



ELEMENTOS DE MATEMÁTICA

Pedro G. Mattos

Sumário

I Conjuntos	1
1 Os Axiomas e as Construções Essenciais	2
1.1 Axiomas do Vazio, da Extensão e das Partes	3
1.2 Axiomas da Especificação e do Par	5
1.3 Axioma da União	5
1.4 Axioma da Escolha	6
1.5 Axiomas do Infinito e da Fundação	8
1.6 Axioma da Substituição	8
2 Famílias e Propriedades de Conjuntos	11
2.1 Famílias e Indexações	11
2.2 Propriedades de União e Interseção	13
2.3 Produto de Conjuntos	15
2.4 Coproduto de Conjuntos	16
2.4.1 Propriedades de Produto e Coproduto	17
2.5 Complementares e Diferença Simétrica	18
2.5.1 Propriedades	18
2.6 Coberturas e Partições	19
2.6.1 Refinamento de Partições	19
3 Funções	22
3.1 Definição e Propriedades Básicas	22
3.2 Composição de Funções	24
3.3 Função Inversa, Injetividade e Sobrejetividade	25
3.4 Imagem Inversa de Função e Propriedades	26
3.5 Propriedades de Imagem e Imagem Inversa	27
4 Relações Binárias	29
4.1 Relações de Equivalência	29
4.2 Relações de Ordem	30
4.2.1 Ordens Parciais, Estritas e Totais	30

4.2.2	Conjuntos Parcialmente Ordenados	32
4.2.3	Funções Monótonas	34
4.2.4	Cadeias e Lema de Zorn	35
4.2.5	Pré-Ordens	35
4.2.6	Conjunto Direcionado	36
4.2.7	Reticulados	36
4.2.8	Álgebras Booleanas	37
5	Cardinalidade de Conjuntos	41
5.1	Relações	41
5.1.1	Igualdade de Cardinais	41
5.1.2	Ordenação de Cardinais	42
5.2	Operações	43
5.2.1	Cardinalidade de Soma (ou União Disjunta)	43
6	Conjuntos Numéricos	46
6.1	Números Naturais	46
6.1.1	Adição	47
6.1.2	Multiplicação	49
6.1.3	Ordenação	52
6.1.4	Base Doze	55
6.2	Números Inteiros	56
6.2.1	Adição e Subtração	57
6.2.2	Multiplicação	58
6.2.3	Ordenação	59
6.3	Números Racionais	59
6.3.1	Adição e Subtração	59
6.3.2	Multiplicação e Divisão	59
6.3.3	Ordenação	59
6.4	Números Reais	59
6.4.1	Adição e Subtração	59
6.4.2	Multiplicação e Divisão	59
6.4.3	Ordenação	59
6.4.4	Completude	59
II	Álgebra	60
7	Operações Binárias e Estruturas Básicas	61
7.1	Operações Binárias	61
7.2	Magma	62

7.3	Semigrupo	63
7.4	Homomorfismo de Semigrupos	65
7.5	Monoide	65
7.6	Homomorfismos de Monoïdes	68
8	Grupos	69
8.1	Construções Algébricas	69
8.1.1	Grupo e Subgrupo	69
8.1.2	Coclasses e Índice de Subgrupo	72
8.1.3	Subgrupo Normal e Grupo Quociente	75
8.1.4	Homomorfismo de Grupo	77
8.1.5	Núcleo, Imagem e Isomorfismo	79
8.1.6	Teoremas de Isomorfismo	81
8.2	Construções Categóricas	82
8.2.1	Produto de Grupos	82
8.2.2	Grupo Livre	83
8.2.3	Coproduto de Grupos	85
8.3	Construções Específicas	87
8.3.1	Grupo Simples e Subgrupo Normal Maximal	87
8.3.2	Sequência subnormal	88
8.3.3	Conjunto gerador	88
8.3.4	Grupos Simétricos e Alternados	88
8.3.5	Grupos Cíclicos	93
8.3.6	Grupos Diedrais	93
8.4	Ação de Grupos	94
8.4.1	Órbitas e Estabilizadores	95
8.5	Grupo Linear Geral	95
8.6	Representação de Grupos	96
8.7	Grupos Topológicos	96
8.7.1	Homomorfismos	97
8.7.2	Ação Contínua	98
8.8	Grupos Diferenciais	98
9	Anéis	99
9.1	Construções Algébricas	99
9.1.1	Anel e Subanel	99
9.1.2	Ideais e Anéis Quocientes	102
9.1.3	Homomorfismos de Anéis	106
9.1.4	Teoremas de Isomorfismo	113
9.2	Construções Categóricas	117
9.2.1	Anel de Polinômios	117

9.2.2	Produto de Anéis	121
9.3	Construções Específicas	122
9.3.1	Domínios e Corpos	122
9.3.2	Divisão e Associação em Anéis	123
9.3.3	Irredutíveis, Primos e Fatoração	128
9.3.4	Ideais Primos e Ideais Maximaís	135
9.3.5	Domínios Euclidianos	137
9.3.6	Raízes de Polinômios	138
9.4	Corpos	139
9.4.1	Extensões de Corpos	139
9.4.2	Extras	143
9.5	Matrizes	144
9.5.1	Soma de Matrizes	145
9.5.2	Produto de Matrizes e Produto Por Escalar	146
9.5.3	Matrizes Quadradas	148
9.5.4	Traço e Determinante	148
10	Espaços Lineares	150
10.1	Módulos	150
10.2	Espaço e Subespaço Lineares	153
10.3	Combinação Linear de Vetores	159
10.4	Soma de Subespaços Vetoriais	163
10.5	Bases de Espaços Vetoriais	165
10.6	Funções Lineares	168
10.7	Produto e Coproduto de Espaços Vetoriais	170
10.7.1	Produto	170
10.7.2	Coproduto (Soma)	172
11	Álgebra Multilinear	174
11.1	Funções Multilineares	174
11.1.1	Simetria, Antissimetria e Alternância	175
11.2	Formas Multilineares	178
11.2.1	Produto Tensorial de Formas Multilineares	178
11.2.2	Produto Alternado de Formas Multilineares	179
11.2.3	Determinante	181
11.2.4	Extras	182
11.3	Produto Tensorial de Espaços Lineares	183
11.3.1	Tensores	186

12 Álgebras sobre Corpos	187
12.1 Álgebra e Ação Adjunta	187
12.2 Derivação	188
12.3 Álgebra de Derivação Adjunta	190
III Topologia e Geometria	193
13 Topologia	194
13.1 Espaços Topológicos	194
13.1.1 Topologia, abertos e fechados	194
13.1.2 Topologias Geradas, Bases e Sub-bases	201
13.1.3 Funções Contínuas	202
13.1.4 Topologias Induzidas	203
13.2 Separação	209
13.2.1 Noções de Separação de Conjuntos	209
13.2.2 Espaços Distinguíveis	211
13.2.3 Espaços Acessíveis	212
13.2.4 Espaços Separados por Vizinhanças	212
13.2.5 Espaços Regulares	213
13.2.6 Espaços Completamente Regulares	214
13.2.7 Espaços Normais	214
13.3 Convergência	216
13.3.1 Redes	216
13.4 Conexidade e Compacidade	217
13.4.1 Conexidades	217
13.4.2 Compacidades	220
13.4.3 Contabilidades	222
13.5 Homotopia e Grupo Fundamental	223
13.5.1 Homotopia	223
13.5.2 Equivalência Homotópica	224
13.5.3 Caminhos e Laços	224
13.5.4 Homotopia de Caminhos	225
13.5.5 Grupo Fundamental	230
13.6 Espaços Fibrados	230
14 Espaços Mensuráveis e de Medida	232
14.1 Espaço Mensurável	232
14.1.1 Sigma-Álgebras e Sub-Sigma-Álgebras	232
14.1.2 Sigma-Álgebras Geradas	234
14.1.3 Limites de Conjuntos	234

14.2 Funções mensuráveis	235
14.2.1 Sigma-Álgebras Puxadas e Empurradas	236
14.3 Produto de espaços mensuráveis	237
14.4 Espaços Mensuráveis Topológicos	239
14.4.1 Boreliano e função mensurável em \mathbb{R}	239
14.5 Medida e Espaço de Medida	241
15 Integração	242
15.1 Integral de Funções Mensuráveis Simples	242
15.2 Integral de Funções Mensuráveis Positivas	247
15.3 Integral de Funções Mensuráveis	247
15.4 Teoremas de Convergências	247
15.5 Funções Absolutamente Integráveis	247
16 Espaços Métricos	249
16.1 Os Espaços Métricos	249
16.1.1 Métricas	249
16.1.2 Diâmetro, Bolas e Conjuntos e Funções Limitadas	253
16.2 Topologia dos Espaços Métricos	254
16.2.1 Interior e Pontos Interiores	254
16.2.2 Limites e Convergência de Sequências	255
16.2.3 Fecho e Pontos Aderentes	257
16.2.4 Conjuntos Densos	258
16.2.5 Conjuntos Compactos	259
16.2.6 Continuidade	260
16.2.7 Ponto Limite e Conjunto Derivado	261
16.2.8 Separação Métrica	261
16.3 Estrutura Uniforme	261
16.3.1 Sequências Aproximantes	261
16.3.2 Continuidade Uniforme	263
16.3.3 Espaços Métricos Completos	263
16.4 Funções que Preservam Distância	265
16.4.1 Funções Métricas (ou Subsemelhanças)	265
16.4.2 Homometrias e Isometrias	267
16.4.3 Contrações	268
16.4.4 Semelhanças	269
16.5 Medida e Dimensão	269
16.5.1 Medidas Exteriores Métricas	269
16.5.2 Medidas por Coberturas Métricas	270
16.5.3 Dimensão Métrica e Fractais	275

17 Espaços Normados	276
17.1 Normas, Espaços Normados e Métricas	276
17.1.1 Bolas e Esferas Unitárias	279
17.2 Isometrias Lineares, Funções Limitadas e Norma de Funções Lineares	280
17.2.1 Os Grupos Lineares Geral e Especial de Transformações e de Isometrias	282
17.3 Espaços Normados de Dimensão Finita	282
17.4 Funções Multilineares	284
17.5 Norma de Funções Multilineares	285
18 Espaços Lineares com Produto Interno	286
18.1 Produto Interno	286
18.2 Norma Induzida, Ortogonalidade e Ângulo	288
18.2.1 Norma	288
18.2.2 Perpendicularidade e Paralelismo	289
18.2.3 Ângulo	292
18.2.4 Funções Ortogonais e Conformes	296
19 Cálculo Diferencial	300
19.1 Diferenciabilidade	300
19.1.1 Diferenciais de Ordem Superior	304
19.2 Derivadas Direcionais e a Geometria da Diferenciabilidade	306
19.3 Os Teoremas Fundamentais	307
19.3.1 Teorema da Função Inversa	307
19.3.2 Teorema da Função Implícita	307
19.3.3 Forma Local da Imersão	307
19.3.4 Forma Local da Submersão	308
19.3.5 Teorema do Posto	308
19.4 Cálculo em Espaços Normados de Dimensão Finita	309
19.4.1 Diferencial	309
20 Variedades	312
20.1 Estrutura Topológica e Diferencial	312
20.1.1 Cartas e Atlas	312
20.2 Variedades e Topologia	315
20.2.1 Exemplos de Variedades	317
20.2.2 Propriedades Topológicas	320
20.3 Funções Diferenciáveis e Espaço Tangente	322
20.3.1 Funções Diferenciáveis	322
20.3.2 Espaço Tangente e a Diferencial	323
20.3.3 Fibrado Tangente	329

20.3.4 Espaço Cotangente	330
20.3.5 Curvas Equivelozes e Espaço Tangente	331
20.4 Funções Separadoras e Partições da Unidade	333
20.5 Orientação	334
20.5.1 Orientação de Espaços Lineares	334
20.5.2 Orientação de Variedades	337
20.6 Conjuntos Nulos	339
20.7 Valores Regulares, Pontos Críticos e Transversalidade	340
20.7.1 Valor Regular	340
20.7.2 Ponto Crítico	341
20.7.3 Transversalidade	341
20.7.4 Mais Transversalidade	342
20.8 Campos Tensoriais	343
20.8.1 Campos Tensoriais, Vetoriais, e Derivações	343
20.9 Derivações e Colchete de Campos Vetoriais	344
20.9.1 Álgebra de Campos Tensoriais	346
20.9.2 Fluxo de Campos Vetoriais	347
20.10 Formas Diferenciáveis	347
20.10.1 Formas Puxadas	348
20.10.2 Derivada Exterior	349

Parte I

Conjuntos

Capítulo 1

Os Axiomas e as Construções 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

$$\forall \quad \exists$$

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

$$\Rightarrow \quad \Leftarrow \quad \Leftrightarrow$$

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, serão substituídos 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 das primeiras propriedades de um conjunto quando pensado intuitivamente: a ideia de que, quando abstrai-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,

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

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 conjunto 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 $Y \not\subseteq X$. 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 $\wp(X)$.

Proposição 1.2. Sejam X e Y conjuntos. Então

$$X \subseteq Y \implies \wp(X) \subseteq \wp(Y).$$

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 uma 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 conjuntos: 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 consequência 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 pertencem 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*

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

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 conjuntos, 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

$$(X, Y) := \{\{X\}, \{X, Y\}\} \in \wp(\wp(X \cup Y)).$$

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

$$X \times Y := \{(x, y) \in \wp(\wp(X \cup Y)) \mid x \in X \text{ e } y \in Y\}.$$

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

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

Esse y é a *imagem* de x , denotada por $f(x)$. Denotam-se $f : X \rightarrow Y$ e $f(x) := y$. 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 $f : A \rightarrow B$.

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 $b \in B$ 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

$$\prod C := \left\{ f : C \rightarrow \bigcup C \mid \forall X \in C \quad f(X) \in X \right\}.$$

$$\prod C := \left\{ f \in (\bigcup C)^C \mid \forall X \in C \quad f(X) \in X \right\}.$$

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 $\emptyset : \emptyset \rightarrow \emptyset$ 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 $f : C \rightarrow \bigcup C$ 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

$$X^+ := X \cup \{X\}.$$

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 $\prod C$ 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 C indexados por I é uma função $F : I \rightarrow C$. O conjunto I é o *conjunto de índices* da família. Denota-se isso por $(F_i)_{i \in I}$ 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, $I = \{0, \dots, n-1\}$ 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 simplesmente uma função sem nenhuma restrição, e a única diferença entre uma família é uma função é o contexto. 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 $F : C \rightarrow C$ 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 indexação 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 $(C_i)_{i \in I}$ de conjuntos é o conjunto

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

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

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

Quando I for finito, pode-se denotar

$$C_1 \cup \dots \cup C_n := \bigcup_{i \in I} C_i \quad \text{e} \quad C_1 \cap \dots \cap C_n := \bigcap_{i \in I} C_i.$$

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

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

Proposição 2.2. Sejam X um conjunto e $(C_i)_{i \in I}$ uma família não vazia de subconjuntos de X . Então

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

Demonstração. 1. Para isso, basta notar que $c \in (\bigcap_{i \in I} C_i)^c$ 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 $c \in (C_i)^c$ que, por sua vez, é equivalente a $c \in \bigcup_{i \in I} (C_i)^c$.

2. Como, para todo conjunto C , $(C^c)^c = C$, segue do item anterior que

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

■

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*

$$1. \bigcap_{i \in I} \wp(C_i) = \wp \left(\bigcap_{i \in I} C_i \right);$$

$$2. \bigcup_{i \in I} \wp(C_i) \subseteq \wp \left(\bigcup_{i \in I} C_i \right).$$

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

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

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

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

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

$$\begin{array}{ccc} & \prod_{i \in I} C_i & \\ f \swarrow & \nearrow \pi_i & \\ X & \xrightarrow{f_i} & C_i \end{array}$$

Demonstração. Defina a função

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

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 $\bar{f} : X \longrightarrow \prod_{i \in I} C_i$ função tal que, para todo $i \in I$, $\pi_i \circ \bar{f} = f_i$. Seja $x \in X$. Como $\bar{f}(x) \in \prod_{i \in I} C_i$, $\bar{f}(x) = (x_i)_{i \in I}$. Da propriedade comutativa de \bar{f} , segue que, para todo $i \in I$,

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

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

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

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

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

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

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

$$\begin{array}{ccc} & \bigsqcup_{i \in I} C_i & \\ \iota_i \uparrow & \swarrow f & \\ C_i & \xrightarrow{f_i} & X \end{array}$$

Demonstração. Defina a função

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

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 $\bar{f} : \bigsqcup_{i \in I} C_i \longrightarrow X$ função tal que, para todo $i \in I$, $\bar{f} \circ \iota_i = f_i$. 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 \bar{f} , segue que

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

Isso mostra que $\bar{f} = f$. ■

2.4.1 Propriedades de Produto e Coproduto

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

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

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

Demonstração.

1.

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

2.

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

■

Notemos que a inclusão contrária no primeiro item não 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 será vazio (pelo axioma da escolha).

Proposição 2.8. Sejam X um conjunto, $(Y_i)_{i \in I}$ uma família de conjuntos, $(S_i)_{i \in I}$ uma família de subconjuntos de $(Y_i)_{i \in I}$, $f : X \longrightarrow \prod_{i \in I} Y_i$ uma função e, para todo $i \in I$, $f_i := \pi_i \circ f$. Então

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

Demonastração. Note que $x \in f^{-1}(\prod_{i \in I} S_i)$ é equivalente a $f(x) \in \prod_{i \in I} S_i$, que por sua vez ocorre se, e somente se, para todo $i \in I$, $\pi_i(f(x)) \in S_i$. Como $f_i(x) = \pi_i(f(x)) \in S_i$, isso é equivalente a, para todo $i \in I$, $x \in f_i^{-1}(S_i)$. ■

Notação alternativa

$$\prod_{i \in I} C_i = \{\lceil c_i \rceil_{i \in I} \mid \forall i \in I \ c_i \in C_i\}$$

$$\lceil c_i \rceil_{i \in I} = c : I \longrightarrow \bigcup_{i \in I} C_i$$

$$\bigsqcup_{i \in I} C_i = \{\lfloor c \rfloor_i \mid i \in I, c \in C_i\}$$

$$\lfloor c \rfloor_i = (i, c)$$

2.5 Complementares e Diferença Simétrica

Definição 2.8. Sejam X e Y conjuntos. O *complementar relativo* de Y em X é o conjunto

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

Definição 2.9. Sejam X um conjunto e S um subconjunto de X . O *complementar* de S em X é o conjunto

$$S^c := X \setminus S.$$

Definição 2.10. Sejam X e Y conjuntos. A *diferença simétrica* de X e Y é o conjunto

$$X \Delta Y := (X \setminus Y) \cup (Y \setminus X).$$

2.5.1 Propriedades

Proposição 2.9. Sejam X, Y subconjuntos de U . Então

1. $(X^c)^c = X$;
2. $\emptyset^c = U$ e $U^c = \emptyset$;

3. $X \cap X^c = \emptyset$ e $X \cup X^c = U$;
4. $X \subseteq Y \iff Y^c \subseteq X^c$.
5. $(X \cup Y)^c = X^c \cap Y^c$ e $(X \cap Y)^c = X^c \cup Y^c$.

2.6 Coberturas e Partições

Definição 2.11. Seja X um conjunto. Uma *cobertura* de X é uma família $(C_i)_{i \in I}$ de subconjuntos de X cuja união é X :

$$\bigcup_{i \in I} C_i = X.$$

Um *subcobertura* de uma cobertura $(C_i)_{i \in I}$ de X é uma cobertura $(C_i)_{i \in J}$ de X , com $J \subseteq I$.

Definição 2.12. Seja X um conjunto. Uma *partição* de X é um conjunto $\mathcal{P} \subseteq \wp(X)$ de subconjuntos de X que satisfaz

1. $\emptyset \notin \mathcal{P}$;
2. $\bigcup \mathcal{P} = X$;
3. Para todos conjuntos distintos $C_0, C_1 \in \mathcal{P}$, $C_0 \cap C_1 = \emptyset$.

Os conjuntos $C \in \mathcal{P}$ são as *células* de \mathcal{P} .

Uma partição, se identificarmos um subconjunto de $\wp(X)$ com uma família de subconjuntos de X , é uma cobertura de X por conjuntos disjuntos (logo distintos) que não contém o conjunto vazio.

2.6.1 Refinamento de Partições

Definição 2.13. Sejam X um conjunto e \mathcal{P} uma partição de X . Um *refinamento* (*superpartição*) de \mathcal{P} é uma partição \mathcal{R} de X que satisfaz: para toda célula $D \in \mathcal{R}$, existe uma célula $C \in \mathcal{P}$ tal que $D \subseteq C$. Denota-se $\mathcal{P} \leq \mathcal{R}$. Diz que \mathcal{P} é um *engrossamento* (*subpartição*) de \mathcal{R} .

Proposição 2.10. *Sejam X um conjunto e \mathcal{P}, \mathcal{R} partições de X tais que $\mathcal{P} \leq \mathcal{R}$. Então*

1. $|\mathcal{P}| \leq |\mathcal{R}|$;

2. Para cada célula $C \in \mathcal{P}$, o conjunto

$$\mathcal{R}|_C := \{D \in \mathcal{R} \mid D \subseteq C\}$$

é uma partição de C .

Demonstração. 1. Por definição de refinamento, para toda célula $D \in \mathcal{R}$ existe célula $C \in \mathcal{P}$ tal que $D \subseteq C$. Notemos que essa célula C é única pois, se existir célula $C' \in \mathcal{P}$ tal que $D \subseteq C'$, então $D \subseteq C \cap C'$ e, como $D \neq \emptyset$, segue que $C = C'$. Assim, consideramos a função que mapeia, para cada célula $D \in \mathcal{R}$ a célula $C_D \in \mathcal{P}$ tal que $D \subseteq C_D$:

$$\begin{aligned} f: \mathcal{R} &\longrightarrow \mathcal{P} \\ D &\longmapsto C_D. \end{aligned}$$

Mostremos que essa função é sobrejetiva. Para isso, seja $C \in \mathcal{P}$. Como $\bigcup \mathcal{R} = X$, para todo $x \in C \subseteq X$ existe $D \in \mathcal{R}$ tal que $x \in D$. Como $C \neq \emptyset$, existe $x \in C$, logo existe $D \in \mathcal{R}$ tal que $x \in D$. Por definição de refinamento, existe $C' \in \mathcal{P}$ tal que $D \subseteq C'$, o que implica $x \in C'$. Como $x \in C' \cap C$, segue que $C = C'$, e concluímos que $D \subseteq C$. Isso mostra que $f(D) = C$, logo que f é sobrejetiva. Concluímos, então, que $|\mathcal{P}| \leq |\mathcal{R}|$.

2. As propriedades 1 e 3 são evidentes por que \mathcal{R} é partição. Para a propriedade 2, seja $C \in \mathcal{P}$ e $U := \bigcup \{D \in \mathcal{R} \mid D \subseteq C\}$. Notemos que $C = U$. Para mostrar isso, seja $x \in C$. Então existe $D \in \mathcal{R}$ tal que $x \in D$, pois $\bigcup \mathcal{P} = X$. Por definição de refinamento, existe $C' \in \mathcal{P}$ tal que $D \subseteq C'$, portanto $x \in C'$. Como $x \in C' \cap C$, segue que $C = C'$. Concluímos que $D \subseteq C$, portanto que $x \in U$, o que mostra $C \subseteq U$. Reciprocamente, para todo $D \in U$, $D \subseteq C$, portanto $U \subseteq C$, e concluímos que $C = U$. ■

Proposição 2.11. Sejam X um conjunto. A relação de refinamento \leq no conjunto de partições de X é uma relação de ordem parcial.

Definição 2.14. Sejam X um conjunto e $(\mathcal{P}_i)_{i \in I}$ uma família de partições de X . O refinamento comum a $(\mathcal{P}_i)_{i \in I}$ é o conjunto

$$\bigvee_{i \in I} \mathcal{P}_i := \left\{ \bigcap_{i \in I} C_i \mid i \in I, C_i \in \mathcal{P}_i \text{ e } \bigcap_{i \in I} C_i \neq \emptyset \right\}.$$

Proposição 2.12. Sejam X um conjunto e $(\mathcal{P}_i)_{i \in I}$ uma família de partições de X . O refinamento comum $\bigvee_{i \in I} \mathcal{P}_i$ a $(\mathcal{P}_i)_{i \in I}$ é a menor partição de que X que refina \mathcal{P}_i para todo $i \in I$.

Demonstração. Primeiro, mostremos que $\mathcal{P} := \bigvee_{i \in I} \mathcal{P}_i$ é uma partição. Por definição, $\emptyset \notin \mathcal{P}$. Seja $x \in X$. Então, para cada $i \in I$, existe $C_i \in \mathcal{P}_i$ tal que $x \in C_i$, pois $\bigcup \mathcal{P}_i = X$. Sendo assim, $x \in \bigcap_{i \in I} C_i$, portanto $X \subseteq \bigcup \mathcal{P}$, e segue que $\bigcup \mathcal{P} = X$. Por fim, sejam $C = \bigcap_{i \in I} C_i, D = \bigcap_{i \in I} D_i \in \mathcal{P}$. Se $C \neq D$, então existe $x \in C \setminus D$ ou existe $x \in D \setminus C$. Sem perda de generalidade, suponha o primeiro. Então, existe $i \in I$ tal que $x \notin D_i$. Como $x \in C$, então $x \in C_i$, portanto $C_i \neq D_i$. Mas então, como \mathcal{P}_i é partição, $C_i \cap D_i = \emptyset$. Por fim, como $C \subseteq C_i$ e $D \subseteq D_i$, segue que $C \cap D = \emptyset$.

Agora mostraremos que \mathcal{P} é refinamento de \mathcal{P}_i para todo $i \in I$. Sejam $i \in I$ e $C \in \mathcal{P}$. Então $\mathcal{P} = \bigcap_{i \in I} C_i$, portanto $C_i \in \mathcal{P}_i$. Por fim, sejam \mathcal{R} partição de X que é refina \mathcal{P}_i para todo $i \in I$ e $D \in \mathcal{R}$ uma célula. Então, para todo $i \in I$, existe $C_i \in \mathcal{P}_i$ tal que $D \subseteq C_i$. Portanto $D \subseteq \bigcap_{i \in I} C_i$, e como $\bigcap_{i \in I} C_i \in \mathcal{P}$, segue que $\mathcal{P} \leq \mathcal{R}$. ■

Alguns tipos especiais de partições são úteis na teoria de integração de Riemann. Em \mathbb{R}^1 , essas partições são chamadas de partições de intervalo, e são representadas como um número finito de pontos em um intervalo. Quando generaliza-se para dimensões maiores, usam-se n -retângulos, que são conjuntos em \mathbb{R}^n produtos de n intervalos limitados. Podemos fixar um critério a mais, o de que um n -retângulo é produto de intervalos fechados em baixo e abertos em cima. Nesse caso, podemos definir que uma partição cujos elementos são n -retângulos é uma *malha*.

Alternativamente, quando temos uma medida, que é o caso de \mathbb{R}^n , podemos enfraquecer a restrição de que as células de uma partição são iguais ou disjuntas para a de que são iguais ou *quase disjuntas* – a interseção tem medida zero – e a restrição de que cobrem para a restrição de que a união da partição é quase total – seu complementar tem medida nula – e por fim, de que nenhum elemento da partição é quase vazio – tem medida nula – e definir que isso é uma μ -partição ou *quase partição com respeito a μ* .

Capítulo 3

Funções

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

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

3.1 Definição e Propriedades Básicas

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

$$\forall a \in A \ \exists! b \in B \quad (a, b) \in f.$$

Denota-se $f : A \rightarrow B$. A *imagem* de $a \in A$ é o único $b \in B$ que satisfaz $(a, b) \in f$. Denota-se $b = f(a)$. Ambas informações podem ser denotadas por

$$\begin{aligned} f : A &\longrightarrow B \\ a &\longmapsto b. \end{aligned}$$

O conjunto das funções de A para B é denotado B^A .

Proposição 3.1. *Seja $f : A \rightarrow B$ uma função. Então*

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 uma contradição. 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 contradição. 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 $f : A \rightarrow B$ e $g : A' \rightarrow B'$. Então*

$$f = g \iff A = A' \text{ e } \forall a \in A \quad f(a) = g(a).$$

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 $f = g$. ■

Definição 3.4. Sejam $f : A \rightarrow B$ uma função e $C \subseteq A$ um conjunto. O *conjunto imagem* de C sob f é

$$f(C) = \{y \in Y \mid \exists c \in C \quad y = f(c)\}.$$

O conjunto $f(A)$ é o *imagem* de f .

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

Definição 3.5. Sejam $f : A \rightarrow B$ uma função e $A' \subseteq A$ um conjunto. A *restrição* de f a A' é a função

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

Proposição 3.4. Sejam $f : A \rightarrow B$, $A' \subseteq A$ 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 Composição de Funções

Definição 3.6. Sejam $f : A \rightarrow B'$ e $g : B \rightarrow C$ funções tais que $B' \subseteq B$. A *função composta* de g com f é a função

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

Proposição 3.5. Sejam $f : A \rightarrow B'$, $g : B \rightarrow C'$ e $h : C \rightarrow D$ 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 $f : A \rightarrow B$. 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 3.7. Seja A um conjunto não vazio. A *função identidade* em A é a função

$$\begin{aligned} \text{Id}_A : A &\longrightarrow A \\ a &\longmapsto a. \end{aligned}$$

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

$$f \circ \text{Id}_A = f \quad \text{e} \quad \text{Id}_B \circ f = f.$$

Demonstração. Primeiro, notemos que $f \circ \text{Id}_A$ e $\text{Id}_B \circ f$ são funções de A em B e, portanto, têm o mesmo domínio de f . Se $A = \emptyset$, então $f : \emptyset \longrightarrow B$ e, portanto, $f = \emptyset$. Notemos que $\text{Id}_{\emptyset} = \emptyset$. 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, $f \circ \text{Id}_A$ é uma função de \emptyset em B e, portanto, $f \circ \text{Id}_A = \emptyset = f$. Ainda, $\text{Id}_B \circ f$ é uma função de \emptyset em B e, portanto, $\text{Id}_B \circ f = \emptyset = f$. Se $A \neq \emptyset$, seja $a \in A$. Então $(f \circ \text{Id}_A)(a) = f(\text{Id}_A(a)) = f(a) = \text{Id}_B(f(a)) = (\text{Id}_B \circ f)(a)$. ■

3.3 Função Inversa, Injetividade e Sobrejetividade

Definição 3.8. Seja $f : A \longrightarrow B$ uma função. Uma *função inversa* de f é uma função $g : B \longrightarrow A$ tal que

$$g \circ f = \text{Id}_A \quad \text{e} \quad f \circ g = \text{Id}_B.$$

Definição 3.9. Uma *função injetiva* (ou *injeção*) é uma função $f : A \longrightarrow B$ que satisfaz

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

Definição 3.10. Uma *função sobrejetiva* sobre um conjunto B é uma função $f : A \longrightarrow B$ que satisfaz $f(A) = B$.

Definição 3.11. Sejam A e B conjuntos. Uma *bijeção* entre A e B é uma função injetiva $f : A \longrightarrow B$ que é sobrejetiva sobre B .

Proposição 3.8. Seja $f : A \longrightarrow B$. Então f é injetiva se, e somente se, existe $g : B \longrightarrow A$ tal que $g \circ f = \text{Id}_A$.

Demonstração. Suponhamos que f é injetiva. Se $A = \emptyset$. Então $f = \emptyset$ e, portanto, tomando $g = \text{Id}_B$, temos que $g \circ f = \text{Id}_B \circ \emptyset = \text{Id}_{\emptyset} = \emptyset$. Se $A \neq \emptyset$, seja $a \in A$.

■

Proposição 3.9. *Seja $f : A \rightarrow B$. Então f é sobrejetiva sobre B se, e somente se, existe $g : B \rightarrow A$ tal que $f \circ g = \text{Id}_B$.*

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 $g : B \rightarrow A$ para cada elemento de B como $g(b) := a$. Assim, segue que $g \circ f = \text{Id}_B$.

■

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

Proposição 3.11. *Sejam $f : A \rightarrow B'$ e $g : B \rightarrow C$ 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 $f : A \rightarrow B$ e $g : B \rightarrow C$ 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.

■

3.4 Imagem Inversa de Função e Propriedades

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

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

Proposição 3.13. *Seja $f : A \rightarrow B$ uma função, $B' \subseteq B$ e $(B_i)_{i \in I} \subseteq \wp(B)$ uma família de subconjuntos de B . Então*

1. $f^{-1}(\emptyset) = \emptyset$;
2. $f^{-1}(B) = A$;
3. $f^{-1}\left((B')^c\right) = (f^{-1}(B'))^c$;

$$4. f^{-1} \left(\bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} f^{-1}(B_i);$$

$$5. f^{-1} \left(\bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} f^{-1}(B_i).$$

Demonstração. 1. Suponha, por absurdo, 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 $a \in f^{-1}((B')^c)$. Então $f(a) \in (B')^c$. Mas isso implica $a \notin f^{-1}(B')$, pois, caso contrário, seguiria que $f(a) \in B'$, o que contradiz a hipótese. Portanto $a \in (f^{-1}(B'))^c$; ou seja, $f^{-1}((B')^c) \subseteq (f^{-1}(B'))^c$. Reciprocamente, seja $a \in (f^{-1}(B'))^c$. Se, por absurdo, $f(a) \in B'$, então $a \notin f^{-1}(B')$, o que contradiz a hipótese. Portanto $f(a) \in (B')^c$, o que implica $a \in f^{-1}((B')^c)$. Assim conclui-se que $(f^{-1}(B'))^c \subseteq f^{-1}((B')^c)$ e, portanto, $f^{-1}((B')^c) = (f^{-1}(B'))^c$.
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 existe $i \in I$ 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 $f^{-1}(\bigcap_{i \in I} B_i) = \bigcap_{i \in I} f^{-1}(B_i)$. ■

3.5 Propriedades de Imagem e Imagem Inversa

Proposição 3.14. *Sejam $f : D \rightarrow C$ 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 $f(\bigcup_{i \in I} C_i) = \emptyset$, 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 $d \in f(\bigcup_{i \in I} C_i)$. 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, $f(\bigcup_{i \in I} C_i) = \emptyset$. 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 $d \in f(\bigcup_{i \in I} C_i)$. ■

Proposição 3.15. *Sejam $f : D \rightarrow C$ 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, $y = f(x) = f(f^{-1}(Y))$. ■

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

Uma relação que satisfaz as propriedades acima é, respectivamente, reflexiva, simétrica, antissimétrica, 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

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

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

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

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 $P := A/\sim$. Claramente, $\emptyset \not\subseteq P$. 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

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

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 $\leq, \subseteq, \trianglelefteq$ ou outros símbolos semelhantes.

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

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

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

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 $x_1, x_2, x_3 \in X$. 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 $\wp(A)$ é uma relação de ordem estrita em $\wp(A)$.

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

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

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, $x_1 < x_3$. \blacksquare

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. \blacksquare

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

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

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

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

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

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

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. $\forall x \in X \quad \min\{x\} = \max\{x\} = x$.

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

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

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

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

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 $y \neq \max Y$ 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

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

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

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

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

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

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

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

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 Pré-Ordens

Definição 4.17. Seja X um conjunto não vazio. Uma *pré-ordem* (ou *precedência*) em X é uma relação binária em X que é reflexiva e transitiva. O par (X, \preceq) é um *conjunto pré-ordenado*.

Definição 4.18. Seja (X, \preceq) um conjunto pré-ordenado. A *equivalência induzida* por \preceq é a relação binária \sim definida por: para todos $x, x' \in X$,

$$x \sim x' \iff x \preceq x' \text{ e } x' \preceq x.$$

A *ordenação induzida* por \leq é a relação binária em X/\sim definida por: para todos $x, x' \in X$,

$$[x] \leq [x'] \iff x \preceq x'.$$

Proposição 4.13. Seja (X, \preceq) um conjunto pré-ordenado. A relação \sim em A é uma equivalência em X e a relação \leq em X/\sim é uma ordem em X/\sim .

Demonstração. EQUIVALÊNCIA \sim : (Reflexividade) Para todo $x \in X$, vale que $x \preceq x$, portanto $x \sim x$. (Simetria) Para todos $x, x' \in X$, se $x \preceq x'$ e $x' \preceq x$, então $x \sim x'$ por definição. (Transitividade) Para todos $x, x', x'' \in X$, se $x \sim x'$ e $x' \sim x''$, então se $x \preceq x'$, $x' \preceq x$, $x' \preceq x''$ e $x'' \preceq x'$, o que implica pela transitividade de \preceq que $x \preceq x''$ e $x'' \preceq x$, portanto $x \sim x''$.

ORDEM \leq : Primeiro devemos mostrar que a relação está bem definida. Sejam $[x], [x'] \in X$. Tomemos $x, y \in [x]$ e $x', y' \in [x']$; queremos mostrar que se $x \preceq x'$, então $y \preceq y'$. Como $x \sim y$, então $y \preceq x$, e como $x' \sim y'$, então $x' \preceq y'$; assim, da transitividade de \preceq segue que

$$y \preceq x \preceq x' \preceq y'.$$

Isso mostra que \leq está bem definida. Agora, mostremos que \leq é ordem. (Reflexividade) Para todo $x \in X$, vale que $[x] \leq [x]$, pois $x \preceq x$. (Antissimetria) Para todos $x, x' \in X$, se $[x] \leq [x']$ e $[x'] \leq [x]$, então $x \preceq x'$ e $x' \preceq x$, o que implica $x \sim x'$, portanto $[x] = [x']$. (Transitividade) Para todos $x, x', x'' \in X$, se $[x] \leq [x']$ e $[x'] \leq [x'']$, então $x \preceq x'$ e $x' \preceq x''$, o que implica que $x \preceq x''$, portanto $[x] \leq [x'']$. ■

4.2.6 Conjunto Direcionado

Definição 4.19. Um *conjunto direcionado (superiormente)* é um par (X, \preceq) em que X é um conjunto não vazio e \preceq é uma pré-ordem em X que satisfaz: para todos $x, x' \in X$, existe $s \in X$ tal que $x \leq s$ e $x' \leq s$.

Proposição 4.14. Sejam (X, \preceq) um conjunto direcionado e $x_0, \dots, x_{n-1} \in X$. Existe $s \in X$ tal que, para todo $i \in [n]$, $x_i \leq s$.

4.2.7 Reticulados

Definição 4.20. Um *reticulado* é um conjunto parcialmente ordenado (X, \leq) em que, para todos $x_1, x_2 \in X$, o conjunto $\{x_1, x_2\}$ tem supremo e ínfimo, denotados, respectivamente, $x_1 \vee x_2$ e $x_1 \wedge x_2$.

Proposição 4.15. Seja (X, \leq) um reticulado e $Y \subseteq X$ um conjunto finito. Então Y tem supremo e ínfimo.

Um reticulado também pode ser entendido como uma estrutura algébrica. As definições a seguir usam definições da parte de Álgebra do livro, e devem ser conferidas nessa parte.

Definição 4.21. Um *reticulado* é uma tripla (R, \vee, \wedge) em que

1. (R, \vee) e (R, \wedge) são semigrupos comutativos;
2. Valem as propriedades de *absorção*: para todos $a, b \in R$,
 - (a) $a \vee (a \wedge b) = a$;
 - (b) $a \wedge (a \vee b) = a$.

Proposição 4.16. Seja (R, \vee, \wedge) um reticulado. Valem as propriedades de idempotência: para todo $a \in R$,

1. $a \vee a = a$;
2. $a \wedge a = a$.

Definição 4.22. Um *reticulado limitado* é uma 5-sequência $(R, \vee, \wedge, 0, 1)$ em que (R, \vee, \wedge) é um reticulado, 0 é elemento neutro de (R, \vee) e 1 é elemento neutro de (R, \wedge) .

\vee e \wedge estão definidos para todo subconjunto não-vazio finito por indução, já que são operações associativas.

Proposição 4.17. *Todo reticulado finito é limitado.*

4.2.8 Álgebras Booleanas

Definição 4.23. 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. Para todo $a \in A$ existe um elemento *complementar* $a' \in A$, que satisfaz $a \vee a' = 1$ e $a \wedge a' = 0$.

Proposição 4.18. *Seja A um conjunto e $\mathcal{A} \subseteq \wp(A)$ um conjunto de partes de A que satisfaz*

1. $\emptyset \in \mathcal{A}$;
2. $X \in \mathcal{A} \Rightarrow X^c \in \mathcal{A}$.

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 $\wp(A)$, 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 $A = \emptyset^c \in \mathcal{A}$. O par (\mathcal{A}, \cup) é um magma comutativo com elemento neutro \emptyset , pois a união de dois conjuntos 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}, \cap) 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 $X \in \mathcal{A}$, $X^c \in \mathcal{A}$ e vale $X \cup X^c = A$ e $X \cap X^c = \emptyset$. Logo $(\mathcal{A}, \cup, \cap)$ é uma álgebra booleana. ■

Proposição 4.19 (Princípio da Dualidade). *Toda afirmação dedutível 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 simetricamente 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 propriedades de álgebra booleana tem uma afirmação associada 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 4.20 (Identidades). *Seja (A, \vee, \wedge) uma álgebra booleana. Então*

$$\forall a \in A \quad a \vee 1 = 1$$

$$\forall a \in A \quad a \wedge 0 = 0$$

Teorema 4.21 (Absorção). *Seja (A, \vee, \wedge) uma álgebra booleana. Então*

$$\forall a, b \in A \quad a \vee (a \wedge b) = a$$

$$\forall a, b \in A \quad a \wedge (a \vee b) = a$$

Corolário 4.22 (Idempotência). *Seja (A, \vee, \wedge) uma álgebra booleana. Então*

$$\forall a \in A \quad a \vee a = a$$

$$\forall a \in A \quad a \wedge a = a$$

Demonstração. Basta tomar $b = 1$ e $b = 0$ nas proposições anteriores. ■

Teorema 4.23 (Associatividade). *Seja (A, \vee, \wedge) uma álgebra booleana. Então*

(A, \vee) é associativo.

(A, \wedge) é associativo.

Teorema 4.24 (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 4.25 (Dupla Complementação). *Seja (A, \vee, \wedge) uma álgebra booleana e $a \in A$. Então o complementar de a' é a .*

Teorema 4.26 (Identidades Complementares). *Seja (A, \vee, \wedge) uma álgebra booleana. Então*

$$0' = 1$$

$$1' = 0$$

Teorema 4.27 (Leis de De Morgan). *Seja (A, \vee, \wedge) uma álgebra booleana. Então*

$$\forall a, b \in A \quad (a \wedge b)' = a' \vee b'$$

$$\forall a, b \in A \quad (a \vee b)' = a' \wedge b'$$

Função Indicadora

Definição 4.24. Sejam X um conjunto. A *função indicadora* em X é a função

$$\begin{aligned} \mathbf{1}: \wp(X) &\longrightarrow 2^X \\ C &\longmapsto \mathbf{1}_C: X &\longrightarrow \{0, 1\} \\ x &\longmapsto \begin{cases} 1, & x \in C \\ 0, & x \notin C. \end{cases} \end{aligned}$$

A função indicadora é uma bijeção e mostra que os conjuntos $\wp(X)$ e 2^X têm a mesma cardinalidade. De fato, sabemos que $(\wp(X), \cap, \cup, \emptyset, X)$ é uma álgebra de conjuntos. Podemos também, usando a estrutura de álgebra em $\{0, 1\}$, dada pelas operações mínimo e máximo $\wedge, \vee: \{0, 1\} \times \{0, 1\} \longrightarrow \{0, 1\}$ e pelos os elementos 0 e 1, induzir uma álgebra em 2^X com as operações definidas pontualmente e as funções constantes $0, 1 \in 2^X$. Assim, podemos mostrar que a bijeção $\mathbf{1}: \wp(X) \longrightarrow 2^X$ é um isomorfismo de álgebras.

Proposição 4.28. *Seja X um conjunto. A função indicadora $\mathbf{1}: \wp(X) \longrightarrow 2^X$ de X é um isomorfismo entre as álgebras $(\wp(X), \cap, \cup, \emptyset, X)$ e $(2^X, \wedge, \vee, 0, 1)$.*

Demonstração. Para isso, devemos mostrar que $\mathbf{1}$ preserva as operações binárias e constantes das álgebras. É imediato verificar que, para todos $C, C' \in \wp(X)$, $\mathbf{1}_{C \cap C'} = \mathbf{1}_C \wedge \mathbf{1}_{C'}$, $\mathbf{1}_{C \cup C'} = \mathbf{1}_C \vee \mathbf{1}_{C'}$, e que $\mathbf{1}_\emptyset = 0$ e $\mathbf{1}_X = 1$. ■

Vale notar, também, que em $\{0, 1\}$ vale que, para todos $n, n' \in \{0, 1\}$, $n \wedge n' = nn'$ e $n \vee n' = n + n' - nn'$. Algumas outras relações da função indicadora estão expostas na proposição seguinte. Todas elas seguem diretamente do fato de $\mathbf{1}$ ser isomorfismo de álgebras. As demonstrações ficam como exercício.

Proposição 4.29. *Sejam X um conjunto e $A, B \subseteq X$, e $n \in \mathbb{N}$. Então*

1. $\mathbf{1}_{A^c} = 1 - \mathbf{1}_A$;
2. $\mathbf{1}_{A \setminus B} = \mathbf{1}_A - \mathbf{1}_A \mathbf{1}_B$;
3. $\mathbf{1}_{A \Delta B} = \mathbf{1}_A + \mathbf{1}_B - 2\mathbf{1}_A \mathbf{1}_B$;
4. $\mathbf{1}_{\bigcap_{i \in [n]} A_i} = \bigtimes_{i \in [n]} \mathbf{1}_{A_i}$;
5. $\mathbf{1}_{\bigcup_{i \in [n]} A_i} = \sum_{\substack{S \subseteq [n] \\ S \neq \emptyset}} \left((-1)^{|S|-1} \bigtimes_{i \in S} \mathbf{1}_{A_i} \right)$;
6. $\mathbf{1}_{\triangle_{i \in [n]} A_i} = \sum_{\substack{S \subseteq [n] \\ S \neq \emptyset}} \left((-2)^{|S|-1} \bigtimes_{i \in S} \mathbf{1}_{A_i} \right)$;

Capítulo 5

Cardinalidade de Conjuntos

5.1 Relações

5.1.1 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

$$|\mathbb{N}| := \aleph_0 \text{ e } |\mathbb{R}| := \mathfrak{c}.$$

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

1. $|X| = |X|$;
2. $|X| = |Y| \Rightarrow |Y| = |X|$;
3. $|X| = |Y| \text{ e } |Y| = |Z| \Rightarrow |X| = |Z|$.

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 $C : X \rightarrow Y$. Mas então $C^{-1} : Y \rightarrow X$ é uma bijeção de Y em X e, portanto, $|Y| = |X|$.
3. Se $|X| = |Y|$ e $|Y| = |Z|$, então existem bijeções $C_1 : X \rightarrow Y$ e $C_2 : Y \rightarrow Z$. Mas então $C_2 \circ C_1 : X \rightarrow Z$ é uma bijeção de X em Z 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 não existe um conjunto de todos os conjuntos no qual defini-la. Todas proposições sobre cardinalidades são, na verdade, proposições sobre funções entre conjuntos e convém saber que as propriedades acima valem.

5.1.2 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 $C : X \rightarrow Y$.

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 $C : X \rightarrow Y$.

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 $E : X \rightarrow \mathbb{N}$ 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. $|X| \leq |Y| \text{ e } |Y| \leq |X| \Rightarrow |X| = |Y|;$
3. $|X| \leq |Y| \text{ e } |Y| \leq |Z| \Rightarrow |X| \leq |Z|;$
4. $|X| \leq |Y| \text{ ou } |Y| \leq |X|.$

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

2. Teorema de Cantor-Schröder-Bernstein.

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

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

5.2 Operações

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

1. $|X| + |Y| := |X + Y|;$
2. $|X| \times |Y| := |X \times Y|;$
3. $|X|^{|Y|} := |X^Y|.$

5.2.1 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

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

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 $c \in C_i$. \blacksquare

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 $C := C_j$. Como todos os conjuntos de $(C_i)_{i \in I}$ têm a mesma cardinalidade, para todo $i \in I$, seja $f_i : C_i \rightarrow C$ bijeção. Considere a função

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

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

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

\blacksquare

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 $|C_j| := \min_{i \in I} |C_i|$ e $C := C_j$. Para cada $i \in I$, existe função injetiva $f_i : C \rightarrow C_i$. Considere a função

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

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 $|C_j| := \max_{i \in I} |C_i|$ e $C := C_j$. Para cada $i \in I$, existe função sobrejetiva $f_i : C_i \rightarrow C$. Considere a função

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

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 $\mathbf{N} = (N, 0, s)$ em que

1. N é um conjunto, o *conjunto de números naturais*;
2. $0 \in N$, o *zero* de \mathbf{N} ;
3. $s : N \rightarrow N$ 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 \mathbf{N} é o elemento $1 := s(0)$.

Pela teoria de conjuntos, é possível definir um conjunto infinito \mathbf{N} que satisfaz os axiomas de um modelo de números naturais. A construção considera $0 := \emptyset$, $1 := \{0\}$, e, de modo geral, $s(n) := n \cup \{n\} = \{0, 1, \dots, n\}$. 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 \mathbf{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 $I := \{n \in N : n = 0 \text{ ou } \exists m \in N \quad n = s(m)\}$. 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 \mathbf{N} um modelo de números naturais. Existe uma única função*

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

que satisfaç

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

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 $I := \{n \in N : \exists! n_3 \in N \quad n_1 + n = n_3\}$. 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 $+_1, +_2 : N \times N \longrightarrow N$ funções satisfazendo $(A_1), (A_2)$, $n_1 \in N$ e $I := \{n \in N : n_1 +_1 n = n_1 +_2 n\}$. 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 \mathbf{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 \mathbf{N} um modelo de números naturais. Então*

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

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

$$(n_1 + n_2) + 0 = n_1 + n_2 \quad (\text{A1})$$

$$= n_1 + (n_2 + 0). \quad (\text{A1})$$

Agora, seja $n \in I$. Então

$$(n_1 + n_2) + s(n) = s((n_1 + n_2) + n) \quad (\text{A2})$$

$$= s(n_1 + (n_2 + n)) \quad (n \in I)$$

$$= n_1 + s(n_2 + n) \quad (\text{A2})$$

$$= n_1 + (n_2 + s(n)), \quad (\text{A2})$$

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

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

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

Demonstração. Seja $n \in N$. Então

$$s(n) = s(n + 0) = n + s(0) = n + 1. \quad \blacksquare$$

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

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

Demonstração. Demonstraremos ambas afirmações por indução em n .

1. Seja $I := \{n \in N : 0 + n = n\}$. 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 $I := \{n \in N : 1 + n = n + 1\}$. 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*

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

Demonstração. Demonstraremos a afirmação por indução. Seja $n_1 \in N$ e $I := \{n \in N : n_1 + n = n + n_1\}$. 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*

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

que satisfaz

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

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 $I := \{n \in N : \exists! n_3 \in N \quad n_1 \times n = n_3\}$. Primeiro, notemos que $0 \in I$, pois $n_1 \times 0 = 0$ e, portanto, n_3 existe 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 $\times_1, \times_2 : N \times N \rightarrow N$ funções satisfazendo $(M_1), (M_2)$, $n_1 \in N$ e $I := \{n \in N : n_1 \times_1 n = n_1 \times_2 n\}$. 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 $\times_1 = \times_2$. \blacksquare

Definição 6.3. Seja 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 N um modelo de números naturais. Então*

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

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

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

Agora, seja $k \in I$. Então

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

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

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

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

Agora, seja $k \in I$. Então

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

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*

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

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

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

Agora, seja $k \in I$. Então

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

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

Demonstração. 1. Vamos mostrar por indução em n . Seja $I := \{n \in N : 0 \times n = 0\}$. 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 $I := \{n \in N : 1 \times n = n\}$. 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 \mathbf{N} um modelo de números naturais. Então*

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

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

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

Agora, seja $m \in I$. Então

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

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

6.1.3 Ordenação

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

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

Demonstração. 1. Seja $I := \{k \in N : \forall n, m \in N \quad n + k = m + k \implies n = m\}$. 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 \mathbf{N} um modelo dos números naturais. A relação binária \leq em N é definida por

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

Proposição 6.13. Seja \mathbf{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 $I := \{m \in N : n \leq m \text{ ou } m \leq n\}$. Primeiro, notemos que $0 \in I$, pois $0+n = n$, logo $0 \leq n$. Agora, seja $m \in I$. Se $n \neq m$, 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 \mathbf{N} um modelo de números naturais. Então (\mathbf{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 $I := \{m \in N : \forall n \in C \quad m < n\}$. Inicialmente, ressaltamos 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 $\emptyset = C \cap I = C \cap N = C$. \blacksquare

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

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

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 \blacksquare

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

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

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, $n_1 \times n_2 \leq m_1 \times m_2$. \blacksquare

6.1.4 Base Doze

Na base doze, os caracteres que usamos são:

Símbolo	Nome
0	Zero
1	Um
2	Dois
3	Três
4	Quatro
5	Cinco
6	Seis
7	Sete
8	Oito
9	Nove
2	Dez
3	Onze

A tabela de multiplicação é:

0	1	2	3	4	5	6	7	8	9	10	3	2	10
1	1	2	3	4	5	6	7	8	9	10	3	2	10
2	2	4	6	8	10	12	14	16	18	20	12	17	20
3	3	6	9	10	13	16	19	20	23	26	29	30	
4	4	8	10	14	18	20	24	28	30	34	38	40	
5	5	10	13	18	21	26	32	34	39	42	47	50	
6	6	12	16	20	26	30	36	40	46	50	56	60	
7	7	14	19	24	28	33	36	41	48	53	57	65	70
8	8	16	20	28	34	40	48	54	60	68	74	80	
9	9	18	23	30	39	46	53	60	69	76	83	90	
10	10	20	30	40	50	60	70	80	90	100			
02	02	04	06	08	10	12	14	16	18	20			
03	03	06	09	12	15	18	21	24	27	30			

6.2 Números Inteiros

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

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

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 $(n_1, n_2) \sim (n_2, n_1)$. 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 \mathbf{N} um modelo de números naturais com a equivalência \sim . O *modelo de números inteiros* associado a \mathbf{N} é o par $\mathbf{Z} = (\mathbf{N}, Z)$, em que Z é o conjunto

$$Z := N \times N / \sim,$$

o conjunto dos números inteiros.

Proposição 6.18. *Seja \mathbf{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, consideremos 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 \mathbf{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 \mathbf{Z} um modelo de números inteiros. O *zero* de \mathbf{Z} é o elemento $0 := [(n, n)]$.

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

$$\begin{aligned} + : \mathbf{Z} \times \mathbf{Z} &\longrightarrow \mathbf{Z} \\ ([(n_1, n_2)], [(m_1, m_2)]) &\longmapsto [(n_1 + m_1, n_2 + m_2)]. \end{aligned}$$

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

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

Demonstração. Sejam $n, m \in \mathbf{Z}$ 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

$$\begin{aligned} [(n_1, n_2)] + [(m_1, m_2)] &= [(n_1 + m_1, n_2 + m_2)] \\ [(n'_1, n'_2)] + [(m'_1, m'_2)] &= [(n'_1 + m'_1, n'_2 + m'_2)]. \end{aligned}$$

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. \blacksquare

Proposição 6.20. Seja \mathbf{Z} um modelo de números inteiros. Então

1. $\forall n \in \mathbf{Z} \quad n + 0 = n;$
2. $\forall n, m, k \in \mathbf{Z} \quad (n + m) + k = n + (m + k);$
3. $\forall n, m \in \mathbf{Z} \quad n + m = m + n.$

Demonstração. Sejam $n, m, k \in \mathbf{Z}$ 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 \mathbf{Z} um modelo de números inteiros. A função *negativo* em \mathbf{Z} é a função

$$\begin{aligned}-: \mathbf{Z} &\longrightarrow \mathbf{Z} \\ [(n_1, n_2)] &\longmapsto [(n_2, n_1)].\end{aligned}$$

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 \mathbf{Z} um modelo de números inteiros. O *um* de \mathbf{Z} é o elemento $1 := [(n+1, n)]$.

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

$$\begin{aligned}\times: \mathbf{Z} \times \mathbf{Z} &\longrightarrow \mathbf{Z} \\ ([(n_1, n_2)], [(m_1, m_2)]) &\longmapsto [(n_1m_1 + n_2m_2, n_2m_1 + n_1m_2)].\end{aligned}$$

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

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

Demonstração. Sejam $n, m \in \mathbf{Z}$ 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

$$\begin{aligned}[(n_1, n_2)] \times [(m_1, m_2)] &= [(n_1m_1 + n_2m_2, n_2m_1 + n_1m_2)] \\ [(n'_1, n'_2)] \times [(m'_1, m'_2)] &= [(n'_1m'_1 + n'_2m'_2, n'_2m'_1 + n'_1m'_2)].\end{aligned}$$

Como $n_1 + n'_2 = n_2 + n'_1$ e $m_1 + m'_2 = m_2 + m'_1$, segue que

$$\begin{aligned} & (n_1m_1 + n_2m_2 + n'_2m'_1 + n'_1m'_2) + (n_1m'_2 + n_2m'_1 + n_1m'_1 + n_2m'_2) \\ &= n_1(m_1 + m'_2) + n_2(m_2 + m'_1) + (n'_2 + n_1)m'_1 + (n'_1 + n_2)m'_2 \\ &= n_1(m'_1 + m_2) + n_2(m'_2 + m_1) + (n_2 + n'_1)m'_1 + (n_1 + n'_2)m'_2 \\ &= (n_2m_1 + n_1m_2 + n'_1m'_1 + n'_2m'_2) + (n_1m'_2 + n_2m'_1 + n_1m'_1 + n_2m'_2), \end{aligned}$$

o que implica que

$$n_1m_1 + n_2m_2 + n'_2m'_1 + n'_1m'_2 = n_2m_1 + n_1m_2 + n'_1m'_1 + n'_2m'_2$$

e, portanto, $(n_1m_1 + n_2m_2, n_2m_1 + n_1m_2) \sim (n'_1m'_1 + n'_2m'_2, n'_2m'_1 + n'_1m'_2)$, o que mostra que o produto $n \times m$ está bem definido. \blacksquare

6.2.3 Ordenação

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

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

Proposição 6.22. Seja \mathbb{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

Parte II

Álgebra

Capítulo 7

Operações Binárias e Estruturas Básicas

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.

7.1 Operações Binárias

Definição 7.1. Seja X um conjunto não vazio. Uma *operação binária* em X é uma função

$$\begin{aligned} *: X \times X &\longrightarrow X \\ (x_1, x_2) &\longmapsto x_1 * x_2. \end{aligned}$$

Proposição 7.1 (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, para todos $y_1, y_2 \in Y$*

$$y_1 * y_2 \in Y.$$

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 7.2. Seja X um conjunto. Uma operação binária *associativa* é uma operação binária $* : X \times X \rightarrow X$ que satisfaz, para todos $x_1, x_2, x_3 \in X$,

$$(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3).$$

Uma operação binária *comutativa* é uma operação binária $* : X \times X \rightarrow X$ que satisfaz, para todos $x_1, x_2 \in X$

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

Definição 7.3. Sejam X um conjunto e $+$ uma operação binária em X . Uma operação binária *distributiva* sobre $+$ é uma operação binária \times em X que satisfaz, para todos $x_1, x_2, x_3 \in X$,

$$x_1 \times (x_2 + x_3) = (x_1 \times x_2) + (x_1 \times x_3).$$

7.2 Magma

Definição 7.4. Um *magma* é um par $\mathbf{X} = (X, *)$ em que X é um conjunto não vazio e $*$ é uma operação binária em X .

Definição 7.5 (Identidade). Seja $\mathbf{X} = (X, *)$ um magma. Uma *identidade* com respeito a $*$ é um elemento $I \in X$ que satisfaz, para todo $x \in X$,

$$I * x = x = x * I.$$

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

Proposição 7.2. Seja $\mathbf{X} = (X, *)$ um magma. Se existe identidade com respeito a $*$, ela é única.

Demonstração. Suponha que existam duas identidades com respeito a $*$, I_1 e I_2 . Então

$$I_1 = I_1 * I_2 = I_2.$$

■

Definição 7.6 (Operação com conjuntos). Sejam \mathbf{X} um magma, $A, B \subseteq X$ e $x \in X$. Definimos

$$\begin{aligned} x * A &:= \{x * a \mid a \in A\} \\ A * x &:= \{a * x \mid a \in A\} \\ A * B &:= \{a * b \mid a \in A, b \in B\}. \end{aligned}$$

7.3 Semigrupo

Definição 7.7. Um *semigrupo* é um magma $\mathbf{X} = (X, *)$ em que $*$ é associativa. Um semigrupo *comutativo* é um semigrupo em que $*$ é comutativa.

Definição 7.8. Seja $\mathbf{X} = (X, *)$ um semigrupo, $n \in \mathbb{N}^*$ e $(x_i)_{i \in [n]}$ elementos de X . O *operatório* desses elementos é

$$\underset{i \in [n]}{\mathbin{\bigstar}} x_i := \begin{cases} x_0, & n = 1 \\ x_{n-1} * \underset{i \in [n-1]}{\mathbin{\bigstar}} x_i, & n > 1. \end{cases}$$

Notação. Costumamos denotar essa operação por

$$x_n * \cdots * x_0 := \underset{i \in [n]}{\mathbin{\bigstar}} x_i = (x_{n-1} * (\cdots (x_1 * x_0)))$$

O símbolo usado para a soma $+$ é o *somatório* $\textcolor{red}{+}$ e o símbolo usado para o produto \times é o *produtório* $\textcolor{blue}{\times}$. Essa definição considera que as operações vão sendo feitos à esquerda, mas uma mesma definição poderia ter sido feita para operações à direita — todas demonstrações ainda valeriam, considerando que as ordens fossem devidamente trocadas.

Proposição 7.3. Sejam $\mathbf{X} = (X, *)$ um semigrupo, $n, k \in \mathbb{N}^*$ e $(x_i)_{i \in [n+k]}$ elementos de X . Então

$$\underset{i \in [n+k]}{\mathbin{\bigstar}} x_i = \underset{i \in [k]}{\mathbin{\bigstar}} x_{n+i} * \underset{i \in [n]}{\mathbin{\bigstar}} x_i.$$

Demonstração. A demonstração será por indução em k . Se $k = 1$, por definição segue que

$$\underset{i \in [n+1]}{\mathbin{\bigstar}} x_i = x_n * \underset{i \in [n]}{\mathbin{\bigstar}} x_i = \underset{i \in [1]}{\mathbin{\bigstar}} x_{n+i} * \underset{i \in [n]}{\mathbin{\bigstar}} x_i.$$

Considere agora que vale a igualdade para algum $k \in \mathbb{N}^*$. Então

$$\begin{aligned} \underset{i \in [n+k+1]}{\mathbin{\bigstar}} x_i &= x_{n+k} * \underset{i \in [n+k]}{\mathbin{\bigstar}} x_i \\ &= x_{n+k} * \left(\underset{i \in [k]}{\mathbin{\bigstar}} x_{n+i} * \underset{i \in [n]}{\mathbin{\bigstar}} x_i \right) \\ &= \left(x_{n+k} * \underset{i \in [k]}{\mathbin{\bigstar}} x_{n+i} \right) * \underset{i \in [n]}{\mathbin{\bigstar}} x_i \\ &= \underset{i \in [k+1]}{\mathbin{\bigstar}} x_{n+i} * \underset{i \in [n]}{\mathbin{\bigstar}} x_i. \end{aligned}$$
■

Proposição 7.4 (Associatividade Generalizada). *Sejam $\mathbf{X} = (X, *)$ um semi-grupo, $n \in \mathbb{N}^*$, $(x_i)_{i \in [n]}$ elementos de X e $(k_j)_{j \in [p]}$ uma partição de $[n]$ (ou seja: $n = +_{j \in [p]} k_j$ e, para todos $j \in [p]$, $k_j \neq 0$). Então*

$$\underset{i \in [n]}{\mathbin{\boldsymbol{*}}} x_i = \underset{j \in [p]}{\mathbin{\boldsymbol{*}}} \left(\underset{i \in [k_j]}{\mathbin{\boldsymbol{*}}} x_{i+k_0+\dots+k_{j-1}} \right).$$

Demonstração. Segue por indução da proposição anterior. ■

Essa proposição diz que podemos colocar os parênteses como quisermos que o resultado será o mesmo, pois

$$\underset{j \in [p]}{\mathbin{\boldsymbol{*}}} \left(\underset{i \in [k_j]}{\mathbin{\boldsymbol{*}}} x_{i+k_0+\dots+k_{j-1}} \right) = \left(\underset{i \in [k_{p-1}]}{\mathbin{\boldsymbol{*}}} x_{i+k_0+\dots+k_{p-2}} \right) * \dots * \left(\underset{i \in [k_0]}{\mathbin{\boldsymbol{*}}} x_i \right)$$

e a partição $(k_j)_{j \in [p]}$ determina essa separação.

Proposição 7.5 (Comutatividade Generalizada). *Sejam $\mathbf{X} = (X, *)$ um semi-grupo comutativo e $n \in \mathbb{N}^*$. Então, para toda bijeção $\psi: [n] \rightarrow [n]$,*

$$\underset{i \in [n]}{\mathbin{\boldsymbol{*}}} x_{\psi(i)} = \underset{i \in [n]}{\mathbin{\boldsymbol{*}}} x_i.$$

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 algum $n \in \mathbb{N}^*$ e seja $\psi: [n+1] \rightarrow [n+1]$ uma bijeção. Definamos $k = \psi^{-1}(n)$ e a bijeção

$$\begin{aligned} \phi: [n] &\rightarrow [n] \\ i &\mapsto \begin{cases} \psi(m) & i < k \\ \psi(m+1) & i > k. \end{cases} \end{aligned}$$

Da associatividade generalizada, da comutatividade e da hipótese para n , segue

que

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

7.4 Homomorfismo de Semigrupos

Definição 7.9. Sejam $\mathbf{X}_1 = (X_1, *_1)$ e $\mathbf{X}_2 = (X_2, *_2)$ semigrupos. Um *homomorfismo de semigrupos* de \mathbf{X}_1 para \mathbf{X}_2 é uma função $h : X_1 \rightarrow X_2$ que satisfaz, para todos $x, x' \in X_1$

$$h(x *_1 x') = h(x') *_2 h(x').$$

Denota-se $h : \mathbf{X}_1 \rightarrow \mathbf{X}_2$.

Proposição 7.6 (Composição de homomorfismos). *Sejam $\mathbf{X}_1 = (X, *_1)$, $\mathbf{X}_2 = (X_2, *_2)$ e $\mathbf{X}_3 = (X_3, *_3)$ semigrupos e $h_1 : \mathbf{X}_1 \rightarrow \mathbf{X}_2$ e $h_2 : \mathbf{X}_2 \rightarrow \mathbf{X}_3$ homomorfismos de semigrupos. Então $h_2 \circ h_1 : \mathbf{X}_1 \rightarrow \mathbf{X}_3$ é homomorfismo de semigrupos.*

Demonstração. Sejam $x, x' \in X_1$. Então

$$\begin{aligned}
 (h_2 \circ h_1)(x *_1 x') &= h_2(h_1(x *_1 x')) \\
 &= h_2(h_1(x) *_2 h_1(x')) \\
 &= h_2(h_1(x)) *_3 h_2(h_1(x')) \\
 &= (h_2 \circ h_1)(x) *_3 (h_2 \circ h_1)(x').
 \end{aligned}$$
■

7.5 Monoide

Definição 7.10. Um *monoide* é uma tripla $\mathbf{M} = (M, *, I)$ em que $(M, *)$ é um semigrupo e I é uma identidade com respeito a $*$. Um monoide *comutativo* é um monoide cuja operação binária $*$ é comutativa.

Notação. Denotaremos a identidade de um monoide M por I_M quando houver ambiguidade. Ainda, como existe identidade, definimos

$$\bigstar_{i \in [0]} x_i = I.$$

Exemplo 7.1. O conjunto \mathbb{N} , com a operação binária

$$\begin{aligned} \max: \mathbb{N}^2 &\longrightarrow \mathbb{N} \\ (n, n') &\longmapsto \max\{n, n'\} \end{aligned}$$

e a identidade 0, formam um monoide comutativo.

Definição 7.11 (Inverso). Sejam $X = (X, *)$ um magma, I uma identidade com respeito a $*$ e $x \in X$. Um *inverso* de x com respeito a $*$ e I é um elemento $\bar{x} \in X$ que satisfaz

$$\bar{x} * x = I = x * \bar{x}.$$

Uma operação unária *inversa* com respeito a $*$ e I é uma operação unária

$$\begin{aligned} {}^{-1}: X &\longrightarrow X \\ x &\longmapsto x^{-1} \end{aligned}$$

tal que, para todo $x \in X$, x^{-1} é o inverso de x com respeito a $*$ e I .

Pode-se distinguir *inverso à esquerda* e *inverso à direita*, que seria o caso de \bar{x} se só satisfizesse, respectivamente, as igualdades da esquerda e da direita acima, mas não adotaremos essa distinção neste livro.

Proposição 7.7. Seja $(M, *, I)$ um monoide. Se $m \in M$ tem inverso com respeito a $*$ e I , ele é único.

Demonstração. Suponha que existam dois inversos \bar{m} e $\overline{\bar{m}}$ de m . Então

$$\bar{m} = \bar{m} * I = \bar{m} * (m * \overline{\bar{m}}) = (\bar{m} * m) * \overline{\bar{m}} = I * \overline{\bar{m}} = \overline{\bar{m}}. \quad \blacksquare$$

Notação. A unicidade do inverso nos permite denotar o inverso de um elemento $m \in M$ de algum modo fixo. Quando a operação binária é a adição (+), denotamos o inverso por $-m$; quando é a multiplicação (\times , \cdot , \circ), denotamo-lo por m^{-1} .

Proposição 7.8. Seja $(M, *, I)$ um monoide. Se $m \in M$ tem inverso com respeito a $*$ e I , então m^{-1} tem inverso e

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

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

Proposição 7.9. *Sejam $\mathbf{M} = (M, *, I)$ um monoide e $S \subseteq M$ um conjunto tal que*

1. (Identidade) $I \in S$.
2. (Fechamento) Para todos $s_1, s_2 \in S$, $s_1 * s_2 \in S$;

*Então $\mathbf{S} = (S, *_S, I)$ é um monoide. Ainda, se \mathbf{M} é comutativo, então \mathbf{S} é comutativo.*

Demonstração. Por simplicidade, definamos $\star := *_S$.

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 (7.1). (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 $I \in S$, da identidade de $*$ segue que

$$I \star s = I * s = s = s * I = s \star I.$$

Logo I é identidade de \mathbf{S} .

Por fim, suponhamos que \mathbf{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 \mathbf{S} é um monoide, isto é, que um subconjunto S de um monoide \mathbf{M} com a operação do monoide restrita a esse subconjunto formam um monoide, não podemos garantir que a identidade de \mathbf{S} é a mesmo que a de \mathbf{M} .

7.6 Homomorfismos de Monoides

Definição 7.13. Sejam $\mathbf{M}_1 = (M_1, *_1, I_1)$ e $\mathbf{M}_2 = (M_2, *_2, I_2)$ monoides. Um *homomorfismo de monoides* de \mathbf{M}_1 para \mathbf{M}_2 é uma função $h : M_1 \rightarrow M_2$ que satisfaz

1. h é um homomorfismo de semigrupos de \mathbf{M}_1 para \mathbf{M}_2 :
 - (a) para todos $m, m' \in M_1$, $h(m *_1 m') = h(m) *_2 h(m')$;
2. $h(I_1) = I_2$.

Denota-se $h : \mathbf{M}_1 \rightarrow \mathbf{M}_2$.

Podemos notar que precisamos garantir que a função h leve a identidade de um monoide para a identidade 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 da identidade do primeiro é a identidade 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 7.10 (Composição de homomorfismos). *Sejam $\mathbf{M}_1 = (M_1, *_1, I_1)$, $\mathbf{M}_2 = (M_2, *_2, I_2)$ e $\mathbf{M}_3 = (M_3, *_3, I_3)$ monoides e $h_1 : \mathbf{M}_1 \rightarrow \mathbf{M}_2$ e $h_2 : \mathbf{M}_2 \rightarrow \mathbf{M}_3$ homomorfismos de monoides. Então $h_2 \circ h_1 : \mathbf{M}_1 \rightarrow \mathbf{M}_3$ 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 (7.6).

2. Para mostrar que a identidade é preservada, basta notar que

$$(h_2 \circ h_1)(I_1) = h_2(h_1(I_1)) = h_2(I_2) = I_3.$$

■

Capítulo 8

Grupos

8.1 Construções Algébricas

8.1.1 Grupo e Subgrupo

Definição 8.1. Um *grupo* é uma quádrupla $\mathbf{G} = (G, *, \text{I}, \text{I}^{-1})$ em que G é um conjunto, $* : G \times G \longrightarrow G$ é uma operação binária associativa, $\text{I} \in G$ é uma identidade com respeito a $*$ e $\text{I}^{-1} : G \longrightarrow G$ é uma operação unária inversa com respeito a $*$ e I ; isto é, satisfazem

G1. (Associatividade) Para todos $g_1, g_2, g_3 \in G$,

$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3);$$

G2. (Identidade) Para todo $g \in G$,

$$\text{I} * g = g = g * \text{I};$$

G3. (Invertibilidade) Para todo $g \in G$,

$$g^{-1} * g = \text{I} = g * g^{-1}.$$

Um grupo *comutativo* é um grupo cuja operação $*$ é comutativa; isto é, satisfaz

G4. (Comutatividade) Para todos $g_1, g_2 \in G$,

$$g_1 * g_2 = g_2 * g_1.$$

Denota-se $g_1 * g_2$ 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 uma quádrupla $\mathbf{G} = (G, *, \text{I}, \text{ }^{-1})$ em que $(G, *, \text{I})$ é um monoide e $\text{ }^{-1} : G \rightarrow G$ é uma operação unária inversa com respeito a $*$ e I .

