol{G}$ é comutativo, então $\boldsymbol{S}$ é comutativo.

Demonstração. Por simplicidade, definamos $\star \coloneqq *|_{S\times S}$.

($\Rightarrow$) (Não-vacuidade) Como $\boldsymbol{S}$ é um grupo, $e \in S$, portanto $S \neq \emptyset$. (Fechamento da multiplicação) Como $\boldsymbol{S}$ é grupo, $\star$ é uma operação binária, portanto segue que, para todo $s_1, s_2 \in S$, $s_1 s_2 \in S$ (8.1). (Fechamento da inversão) Seja $s \in S$. Como $\boldsymbol{S}$ é grupo, existe $s^{-1} \in S$ inverso de s em $\boldsymbol{S}$. Como $s^{-1} \in G$, segue da unicidade do inverso que s^{-1} é o inverso de s em $\boldsymbol{G}$.

($\Leftarrow$) (Operação binária) Pela primeira e segunda propriedades de S, segue que $\star$ é uma operação binária (8.1). (Associatividade) Sejam $s_1, s_2, s_3 \in S$. Então

$$(s_1 \star s_2) \star s_3 = (s_1 * s_2) * s_3 = s_1 * (s_2 * s_3) = s_1 \star (s_2 \star s_3).$$

(Identidade) Como $S \neq \emptyset$, existe $s \in S$, portanto $s^{-1} \in S$. Isso implica que $e = s * s^{-1} \in S$ e, como e é elemento neutro de $\boldsymbol{G}$, segue que, para todo $s \in S$,

$$e \star s = e * s = s = s * e = s \star e.$$

(Invertibilidade) Seja $s \in S$. Pela terceira propriedade de S, segue que o inverso de s em $\boldsymbol{G}$ pertence a S. Então

$$s^{-1} \star s = s^{-1} * s = e = s * s^{-1} = s \star s^{-1},$$

portanto s^{-1} é o inverso de s em $\boldsymbol{S}$.

(Comutatividade) Por fim, suponhamos que $\boldsymbol{G}$ é um grupo comutativo. Sejam $s_1, s_2 \in S$. Como $*$ é comutativa, então

$$s_1 \star s_2 = s_1 * s_2 = s_2 * s_1 = s_2 \star s_1.$$

■

Proposição 9.3. *Sejam $\boldsymbol{G}$ um grupo e $\mathcal{G}$ o conjunto dos subgrupos de $\boldsymbol{G}$. Então $(\mathcal{G}, \leq)$ é um conjunto parcialmente ordenado.*

Demonstração. Claramente, $\boldsymbol{G} \in \mathcal{G}$, portanto $\mathcal{G}$ não é vazio. Mostremos que $\leq$ é uma ordem parcial em $\mathcal{G}$. (Reflexividade) Seja $\boldsymbol{S} \in \mathcal{G}$. Então $\boldsymbol{S} \leq \boldsymbol{S}$, pois $\boldsymbol{S}$ é um grupo, $S \subseteq S$ e $*|_{S\times S} = *|_{S\times S}$. (Antissimetria) Sejam $\boldsymbol{S_1}, \boldsymbol{S_2} \in \mathcal{G}$ tais que $\boldsymbol{S_1} \leq \boldsymbol{S_2}$ e $\boldsymbol{S_2} \leq \boldsymbol{S_1}$. Então $S_1 \subseteq S_2$ e $S_2 \subseteq S_1$, o que implica $S_1 = S_2$, e portanto $*|_{S_1\times S_1} = *|_{S_2\times S_2}$, o que implica $\boldsymbol{S_1} = \boldsymbol{S_2}$. (Transitividade) Sejam $\boldsymbol{S_1}, \boldsymbol{S_2}, \boldsymbol{S_3} \in \mathcal{G}$ tais que $\boldsymbol{S_1} \leq \boldsymbol{S_2}$ e $\boldsymbol{S_2} \leq \boldsymbol{S_3}$. Então $S_1 \subseteq S_2$ e $S_2 \subseteq S_3$, o que implica $S_1 \subseteq S_3$ e, portanto, $*_{S_1} = *|_{S_3\times S_3}$. ■

Proposição 9.4. *Seja $\boldsymbol{G}$ um grupo. Então $\boldsymbol{\{e\}}$ e $\boldsymbol{G}$ são subgrupos de $\boldsymbol{G}$.*

Proposição 9.5. *Sejam $\boldsymbol{G}$ um grupo, $(\boldsymbol{S}_i)_{i\in I}$ uma família de subgrupos de $\boldsymbol{G}$ e*

$$S \coloneqq \bigcap_{i\in I} S_i.$$

Então $\boldsymbol{S}$ é um subgrupo de $\boldsymbol{G}$.

Demonstração. (Não-vacuidade) Para todo $i \in I$, $\boldsymbol{S_i} \leq \boldsymbol{G}$, portanto $e \in N_i$. Logo $e \in N$. (Fechamento da multiplicação) Sejam $s_1, s_2 \in S$. Para todo $i \in I$, $s_1, s_2 \in S_i$. Como $\boldsymbol{S_i} \leq \boldsymbol{G}$, segue que $s_1 s_2 \in S_i$, o que implica que $s_1 s_2 \in S$. (Fechamento da inversão) Seja $s \in S$. Para todo $i \in I$, $s \in S_i$ e, como $\boldsymbol{S_i} \leq \boldsymbol{G}$, segue que $s^{-1} \in S_i$, o que implica que $s^{-1} \in S$. ■

Proposição 9.6. *Sejam $\boldsymbol{G}$ um grupo, $(\boldsymbol{S}_i)_{i\in I}$ uma família de subgrupos de $\boldsymbol{G}$ que satisfaz*

$$\forall i_1, i_2 \in I \ \exists i \in I \qquad S_{i_1} \subseteq S_i \ \ e \ \ S_{i_2} \subseteq S_i$$

e

$$S \coloneqq \bigcup_{i\in I} S_i.$$

Então $\boldsymbol{S}$ é um subgrupo de $\boldsymbol{G}$.

Demonstração. (Não-vacuidade) Para todo $i \in I$, $\boldsymbol{S_i} \leq \boldsymbol{G}$, portanto $e \in N_i$. Logo $e \in N$. (Fechamento) Sejam $s_1, s_2 \in S$. Existem $i_1, i_2 \in I$ tais que $s_1 \in S_{i_1}$ e $s_2 \in S_{i_2}$ e, pela propriedade, existe $i \in I$ tal que $S_{i_1} \subseteq S_i$ e $S_{i_2} \subseteq S_i$. Então $s_1, s_2 \in S_i$. Como $\boldsymbol{S_i} \leq \boldsymbol{G}$, segue que $s_1 s_2 \in S_i$, o que implica que $s_1 s_2 \in S$. (Invertibilidade) Seja $s \in S$. Existe $i \in I$ tal que $s \in N_i$ e, como $\boldsymbol{S_i} \leq \boldsymbol{G}$, segue que $s^{-1} \in S_i$, o que implica que $s^{-1} \in S$. ■

A propriedade definida acima é equivalente a dizer que a família $(S_i)_{i \in I}$ é um conjunto dirigido com respeito a $\subseteq$.

Definição 9.4. Seja $\boldsymbol{M}$ um monoide. O conjunto dos elementos invertíveis de M é denotado por M^*.

O asterisco não tem a ver com a operação $*$ do monoide.

Proposição 9.7. *Seja $\boldsymbol{M} = (M, *)$ um monoide com elemento neutro e_M. Então $\boldsymbol{M^*} = (M^*, *|_{M^* \times M^*})$ é um grupo.*

Demonstração. Sejam $m_1, m_2 \in M^*$. Então existem $m_1^{-1}, m_2^{-1} \in M$ tais que

$$m_1 m_1^{-1} = e_M \quad \text{e} \quad m_2 m_2^{-1} = e_M.$$

Portanto

$$(m_1 m_2)(m_2^{-1} m_1^{-1}) = m_1 (m_2 m_2^{-1}) m_1^{-1} = m_1 m_1^{-1} = e_M,$$

o que mostra que $m_1 m_2 \in M^*$. Ainda, note que $e_M \in M^*$, pois $e_M * e_M = e_M$. Logo M^* é um submonoide de M e, portanto, $\boldsymbol{M^*}$ é um monoide (8.7). Por fim, $\boldsymbol{M^*}$ é um grupo pois, por definição, todo elemento tem inverso. ■

9.3 Coclasses e Índice de Subgrupo

Definição 9.5. Sejam $\boldsymbol{G}$ um grupo, $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo e $g \in G$. A *coclasse à esquerda* de $\boldsymbol{S}$ em $\boldsymbol{G}$ com *representante* g é o conjunto

$$gS \coloneqq \{gs : s \in S\}.$$

A *coclasse à direita* de $\boldsymbol{S}$ em $\boldsymbol{G}$ com *representante* g é o conjunto

$$Sg \coloneqq \{sg : s \in S\}.$$

Coclasses também são conhecidas como classes laterais. As definições de coclasses à esquerda ou à direita são análogas e, por consequência, toda definição ou proposição envolvendo uma das duas tem uma definição ou proposição dual envolvendo a outra. Por esse motivo, durante este capítulo consideraremos sempre coclasses à esquerda.

Proposição 9.8. *Sejam $\boldsymbol{G}$ um grupos, $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo e $g_1 g_2 \in G$. Então*

1. $g_1(g_2 S) = (g_1 g_2)S \quad e \quad (Sg_1)g_2 = S(g_1 g_2)$
2. $g_1 S = g_2 S \Leftrightarrow g_2^{-1} g_1 \in S$ *e* $Sg_1 = Sg_2 \Leftrightarrow g_2^{-1} g_1 \in S$.

Demonstração. 1. ($\subseteq$) Seja $g \in g_1(g_2 S)$. Existem $g' \in g_2 S$ tal que $g = g_1 g'$ e, portanto, existe $s \in S$ tal que $g' = g_2 s$. Mas então, pela associatividade, $g = g_1(g_2 s) = (g_1 g_2)s$, e segue que $g \in (g_1 g_2)S$. ($\supseteq$) Seja $g \in (g_1 g_2)S$. Então existe $s \in S$ tal que $g = (g_1 g_2)s$ e, da associatividade, segue que $g = g_1(g_2 s)$, logo $g \in g_1(g_2 S)$. A outra igualdade é análoga.

2. ($\Leftarrow$) Seja $g \in g_1 S = g_2 S$. Então existem $s, s' \in S$ tais que $g = g_1 s = g_2 s'$, logo $g_2^{-1} g_1 = s' s^{-1}$. Como $\boldsymbol{S}$ é subgrupo, segue que $g_2^{-1} g_1 = s' s^{-1} \in S$.

   ($\Rightarrow$) ($\subseteq$) Se $g_2^{-1} g_1 \in S$, existe $s \in S$ tal que $g_2^{-1} g_1 = s$, portanto $g_1 = g_2 s$, logo $g_1 \in g_2 S$. Assim, dado $g \in g_1 S$, existe $s' \in S$ tal que $g = g_1 s'$. Como $\boldsymbol{S}$ é subgrupo, $ss' \in S$, logo $g = g_2 ss' \in g_2 S$. ($\supseteq$) Da mesma forma, como $\boldsymbol{S}$ é subgrupo, $g_1^{-1} g_2 = (g_2^{-1} g_1)^{-1} = s^{-1} \in S$, o que implica que $g_2 = g_1 s^{-1} \in g_1 S$. Assim, dado $g \in g_2 S$, existe $s' \in S$ tal que $g = g_2 s'$. Como $\boldsymbol{S}$ é subgrupo, $s^{-1} s' \in S$, logo $g = g_1 s^{-1} s' \in g_2 S$.

■

Essa proposição nos permite denotar os conjuntos acima simplesmente por $g_1 g_2 S$ e $S g_1 g_2$, respectivamente.

A proposição a seguir mostra que as cardinalidades das coclasses de um subgrupo são sempre iguais.

Proposição 9.9. *Sejam $\boldsymbol{G}$ um grupo, $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo e $g_1, g_2 \in G$. Então*

$$|g_1 S| = |g_2 S| .$$

Demonstração. Considere a relação

$$\begin{aligned} f : g_1 S &\to g_2 S \\ g &\mapsto g_2 g_1^{-1} g. \end{aligned}$$

Vamos mostrar que f é função; isto é, está bem definida, que $g_1^{-1} g \in S$. Primeiro, note que, se $g \in g_1 S$, existe $s \in S$ tal que $g = g_1 s$. Então segue que $f(s) = g_2 g_1^{-1} g = g_2 g_1^{-1} g_1 s = g_2 s \in g_2 S$, o que mostra que f está bem definida. Agora, note que a função

$$\begin{aligned} f^{-1} : g_2 S &\to g_1 S \\ g &\mapsto g_1 g_2^{-1} g, \end{aligned}$$

que está bem definida pelo mesmo argumento de cima, é a inversa de f, pois $f^{-1} \circ f = \mathbb{1}_{g_1 S}$ e $f \circ f^{-1} = \mathbb{1}_{g_2 S}$. Isso mostra que f é uma bijeção. Portanto $|g_1 S| = |g_2 S|$.

■

Proposição 9.10. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo. A relação binária $\sim$ em G definida por*

$$g_1 \sim g_2 \quad \iff \quad g_2^{-1} g_1 \in S$$

é uma relação de equivalência e suas classes de equivalência são as coclasses à esquerda (à direita) de $\boldsymbol{S}$ em $\boldsymbol{G}$.

Demonstração. Primeiro vamos demonstrar as três propriedades de relação de equivalência. (Reflexividade) Seja $g \in G$. Então $g^{-1} g = e \in S$, pois S é subgrupo. Logo $g \sim g$. (Simetria) Sejam $g_1, g_2 \in G$. Se $g_2^{-1} g_1 \in S$, como S é subgrupo, então $g_1^{-1} g_2 = (g_2^{-1} g_1)^{-1} \in S$. Logo $g_2 \sim g_1$. (Transitividade) Sejam $g_1, g_2, g_3 \in G$. Se $g_1 \sim g_2$ e $g_2 \sim g_3$, então $g_2^{-1} g_1 \in S$ e $g_3^{-1} g_2 \in S$. Como S é subgrupo, segue que $g_3^{-1} g_1 = g_3^{-1} g_2 g_2^{-1} g_1 \in S$. Logo $g_1 \sim g_3$.

Agora, seja $g \in G$. Vamos mostrar que $[g] = gS$. Seja $s \in [g]$. Então $s \sim g$, o que implica que $g^{-1} s \in S$, que por sua vez implica que existe $s' \in S$ tal que $s' = g^{-1} s$ e, portanto, $s = g s'$. Logo $s \in gS$. Agora, seja $s \in gS$. Então existe $s' \in S$ tal que $s = g s'$, o que implica $g^{-1} s = s'$, que por sua ve implica $g^{-1} s \in S$ e, portanto, $s \sim g$. Logo $s \in [g]$. ■

Como $\sim$ é relação de equivalência, particiona G, e essas partições são as coclasses de $\boldsymbol{S}$ em $\boldsymbol{G}$. Assim, podemos considerar o conjunto G/S das classes de equivalências como o conjunto das coclasses de S em $\boldsymbol{G}$. É importante notar que esse conjunto ainda não possui estrutura de grupo. Isso será possível mais à frente, mas não para qualquer subgrupo, somente subgrupos que chamamos de normais.

Definição 9.6. Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo. O *conjunto quociente* de $\boldsymbol{G}$ por $\boldsymbol{S}$ é o conjunto

$$G/S \coloneqq G/\sim .$$

Definição 9.7. Seja $\boldsymbol{G}$ um grupo e $\boldsymbol{S} \leq \boldsymbol{G}$ subgrupo. O *índice* de $\boldsymbol{S}$ em $\boldsymbol{G}$ é número cardinal

$$[G : S] \coloneqq |G/S| .$$

Proposição 9.11. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo. Então*

$$|G| = [G : S] \times |S| .$$

Demonstração. O conjunto G/S é uma partição de G, pois é um conjunto quociente (4.1). Isso implica que G/S é uma família de conjuntos não vazios, disjuntos dois a dois, e que $G = \bigcup_{[g]\in G/S} gS$. Da terceira condição temos que

$$|G| = \left| \bigcup_{[g]\in G/S} gS \right|.$$

Da segunda condição, temos por 5.3 que

$$\left| \bigcup_{[g]\in G/S} gS \right| = \left| \bigsqcup_{[g]\in G/S} gS \right|.$$

Por fim, da primeira condição e do fato de que as coclasses de S têm a mesma cardinalidade, concluímos por 5.4 que

$$\left| \bigsqcup_{[g]\in G/S} gS \right| = |G/S| \times |S|\,.$$

Disso segue que $|G| = [G : S] \times |S|$. ■

9.4 Subgrupo Normal e Grupo Quociente

Definição 9.8. Seja $\boldsymbol{G}$ um grupo. Um subgrupo *normal* de $\boldsymbol{G}$ é um subgrupo $\boldsymbol{N \leq G}$ que satsfaz

(Normalidade) $\qquad \forall g \in G\ \forall n \in N \qquad gng^{-1} \in N$

Denota-se $\boldsymbol{N \trianglelefteq G}$. Um subgrupo normal *próprio* de $\boldsymbol{G}$ é um subgrupo $\boldsymbol{N \trianglelefteq G}$ que é um conjunto próprio de G: $N \subset G$. Denota-se $\boldsymbol{N \triangleleft G}$.

Proposição 9.12. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{N \leq G}$ um subgrupo. São equivalentes:*

1. $\boldsymbol{N \trianglelefteq G}$*;*
2. $\forall g \in G \qquad N = gNg^{-1}$*;*
3. $\forall g \in G \qquad gN = Ng$*;*
4. $\forall g_1, g_2 \in G \qquad g_1g_2N = g_2g_1N$*.*

Proposição 9.13. *Seja $\boldsymbol{G}$ um grupo. Então $\boldsymbol{\{e\}}$ e $\boldsymbol{G}$ são subgrupos normais de $\boldsymbol{G}$.*

Proposição 9.14. *Sejam $\boldsymbol{G}$ um grupo, $(\boldsymbol{N}_i)_{i\in I}$ uma família de subgrupos normais de $\boldsymbol{G}$ e*

$$N \coloneqq \bigcap_{i\in I} N_i.$$

Então $\boldsymbol{N}$ é um subgrupo normal de $\boldsymbol{G}$.

Demonstração. (Subgrupo) Como $(\boldsymbol{N}_i)_{i\in I}$ uma família de subgrupos de $\boldsymbol{G}$, segue que $\boldsymbol{N}$ é um subgrupo de $\boldsymbol{G}$ (9.5). (Normalidade) Sejam $g \in G$ e $n \in N$. Para todo $i \in I$, $n \in N_i$, portanto $gng^{-1} \in N_i$, o que implica $gng^{-1} \in N$. ■

Conjectura 9.15. *Sejam $\boldsymbol{G}$ um grupo, $(\boldsymbol{N}_i)_{i\in I}$ uma família de subgrupos normais de $\boldsymbol{G}$ que satisfaz*

$$\forall i_1, i_2 \in I \ \exists i \in I \qquad N_{i_1} \subseteq N_i \ \ e \ \ N_{i_2} \subseteq N_i$$

e

$$N \coloneqq \bigcup_{i\in I} N_i.$$

Então $\boldsymbol{N}$ é um subgrupo normal de $\boldsymbol{G}$.

Demonstração. (Subgrupo) Como $(\boldsymbol{N}_i)_{i\in I}$ uma família de subgrupos de $\boldsymbol{G}$ com a propriedade enunciada, segue que $\boldsymbol{N}$ é um subgrupo de $\boldsymbol{G}$ (9.6). (Normalidade) Sejam $g \in G$ e $n \in N$. Existe $i \in I$ tal que $n \in N_i$, portanto $gng^{-1} \in N_i$, o que implica $gng^{-1} \in N$. ■

A propriedade definida acima é equivalente a dizer que a família $(N_i)_{i\in I}$ é um conjunto dirigido com respeito a $\subseteq$.

Definição 9.9. Seja $\boldsymbol{G}$ um grupo e $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ um subgrupo normal. O *grupo quociente* de $\boldsymbol{G}$ por $\boldsymbol{N}$ é o par $\boldsymbol{G/N} = (G/N, *)$, em que G/N é o conjunto quociente de G pela relação de equivalência induzida por N e

$$\begin{aligned} * : G/N \times G/N &\to G/N \\ (g_1N, g_2N) &\mapsto g_1g_2N. \end{aligned}$$

Uma notação um pouco mais cuidadosa ressaltaria que as operações binárias de $\boldsymbol{G}$ e de $\boldsymbol{G/N}$ não são a mesma e, se denotarmos a primeira como $*$ e a segunda como $\star$, teríamos a definição acima nos dando $g_1N \star g_2N \coloneqq (g_1 * g_2)N$. No entanto, como $*$ de G/N está sempre relacionada a $*$ de G, mantemos a mesma notação para ambas e a mesma convenção de omiti-la quando possível. Vale notar, também, que pela associatividade da $*$ de $\boldsymbol{G}$, temos que $g_1g_2N = g_1(g_2N) = (g_1g_2)N$.

Proposição 9.16. *Seja $\boldsymbol{G}$ um grupo e $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ um subgrupo normal. Então $\boldsymbol{G/N}$ é um grupo.*

Demonstração. Para simplificar as contas, usaremos a notação $[g] = gN$ quando conveniente. (Operação Binária) Devemos mostrar que a função definida acima está bem definida. Sejam $g_1, g_1', g_2, g_2' \in G$ tais que $g_1N = g_1'N$ e $g_2N = g_2'N$. Então

$$g_1g_2N = g_1Ng_2 = g_1'Ng_2 = g_1'Ng_2 = g_1'g_2N = g_1'g_2'N.$$

(Associatividade) Sejam $g_1, g_2, g_3 \in G$. Da associatividade da $*$ de $\boldsymbol{G}$ segue que

$$([g_1][g_2])[g_3] = [g_1g_2][g_3] = [g_1g_2g_3] = [g_1][g_2g_3] = [g_1]([g_2][g_3]).$$

(Elemento Neutro) Seja $e \in G$ elemento neutro e $g \in G$. Então

$$[e][g] = [eg] = [g] = [ge] = [g][e].$$

(Inverso) Seja $g \in G$. Então

$$[g^{-1}][g] = [g^{-1}g] = [e] = [gg^{-1}] = [g][g^{-1}].$$

■

9.5 Homomorfismo de Grupo

Definição 9.10. Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos. Um *homomorfismo de grupos* de $\boldsymbol{G_1}$ em $\boldsymbol{G_2}$ é uma função $h : G_1 \to G_2$ que satisfaz

$$\forall g_1, g_2 \in G_1 \qquad h(g_1g_2) = h(g_1)h(g_2).$$

Denota-se $h : \boldsymbol{G_1} \to \boldsymbol{G_2}$. O conjunto de todos esses homomorfismos é denotado por $\mathcal{H}\mathrm{om}(\boldsymbol{G_1}, \boldsymbol{G_2})$.

Note que a propriedade de homomorfismos de semigrupos e de grupos é a mesma.

Proposição 9.17 (Homomorfismos preservam a estrutura algébrica)**.** *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos com elementos neutros e_1 e e_2, respectivamente, e $h : \boldsymbol{G_1} \to \boldsymbol{G_2}$ um homomorfismo de grupos. Então*

1. $h(e_1) = e_2$;
2. $\forall g \in G_1 \qquad h(g)^{-1} = h(g^{-1})$.

Demonstração. Seja $g \in G$. Então

1.

$$\begin{aligned} h(e_1) &= h(e_1)e_2 \\ &= h(e_1)h(g)h(g)^{-1} \\ &= h(e_2g)h(g)^{-1} \\ &= h(g)h(g)^{-1} \\ &= e_2. \end{aligned}$$

2.

$$\begin{aligned} h(g)^{-1} &= h(g)^{-1}e_2 \\ &= h(g)^{-1}h(e_1) \\ &= h(g)^{-1}h(gg^{-1}) \\ &= h(g)^{-1}h(g)h(g^{-1}) \\ &= e_2h(g^{-1}) \\ &= h(g^{-1}). \end{aligned}$$

■

Essa proposição mostra que, como mencionado na seção de monoides, um homomorfismo de grupos é, de fato, um homomorfismo de monoides que preserva a inversa.

Corolário 9.18 (Composição de homomorfismos é homomorfismo)**.** *Sejam* $\boldsymbol{G_1}$, $\boldsymbol{G_2}$ *e* $\boldsymbol{G_3}$ *grupos e* $h_1 : \boldsymbol{G_1} \to \boldsymbol{G_2}$ *e* $h_2 : \boldsymbol{G_2} \to \boldsymbol{G_3}$ *homomorfismos de grupos. Então* $(h_2 \circ h_1) : \boldsymbol{G_1} \to \boldsymbol{G_3}$ *é um homomorfismo de grupos.*

Demonstração. Como um homomorfismo de grupos é um homomorfismo de semigrupos, o resultado segue da proposição na seção de semigrupos que afirma que composição de homomorfismos é homomorfismo (8.4). ■

Proposição 9.19. *Sejam* $\boldsymbol{G}$ *um grupo e* $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ *um subgrupo normal. Então a projeção canônica* $\pi : G \to G/N$*, definida por*

$$\begin{aligned} \pi : G &\to G/N \\ g &\mapsto gN \end{aligned}$$

é um homomorfismo de grupos sobrejetivo.

Demonstração. Sejam $g_1, g_2 \in G$. Então, da definição de prduto em $\boldsymbol{G/N}$, segue que

$$\pi(g_1g_2) = g_1g_2N = g_1Ng_2N = \pi(g_1)\pi(g_2).$$

(Sobrejetividade) Seja $gN \in G/N$. Então, $g \in G$, temos que $h(g) = gN$. ■

Proposição 9.20. *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \to \boldsymbol{G_2}$ um homomorfismo de grupos. Se $\boldsymbol{S} \leq \boldsymbol{G_2}$ é um subgrupo, então $\boldsymbol{h^{-1}(S)} \leq \boldsymbol{G_1}$ é um subgrupo, e se $\boldsymbol{N} \trianglelefteq \boldsymbol{G_2}$ é um subgrupo normal, então $\boldsymbol{h^{-1}(N)} \trianglelefteq \boldsymbol{G_1}$ é um subgrupo normal.*

Demonstração. (Não-vacuidade) Como $e_2 \in S$ e h é homomorfismo segue que $h(e_1) = e_2$, portanto $e_1 \in h^{-1}(S)$. (Fechamento da multiplicação) Sejam $s_1, s_2 \in h^{-1}(S)$. Então $h(s_1), h(s_2) \in S$ e, como $\boldsymbol{S}$ é subgrupo, $h(s_1)h(s_2) \in S$. Logo, como h é homomorfismo, $h(s_1s_2) = h(s_1)h(s_2) \in S$ e, portanto, $s_1s_2 \in h^{-1}(S)$. (Fechamento da inversão) Seja $s \in h^{-1}(S)$. Então $h(s) \in S$ e, como $\boldsymbol{S}$ é subgrupo, $h(s)^{-1} \in S$. Como h é homomorfismo, segue que $h(s^{-1}) = h(s)^{-1} \in S$ e, portanto, $s^{-1} \in h^{-1}(S)$. (Normalidade) Sejam $g \in G_1$ e $n \in h^{-1}(N)$. Então $h(g) \in G_2$ e $h(n) \in N$. Como h é homomorfismo, segue que $h(gng^{-1}) = h(g)h(n)h(g)^{-1}$ e, como $\boldsymbol{N}$ é subgrupo normal, segue que $h(g)h(n)h(g)^{-1} \in N$. Logo $gng^{-1} \in h^{-1}(N)$. ■

Proposição 9.21. *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \to \boldsymbol{G_2}$ um homomorfismo de grupos. Se $\boldsymbol{S} \leq \boldsymbol{G_1}$, então $\boldsymbol{h(S)} \leq \boldsymbol{G_2}$, e se h é sobrejetivo e $\boldsymbol{N} \trianglelefteq \boldsymbol{G_1}$ um subgrupo normal, então $\boldsymbol{h(N)} \trianglelefteq \boldsymbol{G_2}$.*

Demonstração. (Não-vacuidade) Como $e_1 \in S$, segue que $e_2 = h(e_1) \in h(S)$. (Fechamento da multiplicação) Sejam $s_1, s_2 \in h(S)$. Então existem $s_1', s_2' \in S$ tais que $h(s_1') = s_1$ e $h(s_2') = s_2$. Como $\boldsymbol{S}$ é subgrupo, segue que $s_1's_2' \in S$ e, como h é homomorfismo, segue que

$$s_1s_2 = h(s_1')h(s_2') = h(s_2's_2') \in h(S).$$

(Fechamento da inversão) Seja $s \in h(S)$. Então existe $s' \in S$ tal que $h(s') = s$. Como $\boldsymbol{S}$ é subgrupo, segue que $s^{-1} \in S$ e, portanto, $h(s)^{-1} = h(s^{-1}) \in h(S)$. (Normalidade) Sejam $g \in G_2$ e $n \in h(N)$. Existe $n' \in N$ tal que $h(n') = n$ e, como h é sobrejetivo, existe $g' \in G_1$ tal que $h(g') = g$. Como N é normal, $gng^{-1} \in N$ e, como h é homomorfismo,

$$gng^{-1} = h(g')h(n')h(g')^{-1} = h(g'n'g'^{-1}) \in h(N).$$

■

9.6 Núcleo, Imagem e Isomorfismo

Definição 9.11. Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \to \boldsymbol{G_2}$ um homomorfismo de grupos. O *núcleo* de h é o conjunto

$$\mathcal{N}(h) \coloneqq h^{-1}(e_2) = \{g \in G_1 : h(g) = e_2\}$$

e a *imagem* de h é o conjunto

$$\mathcal{I}\mathrm{m}(h) \coloneqq h(G_1) = \{g_2 \in G_2 : \exists g_1 \in G_1, h(g_1) = g_2\}.$$

Proposição 9.22. *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \to \boldsymbol{G_2}$ um homomorfismo de grupos. Então h é injetiva se, e somente se, $\mathcal{N}(h) = \{e_1\}$.*

Demonstração. ($\Rightarrow$) Suponha que h é injetiva. Seja $n \in \mathcal{N}(h)$. Então $h(n) = e_2$. Mas $h(e_1) = e_2$ e, como h é injetiva, concluímos que $n = e_1$.
($\Leftarrow$) Suponha que $\mathcal{N}(h) = \{e_1\}$. Sejam $g_1, g_2 \in G_1$. Se $h(g_1) = h(g_2)$, temos que $h(g_1 g_2^{-1}) = h(g_1)h(g_2)^{-1} = e_2$, o que implica que $g_1 g_2^{-1} = e_1$, pois $\mathcal{N}(h) = \{e_1\}$. Logo $g_1 = g_2$, e concluímos que h é injetiva. ■

Definição 9.12. Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos. Um *isomorfismo de grupos* é um homomorfismo de grupos invertível. O conjunto de todos esses ismorfismos é denotado por $\mathfrak{Iso}(\boldsymbol{G_1}, \boldsymbol{G_2})$.

Proposição 9.23. *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \to \boldsymbol{G_2}$ um isomorfimo de grupos. Então $h^{-1} : \boldsymbol{G_2} \to \boldsymbol{G_1}$ é um isomorfismo de grupos.*

Demonstração. Como h é bijetiva, sua inversa h^{-1} também é bijetiva. Sejam $g_1 g_1 \in G_2$. Como h é bijetiva, existem $g_1', g_2' \in G_1$ tais que $h(g_1') = g_1$ e $h(g_2') = g_2$. Assim, como h é homomorfismo, segue que

$$\begin{aligned} h^{-1}(g_1 g_2) &= h^{-1}(h(g_1')h(g_2')) \\ &= h^{-1}(h(g_1' g_2')) \\ &= g_1' g_2' \\ &= h^{-1}(g_1)h^{-1}(g_2). \end{aligned}$$

■

Definição 9.13. Seja $\boldsymbol{G_1}$ um grupo. Um grupo *isomorfo* a $\boldsymbol{G_1}$ é um grupo $\boldsymbol{G_2}$ para o qual existe isomorfismo $h : \boldsymbol{G_1} \to \boldsymbol{G_2}$. Denota-se $\boldsymbol{G_1} \simeq \boldsymbol{G_2}$.

Proposição 9.24. *Sejam $\boldsymbol{G_1}$, $\boldsymbol{G_2}$ e $\boldsymbol{G_3}$ grupos. Então*

1. *(Reflexividade) $\boldsymbol{G_1} \simeq \boldsymbol{G_1}$;*
2. *(Antissimetria) $\boldsymbol{G_1} \simeq \boldsymbol{G_2} \Rightarrow \boldsymbol{G_2} \simeq \boldsymbol{G_1}$;*
3. *(Transitividade) $\boldsymbol{G_1} \simeq \boldsymbol{G_2}$ e $\boldsymbol{G_2} \simeq \boldsymbol{G_3} \Rightarrow \boldsymbol{G_1} \simeq \boldsymbol{G_3}$.*

Demonstração.

1. A função $\mathbb{1}_{G_1}$ é um isomorfismo de grupos.
2. A inversa é um isomorfismo de grupos (9.23).
3. A composição de homomorfismo é homomorfismo e a composição de bijeções é bijeção.

■

Não dizemos que $\simeq$ é uma relação de equivalência porque ela não está propriamente definida em um conjunto, já que não existe o conjunto de todos os grupos por não existir o conjunto de todos os conjuntos. No entanto, é claro que o que a proposição afirma é que ela satisfaz as propriedades de uma relação de equivalência.

9.7 Teoremas de Isomorfismo

Teorema 9.25 (Primeiro teorema de isomorfismo)**.** *Sejam* $\boldsymbol{G_1}$ *e* $\boldsymbol{G_2}$ *grupos e* $h : \boldsymbol{G_1} \to \boldsymbol{G_2}$ *um homomorfismo de grupos. Então* $\boldsymbol{\mathcal{N}(h)} \trianglelefteq \boldsymbol{G_1}$, $\boldsymbol{\mathfrak{Im}(h)} \leq \boldsymbol{G_2}$ *e*

$$\boldsymbol{G_1}\big/\boldsymbol{\mathcal{N}(h)} \simeq \boldsymbol{\mathfrak{Im}(h)}.$$

Demonstração. Como $\mathcal{N}(h) = h^{-1}(e_2)$ e $\boldsymbol{\{e_2\}} \trianglelefteq \boldsymbol{G_2}$ (9.13), a proposição segue da proposição 9.20. Como $\mathfrak{Im}(h) = h^(G_1)$ e $\boldsymbol{G_1} \leq \boldsymbol{G_1}$ (9.13), a proposição segue da proposição 9.20. Por causa disso, $\boldsymbol{G_1/\mathcal{N}(h)}$ e $\boldsymbol{\mathfrak{Im}(h)}$ são grupos. Consideremos a função

$$\begin{aligned} \eta : G_1/\mathcal{N}(h) &\to \mathfrak{Im}(h) \\ g\mathcal{N}(h) &\mapsto h(g). \end{aligned}$$

Primeiro mostremos que η é função. Sejam $g_1, g_2 \in G_1$ tais que $g_1\mathcal{N}(h) = g_2\mathcal{N}(h)$. Então $g_2^{-1}g_1 \in \mathcal{N}(h)$ (9.8), o que implica que $h(g_2^{-1}g_1) = e$. Como h é homomorfismo, $e = h(g_2^{-1}g_1) = h(g_2)^{-1}h(g_1)$, portanto $h(g_1) = h(g_2)$. Isso implica que $\eta(g_1\mathcal{N}(h)) = \eta(g_1\mathcal{N}(h))$.