Definição 8.2. Sejam $\mathbf{G} = (G, *)$ um grupo, $g \in G$ e $n \in \mathbb{N}$. Definimos

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

Proposição 8.1 (Leis de corte e inversão). *Seja \mathbf{G} um grupo. Então*

1. $\forall g, g_1, g_2 \in G \quad gg_1 = gg_2 \Rightarrow g_1 = g_2.$
2. $\forall g, g_1, g_2 \in G \quad g_1g = g_2g \Rightarrow g_1 = g_2.$
3. $\forall g_1, \dots, g_n \in G \quad (g_1 \cdots g_n)^{-1} = g_n^{-1} \cdots g_1^{-1}.$

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. ■

Definição 8.3. Seja $\mathbf{G} = (G, *, \text{I}, \text{ }^{-1})$ um grupo. Um *subgrupo* de \mathbf{G} é um grupo $\mathbf{S} = (S, *|_{S \times S}, \text{I}_S, \text{ }^{-1}|_S)$ em que $S \subseteq G$, $*|_{S \times S} = *|_{S \times S}$, $\text{I}_S = \text{I}$ e $\text{ }^{-1}|_S = \text{ }^{-1}|_S$. Denota-se $\mathbf{S} \leq \mathbf{G}$. Um subgrupo *próprio* de \mathbf{G} é um subgrupo $\mathbf{S} \leq \mathbf{G}$ em que S é um conjunto próprio de G ($S \subset G$). Denota-se $\mathbf{S} < \mathbf{G}$.

Proposição 8.2. *Sejam \mathbf{G} um grupo e $S \subseteq G$ que satisfaz*

SG1. (Não-vacuidade) $S \neq \emptyset$;

SG2. (Fechamento) Para todos $s_1, s_2 \in S$, $s_1s_2 \in S$;

SG3. (Invertibilidade) Para todo $s \in S$, $s^{-1} \in S$.

*Então $\mathbf{S} = (S, *|_{S \times S})$ é um grupo. Ainda, se \mathbf{G} é comutativo, então \mathbf{S} é comutativo.*

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

(Operação binária) Pela primeira e segunda propriedades de S , segue que \star é uma operação binária (7.1). (G1) Sejam $s_1, s_2, s_3 \in S$. Então

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

(G2) Como $S \neq \emptyset$, existe $s \in S$, portanto $s^{-1} \in S$. Isso implica que $\mathbf{I} = s * s^{-1} \in S$ e, como \mathbf{I} é identidade de \mathbf{G} , segue que, para todo $s \in S$,

$$\mathbf{I} * s = \mathbf{I} * s = s = s * \mathbf{I} = s * \mathbf{I}.$$

(G3) Seja $s \in S$. Pela terceira propriedade de S , segue que o inverso de s em \mathbf{G} pertence a S . Então

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

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

(G4) Por fim, suponhamos que \mathbf{G} é um grupo comutativo. Sejam $s_1, s_2 \in S$. Como $*$ é comutativa, então

$$s_1 * s_2 = s_1 * s_2 = s_2 * s_1 = s_2 * s_1.$$

■

Proposição 8.3. *Sejam \mathbf{G} um grupo e \mathcal{G} o conjunto dos subgrupos de \mathbf{G} . Então (\mathcal{G}, \leq) é um conjunto parcialmente ordenado.*

Demonstração. Claramente, $\mathbf{G} \in \mathcal{G}$, portanto \mathcal{G} não é vazio. Mostremos que \leq é uma ordem parcial em \mathcal{G} . (Reflexividade) Seja $\mathbf{S} \in \mathcal{G}$. Então $\mathbf{S} \leq \mathbf{S}$, pois \mathbf{S} é um grupo, $S \subseteq S$ e $*|_{S \times S} = *|_{S \times S}$. (Antissimetria) Sejam $\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{G}$ tais que $\mathbf{S}_1 \leq \mathbf{S}_2$ e $\mathbf{S}_2 \leq \mathbf{S}_1$. 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 $\mathbf{S}_1 = \mathbf{S}_2$. (Transitividade) Sejam $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3 \in \mathcal{G}$ tais que $\mathbf{S}_1 \leq \mathbf{S}_2$ e $\mathbf{S}_2 \leq \mathbf{S}_3$. Então $S_1 \subseteq S_2$ e $S_2 \subseteq S_3$, o que implica $S_1 \subseteq S_3$ e, portanto, $*|_{S_1 \times S_3} = *|_{S_3 \times S_3}$. ■

Proposição 8.4. *Seja \mathbf{G} um grupo. Então $\{\mathbf{I}\}$ e \mathbf{G} são subgrupos de \mathbf{G} .*

Proposição 8.5. *Sejam \mathbf{G} um grupo, $(S_i)_{i \in I}$ uma família de subgrupos de \mathbf{G} e*

$$S := \bigcap_{i \in I} S_i.$$

Então \mathbf{S} é um subgrupo de \mathbf{G} .

Demonstração. (SG1) Para todo $i \in I$, $S_i \leq \mathbf{G}$, portanto $e \in N_i$. Logo $e \in N$.

(SG2) Sejam $s_1, s_2 \in S$. Para todo $i \in I$, $s_1, s_2 \in S_i$. Como $S_i \leq \mathbf{G}$, segue que $s_1 s_2 \in S_i$, o que implica que $s_1 s_2 \in S$. (SG3) Seja $s \in S$. Para todo $i \in I$, $s \in S_i$ e, como $S_i \leq \mathbf{G}$, segue que $s^{-1} \in S_i$, o que implica que $s^{-1} \in S$. ■

Proposição 8.6. *Sejam \mathbf{G} um grupo, $(S_i)_{i \in I}$ uma família superiormente dirigida de subgrupos de \mathbf{G} (para todos $i_1, i_2 \in I$, existe $i \in I$ tal que $S_{i_1} \subseteq S_i$ e $S_{i_2} \subseteq S_i$) e*

$$S := \bigcup_{i \in I} S_i.$$

Então \mathbf{S} é um subgrupo de \mathbf{G} .

Demonstração. (Não-vacuidade) Para todo $i \in I$, $S_i \leq \mathbf{G}$, 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 $S_i \leq \mathbf{G}$, 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 $S_i \leq \mathbf{G}$, 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 8.4. Seja 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 8.7. Seja $M = (M, *, I)$ um monoide. Então existe uma operação unária ${}^{-1} : M^* \rightarrow M^*$ tal que $\mathbf{M}^* = (M^*, *|_{M^* \times M^*}, I, {}^{-1})$ é um grupo.

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

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

Portanto

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

o que mostra que $m_1 m_2 \in M^*$. Ainda, note que $I \in M^*$, pois $I * I = I$. Como M^* é contém a identidade e fechado sob $*$, segue que $(M^*, *, I)$ é um monoide (7.9). Por fim, M^* é um grupo pois, por definição, todo elemento tem inverso e ele é único. ■

8.1.2 Coclasses e Índice de Subgrupo

Definição 8.5. Sejam \mathbf{G} um grupo, $S \leq \mathbf{G}$ um subgrupo e $g \in G$. A *coclasse à esquerda* de S em \mathbf{G} com representante g é o conjunto

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

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

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

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 8.8. Sejam \mathbf{G} um grupos, $\mathbf{S} \leq \mathbf{G}$ um subgrupo e $g_1g_2 \in G$. Então

1. $g_1(g_2S) = (g_1g_2)S$ e $(Sg_1)g_2 = S(g_1g_2)$
2. $g_1S = g_2S \Leftrightarrow g_2^{-1}g_1 \in S$ e $Sg_1 = Sg_2 \Leftrightarrow g_2^{-1}g_1 \in S$.

Demonstração. 1. (\subseteq) Seja $g \in g_1(g_2S)$. Existem $g' \in g_2S$ tal que $g = g_1g'$ e, portanto, existe $s \in S$ tal que $g' = g_2s$. Mas então, pela associatividade, $g = g_1(g_2s) = (g_1g_2)s$, e segue que $g \in (g_1g_2)S$. (\supseteq) Seja $g \in (g_1g_2)S$. Então existe $s \in S$ tal que $g = (g_1g_2)s$ e, da associatividade, segue que $g = g_1(g_2s)$, logo $g \in g_1(g_2S)$. A outra igualdade é análoga.

2. (\Leftarrow) Seja $g \in g_1S = g_2S$. Então existem $s, s' \in S$ tais que $g = g_1s = g_2s'$, logo $g_2^{-1}g_1 = s's^{-1}$. Como \mathbf{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 $g_1 = g_2s$, logo $g_1 \in g_2S$. Assim, dado $g \in g_1S$, existe $s' \in S$ tal que $g = g_1s'$. Como \mathbf{S} é subgrupo, $ss' \in S$, logo $g = g_2ss' \in g_2S$. (\supseteq) Da mesma forma, como \mathbf{S} é subgrupo, $g_1^{-1}g_2 = (g_2^{-1}g_1)^{-1} = s^{-1} \in S$, o que implica que $g_2 = g_1s^{-1} \in g_1S$. Assim, dado $g \in g_2S$, existe $s' \in S$ tal que $g = g_2s'$. Como \mathbf{S} é subgrupo, $s^{-1}s' \in S$, logo $g = g_1s^{-1}s' \in g_1S$. ■

Essa proposição nos permite denotar os conjuntos acima simplesmente por g_1g_2S e Sg_1g_2 , respectivamente.

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

Proposição 8.9. Sejam \mathbf{G} um grupo, $\mathbf{S} \leq \mathbf{G}$ um subgrupo e $g_1, g_2 \in G$. Então

$$|g_1S| = |g_2S|.$$

Demonstração. Considere a relação

$$\begin{aligned} f: g_1S &\longrightarrow g_2S \\ g &\longmapsto g_2g_1^{-1}g. \end{aligned}$$

Vamos mostrar que f é função; isto é, está bem definida, que $g_1^{-1}g \in S$. Primeiro, note que, se $g \in g_1S$, existe $s \in S$ tal que $g = g_1s$. Então segue que $f(s) = g_2g_1^{-1}g = g_2g_1^{-1}g_1s = g_2s \in g_2S$, o que mostra que f está bem definida. Agora, note que a função

$$\begin{aligned} f^{-1}: g_2S &\longrightarrow g_1S \\ g &\longmapsto g_1g_2^{-1}g, \end{aligned}$$

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

Proposição 8.10. *Sejam \mathbf{G} um grupo e $\mathbf{S} \leq \mathbf{G}$ um subgrupo. A relação binária \sim em G definida por*

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

é uma relação de equivalência e suas classes de equivalência são as coclasses à esquerda (à direita) de \mathbf{S} em \mathbf{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 $g_3^{-1}g_1 = g_3^{-1}g_2g_2^{-1}g_1 \in S$. 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, $s = gs'$. Logo $s \in gS$. Agora, seja $s \in gS$. Então existe $s' \in S$ tal que $s = gs'$, o que implica $g^{-1}s = s'$, que por sua vez implica $g^{-1}s \in S$ e, portanto, $s \sim g$. Logo $s \in [g]$. ■

Como \sim é relação de equivalência, partitiona G , e essas partições são as coclasses de \mathbf{S} em \mathbf{G} . Assim, podemos considerar o conjunto G/S das classes de equivalências como o conjunto das coclasses de S em \mathbf{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 8.6. Sejam \mathbf{G} um grupo e $\mathbf{S} \leq \mathbf{G}$ um subgrupo. O *conjunto quociente* de \mathbf{G} por \mathbf{S} é o conjunto

$$G/S := G/\sim.$$

Definição 8.7. Seja \mathbf{G} um grupo e $\mathbf{S} \leq \mathbf{G}$ subgrupo. O *índice* de \mathbf{S} em \mathbf{G} é número cardinal

$$[G : S] := |G/S|.$$

Proposição 8.11. *Sejam \mathbf{G} um grupo e $\mathbf{S} \leq \mathbf{G}$ 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 $|G| = [G : S] \times |S|$. ■

8.1.3 Subgrupo Normal e Grupo Quociente

Definição 8.8. Seja \mathbf{G} um grupo. Um subgrupo *normal* de \mathbf{G} é um subgrupo $\mathbf{N} \leq \mathbf{G}$ que satisfaça

SGN1. (Normalidade) Para todos $g \in G$ e $n \in N$, $gng^{-1} \in N$.

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

Proposição 8.12. *Sejam \mathbf{G} um grupo e $\mathbf{N} \leq \mathbf{G}$ um subgrupo. São equivalentes:*

1. $\mathbf{N} \trianglelefteq \mathbf{G}$;
2. Para todo $g \in G$, $N = gNg^{-1}$;
3. para todo $g \in G$, $gN = Ng$;
4. Para todos $g_1, g_2 \in G$, $g_1g_2N = g_2g_1N$.

Proposição 8.13. *Seja \mathbf{G} um grupo. Então $\{e\}$ e \mathbf{G} são subgrupos normais de \mathbf{G} .*

Proposição 8.14. Sejam \mathbf{G} um grupo, $(\mathbf{N}_i)_{i \in I}$ uma família de subgrupos normais de \mathbf{G} e

$$N := \bigcap_{i \in I} N_i.$$

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

Demonstração. (Subgrupo) Como $(\mathbf{N}_i)_{i \in I}$ uma família de subgrupos de \mathbf{G} , segue que N é um subgrupo de \mathbf{G} (8.5). (SGN1.) 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 $gng^{-1} \in N$. ■

Proposição 8.15. Sejam \mathbf{G} um grupo, $(\mathbf{N}_i)_{i \in I}$ uma família superiormente dirigida de subgrupos normais de \mathbf{G} (para todos $i_1, i_2 \in I$, existe $i \in I$ tal que $N_{i_1} \subseteq N_i$ e $N_{i_2} \subseteq N_i$) e

$$N := \bigcup_{i \in I} N_i.$$

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

Demonstração. (Subgrupo) Como $(\mathbf{N}_i)_{i \in I}$ uma família superiormente dirigida de subgrupos de \mathbf{G} , segue que N é um subgrupo de \mathbf{G} (8.6). (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 $gng^{-1} \in N$. ■

Definição 8.9. Seja \mathbf{G} um grupo e $N \trianglelefteq \mathbf{G}$ um subgrupo normal. O *grupo quociente* de \mathbf{G} por N é a quádrupla $\mathbf{G}/N = (G/N, *, \text{id}, {}^{-1})$, em que G/N é o conjunto quociente de G pela relação de equivalência induzida por N ,

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

e $(gN)^{-1} = g^{-1}N$.

Uma notação um pouco mais cuidadosa ressaltaria que as operações binárias de \mathbf{G} e de \mathbf{G}/N não são a mesma e, se denotarmos a primeira como $*$ e a segunda como \star , teríamos a definição acima nos dando $g_1N \star g_2N := (g_1 * g_2)N$. 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 \mathbf{G} , temos que $g_1g_2N = g_1(g_2N) = (g_1g_2)N$. O mesmo vale para ${}^{-1}$.

Proposição 8.16. Seja \mathbf{G} um grupo e $N \trianglelefteq \mathbf{G}$ um subgrupo normal. Então \mathbf{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 $g_1N = g'_1N$ e $g_2N = g'_2N$. Então

$$g_1g_2N = g_1Ng_2 = g'_1Ng_2 = g'_1N(g_2) = g'_1g_2N = g'_1g'_2N.$$

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

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

(identidade) Seja $g \in G$. Então

$$[I][g] = [Ig] = [g] = [gi] = [g][I].$$

(Invertibilidade) Seja $g \in G$. Então

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

■

8.1.4 Homomorfismo de Grupo

Definição 8.10. Sejam \mathbf{G}_1 e \mathbf{G}_2 grupos. Um *homomorfismo de grupos* de \mathbf{G}_1 para \mathbf{G}_2 é uma função $h : G_1 \rightarrow G_2$ que satisfaz, para todos $g_1, g_2 \in G_1$,

$$h(g_1g_2) = h(g_1)h(g_2).$$

Denota-se $h : \mathbf{G}_1 \rightarrow \mathbf{G}_2$. O conjunto desses homomorfismos é denotado $\mathcal{H}\text{om}(\mathbf{G}_1, \mathbf{G}_2)$.

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

Proposição 8.17 (Homomorfismos preservam a estrutura algébrica). *Sejam \mathbf{G}_1 e \mathbf{G}_2 grupos $h : G_1 \rightarrow G_2$ um homomorfismo de grupos. Então*

1. $h(I_1) = I_2$;
2. Para todo $g \in G_1$, $h(g)^{-1} = h(g^{-1})$.

Demonstração. Seja $g \in G_1$. Então

1.

$$\begin{aligned} h(I_1) &= h(I_1)I_2 \\ &= h(I_1)h(g)h(g)^{-1} \\ &= h(I_1g)h(g)^{-1} \\ &= h(g)h(g)^{-1} \\ &= I_2. \end{aligned}$$

2.

$$\begin{aligned}
 h(g)^{-1} &= h(g)^{-1}I_2 \\
 &= h(g)^{-1}h(I_1) \\
 &= h(g)^{-1}h(gg^{-1}) \\
 &= h(g)^{-1}h(g)h(g^{-1}) \\
 &= I_2h(g^{-1}) \\
 &= h(g^{-1}). \blacksquare
 \end{aligned}$$

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.

Proposição 8.18 (Composição de homomorfismos). *Sejam \mathbf{G}_1 , \mathbf{G}_2 e \mathbf{G}_3 grupos e $h_1 : \mathbf{G}_1 \rightarrow \mathbf{G}_2$ e $h_2 : \mathbf{G}_2 \rightarrow \mathbf{G}_3$ homomorfismos de grupos. Então $(h_2 \circ h_1) : \mathbf{G}_1 \rightarrow \mathbf{G}_3$ 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 (7.6). ■

Proposição 8.19. *Sejam \mathbf{G} um grupo e $\mathbf{N} \trianglelefteq \mathbf{G}$ um subgrupo normal. A projeção canônica $\pi : G \rightarrow G/N$, definida por*

$$\begin{aligned}
 \pi : G &\longrightarrow G/N \\
 g &\longmapsto gN,
 \end{aligned}$$

é um homomorfismo de grupos sobrejetivo.

Demonstração. Sejam $g_1, g_2 \in G$. Então, da definição de produto em \mathbf{G}/\mathbf{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 8.20. *Sejam \mathbf{G}_1 e \mathbf{G}_2 grupos e $h : \mathbf{G}_1 \rightarrow \mathbf{G}_2$ um homomorfismo de grupos. Se $\mathbf{S} \leq \mathbf{G}_2$ é um subgrupo, então $h^{-1}(\mathbf{S}) \leq \mathbf{G}_1$ é um subgrupo, e se $\mathbf{N} \trianglelefteq \mathbf{G}_2$ é um subgrupo normal, então $h^{-1}(\mathbf{N}) \trianglelefteq \mathbf{G}_1$ é um subgrupo normal.*

Demonstração. (SG1) Como $e_2 \in S$ e h é homomorfismo segue que $h(e_1) = e_2$, portanto $e_1 \in h^{-1}(S)$. (SG2) Sejam $s_1, s_2 \in h^{-1}(S)$. Então $h(s_1), h(s_2) \in S$ e, como 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, $s_1s_2 \in h^{-1}(S)$. (SG3) Seja $s \in h^{-1}(S)$. Então $h(s) \in S$

e, como \mathbf{S} é subgrupo, $h(s)^{-1} \in S$. Como h é homomorfismo, segue que $h(s^{-1}) = h(s)^{-1} \in S$ e, portanto, $s^{-1} \in h^{-1}(S)$. (SGN1.) 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 \mathbf{N} é subgrupo normal, segue que $h(g)h(n)h(g)^{-1} \in N$. Logo $gng^{-1} \in h^{-1}(N)$. ■

Proposição 8.21. *Sejam \mathbf{G}_1 e \mathbf{G}_2 grupos e $h : \mathbf{G}_1 \rightarrow \mathbf{G}_2$ um homomorfismo de grupos. Se $\mathbf{S} \leq \mathbf{G}_1$, então $h(\mathbf{S}) \leq \mathbf{G}_2$, e se h é sobrejetivo e $\mathbf{N} \trianglelefteq \mathbf{G}_1$ um subgrupo normal, então $h(\mathbf{N}) \trianglelefteq \mathbf{G}_2$.*

Demonstração. (SG1) Como $e_1 \in S$, segue que $e_2 = h(e_1) \in h(S)$. (SG2) 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 \mathbf{S} é subgrupo, segue que $s'_1 s'_2 \in S$ e, como h é homomorfismo, segue que

$$s_1 s_2 = h(s'_1)h(s'_2) = h(s'_2 s'_1) \in h(S).$$

(SG3) Seja $s \in h(S)$. Então existe $s' \in S$ tal que $h(s') = s$. Como \mathbf{S} é subgrupo, segue que $s^{-1} \in S$ e, portanto, $h(s)^{-1} = h(s^{-1}) \in h(S)$. (SGN1.) 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,

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

■

8.1.5 Núcleo, Imagem e Isomorfismo

Definição 8.11. Sejam \mathbf{G}_1 e \mathbf{G}_2 grupos e $h : \mathbf{G}_1 \rightarrow \mathbf{G}_2$ um homomorfismo de grupos. O *núcleo* de h é o conjunto

$$\text{nuc}(h) := h^{-1}(\mathbf{I}_2) = \{g \in G_1 \mid h(g) = \mathbf{I}_2\}$$

e a *imagem* de h é o conjunto

$$\text{im}(h) := h(G_1) = \{g_2 \in G_2 \mid \exists g_1 \in G_1, h(g_1) = g_2\}.$$

Proposição 8.22. *Sejam \mathbf{G}_1 e \mathbf{G}_2 grupos e $h : \mathbf{G}_1 \rightarrow \mathbf{G}_2$ um homomorfismo de grupos. Então h é injetiva se, e somente se, $\text{nuc}(h) = \{\mathbf{I}_1\}$.*

Demonstração. (\Rightarrow) Suponha que h é injetiva. Seja $n \in \text{nuc}(h)$. Então $h(n) = \mathbf{I}_2$. Mas $h(\mathbf{I}_1) = \mathbf{I}_2$ e, como h é injetiva, concluímos que $n = \mathbf{I}_1$.

(\Leftarrow) Suponha que $\text{nuc}(h) = \{\mathbf{I}_1\}$. Sejam $g_1, g_2 \in G_1$. Se $h(g_1) = h(g_2)$, temos que $h(g_1 g_2^{-1}) = h(g_1)h(g_2)^{-1} = \mathbf{I}_2$, o que implica que $g_1 g_2^{-1} = \mathbf{I}_1$, pois $\text{nuc}(h) = \{\mathbf{I}_1\}$. Logo $g_1 = g_2$, e concluímos que h é injetiva. ■

Definição 8.12. Sejam \mathbf{G}_1 e \mathbf{G}_2 grupos. Um *isomorfismo de grupos* é um homomorfismo de grupos invertível. O conjunto de todos esses isomorfismos é denotado por $\text{Iso}(\mathbf{G}_1, \mathbf{G}_2)$.

Proposição 8.23. *Sejam \mathbf{G}_1 e \mathbf{G}_2 grupos e $h : \mathbf{G}_1 \rightarrow \mathbf{G}_2$ um isomorfismo de grupos. Então $h^{-1} : \mathbf{G}_2 \rightarrow \mathbf{G}_1$ é um isomorfismo de grupos.*

Demonstração. Como h é bijetiva, sua inversa h^{-1} também é bijetiva. Sejam $g_1 g_2 \in G_2$. 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 8.13. Grupo *isomorfos* são grupos \mathbf{G}_1 e \mathbf{G}_2 para os quais existe isomorfismo $h : \mathbf{G}_1 \rightarrow \mathbf{G}_2$. Denota-se $\mathbf{G}_1 \simeq \mathbf{G}_2$.

Proposição 8.24. *Sejam \mathbf{G}_1 , \mathbf{G}_2 e \mathbf{G}_3 grupos. Então*

1. (*Reflexividade*) $\mathbf{G}_1 \simeq \mathbf{G}_1$;
2. (*Antissimetria*) $\mathbf{G}_1 \simeq \mathbf{G}_2 \Rightarrow \mathbf{G}_2 \simeq \mathbf{G}_1$;
3. (*Transitividade*) $\mathbf{G}_1 \simeq \mathbf{G}_2$ e $\mathbf{G}_2 \simeq \mathbf{G}_3 \Rightarrow \mathbf{G}_1 \simeq \mathbf{G}_3$.

Demonstração. 1. A função Id_{G_1} é um isomorfismo de grupos.

2. A inversa é um isomorfismo de grupos (8.23).
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.

8.1.6 Teoremas de Isomorfismo

Teorema 8.25 (1º teorema de isomorfismo). *Sejam \mathbf{G}_1 e \mathbf{G}_2 grupos e $h : \mathbf{G}_1 \rightarrow \mathbf{G}_2$ um homomorfismo de grupos. Então $\text{nuc}(h) \trianglelefteq \mathbf{G}_1$, $\text{im}(h) \leq \mathbf{G}_2$ e*

$$\mathbf{G}_1 / \text{nuc}(h) \simeq \text{im}(h).$$

Demonstração. Como $\text{nuc}(h) = h^{-1}(e_2)$ e $\{e_2\} \trianglelefteq \mathbf{G}_2$ (8.13), a proposição segue da proposição 8.20. Como $\text{im}(h) = h(\mathbf{G}_1)$ e $\mathbf{G}_1 \leq \mathbf{G}_1$ (8.13), a proposição segue da proposição 8.20. Por causa disso, $\mathbf{G}_1 / \text{nuc}(h)$ e $\text{im}(h)$ são grupos. Consideremos a função

$$\begin{aligned}\eta : \mathbf{G}_1 / \text{nuc}(h) &\longrightarrow \text{im}(h) \\ g \text{nuc}(h) &\longmapsto h(g).\end{aligned}$$

Primeiro mostremos que η é função. Sejam $g_1, g_2 \in \mathbf{G}_1$ tais que $g_1 \text{nuc}(h) = g_2 \text{nuc}(h)$. Então $g_2^{-1}g_1 \in \text{nuc}(h)$ (8.8), 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 $\eta(g_1 \text{nuc}(h)) = \eta(g_1 \text{nuc}(h))$.

Agora, mostremos que η é isomorfismo de grupos. Para simplificar as contas, denotamos $[g] = g \text{nuc}(h)$. Primeiro mostramos que η é homomorfismo. Sejam $g_1, g_2 \in \mathbf{G}_1$. 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 $[g] \in \text{nuc}(\eta)$. Então $\eta([g]) = I_2$, logo $h(a) = I_2$. Mas isso implica que $g \in \text{nuc}(h)$. Portanto $[g] = [I_1]$, e segue que $\text{nuc}(\eta) = \{[I_1]\}$, o que é equivalente à injetividade (8.22). (Sobrejetividade) Para todo $g \in \text{im}(h)$, existe $g' \in \mathbf{G}_1$ tal que $g = h(g')$. Mas $h(g') = \eta(g' \text{nuc}(h))$, e segue a sobrejetividade. ■

Teorema 8.26 (2º teorema de isomorfismo). *Sejam \mathbf{G} um grupo, $\mathbf{S} \leq \mathbf{G}$ um subgrupo e $\mathbf{N} \trianglelefteq \mathbf{G}$ um subgrupo normal. Então $\mathbf{SN} \leq \mathbf{G}$, $\mathbf{S} \cap \mathbf{N} \trianglelefteq \mathbf{S}$ e*

$$\mathbf{S} / \mathbf{S} \cap \mathbf{N} \simeq \mathbf{SN} / \mathbf{N}.$$

Teorema 8.27 (3º teorema de isomorfismo). *Sejam \mathbf{G} um grupo e $\mathbf{N} \trianglelefteq \mathbf{G}$ um subgrupo normal. Então*

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

$$(\mathbf{G}/\mathbf{N}) / (\mathbf{N}'/\mathbf{N}) \simeq \mathbf{G} / \mathbf{N}'.$$

8.2 Construções Categóricas

8.2.1 Produto de Grupos

Definição 8.14. Seja $(\mathbf{G}_i)_{i \in I} = (G_i, *_i, \mathbf{I}_i, {}^{-1})_{i \in I}$ uma família de grupos. O *produto* da família $(\mathbf{G}_i)_{i \in I}$ é a quádrupla

$$\prod_{i \in I} \mathbf{G}_i := (G, *_i, \mathbf{I}, {}^{-1}),$$

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

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

$$\mathbf{I} := (\mathbf{I}_i)_{i \in I} \text{ e } g^{-1} := (g_i^{-1})_{i \in I}.$$

Proposição 8.28. Seja $(\mathbf{G}_i)_{i \in I}$ uma família de grupos. Então o produto $\prod_{i \in I} \mathbf{G}_i$ é um grupo. Se para todo $i \in I$ \mathbf{G}_i é comutativo, então $\prod_{i \in I} \mathbf{G}_i$ é comutativo.

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

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

(Identidade) Para todo $g = (g_i)_{i \in I} \in G$,

$$\mathbf{I}g = (\mathbf{I}_i g_i)_{i \in I} = (g_i)_{i \in I} = g = (g_i)_{i \in I} = (g_i \mathbf{I}_i)_{i \in I} = g\mathbf{I}.$$

(Invertibilidade) Seja $g \in G$. Então

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

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

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

■

Proposição 8.29. Seja $(\mathbf{G}_i)_{i \in I}$ uma família de grupos. Para todo $i \in I$, a projeção canônica $\pi_i : \prod_{i \in I} G_i \longrightarrow G_i$ é um homomorfismo de grupos.

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

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

■

Proposição 8.30 (Propriedade Universal). *Sejam $(\mathbf{G}_i)_{i \in I}$ uma família de grupos, \mathbf{X} um grupo e, para todo $i \in I$, $h_i : \mathbf{X} \rightarrow \mathbf{G}_i$ um homomorfismo de grupos. Então existe um único homomorfismo de grupos $h : \mathbf{X} \rightarrow \prod_{i \in I} \mathbf{G}_i$ tal que, para todo $i \in I$, $\pi_i \circ h = h_i$ (o diagrama comuta).*

$$\begin{array}{ccc} & \prod_{i \in I} \mathbf{G}_i & \\ & \downarrow \pi_i & \\ \mathbf{X} & \xrightarrow{\quad h_i \quad} & \mathbf{G}_i \end{array}$$

h ↗

Demonstração. Defina a função

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

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,

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

■

8.2.2 Grupo Livre

Definição 8.15. Seja C um conjunto. O *conjunto de inversos formais* de C é o conjunto $C^{-1} := C \times \{-1\}$ e seus elementos são denotados $c^{-1} := (c, -1)$.

Uma *palavra* em C é uma sequência finita $(c_1, \dots, c_n) \in C^n$. 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 $p^{-1} := c_n^{-1} \cdots c_1^{-1}$.

Definição 8.16. Seja C um conjunto e p_1, p_2 palavras em $C \times \{1, -1\}$. A relação de equivalência entre as palavras p_1 e p_2 é definida por

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

$$C^* := \bigcup_{n \in \mathbb{N}} (C \times \{1, -1\})^n$$

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

$$\langle C \rangle := C^*/\sim$$

A inclusão é definida.

$$\begin{aligned} \iota: C &\longrightarrow \langle C \rangle \\ c &\longmapsto [c]. \end{aligned}$$

Proposição 8.31 (Propriedade Universal). *Seja C um conjunto, $\mathbf{X} = (X, \star)$ um grupo e $f: C \longrightarrow X$ uma função. Então existe um único homomorfismo de grupos $h: \langle C \rangle \longrightarrow \mathbf{X}$ tal que $h \circ \iota = f$ (o diagrama comuta).*

$$\begin{array}{ccc} \langle C \rangle & & \\ \uparrow \iota & \searrow h & \\ C & \xrightarrow{f} & \mathbf{X} \end{array}$$

Demonstração. Defina a função

$$\begin{aligned} h: \langle C \rangle &\longrightarrow X \\ [c_1 \cdots c_n] &\longmapsto f(c_1) \star \cdots \star f(c_n), \end{aligned}$$

de modo que $h([e]) = e_X$. Então, para todo $c \in C$,

$$h \circ \iota(c) = h(\iota(c)) = h([c]) = f(c).$$

Logo $h \circ \iota = f$. Para mostrar que é um homomorfismo de grupos, sejam $[c_1 \cdots c_n]$, $[d_1 \cdots d_m] \in \langle C \rangle$. Então

$$\begin{aligned} h([c_1 \cdots c_n][d_1 \cdots d_m]) &= h([c_1 \cdots c_n d_1 \cdots d_m]) \\ &= f(c_1) \star \cdots \star f(c_n) \star f(d_1) \star \cdots \star f(d_m) \\ &= h([c_1 \cdots c_n]) \star h([d_1 \cdots d_m]). \end{aligned}$$

Isso mostra a existência. Para mostrar a unicidade, seja $\bar{h} : \langle C \rangle \rightarrow X$ um homomorfismo de grupos tal que $\bar{h} \circ \iota = f$. Seja $[c_1 \cdots c_n] \in \langle C \rangle$. Como $[c_1 \cdots c_n] = [c_1] \cdots [c_n] = \iota(c_1) \cdots \iota(c_n)$, segue que

$$\begin{aligned}\bar{h}([c_1 \cdots c_n]) &= \bar{h}(\iota(c_1) \cdots \iota(c_n)) \\ &= \bar{h}(\iota(c_1)) \star \cdots \star \bar{h}(\iota(c_n)) \\ &= f(c_1) \star \cdots \star f(c_n) \\ &= h([c_1 \cdots c_n]),\end{aligned}$$

o que implica que $\bar{h} = h$. ■

8.2.3 Coproduto de Grupos

Definição 8.17. Seja $(G_i)_{i \in I}$ uma família de grupos. O *coproduto* da família $(G_i)_{i \in I}$ é o par

$$\bigsqcup_{i \in I} G_i := (G, *),$$

em que $G := \langle \bigsqcup_{i \in I} G_i \rangle$ é o grupo livre sobre o coproduto de conjuntos $\bigsqcup_{i \in I} G_i$ e

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

Proposição 8.32 (Propriedade Universal). *Sejam $(G_i)_{i \in I}$ uma família de grupos, $X = (X, *)$ um grupo e, para todo $i \in I$, $h_i : G_i \rightarrow X$ um homomorfismo de grupos. Então existe um único homomorfismo de grupos $h : \bigsqcup_{i \in I} G_i \rightarrow X$ tal que, para todo $i \in I$, $h \circ \iota_i = h_i$ (o diagrama comuta).*

$$\begin{array}{ccc} \bigsqcup_{i \in I} G_i & & \\ \downarrow \iota_i & \searrow h & \\ G_i & \xrightarrow{h_i} & X \end{array}$$

Demonstração. Defina a função

$$\begin{aligned}h: \left\langle \bigsqcup_{i \in I} G_i \right\rangle &\longrightarrow X \\ [(g_1, i_1) \cdots (g_n, i_n)] &\longmapsto h_{i_1}(g_1) \star \cdots \star h_{i_n}(g_n).\end{aligned}$$

Por simplicidade, seja $G := \langle \bigsqcup_{i \in I} G_i \rangle$. Para mostrar que h é homomorfismo, sejam $[(g_1, i_1) \cdots (g_n, i_n)]$ e $[(g'_1, i'_1) \cdots (g'_m, i'_m)] \in G$. Então

$$\begin{aligned} h([(g_1, i_1) \cdots (g_n, i_n)][(g'_1, i'_1) \cdots (g'_m, i'_m)]) \\ = h([(g_1, i_1) \cdots (g_n, i_n)(g'_1, i'_1) \cdots (g'_m, i'_m)]) \\ = h_{i_1}(g_1) \star \cdots \star h_{i_n}(g_n) \star h_{i'_1}(g'_1) \star \cdots \star h_{i'_m}(g'_m) \\ = h([(g_1, i_1) \cdots (g_n, i_n)]) \star h([(g'_1, i'_1) \cdots (g'_m, i'_m)]). \end{aligned}$$

■

8.3 Construções Específicas

8.3.1 Grupo Simples e Subgrupo Normal Maximal

Definição 8.18. Um *grupo simples* é um grupo não-trivial \mathbf{G} cujos únicos subgrupos normais são $\{\mathbf{e}\}$ e \mathbf{G} .

Definição 8.19. Seja \mathbf{G} um grupo. Um subgrupo normal *maximal* de \mathbf{G} é um subgrupo normal próprio $\mathbf{M} \triangleleft \mathbf{G}$ que satisfaz

1. (Maximalidade) Para todo $\mathbf{N} \trianglelefteq \mathbf{G}$,

$$M \subseteq N \Rightarrow N = M \text{ ou } N = G.$$

Proposição 8.33. Sejam \mathbf{G} um grupo e $\mathbf{M} \trianglelefteq \mathbf{G}$ um subgrupo normal. Então \mathbf{M} é maximal se, e somente se, \mathbf{G}/\mathbf{M} é simples.

Demonstração. Consideremos a projeção canônica

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

(\Rightarrow) Suponhamos que \mathbf{M} é maximal. Então \mathbf{M} é um subgrupo próprio, o implica que \mathbf{G}/\mathbf{M} é não-trivial. Seja $\mathbf{N} \trianglelefteq \mathbf{G}/\mathbf{M}$. Sabemos que $\pi^{-1}(\mathbf{N}) \trianglelefteq \mathbf{G}$ (8.20). Como $[\mathbf{e}] \in N$, então $\pi^{-1}([\mathbf{e}]) \subseteq \pi^{-1}(N)$. Notando que $\pi^{-1}([\mathbf{e}]) = \text{nuc}(\pi) = M$, segue que $M \subseteq \pi^{-1}(N)$. Como \mathbf{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, $N = \pi(\pi^{-1}(N)) = \pi(M) = \{[\mathbf{e}]\}$. No segundo caso, $N = \pi(\pi^{-1}(N)) = \pi(G) = G/M$. Portanto \mathbf{G}/\mathbf{M} é simples.

(\Leftarrow) Suponhamos que \mathbf{G}/\mathbf{M} é simples. Seja $\mathbf{N} \trianglelefteq \mathbf{G}$ tal que $M \subseteq N$. Como π é homomorfismo de grupos sobrejetivo, segue que $\pi(N) \trianglelefteq \mathbf{G}/\mathbf{M}$ (8.21). Como \mathbf{G}/\mathbf{M} é simples, então $\pi(N) = \{[\mathbf{e}]\}$ ou $\pi(N) = G/M$. No primeiro caso, $N = \text{nuc}(\pi) = M$. No segundo caso, $N = \pi^{-1}(\pi(N)) = \pi^{-1}(N) = G$. Logo \mathbf{M} é maximal. \blacksquare

Conjectura 8.34. Sejam \mathbf{G} um grupo e $\mathbf{N} \triangleleft \mathbf{G}$ um subgrupo normal próprio. Então \mathbf{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 $S \triangleleft \mathbf{G}$. Então (P, \subseteq) é um conjunto parcialmente ordenado com a contenção de conjuntos usual. Agora, seja $(C_i)_{i \in I}$ uma cadeia de (P, \subseteq) . Consideremos o conjunto $C := \bigcup_{i \in I} C_i$. Como

Notemos que P não é vazio, pois $N \in P$. Seja

Então P tem elemento maximal. \blacksquare

8.3.2 Sequência subnormal

Definição 8.20. Seja \mathbf{G} um grupo. Uma *sequência subnormal* de \mathbf{G} é uma sequência finita $(\mathbf{N}_i)_{i \in [n]}$ de subgrupos de \mathbf{G} que satisfaz

$$\{e\} = \mathbf{N}_0 \trianglelefteq \cdots \trianglelefteq \mathbf{N}_{n-1} = \mathbf{G}.$$

O grupo $\mathbf{N}_{i+1}/\mathbf{N}_i$ é o i -ésimo *grupo fator* da sequência. Uma *sequência normal* é uma sequência subnormal em que, para todo $i \in [n]$, $\mathbf{N}_i \trianglelefteq \mathbf{G}$.

Uma sequência subnormal *estrita* de \mathbf{G} é uma sequência subnormal $(\mathbf{N}_i)_{i \in [n]}$ de \mathbf{G} que satisfaz

$$\{e\} = \mathbf{N}_0 \triangleleft \cdots \triangleleft \mathbf{N}_{n-1} = \mathbf{G}.$$

O comprimento

8.3.3 Conjunto gerador

Definição 8.21. Seja \mathbf{G} um grupo e $S \subseteq G$ um conjunto. O grupo *gerado* por S é o grupo $\langle S \rangle \leq \mathbf{G}$ em que

$$\langle S \rangle := \left\{ s_1 \cdots s_n \mid n \in \mathbb{N}, s_i \in S \text{ ou } s_i^{-1} \in S \right\}.$$

$$\langle S \rangle := \left\{ \bigstar_{i \in [n]} s_i \mid n \in \mathbb{N}, s_i \in S \text{ ou } s_i^{-1} \in S \right\}.$$

Um *conjunto gerador* de \mathbf{G} é um conjunto $S \subseteq G$ tal que $\langle S \rangle = G$.

8.3.4 Grupos Simétricos e Alternados

Definição 8.22. Seja C um conjunto. O *grupo simétrico* de C é o par $\mathfrak{S}(C) = (\mathfrak{S}(C), \circ)$, em que

$$\mathfrak{S}(C) := \left\{ p : C \longrightarrow C \mid \exists p^{-1} : C \longrightarrow C \right\}$$

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 $\mathfrak{S}_\alpha := \mathfrak{S}(\alpha)$.

Proposição 8.35. Seja C um conjunto. O grupo simétrico $\mathfrak{S}(C)$ 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 elemento 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 $p_1, p_2 \in \mathfrak{S}(C)$. Como p_1 e p_2 são bijeções, a função $p_2 \circ p_1 : C \longrightarrow C$ 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 I_C é o elemento neutro de $\mathfrak{S}(C)$, pois, para todo $p \in \mathfrak{S}(C)$, vale $p \circ I_C = I_C \circ p = p$ (3.7). Por fim, como p é uma bijeção, existe função inversa $p^{-1} : C \rightarrow C$ que é bijeção entre C e C (3.8 e 3.9); logo existe $p^{-1} \in \mathfrak{S}(C)$ tal que $p \circ p^{-1} = p^{-1} \circ p = I_C$. Portanto concluímos que $\mathfrak{S}(C)$ é um grupo. \blacksquare

Proposição 8.36. *Sejam A e B conjuntos tais que $|A| = |B|$. Então*

$$\mathfrak{S}(A) \simeq \mathfrak{S}(B).$$

Demonstração. Seja $\phi : A \rightarrow B$ uma bijeção e considere a função

$$\begin{aligned} h : \mathfrak{S}(A) &\longrightarrow \mathfrak{S}(B) \\ p &\longmapsto \phi \circ p \circ \phi^{-1}. \end{aligned}$$

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 $\mathfrak{S}(A)$ e $\mathfrak{S}(B)$.

Agora notemos que h é uma bijeção. A inversa de h é a função

$$\begin{aligned} h^{-1} : \mathfrak{S}(B) &\longrightarrow \mathfrak{S}(A) \\ p &\longmapsto \phi^{-1} \circ p \circ \phi, \end{aligned}$$

pois, para todo $p \in \mathfrak{S}(B)$,

$$\begin{aligned} (h \circ h^{-1})(p) &= h(h^{-1}(p)) \\ &= \phi \circ h^{-1}(p) \circ \phi^{-1} \\ &= \phi \circ (\phi^{-1} \circ p \circ \phi) \circ \phi^{-1} \\ &= p \\ &= I_{\mathfrak{S}(B)}(p), \end{aligned}$$

o que mostra que $h \circ h^{-1} = I_{\mathfrak{S}(B)}$, e, para todo $p \in \mathfrak{S}(A)$,

$$\begin{aligned} (h^{-1} \circ h)(p) &= h^{-1}(h(p)) \\ &= \phi^{-1} \circ h(p) \circ \phi \\ &= \phi^{-1} \circ (\phi \circ p \circ \phi^{-1}) \circ \phi \\ &= p \\ &= I_{\mathfrak{S}(A)}(p), \end{aligned}$$

o que mostra que $h^{-1} \circ h = I_{\mathfrak{S}(A)}$. Assim, está provado que h é isomorfismo entre $\mathfrak{S}(A)$ e $\mathfrak{S}(B)$. \blacksquare

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 8.37. *Seja $n \in \mathbb{N}$. Então $|\mathfrak{S}_n| = n!$.*

Teorema 8.38. *Seja G um grupo. Então*

$$G \lesssim \mathfrak{S}(G).$$

Demonstração. Consideremos a função

$$\begin{aligned} h : G &\longrightarrow \mathfrak{S}(G) \\ g &\longmapsto h(g) : G \longrightarrow G \\ x &\longmapsto g * x \end{aligned}$$

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 $x \in G$,

$$(h(g) \circ h(g)^{-1})(x) = h(g)((h(g)^{-1})(x)) = h(g)(g^{-1} * x) = g * g^{-1} * x = x = I_G,$$

o que mostra que $h(g) \circ h(g)^{-1} = I_G$, e

$$(h(g)^{-1} \circ h(g))(x) = h(g)^{-1}((h(g))(x)) = h(g)^{-1}(g * x) = g^{-1} * g * x = x = I_G,$$

o que mostra que $h(g)^{-1} \circ h(g) = I_G$. 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 $x \in G$,

$$g * x = h(g)(x) = I_G(x) = x,$$

o que mostra que $g = e_G$ e, portanto, que $\text{nuc}(h) = \{e_G\}$. \blacksquare

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.

Permutações e Órbitas

Definição 8.23. 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

$$p_2 \circ p_1 = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ p_2(1) & p_2(2) & \cdots & p_2(n-1) & p_2(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ p_1(1) & p_1(2) & \cdots & p_1(n-1) & p_1(n) \end{pmatrix}.$$

Definição 8.24. 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

$$[\mathfrak{S}_n] := \{[p] \mid p \in \mathfrak{S}_n\}.$$

Proposição 8.39. Seja $n \in \mathbb{N}$. Então o par $([\mathfrak{S}_n], \cdot)$, em que \cdot é o produto de matrizes, é um grupo,

$$\mathfrak{S}_n \simeq [\mathfrak{S}_n].$$

Demonstração. Primeiro, notemos que, para todos $p, q \in \mathfrak{S}_n$,

$$[p][q]_{i,j} = \sum_{k=0}^{n-1} [p]_{i,k}[q]_{k,j} = \sum_{k=0}^{n-1} \delta_{i,p(k)}\delta_{k,q(j)}.$$

Mas o produto $\delta_{i,p(k)}\delta_{k,q(j)}$ é igual a 1 se, e somente se, $i = p(k)$ e $k = q(j)$. Como p é bijeção, a segunda condição é equivalente a $p(k) = q(j)$, e isso mostra que as

duas consições são equivalentes a $i = p(k) = pq(j)$. Como p é bijeção, para cada $i \in [n]$, $k = p^{-1}(i)$ é o único $k \in [n]$ tal que a condição é satisfeita, e segue que

$$[p][q]_{i,j} = \sum_{k=1}^n \delta_{i,p(k)} \delta_{k,p(j)} = \sum_{k=1}^n \delta_{i,pq(j)} = [pq]_{i,j}.$$

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 $[p][p^{-1}] = [pp^{-1}] = [id]$

Disso, segue que $[\mathfrak{S}_n]$ é um grupo, pois é subgrupo de $\mathbb{M}_n(\mathbb{Z})$. Por fim, consideremos a função

$$\begin{aligned} h: \mathfrak{S}_n &\longrightarrow [\mathfrak{S}_n] \\ p &\longmapsto [p]. \end{aligned}$$

Note 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 8.25. Sejam $n \in \mathbb{N}$, $p \in \mathfrak{S}_n$ e $m \in [n]$. A *órbita de m sob p* é o conjunto

$$\mathcal{O}_p(m) := \{p^k(m) \mid k \in \mathbb{Z}\}.$$

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 $m \in [n]$ sob p .

O *conjunto de órbitas* de p é o conjunto

$$\mathcal{O}_p := \{\mathcal{O}_p(m) \mid m \in [n]\}.$$

Proposição 8.40. Sejam $n \in \mathbb{N}$ e $p \in \mathfrak{S}_n$. O conjunto \mathcal{O}_p é uma partição de $[n]$.

Demonstração. Primeiro, notemos que $m \in \mathcal{O}_p(m)$ e, portanto, $\emptyset \not\subseteq \mathcal{O}_p$. Ainda, $\bigcup_{m \in [n]} \mathcal{O}_p(m) = [n]$, já que, para todo $m \in [n]$, $m \in \mathcal{O}_p(m)$, o que mostra que $[n] \subseteq \bigcup_{m \in [n]} \mathcal{O}_p(m)$ e, para todo $l \in \bigcup_{m \in [n]} \mathcal{O}_p(m)$, existe $m \in [n]$ tal que $l \in \mathcal{O}_p(m)$ e, portanto, existe $k \in \mathbb{N}$ tal que $l = p^k(m) \in [n]$, o que mostra que $\bigcup_{m \in [n]} \subseteq [n]$. Por fim, sejam $o_1, o_2 \in \mathcal{O}_p$. Então existem $m_1, m_2 \in [n]$ 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 $[n]$. ■

Permutações, Ciclos e Transposições

Definição 8.26. Sejam $n, k \in \mathbb{N}$. Um *ciclo* de \mathfrak{S}_n é um elemento $c \in \mathfrak{S}_n$ para o qual existe $m \in [n]$ tal que, para todo $m' \in [n]$, $c(m') = m'$ ou existe $d \in [n]$ 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

$$c = (m \ c(m) \ c^2(m) \ \cdots \ c^{k-2}(m) \ c^{k-1}(m)).$$

Proposição 8.41. 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 8.42 (Fatoração de Permutação). *Seja $n \in \mathbb{N}$ e $p \in \mathfrak{S}_n$. Então existem únicos ciclos $c_1, \dots, c_k \in \mathfrak{S}_n$ disjuntos dois a dois tais que $p = c_1 \circ \cdots \circ c_k$.*

Demonstração. Seja $k := |\mathcal{O}_p|$. O conjunto \mathcal{O}_p partitiona $[n]$. Sejam $(o_i)_{i \in [k]}$ uma indexação de \mathcal{O}_p e $m_1, \dots, m_k \in [n]$ tais que $o_i = \mathcal{O}_p(m_i)$ para todo $i \in [k]$, e seja $k_i := |\mathcal{O}_p(m_i)|$. Definamos $c_i := (m_i \ \cdots \ p^{k_i-1}(m_i))$. Então segue que

$$p = \bigtimes_{i=1}^k (m_i \ \cdots \ p^{k_i-1}(m_i)) = \bigtimes_{i=1}^k c_i.$$

■

8.3.5 Grupos Cíclicos

8.3.6 Grupos Diedrais

8.4 Ação de Grupos

A noção de uma ação de grupo, de certa forma, generaliza uma estratégia usada na demonstração do teorema de que todo grupo é isomorfo a um subgrupo de seu grupo simétrico.

Definição 8.27. Sejam \mathbf{G} um grupo e X um conjunto. Uma *ação* de \mathbf{G} em X é um homomorfismo de grupos

$$\begin{aligned} A: \mathbf{G} &\longrightarrow \mathfrak{S}(X) \\ g &\longmapsto g_{\bullet}: X \longrightarrow X \\ x &\longmapsto g_{\bullet}x. \end{aligned}$$

Denota-se $A: \mathbf{G} \curvearrowright X$. Diz-se que o grupo \mathbf{G} age no conjunto X , e denota-se $\mathbf{G} \curvearrowright X$, se, e somente se, existe ação de \mathbf{G} em X .

A definição acima é uma definição muito simplificada pois ela depende de conceitos um pouco mais complexos, como de homomorfismo de grupos e de grupo simétrico. A proposição abaixo mostra como essa definição é equivalente a uma definição mais explícita de ação de grupo que também é comumente usada.

Proposição 8.43. *Sejam X um conjunto e \mathbf{G} um grupo. Então $\mathbf{G} \curvearrowright X$ se, e somente se, existe uma função*

$$\begin{aligned} \bullet: \mathbf{G} \times X &\longrightarrow X \\ (g, x) &\longmapsto g_{\bullet}x \end{aligned}$$

que satisfaz

1. (Identidade) Para todo $x \in X$,

$$e_{\bullet}x = x;$$

2. (Compatibilidade) Para todos $g_0, g_1 \in G$ e $x \in X$,

$$(g_1g_0)_{\bullet}x = g_{1\bullet}(g_{0\bullet}x).$$

Demonstração. Se existe ação $A: \mathbf{G} \curvearrowright X$, basta definir $g_{\bullet}x := A(g)(x)$ e segue que $e_{\bullet} = I$ e $(g_1g_0)_{\bullet} = g_{1\bullet} \circ g_{0\bullet}$. Reciprocamente, definimos a ação A a partir de \bullet da mesma forma e, se $g_0, g_1 \in G$ e $x \in X$, segue que

$$A(g_1g_0)(x) = (g_1g_0)_{\bullet}x = g_{1\bullet}(g_{0\bullet}x) = A(g_1)(A(g_0)(x)) = A(g_1) \circ A(g_0)(x),$$

logo $A(g_1g_0) = A(g_1) \circ A(g_0)$. ■

Essa proposição é geralmente considerada a definição de uma ação à *esquerda* de \mathbf{G} em X por causa da posição em que a composição ocorre. Analogamente, uma ação à direita pode ser definida, mas toda ação à direita pode ser traduzida em uma ação à esquerda, de modo que é suficiente estudar somente ações à esquerda. É comum, ainda, estudar ações em conjuntos X com alguma estrutura adicional, geralmente uma topologia. Nesse caso, exige-se que a ação seja uma função contínua, mas também é necessário que G tenha uma estrutura topológica, portanto isso não será definido com cuidado agora.

8.4.1 Órbitas e Estabilizadores

Definição 8.28. Sejam X um conjunto, \mathbf{G} um grupo, $\mathbf{G} \curvearrowright X$ e $x \in X$. A *órbita* de x sob \mathbf{G} é o conjunto

$$G \cdot x := \{g \cdot x \mid g \in G\}.$$

Definição 8.29. Sejam X um conjunto, \mathbf{G} um grupo, $A : \mathbf{G} \curvearrowright X$ e $x \in X$. O *estabilizador* de x é

$$G_x = \{g \in G \mid g \cdot x = x\} = A^{-1}(\{x\}) = \text{nuc}(A).$$

O estabilizador de x é um grupo e por isso é chamado de *subgrupo estabilizador* de \mathbf{G} com respeito a x , e também é conhecido como *grupo de isotropia* de x .

8.5 Grupo Linear Geral

Definição 8.30. Sejam \mathbf{C} um corpo e $n \in \mathbb{N}$. O *grupo linear geral* de \mathbf{C} de ordem n é o conjunto

$$\text{GL}_n(\mathbf{C}) := \{M \in \mathbb{M}_{n \times n}(\mathbf{C}) \mid \det M \neq 0\}.$$

Se \mathbf{V} é um espaço vetorial finito de dimensão d sobre um corpo \mathbf{C} , o *grupo linear geral* de \mathbf{V} é

$$\text{GL}(\mathbf{V}) := \text{GL}_n(\mathbf{C}).$$

Como $\det(AB) = \det(A)\det(B)$ e as matrizes invertíveis são as que têm determinante não nulo, segue que o conjunto acima forma um grupo com respeito ao produto de matrizes.

Definição 8.31. Sejam \mathbf{C} um corpo e $n \in \mathbb{N}$. O *grupo linear especial* de \mathbf{C} de ordem n é o conjunto

$$\text{SL}_n(\mathbf{C}) := \{M \in \text{GL}(n, \mathbf{C}) \mid \det M = 1\}.$$

8.6 Representação de Grupos

Definição 8.32. Sejam \mathbf{G} um grupo e \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} . Uma *representação* de \mathbf{G} em \mathbf{V} é um homomorfismo de grupos

$$\rho : \mathbf{G} \longrightarrow \mathrm{GL}(\mathbf{V}).$$

O espaço \mathbf{V} é o *espaço de representação* e a dimensão de \mathbf{V} é a *dimensão da representação*.

Definição 8.33. Seja \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} .

8.7 Grupos Topológicos

Definição 8.34. Um *grupo topológico* é uma quádrupla $\mathbf{G} = ((G, \mathcal{T}), \times, ^{-1}, e)$ em que (G, \mathcal{T}) é um espaço topológico, $(G, \times, ^{-1}, e)$ é um grupo e as operações

$$\times : G^2 \longrightarrow G \quad \text{e} \quad ^{-1} : G \longrightarrow G$$

são funções contínuas.

Definição 8.35. Sejam \mathbf{G} um grupo e $h \in G$. A *conjugação* por h é a função

$$\begin{aligned} C_h : G &\longrightarrow G \\ g &\longmapsto ghg^{-1}. \end{aligned}$$

A *translação à direita* por h é a função

$$\begin{aligned} D_h : G &\longrightarrow G \\ g &\longmapsto hg. \end{aligned}$$

A *translação à esquerda* por h é a função

$$\begin{aligned} E_h : G &\longrightarrow G \\ g &\longmapsto hg. \end{aligned}$$

Proposição 8.44. Seja \mathbf{G} um grupo topológico. As funções C_h , D_h e E_h são homeomorfismos para todo $h \in G$.

Demonstração. Para ver que as funções são bijeções, basta notar que $(C_h)^{-1} = C_{h^{-1}}$, $(D_h)^{-1} = D_{h^{-1}}$ e $(E_h)^{-1} = E_{h^{-1}}$. Para mostrar a continuidade, basta notar que da continuidade de \times e das relações $E_h = \times \circ (\cdot, h)$ e $D_h = \times \circ (h, \cdot)$, segue que E_h e D_h são contínuas, e que da continuidade de $^{-1}$ e da relação $C_h = D_h \circ E_{h^{-1}}$, segue que C_h é contínua. \blacksquare

Exemplo 8.1. Seja \mathbf{X} um espaço topológico e \mathbf{G} um grupo topológico. Consideremos o conjunto $\mathcal{C}(X, G)$ das funções contínuas de \mathbf{X} para \mathbf{G} e as operações induzidas pontualmente de G em $\mathcal{C}(X, G)$ por $(f \times g)(x) := f(x) \times g(x)$, $(f^{-1})(x) := (f(x))^{-1}$ e $e(x) := e$. A quádrupla $(\mathcal{C}(X, G), \times, ^{-1}, e)$ é um grupo. Consideramos agora a topologia compacto-aberto \mathcal{T} gerada pelos conjuntos

$$A_{K,U} := \{f \in \mathcal{C}(G, X) \mid f(K) \subseteq U\}$$

em que $K \subseteq X$ é um compacto e $U \subseteq G$ é um aberto. Então $((\mathcal{C}(X, G), \mathcal{T}), \times, ^{-1}, e)$ é um grupo topológico.

Proposição 8.45. Seja \mathbf{G} um grupo topológico.

1. Para todos $g \in G$ e $A \subseteq G$ aberto, gA e Ag são abertos;
2. Para todos $g \in G$ e $A \subseteq G$ fechado, gA e Ag são fechados;
3. Para todos $A \subseteq G$ aberto e $C \subseteq G$, AC e CA são abertos;
4. Para todos $F \subseteq G$ fechado e $K \subseteq G$ compacto, FK e KF são fechados.

Demonstração. 1. Segue do fato de que E_g e D_g são homeomorfismos.

2. Segue do fato de que E_g e D_g são homeomorfismos.
3. Segue do fato de que

$$AC = \bigcup_{c \in C} cA \quad \text{e} \quad CA = \bigcup_{c \in C} Ac$$

e de que os conjuntos cA e Ac são abertos para todo $c \in C$.

4. Seja $x \in \overline{FK}$. Então existe uma rede $(x_\lambda)_{\lambda \in \Lambda} = (f_\lambda k_\lambda)$ tal que $x = \lim_{\lambda \in \Lambda} x_\lambda$. Como K é compacto, existe uma sub-rede k_{λ_μ} tal que $k := \lim_{\mu \in M} k_{\lambda_\mu} \in K$, o que implica que $k^{-1} = \lim_{\mu \in M} k_{\lambda_\mu}^{-1}$ pela continuidade da inversa. Pela continuidade do produto, segue que a sub-rede $f_{\lambda_\mu} = (f_{\lambda_\mu} k_{\lambda_\mu})k_{\lambda_\mu}^{-1}$ converge para $f = xk^{-1}$, e $f \in F$ pois F é fechado. Assim segue que $x = fk$, portanto FK é fechado. A demonstração é análoga para KF . ■

8.7.1 Homomorfismos

Proposição 8.46. Sejam \mathbf{G} e \mathbf{H} grupos topológicos e $h : G \longrightarrow H$ um homomorfismo de grupos. Então ϕ é contínuo se, e somente se, ϕ é contínuo na identidade $1 \in G$.

Demonstração. A ida é evidente, basta mostrar a volta. Como h é homomorfismo, $\phi \circ E_g = E_{\phi(g)} \circ \phi$ para todo $g \in G$. Mas $E_{\phi(g)} \circ \phi$ é contínua em I , o que implica que $\phi \circ E_g$ é contínuo em I e, como E_g é um homeomorfismo, segue que ϕ é contínuo em $g = E_g(I)$. \blacksquare

8.7.2 Ação Contínua

Definição 8.36. Sejam \mathbf{G} um grupo topológico e \mathbf{X} um espaço topológico. Uma *ação contínua* de \mathbf{G} em \mathbf{X} é uma ação $\bullet : G \times X \rightarrow X$ que é uma função contínua (com respeito à topologia produto).

$$\begin{aligned} \bullet : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \bullet x \end{aligned}$$

$$\begin{aligned} \bullet : G &\longrightarrow \mathfrak{S}(X) \\ g &\longmapsto g \bullet : X &\longrightarrow X \\ &&x &\longmapsto g \bullet x \end{aligned}$$

8.8 Grupos Diferenciais

Definição 8.37. Um *grupo diferencial* é um par (\mathbf{G}, \cdot) em que \mathbf{G} é uma variedade diferencial, (G, \cdot) é um grupo e as operações

$$\times : G^2 \longrightarrow G \quad \text{e} \quad {}^{-1} : G \longrightarrow G$$

são funções diferenciáveis.

Grupos diferenciais são comumente chamados de grupos de Lie, em homenagem ao matemático Sophus Lie.

Capítulo 9

Anéis

9.1 Construções Algébricas

9.1.1 Anel e Subanel

Definição 9.1. Um *anel* é uma lista $\mathbf{A} = (A, +, -, 0, \times, 1)$ tal que

1. $(A, +, -, 0)$ é um grupo comutativo, em que $+$ é a *adição*, $-$ é a *subtração* e 0 é a *nulidade* (ou o *zero*) de \mathbf{A} ;
2. $(A, \times, 1)$ é um monoide comutativo, em que \times é a *multiplicação* e 1 é a *unidade* (ou o *um*) de \mathbf{A} ;
3. A multiplicação \times é distributiva sobre a adição $+$.

Notação. O símbolo de multiplicação \times será suprimido sempre que possível, de modo que denotaremos a_0a_1 para $a_0 \times a_1$, e notação da multiplicação terá preferência sobre a da adição e a da subtração, pois \times é distributiva sobre $+$, de modo que denotaremos $a_0a_1 + a_2$ para $(a_1a_2) + a_3$ e $-a_1a_2$ para $-(a_1a_2)$. Os símbolos operatórios relativos à adição e à multiplicação serão, respectivamente,

$$+ \text{ e } \times.$$

O elemento a multiplicado por si mesmo n vezes será denotado a^n . Denotaremos o inverso de um elemento $a \in A$ sob \times por a^{-1} , se ele existir, pois sabemos que é único (7.7).

Um comentário sobre as identidades 0 e 1 . Se $0 = 1$, o anel será *trivial*, no sentido de que 0 será seu único elemento, mas mantemos esse caso na definição pois, mais à frente, quando estudarmos anéis quocientes, será proveitoso que qualquer anel quociente seja um anel, e se quocientarmos um anel por ele mesmo, temos o anel trivial.

Proposição 9.1. Seja \mathbf{A} um anel. Então, para todos $a, a' \in A$,

1. $0a = 0$;
2. Se $0 = 1$, então $A = \{0\}$;
3. $-(aa') = (-a)a'$.

Demonstração.

1.

$$\begin{aligned} 0a &= 0a + 0 \\ &= 0a + (0a - 0a) \\ &= (0a + 0a) - 0a \\ &= (0 + 0)a - 0a \\ &= 0a - 0a \\ &= 0. \end{aligned}$$

2. Se $0 = 1$, então, para todo $a \in A$,

$$a = 1a = 0a = 0;$$

3.

$$\begin{aligned} -(aa') &= -(aa') + 0 \\ &= -(aa') + 0a' \\ &= -(aa') + (a - a)a' \\ &= -(aa') + (aa' + (-a)a') \\ &= (-(aa') + aa') + (-a)a' \\ &= 0 + (-a)a' \\ &= (-a)a'. \end{aligned}$$

■

Definição 9.2. Seja \mathbf{A} um anel. O conjunto dos elementos invertíveis sob multiplicação de \mathbf{A} é denotado por A^* .

Proposição 9.2. Seja \mathbf{A} um anel. O par $(A^*, \times|_{(A^*)^2}, ^{-1}, 1)$ é um grupo comutativo.

Demonstração. A tripla $(A, \times, 1)$ é um monoide comutativo com identidade 1. Portanto segue que a quádrupla $(A^*, \times|_{(A^*)^2}, ^{-1}, 1)$ é um grupo (em que a^{-1} denota o inverso de a sob \times). Como \times é comutativa, então $(A^*, \times|_{(A^*)^2}, ^{-1}, 1)$ também o é.

■

Definição 9.3. Seja $\mathbf{A} = (A, +, -, 0, \times, 1)$ um anel. Um *subanel* de \mathbf{A} é um anel $\mathbf{S} = (S, +_S, \times_S)$ em que $S \subseteq A$, $+_S = +|_{S \times S}$ e $\times_S = \times|_{S \times S}$. Denota-se $\mathbf{S} \leq \mathbf{A}$. Um subanel *próprio* de \mathbf{A} é um subanel $\mathbf{S} \leq \mathbf{A}$ em que S é um conjunto próprio de A ($S \subset A$). Denota-se $\mathbf{S} < \mathbf{A}$.

Proposição 9.3. *Sejam $\mathbf{A} = (A, +, \times)$ um anel e $S \subseteq A$. Então*

$$\mathbf{S} = (S, +|_{S \times S}, \times|_{S \times S})$$

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*) $\forall s_1, s_2 \in S \quad s_1 + s_2 \in S$;
- (c) (*Invertibilidade*) $\forall s \in S \quad -s \in S$;

2. $(S, \times|_{S \times S})$ é um submonoide comutativo de (A, \times) com $1 \in S$:

- (a) (*Identidade*) $1 \in S$;
- (b) (*Fechamento*) $\forall s_1, s_2 \in S \quad s_1 \times s_2 \in S$.

Demonstração. (\Rightarrow) Suponhamos que \mathbf{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 (8.2)). (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 (7.9).

(\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 $+|_{S \times S}$. ■

9.1.2 Ideais e Anéis Quocientes

Definição 9.4. Seja \mathbf{A} um anel. Um *ideal* de \mathbf{A} é um conjunto não vazio $I \subseteq A$ tal que

1. $\forall i_1, i_2 \in I \quad i_1 - i_2 \in I$
2. $\forall a \in A, i \in I \quad ai \in I$

Denotamos que I é ideal de \mathbf{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 9.4. *Sejam \mathbf{A} um anel e $I \trianglelefteq A$. Então*

1. $0 \in I$;
2. $\forall i_1, i_2 \in I \quad i_1 + i_2 \in I$;
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 9.5. *Sejam \mathbf{A} um anel e $(I_j)_{j \in J}$ uma família de ideais de \mathbf{A} . Então*

$$I := \bigcap_{j \in J} I_j$$

é um ideal de \mathbf{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 \mathbf{A} , segue que $i_1 - i_2 \in I_j$ e que $ai_1 \in I_j$. Logo $i_1 - i_2 \in I$ e $ai_1 \in I$, o que mostra que I é ideal de \mathbf{A} . ■

Proposição 9.6. Sejam \mathbf{A} um anel e $(I_j)_{n \in \mathbb{N}}$ uma sequência crescente de ideais de \mathbf{A} ; ou seja, $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$. Então

$$I := \bigcup_{n \in \mathbb{N}} W_n$$

é um ideal de \mathbf{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 \mathbf{A} , segue que $ai_1 \in I_n$. Logo $ai_1 \in I$, o que mostra que I é ideal de \mathbf{A} . ■

Definição 9.5. Sejam \mathbf{A} um anel e $a_1, \dots, a_n \in A$. Definimos o conjunto

$$\bigoplus_{i=1}^n a_i A = a_1 A + \dots + a_n A := \left\{ \bigoplus_{i=1}^n a_i b_i \mid b_i \in A \right\}.$$

Proposição 9.7. Sejam \mathbf{A} um anel e $a_1, \dots, a_n \in A$. Então

$$I := \bigoplus_{k=1}^n a_k A \trianglelefteq A.$$

Demonstração. Sejam $a \in A$ e $i_1, i_2 \in I$ tais que $i_1 = \bigoplus_{k=1}^n a_k b_k$ e $i_2 = \bigoplus_{k=1}^n a_k c_k$. Então

$$i_1 - i_2 = \bigoplus_{k=1}^n a_k b_k - \bigoplus_{k=1}^n a_k c_k = \bigoplus_{k=1}^n a_k (b_k - c_k) \in I,$$

pois $(b_k - c_k) \in A$ para todo $k \in \{1, \dots, n\}$. Ainda,

$$ak_1 = a \bigoplus_{k=1}^n a_k b_k = \bigoplus_{k=1}^n a_k (ab_k) \in I,$$

pois $ab_k \in A$ para todo $k \in \{1, \dots, n\}$. Logo $I \trianglelefteq A$. ■

Esse ideal é chamado de ideal de A gerado por a_1, \dots, a_n .

Definição 9.6. Seja \mathbf{A} um anel. Um *ideal principal* de \mathbf{A} é um ideal $I \trianglelefteq A$ tal que

1. $\exists a \in A \quad I = aA$.

Proposição 9.8. Seja \mathbf{A} um anel. Então \mathbf{A} é um corpo se, e somente se, \mathbf{A} é um anel não-trivial cujos únicos ideais de \mathbf{A} são $\{0\}$ e A .

Demonstração. Suponha que \mathbf{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 \mathbf{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 \mathbf{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 \mathbf{A} é corpo. ■

Proposição 9.9. *Sejam \mathbf{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 9.7. Sejam \mathbf{A} um anel e $I \trianglelefteq A$. O conjunto $a + I := \{a + i : i \in I\}$ é a *classe lateral* de I com representante a . O conjunto das classes laterais de A é denotado por $A/I := \{a + I : a \in A\}$.

Proposição 9.10. *Sejam $(A, +, \cdot)$ um anel, $I \trianglelefteq A$ 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 partitionado 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 9.8. Sejam \mathbf{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

$$(a_1 + I) \oplus (a_2 + I) := (a_1 + a_2) + I \quad (a_1 + I) \odot (a_2 + I) := (a_1 \cdot a_2) + I$$

Denotaremos \oplus e \odot por $+$ e \cdot quando não existir ambiguidade.

Proposição 9.11. 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 $(a_1 b_1) + I = (a_2 b_2) + I$. \blacksquare

Proposição 9.12. Sejam $\mathbf{A} = (A, +, \cdot)$ um anel e $I \trianglelefteq A$. Então $\mathbf{A}/I := (A/I, \oplus, \odot)$ 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

$$\begin{aligned} (a + 1 + I) \odot ((a_2 + I) \oplus (a_3 + I)) &= (a + 1 + I) \odot ((a_2 + a_3) + I) \\ &= (a_1 \cdot (a_2 + a_3)) + I \\ &= ((a_1 \cdot a_2) + (a_1 \cdot a_3)) + I \\ &= ((a_1 \cdot a_2) + I) \oplus ((a_1 \cdot a_3) + I) \\ &= ((a_1 + I) \odot (a_2 + I)) \oplus ((a_1 + I) \odot (a_3 + I)). \end{aligned}$$

■

9.1.3 Homomorfismos de Anéis

Definição 9.9. Sejam $\mathbf{A} = (A, +, \cdot)$ e $\mathbf{B} = (B, \oplus, \odot)$ dois anéis. Um *homomorfismo de anéis* entre \mathbf{A} e \mathbf{B} é uma função $\phi : A \longrightarrow B$ que é

1. um homomorfismo de grupos entre $(A, +)$ e (B, \oplus)
 - (a) $\forall a_1, a_2 \in A \quad \phi(a_1 + a_2) = \phi(a_1) \oplus \phi(a_2);$
2. um homomorfismo de monoides entre (A, \cdot) e (B, \odot)

- (a) $\forall a_1, a_2 \in A \quad \phi(a_1 \cdot a_2) = \phi(a_1) \odot \phi(a_2);$
- (b) $\phi(1_A) = 1_B.$

O conjunto de todos os homomorfismos de anéis entre \mathbf{A} e \mathbf{B} é denotado por $\mathcal{H}\text{om}(\mathbf{A}, \mathbf{B})$.