Agora, mostremos que η é isomomorfismo de grupos. Para simplificar as contas, denotamos $[g] = g\mathcal{N}(h)$. Primeiro mostramos que η é homomorfismo. Sejam $g_1, g_2 \in G_1$. Então

$$\eta([g_1][g_2]) = \eta([g_1g_2]) = h(g_1g_2) = h(g_1)h(g_2) = \eta([g_1])\eta([g_2]).$$

Por fim, devemos mostrar que η é bijetivo. (Injetividade) Seja $[g] \in \mathcal{N}(\eta)$. Então $\eta([g]) = e_2$, logo $h(a) = e_2$. Mas isso implica que $g \in \mathcal{N}(h)$. Portanto $[g] = [e_1]$, e segue que $\mathcal{N}(\eta) = \{[e_1]\}$, o que é equivalente à injetividade (9.22). (Sobrejetividade) Para todo $g \in \mathfrak{Im}(h)$, existe $g' \in G_1$ tal que $g = h(g')$. Mas $h(g') = \eta(g'\mathcal{N}(h))$, e segue a sobrejetividade. ■

Definição 9.14. Sejam $\boldsymbol{G}$ um grupo, $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo e $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ um subgrupo normal. Então

$$SN \coloneqq \{sn : s \in S \text{ e } n \in N\}.$$

Teorema 9.26 (Segundo teorema de isomorfismo)**.** *Sejam $\boldsymbol{G}$ um grupo, $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo e $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ um subgrupo normal. Então $\boldsymbol{SN} \leq \boldsymbol{G}$, $\boldsymbol{S} \cap \boldsymbol{N} \trianglelefteq \boldsymbol{S}$ e*

$$\boldsymbol{S}\big/\boldsymbol{S \cap N} \simeq \boldsymbol{SN}\big/\boldsymbol{N}.$$

Teorema 9.27 (Terceiro teorema de isomorfismo)**.** *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ um subgrupo normal. Então*

1. *Se $\boldsymbol{S} \leq \boldsymbol{G}$ tal que $N \subseteq S \subseteq G$, então $\boldsymbol{S/N} \leq \boldsymbol{G/N}$. Por outro lado, se $\boldsymbol{S'} \leq \boldsymbol{G/N}$, existe $\boldsymbol{S} \leq \boldsymbol{G}$ tal que $\boldsymbol{S'} = \boldsymbol{S/N}$.*

2. *Se $\boldsymbol{S} \trianglelefteq \boldsymbol{G}$ tal que $N \subseteq S \subseteq G$, então $\boldsymbol{S/N} \trianglelefteq \boldsymbol{G/N}$. Por outro lado, se $\boldsymbol{S'} \trianglelefteq \boldsymbol{G/N}$, existe $\boldsymbol{S} \leq \boldsymbol{G}$ tal que $\boldsymbol{S'} = \boldsymbol{S/N}$.*

3. *Se $\boldsymbol{N'} \trianglelefteq \boldsymbol{G}$ tal que $N \subseteq N' \subseteq G$, então*

$$\left(\boldsymbol{G}\big/\boldsymbol{N}\right)\Big/\left(\boldsymbol{N'}\big/\boldsymbol{N}\right) \simeq \boldsymbol{G}\big/\boldsymbol{N'}.$$

9.8 Produto de Grupos

Definição 9.15. Seja $(\boldsymbol{G_i})_{i\in I} = (G_i, *_i)_{i\in I}$ uma família de grupos. O *produto* da família $(\boldsymbol{G_i})_{i\in I}$ é o par

$$\prod_{i\in I} \boldsymbol{G_i} \coloneqq (G, *)\,,$$

em que $G = \prod_{i\in I} G_i$ e

$$\begin{aligned} * : G \times G &\to G \\ (g_1, g_2) &\mapsto ((g_1)_i *_i (g_2)_i)_{i\in I}. \end{aligned}$$

Proposição 9.28. *Seja $(\boldsymbol{G_i})_{i\in I} = (G_i, *_i)_{i\in I}$ uma família de grupos. Então o produto $\prod_{i\in I} \boldsymbol{G_i}$ é um grupo. Se, para todo $i \in I$, $\boldsymbol{G_i}$ é comutativo, então $\prod_{i\in I} \boldsymbol{G_i}$ é comutativo.*

Demonstração. (Associatividade) Sejam $g, g', g'' \in G$. Então, da associatividade de cada $*_i$,

$$(gg')g'' = ((g_ig_i')g_i'')_{i\in I} = (g_i(g_i'g_i'')_{i\in I} = g(g'g'').$$

(Identidade) Seja e_i identidade de $(G_i, *_i)$. Então $e \coloneqq (e_i)_{i\in I}$ é a identidade de $(G, *)$, já que, para todo $g = (g_i)_{i\in I} \in G$,

$$eg = (e_ig_i)_{i\in I} = (g_i)_{i\in I} = g = (g_i)_{i\in I} = (g_ie_i)_{i\in I} = ge.$$

(Invertibilidade) Seja $g \in G$. Então $g^{-1} \coloneqq (g_i^{-1})_{i\in I}$ é o inverso de g em $(G, *)$, já que

$$g^{-1}g = (g_i^{-1}g_i)_{i\in I} = (e_i)_{i\in I} = (g_ig_i^{-1})_{i\in I} = gg^{-1}.$$

(Comutatividade) Sejam $g, g' \in G$. Então, da comutatividade de cada $*_i$,

$$gg' = (g_ig_i')_{i\in I} = (g_i'g_i)_{i\in I} = g'g.$$

■

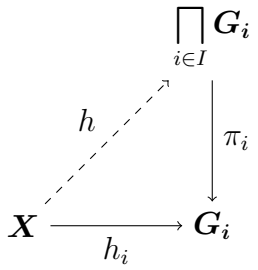
Proposição 9.29. *Seja $(\boldsymbol{G_i})_{i\in I} = (G_i, *_i)_{i\in I}$ uma família de grupos. Para todo $i \in I$, a projeção canônica $\pi_i : \prod_{i\in I} G_i \to G_i$ é um homomorfismo de grupos.*

Demonstração. Sejam $g, g' \in \prod_{i\in I} G_i$. Então

$$\pi_i(gg') = \pi_i((g_ig_i')_{i\in I}) = g_ig_i' = \pi_i(g)\pi_i(g').$$

■

Proposição 9.30 (Propriedade Universal)**.** *Sejam $(\boldsymbol{G_i})_{i\in I}$ uma família de grupos, $\boldsymbol{X} = (X, \star)$ um grupo e, para todo $i \in I$, $h_i : \boldsymbol{X} \to \boldsymbol{G_i}$ um homomorfismo de grupos. Então existe único homomorfismo de grupos $h : \boldsymbol{X} \to \prod_{i\in I} \boldsymbol{G_i}$ tal que, para todo $i \in I$, $\pi_i \circ h = h_i$ (o diagrama comuta).*



Demonstração. Defina a função

$$\begin{aligned} h : X &\to \prod_{i\in I} G_i \\ x &\mapsto (h_i(x))_{i\in I}. \end{aligned}$$

Da propriedade universal para o produto de conjuntos, h é a única função tal que, para todo $i \in I$, $\pi_i \circ h = h_i$. Basta mostrar que h é homomorfismo de grupos. Por simplicidade, apenas a operação $*$ em G será explicitada. Sejam $x_1, x_2 \in X$. Então, como h_i são homomorfismos de grupo,

$$h(x_1 \star x_2) = (h_i(x_1 \star x_2))_{i\in I} = (h_i(x_1) *_i h_i(x_2))_{i\in I} = h(x_1) * h(x_2).$$

■

9.9 Grupo Livre

Definição 9.16. Seja C um conjunto. O *conjunto de inversos formais* de C é o conjunto

$$C^{-1} \coloneqq \{(c, -1) \mid c \in G\}.$$

Os elementos de C^{-1} são denotados $c^{-1} \coloneqq (c, -1)$.

Uma *palavra* em C é uma sequência finita $(c_1, \ldots, c_n) \in C^n$. Denota-se $c_1 \cdots c_n$.

Seja $p = c_1 \cdots c_n$ uma palavra em C. A *palavra inversa* de p é a palavra $p^{-1} \coloneqq c_n^{-1} \cdots c_1^{-1}$.

Definição 9.17. Seja G um conjunto e p_1, p_2 palavras em $G \cup G^{-1}$. A relação de equivalência entre as palavras p_1 e p_2 é definida por

$$p_1 \sim p_2 \quad \iff \quad p_1 p_2^{-1} \rightsquigarrow e.$$

$$G^* \coloneqq \bigcup_{n\in\mathbb{N}} (G \cup G^{-1})^n$$

Define-se $C^0 = \{e \coloneqq \emptyset\}$.

OBS:

$$G^* \coloneqq \overline{G}/\sim$$

9.10 Coproduto de Grupos

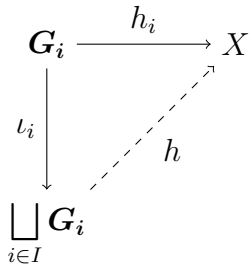
Definição 9.18. Seja $(\boldsymbol{G_i})_{i\in I}$ uma família de grupos. O *coproduto* da família $(\boldsymbol{G_i})_{i\in I}$ é o par

$$\bigsqcup_{i\in I} \boldsymbol{G_i} \coloneqq (G, *)\,,$$

em que $G \coloneqq L(\bigsqcup_{i\in I} G_i)$ é o grupo livre sobre o coproduto de conjuntos $\bigsqcup_{i\in I} G_i$ e

$$\begin{aligned} * : G \times G &\to G \\ ([p_1], [p_2]) &\mapsto [p_1 p_2]. \end{aligned}$$

Proposição 9.31 (Propriedade Universal)**.** *Sejam $(\boldsymbol{G_i})_{i\in I}$ uma família de grupos, $\boldsymbol{X} = (X, \star)$ um grupo e, para todo $i \in I$, $h_i : \boldsymbol{G_i} \to \boldsymbol{X}$ um homomorfismo de grupos. Então existe único homomorfismo de grupos $h : \bigsqcup_{i\in I} \boldsymbol{G_i} \to \boldsymbol{X}$ tal que, para todo $i \in I$, $h \circ \iota_i = h_i$ (o diagrama comuta).*



Demonstração. Defina a função

$$\begin{aligned} h : ... &\to X \\ &\mapsto . \end{aligned}$$

■

9.11 Grupo Simples e Subgrupo Normal Maximal

Definição 9.19. Um *grupo simples* é um grupo não-trivial $\boldsymbol{G}$ cujos únicos subgrupos normais são $\boldsymbol{\{e\}}$ e $\boldsymbol{G}$.

Definição 9.20. Seja $\boldsymbol{G}$ um grupo. Um subgrupo normal *maximal* de $\boldsymbol{G}$ é um subgrupo normal próprio $\boldsymbol{M} \lhd \boldsymbol{G}$ que satisfaz

(Maximalidade) $\qquad \forall \boldsymbol{N} \trianglelefteq \boldsymbol{G} \qquad M \subseteq N \Rightarrow N = M \ \text{ ou } \ N = G.$

Proposição 9.32. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{M} \trianglelefteq \boldsymbol{G}$ um subgrupo normal. Então $\boldsymbol{M}$ é maximal se, e somente se, $\boldsymbol{G/M}$ é simples.*

Demonstração. Consideremos a projeção canônica

$$\begin{aligned} \pi : G &\to G/M \\ g &\mapsto gM. \end{aligned}$$

($\Rightarrow$) Suponhamos que $\boldsymbol{M}$ é maximal. Então $\boldsymbol{M}$ é um subgrupo próprio, o implica que $\boldsymbol{G/M}$ é não-trivial. Seja $\boldsymbol{N} \trianglelefteq \boldsymbol{G/M}$. Sabemos que $\boldsymbol{\pi^{-1}(N)} \trianglelefteq \boldsymbol{G}$ (9.20). Como $[e] \in N$, então $\pi^{-1}(e) \subseteq \pi^{-1}(N)$. Notando que $\pi^{-1}([e]) = \mathcal{N}(\pi) = M$, segue que $M \subseteq \pi^{-1}(N)$. Como $\boldsymbol{M}$ é maximal, segue que $\pi^{-1}(N) = N$ ou $\pi^{-1}(N) = G$. Notemos que $N = \pi(\pi^{-1}(N))$, pois π é sobrejetiva. No primeiro caso, $N = \pi(\pi^{-1}(N)) = \pi(M) = \{[e]\}$. No segundo caso, $N = \pi(\pi^{-1}(N)) = \pi(G) = G/M$. Portanto $\boldsymbol{G/M}$ é simples.
($\Leftarrow$) Suponhamos que $\boldsymbol{G/M}$ é simples. Seja $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ tal que $M \subseteq N$. Como π é homomorfismo de grupos sobrejetivo, ssegue que $\pi(N) \trianglelefteq \boldsymbol{G/M}$ (9.21). Como $\boldsymbol{G/M}$ é simples, então $\pi(N) = \{[e]\}$ ou $\pi(N) = G/M$. No primeiro caso, $N = \mathcal{N}(\pi) = M$. No segundo caso, $N = \pi^{-1}(\pi(N)) = \pi^{-1}(N) = G$. Logo $\boldsymbol{M}$ é maximal. ■

Conjectura 9.33. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{N} \lhd \boldsymbol{G}$ um subgrupo normal próprio. Então $\boldsymbol{G}$ tem subgrupo normal maximal.*

Demonstração. Usaremos o lema de Zorn. Seja $P \subseteq \mathcal{P}(G)$ o conjunto de todos os subconjuntos $S \subset G$ tais que $\boldsymbol{S} \lhd \boldsymbol{G}$. Então $(P, \subseteq)$ é um conjunto parcialmente ordenado com a contenção de conjuntos usual. Agora, seja $(C)_{i \in I}$ uma cadeia de $(P, \subseteq)$. Consideremos o conjunto $C \coloneqq \bigcup_{i \in I} C_i$. Como

Notemos que P não é vazio, pois $N \in P$. Seja

Então P tem elemento maximal. ■

9.12 Sequência subnormal

Definição 9.21. Seja $\boldsymbol{G}$ um grupo. Uma *sequência subnormal* de $\boldsymbol{G}$ é uma sequência finita $(\boldsymbol{N_i})_{i \in \mathtt{I}_n}$ de subgrupos de $\boldsymbol{G}$ que satisfaz

$$\boldsymbol{\{e\} = N_0 \trianglelefteq \cdots \trianglelefteq N_n = G}.$$

O grupo $\boldsymbol{N_{i+1}/N_i}$ é o i-ésimo *grupo fator* da sequência. Uma *sequência normal* é uma sequência subnormal em que, para todo $i \in \mathtt{I}_n$, $\boldsymbol{N_i} \trianglelefteq \boldsymbol{G}$.

Uma sequência subnormal *estrita* de $\boldsymbol{G}$ é uma sequência subnormal $(\boldsymbol{N_i})_{i\in\mathtt{I}_n}$ de $\boldsymbol{G}$ que satisfaz

$$\boldsymbol{\{e\} = N_0 \lhd \cdots \lhd N_n = G}.$$

O comprimento

9.13 Conjunto gerador

Definição 9.22. Seja $\boldsymbol{G}$ um grupo e $C \subseteq G$ um conjunto. O grupo *gerado* por S é o grupo $\boldsymbol{\langle S\rangle \leq G}$ em que

$$\langle S\rangle \coloneqq \{s_1 \cdots s_n : n \in \mathbb{N},\ s_i \in S \ \text{ ou } \ s_i^{-1} \in S\}.$$

$$\langle S\rangle \coloneqq \left\{ \ast_{i\in\mathtt{I}_n} s_i : n \in \mathbb{N},\ s_i \in S \ \text{ ou } \ s_i^{-1} \in S \right\}.$$

Um *conjunto gerador* de $\boldsymbol{G}$ é um conjunto $S \subseteq G$ tal que $\langle S\rangle = G$.

9.14 Grupos Simétricos e Alternados

Definição 9.23. Seja C um conjunto. O *grupo simétrico de* C é o par $\boldsymbol{\mathfrak{S}(C)} = (\mathfrak{S}(C), \circ)$, em que $\mathfrak{S}(C)$ é o conjunto de todas as bijeções entre C e C, e $\circ$ é a composição de funções. Seja α um número cardinal. Para $C = \alpha$, usa-se a notação $\mathfrak{S}_\alpha \coloneqq \mathfrak{S}(\alpha)$.

Proposição 9.34. *Seja C um conjunto. O grupo simétrico $\boldsymbol{\mathfrak{S}(C)}$ é um grupo.*

Demonstração. Se $C = \emptyset$, então $\mathfrak{S}(C) = \{\emptyset\}$. Assim, como $\emptyset\circ\emptyset = \emptyset$, segue que $\circ$ é operação binária em $\{\emptyset\}$. Ainda, segue que $\circ$ é associativa, pois $(\emptyset\circ\emptyset)\circ\emptyset = \emptyset\circ(\emptyset\circ\emptyset)$; tem elemeno neutro $\emptyset$, pois $\emptyset\circ\emptyset = \emptyset$, e que todo elemento tem inverso, pois $\emptyset^{-1} = \emptyset$.

Suponhamos, então, que $C \neq \emptyset$ e sejam $p_1, p_2 \in \mathfrak{S}(C)$. Então, como p_1 e p_2 são bijeções, a função $p_2 \circ p_1 : C \to C$ é uma bijeção entre C e C (3.11 e 3.12) e, portanto, $p_2 \circ p_1 \in \mathfrak{S}(C)$. Isso mostra que $\circ$ é uma operação binária em $\mathfrak{S}(C)$. A composição de funções é associativa, pois, para todos $p_1, p_2, p_3 \in \mathfrak{S}(C)$, $p_3 \circ (p_2 \circ p_1) = (p_3 \circ p_2) \circ p_1$ (3.5). Ainda, notemos que id_C é o elemento neutro de $\boldsymbol{\mathfrak{S}(C)}$, pois, para todo $p \in \mathfrak{S}(C)$, vale $p \circ id_C = id_C \circ p = p$ (3.7). Por fim, como p é uma bijeção, existe função inversa $p^{-1} : C \to C$ que é bijeção entre C e C (3.8 e 3.9); logo existe $p^{-1} \in \mathfrak{S}(C)$ tal que $p \circ p^{-1} = p^{-1} \circ p = id_C$. Portanto concluímos que $\boldsymbol{\mathfrak{S}(C)}$ é um grupo. ∎

Proposição 9.35. *Sejam A e B conjuntos tais que $|A| = |B|$. Então*

$$\mathfrak{S}(\boldsymbol{A}) \simeq \mathfrak{S}(\boldsymbol{B}).$$

Demonstração. Seja $\phi : A \to B$ uma bijeção e considere a função

$$\begin{aligned} h : \mathfrak{S}(A) &\to \mathfrak{S}(B) \\ p &\mapsto \phi \circ p \circ \phi^{-1}. \end{aligned}$$

Primeiro notemos que h é homomorfismo de grupos. Sejam $p_1, p_2 \in \mathfrak{S}(A)$. Então

$$\begin{aligned} h(p_2 \circ p_1)(c) &= \phi \circ (p_2 \circ p_1) \circ \phi^{-1} \\ &= \phi \circ (p_2 \circ \phi^{-1} \circ \phi \circ p_1) \circ \phi^{-1} \\ &= (\phi \circ p_2 \circ \phi^{-1}) \circ (\phi \circ p_1 \circ \phi^{-1}) \\ &= h(p_2) \circ h(p_1). \end{aligned}$$

Portanto h é um homomorfismo de grupos entre $\mathfrak{S}(\boldsymbol{A})$ e $\mathfrak{S}(\boldsymbol{B})$.

Agora notemos que h é uma bijeção. A inversa de h é a função

$$\begin{aligned} h^{-1} : \mathfrak{S}(B) &\to \mathfrak{S}(A) \\ p &\mapsto \phi^{-1} \circ p \circ \phi, \end{aligned}$$

pois, para todo $p \in \mathfrak{S}(B)$,

$$\begin{aligned} (h \circ h^{-1})(p) &= h(h^{-1}(p)) \\ &= \phi \circ h^{-1}(p) \circ \phi^{-1} \\ &= \phi \circ (\phi^{-1} \circ p \circ \phi) \circ \phi^{-1} \\ &= p \\ &= id_{\mathfrak{S}(B)}(p), \end{aligned}$$

o que mostra que $h \circ h^{-1} = id_{\mathfrak{S}(B)}$, e, para todo $p \in \mathfrak{S}(A)$,

$$\begin{aligned} (h^{-1} \circ h)(p) &= h^{-1}(h(p)) \\ &= \phi^{-1} \circ h(p) \circ \phi \\ &= \phi^{-1} \circ (\phi \circ p \circ \phi^{-1}) \circ \phi \\ &= p \\ &= id_{\mathfrak{S}(A)}(p), \end{aligned}$$

o que mostra que $h^{-1} \circ h = id_{\mathfrak{S}(A)}$. Assim, está provado que h é isomorfismo entre $\mathfrak{S}(\boldsymbol{A})$ e $\mathfrak{S}(\boldsymbol{B})$. ■

Essa proposição mostra que podemos estudar somente os grupos simétricos dos números cardinais, pois isso será equivalente a estudar qualquer grupo simétrico. Em particular, para todo conjunto finito, podemos estudar seu grupo simétrico considerando somente o grupo simétrico $\mathfrak{S}_n$, em que n é o número de elementos do conjunto. A partir de agora, as proposições serão considerando esses grupos $\mathfrak{S}_n$.

Proposição 9.36. *Seja $n \in \mathbb{N}$. Então $|\mathfrak{S}_n| = n!$.*

Teorema 9.37. *Seja $\boldsymbol{G}$ um grupo. Então*

$$\boldsymbol{G \lesssim \mathfrak{S}(G)}.$$

Demonstração. Consideremos a função

$$\begin{aligned} h : G &\to \mathfrak{S}(G) \\ g &\mapsto h(g) : G \to G \\ &\qquad\quad x \mapsto g * x \end{aligned}$$

Primeiro, devemos mostrar que $h(g) \in \mathfrak{S}(G)$, para que h esteja bem definida. Para isso, notemos que $h(g)$ está bem definida, já que, para todo $x \in G$, $g * x \in G$. Ainda, $h(g)$ é uma bijeção, pois $h(g)^{-1} = h(g^{-1})$, já que, para todo $x \in G$,

$$(h(g) \circ h(g)^{-1})(x) = h(g)((h(g)^{-1})(x)) = h(g)(g^{-1} * x) = g * g^{-1} * x = x = id_G,$$

o que mostra que $h(g) \circ h(g)^{-1} = id_G$, e

$$(h(g)^{-1} \circ h(g))(x) = h(g)^{-1}((h(g)(x)) = h(g)^{-1}(g * x) = g^{-1} * g * x = x = id_G,$$

o que mostra que $h(g)^{-1} \circ h(g) = id_G$. Isso mostra que $h(g)$ é uma bijeção e, portanto, $h(g) \in \mathfrak{S}(G)$.

Agora, notemos que h é um homomorfismo de grupos, pois, para todos $g_1, g_2 \in G$, segue que, para todo $x \in G$,

$$\begin{aligned} h(g_1 * g_2)(x) &= (g_1 * g_2) * x \\ &= g_1 * (g_2 * x) \\ &= h(g_1)(g_2 * x) \\ &= h(g_1)(h(g_2)(x)) \\ &= (h(g_1) \circ h(g_2))(x), \end{aligned}$$

o que mostra que $h(g_1 * g_2) = h(g_1) \circ h(g_2)$. Por fim, notemos que h é injetiva, já que, se $g \in G$ é tal que $h(g) = id_G$, então, para todo $x \in G$,

$$g * x = h(g)(x) = id_G(x) = x,$$

o que mostra que $g = e_G$ e, portanto, que $\mathcal{N}(h) = \{e_G\}$. ■

Esse teorema é um teorema muito importante, pois ele mostra que, de certa forma, todo grupo é um subconjunto de permutações. Por causa disso que grupos são pensados como os objetos algébricos que modelam a simetria.

9.14.1 Permutações e Órbitas

Definição 9.24. Seja $n \in \mathbb{N}$. Uma *permutação* de n objetos é um elemento $p \in \mathfrak{S}_n$, denotado por

$$p = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ p(1) & p(2) & \cdots & p(n-1) & p(n) \end{pmatrix}.$$

Notação. Seja $n \in \mathbb{N}$. A composição de duas permutações $p_1, p_2 \in \mathfrak{S}_n$, quando representadas na notação acima, é denotada

$$p_2 \circ p_1 = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ p_2(1) & p_2(2) & \cdots & p_2(n-1) & p_2(n) \end{pmatrix}\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ p_1(1) & p_1(2) & \cdots & p_1(n-1) & p_1(n) \end{pmatrix}.$$

$\mathfrak{ICD}$

Definição 9.25. Sejam $n \in \mathbb{N}$ e $p \in \mathfrak{S}_n$. A *matriz de permutação* de p é a matriz $[p] \in \mathbb{M}_n(\mathbb{Z})$ cujas entradas são dadas por

$$[p]_{i,j} = \delta_{i,p(j)} = \begin{cases} 1 & i = p(j) \\ 0 & i \neq p(j). \end{cases}$$

O *conjunto das matrizes de permutação* de $\mathfrak{S}_n$ é o conjunto

$$[\mathfrak{S}_n] \coloneqq \{[p] : p \in \mathfrak{S}_n\}.$$

Proposição 9.38. *Seja $n \in \mathbb{N}$. Então o par $[\mathfrak{S}_n] = ([\mathfrak{S}_n], \cdot)$, em que $\cdot$ é o produto de matrizes, é um grupo, e*

$$\mathfrak{S}_n \simeq [\mathfrak{S}_n].$$

Demonstração. Primeiro, notemos que, para todos $p, q \in \mathfrak{S}_n$,

$$[p][q]_{i,j} = \bigplus_{k=1}^{n} [p]_{i,k}[q]_{k,j} = \bigplus_{k=1}^{n} \delta_{i,p(k)}\delta_{k,p(j)}.$$

Mas o produto $\delta_{i,p(k)}\delta_{k,p(j)}$ é igual a 1 se, e somente se, $i = p(k)$ e $k = q(j)$. Como p é bijeção, a segunda consição é equivalente a $p(k) = pq(j)$, e isso mostra que as duas consições são equivalentes a $i = p(k) = pq(j)$. Como p é bijeção, para cada $i \in \mathtt{I}_n$, $k = p^{-1}(i)$ é o único $k \in \mathtt{I}_n$ tal que a condição é satisfeita, e segue que

$$[p][q]_{i,j} = \bigplus_{k=1}^{n} \delta_{i,p(k)}\delta_{k,p(j)} = \bigplus_{k=1}^{n} \delta_{i,pq(j)} = [pq]_{i,j}.$$

e, como $pq \in \mathfrak{S}_n$, então $[p][q] = [pq] \in [\mathfrak{S}_n]$. Isso mostra que o produto de matrizes é uma operação binária em $[\mathfrak{S}_n]$. Agora, disso segue que $[p][p^{-1}] = [pp^{-1}] = [id]$

MOATRAR QUE O INVERSO DE P ESTA NO GRUPO

Disso, segue que $[\boldsymbol{\mathfrak{S}_n}]$ é um grupo, pois é subgrupo de $\mathbb{M}_n(\mathbb{Z})$. Por fim, consideremos a função

$$\begin{aligned} h : \mathfrak{S}_n &\to [\mathfrak{S}_n] \\ p &\mapsto [p]. \end{aligned}$$

Note que que h é homomorfismo, pois, para todos $p, q \in \mathfrak{S}_n$,

$$h(pq) = [pq] = [p][q] = h(p)h(q).$$

Ainda, h ■

Definição 9.26. Sejam $n \in \mathbb{N}$, $p \in \mathfrak{S}_n$ e $m \in \mathtt{I}_n$. A *órbita de m sob p* é o conjunto

$$\mathcal{O}_p(m) \coloneqq \{p^k(m) : k \in \mathbb{Z}\}.$$

O *período* da órbita $\mathcal{O}_p(m)$ é o número $|\mathcal{O}_p(m)|$. Uma *órbita trivial* é uma órbita de período 1. Uma órbita de p é a órbita de um elemento $m \in \mathtt{I}_n$ sob p.

O *conjunto de órbitas* de p é o conjunto

$$\mathcal{O}_p \coloneqq \{\mathcal{O}_p(m) : m \in \mathtt{I}_n\}.$$

Proposição 9.39. *Sejam $n \in \mathbb{N}$ e $p \in \mathfrak{S}_n$. O conjunto $\mathcal{O}_p$ é uma partição de $\mathtt{I}_n$.*

Demonstração. Primeiro, notemos que $m \in \mathcal{O}_p(m)$ e, portanto, $\emptyset \notin \mathcal{O}_p$. Ainda, $\bigcup_{m\in\mathtt{I}_n} \mathcal{O}_p(m) = \mathtt{I}_n$, já que, para todo $m \in inte_n$, $m \in \mathcal{O}_p(m)$, o que mostra que $\mathtt{I}_n \subseteq \bigcup_{m\in\mathtt{I}_n}$ e, para todo $l \in \bigcup_{m\in\mathtt{I}_n} \mathcal{O}_p(m)$, existe $m \in \mathtt{I}_n$ tal que $l \in \mathcal{O}_p(m)$ e, portanto, existe $k \in \mathbb{N}$ tal que $l = p^k(m) \in \mathtt{I}_n$, o que mostra que $\bigcup_{m\in\mathtt{I}_n} \subseteq \mathtt{I}_n$. Por fim, sejam $o_1, o_2 \in \mathcal{O}_p$. Então existem $m_1, m_2 \in \mathtt{I}_n$ tais que $o_1 = \mathcal{O}_p(m_1)$ e $o_2 = \mathcal{O}_p(m_2)$. Se existe $l \in \mathcal{O}_p(m_1) \cap \mathcal{O}_p(m_2)$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $l = p^{k_1}(m_1) = p^{k_2}(m_2)$. Assim, segue que $m_1 = p^{k_2-k_1}(m_2)$ e, portanto, $m_1 \in \mathcal{O}_p(m_2)$. Mas isso implica que $\mathcal{O}_p(m_1) \subseteq \mathcal{O}_p(m_2)$; a inclusão contrária é análoga e concluímos que $\mathcal{O}_p(m_1) = \mathcal{O}_p(m_2)$. Logo $\mathcal{O}_p$ é uma partição de $\mathtt{I}_n$. ■

9.14.2 Permutações, Ciclos e Transposições

Definição 9.27. Sejam $n, k \in \mathbb{N}$. Um *ciclo* de $\mathfrak{S}_n$ é um elemento $c \in \mathfrak{S}_n$ para o qual existe $m \in \mathtt{I}_n$ tal que, para todo $m' \in \mathtt{I}_n$, $c(m') = m'$ ou existe $d \in \mathtt{I}_n$ tal que $m' = c^d(m)$. O *comprimento* de um ciclo é a ordem desse ciclo. Um ciclo c cujo comprimento é k é denotado

$$c = \Big(m\ c(m)\ c^2(m)\ \cdots\ c^{k-2}(m)\ c^{k-1}(m)\Big).$$

Proposição 9.40. *Sejam $n \in \mathbb{N}$.*

1. *Se $c_1, c_2 \in \mathfrak{S}_n$ são ciclos disjuntos, então $c_2 \circ c_1 = c_1 \circ c_2$.*

Proposição 9.41 (Fatoração de Permutação)**.** *Seja $n \in \mathbb{N}$ e $p \in \mathfrak{S}_n$. Então existem únicos ciclos $c_1, \ldots, c_k \in \mathfrak{S}_n$ disjuntos dois a dois tais que $p = c_1 \circ \cdots \circ c_k$.*

Demonstração. Seja $k \coloneqq |\mathcal{O}_p|$. O cojunto $\mathcal{O}_p$ particiona $\mathtt{I}_n$. Sejam $(o_k)_{i \in \mathtt{I}_k}$ uma indexação de $\mathcal{O}_p$ e $m_1, \cdot, m_k \in \mathtt{I}_n$ tais que $o_i = \mathcal{O}_p(m_i)$ para todo $i \in \mathtt{I}_k$, e seja $k_i \coloneqq |\mathcal{O}_p(m_i)|$. Definamos $c_i \coloneqq \Big(m_i \ \cdots \ p^{k_i - 1}(m_i)\Big)$. Então segue que

$$p = \bigtimes_{i=1}^{k} \Big(m_i \ \cdots \ p^{k_i - 1}(m_i)\Big) = \bigtimes_{i=1}^{k} c_i.$$

■

9.15 Grupos Cíclicos

9.16 Grupos Diedrais

Capítulo 10

Anéis

10.1 Anel

Definição 10.1. Um *anel* é uma tripla $\boldsymbol{A} = (A, +, \cdot)$ em que

1. $(A, +)$ é um grupo comutativo com elemento neutro chamado de *zero* ou *nulidade* e representado por 0 (ou 0_A, caso exista ambiguidade).

2. $(A, \cdot)$ é um monoide comutativo com elemento neutro chamado de *um* ou *unidade* e representado por 1 (ou 1_A, caso exista ambiguidade).

3. A operação $\cdot$ é distributiva sobre $+$.

As operações $+$ e $\cdot$ são chamadas, respectivamente, de *adição* e *multiplicação*. A imagem de dois elementos $a_1, a_2 \in A$ pela adição é chamada de *soma* de a_1 e a_2 e denotada por $a_1 + a_2$. A imagem de a_1, a_2 pela multiplicação é chamada de *produto* de a_1 e a_2 e denotada por $a_1 \cdot a_1$ ou $a_1 a_2$.

Um comentário sobre os elementos neutros 0 e 1. Se $0 = 1$, o anel será trivial, mas garantimos esse anel na definição pois, mais para frente, quando virmos anéis quocientes, vai ser proveitoso que qualquer anel quociente seja um anel, e se quocientarmos um anel por ele mesmo, temos o anel trivial.

Notação. Como $(A, +)$ é um grupo, denotaremos o inverso de um elemento $a \in A$ sob $+$ por $-a$, e escreveremos $a_1 - a_2$ para $a_1 + (-a_2)$. Ainda, a multiplicação tem preferência na notação; ou seja, $a_1 a_2 + a_3 = (a_1 \cdot a_2) + a_3$ e $-a_1 a_2 = -(a_1 \cdot a_2)$. Denotaremos o inverso de um elemento $a \in A$ sob $\cdot$ por a^{-1}, se ele existir, pois sabemos que é único (8.5). Os símbolos operatórios relativos à adição e à multiplicação serão, respectivamente, $\boldsymbol{+}$ e $\boldsymbol{\times}$. Caso não haja ambiguidade, denotaremos um anel pelo símbolo que denota seu conjunto escrito em negrito, como em $\boldsymbol{A} = (A, +, \cdot)$.

Proposição 10.1. *Seja* $\boldsymbol{A}$ *um anel. Então, para todo* $a, b \in A$*,*

1. $0 \cdot a = 0$*;*
2. $-(a \cdot b) = (-a) \cdot b$*.*

Demonstração. 1.

$$\begin{aligned} 0 \cdot a &= 0 \cdot a + 0 \\ &= 0 \cdot a + (0 \cdot a - 0 \cdot a) \\ &= (0 \cdot a + 0 \cdot a) - 0 \cdot a \\ &= (0 + 0) \cdot a - 0 \cdot a \\ &= 0 \cdot a - 0 \cdot a \\ &= 0. \end{aligned}$$

2.

$$\begin{aligned} -(a \cdot b) &= -(a \cdot b) + 0 \\ &= -(a \cdot b) + 0 \cdot b \\ &= -(a \cdot b) + (a - a) \cdot b \\ &= -(a \cdot b) + (a \cdot b + (-a) \cdot b) \\ &= (-(a \cdot b) + a \cdot b) + (-a) \cdot b \\ &= 0 + (-a) \cdot b \\ &= (-a) \cdot b. \end{aligned}$$

■

Definição 10.2. Seja $\boldsymbol{A}$ um anel. O conjunto dos elementos invertíveis sob multiplicação de $\boldsymbol{A}$ é denotado por A^*.

Proposição 10.2. *Seja* $\boldsymbol{A}$ *um anel. O par* $(A^*, \cdot|_{A^* \times A^*})$ *é um grupo comutativo.*

Demonstração. O par $(A, \cdot)$ é um monoide comutativo com elemento neutro 1. Portanto segue que o par $(A^*, \cdot|_{A^* \times A^*})$ é um grupo. Como $(A, \cdot)$ é comutativo, então $(A^*, \cdot|_{A^* \times A^*})$ também o é. ■

Definição 10.3. Um *domínio de integridade* (ou *domínio*) é um anel $\boldsymbol{A}$ em que

$$\forall a_1, a_2 \in A \qquad a_1 \cdot a_2 = 0 \Rightarrow a_1 = 0 \ \text{ ou } \ a_2 = 0.$$

Definição 10.4. Um *corpo* é um anel $\boldsymbol{A}$ em que $(A \setminus \{0\}, \cdot)$ é um grupo.

Proposição 10.3. *Seja $\boldsymbol{A}$ um corpo. Então $\boldsymbol{A}$ é um domínio.*

Demonstração. Sejam $a_1, a_2 \in A$ tais que $a_1 \cdot a_2 = 0$. Suponhamos que $a_2 \neq 0$. Então existe $a_2^{-1} \in A$ e temos

$$\begin{aligned} a_1 &= a_1 \cdot 1 \\ &= a_1 \cdot (a_2 \cdot a_2^{-1}) \\ &= (a_1 \cdot a_2) \cdot a_2^{-1} \\ &= 0 \cdot a_2^{-1} \\ &= 0. \end{aligned}$$

Logo, se $a_1 \cdot a_2 = 0$, $a_1 = 0$ ou $a_2 = 0$. ■

Proposição 10.4 (Lei do corte em domínios)**.** *Seja $\boldsymbol{A}$ um domínio e $a, a_1, a_2 \in A$, $a \neq 0$. Então*

$$aa_1 = aa_2 \Rightarrow a_1 = a_2$$

Demonstração. Se $aa_1 = aa_2$, então $-aa_1 = -aa_2$. Portanto

$$a(a_1 - a_2) = aa_1 - aa_2 = aa_1 - aa_1 = 0.$$

Logo, como $\mathbf{A}$ é um domínio e $a \neq 0$, temos que $a_1 - a_2 = 0$, o que implica $a_1 = a_2$. ■

Essa proposição é interessante pois, mesmo sem exigir que $(A \setminus \{0\}, \cdot)$ seja um grupo, como no caso de $\mathbf{A}$ ser um corpo, se $\mathbf{A}$ for um domínio, vale a lei do corte da multiplicação para elementos de $A \setminus \{0\}$.

10.2 Subanel

Definição 10.5. Seja $\boldsymbol{A} = (A, +, \times)$ um anel. Um *subanel* de $\boldsymbol{A}$ é um anel $\boldsymbol{S} = (S, +_S, \times_S)$ em que $S \subseteq A$, $+_S = +|_{S\times S}$ e $\times_S = \times|_{S\times S}$. Denota-se $\boldsymbol{S} \leq \boldsymbol{A}$. Um subanel *próprio* de $\boldsymbol{A}$ é um subanel $\boldsymbol{S} \leq \boldsymbol{A}$ em que S é um conjunto próprio de A ($S \subset A$). Denota-se $\boldsymbol{S} < \boldsymbol{A}$.

Proposição 10.5. *Sejam $\boldsymbol{A} = (A, +, \times)$ um anel e $S \subseteq A$. Então $\boldsymbol{S} = (S, +|_{S\times S}, \times|_{S\times S})$ é um anel com $1 \in S$ se, e somente se,*

1. *$(S, +|_{S\times S})$ é um subgrupo comutativo de $(A, +)$:*
   - *(a) (Não-vacuidade) $S \neq \emptyset$;*
   - *(b) (Fechamento) $\forall s_1, s_2 \in S \qquad s_1 + s_2 \in S$;*

(c) (Invertibilidade) $\forall s \in S \qquad -s \in S$;

2. $(S, \times|_{S\times S})$ *é um submonoide comutativo de* $(A, \times)$ *com* $1 \in S$*:*

   (a) (Identidade) $1 \in S$;

   (b) (Fechamento) $\forall s_1, s_2 \in S \qquad s_1 \times s_2 \in S$.

Demonstração. ($\Rightarrow$) Suponhamos que $\boldsymbol{S}$ é um anel com $1 \in S$. (Subgrupo) Como $S \subseteq A$ e $(S, +|_{S\times S})$ um grupo comutativo, então é um subgrupo de $(A, +)$ por definição de subgrupo (o que é equivalente às propriedades listadas) e é comutativo (9.2)). (Subanel) Como $S \subseteq A$ e $(S, \times|_{S\times S})$ um monoide comutativo com $1 \in S$, então é um submonoide de $(A, \times)$ por definição de submonoide (o que é equivalente às propriedades listadas) e é comutativo (8.7).

($\Leftarrow$) Suponhamos, agora, que $(S, +|_{S\times S})$ é subgrupo comutativo de $(A, +)$ e $(S, \times_{S\times S})$ é submonoide comutativo de $(A, \times)$. (Grupo comutativo) Como $(S, +|_{S\times S})$ é subgrupo comutativo, então é um grupo comutativo por definição de subgrupo. (Monoide comutativo) Como $(S, \times|_{S\times S})$ é submonoide comutativo, então é um monoide comutativo por definição de monoide. (Distributividade) Sejam $s_1, s_2, s_3 \in S$. Então

$$\begin{aligned} s_1 \times |_{S\times S}(s_2 + |_{S\times S} s_3) &= s_1 \times (s_2 + s_3) \\ &= (s_1 \times s_2) + (s_1 \times s_3) \\ &= (s_1 \times |_{S\times S} s_2) + |_{S\times S}(s_1 \times |_{S\times S} s_3). \end{aligned}$$

Logo $\times_{S\times S}$ é distributiva sobre $+\times_{S\times S}$.

■

10.3 O Anel de Polinômios e o Anel Produto

Definição 10.6. Seja $\boldsymbol{A}$ um anel. O *conjunto dos polinômios em* A é o conjunto

$$A[x] \coloneqq \left\{ \bigdoubleplus_{i=0}^{m} a_i x^i : a_i \in A, m \geq 0 \right\},$$

em que $a_0 x^0 \coloneqq a_0$. Os números a_i são chamados de coeficientes do polinômio. Dizemos que dois polinômios são iguais se todos seus coeficientes não nulos são iguais.

Definição 10.7. Seja $\boldsymbol{A}$ um anel e $f, g \in A[x]$ tais que $f \coloneqq \bigdoubleplus_{i=0}^{m} a_i x^i$ e $g \coloneqq \bigdoubleplus_{i=0}^{n} b_i x^i$. Então definimos as operações binárias $\oplus$ e $\odot$ em $A[x]$ por

$$f \oplus g \coloneqq \bigdoubleplus_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i \qquad f \odot g \coloneqq \bigdoubleplus_{i=0}^{m+n} \left(\bigdoubleplus_{j=0}^{i} a_j b_{i-j} \right) x^i.$$

tal que $a_i = 0$ para $m < i \leq \max\{m, n\}$ e $b_i = 0$ para $n < i \leq \max\{m, n\}$. Denotaremos $\oplus$ e $\odot$ por $+$ e $\cdot$ quando não existir ambiguidade.

Proposição 10.6. *Seja* $\boldsymbol{A} = (A, +, \cdot)$ *um anel. Então* $\boldsymbol{A}[\boldsymbol{x}] \coloneqq (A[x], \oplus, \odot)$ *é um anel.*

Demonstração. Sejam $f, g, h \in A[x]$ tais que $f \coloneqq \bigoplus_{i=0}^{m} a_i x^i$, $g \coloneqq \bigoplus_{i=0}^{n} b_i x^i$ e $h \coloneqq \bigoplus_{i=0}^{l} c_i x^i$. Notemos que $\max\{\max\{m, n\}, l\} = \max\{m, \max\{n, l\}\}$. Denotamos essa quantidade como $\max\{m, n, l\}$. Definamos $a_i = 0$ para $m < i \leq \max\{m, n, l\}$, $b_i = 0$ para $n < i \leq \max\{m, n, l\}$ e $c_i = 0$ para $l < i \leq \max\{m, n, l\}$.

Primeiro vamos mostrar que $(A[x], \oplus)$ é um grupo comutativo. Todas as propriedades de grupo comutativo decorrem do fato de que $(A, +)$ é um grupo comutativo com elemento neutro 0. A operação $\oplus$ é associativa, pois

$$\begin{aligned}
(f \oplus g) \oplus h &= \left(\bigoplus_{i=0}^{\max\{m,n\}} (a_i + b_i)x^i \right) \oplus h \\
&= \left(\bigoplus_{i=0}^{\max\{m,n,l\}} ((a_i + b_i) + c_i)x^i \right) \\
&= \left(\bigoplus_{i=0}^{\max\{m,n,l\}} (a_i + (b_i + c_i))x^i \right) \\
&= f \oplus \left(\bigoplus_{i=0}^{\max\{n,l\}} (b_i + c_i)x^i \right) \\
&= f \oplus (g \oplus h),
\end{aligned}$$

e comutativa, pois

$$f \oplus g = \bigoplus_{i=0}^{\max\{m,n\}} (a_i + b_i)x^i = \bigoplus_{i=0}^{\max\{m,n\}} (b_i + a_i)x^i = g \oplus f.$$

Ainda, o polinômio $0_{A[x]} \coloneqq 0$ é elemento neutro, pois

$$f \oplus 0_{A[x]} = \bigoplus_{i=0}^{\max\{m,0\}} (a_i + 0)x^i = \bigoplus_{i=0}^{m} a_i x^i = f.$$

Por fim, existe $-a_i \in A$ para todo $i \in \{0, \ldots, m\}$. Assim, $-f :- \bigoplus_{i=0}^{m} (-a_i)x^i$ é o polinômio inverso de f, pois

$$f + (-f) = \bigoplus_{i=0}^{\max\{m,m\}} (a_i + (-a_i))x^i = \bigoplus_{i=0}^{m} 0x^i = 0$$

Agora, devemos mostrar que $(A[x], \odot)$ é um monoide comutativo. Novamente, as propriedades decorrem do fato de que $(A, \cdot)$ é um monoide comutativo com elemento neutro 1. A operação $\odot$ é associativa, pois

$$\begin{aligned}
(f \odot g) \odot h &= \left(\bigdoubleplus_{i=0}^{m+n} \left(\bigdoubleplus_{j=0}^{i} a_j b_{i-j} \right) x^i \right) \odot h \\
&= \bigdoubleplus_{i=0}^{m+n+l} \left(\bigdoubleplus_{j=0}^{i} \left(\bigdoubleplus_{k=0}^{j} a_k b_{j-k} \right) c_{i-j} \right) x^i \\
&= \bigdoubleplus_{i=0}^{m+n+l} \left(\bigdoubleplus_{j=0}^{i} \left(\bigdoubleplus_{k=0}^{j} a_k b_{j-k} \right) c_{i-j} \right) x^i \\
&= \\
&= \bigdoubleplus_{i=0}^{m+n+l} () \\
&= f \odot \left(\bigdoubleplus_{i=0}^{n+l} \left(\bigdoubleplus_{j=0}^{i} b_j c_{i-j} \right) x^i \right) \\
&= f \odot (g \odot h).
\end{aligned}$$

e comutativa, pois

$$f \odot g = \bigdoubleplus_{i=0}^{m+n} \left(\bigdoubleplus_{j=0}^{i} a_j b_{i-j} \right) x^i = \bigdoubleplus_{i=0}^{n+m} \left(\bigdoubleplus_{j=0}^{i} b_j a_{i-j} \right) x^i = g \odot f.$$

Ainda, o polinômio $1_{A[x]} \coloneqq 1$ é elemento neutro, pois

$$f \odot 1_{A[x]} = \bigdoubleplus_{i=0}^{m+0} \left(\left(\bigdoubleplus_{j=0}^{i-1} a_j \cdot 0 \right) + a_i \cdot 1 \right) x^i = \bigdoubleplus_{i=0}^{m} a_i x^i = f.$$

Por fim, distributividade... ■

Definição 10.8. Definimos o *grau* de um polinômio $f \in A[x] \subseteq \{0\}$ como o maior índice de um coeficiente não nulo de f; ou seja, se $f = \bigdoubleplus_{i=0}^{m} a_i x^i$ com $a_m \neq 0$, então $\text{grau}(f) = m$.

Proposição 10.7. *Seja $\boldsymbol{A} = (A, +, \cdot)$ um domínio e $f, g \in A[x] \setminus \{0\}$. Então*

$$\text{grau}(fg) = \text{grau}(f) + \text{grau}(g).$$

Demonstração. Sejam $\text{grau}(f) = m$ e $\text{grau}(g) = n$, e sejam $f = \bigdoubleplus_{i=0}^{m} a_i x^i$ e $g = \bigdoubleplus_{i=0}^{n} b_i x^i$. O produto fg terá coeficientes $\bigdoubleplus_{j=0}^{i} a_j b_{i-j}$, com $i \in \{0, \ldots, m+n\}$.

Notemos que, para $i = m + n$, $\bigplus_{j=0}^{i} a_j b_{i-j} = a_m b_n$. Isso ocorre porque todos os termos desse somatório se anulam, menos quando $j = m$. Se $j > m$, temos $a_j = 0$; se $j < m$, então $i - j > m + n - m = n$, e temos $b_{i-j} = 0$. Em ambos os casos, $a_j b_{i-j} = 0$. Portanto $\bigplus_{j=0}^{m+n} a_j b_{i-j} c = a_m b_n$. Como m e n são os graus de f e g, respectivamente, sabemos que $a_m \neq 0$ e $b_n \neq 0$ e, como $\boldsymbol{A}$ é um domínio, isso implica que $a_m b_n \neq 0$ Logo $fg \neq 0$ e $\text{grau}(fg) = m + n$. ■

Proposição 10.8. *Seja $\boldsymbol{A} = (A, +, \cdot)$ um anel. Então $\boldsymbol{A}$ é um domínio se, e somente se, $\boldsymbol{A}[\boldsymbol{x}] = (A[x], +, \cdot)$ é um domínio.*

Demonstração. Suponha que $\boldsymbol{A}$ é um domínio e sejam $f, g \in A[x] \setminus \{0\}$. Então $\text{grau}(fg) = \text{grau}(f) + \text{grau}(g)$, o que mostra que $fg \neq 0$. Logo $\boldsymbol{A}[\boldsymbol{x}]$ é um domínio. Por outro lado, suponha que $\boldsymbol{A}[\boldsymbol{x}]$ é um domínio e sejam $a_1, a_2 \in A \setminus \{0\}$. Então $a_1, a_2 \in A[x] \setminus \{0\}$ e, portanto, $a_1 a_2 \neq 0$. Logo $\boldsymbol{A}$ é um domínio. ■

Podemos ver que $\boldsymbol{A}[\boldsymbol{x}]$ nunca é um corpo, pois x não tem inverso.

Definição 10.9. Sejam $\boldsymbol{A_i} = (A_i, +_i, \cdot_i)$, $i \in I \coloneqq \{1, \ldots, n\}$, n anéis e $a = (a_i)_{i \in I}, b = (b_i)_{i \in I} \in \bigtimes_{i \in I} A_i$. Então definimos as operações binárias $+$ e $\cdot$ em $\bigtimes_{i=1}^{n} A_i$ por

$$a + b \coloneqq (a_i +_i b_i)_{i \in I} \qquad\qquad a \cdot b \coloneqq (a_i \cdot_i b_i)_{i \in I}.$$

Denotaremos as operações $+_i$ todas por $+$ e as operações $\cdot_i$ todas por $\cdot$ quando não existir ambiguidade.

Proposição 10.9. *Sejam $\boldsymbol{A_i} = (A_i, +_i, \cdot_i)$, $i \in I \coloneqq \{1, \ldots, n\}$, n anéis. Então*

$$\bigtimes \boldsymbol{A} = \left(\bigtimes_{i=1}^{n} A_i, +, \cdot \right)$$

é um anel.

Demonstração. Sejam $a = (a_i)_{i \in I}, b = (b_i)_{i \in I}, c = (c_i)_{i \in I} \in \bigtimes_{i=1}^{n} A_i$. Vamos mostrar que a tripla $\left(\bigtimes_{i=1}^{n} A_i, + \right)$ é um grupo comutativo. As popriedades de grupo comutativo decorrem do fato de que $(A_i, +_i)$, $i \in I$, são todos grupos comutativos com elementos neutros 0_i, respectivamente. A operação $+$ é associativa, pois

$$\begin{aligned}
(a + b) + c &= (a_i +_i b_i)_{i \in I} + c \\
&= ((a_i +_i b_i) +_i c_i)_{i \in I} \\
&= (a_i +_i (b_i +_i c_i))_{i \in I} \\
&= a + (b_i +_i c_i)_{i \in I} \\
&= a + (b + c),
\end{aligned}$$

e comutativa, pois

$$a + b = (a_i +_i b_i)_{i \in I} = (b_i +_i a_i)_{i \in I} = b + a.$$

Ainda, $0 \coloneqq (0_i)_{i \in I}$ é elemento neutro, pois

$$a + 0 = (a_i + 0_i)_{i \in I} = (a_i)_{i \in I} = a.$$

Por fim, existe $-a_i \in A_i$ para todo $i \in I$. Assim, $-a = (-a_i)_{i \in I}$ é inverso de a, pois

$$a + (-a) = (a_i + (-a_i))_{i \in I} = (0_i)_{i \in I} = 0.$$

Agora, devemos mostrar que $\left(\bigtimes_{i=1}^{n} A_i, \cdot \right)$ é um monoide comutativo. Novamente, as popriedades de monoide comutativo decorrem do fato de que $(A_i, \cdot_i)$, $i \in I$, são todos monoides comutativos com elementos neutros 1_i, respectivamente. A operação $\cdot$ é associativa, pois

$$\begin{aligned}
(a \cdot b) \cdot c &= (a_i \cdot_i b_i)_{i \in I} \cdot c \\
&= ((a_i \cdot_i b_i) \cdot_i c_i)_{i \in I} \\
&= (a_i \cdot_i (b_i \cdot_i c_i))_{i \in I} \\
&= a \cdot (b_i \cdot_i c_i)_{i \in I} \\
&= a \cdot (b \cdot c),
\end{aligned}$$

e comutativa, pois

$$a \cdot b = (a_i \cdot_i b_i)_{i \in I} = (b_i \cdot_i a_i)_{i \in I} = b \cdot a.$$

Ainda, $1 \coloneqq (1_i)_{i \in I}$ é elemento neutro, pois

$$a \cdot 1 = (a_i \cdot 1_i)_{i \in I} = (a_i)_{i \in I} = a.$$

Por fim, como $\cdot_i$ são ditributivas sobre $+_i$, temos que

$$\begin{aligned}
a \cdot (b + c) &= a \cdot (b_i +_i c_i)_{i \in I} \\
&= (a_i \cdot_i (b_i +_i c_i))_{i \in I} \\
&= ((a_i \cdot_i b_i) +_i (a_i \cdot_i c_i))_{i \in I} \\
&= (a_i \cdot_i b_i)_{i \in I} + (a_i \cdot_i c_i)_{i \in I} \\
&= (a \cdot b) + (a \cdot c).
\end{aligned}$$

■

10.4 Ideais e Anéis Quocientes

Definição 10.10. Seja $\boldsymbol{A}$ um anel. Um *ideal* de $\boldsymbol{A}$ é um conjunto não vazio $I \subseteq A$ tal que

1. $\forall i_1, i_2 \in I \qquad i_1 - i_2 \in I$
2. $\forall a \in A, i \in I \qquad ai \in I$

Denotamos que I é ideal de $\boldsymbol{A}$ por $I \trianglelefteq A$. Ainda, $I \triangleleft A$ significa que $I \neq A$ e $I \trianglelefteq A$.

É interessante observar que I é subgrupo de $(A, +)$. A definição de ideal difere da definição de subanel na propriedade 2.

Proposição 10.10. *Sejam $\boldsymbol{A}$ um anel e $I \trianglelefteq A$. Então*

1. $0 \in I$;
2. $\forall i_1, i_2 \in I \qquad i_1 + i_2 \in I$;
3. $1 \in I \Rightarrow I = A$;
4. $\{0\}$ *e* A *são ideais de* A.

Demonstração.

1. Seja $i \in I$. Então $0 = i - i \in I$.
2. Sejam $i_1, i_2 \in I$. Pelo item anterior, sabemos que $0 \in I$, o que implica $-i_2 = 0 - i_2 \in I$. Logo $i_1 + i_2 = i_1 - (-i_2) \in I$.
3. Se $1 \in I \trianglelefteq A$, então, para todo $a \in A$, temos $a = a \cdot 1 \in A$. Logo $I = A$.
4. Consideremos $\{0\}$. Se $i \in \{0\}$, então $i = 0$. Portanto, para todo $a \in A$ e $i \in \{0\}$, temos $i - i = 0 \in \{0\}$ e $ai = 0 \in \{0\}$. Logo $\{0\} \trianglelefteq A$. Agora, consideremos A. Para todo $a_1, a_2 \in A$, temos $a_1 - a_2 \in A$ e $a_1 a_2 \in A$. Logo $A \trianglelefteq A$.

■

Proposição 10.11. *Sejam $\boldsymbol{A}$ um anel e $(I_j)_{j \in J}$ uma família de ideais de $\boldsymbol{A}$. Então*

$$I \coloneqq \bigcap_{j \in J} I_j$$

é um ideal de $\boldsymbol{A}$.

Demonstração. Sejam $i_1, i_2 \in I$ e $a \in A$. Então, para todo $j \in J$, $i_1, i_2 \in I_j$ e, como I_j é ideal de $\boldsymbol{A}$, segue que $i_1 - i_2 \in I_j$ e que $ai_1 \in W_i$. Logo $i_1 - i_2 \in I$ e $ai_1 \in I$, o que mostra que I é ideal de $\boldsymbol{A}$. ■

Proposição 10.12. *Sejam $\boldsymbol{A}$ um anel e $(I_j)_{n\in\mathbb{N}}$ uma sequência crescente de ideais de $\boldsymbol{A}$; ou seja, $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$. Então*

$$I \coloneqq \bigcup_{n\in\mathbb{N}} W_n$$

é um ideal de $\boldsymbol{A}$.

Demonstração. Sejam $i_1, i_2 \in I$. Então existem $n, m \in \mathbb{N}$ tais que $i_1 \in I_n$ e $i_2 \in I_m$. Nesse caso, $I_n \subseteq I_m$ ou $I_m \subseteq I_n$. Sem perda de generalidade, suponhamos o primeiro caso. Então segue que $i_1 \in I_m$ e, portanto, $i_1 - i_2 \in I_m$, o que mostra que $i_1 - i_2 \in I$. Agora, seja $a \in A$ e notemos que, como I_n é ideal de $\boldsymbol{A}$, segue qque $ai_1 \in I_n$. Logo $ai_1 \in I$, o que mostra que I é ideal de $\boldsymbol{A}$. ■

Definição 10.11. Sejam $\boldsymbol{A}$ um anel e $a_1, \ldots, a_n \in A$. Definimos o conjunto

$$\dotplus_{i=1}^{n} a_i A = a_1 A + \ldots + a_n A \coloneqq \left\{ \dotplus_{i=1}^{n} a_i b_i : b_i \in A \right\}$$

Proposição 10.13. *Seja $\boldsymbol{A}$ um anel e $a_1, \ldots, a_n \in A$. Então*

$$I \coloneqq \dotplus_{k=1}^{n} a_k A \trianglelefteq A.$$

Demonstração. Sejam $a \in A$ e $i_1, i_2 \in I$ tais que $i_1 = \dotplus_{k=1}^{n} a_i b_i$ e $i_2 = \dotplus_{k=1}^{n} a_i c_i$. Então

$$i_1 - i_2 = \dotplus_{k=1}^{n} a_k b_k - \dotplus_{k=1}^{n} a_k c_k = \dotplus_{k=1}^{n} a_k (b_k - c_k) \in I,$$

pois $(b_k - c_k) \in A$ para todo $k \in \{1, \ldots, n\}$. Ainda,

$$ak_1 = a \dotplus_{k=1}^{n} a_k b_k = \dotplus_{k=1}^{n} a_k (ab_k) \in I,$$

pois $ab_k \in A$ para todo $k \in \{1, \ldots, n\}$. Logo $I \trianglelefteq A$. ■

Esse ideal é chamado de ideal de A gerado por $a_1, \ldots, a_n$.

Definição 10.12. Seja $\boldsymbol{A}$ um anel. Um *ideal principal* de $\boldsymbol{A}$ é um ideal $I \trianglelefteq A$ tal que

1. $\exists a \in A \qquad I = aA.$

Proposição 10.14. *Seja $\boldsymbol{A}$ um anel. Então $\boldsymbol{A}$ é um corpo se, e somente se, $\boldsymbol{A}$ é um anel não-trivial cujos únicos ideais de $\boldsymbol{A}$ são $\{0\}$ e A.*

Demonstração. Suponha que $\boldsymbol{A}$ é um corpo. Então $(A \setminus \{0\}, \cdot)$ é um grupo e, portanto, $A \neq \emptyset$. Seja $I \trianglelefteq A$ e suponha que $I \neq \{0\}$. Então existe $i \in I \setminus \{0\}$. Como $\boldsymbol{A}$ é corpo, existe $i^{-1} \in A$. Portanto $1 = i^{-1}i \in I$. Logo $I = A$.

Por outro lado, suponha que os únicos ideais de A são $\{0\}$ e A. Como $\boldsymbol{A}$ é não-trivial, seja $a \in A \setminus \{0\}$ e consideremos o ideal $I = aA$. Notemos que $a = a \cdot 1 \in aA$, o que implica $I \neq \{0\}$. Portanto $I = A$. Mas então $1 \in aA$, o que significa que deve existir $b \in A$ tal que $1 = ab$; ou seja, todo $a \in A \setminus \{0\}$ tem inverso em A. Logo $\boldsymbol{A}$ é corpo. ■

Proposição 10.15. *Sejam $\boldsymbol{A}$ um anel e $I \trianglelefteq A$. A relação binária $\sim_I$ em A, definida por*

$$a \sim_I b \Leftrightarrow a - b \in I,$$

é uma relação de equivalência.

Demonstração. Vamos demonstrar as três propriedades de uma relação de equivalência.

1. (Reflexividade) Seja $a \in A$. Então $a - a = 0 \in I$. Logo $a \sim_I a$.
2. (Simetria) Sejam $a_1, a_2 \in A$ tais que $a_1 \sim_I a_2$. Então $(a_1 - a_2) \in I$. Mas $0 \in I$, o que implica $a_2 - a_1 = 0 - (a_1 - a_2) \in I$. Logo $a_2 \sim_I a_1$.
3. (Transitividade) Sejam $a_1, a_2, a_3 \in A$ tais que $a_1 \sim_I a_2$ e $a_2 \sim_I a_3$. Então $(a_1 - a_2), (a_2 - a_3) \in I$, o que implica $a_1 - a_3 = (a_1 - a_2) + (a_2 - a_3) \in I$. Logo $a_1 \sim_I a_3$.

■

Definição 10.13. Sejam $\boldsymbol{A}$ um anel e $I \trianglelefteq A$. O conjunto $a + I \coloneqq \{a + i : i \in I\}$ é a *classe lateral* de I com representante a. O conjunto das classes laterais de A é denotado por $A/I \coloneqq \{a + I : a \in A\}$.

Proposição 10.16. *Sejam $(A, +, \cdot)$ um anel, $I \trianglelefteq A$ e $\sim_I$ a relação de equivalência definida na proposição anterior e $a \in A$. Então a classe de equivalência $[a] = \{b \in A : b \sim_I a\}$ é igual à classe lateral $a + I$ e, por consequência, o conjunto quociente $A/\sim_I$ é igual ao conjunto A/I.*

Demonstração. Seja $b \in [a]$. Então $b - a \in I$; ou seja, existe $i \in I$ tal que $b - a = i$. Mas isso implica $b = a + i$, que implica, por sua vez, que $b \in a + I$. Por outro lado, seja $b \in a + I$. Então existe $i \in I$ tal que $b = a + i$; ou seja, $b - a = i$, que implica $b - a \in I$ e, assim, $b \in [a]$. Disso, vem que $A/\sim_I = A/I$. ■

Uma consequência disso é que o conjunto A é particionado em classes laterais de I. Outra consequência é que duas classes laterais são iguais se, e somente se, a diferença entre seus representantes está em I.

Definição 10.14. Sejam $\boldsymbol{A}$ um anel, $I \trianglelefteq A$ e $a_1, a_2 \in A$. Então definimos as operações binárias $\oplus$ e $\odot$ em A/I por

$$(a_1 + I) \oplus (a_2 + I) \coloneqq (a_1 + a_2) + I \qquad (a_1 + I) \odot (a_2 + I) \coloneqq (a_1 \cdot a_2) + I$$

Denotaremos $\oplus$ e $\odot$ por $+$ e $\cdot$ quando não existir ambiguidade.

Proposição 10.17. *As operações $\oplus$ e $\odot$ da definição anterior estão bem definidas.*

Demonstração. Sejam $a_1, a_2, b_1, b_2 \in A$ tais que $a_1 + I = a_2 + I$ e $b_1 + I = b_2 + I$. Primeiro, vamos mostrar que $\oplus$ está bem definida. Devemos mostrar que $(a_1 + b_1) + I = (a_2 + b_2) + I$. De $a_1 + I = a_2 + I$, sabemos que $a_1 - a_2 \in I$. Da mesma forma, $b_1 - b_2 \in I$. Mas então $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I$, o que implica $(a_1 + b_1) + I = (a_2 + b_2) + I$.

Agora, vamos mostrar que $\odot$ está bem definida. Devemos mostrar que $(a_1 b_1) + I = (a_2 b_2) + I$. Sejam $c = a_1 - a_2$ e $d = b_1 - b_2$. Notemos que

$$a_1 b_1 = (a_2 + c)(b_2 + d) = a_2 b_2 + a_2 d + c b_2 + cd.$$

Como $c, d \in I$, $(a_2 d + c b_2 + cd) \in I$. Logo $a_1 b_1 - a_2 b_2 \in I$, o que implica $(a_1 b_1) + I = (a_2 b_2) + I$. ■

Proposição 10.18. *Sejam $\boldsymbol{A} = (A, +, \cdot)$ um anel e $I \trianglelefteq A$. Então $\boldsymbol{A/I} \coloneqq (A/I, \oplus, \odot)$ é um anel, chamado* anel quociente *de A por I.*

Demonstração. Sejam $a_1, a_2, a_3 \in A$. Primeiro, vamos mostrar que $(A/I, \oplus)$ é um grupo comutativo. As propriedades de grupo comutativo decorrem do fato de que $(A, +)$ é grupo comutativo com elemento neutro 0. A operação $\oplus$ é associativa, pois

$$\begin{aligned}((a_1 + I) \oplus (a_2 + I)) \oplus (a_3 + I) &= ((a_1 + a_2) + I) \oplus (a_3 + I) \\ &= ((a_1 + a_2) + a_3) + I \\ &= (a_1 + (a_2 + a_3)) + I \\ &= (a_1 + I) \oplus ((a_2 + a_3) + I) \\ &= (a_1 + I) \oplus ((a_2 + I) \oplus (a_3 + I)),\end{aligned}$$

e comutativa, pois

$$(a_1 + I) \oplus (a_2 + I) = (a_1 + a_2) + I = (a_2 + a_1) + I = (a_2 + I) \oplus (a_1 + I).$$

Ainda, $0 + I$ é elemento neutro, pois

$$(a_1 + I) \oplus (0 + I) = (a_1 + 0) + I = a_1 + I.$$

Por fim, existe $-a_1 \in A$. Assim, $(-a_1) + I$ é inverso de $a_1 + I$, pois

$$(a_1 + I) \oplus ((-a_1) + I) = (a_1 + (-a_1)) + I = 0 + I.$$

Agora, devemos mostrar que $(A/I, \odot)$ é um monoide comutativo. Novamente, as propriedades de monoide comutativo decorrem do fato de que $(A, \cdot)$ é um monoide comutativo com elemento neutro 1. A operação $\odot$ é associativa, pois

$$\begin{aligned}((a_1 + I) \odot (a_2 + I)) \odot (a_3 + I) &= ((a_1 \cdot a_2) + I) \odot (a_3 + I) \\ &= ((a_1 \cdot a_2) \cdot a_3) + I \\ &= (a_1 \cdot (a_2 \cdot a_3)) + I \\ &= (a_1 + I) \odot ((a_2 \cdot a_3) + I) \\ &= (a_1 + I) \odot ((a_2 + I) \odot (a_3 + I)),\end{aligned}$$

e comutativa, pois

$$(a_1 + I) \odot (a_2 + I) = (a_1 \cdot a_2) + I = (a_2 \cdot a_1) + I = (a_2 + I) \odot (a_1 + I).$$

Ainda, $1 + I$ é elemento neutro, pois

$$(a_1 + I) \odot (1 + I) = (a_1 \cdot 1) + I = a_1 + I.$$

Por fim, como $\cdot$ é distributiva sobre $+$, temos que

$$\begin{aligned}(a + 1 + I) \odot ((a_2 + I) \oplus (a_3 + I)) &= (a + 1 + I) \odot ((a_2 + a_3) + I) \\ &= (a_1 \cdot (a_2 + a_3)) + I \\ &= ((a_1 \cdot a_2) + (a_1 \cdot a_3)) + I \\ &= ((a_1 \cdot a_2) + I) \oplus ((a_1 \cdot a_3) + I) \\ &= ((a_1 + I) \odot (a_2 + I)) \oplus ((a_1 + I) \odot (a_3 + I)).\end{aligned}$$

■

10.5 Homomorfismos de Anéis

Definição 10.15. Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ dois anéis. Um *homomorfismo de anéis* entre $\boldsymbol{A}$ e $\boldsymbol{B}$ é uma função $\phi : A \to B$ que é

1. um homomorfismo de grupos entres $(A, +)$ e $(B, \oplus)$

   (a) $\forall a_1, a_2 \in A \qquad \phi(a_1 + a_2) = \phi(a_1) \oplus \phi(a_2)$;

2. um homomorfismo de monoides entre $(A, \cdot)$ e $(B, \odot)$

(a) $\forall a_1, a_2 \in A \qquad \phi(a_1 \cdot a_2) = \phi(a_1) \odot \phi(a_2)$;

(b) $\phi(1_A) = 1_B$.

O conjunto de todos os homomorfismos de anéis entre $\boldsymbol{A}$ e $\boldsymbol{B}$ é denotado por $\mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$.

Exemplo 10.1. Seja $(A, +, \cdot)$ um anel e consideremos o anel dos números inteiros $(\mathbb{Z}, +, \cdot)$. Então

$$\begin{aligned} \phi : \mathbb{Z} &\to A \\ z &\mapsto \begin{cases} \overset{z}{\underset{i=1}{+}} 1_A & z > 0 \\ 0_A & z = 0 \\ -\phi(-z) & z > 0 \end{cases} \end{aligned}$$

é um homomorfismo de anéis.

Demonstração. Sejam $z_1, z_2 \in \mathbb{Z}$. Para ver que ϕ é um homomorfismo de anéis, provemos primeiro que $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$. Vamos separar a demonstração em vários casos. Primeiro, notemos que, se $z_1 = 0$ ou $z_2 = 0$, a igualdade é trivial; sem perda de generalidade, suponha que $z_2 = 0$. Então

$$\phi(z_1 + z_2) = \phi(z_1) = \phi(z_1) + 0_A = \phi(z_1) + \phi(z_2).$$

Então, suponhamos $z_1 z_2 \neq 0$. Se $z_1 > 0$ e $z_1 > 0$, então $z_1 + z_2 > 0$. Logo

$$\phi(z_1 + z_2) = \overset{z_1+z_2}{\underset{i=1}{+}} 1_A = \overset{z_1}{\underset{i=1}{+}} 1_A + \overset{z_1+z_2}{\underset{i=z_1+1}{+}} 1_A = \overset{z_1}{\underset{i=1}{+}} 1_A + \overset{z_2}{\underset{i=1}{+}} 1_A = \phi(z_1) + \phi(z_2).$$

Se $z_1 < 0$ e $z_1 < 0$, então $z_1 + z_2 < 0$. Logo $-z_1$, $-z_2$ e $-(z_1 + z_2)$ são positivos e segue da equação anterior que

$$\begin{aligned} \phi(z_1 + z_2) &= -\phi(-(z_1 + z_2)) \\ &= -\phi((-z_1) + (-z_2)) \\ &= -(\phi(-z_1) + \phi(-z_2)) \\ &= -(-\phi(z_1) - \phi(z_2)) \\ &= \phi(z_1) + \phi(z_2). \end{aligned}$$

No caso que resta, z_1 e z_2 são um positivo e um negativo; sem perda de generalidade, suponhamos que $z_1 > 0$ nesse caso $-z_2 > 0$. Se tivermos $z_1 = -z_2$,

então

$$\begin{aligned}\phi(z_1+z_2) &= \phi(0)\\ &= 0_A\\ &= \overset{z_1}{\underset{i=1}{\dotplus}} 1_A - \overset{z_1}{\underset{i=1}{\dotplus}} 1_A\\ &= \phi(z_1)-\phi(-z_1)\\ &= \phi(z_1)+\phi(z_2).\end{aligned}$$

Se tivermos $z_1 > -z_2$, então

$$\begin{aligned}\phi(z_1+z_2) &= \overset{z_1+z_2}{\underset{i=1}{\dotplus}} 1_A\\ &= \overset{z_1+z_2}{\underset{i=1}{\dotplus}} 1_A + \overset{-z_2}{\underset{i=1}{\dotplus}} 1_A - \overset{-z_2}{\underset{i=1}{\dotplus}} 1_A\\ &= \overset{z_1+z_2}{\underset{i=1}{\dotplus}} 1_A + \overset{z_1}{\underset{i=z_1+z_2+1}{\dotplus}} 1_A - \overset{-z_2}{\underset{i=1}{\dotplus}} 1_A\\ &= \overset{z_1}{\underset{i=1}{\dotplus}} 1_A - \overset{-z_2}{\underset{i=1}{\dotplus}} 1_A\\ &= \phi(z_1)+\phi(z_2).\end{aligned}$$

Por fim, se $-z_2 > z_1$, então $-z_1 < 0$ e $-z_2 >$ e segue da equação anterior que

$$\begin{aligned}\phi(z_1+z_2) &= -\phi(-(z_1+z_2))\\ &= -\phi((-z_1)+(-z_2))\\ &= -(\phi(-z_1)+\phi(-z_2))\\ &= -(-\phi(z_1)-\phi(z_2))\\ &= \phi(z_1)+\phi(z_2).\end{aligned}$$

■

Exemplo 10.2. Sejam $\boldsymbol{A}$ um anel e $I \trianglelefteq A$. Então a *projeção canônica* de A em A/I, definida por

$$\begin{aligned}\pi : A &\to {}^{A}\!/_{I}\\ a &\mapsto a+I,\end{aligned}$$

é um homomorfismo de anéis.

Demonstração. Sejam $a_1, a_2 \in A$. Vemos que π é um homomorfismo de grupos entre $(A, +)$ e $(A/I, +)$, pois

$$\pi(a_1 + a_2) = (a_1 + a_2) + I = (a_1 + I) + (a_2 + I) = \pi(a_1) + \pi(a_2).$$

Também, vemos que π é um homomorfismo de monoides entre $(A, \cdot)$ e $(A/I, \cdot)$, pois

$$\pi(a_1 \cdot a_2) = (a_1 \cdot a_2) + I = (a_1 + I) \cdot (a_2 + I) = \pi(a_1) \cdot \pi(a_2)$$

e $\pi(1) = 1 + I = 1_{A/I}$. ■

Corolário 10.19 (Homomorfismos preservam a estrutura algébrica entre anéis)**.** *Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ dois anéis e $\phi : A \to B$ um homomorfismo de anéis. Então*

1. $\phi(0_A) = 0_B$;
2. $-\phi(a) = \phi(-a)$.

Demonstração. Como ϕ é um homomorfismo de grupos entres $(A, +)$ e $(B, \oplus)$, sabemos que ϕ preserva a estrutura algébrica de grupo entre os grupos (9.17). ■

Corolário 10.20 (Composição de homomorfismos é homomorfismo)**.** *Sejam $\boldsymbol{A_1} = (A_1, +_1, \cdot_1)$, $\boldsymbol{A_2} = (A_2, +_2, \cdot_2)$ e $\boldsymbol{A_3} = (A_3, +_3, \cdot_3)$ três anéis e $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A_1}, \boldsymbol{A_2})$ e $\psi \in \mathcal{H}\mathrm{om}(\boldsymbol{A_2}, \boldsymbol{A_3})$. Então $(\psi \circ \phi) \in \mathcal{H}\mathrm{om}(\boldsymbol{A_1}, \boldsymbol{A_3})$.*

Demonstração. As duas propriedades de homomorfismo de anéis para $(\psi \circ \phi)$ seguem de propriedades análogas na seção de grupos e monoides.

1. Como ϕ é um homomorfismo de grupos entre $(A_1, +_1)$ e $(A_2, +_2)$ e ψ é homomorfismos de grupos entre $(A_2, +_2)$ e $(A_3, +_3)$, segue da proposição de composição de homomorfismos da seção de grupos (9.18) que $(\psi \circ \phi)$ é homomorfismo de grupos entre $(A_1, +_1)$ e $(A_3, +_3)$.

2. Como ϕ é um homomorfismo de monoides entre $(A_1, \cdot_1)$ e $(A_2, \cdot_2)$ e ψ é homomorfismos de monoides entre $(A_2, \cdot_2)$ e $(A_3, \cdot_3)$, segue da proposição de composição de homomorfismos da seção de monoides (8.8) que $(\psi \circ \phi)$ é homomorfismo de monoides entre $(A_1, \cdot_1)$ e $(A_3, \cdot_3)$.

■

Proposição 10.21. *Sejam $\boldsymbol{A}$ e $\boldsymbol{B}$ anéis, $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$ e $I \trianglelefteq B$. Então $\phi^{-1}(I) \trianglelefteq A$.*

Demonstração. Sejam $i_1, i_2 \in \phi^{-1}(I)$ e $a \in A$. Então, como $\phi(i_1), \phi(i_2) \in I$, temos $\phi(i_1 - i_1) = \phi(i_1) - \phi(i_2) \in I$, o que implica que $i_1 - i_2 \in \phi^{-1}(I)$. Ainda, como $\phi(a) \in A$, temos que $\phi(ai_1) = \phi(a)\phi(i_1) \in I$, o que implica $ai_1 \in \phi^{-1}(I)$. Logo $\phi^{-1}(I) \trianglelefteq A$. ■

Proposição 10.22. *Sejam $\boldsymbol{A}$ e $\boldsymbol{B}$ anéis, $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$ sobrejetivo e $I \trianglelefteq A$. Então $\phi(I) \trianglelefteq B$.*

Demonstração. Sejam $j_1, j_2 \in \phi(I)$ e $b \in B$. Então existem $i_1, i_2 \in I$ tais que $\phi(i_1) = j_1$ e $\phi(i_2) = j_2$ e, como ϕ é sobrejetiva, existe $a \in A$ tal que $\phi(a) = b$. Então, como $I \trianglelefteq A$, temos que $i_1 - i_2 \in I$ e $ai_1 \in I$, o que implica $j_1 - j_2 = \phi(i_1) - \phi(i_2) = \phi(i_1 - i_2) \in \phi(I)$ e $bj_1 = \phi(a)\phi(i_1) = \phi(ai_1) \in \phi(I)$. Logo $\phi(I) \trianglelefteq B$. ■

Definição 10.16. Sejam $\boldsymbol{A}$ e $\boldsymbol{B}$ dois anéis e $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$. O *núcleo* de ϕ é o conjunto

$$\mathcal{N}(\phi) \coloneqq \{a \in A : \phi(a) = 0_B\}$$

e a *imagem* de ϕ é o conjunto

$$\mathcal{I}\mathrm{m}(\phi) \coloneqq \{b \in B : \exists a \in A, \phi(a) = b\}.$$

Proposição 10.23. *Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ dois anéis e seja $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$. Então*

1. *$\mathcal{N}(\phi) \trianglelefteq A$;*
2. *$\mathcal{I}\mathrm{m}(\phi)$ é subanel de $\boldsymbol{B}$.*

Demonstração. Demonstramos as afirmações separadamente.