Exemplo 9.1. Seja $(A, +, \cdot)$ um anel e consideremos o anel dos números inteiros $(\mathbb{Z}, +, \cdot)$. Então

$$\begin{aligned} \phi: \mathbb{Z} &\longrightarrow A \\ z &\longmapsto \begin{cases} \underset{i=1}{\overset{z}{+}} 1_A & z > 0 \\ 0_A & z = 0 \\ -\phi(-z) & z < 0 \end{cases} \end{aligned}$$

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 $z_2 > 0$, então $z_1 + z_2 > 0$. Logo

$$\phi(z_1 + z_2) = \underset{i=1}{\overset{z_1+z_2}{+}} 1_A = \underset{i=1}{\overset{z_1}{+}} 1_A + \underset{i=z_1+1}{\overset{z_1+z_2}{+}} 1_A = \underset{i=1}{\overset{z_1}{+}} 1_A + \underset{i=1}{\overset{z_2}{+}} 1_A = \phi(z_1) + \phi(z_2).$$

Se $z_1 < 0$ e $z_2 < 0$, 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

$$\begin{aligned}
 \phi(z_1 + z_2) &= \phi(0) \\
 &= 0_A \\
 &= \sum_{i=1}^{z_1} 1_A - \sum_{i=1}^{z_1} 1_A \\
 &= \phi(z_1) - \phi(-z_1) \\
 &= \phi(z_1) + \phi(z_2).
 \end{aligned}$$

Se tivermos $z_1 > -z_2$, então

$$\begin{aligned}
 \phi(z_1 + z_2) &= \sum_{i=1}^{z_1+z_2} 1_A \\
 &= \sum_{i=1}^{z_1+z_2} 1_A + \sum_{i=1}^{-z_2} 1_A - \sum_{i=1}^{-z_2} 1_A \\
 &= \sum_{i=1}^{z_1+z_2} 1_A + \sum_{i=z_1+z_2+1}^{z_1} 1_A - \sum_{i=1}^{-z_2} 1_A \\
 &= \sum_{i=1}^{z_1} 1_A - \sum_{i=1}^{-z_2} 1_A \\
 &= \phi(z_1) + \phi(z_2).
 \end{aligned}$$

Por fim, se $-z_2 > z_1$, então $-z_1 < 0$ e $-z_2 > 0$ e segue da equação anterior que

$$\begin{aligned}
 \phi(z_1 + z_2) &= -\phi(-(z_1 + z_2)) \\
 &= -\phi((-z_1) + (-z_2)) \\
 &= -(\phi(-z_1) + \phi(-z_2)) \\
 &= -(-\phi(z_1) - \phi(z_2)) \\
 &= \phi(z_1) + \phi(z_2).
 \end{aligned}$$

■

Definição 9.10. Sejam \mathbf{A} um anel e $n \in \mathbb{Z}$. O *número inteiro* n em \mathbf{A} é o elemento

$$n_A := \begin{cases} \sum_{i=1}^n 1_A, & n > 0 \\ 0, & n = 0 \\ \sum_{i=1}^{-n} (-1_A), & n < 0. \end{cases}$$

O conjunto dos inteiros de \mathbf{A} é denotado $\mathbb{Z}(\mathbf{A})$. O *coeficiente binomial* de $n_A, k_A \in \mathbb{Z}(\mathbf{A})$ é o número

$$\binom{n_A}{k_A} := \binom{n}{k}_A.$$

Proposição 9.13. *Sejam \mathbf{A} um anel e $a, b \in A$. Então*

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$$

Exemplo 9.2. *Sejam \mathbf{A} um anel e $I \trianglelefteq A$. Então a projeção canônica de A em A/I , definida por*

$$\begin{aligned} \pi: A &\longrightarrow A/I \\ a &\longmapsto a + I, \end{aligned}$$

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 9.14 (Homomorfismos preservam a estrutura algébrica entre anéis). *Sejam $\mathbf{A} = (A, +, \cdot)$ e $\mathbf{B} = (B, \oplus, \odot)$ dois anéis e $\phi: A \longrightarrow B$ um homomorfismo de anéis. Então*

1. $\phi(0_A) = 0_B$;
2. $-\phi(a) = \phi(-a)$.

Demonstração. Como ϕ é um homomorfismo de grupos entre $(A, +)$ e (B, \oplus) , sabemos que ϕ preserva a estrutura algébrica de grupo entre os grupos (8.17). ■

Corolário 9.15 (Composição de homomorfismos é homomorfismo). *Sejam $\mathbf{A}_1 = (A_1, +_1, \cdot_1)$, $\mathbf{A}_2 = (A_2, +_2, \cdot_2)$ e $\mathbf{A}_3 = (A_3, +_3, \cdot_3)$ três anéis e $\phi \in \mathcal{H}\text{om}(\mathbf{A}_1, \mathbf{A}_2)$ e $\psi \in \mathcal{H}\text{om}(\mathbf{A}_2, \mathbf{A}_3)$. Então $(\psi \circ \phi) \in \mathcal{H}\text{om}(\mathbf{A}_1, \mathbf{A}_3)$.*

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 homomorfismo de grupos entre $(A_2, +_2)$ e $(A_3, +_3)$, segue da proposição de composição de homomorfismos da seção de grupos (8.18) 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 (7.10) que $(\psi \circ \phi)$ é homomorfismo de monoides entre (A_1, \cdot_1) e (A_3, \cdot_3) .

■

Proposição 9.16. *Sejam \mathbf{A} e \mathbf{B} anéis, $\phi \in \mathcal{H}\text{om}(\mathbf{A}, \mathbf{B})$ 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 9.17. *Sejam \mathbf{A} e \mathbf{B} anéis, $\phi \in \mathcal{H}\text{om}(\mathbf{A}, \mathbf{B})$ 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 9.11. Sejam \mathbf{A} e \mathbf{B} dois anéis e $\phi \in \mathcal{H}\text{om}(\mathbf{A}, \mathbf{B})$. O *núcleo* de ϕ é o conjunto

$$\text{nuc}(\phi) := \{a \in A : \phi(a) = 0_B\}$$

e a *imagem* de ϕ é o conjunto

$$\text{im}(\phi) := \{b \in B : \exists a \in A, \phi(a) = b\}.$$

Proposição 9.18. *Sejam $\mathbf{A} = (A, +, \cdot)$ e $\mathbf{B} = (B, \oplus, \odot)$ dois anéis e seja $\phi \in \mathcal{H}\text{om}(\mathbf{A}, \mathbf{B})$. Então*

1. $\text{nuc}(\phi) \trianglelefteq A$;
2. $\text{im}(\phi)$ é subanel de \mathbf{B} .

Demonstração. Demonstramos as afirmações separadamente.

1. Primeiro notamos que $\text{nuc}(\phi) \subseteq A$ e que $\text{nuc}(\phi)$ não é vazio, pois, como $\phi(0_A) = 0_B$, então $0_A \in \text{nuc}(\phi)$. Vamos mostrar as duas propriedades de um ideal. Sejam $a \in A$ e $n_1, n_2 \in \text{nuc}(\phi)$. Então $n_1 - n_2 \in \text{nuc}(\phi)$, pois

$$\phi(n_1 - n_2) = \phi(n_1) - \phi(n_2) = 0_B - 0_B = 0_B.$$

Ainda, $a \cdot n_1 \in \text{nuc}(\phi)$, pois

$$\phi(a \cdot n_1) = \phi(a) \odot \phi(n_1) = \phi(a) \odot 0_B = 0_B.$$

Portanto $\text{nuc}(\phi)$ é ideal de A .

2. Claramente, $\text{im}(\phi) \subseteq B$ e $\text{im}(\phi)$ não é vazio. Sejam $i_1, i_2 \in \text{im}(\phi)$. Então existem $a_1, a_2 \in A$ tais que $\phi(a_1) = i_1$ e $\phi(a_2) = i_2$. Portanto $i_1 \ominus i_2 \in \text{im}(\phi)$, já que

$$\phi(a_1 - a_2) = \phi(a_1) - \phi(a_2) = i_1 - i_2.$$

Ainda, $i_1 \odot i_2 \in \text{im}(\phi)$, pois

$$\phi(a_1 \cdot a_2) = \phi(a_1) \odot \phi(a_2) = i_1 \odot i_2.$$

Por fim, $1_B \in \text{im}(\phi)$, pois $\phi(1_A) = 1_B$. Logo $\text{im}(\phi)$ é subanel de B . ■

Proposição 9.19. *Sejam $\mathbf{A} = (A, +, \cdot)$ e $\mathbf{B} = (B, \oplus, \odot)$ dois anéis e seja $\phi \in \mathcal{H}\text{om}(\mathbf{A}, \mathbf{B})$. Então ϕ é injetiva se, e somente se, $\text{nuc}(\phi) = \{0_A\}$.*

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 (8.22), esta proposição está provada. ■

Definição 9.12. Sejam $\mathbf{A} = (A, +, \cdot)$ e $\mathbf{B} = (B, \oplus, \odot)$ dois anéis. Um isomorfismo de anéis é um homomorfismo de anéis $\phi \in \mathcal{H}\text{om}(\mathbf{A}, \mathbf{B})$ que é bijetivo. O conjunto de todos os homomorfismos de anéis entre \mathbf{A} e \mathbf{B} é denotado por $\mathcal{I}\text{so}(\mathbf{A}, \mathbf{B})$.

Proposição 9.20. *Sejam $\mathbf{A} = (A, +, \cdot)$ e $\mathbf{B} = (B, \oplus, \odot)$ anéis e $\phi \in \mathcal{I}\text{so}(\mathbf{A}, \mathbf{B})$. Então $\phi^{-1} \in \mathcal{I}\text{so}(\mathbf{B}, \mathbf{A})$.*

Demonstração. Como ϕ é bijetiva, sua inversa ϕ^{-1} também é bijetiva. Devemos provar que ϕ^{-1} é um homomorfismo de anéis. Sejam $b_1, b_2 \in B$. Primeiro, vamos provar que ϕ^{-1} é um homomorfismo de grupos entre \mathbf{B} e \mathbf{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 9.13. Sejam \mathbf{A} e \mathbf{B} dois anéis. Dizemos que \mathbf{A} é *isomorfo* a \mathbf{B} , e denotamos isso por $\mathbf{A} \simeq \mathbf{B}$, sse existe $\phi \in \text{Iso}(\mathbf{A}, \mathbf{B})$.

Proposição 9.21. *Sejam \mathbf{A}_1 , \mathbf{A}_2 e \mathbf{A}_3 três anéis. Então*

1. (*Reflexividade*) $\mathbf{A}_1 \simeq \mathbf{A}_1$;
2. (*Antissimetria*) $\mathbf{A}_1 \simeq \mathbf{A}_2 \Rightarrow \mathbf{A}_2 \simeq \mathbf{A}_1$;
3. (*Transitividade*) $\mathbf{A}_1 \simeq \mathbf{A}_2$ e $\mathbf{A}_2 \simeq \mathbf{A}_3 \Rightarrow \mathbf{A}_1 \simeq \mathbf{A}_3$.

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 $\phi = Id_A : A \longrightarrow A$ é um isomorfismo de anéis. Logo $\mathbf{A}_1 \simeq \mathbf{A}_1$
2. Se $\mathbf{A}_1 \simeq \mathbf{A}_2$, existe $\phi \in \text{Iso}(\mathbf{A}_1, \mathbf{A}_2)$. Pela proposição (9.20), ϕ^{-1} é um isomorfismo de anéis entre \mathbf{A}_2 e \mathbf{A}_1 . Logo $\mathbf{A}_2 \simeq \mathbf{A}_1$.
3. $\mathbf{A}_1 \simeq \mathbf{A}_2$, existe $\phi \in \text{Iso}(\mathbf{A}_1, \mathbf{A}_2)$ e, como $\mathbf{A}_2 \simeq \mathbf{A}_3$, existe $\psi \in \text{Iso}(\mathbf{A}_2, \mathbf{A}_3)$. Assim, pela proposição (9.15), sabemos que $(\psi \circ \phi) \in \text{Hom}(\mathbf{A}_1, \mathbf{A}_3)$. Ainda, como ϕ e ψ são bijeções, sua composição é uma bijeção. Portanto $(\psi \circ \phi) \in \text{Iso}(\mathbf{A}_1, \mathbf{A}_3)$, o que implica $\mathbf{A}_1 \simeq \mathbf{A}_3$. ■

9.1.4 Teoremas de Isomorfismo

Teorema 9.22 (Primeiro Teorema de Isomorfismo). *Sejam $\mathbf{A} = (A, +, \cdot)$ e $\mathbf{B} = (B, \oplus, \odot)$ dois anéis e $\phi \in \text{Hom}(\mathbf{A}, \mathbf{B})$. Então*

$$\mathbf{A}/\text{nuc}(\phi) \simeq \text{im}(\phi).$$

Demonstração. Primeiro, vale notar que, como $\text{im}(\phi) \trianglelefteq A$, o $\mathbf{A}/\text{nuc}(\phi)$ é um anel. Agora, consideremos a função

$$\begin{aligned}\psi: A/\text{nuc}(\phi) &\longrightarrow \text{im}(\phi) \\ a + \text{nuc}(\phi) &\longmapsto \phi(a).\end{aligned}$$

Notemos que a função ψ é bem definida. Para isso, sejam $a_1, a_2 \in A$ tais que $a_1 + \text{nuc}(\phi) = a_2 + \text{nuc}(\phi)$. Então $(a_1 - a_2) \in \text{nuc}(\phi)$, o que implica $\phi(a_1 - a_2) = 0$. Como ϕ é homomorfismo de anéis, segue que $\phi(a_1) = \phi(a_2)$. Então $\psi(a_1 + \text{nuc}(\phi)) = \psi(a_2 + \text{nuc}(\phi))$.

Vamos mostrar que essa função é um isomorfismo de anéis. Primeiro, vamos mostrar que ψ é homomorfismo de anéis. Para isso, vamos denotar $a + \text{nuc}(\phi) \in A/\text{nuc}(\phi)$ por $[a]$ para facilitar a demonstração. Sejam $[a_1], [a_2] \in A/\text{nuc}(\phi)$. Vemos que ψ é homomorfismo de grupos entre $(A/\text{nuc}(\phi), +)$ e $(\text{im}(\phi), \oplus)$, 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 homomorfismo de monoides entre $(A/\text{nuc}(\phi), \cdot)$ e $(\text{im}(\phi), \odot)$, pois

$$\psi([a_1] \cdot [a_2]) = \psi([a_1 \cdot a_2]) = \phi(a_1 \cdot a_2) = \phi(a_1) \odot \phi(a_2) = \psi([a_1]) \odot \psi([a_2])$$

$$\text{e } \psi([1_A]) = \phi(1_A) = 1_B.$$

Por fim, devemos mostrar que ψ é bijetiva. Primeiro, mostramos que ψ é injetiva. Seja $[a] \in \text{nuc}(\psi)$. Então $\psi([a]) = 0_B$, o que implica $\phi(a) = 0_B$. Mas isso implica $a \in \text{nuc}(\phi)$; ou seja, $[a] = [0_A]$. Logo $\text{nuc}(\psi) = \{[0_A]\}$, que quer dizer que ψ é injetiva (9.19). Agora, notamos que ψ é sobrejetiva por construção, pois tem como contradomínio $\text{im}(\phi)$. ■

Proposição 9.23 (Teorema Chinês do Resto). *Sejam $m_1, \dots, m_n \in \mathbb{N} \setminus \{0, 1\}$ dois a dois coprimos entre si. Então*

$$\mathbb{Z}/(m_1 m_2 \dots m_n \mathbb{Z}) \simeq (\mathbb{Z}/m_1 \mathbb{Z}) \times \dots \times (\mathbb{Z}/m_n \mathbb{Z}).$$

Definição 9.14.

$$B + I := \{b + i : b \in B, i \in I\}$$

Teorema 9.24 (Segundo Teorema de Isomorfismo). *Sejam \mathbf{A} um anel, B um subanel de \mathbf{A} e $I \trianglelefteq A$. Então*

1. $B + I$ é subanel de \mathbf{A} ;

2. $B \cap I \trianglelefteq B$;

3.

$$\mathbf{B}/\mathbf{B} \cap I \simeq B + I/I.$$

Demonstração. 1. Para mostrar que $B + I$ é subanel de \mathbf{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 propriedades 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 \mathbf{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 \mathbf{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 \mathbf{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

$$\begin{aligned}\phi: B &\longrightarrow B + I/I \\ b &\longmapsto b + I.\end{aligned}$$

Essa função é um homomorfismo de anéis. Sejam $b_1, b_2 \in B$. Então $\phi(b_1 + b_2) = (b_1 + b_2) + I = (b_1 + I) + (b_2 + I) = \phi(b_1) + \phi(b_2)$. Ainda, vale $\phi(b_1b_2) = (b_1b_2) + I = (b_1 + I)(b_2 + I) = \phi(b_1)\phi(b_2)$. Por fim, $\phi(1) = 1 + I$.

Agora, notemos que $\text{nuc}(\phi) = B \cap I$. Seja $b \in B$. Então

$$b \in \text{nuc}(\phi) \Leftrightarrow \phi(b) = 0 \Leftrightarrow b + I = I \Leftrightarrow b \in I.$$

Por fim, notemos que $\text{im}(\phi) = B + I/I$, pois um elemento de $B + I/I$ 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 (9.22) que

$$B/B \cap I = B/\text{nuc}(\phi) \simeq \text{im}(\phi) = B + I/I.$$

■

Lema 9.25. *Sejam A um anel e $I \trianglelefteq A$. Então*

1. *Se B é subanel de A tal que $I \subseteq B$, então B/I é subanel de A/I . Por outro lado, todo subanel de A/I é da forma B/I para algum B subanel de 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 A tal que $I \subseteq B$. Para mostrar que o conjunto B/I é subanel de A/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 $(b_1 + I)(b_2 + I) = (b_1 b_2) + I \in B/I$. Ainda, como $1 \in B$, $1 + I \in B/I$. Logo B/I é subanel de A/I .

Seja agora C um subanel de A/I . Como C é subconjunto não vazio de A/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 A . Sejam $b_1, b_2 \in B$. Como B/I é subanel de A/I , temos que $(b_1 + I) - (b_2 + I) = (b_1 - b_2) + I \in B/I$ e $(b_1 + I)(b_2 + I) = (b_1 b_2) + I \in B/I$. Então $b_1 - b_2 \in B$ e $b_1 b_2 \in B$. 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 9.26 (Terceiro Teorema de Isomorfismo). *Sejam A um anel, $I \trianglelefteq A$ e $J \trianglelefteq A$ tais que $I \subseteq J$. Então*

$$(A/I)/(J/I) \simeq A/J.$$

Demonstração. Consideremos a função

$$\begin{aligned}\phi: A/I &\longrightarrow A/J \\ a+I &\longmapsto a+J.\end{aligned}$$

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

$$\text{nuc}(\phi) = \{a + I : \phi(a + I) = 0 + J\} = \{a + I : a \in J\} = J/I,$$

o que prova que $J/I \trianglelefteq A/I$ e que, portanto, o quociente $(A/I)/(J/I)$ pode formar um anel quociente. Notemos também que ϕ é sobrejetiva por construção; ou seja, $\text{im}(\phi) = A/J$. Logo, pelo primeiro teorema de isomorfismo (9.22), temos que

$$(A/I)/(J/I) = (A/I)/\text{nuc}(\phi) \simeq \text{im}(\phi) = A/J.$$

■

9.2 Construções Categóricas

9.2.1 Anel de Polinômios

Definição 9.15. Seja \mathbf{A} um anel. O *anel de polinômios* em \mathbf{A} é o conjunto

$$A[x] := \left\{ p \in A^{\mathbb{N}} \mid |\text{supp}(p)| < |\mathbb{N}| \right\}.$$

Os elementos de $A[x]$ são os *polinômios* em \mathbf{A} .

Definimos os polinômios em \mathbf{A} como as sequências em A com suporte finito. O suporte da sequência $p: \mathbb{N} \rightarrow A$, nesse caso, é o suporte com respeito ao grupo $(A, +, -, 0)$, ou seja, sequências que têm uma quantidade finita de entradas não nulas. Essas sequências são também chamadas de sequências eventualmente nulas. Por enquanto, x é um símbolo qualquer, e pode ser susbtituído por qualquer outro símbolo de preferência, mas mais para frente ele será definido como um elemento de $A[x]$ de modo que os polinômios $p \in A[x]$ tenham a forma usual

$$p = \sum_{i=0}^n p_i x^i.$$

Antes disso, mostraremos que $A[x]$ é um anel, o que justifica seu nome.

Definição 9.16. Seja \mathbf{A} um anel. Definimos em $A[x]$ as operações e as constantes

$$\begin{aligned} +_{A[x]}: A[x] \times A[x] &\longrightarrow A[x] \\ (p, q) &\longmapsto (p_n + q_n)_{n \in \mathbb{N}} \end{aligned}$$

$$\begin{aligned} -_{A[x]}: A[x] &\longrightarrow A[x] \\ p &\longmapsto (-p_n)_{n \in \mathbb{N}} \end{aligned}$$

$$\begin{aligned} 0_{A[x]}: \mathbb{N} &\longrightarrow A \\ n &\longmapsto 0 \end{aligned}$$

$$\begin{aligned} \cdot_{A[x]}: A[x] \times A[x] &\longrightarrow A[x] \\ (p, q) &\longmapsto \left(\sum_{i=0}^n p_i q_{n-i} \right)_{n \in \mathbb{N}}. \end{aligned}$$

$$\begin{aligned} 1_{A[x]}: \mathbb{N} &\longrightarrow A \\ n &\longmapsto \begin{cases} 1, & n = 0 \\ 0, & n \neq 0. \end{cases} \end{aligned}$$

Os sub-índices $A[x]$ serão suprimidos quando possível.

Proposição 9.27. Seja \mathbf{A} um anel. Então $\mathbf{A}[\mathbf{x}] = (A[x], +, -, 0, \cdot, 1)$ é um anel.

Demonastração. Sabemos que $(A[x], +, -, 0)$ é um grupo comutativo, pois $(A, +, -, 0)$ o é. Mostremos que $(A[x], \cdot, 1)$ é um monoide comutativo. Como $(A, \cdot, 1)$ é um monoide comutativo, segue que

1. (Associatividade) Para todos $p, q, r \in A[x]$,

$$\begin{aligned}
(pq)r &= \left(\sum_{i=0}^n (pq)_i r_{n-i} \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{i=0}^n \left(\sum_{j=0}^i p_j q_{i-j} \right) r_{n-i} \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{i=0}^n \sum_{j=0}^i p_j q_{i-j} r_{n-i} \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{0 \leq j \leq i \leq n} p_j q_{i-j} r_{n-i} \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{i=0}^n \sum_{j=0}^{n-i} p_i q_j r_{n-i-j} \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{i=0}^n p_i \left(\sum_{j=0}^{n-i} q_j r_{n-i-j} \right) \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{i=0}^n p_i (qr)_{n-i} \right)_{n \in \mathbb{N}} \\
&= p(qr);
\end{aligned}$$

2. (Unidade) Para todo $p \in A[x]$,

$$1p = \left(\left(1p_n + \sum_{i=1}^n p_i 0 \right) \right)_{n \in \mathbb{N}} = (p_n)_{n \in \mathbb{N}} = p.$$

3. (Comutatividade) Para todos $p, q \in A[x]$,

$$pq = \left(\sum_{i=0}^n p_i q_{n-i} \right)_{n \in \mathbb{N}} = \left(\sum_{i=0}^n q_i p_{n-i} \right)_{n \in \mathbb{N}} = qp.$$

Por fim, mostremos que vale a distributividade. Para todos $p, q, r \in A[x]$,

$$\begin{aligned}
p(q + r) &= \left(\sum_{i=0}^n p_i (q + r)_{n-i} \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{i=0}^n p_i (q_{n-i} + r_{n-i}) \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{i=0}^n (p_i q_{n-i} + p_i r_{n-i}) \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{i=0}^n p_i q_{n-i} + \sum_{i=0}^n p_i r_{n-i} \right)_{n \in \mathbb{N}} \\
&= \left(\sum_{i=0}^n p_i q_{n-i} \right)_{n \in \mathbb{N}} + \left(\sum_{i=0}^n p_i r_{n-i} \right)_{n \in \mathbb{N}} \\
&= pq + pr.
\end{aligned}$$

■

Definição 9.17. Seja A um anel. O *grau* de $p \in A[x] \setminus \{0\}$ é o número

$$\text{gr}(p) := \max \text{supp}(p)$$

(o maior índice de uma entrada não nula de p , que é sempre inteiro porque o suporte de p é finito).

O grau do polinômio 0 não é definido. Se a definição acima fosse mudada de \max para \sup , ele seria 0 pela convenção de $\sup \emptyset = 0$.

A próxima definição justifica a notação $A[x]$, no sentido de que dá significado ao símbolo x .

Definição 9.18. Seja A um anel. A *variável* de $A[x]$ é a função

$$\begin{aligned}
x: \mathbb{N} &\longrightarrow A \\
n &\longmapsto \begin{cases} 1, & n = 1 \\ 0, & n \neq 1. \end{cases}
\end{aligned}$$

Notemos que, para todo $k \in \mathbb{N}$, x^k é a função

$$\begin{aligned}
x^k: \mathbb{N} &\longrightarrow A \\
n &\longmapsto \begin{cases} 1, & n = k \\ 0, & n \neq k \end{cases}
\end{aligned}$$

e assim podemos escrever todo polinômio $p \in A[x]$ como uma soma finita

$$p = \sum_{i=0}^{\text{gr}(p)} p_i x^i.$$

Proposição 9.28. *Sejam \mathbf{A} um domínio e $p, q \in A[x] \setminus \{0\}$. Então*

$$\text{gr}(pq) = \text{gr}(p) + \text{gr}(q).$$

Demonstração. Seja $k := \text{gr}(p) + \text{gr}(q)$. O produto pq terá coeficientes $\sum_{i=0}^n p_i q_{n-i}$, com $n \in \{0, \dots, k\}$. Notemos que, para $k = \text{gr}(p) + \text{gr}(q)$,

$$\sum_{i=0}^k p_i q_{k-i} = p_{\text{gr}(p)} q_{\text{gr}(q)}.$$

Isso ocorre porque todos os termos desse somatório se anulam, menos quando $i = \text{gr}(p)$. Se $i > \text{gr}(p)$, temos $p_i = 0$; se $i < \text{gr}(p)$, então $k - i > \text{gr}(p) + \text{gr}(q) - \text{gr}(p) = \text{gr}(q)$, e temos $q_{k-i} = 0$. Em ambos os casos, $p_i q_{k-i} = 0$. Por definição, $p_{\text{gr}(p)} \neq 0$ e $q_{\text{gr}(q)} \neq 0$ e, como \mathbf{A} é um domínio, isso implica que $p_{\text{gr}(p)} q_{\text{gr}(q)} \neq 0$. Logo $pq \neq 0$ e $\text{gr}(pq) = \text{gr}(p) + \text{gr}(q)$. ■

Proposição 9.29. *Seja \mathbf{A} um anel. Então \mathbf{A} é um domínio se, e somente se, $\mathbf{A}[x]$ é um domínio.*

Demonstração. Suponha que \mathbf{A} é um domínio e sejam $p_0, p_1 \in A[x] \setminus \{0\}$. Então $\text{gr}(p_0 p_1) = \text{gr}(p_1) + \text{gr}(p_1)$, o que mostra que $p_0 p_1 \neq 0$. Logo $\mathbf{A}[x]$ é um domínio. Reciprocamente, suponha que $\mathbf{A}[x]$ é um domínio e sejam $a_0, a_1 \in A \setminus \{0\}$. Então $a_0, a_1 \in A[x] \setminus \{0\}$ e, portanto, $a_0 a_1 \neq 0$. Logo \mathbf{A} é um domínio. ■

Podemos ver que $\mathbf{A}[x]$ nunca é um corpo, pois x não tem inverso.

Anel de Polinômios Multivariados

Definição 9.19. Sejam \mathbf{A} um anel e $n \in \mathbb{N}$. O *anel de polinômios* em n variáveis em \mathbf{A} é o conjunto

$$A[x_0, \dots, x_{n-1}] := \left\{ p \in A^{\mathbb{N}^n} \mid |\text{supp}(p)| < |\mathbb{N}| \right\}.$$

Os elementos de $A[x]$ são os *polinômios em n variáveis* em \mathbf{A} .

9.2.2 Produto de Anéis

Definição 9.20. Seja $(\mathbf{A}_i)_{i \in I} = (A_i, +_i, \times_i)_{i \in I}$ uma família de anéis. O *produto* da família $(\mathbf{A}_i)_{i \in I}$ é a tripla

$$\prod_{i \in I} \mathbf{A}_i := (A, +, \times)$$

em que $A = \prod_{i \in I} A_i$ é o produto de conjuntos,

$$\begin{aligned} +: A \times A &\longrightarrow A \\ (a, b) &\longmapsto (a_i +_i b_i)_{i \in I} \end{aligned}$$

e

$$\begin{aligned} \times: A \times A &\longrightarrow A \\ (a, b) &\longmapsto (a_i \times_i b_i)_{i \in I}. \end{aligned}$$

Denotaremos as operações $+_i$ todas por $+$ e as operações \times_i todas por \times quando não existir ambiguidade.

Proposição 9.30. Seja $(\mathbf{A}_i)_{i \in I} = (A_i, +_i, \times_i)_{i \in I}$ uma família de anéis. Então o produto $\prod_{i \in I} \mathbf{A}_i$ é um anel.

Demonstração. Como, para todo $i \in I$, o par $(A_i, +_i)$ é um grupo comutativo, segue que o par $(\prod_{i \in I} A_i, +)$ é um grupo comutativo.

Agora, devemos mostrar que $(\prod_{i=1}^n A_i, \times)$ é um monoide comutativo. Novamente, as propriedades de monoide comutativo decorrem do fato de que (A_i, \times_i) , $i \in I$, são todos monoides comutativos com elementos neutros 1_i , respectivamente. Sejam $a = (a_i)_{i \in I}, b = (b_i)_{i \in I}, c = (c_i)_{i \in I} \in \prod_{i \in I} A_i$. A operação \times é associativa, pois

$$\begin{aligned} (a \times b) \times c &= (a_i \times_i b_i)_{i \in I} \times c \\ &= ((a_i \times_i b_i) \times_i c_i)_{i \in I} \\ &= (a_i \times_i (b_i \times_i c_i))_{i \in I} \\ &= a \times (b_i \times_i c_i)_{i \in I} \\ &= a \times (b \times c), \end{aligned}$$

e comutativa, pois

$$a \times b = (a_i \times_i b_i)_{i \in I} = (b_i \times_i a_i)_{i \in I} = b \times a.$$

Ainda, $1 := (1_i)_{i \in I}$ é elemento neutro, pois

$$a \times 1 = (a_i \times 1_i)_{i \in I} = (a_i)_{i \in I} = a.$$

Por fim, como \times_i são ditributivas sobre $+_i$, temos que

$$\begin{aligned} a \times (b + c) &= a \times (b_i +_i c_i)_{i \in I} \\ &= (a_i \times_i (b_i +_i c_i))_{i \in I} \\ &= ((a_i \times_i b_i) +_i (a_i \times_i c_i))_{i \in I} \\ &= (a_i \times_i b_i)_{i \in I} + (a_i \times_i c_i)_{i \in I} \\ &= (a \times b) + (a \times c). \end{aligned}$$

■

9.3 Construções Específicas

9.3.1 Domínios e Corpos

Definição 9.21. Um *domínio de integridade* (ou *domínio*) é um anel \mathbf{A} tal que, para todos $a_0, a_1 \in A$,

$$a_0 \cdot a_1 = 0 \implies a_0 = 0 \text{ ou } a_1 = 0.$$

Definição 9.22. Um *corpo* é um anel \mathbf{A} tal que, para todo $a \in A \setminus \{0\}$, existe a^{-1} , de modo que $(A \setminus \{0\}, \times, ^{-1}, 1)$ é um grupo.

Proposição 9.31. *Todo corpo \mathbf{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 9.32 (Lei do corte em domínios). *Sejam \mathbf{A} um domínio e $a, a_1, a_2 \in A$, $a \neq 0$. Então*

$$aa_1 = aa_2 \implies a_1 = a_2$$

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 $(A \setminus \{0\}, \times, ^{-1}, 1)$ 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 $A \setminus \{0\}$.

9.3.2 Divisão e Associação em Anéis

Divisão

Definição 9.23. Sejam \mathbf{A} um anel e $a, a' \in A$. O elemento a divide o elemento a' em \mathbf{A} se, e somente se, existe $q \in A$ tal que $aq = a'$. O elemento a é um divisor de a' em \mathbf{A} , o elemento a' é um múltiplo de a em \mathbf{A} e denota-se $a \preceq_{\mathbf{A}} a'$. A relação $\preceq_{\mathbf{A}}$ é a relação de divisão em \mathbf{A} . Sempre que possível, o subíndice de $\preceq_{\mathbf{A}}$ será omitido.

Proposição 9.33. Seja \mathbf{A} um anel. A relação de divisão \preceq em A é uma pré-ordem.

Demonstração. (Reflexividade) Seja $a \in A$. Então $a \preceq a$, pois $a \cdot 1 = a$. (Transitividade) Sejam $a, a', a'' \in A$ tais que $a \preceq a'$ e $a' \preceq a''$. Então existem $q, q' \in A$ tais que $aq = a'$ e $a'q' = a''$. Logo $aqq' = a''$. Como $qq' \in A$, segue que $a \preceq a''$. ■

Proposição 9.34. Seja \mathbf{A} um anel.

1. Para todos $a \in A$ e $u \in A^*$,

$$u \preceq a \preceq 0;$$

2. Para todos $a \in A$ e $u \in A^*$,

$$a \preceq u \Leftrightarrow a \in A^*;$$

3. Para todo $a \in A$,

$$0 \preceq a \Leftrightarrow a = 0.$$

4. Para todos $a, a', a'' \in A$ tais que $a' \preceq a''$,

$$aa' \preceq aa''.$$

5. Para todos $u \in A^*$ e $a, a' \in A$ tais que $a \preceq a'$,

$$ua \preceq a \quad e \quad a \preceq ua'.$$

Demonstração. Sejam $a \in A$ e $u \in A^*$.

1. Como $u \in A^*$, existe $u^{-1} \in A^*$. Então $u \cdot (u^{-1}a) = a$ e segue que $u \preceq a$; como $a \cdot 0 = 0$, segue que $a \preceq 0$;
2. Se $a \preceq u$, 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 $a \preceq u$;
3. Se $0 \preceq a$, existe $q \in A$ tal que $0q = a$. Mas então $a = 0$. A recíproca segue da reflexividade de \preceq .
4. Se $a' \preceq a''$, existe $q \in D$ tal que $a'q = a''$, logo $aa'q = aa''$, portanto $aa' \preceq aa''$.
5. Usaremos a comutatividade. Se $a \preceq a'$, existe $q \in A$ tal que $aq = a'$, portanto

$$a' = uu^{-1}aq = uau^{-1}q,$$

logo $ua \preceq a'$, e

$$ua' = uaq = auq,$$

logo $a \preceq ua'$. ■

Proposição 9.35. *Sejam \mathbf{A} um anel e $a, a' \in A$. Então $aA \subseteq a'A$ se, e somente se, $a' \preceq a$.*

Demonstração. Se $aA \subseteq a'A$, então $a \in a'A$. Mas isso significa que existe $q \in A$ tal que $a = a'q$, o que mostra que $a' \preceq a$. A implicação contrária segue a mesma demonstração com as implicações invertidas. ■

Definição 9.24. Sejam \mathbf{A} um anel e $Q \subseteq A$. Um *divisor comum* de Q em \mathbf{A} é um elemento $d \in A$ que satisfaz, para todo $q \in Q$,

$$d \preceq q.$$

O conjunto dos divisores comuns de Q em \mathbf{A} é $\text{Div}_{\mathbf{A}}(Q)$. O subíndice \mathbf{A} será omitido sempre que possível.

Dualmente, um *múltiplo comum* de Q em \mathbf{A} é um elemento $m \in A$ que satisfaz, para todo $q \in Q$,

$$q \preceq m.$$

O conjunto dos múltiplos comuns de Q em \mathbf{A} é $\text{Mul}_{\mathbf{A}}(Q)$. O subíndice \mathbf{A} será omitido sempre que possível.

Proposição 9.36. *Sejam \mathbf{A} um anel e $Q \subseteq A$. Então*

1. $\text{Div}(A) = \text{Div}(A^*) = A^*$ e $\text{Div}(\emptyset) = \text{Div}(\{0\}) = A$;

2. $A^* \subseteq \text{Div}(Q) \subseteq A$;
3. $\{0\} \cap \text{Div}(Q) \neq \emptyset \Leftrightarrow Q \subseteq \{0\} \Leftrightarrow \text{Div}(Q) = A$.

Dualmente,

1. $\text{Mul}(A) = \text{Mul}(\{0\}) = \{0\}$ e $\text{Mul}(\emptyset) = \text{Mul}(A^*) = A$;
2. $\{0\} \subseteq \text{Mul}(Q) \subseteq A$;
3. $A^* \cap \text{Mul}(Q) \neq \emptyset \Leftrightarrow Q \subseteq A^* \Leftrightarrow \text{Mul}(Q) = A$.

Demonastração. 1. Seja $u \in A^*$. Então $u \preceq a$ para todo $a \in A$. Logo $u \in \text{Div}(A)$. Por outro lado, seja $d \in \text{Div}(A)$. Então $d \preceq a$ para todo $a \in A$. Em particular, $d \preceq 1$. Como $1 \in A^*$, então $d \in A^*$.

Seja $u \in A^*$. Então $u \preceq v$ para todo $v \in A^*$. Logo $u \in \text{Div}(A^*)$. Por outro lado, seja $d \in \text{Div}(A^*)$. Então $d \preceq u$ para todo $u \in A^*$. Logo $d \in A^*$.

Seja $a \in A$. Se $a \notin \text{Div}(\emptyset)$, existe $q \in \emptyset$ tal que $a \not\preceq q$, o que é absurdo. Logo $a \in \text{Div}(\emptyset)$.

Seja $a \in A$. Então $a \preceq 0$, o que implica $a \in \text{Div}(\{0\})$. A inclusão contrária é óbvia pela definição do conjunto dos divisores comuns.

2. Se $Q = \emptyset$, então $\text{Div}(Q) = A$. Se $Q \neq \emptyset$, sejam $q \in Q$ e $u \in A^*$. Então $u \preceq q$. Logo $u \in \text{Div}(Q)$. A inclusão $\text{Div}(Q) \subseteq A$ é óbvia pela definição do conjunto de divisores comuns;
3. Suponhamos que $\{0\} \cap \text{Div}(Q) \neq \emptyset$. Então $0 \in \text{Div}(Q)$. Se $Q = \emptyset$, então $Q \subseteq \{0\}$. Caso contrário, seja $q \in Q$. Como $0 \preceq q$, 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 $\text{Div}(Q) = A$.

Suponhamos que $\text{Div}(Q) = A$. Então $\{0\} \cap \text{Div}(Q) = \{0\} \neq \emptyset$.

Dualmente,

1. Note que $a \preceq 0$ para todo $a \in A$. Logo $0 \in \text{Mul}(A)$. Por outro lado, seja $m \in \text{Mul}(A)$. Então $a \preceq m$ para todo $a \in A$. Em particular, $0 \preceq m$, o que implica $m = 0$.

Note que $0 \preceq 0$, o que implica $0 \in \text{Mul}(\{0\})$. Por outro lado, seja $m \in \text{Mul}(\{0\})$. Então $0 \preceq m$, o que implica $m = 0$.

Seja $a \in A$. Se $a \notin \text{Mul}(\emptyset)$, existe $q \in \emptyset$ tal que $q \not\preceq a$, o que é absurdo. Logo $a \in \text{Mul}(\emptyset)$.

Sejam $a \in A$ e $u \in A^*$. Então $u \preceq a$, o que implica $a \in \text{Mul}_{bmA}(A^*)$. A inclusão contrária é óbvia pela definição do conjunto dos múltiplos comuns.

2. Se $Q = \emptyset$, então $\text{Mul}(Q) = A$. Se $Q \neq \emptyset$, seja $q \in Q$. Então $q \preceq 0$, o que implica $\{0\} \in \text{Mul}(Q)$. A inclusão $\text{Mul}(Q) \subseteq A$ é óbvia pela definição do conjunto dos múltiplos comuns;
3. Suponhamos que $A^* \cap \text{Mul}(Q) \neq \emptyset$. Seja $m \in A^* \cap \text{Mul}(Q)$. Se $Q = \emptyset$, então $Q \subseteq A^*$. Caso contrário, seja $q \in Q$. Como $q \preceq m$, pois $m \in \text{Mul}(Q)$, 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 $\text{Mul}(Q) = A$. Caso contrário, sejam $q \in Q$ e $a \in A$. Então $q \in A^*$ e segue que $q \preceq a$. Logo $a \in \text{Mul}(Q)$. Por outro lado, a inclusão $\text{Mul}(Q) \subseteq A$ é óbvia pela definição do conjunto de múltiplos comuns;
Suponhamos que $\text{Mul}(Q) = A$. Então $A^* \cap \text{Mul}(Q) = A^*$. Como $1 \in A^*$, segue que $A^* \cap \text{Mul}(Q) \neq \emptyset$. \blacksquare

Definição 9.25. Sejam \mathbf{A} um anel e $Q \subseteq A$. Um *máximo divisor comum* de Q em \mathbf{A} é um elemento $d \in A$ que satisfaz

1. $d \in \text{Div}(Q)$;
2. Para todo $d' \in \text{Div}(Q)$, $d' \preceq d$.

O conjunto dos máximos divisores comuns de Q em \mathbf{A} é $\text{mdc}_{\mathbf{A}}(Q)$. Se Q é um conjunto finito $Q = \{a_1, \dots, a_n\}$, denota-se $\text{mdc}_{\mathbf{A}}(Q) = \text{mdc}_{\mathbf{A}}(a_1, \dots, a_n)$ ou $\text{mdc}_{\mathbf{A}}(Q) = (a_1, \dots, a_n)$. O subíndice \mathbf{A} será omitido sempre que possível.

Dualmente, um *mínimo múltiplo comum* de Q em \mathbf{A} é um elemento $m \in A$ que satisfaz

1. $m \in \text{Mul}_{\mathbf{A}}(Q)$;
2. Para todo $m' \in \text{Mul}(Q)$, $m \preceq m'$.

O conjunto dos mínimos múltiplos comuns de Q em \mathbf{A} é $\text{mmc}_{\mathbf{A}}(Q)$. Se Q é um conjunto finito $Q = \{a_1, \dots, a_n\}$, denota-se $\text{mmc}_{\mathbf{A}} = \text{mmc}_{\mathbf{A}}(a_1, \dots, a_n)$ ou $\text{mmc}_{\mathbf{A}}(Q) = [a_1, \dots, a_n]$. O subíndice \mathbf{A} será omitido sempre que possível.

Proposição 9.37. Sejam \mathbf{A} um anel e $Q \subseteq A$. Então

1. $Q \subseteq \{0\} \Leftrightarrow \text{mdc}(Q) = \{0\}$;
2. $A^* \cap Q \neq \emptyset \Rightarrow \text{mdc}(Q) = A^*$.

Dualmente,

1. $Q \subseteq A^* \Leftrightarrow \text{mmc}(Q) = A^*$;

2. $\{0\} \cap Q \neq \emptyset \Rightarrow \text{mmc}(Q) = \{0\}$.

Demonstração. 1. Suponha que $Q \subseteq \{0\}$. Então $A = \text{Div}(Q)$. Em particular, $0 \in \text{Div}(Q)$. Ainda, para todo $d \in \text{Div}(Q)$, vale que $d \preceq 0$, pois $d \in A$. Logo $0 \in \text{mdc}(Q)$. Ainda, se $d \in \text{mdc}(Q)$, então $0 \preceq d$, pois $0 \in \text{Div}(Q)$ e $d \in \text{mdc}(Q)$. Portanto $d = 0$. Reciprocamente, se $\text{mdc}(Q) = \{0\}$, então $0 \in \text{Div}(Q)$; ou seja, $\{0\} \cap \text{Div}(Q) \neq \emptyset$, 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 $u \in \text{Div}(Q)$. Ainda, se $d \in \text{Div}(Q)$, então, em particular, $d \preceq a$. Mas como $a \in A^*$, segue que $d \in A^*$. Logo $d \preceq u$, o que mostra que $u \in \text{mdc}(Q)$. Por outro lado, se $d \in \text{mdc}(Q)$, então $d \preceq a$. Como $a \in A^*$, então $d \in A^*$, e concluímos que $A^* = \text{mdc}(Q)$.

Dualmente,

1. Suponha que $Q \subseteq A^*$. Então $A = \text{Mul}(Q)$. Seja $u \in A^*$. Então $u \in \text{Mul}(Q)$. Ainda, para todo $m \in \text{Mul}(Q)$, vale que $u \preceq m$, pois $m \in A$. Logo $u \in \text{mmc}(Q)$. Ainda, se $m \in \text{mmc}(Q)$, então $m \preceq u$, pois $u \in \text{Mul}(Q)$ e $m \in \text{mmc}(Q)$. Portanto $m \in A^*$. Reciprocamente, se $\text{mmc}(Q) = A^*$, então $1 \in \text{Mul}(Q)$; ou seja, $A^* \cap \text{Mul}(Q) \neq \emptyset$, o que implica $Q \subseteq A^*$.
2. Como $\{0\} \cap Q \neq \emptyset$, então $0 \in Q$. Note que $0 \in \text{Mul}(Q)$. Ainda, se $m \in \text{Mul}(Q)$, então $0 \preceq m$. Então segue que $0 \in \text{mmc}(Q)$. Por outro lado, se $m \in \text{mmc}(Q)$, então $0 \preceq m$, o que implica $m = 0$, e concluímos que $\text{mmc}(Q) = \{0\}$. ■

Relação de Associação

Definição 9.26. Sejam \mathbf{A} um anel e $a, a' \in A$. O elemento a é *associado* ao elemento a' em \mathbf{A} se, e somente se, $a \preceq_{\mathbf{A}} a'$ e $a' \preceq_{\mathbf{A}} a$. Denota-se $a \sim_{\mathbf{A}} a'$. A relação $\sim_{\mathbf{A}}$ é a relação de *associação* em \mathbf{A} . Sempre que possível, o subíndice de $\sim_{\mathbf{A}}$ será omitido.

A relação \sim de associação em anéis é uma equivaência, pois é a equivalência induzida pela pré-ordem de divisão \preceq em anéis. Quando o anel A é um domínio, essa relação é equivalente a existir $u \in A^*$ tal que $au = a'$.

Proposição 9.38. Sejam \mathbf{A} um domínio e $a, a' \in A$. Então $a \sim a'$ se, e somente se, existe $u \in A^*$ tal que $au = a'$.

Demonstração. Se $a \sim a'$, então $a \preceq a'$ e $a' \preceq a$. Isso é equivalente a existirem $q, q' \in A$ tais que $aq = a'$ e $a'q' = a$, o que é equivalente a $a = aqq'$ e $a' = a'q'q$. Como \mathbf{A} é um domínio, a e a' não são divisores de 0, e concluímos que $qq' = q'q = 1$, portanto $q, q' \in A^*$.

Reciprocamente, se existe $u \in A^*$ tal que $au = a'$, então $a = a'u^{-1}$, portanto $a \preceq a'$ e $a' \preceq a$, logo $a \sim a'$. \blacksquare

Proposição 9.39. *Seja \mathbf{A} um anel.*

1. *Para todos $a_0, \dots, a_{n-1}, a'_0, \dots, a'_{n-1} \in A$, se para todo $i \in [n]$ vale $a_i \sim a'_i$, então*

$$\bigtimes_{i \in [n]} a_i \sim \bigtimes_{i \in [n]} a'_i.$$

Demonstração. 1. Sejam $a_0, \dots, a_{n-1}, a'_0, \dots, a'_{n-1} \in A$ e $i \in [n]$. Se $a_i \sim a'_i$, então existe $u_i \in A^*$ tal que $a_i u_i = a'_i$. Logo $a_0 \cdots a_{n-1} \cdot u_0 \cdots u_{n-1} = a'_0 \cdots a'_{n-1}$. Como $u_0 \cdots u_{n-1} \in A^*$, segue que

$$\bigtimes_{i \in [n]} a_i \sim \bigtimes_{i \in [n]} a'_i. \quad \blacksquare$$

Proposição 9.40. *Sejam \mathbf{D} um domínio e $d_0, \dots, d_{n-1} \in D$ não todos nulos. Se d, d' são máximos divisores comuns de d_0, \dots, d_{n-1} , então $d \sim d'$.*

Demonstração. Como d é máximo divisor comum de d_0, \dots, d_{n-1} e d' é divisor comum de d_0, \dots, d_{n-1} , então $d' \preceq d$. Analogamente, $d \preceq d'$. Portanto $d \sim d'$. \blacksquare

9.3.3 Irredutíveis, Primos e Fatoração

Definição 9.27. Seja \mathbf{D} um domínio. Um elemento *irredutível* em \mathbf{D} é um elemento $i \in D \setminus (D^* \cup \{0\})$ que satisfaz, para todos $d, d' \in D$ tais que $i = dd'$,

$$d \in D^* \text{ ou } d' \in D^*.$$

Proposição 9.41. *Sejam \mathbf{D} um domínio e $i \in D$ irredutível. Para todo $i' \in D$ tal que $i \sim i'$, i' é irredutível.*

Demonstração. Se $i \sim i'$, existe $u \in D^*$ tal que $i' = ui$. Primeiro, devemos mostrar que $ui \notin (D^* \cup \{0\})$. Como $u \neq 0$ e $i \neq 0$ e \mathbf{D} é domínio, então $ui \neq 0$. Supondo que $ui \in D^*$, então existe $u' \in D^*$ tal que $u'(ui) = 1$. Mas então $u'u = i^{-1}$, uma contradição porque $i \notin D^*$. Logo $ui \notin D^*$.

Agora, sejam $d, d' \in D$ tais que $ui = dd'$. Então $i = u^{-1}dd'$. Se $d \notin D^*$ e $d' \notin D^*$, então $u^{-1}d \notin D^*$ e $u^{-1}d' \notin D^*$. Logo segue que $i = (u^{-1}d)d'$, uma contradição porque i é irredutível. \blacksquare

Definição 9.28. Seja \mathbf{D} um domínio. Um elemento *primo* em \mathbf{D} é um elemento $p \in D \setminus (D^* \cup \{0\})$ que satisfaz, para todos $d, d' \in D$ tais que $p \preceq dd'$,

$$p \preceq d \text{ ou } p \preceq d'.$$

Proposição 9.42. *Sejam \mathbf{D} um domínio e p primo.*

1. *Para todo $p' \in D$ tal que $p \sim p'$, p' é primo;*
2. *Para todos d_0, \dots, d_{n-1} tais que $p \preceq d_0 \cdots d_{n-1}$, existe $i \in [n]$ tal que $p \preceq d_i$;*
3. *O elemento p é irreduzível.*

Demonstração. 1. Se $p \sim p'$, existe $u \in D^*$ tal que $p' = up$. Primeiro, devemos mostrar que $up \notin (D^* \cup \{0\})$. Como $u \neq 0$, $p \neq 0$ e \mathbf{D} é domínio, então $up \neq 0$. Supondo que $up \in D^*$, então existe $u' \in D^*$ tal que $u'(up) = 1$. Mas isso implica $u'u = p^{-1}$, uma contradição porque $p \notin D^*$. Logo $p' = up \notin D^*$.

Agora, usaremos a comutatividade. Sejam $d, d' \in D$ tais que $up \preceq dd'$. Então

$$p = u^{-1}up \preceq u^{-1}dd'.$$

Como p é primo, $p \preceq u^{-1}d$ ou $p \preceq d'$. No primeiro caso, $up \preceq uu^{-1}d = d$; no segundo caso, segue pela comutatividade que $p' = up \preceq d'$.

2. Vamos mostrar por indução em n . O caso base é trivial. Para demonstrar o passo indutivo, suponhamos que a propriedade vale para um natural n . Então, se $p \preceq d_0 \cdots d_n$, então como p é primo, $p \preceq d_0 \cdots d_{n-1}$ ou $p \preceq d_n$. Se $p \preceq d_0 \cdots d_{n-1}$, pela hipótese de indução, existe $i \in [n]$ tal que $p \preceq d_i$; caso contrário, $p \preceq d_n$. Logo existe $i \in [n+1]$ tal que $p \preceq d_i$.
3. Se existem $d, d' \in D$ tais que $p = dd'$, então $p \preceq dd'$. Como p é primo, então $p \preceq d$ ou $p \preceq d'$. Se $p \preceq d$, então existe $q \in D$ tal que $pq = d$. Assim, segue que $p = dd' = pqd'$ e, como \mathbf{D} é domínio, $1 = qd'$. Logo $d' \in D^*$. Analogamente, se $p \preceq d'$, segue que $d \in D^*$ (usamos a comutatividade). Portanto p é irreduzível. ■

Proposição 9.43. *Seja \mathbf{D} um domínio euclidiano que não é um corpo e ϕ uma função euclidiana em \mathbf{D} . Então $d_0 \in D$ tal que*

$$\phi(d_0) = \min \{\phi(d) \mid d \in D \setminus (D^* \cup \{0\})\}$$

é um elemento irreduzível em \mathbf{D} .

Demonstração. Primeiro, definamos $m := \min \{\phi(d) \mid d \in D \setminus (D^* \cup \{0\})\}$ e notemos que existe tal mínimo porque o conjunto dos números naturais é bem ordenado. Notemos que $d_0 \notin D^* \cup \{0\}$ por definição. Suponha que $d_0 = d_1d_2$, com $d_1, d_2 \in D$. Como \mathbf{D} é um domínio, então $d_1 \neq 0$ e $d_2 \neq 0$. Suponha que $d_1, d_2 \notin D^*$. Então $\phi(d_1) \geq m = \phi(d_1d_2) \geq \phi(d_1)$ e $\phi(d_2) \geq m = \phi(d_1d_2) \geq \phi(d_2)$. Logo $\phi(d_1) = \phi(d_1d_2)$ e $\phi(d_2) = \phi(d_1d_2)$, o que implica $d_1, d_2 \in D^*$, que é absurdo. ■

Fatoração

Definição 9.29. Sejam D um domínio, $a \in D \setminus \{0\}$ e $n \in \mathbb{N}$. Uma *fatoração* de a em n fatores é uma sequência $(p_i)_{i \in [n]}$ de irredutíveis tal que

$$a \sim \bigtimes_{i \in [n]} p_i.$$

Duas fatorações $(p_i)_{i \in [n]}$ e $(p'_i)_{i \in [n']}$ de a são *associadas* se, e somente se, $n = n'$ e existe uma permutação $\sigma \in \mathfrak{S}_n$ tal que, para todo $i \in [n]$, $p_i \sim p'_{\sigma(i)}$.

Claramente, a relação de associação de fatorações é uma relação de equivalência. Note que só existe uma sequência $(p_i)_{i \in [0]}$ — a sequência vazia \emptyset — pois $D^0 = \emptyset$, e nesse caso

$$\bigtimes_{i \in [0]} p_i = 1,$$

pois $[0]$. Esse é um caso degenerado que admitimos para facilitar as demonstrações. Portanto um elemento $u \in D^*$ tem uma única fatoração $(p_i)_{i \in [0]}$ em 0 fatores, já que

$$u \sim 1 = \bigtimes_{i \in [0]} p_i.$$

Reciprocamente, se $a \in D \setminus \{0\}$ tem fatoração em 0 fatores, então

$$a \sim \bigtimes_{i \in [0]} p_i = 1,$$

logo $a \in D^*$. Para $p \in D$ irredutível, $(p)_{i \in [1]}$ é uma fatoração de p e, se $(p_i)_{i \in [n]}$ é uma fatoração de p , então

$$p \sim \bigtimes_{i \in [n]} p_i.$$

Como $p \notin D^*$, $n \neq 0$. Se $n > 1$, como p é irredutível segue que $\bigtimes_{i \in [n-1]} p_i \in D^*$ ou $p_{n-1} \in D^*$, o que é uma contradição, pois os p_i são irredutíveis; logo $n = 1$ e $p \sim p_0$, portanto as fatorações $(p)_{i \in [1]}$ e $(p_0)_{i \in [1]}$ são associadas.

Isso mostra que elementos unitários têm sempre fatorações associadas, mas isso nem sempre é verdade para outros elementos do domínio. Também é verdade que todo elemento irredutível tem fatoração e que todas suas fatorações são associadas. Ressaltamos na proposição seguinte as propriedades aqui comentadas.

Proposição 9.44. *Seja D um domínio. Então*

1. A relação de associação de fatorações é uma relação de equivalência;
2. Todo elemento unitário ou irredutível tem fatoração e todas suas fatorações são associadas.

Definição 9.30. Um domínio de fatoração única é um domínio \mathbf{D} que satisfaz

1. (Existência de Fatoração) Todo elemento $d \in D \setminus \{0\}$ tem fatoração;
2. (Unicidade de Fatoração) Todas fatorações de $d \in D \setminus \{0\}$ são associadas.

Domínios de fatoração única também são chamados de domínios fatoriais. Antes de demonstrar a próxima proposição, enunciamos um lema simples que usaremos na demonstração.

Lema 9.45. Para todo $k \in [n]$, a função

$$\begin{aligned} f_k: [n-1] &\longrightarrow [n] \setminus \{k\} \\ i &\longmapsto \begin{cases} i, & i < k \\ i+1, & i \geq k. \end{cases} \end{aligned}$$

é bijetiva e sua inversa é

$$\begin{aligned} f_k^{-1}: [n] \setminus \{k\} &\longrightarrow [n-1] \\ i &\longmapsto \begin{cases} i, & i < k \\ i-1, & i > k \end{cases} \end{aligned}$$

Para toda permutação $\sigma': [n-1] \longrightarrow [n-1]$, a função

$$\begin{aligned} \sigma: [n] &\longrightarrow [n] \\ i &\longmapsto \begin{cases} f_k \circ \sigma'(i), & i < n-1 \\ k, & i = n-1, \end{cases} \end{aligned}$$

é uma permutação.

A proposição a seguir relaciona duas noções da teoria de fatoração em anéis. A primeira é a unicidade de fatoração e a segunda é a relação entre elementos irreduzíveis e primos.

Proposição 9.46. Seja \mathbf{D} um domínio tal que todo elemento não nulo tem fatoração. Então as fatorações de $d \in D \setminus \{0\}$ são todas associadas se, e somente se, todo elemento irreduzível de \mathbf{D} é primo.

Demonstração. Suponhamos, primeiro, que todas fatorações de $d \in D \setminus \{0\}$ são associadas. Sejam p irreduzível e $d, d' \in D$ tais que $p \preceq dd'$. Então existe $q \in D$ tal que $pq = dd'$. Se $d = 0$ ou $d' = 0$, então $p \preceq d$ ou $p \preceq d'$. Caso $d, d' \in D \setminus \{0\}$, então existem fatorações $(p_i)_{i \in [n]}$ de d e $(p'_i)_{i \in [n']}$ de d' . Ainda, como $p \neq 0$, segue

que $q \neq 0$, pois D é domínio, e portanto existe fatoração $(q_i)_{i \in [m]}$ de q . Isso implica que

$$p \times_{i \in [m]} q_i \sim pq \sim \left(\times_{i \in [n]} p_i \right) \left(\times_{i \in [n']} p'_i \right).$$

Temos assim duas fatorações para pq , o que implica que existe $i \in [n]$ tal que $p \sim p_i$ ou $i \in [n']$ tal que $p \sim p'_i$. Então $p \preceq p_i$ ou $p \preceq p'_i$. No primeiro caso, como $p_i \preceq d$, segue que $p \preceq d$. No segundo caso, como $p'_i \preceq d'$, segue que $p \preceq d'$. Portanto p é primo.

Reciprocamente, suponhamos todo irreduzível de \mathbf{D} é primo. Sejam $d \in D \setminus \{0\}$, e $(p_i)_{i \in [n]}$ e $(p'_i)_{i \in [n']}$ fatorações de d , de modo que

$$\times_{i \in [n]} p_i \sim d \sim \times_{i \in [n']} p'_i.$$

Todos os irreduzíveis p_0, \dots, p_{n-1} e $p'_0, \dots, p'_{n'-1}$ são primos. Mostraremos que essas fatorações são associadas por indução em $m := \min\{n, n'\}$. Para o caso base, se $m = 0$, então $n = 0$ ou $n' = 0$. Em ambos os casos, $d \sim 1$, ou seja, $d \in D^*$, portanto todas suas fatorações são associadas. Agora, seja $m > 0$ e suponhamos que todas fatorações com k e k' fatores de um elemento $d \in D \setminus \{0\}$ tais que $\min\{k, k'\} < m$ sejam associadas. Como p_{n-1} é primo e $p_{n-1} \preceq d \sim p'_0 \cdots p'_{n'-1}$, existe $k \in [n']$ tal que $p_{n-1} \preceq p'_k$. Portanto existe $q \in D$ tal que $p_{n-1}q = p'_k$. Como p_{n-1} e p'_k são irreduzíveis, então $q \in D^*$. Portanto segue que

$$\begin{aligned} \left(\times_{i \in [n-1]} p_i \right) p_{n-1} &\sim \left(\times_{i \in [k]} p'_i \right) p_{n-1} \left(\times_{i \in [n'-k-1]} p'_{i+k+1} \right) \\ &= \left(\times_{i \in [k]} p'_i \right) \left(\times_{i \in [n'-k-1]} p'_{i+k+1} \right) p_{n-1}. \end{aligned}$$

Como \mathbf{D} é domínio e $p_{n-1} \neq 0$, então

$$\times_{i \in [n-1]} p_i \sim \left(\times_{i \in [k]} p'_i \right) \left(\times_{i \in [n'-k-1]} p'_{i+k+1} \right).$$

Considerando a bijeção (9.45)

$$\begin{aligned} f_k: [n-1] &\longrightarrow [n] \setminus \{k\} \\ i &\longmapsto \begin{cases} i, & i < k \\ i+1, & i \geq k \end{cases} \end{aligned}$$

e definindo, para todo $i \in [n'] \setminus \{k\}$, $q_i := p'_{f_k(i)}$, temos uma sequência de irreduíveis $(q_i)_{i \in [n'-1]}$ tais que

$$\bigtimes_{i \in [n-1]} p_i \sim \bigtimes_{i \in [n'-1]} q_i.$$

Como $m > 0$, então $n > 0$ e $n' > 0$, portanto as expressões são duas fatorações, uma com $n - 1$ e outra com $n' - 1$ fatores. Como $\min\{n - 1, n' - 1\} = m - 1 < m$, vale a hipótese de indução, e então, $n - 1 = n' - 1$ e existe permutação σ' de $[n - 1]$ tal que, para todo $i \in [n - 1]$, $p_i \sim q_{\sigma'(i)}$. Então $n = n'$ e, considerando a permutação (9.45)

$$\begin{aligned} \sigma: [n] &\longrightarrow [n] \\ i &\longmapsto \begin{cases} f_k \circ \sigma'(i), & i < n - 1 \\ k, & i = n - 1, \end{cases} \end{aligned}$$

segue que, para todo $i \in [n]$, $p_i \sim q_{\sigma(i)}$, pois, se $i < n - 1$, então

$$p_i \sim q_{\sigma'(i)} = p'_{f_k(\sigma'(i))} = p'_{\sigma(i)},$$

e, se $i = n - 1$, então $p_{n-1} \sim p'_k = p'_{\sigma(n-1)}$. Isso mostra que as fatorações $(p_i)_{i \in [n]}$ e $(p'_i)_{i \in [n']}$ são associadas. \blacksquare

Definição 9.31. Sejam D um domínio, $a \in D \setminus \{0\}$ e $n \in \mathbb{N}$. Uma *fatoração reduzida* de a em n fatores é uma sequência $(p_i, e_i)_{i \in [n]}$ em que $(p_i)_{i \in [n]}$ é uma sequência de irreduíveis e $(e_i)_{i \in [n]}$ é uma sequência de naturais estritamente positivos tais que

$$a \sim \bigtimes_{i \in [n]} p_i^{e_i}$$

e, para todos $i, i' \in [n]$, $i \neq i'$ implica que $p_i \not\sim p_{i'}$.

Proposição 9.47. *Seja D um domínio de fatoração única. Então*

1. (*Existência de Fatoração Reduzida*) Todo $d \in D \setminus \{0\}$ tem fatoração reduzida;
2. (*Unicidade de Fatoração Reduzida*) Para todo $d \in D \setminus \{0\}$, se

$$(p_i, e_i)_{i \in [n]} \quad e \quad (p'_i, e'_i)_{i \in [n']}$$

são fatorações reduzidas de d , então $n = n'$ e existe permutação $\sigma \in \mathfrak{S}_n$ tal que, para todo $i \in [n]$, $p_i \sim p'_{\sigma(i)}$ e $e_i = e'_{\sigma(i)}$.

Demonstração. Seja $d \in D \setminus \{0\}$. Como \mathbf{D} é domínio de fatoração única, existe fatoração $(p'_i)_{i \in [n']}$ de d em irreduutíveis tais que

$$d \sim \bigtimes_{i \in [n']} p'_i.$$

Vamos considerar os conjuntos $I_i := \{j \in [n'] \mid p'_j \sim p'_i\}$ dos índices de elementos da fatoração de d que são associados. Esses conjuntos são uma partição de $[n']$: ou seja, $P := \{I_i \mid i \in [n']\}$ é uma partição de $[n']$. Para mostrar isso, seja $n := |P|$ e sejam P_0, \dots, P_{n-1} os elementos de P (note que os conjuntos P_i são os conjuntos I_i , mas reindexados). Primeiro, notemos que $\emptyset \notin P$ por definição. Segundo, notemos que

$$\bigcup_{j \in [n]} P_j = [n']$$

pois, para todo $j \in [n']$, existe $k \in [n]$ tal que $I_j = P_k$ e, como $j \in I_j$, isso implica que $j \in \bigcup_{i \in [n]} P_i$. Terceiro, sejam $j, k \in [n]$; 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

$$d \sim \bigtimes_{i \in [n']} p'_i = \bigtimes_{k \in [n]} \bigtimes_{i \in P_k} p'_i.$$

Sendo assim, seja $k \in [n]$. Definamos $p_k := p'_{\min(P_k)}$ e $e_k := |P_k|$. Segue claramente que p_k é irreduutível e que $e_k \in \mathbb{N}^*$. Como, para todo $i \in P_k$, vale $p'_i \sim p_k$,

$$\bigtimes_{i \in P_k} p'_i \sim \bigtimes_{i \in P_k} p_k = p_k^{e_k}.$$

Assim, segue que

$$d \sim \bigtimes_{k \in [n]} \bigtimes_{i \in P_k} p'_i = \bigtimes_{k \in [n]} p_k^{e_k}.$$

A unicidade segue da unicidade de fatorações. ■

A proposição seguinte vale para um número finito de elementos, mas mostramos somente para dois elementos.

Proposição 9.48. *Seja \mathbf{D} um domínio de fatoração única. Então, para todos $a, b \in D \setminus \{0\}$, existe $d \in \text{mdc}(a, b)$.*

Demonstração. Se $\{a, b\} \cap D^* \neq \emptyset$, então $\text{mdc}(a, b) = D^*$. Suponhamos, então, que $\{a, b\} \notin D \setminus (D^* \cup \{0\})$. Como \mathbf{D} é domínio de fatoração única, existem fatorações $(p_i)_{i \in [n]}$ de a e $(q_i)_{i \in [n']}$ de b . 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 $\text{mdc}(a, b) = D^*$. Para isso, mostraremos que $1 \in \text{mdc}(a, b)$. Notamos que $1 \in D^* \subseteq \text{Div}(a, b)$. Agora, seja $d \in \text{Div}(a, b)$. Como $0 \notin \{a, b\}$, então $0 \notin \text{Div}(a, b)$. Se $d \in D^*$, então $d \preceq 1$, logo $1 \in \text{mdc}(a, b)$. Se $d \in D \setminus (D^* \cup \{0\})$, então existe p irredutível tal que $p \preceq d$, portanto $p \preceq a$ e $p \preceq b$. Como \mathbf{D} é domínio de fatoração única, p é primo. Então segue que existem i e j tais que $p \preceq p_i$ e $p \preceq q_j$. Como esses elementos são irredutíveis, $p \sim p_i$ e $p \sim q_j$, portanto $p_i \sim q_j$, o que é uma contradição. Logo $1 \in \text{mdc}(a, b)$. Como todos os máximos divisores comuns são associados, então $D^* = \text{mdc}(a, b)$.

Se $k \geq 1$, mostraremos que $p_1 \cdots p_k \in \text{mdc}(a, b)$. Primeiro, notamos que $p_1 \cdots p_k \preceq a$ e $q_1 \cdots q_k \preceq b$. Como $p_i \sim q_i$ para todo $i \leq k$, então $p_1 \cdots p_k \sim q_1 \cdots q_k$. Logo $p_1 \cdots p_k \preceq q_1 \cdots q_k$ e, da transitividade de \preceq , segue que $p_1 \cdots p_k \preceq b$. Logo $p_1 \cdots p_k \in \text{Div}(a, b)$. Então, seja $d \in \text{Div}(a, b)$. Se $d \in D^*$, então $d \preceq p_1 \cdots p_k$. Logo $p_1 \cdots p_k \in \text{mdc}(a, b)$. Se $d \in D \setminus (D^* \cup \{0\})$, então existem r_1, \dots, r_l irredutíveis tais que $d = r_1 \cdots r_l$. Por \mathbf{D} ser domínio, r_1, \dots, r_l são primos. Como $d \preceq a$, então $r_1 \preceq p_1 \cdots p_k$. Como r_1 é primo, existe $i_1 \in \{1, \dots, k\}$ tal que $r_1 \preceq p_{i_1}$. 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 $r_2 \cdots r_l \preceq p_1 \cdots p_{i_1-1} \cdot s_1 \cdot p_{i_1+1} \cdots p_k$, pois \mathbf{D} é domínio. Repetindo o processo indutivamente, conclui-se que existem i_1, \dots, i_m tais que $r_j \sim p_{i_j}$ para todo $j \in \{1, \dots, l\}$. Da mesma forma, conclui-se que existem i'_1, \dots, i'_m tais que $r_j \sim q_{i'_j}$ para todo $j \in \{1, \dots, l\}$. 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 $p_{i_1} \cdots p_{i_m} \preceq p_1 \cdots p_k$ e $q_{i'_1} \cdots q_{i'_m} \preceq q_1 \cdots q_k$, então $d \preceq p_1 \cdots p_k$. ■

9.3.4 Ideais Primos e Ideais Maximaais

Definição 9.32. Seja \mathbf{A} um anel. Um *ideal primo* de \mathbf{A} é um ideal $I \trianglelefteq A$ tal que

1. $\forall a, b \in A \quad ab \in I \Rightarrow a \in I \text{ ou } b \in I$.

Teorema 9.49. Seja \mathbf{A} um anel e $I \trianglelefteq A$. Então I é um ideal primo de \mathbf{A} se, e somente se, \mathbf{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 \mathbf{A}/I é um domínio se, e somente se,

$$\forall \alpha, \beta \in A/I \quad \alpha\beta = 0_{A/I} \Rightarrow \alpha = 0_{A/I} \text{ ou } \beta = 0_{A/I}.$$

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

$$\forall a, b \in A \quad ab = 0 \Rightarrow a = 0 \text{ ou } b = 0,$$

que é a definição de ideal primo. ■

Definição 9.33. Seja \mathbf{A} um anel. Um *ideal maximal* de \mathbf{A} é um ideal $I \triangleleft A$ tal que

$$\forall J \in \wp(A) \quad I \subseteq J \text{ e } J \trianglelefteq A \Rightarrow J = I \text{ ou } J = A.$$

Teorema 9.50. Seja \mathbf{A} um anel e $I \triangleleft A$. Então I é um ideal maximal de \mathbf{A} se, e somente se, \mathbf{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 (9.8).

\Leftarrow Suponha que I é um ideal maximal de \mathbf{A} . Vamos mostrar que os únicos ideais de \mathbf{A}/I são $\{0+I\}$ e A/I . Seja $L \trianglelefteq A/I$ e consideremos a projeção canônica

$$\begin{aligned} \pi: A &\longrightarrow A/I \\ a &\longmapsto a + I. \end{aligned}$$

Sabemos que $\pi^{-1}(L) = \{a \in A : \pi(a) \in L\} \trianglelefteq A$ (9.16). Como $0+I = 0_{A/I} \in L$, isso implica que $\pi^{-1}(0+I) \subseteq \pi^{-1}(L)$. Notando que $\pi^{-1}(0+I) = \text{nuc}(\phi) = I$, 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 \mathbf{A}/I é um corpo. Consideremos $J \trianglelefteq A$ tal que $I \subseteq J$ e a projeção canônica $\pi: A \longrightarrow A/I$. Como π é um homomorfismo de anéis bijetivo, temos que $\pi(J) \trianglelefteq A/I$ (9.17). Como \mathbf{A}/I é corpo, $\pi(J) = 0_{A/I}$ ou $\pi(J) = A/I$. No primeiro caso, $J = \text{nuc}(\pi) = I$. No segundo caso, $J = \pi^{-1}(\pi(J)) = \pi^{-1}(A/I) = A$. Logo I é ideal maximal de A . ■

Proposição 9.51. Seja \mathbf{A} um anel e $I \triangleleft A$ 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 (9.50). Mas isso implica que A/I é um domínio (9.31). Concluímos, portanto, que I é um ideal primo (9.49). ■

9.3.5 Domínios Euclidianos

Definição 9.34. Seja \mathbf{D} um domínio. Uma *função euclidiana* em \mathbf{D} é uma função $\phi : D \setminus \{0\} \rightarrow \mathbb{N}$ que satisfaz

1. Para todos $a \in D$ e $b \in D \setminus \{0\}$, existem $q, r \in D$ tais que
 - (a) $a = qb + r$;
 - (b) $r = 0$ ou $\phi(r) < \phi(b)$;
2. Para todos $a, b \in D \setminus \{0\}$, $\phi(a) \leq \phi(ab)$.

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 9.52. *Sejam \mathbf{D} um domínio e $\phi : D \setminus \{0\} \rightarrow \mathbb{N}$ uma função que satisfaz*

1. *Para todos $a \in D$ e $b \in D \setminus \{0\}$, existem $q, r \in D$ tais que*
 - (a) $a = qb + r$;
 - (b) $r = 0$ ou $\phi(r) < \phi(b)$;

Então existe uma função euclidiana em \mathbf{D} .

Proposição 9.53. *Sejam \mathbf{D} um domínio, ϕ uma função euclidiana em \mathbf{D} e $a, b \in D$.*

Definição 9.35. Um *domínio euclidiano* é um domínio em que existe uma função euclidiana.

Proposição 9.54. *Os anéis \mathbb{Z} e $\mathbb{Z}[i]$ são domínios euclidianos.*

Proposição 9.55. *Seja \mathbf{C} um corpo. Então $\mathbf{C}[x]$ é um domínio euclidiano.*

Definição 9.36. Um *domínio principal* é um domínio em que todo ideal é principal.