1. Primeiro notamos que $\mathcal{N}(\phi) \subseteq A$ e que $\mathcal{N}(\phi)$ não é vazio, pois, como $\phi(0_A) = 0_B$, então $0_A \in \mathcal{N}(\phi)$. Vamos mostrar as duas propriedades de um ideal. Sejam $a \in A$ e $n_1, n_2 \in \mathcal{N}(\phi)$. Então $n_1 - n_2 \in \mathcal{N}(\phi)$, pois

   $$\phi(n_1 - n_2) = \phi(n_1) - \phi(n_2) = 0_B - 0_B = 0_B.$$

   Ainda, $a \cdot n_1 \in \mathcal{N}(\phi)$, pois

   $$\phi(a \cdot n_1) = \phi(a) \odot \phi(n_1) = \phi(a) \odot 0_B = 0_B.$$

   Portanto $\mathcal{N}(\phi)$ é ideal de A.

2. Claramente, $\mathrm{Im}(\phi) \subseteq B$ e $\mathrm{Im}(\phi)$ não é vazio. Sejam $i_1, i_2 \in \mathrm{Im}(\phi)$. Então existem $a_1, a_2 \in A$ tais que $\phi(a_1) = i_1$ e $\phi(a_2) = i_2$. Portanto $i_1 \ominus i_2 \in \mathrm{Im}(\phi)$, já que
$$\phi(a_1 - a_2) = \phi(a_1) - \phi(a_2) = i_1 - i_2.$$
Ainda, $i_1 \odot i_2 \in \mathrm{Im}(\phi)$, pois
$$\phi(a_1 \cdot a_2) = \phi(a_1) \odot \phi(a_2) = i_1 \odot i_2.$$
Por fim, $1_B \in \mathrm{Im}(\phi)$, pois $\phi(1_A) = 1_B$. Logo $\mathrm{Im}(\phi)$ é subanel de $\boldsymbol{B}$.

■

Proposição 10.24. *Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ dois anéis e seja $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$. Então ϕ é injetiva se, e somente se, $\mathcal{N}(\phi) = \{0_A\}$.*

Demonstração. Como ϕ é um homomorfismo de anéis, ele é um homomorfismo de grupos entre $(A, +)$ e $(B, \oplus)$. Então, pela proposição análoga da seção de grupos (9.22), esta proposição está provada. ■

Definição 10.17. Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ dois anéis. Um isomorfismo de anéis é um homomorfismo de anéis $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$ que é bijetivo. O conjunto de todos os homomorfismos de anéis entre $\boldsymbol{A}$ e $\boldsymbol{B}$ é denotado por $\mathcal{I}\mathrm{so}(\boldsymbol{A}, \boldsymbol{B})$.

Proposição 10.25. *Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ anéis e $\phi \in \mathcal{I}\mathrm{so}(\boldsymbol{A}, \boldsymbol{B})$. Então $\phi^{-1} \in \mathcal{I}\mathrm{so}(\boldsymbol{B}, \boldsymbol{A})$.*

Demonstração. Como ϕ é bijetiva, sua inversa ϕ^{-1} também é bijetiva. Devemos provar que ϕ^{-1} é um homomorfismo de anéis. Sejam $b_1, b_1 \in B$. Primeiro, vamos provar que ϕ^{-1} é um homomorfismo de grupos entre $\boldsymbol{B}$ e $\boldsymbol{A}$. Como ϕ é isomorfismo, existem $a_1, a_2 \in A$ tais que $\phi(a_1) = b_1$ e $\phi(a_2) = b_2$. Então
$$\begin{aligned}\phi^{-1}(b_1 \oplus b_2) &= \phi^{-1}(\phi(a_1) \oplus \phi(a_2)) \\ &= \phi^{-1}(\phi(a_1 + a_2)) \\ &= a_1 + a_2 \\ &= \phi^{-1}(b_1) \oplus \phi^{-1}(b_2)\end{aligned}$$
e
$$\phi^{-1}(\ominus b_1) = \phi^{-1}(\phi(-a_1)) = -a_1 = \ominus\phi(b_1).$$
Agora, mostramos que ϕ^{-1} é homomorfismo de monoides entre $(B, \odot)$ e $(A, \cdot)$.
$$\begin{aligned}\phi^{-1}(b_1 \odot b_2) &= \phi^{-1}(\phi(a_1) \odot \phi(a_2)) \\ &= \phi^{-1}(\phi(a_1 \cdot a_2)) \\ &= a_1 \cdot a_2 \\ &= \phi^{-1}(b_1) \odot \phi^{-1}(b_2)\end{aligned}$$
e, como $\phi(1_A) = 1_B$, temos $\phi^{-1}(1_B) = 1_A$. ■

Definição 10.18. Sejam $\boldsymbol{A}$ e $\boldsymbol{B}$ dois anéis. Dizemos que $\boldsymbol{A}$ é *isomorfo* a $\boldsymbol{B}$, e denotamos isso por $\boldsymbol{A} \simeq \boldsymbol{B}$, sse existe $\phi \in \mathcal{I}\mathrm{so}(\boldsymbol{A}, \boldsymbol{B})$.

Proposição 10.26. *Sejam $\boldsymbol{A_1}$, $\boldsymbol{A_2}$ e $\boldsymbol{A_3}$ três anéis. Então*

1. *(Reflexividade) $\boldsymbol{A_1} \simeq \boldsymbol{A_1}$;*
2. *(Antissimetria) $\boldsymbol{A_1} \simeq \boldsymbol{A_2} \Rightarrow \boldsymbol{A_2} \simeq \boldsymbol{A_1}$;*
3. *(Transitividade) $\boldsymbol{A_1} \simeq \boldsymbol{A_2}$ e $\boldsymbol{A_2} \simeq \boldsymbol{A_3} \Rightarrow \boldsymbol{A_1} \simeq \boldsymbol{A_3}$.*

OBS: *Não dizemos que $\simeq$ é uma relação de equivalência porque ela não está propriamente definida em um conjunto, já que não existe o conjunto de todos os anéis por não existir o conjunto de todos os conjuntos. No entanto, é claro que o que a proposição afirma é que ela satisfaz as propriedades de uma relação de equivalência.*

Demonstração. Vamos demonstrar as três propriedades separadamente.

1. Claramente, a função $\phi = Id_A : A \to A$ é um isomorfismo de anéis. Logo $\boldsymbol{A_1} \simeq \boldsymbol{A_1}$
2. Se $\mathbf{A}_1 \simeq \boldsymbol{A_2}$, existe $\phi \in \mathcal{I}\mathrm{so}(\boldsymbol{A_1}, \boldsymbol{A_2})$. Pela proposição (10.25), ϕ^{-1} é um isomorfismo de anéis entre $\boldsymbol{A_2}$ e $\boldsymbol{A_1}$. Logo $\boldsymbol{A_2} \simeq \boldsymbol{A_1}$.
3. $\boldsymbol{A_1} \simeq \boldsymbol{A_2}$, existe $\phi \in \mathcal{I}\mathrm{so}(\boldsymbol{A_1}, \boldsymbol{A_2})$ e, como $\boldsymbol{A_2} \simeq \boldsymbol{A_3}$, existe $\psi \in \mathcal{I}\mathrm{so}(\boldsymbol{A_2}, \boldsymbol{A_3})$. Assim, pela proposição (10.20), sabemos que $(\psi \circ \phi) \in \mathcal{H}\mathrm{om}(\boldsymbol{A_1}, \boldsymbol{A_3})$. Ainda, como ϕ e ψ são bijeções, sua composição é uma bijeção. Portanto $(\psi \circ \phi) \in \mathcal{I}\mathrm{so}(\boldsymbol{A_1}, \boldsymbol{A_3})$, o que implica $\boldsymbol{A_1} \simeq \boldsymbol{A_3}$.

■

10.6 Teoremas de Isomorfismo

Teorema 10.27 (Primeiro Teorema de Isomorfismo)**.** *Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ dois anéis e $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$. Então*

$$\boldsymbol{A}/\boldsymbol{\mathcal{N}(\varphi)} \simeq \boldsymbol{\mathcal{I}m(\varphi)}.$$

Demonstração. Primeiro, vale notar que, como $\mathrm{Im}(\phi) \trianglelefteq A$, o $\boldsymbol{A/\mathcal{N}(\phi)}$ é um anel. Agora, consideremos a função

$$\begin{aligned} \psi : A/\mathcal{N}(\phi) &\to \mathrm{Im}(\phi) \\ a + \mathcal{N}(\phi) &\mapsto \phi(a). \end{aligned}$$

Notemos que a função ψ é bem definida. Para isso, sejam $a_1, a_2 \in A$ tais que $a_1 + \mathcal{N}(\phi) = a_2 + \mathcal{N}(\phi)$. Então $(a_1 - a_2) \in \mathcal{N}(\phi)$, o que implica $\phi(a_1 - a_2) = 0$. Como ϕ é homomorfismo de anéis, segue que $\phi(a_1) = \phi(a_2)$. Então $\psi(a_1 + \mathcal{N}(\phi)) = \psi(a_2 + \mathcal{N}(\phi))$.

Vamos mostrar que essa função é um isomorfismo de anéis. Primeiro, vamos mostrar que ψ é homomorfismo de anéis. Para isso, vamos denotar $a + \mathcal{N}(\phi) \in A/\mathcal{N}(\phi)$ por $[a]$ para facilitar a demonstração. Sejam $[a_1], [a_2] \in A/\mathcal{N}(\phi)$. Vemos que ψ é homomosfismo de grupos entre $(A/\mathcal{N}(\phi), +)$ e $(\mathfrak{Im}(\phi), \oplus)$, pois

$$\psi([a_1] + [a_2]) = \psi([a_1 + a_2]) = \phi(a_1 + a_2) = \phi(a_1) \oplus \phi(a_2) = \psi([a_1]) \oplus \psi([a_2]).$$

Agora, vemos que ψ é homomosfismo de monoides entre $(A/\mathcal{N}(\phi), \cdot)$ e $(\mathfrak{Im}(\phi), \odot)$, pois

$$\psi([a_1] \cdot [a_2]) = \psi([a_1 \cdot a_2]) = \phi(a_1 \cdot a_2) = \phi(a_1) \odot \phi(a_2) = \psi([a_1]) \odot \psi([a_2])$$

e $\psi([1_A]) = \phi(1_A) = 1_B$.

Por fim, devemos mostrar que ψ é bijetiva. Primeiro, mostramos que ψ é injetiva. Seja $[a] \in \mathcal{N}(\psi)$. Então $\psi([a]) = 0_B$, o que implica $\phi(a) = 0_B$. Mas isso implica $a \in \mathcal{N}(\phi)$; ou seja, $[a] = [0_A]$. Logo $\mathcal{N}(\psi) = \{[0_A]\}$, que quer dizer que ψ é injetiva (10.24). Agora, notamos que ψ é sobrejetiva por construção, pois tem como contradomínio $\mathfrak{Im}(\phi)$. ■

Proposição 10.28 (Teorema Chinês do Resto)**.** *Sejam $m_1, \ldots, m_n \in \mathbb{N} \setminus \{0, 1\}$ dois a dois coprimos entre si. Então*

$$\mathbb{Z}\big/_{m_1 m_2 \ldots m_n \mathbb{Z}} \simeq \mathbb{Z}\big/_{m_1 \mathbb{Z}} \bigtimes \mathbb{Z}\big/_{m_2 \mathbb{Z}} \bigtimes \cdots \bigtimes \mathbb{Z}\big/_{m_n \mathbb{Z}}.$$

Demonstração. ■

Definição 10.19.

$$B + I \coloneqq \{b + i : b \in B, i \in I\}$$

Teorema 10.29 (Segundo Teorema de Isomorfismo)**.** *Sejam $\boldsymbol{A}$ um anel, B um subanel de $\boldsymbol{A}$ e $I \trianglelefteq A$. Então*

1. *$B + I$ é subanel de $\boldsymbol{A}$;*
2. *$B \cap I \trianglelefteq B$;*
3. $$\boldsymbol{B}\big/_{\boldsymbol{B} \cap \boldsymbol{I}} \simeq \boldsymbol{B} + \boldsymbol{I}\big/_{\boldsymbol{I}}.$$

Demonstração. 1. Para mostrar que $B + I$ é subanel de $\boldsymbol{A}$, primeiro notamos que $B + I$ não é vazio, pois B não é vazio e I não é vazio. Ainda, notamos que $B + I \subseteq A$, pois $B \subseteq A$ e $I \subseteq A$. Agora, mostramos as pripriedades de subanel. Sejam $b_1, b_2 \in B$ e $i_1, i_2 \in I$. Primeiro, mostraremos que $B + I$ é subgrupo de $(A, +)$. Note que $(b_1 + i_1) - (b_2 + i_2) \in B + I$, pois, como B é subgrupo de $(A, +)$, $b_1 - b_2 \in B$ e, como $I \trianglelefteq A$, $i_1 - i_2 \in A$, o que implica $(b_1 + i_1) - (b_2 + i_2) = (b_1 - b_2) + (i_1 - i_2) \in B + I$. Mostremos agora que $B + I$ é submonoide de $(A, \cdot)$. Note que

$$(b_1 + i_1)(b_2 + i_2) = b_1b_2 + b_1i_2 + i_1b_2 + i_1i_2.$$

Como B é submonoide de $(A, \cdot)$, $b_1b_2 \in B$ e, como $i \trianglelefteq A$, $b_1i_2, i_1b_2, i_1i_2 \in I$, o que implica $b_1i_2 + i_1b_2 + i_1i_2 \in I$. Logo $(b_1 + i_1)(b_2 + i_2) = (b_1b_2) + (b_1i_2 + i_1b_2 + i_1i_2) \in B + I$. Ainda, $1 \in B$ e $0 \in I$. Logo $1 = 1 + 0 \in B + I$.

2. Para mostrar que $B \cap I \trianglelefteq B$, notemos primeiro que $B \cap I$ não é vazio. De fato, como B é subanel de $\boldsymbol{A}$, segue que $0 \in B$ e, como $I \trianglelefteq A$, também segue que $0 \in I$, o que implica $0 \in B \cap I$. Claramente, $B \cap I \subseteq A$. Então basta provar as propriedades de ideal. Sejam $b_1, b_2 \in B \cap I$. Como B é subanel de $\boldsymbol{A}$, temos $b_1 - b_2 \in B$ e, como $I \trianglelefteq A$, temos $b_1 - b_2 \in I$. Logo $b_1 - b_2 \in B \cap I$. Seja $b \in B$. Como B é subanel de $\boldsymbol{A}$, temos $bb_1 \in B$ e, como $I \trianglelefteq A$, temos $bb_1 \in I$. Logo $bb_1 \in B \cap I$.

3. O isomorfismo só faz sentido se os dois quocientes fazem sentido. O primeiro faz sentido pelo item anterior. O segundo faz sentido pois, pela definição de ideal, segue direto que $I \trianglelefteq B + I$, pois $I \subseteq B + I \subseteq A$. Então devemos exibir um isomorfismo de anéis entre os dois anéis. Considere a função

$$\begin{aligned} \phi : B &\to {}^{B+I}\big/_{I} \\ b &\mapsto b + I. \end{aligned}$$

Essa função é um homomorfismo de anéis. Sejam $b_1, b_2 \in B$. Então $\phi(b_1 + b_2) = (b_1 + b_2) + I = (b_1 + I) + (b_1 + I) = \phi(b_1) + \phi(b_2)$. Ainda, vale $\phi(b_1b_2) = (b_1b_2) + I = (b_1 + I)(b_1 + I) = \phi(b_1)\phi(b_2)$. Por fim, $\phi(1) = 1 + I$.

Agora, notemos que $\mathcal{N}(\phi) = B \cap I$. Seja $b \in B$. Então

$$b \in \mathcal{N}(\phi) \Leftrightarrow \phi(b) = 0 \Leftrightarrow b + I = I \Leftrightarrow b \in I.$$

Por fim, notemos que $\mathfrak{Im}(\phi) = {}^{B+I}\big/_{I}$, pois um elemento de ${}^{B+I}\big/_{I}$ é da forma $b = i + I$, com $b \in B$ e $i \in I$. Mas então $b + i + I = b + I$. Logo segue do primeiro teorema de isomorfismo (10.27) que

$$\boldsymbol{{}^{B}\big/_{B \cap I} = {}^{B}\big/_{\mathcal{N}(\phi)} \simeq \mathfrak{Im}(\phi) = {}^{B+I}\big/_{I}}.$$

■

Lema 10.30. *Sejam $\boldsymbol{A}$ um anel e $I \trianglelefteq A$. Então*

1. *Se B é subanel de $\boldsymbol{A}$ tal que $I \subseteq B$, então ${}^{B}\!/_{I}$ é subanel de ${}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}$. Por outro lado, todo subanel de ${}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}$ é da forma ${}^{B}\!/_{I}$ para algum B subanel de $\boldsymbol{A}$ tal que $I \subseteq B$.*

2. *Se $J \trianglelefteq A$ tal que $I \subseteq J$, então ${}^{J}\!/_{I} \trianglelefteq {}^{A}\!/_{I}$. Por outro lado, todo ideal de ${}^{A}\!/_{I}$ é da forma ${}^{J}\!/_{I}$ para algum $J \trianglelefteq A$, tal que $I \subseteq J$.*

Demonstração. 1. Seja B um subanel de $\boldsymbol{A}$ tal que $I \subseteq B$. Para mostrar que o conjunto ${}^{B}\!/_{I}$ é subanel de ${}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}$, sejam $b_1+I, b_2+I \in {}^{B}\!/_{I}$. Então, como $b_1, b_2 \in B$, vale $b_1 - b_2 \in B$ e $b_1 b_2 \in B$ e segue que $(b_1+I)-(b_2+I) = (b_1-b_2)+I \in {}^{B}\!/_{I}$ e $(b_1+I)(b_2+I) = (b_1b_2)+I \in {}^{B}\!/_{I}$. Ainda, como $1 \in B$, $1+I \in {}^{B}\!/_{I}$. Logo ${}^{B}\!/_{I}$ é subanel de ${}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}$.

   Seja agora C um subanel de ${}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}$. Como C é subconjunto não vazio de ${}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}$, é da forma $C = \{b+I : b \in B\}$, com $I \subseteq B \subseteq A$; ou seja, $C = {}^{B}\!/_{I}$. Vamos mostrar que B é subanel de $\boldsymbol{A}$. Sejam $b_1, b_2 \in B$. Como ${}^{B}\!/_{I}$ é subanel de ${}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}$, temos que $(b_1+I)-(b_2+I) = (b_1-b_2)+I \in {}^{B}\!/_{I}$ e $(b_1+I)(b_2+I) = (b_1b_2)+I \in {}^{B}\!/_{I}$. Então $b_1 - b_2 \in B$ e $b_1b_2 \in B$. Ainda, como $1+I \in {}^{B}\!/_{I}$, temos que $1 \in B$, e a demonstração está completa.

2. Seja $J \trianglelefteq A$ tal que $I \subseteq J$. Para mostrar que ${}^{J}\!/_{I} \trianglelefteq {}^{A}\!/_{I}$, sejam $j_1+I, j_2+I \in {}^{J}\!/_{I}$ e $a+I \in {}^{A}\!/_{I}$. Como $J \trianglelefteq A$, vale $j_1 - j_2 \in J$ e $aj_1 \in J$. Então $(j_1+I)-(j_2+I) = (j_1-j_2)+I \in {}^{J}\!/_{I}$ e $(a+I)(j_1+I) = (aj_1)+I \in {}^{J}\!/_{I}$.

   Seja $C \trianglelefteq {}^{A}\!/_{I}$. Como C é subconjunto de ${}^{A}\!/_{I}$, é da forma $C = \{j+I : j \in J\}$, com $I \subseteq J \subseteq A$; ou seja, $C = {}^{J}\!/_{I}$. Vamos mostrar que $J \trianglelefteq A$. Sejam $j_1, j_2 \in J$ e $a \in A$. Como ${}^{J}\!/_{I} \trianglelefteq {}^{A}\!/_{I}$, temos que $(j_1+I)-(j_2+I) = (j_1-j_2)+I \in {}^{J}\!/_{I}$ e $(a+I)(j_1+I) = (aj_1)+I \in {}^{J}\!/_{I}$. Então $j_1 - j_2 \in J$ e $aj_1 \in J$, e a demonstração está completa.

■

Teorema 10.31 (Terceiro Teorema de Isomorfismo)**.** *Sejam $\boldsymbol{A}$ um anel, $I \trianglelefteq A$ e $J \trianglelefteq A$ tais que $I \subseteq J$. Então*

$$\left({}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}\right)\Big/\left({}^{\boldsymbol{J}}\!/_{\boldsymbol{I}}\right) \simeq {}^{\boldsymbol{A}}\!/_{\boldsymbol{J}}.$$

Demonstração. Consideremos a função

$$\begin{aligned} \phi : {}^{A}\!/_{I} &\to {}^{A}\!/_{J} \\ a + I &\mapsto a + J. \end{aligned}$$

Primeiro, notemos que ϕ é bem definida, pois, se $a_1 + I = a_2 + I$, então $a_1 - a_2 \in I \subseteq J$, o que implica $a_1 + J = a_2 + J$. Agora, provemos que ϕ é homomorfismo de anéis. Sejam $a_1 + I, a_2 + I \in A/I$. Então

$$\begin{aligned} \phi((a_1 + I) + (a_2 + I)) &= \phi((a_1 + a_2) + I) \\ &= (a_1 + a_2) + J \\ &= (a_1 + J) + (a_2 + J) \\ &= \phi(a_1) + \phi(a_2). \end{aligned}$$

Também, vale que

$$\begin{aligned} \phi((a_1 + I)(a_2 + I)) &= \phi((a_1 a_2) + I) \\ &= (a_1 a_2) + J \\ &= (a_1 + J)(a_2 + J) \\ &= \phi(a_1)\phi(a_2). \end{aligned}$$

Por fim, notamos que $\phi(1 + I) = 1 + J$. Assim, provamos que ϕ é homomorfismo de anéis.

Agora, notemos que

$$\mathcal{N}(\phi) = \{a + I : \phi(a + I) = 0 + J\} = \{a + I : a \in J\} = {}^{J}\!/_{I},$$

o que prova que ${}^{J}\!/_{I} \trianglelefteq {}^{A}\!/_{I}$ e que, portanto, o quociente $\left({}^{A}\!/_{I}\right)\Big/\left({}^{J}\!/_{I}\right)$ pode formar um anel quociente. Notemos também que ϕ é sobrejetiva por construção; ou seja, $\mathfrak{Im}(\phi) = {}^{A}\!/_{J}$. Logo, pelo primeiro teorema de isomorfismo (10.27), temos que

$$\left({}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}\right)\Big/\left({}^{\boldsymbol{J}}\!/_{\boldsymbol{I}}\right) = \left({}^{\boldsymbol{A}}\!/_{\boldsymbol{I}}\right)\Big/\boldsymbol{\mathcal{N}(\phi)} \simeq \boldsymbol{\mathfrak{Im}(\phi)} = {}^{\boldsymbol{A}}\!/_{\boldsymbol{J}}.$$

■

10.7 Ideais Primos e Ideais Maximais

Definição 10.20. Seja $\boldsymbol{A}$ um anel. Um *ideal primo* de $\boldsymbol{A}$ é um ideal $I \trianglelefteq A$ tal que

1. $\forall a, b \in A \qquad ab \in I \Rightarrow a \in I \ \text{ ou } \ b \in I.$

Teorema 10.32. *Seja* $\boldsymbol{A}$ *um anel e* $I \trianglelefteq A$*. Então* I *é um ideal primo de* $\boldsymbol{A}$ *se, e somente se,* $\boldsymbol{A/I}$ *é um domínio.*

Demonstração. Vamos demonstrar as duas implicações ao mesmo tempo. Sejam $a, b \in A$ e $\alpha, \beta \in A/I$ tais que $\alpha = a + I$ e $\beta = b + I$. Note que $\boldsymbol{A/I}$ é um domínio se, e somente se,

$$\forall \alpha, \beta \in A/I \qquad \alpha\beta = 0_{A/I} \Rightarrow \alpha = 0_{A/I} \ \text{ ou } \ \beta = 0_{A/I}.$$

Mas $\alpha\beta = (a + I)(b + I) = ab + I$ e $0_{A/I} = 0 + I$. Ainda, para qualquer $a' \in A$, $a' + I = 0 + I$ se, e somente se, $a' \in I$. Logo segue que a implicação acima é equivalente a

$$\forall a, b \in A \qquad ab = 0 \Rightarrow a = 0 \ \text{ ou } \ b = 0,$$

que é a definição de ideal primo. ■

Definição 10.21. Seja $\boldsymbol{A}$ um anel. Um *ideal maximal* de $\boldsymbol{A}$ é um ideal $I \triangleleft A$ tal que

$$\forall J \in \mathcal{P}(A) \qquad I \subseteq J \ \text{ e } \ J \trianglelefteq A \Rightarrow J = I \ \text{ ou } \ J = A.$$

Teorema 10.33. *Seja* $\boldsymbol{A}$ *um anel e* $I \triangleleft A$*. Então* I *é um ideal maximal de* $\boldsymbol{A}$ *se, e somente se,* $\boldsymbol{A/I}$ *é um corpo.*

Demonstração. Em ambas implicações, usaremos o fato que um anel é um corpo se, e somente se, seus únicos ideais são o anel trivial e o anel todo (10.14).

⇐ Suponha que I é um ideal maximal de $\boldsymbol{A}$. Vamos mostrar que os únicos ideais de $\boldsymbol{A/I}$ são $\{0+I\}$ e A/I. Seja $L \trianglelefteq A/I$ e consideremos a projeção canônica

$$\begin{aligned} \pi : A &\to A/I \\ a &\mapsto a + I. \end{aligned}$$

Sabemos que $\pi^{-1}(L) = \{a \in A : \pi(a) \in L\} \trianglelefteq A$ (10.21). Como $0 + I = 0_{A/I} \in L$, isso implica que $\pi^{-1}(0 + I) \subseteq \pi^{-1}(L)$. Notando que $\pi^{-1}(0 + I) = \mathcal{N}(\phi) = I$, temos que $I \subseteq \pi^{-1}(L) \subseteq A$. Como I é ideal maximal, então $\pi^{-1}(L) = I$ ou $\pi^{-1}(L) = A$. Vamos então avaliar os dois casos. Para isso, ressaltamos antes que $L = \pi(\pi^{-1}(L))$. No primeiro caso, $L = \pi(\pi^{-1}(L)) = \pi(I) = 0+I = 0_{A/I}$. No segundo caso, $L = \pi(\pi^{-1}(L)) = \pi(A) = A/I$. Logo A/I é um corpo.

$\Rightarrow$ Suponha que $\boldsymbol{A}/\boldsymbol{I}$ é um corpo. Consideremos $J \trianglelefteq A$ tal que $I \subseteq J$ e a projeção canônica $\pi : A \to A/I$. Como π é um homomorfismo de anéis bijetivo, temos que $\pi(J) \trianglelefteq A/I$ (10.22). Como $\boldsymbol{A}/\boldsymbol{I}$ é corpo, $\pi(J) = 0_{A/I}$ ou $\pi(J) = A/I$. No primeiro caso, $J = \mathcal{N}(\pi) = I$. No segundo caso, $J = \pi^{-1}(\pi(J)) = \pi^{-1}(A/I) = A$. Logo I é ideal maximal de A.

■

Proposição 10.34. *Seja $\boldsymbol{A}$ um anel e $I \lhd A$ um ideal maximal. Então I é ideal primo.*

Demonstração. A demonstração é simples. Sabemos que, se I é ideal maximal, então A/I é um corpo (10.33). Mas isso implica que A/I é um domínio (10.3). Concluímos, portanto, que I é um ideal primo (10.32). ■

10.8 Domínios Euclidianos

Definição 10.22. Seja $\boldsymbol{D}$ um domínio. Uma *função euclidiana* em $\boldsymbol{D}$ é uma função $\phi : D \setminus \{0\} \to \mathbb{N}$ que satisfaz

1. $\forall a \in D,\ b \in D \setminus \{0\} \quad \exists q, r \in D \qquad a = qb + r \qquad \text{e} \qquad r = 0 \ \text{ ou } \ \phi(r) < \phi(b)$;
2. $\forall a, b \in D \setminus \{0\} \qquad \phi(a) \leq \phi(ab)$.

Nesse caso, q é chamado *quociente* e r é chamado de *resto* da divisão de a por b.

É possível mostrar que a segunda propriedade é desnecessária no seguinte sentido.

Proposição 10.35. *Seja $\boldsymbol{D}$ um domínio e $\phi : D \setminus \{0\} \to \mathbb{N}$ uma função que satisfaz*

1. $\forall a \in D,\ b \in D \setminus \{0\} \quad \exists q, r \in D \qquad a = qb + r \qquad e \qquad r = 0 \ \text{ ou } \ \phi(r) < \phi(b)$.

Então existe uma função euclidiana em $\boldsymbol{D}$.

Demonstração. Seja $\psi : D \setminus \{0\} \to \mathbb{N}$ uma função definida por $\psi(d) = \min\{\phi(dx) : x \in D \setminus \{0\}\}$. Mostraremos que ψ é uma função euclidiana em $\boldsymbol{D}$. Sejam $a \in D, b \in D \setminus \{0\}$. Então existem $q, r \in D$ tais que $a = qb + r$. Se $r \neq 0$, então $\phi(r) < \phi(b)$. Ainda, seja $d \in D \setminus \{0\}$. Como $\boldsymbol{D}$ é domínio, então $db \in D \setminus \{0\}$. Logo existem $q_d, r_d \in D$ tais que $a = q_d db + r_d$. Em particular, $r = r_1$ e $q = q_1$.

Tentar mostrar que, se $r_d = 0$, então $\psi(r) \neq \min\{\phi(rx) : x \in D \setminus \{0\}\}$...
$\psi(r) < \psi(b)$
$\psi(d) \leq \phi(d)$
$\psi(r_d) < \phi(r_d) < \phi(bd)$
$\min\{\phi(rx) : x \in D \setminus \{0\}\} < \min\{\phi(bx) : x \in D \setminus \{0\}\}$
Se $r \neq 0$, então $rd \neq 0$. Isso implica que

Agora, mostremos que ψ satisfaz a segunda propriedade de função euclidiana. Sejam $a, b \in D \setminus \{0\}$ e $d \in D \setminus \{0\}$ tal que $\psi(ab) = \phi(abd)$. Como $\boldsymbol{D}$ é domínio, $bd \in D \setminus \{0\}$, e segue que

$$\psi(a) = \min\{\phi(ax) : x \in D \setminus \{0\}\} \leq \phi(abd).$$

Logo $\psi(a) \leq \psi(ab)$.

■

Proposição 10.36. *Sejam $\boldsymbol{D}$ um domínio, ϕ uma função euclidiana em $\boldsymbol{D}$ e $a, b \in D$.*

Demonstração. ■

Definição 10.23. Um *domínio euclidiano* é um domínio em que existe uma função euclidiana.

Proposição 10.37. *Os anéis $\mathbb{Z}$ e $\mathbb{Z}[i]$ são domínios euclidianos.*

Demonstração. ■

Proposição 10.38. *Seja $\boldsymbol{C}$ um corpo. Então $\boldsymbol{C}[\boldsymbol{x}]$ é um domínio euclidiano.*

Demonstração. ■

Definição 10.24. Um *domínio principal* é um domínio em que todo ideal é principal.

Proposição 10.39. *Seja $\boldsymbol{D}$ um domínio euclidiano. Então $\boldsymbol{D}$ é um domínio principal.*

Demonstração. Seja ϕ uma função euclidiana em $\boldsymbol{D}$ e $I \trianglelefteq D$. Se $I = \{0\}$, então $I = 0I$. Se $I \neq 0$, seja $a \in I \setminus \{0\}$ tal que $\phi(a) = \min\{\phi(i) : a \in I \setminus \{0\}\}$. Tome $b \in I$. Então existem $q, r \in D$ tais que $b = aq + r$. Então $r = aq - b \in I$, pois $a, b \in I$. Se $r \neq 0$, então $\phi(r) < \phi(a)$. Mas isso é absurdo, pois $\phi(a) = \min\{\phi(i) : a \in I \setminus \{0\}\}$. Logo $r = 0$, o que implica $b = aq$; ou seja, $I \subseteq aD$. Como a inclusão inversa sempre vale, então $I = aD$. ■

Proposição 10.40. *Sejam $\boldsymbol{D}$ um domínio eucidiano, ϕ uma função euclidiana em $\boldsymbol{D}$ e $d_1, d_2 \in D \setminus \{0\}$. Então $d_1 \in D^*$ se, e somente se, $\phi(d_2) = \phi(d_1 d_2)$.*

Demonstração. Se $d_1 \in D^*$, então existe $d_1^{-1} \in D$. Assim, temos que $\phi(d_1 d_2) \leq \phi(d_1 d_2 d_1^{-1}) = \phi(d_2)$. Por outro lado, sempre vale $\phi(d_2) \leq \phi(d_1 d_2)$. Logo $\phi(d_1 d_2) = \phi(d_2)$. Por outro lado, suponha $\phi(d_1 d_1) = \phi(d_2)$. Existem $q, r \in D$ tais que $d_2 = d_1 d_2 q + r$. Se $r \neq 0$, então, como $r = d_2 - d_1 d_2 q = d_2(1 - d_1 q)$ e $\boldsymbol{D}$ é domínio, segue que $1 - qa \neq 0$. Logo $\phi(r) = \phi(d_2(1 - d_1 q)) \geq \phi(d_2) = \phi(d_1 d_2)$, contradição. Logo $r = 0$ e temos $d_2 = d_1 d_2 q$. Como $d_2 \neq 0$ e $\boldsymbol{D}$ é domínio, então $d_1 q = 1$, o que implica $d_1 \in D^*$. ■

Proposição 10.41. *Seja $\boldsymbol{D}$ um domínio euclidiano e ϕ uma função eucliana em $\boldsymbol{D}$. Então*

$$D^* = \{d \in D : \phi(d) = \phi(1)\}.$$

Demonstração. Tome $d_2 = 1$ na proposição anterior. ■

10.9 Divisão e Associação em Anéis

10.9.1 Divisão e Associação

Definição 10.25. Seja $\boldsymbol{A}$ um anel. A relação binária $\mid$ em A é definida por

$$\forall a, b \in A \qquad a \mid b \text{ em } \boldsymbol{A} \quad \Leftrightarrow \quad \exists q \in A \quad aq = b.$$

Se $a \mid b$, diz-se que a é um *divisor* de b em $\boldsymbol{A}$ (ou que a *divide* b em $\boldsymbol{A}$) e que b é um *múltiplo* de a em A. Caso contrário, a não é um divisor de b em A e b não é um múltiplo de a em A, e denota-se $a \nmid b$.

Proposição 10.42. *Seja $\boldsymbol{A}$ um anel. A relação binária $\mid$ em A é uma relação reflexiva e transitiva.*

Demonstração. Reflexividade: Seja $a \in A$. Então $a \mid a$, pois $a \cdot 1 = a$.

Transitividade: Sejam $a, b, c \in A$ tais que $a \mid b$ e $b \mid c$. Então existem $q, q' \in A$ tais que $aq = b$ e $bq' = c$. Logo $aqq' = c$. Como $qq' \in A$, segue que $a \mid c$. ■

Proposição 10.43. *Seja $\boldsymbol{A}$ um anel. Então*

1. $\forall a \in A, \forall u \in A^* \qquad u \mid a \mid 0$ *em* $\boldsymbol{A}$;
2. $\forall a \in A, \forall u \in A^* \qquad a \mid u$ *em* $\boldsymbol{A} \Leftrightarrow a \in A^*$;
3. $\forall a \in A \qquad 0 \mid a$ *em* $\boldsymbol{A} \Leftrightarrow a = 0$.

Demonstração. Seja $a \in A$, $u \in A^*$.

1. Como $u \in A^*$, existe $u^{-1} \in A^*$. Então $u \cdot (u^{-1} a) = a$ e segue que $u \mid a$; como $a \cdot 0 = 0$, segue que $a \mid 0$;

2. Se $a \mid u$, existe $q \in A$ tal que $aq = u$. Como $u \in A^*$, segue que $aqu^{-1} = uu^{-1} = 1$. Logo $a \in A^*$. Reciprocamente, se $a \in A^*$, existe a^{-1} tal que $aa^{-1} = 1$. Então $aa^{-1}u = u$ Logo $a \mid u$;

3. Se $0 \mid a$, existe $q \in A$ tal que $0q = a$. Mas então $a = 0$. A recíproca segue da reflexividade de $|$.

■

Proposição 10.44. *Seja $\boldsymbol{A}$ um anel e $a_1, a_2 \in A$. Então $a_1A \subseteq a_2A$ se, e somente se, $a_2 \mid a_1$.*

Demonstração. Se $a_1A \subseteq a_2A$, então $a_1 \in a_2A$. Mas isso significa que existe $q \in A$ tal que $a_1 = a_2q$, o que mostra que $a_2 \mid a_1$. A implicação contrária segue a mesma demonstração com as implicação invertidas. ■

Definição 10.26. Sejam $\boldsymbol{A}$ um anel e $Q \subseteq A$. Um *divisor comum* de Q em $\boldsymbol{A}$ é um elemento $d \in A$ que satisfaz

$$\forall q \in Q \qquad d \mid q \text{ em } \boldsymbol{A}.$$

O conjunto dos divisores comuns de Q em $\boldsymbol{A}$ é $\mathrm{div}_{\boldsymbol{A}}(Q)$. O índice $\boldsymbol{A}$ pode ser omitido caso não haja ambiguidade.

Dualmente, um *múltiplo comum* de Q em $\boldsymbol{A}$ é um elemento $m \in A$ que satisfaz

$$\forall q \in Q \qquad q \mid m \text{ em } \boldsymbol{A}.$$

O conjunto dos múltiplos comuns de Q em $\boldsymbol{A}$ é $\mathrm{mul}_{\boldsymbol{A}}(Q)$. O índice $\boldsymbol{A}$ pode ser omitido caso não haja ambiguidade.

Proposição 10.45. *Sejam $\boldsymbol{A}$ um anel e $Q \subseteq A$. Então*

1. $\mathrm{div}_{\boldsymbol{A}}(A) = \mathrm{div}_{\boldsymbol{A}}(A^*) = A^*$ *e* $\mathrm{div}_{\boldsymbol{A}}(\emptyset) = \mathrm{div}_{\boldsymbol{A}}(\{0\}) = A$;

2. $A^* \subseteq \mathrm{div}_{\boldsymbol{A}}(Q) \subseteq A$;

3. $\{0\} \cap \mathrm{div}_{\boldsymbol{A}}(Q) \neq \emptyset \Leftrightarrow Q \subseteq \{0\} \Leftrightarrow \mathrm{div}_{\boldsymbol{A}}(Q) = A$.

Dualmente,

1. $\mathrm{mul}_{\boldsymbol{A}}(A) = \mathrm{mul}_{\boldsymbol{A}}(\{0\}) = \{0\}$ *e* $\mathrm{mul}_{\boldsymbol{A}}(\emptyset) = \mathrm{mul}_{\boldsymbol{A}}(A^*) = A$;

2. $\{0\} \subseteq \mathrm{mul}_{\boldsymbol{A}}(Q) \subseteq A$;

3. $A^* \cap \mathrm{mul}_{\boldsymbol{A}}(Q) \neq \emptyset \Leftrightarrow Q \subseteq A^* \Leftrightarrow \mathrm{mul}_{\boldsymbol{A}}(Q) = A$.

Demonstração. 1. Seja $u \in A^*$. Então $u \mid a$ para todo $a \in A$. Logo $u \in \operatorname{div}_{\boldsymbol{A}}(A)$. Por outro lado, seja $d \in \operatorname{div}_{\boldsymbol{A}}(A)$. Então $d \mid a$ para todo $a \in A$. Em particular, $d \mid 1$. Como $1 \in A^*$, então $d \in A^*$.

Seja $u \in A^*$. Então $u \mid v$ para todo $v \in A^*$. Logo $u \in \operatorname{div}_{\boldsymbol{A}}(A^*)$. Por outro lado, seja $d \in \operatorname{div}_{\boldsymbol{A}}(A^*)$. Então $d \mid u$ para todo $u \in A^*$. Logo $d \in A^*$.

Seja $a \in A$. Se $a \notin \operatorname{div}_{\boldsymbol{A}}(\emptyset)$, existe $q \in \emptyset$ tal que $a \nmid q$, o que é absurdo. Logo $a \in \operatorname{div}_{\boldsymbol{A}}(\emptyset)$.

Seja $a \in A$. Então $a \mid 0$, o que implica $a \in \operatorname{div}_{\boldsymbol{A}}(\{0\})$. A inclusão contrária é óbvia pela definição do conjunto dos divisores comuns.

2. Se $Q = \emptyset$, então $\operatorname{div}_{\boldsymbol{A}}(Q) = A$. Se $Q \neq \emptyset$, sejam $q \in Q$ e $u \in A^*$. Então $u \mid q$. Logo $u \in \operatorname{div}_{\boldsymbol{A}}(Q)$. A inclusão $\operatorname{div}_{\boldsymbol{A}}(Q) \subseteq A$ é óbvia pela definição do conjunto de divisores comuns;

3. Suponhamos que $\{0\} \cap \operatorname{div}_{\boldsymbol{A}}(Q) \neq \emptyset$. Então $0 \in \operatorname{div}_{\boldsymbol{A}}(Q)$. Se $Q = \emptyset$, então $Q \subseteq \{0\}$. Caso contrário, seja $q \in Q$. Como $0 \mid q$, segue que $q = 0$. Em ambos os casos, $Q \subseteq \{0\}$.

   Suponhamos que $Q \subseteq \{0\}$. Então $Q = \emptyset$ ou $Q = \{0\}$. Pelo item 1, segue que $\operatorname{div}_{\boldsymbol{A}}(Q) = A$.

   Suponhamos que $\operatorname{div}_{\boldsymbol{A}}(Q) = A$. Então $\{0\} \cap \operatorname{div}_{\boldsymbol{A}}(Q) = \{0\} \neq \emptyset$.

Dualmente,

1. Note que $a \mid 0$ para todo $a \in A$. Logo $0 \in \operatorname{mul}_{\boldsymbol{A}}(A)$. Por outro lado, seja $m \in \operatorname{mul}_{\boldsymbol{A}}(A)$. Então $a \mid m$ para todo $a \in A$. Em particular, $0 \mid m$, o que implica $m = 0$.

   Note que $0 \mid 0$, o que implica $0 \in \operatorname{mul} \boldsymbol{A}(\{0\})$. Por outro lado, seja $m \in \operatorname{mul}_{\boldsymbol{A}}(\{0\})$. Então $0 \mid m$, o que implica $m = 0$.

   Seja $a \in A$. Se $a \notin \operatorname{mul}_{\boldsymbol{A}}(\emptyset)$, existe $q \in \emptyset$ tal que $q \nmid a$, o que é absurdo. Logo $a \in \operatorname{mul}_{\boldsymbol{A}}(\emptyset)$.

   Sejam $a \in A$ e $u \in A^*$. Então $u \mid a$, o que implica $a \in \operatorname{mul}_{bmA}(A^*)$. A inclusão contrária é óbvia pela definição do conjunto dos múltiplos comuns.

2. Se $Q = \emptyset$, então $\operatorname{mul}_{\boldsymbol{A}}(Q) = A$. Se $Q \neq \emptyset$, seja $q \in Q$. Então $q \mid 0$, o que implica $\{0\} \in \operatorname{mul}_{\boldsymbol{A}}(Q)$. A inclusão $\operatorname{mul}_{\boldsymbol{A}}(Q) \subseteq A$ é óbvia pela definição do conjunto dos múltiplos comuns;

3. Suponhamos que $A^* \cap \operatorname{mul}_{\boldsymbol{A}}(Q) \neq \emptyset$. Seja $m \in A^* \cap \operatorname{mul} \boldsymbol{A}(Q)$. Se $Q = \emptyset$, então $Q \subseteq A^*$. Caso contrário, seja $q \in Q$. Como $q \mid m$, pois $m \in \operatorname{mul}_{\boldsymbol{A}}(Q)$, então $q \in A^*$, pois $m \in A^*$. Logo $Q \subseteq A^*$.

Suponhamos que $Q \subseteq A^*$. Se $Q = \emptyset$, do item 1 segue que $\mathrm{mul}_{\boldsymbol{A}}(Q) = A$. Caso contrário, sejam $q \in Q$ e $a \in A$. Então $q \in A^*$ e segue que $q \mid a$. Logo $a \in \mathrm{mul}_{\boldsymbol{A}}(Q)$. Por outro lado, a inclusão $\mathrm{mul}_{\boldsymbol{A}}(Q) \subseteq A$ é óbvia pela definição do conjunto de múltiplos comuns;

Suponhamos que $\mathrm{mul}_{\boldsymbol{A}}(Q) = A$. Então $A^* \cap \mathrm{mul}_{\boldsymbol{A}}(Q) = A^*$. Como $1 \in A^*$, segue que $A^* \cap \mathrm{mul}_{\boldsymbol{A}}(Q) \neq \emptyset$.

■

Definição 10.27. Sejam $\boldsymbol{A}$ um anel e $Q \subseteq A$. Um *máximo divisor comum* de Q em $\boldsymbol{A}$ é um elemento $d \in A$ que satisfaz

1. $d \in \mathrm{div}_{\boldsymbol{A}}(Q)$;
2. $d' \in \mathrm{div}_{\boldsymbol{A}}(Q) \Rightarrow d' \mid d$ em $\boldsymbol{A}$.

O conjunto dos máximos divisores comuns de Q em $\boldsymbol{A}$ é $\mathrm{mdc}_{\boldsymbol{A}}(Q)$. Se Q é um conjunto finito $Q = \{a_1, \ldots, a_n\}$, denota-se $\mathrm{mdc}_{\boldsymbol{A}}(Q) = \mathrm{mdc}_{\boldsymbol{A}}(Q)(a_1, \ldots, a_n)$ ou $\mathrm{mdc}_{\boldsymbol{A}}(Q) = (a_1, \ldots, a_n)$. O índice $\boldsymbol{A}$ pode ser omitido caso não haja ambiguidade.

Dualmente, um *mínimo múltiplo comum* de Q em $\boldsymbol{A}$ é um elemento $m \in A$ que satisfaz

1. $m \in \mathrm{mul}_{\boldsymbol{A}}(Q)$;
2. $m' \in \mathrm{mul}_{\boldsymbol{A}}(Q) \Rightarrow m \mid m'$ em $\boldsymbol{A}$.

O conjunto dos mínimos múltiplos comuns de Q em $\boldsymbol{A}$ é $\mathrm{mmc}_{\boldsymbol{A}}(Q)$. Se Q é um conjunto finito $Q = \{a_1, \ldots, a_n\}$, denota-se $\mathrm{mmc}_{\boldsymbol{A}}(Q) = \mathrm{mmc}_{\boldsymbol{A}}(Q)[a_1, \ldots, a_n]$. ou $\mathrm{mmc}_{\boldsymbol{A}}(Q) = [a_1, \ldots, a_n]$ O índice $\boldsymbol{A}$ pode ser omitido caso não haja ambiguidade.

Proposição 10.46. *Seja $\boldsymbol{A}$ um anel e $Q \subseteq A$. Então*

1. $Q \subseteq \{0\} \Leftrightarrow \mathrm{mdc}_{\boldsymbol{A}}(Q) = \{0\}$;
2. $A^* \cap Q \neq \emptyset \Rightarrow \mathrm{mdc}_{\boldsymbol{A}}(Q) = A^*$.

Dualmente,

1. $Q \subseteq A^* \Leftrightarrow \mathrm{mmc}_{\boldsymbol{A}}(Q) = A^*$;
2. $\{0\} \cap Q \neq \emptyset \Rightarrow \mathrm{mmc}_{\boldsymbol{A}}(Q) = \{0\}$.

Demonstração. 1. Suponha que $Q \subseteq \{0\}$. Então $A = \mathrm{div}_{\boldsymbol{A}}(Q)$. Em particular, $0 \in \mathrm{div}_{\boldsymbol{A}}(Q)$. Ainda, para todo $d \in \mathrm{div}_{\boldsymbol{A}}(Q)$, vale que $d \mid 0$, pois $d \in A$. Logo $0 \in \mathrm{mdc}_{\boldsymbol{A}}(Q)$. Ainda, se $d \in \mathrm{mdc}_{\boldsymbol{A}}(Q)$, então $0 \mid d$, pois $0 \in \mathrm{div}_{\boldsymbol{A}}(Q)$ e $d \in \mathrm{mdc}_{\boldsymbol{A}}(Q)$. Portanto $d = 0$. Reciprocamente, se $\mathrm{mdc}_{\boldsymbol{A}}(Q) = \{0\}$, então $0 \in \mathrm{div}_{\boldsymbol{A}}(Q)$; ou seja, $\{0\} \cap \mathrm{div}_{\boldsymbol{A}}(Q) \neq \emptyset$, o que implica que $Q \subseteq \{0\}$.

2. Como $A^* \cap Q \neq \emptyset$, seja $a \in A^* \cap Q$. Se $u \in A^*$, então $u \in \mathrm{div}_{\boldsymbol{A}}(Q)$. Ainda, se $d \in \mathrm{div}_{\boldsymbol{A}}(Q)$, então, em particular, $d \mid a$. Mas como $a \in A^*$, segue que $d \in A^*$. Logo $d \mid u$, o que mostra que $u \in \mathrm{mdc}_{\boldsymbol{A}}(Q)$. Por outro lado, se $d \in \mathrm{mdc}_{\boldsymbol{A}}(Q)$, então $d \mid a$. Como $a \in A^*$, então $d \in A^*$, e concluímos que $A^* = \mathrm{mdc}_{\boldsymbol{A}}(Q)$.

Dualmente,

1. Suponha que $Q \subseteq A^*$. Então $A = \mathrm{mul}_{\boldsymbol{A}}(Q)$. Seja $u \in A^*$. Então $u \in \mathrm{mul}_{\boldsymbol{A}}(Q)$. Ainda, para todo $m \in \mathrm{mul}_{\boldsymbol{A}}(Q)$, vale que $u \mid m$, pois $m \in A$. Logo $u \in \mathrm{mmc}_{\boldsymbol{A}}(Q)$. Ainda, se $m \in \mathrm{mmc}_{\boldsymbol{A}}(Q)$, então $m \mid u$, pois $u \in \mathrm{mul}_{\boldsymbol{A}}(Q)$ e $m \in \mathrm{mmc}_{\boldsymbol{A}}(Q)$. Portanto $m \in A^*$. Reciprocamente, se $\mathrm{mmc}_{\boldsymbol{A}}(Q) = A^*$, então $1 \in \mathrm{mul}_{\boldsymbol{A}}(Q)$; ou seja, $A^* \cap \mathrm{mul}_{\boldsymbol{A}}(Q) \neq \emptyset$, o que implica $Q \subseteq A^*$.

2. Como $\{0\} \cap Q \neq \emptyset$, então $0 \in Q$. Note que $0 \in \mathrm{mul}_{\boldsymbol{A}}(Q)$. Ainda, se $m \in \mathrm{mul}_{\boldsymbol{A}}(Q)$, então $0 \mid m$. Então segue que $0 \in \mathrm{mmc}_{\boldsymbol{A}}(Q)$. Por outro lado, se $m \in \mathrm{mmc}_{\boldsymbol{A}}(Q)$, então $0 \mid m$, o que implica $m = 0$, e concluímos que $\mathrm{mmc}_{\boldsymbol{A}}(Q) = \{0\}$.

■

Proposição 10.47. *Sejam $\boldsymbol{A}$ um anel e B e C conjuntos tais que $C \subseteq B \subseteq A$. Então,* $\mathrm{mdc}_{\boldsymbol{A}}(B) \neq \emptyset$ *e* $\mathrm{mdc}_{\boldsymbol{A}}(C) \neq \emptyset$*,*

$$\mathrm{mdc}_{\boldsymbol{A}}(B) = \mathrm{mdc}_{\boldsymbol{A}}(\mathrm{mdc}_{\boldsymbol{A}}(C) \cup (B \setminus C)).$$

Demonstração. Seja $d \in \mathrm{mdc}_{\boldsymbol{A}}(B)$. Então $d \in \div_{\boldsymbol{A}}(B)$. Seja $x \in \mathrm{mdc}_{\boldsymbol{A}}(C) \cup (B \setminus C)$. Se $x \in B \setminus C$, então $x \in B$, o que implica $d \mid x$. Se $x \in \mathrm{mdc}_{\boldsymbol{A}}(C)$

...

...

...

Então, como $C \subseteq B$, para todo $c \in C$, segue que $c \in B$ e, portanto, $d \mid c$. Ainda, para todo $b \in B \setminus C$, segue que $b \in B$ e, portanto, $d \mid b$.

■

10.9.2 Relação de Associação

Definição 10.28. Seja $\boldsymbol{A}$ um anel. A relação binária $\sim$ (é associado a) em A é definida por

$$\forall a, b \in A \qquad a \sim b \quad \Leftrightarrow \quad \exists u \in A^* \quad au = b.$$

Se $a \sim b$, diz-se que a é *associado* a b em A (ou que a e b são *associados* em $\boldsymbol{A}$). Caso contrário, a não é associado a b.

Proposição 10.48. *Seja $\boldsymbol{A}$ um anel. A relação binária $\sim$ em A é uma relação de equivalência.*

Demonstração. Reflexividade: Seja $a \in A$. Como $1 \in A^*$, segue que $a \cdot 1 = a$ e, portanto, $a \sim a$.

Simetria: Seja $a, b \in A$ tais que $a \sim b$. Então existe $u \in A^*$ tal que $au = b$. Como $u \in A^*$, então $bu^{-1} = a$, o que implica $b \sim a$.

Transitividade: Sejam $a, b, c \in A$ tais que $a \sim b$ e $b \sim c$. Então existem $u, v \in A^*$ tai que $au = b$ e $bv = c$. Assim segue que $auv = c$. Como $uv \in A^*$, conclui-se que $a \sim c$. ■

Proposição 10.49. *Seja $\boldsymbol{A}$ um anel. Então*

1. $\forall a, b \in A \qquad a \sim b \Rightarrow a \mid b$;
2. $\forall a_1, \ldots, a_n, b_1, \ldots, b_n \in A \qquad \forall i \in \mathtt{I}_n \quad a_i \sim b_i \Rightarrow \bigtimes_{i=1}^{n} a_i \sim \bigtimes_{i=1}^{n} b_i$.

Demonstração.

1. Sejam $a, b \in A$. Se $a \sim b$, então existe $u \in A^*$ tal que $au = b$. Mas isso significa que $a \mid b$.
2. Sejam $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ e $i \in \mathtt{I}_n$. Se $a_i \sim b_i$, então existe $u_i \in A^*$ tal que $a_i u_i = b_i$. Logo $a_1 \cdots a_n \cdot u_1 \cdots u_n = b_1 \cdots b_n$. Como $u_1 \cdots u_n \in A^*$, segue que $\bigtimes_{i=1}^{n} a_i \sim \bigtimes_{i=1}^{n} b_i$.

■

Proposição 10.50. *Sejam $\boldsymbol{D}$ um domínio e $d_1, \ldots, d_n \in D$ não todos nulos. Se d, d' são máximos divisores comuns de $d_1, \ldots, d_n$, então d e d' são associados, $d \sim d'$.*

Demonstração. Como d é máximo divisor comum de $d_1, \ldots, d_n$ e d' é divisor comum de $d_1, \ldots, d_n$, então $d' \mid d$. Analogamente, $d \mid d'$. Então existem $u, v \in D$ tais que $d = d'u$ e $d' = dv$. Então $d = dvu$. Como $d \neq 0$ e $\boldsymbol{D}$ é domínio, segue que e $vu = 1$. Portanto $u, v \in D^*$, o que implica $d \sim d'$. ■

10.10 Domínios de Fatoração Única

Definição 10.29. Seja $\boldsymbol{D}$ um domínio. Um elemento *irredutível* em $\boldsymbol{D}$ é um elemento $i \in D$ que satisfaz

1. $i \notin (D^* \cup \{0\})$;
2. $\exists d_1, d_2 \in D \quad i = d_1 d_2 \quad \Rightarrow \quad d_1 \in D^* \text{ ou } d_2 \in D^*$.

Proposição 10.51. *Sejam $\boldsymbol{D}$ um domínio e $u_1, u_2 \in D^*$. Se existe $d \in D$ tal que $u_1 d = u_2$, então $d \in D^*$.*

Demonstração. Como $u_1 \in D^*$, existe u_1^{-1}. Assim, segue que $d = u_1^{-1}u_2$ e, portanto,

$$du_2^{-1}u_1 = u_1^{-1}u_2u_2^{-1}u_1 = u_1^{-1}u_1 = 1.$$

Logo $d \in D^*$. ■

Proposição 10.52. *Sejam $\boldsymbol{D}$ um domínio, $u \in D^*$ e $i \in D$ um elemento irredutível em $\boldsymbol{D}$. Então iu é irredutível em $\boldsymbol{D}$.*

Demonstração. Primeiro, devemos mostrar que $iu \notin (D^* \cup \{0\})$. Como $u \neq 0$ e $i \neq 0$ e $\boldsymbol{D}$ é domínio, então $iu \neq 0$. Supondo que $iu \in D^*$, então existe $v \in D^*$ tal que $(iu)v = 1$. Mas então $uv = i^{-1}$, o que é absurdo, pois $i \notin D^*$. Logo $iu \notin D^*$. Suponha, agora, que existem $d_1, d_2 \in D$ tais que $iu = d_1d_2$. Se $d_1 \notin D^*$ e $d_2 \notin D^*$, então $u^{-1}d_1 \notin D^*$ e $u^{-1}d_1 \neq 0$. Logo segue que $i = (u^{-1}d_1)d_2$, o que é absurdo, pois i é irredutível. ■

Definição 10.30. Seja $\boldsymbol{D}$ um domínio. Um elemento *primo* em $\boldsymbol{D}$ é um elemento $p \in D$ que satisfaz

1. $p \notin (D^* \cup \{0\})$;
2. $\forall d_1, d_2 \in D \qquad p \mid d_1d_2 \Rightarrow p \mid d_1 \text{ ou } p \mid d_2$.

Proposição 10.53. *Sejam $\boldsymbol{D}$ um domínio e p um primo em $\boldsymbol{D}$. Se existem $d_1, \ldots, d_n$ tais que $p \mid d_1 \cdots d_n$, então existe $i \in \{1, \ldots, n\}$ tal que $p \mid d_i$.*

Demonstração. Vamos mostrar por indução em n. Para o caso base, se $n = 1$, então $i = 1$ satisfaz o procurado. Para demonstrar o passo indutivo, suponhamos que a propridade vale para um natural n. Então, se $p = d_1 \cdots d_{n+1}$, como p é primo, $p \mid d_1 \cdots d_n$ ou $p \mid d_{n+1}$. Se $p \mid d_1 \cdots d_n$, pela hipótese de indução, existe $i \in \{1, \ldots, n\}$ tal que $p \mid d_i$; caso contrário, $p \mid d_{n+1}$, Logo, existe $i \in \{1, \ldots, n+1\}$ tal que $p \mid d_i$. ■

Proposição 10.54. *Seja $\boldsymbol{D}$ um domínio. Se p é primo em $\boldsymbol{D}$, então p é irredutível em $\boldsymbol{D}$.*

Demonstração. Seja p primo em $\boldsymbol{D}$. Se existem $d_1, d_2 \in D$ tais que $p = d_1d_2$, então $p \mid d_1d_2$. Como p é primo, então $p \mid d_1$ ou $p \mid d_2$. Se $p \mid d_1$, então existe $q \in D$ tal que $pq = d_1$. Assim, segue que $p = d_1d_2 = pqd_2$ e, como $\boldsymbol{D}$ é domínio, $1 = qd_2$. Logo $d_2 \in D^*$. Analogamente, se $p \mid d_2$, segue que $d_1 \in D^*$. Portanto p é irredutível. ■

Proposição 10.55. *Seja $\boldsymbol{D}$ um domínio euclidiano que não é um corpo e ϕ uma função euclidiana em $\boldsymbol{D}$. Então $d_0 \in D$ tal que*

$$\phi(d_0) = \min\{\phi(d) : d \in D \setminus (D^* \cup \{0\})\}$$

é um elemento irredutível em $\boldsymbol{D}$.

Demonstração. Primeiro, definamos $m \coloneqq \min\{\phi(d) : d \in D\setminus(D^*\cup\{0\})\}$ e notemos que existe tal mínimo porque o conjunto dos naturais é bem ordenado. Notemos que $d_0 \notin D^* \cup \{0\}$ por definição. Suponha que $d_0 = d_1 d_2$, com $d_1, d_2 \in D$. Como D é um domínio, então $d_1 \neq 0$ e $d_2 \neq 0$. Suponha que $d_1, d_2 \notin D^*$. Então $\phi(d_1) \geq m = \phi(d_1 d_2) \geq \phi(d_1)$ e $\phi(d_2) \geq m = \phi(d_1 d_2) \geq \phi(d_2)$. Logo $\phi(d_1) = \phi(d_1 d_2)$ e $\phi(d_2) = \phi(d_1 d_2)$, o que implica $d_1, d_2 \in D^*$, que é absurdo. ■

NOTA: Tentar mostrar a recíproca.

Definição 10.31. Um *domínio de fatoração única* é um domínio $\boldsymbol{D}$ que satisfaz

1. (Existência de Fatoração) Para todo $d \in D \setminus (D^* \cup \{0\})$, existem $p_1, \ldots, p_n$ irredutíveis em $\boldsymbol{D}$ tais que
$$d = \bigtimes_{i=1}^{n} p_i;$$
2. (Unicidade de Fatoração) Para todo $d \in D \setminus (D^* \cup \{0\})$, se existem $p_1, \ldots, p_n$ e $q_1, \ldots, q_m$ irredutíveis em $\boldsymbol{D}$ tais que
$$d = \bigtimes_{i=1}^{n} p_i = \bigtimes_{i=1}^{m} q_i,$$
então $m = n$ e existe uma permutação ϕ de $\mathtt{I}_n$ tal que, para todo $i \in \mathtt{I}_n$, $p_i \sim q_{\phi(i)}$ em $\boldsymbol{D}$.

Domínios de fatoração única também são chamados de domínios fatoriais.

Proposição 10.56. *A função $\phi_k : \mathtt{I}_{m-1} \to \mathtt{I}_m$, definida por*

$$\phi_k(i) \coloneqq \begin{cases} i & 1 \leq i \leq k-1 \\ i+1 & k \leq i \leq m-1, \end{cases}$$

é uma função injetiva e $k \notin \mathfrak{Im}(\phi_k)$.

Demonstração. Para mostrar que ϕ_k é , sejam $i, j \in \mathtt{I}_m$, tais que $i = j$. Se $\phi(i) = i$ e $\phi(j) = j$, então $\phi(i) = \phi(j)$. Se $\phi(i) = i + 1$ e $\phi(j) = j + 1$, então $\phi(i) = \phi(j)$. Se $\phi(i) = i$ e $\phi(j) = j + 1$, então $1 \leq i \leq k - 1$ e $k \leq j \leq m - 1$, absurdo. Se $\phi(i) = i + 1$ e $\phi(j) = j$, então $1 \leq j \leq k - 1$ e $k \leq i \leq m - 1$, absurdo. Ainda, é fácil notar que $k \notin \mathfrak{Im}(\phi_k)$, pois, se $1 \leq i \leq k - 1$, então $1 \leq \phi(i) \leq k - 1$ e, se $k \leq i \leq m - 1$, então $k + 1 \leq \phi(i) \leq m$. ■

Teorema 10.57. *Seja $\boldsymbol{D}$ um domínio. Então $\boldsymbol{D}$ é um domínio de fatoração única se, e somente se, satisfaz*

1. *Para todo $d \in D \setminus (D^* \cup \{0\})$, existem $p_1, \ldots, p_n \in D$ irredutíveis em $\boldsymbol{D}$ tais que*
$$d = \bigtimes_{i=1}^{n} p_i;$$
2. *Se p é irredutível em $\boldsymbol{D}$, então p é primo em $\boldsymbol{D}$.*

Demonstração. Nota-se que a primeira propriedade do enunciado é a mesma da definição de domínio de fatoração única. Basta, portanto, que assumamos essa propriedade e mostremos que as segundas propriedades são equivalentes.

Suponhamos, primeiro, que $\boldsymbol{D}$ é domínio de fatoração única. Sejam p irredutível em $\boldsymbol{D}$ e $d_1, d_2 \in D$ tais que $p \mid d_1 d_2$. Então existe $q \in D$ tal que $pq = d_1 d_2$. Se $d_1 \in D^*$, então $pqd_1^{-1} = d_2$, o que implica $p \mid d_2$. Analogamente, se $d_2 \in D^*$, então $p \mid d_1$. Se $d_1 = 0$, então $p \mid d_1$. Se $d_2 = 0$, então $p \mid d_2$. Caso $d_1, d_2 \notin (D^* \cup \{0\})$, então, como $\boldsymbol{D}$ é domínio de fatoração única, existem $p_1, \ldots, p_n$ e $q_1, \ldots, q_m$ irredutíveis em $\boldsymbol{D}$ tais que

$$d_1 = \bigtimes_{i=1}^{n} p_i \quad \text{e} \quad d_2 = \bigtimes_{i=1}^{m} q_i.$$

Então

$$pq = \left(\bigtimes_{i=1}^{n} p_i \right) \left(\bigtimes_{i=1}^{m} q_i \right).$$

Se $q \in D^*$, então pq é irredutível, pois p é irredutível. Então pq pode ser escrito como produto de 1 irredutível e como produto de $n + m$ irredutíveis, o que é absurdo, pois $n+m \geq 2$. Logo $q \notin D^*$. Se $q = 0$, então $0 = pq = d_1 d_2$. Mas $d_1 \neq 0$ e $d_2 \neq 0$, o que é absurdo, pois $\boldsymbol{D}$ é domínio. Portanto $q \in D \setminus (D^* \cup \{0\})$. Como $\boldsymbol{D}$ é domínio de fatoração única, existem $r_1, \ldots, r_l$ irredutíveis em $\boldsymbol{D}$ tais que

$$q = \bigtimes_{i=1}^{l} r_i.$$

Então

$$p \left(\bigtimes_{i=1}^{l} r_i \right) = \left(\bigtimes_{i=1}^{n} p_i \right) \left(\bigtimes_{i=1}^{m} q_i \right).$$

Como $\boldsymbol{D}$ é domínio de fatoração única, então existe $i \in \mathtt{I}_n$ tal que $p \sim p_i$ em $\boldsymbol{D}$ ou existe $j \in \mathtt{I}_m$ tal que $p \sim q_j$ em $\boldsymbol{D}$. Então $p \mid p_i$ ou $p \mid q_j$. No primeiro caso, como $p_i \mid d_1$, da transitividade de $\mid$ segue que $p \mid d_1$. No segundo caso, como $q_j \mid d_2$, da transitividade de $\mid$ segue que $p \mid d_2$.

Suponhamos agora que $\boldsymbol{D}$ satisfaz a segunda propriedade do enunciado. Sejam $d \in D \setminus (D^* \cup \{0\})$ e $p_1, \ldots, p_n$ e $q_1, \ldots, q_m$ irredutíveis em $\boldsymbol{D}$ tais que

$$d = \bigtimes_{i=1}^{n} p_i = \bigtimes_{i=1}^{m} q_i.$$

Pela segunda propriedade do enunciado, $p_1, \ldots, p_n$ e $q_1, \ldots, q_m$ são primos em $\boldsymbol{D}$. Demonstraremos a segunda propriedade de domínios de fatoração única por indução em $l \coloneqq \min\{n, m\}$. Para o caso base, se $l = 1$, então $n = 1$ ou $m = 1$; sem perda de generalidade, tomemos $n = 1$. Nesse caso, $d = p_1 = q_1 \cdots q_m$. Como $p_1 \mid d$, então existe $k \in \mathtt{I}_m$ tal que $p_1 \mid q_k$, pois p_1 é primo. Portanto existe $r \in D$ tal que $p_1 r = q_k$. Então

$$p_1 = \left(\bigtimes_{i=1}^{k-1} q_i\right) p_1 r \left(\bigtimes_{i=k+1}^{m} q_i\right).$$

Como $\boldsymbol{D}$ é domínio e $p_1 \neq 0$, então

$$1 = \left(\bigtimes_{i=1}^{k-1} q_i\right) r \left(\bigtimes_{i=k+1}^{m} q_i\right).$$

Como p_n e q_k são irredutíveis, então $r \in D^*$. Suponhamos $m > 1$. Então existe q_2. Se $k = 1$, rq_2 é irredutível, pois q_2 é irredutível e $r \in D^*$; caso contrário, se $k > 1$, então $q_{k-1} r$ é irredutível pelo mesmo motivo. Em ambos os casos, 1 é um produto de irredutíveis, o que é absurdo, pois 1 é invertível. Logo $m = 1$, o que demonstra o caso base da indução.

Agora, seja $l > 1$ e suponhamos que a propriedade vale para todo natural $k < l$. Como $p_n \mid d$, então existe $k \in \mathtt{I}_m$ tal que $p_n \mid q_k$, pois p_n é primo. Portanto existe $r \in D$ tal que $p_n r = q_k$. Então

$$\left(\bigtimes_{i=1}^{n-1} p_i\right) p_n = \left(\bigtimes_{i=1}^{k-1} q_i\right) p_n r \left(\bigtimes_{i=k+1}^{m} q_i\right).$$

Como $\boldsymbol{D}$ é domínio e $p_n \neq 0$, então

$$\bigtimes_{i=1}^{n-1} p_i = \left(\bigtimes_{i=1}^{k-1} q_i\right) r \left(\bigtimes_{i=k+1}^{m} q_i\right) = r \left(\bigtimes_{i=1}^{k-1} q_i\right) \left(\bigtimes_{i=k+1}^{m} q_i\right).$$

Como p_n e q_k são irredutíveis, então $r \in D^*$. Como $l > 1$, segue que $n > 1$ e $m > 1$. Então existe q_2. Consideremos a função $\phi_k : \mathtt{I}_{m-1} \to \mathtt{I}_m$, definida por

$$\phi_k(i) \coloneqq \begin{cases} i & 1 \leq i \leq k-1 \\ i+1 & k \leq i \leq m-1. \end{cases}$$

Os casos especiais são $\phi_1(i) = i + 1$ e $\phi_m(i) = i$. Notemos que ϕ_k é injetiva para todo $k \in \mathtt{I}_m$ e que $k \notin \mathfrak{Im}(\phi_k)$.

Notemos que rq_2 é irredutível, pois q_2 é irredutível e $r \in D^*$. Definamos

$$q'_i \coloneqq \begin{cases} rq_{\phi_1(i)} & i = 1 \\ q_{\phi_1(i)} & 2 \leq i \leq m-1. \end{cases}$$

Caso contrário, se $k > 1$, $q_{k-1}r$ é irredutível pelo mesmo motivo, e definamos

$$q'_i \coloneqq \begin{cases} q_{\phi_k(i)} & 1 \leq i \leq k-2 \ \text{ ou } \ k \leq i \leq m-1 \\ q_{_{\phi_k(i)}}r & i = k-1 \end{cases}$$

Em ambos os casos, o lado direito da equação acima é um produto de $m-1$ termos irredutíveis e o lado esquerdo é um produto de $n-1$

$$\bigtimes_{i=1}^{n-1} p_i = \bigtimes_{i=1}^{m-1} q'_i.$$

Logo, como $\min\{n-1, m-1\} = l - 1 < l$, vale a hipótese de indução e então, $n-1 = m-1$ e existe permutação ϕ' de $\mathtt{I}_{n-1}$ tal que, para todo $i \in \mathtt{I}_{n-1}$, $p_i \sim q'_{\phi'(i)}$ em $\boldsymbol{D}$. Então segue que $n = m$. Portanto, podemos criar a permutação ϕ de $\mathtt{I}_n$, definida por

$$\phi(i) \coloneqq \begin{cases} (\phi_k \circ \phi')(i) & 1 \leq i < n-1 \\ k & i = n. \end{cases}$$

Por fim, mostremos que ϕ é uma permutação de $\mathtt{I}_n$ e que, para todo $i \in \mathtt{I}_n$, $p_i \sim q_{\phi(i)}$ em $\boldsymbol{D}$. Primeiro, mostremos que ϕ é injetiva. Para isso, notemos que, como ϕ' é injetiva, ϕ_k é injetiva e $k \notin \mathfrak{Im}(\phi_k)$, então $(\phi_k \circ \phi')|_{\mathtt{I}_{n-1}}$ é injetiva e, então, segue que ϕ é injetiva, pois $\phi(n) = k$. Agora, para mostrar que ϕ é sobrejetiva, seja $j \in \mathtt{I}_n$ e notemos que, como ϕ_k é injetiva e $k \notin \mathfrak{Im}(\phi_k)$, então, se $1 \leq j \leq k-1$ ou $k+1 \leq j \leq m$, existe $i \in \mathtt{I}_{n-1}$ tal que $\phi(i) = j$; e, se $j = k$, então $\phi(n) = k$. Logo ϕ é sobrejetiva e concluímos que ϕ é uma permutação de $\mathtt{I}_n$.

Agora, seja $i \in \mathtt{I}_n$. Se $i = n$, então $\phi(i) = k$. Por construção, $p_n \sim q_k = q_{\phi(n)}$. Se $1 \leq i \leq n-1$, então $p_i \sim q'_{\phi'(i)}$. Se $k = 1$, separamos em dois casos. Primeiro, se $\phi'(i) = 1$, então $p_i \sim q'_{\phi'(i)}$. Mas $q'_{\phi'(i)} = q'_1$ e, como $r \in D^*$, temos que $q'_1 = rq_2$ implica $q'_1 \sim q_2$. Pela transitividade de $\sim$, segue que $p_i \sim q_2$ e, notando que $\phi_1(\phi'(i)) = \phi_1(1) = 2$, segue que $p_i \sim q_{\phi(i)}$. No segundo caso, se $2 \leq \phi'(i) \leq n-1$, então $p_i \sim q'_{\phi'(i)} \sim q_{\phi_1(\phi'(i))}$, pois $\sim$ é transitiva, e segue que $p_i \sim q_{\phi(i)}$. Agora, consideremos $k > 1$. Se paramos em dois casos, novamente. Se $\phi'(i) = k-1$, então $q'_{\phi'(i)} = q_{\phi_k(\phi'(i))}r$ e, como $r \in D^*$, segue que $q'_{\phi'(i)} \sim q_{\phi_k(\phi'(i))} = q_{\phi(i)}$. Mas $p_i \sim q'_{\phi'(i)}$ e segue, da transitividade de $\sim$, que $p_i \sim q_{\phi(i)}$. No outro caso, se $1 \leq \phi'(i) \leq k-2$ ou $k \leq \phi'(i) \leq m-1$, então $q'_{\phi'(i)} = q_{\phi_k(\phi'(i))} = q_{\phi(i)}$ e segue, da transitividade de $\sim$, que $p_i \sim q_{\phi(i)}$, e está provado o teorema. ■

Proposição 10.58. *Seja $\boldsymbol{D}$ um domínio de fatoração única. Então*

1. *(Existência de Fatoração Reduzida) Para todo $d \in D \setminus (D^* \cup \{0\})$, existem $p_1, \ldots, p_n$ irredutíveis em $\boldsymbol{D}$, $u \in D^*$ e $\alpha_1, \ldots, \alpha_n \in \mathbb{N}^*$ tais que*

$$d = u \bigtimes_{k=1}^{n} p_k^{\alpha_k}$$

   e, para todos $i, j \in \mathtt{I}_n$, $i \neq j$ implica que $p_i \not\sim p_j$ em $\boldsymbol{D}$.

2. *(Unicidade de Fatoração Reduzida) Para todo $d \in D \setminus (D^* \cup \{0\})$, se existem $p_1, \ldots, p_n$ e $q_1, \ldots, q_m$ irredutíveis em $\boldsymbol{D}$, $u, v \in D^*$ e $\alpha_1, \ldots, \alpha_n \in \mathbb{N}^*$ e $\beta_1, \ldots, \beta_m \in \mathbb{N}^*$ tais que*

$$d = u \bigtimes_{k=1}^{n} p_k^{\alpha_k} = v \bigtimes_{k=1}^{m} q_k^{\beta_k},$$

   e, para todos $i, j \in \mathtt{I}_n$, $i \neq j$ implica que $p_i \not\sim p_j$ em $\boldsymbol{D}$ e que $q_i \not\sim q_j$ em $\boldsymbol{D}$, então $m = n$ e existe permutação ϕ de $\mathtt{I}_n$ tal que, para todo $i \in \mathtt{I}_n$, $q_{\phi(i)}$ e p_i são associados em $\boldsymbol{D}$ e $\alpha_i = \beta_{\phi(i)}$.