Proposição 9.56. *Seja \mathbf{D} um domínio euclidiano. Então \mathbf{D} é um domínio principal.*

Demonstração. Seja ϕ uma função euclidiana em \mathbf{D} e $I \trianglelefteq D$. Se $I = \{0\}$, então $I = 0I$. Se $I \neq 0$, seja $a \in I \setminus \{0\}$ tal que $\phi(a) = \min \{\phi(i) \mid i \in I \setminus \{0\}\}$. 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 $\phi(a) = \min \{\phi(i) \mid i \in I \setminus \{0\}\}$. Logo $r = 0$, o que implica $b = aq$; ou seja, $I \subseteq aD$. Como a inclusão inversa sempre vale, então $I = aD$. ■

Proposição 9.57. *Sejam \mathbf{D} um domínio euclidiano, ϕ uma função euclidiana em \mathbf{D} e $d_1, d_2 \in D \setminus \{0\}$. Então $d_1 \in D^*$ se, e somente se, $\phi(d_2) = \phi(d_1d_2)$.*

Demonstração. Se $d_1 \in D^*$, então existe $d_1^{-1} \in D$. Assim, temos que $\phi(d_1d_2) \leq \phi(d_1d_2d_1^{-1}) = \phi(d_2)$. Por outro lado, sempre vale $\phi(d_2) \leq \phi(d_1d_2)$. Logo $\phi(d_1d_2) = \phi(d_2)$. Por outro lado, suponha $\phi(d_1d_1) = \phi(d_2)$. Existem $q, r \in D$ tais que $d_2 = d_1d_2q + r$. Se $r \neq 0$, então, como $r = d_2 - d_1d_2q = d_2(1 - d_1q)$ e \mathbf{D} é domínio, segue que $1 - qa \neq 0$. Logo $\phi(r) = \phi(d_2(1 - d_1q)) \geq \phi(d_2) = \phi(d_1d_2)$, contradição. Logo $r = 0$ e temos $d_2 = d_1d_2q$. Como $d_2 \neq 0$ e \mathbf{D} é domínio, então $d_1q = 1$, o que implica $d_1 \in D^*$. ■

Proposição 9.58. *Seja \mathbf{D} um domínio euclidiano e ϕ uma função euclidiana em \mathbf{D} . Então*

$$D^* = \{d \in D \mid \phi(d) = \phi(1)\}.$$

Demonstração. Tome $d_2 = 1$ na proposição anterior. ■

9.3.6 Raízes de Polinômios

Proposição 9.59. *Seja 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 $\text{gr}(r) < \text{gr}(g)$.*

Demonstração. Sejam $n := \text{gr}(f)$, $m := \text{gr}(g)$,

$$f = \sum_{i=0}^n a_i x^i \quad \text{e} \quad g = \sum_{i=0}^{m-1} b_i x^i + x^m$$

Se $m \leq n$, definimos $q(x) := a_n x^{n-m}$ e $r := f - qg$ e temos

$$\begin{aligned} r(x) &= f(x) - q(x)g(x) \\ &= \sum_{i=0}^n a_i x^i - a_n x^{n-m} \left(\sum_{i=0}^{m-1} b_i x^i + x^m \right) \\ &= \sum_{i=0}^n a_i x^i - \left(\sum_{i=0}^{m-1} a_n b_i x^{n-m+i} + a_n x^n \right) \\ &= \sum_{i=0}^{n-1} a_i x^i - \sum_{i=n-m}^{n-1} a_n b_{i-n+m} x^i \\ &= \sum_{i=0}^{n-m-1} a_i x^i + \sum_{i=n-m}^{n-1} (a_i - a_n b_{i-n+m}) x^i. \end{aligned}$$

Daí, segue que, se $r \neq 0$, $\text{gr}(r) \leq n-1 < m \leq \text{gr}(g)$.

... TERMINAR, USEI ISSO NUMA DEMONSTRAÇÃO MAIS A FRENTE,
TENHO QUE DEMONSTRAR. ■

Definição 9.37. Sejam \mathbf{A} um anel, $p = +_{i=0}^n p_i x^i \in A[x]$ e $a \in A$. O *valor* de p em a é o elemento

$$p(a) := \sum_{i=0}^n p_i a^i \in A.$$

Definição 9.38. Sejam \mathbf{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 9.60. Sejam \mathbf{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 . ■

...

9.4 Corpos

9.4.1 Extensões de Corpos

Definição 9.39. Seja \mathbf{C} um corpo. Uma *extensão* de \mathbf{C} é um corpo \mathbf{E} tal que \mathbf{C} é um subcorpo de \mathbf{E} .

Proposição 9.61. Sejam \mathbf{C} um corpo e $\mathbf{E} = (E, +, \cdot)$ uma extensão de \mathbf{C} . Então (E, \oplus, \odot) é um espaço vetorial sobre \mathbf{C} , em que $\oplus := +$ e $\odot := \cdot|_{C \times E}$.

Demonstração. Como \mathbf{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 $e \in E$, $(c_1 + c_2) \odot e = (c_1 + c_2)e = c_1 e + c_2 e = c_1 \odot e \oplus c_2 \odot e$. Por tanto, concluímos que (E, \oplus, \odot) é um espaço vetorial sobre \mathbf{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 vetorial.

Definição 9.40. Sejam \mathbf{C} um corpo e \mathbf{E} uma extensão de \mathbf{C} . Então a *dimensão* da extensão \mathbf{E} com respeito a \mathbf{C} é a dimensão do espaço vetorial \mathbf{E} sobre \mathbf{C} . A extensão \mathbf{E} é *finita* de sua dimensão é finita e *infinita* se sua dimensão é infinita.

Definição 9.41. Sejam \mathbf{C} um corpo e \mathbf{E} uma extensão de \mathbf{C} . Um *elemento algébrico* sobre \mathbf{C} é um elemento $\alpha \in E$ que é raiz de um polinômio em $C[x]^*$.

Proposição 9.62. *Sejam \mathbf{C} um corpo e \mathbf{E} uma extensão de \mathbf{C} . Então*

1. *Todo elemento de C é algébrico sobre \mathbf{C} ;*
2. *Se $\alpha \in E \setminus \{0\}$ é um elemento algébrico sobre \mathbf{C} , então existem $c_0, \dots, c_n \in C$ tais que $c_0 \neq 0$ e*

$$\sum_{i=0}^n c_i \alpha^i = 0.$$

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 \mathbf{C} e $c'_0, \dots, c'_m \in C$ tais que

$$\sum_{i=0}^m c'_i \alpha^i = 0.$$

Como c'_0, \dots, c'_m não são todos nulos, seja $k := \min\{i \in \{0, \dots, m\} : c'_i \neq 0\}$. Então, para todo $i < k$, $c'_i = 0$, e segue que

$$0 = \sum_{i=0}^m c'_i \alpha^i = \sum_{i=k}^m c'_i \alpha^i = \alpha^k \sum_{i=k}^m c'_i \alpha^{i-k}$$

e, como E é corpo e $\alpha \neq 0$, podemos dividir por α^k em ambos lados e temos

$$\sum_{i=k}^m c'_i \alpha^{i-k} = 0.$$

Fazendo, $n := m - k$ e, para todo $i \in \{0, \dots, n\}$, $c_i := c'_{k+i}$, temos que $c_0, \dots, c_n \in E$ — com $c_0 = c'_k \neq 0$ e, portanto, não todos nulos — tais que

$$\sum_{i=0}^n c_i \alpha^i = \sum_{i=0}^n c'_{k+i} \alpha^i = \sum_{i=k}^m c'_i \alpha^{i-k} = 0.$$

■

Definição 9.42. Sejam \mathbf{C} um corpo, \mathbf{E} uma extensão de \mathbf{C} e $\alpha \in E$ um elemento algébrico sobre \mathbf{C} . Um *polinômio minimal* de α sobre \mathbf{C} é um polinômio $p \in C[x]$ que satisfaz

1. $p(\alpha) = 0$;
2. p é mônico;
3. $\text{gr}(p) = \min\{\text{gr}(f) : f \in C[x]^*, f(\alpha) = 0 \text{ e } f \text{ é mônico}\}$.

Proposição 9.63. *Sejam \mathbf{C} um corpo, \mathbf{E} uma extensão de \mathbf{C} e $\alpha \in E$ um elemento algébrico sobre \mathbf{C} . Então existe um único polinômio minimal de α sobre \mathbf{C} .*

Demonstração. Pela definição de elemento algébrico, existe $p \in C[x]^*$ tal que $p'(\alpha) = 0$. Seja $n := \text{gr}(p')$ e $p'(x) = +_{i=0}^n a'_i x^i$. Como \mathbf{C} é corpo e $a'_n \neq 0$, existe $(a'_n)^{-1} \in C$. Definindo

$$p := (a'_n)^{-1} p = +_{i=0}^{n-1} (a'_n)^{-1} a_i x^i + x^n,$$

segue que $p \in C[x]^*$, $\text{gr}(p) = n$, $p(\alpha) = (a'_n)^{-1} p'(\alpha) = 0$ e p é mônico. Portanto $\{\text{gr}(f) : f \in C[x]^*, f(\alpha) = 0\}$ não é vazio, e, como é subconjunto de \mathbb{N} , admite mínimo, o que mostra que existe polinômio minimal de α sobre \mathbf{C} .

Para mostrar a unicidade, suponhamos que p_1 e p_2 são polinômios minimais de α sobre \mathbf{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, $\text{gr}(p_1) = \text{gr}(p_2)$. Seja $n := \text{gr}(p_1)$ e sejam $p_1 = +_{i=0}^n a_i x^i$ e $p_2 = +_{i=0}^n b_i x^i$. Pela segunda propriedade de polinômio minimal, $a_n = b_n = 1$. Então $a_n - b_n = 0$ e

$$(p_1 - p_2)(x) = +_{i=0}^{n-1} (a_i - b_i) x^i,$$

e conclui-se que $\text{gr}(p_1 - p_2) < n$. Se $p_1 \neq p_2$, existe $i \in \{0, \dots, n-1\}$ tal que $a_i \neq b_i$. Então seja $k := \max\{i \in \{0, \dots, n-1\} : a_i \neq b_i\}$. Assim, para todo $i > k$, $a_i = b_i$, o que implica $a_i - b_i = 0$, e temos que $\text{gr}(p_1 - p_2) = k$ e

$$(p_1 - p_2)(x) = +_{i=0}^k (a_i - b_i) x^i.$$

Como \mathbf{C} é corpo e $a_k - b_k \neq 0$, existe $(a_k - b_k)^{-1} \in C$. Definindo

$$p := (a_k - b_k)^{-1} (p_1 - p_2) = +_{i=0}^{k-1} (a_k - b_k)^{-1} (a_i - b_i) x^i + x^k,$$

segue que $p \in C[x]^*$, $\text{gr}(p) = k$, $p(\alpha) = (a_k - b_k)^{-1} (p_1 - p_2)(\alpha) = (a_k - b_k)^{-1} (p_1(\alpha) - p_2(\alpha)) = 0$ e p é mônico. Mas $\text{gr}(p) = k < n = \text{gr}(p_1) = \text{gr}(p_2)$, o que contradiz a minimalidade do grau de p_1 e p_2 . Portanto $p_1 = p_2$ e está provada a unicidade. ■

Proposição 9.64. *Seja \mathbf{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 $n := \text{gr}(p_1)$, $p_1 = +_{i=0}^n a_i x^i$, e $m := \text{gr}(p_2)$, $p_2 = +_{i=0}^m b_i x^i$. Pela definição de produto, sabemos que $a_n b_m = 1$, pois p é mônico. Como C é um corpo, existem $(a_n)^{-1}, (b_m)^{-1} \in C$. Definindo

$$p_1 := (a_n)^{-1} p'_1 = \sum_{i=0}^{n-1} (a_n)^{-1} a_i x^i + x^n \quad \text{e} \quad p_2 := (b_m)^{-1} p'_2 = \sum_{i=0}^{m-1} (b_m)^{-1} b_i x^i + x^m,$$

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 9.65. *Sejam C um corpo, E uma extensão de C , $\alpha \in E$ um elemento algébrico sobre C e $p \in C[x]^*$ um polinômio mônico tal que $p(\alpha)$. Então p é o polinômio minimal de α sobre C se, e somente se, p é irreduzível em $C[x]$.*

Demonstração. Suponhamos que p é polinômio minimal de α sobre C . Se p não é irreduzível em $C[x]$, como p é mônico, então existem $p_1, p_2 \in C[x]^*$ mônicos tais que $0 < \text{gr}(p_i) < \text{gr}(p)$ para todo $i \in \{1, 2\}$. Como $p(\alpha) = p_1(\alpha)p_2(\alpha) = 0$ e 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 $\text{gr}(p_1) < \text{gr}(p)$, o que contradiz a minimalidade de p . No segundo caso, $p_2 \in C[x]^*$ é um polinômio mônico, $p_2(\alpha) = 0$ e $\text{gr}(p_2) < \text{gr}(p)$, o que também contradiz a minimalidade de p , e temos um absurdo. Portanto p é irreduzível em $C[x]$.

Reciprocamente, suponhamos que p é irreduzível em $C[x]$. Por hipótese, $p(\alpha) = 0$ e p é mônico. Seja $p_\alpha \in C[x]^*$ o polinômio minimal de α sobre C . Então $\text{gr}(p_\alpha) \leq \text{gr}(p)$. Como p_α é mônico, existe $q, r \in C[x]$ tais que $p = qp_\alpha + r$. Como $p(\alpha) = p_\alpha(\alpha) = 0$, então $r(\alpha) = p(\alpha) - q(\alpha)p_\alpha(\alpha) = 0$. Se $r \neq 0$, então $\text{gr}(r) < \text{gr}(p_\alpha)$. Seja $n := \text{gr}(r)$. Como $r(\alpha) = 0$, segue que $\text{gr}(r) > 0$. Então seja $r(x) = +_{i=0}^n a_i x^i$. Como C é corpo, existe $(a_n)^{-1} \in C$. Assim, definindo

$$p' := (a_n)^{-1} r = \sum_{i=0}^{n-1} (a_n)^{-1} a_i x^i + x^n,$$

e segue que $p' \in C[x]^*$, $p'(\alpha) = (a_n)^{-1} p'(\alpha) = 0$ e p' é mônico. Mas $\text{gr}(p') = n = \text{gr}(r) < \text{gr}(p_\alpha)$, o que contradiz a minimalidade do grau de p_α . Então $r \neq 0$. Se $r = 0$, então $p = qp_\alpha$. Mas p é irreduzível, 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, $p = p_\alpha$. ■

9.4.2 Extras

Teorema 9.66. Seja $k \subseteq K$ uma extensão de corpos, \bar{k} fecho algébrico de k . Então as seguintes condições são equivalentes:

1. DIAGRAMA COMUTATIVO

$$\begin{array}{ccc} k & \xrightarrow{\cdot} & \bar{k} \\ \downarrow & \nearrow \sigma & \\ K & & \end{array}$$

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 9.43. Uma extensão de corpos $k \subseteq K$ é uma *extensão normal* se ela satisfaz uma das três condições do teorema acima.

OBS: Se $k \subseteq \bar{k}$ é uma extensão algébrica, então todo $\beta \in \bar{k}$ é algébrico sobre k vale para $\beta \in K$, então $k \subseteq K$ é extensão algébrica.

Se $k \subseteq K$ é extensão algébrica, então $k \subseteq K \subseteq \bar{K}$ são extensões algébricas, então $k \subseteq \bar{K}$ é extensão algébrica. Então $\bar{k} \sim \bar{K}$ é fecho algébrico de k .

(?????)

Proposição 9.67. Seja $k \subseteq K$ um extensão algébrica e $\sigma : K \rightarrow K$ um homomorfismo de corpos que satisfaça $\sigma|_k = id|_k$. Então σ é um isomorfismo de corpos.

Demonstração. ... ■

Definição 9.44. Seja $E \subseteq F$ uma extensão algébrica e $\sigma : E \rightarrow L$ um homomorfismo de corpos tal que L é algebraicamente fechado, $\sigma(E) \subseteq L$ é uma extensão algébrica (L é fecho algébrico de $\sigma(E)$)

$$S_\sigma := \{\mu : \mu : F \rightarrow L \text{ homomorfismo de corpos}, \mu|_E = \sigma\}.$$

Lema 9.68. $|S_\sigma|$ depende de $E \subseteq F$, mas não depende de σ nem de L .

Demonstração. ... vários diagramas ■

Definição 9.45. Seja $E \subseteq F$ uma extensão algébrica. O *grau de separabilidade* da extensão é $[F : E]_S := |S_\sigma|$. (Pode escolher $l = \overline{E}$ e σ inclusão.)

Teorema 9.69. 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 9.46. Seja $E \subseteq K$ uma extensão finita. Ela é *separável* se $[K : E]_S = [K : E]$.

Corolário 9.70. Sejam $E \subseteq F \subseteq K$ extensões de corpos, $[K : E] < \infty$, $E \subseteq K$ separável. Então $E \subseteq F$ e $F \subsetneq K$ 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. ■

9.5 Matrizes

Definição 9.47. Seja A um anel e $l, c \in \mathbb{N}$. Uma *matriz* de dimensão $l \times c$ sobre A é uma função $M : [l] \times [c] \rightarrow A$. 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 $m_{i,j} := M(i, j) \in A$. O conjunto $[l]$ é o conjunto dos *índices das linhas* e $[c]$ 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 A é denotado por $\mathbb{M}_{l \times c}(A)$.

Definição 9.48. Seja A um anel e $d \in \mathbb{N}$. Uma *matriz quadrada* de dimensão d sobre A é uma matriz $M \in \mathbb{M}_{d \times d}(A)$. O conjunto de todas as matrizes quadradas de dimensão d sobre A é denotado por $\mathbb{M}_d(A)$.

Definição 9.49. Sejam A um anel e $M \in \mathbb{M}_{l \times c}(A)$. A *matriz transposta* de M é a matriz $M^\top \in \mathbb{M}_{c \times l}(A)$ definida por

$$(M^\top)(i, j) := m_{j,i}.$$

9.5.1 Soma de Matrizes

Definição 9.50. Sejam \mathbf{A} um anel e $M, N \in \mathbb{M}_{l \times c}(\mathbf{A})$. A *matriz soma* das matrizes M e N é a matriz $(M + N) \in \mathbb{M}_{l \times c}(\mathbf{A})$ definida por

$$(M + N)(i, j) := m_{i,j} + n_{i,j}.$$

Definição 9.51. Sejam \mathbf{A} um anel e 0 o elemento neutro da soma de \mathbf{A} .

1. A *matriz nula* de dimensão $l \times c$ sobre \mathbf{A} é a matriz $\mathbb{O}_{l \times c} \in \mathbb{M}_{l \times c}(\mathbf{A})$, definida por

$$\mathbb{O}_{l \times c}(i, j) := 0.$$

2. Se $M \in \mathbb{M}_{l \times c}$, a *matriz negativa* de M é a matriz $-M \in \mathbb{M}_{l \times c}(\mathbf{A})$, definida por

$$(-M)(i, j) := -m_{i,j}.$$

Proposição 9.71. Seja \mathbf{A} um anel e $+$ a operação binária em $\mathbb{M}_{l \times c}(\mathbf{A})$ definida por

$$\begin{aligned} +: \mathbb{M}_{l \times c}(\mathbf{A}) \times \mathbb{M}_{l \times c}(\mathbf{A}) &\longrightarrow \mathbb{M}_{l \times c}(\mathbf{A}) \\ (M, N) &\longmapsto M + N. \end{aligned}$$

Então $(\mathbb{M}_{l \times c}(\mathbf{A}), +)$ é um grupo com elemento neutro $\mathbb{O}_{l \times c}$. Se \mathbf{A} é comutativo, então $(\mathbb{M}_{l \times c}(\mathbf{A}), +)$ é comutativo.

Demonstração. Sejam $M, N, P \in \mathbb{M}_{l \times c}(\mathbf{A})$. 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 $(\mathbb{M}_{l \times c}(\mathbf{A}), +)$ é um anel. Por fim, notemos que, se \mathbf{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 \mathbf{A} é comutativo, então $(\mathbb{M}_{l \times c}(\mathbf{A}), +)$ é comutativo. ■

9.5.2 Produto de Matrizes e Produto Por Escalar

Definição 9.52. Sejam \mathbf{A} um anel e $M \in \mathbb{M}_{l \times d}(\mathbf{A})$ e $N \in \mathbb{M}_{d \times c}(\mathbf{A})$. A *matriz produto* das matrizes M e N é a matriz $(MN) \in \mathbb{M}_{l \times c}(\mathbf{A})$ definida por

$$(MN)(i, j) := \sum_{k=1}^d m_{i,k} n_{k,j}.$$

Proposição 9.72. Sejam \mathbf{A} um anel e $M \in \mathbb{M}_{l \times d_1}(\mathbf{A})$, $N \in \mathbb{M}_{d_1 \times d_2}(\mathbf{A})$ e $P \in \mathbb{M}_{d_2 \times c}(\mathbf{A})$. Então

$$(MN)P = M(NP).$$

Demonstração. Um elemento de MN é dado por

$$(mn)_{i,j} = \sum_{k_1=1}^{d_1} m_{i,k_1} n_{k_1,j}.$$

Logo, um elemento de $(MN)P$ é dado por

$$((mn)p)_{i,j} = \sum_{k_2=1}^{d_2} (mn)_{i,k_2} p_{k_2,j} = \sum_{k_2=1}^{d_2} \left(\sum_{k_1=1}^{d_1} m_{i,k_1} n_{k_1,k_2} \right) p_{k_2,j}.$$

Analogamente, um elemento de $M(NP)$ é dado por

$$(m(np))_{i,j} = \sum_{k_1=1}^{d_1} m_{i,k_1} (np)_{k_1,j} = \sum_{k_1=1}^{d_1} m_{i,k_1} \left(\sum_{k_2=1}^{d_2} n_{k_1,k_2} p_{k_2,j} \right).$$

Mas então, como \mathbf{A} é um anel, segue que

$$\begin{aligned} ((mn)p)_{i,j} &= \sum_{k_2=1}^{d_2} \left(\sum_{k_1=1}^{d_1} m_{i,k_1} n_{k_1,k_2} \right) p_{k_2,j} \\ &= \sum_{k_2=1}^{d_2} \left(\sum_{k_1=1}^{d_1} m_{i,k_1} n_{k_1,k_2} p_{k_2,j} \right) \\ &= \sum_{k_1=1}^{d_1} \left(\sum_{k_2=1}^{d_2} m_{i,k_1} n_{k_1,k_2} p_{k_2,j} \right) \\ &= \sum_{k_1=1}^{d_1} m_{i,k_1} \left(\sum_{k_2=1}^{d_2} n_{k_1,k_2} p_{k_2,j} \right) \\ &= (m(np))_{i,j}. \end{aligned}$$

■

Definição 9.53. Sejam \mathbf{A} um anel e 0 e 1 os elementos neutros da soma e da multiplicação de \mathbf{A} respectivamente. A *matriz identidade* de dimensão d sobre \mathbf{A} é a matriz $\mathbf{I}_d \in \mathbb{M}_d(\mathbf{A})$ definida por

$$\mathbf{I}_d(i, j) := \delta_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j, \end{cases}$$

Essa função δ é conhecida como delta de Kronecker.

Proposição 9.73. Seja \mathbf{A} um anel e \cdot a operação binária em $\mathbb{M}_d(\mathbf{A})$ definida por

$$\begin{aligned} \cdot : \mathbb{M}_d(\mathbf{A}) \times \mathbb{M}_d(\mathbf{A}) &\longrightarrow \mathbb{M}_d(\mathbf{A}) \\ (M, N) &\longmapsto MN. \end{aligned}$$

Então $(\mathbb{M}_d(\mathbf{A}), \cdot)$ é um monoide com elemento neutro \mathbf{I}_d .

Demonstração. Sejam $M, N, P \in \mathbb{M}_d(\mathbf{A})$. Pela proposição anterior, sabemos que vale $(MN)P = M(NP)$ e que, portanto, \cdot é associativa. Agora, notemos que um elemento de $M\mathbf{I}_d$ é da forma

$$\sum_{k=0}^{d-1} m_{i,k} \delta_{k,j}.$$

Mas, para $k \in [d]$, se $k \neq j$, então $\delta_{k,j} = 0$ e, se $k = j$, então $\delta_{k,j} = 1$ e, portanto, segue que

$$\sum_{k=1}^d m_{i,k} \delta_{k,j} = m_{i,j}.$$

Assim, concluímos que $M\mathbf{I}_d = M$. Analogamente, mostra-se que $\mathbf{I}_d M = M$, e concluímos que \mathbf{I}_d é elemento neutro de \cdot . Isso mostra que $(\mathbb{M}_d(\mathbf{A}), \cdot)$ é um monoide. \blacksquare

Definição 9.54. Seja \mathbf{A} um anel. Uma *matriz invertível* é uma matriz $M \in \mathbb{M}_d(\mathbf{A})$ que é invertível com respeito ao produto do monoide $(\mathbb{M}_d(\mathbf{A}), \cdot)$. A matriz inversa de M é denotada M^{-1} .

Definição 9.55. Seja \mathbf{A} um anel, $a \in A$ e $M \in \mathbb{M}_{l \times c}(\mathbf{A})$. O *produto por escalar* de a e M é a matriz $aM \in \mathbb{M}_{l \times c}$ definida por

$$(aM)(i, j) := am_{i,j}.$$

9.5.3 Matrizes Quadradas

Definição 9.56. Seja \mathbf{A} um anel.

- Uma *matriz triangular superior* é uma matriz quadrada $M \in \mathbb{M}_d(\mathbf{A})$ que satisfaça

$$\forall i, j \in [d] \quad i > j \Rightarrow m_{i,j} = 0.$$

- Uma *matriz triangular inferior* é uma matriz quadrada $M \in \mathbb{M}_d(\mathbf{A})$ sobre \mathbf{A} que satisfaça

$$\forall i, j \in [d] \quad i < j \Rightarrow m_{i,j} = 0.$$

- Uma *matriz triangular superior* é uma matriz quadrada $M \in \mathbb{M}_d(\mathbf{A})$ que satisfaça

$$\forall i, j \in [d] \quad i > j \Rightarrow m_{i,j} = 0.$$

- Uma *matriz triangular* é uma matriz quadrada $M \in \mathbb{M}_d(\mathbf{A})$ que é triangular superior ou triangular inferior.

- Uma *matriz diagonal* é uma matriz quadrada $M \in \mathbb{M}_d(\mathbf{A})$ que é triangular superior e triangular inferior; ou seja, que satisfaça

$$\forall i, j \in [d] \quad i \neq j \Rightarrow m_{i,j} = 0.$$

- Uma *matriz simétrica* é uma matriz quadrada $M \in \mathbb{M}_d(\mathbf{A})$ que é igual à sua transposta

$$M = M^\top.$$

- Uma *matriz antissimétrica* é uma matriz quadrada $M \in \mathbb{M}_d(\mathbf{A})$ que é igual à negativa da sua transposta

$$M = -M^\top.$$

- Uma *matriz ortogonal* é uma matriz quadrada $M \in \mathbb{M}_d(\mathbf{A})$ cuja transposta é igual à sua inversa

$$M^\top = M^{-1}.$$

9.5.4 Traço e Determinante

Definição 9.57. Sejam \mathbf{A} um anel e $M \in \mathbb{M}_d(\mathbf{A})$. O *traço* de M é o elemento $\text{tr}(M) \in A$ definido por

$$\text{tr}(M) := \sum_{i=1}^d m_{i,i}.$$

Proposição 9.74. *Sejam \mathbf{A} um anel, $a \in A$ e $M, N \in \mathbb{M}_d(\mathbf{A})$. Então*

1. $\text{tr}(M^\top) = \text{tr}(M)$;
2. $\text{tr}(MN) = \text{tr}(NM)$;
3. $\text{tr}(M + N) = \text{tr}(M) + \text{tr}(N)$;
4. $\text{tr}(aM) = a \text{tr}(M)$.

Demonstração.

1.

$$\text{tr}(M) = \sum_{i=1}^d m_{i,i} = \text{tr}(M^\top).$$

2.

$$\begin{aligned} \text{tr}(MN) &= \sum_{i=1}^d \left(\sum_{k=1}^d m_{i,k} n_{k,i} \right) \\ &= \sum_{i=1}^d \left(\sum_{k=1}^d n_{k,i} m_{i,k} \right) \\ &= \sum_{k=1}^d \left(\sum_{i=1}^d n_{k,i} m_{i,k} \right) \\ &= \text{tr}(NM). \end{aligned}$$

3.

$$\begin{aligned} \text{tr}(M + N) &= \sum_{i=1}^d (m_{i,i} + n_{i,i}) \\ &= \sum_{i=1}^d m_{i,i} + \sum_{i=1}^d n_{i,i} \\ &= \text{tr}(M) + \text{tr}(N). \end{aligned}$$

4.

$$\text{tr}(aM) = \sum_{i=1}^d am_{i,i} = a \sum_{i=1}^d m_{i,i} = a \text{tr}(M).$$

■

Capítulo 10

Espaços Lineares

10.1 Módulos

Definição 10.1. Seja $\mathbf{A} = (A, +, -, 0, \cdot, 1)$ um anel. Um *módulo (à esquerda)* sobre \mathbf{A} é um par (\mathbf{M}, \cdot) em que $\mathbf{M} = (M, +, -, \mathbf{0})$ é um grupo comutativo e $\cdot : \mathbf{A} \curvearrowright \mathbf{M}$ é uma ação de anel ($\cdot : \mathbf{A} \longrightarrow \text{End}(\mathbf{M})$ é um homomorfismo de anel); ou seja,

1. Para todo $a \in \mathbf{A}$, a função $a \cdot : \mathbf{M} \longrightarrow \mathbf{M}$ é um homomorfismo de grupo:

- (a) Para todos $m_0, m_1 \in M$,

$$a \cdot (m_0 + m_1) = a \cdot m_0 + a \cdot m_1.$$

2. $\cdot : A \times M \longrightarrow M$ é uma ação de anel:

- (a) Para todos $a_0, a_1 \in A$ e $m \in M$,

$$(a_0 + a_1) \cdot m = a_0 \cdot m + a_1 \cdot m;$$

- (b) Para todos $a_0, a_1 \in A$ e $m \in M$,

$$(a_0 \cdot a_1) \cdot m = a_0 \cdot (a_1 \cdot m);$$

- (c) Para todo $m \in M$,

$$1 \cdot m = m;$$

Os símbolos da operação \cdot de \mathbf{A} e da ação \cdot serão suprimidos (e parênteses desnecessários relacionados a elas também), e os símbolos das operações $+, -$ de \mathbf{A} e $+, -$ de \mathbf{M} não serão diferenciadas em notação, nem os das constantes $0 \in A$ e $\mathbf{0} \in M$.

Na definição usamos o fato de que $\text{End}(\mathbf{M})$ é um anel com as operações puxadas para o espaço de funções, a soma pontual sendo a soma do anel e a composição de função sendo o produto. De fato, se X é um conjunto e \mathbf{G} um grupo comutativo, o conjunto G^X de funções de X para G , com a soma pontual e a composição, é um anel, e basta mostrar que quando $X = G$, o conjunto $\text{End}(\mathbf{G})$ de endomorfismos de grupo de \mathbf{G} é um subanel de G^G .

Proposição 10.1. *Sejam X um conjunto e \mathbf{G} um grupo comutativo. Então*

$$(G^X, +, -, 0, \circ, \text{Id})$$

é um anel.

Demonstração. 1. $(G^X, +, -, 0)$ é um grupo comutativo.

(a) Para todos $f_0, f_1, f_2 \in G^X$ e $x \in X$,

$$\begin{aligned} ((f_0 + f_1) + f_2)(x) &= (f_0 + f_1)(x) + f_2(x) \\ &= (f_0(x) + f_1(x)) + f_2(x) \\ &= f_0(x) + (f_1(x) + f_2(x)) \\ &= f_0(x) + (f_1 + f_2)(x) \\ &= (f_0 + (f_1 + f_2))(x); \end{aligned}$$

(b) Para todos $f \in G^X$ e $x \in X$,

$$\begin{aligned} (0 + f)(x) &= 0(x) + f(x) \\ &= 0 + f(x) \\ &= f(x) \\ &= f(x) + 0 \\ &= f(x) + 0(x) \\ &= (f + 0)(x); \end{aligned}$$

(c) Para todos $f \in G^X$ e $x \in X$,

$$\begin{aligned} ((-f) + f)(x) &= (-f)(x) + f(x) \\ &= -f(x) + f(x) \\ &= 0 \\ &= f(x) + (-f(x)) \\ &= f(x) + (-f)(x) \\ &= (f + (-f))(x); \end{aligned}$$

(d) Para todos $f_0, f_1 \in G^X$ e $x \in X$,

$$(f_0 + f_1)(x) = f_0(x) + f_1(x) = f_1(x) + f_0(x) = (f_1 + f_0)(x).$$

2. (G^X, \circ, Id) é um monoide.

(a) Para todos $f_0, f_1, f_2 \in G^X$ e $x \in X$,

$$\begin{aligned} ((f_0 \circ f_1) \circ f_2)(x) &= (f_0 \circ f_1)(f_2(x)) \\ &= (f_0(f_1(f_2(x)))) \\ &= f_0((f_1 \circ f_2)(x)) \\ &= (f_0 \circ (f_1 \circ f_2))(x); \end{aligned}$$

(b) Para todos $f \in G^X$ e $x \in X$,

$$(\text{Id} \circ f)(x) = \text{Id}(f(x)) = f(x) = f(\text{Id}(x)) = (f \circ \text{Id})(x).$$

3. A composição \circ é distributiva à esquerda e à direita sobre a soma pontual $+$.

(a) Para todos $f, f_0, f_1 \in G^X$ e $x \in X$,

$$\begin{aligned} (f \circ (f_0 + f_1))(x) &= f((f_0 + f_1)(x)) \\ &= f(f_0(x) + f_1(x)) \\ &= f(f_0(x)) + f(f_1(x)) \\ &= (f \circ f_0)(x) + (f \circ f_1)(x); \end{aligned}$$

(b) Para todos $f_0, f_1, f \in G^X$ e $x \in X$,

$$\begin{aligned} ((f_0 + f_1) \circ f)(x) &= (f_0 + f_1)(f(x)) \\ &= f_0(f(x)) + f_1(f(x)) \\ &= (f_0 \circ f)(x) + (f_1 \circ f)(x). \end{aligned}$$

■

Proposição 10.2. *Seja \mathbf{G} um grupo comutativo. Então*

$$(\text{End}(G), +, -, 0, \circ, \text{Id})$$

é um anel.

Demonstração. Como $\text{End}(\mathbf{G}) \subseteq G^G$, basta mostrar que $\text{End}(\mathbf{G})$ é subanel de G^G .

1. $\text{End}(\mathbf{G})$ é subgrupo.

(a) Para todos $h_0, h_1 \in \text{End}(\mathbf{G})$ e $g_0, g_1 \in G$,

$$\begin{aligned}(h_0 + h_1)(g_0 + g_1) &= h_0(g_0 + g_1) + h_1(g_0 + g_1) \\&= h_0(g_0) + h_0(g_1) + h_1(g_0) + h_1(g_1) \\&= h_0(g_0) + h_1(g_0) + h_0(g_1) + h_1(g_1) \\&= (h_0 + h_1)(g_0) + (h_0 + h_1)(g_1);\end{aligned}$$

(b) Para todos $h \in \text{End}(\mathbf{G})$ e $g_0, g_1 \in G$,

$$\begin{aligned}(-h)(g_0 + g_1) &= -h(g_0 + g_1) \\&= -(h(g_0) + h(g_1)) \\&= -h(g_0) - h(g_1) \\&= (-h)(g_0) + (-h)(g_1).\end{aligned}$$

2. $\text{End}(\mathbf{G})$ é submonoide.

(a) Para todos $h_0, h_1 \in \text{End}(\mathbf{G})$ e $g_0, g_1 \in G$,

$$\begin{aligned}(h_0 \circ h_1)(g_0 + g_1) &= h_0(h_1(g_0 + g_1)) \\&= h_0(h_1(g_0) + h_1(g_1)) \\&= h_0(h_1(g_0)) + h_0(h_1(g_1)) \\&= (h_0 \circ h_1)(g_0) + h_0 \circ h_1)(g_1);\end{aligned}$$

(b) Para todos $g_0, g_1 \in G$,

$$\text{Id}(g_0 + g_1) = g_0 + g_1 = \text{Id}(g_0) + \text{Id}(g_1).$$

■

10.2 Espaço e Subespaço Lineares

Definição 10.2. Seja $\mathbf{C} = (C, +, -, 0, \cdot, 1)$ um corpo. Um *espaço linear* sobre \mathbf{C} é um módulo (\mathbf{V}, \cdot) sobre \mathbf{C} ; ou seja,

1. Para todo $c \in C$, a função $c \cdot: \mathbf{V} \rightarrow \mathbf{V}$ é um homomorfismo de grupo:

(a) Para todos $v_0, v_1 \in M$,

$$c \cdot (v_0 + v_1) = c \cdot v_0 + c \cdot v_1.$$

2. $\cdot : C \times V \longrightarrow V$ é uma ação de corpo (ou de anel):

(a) Para todos $c_0, c_1 \in C$ e $v \in V$,

$$(c_0 + c_1) \cdot v = c_0 \cdot v + c_1 \cdot v;$$

(b) Para todos $c_0, c_1 \in C$ e $v \in V$,

$$(c_0 \cdot c_1) \cdot v = c_0 \cdot (c_1 \cdot v);$$

(c) Para todo $v \in V$,

$$1 \cdot v = v;$$

Os símbolos da operação \cdot de C e da ação \cdot serão suprimidos (e parênteses desnecessários relacionados a elas também), e os símbolos das operações $+, -$ de C e $+, -$ de V não serão diferenciadas em notação. Um espaço linear será denotado como V quando não for relevante explicitar a ação \cdot .

Proposição 10.3. *Seja V um espaço linear sobre um corpo C . Para todos $v \in V$ e $c \in C$,*

$$1. cv = \mathbf{0} \Leftrightarrow c = 0 \text{ ou } v = \mathbf{0};$$

$$2. -(cv) = (-c)v = c(-v);$$

$$3. cv = (-c)(-v).$$

Demonstração. Sejam $v \in V$ e $c \in C$.

1. Primeiro, notemos que

$$\begin{aligned} 0v &= 0v + \mathbf{0} \\ &= 0v + (0v - 0v) \\ &= (0v + 0v) - 0v \\ &= (0 + 0)v - 0v \\ &= 0v - 0v \\ &= \mathbf{0}. \end{aligned}$$

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 $\mathbf{v} = \mathbf{0}$, então $c\mathbf{v} = \mathbf{0}$. Agora, suponhamos que $c\mathbf{v} = \mathbf{0}$. Se $c \neq 0$, como \mathbf{C} é corpo, segue da demonstração anterior que

$$\mathbf{v} = c^{-1}c\mathbf{v} = c^{-1}\mathbf{0} = \mathbf{0}.$$

2. Basta notar que

$$\begin{aligned} -(c\mathbf{v}) &= -(c\mathbf{v}) + \mathbf{0} \\ &= -(c\mathbf{v}) + (0\mathbf{v}) \\ &= -(c\mathbf{v}) + (c - c)\mathbf{v} \\ &= -(c\mathbf{v}) + (c\mathbf{v} + (-c)\mathbf{v}) \\ &= (-(c\mathbf{v}) + c\mathbf{v}) + (-c)\mathbf{v} \\ &= \mathbf{0} + (-c)\mathbf{v} \\ &= (-c)\mathbf{v} \end{aligned}$$

e que

$$\begin{aligned} -(c\mathbf{v}) &= -(c\mathbf{v}) + \mathbf{0} \\ &= -(c\mathbf{v}) + (c\mathbf{0}) \\ &= -(c\mathbf{v}) + c(\mathbf{v} - \mathbf{v}) \\ &= -(c\mathbf{v}) + (c\mathbf{v} + c(-\mathbf{v})) \\ &= (-(c\mathbf{v} + c\mathbf{v}) + c(-\mathbf{v})) \\ &= \mathbf{0} + c(-\mathbf{v}) \\ &= c(-\mathbf{v}). \end{aligned}$$

3. Do item anterior, segue que

$$c\mathbf{v} = (-(-c))\mathbf{v} = (-c)(-\mathbf{v}). \quad \blacksquare$$

Proposição 10.4. *Seja \mathbf{C} um corpo e n um natural positivo. Então $(C^n, +, \cdot)$, em que*

$$\begin{aligned} \cdot : C \times C^n &\longrightarrow C^n \\ (c, (c_1, \dots, c_n)) &\longmapsto (c \cdot c_1, \dots, c \cdot c_n), \end{aligned}$$

é um espaço vetorial sobre \mathbf{C} .

Demonstração. Claramente $(C^n, +)$ é um grupo comutativo com elemento neutro $(0, \dots, 0)$. Note que, para todos $(c_1, \dots, c_n) \in C^n$ e $c, c' \in C$,

$$1 \cdot (c_1, \dots, c_n) = (1 \cdot c_1, \dots, 1 \cdot c_n) = (c_1, \dots, c_n)$$

e

$$\begin{aligned}
 (c \cdot c') \cdot (c_1, \dots, c_n) &= ((c \cdot c') \cdot c_1, \dots, (c \cdot c') \cdot c_n) \\
 &= ((c \cdot (c' \cdot c_1), \dots, (c \cdot (c' \cdot c_n))) \\
 &= c \cdot (c' \cdot c_1, \dots, c' \cdot c_n) \\
 &= c \cdot (c' \cdot (c_1, \dots, c_n)).
 \end{aligned}$$

Ainda, note que, para todos $(c_1, \dots, c_n), (c'_1, \dots, c'_n) \in C^n$ e $c, c' \in C$,

$$\begin{aligned}
 c \cdot ((c_1, \dots, c_n) + (c'_1, \dots, c'_n)) &= c \cdot (c_1 + c'_1, \dots, c_n + c'_n) \\
 &= (c \cdot (c_1 + c'_1), \dots, c \cdot (c_n + c'_n)) \\
 &= (c \cdot c_1 + c \cdot c'_1, \dots, c \cdot c_n + c \cdot c'_n) \\
 &= (c \cdot c_1, \dots, c \cdot c_n) + (c \cdot c'_1, \dots, c \cdot c'_n) \\
 &= c \cdot (c_1, \dots, c_n) + c \cdot (c'_1, \dots, c'_n)
 \end{aligned}$$

e

$$\begin{aligned}
 (c + c') \cdot (c_1, \dots, c_n) &= ((c + c')c_1, \dots, (c + c')c_n) \\
 &= (c \cdot c_1 + c' \cdot c_1, \dots, c \cdot c_n + c' \cdot c_n)_{i \in I} \\
 &= (c \cdot c_1, \dots, c \cdot c_n) + (c' \cdot c_1, \dots, c' \cdot c_n) \\
 &= c \cdot (c_1, \dots, c_n) + c' \cdot (c_1, \dots, c_n).
 \end{aligned}$$

■

Para generalizar esse resultado, lembremos que o produto de uma família $(C_i)_{i \in I}$ de conjuntos é $\prod_{i \in I} C_i$ e, quando $C_i = C$, temos que $\prod_{i \in I} C_i = C^I$ e os elementos de C^I são funções $c = (c_i)_{i \in I}$ de I em C .

Proposição 10.5. *Sejam X um conjunto e \mathbf{C} um corpo. Então $\mathbf{C}^I = (C^I, +, \cdot)$, em que*

$$\begin{aligned}
 +: C^I &\longrightarrow C^I \\
 (\mathbf{c}, \mathbf{c}') &\longmapsto (c_i + c'_i)_{i \in I}
 \end{aligned}$$

e

$$\begin{aligned}
 \cdot: C \times C^I &\longrightarrow C^I \\
 (a, \mathbf{c}) &\longmapsto (a \cdot c_i)_{i \in I}
 \end{aligned}$$

é um espaço vetorial sobre \mathbf{C} .

Proposição 10.6 (Espaço de Funções). *Sejam \mathbf{V} e \mathbf{W} espaços vetoriais sobre um corpo \mathbf{C} . Então $\mathbf{W}^{\mathbf{V}} = (W^V, +, \cdot)$, em que*

$$\begin{aligned}
 +: W^V \times W^V &\longrightarrow W^V \\
 (\mathbf{f}_1, \mathbf{f}_2) &\longmapsto \mathbf{f}_1 + \mathbf{f}_2: V \longrightarrow W \\
 \mathbf{v} &\longmapsto \mathbf{f}_1(\mathbf{v}) + \mathbf{f}_2(\mathbf{v}).
 \end{aligned}$$

e

$$\begin{aligned}\cdot : C \times W^V &\longrightarrow W^V \\ (c, \mathbf{f}) &\longmapsto c\mathbf{f} : V \longrightarrow W \\ \mathbf{v} &\longmapsto c\mathbf{f}(\mathbf{v}),\end{aligned}$$

é um espaço vetorial sobre \mathbf{C} .

Demonstração. Primeiro, sabemos que $(W^V, +)$ é um grupo comutativo com identidade $0 : W^V \times W^V \longrightarrow W^V$ definida por $0(\mathbf{v}) = 0$. Devemos então mostrar que $\cdot : C \times W^V \longrightarrow W^V$ satisfaz os itens da definição de espaço vetorial. Primeiro, seja $\mathbf{f} \in W^V$. Então, para todo $\mathbf{v} \in V$, $(1\mathbf{f})(\mathbf{v}) = 1\mathbf{f}(\mathbf{v}) = \mathbf{f}(\mathbf{v})$, o que mostra que $1\mathbf{f} = \mathbf{f}$. Agora, sejam $c_1, c_2 \in C$ e $\mathbf{f} \in W^V$. Então, para todo $\mathbf{v} \in V$,

$$((c_1 c_2)\mathbf{f})(\mathbf{v}) = (c_1 c_2)\mathbf{f}(\mathbf{v}) = c_1(c_2\mathbf{f}(\mathbf{v})) = c_1(c_2\mathbf{f})(\mathbf{v}) = (c_1(c_2\mathbf{f}))(\mathbf{v}),$$

o que mostra que $(c_1 c_2)\mathbf{f} = c_1(c_2\mathbf{f})$.

Por fim, devemos mostrar as propriedades distributivas. Sejam $c \in C$ e $\mathbf{f}_1, \mathbf{f}_2 \in W^V$. Então, para todo $\mathbf{v} \in V$,

$$\begin{aligned}(c(\mathbf{f}_1 + \mathbf{f}_2))(\mathbf{v}) &= c(\mathbf{f}_1 + \mathbf{f}_2)(\mathbf{v}) \\ &= c(\mathbf{f}_1(\mathbf{v}) + \mathbf{f}_2(\mathbf{v})) \\ &= c\mathbf{f}_1(\mathbf{v}) + c\mathbf{f}_2(\mathbf{v}) \\ &= (c\mathbf{f}_1)(\mathbf{v}) + (c\mathbf{f}_2)(\mathbf{v}) \\ &= (c\mathbf{f}_1 + c\mathbf{f}_2)(\mathbf{v}),\end{aligned}$$

o que mostra que $c(\mathbf{f}_1 + \mathbf{f}_2) = c\mathbf{f}_1 + c\mathbf{f}_2$. Agora, sejam $c_1, c_2 \in C$ e $\mathbf{f} \in W^V$. Então, para todo $\mathbf{v} \in V$,

$$\begin{aligned}((c_1 + c_2)\mathbf{f})(\mathbf{v}) &= (c_1 + c_2)\mathbf{f}(\mathbf{v}) \\ &= c_1\mathbf{f}(\mathbf{v}) + c_2\mathbf{f}(\mathbf{v}) \\ &= (c_1\mathbf{f})(\mathbf{v}) + (c_2\mathbf{f})(\mathbf{v}) \\ &= (c_1\mathbf{f} + c_2\mathbf{f})(\mathbf{v}),\end{aligned}$$

o que mostra que $(c_1 + c_2)\mathbf{f} = c_1\mathbf{f} + c_2\mathbf{f}$. Assim, concluímos que $(W^V, +, \cdot)$ é um espaço vetorial sobre \mathbf{C} . ■

Definição 10.3. Seja \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} . Um *subespaço vetorial* de \mathbf{V} é um conjunto não vazio $W \subseteq V$ tal que

1. $\forall \mathbf{w}_1, \mathbf{w}_2 \in W \quad \mathbf{w}_1 + \mathbf{w}_2 \in W;$
2. $\forall c \in C \ \forall \mathbf{w} \in W \quad c\mathbf{w} \in W.$

Proposição 10.7. Seja $\mathbf{V} = (V, +, \cdot)$ um espaço vetorial sobre um corpo \mathbf{C} . Então um conjunto não vazio $W \subseteq V$ é um subespaço vetorial de \mathbf{V} se, e somente se, $W = (W, +|_{W \times W}, \cdot|_{\mathbf{C} \times W})$ é um espaço vetorial sobre \mathbf{C} .

Proposição 10.8. Seja \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} e W um subespaço vetorial de \mathbf{V} . Então

1. $\mathbf{0} \in W$;
2. $\{\mathbf{0}\}$ e V são subespaços vetoriais de \mathbf{V} .

Demonstração. 1. Como W não é vazio, seja $\mathbf{w} \in W$. Então $0\mathbf{w} = \mathbf{0} \in W$.

2. Seja $W = \{\mathbf{0}\}$. Se $\mathbf{w}_1, \mathbf{w}_2 \in W$, $\mathbf{w}_1 = \mathbf{0}$ e $\mathbf{w}_2 = \mathbf{0}$, e segue que $\mathbf{w}_1 + \mathbf{w}_2 = \mathbf{0} + \mathbf{0} = \mathbf{0}$. Ainda, para todo $c \in \mathbf{C}$, segue que $c\mathbf{w}_1 = c\mathbf{0} = \mathbf{0} \in W$. Seja $W = V$. Como \mathbf{V} é espaço vetorial, então V é subespaço vetorial de \mathbf{V} pala proposição anterior. ■

Proposição 10.9. Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} e $(W_i)_{i \in I}$ uma família de subespaços vetoriais de \mathbf{V} . Então

$$W := \bigcap_{i \in I} W_i$$

é um subespaço vetorial de \mathbf{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 $\mathbf{w}_1, \mathbf{w}_2 \in W$ e $c \in \mathbf{C}$. Então, para todo $i \in I$, $\mathbf{w}_1, \mathbf{w}_2 \in W_i$ e, como W_i é subespaço vetorial de \mathbf{V} , segue que $\mathbf{w}_1 + \mathbf{w}_2 \in W_i$ e que $c\mathbf{w}_1 \in W_i$. Logo $\mathbf{w}_1 + \mathbf{w}_2 \in W$ e $c\mathbf{w}_1 \in W$, o que mostra que W é subespaço vetorial de \mathbf{V} . ■

Proposição 10.10. Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} e $\{W_i\}_{i \in I}$ uma cadeia de subespaços vetoriais de \mathbf{V} (ou seja, para todos $I, j \in I$, $W_I \subseteq W_j$ ou $W_j \subseteq W_i$). Então

$$W := \bigcup_{i \in I} W_i$$

é um subespaço vetorial de \mathbf{V} .

Demonstração. Como, para todo $i \in I$, $\mathbf{0} \in W_i$, pois W_i é subespaço vetorial de \mathbf{V} , segue que $\mathbf{0} \in W$ e, portanto, W não é vazio. Agora, sejam $\mathbf{w}_1, \mathbf{w}_2 \in W$. Então existem $i, j \in I$ tais que $\mathbf{w}_1 \in W_i$ e $\mathbf{w}_2 \in W_j$. Nesse caso, $W_i \subseteq W_j$ ou $W_j \subseteq W_i$. Sem perda de generalidade, suponhamos o primeiro caso. Então segue que $\mathbf{w}_1 \in W_j$ e, portanto, $\mathbf{w}_1 + \mathbf{w}_2 \in W_j$, o que mostra que $\mathbf{w}_1 + \mathbf{w}_2 \in W$. Agora, seja $c \in \mathbf{C}$ e notemos que, como W_i é subespaço vetorial de \mathbf{V} , segue que $c\mathbf{w}_1 \in W_i$. Logo $c\mathbf{w}_1 \in W$, o que mostra que W é subespaço vetorial de \mathbf{V} . ■

Definição 10.4. Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} , $W \subseteq V$ e $(W_i)_{i \in I}$ uma indexação do conjunto de todos subespaços vetoriais de \mathbf{V} dos quais W é subconjunto. O *subespaço vetorial gerado por W* em \mathbf{V} é o subespaço vetorial

$$\langle W \rangle := \bigcap_{i \in I} W_i.$$

Nesse caso, dizemos que W é um *conjunto gerador* de $\langle W \rangle$ ou que W gera $\langle W \rangle$.

Proposição 10.11. *Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{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 $\mathbf{v} \in \langle \emptyset \rangle$, então $\mathbf{v} \in \{\mathbf{0}\}$, o que implica $\mathbf{v} = \mathbf{0}$ e, portanto, que $\langle \emptyset \rangle = \{\mathbf{0}\}$. ■

10.3 Combinação Linear de Vetores

Definição 10.5. Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} e $W \subseteq V$ um conjunto finito tal que $W = \{\mathbf{w}_1, \dots, \mathbf{w}_n\}$. Uma *combinação linear* de W em \mathbf{V} é um vetor $\mathbf{v} \in V$ tal que existem $c_1, \dots, c_n \in C$ satisfazendo

$$\mathbf{v} = \sum_{i=1}^n c_i \mathbf{w}_i.$$

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 10.12. *Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} e $W \subseteq V$ não vazio. Então $\langle W \rangle$ é o conjunto de todas as combinações lineares de W em \mathbf{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 \mathbf{V} que contêm W . Primeiro, mostraremos que uma combinação linear de W em \mathbf{V} está em $\langle W \rangle$. Seja $\mathbf{v} := \sum_{i=1}^n c_i \mathbf{w}_i$ uma combinação linear de W em \mathbf{V} . Para todo $j \in J$, W_j é um subespaço vetorial de \mathbf{V} . Portanto, para todo $i \in [n]$, segue que $c_i \mathbf{w}_i \in W_j$ e, então, que $\mathbf{v} \in W_j$. Logo $\mathbf{v} \in \langle W \rangle$.

Reciprocamente, mostraremos que o conjunto de todas combinações lineares de W em \mathbf{V} é um subespaço vetorial de \mathbf{V} . Primeiro, notemos que $\mathbf{0}$ é uma combinação linear de W , pois, para todo $\mathbf{w} \in W$, vale $\mathbf{0} = 0\mathbf{w}$. Agora, sejam

$\mathbf{v}_1 = +_{i=1}^n c_i \mathbf{w}_i$ e $\mathbf{v}_2 = +_{i=1}^m c'_i \mathbf{w}'_i$ combinações lineares de W em \mathbf{V} e $c \in C$. Então, se definirmos, para todo $i \in [m]$, $\mathbf{w}_{n+i} := \mathbf{w}'_i$ e $c_{n+i} := c'_i$ e, para todo $i \in [n]$, $\bar{c}_i := cc_i$, segue que

$$\mathbf{v}_1 + \mathbf{v}_2 = \sum_{i=1}^n c_i \mathbf{w}_i + \sum_{i=1}^m c'_i \mathbf{w}'_i = \sum_{i=1}^{n+m} c_i \mathbf{w}_i$$

e

$$c\mathbf{v}_1 = \sum_{i=1}^n (cc_i) \mathbf{w}_i = \sum_{i=1}^n \bar{c}_i \mathbf{w}_i$$

são combinações lineares de W em \mathbf{V} , o que implica que o conjunto de todas combinações lineares de W em \mathbf{V} é um subespaço de \mathbf{V} . Assim, como $\langle W \rangle$ é subconjunto de todo conjunto que é subespaço vetorial de \mathbf{V} contendo W , segue que o conjunto de todas combinações lineares de W em \mathbf{V} é igual ao subespaço gerado por W . \blacksquare

Proposição 10.13. *Sejam \mathbf{V} um espaço vetorial sobre um corpo C , $W \subseteq V$ e $\mathbf{v} \in \langle W \rangle$. Então existem $\mathbf{w}_1, \dots, \mathbf{w}_n \in W$ distintos e $c_1, \dots, c_n \in C$ tais que*

$$\mathbf{v} = \sum_{i=1}^n c_i \mathbf{w}_i.$$

Demonstração. Como $\mathbf{v} \in \langle W \rangle$, existem $\mathbf{w}'_1, \dots, \mathbf{w}'_m \in W$ e $c'_1, \dots, c'_m \in C$ tais que $\mathbf{v} = +_{i=1}^m c'_i \mathbf{w}'_i$. Vamos partitionar o conjunto dos índices $[m]$ com a seguinte relação de equivalência: para todo $i, j \in [m]$, $i \sim j$ se, e somente se, $\mathbf{w}'_i = \mathbf{w}'_j$. Essa relação é de equivalência pois a igualdade de vetores é uma relação de equivalência. Agora, seja n o número de classes de equivalências dessa relação. Para cada $i \in [n]$, seja $j \in P_i$ e definimos os vetores $\mathbf{w}_i := \mathbf{w}'_j$. Notemos que os vetores \mathbf{w}_i estão bem definidos, não dependem do j , pois, se $k \in P_i$, então $\mathbf{w}_i = \mathbf{w}'_j = \mathbf{w}'_k$. Ainda, definimos os coeficientes $c_i := +_{j \in P_i} c'_j$. Desse modo, segue que

$$\mathbf{v} = \sum_{i=1}^m c'_i \mathbf{w}'_i = \sum_{i=1}^n \sum_{j \in P_i} c'_j \mathbf{w}'_j = \sum_{i=1}^n \sum_{j \in P_i} c'_j \mathbf{w}_i = \sum_{i=1}^n c_i \mathbf{w}_i.$$

Por fim, notemos que os $\mathbf{w}_1, \dots, \mathbf{w}_n$ são distintos por definição, já que, se $\mathbf{w}_i = \mathbf{w}_j$ para $i, j \in [n]$, então existem $k, l \in [m]$ tais que $k \in P_i$, $l \in P_j$ e $\mathbf{w}_i = \mathbf{w}'_k$, $\mathbf{w}_j = \mathbf{w}'_l$. Mas isso implica $\mathbf{w}'_k = \mathbf{w}'_l$, o que implica $P_i = P_j$ e, portanto, $i = j$. \blacksquare

Definição 10.6 (Dependência Linear). Sejam \mathbf{V} um espaço vetorial sobre um corpo C e $W \subseteq V$. Dizemos que W é *linearmente dependente* em \mathbf{V} se existem $\mathbf{w}_1, \dots, \mathbf{w}_n \in W$ distintos e $c_1, \dots, c_n \in C$ não nulos tais que

$$\mathbf{0} = \sum_{i=1}^n c_i \mathbf{w}_i.$$

Caso contrário, dizemos que W é *linearmente independente* em \mathbf{V} .

Proposição 10.14. *Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} e $W \subseteq V$. Então W é linearmente dependente se, e somente se, existe $\mathbf{w} \in W$ que é combinação linear de $W \setminus \{\mathbf{w}\}$ em \mathbf{V} .*

Demonstração. Suponhamos que W é linearmente dependente. Então existem vetores $\mathbf{w}'_1, \dots, \mathbf{w}'_n \in W$ distintos e $c'_1, \dots, c'_n \in C$ não nulos tais que

$$\mathbf{0} = \sum_{i=1}^n c'_i \mathbf{w}'_i.$$

Como c'_1, \dots, c'_n são não nulos, então existe $j \in [n]$ tal que $c'_j \neq 0$. Definindo $\mathbf{w}_i := \mathbf{w}'_i$ se $1 \leq i < j$ e $\mathbf{w}_i := \mathbf{w}'_{i-1}$ se $j < i \leq n$, e $c_i := (c'_j)^{-1}(-c'_i)$ para todo $1 \leq i < j$ ou $j < i \leq n$, segue que

$$\mathbf{w}'_j = \sum_{i=1}^{j-1} (c'_j)^{-1}(-c'_i) \mathbf{w}'_i + \sum_{i=j+1}^n (c'_j)^{-1}(-c'_i) \mathbf{w}'_i = \sum_{i=1}^{n-1} c_i \mathbf{w}_i.$$

Por tanto, como $\mathbf{w}_i \in W \setminus \{\mathbf{w}'_j\}$ e $c_i \in C$ para todo $i \in [n-1]$, \mathbf{w}'_j é combinação linear de $W \setminus \{\mathbf{w}'_j\}$ em \mathbf{V} .

Reciprocamente, suponhamos que existe $\mathbf{w} \in W$ que é combinação linear de $W \setminus \{\mathbf{w}\}$ em \mathbf{V} . Então existem $\mathbf{w}_1, \dots, \mathbf{w}_n \in W \setminus \{\mathbf{w}\}$ distintos e $c_1, \dots, c_n \in C$ tais que

$$\mathbf{w} = \sum_{i=1}^n c_i \mathbf{w}_i.$$

Definindo $\mathbf{w}_{n+1} := \mathbf{w}$ e $c_{n+1} := -1$, segue que

$$\mathbf{0} = \sum_{i=1}^n c_i \mathbf{w}_i - \mathbf{w} = \sum_{i=1}^{n+1} c_i \mathbf{w}_i.$$

Então, como $\mathbf{w}_1, \dots, \mathbf{w}_{n+1}$ são distintos e $c_{n+1} = -1 \neq 0$, segue que W é linearmente dependente. \blacksquare

Proposição 10.15. *Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} e $W \subseteq V$. Então*

1. \emptyset é linearmente independente em \mathbf{V} ;
2. Se $\mathbf{0} \in W$, então W é linearmente dependente em \mathbf{V} ;
3. Se $W = \{\mathbf{v}\} \neq \{\mathbf{0}\}$, então W é linearmente independente em \mathbf{V} .
4. Sejam $\mathbf{v}, \mathbf{v}' \neq 0$. $W = \{\mathbf{v}, \mathbf{v}'\}$ é linearmente dependente se, e somente se, existe $c \in C \setminus \{0\}$ tal que $\mathbf{v}' = c\mathbf{v}$.

Demonstração. 1. Suponha, por absurdo, que \emptyset não é linearmente independente. Então existem $\mathbf{w}_1, \dots, \mathbf{w}_n \in \emptyset$ distintos e $c_1, \dots, c_n \in C$ não nulos tais que

$$\mathbf{0} = \sum_{i=1}^n c_i \mathbf{w}_i.$$

Mas $\mathbf{w}_1, \dots, \mathbf{w}_n \in \emptyset$ é um absurdo.

2. Seja $c \in C \setminus \{0\}$. Então, como $\mathbf{0} = c\mathbf{0}$, segue que W é linearmente dependente em \mathbf{V} .
3. Se $\mathbf{0} = cv$, como $v \neq \mathbf{0}$, segue que $c = 0$, o que mostra que W é linearmente independente em \mathbf{V} .
4. Se W é linearmente dependente, então existem $c, c' \in C \setminus \{0\}$ tais que $0 = cv + c'v'$, o que implica que

$$v' = -\frac{c}{c'}v.$$

Reciprocamente, se existe $c \in C \setminus \{0\}$ tal que $v' = cv$, então

$$0 = -cv + cv = -cv + v',$$

o que mostra que W é linearmente dependente. ■

Proposição 10.16. *Sejam \mathbf{V} um espaço vetorial sobre um corpo C e $W \subseteq V$. Então W é linearmente independente em \mathbf{V} se, e somente se, para toda combinação linear $v = \sum_{i=1}^n c_i \mathbf{w}_i \neq \mathbf{0}$ de W em \mathbf{V} tal que $\mathbf{w}_1, \dots, \mathbf{w}_n$ são distintos e não nulos, então c_1, \dots, c_n são únicos.*

Demonstração. Primeiro, suponhamos que W é linearmente dependente em \mathbf{V} . Então existem $\mathbf{w}'_1, \dots, \mathbf{w}'_{n'} \in W$ distintos e $c'_1, \dots, c'_{n'} \in C$ não nulos tais que

$$\mathbf{0} = \sum_{i=1}^{n'} c'_i \mathbf{w}'_i.$$

Nesse caso, seja $v \in \langle W \rangle$. Se $v = \mathbf{0}$, então segue que

..... . Se $v \neq \mathbf{0}$ ■

Proposição 10.17. *Sejam \mathbf{V} um espaço vetorial sobre um corpo C e $\{W_i\}_{i \in I}$ uma cadeia de conjuntos linearmente independentes em \mathbf{V} (ou seja, para todos $i, j \in I$, $W_i \subseteq W_j$ ou $W_j \subseteq W_i$). Então*

$$W := \bigcup_{i \in I} W_i$$

é um conjunto linearmente independente em \mathbf{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 $\mathbf{w}_1, \mathbf{w}_2 \in W$. Então existem $i, j \in I$ tais que $\mathbf{w}_1 \in W_i$ e $\mathbf{w}_2 \in W_j$. Nesse caso, $W_i \subseteq W_j$ ou $W_j \subseteq W_i$. Sem perda de generalidade, suponhamos o primeiro caso. Então segue que $\mathbf{w}_1 \in W_j$ e, portanto, $\mathbf{w}_1 + \mathbf{w}_2 \in W_j$, o que mostra que $\mathbf{w}_1 + \mathbf{w}_2 \in W$. Agora, seja $c \in C$ e notemos que, como W_i é subespaço vetorial de \mathbf{V} , segue que $c\mathbf{w}_1 \in W_i$. Logo $c\mathbf{w}_1 \in W$, o que mostra que W é subespaço vetorial de \mathbf{V} . ■

10.4 Soma de Subespaços Vetoriais

Definição 10.7. Sejam \mathbf{V} um espaço vetorial sobre um corpo C e $(W_i)_{i \in I}$ uma família de subespaços vetoriais de \mathbf{V} . A *soma* de $(W_i)_{i \in I}$ é o subespaço vetorial gerado pela união de W_i . Denotamos

$$\bigoplus_{i \in I} W_i := \left\langle \bigcup_{i \in I} W_i \right\rangle.$$

Caso $(W_i)_{i \in I}$ seja uma família finita, escrevemos $W_1 + \cdots + W_n$.

Definição 10.8. Seja \mathbf{V} um espaço vetorial sobre um corpo C . Uma *soma direta* é a soma de uma família $(W_i)_{i \in I}$ de subespaços vetoriais de \mathbf{V} tal que $W_i \cap W_j = \{\mathbf{0}\}$ para todo $i, j \in I$, $i \neq j$. Nesse caso, denotamos

$$\bigoplus_{i \in I} W_i := \left\langle \bigcup_{i \in I} W_i \right\rangle.$$

Caso $(W_i)_{i \in I}$ seja uma família finita, escrevemos $W_1 \oplus \cdots \oplus W_n$.

Proposição 10.18. Seja \mathbf{V} um espaço vetorial sobre um corpo C e W_1, \dots, W_n subespaços vetoriais de \mathbf{V} tais que $V = \bigoplus_{i=1}^n W_i$. Então

$$V = \bigoplus_{i=1}^n W_i$$

se, e somente se, para todo $\mathbf{v} \in V$, existem únicos $\mathbf{w}_1 \in W_1, \dots, \mathbf{w}_n \in W_n$ tais que

$$\mathbf{v} = \bigoplus_{i=1}^n \mathbf{w}_i.$$

Demonstração. Mostraremos, primeiro, que se V é soma direta de W_1, \dots, W_n , então todo vetor de V é soma única de vetores de W_1, \dots, W_n . A demonstração será por indução em n . O caso base é trivial, pois, se $V = W_1$, então, para todo $\mathbf{v} \in V$,

$\mathbf{v} \in W_1$. Agora, suponhamos que a proposição vale para todo natural menor ou igual a n . Sejam W_1, \dots, W_{n+1} subespaços vetoriais de V tais que $V = +_{i=1}^{n+1} W_i$. Então existem $\mathbf{w}_1 \in W_1, \dots, \mathbf{w}_{n+1} \in W_{n+1}$ tais que

$$\mathbf{v} = \sum_{i=1}^{n+1} \mathbf{w}_i.$$

Suponhamos que existam $\mathbf{w}_1 \in W_1, \dots, \mathbf{w}_{n+1} \in W_{n+1}$ tais que

$$\mathbf{v} = \sum_{i=1}^{n+1} \mathbf{w}'_i.$$

Então

$$\mathbf{v} = \sum_{i=1}^{n+1} \mathbf{w}_i = \sum_{i=1}^{n+1} \mathbf{w}'_i,$$

o que implica

$$\sum_{i=1}^n (\mathbf{w}_i - \mathbf{w}'_i) = \mathbf{w}'_{n+1} - \mathbf{w}_{n+1}.$$

Como, para todo $i \in [n+1]$, $\mathbf{w}_i, \mathbf{w}'_i \in W_i$, segue que $\mathbf{w}_i - \mathbf{w}'_i \in W_i$. Definamos $W := \bigcup_{i=1}^n W_i$. Assim, segue que

$$\sum_{i=1}^n (\mathbf{w}_i - \mathbf{w}'_i) \in \langle W \rangle$$

e

$$\mathbf{w}'_{n+1} - \mathbf{w}_{n+1} \in W_{n+1}.$$

Ainda, como V é soma direta de W_1, \dots, W_{n+1} , então segue que $W \cap W_{n+1} = \{\mathbf{0}\}$. Portanto concluímos que

$$\sum_{i=1}^n (\mathbf{w}_i - \mathbf{w}'_i) = \mathbf{w}'_{n+1} - \mathbf{w}_{n+1} = \mathbf{0}.$$

Assim, concluímos que $\mathbf{w}'_{n+1} = \mathbf{w}_{n+1}$ e que

$$\sum_{i=1}^n \mathbf{w}_i = \sum_{i=1}^n \mathbf{w}'_i.$$

Mas notemos que

$$\langle W \rangle = (\langle W \rangle, +|_{\langle W \rangle \times \langle W \rangle}, \cdot|_{\langle W \rangle \times \langle W \rangle})$$

é um espaço vetorial e W_1, \dots, W_n são subespaços vetoriais de $\langle \mathbf{W} \rangle$ tais que $\langle W \rangle = \bigoplus_{i=1}^n W_i$. Portanto, pela hipótese de indução, segue que, para todo $i \in [n]$, $\mathbf{w}_i = \mathbf{w}'_i$ e, portanto, concluímos que existem únicos $\mathbf{w}_1 \in W_1, \dots, \mathbf{w}_{n+1} \in W_{n+1}$ tais que

$$\mathbf{v} = \bigoplus_{i=1}^{n+1} \mathbf{w}_i.$$

Suponhamos, então, que todo vetor de V é soma de únicos vetores de W_1, \dots, W_n . Sejam $i, j \in [n]$, $i \neq j$, e $\mathbf{v} \in W_i \cap W_j$. Como $\mathbf{v} \in V$, segue que existem únicos $\mathbf{w}_1 \in W_1, \dots, \mathbf{w}_n \in W_n$ tais que

$$\mathbf{v} = \bigoplus_{k=1}^n \mathbf{w}_k.$$

Sem perda de generalidade, suponhamos $i < j$. Notemos que

$$\mathbf{v} = \bigoplus_{i=1}^n \mathbf{w}_i = \bigoplus_{k=1}^{i-1} \mathbf{w}_k + (\mathbf{w}_i + \mathbf{v}) + \bigoplus_{k=i+1}^{j-1} \mathbf{w}_k + (\mathbf{w}_j - \mathbf{v}) + \bigoplus_{k=j+1}^n \mathbf{w}_k.$$

Como $\mathbf{v} \in W_i \cap W_j$, segue que $(\mathbf{w}_i + \mathbf{v}) \in W_i$ e $(\mathbf{w}_j - \mathbf{v}) \in W_j$ e, portanto, como $\mathbf{w}_1 \in W_1, \dots, \mathbf{w}_n \in W_n$ são únicos, segue que $(\mathbf{w}_i + \mathbf{v}) = \mathbf{w}_i$ e $(\mathbf{w}_j - \mathbf{v}) = \mathbf{w}_j$; ou seja, $\mathbf{v} = \mathbf{0}$. Logo V é soma direta de W_1, \dots, W_n . ■

10.5 Bases de Espaços Vetoriais

Definição 10.9. Seja \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} . Uma *base* de \mathbf{V} é um conjunto $B \subseteq V$ linearmente independente em \mathbf{V} que gera V ; ou seja, $V = \langle B \rangle$. Uma base de um subespaço vetorial W de \mathbf{V} é uma base do espaço vetorial $\mathbf{W} = (W, +|_{W \times W}, \cdot|_{W \times W})$.

Teorema 10.19. *Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} . Então existe base B de \mathbf{V} e, se L é um conjunto linearmente independente em \mathbf{V} , existe uma base B de \mathbf{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 \mathbf{V} que contém \emptyset . Demonstraremos a segunda afirmação.