Demonstração. Seja $d \in D \setminus (D^* \cup \{0\})$. Então existem $p'_1, \cdots, p'_m$ irredutíveis em $\boldsymbol{D}$ tais que

$$d = \bigtimes_{i=1}^{m} p'_i.$$

Vamos considerar os conjuntos $I_i \coloneqq \{j \in \mathtt{I}_m : p'_j \sim p'_i\}$ dos índices de elementos da fatoração de d que são associados. Esses conjuntos são uma partição de $\mathtt{I}_m$; ou seja, $P \coloneqq \{I_i : i \in \mathtt{I}_m\}$ é uma partição de $\mathtt{I}_m$. Para mostrar isso, seja $n \coloneqq |P|$ e sejam $P_1, \ldots, P_n$ os elementos de P. Primeiro, notemos que $\emptyset \notin P$ por definição. Segundo, notemos que

$$\bigcup_{j \in \mathtt{I}_n} P_j = \mathtt{I}_m$$

pois, para todo $j \in \mathtt{I}_m$, existe $k \in \mathtt{I}_n$ tal que $I_j = P_k$ e, como $j \in I_j$, isso implica que $j \in \bigcup_{i \in \mathtt{I}_n} P_i$. Terceiro, sejam $j, k \in \mathtt{I}_n$; se $P_j \cap P_k \neq \emptyset$, então seja $i \in P_j \cap P_k$; logo, para todos $i_j \in P_j, i_k \in P_k$, segue que $i_j \sim i \sim i_k$, o que implica $P_j = P_k$. Portanto podemos escrever

$$d = \bigtimes_{i=1}^{m} p'_i = \bigtimes_{k=1}^{n} \bigtimes_{i \in P_k} p'_i.$$

Sendo assim, seja $k \in \mathtt{I}_n$ e definamos $p_k \coloneqq p'_{\min(P_k)}$ e $\alpha_k \coloneqq |P_k|$. Segue claramente que p_k é irredutível em $\boldsymbol{D}$ e que $\alpha_k \in \mathbb{N}^*$. Como, para todo $i \in P_k$,

vale $p'_i \sim p_k$, então existe $u'_i \in A^*$ tal que $p'_i = u'_i p_k$. Assim, definindo $u_k \coloneqq \bigtimes_{i \in P_k} u'_i$, temos que $u_k \in A^*$ e

$$\bigtimes_{i \in P_k} p'_i = \bigtimes_{i \in P_k} u'_i p_k = \left(\bigtimes_{i \in P_k} u'_i \right) p_k^{\alpha_k} = u_k p_k^{\alpha_k}.$$

Assim, segue que

$$d = \bigtimes_{k=1}^{n} \bigtimes_{i \in P_k} p'_i = \bigtimes_{k=1}^{n} u_k p_k^{\alpha_k}.$$

Definindo $u \coloneqq \bigtimes_{k=1}^{n} u_k$, temos que $u \in A^*$ e segue a existência da fatoração reduzida

$$d = \left(\bigtimes_{k=1}^{n} u_k \right) \left(\bigtimes_{k=1}^{n} p_k^{\alpha_k} \right) = u \bigtimes_{k=1}^{n} p_k^{\alpha_k}.$$

Devemos, então, mostrar a UNICIDADE... ■

NOTA: O teorema seguinte vale para um número finito de valores.

Teorema 10.59. *Seja $\boldsymbol{D}$ um domínio de fatoração única. Então, para todo $a, b \in D \setminus \{0\}$, existe $d \in \mathrm{mdc}_{\boldsymbol{D}}(a, b)$.*

Demonstração. Se $\{a, b\} \cap D^* \neq \emptyset$, então $\mathrm{mdc}_{\boldsymbol{D}}(a, b) = D^*$. Suponhamos, então, que $\{a, b\} \notin D \setminus (D^* \cup \{0\})$. Como $\boldsymbol{D}$ é domínio de fatoração única, existem $p_1, \ldots, p_n$ e $q_1, \ldots, q_m$ irredutíveis em $\boldsymbol{D}$ tais que $a = p_1 \cdots p_n$ e $b = q_1 \cdots q_m$. Seja k o número de fatores p_i e q_j associados, e suponhamos, sem perda de generalidade, que, para todo $i \leq k$, $p_i \sim q_i$ e, para todo $i \geq k+1$ e $j \geq k+1$, $p_i \not\sim q_j$.

Se $k = 0$, mostraremos que $\mathrm{mdc}_{\boldsymbol{D}}(a, b) = D^*$. Para isso, mostraremos que $1 \in \mathrm{mdc}_{\boldsymbol{D}}(a, b)$. Notamos que $1 \in D^* \subseteq \mathrm{div}_{\boldsymbol{D}}(a, b)$. Agora, seja $d \in \mathrm{div}_{\boldsymbol{A}}(a, b)$. Como $\{a, b\} \cap \{0\} = \emptyset$, então $\{0\} \cap \mathrm{div}_{\boldsymbol{D}}(a, b) = \emptyset$. Se $d \in D^*$, então $d \mid 1$, logo $1 \in \mathrm{mdc}_{\boldsymbol{D}}(a, b)$. Se $d \in D \setminus (D^* \cup \{0\})$, então existe p irredutível em $\boldsymbol{D}$ tal que $p \mid d$. Pela transitividade de $\mid$, $p \mid a$ e $p \mid b$. Como $\boldsymbol{D}$ é domínio de fatoração única, p é primo em $\boldsymbol{D}$. Então segue que existe i e j tais que $p \mid p_i$ e $p \mid q_j$. Como esses elementoss são irredutíveis, $p \sim p_i$ e $p \sim q_j$. Da transitividade e reflexividade de $\sim$, segue que $p_i \sim q_j$, o que é absurdo. Logo $1 \in \mathrm{mdc}_{\boldsymbol{D}}(a, b)$. Como todos os máximos divisores comuns são associados, então $D^* = \mathrm{mdc}_{\boldsymbol{D}}(a, b)$.

Se $k \geq 1$, mostraremos que $p_1 \cdots p_k \in \mathrm{mdc}_{\boldsymbol{D}}(a, b)$. Primeiro, notamos que $p_1 \cdots p_k \mid a$ e $q_1 \cdots q_k \mid b$. Como $p_i \sim q_i$ para todo $i \leq k$, então $p_1 \cdots p_k \sim q_1 \cdots q_k$. Logo $p_1 \cdots p_k \mid q_1 \cdots q_k$ e, da trasitividade de $\mid$, segue que $p_1 \cdots p_k \mid b$. Logo $p_1 \cdots p_k \in \mathrm{div}_{\boldsymbol{D}}(a, b)$. Então, seja $d \in \mathrm{div}_{\boldsymbol{D}}(a, b)$. Se $d \in D^*$, então $d \mid p_1 \cdots p_k$.

Logo $p_1 \cdots p_k \in \mathrm{mdc}_{\boldsymbol{D}}(a,b)$. Se $d \in D \setminus (D^* \cup \{0\})$, então existem $r_1, \ldots, r_l$ irredutíveis em $\boldsymbol{D}$ tais que $d = r_1 \cdots r_l$. Por $\boldsymbol{D}$ ser domínio, $r_1, \ldots, r_l$ são primos em $\boldsymbol{D}$. Como $d \mid a$, então $r_1 \mid p_1 \cdots p_k$. Como r_1 é primo, existe $i_1 \in \{1, \ldots, k\}$ tal que $r_1 \mid p_{i_1}$. Seja $s_1 \in D$ tal que $r_1 s_1 = p_{i_1}$. Como r_1 e p_{i_1} são irredutíveis, então $r_1 \sim p_{i_1}$, o que implica $s_1 \in D^*$. Então $r_2 \cdots r_l \mid p_1 \cdots p_{i_1 - 1} \cdot s_1 \cdot p_{i_1+1} \cdots p_k$, pois $\boldsymbol{D}$ é domínio. Repetindo o processo indutivamente, conclui-se que existem $i_1, \ldots, i_m$ tais que $r_j \sim p_{i_j}$ para todo $j \in \{1, \ldots, l\}$ (MELHORAR ARUMENTAÇÃO DA INDUÇÃO). Da mesma forma, cocnlui-se que que existem $i'_1, \ldots, i'_m$ tais que $r_j \sim q_{i'_j}$ para todo $j \in \{1, \ldots, l\}$. Portanto, da reflexividade e transitividade de $\sim$, segue que $p_{i_j} \sim q_{i'_j}$ para todo i, j. Então $d \sim p_{i_1} \cdots p_{i_m} \sim q_{i'_1} \cdots q_{i'_m}$. Como $p_{i_1} \cdots p_{i_m} \mid p_1 \cdots p_k$ e $q_{i'_1} \cdots q_{i'_m} \mid q_1 \cdots q_k$, então $d \mid p_1 \cdots p_k$(MELHORAR ARGUMENTAÇÃO FINAL). ■

Lema 10.60. *Seja $\boldsymbol{D}$ um domínio.*

10.11 Raízes de Polinômios

Proposição 10.61. *Seja $\boldsymbol{A}$ um anel e $f, g \in A[x]$. Se g é mônico, então existem $q, r \in A[x]$ tais que $f = qg + r$ e $r = 0$ ou $\mathrm{grau}(r) < \mathrm{grau}(g)$.*

Demonstração. Sejam $n \coloneqq \mathrm{grau}(f)$, $f = \bigplus_{i=0}^{n} a_i x^i$, e $m \coloneqq \mathrm{grau}(g)$, $g = \bigplus_{i=0}^{m-1} b_i x^i + x^m$. Se $m \leq n$, definimos $q(x) \coloneqq a_n x^{n-m}$ e $r \coloneqq f - qg$ e temos

$$\begin{aligned} r(x) &= f(x) - q(x)g(x) \\ &= \bigplus_{i=0}^{n} a_i x^i - a_n x^{n-m} \left(\bigplus_{i=0}^{m-1} b_i x^i + x^m \right) \\ &= \bigplus_{i=0}^{n} a_i x^i - \left(\bigplus_{i=0}^{m-1} a_n b_i x^{n-m+i} + a_n x^n \right) \\ &= \bigplus_{i=0}^{n-1} a_i x^i - \bigplus_{i=n-m}^{n-1} a_n b_{i-n+m} x^i \\ &= \bigplus_{i=0}^{n-m-1} a_i x^i + \bigplus_{i=n-m}^{n-1} (a_i - a_n b_{i-n+m}) x^i. \end{aligned}$$

Daí, segue que, se $r \neq 0$, $\mathrm{grau}(r) \leq n - 1 < m \leq \mathrm{grau}(g)$.

... TERMINAR, USEI ISSO NUMA DEMONSTRAÇÃOMAIS A FRENTE, TENHO QUE DEMMONSTRAR. ■

Definição 10.32. Sejam $\boldsymbol{A}$ um anel, $p = \bigplus_{i=0}^{n} a_i x^i \in A[x]$ e $a \in A$. O *valor* de p em a é o elemento

$$p(a) \coloneqq \bigplus_{i=0}^{n} a_i a^i \in A.$$

Definição 10.33. Sejam $\boldsymbol{A}$ um anel e $p \in A[x]^* = A[x] \setminus A$. Uma *raiz* de p é um elemento $r \in A$ tal que $p(r) = 0$.

Proposição 10.62. *Sejam $\boldsymbol{A}$ um anel, $p \in A[x]^*$ e $r \in A$. Então r é raiz de p se, e somente se, existe $q \in A[x]$ tal que $p(x) = (x - r)q(x)$.*

Demonstração. Primeiro, notemos que, se existe $q \in A[x]$ tal que $p(x) = (x - r)q(x)$, então $p(r) = (r - r)q(r) = 0q(r) = 0$. Reciprocamente, suponhamos que r é raiz de p.

... ■

Capítulo 11

Corpos

11.1 Extensões de Corpos

Definição 11.1. Seja $\boldsymbol{C}$ um corpo. Uma *extensão* de $\boldsymbol{C}$ é um corpo $\boldsymbol{E}$ tal que $\boldsymbol{C}$ é um subcorpo de $\boldsymbol{E}$.

Proposição 11.1. *Sejam $\boldsymbol{C}$ um corpo e $\boldsymbol{E} = (E, +, \cdot)$ uma extensão de $\boldsymbol{C}$. Então $(E, \oplus, \odot)$ é um espaço vetorial sobre $\boldsymbol{C}$, em que $\oplus \coloneqq +$ e $\odot \coloneqq \cdot|_{C \times E}$.*

Demonstração. Como $\boldsymbol{E}$ é um anel, então $(E, \oplus) = (E, +)$ é um grupo comutativo com elemento neutro 0 do corpo. Agora, como $\odot$ é a restrição de $\cdot$ a $C \times E$, então, para todo $e \in E$, $1 \odot e = 1e = e$ e, para todos $c_1, c_2 \in C$, $(c_1 \cdot c_2) \odot e = c_1 c_2 e = c_1 \odot (c_2 \odot e)$. Por fim, como $\cdot$ é distributiva sobre $+$, segue que, para todos $c \in C$ e $e_1, e_2 \in E$, $c \odot (e_1 \oplus e_2) = c(e_1 + e_2) = ce_1 + ce_2 = c \odot e_1 \oplus c \odot e_2$ e, para todos $c_1, c_2 \in C$ e $e \in E$, $(c_1 + c_2) \odot e = (c_1 + c_2)e = c_1 e + c_2 e = c_1 odote \oplus c_2 \odot e$. Por tanto, concluímos que $(E, \oplus, \odot)$ é um espaço vetorial sobre $\boldsymbol{C}$. ■

Notação. Nesse caso, quando não houver ambiguidade, denotaremos $\oplus$ como $+$ e $\odot$ como $\cdot$, bem como todas outras notações relacionadas às operações do espaço veorial.

Definição 11.2. Sejam $\boldsymbol{C}$ um corpo e $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$. Então a *dimensão* da extensão $\boldsymbol{E}$ com respeito a $\boldsymbol{C}$ é a dimensão do espaço vetorial $\boldsymbol{E}$ sobre $\boldsymbol{C}$. A extensão $\boldsymbol{E}$ é *finita* de sua dimensão é finita e *infitina* se sua dimensão é infinita.

Definição 11.3. Sejam $\boldsymbol{C}$ um corpo e $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$. Um *elemento algébrico* sobre $\boldsymbol{C}$ é um elemento $\alpha \in E$ que é raiz de um polinômio em $C[x]^*$.

Proposição 11.2. *Sejam $\boldsymbol{C}$ um corpo e $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$. Então*

1. *Todo elemento de C é algébrico sobre $\boldsymbol{C}$;*

2. *Se $\alpha \in E \backslash \{0\}$ é um elemento algébrico sobre $\boldsymbol{C}$, então existem $c_0, \ldots, c_n \in C$ tais que $c_0 \neq 0$ e*
$$\dotplus_{i=0}^{n} c_i \alpha^i = 0.$$

Demonstração. 1. Seja $\alpha \in C$. Então $\alpha \in E$, pois $C \subseteq E$. Tomando $p(x) = x - \alpha$, temos que $p(\alpha) = \alpha - \alpha = 0$.

2. Sejam $\alpha \in E$ um elemento algébrico sobre $\boldsymbol{C}$ e $c'_0, \ldots, c'_m \in C$ tais que
$$\dotplus_{i=0}^{m} c'_i \alpha^i = 0.$$
Como $c'_0, \ldots, c'_m$ não são todos nulos, seja $k \coloneqq \min\{i \in \{0, \ldots, m\} : c'_i \neq 0\}$. Então, para todo $i < k$, $c'_i = 0$, e segue que
$$0 = \dotplus_{i=0}^{m} c'_i \alpha^i = \dotplus_{i=k}^{m} c'_i \alpha^i = \alpha^k \dotplus_{i=k}^{m} c'_i \alpha^{i-k}$$
e, como E é corpo e $\alpha \neq 0$, podemos dividir por α^k em ambos lados e temos
$$\dotplus_{i=k}^{m} c'_i \alpha^{i-k} = 0.$$
Fazendo, $n \coloneqq m - k$ e, para todo $i \in \{0, \ldots, n\}$, $c_i \coloneqq c'_{k+i}$, temos que $c_0, \ldots, c_n \in E$ — com $c_0 = c'_k \neq 0$ e, portanto, não todos nulos — tais que
$$\dotplus_{i=0}^{n} c_i \alpha^i = \dotplus_{i=0}^{n} c'_{k+i} \alpha^i = \dotplus_{i=k}^{m} c'_i \alpha^{i-k} = 0.$$

■

Definição 11.4. Sejam $\boldsymbol{C}$ um corpo, $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$ e $\alpha \in E$ um elemento algébrico sobre $\boldsymbol{C}$. Um *polinômio minimal* de α sobre $\boldsymbol{C}$ é um polinômio $p \in C[x]$ que satisfaz

1. $p(\alpha) = 0$;
2. p é mônico;
3. $\text{grau}(p) = \min\{\text{grau}(f) : f \in C[x]^*, f(\alpha) = 0 \text{ e } f \text{ é mônico}\}$.

Proposição 11.3. *Sejam $\boldsymbol{C}$ um corpo, $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$ e $\alpha \in E$ um elemento algébrico sobre $\boldsymbol{C}$. Então existe um único polinômio minimal de α sobre $\boldsymbol{C}$.*

Demonstração. Pela definição de elemento algébrico, existe $p \in C[x]^*$ tal que $p'(\alpha) = 0$. Seja $n \coloneqq \text{grau}(p')$ e $p'(x) = \bigdoublebarwedge_{i=0}^{n} a'_i x^i$. Como $\boldsymbol{C}$ é corpo e $a'_n \neq 0$, existe $(a'_n)^{-1} \in C$. Definindo

$$p \coloneqq (a'_n)^{-1} p = \bigdoublebarwedge_{i=0}^{n-1} (a'_n)^{-1} a_i x^i + x^n,$$

segue que $p \in C[x]^*$, $\text{grau}(p) = n$, $p(\alpha) = (a'_n)^{-1} p'(\alpha) = 0$ e p é mônico. Portanto $\{\text{grau}(f) : f \in C[x]^*, f(\alpha) = 0 \text{ e } f \text{ é mônico}\}$ não é vazio, e, como é subconjunto de $\mathbb{N}$, admite mínimo, o que mostra que existe polinômio minimal de α sobre $\boldsymbol{C}$.

Para mostrar a unicidade, suponhamos que p_1 e p_2 são polinômios minimais de α sobre $\boldsymbol{C}$. Pela primeira propriedade de polinômio minimal, $(p_1 - p_2)(\alpha) = p_1(\alpha) - p_2(\alpha) = 0$. Pela terceira propriedade de polinômio minimal, $\text{grau}(p_1) = \text{grau}(p_2)$. Seja $n \coloneqq \text{grau}(p_1)$ e sejam $p_1 = \bigdoublebarwedge_{i=0}^{n} a_i x^i$ e $p_2 = \bigdoublebarwedge_{i=0}^{n} b_i x^i$. Pela segunda propriedade de polinômio minimal, $a_n = b_n = 1$. Então $a_n - b_n = 0$ e

$$(p_1 - p_2)(x) = \bigdoublebarwedge_{i=0}^{n-1} (a_i - b_i) x^i,$$

e conclui-se que $\text{grau}(p_1 - p_2) < n$. Se $p_1 \neq p_2$, existe $i \in \{0, \ldots, n-1\}$ tal que $a_i \neq b_i$. Então seja $k \coloneqq \max\{i \in \{0, \ldots, n-1\} : a_i \neq b_i\}$. Assim, para todo $i > k$, $a_i = b_i$, o que implica $a_i - b_i = 0$, e temos que $\text{grau}(p_1 - p_2) = k$ e

$$(p_1 - p_2)(x) = \bigdoublebarwedge_{i=0}^{k} (a_i - b_i) x^i.$$

Como $\boldsymbol{C}$ é corpo e $a_k - b_k \neq 0$, existe $(a_k - b_k)^{-1} \in C$. Definindo

$$p \coloneqq (a_k - b_k)^{-1} (p_1 - p_2) = \bigdoublebarwedge_{i=0}^{k-1} (a_k - b_k)^{-1} (a_i - b_i) x^i + x^k,$$

segue que $p \in C[x]^*$, $\text{grau}(p) = k$, $p(\alpha) = (a_k - b_k)^{-1}(p_1 - p_2)(\alpha) = (a_k - b_k)^{-1}(p_1(\alpha) - p_2(\alpha)) = 0$ e p é mônico. Mas $\text{grau}(p) = k < n = \text{grau}(p_1) = \text{grau}(p_2)$, o que contradiz a minimalidade do grau de p_1 e p_2. Portanto $p_1 = p_2$ e está provada a unicidade. ■

Proposição 11.4. *Seja $\boldsymbol{C}$ um corpo e $p \in C[x]^*$. Se p é mônico e redutível, então existem $p_1, p_2 \in C[x]^*$ tais que $p = p_1 p_2$ e p_1 e p_2 são mônicos.*

Demonstração. Como p é redutível, existem $p'_1, p'_2 \in C[x]^*$ tais que $p = p'_1 p'_2$. Sejam $n \coloneqq \text{grau}(p_1)$, $p_1 = \bigdoublebarwedge_{i=0}^{n} a_i x^i$, e $m \coloneqq \text{grau}(p_2)$, $p_2 = \bigdoublebarwedge_{i=0}^{m} b_i x^i$. Pela

definição de produto, sabemos que $a_n b_m = 1$, pois p é mônico. Como $\boldsymbol{C}$ é um corpo, existem $(a_n)^{-1}, (b_m)^{-1} \in C$. Definindo

$$p_1 \coloneqq (a_n)^{-1} p_1' = \bigdotplus_{i=0}^{n-1} (a_n)^{-1} a_i x^i + x^n \quad \text{e} \quad p_2 \coloneqq (b_m)^{-1} p_2' = \bigdotplus_{i=0}^{m-1} (b_m)^{-1} b_i x^i + x^m,$$

segue que $p_1, p_2 \in C[x]^*$ são mônicos e que

$$p = p_1' p_2' = (a_n) p_1 (b_m) p_2 = (a_n b_m) p_1 p_2 = p_1 p_2.$$

■

Proposição 11.5. *Sejam $\boldsymbol{C}$ um corpo, $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$, $\alpha \in E$ um elemento algébrico sobre $\boldsymbol{C}$ e $p \in C[x]^*$ um polinômio mônico tal que $p(\alpha)$. Então p é o polinômio minimal de α sobre $\boldsymbol{C}$ se, e somente se, p é irredutível em $\boldsymbol{C}[x]$.*

Demonstração. Suponhamos que p é polinômio minimal de α sobre $\boldsymbol{C}$. Se p não é irredutível em $C[x]$, como p é mônico, então existem $p_1, p_2 \in C[x]^*$ mônicos tais que $0 < \text{grau}(p_i) < \text{grau}(p)$ para todo $i \in \{1, 2\}$. Como $p(\alpha) = p_1(\alpha) p_2(\alpha) = 0$ e $\boldsymbol{C}$ é corpo, segue que $p_1(\alpha) = 0$ ou $p_2(\alpha) = 0$. No primeiro caso, $p_1 \in C[x]^*$ é um polinômio mônico, $p_1(\alpha) = 0$ e $\text{grau}(p_1) < \text{grau}(p)$, o que contradiz a minimalidade de p. No segundo caso, $p_2 \in C[x]^*$ é um polinômio mônico, $p_2(\alpha) = 0$ e $\text{grau}(p_2) < \text{grau}(p)$, o que também contradiz a minimalidade de p, e temos um absurdo. Portanto p é irredutível em $\boldsymbol{C}[x]$.

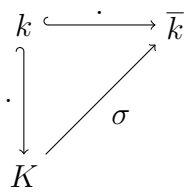
Reciprocamente, suponhamos que p é irredutível em $\boldsymbol{C}[x]$. Por hipótese, $p(\alpha) = 0$ e p é mônico. Seja $p_\alpha \in C[x]^*$ o polinômio minimal de α sobre $\boldsymbol{C}$. Então $\text{grau}(p_\alpha) \leq \text{grau}(p)$. Como p_α é mônico, exitem $q, r \in C[x]$ tais que $p = q p_\alpha + r$. Como $p(\alpha) = p_\alpha(\alpha) = 0$, então $r(\alpha) = p(\alpha) - q(\alpha) p_\alpha(\alpha) = 0$. Se $r \neq 0$, então $\text{grau}(r) < \text{grau}(p_\alpha)$. Seja $n \coloneqq \text{grau}(r)$. Como $r(\alpha) = 0$, segue que $\text{grau}(r) > 0$. Então seja $r(x) = \bigdotplus_{i=0}^{n} a_i x^i$. Como $\boldsymbol{C}$ é corpo, existe $(a_n)^{-1} \in C$. Assim, definindo

$$p' \coloneqq (a_n)^{-1} r = \bigdotplus_{i=0}^{n-1} (a_n)^{-1} a_i x^i + x^n,$$

e segue que $p' \in C[x]^*$, $p'(\alpha) = (a_n)^{-1} p'(\alpha) = 0$ e p' é mônico. Mas $\text{grau}(p') = n = \text{grau}(r) < \text{grau}(p_\alpha)$, o que contradiz a minimalidade do grau de p_α. Então $r \neq 0$. Se $r = 0$, então $p = q p_\alpha$. Mas p é irredutível, e $p_\alpha \in C[x]^*$, o que implica $q \in C$. Como p e p_α são mônicos, segue que $q = 1$ e, portanto, $p = p_\alpha$. ■

11.2 COISAS DA PROVA 3

Teorema 11.6. *Seja $k \subseteq K$ uma estensão de corpos, $\overline{k}$ fecho algébrico de k. Então as seguintes condições são equivalentes:*



1. *DIAGRAMA COMUTATIVO*

2. *K é corpo de raízes sobre k de uma família $(f_i)_{i\in I}$ de polinômios em $k[x]\setminus k$;*

3. *Se $f \in k[x]\setminus k$ é irredutível em $k[x]$ com raiz α, então $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ em $k[x]$, com $\alpha_1 = \alpha$ e $c \in k \setminus \{0\}$.*

Demonstração. PULEI, tem nas notas mas não tudo. ■

Definição 11.5. Uma extensão de corpos $k \subseteq K$ é uma *extensão normal* se ela satisfaz uma das três condições do teorema acima.

OBS: Se $k \subseteq \overline{k}$ é uma extensão algébrica, então todo $\beta \in \overline{k}$ é algébrico sobre k vale para $\beta \in K$, então $k \subseteq K$ é extensão algébrica.

Se $k \subseteq K$ é extensão algébrica, então $k \subseteq K \subseteq \overline{K}$ são extensões algébricas, então $k \subseteq \overline{K}$ é extensão algébrica. Então $\overline{k} \sim \overline{K}$ é fecho algébrico de k.

(?????)

Proposição 11.7. *Seja $k \subseteq K$ um extensão algébrica e $\sigma : K \to K$ um homomorfismo de cropos que satisfaz $\sigma|_k = id|_k$. Então σ é um isomorfismo de corpos.*

Demonstração. ... ■

Definição 11.6. Seja $E \subseteq F$ uma extensão algébrica e $\sigma : E \to L$ um homomorfismo de corpos tal que L é algebricamente fechaado, $\sigma(E) \subseteq L$ é uma extensão algébrica (L é fecho algébrico de $\sigma(E)$)

$$S_\sigma \coloneqq \{\mu : \mu : F \to L \text{ homomorfismo de corpos}, \mu|_E = \sigma\}.$$

Lema 11.8. *$|S_\sigma|$ depende de $E \subseteq F$, mas não depende de σ nem de L.*

Demonstração. ... vários diagramas ■

Definição 11.7. Seja $E \subseteq F$ uma extensão algébrica. O *grau de separabilidade* da extensão é $[F : E]_S \coloneqq |S_\sigma|$. (Pode escolher $l = \overline{E}$ e σ inclusão.)

Teorema 11.9. *1. $E \subseteq F \subseteq K$ extensões algébricas, então*

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

2. $E \subseteq F$ extensão finita (logo algébrica), então

$$[F : E]_S \leq [F : E]$$

Demonstração. ... ■

Definição 11.8. Seja $E \subseteq K$ uma extensão finita. Ela é *separável* se $[K : E]_S = [K : E]$.

Corolário 11.10. *Sejam $E \subseteq F \subseteq K$ extensões de corpos, $[K : E] < \infty$, $E \subseteq K$ separável. Então $E \subseteq F$ e $FsubseteqK$ são separáveis.*

Demonstração.

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

Como $[F : E]_S \leq [F : E]$ e $[K : F]_S \leq [K : F]$, segue o corolário. ■

Capítulo 12

Matrizes

Definição 12.1. Seja $\boldsymbol{A}$ um anel e $l, c \in \mathbb{N}$. Uma *matriz* de dimensão $l \times c$ sobre $\boldsymbol{A}$ é uma função $M : \mathtt{I}_l \times \mathtt{I}_c \to A$. Representa-se isso por

$$M = \begin{bmatrix} m_{1,1} & \cdots & m_{1,c} \\ \vdots & \ddots & \vdots \\ m_{l,1} & \cdots & m_{l,c} \end{bmatrix},$$

em que $m_{i,j} \coloneqq M(i,j) \in A$. O conjunto $\mathtt{I}_l$ é o conjunto dos *índices das linhas* e $\mathtt{I}_c$ é o conjunto dos *índices das colunas* da matriz M. A imagem de M é o conjunto das *entradas* da matriz M e o elemento $m_{i,j}$ é a entrada da linha i e coluna j.

O conjunto de todas as matrizes de dimensão $l \times c$ sobre $\boldsymbol{A}$ é denotado por $\mathbb{M}_{l\times c}(\boldsymbol{A})$.

Definição 12.2. Seja $\boldsymbol{A}$ um anel e $d \in \mathbb{N}$. Uma *matriz quadrada* de dimensão d sobre $\boldsymbol{A}$ é uma matriz $M \in \mathbb{M}_{d\times d}(\boldsymbol{A})$. O conjunto de todas as matrizes quadradas de dimensão d sobre $\boldsymbol{A}$ é denotado por $\mathbb{M}_d(\boldsymbol{A})$.

Definição 12.3. Sejam $\boldsymbol{A}$ um anel e $M \in \mathbb{M}_{l\times c}(\boldsymbol{A})$. A *matriz transposta* de M é a matriz $M^\intercal \in \mathbb{M}_{c\times l}(\boldsymbol{A})$ definida por

$$(M^\intercal)(i,j) \coloneqq m_{j,i}.$$

12.1 Soma de Matrizes

Definição 12.4. Sejam $\boldsymbol{A}$ um anel e $M, N \in \mathbb{M}_{l\times c}(\boldsymbol{A})$. A *matriz soma* das matrizes M e N é a matriz $(M+N) \in \mathbb{M}_{l\times c}(\boldsymbol{A})$ definida por

$$(M+N)(i,j) \coloneqq m_{i,j} + n_{i,j}.$$

Definição 12.5. Sejam $\boldsymbol{A}$ um anel e 0 o elemento neutro da soma de $\boldsymbol{A}$.

1. A *matriz nula* de dimensão $l \times c$ sobre $\boldsymbol{A}$ é a matriz $\mathbb{O}_{l\times c} \in \mathbb{M}_{l\times c}(\boldsymbol{A})$, definida por
$$\mathbb{O}_{l\times c}(i,j) \coloneqq 0.$$
2. Se $M \in \mathbb{M}_{l\times c}$, a *matriz negativa* de M é a matriz $-M \in \mathbb{M}_{l\times c}(\boldsymbol{A})$, definida por
$$(-M)(i,j) \coloneqq -m_{i,j}.$$

Proposição 12.1. *Seja $\boldsymbol{A}$ um anel e $+$ a operação binária em $\mathbb{M}_{l\times c}(\boldsymbol{A})$ definida por*

$$\begin{aligned} + : \mathbb{M}_{l\times c}(\boldsymbol{A}) \times \mathbb{M}_{l\times c}(\boldsymbol{A}) &\to \mathbb{M}_{l\times c}(\boldsymbol{A}) \\ (M,N) &\mapsto M+N. \end{aligned}$$

Então $(\mathbb{M}_{l\times c}(\boldsymbol{A}),+)$ é um grupo com elemento neutro $\mathbb{O}_{l\times c}$. Se $\boldsymbol{A}$ é comutativo, então $(\mathbb{M}_{l\times c}(\boldsymbol{A}),+)$ é comutativo.

Demonstração. Sejam $M,N,P \in \mathbb{M}_{l\times c}(\boldsymbol{A})$. Primeiro, notemos que $+$ é associativa, pois, como a soma no anel é associativa, segue que

$$(m_{i,j}+n_{i,j})+p_{i,j} = m_{i,j}+(n_{i,j}+p_{i,j})$$

e, portanto, $(M+N)+P = M+(N+P)$. Então, notemos que $\mathbb{O}$ é elemento neutro de $+$. Como 0 é elemento neutro da soma da anel, segue que

$$m_{i,j}+0 = 0+m_{i,j} = m_{i,j}$$

e, portanto, $M+\mathbb{O} = \mathbb{O}+M = M$. Ainda, notemos que, como $-m_{i,j}$ é o inverso aditivo de $m_{i,j}$ no anel, segue que

$$m_{i,j}+(-m_{i,j}) = (-m_{i,j})+m_{i,j} = 0$$

e, portanto, $M+(-M) = (-M)+M = \mathbb{O}$. Assim, concluímos que $(\mathbb{M}_{l\times c}(\boldsymbol{A}),+)$ é um anel. Por fim, notemos que, se $\boldsymbol{A}$ é comutativo, então $+$ é comutativa, pois, como a soma no anel é comutativa, segue que

$$m_{i,j}+n_{i,j} = n_{i,j}+m_{i,j}$$

e, portanto, $M+N = N+M$. Assim, concluímos que, se $\boldsymbol{A}$ é comutativo, então $(\mathbb{M}_{l\times c}(\boldsymbol{A}),+)$ é comutativo. ■

12.2 Produto de Matrizes e Produto Por Escalar

Definição 12.6. Sejam $\boldsymbol{A}$ um anel e $M \in \mathbb{M}_{l\times d}(\boldsymbol{A})$ e $N \in \mathbb{M}_{d\times c}(\boldsymbol{A})$. A *matriz produto* das matrizes M e N é a matriz $(MN) \in \mathbb{M}_{l\times c}(\boldsymbol{A})$ definida por

$$(MN)(i,j) \coloneqq \bigplus_{k=1}^{d} m_{i,k}n_{k,j}.$$

Proposição 12.2. *Sejam $\boldsymbol{A}$ um anel e $M \in \mathbb{M}_{l\times d_1}(\boldsymbol{A})$, $N \in \mathbb{M}_{d_1\times d_2}(\boldsymbol{A})$ e $P \in \mathbb{M}_{d_2\times c}(\boldsymbol{A})$. Então*

$$(MN)P = M(NP).$$

Demonstração. Um elemento de MN é dado por

$$(mn)_{i,j} = \bigplus_{k_1=1}^{d_1} m_{i,k_1}n_{k_1,j}.$$

Logo, um elemento de $(MN)P$ é dado por

$$((mn)p)_{i,j} = \bigplus_{k_2=1}^{d_2} (mn)_{i,k_2}p_{k_2,j} = \bigplus_{k_2=1}^{d_2} \left(\bigplus_{k_1=1}^{d_1} m_{i,k_1}n_{k_1,k_2} \right) p_{k_2,j}.$$

Analogamente, um elemento de $M(NP)$ é dado por

$$(m(np))_{i,j} = \bigplus_{k_1=1}^{d_1} m_{i,k_1}(np)_{k_1,j} = \bigplus_{k_1=1}^{d_1} m_{i,k_1} \left(\bigplus_{k_2=1}^{d_2} n_{k_1,k_2}p_{k_2,j} \right).$$

Mas então, como $\boldsymbol{A}$ é um anel, segue que

$$\begin{aligned}
((mn)p)_{i,j} &= \bigplus_{k_2=1}^{d_2} \left(\bigplus_{k_1=1}^{d_1} m_{i,k_1}n_{k_1,k_2} \right) p_{k_2,j} \\
&= \bigplus_{k_2=1}^{d_2} \left(\bigplus_{k_1=1}^{d_1} m_{i,k_1}n_{k_1,k_2}p_{k_2,j} \right) \\
&= \bigplus_{k_1=1}^{d_1} \left(\bigplus_{k_2=1}^{d_2} m_{i,k_1}n_{k_1,k_2}p_{k_2,j} \right) \\
&= \bigplus_{k_1=1}^{d_1} m_{i,k_1} \left(\bigplus_{k_2=1}^{d_2} n_{k_1,k_2}p_{k_2,j} \right) \\
&= (m(np))_{i,j}.
\end{aligned}$$

■

Definição 12.7. Sejam $\boldsymbol{A}$ um anel e 0 e 1 os elementos neutros da soma e da multiplicação de $\boldsymbol{A}$ respectivamente. A *matriz identidade* de dimensão d sobre $\boldsymbol{A}$ é a matriz $\mathbb{1}_d \in \mathbb{M}_d(\boldsymbol{A})$ definida por

$$\mathbb{1}_d(i,j) \coloneqq \delta_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j, \end{cases}$$

Essa função δ é conhecida como delta de Kronecker.

Proposição 12.3. *Seja $\boldsymbol{A}$ um anel e $\cdot$ a operação binária em $\mathbb{M}_d(\boldsymbol{A})$ definida por*

$$\begin{aligned} \cdot : \mathbb{M}_d(\boldsymbol{A}) \times \mathbb{M}_d(\boldsymbol{A}) &\to \mathbb{M}_d(\boldsymbol{A}) \\ (M, N) &\mapsto MN. \end{aligned}$$

Então $(\mathbb{M}_d(\boldsymbol{A}), \cdot)$ é um monoide com elemento neutro $\mathbb{1}_d$.

Demonstração. Sejam $M, N, P \in \mathbb{M}_d(\boldsymbol{A})$. Pela proposição anterior, sabemos que vale $(MN)P = M(NP)$ e que, portanto, $\cdot$ é associativa. Agora, notemos que um elemento de $M\mathbb{1}_d$ é da forma

$$\bigdotplus_{k=1}^{d} m_{i,k}\delta_{k,j}.$$

Mas, para $k \in \mathtt{I}_d$, se $k \neq j$, então $\delta_{k,j} = 0$ e, se $k = j$, então $\delta_{k,j} = 1$ e, portanto, segue que

$$\bigdotplus_{k=1}^{d} m_{i,k}\delta_{k,j} = m_{i,j}.$$

Assim, concluímos que $M\mathbb{1}_d = M$. Analogamente, mostra-se que $\mathbb{1}_d M = M$, e concluímos que $\mathbb{1}_d$ é elemento neutro de $\cdot$. Isso mostra que $(\mathbb{M}_d(\boldsymbol{A}), \cdot)$ é um monoide. ■

Definição 12.8. Seja $\boldsymbol{A}$ um anel. Uma *matriz invertível* é uma matriz $M \in \mathbb{M}_d(\boldsymbol{A})$ que é invertível com respeito ao produto do monoide $(\mathbb{M}_d(\boldsymbol{A}), \cdot)$. A matriz inversa de M é denotada M^{-1}.

Definição 12.9. Seja $\boldsymbol{A}$ um anel, $a \in A$ e $M \in \mathbb{M}_{l\times c}(\boldsymbol{A})$. O *produto por escalar* de a e M é a matriz $aM \in \mathbb{M}_{l\times c}$ definida por

$$(aM)(i,j) \coloneqq am_{i,j}.$$

12.3 Matrizes Quadradas

Definição 12.10. Seja $\boldsymbol{A}$ um anel.

1. Uma *matriz triangular superior* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que satisfaz
$$\forall i, j \in \mathtt{I}_d \qquad i > j \Rightarrow m_{i,j} = 0.$$
2. Uma *matriz triangular inferior* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ sobre $\boldsymbol{A}$ que satisfaz
$$\forall i, j \in \mathtt{I}_d \qquad i < j \Rightarrow m_{i,j} = 0.$$
3. Uma *matriz triangular superior* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que satisfaz
$$\forall i, j \in \mathtt{I}_d \qquad i > j \Rightarrow m_{i,j} = 0.$$
4. Uma *matriz triangular* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que é triangular superior ou triangular inferior.
5. Uma *matriz diagonal* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que é triangular superior e triangular inferior; ou seja, que satisfaz
$$\forall i, j \in \mathtt{I}_d \qquad i \neq j \Rightarrow m_{i,j} = 0.$$
6. Uma *matriz simétrica* uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que é igual a sua transposta
$$M = M^\intercal.$$
7. Uma *matriz antissimétrica* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que é igual à negativa da sua transposta
$$M = -M^\intercal.$$
8. Uma *matriz ortogonal* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ cuja transposta é igual à sua inversa
$$M^\intercal = M^{-1}.$$

12.4 Traço e Determinante

Definição 12.11. Sejam $\boldsymbol{A}$ um anel e $M \in \mathbb{M}_d(\boldsymbol{A})$. O *traço* de M é o elemento $\mathrm{tr}(M) \in A$ definido por
$$\mathrm{tr}(M) \coloneqq \bigboxplus_{i=1}^{d} m_{i,i}.$$

Proposição 12.4. *Sejam $\boldsymbol{A}$ um anel, $a \in A$ e $M, N \in \mathbb{M}_d(\boldsymbol{A})$. Então*

1. $\operatorname{tr}(M^\intercal) = \operatorname{tr}(M)$;
2. $\operatorname{tr}(MN) = \operatorname{tr}(NM)$;
3. $\operatorname{tr}(M+N) = \operatorname{tr}(M) + \operatorname{tr}(N)$;
4. $\operatorname{tr}(aM) = a \operatorname{tr}(M)$.

Demonstração. 1.

$$\operatorname{tr}(M) = \bigplus_{i=1}^{d} m_{i,i} = \operatorname{tr}(M^\intercal).$$

2.

$$\begin{aligned}
\operatorname{tr}(MN) &= \bigplus_{i=1}^{d} \left(\bigplus_{k=1}^{d} m_{i,k} n_{k,i} \right) \\
&= \bigplus_{i=1}^{d} \left(\bigplus_{k=1}^{d} n_{k,i} m_{i,k} \right) \\
&= \bigplus_{k=1}^{d} \left(\bigplus_{i=1}^{d} n_{k,i} m_{i,k} \right) \\
&= \operatorname{tr}(NM).
\end{aligned}$$

3.

$$\begin{aligned}
\operatorname{tr}(M+N) &= \bigplus_{i=1}^{d} (m_{i,i} + n_{i,i}) \\
&= \bigplus_{i=1}^{d} m_{i,i} + \bigplus_{i=1}^{d} n_{i,i} \\
&= \operatorname{tr}(M) + \operatorname{tr}(N).
\end{aligned}$$

4.

$$\operatorname{tr}(aM) = \bigplus_{i=1}^{d} a m_{i,i} = a \bigplus_{i=1}^{d} m_{i,i} = a \operatorname{tr}(M).$$

■

Capítulo 13

Espaços Vetoriais

13.1 Espaço e Subespaço Vetoriais

Definição 13.1. Um *espaço vetorial* (ou *espaço linear*) sobre um corpo $\boldsymbol{C} = (C, +, \cdot)$ é uma tripla $\boldsymbol{V} = (V, +, \cdot)$ em que

1. $(V, +)$ é um grupo comutativo com elemento neutro $\mathbf{0}$;
2. $\cdot : C \times V \to V$ é uma função que satisfaz
   (a) $\forall \boldsymbol{v} \in V \qquad 1 \cdot \boldsymbol{v} = \boldsymbol{v}$;
   (b) $\forall c_1, c_2 \in C \ \forall \boldsymbol{v} \in V \qquad (c_1 \cdot c_2) \cdot \boldsymbol{v} = c_1 \cdot (c_2 \cdot \boldsymbol{v})$;
3. (Distributividades)
   (a) $\forall c \in C \ \forall \boldsymbol{v}_1, \boldsymbol{v}_2 \in V \qquad c \cdot (\boldsymbol{v}_1 + \boldsymbol{v}_2) = c \cdot \boldsymbol{v}_1 + c \cdot \boldsymbol{v}_2$;
   (b) $\forall c_1, c_2 \in C \ \forall \boldsymbol{v} \in V \qquad (c_1 + c_2) \cdot \boldsymbol{v} = c_1 \cdot \boldsymbol{v} + c_2 \cdot \boldsymbol{v}$.

Os elementos de V são chamados de *vetores* e denotados em negrito e os elementos de C são chamados de *escalares*. As operações $+$ e $\cdot$ são denotadas por $+$ e $\cdot$, o inverso de $\boldsymbol{v} \in V$ é denotado $-\boldsymbol{v}$ e a imagem de $(c, v) \in C \times V$, chamada de *produto* de c e $\boldsymbol{v}$, é denotada por $c\boldsymbol{v}$. Quando o corpo é $\mathbb{R}$, dizemos *espaço vetorial real*, quando o corpo é $\mathbb{C}$, dizemos *espaço vetorial complexo*.

Proposição 13.1. *Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Então, para todos $\boldsymbol{v} \in V$ e $c \in C$,*

1. $c\boldsymbol{v} = \mathbf{0} \Leftrightarrow c = 0 \ \ ou \ \ \boldsymbol{v} = \mathbf{0}$;
2. $-(c\boldsymbol{v}) = (-c)\boldsymbol{v} = c(-\boldsymbol{v})$;
3. $c\boldsymbol{v} = (-c)(-\boldsymbol{v})$.

Demonstração. Sejam $\boldsymbol{v} \in V$ e $c \in C$.

1. Primeiro, notemos que

$$\begin{aligned} 0\boldsymbol{v} &= 0\boldsymbol{v} + \mathbf{0} \\ &= 0\boldsymbol{v} + (0\boldsymbol{v} - 0\boldsymbol{v}) \\ &= (0\boldsymbol{v} + 0\boldsymbol{v}) - 0\boldsymbol{v} \\ &= (0+0)\boldsymbol{v} - 0\boldsymbol{v} \\ &= 0\boldsymbol{v} - 0\boldsymbol{v} \\ &= \mathbf{0}. \end{aligned}$$

   Agora, notemos que

$$\begin{aligned} c\mathbf{0} &= c\mathbf{0} + \mathbf{0} \\ &= c\mathbf{0} + (c\mathbf{0} - c\mathbf{0}) \\ &= (c\mathbf{0} + c\mathbf{0}) - c\mathbf{0} \\ &= c(\mathbf{0} + \mathbf{0}) - c\mathbf{0} \\ &= c\mathbf{0} - c\mathbf{0} \\ &= \mathbf{0}. \end{aligned}$$

   Portanto, se $c = 0$ ou $\boldsymbol{v} = \mathbf{0}$, então $c\boldsymbol{v} = \mathbf{0}$. Agora, suponhamos que $c\boldsymbol{v} = \mathbf{0}$. Se $c \neq 0$, como $\boldsymbol{C}$ é corpo, segue da demonstração anterior que

$$\boldsymbol{v} = c^{-1}c\boldsymbol{v} = c^{-1}\mathbf{0} = \mathbf{0}.$$

2. Basta notar que

$$\begin{aligned} -(c\boldsymbol{v}) &= -(c\boldsymbol{v}) + \mathbf{0} \\ &= -(c\boldsymbol{v}) + (0\boldsymbol{v}) \\ &= -(c\boldsymbol{v}) + (c - c)\boldsymbol{v} \\ &= -(c\boldsymbol{v}) + (c\boldsymbol{v} + (-c)\boldsymbol{v}) \\ &= (-(c\boldsymbol{v}) + c\boldsymbol{v}) + (-c)\boldsymbol{v} \\ &= \mathbf{0} + (-c)\boldsymbol{v} \\ &= (-c)\boldsymbol{v} \end{aligned}$$

e que

$$\begin{aligned}
-(c\boldsymbol{v}) &= -(c\boldsymbol{v}) + \mathbf{0} \\
&= -(c\boldsymbol{v}) + (c\mathbf{0}) \\
&= -(c\boldsymbol{v}) + c(\boldsymbol{v} - \boldsymbol{v}) \\
&= -(c\boldsymbol{v}) + (c\boldsymbol{v} + c(-\boldsymbol{v})) \\
&= (-(c\boldsymbol{v} + c\boldsymbol{v}) + c(-\boldsymbol{v}) \\
&= \mathbf{0} + c(-\boldsymbol{v}) \\
&= c(-\boldsymbol{v}).
\end{aligned}$$

3. Do item anterior, segue que

$$c\boldsymbol{v} = (-(-c))\boldsymbol{v} = (-c)(-\boldsymbol{v}).$$ ■

Proposição 13.2. *Seja $\boldsymbol{C}$ um corpo e n um natural positivo. Então $(C^n, +, \cdot)$, em que*

$$\begin{aligned}
\cdot : C \times C^n &\to C^n \\
(c, (c_1, \ldots, c_n)) &\mapsto (c \cdot c_1, \ldots, c \cdot c_n),
\end{aligned}$$

é um espaço vetorial sobre $\boldsymbol{C}$.

Demonstração. Claramente $(C^n, +)$ é um grupo comutativo com elemento neutro $(0, \ldots, 0)$. Note que, para todos $(c_1, \ldots, c_n) \in C^n$ e $c, c' \in C$,

$$1 \cdot (c_1, \ldots, c_n) = (1 \cdot c_1, \ldots, 1 \cdot c_n) = (c_1, \ldots, c_n)$$

e

$$\begin{aligned}
(c \cdot c') \cdot (c_1, \ldots, c_n) &= ((c \cdot c') \cdot c_1, \ldots, (c \cdot c') \cdot c_n) \\
&= ((c \cdot (c' \cdot c_1), \ldots, (c \cdot (c' \cdot c_n)) \\
&= c \cdot (c' \cdot c_1, \ldots, c' \cdot c_n) \\
&= c \cdot (c' \cdot (c_1, \ldots, c_n)).
\end{aligned}$$

Ainda, note que, para todos $(c_1, \ldots, c_n), (c'_1, \ldots, c'_n) \in C^n$ e $c, c' \in C$,

$$\begin{aligned}
c \cdot ((c_1, \ldots, c_n) + (c'_1, \ldots, c'_n)) &= c \cdot (c_1 + c'_1, \ldots, c_n + c'_n) \\
&= (c \cdot (c_1 + c'_1), \ldots, c \cdot (c_n + c'_n)) \\
&= (c \cdot c_1 + c \cdot c'_1, \ldots, c \cdot c_n + c \cdot c'_n) \\
&= (c \cdot c_1, \ldots, c \cdot c_n) + (c \cdot c'_1, \ldots, c \cdot c'_n) \\
&= c \cdot (c_1, \ldots, c_n) + c \cdot (c'_1, \ldots, c'_n)
\end{aligned}$$

e

$$\begin{aligned}(c+c')\cdot(c_1,\ldots,c_n) &= ((c+c')c_1,\ldots,(c+c')c_n)\\ &= (c\cdot c_1 + c'\cdot c_1,\ldots,c\cdot c_n + c'\cdot c_n)_{i\in I}\\ &= (c\cdot c_1,\ldots,c\cdot c_n) + (c'\cdot c_1,\ldots,c'\cdot c_n)\\ &= c\cdot(c_1,\ldots,c_n) + c'\cdot(c_1,\ldots,c_n).\end{aligned}$$ ■

Para generalizar esse resultado, lembremos que o produto de uma família $(C_i)_{i\in I}$ de conjuntos é $\bigtimes_{i\in I} C_i$ e, quando $C_i = C$, temos que $\bigtimes_{i\in I} C_i = C^I$ e os elementos de C^I são funções $c = (c_i)_{i\in I}$ de I em C.

Proposição 13.3 (EXERCÍCIO)**.** *Sejam $\boldsymbol{C}$ um corpo e I um conjunto não vazio. Então $\boldsymbol{C^I} = (C^I, +, \cdot)$, em que*

$$\begin{aligned}+ : C^I \times C^I &\to C^I\\ (\boldsymbol{c}, \boldsymbol{c'}) &\mapsto (c_i + c'_i)_{i\in I}\end{aligned}$$

e

$$\begin{aligned}\cdot : C \times C^I &\to C^I\\ (a, \boldsymbol{c}) &\mapsto (a\cdot c_i)_{i\in I},\end{aligned}$$

é um espaço vetorial sobre $\boldsymbol{C}$.

Proposição 13.4 (Espaço de Funções)**.** *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços vetoriais sobre um corpo $\boldsymbol{C}$. Então $\boldsymbol{W^V} = (W^V, +, \cdot)$, em que*

$$\begin{aligned}+ : W^V \times W^V &\to W^V\\ (\boldsymbol{f}_1, \boldsymbol{f}_2) &\mapsto \boldsymbol{f}_1 + \boldsymbol{f}_2 : V \to W\\ &\qquad \boldsymbol{v} \mapsto \boldsymbol{f}_1(\boldsymbol{v}) + \boldsymbol{f}_2(\boldsymbol{v}).\end{aligned}$$

e

$$\begin{aligned}\cdot : C \times W^V &\to W^V\\ (c, \boldsymbol{f}) &\mapsto c\boldsymbol{f} : V \to W\\ &\qquad \boldsymbol{v} \mapsto c\boldsymbol{f}(\boldsymbol{v}),\end{aligned}$$

é um espaço vetorial sobre $\boldsymbol{C}$.

Demonstração. Primeiro, sabemos que $(W^V, +)$ é um grupo comutativo com elemento neutro $0 : W^V \times W^V \to W^V$ definido por $0(\boldsymbol{v}) = 0$. Devemos então mostrar que $\cdot : C \times W^V \to W^V$ satisfaz os itens da definição de espaço vetorial. Primeiro,

seja $\boldsymbol{f} \in W^V$. Então, para todo $\boldsymbol{v} \in V$, $(1\boldsymbol{f})(\boldsymbol{v}) = 1\boldsymbol{f}(\boldsymbol{v}) = \boldsymbol{f}(\boldsymbol{v})$, o que mostra que $1\boldsymbol{f} = \boldsymbol{f}$. Agora, sejam $c_1, c_2 \in C$ e $\boldsymbol{f} \in W^V$. Então, para todo $\boldsymbol{v} \in V$,

$$((c_1c_2)\boldsymbol{f})(\boldsymbol{v}) = (c_1c_2)\boldsymbol{f}(\boldsymbol{v}) = c_1(c_2\boldsymbol{f}(\boldsymbol{v})) = c_1(c_2\boldsymbol{f})(\boldsymbol{v}) = (c_1(c_2\boldsymbol{f}))(\boldsymbol{v}),$$

o que mostra que $(c_1c_2)\boldsymbol{f} = c_1(c_2\boldsymbol{f})$.

Por fim, devemos mostrar as propriedades distributivas. Sejam $c \in C$ e $\boldsymbol{f}_1, \boldsymbol{f}_2 \in W^V$. Então, para todo $\boldsymbol{v} \in V$,

$$\begin{aligned}(c(\boldsymbol{f}_1 + \boldsymbol{f}_2))(\boldsymbol{v}) &= c(\boldsymbol{f}_1 + \boldsymbol{f}_2)(\boldsymbol{v}) \\ &= c(\boldsymbol{f}_1(\boldsymbol{v}) + \boldsymbol{f}_2(\boldsymbol{v})) \\ &= c\boldsymbol{f}_1(\boldsymbol{v}) + c\boldsymbol{f}_2(\boldsymbol{v}) \\ &= (c\boldsymbol{f}_1)(\boldsymbol{v}) + (c\boldsymbol{f}_2)(\boldsymbol{v}) \\ &= (c\boldsymbol{f}_1 + c\boldsymbol{f}_2)(\boldsymbol{v}),\end{aligned}$$

o que mostra que $c(\boldsymbol{f}_1 + \boldsymbol{f}_2) = c\boldsymbol{f}_1 + c\boldsymbol{f}_2$. Agora, sejam $c_1, c_2 \in C$ e $\boldsymbol{f} \in W^V$. Então, para todo $\boldsymbol{v} \in V$,

$$\begin{aligned}((c_1 + c_2)\boldsymbol{f})(\boldsymbol{v}) &= (c_1 + c_2)\boldsymbol{f}(\boldsymbol{v}) \\ &= c_1\boldsymbol{f}(\boldsymbol{v}) + c_2\boldsymbol{f}(\boldsymbol{v}) \\ &= (c_1\boldsymbol{f})(\boldsymbol{v}) + (c_2\boldsymbol{f})(\boldsymbol{v}) \\ &= (c_1\boldsymbol{f} + c_2\boldsymbol{f})(\boldsymbol{v}),\end{aligned}$$

o que mostra que $(c_1 + c_2)\boldsymbol{f} = c_1\boldsymbol{f} + c_2\boldsymbol{f}$. Assim, concluímos que $(W^V, +, \cdot)$ é um espaço vetorial sobre $\boldsymbol{C}$. ■

Definição 13.2. Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Um *subespaço vetorial* de $\boldsymbol{V}$ é um conjunto não vazio $W \subseteq V$ tal que

1. $\forall \boldsymbol{w}_1, \boldsymbol{w}_2 \in W \qquad \boldsymbol{w}_1 + \boldsymbol{w}_2 \in W$;
2. $\forall c \in C \ \forall \boldsymbol{w} \in W \qquad c\boldsymbol{w} \in W$.

Proposição 13.5. *Seja $\boldsymbol{V} = (V, +, \cdot)$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Então um conjunto não vazio $W \subseteq V$ é um subespaço vetorial de $\boldsymbol{V}$ se, e somente se, $\boldsymbol{W} = (W, +|_{W\times W}, \cdot|_{C\times W})$ é um espaço vetorial sobre $\boldsymbol{C}$.*

Demonstração. ... ■

Proposição 13.6. *Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e W um subespaço vetorial de $\boldsymbol{V}$. Então*

1. $\boldsymbol{0} \in W$;

2. $\{\mathbf{0}\}$ *e* V *são subespaços vetoriais de* $\boldsymbol{V}$*.*

Demonstração. 1. Como W não é vazio, seja $\boldsymbol{w} \in W$. Então $0\boldsymbol{w} = \mathbf{0} \in W$.

2. Seja $W = \{\mathbf{0}\}$. Se $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$, $\boldsymbol{w}_1 = \mathbf{0}$ e $\boldsymbol{w}_2 = \mathbf{0}$, e segue que $\boldsymbol{w}_1 + \boldsymbol{w}_2 = \mathbf{0} + \mathbf{0} = \mathbf{0}$. Ainda, para todo $c \in C$, segue que $c\boldsymbol{w}_1 = c\mathbf{0} = \mathbf{0} \in W$. Seja $W = V$. Como $\boldsymbol{V}$ é espaço vetorial, então V é subespaço vetorial de $\boldsymbol{V}$ pala proposição anterior. ■

Proposição 13.7. *Sejam* $\boldsymbol{V}$ *um espaço vetorial sobre um corpo* $\boldsymbol{C}$ *e* $(W_i)_{i\in I}$ *uma família de subespaços vetoriais de* $\boldsymbol{V}$*. Então*

$$W \coloneqq \bigcap_{i\in I} W_i$$

é um subespaço vetorial de $\boldsymbol{V}$*.*

Demonstração. Como, para todo $i \in I$, $\mathbf{0} \in W_i$, segue que $\mathbf{0} \in W$ e, portanto, W não é vazio. Agora, sejam $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$ e $c \in C$. Então, para todo $i \in I$, $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W_i$ e, como W_i é subespaço vetorial de $\boldsymbol{V}$, segue que $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W_i$ e que $c\boldsymbol{w}_1 \in W_i$. Logo $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W$ e $c\boldsymbol{w}_1 \in W$, o que mostra que W é subespaço vetorial de $\boldsymbol{V}$. ■

Proposição 13.8. *Sejam* $\boldsymbol{V}$ *um espaço vetorial sobre um corpo* $\boldsymbol{C}$ *e* $\{W_i\}_{i\in I}$ *uma cadeia de subespaços vetoriais de* $\boldsymbol{V}$ *(ou seja, para todos* $I, j \in I$*,* $W_I \subseteq W_j$ *ou* $W_j \subseteq W_i$*). Então*

$$W \coloneqq \bigcup_{i\in I} W_i$$

é um subespaço vetorial de $\boldsymbol{V}$*.*

Demonstração. Como, para todo $i \in I$, $\mathbf{0} \in W_i$, pois W_i é subespaço vetoriasl de $\boldsymbol{V}$, segue que $\mathbf{0} \in W$ e, portanto, W não é vazio. Agora, sejam $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$. Então existem $i, j \in I$ tais que $\boldsymbol{w}_1 \in W_i$ e $\boldsymbol{w}_2 \in W_j$. Nesse caso, $W_i \subseteq W_j$ ou $W_j \subseteq W_i$. Sem perda de generalidade, suponhamos o primeiro caso. Então segue que $\boldsymbol{w}_1 \in W_j$ e, portanto, $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W_j$, o que mostra que $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W$. Agora, seja $c \in C$ e notemos que, como W_i é subespaço vetorial de $\boldsymbol{V}$, segue que $c\boldsymbol{w}_1 \in W_i$. Logo $c\boldsymbol{w}_1 \in W$, o que mostra que W é subespaço vetorial de $\boldsymbol{V}$. ■

Definição 13.3. Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$, $W \subseteq V$ e $(W_i)_{i\in I}$ uma indexação do conjunto de todos subespaços vetoriais de $\boldsymbol{V}$ dos quais W é subconjunto. O *subespaço vetorial gerado por* W em $\boldsymbol{V}$ é o subespaço vetorial

$$\langle W \rangle \coloneqq \bigcap_{i\in I} W_i.$$

Nesse caso, dizemos que W é um *conjunto gerador* de $\langle W \rangle$ ou que W gera $\langle W \rangle$.

Proposição 13.9. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Então $\langle\emptyset\rangle = \{\mathbf{0}\}$.*

Demonstração. Como $\{\mathbf{0}\}$ é um subespaço vetorial de V e $\emptyset \subseteq \{\mathbf{0}\}$, segue que, se $\boldsymbol{v} \in \langle\emptyset\rangle$, então $\boldsymbol{v} \in \{\mathbf{0}\}$, o que implica $\boldsymbol{v} = \mathbf{0}$ e, portanto, que $\langle\emptyset\rangle = \{\mathbf{0}\}$. ■

13.2 Combinação Linear de Vetores

Definição 13.4. Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$ um conjunto finito tal que $W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$. Uma *combinação linear* de W em $\boldsymbol{V}$ é um vetor $\boldsymbol{v} \in V$ tal que existem $c_1, \ldots, c_n \in C$ satisfazendo

$$\boldsymbol{v} = \bigplus_{i=1}^{n} c_i \boldsymbol{w}_i.$$

Se W é um conjunto infinito, uma *combinação linear* de W é uma combinação linear de um subconjunto finito de W.

O vetor $\mathbf{0}$ é combinação linear de qualquer conjunto, pois é a soma vazia.

Teorema 13.10. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$ não vazio. Então $\langle W\rangle$ é o conjunto de todas as combinações lineares de W em $\boldsymbol{V}$.*

Demonstração. Consideremos, primeiro, o caso em que $W = \emptyset$. Nesse caso, $\langle W\rangle = \{\mathbf{0}\}$, e a única combinação linear de W é a soma vazia $\mathbf{0}$, o que mostra a igualdade dos conjuntos.

Agora, assumamos que $W \neq \emptyset$ e seja $(W_j)_{j\in J}$ uma indexação do conjunto de todos subespaços de $\boldsymbol{V}$ que contêm W. Primeiro, mostraremos que uma combinação linear de W em $\boldsymbol{V}$ está em $\langle W\rangle$. Seja $\boldsymbol{v} \coloneqq \bigplus_{i=1}^{n} c_i \boldsymbol{w}_i$ uma combinação linear de W em $\boldsymbol{V}$. Para todo $j \in J$, W_j é um subespaço vetorial de $\boldsymbol{V}$. Portanto, para todo $i \in \mathtt{I}_n$, segue que $c_i\boldsymbol{w_i} \in W_j$ e, então, que $\boldsymbol{v} \in W_j$. Logo $\boldsymbol{v} \in \langle W\rangle$.

Reciprocamente, mostraremos que o conjunto de todas combinações lineares de W em $\boldsymbol{V}$ é um subespaço vetorial de $\boldsymbol{V}$. Primeiro, notemos que $\mathbf{0}$ é uma combinação linear de W, pois, para todo $\boldsymbol{w} \in W$, vale $\mathbf{0} = 0\boldsymbol{w}$. Agora, sejam $\boldsymbol{v}_1 = \bigplus_{i=1}^{n} c_i\boldsymbol{w}_i$ e $\boldsymbol{v}_2 = \bigplus_{i=1}^{m} c'_i\boldsymbol{w}'_i$ combinações lineares de W em $\boldsymbol{V}$ e $c \in C$. Então, se definirmos, para todo $i \in \mathtt{I}_m$, $\boldsymbol{w}_{n+i} \coloneqq \boldsymbol{w}'_i$ e $c_{n+i} \coloneqq c'_i$ e, para todo $i \in \mathtt{I}_n$, $\overline{c}_i \coloneqq cc_i$, segue que

$$\boldsymbol{v}_1 + \boldsymbol{v}_2 = \bigplus_{i=1}^{n} c_i\boldsymbol{w}_i + \bigplus_{i=1}^{m} c'_i\boldsymbol{w}'_i = \bigplus_{i=1}^{n+m} c_i\boldsymbol{w}_i$$

e

$$c\boldsymbol{v}_1 = \bigplus_{i=1}^{n} (cc_i)\boldsymbol{w}_i = \bigplus_{i=1}^{n} \overline{c}_i\boldsymbol{w}_i$$

são combinações lineares de W em $\boldsymbol{V}$, o que implica que o conjunto de todas combinações lineares de W em $\boldsymbol{V}$ é um subespaço de $\boldsymbol{V}$. Assim, como $\langle W \rangle$ é subconjunto de todo conjunto que é subespaço vetorial de $\boldsymbol{V}$ contendo W, segue que o conjunto de todas combinações lineares de W em $\boldsymbol{V}$ é igual ao subespaço gerado por W. ■

Proposição 13.11. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$, $W \subseteq V$ e $\boldsymbol{v} \in \langle W \rangle$. Então existem $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in W$ distintos e $c_1, \ldots, c_n \in C$ tais que*

$$\boldsymbol{v} = \bigplus_{i=1}^{n} c_i \boldsymbol{w}_i.$$

Demonstração. Como $\boldsymbol{v} \in \langle W \rangle$, existem $\boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_m \in W$ e $c'_1, \ldots, c'_m \in C$ tais que $\boldsymbol{v} = \bigplus_{i=1}^{m} c'_i \boldsymbol{w}'_i$. Vamos particionar o conjunto dos índices $\mathtt{I}_m$ com a seguinte relação de equivalência: para todo $i, j \in \mathtt{I}_m$, $i \sim j$ se, e somente se, $\boldsymbol{w}'_i = \boldsymbol{w}'_j$. Essa relação é de equivalência pois a igualddade de vetores é uma relação de equivalência. Agora, seja n o número de classes de equivalências dessa relação. Para cada $i \in \mathtt{I}_n$, seja $j \in P_i$ e definimos os vetores $\boldsymbol{w}_i \coloneqq \boldsymbol{w}'_j$. Notemos que os vetores $\boldsymbol{w}_i$ estão bem definidos, não dependem do j, pois, se $k \in P_i$, então $\boldsymbol{w}_i = \boldsymbol{w}'_j = \boldsymbol{w}'_k$. Ainda, definimos os coeficientes $c_i \coloneqq \bigplus_{j \in P_i} c'_j$. Desse modo, segue que

$$\boldsymbol{v} = \bigplus_{i=1}^{m} c'_i \boldsymbol{w}'_i = \bigplus_{i=1}^{n} \bigplus_{j \in P_i} c'_j \boldsymbol{w}'_j = \bigplus_{i=1}^{n} \bigplus_{j \in P_i} c'_j \boldsymbol{w}_i = \bigplus_{i=1}^{n} c_i \boldsymbol{w}_i.$$

Por fim, notemos que os $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$ são distintos por definição, já que, se $\boldsymbol{w}_i = \boldsymbol{w}_j$ para $i, j \in \mathtt{I}_n$, então existem $k, l \in \mathtt{I}_m$ tais que $k \in P_i$, $l \in P_j$ e $\boldsymbol{w}_i = \boldsymbol{w}'_k$, $\boldsymbol{w}_j = \boldsymbol{w}'_l$. Mas isso implica $\boldsymbol{w}'_k = \boldsymbol{w}'_l$, o que implica $P_i = P_j$ e, portanto, $i = j$. ■

Definição 13.5 (Dependência Linear)**.** Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$. Dizemos que W é *linarmente dependente* em $\boldsymbol{V}$ se existem $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in W$ distintos e $c_1, \ldots, c_n \in C$ não nulos tais que

$$\boldsymbol{0} = \bigplus_{i=1}^{n} c_i \boldsymbol{w}_i.$$

Caso contrário, dizemos que W é *linearmente independente* em $\boldsymbol{V}$.

Proposição 13.12. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$. Então W é linearmente dependente se, e somente se, existe $\boldsymbol{w} \in W$ que é combinação linear de $W \setminus \{\boldsymbol{w}\}$ em $\boldsymbol{V}$.*

Demonstração. Suponhamos que W é linearmente dependente. Então existem vetores $\boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_n \in W$ distintos e $c'_1, \ldots, c'_n \in C$ não nulos tais que

$$\mathbf{0} = \bigplus_{i=1}^{n} c'_i \boldsymbol{w}'_i.$$

Como $c'_1, \ldots, c'_n$ são não nulos, então existe $j \in \mathtt{I}_n$ tal que $c'_j \neq 0$. Definindo $\boldsymbol{w}_i \coloneqq \boldsymbol{w}'_i$ se $1 \leq i < j$ e $\boldsymbol{w}_i \coloneqq \boldsymbol{w}'_{i-1}$ se $j < i \leq n$, e $c_i \coloneqq (c'_j)^{-1}(-c'_i)$ para todo $1 \leq i < j$ ou $j < i \leq n$, segue que

$$\boldsymbol{w}'_j = \bigplus_{i=1}^{j-1} (c'_j)^{-1}(-c'_i)\boldsymbol{w}'_i + \bigplus_{i=j+1}^{n} (c'_j)^{-1}(-c'_i)\boldsymbol{w}'_i = \bigplus_{i=1}^{n-1} c_i \boldsymbol{w}_i.$$

Por tanto, como $\boldsymbol{w}_i \in W \setminus \{\boldsymbol{w}'_j\}$ e $c_i \in C$ para todo $i \in \mathtt{I}_{n-1}$, $\boldsymbol{w}'_j$ é combinação linear de $W \setminus \{\boldsymbol{w}'_j\}$ em $\boldsymbol{V}$.

Reciprocamente, suponhamos que existe $\boldsymbol{w} \in W$ que é combinação linear de $W \setminus \{\boldsymbol{w}\}$ em $\boldsymbol{V}$. Então existem $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in W \setminus \{\boldsymbol{w}\}$ distintos e $c_1, \ldots, c_n \in C$ tais que

$$\boldsymbol{w} = \bigplus_{i=1}^{n} c_i \boldsymbol{w}_i.$$

Definindo $\boldsymbol{w}_{n+1} \coloneqq \boldsymbol{w}$ e $c_{n+1} \coloneqq -1$, segue que

$$\mathbf{0} = \bigplus_{i=1}^{n} c_i \boldsymbol{w}_i - \boldsymbol{w} = \bigplus_{i=1}^{n+1} c_i \boldsymbol{w}_i.$$

Então, como $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n+1}$ são distintos e $c_{n+1} = -1 \neq 0$, segue que W é linearmente dependente. ■

Proposição 13.13. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$. Então*

1. *$\emptyset$ é linearmente independente em $\boldsymbol{V}$;*
2. *Se $\mathbf{0} \in W$, então W é linearmente dependente em $\boldsymbol{V}$;*
3. *Se $W = \{\boldsymbol{v}\} \neq \{\mathbf{0}\}$, então W é linearmente independente em $\boldsymbol{V}$.*

Demonstração. 1. Suponha, por absurdo, que $\emptyset$ não é linearmente independente. Então existem $\boldsymbol{w_1}, \ldots, \boldsymbol{w_n} \in \emptyset$ distintos e $c_1, \ldots, c_n \in C$ não nulos tais que

$$\mathbf{0} = \bigplus_{i=1}^{n} c_i \boldsymbol{w_i}.$$

Mas $\boldsymbol{w_1}, \ldots, \boldsymbol{w_n} \in \emptyset$ é um absurdo.

2. Seja $c \in C \setminus \{0\}$. Então, como $\mathbf{0} = c\mathbf{0}$, segue que W é linearmente dependente em $\boldsymbol{V}$.

3. Se $\mathbf{0} = c\boldsymbol{v}$, como $\boldsymbol{v} \neq \mathbf{0}$, segue que $c = 0$, o que mostra que W é linearmente independente em $\boldsymbol{V}$. ■

Proposição 13.14. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$. Então W é linearmente independente em $\boldsymbol{V}$ se, e somente se, para toda combinação linear $\boldsymbol{v} = \bigplus_{i=1}^{n} c_i\boldsymbol{w}_i \neq \mathbf{0}$ de W em $\boldsymbol{V}$ tal que $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$ são distintos e não nulos, então $c_1, \ldots, c_n$ são únicos.*

Demonstração. Primeiro, suponhamos que W é linearmente dependente em $\boldsymbol{V}$. Então existem $\boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_{n'} \in W$ distintos e $c'_1, \ldots, c'_{n'} \in C$ não nulos tais que

$$\mathbf{0} = \bigplus_{i=1}^{n'} c'_i\boldsymbol{w}'_i.$$

Nesse caso, seja $\boldsymbol{v} \in \langle W \rangle$. Se $\boldsymbol{v} = \mathbf{0}$, então segue que
..... . Se $\boldsymbol{v} \neq \mathbf{0}$

■

Proposição 13.15. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $\{W_i\}_{i \in I}$ uma cadeia de conjuntos linearmente independentes em $\boldsymbol{V}$ (ou seja, para todos $i, j \in I$, $W_i \subseteq W_j$ ou $W_j \subseteq W_i$). Então*

$$W \coloneqq \bigcup_{i \in I} W_i$$

é um conjunto linearmente independente em $\boldsymbol{V}$.

Demonstração. Como, para todo $i \in I$, $\mathbf{0} \in W_i$, segue que $\mathbf{0} \in W$ e, portanto, W não é vazio. Agora, sejam $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$. Então existem $i, j \in I$ tais que $\boldsymbol{w}_1 \in W_i$ e $\boldsymbol{w}_2 \in W_j$. Nesse caso, $W_i \subseteq W_j$ ou $W_j \subseteq W_i$. Sem perda de generalidade, suponhamos o primeiro caso. Então segue que $\boldsymbol{w}_1 \in W_j$ e, portanto, $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W_j$, o que mostra que $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W$. Agora, seja $c \in C$ e notemos que, como W_i é subespaço vetorial de $\boldsymbol{V}$, segue que $c\boldsymbol{w}_1 \in W_i$. Logo $c\boldsymbol{w}_1 \in W$, o que mostra que W é subespaço vetorial de $\boldsymbol{V}$. ■

13.3 Soma de Subespaços Vetoriais

Definição 13.6. Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $(W_i)_{i \in I}$ uma família de subespaços vetoriais de $\boldsymbol{V}$. A *soma* de $(W_i)_{i \in I}$ é o subespaço vetorial gerado pela união de W_i. Denotamos

$$\bigplus_{i \in I} W_i \coloneqq \left\langle \bigcup_{i \in I} W_i \right\rangle.$$

Caso $(W_i)_{i\in I}$ seja uma família finita, escrevemos $W_1 + \cdots + W_n$.

Definição 13.7. Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Uma *soma direta* é a soma de uma família $(W_i)_{i\in I}$ de subespaços vetoriais de $\boldsymbol{V}$ tal que $W_i \cap W_j = \{\boldsymbol{0}\}$ para todo $i, j \in I$, $i \neq j$. Nesse caso, denotamos

$$\bigoplus_{i\in I} W_i \coloneqq \left\langle \bigcup_{i\in I} W_i \right\rangle.$$

Caso $(W_i)_{i\in I}$ seja uma família finita, escrevemos $W_1 \oplus \cdots \oplus W_n$.