Sejam L um conjunto linearmente independente em \mathbf{V} e P o conjunto dos subconjuntos $S \subseteq V$ tais que $L \subseteq S$ e S é linearmente independente em \mathbf{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 $S := \bigcup_{i \in I} S_i$. Como $L \subseteq S_i$ para todo $i \in I$, então $L \subseteq S$. Devemos mostrar que S é um conjunto linearmente independente em \mathbf{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 limite 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 \mathbf{V} . Devemos mostrar que B gera V , ou seja, que $V = \langle B \rangle$. Seja $\mathbf{v} \in V$ e suponhamos, por absurdo, que $\mathbf{v} \notin \langle B \rangle$. Então, em particular, $\mathbf{v} \notin B$; logo $B \subset B \cup \{\mathbf{v}\}$. Concluiremos que $B \cup \{\mathbf{v}\}$ é linearmente independente, o que contradiz a maximalidade de B . Seja S um subconjunto finito de $B \cup \{\mathbf{v}\}$. Se $\mathbf{v} \notin S$, então $S \subseteq B$ e, portanto, é linearmente independente, pois B o é; se $\mathbf{v} \in S$, sejam $\{\mathbf{v}_1, \dots, \mathbf{v}_n\} := S \setminus \{\mathbf{v}\} \subseteq B$ e $c, c_1, \dots, c_n \in C$ tais que

$$c_1 \mathbf{v}_1 + \cdots + c_n \mathbf{v}_n - c \mathbf{v} = \mathbf{0}.$$

Como $\mathbf{v} \notin \langle B \rangle$, então $c = 0$, pois, caso contrário, teríamos

$$\mathbf{v} = \frac{c_1}{c} \mathbf{v}_1 + \cdots + \frac{c_n}{c} \mathbf{v}_n.$$

Assim, segue que $c_1 \mathbf{v}_1 + \cdots + c_n \mathbf{v}_n = \mathbf{0}$. Mas $S \setminus \{\mathbf{v}\} \subseteq B$ 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 $B \cup \{\mathbf{v}\}$ é linearmente independente, pois todo subconjunto finito é, e isso contradiz a maximalidade de B . Por esse absurdo, segue que $\mathbf{v} \in \langle B \rangle$ e, portanto, que $V = \langle B \rangle$. Concluímos que B é uma base de \mathbf{V} que contém L . ■

Proposição 10.20. *Sejam \mathbf{V} um espaço vetorial sobre um corpo C e $W, W' \subseteq V$ conjuntos finitos. Se W é linearmente independente em \mathbf{V} e W' gera V , então $|W| \leq |W'|$.*

Demonstração. Se $W = \emptyset$, então $0 = |W'| \leq |W|$. Caso contrário, seja $|W| = n$ e $(\mathbf{w}_i)_{i \in [n]}$ 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 $(\mathbf{w}'_i)_{i \in [m]}$ uma indexação de W' . Queremos mostrar que $n \leq m$. Suponhamos, por absurdo, que $m < n$. Como W é linearmente independente, então, para todo $i \in [n]$, $\mathbf{w}_i \neq \mathbf{0}$. Como W' gera V , existem $c_1, \dots, c_m \in C$ tais que

$$\mathbf{w}_1 = \sum_{i=1}^m c_i \mathbf{w}'_i,$$

e os $c_1, \dots, c_m \in C$ não são todos nulos pois, caso contrário, teríamos $\mathbf{w}_1 = \mathbf{0}$. Assim, suponhamos, sem perda de generalidade, que $c_1 \neq 0$. Então

$$\mathbf{w}'_1 = c_1^{-1} \mathbf{w}_1 - \sum_{i=2}^m c_1^{-1} c_i \mathbf{w}'_i.$$

Seja $W_1 := \{\mathbf{w}_1, \mathbf{w}'_2, \dots, \mathbf{w}'_m\}$. 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 \mathbf{w}_2 como combinação linear de W_1 , como $\mathbf{w}_2 \neq \mathbf{0}$, segue que nem todos os coeficientes da combinação linear são nulos. Mais ainda, se somente o coeficiente de \mathbf{w}_1 é não nulo, então \mathbf{w}_2 é múltiplo de \mathbf{w}_1 , o que contradiz a independência linear de W . Portanto, deve existir um coeficiente dos $\mathbf{w}'_2, \dots, \mathbf{w}'_m$ não nulo. Assim, sem perda de generalidade, suponhamos que o coeficiente de \mathbf{w}'_2 é não nulo. Então, como no caso anterior, \mathbf{w}'_2 pode ser escrito como combinação linear de $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}'_3, \dots, \mathbf{w}'_m$ e segue que o conjunto $W_2 := \{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}'_3, \dots, \mathbf{w}'_m\}$ gera V . Repetindo o processo, que termina porque $m < n$ são finitos, achamos o conjunto $W_m := \{\mathbf{w}_1, \dots, \mathbf{w}_m\}$, que gera V e é um subconjunto próprio de W , pois $m < n$. Mas isso implica que $\mathbf{w}_{m+1} \in W$ é uma combinação linear de W_m em V , o que implica que W é linearmente dependente, uma contradição. Logo $m \leq n$. ■

Teorema 10.21. *Sejam V um espaço vetorial sobre um corpo C . Se $B, B' \subseteq V$ são bases de 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 $|B| = n$, $\{\mathbf{b}_1, \dots, \mathbf{b}_n\} := B$, e B' é um conjunto infinito. Seja $i \in [n]$. Como $\mathbf{b}_i \in V$ e B' gera V , segue que existem $\mathbf{b}_{i,1}, \dots, \mathbf{b}_{i,n_i} \in B'$ e $c_{i,1}, \dots, c_{i,n_i} \in C$ tais que

$$\mathbf{b}_i = \sum_{j=1}^{n_i} c_{i,j} \mathbf{b}_{i,j}.$$

Notemos que o conjunto de todos esses $\mathbf{b}_{i,j}$ é $B'' := \bigcup_{i=1}^n \{\mathbf{b}_{i,j} : j \in [n_i]\}$, que é um subconjunto finito de B' e, portanto, um subconjunto próprio. Assim, como $B'' \subset B'$, existe $\mathbf{b} \in B' \setminus B''$. Como $\mathbf{b} \in V$ e B é base, segue que existem $c_1, \dots, c_n \in C$ tais que $\mathbf{b} = \sum_{i=1}^n c_i \mathbf{b}_i$. Mas então

$$\mathbf{b} = \sum_{i=1}^n c_i \mathbf{b}_i = \sum_{i=1}^n c_i \sum_{j=1}^{n_i} c_{i,j} \mathbf{b}_{i,j} = \sum_{i=1}^n \sum_{j=1}^{n_i} c_i c_{i,j} \mathbf{b}_{i,j},$$

o que mostra que $\mathbf{b} \in B'$ pode ser escrito como uma combinação linear de $B' \setminus \{\mathbf{b}\}$ em 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 10.10. Sejam \mathbf{V} um espaço vetorial sobre um corpo \mathbf{C} e $B \subseteq V$ uma base \mathbf{V} . A *dimensão* de \mathbf{V} é o número ordinal $\dim \mathbf{V} := |B|$.

10.6 Funções Lineares

Definição 10.11. Sejam \mathbf{V} e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} . Uma função *linear* de \mathbf{V} para \mathbf{W} é uma função $L: V \rightarrow W$ que satisfaz

1. (Aditividade) Para todos $\mathbf{v}_1, \mathbf{v}_2 \in V$,

$$L(\mathbf{v}_1 + \mathbf{v}_2) = L(\mathbf{v}_1) + L(\mathbf{v}_2);$$

2. (Homogeneidade) Para todos $c \in C, \forall \mathbf{v} \in V$,

$$L(c\mathbf{v}) = cL(\mathbf{v}).$$

Denota-se $L: \mathbf{V} \rightarrow \mathbf{W}$. O conjunto das funções lineares de \mathbf{V} para \mathbf{W} é denotado $\mathcal{L}(\mathbf{V}, \mathbf{W})$ e o conjunto das funções lineares de \mathbf{V} para \mathbf{V} é denotado $\mathcal{L}(\mathbf{V})$.

É imediato da definição que as duas propriedades são equivalentes à seguinte propriedade

1. (Linearidade) Para todos $c_1, c_2 \in C$ e $\mathbf{v}_1, \mathbf{v}_2 \in V$,

$$L(c_1\mathbf{v}_1 + c_2\mathbf{v}_2) = c_1L(\mathbf{v}_1) + c_2L(\mathbf{v}_2).$$

Proposição 10.22. Sejam \mathbf{V} e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} e $L \in \mathcal{L}(\mathbf{V}, \mathbf{W})$. Então

1. (Linearidade generalizada) Para todos $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$ e $c_1, \dots, c_n \in C$,

$$L\left(\sum_{i=1}^n c_i \mathbf{v}_i\right) = \sum_{i=1}^n c_i L(\mathbf{v}_i).$$

2. $L(\mathbf{0}) = \mathbf{0}$;
3. $L(-\mathbf{v}) = -L(\mathbf{v})$.

Proposição 10.23. Sejam \mathbf{V} e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} . O espaço linear $\mathcal{L}(\mathbf{V}, \mathbf{W})$ é um subespaço linear de $\mathbf{W}^{\mathbf{V}}$.

Demonstração. Primeiro, sejam $L_1, L_2 \in \mathcal{L}(\mathbf{V}; \mathbf{W})$. Então, para todos $c \in C$ e $\mathbf{v}_1, \mathbf{v}_2 \in V$,

$$\begin{aligned} (L_1 + L_2)(\mathbf{v}_1 + c\mathbf{v}_2) &= L_1(\mathbf{v}_1 + c\mathbf{v}_2) + L_2(\mathbf{v}_1 + c\mathbf{v}_2) \\ &= L_1(\mathbf{v}_1) + cL_1(\mathbf{v}_2) + L_2(\mathbf{v}_1) + cL_2(\mathbf{v}_2) \\ &= L_1(\mathbf{v}_1) + L_2(\mathbf{v}_1) + cL_1(\mathbf{v}_2) + cL_2(\mathbf{v}_2) \\ &= (L_1 + L_2)(\mathbf{v}_1) + c(L_1 + L_2)(\mathbf{v}_2). \end{aligned}$$

Agora, sejam $c' \in C$ e $L \in \mathcal{L}(\mathbf{V}; \mathbf{W})$. Então

$$\begin{aligned} (c'L)(\mathbf{v}_1 + c\mathbf{v}_2) &= c'L(\mathbf{v}_1 + c\mathbf{v}_2) \\ &= c'(L(\mathbf{v}_1) + cL(\mathbf{v}_2)) \\ &= c'L(\mathbf{v}_1) + c'cL(\mathbf{v}_2) \\ &= (c'L)(\mathbf{v}_1) + c(c'L)(\mathbf{v}_2). \end{aligned}$$

Portanto concluímos que $\mathcal{L}(\mathbf{V}, \mathbf{W})$ é um subespaço linear de $\mathbf{W}^{\mathbf{V}}$. ■

Proposição 10.24. Sejam $\mathbf{V}_1, \mathbf{V}_2$ e \mathbf{V}_3 espaços lineares sobre um corpo \mathbf{C} . Se $L_1 \in \mathcal{L}(\mathbf{V}_1, \mathbf{V}_2)$, $L_2 \in \mathcal{L}(\mathbf{V}_2, \mathbf{V}_3)$, então $L_2 \circ L_1 \in \mathcal{L}(\mathbf{V}_1, \mathbf{V}_3)$.

Demonstração. Sejam $c \in C$ e $\mathbf{v}_1, \mathbf{v}_2 \in V$. Então

$$\begin{aligned} (L_2 \circ L_1)(\mathbf{v}_1 + c\mathbf{v}_2) &= L_2(L_1(\mathbf{v}_1 + c\mathbf{v}_2)) \\ &= L_2(L_1(\mathbf{v}_1) + cL_1(\mathbf{v}_2)) \\ &= L_2(L_1(\mathbf{v}_1)) + cL_2(L_1(\mathbf{v}_2)) \\ &= (L_2 \circ L_1)(\mathbf{v}_1) + c(L_2 \circ L_1)(\mathbf{v}_2), \end{aligned}$$

o que mostra que $L_2 \circ L_1$ é linear. ■

Proposição 10.25. Sejam \mathbf{V} e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} e $L \in \mathcal{L}(\mathbf{V}, \mathbf{W})$. Se L é invertível, então $L^{-1} \in \mathcal{L}(\mathbf{W}, \mathbf{V})$.

Demonstração. Seja $L \in \mathcal{L}(\mathbf{V}, \mathbf{W})$. Se L é invertível, $L^{-1} \in V^W$ e, para todos $c \in C$ e $\mathbf{w}_1, \mathbf{w}_2 \in W$, existem $\mathbf{v}_1, \mathbf{v}_2 \in V$ tais que $L(\mathbf{v}_1) = \mathbf{w}_1$ e $L(\mathbf{v}_2) = \mathbf{w}_2$ e

segue que

$$\begin{aligned} L^{-1}(\mathbf{w}_1 + c\mathbf{w}_2) &= L^{-1}(L(\mathbf{v}_1) + cL(\mathbf{v}_2)) \\ &= L^{-1}(L(\mathbf{v}_1 + c\mathbf{v}_2)) \\ &= \mathbf{v}_1 + c\mathbf{v}_2 \\ &= L^{-1}(\mathbf{w}_1) + cL^{-1}(\mathbf{w}_2), \end{aligned}$$

o que mostra que L^{-1} é linear. ■

Proposição 10.26. *Sejam \mathbf{V} e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} , $B_V = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ base de \mathbf{V} , $B_W = \{\mathbf{w}_1, \dots, \mathbf{w}_m\}$ base de \mathbf{W} e $L \in \mathcal{L}(\mathbf{V}, \mathbf{W})$. Então, para todo $\mathbf{v} \in V$, existem únicos $c_1, \dots, c_m \in C$ tais que*

$$L(\mathbf{v}) = \sum_{i=1}^m c_i \mathbf{w}_i.$$

Demonstração. Primeiro demonstraremos a existência. Sabemos que, como B_V é base de V , então existem únicos $a_1, \dots, a_n \in C$ tais que $\mathbf{v} = \sum_{i=1}^n a_i \mathbf{v}_i$. Mas, como L é linear, então

$$L(\mathbf{v}) = L\left(\sum_{i=1}^n a_i \mathbf{v}_i\right) = \sum_{i=1}^n a_i L(\mathbf{v}_i).$$

Agora, como B_W é base de \mathbf{W} , para cada $i \in \{1, \dots, n\}$ existem únicos

$$b_{i1}, \dots, b_{im} \in C$$

tais que $L(\mathbf{v}_i) = \sum_{j=1}^m b_{ij} \mathbf{w}_j$. Assim, definindo $c_j := \sum_{i=1}^n a_i b_{ij}$, segue que

$$L(\mathbf{v}) = \sum_{i=1}^n a_i \left(\sum_{j=1}^m b_{ij} \mathbf{w}_j \right) = \sum_{j=1}^m \left(\sum_{i=1}^n a_i b_{ij} \right) \mathbf{w}_j = \sum_{j=1}^m c_j \mathbf{w}_j.$$
■

10.7 Produto e Coproduto de Espaços Vetoriais

10.7.1 Produto

Definição 10.12. Seja $(\mathbf{V}_i)_{i \in I} = ((V_i, +_i, \cdot_i))_{i \in I}$ uma família de espaços vetoriais sobre um corpo \mathbf{C} . O *produto categórico* de $(\mathbf{V}_i)_{i \in I}$ é a tripla

$$\prod_{i \in I} \mathbf{V}_i = (V, +, \cdot),$$

em que $V = \prod_{i \in I} V_i$,

$$\begin{aligned} +: V \times V &\longrightarrow V \\ (v_1, v_2) &\longmapsto ((v_1)_i +_i (v_2)_i)_{i \in I} \end{aligned}$$

e

$$\begin{aligned} \cdot: C \times V &\longrightarrow V \\ (c, v) &\longmapsto (c \cdot_i v_i)_{i \in I}. \end{aligned}$$

Proposição 10.27. *Seja $(V_i)_{i \in I} = ((V_i, +_i, \cdot_i))_{i \in I}$ uma família de espaços vetoriais sobre um corpo C . Então $\prod_{i \in I} V_i = (V, +, \cdot)$ é um espaço vetorial sobre C .*

Demonstração. 1. $(V, +)$ é um grupo pois tem a mesma operação do produto de grupos (8.28).

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

$$\begin{aligned} (c_1 c_2)v &= ((c_1 c_2)v_i)_{i \in I} \\ &= (c_1(c_2 v_i))_{i \in I} \\ &= c_1(c_2 v_i)_{i \in I} \\ &= c_1(c_2 v). \end{aligned}$$

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 10.28. Seja $(\mathbf{V}_i)_{i \in I} = ((V_i, +_i, \cdot_i))_{i \in I}$ uma família de espaços vetoriais sobre um corpo \mathbf{C} . Para todo $i \in I$, a projeção canônica $\pi_i : \prod_{i \in I} \mathbf{V}_i \rightarrow \mathbf{V}_i$ é uma função linear.

Demonstração. Sejam $c \in C$ e $v, v' \in \prod_{i \in I} V_i$. Então

$$\pi_i(v + cv') = \pi_i((v_i + cv'_i)_{i \in I}) = v_i + cv'_i = \pi_i(v) + c\pi_i(v'). \quad \blacksquare$$

Proposição 10.29 (Propriedade Universal). Sejam $(\mathbf{V}_i)_{i \in I}$ uma família de espaços vetoriais sobre um corpo \mathbf{C} , \mathbf{X} um espaço vetorial sobre \mathbf{C} e, para todo $i \in I$, $L_i : \mathbf{X} \rightarrow \mathbf{V}_i$ uma função linear. Então existe única função linear $L : \mathbf{X} \rightarrow \prod_{i \in I} \mathbf{V}_i$ tal que, para todo $i \in I$, $\pi_i \circ L = L_i$ (o diagrama comuta).

$$\begin{array}{ccc} & \prod_{i \in I} \mathbf{V}_i & \\ L \swarrow & \nearrow \pi_i & \downarrow \\ \mathbf{X} & \xrightarrow[L_i]{\quad} & \mathbf{V}_i \end{array}$$

Demonstração. Defina a função

$$\begin{aligned} L : X &\longrightarrow \prod_{i \in I} V_i \\ x &\longmapsto (L_i(x))_{i \in I}. \end{aligned}$$

Da propriedade universal para conjuntos, L é a única função de X para $\prod_{i \in I} \mathbf{V}_i$ tal que, para todo $i \in I$, $\pi_i \circ L = L_i$. Falta mostrar que L é função linear. Sejam $c \in C$ e $x_1, x_2 \in V$. Então

$$\begin{aligned} L(x_1 + cx_2) &= (L_i(x_1 + cx_2))_{i \in I} \\ &= (L_i(x_1) + cL_i(x_2))_{i \in I} \\ &= (L_i(x_1))_{i \in I} + c(L_i(x_2))_{i \in I} \\ &= L(x_1) + cL(x_2). \end{aligned} \quad \blacksquare$$

10.7.2 Coproduto (Soma)

Definição 10.13. Seja $(\mathbf{V}_i)_{i \in I} = ((V_i, +_i, \cdot_i))_{i \in I}$ uma família de espaços vetoriais. A soma categórica de $(\mathbf{V}_i)_{i \in I}$ é

$$\bigsqcup_{i \in I} \mathbf{V}_i = (V, +, \cdot),$$

em que

$$V = \left\{ v = (v_i)_{i \in I} \in \prod_{i \in I} V_i \mid |\text{supp}(v)| < |\mathbb{N}| \right\},$$

$$\begin{aligned} +: V \times V &\longrightarrow V \\ (v, v') &\longmapsto (v_i +_i v'_i)_{i \in I} \end{aligned}$$

e

$$\begin{aligned} \cdot: C \times V &\longrightarrow V \\ (c, v) &\longmapsto (cv_i)_{i \in I}. \end{aligned}$$

Observe que, se $|I| < |\mathbb{N}|$, então $\prod_{i \in I} \mathbf{V}_i = \bigsqcup_{i \in I} \mathbf{V}_i$.

Proposição 10.30 (Propriedade Universal). *Sejam $(\mathbf{V}_i)_{i \in I}$ uma família de espaços vetoriais sobre um corpo \mathbf{C} , \mathbf{X} um espaço vetorial sobre \mathbf{C} e, para todo $i \in I$, $L_i: \mathbf{V}_i \rightarrow \mathbf{X}$ uma função linear. Então existe única função linear $L: \mathbf{X} \rightarrow \bigsqcup_{i \in I} \mathbf{V}_i$ tal que, para todo $i \in I$, $L \circ \iota_i = L_i$ (o diagrama comuta).*

$$\begin{array}{ccc} \mathbf{V}_i & \xrightarrow{L_i} & \mathbf{X} \\ \iota_i \downarrow & \nearrow L & \\ \bigsqcup_{i \in I} \mathbf{V}_i & & \end{array}$$

O coproduto de espaços vetoriais é também chamado de *soma* ou *soma direta* e denotado

$$\bigoplus_{i \in I} \mathbf{V}_i.$$

Capítulo 11

Álgebra Multilinear

11.1 Funções Multilineares

Definição 11.1. Sejam $\mathbf{V}_0, \dots, \mathbf{V}_{n-1}$ e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} e $k \in \mathbb{N}$. Uma função k -linear de $(\mathbf{V}_0, \dots, \mathbf{V}_{k-1})$ para \mathbf{W} é uma função

$$L: V_0 \times \cdots \times V_{k-1} \longrightarrow W$$

que satisfaz

1. (Multilinearidade) Para todos $i \in [k]$ e

$$(v_0, \dots, v_{i-1}, v_{i+1}, \dots, v_{k-1}) \in V_0 \times \cdots \times V_{i-1} \times V_{i+1} \times \cdots \times V_{k-1},$$

a função

$$\begin{aligned} L(v_0, \dots, v_{i-1}, \cdot, v_{i+1}, \dots, v_{k-1}): \mathbf{V}_i &\longrightarrow \mathbf{W} \\ v &\longmapsto L(v_0, \dots, v_{i-1}, v, v_{i+1}, \dots, v_{k-1}) \end{aligned}$$

é uma função linear.

O conjunto dessas funções é denotado

$$\mathcal{L}(V_0, \dots, V_{k-1}; W)$$

e, quando todos os espaços \mathbf{V}_i são iguais, denota-se

$$\mathcal{L}^k(V, W) := \mathcal{L}\left(\underbrace{V, \dots, V}_k; W\right)$$

Proposição 11.1. Sejam $\mathbf{V}_0, \dots, \mathbf{V}_{k-1}$ e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} e, para cada $i \in [k]$, $d_i \in \mathbb{N}$ a dimensão e $b^{(i)} = (b_j^{(i)})_{j \in [d_i]}$ uma base ordenada de \mathbf{V}_i . Toda função k -linear $L \in \mathcal{L}(V_0, \dots, V_{k-1}; W)$ está determinada pelos seus valores em $(b_{j_0}^{(0)}, \dots, b_{j_{k-1}}^{(k-1)})_{(j_0, \dots, j_{k-1}) \in [d_0] \times \cdots \times [d_{k-1}]}$.

Demonstração. Sejam $v_0, \dots, v_{m-1} \in V_k$, $c^0, \dots, c^{m-1} \in C$, e, para todo $i \in [k] \setminus \{k\}$, $v'_i \in V_i$. Como consequência da propriedade de linearidade generalizada para funções lineares,

$$L\left(v'_0, \dots, \bigoplus_{i \in [m]} c^i v_i, \dots, v'_{k-1}\right) = \bigoplus_{i \in [m]} c^i L(v'_0, \dots, v_i, \dots, v'_{k-1}).$$

Sendo assim, para cada $i \in [k]$, sejam $v_i \in V_i$ e $v_{(i)}^0, \dots, v_{(i)}^{d_i} \in C$ os coeficientes de v_i na base $b^{(i)}$, de modo que

$$v_i = \bigoplus_{j \in [d_i]} v_{(i)}^j b_j^{(i)}.$$

Pela linearidade em cada entrada, temos que

$$\begin{aligned} L(v_0, \dots, v_{k-1}) &= L\left(\bigoplus_{j_0 \in [d_0]} v_{(0)}^{j_0} b_{j_0}^{(0)}, \dots, \bigoplus_{j_{k-1} \in [d_{k-1}]} v_{(k-1)}^{j_{k-1}} b_{j_{k-1}}^{(k-1)}\right) \\ &= \bigoplus_{j_0 \in [d_0]} v_{(0)}^{j_0} L\left(b_{j_0}^{(0)}, \dots, \bigoplus_{j_{k-1} \in [d_{k-1}]} v_{(k-1)}^{j_{k-1}} b_{j_{k-1}}^{(k-1)}\right) \\ &\quad \vdots \qquad \vdots \\ &= \bigoplus_{j_0 \in [d_0]} \cdots \bigoplus_{j_{k-1} \in [d_{k-1}]} v_{(0)}^{j_0} \cdots v_{(k-1)}^{j_{k-1}} L\left(b_{j_0}^{(0)}, \dots, b_{j_{k-1}}^{(k-1)}\right) \\ &= \bigoplus_{(j_0, \dots, j_{k-1}) \in [d_0] \times \cdots \times [d_{k-1}]} v_{(0)}^{j_0} \cdots v_{(k-1)}^{j_{k-1}} L\left(b_{j_0}^{(0)}, \dots, b_{j_{k-1}}^{(k-1)}\right). \end{aligned}$$

Portanto a função L está determinada pelos valores que tem nos elementos

$$(b_{j_0}^{(0)}, \dots, b_{j_{k-1}}^{(k-1)})_{(j_0, \dots, j_{k-1}) \in [d_0] \times \cdots \times [d_{k-1}]}. \quad \blacksquare$$

Proposição 11.2. *Sejam V_0, \dots, V_{k-1} e W espaços lineares sobre um corpo C . Então*

$$\mathcal{L}(V_0, \dots, V_{k-1}; W) := (\mathcal{L}(V_0, \dots, V_{k-1}; W), +, \cdot),$$

em que $+$ e \cdot são a soma e o produto escalar pontuais induzidos por W , é um espaço linear sobre C .

11.1.1 Simetria, Antissimetria e Alternância

Definição 11.2. Sejam V e W espaços lineares sobre um corpo C . Uma função k -linear de V para W

1. *simétrica* é uma função $f \in \mathcal{L}^k(\mathbf{V}, \mathbf{W})$ tal que, para toda permutação $p \in \mathfrak{S}_k$ e todos $v_0, \dots, v_{k-1} \in V$,

$$f(v_{p(0)}, \dots, v_{p(k-1)}) = f(v_0, \dots, v_{k-1});$$

O conjunto das funções k -lineares simétricas é denotado $\mathcal{S}^k(\mathbf{V}, \mathbf{W})$.

2. *antissimétrica* é uma função $f \in \mathcal{L}^k(\mathbf{V}, \mathbf{W})$ tal que, para toda permutação $p \in \mathfrak{S}_k$ e todos $v_0, \dots, v_{k-1} \in V$,

$$f(v_{p(0)}, \dots, v_{p(k-1)}) = \epsilon(p) f(v_0, \dots, v_{k-1});$$

3. *alternada* é uma função $f \in \mathcal{L}^k(\mathbf{V}, \mathbf{W})$ tal que, para todos $v_0, \dots, v_{k-1} \in V$ linearmente dependentes,

$$f(v_0, \dots, v_{k-1}) = 0.$$

O conjunto das funções k -lineares alternadas é denotado $\mathcal{A}^k(\mathbf{V}, \mathbf{W})$.

Proposição 11.3. *Sejam \mathbf{V} e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} e $f \in \mathcal{L}^k(\mathbf{V}, \mathbf{W})$.*

1. A função f é alternada se, e somente se, para todos $v_0, \dots, v_{k-1} \in V$ tais que existem $i, j \in [k]$ distintos satizfazendo $v_i = v_j$,

$$f(v_0, \dots, v_{k-1}) = 0.$$

2. Se f é alternada, então é antissimétrica. Se $\text{car}(\mathbf{C}) \neq 2$ e f é antissimétrica, então é alternada.

3. Se $\text{car}(\mathbf{C}) = 2$, então f é antissimétrica se, e somente se, é simétrica.

Demonstração. 1. Se f é alternada, então, para todos $v_0, \dots, v_{k-1} \in V$ tais que $v_i = v_j$ para dois $i, j \in [k]$ distintos, o conjunto $\{v_0, \dots, v_{k-1}\}$ é linearmente dependente, portanto $f(v_0, \dots, v_{k-1}) = 0$. Reciprocamente, suponha que f satisfaça a propriedade e sejam $v_0, \dots, v_{k-1} \in V$ linearmente dependentes. Então existe $i \in [k]$ tal que v_i é combinação linear dos outros v_j : existem $c_j \in \mathbf{C}$, com $j \in [k] \setminus \{i\}$, tais que

$$v_i = \sum_{j \in [k] \setminus \{i\}} c_j v_j.$$

Assim, segue da k -linearidade e da propriedade enunciada que

$$\begin{aligned} f(v_0, \dots, v_{k-1}) &= f\left(v_0, \dots, \sum_{j \in [k] \setminus \{i\}} c_j v_j, \dots, v_{k-1}\right) \\ &= \sum_{j \in [k] \setminus \{i\}} c_j f(v_0, \dots, v_i, \dots, v_{k-1}) \\ &= \sum_{j \in [k] \setminus \{i\}} c_j 0 = 0. \end{aligned}$$

2. Suponha f alternada e sejam $v_0, \dots, v_{k-1} \in V$. Então segue da k -linearidade e da alternância de f que

$$\begin{aligned} 0 &= f(v_0, \dots, v_i + v_j, \dots, v_i + v_j, \dots, v_{k-1}) \\ &= f(v_0, \dots, v_i, \dots, v_i, \dots, v_{k-1}) + f(v_0, \dots, v_i, \dots, v_j, \dots, v_{k-1}) \\ &\quad + f(v_0, \dots, v_j, \dots, v_i, \dots, v_{k-1}) + f(v_0, \dots, v_j, \dots, v_j, \dots, v_{k-1}) \\ &= f(v_0, \dots, v_i, \dots, v_j, \dots, v_{k-1}) + f(v_0, \dots, v_j, \dots, v_i, \dots, v_{k-1}), \end{aligned}$$

portanto

$$f(v_0, \dots, v_i, \dots, v_j, \dots, v_{k-1}) = -f(v_0, \dots, v_j, \dots, v_i, \dots, v_{k-1}).$$

Como toda permutação $p \in \mathfrak{S}_k$ é um produto de $N \in \mathbb{N}$ inversões, e como $\epsilon(p) = (-1)^N$, segue por indução que, para toda permutação $p \in \mathfrak{S}_k$,

$$f(v_{p(0)}, \dots, v_{p(k-1)}) = (-1)^N f(v_0, \dots, v_{k-1}) = \epsilon(p) f(v_0, \dots, v_{k-1}).$$

Suponha que $\text{car}(\mathbf{C}) \neq 2$. Sejam $f \in \mathcal{L}^k(\mathbf{V}, \mathbf{W})$ antissimétrica e $v_0, \dots, v_{k-1} \in V$ tais que $v_i = v_j$ para dois $i, j \in [k]$ distintos. Considerando a permutação $(i \ j) \in \mathfrak{S}_k$, segue da antissimetria de f e de $\epsilon((i \ j)) = -1$ que

$$\begin{aligned} f(v_0, \dots, v_i, \dots, v_j, \dots, v_{k-1}) &= f(v_0, \dots, v_j, \dots, v_i, \dots, v_{k-1}) \\ &= -f(v_0, \dots, v_i, \dots, v_j, \dots, v_{k-1}), \end{aligned}$$

portanto

$$2f(v_0, \dots, v_{k-1}) = 0.$$

Como $\text{car}(\mathbf{C}) \neq 2$, segue que $f(v_0, \dots, v_{k-1}) = 0$. Do item 1 segue que f é alternada.

3. Se $\text{car}(\mathbf{C}) = 2$, então $-1 = 1$. Isso implica que, para qualquer permutação p , $\epsilon(p) = 1$.

■

Um exemplo de uma função multilinear que é antissimétrica mas não é alternada em para um corpo de característica 2 é o seguinte. Seja $\mathbb{Z}_2 = \{0, 1\}$ o corpo de característica 2 e considere a função $f: \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ dada por

$$\begin{aligned} f: \mathbb{Z}_2 \times \mathbb{Z}_2 &\longrightarrow \mathbb{Z}_2 \\ (0, 0) &\longmapsto 0 \\ (0, 1) &\longmapsto 0 \\ (1, 0) &\longmapsto 0 \\ (1, 1) &\longmapsto 1 \end{aligned}$$

Pode-se verificar que essa função é bilinear e antissimétrica, mas não é alternada porque $f(1, 1) = 1 \neq 0$.

De modo mais geral, para qualquer função $p: [k] \rightarrow [k]$, não necessariamente bijetiva, considerando o caráter $\epsilon(p)$ que vale 0 se p não é uma permutação, e 1 ou -1 conforme a paridade da permutação p , as definições de formas antissimétricas e alternadas podem ser unificadas: a de formas antissimétricas pode ser mantida como foi feita e, para o caso de formas alternadas, devido à propriedade 1 da proposição anterior, pode-se enunciar: para qualquer $p: [k] \rightarrow [k]$,

$$f(v_{p(0)}, \dots, v_{p(k-1)}) = \epsilon(p)f(v_0, \dots, v_{k-1}).$$

O caso em que p é bijetiva recai na definição de formas antissimétricas, e o caso em que p não é bijetiva recai na definição de formas alternadas, mais precisamente da propriedade 1 da proposição anterior, que é equivalente à definição de forma alternada.

Proposição 11.4. *Sejam \mathbf{V} e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} . Os espaços $\mathcal{S}^k(\mathbf{V}, \mathbf{W})$ e $\mathcal{A}^k(\mathbf{V}, \mathbf{W})$ são subespaços lineares de $\mathcal{L}^k(\mathbf{V}, \mathbf{W})$.*

11.2 Formas Multilineares

Definição 11.3. Seja \mathbf{V} um espaço linear sobre um corpo \mathbf{C} . Uma *forma k -linear* em \mathbf{V} é uma função $f \in \mathcal{L}^k(\mathbf{V}; \mathbf{C})$, ou seja, um funcional k -linear em $(\mathbf{V}, \dots, \mathbf{V})$. O conjunto das formas k -lineares simétricas é denotado $\mathcal{S}^k(\mathbf{V})$ e o das alternadas é denotado $\mathcal{A}^k(\mathbf{V})$.

Temos que $\mathcal{S}^1(\mathbf{V}) = \mathcal{A}^1(\mathbf{V}) = \mathcal{L}^k(\mathbf{V})$ e $\mathcal{S}^0(\mathbf{V}) = \mathcal{A}^0(\mathbf{V}) = \mathcal{L}^0(\mathbf{V}) = \mathbf{C}$.

11.2.1 Produto Tensorial de Formas Multilineares

Definição 11.4. Sejam \mathbf{V} um espaço linear sobre um corpo \mathbf{C} , $f \in \mathcal{L}^k(\mathbf{V})$, $f' \in \mathcal{L}^{k'}(\mathbf{V})$ e $v_0, \dots, v_{k+k'-1} \in \mathbf{V}$. O *produto tensorial* de f e f' em $(v_0, \dots, v_{k+k'-1})$ é

$$(f \otimes f')(v_0, \dots, v_{k+k'-1}) := f(v_0, \dots, v_{k-1})f'(v_k, \dots, v_{k+k'-1}).$$

Sejam $n \in \mathbb{N}$ e $(f_i)_{i \in [n]}$ formas multilineares em \mathbf{V} . O *produto tensorial* dessas formas é definido recursivamente

$$\bigotimes_{i \in [n]} f_i := \begin{cases} f_0, & n = 1 \\ \left(\bigotimes_{i \in [n-1]} f_i \right) \otimes f_{n-1}, & n > 1. \end{cases}$$

Proposição 11.5. *Seja \mathbf{V} um espaço linear sobre um corpo \mathbf{C} .*

1. *Para todas formas $f \in \mathcal{L}^k(\mathbf{V})$ e $f' \in \mathcal{L}^{k'}(\mathbf{V})$, a função $f \otimes f'$ é uma forma $k + k'$ -linear.*
2. *(Bilinearidade) A função*

$$\begin{aligned} \otimes: \mathcal{L}^k(\mathbf{V}) \times \mathcal{L}^{k'}(\mathbf{V}) &\longrightarrow \mathcal{L}^{k+k'}(\mathbf{V}) \\ (f, f') &\longmapsto f \otimes f' \end{aligned}$$

é bilinear.

3. *(Associatividade) Para todas formas $f \in \mathcal{L}^k(\mathbf{V})$, $f' \in \mathcal{L}^{k'}(\mathbf{V})$ e $f'' \in \mathcal{L}^{k''}(\mathbf{V})$,*
- $$(f \otimes f') \otimes f'' = f \otimes (f' \otimes f'').$$

11.2.2 Produto Alternado de Formas Multilineares

Definição 11.5. Sejam \mathbf{V} um espaço linear sobre um corpo \mathbf{C} , $f \in \mathcal{A}^k(\mathbf{V})$, $f' \in \mathcal{A}^{k'}(\mathbf{V})$ e $v_0, \dots, v_{k+k'-1} \in \mathbf{V}$. O *produto alternado* (ou *exterior*) de f e f' em $(v_0, \dots, v_{k+k'-1})$ é

$$(f \wedge f')(v_0, \dots, v_{k+k'-1}) := \frac{1}{k!k'!} \sum_{p \in \mathfrak{S}_{k+k'}} \epsilon(p)(f \otimes f')(v_{p(i)})_{i \in [k+k']}.$$

Sejam $n \in \mathbb{N}$ e $(f_i)_{i \in [n]}$ formas multilineares em \mathbf{V} . O *produto alternado* dessas formas é definido recursivamente

$$\bigwedge_{i \in [n]} f_i := \begin{cases} f_0, & n = 1 \\ \left(\bigwedge_{i \in [n-1]} f_i \right) \wedge f_{n-1}, & n > 1. \end{cases}$$

Proposição 11.6. *Seja \mathbf{V} um espaço linear sobre um corpo \mathbf{C} .*

1. *Para todas formas $f \in \mathcal{L}^k(\mathbf{V})$ e $f' \in \mathcal{L}^{k'}(\mathbf{V})$, a função $f \wedge f'$ é uma forma $k + k'$ -linear alternada.*

2. (*Bilinearidade*) A função

$$\wedge: \mathcal{A}^k(\mathbf{V}) \times \mathcal{A}^{k'}(\mathbf{V}) \longrightarrow \mathcal{A}^{k+k'}(\mathbf{V})$$

$$(f, f') \longmapsto f \wedge f'$$

é bilinear.

3. (*Associatividade*) Para todas formas alternadas $f \in \mathcal{A}^k(\mathbf{V})$, $f' \in \mathcal{A}^{k'}(\mathbf{V})$ e $f'' \in \mathcal{A}^{k''}(\mathbf{V})$,

$$(f \wedge f') \wedge f'' = f \wedge (f' \wedge f'').$$

4. Para todas formas $f \in \mathcal{A}^k(\mathbf{V})$ e $f' \in \mathcal{A}^{k'}(\mathbf{V})$

$$f' \wedge f = (-1)^{kk'} f \wedge f'.$$

Demonstração. 1. Seja $v_0, \dots, v_{k+k'-1} \in V$ e $\bar{p} \in \mathfrak{S}_{k+k'}$. Então

$$\begin{aligned} (f \wedge f')(v_{\bar{p}(i)})_{i \in [k+k']} &= \frac{1}{k!k'!} \sum_{p \in \mathfrak{S}_{k+k'}} \epsilon(p)(f \otimes f')(v_{p(\bar{p}(i))})_{i \in [k+k']} \\ &= \frac{1}{k!k'!} \sum_{p \in \mathfrak{S}_{k+k'}} \epsilon(\bar{p}^{-1}p)(f \otimes f')(v_{p(i)})_{i \in [k+k']} \\ &= \frac{1}{k!k'!} \sum_{p \in \mathfrak{S}_{k+k'}} \epsilon(\bar{p}^{-1})\epsilon(p)(f \otimes f')(v_{p(i)})_{i \in [k+k']} \\ &= \epsilon(\bar{p}^{-1}) \frac{1}{k!k'!} \sum_{p \in \mathfrak{S}_{k+k'}} \epsilon(p)(f \otimes f')(v_{p(i)})_{i \in [k+k']} \\ &= \epsilon(\bar{p})(f \wedge f')(v_i)_{i \in [k+k']}. \end{aligned}$$

2. ■

Proposição 11.7. Sejam \mathbf{V} um espaço linear de dimensão finita d sobre um corpo \mathbf{C} , $(b_i)_{i \in [d]}$ um base ordenada de \mathbf{V} e $(b_i^*)_{i \in [d]}$ a base dual de \mathbf{V}^* . Então $\mathcal{A}^k(\mathbf{V})$ é um espaço linear sobre \mathbf{C} de dimensão $\binom{d}{k}$ e o conjunto

$$\left\{ b_{i_0}^* \wedge \cdots \wedge b_{i_{k-1}}^* \mid i_0 < \cdots < i_{k-1} \in [d] \right\}$$

de formas alternadas k -lineares em \mathbf{V} é uma base para $\mathcal{A}^k(\mathbf{V})$.

Em particular, isso mostra que formas d -lineares num espaço de dimensão d são todas múltiplos umas das outras, pois $\binom{d}{d} = 1$. Podemos fixar o valor de uma das formas como 1 na base canônica e chamá-la de *determinante*.

11.2.3 Determinante

Definição 11.6. Seja $d \in \mathbb{N}$. O *determinante* em \mathbb{R}^d é a forma d -linear

$$\det := e_0^* \wedge \dots \wedge e_{d-1}^*.$$

Como comentado, essa é a única forma d -linear em \mathbb{R}^d tal que

$$\det(e_0, \dots, e_{d-1}) = 1.$$

Definição 11.7. Sejam \mathbf{V} e \mathbf{W} espaços lineares sobre um corpo \mathbf{C} , $L: V \rightarrow W$ uma função linear e $f \in \mathcal{L}^k(\mathbf{W})$. A função puxada por L de f é a função

$$\begin{aligned} L^* f: V^k &\longrightarrow C \\ (v_0, \dots, v_{k-1}) &\longmapsto f(L(v_0), \dots, L(v_{k-1})). \end{aligned}$$

Essa função $L^* f$ é multilinear e, se f for alternada, é alternada.

Proposição 11.8. Sejam \mathbf{V}_0 , \mathbf{V}_1 e \mathbf{V}_2 espaços lineares sobre um corpo \mathbf{C} e $L_0: V_0 \rightarrow V_1$ e $L_1: V_1 \rightarrow V_2$ funções lineares. Então

$$(L_1 \circ L_0)^* = L_0^* \circ L_1^*.$$

Essas função k -adjuntas estão também definidas se restringimos os espaços de funcionais \mathcal{L}^k para espaços de funcionais alternados \mathcal{A}^k . Se considerarmos um espaço \mathbf{V} d -dimensional, o espaço $\mathcal{A}^d(\mathbf{V})$ é um espaço 1-dimensional, o que implica que todas funções lineares são multiplicações por constantes. Isso nos permite definir o determinante de uma função linear instrinsecamente como a constante de que consiste seu d -adjunto.

Definição 11.8. Sejam \mathbf{V} um espaço linear d -dimensional sobre um corpo \mathbf{C} , $L: V \rightarrow V$ uma função linear e $L^*: \mathcal{A}^d(V) \rightarrow \mathcal{A}^d(V)$. O *determinante* de L é a constante $\det(L) \in \mathbf{C}$ tal que, para todas formas $f \in \mathcal{A}^d(\mathbf{V})$,

$$L^* f = \det(L) f.$$

Isso nos dá por definição a igualdade

$$f(L(v_0), \dots, L(v_{d-1})) = \det(L) f(v_0, \dots, v_{d-1}).$$

Proposição 11.9. Sejam \mathbf{V} um espaço linear d -dimensional sobre um corpo \mathbf{C} e $L_0, L_1 \in \mathcal{L}(V)$. Então

$$\det(L_1 \circ L_0) = \det(L_0) \det(L_1).$$

Demonstração. Seja $f \in \mathcal{A}^n(V)$ tal que $f \neq 0$. Então

$$\det(L_1 \circ L_0) f = (L_1 \circ L_0)^* f = (L_0^* \circ L_1^*) f = \det(L_0) \det(L_1) f.$$

■

11.2.4 Extras

Definimos

$$[d]^{\uparrow k} := \left\{ (i_0, \dots, i_{k-1}) \in [d]^k \mid i_0 < \dots < i_{k-1} \right\}.$$

Note que

$$\left| [d]^{\uparrow k} \right| = \left| \binom{[d]}{k} \right| = \binom{d}{k},$$

em que $\binom{[d]}{k} = \{I \subseteq [d] \mid |I| = k\}$.

11.3 Produto Tensorial de Espaços Lineares

Definição 11.9. Sejam X um conjunto, \mathbf{C} um corpo e $f : X \rightarrow C$ uma função. O *suporte* de f é o conjunto

$$\text{supp}(f) := f^{-1}(\{0\}^{\complement}) = \{x \in X \mid f(x) \neq 0\}.$$

Definição 11.10. Sejam I um conjunto e \mathbf{C} um corpo. O *espaço linear livre em I* sobre \mathbf{C} é o conjunto

$$\mathcal{F}(I) := \{v \in C^I \mid |\text{supp}(v)| < |\mathbb{N}|\}.$$

Os elementos de $\mathcal{F}(I)$ são as *combinações lineares formais* de elementos de I sobre \mathbf{C} .

A *inclusão* de I em $\mathcal{F}(I)$ é a função

$$\begin{aligned} \iota : I &\longrightarrow \mathcal{F}(I) \\ v &\longmapsto \delta_v : I \longrightarrow C \\ i &\longmapsto \begin{cases} 1, & i = v \\ 0, & i \neq v. \end{cases} \end{aligned}$$

Denotaremos os elementos δ_v por v quando não houver necessidade de diferenciá-los.

Note que $\mathcal{F}(I) = \bigsqcup_{i \in I} \mathbf{C}$ e, portanto,

$$\mathcal{F}(I) := (\mathcal{F}(I), +, \cdot),$$

em que $+$ e \cdot são a soma e o produto escalar pontuais induzidos por \mathbf{W} , é um espaço linear sobre \mathbf{C} com base $\{\delta_v \mid v \in I\}$. Por isso, definido $c_i := v(i) \in C$, uma função $v : I \rightarrow C$ de suporte finito é uma soma

$$v = \bigoplus_{i \in I} c_i \delta_i = \bigoplus_{i \in I} c_i v_i,$$

que é uma soma finita porque $\text{supp}(v)$ é finito, ou seja, somente uma quantidade finita dos c_i é não nulo.

Proposição 11.10 (Propriedade Característica dos Espaços Lineares Livres). *Sejam I um conjunto, \mathbf{C} um corpo e V um espaço linear sobre \mathbf{C} . Para toda função $f : I \rightarrow V$, existe uma única função linear $\bar{f} : \mathcal{F}(I) \rightarrow V$ tal que $\bar{f} \circ \iota = f$ (o diagrama comuta).*

$$\begin{array}{ccc}
 \mathcal{F}(I) & & \\
 \uparrow \iota & \searrow \bar{f} & \\
 I & \xrightarrow{f} & V
 \end{array}$$

Demonstração. Basta usar a propriedade característica de coproduto de espaços lineares, ou notar o que uma função \bar{f} pode ser construída definindo seus valores em $\delta_v \in \mathcal{F}(I)$. Para todo $v = +_{i \in I} c_i v_i \in \mathcal{F}(I)$, define-se

$$\bar{f}\left(\sum_{v_i \in I} c_i v_i\right) := \sum_{v_i \in I} c_i f(v_i)$$

A função é única pois está definida da base δ_v . ■

Definição 11.11. Sejam C um corpo e V_0, \dots, V_{n-1} conjuntos. Consideremos o conjunto \mathcal{R} gerado por vetores de $\mathcal{F}(V_0 \times \dots \times V_{n-1})$ da forma

$$(v_0, \dots, v_i + v'_i, \dots, v_{n-1}) - (v_0, \dots, v_i, \dots, v_{n-1}) - (v_0, \dots, v'_i, \dots, v_{n-1}),$$

$$(v_0, \dots, cv_i, \dots, v_{n-1}) - c(v_0, \dots, v_i, \dots, v_{n-1}),$$

em que $v_i, v'_i \in V_i$ para todo $i \in [n]$ e $c \in C$. O *produto tensorial* de V_0, \dots, V_{n-1} é o espaço linear

$$V_0 \otimes \dots \otimes V_{n-1} := \mathcal{F}(V_0 \times \dots \times V_{n-1}) / \mathcal{R}$$

A classe de equivalência de $(v_0, \dots, v_{n-1}) \in V_0 \times \dots \times V_{n-1}$ em $V_0 \otimes \dots \otimes V_{n-1}$ é denotada $v_0 \otimes \dots \otimes v_{n-1}$ e o *mapa tensorial canônico* é a função $\otimes := \pi \circ \iota: V_0 \times \dots \times V_{n-1} \longrightarrow V_0 \otimes \dots \otimes V_{n-1}$, em que $\pi: \mathcal{F}(V_0 \times \dots \times V_{n-1}) \longrightarrow \mathcal{R}$ é a projeção do quociente de espaços lineares.

Proposição 11.11 (Propriedade Característica de Produto Tensorial). *Sejam V_0, \dots, V_{n-1}, W espaços lineares sobre um corpo C .*

1. *O mapa tensorial canônico*

$$\otimes: V_0 \times \dots \times V_{n-1} \longrightarrow V_0 \otimes \dots \otimes V_{n-1}$$

é uma função multilinear.

2. Para toda função multilinear $L: \mathbf{V}_0 \times \cdots \times \mathbf{V}_{n-1} \rightarrow \mathbf{W}$, existe única função linear $\bar{L}: \mathbf{V}_0 \otimes \cdots \otimes \mathbf{V}_{n-1} \rightarrow \mathbf{W}$ tal que $\bar{L} \circ \otimes = L$ (o diagrama comuta).

$$\begin{array}{ccc}
 \mathbf{V}_0 \otimes \cdots \otimes \mathbf{V}_{n-1} & & \\
 \uparrow \otimes & \searrow \bar{L} & \\
 \mathbf{V}_0 \times \cdots \times \mathbf{V}_{n-1} & \xrightarrow{L} & \mathbf{W}
 \end{array}$$

Demonstração. 1. Vale por definição.

2. Pela propriedade característica de espaços lineares livres, existe única função linear $\tilde{L}: \mathcal{F}(V_0 \times \cdots \times V_{n-1}) \rightarrow W$ tal que $\tilde{L} \circ \iota = L$. Mas como L é multilinear, o subespaço \mathcal{R} está contido no núcleo de \tilde{L} , pois, para todos $v_i, v'_i \in V_i$, com $i \in [n]$, e $c \in C$,

$$\begin{aligned}
 \tilde{L}(v_0, \dots, v_i + v'_i, \dots, v_{n-1}) &= L(v_0, \dots, v_i + v'_i, \dots, v_{n-1}) \\
 &= L(v_0, \dots, v_i, \dots, v_{n-1}) + L(v_0, \dots, v'_i, \dots, v_{n-1}) \\
 &= \tilde{L}(v_0, \dots, v_i, \dots, v_{n-1}) + \tilde{L}(v_0, \dots, v'_i, \dots, v_{n-1}) \\
 &= \tilde{L}((v_0, \dots, v_i, \dots, v_{n-1}) + (v_0, \dots, v'_i, \dots, v_{n-1}))
 \end{aligned}$$

e

$$\begin{aligned}
 \tilde{L}(v_0, \dots, cv_i, \dots, v_{n-1}) &= L(v_0, \dots, cv_i, \dots, v_{n-1}) \\
 &= cL(v_0, \dots, v_i, \dots, v_{n-1}) \\
 &= c\tilde{L}(v_0, \dots, v_i, \dots, v_{n-1}) \\
 &= \tilde{L}(c(v_0, \dots, v_i, \dots, v_{n-1})).
 \end{aligned}$$

Isso implica que existe função linear $\bar{L}: V_0 \otimes \cdots \otimes V_{n-1} \rightarrow W$ que satisfaz $\bar{L} \circ \pi = \tilde{L}$. Como $\otimes = \pi \circ \iota$, segue que

$$\bar{L} \circ \otimes = \bar{L} \circ \pi \circ \iota = \tilde{L} \circ \iota = L.$$

■

Algumas identidades importantes. Os espaços lineares das funções multilineares é isomorfo ao espaço das funções lineares no produto tensorial:

$$\mathcal{L}(\mathbf{V}_0, \dots, \mathbf{V}_{n-1}; \mathbf{W}) \simeq \mathcal{L}(\mathbf{V}_0 \otimes \cdots \otimes \mathbf{V}_{n-1}; \mathbf{W}).$$

11.3.1 Tensores

Definição 11.12. Seja \mathbf{V} um espaço linear sobre um corpo C . A k -potência tensorial de \mathbf{V} é o espaço

$$V^{\otimes k} := \bigotimes_{i \in [k]} V = \underbrace{V \otimes \cdots \otimes V}_k.$$

Um k -vetor de \mathbf{V} é um elemento de $V^{\otimes k}$ e um k -covetor de \mathbf{V} é um elemento de $(V^*)^{\otimes k}$.

A (p, q) -potência tensorial de \mathbf{V} é o espaço

$$V^{\otimes(p,q)} := V^{\otimes p} \otimes (V^*)^{\otimes q}.$$

Um (p, q) -tensor de \mathbf{V} é um elemento de $V^{\otimes(p,q)}$. A álgebra tensorial de \mathbf{V} é o espaço

$$\bigotimes V := \bigoplus_{(p,q) \in \mathbb{N} \times \mathbb{N}} V^{\otimes(p,q)}.$$

Temos as identificações

$$\begin{aligned} V^{\otimes(0,0)} &= C \\ V^{\otimes(1,0)} &= V \\ V^{\otimes(0,1)} &= V^* \\ V^{\otimes(1,1)} &= \mathcal{L}(V, V). \end{aligned}$$

Capítulo 12

Álgebras sobre Corpos

12.1 Álgebra e Ação Adjunta

Definição 12.1. Seja \mathbf{C} um corpo. Uma *álgebra* sobre \mathbf{C} é um par (\mathbf{A}, \cdot) em que \mathbf{A} é um espaço vetorial sobre \mathbf{C} e $\cdot: A \times A \rightarrow A$ é uma função bilinear. Uma álgebra é *associativa*, *comutativa* ou *antissimétrica* conforme a respectiva propriedade do produto \cdot , e é unitária se \cdot tem identidade.

Definição 12.2. Sejam (\mathbf{A}, \cdot) uma álgebra sobre um corpo \mathbf{C} e $a \in A$. A *ação adjunta* em \mathbf{A} baseada em a é a função linear

$$\begin{aligned} \text{ad}_a: A &\longrightarrow A \\ a' &\longmapsto a \cdot a'. \end{aligned}$$

Proposição 12.1. Seja (\mathbf{A}, \cdot) uma álgebra sobre um corpo \mathbf{C} . Então $(\mathcal{L}(A, A), \circ)$ é uma álgebra associativa sobre \mathbf{C} .

Demonstração. Sabemos que $\mathcal{L}(A, A)$ é um espaço linear. Para mostrar que é uma álgebra, devemos mostrar que \circ é bilinear. Sejam $L, L, L'' \in \mathcal{L}(A, A)$ e $c \in C$. Então, para todo $a \in A$,

$$\begin{aligned} ((cL + L') \circ L'')(a) &= (cL + L')(L''(a)) \\ &= cL(L''(a)) + L'(L''(a)) \\ &= cL \circ L''(a) + L' \circ L''(a) \\ &= (cL \circ L'' + L' \circ L'')(a). \end{aligned}$$

Isso mostra que $(cL + L') \circ L'' = cL \circ L'' + L' \circ L''$. Agora,

$$\begin{aligned} (L \circ (cL' + L''))(a) &= L((cL' + L'')(a)) \\ &= L(cL'(a) + L''(a)) \\ &= cL(L'(a)) + L(L''(a)) \\ &= cL \circ L'(a) + L \circ L''(a) \\ &= (cL \circ L' + L \circ L'')(a). \end{aligned}$$

Isso mostra que $L \circ (cL' + L'') = cL \circ L' + L \circ L''$. A composição de funções é associativa, portanto a álgebra é associativa. \blacksquare

Proposição 12.2. *Sejam (A, \cdot) uma álgebra sobre um corpo C e I um conjunto. Então (A^I, \cdot) , em que $\cdot : A^I \times A^I \rightarrow A^I$ é o produto entrada a entrada, é uma álgebra sobre C . Se o produto de A é associativo ou comutativo, então o produto de A^I é, respectivamente, associativo ou comutativo, e é se A é unitária, $(1)_{i \in I}$ é identidade do produto de A^I .*

Demonstração. Sabemos que A^I é um espaço linear sobre C . Basta mostrar que \cdot é um produto bilinear. Sejam $(a_i)_{i \in I}, (a'_i)_{i \in I}, (a''_i)_{i \in I} \in A^I$ e $c \in C$. Então

$$\begin{aligned} (c(a_i)_{i \in I} + (a'_i)_{i \in I}) \cdot (a''_i)_{i \in I} &= (ca_i + a'_i)_{i \in I} \cdot (a''_i)_{i \in I} \\ &= ((ca_i + a'_i) \cdot a''_i)_{i \in I} \\ &= (ca_i \cdot a''_i + a'_i \cdot a''_i)_{i \in I} \\ &= c(a_i \cdot a''_i)_{i \in I} + (a'_i \cdot a''_i)_{i \in I} \\ &= c(a_i)_{i \in I} \cdot (a''_i)_{i \in I} + (a'_i)_{i \in I} \cdot (a''_i)_{i \in I}. \end{aligned}$$

A demonstração da linearidade na segunda entrada é análoga, e as demonstrações de associatividade e comutatividade e identidade são triviais. \blacksquare

Proposição 12.3. *Seja (A, \cdot) uma álgebra sobre um corpo C . A álgebra A é associativa se, e somente se, para todos $a, a' \in A$,*

$$\text{ad}_{a \cdot a'} = \text{ad}_a \circ \text{ad}_{a'}.$$

12.2 Derivação

Definição 12.3. Seja (A, \cdot) uma álgebra sobre um corpo C . Uma *derivação* em A é uma função linear $D: A \rightarrow A$ tal que

1. (Regra do Produto) Para todos $a, a' \in A$,

$$D(a \cdot a') = D(a) \cdot a' + a \cdot D(a').$$

O conjunto dessas derivações é $\text{Der}(A)$.

Note que a propriedade acima nem sempre é equivalente a

$$D(a \cdot a') = a' \cdot D(a) + a \cdot D(a'),$$

pois o produto \cdot nem sempre é comutativo, mas sempre é equivalente a

$$D(a \cdot a') = a \cdot D(a') + D(a) \cdot a',$$

pois a soma $+$ é comutativa.

Proposição 12.4. *Sejam (\mathbf{A}, \cdot) uma álgebra sobre um corpo \mathbf{C} e $D: A \rightarrow A$ uma derivação em \mathbf{A} .*

1. *Para todos $a_0, \dots, a_{n-1} \in A$,*

$$D(a_0 \cdots a_{n-1}) = \sum_{i \in [n]} a_0 \cdots D(a_i) \cdots a_{n-1};$$

2. *Se \cdot é comutativo, então, para todos $a \in A$ e $n \in \mathbb{N}^*$,*

$$D(a^n) = n a^{n-1} D(a);$$

3. *Se existe identidade $1 \in A$ do produto, então*

$$D(1) = 0.$$

4. *(Regra do produto de ordem superior) Para todos $a, a' \in A$ e $n \in \mathbb{N}$,*

$$D^n(aa') = \sum_{i \in [n+1]} \binom{n}{i} D^{n-i}(a) D^i(a').$$

Definição 12.4. Seja (\mathbf{A}, \cdot) uma álgebra sobre um corpo \mathbf{C} . O *colchete comutador* de (\mathbf{A}, \cdot) é a função

$$\begin{aligned} [\cdot, \cdot]: A \times A &\longrightarrow A \\ (a, a') &\longmapsto a \cdot a' - a' \cdot a. \end{aligned}$$

Proposição 12.5. *Seja (\mathbf{A}, \cdot) uma álgebra sobre um corpo \mathbf{C} . Então*

1. $(A, [\cdot, \cdot])$ é uma álgebra antissimétrica sobre \mathbf{C} ;
2. O produto \cdot é comutativo se, e somente se, $[\cdot, \cdot] = 0$;

Demonstração. 1. Primeiro, notemos que, para todos $a, a' \in A$,

$$[a, a'] = a \cdot a' - a' \cdot a = -(a' \cdot a - a \cdot a') = -[a', a].$$

Sendo assim, para mostrar que $[\cdot, \cdot]$ é bilinear antissimétrica, basta mostrar que ela é linear na primeira entrada. Para todos $a, a', a'' \in A$ e $c \in C$,

$$\begin{aligned} [ca + a', a''] &= (ca + a')a'' - a''(ca + a') \\ &= caa'' + a'a'' - ca''a - a''a' \\ &= caa'' - ca''a + a'a'' - a''a' \\ &= c[a, a''] + [a', a'']. \end{aligned}$$

2. Suponhamos, primeiro, que \cdot é comutativo. Então, para todos $a, a' \in A$,

$$[a, a'] = aa' - a'a = aa' - aa' = 0.$$

Reciprocamente, suponhamos que $[\cdot, \cdot] = 0$. Então, para todos $a, a' \in A$,

$$aa' = aa' + 0 = aa' + [a', a] = aa' + a'a - aa' = a'a.$$

■

12.3 Álgebra de Derivação Adjunta

Proposição 12.6. Sejam (A, \cdot) uma álgebra sobre um corpo C e $a \in A$. A função adjunta ad_a é uma derivação em A se, e somente se, para todos $a', a'' \in A$,

$$a \cdot (a' \cdot a'') = (a \cdot a') \cdot a'' + a' \cdot (a \cdot a'').$$

A demonstração é imediata. Essa propriedade é conhecida às vezes como identidade de Jacobi. No entanto, a identidade mais conhecida como identidade de Jacobi é

$$a \cdot (a' \cdot a'') + a' \cdot (a'' \cdot a) + a'' \cdot (a \cdot a') = 0,$$

que é equivalente à anterior se o produto é antissimétrico. Na maioria das vezes em que se usa essa identidade o produto é de fato antissimétrico, o que torna as duas propriedades equivalentes.

Definição 12.5. Seja C um corpo. Uma álgebra de derivação adjunta¹ sobre C é um par $(A, [\cdot, \cdot])$ em que $[\cdot, \cdot]: A \times A \rightarrow A$ é um produto alternado tal que, para todo $a \in A$, ad_a é uma derivação em A . O produto $[\cdot, \cdot]$ é o colchete de derivação.

¹Essas álgebras são conhecidas como ‘álgebras de Lie’.

Como $[\cdot, \cdot]$ é alternada, é antissimétrica, portanto a bilinearidade é equivalente à linearidade na segunda entrada de $[\cdot, \cdot]$. A alternância é equivalente a termos ao produto de um elemeto com ele mesmo ser 0, o que é o mesmo que a derivação adjunta baseada em um elemento aplicada a esse elemento é 0.

As três propriedades de $[\cdot, \cdot]: A \times A \rightarrow A$ são equivalentes a

1. (Linearidade na 2^a entrada) Para todos $a, a', a'' \in A$ e $c \in C$,

$$[a, ca' + a''] = c[a, a'] + [a, a''];$$

2. (Alternância) Para todo $a' \in A$,

$$[a, a] = 0;$$

3. (Derivação adjunta) Para todo $a \in A$, ad_a é uam derivação: para todos $a', a'' \in A$,

$$[a, [a', a'']] = [[a, a'], a''] + [a', [a, a'']].$$

Nesse caso em que a função adjunta é sempre uma derivação, pode-se também denotar $\partial_a := \text{ad}_a$, de modo que as prorpiedades acima se reduzem a termos: para todo $a \in A$, ∂_a é uma derivação tal que $\partial_a(a) = 0$.

Consideremos, agora, o conjunto $\text{Der}(A)$ das derivações em uma álgebra associativa (A, \cdot) . O espaço $\text{Der}(A)$ é um subespaço linear de $\mathcal{L}(A, A)$. Para mostrar isso, mostraremos que $\text{Der}(A)$ é fechado pela soma e pelo produto por escalar pontuais. Soma: para todas derivações $D, D' \in \text{Der}(A)$, a soma $D + D'$ é uma função linear, pois D e D' são lineares, portanto basta mostrar que ela é uma derivação. Para todos $a, a' \in A$,

$$\begin{aligned} (D + D')(aa') &= D(aa') + D'(aa') \\ &= D(a)a' + aD(a') + D'(a)a' + aD'(a') \\ &= (D(a) + D'(a))a' + a(D(a') + D'(a')) \\ &= (D + D')(a)a' + a(D + D')(a'). \end{aligned}$$

portanto $D + D'$ é uma derivação. Produto: para toda derivação $D \in \text{Der}(A)$ e escalar $c \in C$, o produto cD é linear, pois D é linear, portanto basta mostrar que ele é uma derivação. Para todos $a, a' \in A$,

$$(cD)(aa') = c(D(aa')) = c(D(a)a' + aD(a')) = (cD)(a)a' + a(cD)(a'),$$

portanto cD é uma derivação. Isso mostra que $\text{Der}(A)$ é subespaço linear de $\mathcal{L}(A, A)$.

No entanto, $\text{Der}(A)$ não é uma subálgebra de $\mathcal{L}(A, A)$ com o produto de composição de funções, pois, para todos $D, D' \in \text{Der}(A)$ e $a, a' \in A$,

$$\begin{aligned} (D \circ D')(aa') &= D(D'(aa')) = D(D'(a)a' + aD'(a')) \\ &= D(D'(a))a' + D'(a)D(a') + D(a)D'(a') + aD(D'(a')) \\ &= (D \circ D')(a)a' + a(D \circ D')(a') + D'(a)D(a') + D(a)D'(a'). \end{aligned}$$

Notando que invertendo as posições de D e D' obtemos a expressão

$$(D' \circ D)(aa') = (D' \circ D)(a)a' + a(D' \circ D)(a') + D(a)D'(a') + D'(a)D(a'),$$

podemos definir o produto $[D, D'] := D \circ D' - D' \circ D$ de modo a obter das expressões anteriores que

$$\begin{aligned} [D, D'](aa') &= (D \circ D')(aa') - (D' \circ D)(aa') \\ &= (D \circ D')(a)a' + a(D \circ D')(a') - (D' \circ D)(a)a' - a(D' \circ D)(a') \\ &= [D, D'](a)a' + a[D, D'](a'). \end{aligned}$$

O produto $[\cdot, \cdot]$ é bilinear, pois envolve somente diferença e composição de funções linear. Assim, está demonstrado a seguinte proposição.

Proposição 12.7. *Seja (A, \cdot) uma álgebra sobre um corpo C . Então $(\text{Der}(A), [\cdot, \cdot])$ é uma subálgebra de $(\mathcal{L}(A, A), [\cdot, \cdot])$.*

Parte III

Topologia e Geometria

Capítulo 13

Topologia

13.1 Espaços Topológicos

13.1.1 Topologia, abertos e fechados

A noção de topologia que será abordada nesta parte do livro é a topologia baseada em teoria dos conjuntos.

Definição 13.1. Seja X um conjunto. Uma *topologia* de X é um conjunto $\mathcal{T} \subseteq \wp(X)$ que satisfaz

1. Vazio e conjunto todo são abertos.

$$\emptyset, X \in \mathcal{T}$$

2. União de abertos é aberto.

$$(A_i)_{i \in I} \subseteq \mathcal{T} \Rightarrow \bigcup_{i \in I} A_i \in \mathcal{T}$$

3. Interseção finita de abertos é aberto.

$$(A_i)_{i \in [n]} \subseteq \mathcal{T} \Rightarrow \bigcap_{i=0}^{n-1} A_i \in \mathcal{T}$$

Proposição 13.1. Seja X um conjunto.

1. (Topologia trivial) $\{\emptyset, X\}$ é uma topologia de X ;
2. (Topologia discreta) $\wp(X)$ é uma topologia de X .

Demonstração. 1. Primeiramente, \emptyset e X pertencem a $\{\emptyset, X\}$. Agora, consideremos uma família $(A_i)_{i \in I} \subseteq \{\emptyset, X\}$ de abertos. Caso $A_i = \emptyset$ para todo $i \in I$, então $\bigcup_{i \in I} A_i = \emptyset \in \mathcal{T}$. Caso contrário, existe $j \in I$ tal que $A_j = X$, o que implica $\bigcup_{i \in I} A_i = X \in \mathcal{T}$. Assim, concluímos que vale a segunda propriedade. Para mostrar a terceira propriedade, seja $(A_i)_{i \in [n]} \subseteq \mathcal{T}$ uma família finita de abertos. Caso $A_i = X$ para todo $i \in I$, o que implica $\bigcap_{i=0}^{n-1} A_i = X \in \mathcal{T}$. Caso contrário, existe $j \in I$ tal que $A_j = \emptyset$, o que implica $\bigcap_{i=0}^{n-1} A_i = \emptyset \in \mathcal{T}$.

2. Todas propriedades valem pois $\mathcal{T} = \wp(X)$. ■

Definição 13.2. Um *espaço topológico* é um par (X, \mathcal{T}) em que X é um conjunto não vazio e \mathcal{T} é uma topologia de X . Um *aberto* de (X, \mathcal{T}) é um conjunto de \mathcal{T} . Um *fechado* de (X, \mathcal{T}) é um conjunto cujo complementar em X é um aberto de (X, \mathcal{T}) . O conjunto dos fechados de (X, \mathcal{T}) é denotado $\mathbb{C}(\mathcal{T})$.

Proposição 13.2 (Dualidade de abertos e fechados). *Seja X um conjunto. Então*

1. *Vazio e conjunto todo são fechados.*

$$\emptyset, X \in \mathbb{C}(\mathcal{T})$$

2. *Interseção de fechados é fechado.*

$$(F_i)_{i \in I} \subseteq \mathbb{C}(\mathcal{T}) \Rightarrow \bigcap_{i \in I} F_i \in \mathbb{C}(\mathcal{T})$$

3. *União finita de fechados é fechado.*

$$(F_i)_{i \in [n]} \subseteq \mathbb{C}(\mathcal{T}) \Rightarrow \bigcup_{i=0}^{n-1} F_i \in \mathbb{C}(\mathcal{T})$$

Demonstração. Todas as demonstrações dependem de propriedades básicas de teoria de conjuntos.

1. Como $\emptyset, X \in \mathcal{T}$, $\emptyset^c = X$ e $X^c = \emptyset$, segue que $\emptyset, X \in \mathbb{C}(\mathcal{T})$.
2. Seja $(F_i)_{i \in I} \subseteq \mathbb{C}(\mathcal{T})$. Então $((F_i)^c)_{i \in I} \subseteq \mathcal{T}$, o que implica que $\bigcup_{i \in I} (F_i)^c \in \mathcal{T}$. Para concluir a demonstração, basta notar que

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

3. Seja $(F_i)_{i \in [n]} \subseteq \mathbb{C}(\mathcal{T})$. Então $((F_i)^c)_{i \in [n]} \subseteq \mathcal{T}$, o que implica que $\bigcap_{i=0}^{n-1} (F_i)^c \in \mathcal{T}$. Para concluir a demonstração, basta notar que

$$\left(\bigcap_{i=0}^{n-1} (F_i)^c \right)^c = \bigcup_{i=0}^{n-1} F_i.$$
■

Interior e Fecho

Intuitivamente, sabemos dizer quais pontos de um subconjunto da reta, do plano ou do espaço estão dentro do conjunto, quais estão fora e quais formam uma espécie de fronteira entre a parte de dentro e a de fora. Para uma bola aberta de raio unitário e centro na origem, é claro que os pontos de norma menor que 1 são os pontos do interior da bola, os pontos de norma igual a 1 são os pontos de fronteira e os pontos com norma maior que 1 são os pontos do exterior. Para conjuntos mais complicados, no entanto, parece ser mais difícil dizer o que está dentro e o que está fora. Se analisamos o conjunto dos racionais na reta, não é óbvio o que está dentro, o que está fora, o que é fronteira.

Além disso, a nossa intuição usa a ideia de norma ou distância no caso da bola e em espaços topológicos gerais isso não é possível. Para continuar a generalização dos conceitos topológicos existentes na reta, plano e espaço, devemos tentar formular a ideia de ponto interior usando os conceitos topológicos gerais, e fazemos isso notando que, no caso da bola e de conjuntos simples dos espaços tradicionais, um ponto está dentro do conjunto se existe um aberto em torno do ponto que está inteiramente contido no conjunto. Esse conceito não é o conceito que usaremos para definir o interior de um conjunto, mas é equivalente.

No começo dessa seção, o foco será o conceito de interior de um conjunto. A definição de interior que usaremos é a de que o interior de um conjunto é o maior conjunto aberto contido no conjunto. Maior, nesse caso, significa maior em relação à ordem parcial de contenção de conjuntos abertos. Como união de abertos é aberto, sabemos que a união de todos abertos contidos em um conjunto é aberto e, portanto, é o maior aberto contido no conjunto. Podemos perceber, ainda, que essa definição é equivalente à comentada acima pois, se um ponto está em um aberto do conjunto, ele está na união de todos eles e, se ele está na união, está, em particular, em algum aberto. Seguem abaixo a definição formal de interior de um conjunto e, em seguida, algumas propriedades básicas.

Definição 13.3. Sejam X um espaço topológico, $C \subseteq X$ e $(A_i)_{i \in I}$ uma indexação do conjunto de todos conjuntos abertos de X que são subconjunto de C . O *interior* de C é o conjunto aberto

$$C^\circ := \bigcup_{i \in I} A_i.$$

De acordo com essa definição, o interior de um conjunto é o maior aberto contido no conjunto, no sentido de que qualquer aberto contido no conjunto está também contido no seu interior. Ainda, podemos ver o interior como um operador topológico — uma função $\mathcal{I} : \wp(X) \rightarrow \wp(X)$ que leva $C \mapsto C^\circ$. Nesse sentido, podemos pensar em propriedades que esse operador satisfaz. Algumas dessas propriedades estão na proposição abaixo. Além disso, se temos um operador qualquer

em $\wp(X)$ que satisfaça algumas das propriedades abaixo, então esse operador é o operador interior de alguma topologia de X . Isso está demonstrado na proposição que segue a proposição abaixo.

Proposição 13.3. *Sejam X um espaço topológico e $A, B \subseteq X$. Então*

1. $A^\circ \subseteq A$
2. $A \in \mathcal{T} \Leftrightarrow A^\circ = A$
3. $(A \cap B)^\circ = A^\circ \cap B^\circ$
4. $(A^\circ)^\circ = A^\circ$
5. $A \subseteq B \Rightarrow A^\circ \subseteq B^\circ$

Demonstração. Sejam $(A_i)_{i \in I}$, $(B_j)_{j \in J}$ e $(C_k)_{k \in K}$ indexações dos subconjuntos abertos de A , B e $A \cap B$, respectivamente.

1. Seja $a \in A^\circ$. Então existe $j \in J$ tal que $a \in A_j$. Como $A_i \subseteq A$ para todo $i \in I$, então $a \in A$, o que mostra que $A^\circ \subseteq A$.
2. Suponha que A um aberto. Como $A^\circ \subseteq A$ para todo $A \subseteq X$, basta mostrar que $A \subseteq A^\circ$. Seja $a \in A$. Se A é aberto, então existe $i \in I$ tal que $A_i = A$, o que implica $a \in A_i$ e, portanto, que $a \in A^\circ$, o que mostra que $A \subseteq A^\circ$. Assim, concluímos que $A^\circ = A$. Reciprocamente, suponha que $A^\circ = A$. Como A° é união de abertos, é um conjunto aberto e isso implica que A é aberto.
3. Vamos mostrar a inclusão $(A \cap B)^\circ \subseteq A^\circ \cap B^\circ$. Seja $a \in (A \cap B)^\circ$. Então existe $k \in K$ tal que $a \in C_k$. Como C_k é subconjunto aberto de $A \cap B$, então C_k é subconjunto aberto de A e de B , o que implica que $a \in A^\circ$ e $a \in B^\circ$. Assim, concluímos que $a \in A^\circ \cap B^\circ$. Reciprocamente, vamos mostrar a inclusão $A^\circ \cap B^\circ \subseteq (A \cap B)^\circ$. Seja $a \in A^\circ \cap B^\circ$. Então $a \in A^\circ$ e $a \in B^\circ$, o que implica que existem $i \in I$ e $j \in J$ tais que $a \in A_i$ e $a \in B_j$; ou seja, $a \in A_i \cap B_j$. Como A_i e B_j são abertos, sua interseção é aberto e, como $A_i \subseteq A$ e $B_j \subseteq B$, segue que $A_i \cap B_j \subseteq A \cap B$, e isso implica que $a \in (A \cap B)^\circ$.
4. Como A° é um conjunto aberto, pelo item 2 segue que $(A^\circ)^\circ = A^\circ$. ■

Proposição 13.4. *Sejam X um conjunto e $\mathcal{J} : \wp(X) \longrightarrow \wp(X)$ uma função que satisfaz, para todos $A, B \subseteq X$,*

1. $\mathcal{J}(X) = X$;

2. $\mathcal{I}(A) \subseteq A$;
3. $\mathcal{I}(A \cap B) = \mathcal{I}(A) \cap \mathcal{I}(B)$;
4. $\mathcal{I}(\mathcal{I}(A)) = \mathcal{I}(A)$.