Proposição 13.16. *Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W_1, \ldots, W_n$ subespaços vetoriais de $\boldsymbol{V}$ tais que $V = \sum_{i=1}^{n} W_i$. Então*

$$V = \bigoplus_{i=1}^{n} W_i$$

se, e somente se, para todo $\boldsymbol{v} \in V$, existem únicos $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_n \in W_n$ tais que

$$\boldsymbol{v} = \sum_{i=1}^{n} \boldsymbol{w}_i.$$

Demonstração. Mostraremos, primeiro, que se V é soma direta de $W_1, \ldots, W_n$, então todo vetor de V é soma única de vetores de $W_1, \ldots, W_n$. A demontração será por indução em n. O caso base é trivial, pois, se $V = W_1$, então, para todo $\boldsymbol{v} \in V$, $\boldsymbol{v} \in W_1$. Agora, suponhamos que a proposição vale para todo natural menor ou igual a n. Sejam $W_1, \ldots, W_{n+1}$ subespaços vetoriais de V tais que $V = \sum_{i=1}^{n+1} W_i$. Então existem $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_{n+1} \in W_{n+1}$ tais que

$$\boldsymbol{v} = \sum_{i=1}^{n+1} \boldsymbol{w}_i.$$

Suponhamos que existam $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_{n+1} \in W_{n+1}$ tais que

$$\boldsymbol{v} = \sum_{i=1}^{n+1} \boldsymbol{w}'_i.$$

Então

$$\boldsymbol{v} = \sum_{i=1}^{n+1} \boldsymbol{w}_i = \sum_{i=1}^{n+1} \boldsymbol{w}'_i,$$

o que implica

$$\sum_{i=1}^{n} (\boldsymbol{w}_i - \boldsymbol{w}'_i) = \boldsymbol{w}'_{n+1} - \boldsymbol{w}_{n+1}.$$

Como, para todo $i \in \mathtt{I}_{n+1}$, $w_i, w_i' \in W_i$, segue que $\boldsymbol{w}_i - \boldsymbol{w}_i' \in W_i$. Definamos $W := \bigcup_{i=1}^{n} W_i$. Assim, segue que

$$\dotplus_{i=1}^{n}(\boldsymbol{w}_i - \boldsymbol{w}_i') \in \langle W \rangle$$

e

$$\boldsymbol{w}_{n+1}' - \boldsymbol{w}_{n+1} \in W_{n+1}.$$

Ainda, como V é soma direta de $W_1, \ldots, W_{n+1}$, então segue que $W \cap W_{n+1} = \{\mathbf{0}\}$. Portanto concluímos que

$$\dotplus_{i=1}^{n}(\boldsymbol{w}_i - \boldsymbol{w}_i') = \boldsymbol{w}_{n+1}' - \boldsymbol{w}_{n+1} = \mathbf{0}.$$

Assim, concluímos que $\boldsymbol{w}_{n+1}' = \boldsymbol{w}_{n+1}$ e que

$$\dotplus_{i=1}^{n} \boldsymbol{w}_i = \dotplus_{i=1}^{n} \boldsymbol{w}_i'.$$

Mas notemos que

$$\langle \boldsymbol{W} \rangle = (\langle W \rangle, +|_{\langle W \rangle \times \langle W \rangle}, \cdot|_{\langle W \rangle \times \langle W \rangle})$$

é um espaço vetorial e $W_1, \ldots, W_n$ são subespaços vetoriais de $\langle \boldsymbol{W} \rangle$ tais que $\langle W \rangle = \dotplus_{i=1}^{n} W_i$. Portanto, pela hipótese de indução, segue que, para todo $i \in \mathtt{I}_n$, $\boldsymbol{w}_i = \boldsymbol{w}_i'$ e, portanto, concluímos que existem únicos $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_{n+1} \in W_{n+1}$ tais que

$$\boldsymbol{v} = \dotplus_{i=1}^{n+1} \boldsymbol{w}_i.$$

Suponhamos, então, que todo vetor de V é soma de únicos vetores de $W_1, \ldots, W_n$. Sejam $i, j \in \mathtt{I}_n$, $i \neq j$, e $\boldsymbol{v} \in W_i \cap W_j$. Como $\boldsymbol{v} \in V$, segue que existem únicos $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_n \in W_n$ tais que

$$\boldsymbol{v} = \dotplus_{k=1}^{n} \boldsymbol{w}_k.$$

Sem perda de generalidade, suponhamos $i < j$. Notemos que

$$\boldsymbol{v} = \dotplus_{i=1}^{n} \boldsymbol{w}_i = \dotplus_{k=1}^{i-1} \boldsymbol{w}_k + (\boldsymbol{w}_i + \boldsymbol{v}) + \dotplus_{k=i+1}^{j-1} \boldsymbol{w}_k + (\boldsymbol{w}_j - \boldsymbol{v}) + \dotplus_{k=j+1}^{n} \boldsymbol{w}_k.$$

Como $\boldsymbol{v} \in W_i \cap W_j$, segue que $(\boldsymbol{w}_i + \boldsymbol{v}) \in W_i$ e $(\boldsymbol{w}_j - \boldsymbol{v}) \in W_j$ e, portanto, como $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_n \in W_n$ são únicos, segue que $(\boldsymbol{w}_i + \boldsymbol{v}) = \boldsymbol{w}_i$ e $(\boldsymbol{w}_j - \boldsymbol{v}) = \boldsymbol{w}_j$; ou seja, $\boldsymbol{v} = \mathbf{0}$. Logo V é soma direta de $W_1, \ldots, W_n$. ■

13.4 Bases de Espaços Vetoriais

Definição 13.8. Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Uma *base* de $\boldsymbol{V}$ é um conjunto $B \subseteq V$ linearmente independente em $\boldsymbol{V}$ que gera V; ou seja, $V = \langle B \rangle$. Uma base de um subespaço vetorial W de $\boldsymbol{V}$ é uma base do espaço vetorial $\boldsymbol{W} = (W, +|_{W\times W}, \cdot|_{W\times W})$.

Teorema 13.17. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Então existe base B de $\boldsymbol{V}$ e, se L é um conjunto linearmente independente em $\boldsymbol{V}$, existe uma base B de $\boldsymbol{V}$ tal que $L \subseteq B$.*

Demonstração. A afirmação de que todo espaço vetorial tem uma base é consequência da segunda afirmação porque, tomando $L = \emptyset$, sabemos que L é linearmente independente e, portanto, existe base B de $\boldsymbol{V}$ que contém $\emptyset$. Demonstraremos a segunda afirmação.

Sejam L um conjunto linearmente independente em $\boldsymbol{V}$ e P o conjunto dos subconjuntos $S \subseteq V$ tais que $L \subseteq S$ e S é linearmente independente em $\boldsymbol{V}$. Então $(P, \subseteq)$ é um conjunto parcialmente ordenado com a contenção de conjuntos usual. Agora, seja $(S_i)_{i\in I}$ uma cadeia de $(P, \subseteq)$. Consideremos o conjunto $S \coloneqq \bigcup_{i\in I} S_i$. Como $L \subseteq S_i$ para todo $i \in I$, então $L \subseteq S$. Devemos mostrar que S é um conjunto linearmente independente em $\boldsymbol{V}$. Para isso, seja $M \subseteq S$ subconjunto finito de S. Como $(S_i)_{i\in I}$ é uma cadeia, existe $i \in I$ tal que $M \subseteq S_i$. Mas, como S_i é linearmente independente, então M também o é e, portanto, S é linearmente independente. Logo S é um limitante superior da cadeia. Concluímos, portanto, que existe um elemento maximal B de $(P, \subseteq)$ que, por definição de P, é linearmente independente e $L \subseteq B$.

Vamos mostrar que B é base de $\boldsymbol{V}$. Devemos mostrar que B gera V, ou seja, que $V = \langle B \rangle$. Seja $\boldsymbol{v} \in V$ e suponhamos, por absurdo, que $\boldsymbol{v} \notin \langle B \rangle$. Então, em particular, $\boldsymbol{v} \notin B$; logo $B \subset B \cup \{\boldsymbol{v}\}$. Concluiremos que $B \cup \{\boldsymbol{v}\}$ é linearmente independente, o que constradiz a maximalidade de B. Seja S um subconjunto finito de $B \cup \{\boldsymbol{v}\}$. Se $\boldsymbol{v} \notin S$, então $S \subseteq B$ e, portanto, é linearmente independente, pois B o é; se $\boldsymbol{v} \in S$, sejam $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} \coloneqq S \setminus \{\boldsymbol{v}\} \subseteq B$ e $c, c_1, \ldots, c_n \in C$ tais que

$$c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n - c\boldsymbol{v} = \boldsymbol{0}.$$

Como $\boldsymbol{v} \notin \langle B \rangle$, então $c = 0$, pois, caso contrário, teríamos

$$\boldsymbol{v} = \frac{c_1}{c}\boldsymbol{v}_1 + \cdots + \frac{c_n}{c}\boldsymbol{v}_n.$$

Assim, segue que $c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n = \boldsymbol{0}$. Mas $S \setminus \{\boldsymbol{v}\} \subseteq B$ é linearmente independente, pois B o é, o que implica que $c_1 = \cdots = c_n = 0$ e, portanto, S é linearmente independente. Com isso, concluímos que $B \cup \{\boldsymbol{v}\}$ é linearmente independente, pois

todo subconjunto finito é, e isso contradiz a maximalidade de B. Por esse absurdo, segue que $\boldsymbol{v} \in \langle B \rangle$ e, portanto, que $V = \langle B \rangle$. Concluímos que B é uma base de $\boldsymbol{V}$ que contém L. ■

Proposição 13.18. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W, W' \subseteq V$ conjuntos finitos. Se W é linearmente independente em $\boldsymbol{V}$ e W' gera V, então $|W| \leq |W'|$.*

Demonstração. Se $W = \emptyset$, então $0 = |W'| \leq |W|$. Caso contrário, seja $|W| = n$ e $(\boldsymbol{w}_i)_{i \in \mathtt{I}_n}$ uma indexação de W. Suponhamos, por absurdo, que $W' = \emptyset$. Então, como W' gera V e $\langle W' \rangle = \{\mathbf{0}\}$, segue que $V = \{\mathbf{0}\}$, o que é absurdo, pois isso implica que $W = \{\mathbf{0}\}$, que é um conjunto linearmente dependente. Então $W' \neq \emptyset$. Seja $|W'| = m$ e $(\boldsymbol{w}'_i)_{i \in \mathtt{I}_m}$ uma indexação de W'. Queremos mostrar que $n \leq m$. Suponhamos, por absurdo, que $m < n$. Como W é linearmente independente, então, para todo $i \in \mathtt{I}_n$, $\boldsymbol{w}_i \neq \mathbf{0}$. Como W' gera V, existem $c_1, \ldots, c_m \in C$ tais que

$$\boldsymbol{w}_1 = \bigplus_{i=1}^{m} c_i \boldsymbol{w}'_i,$$

e os $c_1, \ldots, c_m \in C$ não são todos nulos pois, caso contrário, teríamos $\boldsymbol{w}_1 = \mathbf{0}$. Assim, suponhamos, sem perda de generalidade, que $c_1 \neq 0$. Então

$$\boldsymbol{w}'_1 = c_1^{-1} \boldsymbol{w}_1 - \bigplus_{i=2}^{m} c_1^{-1} c_i \boldsymbol{w}'_i.$$

Seja $W_1 \coloneqq \{\boldsymbol{w}_1, \boldsymbol{w}'_2, \ldots, \boldsymbol{w}'_m\}$. Como W' gera V e todo elemento de W' pode ser escrito como combinação linear de W_1, W_1 gera V. Assim, analogamente, podemos escrever $\boldsymbol{w}_2$ como combinação linear de W_1, como $\boldsymbol{w}_2 \neq \mathbf{0}$, segue que nem todo os coeficientes da combinação linear são nulos. Mais ainda, se somente o coeficiente de $\boldsymbol{w}_1$ é não nulo, então $\boldsymbol{w}_2$ é múltiplo de $\boldsymbol{w}_1$, o que contradiz a independência linear de W. Portanto, deve existir um coeficiente dos $\boldsymbol{w}'_2, \ldots, \boldsymbol{w}'_m$ não nulo. Assim, sem perda de generalidade, suponhamos que o coeficiente de $\boldsymbol{w}'_2$ é não nulo. Então, como no caso anterior, $\boldsymbol{w}'_2$ pode ser escrito como combinação linear de $\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}'_3, \ldots, \boldsymbol{w}'_m$ e segue que o conjunto $W_2 \coloneqq \{\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}'_3, \ldots, \boldsymbol{w}'_m\}$ gera V. Repetindo o processo, que termina porque $m < n$ são finitos, achamos o conjunto $W_m \coloneqq \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$, que gera V e é um subconjunto próprio de W, pois $m < n$. Mas isso implica que $\boldsymbol{w}_{m+1} \in W$ é uma combinação linear de W_m em $\boldsymbol{V}$, o que implica que W é linearmente dependente, uma contradição. Logo $m \leq n$. ■

Teorema 13.19. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Se $B, B' \subseteq V$ são bases de $\boldsymbol{V}$, então $|B| = |B'|$.*

Demonstração. Primeiro, vamos mostrar que não ocorre o caso de uma base ser um conjunto finito e outra ser um conjunto infinito. Suponhamos, sem perda de generalidade, que B é um conjunto finito com $|B| = n$, $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\} \coloneqq B$, e B' é um conjunto infinito. Seja $i \in \mathtt{I}_n$. Como $\boldsymbol{b}_i \in V$ e B' gera V, segue que existem $\boldsymbol{b}_{i,1}, \ldots, \boldsymbol{b}_{i,n_i} \in B'$ e $c_{i,1}, \ldots, c_{i,n_i} \in C$ tais que

$$\boldsymbol{b}_i = \bigplus_{j=1}^{n_i} c_{i,j}\boldsymbol{b}_{i,j}.$$

Notemos que o conjunto de todos esses $\boldsymbol{b}_{i,j}$ é $B'' \coloneqq \bigcup_{i=1}^{n}\{\boldsymbol{b}_{i,j} : j \in \mathtt{I}_{n_i}\}$, que é um subconjunto finito de B' e, portanto, um subconjunto próprio. Assim, como $B'' \subset B'$, existe $\boldsymbol{b} \in B' \setminus B''$. Como $\boldsymbol{b} \in V$ e B é base, segue que existem $c_1, \ldots, c_n \in C$ tais que $\boldsymbol{b} = \bigplus_{i=1}^{n} c_i\boldsymbol{b}_i$. Mas então

$$\boldsymbol{b} = \bigplus_{i=1}^{n} c_i\boldsymbol{b}_i = \bigplus_{i=1}^{n} c_i \bigplus_{j=1}^{n_i} c_{i,j}\boldsymbol{b}_{i,j} = \bigplus_{i=1}^{n}\bigplus_{j=1}^{n_i} c_i c_{i,j}\boldsymbol{b}_{i,j},$$

o que mostra que $\boldsymbol{b} \in B'$ pode ser escrito como uma combinação linear de $B' \setminus \{\boldsymbol{b}\}$ em $\boldsymbol{V}$; ou seja, B' não é linearmente independente, o que é um absurdo. Assim, existem dois casos a serem considereados; o primeiro em que ambas as bases são conjuntos finitos e o outro em que ambas são conjuntos infinitos.

Suponhamos, no primeiro caso, que B e B' são conjuntos finitos com $|B| = n$ e $|B'| = m$. Como B é linearmente independente e B' gera V, segue que $|B| \leq |B'|$. Reciprocamente, como B' é linearmente independente e B gera V, segue que $|B'| \leq |B|$. Assim, segue que $|B| = |B'|$. Agora, suponhamos que B e B' são conjuntos infinitos.

TERMINAR ■

Definição 13.9. Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $B \subseteq V$ uma base $\boldsymbol{V}$. A *dimensão* de $\boldsymbol{V}$ é o número ordinal $\dim \boldsymbol{V} \coloneqq |B|$.

13.5 Transformações Lineares

Definição 13.10. Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços vetoriais sobre um corpo $\boldsymbol{C}$. Uma *transformação linear* de $\boldsymbol{V}$ em $\boldsymbol{W}$ é uma função $T : V \to W$ que satisfaz

1. (Aditividade) $\forall \boldsymbol{v}_1, \boldsymbol{v}_2 \in V \qquad T(\boldsymbol{v}_1 + \boldsymbol{v}_2) = T(\boldsymbol{v}_1) + T(\boldsymbol{v}_2)$;
2. (Homogeneidade) $\forall c \in C, \forall \boldsymbol{v} \in V \qquad T(c\boldsymbol{v}) = cT(\boldsymbol{v})$.

O conjunto das transformações lineares de $\boldsymbol{V}$ em $\boldsymbol{W}$ é o conjunto $\mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$ e o conjunto das tranformações lineares de $\boldsymbol{V}$ em $\boldsymbol{V}$ é o conjunto $\mathcal{L}(\boldsymbol{V}) \coloneqq \mathcal{L}(\boldsymbol{V}; \boldsymbol{V})$.

É imediato da definição que as duas propriedades são equivalentes à seguinte propriedade

$$\text{(Linearidade) } \forall c \in C, \forall \boldsymbol{v}_1, \boldsymbol{v}_2 \in V \qquad T(\boldsymbol{v}_1 + c\boldsymbol{v}_2) = T(\boldsymbol{v}_1) + cT(\boldsymbol{v}_2).$$

Proposição 13.20. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços vetoriais sobre um corpo $\boldsymbol{C}$ e $T \in \mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$. Então*

1. *(Linearidade generalizada) Para todos $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in V$ e $c_1, \ldots, c_n \in C$,*

$$T\left(\bigplus_{i=1}^{n} c_i \boldsymbol{v}_i\right) = \bigplus_{i=1}^{n} c_i T(\boldsymbol{v}_i).$$

2. *$T(\mathbf{0}) = \mathbf{0}$;*

3. *$T(-\boldsymbol{v}) = -T(\boldsymbol{v})$.*

Proposição 13.21. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços vetoriais sobre um corpo $\boldsymbol{C}$ e $T \in \mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$. Então*

Proposição 13.22. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços vetoriais sobre um corpo $\boldsymbol{C}$. Então $\mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$ é um subespaço vetorial de $\boldsymbol{W}^{\boldsymbol{V}}$.*

Demonstração. Primeiro, sejam $T_1, T_2 \in \mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$. Então, para todos $c \in C$ e $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$,

$$\begin{aligned}(T_1 + T_2)(\boldsymbol{v}_1 + c\boldsymbol{v}_2) &= T_1(\boldsymbol{v}_1 + c\boldsymbol{v}_2) + T_2(\boldsymbol{v}_1 + c\boldsymbol{v}_2) \\ &= T_1(\boldsymbol{v}_1) + cT_1(\boldsymbol{v}_2) + T_2(\boldsymbol{v}_1) + cT_2(\boldsymbol{v}_2) \\ &= T_1(\boldsymbol{v}_1) + T_2(\boldsymbol{v}_1) + cT_1(\boldsymbol{v}_2) + cT_2(\boldsymbol{v}_2) \\ &= (T_1 + T_2)(\boldsymbol{v}_1) + c(T_1 + T_2)(\boldsymbol{v}_2).\end{aligned}$$

Agora, sejam $c' \in C$ e $T \in \mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$. Então

$$\begin{aligned}(c'T)(\boldsymbol{v}_1 + c\boldsymbol{v}_2) &= c'T(\boldsymbol{v}_1 + c\boldsymbol{v}_2) \\ &= c'(T(\boldsymbol{v}_1) + cT(\boldsymbol{v}_2)) \\ &= c'T(\boldsymbol{v}_1) + c'cT(\boldsymbol{v}_2) \\ &= (c'T)(\boldsymbol{v}_1) + c(c'T)(\boldsymbol{v}_2).\end{aligned}$$

Portanto concluímos que $\mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$ é um subespaço vetorial de $\boldsymbol{W}^{\boldsymbol{V}}$. ■

Proposição 13.23. *Sejam $\boldsymbol{V}_1$, $\boldsymbol{V}_2$ e $\boldsymbol{V}_3$ espaços vetoriais sobre um corpo $\boldsymbol{C}$. Se $T_1 \in \mathcal{L}(\boldsymbol{V}_1; \boldsymbol{V}_2)$, $T_2 \in \mathcal{L}(\boldsymbol{V}_2; \boldsymbol{V}_3)$, então $T_2 \circ T_1 \in \mathcal{L}(\boldsymbol{V}_1; \boldsymbol{V}_3)$.*

Demonstração. Sejam $c \in C$ e $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$. Então

$$\begin{aligned}(T_2 \circ T_1)(\boldsymbol{v}_1 + c\boldsymbol{v}_2) &= T_2(T_1(\boldsymbol{v}_1 + c\boldsymbol{v}_2)) \\ &= T_2(T_1(\boldsymbol{v}_1) + cT_1(\boldsymbol{v}_2)) \\ &= T_2(T_1(\boldsymbol{v}_1)) + cT_2(T_1(\boldsymbol{v}_2)) \\ &= (T_2 \circ T_1)(\boldsymbol{v}_1) + c(T_2 \circ T_1)(\boldsymbol{v}_2),\end{aligned}$$

o que mostra que $T_2 \circ T_1$ é linear. ■

Proposição 13.24. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços vetoriais sobre um corpo $\boldsymbol{C}$ e $T \in \mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$. Se T é invertível, então $T^{-1} \in \mathcal{L}(\boldsymbol{W}; \boldsymbol{V})$.*

Demonstração. Seja $T \in \mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$. Se T é invertível, $T^{-1} \in V^W$ e, para todos $c \in C$ e $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$, existem $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ tais que $T(\boldsymbol{v}_1) = \boldsymbol{w}_1$ e $T(\boldsymbol{v}_2) = \boldsymbol{w}_2$ e segue que

$$\begin{aligned}T^{-1}(\boldsymbol{w}_1 + c\boldsymbol{w}_2) &= T^{-1}(T(\boldsymbol{v}_1) + cT(\boldsymbol{v}_2)) \\ &= T^{-1}(T(\boldsymbol{v}_1 + c\boldsymbol{v}_2)) \\ &= \boldsymbol{v}_1 + c\boldsymbol{v}_2 \\ &= T^{-1}(\boldsymbol{w}_1) + cT^{-1}(\boldsymbol{w}_2),\end{aligned}$$

o que mostra que T^{-1} é linear. ■

Proposição 13.25. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços vetoriais sobre um corpo $\boldsymbol{C}$, $B_V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ base de $\boldsymbol{V}$, $B_W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$ base de $\boldsymbol{W}$ e $T \in \mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$. Então, para todo $\boldsymbol{v} \in V$, existem únicos $c_1, \ldots, c_m \in C$ tais que*

$$T(\boldsymbol{v}) = \bigplus_{i=1}^{m} c_j \boldsymbol{w}_j.$$

Demonstração. Primeiro demonstraremos a existência. Sabemos que, como B_V é base de V, então existem únicos $a_1, \ldots, a_n \in C$ tais que $\boldsymbol{v} = \bigplus_{i=1}^{n} a_i \boldsymbol{v}_i$. Mas, como T é linear, então

$$T(\boldsymbol{v}) = T\left(\bigplus_{i=1}^{n} a_i \boldsymbol{v}_i\right) = \bigplus_{i=1}^{n} a_i T(\boldsymbol{v}_i).$$

Agora, como B_W é base de $\boldsymbol{W}$, para cada $i \in \{1, \ldots, n\}$ existem únicos $b_{i1}, \ldots, b_{im} \in C$ tais que $T(\boldsymbol{v}_i) = \bigplus_{j=1}^{m} b_{ij} \boldsymbol{w}_j$. Assim, definindo $c_j \coloneqq \bigplus_{i=1}^{n} a_i b_{ij}$, segue que

$$T(\boldsymbol{v}) = \bigplus_{i=1}^{n} a_i \left(\bigplus_{j=1}^{m} b_{ij} \boldsymbol{w}_j\right) = \bigplus_{j=1}^{m} \left(\bigplus_{i=1}^{n} a_i b_{ij}\right) \boldsymbol{w}_j = \bigplus_{j=1}^{m} c_j \boldsymbol{w}_j.$$

■

.

13.6 Representação Matricial de Espaços Vetoriais e Transformações Lineares

Definição 13.11. Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $B = \{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ uma base de $\boldsymbol{V}$. Seja $\boldsymbol{v} \in V$. A *matriz de coordenadas* de $\boldsymbol{v}$ com respeito à base B é a matriz

$$[\boldsymbol{v}]_B \coloneqq [c_i]_{n\times 1} = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$$

tal que $\boldsymbol{v} = \bigplus_{i=1}^{n} c_i \boldsymbol{b}_i$.

Proposição 13.26. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $B = \{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ uma base de $\boldsymbol{V}$. Então*

1. $\forall \boldsymbol{v}, \boldsymbol{w} \in V \qquad [\boldsymbol{v}]_B + [\boldsymbol{w}]_B = [\boldsymbol{v} + \boldsymbol{w}]_B.$
2. $\forall c \in C, \boldsymbol{v} \in V \qquad c[\boldsymbol{v}]_B = [c\boldsymbol{v}]_B.$

13.7 Espaços Vetoriais Normados

Definição 13.12. Seja $\boldsymbol{V}$ um espaço vetorial real. Uma *norma em* $\boldsymbol{V}$ é uma função $\|\cdot\| : V \to \mathbb{R}$ tal que

1. $\forall \boldsymbol{v} \in V, \forall c \in \mathbb{R} \qquad \|c\boldsymbol{v}\| = |c| \, \|\boldsymbol{v}\|$;
2. $\forall \boldsymbol{v}_1, \boldsymbol{v}_2 \in V \qquad \|\boldsymbol{v}_1 + \boldsymbol{v}_2\| \leq \|\boldsymbol{v}_1\| + \|\boldsymbol{v}_2\|$;
3. $\|\boldsymbol{v}\| = 0 \Rightarrow \boldsymbol{v} = \boldsymbol{0}$.

Proposição 13.27. *Sejam* $\boldsymbol{V}$ *um espaço vetorial real e* $\|\cdot\|$ *uma norma em* $\boldsymbol{V}$. *Então*

1. $\|\boldsymbol{0}\| = 0$
2. $\|-\boldsymbol{v}\| = \|\boldsymbol{v}\|$
3. $\forall \boldsymbol{v} \in V \qquad 0 \leq \|\boldsymbol{v}\|$.

13.8 Produto e Soma Catogóricas de Espaços Vetoriais

13.8.1 Produto

Definição 13.13. Seja $(\boldsymbol{V_i})_{i\in I} = ((V_i, +_i, \cdot_i))_{i\in I}$ uma família de espaços vetoriais sobre um corpo $\boldsymbol{C}$. O *produto categórico* de $(\boldsymbol{V_i})_{i\in I}$ é a tripla

$$\prod_{i\in I} \boldsymbol{V_i} = (V, +, \cdot),$$

em que $V = \prod_{i\in I} V_i$,

$$\begin{aligned} + : V \times V &\to V \\ (v_1, v_2) &\mapsto ((v_1)_i +_i (v_2)_i)_{i\in I} \end{aligned}$$

e

$$\begin{aligned} \cdot : C \times V &\to V \\ (c, v) &\mapsto (c \cdot_i v_i)_{i\in I}. \end{aligned}$$

Proposição 13.28. *Seja $(\boldsymbol{V_i})_{i\in I} = ((V_i, +_i, \cdot_i))_{i\in I}$ uma família de espaços vetoriais sobre um corpo $\boldsymbol{C}$. Então $\prod_{i\in I} \boldsymbol{V_i} = (V, +, \cdot)$ é um espaço vetorial sobre $\boldsymbol{C}$.*

Demonstração. 1. $(V, +)$ é um grupo pois tem a mesma operação do produto de grupos (9.28).

2. Seja $v \in V$. Então
$$1v = (1v_i)_{i\in I} = (v_i)_{i\in I} = v.$$
Sejam $c_1, c_2 \in C$ e $v \in V$. Então
$$\begin{aligned} (c_1c_2)v &= ((c_1c_2)v_i)_{i\in I} \\ &= (c_1(c_2v_i))_{i\in I} \\ &= c_1(c_2v_i)_{i\in I} \\ &= c_1(c_2v). \end{aligned}$$

3. (Distributividades) Sejam $c \in C$ e $v, v' \in V$. Então
$$\begin{aligned} c(v + v') &= c(v_i + v'_i)_{i\in I} \\ &= (c(v_i + v'_i))_{i\in I} \\ &= (cv_i + cv'_i)_{i\in I} \\ &= (cv_i)_{i\in I} + (cv'_i)_{i\in I} \\ &= cv + cv'. \end{aligned}$$

Sejam $c_1, c_2 \in C$ e $v \in V$. Então

$$\begin{aligned}(c_1 + c_2)v &= ((c_1 + c_2)v_i)_{i\in I} \\ &= (c_1 v_i + c_2 v_i)_{i\in I} \\ &= (c_1 v_i)_{i\in I} + (c_2 v_i)_{i\in I} \\ &= c_1 v + c_2 v.\end{aligned}$$

■

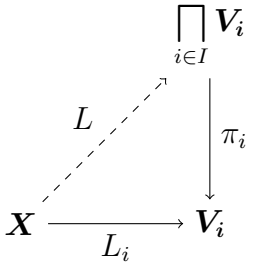
Proposição 13.29. *Seja $(\boldsymbol{V_i})_{i\in I} = ((V_i, +_i, \cdot_i))_{i\in I}$ uma família de espaços vetoriais sobre um corpo $\boldsymbol{C}$. Para todo $i \in I$, a projeção canônica $\pi_i : \prod_{i\in I} \boldsymbol{V_i} \to \boldsymbol{V_i}$ é uma transformação linear.*

Demonstração. Sejam $c \in C$ e $v, v' \in \prod_{i\in I} V_i$. Então

$$\pi_i(v + cv') = \pi_i((v_i + cv'_i)_{i\in I}) = v_i + cv'_i = \pi_i(v) + c\pi_i(v').$$

■

Proposição 13.30 (Propriedade Universal)**.** *Sejam $(\boldsymbol{V_i})_{i\in I}$ uma família de espaços vetoriais sobre um corpo $\boldsymbol{C}$, $\boldsymbol{X}$ um espaço vetorial sobre $\boldsymbol{C}$ e, para todo $i \in I$, $L_i : \boldsymbol{X} \to \boldsymbol{V_i}$ uma transformação linear. Então existe única transformação linear $L : \boldsymbol{X} \to \prod_{i\in I} \boldsymbol{V_i}$ tal que, para todo $i \in I$, $\pi_i \circ L = L_i$ (o diagrama comuta).*



Demonstração. Defina a função

$$\begin{aligned}L : X &\to \prod_{i\in I} V_i \\ x &\mapsto (L_i(x))_{i\in I}.\end{aligned}$$

Da propriedade universal para conjuntos, L é a única função de X para $\bigtimes_{i\in I} \boldsymbol{V_i}$ tal que, para todo $i \in I$, $\pi_i \circ L = L_i$. Falta mostrar que L é transformação linear. Sejam $c \in C$ e $x_1, x_2 \in V$. Então

$$\begin{aligned}L(x_1 + cx_2) &= (L_i(x_1 + cx_2))_{i\in I} \\ &= (L_i(x_1) + cL_i(x_2))_{i\in I} \\ &= (L_i(x_1))_{i\in I} + c(L_i(x_2))_{i\in I} \\ &= L(x_1) + cL(x_2).\end{aligned}$$

■

13.8.2 Soma (Coproduto)

Definição 13.14. Seja $(\boldsymbol{V_i})_{i\in I} = ((V_i, +_i, \cdot_i))_{i\in I}$ uma família de espaços vetoriais. A *soma categórica* de $(\boldsymbol{V_i})_{i\in I}$ é

$$\bigsqcup_{i\in I} \boldsymbol{V_i} = (V, +, \cdot),$$

em que $V = \{(v_i)_{i\in I} \in \bigsqcap_{i\in I} V_i \mid \exists J \subseteq I \qquad |J| < |\mathbb{N}| \quad \text{e} \quad v_i \neq 0\}$,

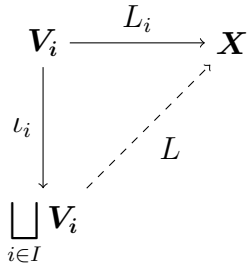
$$\begin{aligned} + : V \times V &\to V \\ (v_1, v_2) &\mapsto ((v_1)_i +_i (v_2)_i)_{i\in I} \end{aligned}$$

e

$$\begin{aligned} \cdot : C \times V &\to V \\ (c, v) &\mapsto (c(v)_i)_{i\in I}. \end{aligned}$$

Observe que, se $|I| < |\mathbb{N}|$, então $\bigsqcap_{i\in I} \boldsymbol{V_i} = \bigsqcup_{i\in I} \boldsymbol{V_i}$.

Proposição 13.31 (Propriedade Universal)**.** *Sejam $(\boldsymbol{V_i})_{i\in I}$ uma família de espaços vetoriais sobre um corpo $\boldsymbol{C}$, $\boldsymbol{X}$ um espaço vetorial sobre $\boldsymbol{C}$ e, para todo $i \in I$, $L_i : \boldsymbol{V_i} \to \boldsymbol{X}$ uma transformação linear. Então existe única transformação linear $L : \boldsymbol{X} \to \bigsqcup_{i\in I} \boldsymbol{V_i}$ tal que, para todo $i \in I$, $L \circ \iota_i = L_i$ (o diagrama comuta).*



Capítulo 14

Álgebras Booleanas

Definição 14.1. Uma *álgebra booleana* é uma tripla $(A, \vee, \wedge)$, em que A é um conjunto não vazio, que satisfaz

1. $(A, \vee)$ e $(A, \wedge)$ são magmas comutativos com elementos neutros 0 e 1, respectivamente;
2. As operações $\vee$ e $\wedge$ são distributivas uma sobre a outra;
3. Todo elemento de $a_1 \in A$ tem um elemento *complementar* $a_2 \in A$ que satisfaz $a_1 \vee a_2 = 1$ e $a_1 \wedge a_2 = 0$.

Proposição 14.1. *Seja A um conjunto e $\mathcal{A} \subseteq \mathcal{P}(A)$ um conjunto de partes de A que satisfaz*

1. $\emptyset \in \mathcal{A}$;
2. $X \in \mathcal{A} \Rightarrow X^{\complement} \in \mathcal{A}$.

Então $(\mathcal{A}, \cup, \cap)$ é uma álgebra booleana.

Demonstração. Primeiramente, é necessário notar, embora os símbolos $\cup$ e $\cap$ não sejam funções propriamente ditas, ao fixarmos um conjunto A, podemos definir $\cup$ e $\cap$ como operações binárias em $\mathcal{P}(A)$, dadas por $(X, Y) \mapsto X \cup Y$ e $(X, Y) \mapsto X \cap Y$, respectivamente. Para $X, Y \in \mathcal{A}$, temos que $X \cup Y, X \cap Y \in \mathcal{A}$, o que mostra que as operações estão bem definidas.

Sendo assim, podemos prosseguir com a demonstração. Se $\mathcal{A}$ satisfaz as propriedades do enunciado, então $A = \emptyset^{\complement} \in \mathcal{A}$. O par $(\mathcal{A}, \cup)$ é um magma comutativo com elemento neutro $\emptyset$, pois a união de dois cojuntos é comutativa por definição e a união de um conjunto qualquer com o conjunto vazio dá o próprio conjunto. Da mesma forma, o par $(\mathcal{A}, \wedge)$ é um magma comutativo com elemento neutro A, pois

a interseção de dois conjuntos é comutativa por definição e a interseção de qualquer conjunto com o conjunto A é o próprio conjunto. Ainda, vale que, para todo $X, Y, Z \in \mathcal{A}$, $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ e $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$; ou seja, as operações binárias $\cup$ e $\cap$ são distributivas uma sobre a outra. Por fim, nota-se que, dado $X \in \mathcal{A}$, $X^{\complement} \in \mathcal{A}$ e vale $X \cup X^{\complement} = A$ e $X \cap X^{\complement} = \emptyset$. Logo $(\mathcal{A}, \cup, \cap)$ é uma álgebra booleana. ■

Proposição 14.2 (Princípio da Dualidade)**.** *Toda afirmação dudutível somente a partir da definição de álgebra booleana continua válida se são trocados entre si os símbolos* $\vee$ *e* $\wedge$ *e os símbolos* 0 *e* 1 *que aparecem na expressão.*

Demonstração. Todas as propriedades de uma álgebra booleana são definidas simetricaente e continuam iguais se trocamos entre si os símbolos $\vee$ e $\wedge$ e os símbolos 0 e 1. Logo isso também vale para qualquer afirmação dedutível dessas propriedades. ■

Como consequência do princípio da dualidade, qualquer afirmação dedutível das pripriedades de álbegra booleana tem uma afirmação associadad a ela ao trocarmos entre si os símbolos $\vee$ e $\wedge$ e os símbolos 0 e 1, que chamaremos que sua afirmação *dual*. Claramente, a afirmação dual da dual é a própria afirmação. Portanto só será necessário demonstrar a afirmação para demonstrar sua afirmação dual. Toda proposição, lema e teorema dessa seção exibirá sua proposição, lema e teorema dual, mas a afirmação dual não será demonstrada.

Teorema 14.3 (Operações com Identidades)**.** *Seja* $(A, \vee, \wedge)$ *uma álgebra booleana. Então*

$$\forall a \in A \qquad a \vee 1 = 1$$

$$\forall a \in A \qquad a \wedge 0 = 0$$

Teorema 14.4 (Leis de Absorção)**.** *Seja* $(A, \vee, \wedge)$ *uma álgebra booleana. Então*

$$\forall a, b \in A \qquad a \vee (a \wedge b) = a$$

$$\forall a, b \in A \qquad a \wedge (a \vee b) = a$$

Corolário 14.5 (Leis da Tautologia)**.** *Seja* $(A, \vee, \wedge)$ *uma álgebra booleana. Então*

$$\forall a \in A \qquad a \vee a = a$$

$$\forall a \in A \qquad a \wedge a = a$$

Demonstração. Basta tomar $b = 1$ e $b = 0$ nas proposições anteriores. ■

Teorema 14.6 (Associatividade)**.** *Seja* $(A, \vee, \wedge)$ *uma álgebra booleana. Então*

$$(A, \vee) \text{ é associativo.}$$

$$(A, \wedge) \text{ é associativo.}$$

Teorema 14.7 (Unicidade do Complementar)**.** *Seja* $(A, \vee, \wedge)$ *uma álgebra booleana e* $a \in A$*. Então o complementar de* a *é único.*

Note que esse teorema é seu próprio dual.

Teorema 14.8 (Dupla Complementação)**.** *Seja* $(A, \vee, \wedge)$ *uma álgebra booleana e* $a \in A$*. Então o complementar de* a' *é* a*.*

Teorema 14.9 (Identidades Complementares)**.** *Seja* $(A, \vee, \wedge)$ *uma álgebra booleana. Então*

$$0' = 1$$

$$1' = 0$$

Teorema 14.10 (Leis de De Morgan)**.** *Seja* $(A, \vee, \wedge)$ *uma álgebra booleana. Então*

$$\forall a, b \in A \qquad (a \wedge b)' = a' \vee b'$$

$$\forall a, b \in A \qquad (a \vee b)' = a' \wedge b'$$