Então o conjunto $\mathcal{T} := \{C \subseteq X \mid C = \mathcal{I}(C)\}$ é uma topologia de X e $\mathcal{I}(C) = C^\circ$ para cada $C \subseteq X$.

Demonstração. Primeiro, notemos que, pela primeira propriedade, $X \in \mathcal{T}$ e, pela segunda propriedade, como $\mathcal{I}(\emptyset) \subseteq \emptyset$, concluímos que $\mathcal{I}(\emptyset) = \emptyset$, o que significa que $\emptyset \in \mathcal{T}$.

Vamos mostrar a seguinte propriedade: para todos $A, B \subseteq X$,

$$A \subseteq B \Rightarrow \mathcal{I}(A) \subseteq \mathcal{I}(B)$$

Supondo que $A \subseteq B$, temos que $A = A \cap B$. Então, pela terceira propriedade, $\mathcal{I}(A) = \mathcal{I}(A) \cap \mathcal{I}(B)$. Assim, segue que $\mathcal{I}(A) \subseteq \mathcal{I}(B)$.

Agora, seja $(A_i)_{i \in I}$ uma família de conjuntos em \mathcal{T} . Então, para cada $j \in I$, $A_j \subseteq \bigcup_{i \in I} A_i$ e, portanto, $\mathcal{I}(A_j) \subseteq \mathcal{I}(\bigcup_{i \in I} A_i)$. Mas a família satisfaz $\mathcal{I}(A_i) = A_i$. Assim, concluímos que

$$\bigcup_{i \in I} \mathcal{I}(A_i) = \bigcup_{i \in I} A_i \subseteq \mathcal{I}\left(\bigcup_{i \in I} A_i\right)$$

Pela segunda propriedade, $\mathcal{I}(\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} A_i$. Portanto $\bigcup_{i \in I} A_i = \mathcal{I}(\bigcup_{i \in I} A_i)$, e concluímos que $\bigcup_{i \in I} A_i \in \mathcal{T}$.

Então, seja $(A_i)_{i \in [n]}$ uma família finita de conjuntos em \mathcal{T} . Usando a terceira propriedade e indução, provaremos que $\bigcap_{i=0}^{n-1} A_i \in \mathcal{T}$. Para 0, a propriedade é trivialmente verdade. Suponhamos que vale para k . Então, pela terceira propriedade,

$$\begin{aligned} \mathcal{I}\left(\bigcap_{i=0}^k A_i\right) &= \mathcal{I}\left(\left(\bigcap_{i=0}^{k-1} A_i\right) \cap A_k\right) \\ &= \mathcal{I}\left(\bigcap_{i=0}^{k-1} A_i\right) \cap \mathcal{I}(A_k) \\ &= \bigcap_{i=0}^{k-1} A_i \cap A_k \\ &= \bigcap_{i=0}^k A_i, \end{aligned}$$

o que mostra que $\bigcap_{i=0}^k A_i \in \mathcal{T}$ e que, para todo $n \in \mathbb{N}$, $\bigcap_{i=0}^{n-1} A_i \in \mathcal{T}$. Logo concluímos que \mathcal{T} é uma topologia de X .

Devemos, por fim, mostrar que $\mathcal{I}(C) = C^\circ$ para todo $C \subseteq X$. Seja $(C_I)_{i \in I}$ uma indexação dos subconjuntos abertos de C . Vamos mostrar primeiro que $C^\circ \subseteq \mathcal{I}(C)$. Para todo $i \in I$, temos que $C_i \subseteq C$ implica $\mathcal{I}(C_i) \subseteq \mathcal{I}(C)$. Como $C_i = \mathcal{I}(C_i)$, segue que $C_i \subseteq \mathcal{I}(C)$ e, portanto,

$$C^\circ = \bigcup_{i \in I} C_i \subseteq \mathcal{I}(C).$$

Por outro lado, notemos que $\mathcal{I}(C)$ é um aberto, pois, pela quarta propriedade, $\mathcal{I}(\mathcal{I}(C)) = \mathcal{I}(C)$. Pela segunda propriedade, $\mathcal{I}(C) \subseteq C$, e segue que $\mathcal{I}(C)$ é um dos subconjuntos abertos C_i de C . Portanto

$$\mathcal{I}(C) \subseteq \bigcup_{i \in I} C_i = C^\circ.$$

■

Proposição 13.5. *Sejam (X, \mathcal{T}) um espaço topológico e $C \subseteq X$. Então*

$$C^\circ = \{x \in X \mid \exists A \in \mathcal{T} \quad x \in A \subseteq C\}$$

Demonstração. Se o único aberto contido em C é \emptyset , então $C^\circ = \emptyset$ e segue que, para todo $x \in X$, todo aberto $A \in \mathcal{T}$ tal que $x \in A$ não está contido em C . Então os conjuntos são iguais. Se $C^\circ = \emptyset$, então o único aberto contido em

Se $x \in C^\circ$, então existe

■

Dualmente, consideraremos agora o conceito de fecho.

Definição 13.4. Sejam (X, \mathcal{T}) um espaço topológico, $C \subseteq X$ e $(F_i)_{i \in I}$ uma indexação do conjunto de todos conjuntos fechados de X dos quais C é subconjunto. O *fecho* de C é o conjunto fechado

$$\overline{C} := \bigcap_{i \in I} F_i.$$

Proposição 13.6. *Seja \mathbf{X} um espaço topológico. Então*

1. *Para todo $A \subseteq X$, $A \subseteq \overline{A}$;*
2. *Um conjunto A é fechado se, e somente se, $\overline{A} = A$;*
3. $\overline{(A \cup B)} = \overline{A} \cup \overline{B}$;
4. $\overline{\overline{A}} = \overline{A}$;

Demonstração. Demonstração análoga à de interior.

■

Proposição 13.7. Sejam X um conjunto e $\mathcal{F} : \wp(X) \longrightarrow \wp(X)$ uma função que satisfaçõe, para todos $A, B \subseteq X$,

1. $\mathcal{F}(\emptyset) = \emptyset$;
2. $A \subseteq \mathcal{F}(A)$;
3. $\mathcal{F}(A \cup B) = \mathcal{F}(A) \cup \mathcal{F}(B)$.
4. $\mathcal{F}(\mathcal{F}(A)) = \mathcal{F}(A)$.

Então o conjunto $\mathbb{C}(\mathcal{T}) := \{C \subseteq X \mid C = \mathcal{F}(C)\}$ é o conjunto de fechados de uma topologia \mathcal{T} de X e $\mathcal{F}(C) = \overline{C}$ para cada $C \subseteq X$.

Demonstração. Demonstração análoga à de interior. ■

Proposição 13.8. Sejam X um espaço topológico e $A \subseteq X$. Então

1. $(\overline{A})^c = (A^c)^\circ$;
2. $(A^\circ)^c = \overline{(A^c)}$.

Demonstração. 1.

2. ■

Fronteira

Definição 13.5. Sejam X um espaço topológico e $C \subseteq X$. A fronteira de C é o conjunto

$$\text{fro } C := \overline{C} \setminus C^\circ.$$

Proposição 13.9. Sejam X um espaço topológico e $C \subseteq X$. Então

1. O fecho é a união disjunta de interior e fronteira.

$$\overline{C} = C^\circ \cup \text{fro } C \quad \text{e} \quad C^\circ \cap \text{fro } C = \emptyset$$

2. A fronteira é a interseção dos fechos do conjunto e de seu complementar.

$$\text{fro } C = \overline{C} \cap \overline{C^c}$$

3. Um conjunto é aberto se, e somente se, não contém pontos da fronteira.

$$C \in \mathcal{T} \Leftrightarrow \text{fro } C \cap C = \emptyset$$

4. Um conjunto é fechado se, e somente se, contém todos pontos da fronteira.

$$C \in \mathbb{C}(\mathcal{T}) \Leftrightarrow \text{fro } C \subseteq C$$

5. A fronteira de um conjunto é fechada.

$$\text{fro } C \in \mathbb{C}(\mathcal{T})$$

6. $\text{fro}(\text{fro}(\text{fro } C)) = \text{fro}(\text{fro } C)$.

Demonstração.

1.

$$\text{fro } C = \overline{C} \setminus C^\circ \Leftrightarrow \overline{C} = C^\circ \cup \text{fro } C$$

2.

3.

$$\text{fro } C = \overline{C} \setminus C^\circ = \overline{C} \cap (C^\circ)^\complement = \overline{C} \cap \overline{C}^\complement$$

■

13.1.2 Topologias Geradas, Bases e Sub-bases

Topologias Finas e Grossas e Topologias Geradas

Definição 13.6. Seja X um conjunto e \mathcal{T} uma topologia de X . Uma *topologia mais grossa* (ou *fraca*) que a topologia \mathcal{T} é uma topologia \mathcal{T}' de X tal que $\mathcal{T}' \subseteq \mathcal{T}$. Uma *topologia mais fina* (ou *forte*) que a topologia \mathcal{T} é uma topologia \mathcal{T}' de X tal que $\mathcal{T} \subseteq \mathcal{T}'$.

A topologia mais fraca é a topologia trivial e a topologia mais forte é a topologia discreta.

Proposição 13.10. Sejam X um conjunto e $(\mathcal{T}_i)_{i \in I}$ uma família de topologias de X . Então

$$\mathcal{T} := \bigcap_{i \in I} \mathcal{T}_i$$

é uma topologia de X .

Demonstração. Primeiro, notemos que, para todo $i \in I$, $\emptyset, X \in \mathcal{T}_i$, e segue que $\emptyset, X \in \mathcal{T}$. Agora, seja $(A_j)_{j \in J} \subseteq \mathcal{T}$. Então, para todo $i \in I$, $(A_j)_{j \in J} \in \mathcal{T}_i$, e segue que $\bigcup_{j \in J} A_j \in \mathcal{T}_i$, o que implica que $\bigcup_{j \in J} A_j \in \mathcal{T}$. Por fim, seja $(A_j)_{j \in [n]} \subseteq \mathcal{T}$. Então, para todo $i \in I$, $(A_j)_{j \in [n]} \in \mathcal{T}_i$, e segue que $\bigcap_{j=0}^{n-1} A_j \in \mathcal{T}_i$, o que implica que $\bigcap_{j=0}^{n-1} A_j \subseteq \mathcal{T}$. ■

Definição 13.7. Sejam X um conjunto, $G \subseteq \wp(X)$ e $(\mathcal{T}_i)_{i \in I}$ uma indexação do conjunto de todas as topologias de X das quais G é subconjunto. A *topologia gerada por G* é a topologia

$$\langle G \rangle := \bigcap_{i \in I} \mathcal{T}_i.$$

Nesse caso, dizemos que G é o *conjunto gerador* de $\langle G \rangle$ ou que G gera $\langle G \rangle$.

Bases e Sub-bases

13.1.3 Funções Contínuas

Definição 13.8. Sejam $\mathbf{X} = (X, \mathcal{T}_X)$ e $\mathbf{Y} = (Y, \mathcal{T}_Y)$ espaços topológicos. Uma *função contínua* de \mathbf{X} para \mathbf{Y} é uma função $f : X \rightarrow Y$ tal que, para todo $A \in \mathcal{T}_Y$,

$$f^{-1}(A) \in \mathcal{T}_X.$$

Denota-se $f : \mathbf{X} \rightarrow \mathbf{Y}$. O conjunto dessas funções é denotado por $\mathcal{C}(\mathbf{X}, \mathbf{Y})$.

Proposição 13.11. (Propriedades categóricas).

1. (*Identidade*) Seja \mathbf{X} um espaço topológico. A função $\text{Id}_X : X \rightarrow X$ é uma função contínua.
2. (*Associatividade*) Sejam \mathbf{X}_0 , \mathbf{X}_1 e \mathbf{X}_2 espaços topológicos e $f_0 : \mathbf{X}_0 \rightarrow \mathbf{X}_1$ e $f_1 : \mathbf{X}_1 \rightarrow \mathbf{X}_2$ funções contínuas. Então $f_1 \circ f_0 : \mathbf{X}_0 \rightarrow \mathbf{X}_2$ é uma função contínua.

$$\begin{array}{ccccc} \mathbf{X}_0 & \xrightarrow{f_0} & \mathbf{X}_1 & \xrightarrow{f_1} & \mathbf{X}_2 \\ & \underbrace{\qquad\qquad\qquad}_{f_1 \circ f_0} & & & \end{array}$$

Demonstração. 1. Seja $A \in \mathcal{T}$. Então $\text{Id}_X^{-1}(A) = A \in \mathcal{T}$, logo Id_X é contínua.

2. Seja $A \in \mathcal{T}_2$. Como f_1 é contínua, $f_1^{-1}(A) \in \mathcal{T}_1$. Como f_0 é contínua, $f_0^{-1}(f_1^{-1}(A)) \in \mathcal{T}_0$. Portanto

$$(f_1 \circ f_0)^{-1}(A) = f_1^{-1} \circ f_0^{-1}(A) = f_0^{-1}(f_1^{-1}(A)) \in \mathcal{T}_0.$$

Logo $f_1 \circ f_0$ é contínua. ■

13.1.4 Topologias Induzidas

Nesta seção estudaremos como induzir topologias em conjuntos a partir de topologias que já temos. Isso será feito, em geral, de modo que uma ou mais funções sejam contínuas e a topologia induzida seja a menor ou a maior possível, dependendo do caso. Quando temos uma função de um conjunto em um espaço topológico, podemos induzir uma topologia nesse conjunto de modo que a topologia faça com que a função seja contínua. Nesse caso, a maior topologia que faz a função ser contínua é a topologia discreta, e o nosso interesse será achar a menor topologia tal que a função é discreta. Quando temos uma função de um espaço topológico em um conjunto, o caso se inverte. A menor topologia tal que a função é contínua sempre é a topologia trivial, e o nosso interesse está na maior topologia que garante a continuidade. De maneira parecida, podemos induzir topologias garantindo a continuidade de várias funções e também considerando funções injetivas e sobrejetivas quando necessário. O estudo desta seção envolve a definição dessas noções e a investigação inicial como sobre esses objetos se comportam e por que são os menores ou maiores com determinadas características.

Topologias Puxada e Inicial

Definição 13.9. Sejam X um conjunto, $\mathbf{Y} = (Y, \mathcal{T}_Y)$ um espaço topológico e $f : X \rightarrow Y$ uma função. A *topologia puxada* por f de \mathbf{Y} para X é

$$f^*(\mathcal{T}_Y) := \left\{ f^{-1}(A) \mid A \in \mathcal{T}_Y \right\}.$$

Proposição 13.12. Sejam X um conjunto, $\mathbf{Y} = (Y, \mathcal{T}_Y)$ um espaço topológico e $f : X \rightarrow Y$ uma função. Então $f^*(\mathcal{T}_Y)$, a topologia puxada por f de \mathbf{Y} para X , é uma topologia de X .

Demonstração. (1) Notemos que, como $\emptyset \in \mathcal{T}_Y$ e $\emptyset = f^{-1}(\emptyset)$, temos que $\emptyset \in f^*(\mathcal{T}_Y)$. (2) Seja $(A_i)_{i \in I}$ uma família de conjuntos em $f^*(\mathcal{T}_Y)$. Então, para cada $i \in I$, existe aberto $U_i \in \mathcal{T}_Y$ tal que $A_i = f^{-1}(U_i)$. Como \mathcal{T}_Y é topologia, a união de abertos é aberto $\bigcup_{i \in I} U_i \in \mathcal{T}_Y$. Portanto

$$\bigcup_{i \in I} A_i = \bigcup_{i \in I} f^{-1}(U_i) = f^{-1}\left(\bigcup_{i \in I} U_i\right),$$

logo $\bigcup_{i \in I} A_i \in f^*(\mathcal{T}_Y)$. (3) Seja $(A_i)_{i=1}^n$ uma família de conjuntos em $f^*(\mathcal{T}_Y)$. Então, para cada $1 \leq i \leq n$, existe aberto $U_i \in \mathcal{T}_Y$ tal que $A_i = f^{-1}(U_i)$. Como \mathcal{T}_Y é topologia, a interseção finita de abertos é aberto $\bigcap_{i=1}^n U_i \in \mathcal{T}_Y$. Portanto

$$\bigcap_{i=1}^n A_i = \bigcap_{i=1}^n f^{-1}(U_i) = f^{-1}\left(\bigcap_{i=1}^n U_i\right),$$

logo $\bigcap_{i=1}^n A_i \in f^*(\mathcal{T}_Y)$. ■

Proposição 13.13. Sejam $\mathbf{X} = (X, \mathcal{T}_X)$ e $\mathbf{Y} = (Y, \mathcal{T}_Y)$ espaços topológicos. Uma função $f : X \rightarrow Y$ é função contínua de \mathbf{X} para \mathbf{Y} se, e somente se, a topologia $f^*(\mathcal{T}_Y)$ puxada por f de \mathbf{Y} para X é uma subtopologia de \mathcal{T}_X .

$$f \in \mathcal{C}(\mathbf{X}, \mathbf{Y}) \iff f^*(\mathcal{T}_Y) \subseteq \mathcal{T}_X.$$

Demonstração. Suponha que $f \in \mathcal{C}(\mathbf{X}, \mathbf{Y})$ e seja $B \in f^*(\mathcal{T}_Y)$. Então existe $A \in \mathcal{T}_Y$ tal que $B = f^{-1}(A)$. Como f é contínua, segue que $f^{-1}(A) \in \mathcal{T}_X$, portanto, $f^*(\mathcal{T}_Y) \subseteq \mathcal{T}_X$. Reciprocamente, suponha que $f^*(\mathcal{T}_Y) \subseteq \mathcal{T}_X$. Então, para todo $A \in \mathcal{T}_Y$, $f^{-1}(A) \in f^*(\mathcal{T}_Y)$, portanto $f^{-1}(A) \in \mathcal{T}_X$, o que mostra que $f \in \mathcal{C}(\mathbf{X}, \mathbf{Y})$. ■

Definição 13.10. Sejam \mathbf{X} um conjunto, $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{T}_i)_{i \in I}$ uma família de espaços topológicos e, para todo $i \in I$, $f_i : X \rightarrow X_i$ uma função. A *topologia inicial* de X com respeito à família $(f_i)_{i \in I}$ é a menor topologia de X tal que, para todo $i \in I$, f_i é contínua.

Proposição 13.14. Sejam \mathbf{X} um conjunto, $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{T}_i)_{i \in I}$ uma família de espaços topológicos e, para todo $i \in I$, $f_i : X \rightarrow X_i$ uma função. A *topologia inicial* de X com respeito à família $(f_i)_{i \in I}$ é a topologia

$$\left\langle \bigcup_{i \in I} f_i^*(\mathcal{T}_i) \right\rangle.$$

Demonstração. Seja \mathcal{T} uma topologia de X tal que, para todo $i \in I$, $f_i : X \rightarrow X_i$ é contínua. Então, para todo $i \in I$, $f_i^*(\mathcal{T}_i) \subseteq \mathcal{T}$ (13.13), o que implica que $\bigcup_{i \in I} f_i^*(\mathcal{T}_i) \subseteq \mathcal{T}$ e, portanto, $\langle \bigcup_{i \in I} f_i^*(\mathcal{T}_i) \rangle \subseteq \mathcal{T}$. ■

Topologias Empurrada e Final

Definição 13.11. Sejam $\mathbf{X} = (X, \mathcal{T}_X)$ um espaço topológico, Y um conjunto e $f : X \rightarrow Y$ uma função. A *topologia empurrada* por f de \mathbf{X} para Y é

$$f_*(\mathcal{T}_X) := \left\{ A \subseteq Y \mid f^{-1}(A) \in \mathcal{T}_X \right\}.$$

Proposição 13.15. Sejam $\mathbf{X} = (X, \mathcal{T}_X)$ um espaço topológico, Y um conjunto e $f : X \rightarrow Y$ uma função. Então $\mathcal{T}_Y := f_*(\mathcal{T}_X)$, a topologia empurrada por f de \mathbf{X} para Y , é uma topologia de Y .

Demonstração. (1) Como $f^{-1}(\emptyset) = \emptyset$ e $f^{-1}(Y) = X$, segue que $\emptyset, Y \in f_*(\mathcal{T}_X)$.
(2) Seja $(A_i)_{i \in I}$ uma família de conjuntos de $f_*(\mathcal{T}_X)$. Então, para cada $i \in I$, $f^{-1}(A_i) \in \mathcal{T}_X$, o que implica que

$$f^{-1} \left(\bigcup_{i \in I} A_i \right) = \bigcup_{i \in I} f^{-1}(A_i) \in \mathcal{T}_X,$$

portanto $\bigcup_{i \in I} A_i \in f_*(\mathcal{T}_X)$. (3) Seja $(A_i)_{i=1}^n$ uma família de conjuntos de $f_*(\mathcal{T}_X)$. Então, para cada $1 \leq i \leq n$, $f^{-1}(A_i) \in \mathcal{T}_X$, o que implica que

$$f^{-1}\left(\bigcap_{i=1}^n A_i\right) = \bigcap_{i=1}^n f^{-1}(A_i) \in \mathcal{T}_X,$$

portanto $\bigcap_{i=1}^n A_i \in f_*(\mathcal{T}_X)$. ■

Definição 13.12. Sejam \mathbf{X} um conjunto, $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{T}_i)_{i \in I}$ uma família de espaços topológicos e, para todo $i \in I$, $f_i : X_i \rightarrow X$ uma função. A *topologia final* de X com respeito à família $(f_i)_{i \in I}$ é a maior topologia de X tal que, para todo $i \in I$, f_i é contínua.

Proposição 13.16. Sejam \mathbf{X} um conjunto, $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{T}_i)_{i \in I}$ uma família de espaços topológicos e, para todo $i \in I$, $f_i : X_i \rightarrow X$ uma função. A topologia final de X com respeito à família $(f_i)_{i \in I}$ é a topologia

$$\bigcap_{i \in I} f_{i*}(\mathcal{T}_i).$$

Demonstração. Seja \mathcal{T} uma topologia de X tal que, para todo $i \in I$, $f_i : X_i \rightarrow X$ é contínua, e seja $A \in \mathcal{T}$. Então, para todo $i \in I$, $f_i^{-1}(A) \in \mathcal{T}_i$, o que implica que $A \in f_{i*}(\mathcal{T}_i)$, portanto $A \in \bigcap_{i \in I} f_{i*}(\mathcal{T}_i)$. Isso mostra que $\mathcal{T} \subseteq \bigcap_{i \in I} f_{i*}(\mathcal{T}_i)$, e como interseção de topologias é topologia, segue o procurado. ■

Produto de Espaços Topológicos

Definição 13.13. Seja $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{T}_i)_{i \in I}$ uma família de espaços topológicos. O *produto* da família $(\mathbf{X}_i)_{i \in I}$ é o par

$$\prod_{i \in I} \mathbf{X}_i := \left(\prod_{i \in I} X_i, \left\langle \bigcup_{i \in I} \pi_i^*(\mathcal{T}_i) \right\rangle \right).$$

A topologia $\langle \bigcup_{i \in I} \pi_i^*(\mathcal{T}_i) \rangle$ é a *topologia produto* de $\prod_{i \in I} X_i$.

Proposição 13.17. Sejam $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{T}_i)_{i \in I}$ uma família de espaços topológicos e $X = \prod_{i \in I} X_i$ o produto de conjuntos. A topologia produto de X é a topologia gerada pela base cujos elementos são $\prod_{i \in I} A_i$, tal que $A_i \in \mathcal{T}_i$ e existe $J \subseteq I$ finito com $A_i = X_i$ para $i \in I \setminus J$.

Demonstração. Como $\pi_i = \pi_i \circ \text{Id}_X$, segue de uma propriedade básica de imagem inversa de produto (2.8) que

$$\prod_{i \in I} A_i = \text{Id}_X^{-1} \left(\prod_{i \in I} A_i \right) = \bigcap_{i \in I} \pi_i^{-1}(A_i)$$

Para todo $i \in I \setminus J$, $A_i = X_i$, então $\pi_i^{-1}(A_i) = X$ e, portanto,

$$\bigcap_{i \in I \setminus J} \pi_i^{-1}(A_i) = \bigcap_{i \in I \setminus J} X = X.$$

Isso implica que

$$\bigcap_{i \in I} \pi_i^{-1}(A_i) = \left(\bigcap_{i \in I \setminus J} \pi_i^{-1}(A_i) \right) \cap \left(\bigcap_{j \in J} \pi_j^{-1}(A_j) \right) = \bigcap_{j \in J} \pi_j^{-1}(A_j)$$

Logo $\prod_{i \in I} A_i = \bigcap_{j \in J} \pi_j^{-1}(A_j)$. Seja A aberto da topologia descrita na proposição. Então

$$A = \bigcup_{k \in K} A_k = \bigcup_{k \in K} \prod_{i \in I} A_{ki} = \bigcup_{k \in K} \bigcap_{j \in J} \pi_j^{-1}(A_{kj}),$$

o que mostra que A é aberto da topologia produto. O resto da demonstração é simples. \blacksquare

Proposição 13.18 (Propriedade Universal). *Sejam $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{T}_i)_{i \in I}$ uma família de espaços topológicos, $\mathbf{T} = (T, \mathcal{T}_T)$ um espaço topológico e, para todo $i \in I$, $f_i : \mathbf{T} \rightarrow \mathbf{X}_i$ uma função contínua. Então existe uma única função contínua $f : \mathbf{T} \rightarrow \prod_{i \in I} \mathbf{X}_i$ tal que, para todo $i \in I$, $\pi_i \circ f = f_i$ (o diagrama comuta).*

$$\begin{array}{ccc} & \prod_{i \in I} \mathbf{X}_i & \\ f \swarrow & \nearrow \pi_i & \\ \mathbf{T} & \xrightarrow{f_i} & \mathbf{X}_i \end{array}$$

Definição 13.14. Defina a função

$$\begin{aligned} f : T &\longrightarrow \prod_{i \in I} X_i \\ x &\longmapsto (f_i(x))_{i \in I}. \end{aligned}$$

Pela propriedade universal do produto de conjuntos, f é única e $\pi_i \circ f = f_i$. Resta mostrar que f é contínua. Seja $A \in \mathcal{T}_X$. Então $A = \bigcup_{k \in K} A_k$ é uma união de abertos básicos $A_k \in \mathcal{T}$. Isso significa que, para todo $k \in K$, $A_k = \prod_{i \in I} A_{ki}$, com $A_{ki} \in \mathcal{T}_i$ para todo $i \in I$ e existe $J_k \subseteq I$ finito tal que, para todo $i \in I \setminus J_k$,

$A_{ki} = X_i$. Assim, por propriedades básicas de imagem inversa de união e produto (2.8),

$$f^{-1}(A) = f^{-1}\left(\bigcup_{k \in K} \prod_{i \in I} A_{ki}\right) = \bigcup_{k \in K} f^{-1}\left(\prod_{i \in I} A_{ki}\right) = \bigcup_{k \in K} \bigcap_{i \in I} f_i^{-1}(A_{ki}).$$

Seja $k \in K$. Como, para todo $i \in I \setminus J_k$, $A_{ki} = X_i$, então $f_i^{-1}(A_{ki}) = f_i^{-1}(X_i) = T$. Disso segue que

$$\bigcap_{i \in I} f_i^{-1}(A_{ki}) = \bigcap_{j \in J_k} f_j^{-1}(A_{kj})$$

e, portanto,

$$f^{-1}(A) = \bigcup_{k \in K} \bigcap_{j \in J_k} f_j^{-1}(A_{kj}).$$

Seja $k \in K$. Para todo $j \in J_k$, f_j é contínua, o que implica que $f_j^{-1}(A_{kj})$ é aberto e, por J_k ser finito, a interseção $\bigcap_{j \in J_k} f_j^{-1}(A_{kj})$ é aberta. Isso significa que a união $\bigcup_{k \in K} \bigcap_{j \in J_k} f_j^{-1}(A_{kj})$ é aberta e, portanto, $f^{-1}(A) \in \mathcal{T}_T$. Logo f é contínua.

Coproduto de Espaços Topológicos

Definição 13.15. Seja $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{T}_i)_{i \in I}$ uma família de espaços topológicos. O *coproduto* da família $(\mathbf{X}_i)_{i \in I}$ é o par

$$\bigsqcup_{i \in I} \mathbf{X}_i := \left(\bigsqcup_{i \in I} X_i, \bigcap_{i \in I} \iota_{i*}(\mathcal{T}_i) \right).$$

A topologia $\bigcap_{i \in I} \pi_{i*}(\mathcal{T}_i)$ é a *topologia coproduto* de $\bigsqcup_{i \in I} X_i$.

Proposição 13.19 (Propriedade Universal). *Sejam $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{T}_i)_{i \in I}$ uma família de espaços topológicos, $\mathbf{T} = (T, \mathcal{T}_T)$ um espaço topológico e, para todo $i \in I$, $f_i : \mathbf{X}_i \rightarrow \mathbf{T}$ uma função contínua. Então existe uma única função contínua $f : \bigsqcup_{i \in I} \mathbf{X}_i \rightarrow \mathbf{T}$ tal que, para todo $i \in I$, $f \circ \iota_i = f_i$ (o diagrama comuta).*

$$\begin{array}{ccc} \bigsqcup_{i \in I} \mathbf{X}_i & & \\ \iota_i \uparrow & \swarrow f & \\ \mathbf{X}_i & \xrightarrow{f_i} & \mathbf{T} \end{array}$$

Subespaços Topológicos

Definição 13.16. Sejam (X, \mathcal{T}) um espaço topológico e $S \subseteq X$ um subconjunto. A *topologia induzida* por \mathcal{T} em S é o conjunto

$$\mathcal{T}|_S := \{A \cap S \mid A \in \mathcal{T}\}.$$

Proposição 13.20. Sejam (X, \mathcal{T}) um espaço topológico e $S \subseteq X$ um subconjunto. A *topologia induzida* por \mathcal{T} em S é o conjunto

$$\mathcal{T}|_S = \iota_*(\mathcal{T}),$$

a maior topologia tal que a inclusão $\iota : S \rightarrow X$ é contínua.

Proposição 13.21. Sejam (X, \mathcal{T}) um espaço topológico e $S \subseteq X$ um subconjunto. A *topologia induzida* por \mathcal{T} em S é uma topologia de S .

Demonstração. (1) Notemos que $\emptyset, Y \in \mathcal{T}|_Y$, pois $\emptyset \cap Y = \emptyset$ e $X \cap Y = Y$. (2) Seja $(A_i)_{i \in I}$ uma família de abertos de $\mathcal{T}|_Y$. Então, para cada $i \in I$, existe um aberto $B_i \in \mathcal{T}$ tal que $A_i = B_i \cap Y$. Assim, temos que

$$\bigcup_{i \in I} A_i = \bigcup_{i \in I} (B_i \cap Y) = \left(\bigcup_{i \in I} B_i \right) \cap Y,$$

que pertence à topologia induzida pois $\bigcup_{i \in I} B_i \in \mathcal{T}$. (3) Seja $(A_i)_{i=1}^n$ uma família de abertos de $\mathcal{T}|_Y$. Então, para cada $1 \leq i \leq n$, existe um aberto $B_i \in \mathcal{T}$ tal que $A_i = B_i \cap Y$. Assim, temos que

$$\bigcap_{i=1}^n A_i = \bigcap_{i=1}^n (B_i \cap Y) = \left(\bigcap_{i=1}^n B_i \right) \cap Y,$$

que pertence à topologia induzida pois $\bigcap_{i=1}^n B_i \in \mathcal{T}$. ■

Proposição 13.22 (Propriedade característica). Sejam $\mathbf{X} = (X, \mathcal{T}_X)$ e (Y, \mathcal{T}_Y) espaços topológicos e $S \subseteq \mathbf{X}$ um subespaço. Uma função $f : Y \rightarrow S$ é contínua se, e somente se, $\iota \circ f : Y \rightarrow X$ é contínua (o diagrama comuta).

$$\begin{array}{ccc} & \mathbf{X} & \\ & \downarrow \iota & \\ \mathbf{T} & \xrightarrow{f} & S \end{array}$$

$\iota \circ f$

Proposição Restrição de função contínua é contínua na topologia induzida.

Proposição 13.23 (Colagem por abertos). *Sejam \mathbf{X} e \mathbf{Y} espaços topológicos, $f : X \rightarrow Y$ uma função e $(X_i)_{i \in I}$ uma cobertura de X por conjuntos abertos tal que, para todo $i \in I$, $f|_{X_i} : X_i \rightarrow Y$ é contínua. Então $f : X \rightarrow Y$ é contínua.*

Proposição 13.24 (Colagem por fechados). *Sejam \mathbf{X} e \mathbf{Y} espaços topológicos, $f : X \rightarrow Y$ uma função e $(X_i)_{i=1}^n$ uma cobertura de X por conjuntos fechados tal que, para todo $1 \leq i \leq n$, $f|_{X_i} : X_i \rightarrow Y$ é contínua. Então $f : X \rightarrow Y$ é contínua.*

Quociente de Espaços Topológicos

Definição 13.17. Sejam $\mathbf{X} = (X, \mathcal{T})$ um espaço topológico e \sim uma relação de equivalência em X . O espaço quociente com respeito a \sim é o espaço topológico

$$\mathbf{X}/\sim := (X/\sim, \pi^*(\mathcal{T})),$$

em que $\pi : X \rightarrow X/\sim$ é a projeção canônica de equivalências.

É fácil notar que os abertos de \mathbf{X}/\sim são conjuntos de classes de equivalência cuja união é um aberto de \mathbf{X} . Notemos, ainda, que se $f : X \rightarrow Y$ é sobrejetivo, existe uma relação de equivalência em X induzida por f , definida como dois elementos são equivalentes se suas imagens são iguais, e essa relação de equivalência faz com que possamos identificar Y com X/\sim como conjuntos. Definimos a topologia em Y de modo que Y e X/\sim sejam homeomorfos.

Proposição 13.25 (Propriedade característica). *Sejam $\mathbf{X} = (X, \mathcal{T}_X)$ e (Y, \mathcal{T}_Y) espaços topológicos e \mathbf{Q} um espaço quociente de \mathbf{X} . Uma função $f : Q \rightarrow Y$ é contínua se, e somente se, $f \circ \pi : X \rightarrow Y$ é contínua (o diagrama comuta).*

$$\begin{array}{ccc} \mathbf{X} & & \\ \downarrow \pi & \searrow f \circ \pi & \\ \mathbf{Q} & \xrightarrow{f} & \mathbf{Y} \end{array}$$

13.2 Separação

13.2.1 Noções de Separação de Conjuntos

Nesta seção são apresentadas algumas noções de como dois conjuntos de um espaço topológico podem ser separadas. As duas noções mais simples de separação são

noções conjuntistas. A primeira é a de conjuntos distintos, ou diferentes, $A \neq B$, e a outra é a de conjuntos disjuntos, $A \cap B = \emptyset$. A seguir, mostramos noções que envolvem construções topológicas e não meramente conjuntistas.

Definição 13.18. Sejam X um espaço topológico e $A, B \subseteq X$. Definimos as seguintes relações entre A e B :

1. (*Separação*) Cada conjunto é disjunto do feixe do outro.

$$A \cap \overline{B} = \overline{A} \cap B = \emptyset.$$

2. (*Separação por vizinhanças*) Existem vizinhanças $V_A \in \mathcal{V}_A$ e $V_B \in \mathcal{V}_B$ que são disjuntas.

$$V_A \cap V_B = \emptyset.$$

3. (*Separação por função contínua*) Existe uma função contínua $f \in \mathscr{C}(X, [0, 1])$ tal que

$$f(A) = \{0\} \text{ e } f(B) = \{1\}.$$

4. (*Separação precisa por função contínua*) Existe uma função contínua $f \in \mathscr{C}(X, [0, 1])$ tal que

$$f^{-1}(\{0\}) = A \text{ e } f^{-1}(\{1\}) = B.$$

Cada uma das relações vale entre pontos $x, y \in X$, ou entre um conjunto A e um ponto x , ao considerarmos no lugar no ponto o conjunto unitário que o contém: valem entre os conjuntos $\{x\}$ e $\{y\}$, ou entre A e $\{x\}$, respectivamente.

As primeiras duas relações binárias são claramente simétricas, mas isso não é necessariamente claro no caso da terceira e quarta. No entanto, isso pode ser concluído ao considerar, dada uma função f que faz A e B separados por função contínua, a função $1 - f$ que faz o mesmo entre B e A .

Proposição 13.26. *Sejam X um espaço topológico e $A, B \subseteq X$. Então*

1. *Se A e B são precisamente separados por função contínua, então são separados por função contínua.*
2. *Se A e B são separados por função contínua, então são separados por vizinhanças.*
3. *Se A e B são separados por vizinhanças, então são separados.*
4. *Se A e B são separados, então são disjuntos.*

13.2.2 Espaços Distinguíveis

Definição 13.19. Seja \mathbf{X} um espaço topológico. Pontos *topologicamente indistinguíveis* em \mathbf{X} são pontos $x, y \in X$ tais que $\mathcal{V}_x = \mathcal{V}_y$. Pontos *topologicamente disntinguíveis* em \mathbf{X} são pontos que não são topologicamente indistinguíveis.

Proposição 13.27. Seja \mathbf{X} um espaço topológico. A relação binária de indistin-gibilidade topológica é uma relação de equivalência em X .

Demonstração. Denotemos por \sim a relação binária de indistinguibilidade topológica. Sejam $x, y, z \in X$. Para mostrar a reflexividade, notemos que, como $\mathcal{V}_x = \mathcal{V}_y$, então $x \sim x$. Para mostrar a simetria, se $x \sim y$, então $\mathcal{V}_x = \mathcal{V}_y$, o que é equivalente a $\mathcal{V}_y = \mathcal{V}_x$ e, portanto, $y \sim x$. Por fim, para mostrar a transitividade, se $x \sim y$ e $y \sim z$, então $\mathcal{V}_x = \mathcal{V}_y$ e $\mathcal{V}_y = \mathcal{V}_z$, o que implica $\mathcal{V}_x = \mathcal{V}_z$ e, portanto, $x \sim z$. ■

O fato de que essa é uma relação de equivalência mostra que podemos obter a partir de qualquer espaço topológico um espaço topológico em que nenhum ponto é topologicamente indistinguível. Para isso, basta considerar o espaço quociente definido pela relação. de indistinguibilidade topológica. Espaços com essa propriedade são definidos a seguir.

Definição 13.20 (T_0). Um espaço topológico *distinguível* é um espaço topológico \mathbf{X} em que todo par de pontos distintos é topologicamente distinguível:

$$\forall x, y \in X \quad x \neq y \quad \Rightarrow \quad \mathcal{V}_x \neq \mathcal{V}_y.$$

Proposição 13.28. Seja \mathbf{X} um espaço topológico. São equivalentes as seguintes propriedades:

1. \mathbf{X} é dinstinguível.
2. $\forall x, y \in X \quad x \neq y \quad \Rightarrow \quad \mathcal{V}_x \not\subseteq \mathcal{V}_y \text{ ou } \mathcal{V}_y \not\subseteq \mathcal{V}_x.$
3. $\forall x, y \in X \quad x \neq y \quad \Rightarrow \quad x \notin \overline{\{y\}} \text{ ou } y \notin \overline{\{x\}}.$
4. $\forall x, y \in X \quad x \neq y \quad \Rightarrow \quad \overline{\{x\}} \neq \overline{\{y\}}.$

Proposição 13.29. Sejam \mathbf{X} um espaço topológico distinguível e $Y \subseteq X$. Então \mathbf{Y} é um espaço topológico distinguível.

Proposição 13.30. Seja $(X_i)_{i \in I}$ uma família não vazia de espaços topológicos não vazios. O espaço produto $\prod_{i \in I} \mathbf{X}_i$ é distinguível se, e somente se, todos os espaços \mathbf{X}_i são distinguíveis.

13.2.3 Espaços Acessíveis

Definição 13.21 (T_1). Um espaço topológico *acessível* é um espaço topológico \mathbf{X} em que

$$\forall x, y \in X \quad x \neq y \quad \Rightarrow \quad \mathcal{V}_x \not\subseteq \mathcal{V}_y \text{ e } \mathcal{V}_y \not\subseteq \mathcal{V}_x.$$

Proposição 13.31 ($T_1 \Rightarrow T_0$). Seja \mathbf{X} um espaço topológico. Se \mathbf{X} é acessível, então \mathbf{X} é distinguível.

Demonstração. Se \mathbf{X} é acessível, então, para todos $x, y \in X$ tais que $x \neq y$, temos que $\mathcal{V}_x \not\subseteq \mathcal{V}_y$ e $\mathcal{V}_y \not\subseteq \mathcal{V}_x$. Mas isso implica que $\mathcal{V}_x \not\subseteq \mathcal{V}_y$ ou $\mathcal{V}_y \not\subseteq \mathcal{V}_x$, o que é equivalente a $\mathcal{V}_x \neq \mathcal{V}_y$. Logo \mathbf{X} é distinguível. ■

Proposição 13.32. Seja \mathbf{X} um espaço topológico. São equivalentes as seguintes propriedades:

1. \mathbf{X} é acessível.
2. Todo par de pontos distintos é separado:

$$\forall x, y \in X \quad x \neq y \quad \Rightarrow \quad x \notin \overline{\{y\}} \text{ e } y \notin \overline{\{x\}}.$$

3. $\forall x, y \in X \quad x \neq y \quad \Rightarrow \quad \exists U \in \mathcal{V}_x, V \in \mathcal{V}_y \quad y \notin U \text{ e } x \notin V.$
4. $\forall x \in X \quad \overline{\{x\}} = \{x\}.$

Proposição 13.33. Sejam \mathbf{X} um espaço topológico acessível e $Y \subseteq X$. Então \mathbf{Y} é um espaço topológico acessível.

Proposição 13.34. Seja $(X_i)_{i \in I}$ uma família não vazia de espaços topológicos não vazios. O espaço produto $\prod_{i \in I} \mathbf{X}_i$ é acessível se, e somente se, todos os espaços \mathbf{X}_i são acessíveis.

13.2.4 Espaços Separados por Vizinhanças

Definição 13.22 (T_2). Um espaço topológico *separado por vizinhanças* é um espaço topológico \mathbf{X} em que todo par de pontos distintos é separado por vizinhanças:

$$\forall x, y \in X \quad x \neq y \quad \Rightarrow \quad \exists U \in \mathcal{V}_x, V \in \mathcal{V}_y \quad U \cap V = \emptyset.$$

Esses espaços também são conhecidos como espaços de Hausdorff.

Proposição 13.35 ($T_2 \Rightarrow T_1$). Seja \mathbf{X} um espaço topológico. Se \mathbf{X} é separado por vizinhanças, então \mathbf{X} é acessível.

Proposição 13.36. *Seja \mathbf{X} um espaço topológico. São equivalentes as seguintes propriedades:*

1. \mathbf{X} é separado por vizinhanças.
2. Toda rede convergente em \mathbf{X} tem limite único.
3. Todo filtro convergente em \mathbf{X} tem limite único.

Proposição 13.37. *Sejam \mathbf{X} um espaço topológico separado por vizinhanças e $Y \subseteq X$. Então \mathbf{Y} é um espaço topológico separado por vizinhanças.*

Proposição 13.38. *Seja $(\mathbf{X}_i)_{i \in I}$ uma família não vazia de espaços topológicos não vazios. O espaço produto $\prod_{i \in I} \mathbf{X}_i$ é separado por vizinhanças se, e somente se, todos os espaços \mathbf{X}_i são separados por vizinhanças.*

Proposição 13.39. *Sejam \mathbf{X} um espaço topológico, \mathbf{Y} um espaço topológico separado por vizinhanças, $D \subseteq X$ um subconjunto denso em X e $f, g : X \rightarrow Y$ funções contínuas tais que $f|_D = g|_D$. Então $f = g$.*

13.2.5 Espaços Regulares

Definição 13.23. Um espaço topológico *regular* é um espaço topológico em que é possível separar por vizinhanças qualquer ponto de qualquer conjunto fechado que não o contém.

Espaços separados regulares são também chamados de T_3 .

Proposição 13.40. *Seja \mathbf{X} um espaço topológico regular. Então \mathbf{X} é separado por vizinhanças se, e somente se, é distinguível.*

Demonstração. Sabemos que todo espaço separado por vizinhanças é distinguível. Para demonstrar a recíproca, supondo que \mathbf{X} é distinguível, então para todos pontos $x, y \in X$, $x \notin \overline{\{y\}}$ ou $y \notin \overline{\{x\}}$. Sem perda de generalidade, assumamos o primeiro caso. Seja $F := \overline{\{y\}}$. Então F é fechado e $x \notin F$. Da regularidade de \mathbf{X} , segue que existem $U \in \mathcal{V}_x$ e $V \in \mathcal{V}_F$ tais que $U \cap V = \emptyset$. Como $y \in F$, então $V \in \mathcal{V}_y$, o que implica que \mathbf{X} é separado por vizinhanças. ■

Proposição 13.41. *Seja \mathbf{X} um espaço topológico. São equivalentes as seguintes propriedades:*

1. \mathbf{X} é regular.
2. Para todos ponto $x \in X$ e aberto $A \in \mathcal{V}_x$, existe aberto $V \in \mathcal{V}_x$ tal que

$$x \in V \subseteq \overline{V} \subseteq A.$$

Proposição 13.42. *Sejam \mathbf{X} um espaço topológico regular e $Y \subseteq X$. Então \mathbf{Y} é um espaço topológico regular.*

Proposição 13.43. *Seja $(X_i)_{i \in I}$ uma família não vazia de espaços topológicos não vazios. O espaço produto $\prod_{i \in I} \mathbf{X}_i$ é regular se, e somente se, todos os espaços \mathbf{X}_i são regulares.*

13.2.6 Espaços Completamente Regulares

Definição 13.24. Um espaço topológico *completamente regular* é um espaço topológico em que é possível separar por função contínua qualquer ponto de qualquer conjunto fechado que não o contém.

Proposição 13.44. *Seja \mathbf{X} um espaço topológico. Se \mathbf{X} é completamente regular, então \mathbf{X} é regular.*

Proposição 13.45. *Sejam \mathbf{X} um espaço topológico completamente regular e $Y \subseteq X$. Então \mathbf{Y} é um espaço topológico completamente regular.*

Proposição 13.46. *Seja $(X_i)_{i \in I}$ uma família não vazia de espaços topológicos não vazios. O espaço produto $\prod_{i \in I} \mathbf{X}_i$ é completamente regular se, e somente se, todos os espaços \mathbf{X}_i são completamente regulares.*

13.2.7 Espaços Normais

Definição 13.25. Um espaço topológico *normal* é um espaço topológico em que todo par de conjuntos fechados disjuntos é separado por vizinhanças.

Espaços normais separados por vizinhanças são também chamados de T_4 .

Proposição 13.47. *Seja \mathbf{X} um espaço topológico normal. Então \mathbf{X} é separado por vizinhanças se, e somente se, é acessível.*

Demonstração. Sabemos que todo espaço separado por vizinhanças é distinguível. Para demonstrar a recíproca, suponhamos que \mathbf{X} é acessível e sejam $x, y \in X$ tais que $x \neq y$. Então vale que $\overline{\{x\}} = \{x\}$ e $\overline{\{y\}} = \{y\}$. Como $x \neq y$, da normalidade de \mathbf{X} existem $V_x \in \mathcal{V}_x$ e $V_y \in \mathcal{V}_y$ tais que $V_x \cap V_y = \emptyset$; ou seja, \mathbf{X} é separado por vizinhanças. ■

Proposição 13.48. *Sejam \mathbf{X} um espaço topológico normal e $Y \subseteq X$ fechado. Então \mathbf{Y} é um espaço topológico normal.*

Proposição 13.49. *Seja \mathbf{X} um espaço topológico. São equivalentes as seguintes propriedades:*

1. \mathbf{X} é normal.

2. Para todos fechado F e aberto $A \in \mathcal{V}_F$, existe aberto $V \in \mathcal{V}_F$ tal que

$$F \subseteq V \subseteq \overline{V} \subseteq A.$$

Proposição 13.50 (Lema de Urysohn). *Um espaço topológico \mathbf{X} é normal se, e somente se, todo par de conjuntos fechados disjuntos é separado por função contínua.*

Demonstração. Se todo par de conjuntos fechados é separado por função contínua, segue da proposição 13.26 que eles são separados por vizinhanças.

Para demonstrar a recíproca, suponhamos que \mathbf{X} é normal. Sejam $F_0, F_1 \subseteq X$ conjuntos fechados disjuntos. Seja $Q := \mathbb{Q} \cap [0, 1]$. Construiremos uma família de abertos $(A_q)_{q \in Q}$ com a seguinte propriedade:

- Se $p, q \in Q$ são racionais tais que $p < q$, então $\overline{A_p} \subseteq A_q$.

Consideremos uma enumeração de $r : \mathbb{N} \longrightarrow Q$ tal que $r(0) = 0$ e $r(1) = 1$, de modo que possamos fazer indução nos elementos de Q . Definimos $A_1 := F_1^c$ e notamos que $F_0 \subseteq A_1$, pois F_0 e F_1 são disjuntos. Como \mathbf{X} é normal e $F_0 \subseteq A_1$, existe aberto A_0 tal que

$$F_0 \subseteq A_0 \subseteq \overline{A_0} \subseteq A_1.$$

Mostremos por indução que para todo $q \in Q$ existe A_q com a propriedade enunciada. O caso base já está mostrado pela construção de A_0 e A_1 , então consideremos o passo indutivo. Seja $Q_n := \{r(k) \mid k \in \{0, \dots, n\}\}$ e suponha que $\overline{A_p} \subseteq A_q$ para todos racionais $p, q \in Q_n$ tais que $p < q$. Consideremos $r = r(n+1) \in Q$. O conjunto Q_{n+1} é um subconjunto finito de Q e, com essa ordem, todo elemento do conjunto tem um antecessor e um sucessor imediatos. Sejam $p, q \in Q_{n+1}$ tais racionais satisfazendo $p < r < q$. Os conjuntos abertos A_p e A_q já estão definidos pela hipótese de indução, então pela normalidade segue que existe aberto $A_r \subseteq X$ tal que

$$\overline{A_p} \subseteq A_r \subseteq \overline{A_r} \subseteq A_q.$$

Mostremos que a propriedade vale para todos elementos de Q_{n+1} . Se $p, q \in Q_n$, a propriedade vale. Consideremos $r = r(n+1)$ e $s \in Q_n$. Se $s < r(n+1)$, então $s \leq p$, portanto $\overline{A_s} \subseteq \overline{A_p} \subseteq A_r$, e se $r(n+1) < s$, então $q \leq s$, portanto $\overline{A_r} \subseteq A_q \subseteq A_s$. Assim isso vale para todo Q_n e portanto para Q , e construímos uma família $(A_q)_{q \in Q}$ satisfazendo a propriedade.

Definamos agora a função

$$\begin{aligned} f : X &\longrightarrow [0, 1] \\ x &\longmapsto \inf \{q \in Q \mid x \in A_q\}. \end{aligned}$$

A função f separa F_0 e F_1 : por definição, $F_0 \subseteq A_0$, portanto $f(F_0) = \{0\}$; ainda, por definição, para todo $q \in Q$, tem-se $A_q \subseteq A_1 = F_1^c$, portanto $f(F_1) = \{1\}$. Para mostrar que f é contínua, notemos antes dois fatos. (1) Para todo $q \in Q$, se $x \in \overline{A_q}$ então $f(x) \leq q$. Isso ocorre porque, se $x \in \overline{A_q}$, então $x \in A_r$ para todo $r \in \mathbb{Q} \cap]q, 1]$, portanto $\{q \in Q \mid x \in A_q\} \subseteq \mathbb{Q} \cap]q, 1]$ o que implica $f(x) \leq q$ por definição de f . (2) Para todo $q \in Q$, se $x \notin A_q$ então $f(x) \geq q$. Isso ocorre porque, se $x \notin A_q$, então $x \notin A_r$ para todo $r \in \mathbb{Q} \cap [0, q[$, portanto $\{q \in Q \mid x \in A_q\} \subseteq \mathbb{Q} \cap [0, q[$ o que implica $f(x) \geq q$ por definição de f .

Agora que provamos esses fatos, seja $x \in]a, b[\subseteq [0, 1]$. Mostremos que existe vizinhança $A \subseteq X$ de x tal que $f(A) \subseteq]a, b[$. Para isso, sejam $p, q \in Q$ tais que $a < p < f(x) < q < b$ e definamos $A := A_q \setminus \overline{A_p}$. Então, pelos fatos acima, $x \in A_q$ porque $f(x) < q$ e $x \notin \overline{A_p}$ porque $f(x) > p$, o que mostra que $x \in A$. Por fim, seja $x' \in A$. Então $x' \in A_q \subseteq \overline{A_q}$, portanto $f(x') \leq q$ e $x' \notin \overline{A_p} \supseteq A_p$, portanto $f(x') \geq p$, o que implica $f(x') \subseteq [p, q] \subseteq]a, b[$. Isso mostra que f é contínua. ■

13.3 Convergência

13.3.1 Redes

Proposição 13.51. *Sejam X um espaço topológico e $C \subseteq X$. Então $(\mathcal{V}_C, \supseteq)$, o conjunto de vizinhanças de C com ordem de contenção invertida, é um conjunto direcionado.*

Demonstração. Sabemos que \supseteq é uma ordem parcial. Sejam $V_0, V_1 \in \mathcal{V}_C$. Então $V := V_0 \cap V_1$ é uma vizinhança de C tal que $V_0 \supseteq V$ e $V_1 \supseteq V$. ■

Definição 13.26. Sejam X um conjunto e (Λ, \leq) um conjunto direcionado. Uma rede de elementos de X indexados por Λ é uma função $x : \Lambda \rightarrow X$. O conjunto Λ é o conjunto de índices da rede. Denota-se $(x_\lambda)_{\lambda \in \Lambda}$ e a imagem de $\lambda \in \Lambda$ por x é denotada x_λ e chamada de λ -ésimo membro da rede.

Note que uma sequência é uma rede cujo conjunto direcionado é (\mathbb{N}, \leq) .

Definição 13.27 (Limite e convergência). Sejam X um espaço topológico e $(x_\lambda)_{\lambda \in \Lambda}$ uma rede de X . Um limite de $(x_\lambda)_{\lambda \in \Lambda}$ em X é um ponto $\ell \in X$ que satisfaz: para toda vizinhança V de ℓ , existe $\lambda \in \Lambda$ tal que, para todo $\mu \geq \lambda$, $x_\mu \in V$. Denota-se $(x_\lambda)_{\lambda \in \Lambda} \rightarrow \ell$. Uma rede convergente é uma rede que tem limite.

Proposição 13.52. *Um espaço topológico X é separado por vizinhanças (T_2) se, e somente se, toda rede convergente $(x_\lambda)_{\lambda \in \Lambda}$ de X tem limite único.*

Demonstração. (\Rightarrow) Sejam ℓ_0 e ℓ_1 limites de $(x_\lambda)_{\lambda \in \Lambda}$. Se ℓ_0 e ℓ_1 são distintos, então por \mathbf{X} ser T_2 existem vizinhanças disjuntas V_0 de ℓ_0 e V_1 de ℓ_1 . Da convergência da rede, existem λ_0 e $\lambda_1 \in \Lambda$ tais que, para todo $\mu \geq \lambda_0$, $x_\mu \in V_0$ e, para todo $\mu \geq \lambda_1$, $x_\mu \in V_1$. Como (Λ, \leq) é direcionado, existe $\lambda \in \Lambda$ tal que $\lambda_0 \leq \lambda$ e $\lambda_1 \leq \lambda$, o que implica pela convergência da rede que $x_\lambda \in V_0 \cap V_1$, que é uma contradição. Portanto $\ell_0 = \ell_1$.

(\Leftarrow) Suponhamos que \mathbf{X} não é T_2 . Então existem pontos distintos x_0 e $x_1 \in X$ tais que, para todas vizinhanças V_0 de x_0 e V_1 de x_1 , $V_0 \cap V_1 \neq \emptyset$. Definamos $\mathcal{V} := \mathcal{V}_{\{x_0, x_1\}}$ e notemos que $(\mathcal{V}_{\{x_0, x_1\}}, \supseteq)$ é um conjunto direcionado. Para todos vizinhanças $V_0 \in \mathcal{V}_{x_0}$ e $V_1 \in \mathcal{V}_{x_1}$, tomamos $x_{V_0 \cap V_1} \in V_0 \cap V_1$, que existe pois o conjunto $V_0 \cap V_1$ não é vazio. Mostraremos que a rede $(x_V)_{V \in \mathcal{V}}$ então converge para x_0 e para x_1 . Sejam V_0 uma vizinhança de x_0 e V_1 uma vizinhança de x_1 e defina $V := V_0 \cap V_1$. Então, para toda vizinhança de $U \in \mathcal{V}$ tal que $U \subseteq V$, segue que $x_U \in U \subseteq V$, portanto a rede $(x_V)_{V \in \mathcal{V}}$ converge para x_0 e para x_1 . ■

Usamos o axioma da escolha para construir a rede na volta da demonstração, pois a rede é elemento do produto de todas as vizinhanças de \mathcal{V} .

Proposição 13.53. *Sejam \mathbf{X}_0 e \mathbf{X}_1 espaços topológicos e $f : X_0 \rightarrow X_1$ uma função. Então f é contínua se, e somente se, para todo $\ell \in X_0$ e toda rede $(x_\lambda)_{\lambda \in \Lambda}$ que converge para $\ell \in X_0$, a rede $(f(x_\lambda))_{\lambda \in \Lambda}$ converge para $f(\ell) \in X_1$.*

Proposição 13.54. *Sejam $(\mathbf{X}_i)_{i \in I}$ uma família de espaços topológicos e $(x_\lambda)_{\lambda \in \Lambda}$ uma rede de $\mathbf{X} = \prod_{i \in I} \mathbf{X}_i$. Então $(x_\lambda)_{\lambda \in \Lambda} \rightarrow \ell \in X$ se, e somente se, para todo $i \in I$, $(\pi_i(x_\lambda))_{\lambda \in \Lambda} \rightarrow \pi_i(\ell) \in X_i$.*

Demonstração.

(\Rightarrow) Segue da continuidade de π_i .

(\Leftarrow) Seja V uma vizinhança de $(\ell_i)_{i \in I}$. Então existe um aberto básico $A = \bigcap_{i \in J} \pi_i^{-1}(A_i)$ tal que $A \subseteq V$, $J \subseteq I$ é um conjunto finito e $A_i \subseteq X_i$ é um aberto. Sendo assim, para cada $i \in J$, existe $\lambda_i \in \Lambda$ tal que, para todo $\mu \geq \lambda_i$, $x_{i,\mu} \in A_i$. Portanto, como Λ é um conjunto direcionado (e J é fininto), existe λ tal que, para todo $i \in J$, $\lambda_i \leq \lambda$, o que implica que, para todo $\mu \geq \lambda$, $(x_{i,\mu})_{i \in I} \in A \subseteq V$. Isso mostra que $((x_{i,\lambda})_{i \in I})_{\lambda \in \Lambda} \rightarrow (\ell_i)_{i \in I}$. ■

13.4 Conexidade e Compacidade

13.4.1 Conexidades

Definimos o conceito de desconexo antes por ele ser mais intuitivo de ser enunciado. Ser desconexo é ter como separar o espaço \mathbf{X} em dois conjuntos disjuntos, aberto e não triviais (não são \emptyset nem X). Esses abertos cobrem todo espaço e, como são abertos, o separam pela definição de separação de conjuntos.

Definição 13.28. Um espaço topológico *desconexo* é um espaço topológico \mathbf{X} tal que X admite partição por dois conjuntos abertos. Um espaço topológico *conexo* é um espaço topológico que não é desconexo. Um subconjunto de X é conexo ou desconexo de acordo com sua topologia induzida.

Uma partição por dois abertos é equivalente a uma cobertura por dois conjuntos abertos, disjuntos e não triviais. Notemos que, por essa definição, o espaço topológico \emptyset é conexo, pois todos subconjuntos de \emptyset são triviais, logo \emptyset não admite partições. A conexidade de \emptyset não é consenso entre autores, mas adotaremos esse resultado aqui. É importante notar que, na definição, porderíamos escolher uma partição por conjuntos fechados, já que, como cada conjunto da partição é o complementar do outro, ambos são fechados, pois ambos são abertos. A definição de separação de conjuntos vale nesse caso, os conjuntos da partição são separados no sentido que cada um é disjunto do fecho do outro, já que são fechados e disjuntos. Isso sugere que conexidade está relacionada com o problema de confusão semântica clássica em topologia: nem todo conjunto aberto é necessariamente não fechado, e vice-versa. Claro que \emptyset e X são sempre abertos e fechados, mas em espaços conexos eles são os únicos. Com o conceito de conexidade, temos o seguinte resultado.

Proposição 13.55. *Um espaço topológico \mathbf{X} é conexo se, e somente se, não existe um conjunto não trivial que é aberto e fechado.*

Demonstração. Vamos mostrar a ida e a volta pela contrapositiva. Se \mathbf{X} é desconexo, os conjuntos que formam sua partição por abertos são ambos abertos e fechados. Reciprocamente, se $A \subseteq X$ é não trivial, aberto e fechado, A^c também é não trivial e aberto (e fechado), logo $\{A, A^c\}$ é uma partição de X por dois conjuntos abertos. ■

As noções de conexidade de um espaço topológico e de um subconjunto de um espaço topológico são, de fato, a mesma, mas alguns cuidados devem ser tomados para escolher onde os conjuntos são abertos ou fechados, se na topologia original ou na induzida. A proposição a seguir oferece um critério para conjuntos conexos.

Proposição 13.56. *Seja \mathbf{X} um espaço topológico. Então $S \subseteq X$ é conexo se, e somente se, não existem conjuntos não triviais separados em \mathbf{X} cuja união é S .*

Demonstração. Se S é desconexo, existe uma partição $\{A, B\}$ de S por abertos de \mathbf{S} . Então $A \cup B = S$,

$$A \cap \overline{B}^x = (A \cap S) \cap \overline{B}^x = A \cap (S \cap \overline{B}^x) = A \cap \overline{B}^s = A \cap B = \emptyset$$

e, similmente, $\overline{A}^x \cap B = \emptyset$, o que mostra que A e B são separados em \mathbf{X} . Reciprocamente, se existem $A, B \subseteq X$ conjuntos não triviais separados em \mathbf{X} tais

que $A \cup B = S$, então

$$\overline{A}^S = S \cap \overline{A}^X = (A \cap B) \cap \overline{A}^X = (A \cap \overline{A}^X) \cup (B \cap \overline{A}^X) = A \cup \emptyset = A$$

e, similarmente, $\overline{B}^S = B$, portanto $\{A, B\}$ é partição de S por fechados de S , o que mostra que S é desconexo. ■

A seguir, enunciamos uma equivalência da definição de conexidade e um resultado trivial, mas importantíssimo na topologia: conexidade é um invariante topológico.

Proposição 13.57. *Sejam X um espaço topológico, e $\{0, 1\}$ espaço topológico com a topologia discreta. Então X é conexo se, e somente se, toda função contínua $f : X \rightarrow \{0, 1\}$ é constante.*

Demonstração. Demonstraremos a ida e a volta pela contrapositiva. Se X é desconexo, seja $\{A_0, A_1\}$ uma partição de X por dois conjuntos abertos. Definamos

$$\begin{aligned} f : X &\longrightarrow \{0, 1\} \\ x &\longmapsto \begin{cases} 0, & x \in A_0 \\ 1, & x \in A_1. \end{cases} \end{aligned}$$

Então $f^{-1}(\emptyset) = \emptyset$, $f^{-1}(\{0\}) = A_0$, $f^{-1}(\{1\}) = A_1$ e $f^{-1}(\{0, 1\}) = X$. Portanto f é contínua, mas não é constante. Reciprocamente, seja $f : X \rightarrow \{0, 1\}$ uma função contínua não constante. Então $f^{-1}(\{0\})$ e $f^{-1}(\{1\})$ são abertos, pois f é contínua, e formam uma partição de X : (1) não são vazios, pois f não é constante, (2) são disjuntos e (3) sua união é X . Logo X é desconexo. ■

Proposição 13.58. *Sejam X e Y espaços topológicos e $f : X \rightarrow Y$ uma função contínua. Se X é conexo, então Y é conexo.*

Demonstração. Se Y fosse desconexo, existiria uma partição de Y por abertos $\{A, B\}$, e como f é contínua, $\{f^{-1}(A), f^{-1}(B)\}$ seria uma partição de X por abertos, contradizendo a conexidade de X . ■

Componentes Conexas

Proposição 13.59. *Seja X um espaço topológico e $(C_i)_{i \in I}$ uma família de conjuntos conexos tais que $\bigcap_{i \in I} C_i \neq \emptyset$. Então $\bigcup_{i \in I} C_i$ é conexo.*

Demonstração. Se $\bigcup_{i \in I} C_i$ for desconexo, existe partição $\{A, B\}$ por abertos de $\bigcup_{i \in I} C_i$. Como $p \in \bigcap_{i \in I} C_i \neq \emptyset$, existe $p \in \bigcap_{i \in I} C_i$ e, portanto, sem perda de generalidade, suponhamos $p \in A$. Seja $q \in B$. Então existe $i \in I$ tal que $q \in C_i$ e, como $p \in C_i$, temos que $p \in A \cap C_i$ e $q \in B \cap C_i$. Então $A \cap C_i$ e $B \cap C_i$ são não vazios e são abertos de C_i , o que implica que eles são uma partição de C_i por conjuntos abertos, e isso contradiz sua conexidade. ■

Definição 13.29. Sejam \mathbf{X} um espaço topológico, $p \in X$ e $(C_i)_{i \in I}$ uma indexação dos conjuntos conexos que contêm p . A *componente conexa* de \mathbf{X} em p é o conjunto conexo

$$\Gamma_p := \bigcup_{i \in I} C_i.$$

O conjunto Γ_p é conexo pela proposição 13.59, pois a interseção de $(C_i)_{i \in I}$ contém p . A componente conexa em um ponto é o maior conjunto conexo que contém o ponto. A relação de estar na mesma componente conexa é uma relação de equivalência, como mostra a proposição a seguir, pois o conjunto de componentes conexas é uma partição de X .

Proposição 13.60. As componentes conexas de um espaço topológico \mathbf{X} são uma partição de X .

Demonstração. Claramente nenhuma componente conexa é vazia, pois contém o próprio ponto. Ainda, a união de todas as componentes conexas é X , pelo mesmo motivo. Falta mostrar que elas são disjuntas duas a duas. Sejam $p, q \in X$ pontos distintos. Vamos mostrar que $\Gamma_p = \Gamma_q$ ou $\Gamma_p \cap \Gamma_q = \emptyset$. Se $C_p \neq C_q$ e $C_p \cap C_q \neq \emptyset$, então $C_p \cup C_q$ seria um conjunto conexo estritamente maior que C_p , contradizendo a maximalidade da componente conexa. ■

Na prática, podemos sempre reduzir o estudo de um espaço topológico ao estudo das suas componentes conexas, já que elas são abertos e definir funções contínuas no espaço é equivalente a definir em abertos que cobrem o espaço.

Conexidade por Caminhos

13.4.2 Compacidades

As propriedade de compacidade de um espaço topológico são propriedades relacionadas a coberturas de um espaço.

Compacidade

Definição 13.30. Um espaço topológico *compacto* é um espaço topológico \mathbf{X} em que toda cobertura aberta \mathcal{C} de \mathbf{X} tem subcobertura finita. Um subconjunto *compacto* de \mathbf{X} é um conjunto $C \subseteq X$ que é compacto com a topologia de subespaço.

Proposição 13.61. Seja \mathbf{X} um espaço topológico. São equivalentes

1. \mathbf{X} é compacto;
2. Toda rede em \mathbf{X} tem sub-rede convergente.

Proposição 13.62. *Seja \mathbf{X} um espaço topológico.*

1. *Se \mathbf{X} é compacto, todo fechado $F \subseteq X$ é compacto;*
2. *Se \mathbf{X} é separado por vizinhanças, todo compacto $C \subseteq X$ é fechado;*
3. *Se $C \subseteq X$ é compacto e $F \subseteq C$ é fechado, F é compacto.*

Proposição 13.63. *Sejam \mathbf{X}_0 e \mathbf{X}_1 espaços topológicos e $f : X_0 \rightarrow X_1$ uma função contínua. Se \mathbf{X}_0 é compacto, então $f(\mathbf{X}_0)$ é compacto.*

Demonstração. Seja $(C_I)_{i \in I}$ uma cobertura aberta de $f(\mathbf{X}_0)$. A família $(f^{-1}(C_i))_{i \in I}$ é uma cobertura de X_0 , pois

$$\bigcup_{i \in I} f^{-1}(C_i) = f^{-1}\left(\bigcup_{i \in I} C_i\right) = f^{-1}(X_1) = X_0.$$

A cobertura é aberta pois f é contínua. Como \mathbf{X}_0 é compacto, existem $i_0, \dots, i_{n-1} \in I$ tal que $(f^{-1}(A_{i_k}))_{k \in [n]}$ é uma cobertura aberta de \mathbf{X}_0 . Então $(A_{i_k})_{k \in [n]}$ é uma cobertura aberta de $f(\mathbf{X}_0)$, pois

$$f(X_0) = f\left(\bigcup_{k \in [n]} f^{-1}(A_{i_k})\right) = \bigcup_{k \in [n]} f(f^{-1}(A_{i_k})) \subseteq \bigcup_{k \in [n]} A_{i_k}.$$

Isso mostra que $f(\mathbf{X}_0)$ é compacto. ■

Compacidade Contável (Lindelöf)

Definição 13.31. Um espaço topológico *contavelmente compacto* (*Lindelöf*) é um espaço topológico \mathbf{X} em que toda cobertura aberta \mathcal{C} de \mathbf{X} tem subcobertura contável.

Alguns autores definem compacidade contável como a propriedade de que toda cobertura aberta contável admite subcobertura finita.

Compacidade Local

Definição 13.32. Um espaço topológico *localmente compacto* é um espaço topológico \mathbf{X} em que todo ponto $x \in X$ tem uma vizinhança compacta.

Paracompacidade

Definição 13.33. Um espaço topológico *localmente compacto* é um espaço topológico \mathbf{X} em que toda cobertura aberta \mathcal{C} de \mathbf{X} tem refinamento aberto localmente finito.

Compacidade Sequencial

13.4.3 Contabilidades

Base de Vizinhanças Contável (1º Contável)

Base Contável (2º Contável)

13.5 Homotopia e Grupo Fundamental

13.5.1 Homotopia

Definição 13.34. Sejam X e X' espaços topológicos e $f, f' \in \mathcal{C}(X, X')$ funções contínuas. Uma *homotopia* de f para f' é uma função contínua

$$\begin{aligned} H: [0, 1] \times X &\longrightarrow X' \\ (t, x) &\longmapsto H^t(x) \end{aligned}$$

tal que $H^0 = f$ e $H^1 = f'$. As funções f e f' são *homotópicas* e denota-se $f \approx g$.

Proposição 13.64. *Sejam X e X' espaços topológicos. A relação de homotopia é uma equivalência no conjunto $\mathcal{C}(X, X')$ das funções contínuas de X para X' .*

Demonstração. 1. (Reflexividade) Seja $f \in \mathcal{C}(X, X')$. Consideremos a função

$$\begin{aligned} H: [0, 1] \times X &\longrightarrow X' \\ (t, x) &\longmapsto f(x) \end{aligned}$$

Então H é uma função contínua, pois f é contínua, e vale que $H^0 = H^1 = f$, portanto $f \approx f$.

2. (Simetria) Sejam $f, f' \in \mathcal{C}(X, X')$ tais que $f \approx f'$ e $H: [0, 1] \times X \longrightarrow X'$ uma homotopia de f para f' . Consideremos a função

$$\begin{aligned} H': [0, 1] \times X &\longrightarrow X' \\ (t, x) &\longmapsto H^{1-t}(x). \end{aligned}$$

Como H e $1 - t$ são contínuas, a função H' é contínua. Ainda, notemos que $H'^0 = H^1 = f'$ e $H'^1 = H^0 = f$, portanto $f' \approx f$.

3. (Transitividade) Sejam $f, f', f'' \in \mathcal{C}(X, X')$ tais que $f \approx f'$ e $f' \approx f''$ e $H: [0, 1] \times X \longrightarrow X'$ uma homotopia de f para f' e $H': [0, 1] \times X \longrightarrow X'$ uma homotopia de f' para f'' . Consideremos a função

$$\begin{aligned} H'': [0, 1] \times X &\longrightarrow X' \\ (t, x) &\longmapsto \begin{cases} H^{2t}(x), & t \in [0, \frac{1}{2}] \\ H'^{2t-1}(x), & t \in [\frac{1}{2}, 1] \end{cases}. \end{aligned}$$

Como $H^1 = f' = H'^0$ e H e H' são contínuas, então H'' é contínua. Ainda, como H é uma homotopia de f para f' , então $H''^0 = H^0 = f$ e, como H' é uma homotopia de f' para f'' , então $H''^1 = H'^1 = f''$, portanto H'' é uma homotopia de f para f'' . ■

Proposição 13.65. Sejam \mathbf{X} , \mathbf{X}' e \mathbf{X}'' espaços topológicos, $f, f' \in \mathcal{C}(X, X')$ e $g, g' \in \mathcal{C}(X', X'')$ funções contínuas tais que $f \approx f'$ e $g \approx g'$. Então

$$(g \circ f) \approx (g' \circ f').$$

Demonstração. Sejam $H: [0, 1] \times X \rightarrow X'$ uma homotopia de f para f' e $H': [0, 1] \times X' \rightarrow X''$ uma homotopia de g para g' . Consideremos a função

$$\begin{aligned} H'': [0, 1] \times X &\rightarrow X'' \\ (t, x) &\mapsto H'^t \circ H^t(x). \end{aligned}$$

Como H e H' são contínuas, então H'' é contínua. Como H é homotopia de f para f' e H' é homotopia de g para g' , então $H^0 = f$, $H^1 = f'$, $H'^0 = g$ e $H'^1 = g'$, o que implica

$$H''^0 = H'^0 \circ H^0 = g \circ f$$

e

$$H''^1 = H'^1 \circ H^1 = g' \circ f',$$

o que mostra que H'' é homotopia de $g \circ f$ para $g' \circ f'$. ■

13.5.2 Equivalência Homotópica

Definição 13.35. Sejam \mathbf{X} e \mathbf{X}' espaços topológicos. Uma *equivalência homotópica* entre \mathbf{X} e \mathbf{X}' é uma par $(f, f') \in \mathcal{C}(X, X') \times \mathcal{C}(X', X)$ de funções contínuas tais que $f' \circ f \approx \text{Id}_X$ e $f \circ f' \approx \text{Id}_{X'}$. Os espaços \mathbf{X} e \mathbf{X}' são *homotopicamente equivalentes* e denota-se $X \approx X'$.

13.5.3 Caminhos e Laços

Definição 13.36 (Caminho e laço). Seja \mathbf{X} um espaço topológico. Um *caminho* em X é uma função contínua $c: [0, 1] \rightarrow X$. Um *laço* em X é uma função contínua $\ell: \mathbb{S}^1 \rightarrow X$ e a *origem* desse laço é o ponto $\ell(0)$. Denotaremos o conjunto dos laços em X com origem em $x_0 \in X$ por $L(X, x_0)$

Note que um laço é um caminho c tal que $c(0) = c(1)$.

Definição 13.37. Seja X um espaço métrico e $c: [0, 1] \rightarrow X$ um caminho em X . O *caminho inverso* de c é o caminho

$$\begin{aligned} c^{-1}: [0, 1] &\rightarrow X \\ s &\mapsto c(1 - s). \end{aligned}$$

Definição 13.38. Seja X um espaço métrico e $x_0 \in X$. O *caminho constante* em x_0 é o caminho

$$\begin{aligned} e_{x_0} : [0, 1] &\longrightarrow X \\ s &\longmapsto x_0. \end{aligned}$$

Definição 13.39. Sejam X um espaço métrico e $c_1, c_2 : [0, 1] \longrightarrow X$ caminhos em X tais que $c_1(1) = c_2(0)$. A *composição* dos caminhos c_1 e c_2 é o caminho

$$\begin{aligned} (c_1 \cdot c_2) : [0, 1] &\longrightarrow X \\ s &\longmapsto \begin{cases} c_1(2s) & \text{se } 0 \leq s \leq \frac{1}{2} \\ c_2(2s - 1) & \text{se } \frac{1}{2} \leq s \leq 1. \end{cases} \end{aligned}$$

13.5.4 Homotopia de Caminhos

Definição 13.40. Sejam X um espaço métrico e $c_1 : [0, 1] \longrightarrow X$ e $c_2 : [0, 1] \longrightarrow X$ caminhos em X tal que $c_1(0) = c_2(0)$ e $c_1(1) = c_2(1)$. Uma *homotopia de caminhos* entre c_1 e c_2 é uma homotopia H entre c_1 e c_2 tal que, para todo $t \in [0, 1]$, $H(0, t) = c_1(0)$ e $H(1, t) = c_1(1)$. No caso de existir uma homotopia de caminhos entre c_1 e c_2 , denota-se $c_1 \approx c_2$.

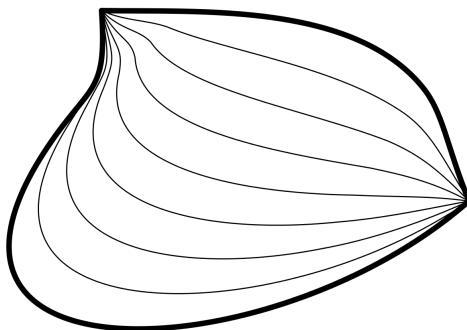


Figura 13.1: Ilustração de uma homotopia de caminhos.

Proposição 13.66. Sejam X um espaço métrico e $x_0 \in X$. Então a relação \approx de homotopia de caminhos é uma relação de equivalência em $L(X, x_0)$.

Demonstração. Sejam $l_1, l_2, l_3 \in L(X, x_0)$. Então

1. Reflexividade: $l_1 \approx l_1$.

Consideremos a função

$$\begin{aligned} H : S^1 \times [0, 1] &\longrightarrow X \\ (x, t) &\longmapsto l(x). \end{aligned}$$

Sabemos que H é uma homotopia entre l_1 e l_1 . Basta notar que, para todo $t \in [0, 1]$, $H(0, t) = H(1, t) = l_1(0)$, o que termina a demonstração de que H é uma homotopia de laços entre l_1 e l_1 .

2. Simetria: $l_1 \approx l_2 \Rightarrow l_2 \approx l_1$.

Seja $H : S^1 \times [0, 1] \rightarrow X$ uma homotopia de laços entre l_1 e l_2 . Então consideremos a função

$$\begin{aligned} H' : S^1 \times [0, 1] &\rightarrow X \\ (x, t) &\mapsto H(x, 1-t). \end{aligned}$$

Sabemos que H' é uma homotopia entre l_2 e l_1 . Basta notar que, para todo $t \in [0, 1]$, $H'(0, t) = H(0, 1-t) = l_1(0) = H(1, 1-t) = H'(1, t)$, o que termina a demonstração de que H' é uma homotopia de laços entre l_2 e l_1 .

3. Transitividade: $l_1 \approx l_2$ e $l_2 \approx l_3 \Rightarrow l_1 \approx l_3$.

Sejam $H_1 : S^1 \times [0, 1] \rightarrow X$ uma homotopia entre l_1 e l_2 e $H_2 : S^1 \times [0, 1] \rightarrow X$ uma homotopia entre l_2 e l_3 . Então consideremos a função

$$\begin{aligned} H : S^1 \times [0, 1] &\rightarrow X \\ (x, t) &\mapsto \begin{cases} H_1(x, 2t) & \text{se } 0 \leq t \leq \frac{1}{2} \\ H_2(x, 2t - 1) & \text{se } \frac{1}{2} \leq t \leq 1. \end{cases} \end{aligned}$$

Sabemos que H é uma homotopia entre l_1 e l_3 . Basta notar que, como H_1 é homotopia de laços, para todo $t \in [0, \frac{1}{2}]$, $H(0, t) = H_1(0, 2t) = l_1(0)$ e, como H_2 é homotopia de laços entre l_2 e l_3 , para todo $t \in [\frac{1}{2}, 1]$, $H(0, t) = H_2(0, 2t - 1) = l_2(0) = l_1(0)$ o que termina a demonstração de que H é uma homotopia de laços entre l_1 e l_3 .

■

Proposição 13.67. *Seja X um espaço métrico e $c_1, c_2, c_3 : [0, 1] \rightarrow X$ caminhos em X tais que $c_1(0) = x_0$, $c_1(1) = c_2(0)$, $c_2(1) = c_3(0)$ e $c_3(0) = x_1$. Então*

1. $c_1 \cdot (c_1)^{-1} \approx e_{x_0}$;
2. $(c_1)^{-1} \cdot c_1 \approx e_{x_1}$;
3. $e_{x_0} \cdot c_1 \approx c_1 \approx c_1 \cdot e_{x_1}$;
4. $(c_1 \cdot c_2) \cdot c_3 \approx c_1 \cdot (c_2 \cdot c_3)$.

Demonstração. 1. Notemos que

$$c_1 \cdot (c_1)^{-1}(s) = \begin{cases} c_1(2s) & \text{se } s \in [0, \frac{1}{2}] \\ (c_1)^{-1}(2s - 1) & \text{se } s \in [\frac{1}{2}, 1]. \end{cases} = \begin{cases} c_1(2s) & \text{se } s \in [0, \frac{1}{2}] \\ c_1(2 - 2s) & \text{se } s \in [\frac{1}{2}, 1]. \end{cases}$$

Assim, considereando a parametrização $\phi : [0, 1] \longrightarrow [0, 1]$

$$\phi(s) = \begin{cases} 2s & \text{se } s \in [0, \frac{1}{2}] \\ 2 - 2s & \text{se } s \in [\frac{1}{2}, 1] \end{cases}$$

segue que $c_1 \cdot (c_1)^{-1}(s) = c_1(\phi(s))$. Consideremos, assim, a função

$$\begin{aligned} H : [0, 1] \times [0, 1] &\longrightarrow X \\ (s, t) &\longmapsto c_1((1 - t)\phi(s)). \end{aligned}$$

Temos que H é contínua, pois c_1 , $1 - t$ e ϕ são contínuas. Agora, notemos que, para todo $s, t \in [0, 1]$, $1 - t \in [0, 1]$ e $\phi(s) \in [0, 1]$, o que mostra que $(1 - t)\phi(s) \in [0, 1]$ e, portanto, que H está bem definida. Ainda, para todo $s \in [0, 1]$, $H(s, 0) = c_1(\phi(s)) = c_1 \cdot (c_1)^{-1}(s)$ e $H(s, 1) = c_1(0) = x_0$. Portanto H é homotopia entre $c_1 \cdot (c_1)^{-1}$ e e_{x_0} . Para mostrar que H é homotopia de caminhos, note que, para todo $t \in [0, 1]$, $H(0, t) = c_1((1 - t)\phi(0)) = c_1(0)$ e $H(1, t) = c_1((1 - t)\phi(1)) = c_1(0)$, o que termina a demonstração.

2. Análogo ao item anterior, mas considerando a parametrização $\phi : [0, 1] \longrightarrow [0, 1]$

$$\phi(s) = \begin{cases} 1 - 2s & \text{se } s \in [0, \frac{1}{2}] \\ 2s - 1 & \text{se } s \in [\frac{1}{2}, 1]. \end{cases}$$

3. Análogo ao item anterior, mas considerando as parametrizações $\phi, \phi' : [0, 1] \longrightarrow [0, 1]$

$$\phi(s) = \begin{cases} 0 & \text{se } s \in [0, \frac{1}{2}] \\ 2s - 1 & \text{se } s \in [\frac{1}{2}, 1]. \end{cases}$$

$$\phi'(s) = \begin{cases} 2s & \text{se } s \in [0, \frac{1}{2}] \\ 0 & \text{se } s \in [\frac{1}{2}, 1]. \end{cases}$$

4. Notemos que

$$(c_1 \cdot c_2) \cdot c_3 = \begin{cases} c_1(4s) & \text{se } s \in [0, \frac{1}{4}] \\ c_2(4s - 1) & \text{se } s \in [\frac{1}{4}, \frac{1}{2}] \\ c_3(2s - 1) & \text{se } s \in [\frac{1}{2}, 1] \end{cases}$$

$$c_1 \cdot (c_2 \cdot c_3) = \begin{cases} c_1(2s) & \text{se } s \in [0, \frac{1}{2}] \\ c_2(4s - 2) & \text{se } s \in [\frac{1}{2}, \frac{3}{4}] \\ c_3(4s - 3) & \text{se } s \in [\frac{3}{4}, 1]. \end{cases}$$

Assim, considerando a parametrização $\phi : [0, 1] \rightarrow [0, 1]$

$$\phi(s) = \begin{cases} 2s & \text{se } s \in [0, \frac{1}{4}] \\ s + \frac{1}{4} & \text{se } s \in [\frac{1}{4}, \frac{1}{2}] \\ \frac{s}{2} + \frac{1}{2} & \text{se } s \in [\frac{1}{2}, 1]. \end{cases}$$

segue que $((c_1 \cdot c_2) \cdot c_3)(s) = (c_1 \cdot (c_2 \cdot c_3))(\phi(s))$. Consideremos, assim, a função

$$H : [0, 1] \times [0, 1] \rightarrow X$$

$$(s, t) \mapsto (c_1 \cdot c_2) \cdot c_3((1-t)s + t\phi(s)).$$

Analogamente aos itens anteriores, mostra-se que H é homotopia de caminhos.

■

Proposição 13.68. *Sejam X um espaço métrico, $x_0 \in X$ e $c_1, c_2, c'_1, c'_2 : [0, 1] \rightarrow X$ caminhos em X . Então*

1. *Se $c_1 \approx c'_1$ e $c_2 \approx c'_2$, então $c_1 \cdot c_2 \approx c'_1 \cdot c'_2$.*
2. *$(c_1)^{-1} \approx (c'_1)^{-1}$.*

Demonstração. 1. Seja H_1 a homotopia de caminhos entre c_1 e c'_1 e H_2 a homotopia de caminhos entre c_2 e c'_2 . Consideremos a função

$$H : [0, 1] \times [0, 1] \rightarrow X$$

$$(s, t) \mapsto \begin{cases} H_1(2s, t) & \text{se } 0 \leq s \leq \frac{1}{2} \\ H_2(2s - 1, t) & \text{se } \frac{1}{2} \leq s \leq 1. \end{cases}$$

Primeiro, notemos que H é uma homotopia entre c_1 e c_2 . Pois como H_1 e H_2 são contínuas, basta mostrar que H é contínua nos pontos em que $s = \frac{1}{2}$.

Para isso, notemos que, para todo $t \in [0, 1]$, $H_1(2\frac{1}{2}, t) = H_1(1, t) = c'_1(1)$, pois H_1 é homotopia de caminhos, e $H_2(2\frac{1}{2} - 1, t) = H_2(0, t) = c_2(0)$, pois H_2 é homotopia de caminhos. Assim, segue que as funções nesses pontos são iguais e, portanto, H é contínua. Ainda, para todo $s \in [0, 1]$,

$$H(s, 0) = \begin{cases} H_1(2s, 0) = c_1(2s) & \text{se } 0 \leq s \leq \frac{1}{2} \\ H_2(2s - 1, 0) = c_2(2s - 1) & \text{se } \frac{1}{2} \leq s \leq 1, \end{cases}$$

o que mostra que $H(s, 0) = (c_1 \cdot c_2)(s)$, e

$$H(s, 0) = \begin{cases} H_1(2s, 1) = c'_1(2s) & \text{se } 0 \leq s \leq \frac{1}{2} \\ H_2(2s - 1, 1) = c'_2(2s - 1) & \text{se } \frac{1}{2} \leq s \leq 1, \end{cases}$$

o que mostra que $H(s, 0) = (c'_1 \cdot c'_2)(s)$ e, portanto, que H é homotopia.

Agora, devemos mostrar que H é homotopia de caminhos. Notemos que, para todo $t \in [0, 1]$, $H(0, t) = H_1(0, t) = c_1(0) = (c_1 \cdot c_2)(0)$, pois H_1 é homotopia de caminhos, e $H(1, t) = H_2(1, t) = c'_2(1) = (c'_1 \cdot c'_2)(1)$, o que mostra que H é homotopia de caminhos.

2. Seja H uma homotopia de caminhos entre c_1 e c'_1 . Consideremos a função

$$\begin{aligned} H' : [0, 1] \times [0, 1] &\longrightarrow X \\ (s, t) &\longmapsto H(1 - s, t). \end{aligned}$$

Primeiro notemos que H' é uma homotopia entre $(c_1)^{-1}$ e $(c'_1)^{-1}$. Claramente, H' é contínua, pois H e $1 - s$ são contínuas. Ainda, para todo $s \in [0, 1]$,

$$H'(s, 0) = H(1 - s, 0) = c_1(1 - s) = (c_1)^{-1}(s)$$

e

$$H'(s, 1) = H(1 - s, 1) = c'_1(1 - s) = (c'_1)^{-1}(s),$$

pois H é homotopia. Assim, mostramos que H' é homotopia entre $(c_1)^{-1}$ e $(c'_1)^{-1}$.

Agora, mostremos que H' é homotopia de caminhos. Para todo $t \in [0, 1]$, $H'(0, t) = H(1, t) = c'_1(1) = (c'_1)^{-1}(0)$ e $H'(1, t) = H(0, t) = c_1(0) = (c_1)^{-1}(1)$, pois H é homotopia de caminhos. Assim, mostramos que H' é homotopia de caminhos entre $(c_1)^{-1}$ e $(c'_1)^{-1}$. ■

13.5.5 Grupo Fundamental

Como \approx é uma relação de equivalência em $L(X, x_0)$, podemos considerar o espaço quociente $L(X, x_0)/\approx$ das classes de equivalência de laços em $L(X, x_0)$.

Definição 13.41. Sejam X um espaço métrico conexo por caminhos e $x_0 \in X$. Então o *grupo fundamental* de X com base em x_0 é o conjunto

$$\pi_1(X, x_0) := L(X, x_0)/\approx.$$

Definição 13.42. Sejam X um espaço métrico conexo por caminhos. A *composição* de classes de equivalência de laços em $\pi_1(X)$ é a função

$$\begin{aligned} \cdot : \pi_1(X) \times \pi_1(X) &\longrightarrow \pi_1(X) \\ ([l_1], [l_2]) &\longmapsto [l_1 \cdot l_2]. \end{aligned}$$

Notemos que a composição de caminhos está bem definida por causa da proposição 13.68.

Teorema 13.69. Sejam X um espaço métrico conexo por caminhos e $x_0 \in X$. Então $(\pi_1(X), \cdot)$ é um grupo.

Demonstração. Segue direto das proposições 13.67 e 13.68. ■

13.6 Espaços Fibrados

Definição 13.43. Sejam B e F espaços topológicos. Um *espaço F -fibrado sobre B* é um espaço topológico E munido de uma função contínua sobrejetiva $p: E \rightarrow B$ satisfazendo que, para todo $x \in E$, existem vizinhança $V \subseteq B$ de $p(x)$ e homeomorfismo $h: p^{-1}(V) \rightarrow V \times F$ tais que $p_V \circ h = p$ (o diagrama comuta).

$$\begin{array}{ccc} p^{-1}(V) & \xrightarrow{\quad h \quad} & V \times F \\ \searrow p & & \swarrow p_V \\ & V & \end{array}$$

O espaço B é a *base* e o espaço F é a *fibra*, e a função $p: E \rightarrow F$ é a *projeção fibrada* de E . Para cada $b \in B$, o espaço $p^{-1}(\{b\})$ é a *fibra sobre b* .

A definição significa que o espaço fibrado \mathbf{E} é localmente um produto de sua base \mathbf{B} e sua fibra \mathbf{F} . Globalmente isso não precisa ocorrer, o espaço fibrado não precisa ser homeomorfo ao produto de sua base com sua fibra. Quanto isso ocorre, o fibrado é chamado trivial.

Proposição 13.70. *Sejam \mathbf{B} e \mathbf{F} espaços topológicos e \mathbf{E} um espaço \mathbf{F} -fibrado sobre \mathbf{B} com projeção fibrada $p: E \rightarrow B$.*

1. *Para todo $b \in B$, a fibra $p^{-1}(\{b\})$ é homeomorfa a F ;*
2. *A projeção fibrada $p: E \rightarrow B$ é aberta e a topologia de \mathbf{B} é a topologia quociente de \mathbf{E} por p .*

Proposição 13.71. *Sejam \mathbf{B} e \mathbf{F} espaços topológicos. O produto $\mathbf{B} \times \mathbf{F}$ é um espaço \mathbf{F} -fibrado sobre \mathbf{B} com projeção fibrada $p_B: B \times F \rightarrow B$.*

Capítulo 14

Espaços Mensuráveis e de Medida

14.1 Espaço Mensurável

14.1.1 Sigma-Álgebras e Sub-Sigma-Álgebras

Definição 14.1. Seja X um conjunto. Uma *sigma-álgebra* sobre X é um conjunto $\mathcal{M} \subseteq \mathcal{P}(X)$ de subconjuntos X que satisfaz

1. (Vazio) $\emptyset \in \mathcal{M}$;
2. (Fechamento por complementação) Para todo $M \in \mathcal{M}$, $M^c \in \mathcal{M}$;
3. (Fechamento por união enumerável) Para toda sequência $(M_i)_{i \in \mathbb{N}}$ de conjuntos de \mathcal{M} ,

$$\bigcup_{i \in \mathbb{N}} M_i \in \mathcal{M}.$$

Vale notar que uma sigma-álgebra \mathcal{M} é uma álgebra booleana (4.18) e, portanto, todas propriedades de álgebras booleanas valem para uma sigma-álgebra. De fato, o *sigma* no nome vem da terceira propriedade das sigma-álgebras, pois veremos que essa propriedade tem a ver com um tipo de soma de medidas a ser definido adiante.

Proposição 14.1. *Seja X um conjunto não vazio e \mathcal{M} uma sigma-álgebra sobre X . Então*

1. (*Universo*) $X \in \mathcal{M}$;
2. (*Fechamento por interseção enumerável*) Para toda sequência $(M_i)_{i \in \mathbb{N}}$ de conjuntos de \mathcal{M} ,

$$\bigcap_{i \in \mathbb{N}} M_i \in \mathcal{M}.$$

Demonstração. 1. Da primeira propriedade de \mathcal{M} , tem-se que $\emptyset \in \mathcal{M}$. Da segunda propriedade de \mathcal{M} , tem-se que $X = \emptyset^c \in \mathcal{M}$.

2. Da segunda propriedade, tem-se que, para todo $i \in \mathbb{N}$, $M_i^c \in \mathcal{M}$. Da terceira propriedade de \mathcal{M} , tem-se que $\bigcup_{i \in \mathbb{N}} M_i^c \in \mathcal{M}$. Das Leis de De Morgan (4.27), tem-se que

$$\left(\bigcap_{i \in \mathbb{N}} M_i \right)^c = \bigcup_{i \in \mathbb{N}} (M_i)^c \in \mathcal{M},$$

e conclui-se que $\bigcap_{i \in \mathbb{N}} M_i \in \mathcal{M}$. ■

Exemplo 14.1. $\mathcal{M} = \{\emptyset, X\}$ e $\mathcal{M} = \wp(X)$ são sigma-álgebras sobre X .

Definição 14.2. Seja X um conjunto não vazio e \mathcal{M} uma sigma-álgebra sobre X . Uma *sub-sigma-álgebra* de \mathcal{M} é um conjunto $\mathcal{M}' \subseteq \mathcal{M}$ que é uma sigma-álgebra sobre X .

Definição 14.3. Um *espaço mensurável* é um par (X, \mathcal{M}) em que X é um conjunto não vazio e \mathcal{M} é uma sigma-álgebra sobre X . Um *conjunto mensurável* é um elemento da sigma-álgebra \mathcal{M} .

Proposição 14.2. Seja $(C_n)_{n \in \mathbb{N}}$ uma sequência de conjuntos.

1. A sequência

$$M_n := \bigcup_{k=0}^n C_k$$

é uma sequência crescente de conjuntos;

2. A sequência $D_0 := C_0$ e, para $n \in \mathbb{N}^*$,

$$D_n := C_n \setminus M_{n-1}$$

é uma sequência disjunta de conjuntos;

3.

$$\bigcup_{n \in \mathbb{N}} C_n = \bigcup_{n \in \mathbb{N}} M_n = \bigcup_{n \in \mathbb{N}} D_n.$$

14.1.2 Sigma-Álgebras Geradas

Proposição 14.3. Seja X um conjunto não vazio e $(\mathcal{M}_i)_{i \in I}$ uma família de sigma-álgebras sobre X . Então

$$\mathcal{M} := \bigcap_{i \in I} \mathcal{M}_i$$

é uma sigma-álgebra sobre X .

Demonstração. Como \mathcal{M}_i são sigma-álgebras, então $\emptyset \in \mathcal{M}_i$ para todo $i \in I$. Assim, segue que $\emptyset \in \mathcal{M}$. Ainda, se $A \in \mathcal{M}$, então $A \in \mathcal{M}_i$ para todo $i \in I$. Logo $A^c \in \mathcal{M}_i$ para todo $i \in I$, o que implica $A^c \in \mathcal{M}$. Por fim, se $(A_j)_{j \in \mathbb{N}}$ é uma sequência de conjuntos em \mathcal{M} , então $A_j \in \mathcal{M}$ para todo $j \in \mathbb{N}$. Mas isso implica que $A_j \in \mathcal{M}_i$ para todo $j \in \mathbb{N}$, $i \in I$, o que, por sua vez, implica que, para todo $i \in I$,

$$\bigcup_{j \in \mathbb{N}} A_j \in \mathcal{M}_i.$$

Então conclui-se que $\bigcup_{j \in \mathbb{N}} A_j \in \mathcal{M}$ e, portanto, \mathcal{M} é uma sigma-álgebra sobre X . ■

Definição 14.4. Seja X um conjunto e $\mathcal{C} \in \mathcal{P}(X)$ um conjunto de subconjuntos de X . A *sigma-álgebra gerada por \mathcal{C}* é a interseção da família de todas as sigma-álgebras sobre X de que \mathcal{C} é subconjunto, denotada $\langle \mathcal{C} \rangle$.

A sigma-álgebra gerada por um conjunto é a menor sigma-álgebra que contém esse conjunto no sentido que não existe subconjunto dessa sigma-álgebra que contenha o conjunto e também seja uma sigma-álgebra.

Exemplo 14.2. A sigma-álgebra sobre X gerada por \emptyset é $\{\emptyset, X\}$.

14.1.3 Limites de Conjuntos

Definição 14.5. 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

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

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

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

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

Proposição 14.4. 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 14.5. 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 crescente,

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

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

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

Definição 14.6. 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

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

14.2 Funções mensuráveis

Definição 14.7. Sejam $\mathbf{X} = (X, \mathcal{M}_X)$ e $\mathbf{Y} = (Y, \mathcal{M}_Y)$ espaços mensuráveis. Uma função mensurável de \mathbf{X} para \mathbf{Y} é uma função $f: X \rightarrow Y$ tal que, para todo $M \in \mathcal{M}$,

$$f^{-1}(M) \in \mathcal{M}_X.$$

Denota-se $f: \mathbf{X} \rightarrow \mathbf{Y}$. O conjunto dessas funções é denotado $\mathcal{M}(\mathbf{X}, \mathbf{Y})$.

Proposição 14.6. Seja \mathbf{X} um espaço mensurável. A função $\text{Id}_X: X \rightarrow X$ é uma função mensurável.

Proposição 14.7. Sejam \mathbf{X}_0 , \mathbf{X}_1 e \mathbf{X}_2 espaços mensuráveis e $f_0: \mathbf{X}_0 \rightarrow \mathbf{X}_1$ e $f_1: \mathbf{X}_1 \rightarrow \mathbf{X}_2$ funções mensuráveis. Então $f_1 \circ f_0: \mathbf{X}_0 \rightarrow \mathbf{X}_2$ é uma função mensurável.

14.2.1 Sigma-Álgebras Puxadas e Empurradas

Definição 14.8. Sejam X um conjunto, $\mathbf{Y} = (Y, \mathcal{M}_Y)$ um espaço mensurável e $f : X \rightarrow Y$ uma função. A *sigma-álgebra puxada* por f é

$$f^*(\mathcal{M}_Y) := \left\{ f^{-1}(M) \mid M \in \mathcal{M}_Y \right\}.$$

Proposição 14.8. Sejam X um conjunto, $\mathbf{Y} = (Y, \mathcal{M}_Y)$ um espaço mensurável e $f : X \rightarrow Y$ uma função. Então $\mathcal{M}_X := f^*(\mathcal{M}_Y)$, a *sigma-álgebra puxada* por f , é uma *sigma-álgebra* sobre X .

Demonstração. Primeiro, notemos que $\emptyset \in \mathcal{M}_X$, pois $\emptyset \in \mathcal{M}_Y$ e $f^{-1}(\emptyset) = \emptyset$ (3.13). Segundo, seja $B \in \mathcal{M}_X$. Então existe $A \in \mathcal{M}_Y$ tal que $B = f^{-1}(A)$. Como \mathcal{M}_Y é uma *sigma-álgebra*, então $A^c \in \mathcal{M}_Y$, o que implica $f^{-1}(A^c) \in \mathcal{M}_X$. Mas $(f^{-1}(A))^c = f^{-1}(A^c)$ (3.13). Então $B^c \in \mathcal{M}_X$. Terceiro, seja $(B_i)_{i \in \mathbb{N}}$ uma sequência de conjuntos de \mathcal{M}_X . Então, para todo $i \in I$, existe $A_i \in \mathcal{M}_Y$ tal que $B_i = f^{-1}(A_i)$. Como \mathcal{M}_Y é uma *sigma-álgebra*, então $\bigcup_{i \in \mathbb{N}} A_i \in \mathcal{M}_Y$. Isso implica que $f^{-1}(\bigcup_{i \in \mathbb{N}} A_i) \in \mathcal{M}_X$. Mas $f^{-1}(\bigcup_{i \in \mathbb{N}} A_i) = \bigcup_{i \in \mathbb{N}} f^{-1}(A_i)$ (3.13). Então $\bigcup_{i \in \mathbb{N}} B_i \in \mathcal{M}_X$ e, assim, conclui-se que \mathcal{M}_X é uma *sigma-álgebra* sobre X . ■

Definição 14.9. Sejam $\mathbf{X} = (X, \mathcal{M}_X)$ um espaço mensurável, Y um conjunto e $f : X \rightarrow Y$ uma função. A *sigma-álgebra empurrada* por f é

$$f_*(\mathcal{M}_X) := \left\{ M \subseteq Y \mid f^{-1}(M) \in \mathcal{M}_X \right\}.$$

Proposição 14.9. Sejam $\mathbf{X} = (X, \mathcal{M}_X)$ um espaço mensurável, Y um conjunto e $f : X \rightarrow Y$ uma função. Então $\mathcal{M}_Y := f_*(\mathcal{M}_X)$, a *sigma-álgebra empurrada* por f , é uma *sigma-álgebra* sobre Y .

Demonstração. Primeiro, notemos que $\emptyset \in \mathcal{M}_Y$, pois $\emptyset \in \mathcal{M}_X$ e $f^{-1}(\emptyset) = \emptyset$ (3.13). Segundo, seja $A \in \mathcal{M}_Y$. Então $f^{-1}(A) \in \mathcal{M}_X$, o que implica $(f^{-1}(A))^c \in \mathcal{M}_X$, pois \mathcal{M}_X é *sigma-álgebra*. Mas $(f^{-1}(A))^c = f^{-1}(A^c)$ (3.13), o que implica $f^{-1}(A^c) \in \mathcal{M}_X$ e, portanto, $A^c \in \mathcal{M}_Y$. Terceiro, seja $(A_i)_{i \in \mathbb{N}}$ uma sequência de conjuntos de \mathcal{M}_Y . Então, para todo $i \in \mathbb{N}$, $f^{-1}(A_i) \in \mathcal{M}_X$, o que implica que $\bigcup_{i \in \mathbb{N}} f^{-1}(A_i) \in \mathcal{M}_X$, pois \mathcal{M}_X é uma *sigma-álgebra*. Mas, como $\bigcup_{i \in \mathbb{N}} f^{-1}(A_i) = f^{-1}(\bigcup_{i \in \mathbb{N}} A_i)$ (3.13), segue que $\bigcup_{i \in \mathbb{N}} A_i \in \mathcal{M}_Y$ e, assim, conclui-se que \mathcal{M}_Y é uma *sigma-álgebra* sobre Y . ■

Proposição 14.10. Sejam $\mathbf{X} = (X, \mathcal{M}_X)$ e $\mathbf{Y} = (Y, \mathcal{M}_Y)$ espaços mensuráveis. Uma função $f : X \rightarrow Y$ é função mensurável de \mathbf{X} para \mathbf{Y} se, e somente se, a *sigma-álgebra* $f^*(\mathcal{M}_Y)$ puxada por f é uma sub-*sigma-álgebra* de \mathcal{M}_X .

$$f \in \mathcal{M}(\mathbf{X}, \mathbf{Y}) \iff f^*(\mathcal{M}_Y) \subseteq \mathcal{M}_X.$$

Demonstração. Suponha que f é uma função mensurável. Seja $B \in f^*(\mathcal{M}_Y)$. Então existe $A \in \mathcal{M}_Y$ tal que $B = f^{-1}(A)$. Como f é mensurável, vale $f^{-1}(A) \in \mathcal{M}_X$, o que implica $B \in \mathcal{M}_X$ e, portanto, $f^*(\mathcal{M}_Y) \subseteq \mathcal{M}_X$. Como $f^*(\mathcal{M}_Y)$ é uma sigma-álgebra sobre X pela proposição acima, segue que $f^*(\mathcal{M}_Y)$ é uma sub-sigma-álgebra de \mathcal{M}_X . Reciprocamente, suponha que $f^*(\mathcal{M}_Y)$ é uma sub-sigma-álgebra de \mathcal{M}_X . Seja $A \in \mathcal{M}_Y$. Então $f^{-1}(A) \in f^*(\mathcal{M}_Y)$. Mas como $f^*(\mathcal{M}_Y)$ é uma sub-sigma-álgebra de \mathcal{M}_X , segue que $f^{-1}(A) \in \mathcal{M}_X$, o que mostra que f é mensurável. ■

14.3 Produto de espaços mensuráveis

Definição 14.10. Seja $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{M}_i)_{i \in I}$ uma família de espaços mensuráveis. O *produto* da família $(\mathbf{X}_i)_{i \in I}$ é o par

$$\prod_{i \in I} \mathbf{X}_i := (X, \mathcal{M})$$

em que $X := \prod_{i \in I} X_i$ é o produto de conjuntos e

$$\mathcal{M} := \left\langle \bigcup_{i \in I} \pi_i^*(\mathcal{M}_i) \right\rangle.$$

Proposição 14.11. Seja $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{M}_i)_{i \in I}$ uma família de espaços mensuráveis. Então o produto $\prod_{i \in I} \mathbf{X}_i$ é um espaço mensurável.

Demonstração. Sejam $X := \prod_{i \in I} X_i$ e $\mathcal{M} = \langle \bigcup_{i \in I} \pi_i^*(\mathcal{M}_i) \rangle$. Devemos somente argumentar que \mathcal{M} é uma sigma-álgebra sobre $X = \prod_{i \in I} X_i$. Para isso, notemos que, para cada $i \in I$, a sigma-álgebra $\pi_i^*(\mathcal{M}_i)$ é a sigma-álgebra puxada por $\pi_i : X \rightarrow X_i$, portanto uma sigma-álgebra sobre X . Assim, sendo, $\bigcup_{i \in I} \pi_i^*(\mathcal{M}_i) \subseteq \mathcal{P}(X)$ e, portanto, a sigma-álgebra \mathcal{M} gerada por esse conjunto é uma sigma-álgebra sobre X . ■

Proposição 14.12. Seja $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{M}_i)_{i \in I}$ uma família de espaços mensuráveis. Para todo $i \in I$, a projeção canônica $\pi_i : \prod_{i \in I} X_i \rightarrow X_i$ é uma função mensurável.

Demonstração. Sejam $i \in I$ e $M \in \mathcal{M}_i$. Então $\pi_i^{-1}(M) \in \pi_i^*(\mathcal{M}_i)$ e, portanto, $\pi_i^{-1}(M) \in \mathcal{M}$. ■

Proposição 14.13 (Propriedade Universal). Seja $(\mathbf{X}_i)_{i \in I} = (X_i, \mathcal{M}_i)_{i \in I}$ uma família de espaços mensuráveis, $\mathbf{Y} = (Y, \mathcal{M}_Y)$ um espaço mensurável e, para todo $i \in I$, $f_i : \mathbf{Y} \rightarrow \mathbf{X}_i$ uma função mensurável. Então existe uma única função

mensurável $f : Y \rightarrow \prod_{i \in I} X_i$ tal que, para todo $i \in I$, $\pi_i \circ f = f_i$ (o diagrama comuta).

$$\begin{array}{ccc} & \prod_{i \in I} X_i & \\ f \nearrow & & \downarrow \pi_i \\ Y & \xrightarrow{f_i} & X_i \end{array}$$

Demonstração. Defina a função

$$\begin{aligned} f : Y &\longrightarrow \prod_{i \in I} X_i \\ y &\longmapsto (f_i(y))_{i \in I}. \end{aligned}$$

Da propriedade universal para o produto de conjuntos, f é a única função tal que, para todo $i \in I$, $\pi_i \circ f = f_i$. Basta mostrar que f é uma função mensurável. Para simplificar a notação, definamos $(X, \mathcal{M}) := \prod_{i \in I} X_i$. Todo elemento de \mathcal{M} é formado a partir de complementos e uniões de elementos de $\bigcup_{i \in I} \pi_i^*(\mathcal{M})$. Sendo assim, como f^{-1} preserva complemento e união, e $f^{-1}(\emptyset) = \emptyset$, se mostrarmos que, para todo $M \in \bigcup_{i \in I} \pi_i^*(\mathcal{M}_i)$, $f^{-1}(M) \in \mathcal{M}_Y$, seguirá que, para todo $M \in \mathcal{M}$, $f^{-1}(M) \in \mathcal{M}_Y$. Seja $M \in \bigcup_{i \in I} \pi_i^*(\mathcal{M}_i)$. Então existe $i \in I$ tal que $M \in \pi_i^*(\mathcal{M}_i)$ e, portanto, existe $M_i \in \mathcal{M}_i$ tal que $M = \pi_i^{-1}(M_i)$. Então segue que

$$f^{-1}(M) = f^{-1}(\pi_i^{-1}(M_i)) = (\pi_i \circ f)^{-1}(M_i) = f_i^{-1}(M_i)$$

e portanto, como f_i é mensurável, $f_i^{-1}(M_i) \in \mathcal{M}_Y$, portanto $f^{-1}(M) \in \mathcal{M}_Y$. Isso prova, pelos comentários anteriores, que para todo $M \in \mathcal{M}$, $f^{-1}(M) \in \mathcal{M}$ e, portanto, f é mensurável. ■

14.4 Espaços Mensuráveis Topológicos

Definição 14.11. Seja $\mathbf{X} = (X, \mathcal{T})$ um espaço topológico. A σ -álgebra topológica de \mathbf{X} é

$$\mathcal{M}_{\mathbf{X}} := \langle \mathcal{T} \rangle,$$

a σ -álgebra gerada pela topologia \mathcal{T} .

Essa σ -álgebra é comumente chamada de σ -álgebra de Borel e seus conjuntos mensuráveis de *boreianos* em homenagem ao matemático francês Émile Borel¹.

Proposição 14.14. Sejam $\mathbf{X} = (X, \mathcal{T})$ um espaço topológico e $\mathcal{B} \subseteq \mathcal{T}$ uma base da topologia. Então

$$\mathcal{M}_{\mathbf{X}} = \langle \mathcal{B} \rangle.$$

Demonstração. Queremos mostrar que $\langle \mathcal{B} \rangle = \langle \mathcal{T} \rangle$. Claramente, como $\mathcal{B} \subseteq \mathcal{T}$, então $\langle \mathcal{B} \rangle \subseteq \langle \mathcal{T} \rangle$. Para a inclusão contrária, seja $M \in \langle \mathcal{T} \rangle$. Então existe

■

14.4.1 Boreiano e função mensurável em \mathbb{R}

Definição 14.12. A álgebra de Borel \mathcal{B} é a sigma-álgebra sobre \mathbb{R} gerada pelo conjunto de intervalos abertos de \mathbb{R} da forma (a, b) , com $a, b \in \mathbb{R}$. Um conjunto de Borel é um elemento de \mathcal{B} .

Definição 14.13. A álgebra de Borel extendida $\overline{\mathcal{B}}$ é o conjunto de todos os conjuntos de Borel e de todos conjuntos de Borel unidos a $\{-\infty\}$, $\{+\infty\}$ ou $(-\infty, +\infty)$.

Definição 14.14. Seja (X, \mathcal{M}) um espaço mensurável. Uma função $f : X \rightarrow \mathbb{R}$ X -mensurável (ou mensurável) é uma função que satisfaz

$$\forall \alpha \in \mathbb{R} \quad \{x \in X : f(x) \leq \alpha\} \in \mathcal{M}.$$

Proposição 14.15. Seja (X, \mathcal{M}) um espaço mensurável e $f : X \rightarrow \mathbb{R}$. Então as quatro afirmações abaixo são equivalentes

1. $\forall \alpha \in \mathbb{R} \quad A_{\alpha} := \{x \in X \mid f(x) \leq \alpha\} \in \mathcal{M};$
2. $\forall \alpha \in \mathbb{R} \quad B_{\alpha} := \{x \in X \mid f(x) < \alpha\} \in \mathcal{M};$
3. $\forall \alpha \in \mathbb{R} \quad C_{\alpha} := \{x \in X \mid f(x) \geq \alpha\} \in \mathcal{M};$
4. $\forall \alpha \in \mathbb{R} \quad D_{\alpha} := \{x \in X \mid f(x) > \alpha\} \in \mathcal{M}.$

¹Félix Édouard Justin Émile Borel (7 January 1871 – 3 February 1956)

Demonstração. Claramente, como $A_\alpha^c = D_\alpha$, (1) e (4) são equivalentes; do mesmo modo, como $B_\alpha^c = C_\alpha$, (2) e (3) são equivalentes. Vamos demonstrar que (1) e (2) são equivalentes, o que demonstrará a proposição. ■

...

Proposição 14.16. *Seja (X, \mathcal{M}) um espaço mensurável e $f : X \rightarrow \mathbb{R}$. Então f é uma função mensurável de (X, \mathcal{M}) para $(\mathbb{R}, \mathcal{B})$ se, e somente se,*

$$\forall \alpha \in \mathbb{R} \quad \{x \in X \mid f(x) \leq \alpha\} \in \mathcal{M}.$$

14.5 Medida e Espaço de Medida

Definição 14.15. Seja $\mathbf{X} = (X, \mathcal{M})$ um espaço mensurável. Uma *medida* sobre \mathbf{X} é uma função $m: \mathcal{M} \rightarrow [0, \infty]$ que satisfaz

1. $m(\emptyset) = 0$;
2. Para toda sequência $(M_i)_{i \in \mathbb{N}}$ de conjuntos mensuráveis disjuntos aos pares,

$$m\left(\bigcup_{i \in \mathbb{N}} M_i\right) = \sum_{i \in \mathbb{N}} m(M_i).$$

Definição 14.16. Um *espaço de medida* é uma tripla (X, \mathcal{M}, m) em que (X, \mathcal{M}) é um espaço mensurável e m é uma medida sobre (X, \mathcal{M}) .

Proposição 14.17. Sejam (X, \mathcal{M}, m) um espaço de medida e $M_1, M_2 \in \mathcal{M}$ conjuntos mensuráveis tais que $M_1 \subseteq M_2$. Então

1. $m(M_1) \leq m(M_2)$;
2. $m(M_1) < +\infty \implies m(M_2 \setminus M_1) = m(M_2) - m(M_1)$.

Demonstração. Como $M_2 = M_1 \cup (M_2 \setminus M_1)$ e $M_1 \cap (M_2 \setminus M_1) = \emptyset$, segue que

$$m(M_2) = m(M_1) + m(M_2 \setminus M_1).$$

1. Daí, como $m(M_2 \setminus M_1) \geq 0$, segue que $m(M_2) \geq m(M_1)$.
2. Se $m(M_1) < +\infty$, então, subtraindo-a dos dois lados da equação, temos $m(M_2) - m(M_1) = m(M_2 \setminus M_1)$.

■

Proposição 14.18. Sejam (X, \mathcal{M}, m) um espaço de medida e $(M_n)_{n \in \mathbb{N}}$ uma sequência de conjuntos mensuráveis.

1. Se $(M_n)_{n \in \mathbb{N}}$ é crescente, então

$$m\left(\bigcup_{n \in \mathbb{N}} M_n\right) = \lim_{n \rightarrow +\infty} m(M_n);$$

2. Se $(M_n)_{n \in \mathbb{N}}$ é descrescente e $m(M_1) < +\infty$, então

$$m\left(\bigcap_{n \in \mathbb{N}} M_n\right) = \lim_{n \rightarrow +\infty} m(M_n).$$

Capítulo 15

Integração

Adotaremos nesta seção as definições de que, em $[0, \infty]$,

1. Para todo $c \in [0, \infty]$, $c + \infty = \infty + c = \infty$;
2. $0 \cdot \infty = \infty \cdot 0 = 0$;
3. Para todo $c \in]0, \infty]$, $c \cdot \infty = \infty \cdot c = \infty$.

15.1 Integral de Funções Mensuráveis Simples

Lembremos que a função indicadora de um conjunto X é a função

$$\begin{aligned} \mathbf{1}: \wp(X) &\longrightarrow 2^X \\ C &\longmapsto \mathbf{1}_C: X &\longrightarrow \{0, 1\} \\ x &\longmapsto \begin{cases} 1, & x \in C \\ 0, & x \notin C. \end{cases} \end{aligned}$$

Na proposição a seguir mostramos que funções indicadoras são mensuráveis se, e somente se, o conjunto que elas indicam são. Para fazer sentido uma função indicadora ser mensurável, precisamos dar uma estrutura mensurável para $\{0, 1\}$, e a estrutura que escolhemos é a álgebra discreta. Essa é a álgebra induzida se consideramos $\{0, 1\}$ como subconjunto de \mathbb{R} , logo a função indicadora será mensurável também como uma função para \mathbb{R} .

Proposição 15.1. *Seja (X, \mathcal{M}) um espaço mensurável. Um conjunto $M \subseteq X$ é mensurável se, e somente se, $\mathbf{1}_M \in \mathcal{M}(X, \{0, 1\}) \subseteq \mathcal{M}(X, \mathbb{R}^+)$ é mensurável.*

Demonstração. Basta notar que $\mathbf{1}_M^{-1}(\{1\}) = M$ e $\mathbf{1}_M^{-1}(\{0\}) = M^c$. Se M é mensurável, então M^c é mensurável, logo $\mathbf{1}_M$ também é. Reciprocamente, se $\mathbf{1}_M$ é mensurável, então $M = \mathbf{1}_M^{-1}(\{1\})$ é mensurável, pois $\{1\}$ é mensurável. ■

Usaremos funções indicadoras na teoria de integração. Elas permitem cancelar funções $f: X \rightarrow \mathbb{R}$ em um conjunto C se multiplicarmos f por $\mathbf{1}_C$ (com a multiplicação definida pontualmente). Nesse caso, temos a função

$$\begin{aligned} \mathbf{1}_C f: X &\longrightarrow \mathbb{R} \\ x &\longmapsto \mathbf{1}_C(x)f(x) = \begin{cases} f(x), & x \in C \\ 0, & x \notin C. \end{cases} \end{aligned}$$

Consideraremos primeiro funções que têm um número finito de valores. Essas funções são chamadas simples, por simplicidade de nomenclatura.

Definição 15.1. Seja (X, \mathcal{M}, m) um espaço de medida. Uma função *simples* em X é uma função $f: X \rightarrow \mathbb{R}$ tal que $f(X)$ é finito. A *partição por níveis* de f é o conjunto

$$\mathcal{P}_f := \{f^{-1}(c)\}_{c \in f(X)}.$$

Proposição 15.2. Sejam (X, \mathcal{M}, m) um espaço de medida e $f, f' \in \mathcal{M}(X, [0, \infty])$ funções simples mensuráveis.

1. A partição por níveis \mathcal{P}_f é uma partição por medida de X e

$$f = \bigoplus_{c \in f(X)} c \mathbf{1}_{f^{-1}(c)}.$$

2. A partição por níveis de $f + f'$ é mais grossa que o refinamento das partições por níveis de f e f' :

$$\mathcal{P}_{f+f'} \leq \mathcal{P}_f \vee \mathcal{P}_{f'}.$$

Definição 15.2. Sejam $X = (X, \mathcal{M}, m)$ um espaço de medida e $f \in \mathcal{M}(X, [0, \infty])$ uma função simples mensurável. A *integral* de f em X é

$$\int f dm := \bigoplus_{c \in f(X)} c m(f^{-1}(c)).$$

Para todo conjunto mensurável $M \in \mathcal{M}$, a *integral* de f sobre M em X é

$$\int_M f dm := \int \mathbf{1}_M f.$$

Quando for necessário explicitar a variável da função f , escreveremos

$$\int f(x) dm(x).$$

Para denotar a integral, a notação

$$\int_{x \in X} f(x)$$

também poderia ser usada, e teria a vantagem de se assemelhar mais com a notação de somatório

$$\sum_{i \in I} f_i.$$

A notação da definição, no entanto, tem a vantagem de evitar escrever a variável x , que é de fato desnecessária na maioria dos contextos. Essa notação não é usual e não será usada aqui.

Proposição 15.3. *Sejam $\mathbf{X} = (X, \mathcal{M}, m)$ um espaço de medida.*

1. *Para todo $M \in \mathcal{M}$, $\int \mathbf{1}_M = m(M)$.*

$$\int_M f = \sum_{c \in f(X)} c m(M \cap f^{-1}(c)).$$

2. *Se $f \in \mathcal{M}(\mathbf{X}, [0, \infty])$ é uma função simples mensurável, \mathcal{P} é uma partição tal que $\mathcal{P}_f \leq \mathcal{P}$ e, para todo $P \in \mathcal{P}$, $f|_P = c_P$, então*

$$\int f = \sum_{P \in \mathcal{P}} c_P m(P).$$

Demonstração. 1. Como $\mathbf{1}_M(X) = \{0, 1\}$, $\mathbf{1}_M^{-1}(1) = M$ e $\mathbf{1}_M^{-1}(0) = M^0$,

$$\int \mathbf{1}_M = \sum_{c \in \mathbf{1}_M(X)} c m(\mathbf{1}_M^{-1}(c)) = 1m(M) + 0m(M^0) = m(M).$$

■

Proposição 15.4. *Sejam (X, \mathcal{M}, m) um espaço de medida, $M \in \mathcal{M}$ um conjunto mensurável $f: X \rightarrow \mathbb{R}$ e $f': X \rightarrow \mathbb{R}$ funções simples e $a \in \mathbb{R}$. Então*

1. *A função af é função simples mensurável e $\int_M af = a \int_M f$.*

2. *A função $f + f'$ é função simples mensurável e $\int_M (f + f') = \int_M f + \int_M f'$.*

Demonstração. 1. Notemos que $(af)(X) = af(X)$, pois todo elemento de $(af)(X)$ é da forma ac , para $c \in f(X)$. Isso significa que $(af)(X)$ é finito, logo af é simples. Agora, separamos em dois casos. Se $a = 0$, então $af = 0f = 0$, logo $0f(X) = \{0\}$ e $(0f)^{-1}(0) = X$, portanto

$$\int_M 0f = \sum_{c \in (0f)(X)} cm(M \cap (0f)^{-1}(c)) = 0m(M \cap X) = 0 = 0 \int_m f.$$

Se $a \neq 0$, então

$$(af)^{-1}(ac) = \{x \in X \mid af(x) = ac\} = \{x \in X \mid f(x) = c\} = f^{-1}(c).$$

Nesse caso segue que

$$\begin{aligned} \int_M af &= \sum_{c \in (af)(X)} cm(M \cap (af)^{-1}(c)) \\ &= \sum_{c \in f(X)} acm(M \cap (af)^{-1}(ac)) \\ &= \sum_{c \in f(X)} acm(M \cap f^{-1}(c)) \\ &= a \sum_{c \in f(X)} cm(M \cap f^{-1}(c)) \\ &= a \int_M f. \end{aligned}$$

2. Notemos que

$$\begin{aligned} (f + f')(X) &= \{f(x) + f'(x) \mid x \in X\} \\ &= \left\{c + c' \mid (c, c') \in f(X) \times f'(X), f^{-1}(c) \cap (f')^{-1}(c') \neq \emptyset\right\} \\ &\subseteq f(X) + f'(X). \end{aligned}$$

Como $f(X) + f'(X)$ é finito, então $(f + f')(X)$ é finito, logo $f + f'$ é simples. Para todo $x \in X$, existem únicos $c \in f(X)$ e $c' \in f'(X)$ tais que $x \in f^{-1}(c)$ e $x \in (f')^{-1}(c')$, pois $\{f^{-1}(c)\}_{c \in f(X)}$ e $\{(f')^{-1}(c)\}_{c \in f'(X)}$ são partições de X . Logo $(f + f')(x) = f(x) + f'(x) = c + c' = (c + c')\mathbf{1}_{f^{-1}(c) \cap f'^{-1}(c')}(x)$, o que mostra que

$$f + f' = \sum_{c \in f(X)} \sum_{c' \in f'(X)} (c + c')\mathbf{1}_{f^{-1}(c) \cap f'^{-1}(c')}.$$

Como $\{f^{-1}(c) \cap f'^{-1}(c')\}_{(c,c') \in f(X) \times f'(X)} = \{f^{-1}(c)\}_{c \in f(X)} \vee \{(f')^{-1}(c)\}_{c \in f'(X)}$

é o refinamento comum da partição por níveis de $f + f'$, segue que

$$\begin{aligned}
 \int f + f' &= \bigoplus_{c \in f(X)} \bigoplus_{c' \in f(X)} (c + c') m(f^{-1}(c) \cap f^{-1}(c')) \\
 &= \bigoplus_{c \in f(X)} \bigoplus_{c' \in f(X)} c m(f^{-1}(c) \cap f^{-1}(c')) + c' m(f^{-1}(c) \cap f^{-1}(c')) \\
 &= \bigoplus_{c \in f(X)} c \left(\bigoplus_{c' \in f(X)} m(f^{-1}(c) \cap f^{-1}(c')) \right) \\
 &\quad + \bigoplus_{c' \in f(X)} c' \left(\bigoplus_{c \in f(X)} m(f^{-1}(c) \cap f^{-1}(c')) \right) \\
 &= \bigoplus_{c \in f(X)} c m(f^{-1}(c)) + \bigoplus_{c' \in f'(X)} c' m((f')^{-1}(c')) \\
 &= \int f + \int f'.
 \end{aligned}$$

■

Demonstração. Sejam $f = \sum_{i=1}^n c_i \mathbf{1}_{P_i}$, $g = \sum_{j=1}^m d_j \mathbf{1}_{Q_j}$, $I := \{1, \dots, n\}$ e $J := \{1, \dots, m\}$.

1. Se $c = 0$, vale a igualdade, pois $0f = 0\mathbf{1}_X$, logo

$$\int_M 0f = 0m(M \cap X) = 0 = 0 \int_M f.$$

Se $c \neq 0$, então $cf(X) = \{cc_1, \dots, cc_n\}$ e as constantes cc_1, \dots, cc_n são todas distintas. Definindo, para todo $i \in I$, $R_i := \{x \in X \mid cf(x) = cc_i\}$, os conjuntos R_1, \dots, R_n formam uma partição de X em conjuntos mensuráveis. Além disso, temos $R_i = P_i$ para todo $i \in I$ porque, como $c \neq 0$, segue que $f(x) = c_i$ se, e somente se, $cf(x) = cc_i$. Portanto

$$\int_M cf = \bigoplus_{i=1}^n cc_i m(R_i \cap M) = c \bigoplus_{i=1}^n c_i m(P_i \cap M) = c \int_M f.$$

2. Como $f(X)$ e $g(X)$ são conjuntos finitos,

$$(f + g)(X) := \{c_i + d_j \mid (i, j) \in I \times J\}$$

é um conjunto finito. No entanto, não necessariamente $(f + g)(X)$ tem mn elementos, pois podem existir $(i_1, j_1), (i_2, j_2) \in I \times J$ distintos tais que $c_{i_1} + d_{j_1} = c_{i_2} + d_{j_2}$. Sejam $e_1, \dots, e_l \in \mathbb{R}$ as constantes distintas tais que $(f +$

$g)(X) = \{e_1, \dots, e_l\}$, $K := \{1, \dots, l\}$ e $R_k := \{x \in X \mid (f + g)(x) = e_k\}$. Nesse caso, $\{R_k \mid k \in K\}$ é uma partição de X em conjuntos mensuráveis e

$$f + g = \bigoplus_{k=1}^l e_k \mathbf{1}_{R_k}.$$

Por outro lado, temos

$$\begin{aligned} (f + g)(x) &= f(x) + g(x) \\ &= \bigoplus_{i=1}^n c_i \mathbf{1}_{P_i}(x) + \bigoplus_{j=1}^m d_j \mathbf{1}_{Q_j}(x) \\ &= \\ f + g &= \bigoplus_{i=1}^n \bigoplus_{j=1}^m (c_i + d_j) \mathbf{1}_{P_i \cap Q_j}. \end{aligned}$$

Isso significa que os conjuntos

■

15.2 Integral de Funções Mensuráveis Positivas

15.3 Integral de Funções Mensuráveis

15.4 Teoremas de Convergência

15.5 Funções Absolutamente Integráveis

Lembremos que $\sup \text{ess}(f) := \inf \{c \in]0, \infty[\mid \forall_{x \in X}^{\circ} f(x) \leq c\}$.

Definição 15.3. Sejam \mathbf{X} um espaço de medida e $p \in [1, \infty]$. Uma função *absolutamente p-integrável*¹ é uma função $f \in \mathcal{M}(\mathbf{X}, [0, \infty])$ tal que

$$\int |f|^p dm < \infty.$$

O conjunto das quase-funções absolutamente p -integráveis é denotado $\mathcal{I}^p(\mathbf{X})$.

¹Essas funções não recebem esse nome usualmente. O espaço $\mathcal{I}^p(\mathbf{X})$ é geralmente chamado de espaço $L^p(\mathbf{X})$, em homenagem a Henri Lebesgue, embora de acordo com conjunto dos Bourbaki o criador dos espaços tenha sido Frigyes Riesz (https://en.wikipedia.org/wiki/Lp_space).

Uma função *absolutamente ∞ -integrável* é uma função $f \in \mathcal{M}(\mathbf{X}, [0, \infty])$ tal que

$$\sup \text{ess}(|f|) < \infty.$$

O conjunto das quase-funções absolutamente ∞ -integráveis é denotado $\mathcal{I}^\infty(\mathbf{X})$.

Definição 15.4. Sejam \mathbf{X} um espaço de medida e $p \in [1, \infty[$. A *norma* de $f \in \mathcal{I}^p(\mathbf{X})$ é

$$\|f\|_p := \left(\int |f|^p dm \right)^{\frac{1}{p}}.$$

A *norma* de $f \in \mathcal{I}^\infty(\mathbf{X})$ é

$$\|f\|_\infty := \sup \text{ess}(|f|).$$

O *produto interno* de $f, f' \in \mathcal{I}^2(\mathbf{X})$ é

$$\langle f, f' \rangle := \left(\int ff' dm \right).$$

Proposição 15.5. Sejam \mathbf{X} um espaço de medida e $p \in [1, \infty]$. O espaço $(\mathcal{I}^p(\mathbf{X}), \|\cdot\|_p)$ é um espaço normado completo. O espaço $(\mathcal{I}^2(\mathbf{X}), \langle \cdot, \cdot \rangle)$ é um espaço com produto interno.

Capítulo 16

Espaços Métricos

16.1 Os Espaços Métricos

16.1.1 Métricas

Definição 16.1. Seja M um conjunto. Uma *métrica* em M é uma função

$$d(\cdot, \cdot) : M \times M \longrightarrow [0, \infty[$$

que satisfaz

1. (Separação) Para todos $p, p' \in M$,

$$d(p, p') = 0 \iff p = p';$$

2. (Simetria) Para todos $p, p' \in M$

$$d(p, p') = d(p', p);$$

3. (Desigualdade Triangular) Para todos $p, p', p'' \in M$,

$$d(p, p'') \leq d(p, p') + d(p', p'').$$

A *distância* entre p e p' é o número real $d(p, p')$.

Na definição, enunciámos uma função com contradomínio $[0, \infty[$. No entanto, pode-se mostrar que qualquer função real que satisfaz separação, simetria e desigualdade triangular é positiva. Por isso a proposição seguinte.

Definição 16.2. Um *espaço métrico* é um par $\mathbf{M} = (M, d)$ em que M é um conjunto e d é uma métrica em M . Os elementos de M são *pontos*. Um *subespaço métrico* de \mathbf{M} é o par $\mathbf{S} = (S, d|_{S \times S})$.

Proposição 16.1. *Seja M um espaço métrico. Então*

1. (Positividade) Para todos $p, p' \in M$, $d(p, p') \geq 0$.
2. (Desigualdade Triangular Generalizada) Para todos $p_0, \dots, p_n \in M$,

$$d(p_0, p_n) \leq \sum_{i=1}^{n-1} d(p_i, p_{i+1})$$

Demonstração. 1. Sejam $p, p' \in M$. Da desigualdade triangular e da simetria de d , segue que

$$d(p, p) \leq d(p, p') + d(p', p) = 2d(p, p'),$$

Mas $d(p, p) = 0$, o que implica $d(p, p') \geq 0$.

2. Para $n = 1$, seja $p_1 \in M$; então $d(p_1, p_1) = 0$ e $\sum_{i=1}^0 d(p_i, p_{i+1}) = 0$, pois a soma é vazia. Para $n = 2$, sejam $p_1, p_2 \in M$; então $d(p_1, p_2)$ e $\sum_{i=1}^1 d(p_i, p_{i+1}) = d(p_1, p_2)$, e vale a propriedade. Para $n = 3$, sejam $p_1, p_2, p_3 \in M$; então a propriedade é a desigualdade triangular. Agora, sejam $n \geq 4$, $p_1, \dots, p_n \in M$ e assumamos que a propriedade vale para todo $k \in \mathbb{N}$, tal que $3 \leq k \leq n - 1$. Então

$$d(p_1, p_n) \leq \sum_{i=1}^{n-3} d(p_i, p_{i+1}) + d(p_{n-2}, p_n),$$

pois essa soma tem $n - 1$ termos e vale a hipótese de indução. Pela desigualdade triangular, vale que $d(p_{n-2}, p_n) \leq d(p_{n-2}, p_{n-1}) + d(p_{n-1}, p_n)$, e, portanto,

$$\begin{aligned} d(p_1, p_n) &\leq \sum_{i=1}^{n-3} d(p_i, p_{i+1}) + d(p_{n-2}, p_n) \\ &\leq \sum_{i=1}^{n-3} d(p_i, p_{i+1}) + d(p_{n-2}, p_{n-1}) + d(p_{n-1}, p_n) \\ &= \sum_{i=1}^{n-1} d(p_i, p_{i+1}). \end{aligned}$$

■

Alguns exemplos de métricas seguem.

Proposição 16.2. *Seja M um conjunto.*

1. A métrica discreta

$$\begin{aligned} d: M \times M &\longrightarrow [0, \infty[\\ (p, p') &\longmapsto \begin{cases} 0, & p = p' \\ 1, & p \neq p' \end{cases} \end{aligned}$$

é uma métrica em M .

Mostramos agora que podem-se definir distâncias a partir de distâncias já conhecidas no espaço.

Proposição 16.3. *Sejam M um conjunto e d_0, \dots, d_{n-1} métricas em M . Então a função*

$$\begin{aligned} d: M \times M &\longrightarrow \mathbb{R} \\ (p, p') &\longmapsto \sum_{i=0}^{n-1} d_i(p, p') \end{aligned}$$

é uma métrica em M .

Demonstração. 1. (Separação) Sejam $p, p' \in M$. Suponhamos que

$$d(p, p') = \sum_{i=0}^n d_i(p, p') = 0.$$

Como, para todo $i \in [n]$, $d_i(p, p') \geq 0$, então, para todo $i \in [n]$, $d_i(p, p') = 0$. Logo $p = p'$. Reciprocamente, suponhamos $p = p'$. Então, para todo $i \in [n]$, $d_i(p, p') = 0$, o que implica

$$d(p, p') = \sum_{i=0}^{n-1} 0 = 0.$$

2. (Simetria) Sejam $p, p' \in M$. Então, pela simetria de d_i para todo $i \in [n]$,

$$d(p, p') = \sum_{i=0}^{n-1} d_i(p, p') = \sum_{i=1}^{n-1} d_i(p, p') = d(p, p').$$

3. (Desigualdade Triangular) Sejam $p, p', p'' \in M$. Então, para todo $i \in [n]$, vale

$d_i(p, p'') \leq d_i(p, p') + d_i(p', p'')$ pela desigualdade triangular de d_i , e segue que

$$\begin{aligned} d(p, p'') &= \sum_{i=0}^{n-1} d_i(p, p'') \\ &\leq \sum_{i=0}^{n-1} (d_i(p, p') + d_i(p', p'')) \\ &= \sum_{i=0}^{n-1} d_i(p, p') + \sum_{i=0}^{n-1} d_i(p', p'') \\ &= d(p, p') + d(p', p''). \end{aligned}$$

■

Proposição 16.4. *Sejam M um conjunto não vazio e d_0, \dots, d_{n-1} métricas em M . Então a função*

$$\begin{aligned} d: M \times M &\longrightarrow \mathbb{R} \\ (p, p') &\longmapsto \max \{d_i(p, p') \mid i \in [n]\} \end{aligned}$$

é uma métrica em M .

Demonstração. Demonstraremos para $n = 2$, pois o caso geral é análogo.

1. (Separação) Sejam $p, p' \in M$. Suponhamos que

$$d(p, p') = \max\{d_1(p, p'), d_2(p, p')\} = 0.$$

Então $d_1(p, p') = 0$ ou $d_2(p, p') = 0$. Em ambos os casos, temos $p = p'$. Reciprocamente, suponhamos que $p = p'$. Então $d_1(p, p') = 0$ e $d_2(p, p') = 0$, o que implica $d(p, p') = \max\{d_1(p, p'), d_2(p, p')\} = 0$.

2. (Simetria) Sejam $p, p' \in M$. Então

$$d(p, p') = \max\{d_1(p, p'), d_2(p, p')\} = \max\{d_1(p', p), d_2(p', p)\} = d(p', p).$$

3. (Desigualdade Triangular) Sejam $p, p', p'' \in M$. Então $d(p, p'') = d_1(p, p'')$ ou $d(p, p'') = d_2(p, p'')$. No primeiro caso, segue que

$$d(p, p'') = d_1(p, p'') \leq d_1(p, p') + d_1(p', p'') \leq d(p, p') + d(p', p'').$$

No segundo caso, segue que

$$d(p, p'') = d_2(p, p'') \leq d_2(p, p') + d_2(p', p'') \leq d(p, p') + d(p', p'').$$

■

16.1.2 Diâmetro, Bolas e Conjuntos e Funções Limitadas

Definição 16.3. Sejam M um espaço métrico e $C \subseteq M$. O *diâmetro* de C é

$$\varnothing(C) := \sup(d(C \times C)) = \sup\{d(p, p') \mid p, p' \in C\}$$

se $d(C \times C)$ é limitado superiormente, e ∞ , caso contrário. Um *conjunto limitado* em M é um conjunto $C \subseteq M$ tal que $\varnothing(C) < \infty$.

Na definição, adotamos a convenção de que $\sup \emptyset = 0$ e $\sup [0, \infty[= \infty$. Isso é só parcialmente uma convenção, pois a ambiguidade não está em que valor atribuir a $\sup \emptyset$, mas sim em qual conjunto parcialmente ordenado está sendo considerado. Quando o conjunto ordenado é $[0, \infty]$, $\sup_{[0, \infty]} \emptyset = 0$; quando o conjunto ordenado é $[-\infty, +\infty]$, $\sup_{[-\infty, +\infty]} \emptyset = -\infty$, e assim por diante. Isso define uma função

$$\begin{aligned} \varnothing: \wp(M) &\longrightarrow [0, \infty] \\ C &\longmapsto \varnothing(C). \end{aligned}$$

Definição 16.4. Sejam M um espaço métrico, $c \in M$ e $r \in [0, \infty[$. A *bola aberta* de centro c e raio r em M é o conjunto

$$\circlearrowleft_r(c) := \{p \in M \mid d(c, p) < r\}.$$

A *bola fechada* de centro c e raio r em M é o conjunto

$$\overline{\circlearrowleft}_r(c) := \{p \in M \mid d(c, p) \leq r\}.$$



Figura 16.1: Bolas aberta e fechada de centro c e raio r , respectivamente.

Proposição 16.5. Sejam M um espaço métrico e $C \subseteq M$ um conjunto. Então C é um conjunto limitado se, e somente se, existe bola $\overline{\circlearrowleft}_r(c)$ tal que $C \subseteq \overline{\circlearrowleft}_r(c)$.

Demonstração. Se C é limitado, basta tomar $r = \varnothing(C)$ e $c \in C$. Reciprocamente, se existe bola $\overline{\circlearrowleft}_r(c)$ tal que $C \subseteq \overline{\circlearrowleft}_r(c)$, então para todos $p, p' \in C$, segue da desigualdade triangular que

$$d(p, p') \leq d(p, c) + d(c, p') \leq r + r = 2r,$$

portanto $\varnothing(C) \leq 2r \in [0, \infty[$. ■

Definição 16.5. Seja M um espaço métrico. Uma função *limitada* em M é uma função $f: X \longrightarrow M$ de um conjunto X para M cuja imagem $f(X)$ é limitada.

16.2 Topologia dos Espaços Métricos

16.2.1 Interior e Pontos Interiores

Definição 16.6. Sejam \mathbf{M} um espaço métrico e $C \subseteq M$ um conjunto. Um *ponto interior* de C é um ponto $p \in C$ para o qual existe um número real $r > 0$ tal que $\odot_r(p) \subseteq C$. O *interior* de C é o conjunto C° de todos pontos interiores de C . Um *conjunto aberto* de \mathbf{M} é um conjunto $A \subseteq M$ tal que $A = A^\circ$. O conjunto dos conjuntos abertos de \mathbf{M} é denotado \mathcal{T}_M .

Proposição 16.6. *Seja $\mathbf{M} = (M, d)$ um espaço métrico. Então*

1. *Para todo $c \in M$ e para todo número real $r > 0$, a bola aberta $\odot_r(c)$ é um conjunto aberto;*
2. *O conjunto \mathcal{T}_M é uma topologia de M .*

Demonstração. 1. Sejam $c \in M$ e $r \in]0, \infty[$. Queremos mostrar que $\odot_r(c)$ é aberto. Para isso, seja $p \in \odot_r(c)$. Então segue que $d := d(c, p) < r$, pela definição de bola aberta, e, portanto, $r - d \in]0, \infty[$. Para mostrar que essa bola centrada em p está contida na bola maior centrada em c , seja $p' \in \odot_{r-d}(p)$. Então $d(p, p') < r - d$ e, pela desigualdade triangular, segue que

$$d(c, p') \leq d(c, p) + d(p, p') < D + (r - d) = r,$$

o que mostra que $p' \in \odot_r(c)$ e que, portanto, $\odot_s(p) \subseteq \odot_r(c)$. Assim, mostramos que $\odot_r(c)$ é aberta.

2. (a) Podemos notar que \emptyset é aberto por vacuidade, pois, se não fosse, existiria $p \in \emptyset$ para o qual não há $r \in]0, \infty[$ satisfazendo $\odot_r(p) \subseteq \emptyset$, o que é absurdo. Para mostrar que M é aberto, sejam $p \in M$ e $r \in]0, \infty[$. Então $\odot_r(p) \subseteq M$, pois qualquer bola aberta é subconjunto de M . Portanto M é aberto.
- (b) Seja $(A_i)_{i \in I}$ uma família de abertos em \mathbf{M} e seja $p \in (A_i)_{i \in I}$. Então existe $k \in I$ tal que $p \in A_k$. Como A_k é aberto, então existe $r \in]0, \infty[$ tal que $\odot_r(p) \subseteq A_k$. Como $A_k \subseteq (A_i)_{i \in I}$, segue que $\odot_r(p) \subseteq (A_i)_{i \in I}$ e que, portanto, $(A_i)_{i \in I}$ é aberto.
- (c) Seja $(A_i)_{i \in [n]}$ uma sequência de abertos em \mathbf{M} e seja $p \in (A_i)_{i \in [n]}$. Então, para todo $k \in [n]$, $p \in A_k$. Como, para todo $k \in [n]$, A_k é aberto, segue que existe $r_k \in]0, \infty[$ tal que $\odot_{r_k}(p) \subseteq A_k$. Seja $r := \min\{r_k : k \in [n]\}$. Então, para todo $k \in [n]$, vale $\odot_r(p) \subseteq \odot_{r_k}(p)$, e segue que $\odot_r(p) \subseteq A_k$ e, portanto, $\odot_r(p) \subseteq (A_i)_{i \in [n]}$, o que mostra que $(A_i)_{i \in [n]}$ é aberto.

■

16.2.2 Limites e Convergência de Sequências

Definição 16.7. Sejam M um espaço métrico, $(p_n)_{n \in \mathbb{N}}$ uma sequência de pontos em M e $p \in M$. A sequência $(p_n)_{n \in \mathbb{N}}$ converge para o ponto p se, e somente se, para todo número real $\varepsilon > 0$, existe um número natural N tal que

$$\forall n \in \mathbb{N} \quad n \geq N \Rightarrow p_n \in \odot_\varepsilon(p).$$

Denota-se $(p_n)_{n \in \mathbb{N}} \rightarrow p$. O ponto p é um *limite* da sequência. Caso contrário, a sequência não converge para p . Uma *sequência convergente* é uma sequência que tem limite. Uma *sequência divergente* é uma sequência que não tem limite.

Proposição 16.7. *Todo espaço métrico M é um espaço topológico separado.*

Demonstração. Sejam $p, p' \in M$ pontos distintos. Mostraremos que existe um número real r tal que $0 < r \leq \frac{1}{2}d(p, p')$, e que isso implica que $\odot_r(p) \cap \odot_r(p') = \emptyset$. Como $p \neq p'$, então $d(p, p') > 0$, portanto existe $r \in \mathbb{R}$ tal que $0 < r \leq \frac{1}{2}d(p, p')$. Suponhamos que existe $p'' \in \odot_r(p) \cap \odot_r(p')$. Então $d(p, p'') < r$ e $d(p', p'') < r$. Mas, pela desigualdade triangular, segue que

$$d(p, p') \leq d(p, p'') + d(p'', p') < r + r \leq d(p, p'),$$

o que é absurdo. Portanto $\odot_r(p) \cap \odot_r(p') = \emptyset$. ■

Corolário 16.8. *Toda sequência convergente em um espaço métrico M tem limite único.*

Demonstração. Suponhamos que p, p' são limites de $(p_n)_{n \in \mathbb{N}}$. Se $p \neq p'$, então $d(p, p') > 0$. Seja $\varepsilon \in \mathbb{R}$ tal que $0 < \varepsilon \leq \frac{1}{2}d(p, p')$. Então existe $N_1 \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, se $n \geq N_1$, então $p_n \in \odot_\varepsilon(p)$, e existe $N_2 \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, se $n \geq N_2$, então $p_n \in \odot_\varepsilon(p')$. Assim, definindo $N := \max\{N_1, N_2\}$, segue que, se $n \geq N$, então $n \geq N_1$ e $n \geq N_2$, e, portanto, que $p_n \in \odot_\varepsilon(p)$ e $p_n \in \odot_\varepsilon(p')$; ou seja, $p_n \in \odot_\varepsilon(p) \cap \odot_\varepsilon(p')$, mas isso é absurdo, pois $\odot_\varepsilon(p) \cap \odot_\varepsilon(p') = \emptyset$. Portanto $p = p'$. ■

Essa proposição nos permite tratar o limite de uma sequência como um número único e, por isso, podemos usar a notação $\lim_{n \in \mathbb{N}} p_n = p$ para quando $(p_n)_{n \in \mathbb{N}} \rightarrow p$.

Proposição 16.9. *Uma sequência de em um espaço métrico M é convergente se, e somente se, todas suas subsequências são convergentes.*

Demonstração. Suponhamos que $(p_n) \rightarrow p$ e seja $(p_{n_k})_{k \in \mathbb{N}}$ uma subsequência de $(p_n)_{n \in \mathbb{N}}$. Seja $\varepsilon \in \mathbb{R}$ tal que $\varepsilon > 0$. Como $(p_n) \rightarrow p$, existe $N \in \mathbb{N}$ tal que, para

todo $n \in \mathbb{N}$, se $n \geq N$, então $p_n \in \odot_\varepsilon(p)$; como $(n_k)_{k \in \mathbb{N}}$ é estritamente crescente, existe $K \in \mathbb{N}$ tal que, para todo $k \in \mathbb{N}$, se $k \geq K$, então $n_k \geq N$. Mas então

$$k \geq K \Rightarrow n_k \geq N \Rightarrow p_{n_k} \in \odot_\varepsilon(p)$$

e, portanto, $(p_{n_k}) \rightarrow p$. Reciprocamente, se toda subsequência de $(p_n)_{n \in \mathbb{N}}$ converge para p , $(p_n)_{n \in \mathbb{N}}$, em particular, é uma dessas subsequências e, portanto, $(p_n) \rightarrow p$. \blacksquare

Proposição 16.10. *Toda sequência convergente em um espaço métrico M é limitada.*

Demonstração. Seja $(p_n)_{n \in \mathbb{N}}$ uma sequência de pontos em M tal que $(p_n) \rightarrow p$. Então, para $\varepsilon = 1$, existe $N \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, se $n \geq N$, então $p_n \in \odot_1(p)$. Assim, seja $l \in \mathbb{R}$ tal que

$$l > \max(\{1\} \cup \{d(p, p_n) : n \in [N]\}),$$

segue que, para todo $n \in \mathbb{N}$, $p_n \in \odot_l(p)$ pois, se $0 \leq n \leq N$, $d(p, p_n) < l$ pela definição de l e, se $n \geq N$, então $p_n \in \odot_1(p) \subseteq B_l(p)$, pois $1 < l$. Logo $(p_n)_{n \in \mathbb{N}}$ é limitada. \blacksquare

Proposição 16.11. *Sejam M um espaço métrico, $C \subseteq M$ um conjunto e $p \in M$. Então existe uma sequência de pontos em C que converge para p se, e somente se, para todo número real $\varepsilon > 0$, $C \cap \odot_\varepsilon(p) \neq \emptyset$.*

Demonstração. Suponhamos que exista uma sequência $(p_n)_{n \in \mathbb{N}}$ de pontos em C tal que $(p_n) \rightarrow p$. Então, para todo número real $\varepsilon > 0$, existe $N \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, se $n \geq N$, então $p_n \in \odot_\varepsilon(p)$. Mas isso implica que $p_n \in C \cap \odot_\varepsilon(p)$. Reciprocamente, suponhamos que, para todo número real $\varepsilon > 0$, $C \cap \odot_\varepsilon(p) \neq \emptyset$. Então, em particular, para todo $n \in \mathbb{N}$, escolhamos $p_n \in C \cap \odot_{\frac{1}{n}}(p)$. Assim, temos a sequência $(p_n)_{n \in \mathbb{N}}$. Para mostrar que $(p_n) \rightarrow p$, seja $\varepsilon \in \mathbb{R}$ tal que $\varepsilon > 0$. Então existe $N \in \mathbb{N}$ tal que $\frac{1}{N} \leq \varepsilon$. Mas isso implica que, para todo número natural $n \geq N$, $\frac{1}{n} \leq \frac{1}{N}$, e segue que

$$d(p, p_n) < \frac{1}{n} \leq \frac{1}{N} \leq \varepsilon$$

e, portanto, $(p_n) \rightarrow p$. \blacksquare

Proposição 16.12. *Sejam M um espaço métrico, $p, q \in M$ e $(p_n)_{n \in \mathbb{N}}$ e $(q_n)_{n \in \mathbb{N}}$ sequências em M que convergem para p e q respectivamente. Então a sequência $(d(p_n, q_n))_{n \in \mathbb{N}}$ em \mathbb{R} converge para $d(p, q)$.*

Demonstração. Para todo $n \in \mathbb{N}$, segue da desigualdade triangular que

$$d(p_n, q_n) \leq d(p_n, p) + d(p, q) + d(q, q_n).$$

Seja $\varepsilon > 0$ um número real. Então existem $N_{1,2} \in \mathbb{N}$ tais que

$$\forall n \in \mathbb{N} \quad n \geq N_1 \Rightarrow d(p, p_n) < \frac{\varepsilon}{2}$$

e

$$\forall n \in \mathbb{N} \quad n \geq N_2 \Rightarrow d(q, q_n) < \frac{\varepsilon}{2}.$$

Fazendo $N_3 := \max\{N_1, N_2\}$, segue que

$$\forall n \in \mathbb{N} \quad n \geq N_3 \Rightarrow d(p_n, q_n) \leq d(p_n, p) + d(p, q) + d(q, q_n) < d(p, q) + \varepsilon;$$

ou seja, $d(p_n, q_n) - d(p, q) < \varepsilon$. Analogamente, achamos $N_6 \in \mathbb{N}$ tal que

$$\forall n \in \mathbb{N} \quad n \geq N_6 \Rightarrow d(p_n, q_n) \leq d(p_n, p) + d(p, q) + d(q, q_n) < d(p, q) + \varepsilon$$

e fazendo $n := \max\{N_3, N_6\}$, segue que

$$\forall n \in \mathbb{N} \quad n \geq N \Rightarrow |d(p, q) - d(p_n, q_n)| < \varepsilon,$$

o que mostra que $(d(p_n, q_n)) \rightarrow d(p, q)$ em \mathbb{R} .

■

16.2.3 Fecho e Pontos Aderentes

Definição 16.8. Sejam M um espaço métrico e $C \subseteq M$ um conjunto. Um *ponto aderente* a C é um ponto $p \in M$ para o qual existe uma sequência $(p_n)_{n \in \mathbb{N}}$ de pontos de C que converge para p . O *fecho* de C é o conjunto \overline{C} de todos os pontos aderentes a C . Um *conjunto fechado* de M é um conjunto $F \subseteq M$ tal que $F = \overline{F}$.

Proposição 16.13. Sejam M um espaço métrico e $F \subseteq M$. Então F é um conjunto fechado se, e somente se, F^c é um conjunto aberto.

Demonstração. Suponhamos que F é um conjunto fechado. Se $F^c = \emptyset$, Mas \emptyset é aberto pois, caso contrário, existe $p \in \emptyset$ para o qual não há número real $\varepsilon > 0$ tal que $\odot_\varepsilon(p) \subseteq \emptyset$, mas isso é absurdo. Se $F^c \neq \emptyset$, seja $p \in F^c$. Se não existe número real $\varepsilon > 0$ tal que $\odot_\varepsilon(p) \subseteq F^c$, então, para todo número real $\varepsilon > 0$, $F \cap \odot_\varepsilon(p) \neq \emptyset$. Mas isso implica que existe uma sequência $(p_n)_{n \in \mathbb{N}}$ de pontos em F tal que $(p_n) \rightarrow p$. Como F é fechado, isso implica $p \in F$, o que é uma contradição. Então existe número real $\varepsilon > 0$ tal que $\odot_\varepsilon(p) \subseteq F^c$, e isso mostra que F^c é aberto.

Reciprocamente, suponhamos que F^c é aberto. Se $F = \emptyset$, então F é fechado. Se $F \neq \emptyset$, seja $(p_n)_{n \in \mathbb{N}}$ uma sequência em F que converge para $p \in M$. Suponhamos que $p \notin F$. Então $p \in F^c$ e, como F^c é aberto, existe um número real $\varepsilon > 0$ tal que $\bigcirc_\varepsilon(p) \subseteq F^c$. Como $(p_n) \rightarrow p$, existe $N \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, se $n \geq N$, então $p_n \in \bigcirc_\varepsilon(p)$. Mas isso implica que $p_N \in \bigcirc_\varepsilon(p) \subseteq F^c$, o que é absurdo, pois $p_N \in F$. Portanto $p \in F$ e isso mostra que F é fechado. ■

Proposição 16.14. *Seja M um espaço métrico. Então, para todo $c \in M$ e para todo número real $r > 0$, a bola fechada $\bar{\bigcirc}_r(c)$ é um conjunto fechado.*

Demonstração. Basta notar que $\bar{\bigcirc}_r(c)^c$ é aberto. ■

16.2.4 Conjuntos Densos

Definição 16.9. Sejam M um espaço métrico e $C \subseteq M$ um conjunto. Um conjunto *denso em C* é um conjunto $D \subseteq M$ tal que $C \subseteq \overline{D}$.

Isso que dizer que, para todo ponto de C , existe uma sequência em D que converge para esse ponto.

Proposição 16.15. *Sejam $M = (M, d)$ um espaço métrico e $C, D \subseteq M$ conjuntos. Então D é denso em C se, e somente se, para todo conjunto aberto A de M , $A \cap C \neq \emptyset$ implica $A \cap D \neq \emptyset$.*

Demonstração. Suponhamos que D é denso em C . Sejam A um conjunto aberto de M tal que $A \cap C \neq \emptyset$ e seja $p \in A \cap C$. Como D é denso em C e $p \in C$, existe uma sequência $(p_n)_{n \in \mathbb{N}}$ em D que converge para p . Como A é aberto e $p \in A$, existe um número real $\varepsilon > 0$ tal que $\bigcirc_\varepsilon(p) \subseteq A$. Então, como $(p_n) \rightarrow p$, existe um número natural N tal que, para todo natural $n \geq N$, $p_n \in \bigcirc_\varepsilon(p)$. Mas isso implica que $p_n \in A \cap D$.

Reciprocamente, suponhamos que, para todo conjunto aberto A de M , $A \cap C \neq \emptyset$ implica $A \cap D \neq \emptyset$. Se $C = \emptyset$, então $C \subseteq \overline{D}$. Se $C \neq \emptyset$, seja $p \in C$. Para todo $n \in \mathbb{N}$, o conjunto $\bigcirc_{\frac{1}{n}}(p)$ é um conjunto aberto que contém p . Mas então $\bigcirc_{\frac{1}{n}}(p) \cap C \neq \emptyset$, o que implica $\bigcirc_{\frac{1}{n}}(p) \cap D \neq \emptyset$. Para cada $n \in \mathbb{N}$, escolhemos $p_n \in \bigcirc_{\frac{1}{n}}(p) \cap D$. Assim, temos uma sequência $(p_n)_{n \in \mathbb{N}}$ de pontos em D que converge para p , pois, para todo número real $\varepsilon > 0$, existe um natural N tal que $\frac{1}{N} \leq \varepsilon$ e, então

$$\forall n \in \mathbb{N} \quad n \geq N \Rightarrow \frac{1}{n} \leq \frac{1}{N} \leq \varepsilon \Rightarrow p_n \in \bigcirc_{\frac{1}{n}}(p) \subseteq \bigcirc_{\frac{1}{N}}(p) \subseteq \bigcirc_\varepsilon(p).$$

Isso mostra que $p \in \overline{D}$ e, portanto, que $C \subseteq \overline{D}$. ■

Proposição 16.16. *Sejam M_1 e M_2 espaços métricos e $f, g: M_1 \rightarrow M_2$ funções contínuas. Então o conjunto*

$$F := \{p \in M_1 \mid f(p) = g(p)\}$$

é um conjunto fechado.

Demonstração. Se $F = \emptyset$, então F é fechado. Se $F \neq \emptyset$, seja $(p_n)_{n \in \mathbb{N}}$ uma sequência em F que converge para $p \in M_1$. Mostraremos que $p \in F$. Como f e g são contínuas em p , segue que

$$(f(p_n)) \rightarrow f(p) \quad \text{e} \quad (g(p_n)) \rightarrow g(p).$$

Como $(p_n)_{n \in \mathbb{N}}$ é uma sequência em F , as sequências $(f(p_n))_{n \in \mathbb{N}}$ e $(g(p_n))_{n \in \mathbb{N}}$ são a mesma sequência e segue da unicidade do limite que $f(p) = g(p)$, o que mostra que $p \in F$ e que, portanto, F é um conjunto fechado. ■

Proposição 16.17. *Sejam M_1 e M_2 espaços métricos, $f, g: M_1 \rightarrow M_2$ funções contínuas e $C, D \subseteq M_1$ conjuntos tais que D é denso em C . Se $f|_D = g|_D$, então $f|_C = g|_C$.*

Demonstração. Pela proposição anterior, sabemos que $F := \{p \in M_1 : f(p) = g(p)\}$ é um conjunto fechado. Como $f|_D = g|_D$, então $D \subseteq F$. Mas isso significa que $\overline{D} \subseteq \overline{F} = F$ e, como D é denso em C , segue que $C \subseteq \overline{D} \subseteq F$ e, portanto, que $f|_C = g|_C$. ■

16.2.5 Conjuntos Compactos

Proposição 16.18. *Sejam M um espaço métrico e $C \subseteq M$. Se C é compacto, então é limitado.*

Demonstração. Seja $p \in M$ e consideremos a cobertura $\{\odot_r(p) \mid r \in]0, \infty[\}$ de C . Pela compacidade, existe subcobertura finita $\{\odot_{r_0}(p), \dots, \odot_{r_{n-1}}(p)\}$ de C . Tomando $r := \max\{r_i \mid i \in [n]\}$, segue que $\odot_{r_i}(p) \subseteq \odot_r(p)$ para todo $i \in [n]$, logo $C \subseteq \odot_r(p)$, o que implica que $\varnothing(C) \leq 2r < \infty$. ■

A recíproca nem sempre é verdade. Nos espaços \mathbb{R}^d , $d \in \mathbb{N}$, vale que um conjunto é compacto se, e somente se, é fechado e limitado. Esse resultado é conhecido como Teorema de Heine-Borel. No entanto, isso não vale em qualquer espaço métrico¹.

¹Para mais detalhes, conferir <https://math.stackexchange.com/questions/674982/difference-between-closed-bounded-and-compact-sets>.

16.2.6 Continuidade

Definição 16.10. Sejam M e M' espaços métricos e $p \in M$. Uma função *contínua em p* é uma função $f: M \rightarrow M'$ que satisfaz: para todo $\varepsilon \in]0, \infty[$, existe $\delta \in]0, \infty[$ tal que, para todo $x \in M$

$$x \in \odot_\delta(p) \Rightarrow f(x) \in \odot_\varepsilon(f(p)).$$

Uma função *descontínua* em p é uma função que não é contínua em p .

Denotamos as bolas abertas em M e em M' por \odot , mas deve-se perceber que elas são relativas a métricas possivelmente diferentes.

Proposição 16.19. Sejam M_1 e M_2 espaços métricos, $f: M_1 \rightarrow M_2$ uma função e $p \in M_1$. Então f é contínua em p se, e somente se, para toda sequência $(p_n)_{n \in \mathbb{N}}$ de pontos em M_1 que converge para p , a sequência $(f(p_n))_{n \in \mathbb{N}}$ de pontos em M_2 converge para $f(p)$; ou seja

$$\lim f(p_n) = f(\lim p_n).$$

Demonstração. Suponhamos que f é contínua em p . Seja $(p_n)_{n \in \mathbb{N}}$ uma sequência de pontos em M_1 que converge para p . Seja um número real $\varepsilon > 0$. Como f é contínua, existe um número real $\delta > 0$ tal que $p_n \in \odot_\delta(p)$ implica $f(p_n) \in \odot_\varepsilon(f(p))$. Mas, como $(p_n) \rightarrow p$, existe $N \in \mathbb{N}$ tal que

$$\forall n \in \mathbb{N} \quad n \geq N \Rightarrow p_n \in \odot_\delta(p) \Rightarrow f(p_n) \in \odot_\varepsilon(f(p))$$

o que mostra que $(f(p_n)) \rightarrow f(p)$.

Reciprocamente, suponhamos que, para toda sequência $(p_n)_{n \in \mathbb{N}}$ em M_1 que converge para p , a sequência $(f(p_n))_{n \in \mathbb{N}}$ converge para $f(p)$. Suponhamos, por absurdo, que f não é contínua em p . Então existe um número real $\varepsilon > 0$ tal que, para todo número real $\delta > 0$, existe $x \in M_1$ tal que $x \in \odot_\delta(p)$, mas $f(x) \notin \odot_\varepsilon(f(p))$. Vamos mostrar que isso implica que existe uma sequência $(p_n)_{n \in \mathbb{N}}$ em M_1 que converge para p , mas que a sequência $(f(p_n))_{n \in \mathbb{N}}$ não converge para $f(p)$; ou seja, que existe um número real $\varepsilon > 0$ tal que, para todo número natural N , existe $n \in \mathbb{N}$ tal que $n \geq N$, mas $f(p_n) \notin \odot_\varepsilon(f(p))$. Seja $n \in \mathbb{N}$ e tomemos $\delta = \frac{1}{n}$. Então existe $x \in M_1$ tal que $x \in \odot_{\frac{1}{n}}(p)$, mas $f(x) \notin \odot_\varepsilon(f(p))$. Nomeando esse $x \in M_1$ de p_n , obtemos uma sequência $(p_n)_{n \in \mathbb{N}}$ que converge para p pois, para todo número real $\varepsilon' > 0$, existe um número natural $N \in \mathbb{N}$ tal que $\frac{1}{N} \leq \varepsilon'$ e isso implica que

$$\forall n \in \mathbb{N} \quad n \geq N \Rightarrow \frac{1}{n} \leq \frac{1}{N} \leq \varepsilon' \Rightarrow p_n \in \odot_{\frac{1}{n}}(p) \subseteq \odot_{\frac{1}{N}}(p) \subseteq \odot_{\varepsilon'}(p).$$

No entanto, $(f(p_n))_{n \in \mathbb{N}}$ é uma sequência que não converge para $f(p)$ pois, considerando o ε original tomado da descontinuidade de f , para todo número natural N , $f(p_N) \notin \odot_\varepsilon(f(p))$ e isso contradiz a hipótese de que, para toda sequência $(p_n)_{n \in \mathbb{N}}$ em M_1 que converge para p , a sequência $(f(p_n))_{n \in \mathbb{N}}$ converge para $f(p)$. Portanto f é contínua. ■

Definição 16.11. Sejam M_1 e M_2 espaços métricos, $D \subseteq M_1$ e $f : D \rightarrow M_2$ uma função. A função f é *contínua* em D se ela é contínua em todo ponto de D . Caso contrário, a função f é *descontínua* em D . Para $D = M_1$, dizemos simplesmente que f é contínua ou descontínua.

16.2.7 Ponto Limite e Conjunto Derivado

Definição 16.12. Sejam M um espaço métrico e $C \subseteq M$ um conjunto. Um *ponto limite* (ou *ponto de acumulação*) de C é um ponto $p \in M$ para o qual existe uma sequência $(p_n)_{n \in \mathbb{N}}$ de pontos de $C \setminus \{p\}$ que converge para p . O *derivado* de C é o conjunto de todos os pontos limites de C .

Da definição, segue que $C' \subseteq \bar{C}$. A inclusão contrária caracteriza a seção a seguir.

Definição 16.13. Sejam M um espaço métrico e $C \subseteq M$ um conjunto. Um *ponto isolado* de C é um ponto $p \in M$ que é um ponto aderente a C mas que não é um ponto limite de C .

Um ponto isolado de C é um ponto $p \in \bar{C} \setminus C'$.

16.2.8 Separação Métrica

Definição 16.14. Seja M um espaço métrico. Conjuntos *metricamente separados* de M são conjuntos $C, C' \subseteq M$ tais que

$$d(C, C') > 0.$$

16.3 Estrutura Uniforme

16.3.1 Sequências Aproximantes

Definição 16.15. Seja M um espaço métrico. Uma sequência *aproximante* em M é uma sequência $(p_n)_{n \in \mathbb{N}}$ de pontos em M tal que, para todo número real $\varepsilon > 0$, existe um número natural N satisfazendo

$$\forall n, m \in \mathbb{N} \quad n, m \geq N \Rightarrow d(p_n, p_m) < \varepsilon.$$

Essas sequências são conhecidas como *sequências de Cauchy*. O nome aproximante se dá pelo fato de que os termos da sequência ficam cada vez mais próximos entre si, e será adotado por ser mais intuitivo, embora não seja a nomenclatura padrão.

Proposição 16.20. *Toda sequência convergente em um espaço métrico M é aproximante.*

Demonstração. Seja $(p_n)_{n \in \mathbb{N}}$ uma sequência em M que converge para p . Seja $\varepsilon \in \mathbb{R}$ tal que $\varepsilon > 0$. Então $\frac{1}{2}\varepsilon > 0$ é um número real e segue que existe $N \in \mathbb{N}$ tal que, para todo número natural $n \geq N$, $p_n \in \odot_{\frac{1}{2}\varepsilon}(p)$. Assim, segue que

$$\forall n, m \in \mathbb{N} \quad n, m \geq N \Rightarrow d(p_n, p_m) \leq d(p_n, p) + d(p, p_m) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

o que mostra que $(p_n)_{n \in \mathbb{N}}$ é uma sequência aproximante. ■

Proposição 16.21. *Toda sequência aproximante em um espaço métrico M que tem uma subsequência convergente é convergente.*

Demonstração. Seja $(p_{n_k})_{k \in \mathbb{N}}$ uma subsequência de $(p_n)_{n \in \mathbb{N}}$ que converge para p . Seja $\varepsilon > 0$ um número real. Como $(p_n)_{n \in \mathbb{N}}$ é uma sequência de Cauchy e $\frac{1}{2}\varepsilon > 0$ é um número real, existe um número natural N tal que

$$\forall n, m \in \mathbb{N} \quad n, m \geq N \Rightarrow d(p_n, p_m) < \frac{\varepsilon}{2}.$$

Como $(p_{n_k})_{k \in \mathbb{N}}$ é uma subsequência convergente, existe $K_1 \in \mathbb{N}$ tal que

$$\forall k \in \mathbb{N} \quad k \geq K_1 \Rightarrow d(p, p_{n_k}) < \frac{\varepsilon}{2}.$$

Como $(n_k)_{k \in \mathbb{N}}$ é uma sequência estritamente crescente, existe $K_2 \in \mathbb{N}$ tal que, para todo número natural $k \geq K_2$, $n_k \geq N$. Assim, tomando $K := \max\{K_1, K_2\}$, segue que, para todo número natural $n \in \mathbb{N}$, existe $k \in \mathbb{N}$ tal que $n_k \geq N$ e, pela desigualdade triangular, que

$$\forall n \in \mathbb{N} \quad n \geq N \Rightarrow d(p_n, p) \leq d(p_n, p_{n_k}) + d(p_{n_k}, p) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$
■

Proposição 16.22. *Toda sequência aproximante em um espaço métrico M é limitada.*

Demonstração. Seja $(p_n)_{n \in \mathbb{N}}$ uma sequência aproximante em \mathbf{M} . Então, para $\varepsilon = 1$, existe $N \in \mathbb{N}$ tal que

$$\forall n, m \in \mathbb{N} \quad n, m \geq N \Rightarrow d(p_n, p_m) < 1.$$

Definamos $P := \{p_n : n \in \mathbb{N}\}$. Então segue que

$$\begin{aligned} \sigma(P) &= \sup \{d(p_n, p_m) \mid n, m \in \mathbb{N}\} \\ &= \max\{1 \cup \{d(p_n, p_m) \mid 0 \leq n, m \leq N\}\} \in \mathbb{R}, \end{aligned}$$

o que mostra que $(p_n)_{n \in \mathbb{N}}$ é limitada. ■

16.3.2 Continuidade Uniforme

Definição 16.16. Sejam \mathbf{M}_1 e \mathbf{M}_2 espaços métricos. Uma função *uniformemente contínua* é uma função $f : M_1 \rightarrow M_2$ tal que, para todo número real $\varepsilon > 0$, existe um número real $\delta > 0$ tal que

$$\forall p_1, p_2 \in M_1 \quad d_1(p_1, p_2) < \delta \Rightarrow d_2(f(p_1), f(p_2)) < \varepsilon.$$

Proposição 16.23. Sejam \mathbf{M}_1 e \mathbf{M}_2 espaços métricos, $f : M_1 \rightarrow M_2$ uma função uniformemente contínua e $(p_n)_{n \in \mathbb{N}}$ uma sequência aproximante em M_1 . Então a sequência $(f(p_n))_{n \in \mathbb{N}}$ em M_2 é aproximante.

Demonstração. Seja $\varepsilon > 0$ um número real. Da continuidade uniforme de f , existe um número real $\delta > 0$ tal que, para todo $p, p' \in M_1$, $d_1(p, p') < \delta$ implica $d_2(f(p), f(p')) < \varepsilon$. Como $(p_n)_{n \in \mathbb{N}}$ é sequência aproximante, existe $N \in \mathbb{N}$ tal que

$$\forall n, m \in \mathbb{N} \quad n, m \geq N \Rightarrow d_1(p_n, p_m) < \delta.$$

Mas, da continuidade uniforme de f , isso implica que

$$\forall n, m \in \mathbb{N} \quad n, m \geq N \Rightarrow d_1(p_n, p_m) < \delta \Rightarrow d_2(f(p_n), f(p_m)) < \varepsilon,$$

e isso mostra que $(f(p_n))_{n \in \mathbb{N}}$ é uma sequência aproximante. ■

16.3.3 Espaços Métricos Completos

Definição 16.17. Um espaço métrico *completo* é um espaço métrico em que todas sequências aproximantes convergem.

Proposição 16.24. Seja \mathbf{M} um espaço métrico. Todo subespaço completo de \mathbf{M} é um conjunto fechado em \mathbf{M} .

Demonstração. Sejam $C \subseteq M$ subespaço métrico completo e $(p_n)_{n \in \mathbb{N}}$ uma sequência convergente em C . Então $(p_n)_{n \in \mathbb{N}}$ é aproximante e, como C é completo, converge para um ponto em C , o que significa que C é fechado. ■

Proposição 16.25. *Sejam M um espaço métrico, $C \subseteq M$ um subespaço completo e $F \subseteq C$ um conjunto fechado em M . Então F é completo.*

Demonstração. Seja $(p_n)_{n \in \mathbb{N}}$ uma sequência aproximante em F . Então $(p_n)_{n \in \mathbb{N}}$ é uma sequência aproximante em C e, como C é completo, $(p_n)_{n \in \mathbb{N}}$ converge. Porém, como F é fechado, então $(p_n)_{n \in \mathbb{N}}$ converge para um ponto em F , o que mostra que F é completo. ■

Teorema 16.26. *Seja M um espaço métrico. Então M é completo se, e somente se, para toda sequência descendente $(F_n)_{n \in \mathbb{N}}$ de conjuntos não vazios e fechados em M tais que $(\varnothing(F_n))_{n \in \mathbb{N}} \rightarrow 0$ em \mathbb{R} , vale que*

$$\bigcap_{n \in \mathbb{N}} A_n \neq \emptyset.$$

Teorema 16.27. *Sejam M_1 um espaço métrico, M_2 espaço métrico completo, $D \subseteq M_1$ um conjunto denso em M_1 e $f : D \rightarrow M_2$ uma função uniformemente contínua. Então f tem uma única extensão para uma função uniformemente contínua $f^* : M_1 \rightarrow M_2$. Ainda, se f é uma isometria, então f^* é uma isometria.*

Demonstração. Seja $p \in M_1$. Como D é denso em M_1 , existe uma sequência $(p_n)_{n \in \mathbb{N}}$ em D que converge para p . Como $(p_n)_{n \in \mathbb{N}}$ é convergente, é uma sequência de Cauchy e, como f é uniformemente contínua em D , segue que $(f(p_n))_{n \in \mathbb{N}}$ é uma sequência de Cauchy em M_2 . Mas M_2 é completo, o que implica que $(f(p_n))_{n \in \mathbb{N}}$ converge para um ponto $p' \in M_2$. Definimos, portanto, a função f^* em p como $f^*(p) = p'$. Precisamos mostrar que f^* independe da escolha da sequência em D que converge para p . Se $(q_n)_{n \in \mathbb{N}}$ é uma sequência em D que converge para p , definamos a sequência $(r_n)_{n \in \mathbb{N}}$ em D por

$$r_n := \begin{cases} p_n & \text{se } n = 2k \\ q_n & \text{se } n = 2k + 1. \end{cases}$$

A sequência $(r_n)_{n \in \mathbb{N}}$ converge para p e, portanto, é uma sequência de Cauchy. A continuidade uniforme de f implica que a sequência $(f(r_n))_{n \in \mathbb{N}}$ é de Cauchy e, portanto, como $(f(p_n))_{n \in \mathbb{N}} = (f(r_{2k}))_{k \in \mathbb{N}}$ é uma subsequência que converge para p' , a sequência $(f(r_n))_{n \in \mathbb{N}}$ converge para p' , o que implica que a subsequência $(f(q_n))_{n \in \mathbb{N}} = (f(r_{2k+1}))_{k \in \mathbb{N}}$ converge para p' . Assim, mostramos que f^* está bem definida. Claramente, se $p \in D$, então $f(p) = f^*(p)$, pois, como D é denso em M_1 , se $(p_n)_{n \in \mathbb{N}}$ é uma sequência em D que converge para p , então, como f é contínua, segue que $f(p_n) \rightarrow f(p)$, o que mostra que $f^*(p) = f(p)$.

Agora, devemos mostrar que f^* é uniformemente contínua. Seja $\varepsilon > 0$ um número real, então $\frac{1}{2}\varepsilon > 0$ é um número real e, como f é uniformemente contínua, existe número real $\delta > 0$ tal que

$$\forall p, p' \in M_1 \quad d_1(p, p') < \delta \Rightarrow d_2(f(p), f(p')) < \frac{\varepsilon}{2}.$$

Assim, sejam $p, q \in M_1$ tais que $d_1(p, q) < \delta$. Queremos mostrar que $d_2(f(p), f(q)) < \varepsilon$. Sejam $(p_n)_{n \in \mathbb{N}}$ e $(q_n)_{n \in \mathbb{N}}$ sequências que convergem para p e q , respectivamente. Então $d_1(p_n, q_n) \rightarrow d_1(p, q)$ em \mathbb{R} .

...

A unicidade de f^* ocorre pois, se existem f^* e f'^* uniformemente contínuas que extendem f , como D é denso em M_1 e $f^*|_D = f'^*|_D$, segue que $f^* = f'^*$.

Por fim, mostramos que a isometria se preserva... ■

Definição 16.18. Seja M_1 um espaço métrico. Um *completamento* de M é um espaço métrico M_2 completo tal que M_1 é denso em M_2 .

Proposição 16.28. Seja M um espaço métrico e M_1 e M_2 completamentos de M . Então existe uma isometria entre M_1 e M_2 que é a função identidade quando restrita a M .

Demonstração. Seja f a função identidade em M . Pela proposição anterior, existe uma única extensão uniformemente contínua de f^* em M_1 ... ■

...

Proposição 16.29. Sejam $K \subseteq M$ compacto e $f : M \rightarrow \bar{M}$ contínua. Então f é uniformemente contínua.

Demonstração. Suponhamos, por absurdo, que f não é uniformemente contínua. Então existem $\varepsilon > 0$ e $(x_n)_{n \in \mathbb{N}}, (y_n)_{n \in \mathbb{N}}$ sequências em K tais que

$$\|x_n - y_n\| < \frac{1}{n} \quad \text{e} \quad \|f(x_n) - f(y_n)\| \geq \varepsilon.$$

Como K é compacto, existem subsequências $(x_{n_k})_{k \in \mathbb{N}}$ e $(y_{n_k})_{k \in \mathbb{N}}$ convergindo a $x \in K$ com $\|f(x_{n_k}) - f(y_{n_k})\| \geq \varepsilon$. Por continuidade de f , existe $\delta > 0$ tal que, se $x_{n_k}, y_{n_k} \in B(x, \delta)$, então $\|f(x_{n_k}) - f(x)\| < \frac{\varepsilon}{2}$ e $\|f(y_{n_k}) - f(x)\| < \frac{\varepsilon}{2}$. Pela desigualdade triangular, temos um absurdo. ■

16.4 Funções que Preservam Distância

16.4.1 Funções Métricas (ou Subsemelhanças)

Definição 16.19. Sejam M_0 e M_1 espaços métricos e $c \in [0, \infty[$. Uma função métrica² de M_0 para M_1 (com constante c) é uma função $f : M_0 \rightarrow M_1$ que

²Essas funções são conhecidas geralmente como funções ‘Lipschitz’ contínuas.

satisfaz, para todos $p, p' \in M_0$,

$$d_1(f(p), f(p')) \leq cd_0(p, p').$$

Para $0 \leq c < 1$, a função f é uma *contração*; para $c = 1$, é uma *homometria*³.

Proposição 16.30. *Sejam M_0, M_1 e M_2 espaços métricos, $f_0: M_0 \rightarrow M_1$ uma função métrica (com constante c_0) e $f_1: M_1 \rightarrow M_2$ uma função métrica (com constante c_1). Então $f_1 \circ f_0: M_0 \rightarrow M_2$ é uma função métrica (com constante c_1c_0). Se f_0 e f_1 são contrações, $f_1 \circ f_0$ é uma contração, e se f_0 e f_1 são funções métricas, então $f_1 \circ f_0$ é uma função métrica.*

Demonstração. Para todos $p, p' \in M_0$,

$$d_2(f_1 \circ f_0(p), f_1 \circ f_0(p')) \leq c_1 d_2(f_0(p), f_0(p')) \leq c_1 c_0 d_0(p, p').$$

Claramente, se $0 \leq c_0 < 1$ e $0 \leq c_1 < 1$, então $0 \leq c_1 c_0 < 1$, e se $c_0 = c_1 = 1$, então $c_1 c_0 = 1$. ■

Proposição 16.31. *Sejam M_0 e M_1 espaços métricos e $f: M_0 \rightarrow M_1$ uma função métrica (com constante c). Então f é uniformemente contínua.*

Demonstração. Se $c = 0$, a demonstração é óbvia. Se $c \neq 0$, seja $\varepsilon > 0$. Tomando $\delta = \frac{\varepsilon}{c}$, segue que, para todos $p, p' \in M_0$, se $d_0(p, p') \leq \delta$, então

$$d_1(f(p), f(p')) \leq cd_0(p, p') \leq c \frac{\varepsilon}{c} = \varepsilon. \quad \blacksquare$$

Proposição 16.32. *Sejam M_0 e M_1 espaços métricos e $f: M_0 \rightarrow M_1$ uma função métrica (com constante c). Então f tem inversa à esquerda que restrita a $f(M_0)$ é métrica (com constante c) se, e somente se, para todos $p, p' \in M_0$,*

$$c^{-1}d_0(p, p') \leq d_1(f(p), f(p')) \leq cd_0(p, p').$$

Demonstração. Se f tem inversa à esquerda c -métrica, então, para todos $q, q' \in M_1$,

$$d_0(f^{-1}(q), f^{-1}(q')) \leq cd_1(q, q').$$

Assim, para todos $p, p' \in M_0$,

$$d_0(p, p') = d_0(f^{-1}(f(p)), f^{-1}(f(p'))) \leq cd_1(f(p), f(p')),$$

³Essas funções são também conhecidas como funções métricas, funções não expansoras, entre outros. Escolhi o nome homometria por uma relação que elas têm com as isometrias que serão definidas mais à frente

portanto $c^{-1}d_0(p, p') \leq d_1(f(p), f(p'))$.

Reciprocamente, se valem as desigualdades acima, então para todos $p, p' \in M_0$ tais que $p \neq p'$, logo $d_0(p, p') > 0$. De $0 < c^{-1}d_0(p, p') \leq d_1(f(p), f(p'))$, segue que $d_1(f(p), f(p')) > 0$, o que implica $f(p) \neq f(p')$, portanto f é injetiva. Ainda, temos que $d_0(p, p') \leq cd_1(f(p), f(p'))$, logo para todos $q, q' \in f(M_0)$, existem $p, p' \in M_0$ tais que $q = f(p)$ e $q' = f(p')$, portanto

$$\begin{aligned} d_0(f^{-1}(q), f^{-1}(q')) &= d_0(f^{-1}(f(p)), f^{-1}(f(p'))) \\ &= d_0(p, p') \leq cd_1(f(p), f(p')) \\ &= cd_1(q, q'), \end{aligned}$$

o que mostra que f^{-1} é c -métrica. ■

16.4.2 Homometrias e Isometrias

Definição 16.20. Sejam M_0 e M_1 espaços métricos. Uma *isometria local* ou (*imersão isométrica*) de M_0 para M_1 é uma função $f: M_0 \rightarrow M_1$ que satisfaz, para todos $p, p' \in M_0$,

$$d_1(f(p), f(p')) = d_0(p, p').$$

Uma *isometria* é isometria local bijetiva.

Proposição 16.33. Sejam M_0 e M_1 espaços métricos e $f: M_0 \rightarrow M_1$ uma isometria local. Então f é injetiva.

Demonstração. Sejam $p, p' \in M_0$ tais que $p \neq p'$. Então $d_0(p, p') \neq 0$, logo

$$d_1(f(p), f(p')) = d_0(p, p') \neq 0,$$

o que implica $f(p) \neq f(p')$. ■

Proposição 16.34. Sejam M_0 e M_1 espaços métricos e $f: M_0 \rightarrow M_1$ uma homometria injetiva cuja inversa à esquerda é homometria. Então f é uma isometria local.

Demonstração. Sejam $p, p' \in M_0$. Então, como f é homometria,

$$d_1(f(p), f(p')) \leq d_0(p, p')$$

e, como f^{-1} é homometria,

$$d_0(p, p') = d_1(f^{-1} \circ f(p), f^{-1} \circ f(p')) \leq d_1(f(p), f(p'));$$

portanto $d_0(p, p') = d_1(f(p), f(p'))$. ■

Proposição 16.35. *Sejam M_0 e M_1 espaços métricos e $f: M_0 \rightarrow M_1$ homometria. A função f é isometria se, e somente se, é invertível e sua inversa é homometria.*

Demonstração. Suponhamos que f é isometria. Então f é bijetiva e, portanto, invertível. Sua inversa satisfaz, para todos $p, p' \in M_1$,

$$d_0(f^{-1}(p), f^{-1}(p')) = d_1(f(f^{-1}(p)), f(f^{-1}(p'))) = d_0(p, p').$$

Portanto f^{-1} é isometria local, logo homometria.

Reciprocamente, suponhamos que f é invertível e sua inversa é homometria. Segue da proposição anterior que f é isometria local e, como é bijetiva, é isometria. \blacksquare

16.4.3 Contrações

Proposição 16.36 (Ponto Fixo para Contrações). *Sejam M um espaço métrico completo e $f: M \rightarrow M$ uma contração. Existe único ponto fixo $\bar{p} \in M$ para f e, para todo $p \in M$,*

$$\lim_{n \rightarrow \infty} f^n(p) = \bar{p}.$$

Demonstração. Seja $c \in [0, \infty[$ a constante de contração de f . Mostremos por indução que, para todos $p \in M$ e $n \in \mathbb{N}$,

$$d(f^n(p), f^{n+1}(p)) \leq c^n d(p, f(p)).$$

Claramente, para $n = 0$ isso claramente vale. Agora, suponhamos que a desigualdade valha para $n = k$ e mostremos que ela vale para $n = k + 1$. Como f é contração,

$$d(f^k(p), f^{k+1}(p)) \leq c d(f^{k-1}(p), f^k(p)) \leq c c^{k-1} d(p, f(p)) = c^k d(p, f(p)).$$

Agora, notemos que, para todos $n, p \in \mathbb{N}$, segue da desigualdade triangular generalizada que

$$\begin{aligned} d(f^n(p), f^{n+p}(p)) &\leq \sum_{i=0}^{p-1} d(f^{n+i}(p), f^{n+i+1}(p)) \\ &\leq \sum_{i=0}^{p-1} c^{n+i} d(p, f(p)) \\ &= c^n \frac{1 - c^p}{1 - c} d(p, f(p)) \\ &\leq \frac{c^n}{1 - c} d(p, f(p)), \end{aligned}$$

pois $c \geq 0$ implica $1 - c^p < 1$. Como $c < 1$, então $\lim_{n \rightarrow \infty} \frac{c^n}{1-c} = 0$, portanto, para todos $n, p \in \mathbb{N}$,

$$\lim_{n \rightarrow \infty} d(f^n(p), f^{n+p}(p)) = 0,$$

o que mostra que $(f^n(p))_{n \in \mathbb{N}}$ é uma sequência aproximante e, como M é completo, converge para $\bar{p} \in M$. Como f é contínua,

$$f(\bar{p}) = f\left(\lim_{n \rightarrow \infty} f^n(p)\right) = \lim_{n \rightarrow \infty} f^{n+1}(p) = \bar{p},$$

esse ponto \bar{p} é um ponto fixo. Para mostrarmos que \bar{p} é único, suponhamos que p é ponto fixo de f . Então

$$d(\bar{p}, p) = d(f(\bar{p}), f(p)) \leq cd(\bar{p}, p)$$

e como $c < 1$ isso implica $d(\bar{p}, p) = 0$, logo $\bar{p} = p$. ■

16.4.4 Semelhanças

Definição 16.21. Sejam M_0 e M_1 espaços métricos e $c \in [0, \infty[$. Uma c -semelhança local ou (*imersão c-semelhante*) de M_0 para M_1 é uma função $f: M_0 \longrightarrow M_1$ que satisfaz, para todos $p, p' \in M_0$,

$$d_1(f(p), f(p')) = cd_0(p, p').$$

Uma *semelhança* é semelhança local bijetiva.

16.5 Medida e Dimensão

16.5.1 Medidas Exteriores Métricas

Definição 16.22. Seja M um espaço métrico. Uma medida exterior *métrica* em M é uma medida exterior $m: \wp(M) \longrightarrow [0, \infty]$ sobre M tal que, para todos $C, C' \subseteq M$ metricamente separados,

$$m(C \cup C') = m(C) + m(C').$$

Proposição 16.37. Sejam M um espaço métrico, com σ -álgebra topológica \mathcal{M}_T e m uma medida exterior métrica em M . Então todo $M \in \mathcal{M}_T$ é m -mensurável.

Demonstração. Para mostrar isso, basta mostrar que todo conjunto fechado é m -mensurável. Basta mostrar que, para todo $C \subseteq M$ com $m(C) < \infty$ e todo fechado $F \subseteq M$,

$$m(C) \geq m(C \cap F) + m(C \cap F^c),$$

pois a desigualdade contrária sempre vale por subaditividade e a igualdade vale trivialmente se $m(C) = \infty$. Consideremos as vizinhanças fechadas

$$F_j := \overline{\odot}_{\frac{1}{j}}(F) = \left\{ p \in M \mid d(F, p) \leq \frac{1}{j} \right\}.$$

Vale que $d(C \cap F, C \cap F_j^c) > 0$, portanto

$$m(C) \geq m((C \cap F) \cup (C \cap F_j^c)) = m(C \cap F) + m(C \cap F_j^c).$$

Resta mostrar agora que $\lim_{j \rightarrow \infty} m(C \cap F_j^c) = m(C \cap F^c)$. Como F é fechado, podemos escrever, para todo $j \in \mathbb{N}^*$,

$$\overline{\odot}_{\frac{1}{j}}(F) \cap F = \{p \in M \mid d(F, p) > 0\} = (S \cap F_j^c) \cup \bigcup_{k=j}^{\infty} R_k,$$

em que $R_k := C \cap \overline{\odot}_{\frac{1}{k}}(F) \setminus \overline{\odot}_{\frac{1}{k+1}}(F) = \left\{ p \in C \mid \frac{1}{k+1} < d(F, p) \leq \frac{1}{k} \right\}$. Pela subaditividade de m , segue que

$$m(C \cap F_j^c) \leq m(C \cap F^c) \leq m(C \cap F_j^c) + \sum_{k=j}^{\infty} m(R_k).$$

Mas note que $\sum_{k=1}^{\infty} m(R_k) < \infty$. Isso ocorre pois, para todo $j \geq i+2$, $d(F_i, F_j) > 0$, portanto por indução em N segue que

$$\sum_{k=1}^N m(R_{2k}) = m\left(\bigcup_{k=1}^N R_{2k}\right) \leq m(C) < \infty$$

e

$$\sum_{k=1}^N m(R_{2k-1}) = m\left(\bigcup_{k=1}^N R_{2k-1}\right) \leq m(C) < \infty.$$

Portanto $\sum_{k=1}^{\infty} m(R_k) < \infty$, o que implica que $\lim_{j \rightarrow \infty} m(C \cap F_j^c) = m(C \cap F^c)$, e concluímos que F é m -mensurável, resultando que todo $M \in \mathcal{M}_\mathcal{T}$ é m -mensurável. ■

16.5.2 Medidas por Coberturas Métricas

Nesta seção, definiremos uma família de medidas exteriores em um espaço métrico e usaremos essas medidas para definir a dimensão do espaço métrico e de seus subconjuntos mensuráveis. No entanto, é importante ressaltar que existem diferentes definições de medida e de dimensão em espaços métricos e aqui abordaremos

somente uma delas, a medida por coberturas métricas. Uma outra abordagem considera, em vez de coberturas métricas, empacotamentos, e essa abordagem chega a resultados semelhantes, mas às vezes distintos dos que chegaremos aqui. Essa abordagem por empacotamentos é, de certa forma, a noção dual da abordagem que estudaremos usando coberturas. No entanto, um paradigma que é em geral seguido é que as dimensões definidas coinsidam com as dimensões de espaços lineares como a reta, o plano, e de variedades.

Consideremos a função diâmetro em M

$$\begin{aligned}\varnothing: \wp(M) &\longrightarrow [0, \infty] \\ C &\longmapsto \varnothing(C).\end{aligned}$$

Essa função \varnothing não é uma medida exterior em M . Ela satisfaz (1) $\varnothing(\emptyset) = 0$ e (2) Para todos $C, D \subseteq M$ tais que $C \subseteq D$, então $C \times C \subseteq D \times D$, portanto $d(C \times C) \leq d(D \times D)$, o que implica

$$\varnothing(C) \leq \varnothing(D);$$

No entanto, não satisfaz (3) Para todos $(C_i)_{i \in \mathbb{N}}$ subconjuntos de M ,

$$\varnothing\left(\bigcup_{i \in \mathbb{N}} C_i\right) \leq \sum_{i \in \mathbb{N}} \varnothing(C_i).$$

Para ver isso, considere o intervalo $[0, 1]$ e os conjuntos C_i como os intervalos de tamanho $\frac{1}{2^{i+2}}$ e que tocam pela direita nos pontos $\frac{1}{2^i}$ do intervalo $[0, 1]$. Facilmente nota-se que

$$\varnothing\left(\bigcup_{i \in \mathbb{N}} C_i\right) = 1 > \frac{1}{2} = \sum_{i \in \mathbb{N}} \varnothing(C_i).$$

Isso ocorre porque a distância entre os conjuntos C_i não é considerada na soma dos diâmetros individuais, mas é considerada na união, e essa distância resulta em $\frac{1}{2}$ nesse caso. Pode-se fazer com que essa diferença seja tão grande quanto se queira.

Definiremos uma família de medidas exteriores em M com um parâmetro d , que representa a ‘dimensão’ da medida utilizando a função diâmetro \varnothing . Mas antes brevemente comentamos a definição de cobertura que usaremos.

Definição 16.23. Sejam M um espaço métrico, $C \subseteq M$ e $\delta \in]0, \infty[$. Uma δ -cobertura de C é uma cobertura $(C_i)_{i \in I}$ de C tal que, para todo $i \in I$, $\varnothing(C_i) \leq \delta$. O conjunto de δ -coberturas de C é $\mathcal{C}_\delta(C)$.

Definição 16.24. Sejam \mathbf{M} um espaço métrico, $C \subseteq M$, $d \in [0, \infty[$ e $\delta \in]0, \infty[$. A medida d -dimensional δ -precisa de C em \mathbf{M} é

$$H_\delta^d(C) := \inf \left\{ \sum_{i \in \mathbb{N}} \varnothing(U_i)^d \mid (U_i)_{i \in \mathbb{N}} \in \mathcal{C}_\delta(C) \right\}.$$

A medida d -dimensional δ -precisa em \mathbf{M} é a função

$$\begin{aligned} H_\delta^d: \wp(M) &\longrightarrow [0, \infty] \\ C &\longmapsto H_\delta^d(C). \end{aligned}$$

A sequência $(U_i)_{i \in \mathbb{N}}$ é uma δ -cobertura de C . Mostremos que H_δ^d é uma medida exterior em M .

Proposição 16.38. Sejam \mathbf{M} um espaço métrico, $d \in [0, \infty[$ e $\delta \in]0, \infty[$. A função $H_\delta^d: \wp(M) \longrightarrow [0, \infty]$ é uma medida exterior em M .

Demonstração. (Conjunto vazio) $H_\delta^d(\emptyset) = 0$, pois se tomamos a cobertura vazia $(\emptyset)_{i \in \mathbb{N}}$, temos que $\emptyset \subseteq \bigcup_{i \in \mathbb{N}} \emptyset$ e $\varnothing(\emptyset) \leq \delta$; (Monotonicidade) Para todos $C, C' \subseteq M$ tais que $C \subseteq C'$, temos que uma δ -cobertura de C' é uma δ -cobertura de C , logo $H_\delta^d(C) \leq H_\delta^d(C')$; (Subaditividade contável) Seja $(C_i)_{i \in \mathbb{N}}$ uma sequência de subconjuntos de M . Para todos $i \in \mathbb{N}$ e $\varepsilon \in]0, \infty[$, seja $U^i = (U_{i,j})_{j \in \mathbb{N}}$ é uma cobertura de C_i tal que

$$\sum_{j \in \mathbb{N}} \varnothing(U_{i,j})^s \leq H_\delta^d(C_i) + \frac{\varepsilon}{2^{i+1}}.$$

Essa cobertura existe porque $H_\delta^d(C_i)$ é um ínfimo. Então $(U_{i,j})_{(i,j) \in \mathbb{N}^2}$ é uma cobertura de $\bigcup_{i \in \mathbb{N}} C_i$ e segue que

$$\begin{aligned} H_\delta^d \left(\bigcup_{i \in \mathbb{N}} C_i \right) &\leq H_\delta^d \left(\bigcup_{(i,j) \in \mathbb{N}^2} U_{i,j} \right) \\ &\leq \sum_{(i,j) \in \mathbb{N}^2} \varnothing(U_{i,j})^d \\ &\leq \sum_{i \in \mathbb{N}} \left(H_\delta^d(C_i) + \frac{\varepsilon}{2^{i+1}} \right) \\ &= \sum_{i \in \mathbb{N}} \left(H_\delta^d(C_i) \right) + \sum_{i \in \mathbb{N}} \frac{\varepsilon}{2^{i+1}} \\ &= \sum_{i \in \mathbb{N}} \left(H_\delta^d(C_i) \right) + \varepsilon. \end{aligned}$$

A primeira desigualdade vem da monotonicidade de H_δ^d , a segunda de H_δ^d ser ínfimo, e a terceira vem da condição para as coberturas $(U_{i,j})_{j \in \mathbb{N}}$. Como isso vale para qualquer ε , segue que

$$H_\delta^d \left(\bigcup_{i \in \mathbb{N}} C_i \right) \leq \sum_{i \in \mathbb{N}} H_\delta^d(C_i). \quad \blacksquare$$

Definimos agora a medida H^d que independe de δ . Notemos que, se $\delta \leq \delta'$, então $H_{\delta'}^d(C) \leq H_\delta^d(C)$, pois toda cobertura de C com diâmetro δ é uma cobertura com diâmetro δ' . Isso implica que existe em $[0, \infty]$ o limite

$$\lim_{\delta \rightarrow 0} H_\delta^d(C) = \sup_{\delta \in]0, \infty[} H_\delta^d(C).$$

Definição 16.25. Sejam M um espaço métrico e $d \in [0, \infty[$. A *medida d-dimensional* em M é a função

$$\begin{aligned} H^d: \wp(M) &\longrightarrow [0, \infty] \\ C &\longmapsto H^d(C) := \sup_{\delta \in]0, \infty[} H_\delta^d(C). \end{aligned}$$

Proposição 16.39. Sejam M um espaço métrico e $d \in [0, \infty[$. A função

$$H^d: \wp(M) \longrightarrow [0, \infty]$$

é uma medida exterior métrica em M .

Demonstração. (Conjunto vazio) $H^d(\emptyset) = 0$, pois $H_\delta^d(\emptyset) = 0$ para todo $\delta \in]0, \infty[$; (Monotonicidade) Para todos $C, C' \subseteq M$ tais que $C \subseteq C'$, temos que $H_\delta^d(C) \leq H_\delta^d(C')$ para todo $\delta \in]0, \infty[$, logo $H^d(C) \leq H^d(C')$; (Subaditividade contável) Seja $(C_i)_{i \in \mathbb{N}}$ uma sequência de subconjuntos de M . Como para todo $i \in \mathbb{N}$ e $\delta \in]0, \infty[$ vale por definição que $H_\delta^d(C_i) \leq H^d(C_i)$, segue que

$$H_\delta^d \left(\bigcup_{i \in \mathbb{N}} C_i \right) \leq \sum_{i \in \mathbb{N}} H_\delta^d(C_i) \leq \sum_{i \in \mathbb{N}} H^d(C_i).$$

Como isso vale para todo δ , segue que

$$H^d \left(\bigcup_{i \in \mathbb{N}} C_i \right) \leq \sum_{i \in \mathbb{N}} H^d(C_i).$$

Por fim, pode-se mostrar que, para todos conjuntos $C, C' \in M$ e para todo $\delta < d(C, C')$, tem-se

$$H_\delta^d(C \cup C') = H_\delta^d(C) + H_\delta^d(C'),$$

portanto, se $d(C, C') > 0$, tem-se

$$H^d(C \cup C') = H^d(C) + H^d(C'). \quad \blacksquare$$

Essa medida é comumente chamada de *medida de Hausdorff d-dimensional*. Definem-se os conjuntos mensuráveis como usual para medidas exteriores. Um conjunto $E \subseteq M$ é mensurável se, e somente se, para todo conjunto $C \in M$,

$$H^d(E) = H^d(E \cap C) + H^d(E \cap E^C).$$

A proposição mostra que H^d é uma medida exterior métrica, todos os conjuntos da σ -álgebra topológica (conjuntos de Borel) são mensuráveis pela medida exterior H^d (16.37) e H^d pode ser restringida para uma medida em M . Em geral, não se pode garantir o mesmo para as medidas exteriores⁴ H_δ^d . Pode-se ainda mostrar a seguinte proposição.

Proposição 16.40. *Seja $n \in \mathbb{N}$ e \mathbb{R}^n o espaço métrico real n-dimensional. A medida H^n é um múltiplo da medida de volume vol^n em \mathbb{R}^n (Lebesgue):*

$$H^n = \frac{2^n}{\text{vol}^n(\mathbb{B}^n)} \text{vol}^n.$$

Lembrando que

$$\text{vol}^n(\mathbb{B}^n) = \frac{(\tau/2)^{\frac{n}{2}}}{(n/2)!}$$

em que $\tau = 6,28\dots$ é a constante do círculo (razão da circunferência pelo raio) e a função factorial ! é entendida como a extensão dada pela função Γ , definida $x! = \Gamma(x+1)$, ou mais explicitamente por

$$\begin{aligned} !: [0, \infty] &\longrightarrow [0, \infty] \\ x &\longmapsto \int_0^\infty t^x e^{-t} dt. \end{aligned}$$

Alguns casos particulares são

$$\begin{array}{ll} H^0 = \text{vol}^0 = \# & H^1 = \text{vol}^1 \\ H^2 = \frac{8}{\tau} \text{vol}^2 & H^3 = \frac{12}{\tau} \text{vol}^3 \end{array}$$

O fator $\text{vol}^n(\mathbb{B}^n)$ poderia ser evitado multiplicando-o na definição de H_δ^n , e o fator 2^n poderia ser evitado avaliando a soma de $\left(\frac{\phi(U_i)}{2}\right)^n$ em vez de somente $\phi(U_i)^n$. O número $\frac{\phi(C)}{2}$ pode ser naturalmente entendido como o *raio* do conjunto C .

⁴<https://web.stanford.edu/class/math285/ts-gmt.pdf>

16.5.3 Dimensão Métrica e Fractais

Seja $C \subseteq M$ um conjunto. A função

$$\begin{aligned} H^{(\cdot)}(C) : [0, \infty[&\longrightarrow [0, \infty] \\ d &\longmapsto H^d(C) \end{aligned}$$

é uma função com uma propriedade interessante. Ela admite no máximo três valores. Pode-se notar que, se $d \leq d'$, então $H^{d'}(C) \leq H^d(C)$. Além disso, existe $d \in [0, \infty[$ tal que $H^d(C) = 0$. Portanto podemos definir a *dimensão métrica* de C como

$$\dim(C) := \inf \{d \in [0, \infty[\mid H^d(C) = 0\}.$$

Nesse caso, pode-se mostrar que, para todo $d > \dim(C)$, $H^d(C) = 0$ e, para todo $d < \dim(C)$, $H^d(C) = \infty$. No entanto, o valor $H^{\dim(C)}(C)$ pode ser qualquer número em $[0, \infty]$. O valor de $H^{\dim(C)}(C)$ pode ser qualquer valor na linha tracejada do gráfico da figura 16.2. Existem subconjuntos de \mathbb{R}^d que têm dimensões não inteiras. Esses conjuntos são conhecidos como *fractais*.

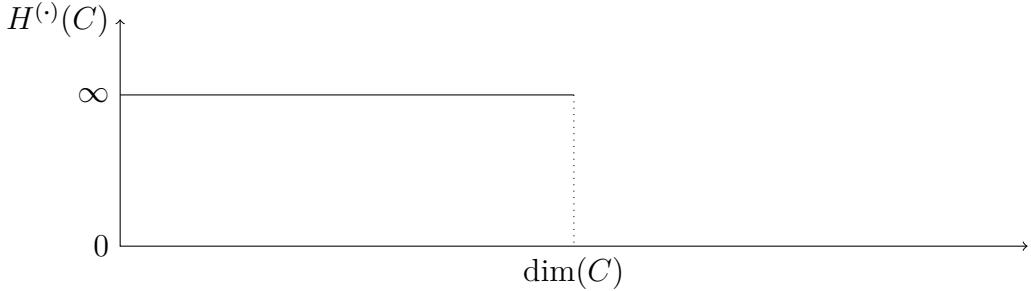


Figura 16.2: Gráfico de $H^d(C)$ em função de d .

Capítulo 17

Espaços Normados

17.1 Normas, Espaços Normados e Métricas

Definição 17.1. Seja \mathbf{E} um espaço linear sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$. Uma *norma* em \mathbf{E} é uma função $\|\cdot\| : E \rightarrow \mathbb{R}$ que satisfaz

1. (Separação) Para todo $v \in E$, se $\|v\| = 0$, então $v = 0$.
2. (Homogeneidade absoluta) Para todos $c \in C$ e $v \in E$,

$$\|cv\| = |c| \|v\|;$$

3. (Subaditividade) Para todos $v_0, v_1 \in E$,

$$\|v_0 + v_1\| \leq \|v_0\| + \|v_1\|;$$

Claramente $|\cdot| : \mathbb{C} \rightarrow \mathbb{R}$ é uma norma em \mathbb{C} . Pode-se, de modo mais geral, considerar outro valor absoluto em \mathbf{C} , mas não faremos isso aqui.

Proposição 17.1 (Propriedades da Norma). *Sejam \mathbf{E} um espaço linear sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$ e $\|\cdot\|$ uma norma em \mathbf{E} . Então*

1. $\|0\| = 0$;
2. Para todo $v \in E$, $\|-v\| = \|v\|$;
3. Para todo $v \in E$, $\|v\| \geq 0$.
4. (Subaditividade generalizada) Sejam $v_0, \dots, v_{n-1} \in E$. Então

$$\left\| \sum_{i \in [n]} v_i \right\| \leq \sum_{i \in [n]} \|v_i\|$$

Definição 17.2. Um *espaço normado* é um par $\mathbb{E} = (\mathbf{E}, \|\cdot\|)$ em que \mathbf{E} é um espaço linear sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$ e $\|\cdot\|$ é uma norma em \mathbf{E} . A dimensão de \mathbb{E} é a dimensão do espaço linear \mathbf{E} .

Definição 17.3. Seja \mathbf{E} um espaço linear sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$. Uma *métrica linear* em \mathbf{E} é uma métrica d em E que satisfaz

1. (Invariância por translação) Para todos $v, v', w \in E$,

$$d(v + w, v' + w) = d(v, v').$$

2. (Homogeneidade absoluta) Para todos $v, v' \in E$ e $c \in C$,

$$d(cv, cv') = |c| d(v, v');$$

Definição 17.4. Seja \mathbb{E} um espaço normado. A *métrica* (induzida pela norma) de \mathbb{E} é a função

$$\begin{aligned} d: E \times E &\longrightarrow \mathbb{R} \\ (v, \bar{v}) &\longmapsto \|v - \bar{v}\|. \end{aligned}$$

A *topologia* de \mathbb{E} é a topologia de (E, d) .

Para que essa definição seja boa, mostramos a seguir a proposição.

Proposição 17.2. *Seja \mathbb{E} um espaço normado. A função*

$$\begin{aligned} d: E \times E &\longrightarrow \mathbb{R} \\ (v_0, v_1) &\longmapsto \|v_0 - v_1\|. \end{aligned}$$

é uma métrica linear em E .

Demonstração. Primeiro mostramos que d é uma métrica.

1. (Separação) Sejam $v, \bar{v} \in E$. Se $v = \bar{v}$, então segue da positividade que

$$d(v, \bar{v}) = d(v, v) = \|v - v\| = \|v - v\| = \|0\| = 0.$$

Reciprocamente, se $d(v, \bar{v}) = 0$, então $\|v - \bar{v}\| = 0$. Segue da separação que $v - \bar{v} = 0$, logo $v = \bar{v}$.

2. (Simetria) Sejam $v, \bar{v} \in E$. Então segue da homogeneidade absoluta que

$$d(v, \bar{v}) = \|v - \bar{v}\| = \|-1(\bar{v} - v)\| = |-1| \|\bar{v} - v\| = d(\bar{v}, v).$$

3. (Desigualdade triangular) Sejam $v_0, v_1, v_2 \in E$. Então segue da subaditividade que

$$\begin{aligned} d(v_0, v_2) &= \|v_0 - v_2\| \\ &= \|v_0 - v_1 + v_1 - v_2\| \\ &\leq \|v_0 - v_1\| + \|v_1 - v_2\| \\ &= d(v_0, v_1) + d(v_1, v_2). \end{aligned}$$

Agora, mostremos que d é métrica linear.

1. (Invariância por translação) Sejam $v, v', w \in E$. Então

$$d(v + w, v' + w) = \|(v + w) - (v' + w)\| = \|v - v'\| = d(v, v').$$

2. (Homogeneidade absoluta) Sejam $v, v' \in E$ e $c \in C$. Então

$$d(cv, cv') = \|cv - cv'\| = \|c(v - v')\| = |c| \|v - v'\| = |c| d(v, v'). \quad \blacksquare$$

Reciprocamente, se temos uma métrica linear em um espaço linear, essa métrica define uma norma no espaço e a métrica que essa norma define, por sua vez, é a métrica original. Isso mostra, de fato, que existe uma relação bijetiva entre normas e métricas lineares em um espaço linear.

Proposição 17.3. *Sejam E um espaço linear sobre um corpo $C \subseteq \mathbb{C}$ e d uma métrica linear em E . A função*

$$\begin{aligned} \|\cdot\|: E &\longrightarrow \mathbb{R} \\ v &\longmapsto d(v, 0) \end{aligned}$$

é uma norma em E e a métrica induzida por essa norma é d .

Demonstração. Mostremos primeiro que a função é uma norma.

1. (Separação) Seja $v \in E$. Então $\|v\| = d(v, 0) = 0$, logo da separação de d segue que $v = 0$.
2. (Homogeneidade absoluta) Sejam $c \in C$ e $v \in E$. Então segue da homogeneidade absoluta de d que

$$\|cv\| = d(cv, 0) = |c| d(v, 0) = |c| \|v\|.$$

3. (Subaditividade) Sejam $v, v' \in E$. Então da invariância por translação, da simetria e da desigualdade triangular de d que

$$\begin{aligned}\|v + v'\| &= d(v + v', 0) \\ &= d(v, -v') \\ &\leq d(v, 0) + d(0, -v') \\ &\leq d(v, 0) + d(v', 0) \\ &= \|v\| + \|v'\|.\end{aligned}$$

Agora, mostremos que a métrica induzida por essa norma é a métrica original d . Sejam $v, v' \in E$. Então da invariância por translação de d segue que

$$d_{\|\cdot\|}(v, v') = \|v - v'\| = d(v - v', 0) = d(v, v'). \quad \blacksquare$$

17.1.1 Bolas e Esferas Unitárias

Definição 17.5. Seja \mathbb{E} um espaço normado. A *bola unitária* de \mathbb{E} é o conjunto

$$\mathbb{B} := \{v \in E \mid \|v\| \leq 1\}$$

e a *esfera unitária* de \mathbb{E} é o conjunto

$$\mathbb{S} := \{v \in E \mid \|v\| = 1\}.$$

A bola unitária é a bola fechada, de raio 1 e centro na origem, com respeito à métrica induzida pela norma. Isto é, $\mathbb{B} = \overline{\odot}_1(0)$. Com essa notação para a bola unitária, podemos representar qualquer bola de centro c e raio r como $c + r\mathbb{B}$, pois

$$\begin{aligned}c + r\mathbb{B} &= \{c + rv \mid v \in \mathbb{B}\} \\ &= \{c + rv \mid \|v\| \leq 1\} \\ &= \left\{v \mid \left\|\frac{v - c}{r}\right\| \leq 1\right\} \\ &= \{v \mid \|v - c\| \leq r\} \\ &= \overline{\odot}_r(c).\end{aligned}$$

Proposição 17.4. Seja \mathbb{E} um espaço normado. A bola unitária \mathbb{B} é um conjunto convexo e centrossimétrico na origem.

Demonstração. Sejam $t \in]0, 1[$ e $v, v' \in \mathbb{B}$. Então

$$\|(1-t)v + tv'\| \leq (1-t)\|v\| + t\|v'\| = (1-t) + t = 1,$$

logo $(1-t)v + tv' \in \mathbb{B}$, o que mostra que \mathbb{B} é convexo. Agora, seja $v \in \mathbb{B}$. Então $1 \geq \|v\| = \|-v\|$, logo $-v \in \mathbb{B}$, o que mostra a centrossimetria. \blacksquare

17.2 Isometrias Lineares, Funções Limitadas e Norma de Funções Lineares

Definição 17.6. Sejam \mathbb{E} e \mathbb{E}' espaços normados. Uma *isometria linear local* de \mathbb{E} para \mathbb{E}' é uma função linear $L: E \rightarrow E'$ tal que, para todo $v \in E$,

$$\|L(v)\|' = \|v\|.$$

O conjunto dessas funções é $\mathcal{L}_{|||}(\mathbb{E}, \mathbb{E}')$. Uma *isometria linear* é uma isometria linear local bijetiva.

Uma isometria linear local é uma isometria local com respeito à distância induzida pela norma, pois, para todos $v, v' \in E$,

$$d(L(v), L(v')) = \|L(v) - L(v')\| = \|L(v - v')\| = \|v - v'\| = d(v, v').$$

De modo mais geral, para $c \in [0, \infty[$ podemos definir funções c -métricas lineares como funções que satisfazem, para todo $v \in E$,

$$\|L(v)\|' \leq c \|v\|.$$

Essas funções lineares são chamadas de funções lineares limitadas.

Definição 17.7. Sejam \mathbb{E} e \mathbb{E}' espaços normados. Uma função linear *limitada* é uma função linear $f: E \rightarrow E'$ para a qual existe $c \in [0, \infty[$ satisfazendo, para todo $v \in E$,

$$\|f(v)\|' \leq c \|v\|.$$

O conjunto dessas funções é denotado $\mathcal{L}(\mathbb{E}, \mathbb{E}')$.

Claramente, segue direto da definição que $\mathcal{L}_{|||}(\mathbb{E}, \mathbb{E}') \subseteq \mathcal{L}(\mathbb{E}, \mathbb{E}')$.

Proposição 17.5. *Sejam \mathbb{E} e \mathbb{E}' espaços normados e $L: E \rightarrow E'$ uma função linear. Então L é limitada se, e somente se, é contínua.*

$$\mathcal{L}(\mathbb{E}, \mathbb{E}') = \mathcal{L}(\mathbb{E}, \mathbb{E}') \cap \mathcal{C}(\mathbb{E}, \mathbb{E}').$$

Demonstração. Se L é limitada por uma constante $c \in [0, \infty[$, então L é uma função c -métrica e, portanto, é contínua.

Reciprocamente, suponhamos que L é contínua. Para $v = 0$, claramente vale $\|L(0)\| = 0 \leq 0 - \|0\|$. Consideremos o seguinte para $v \neq 0$: como L é contínua, é contínua em 0; portanto existe $\delta \in]0, \infty[$ tal que, para todo $v \in E$, se $\|v\| \leq \delta$ então $\|L(v)\|' \leq 1$. Sendo assim, seja $v \in \mathbb{E} \setminus \{0\}$. Então, como $\|\delta \frac{v}{\|v\|}\| = \delta$, segue que

$$\|L(v)\|' = \left\| L\left(\frac{\|v\|}{\delta} \frac{\delta}{\|v\|} v\right) \right\|' = \left\| \frac{\|v\|}{\delta} L\left(\delta \frac{v}{\|v\|}\right) \right\|' = \frac{\|v\|}{\delta} \left\| L\left(\delta \frac{v}{\|v\|}\right) \right\|' \leq \frac{1}{\delta} \|v\|,$$

o que mostra que L é limitada. ■

Definição 17.8. Sejam \mathbb{E} e \mathbb{E}' espaços normados e $L: E \rightarrow E'$ uma função linear contínua. A *norma* de L é

$$\|L\| := \inf \{c \in [0, \infty[\mid \forall_{v \in \mathbb{E}} \|L(v)\| \leq c \|v\|\}.$$

Assim, para toda função linear contínua vale que

$$\|Lv\| \leq \|L\| \|v\|.$$

Como L é linear, segue que, para todo $v \in E \setminus \{0\}$,

$$\|L(v)\| = \left\| \|v\| L\left(\frac{v}{\|v\|}\right) \right\| = \|v\| \left\| L\left(\frac{v}{\|v\|}\right) \right\|,$$

portanto $\|L(v)\| \leq c \|v\|$ se, e somente se, $\left\| L\left(\frac{v}{\|v\|}\right) \right\| \leq c$. Isso implica que

$$\|L\| = \sup \{\|L(v)\| \mid v \in \mathbb{S}\}.$$

Proposição 17.6. *Sejam \mathbb{E} e \mathbb{E}' espaços normados. A função*

$$\begin{aligned} \|\cdot\|: \mathcal{L}(\mathbb{E}, \mathbb{E}') &\longrightarrow \mathbb{R} \\ L &\longmapsto \|L\| \end{aligned}$$

é uma norma em $\mathcal{L}(\mathbb{E}, \mathbb{E}')$.

Demonstração. 1. (Separação) Seja $0 \in \mathcal{L}(\mathbb{E}, \mathbb{E}')$. Para todo $v \in E$,

$$\|0(v)\| = \|0\| = 0 \|v\|,$$

portanto $\|0\| = 0$.

2. (Homogeneidade absoluta) Sejam $c \in C$ e $L \in \mathcal{L}(\mathbb{E}, \mathbb{E}')$. Se $c = 0$, $\|0L\| = \|0\| = 0$. Se $c \neq 0$, para todo $v \in E$ vale

$$\|(cL)(v)\| = \|cL(v)\| = |c| \|L(v)\| \leq |c| \|L\| \|v\|.$$

Como $\|L\|$ é ínfimo, então $|c| \|L\|$ deve ser também; caso contrário existiria $c \in [0, \infty[$ tal que

$$|c| \|L(v)\| \leq c \|v\| < |c| \|L\| \|v\|,$$

e seguiria que

$$\|L(v)\| \leq \frac{c}{|c|} \|v\| < \|L\| \|v\|,$$

o que contradiz a infimidade de $\|L\|$.

3. (Subaditividade) Sejam $L, L' \in \mathcal{L}(\mathbb{E}, \mathbb{E}')$. Para todo $v \in E$,

$$\begin{aligned}\|(L + L')(v)\| &= \|L(v) + L'(v)\| \\ &\leq \|L(v)\| + \|L'(v)\| \\ &\leq \|L\| \|v\| + \|L'\| \|v\| \\ &= (\|L\| + \|L'\|) \|v\|,\end{aligned}$$

portanto $\|L + L'\| \leq \|L\| + \|L'\|$. ■

17.2.1 Os Grupos Lineares Geral e Especial de Transformações e de Isometrias

O espaço normado $\overset{\leftrightarrow}{\mathcal{L}}(\mathbb{E})$ das transformações lineares contínuas invertíveis é um grupo com respeito à operação de composição, chamado *grupo de transformações lineares de \mathbb{E}* . Esse grupo é geralmente chamado de *grupo linear geral* e denotado $GL(\mathbb{E})$ e, se $\mathbb{E} = C^d$, C o corpo de escalares, denota-se $GL_d(C)$.

O conjunto das transformações de $\overset{\leftrightarrow}{\mathcal{L}}(\mathbb{E})$ que têm determinante unitário é um subgrupo, pois se $\det(f) = \det(f') = 1$, então $\det(f' \circ f) = \det(f') \det(f) = 1$. Esse grupo é geralmente chamado de *grupo linear especial* e denotado $SL(\mathbb{E})$ e, se $\mathbb{E} = C^d$, C o corpo de escalares, denota-se $SL_d(C)$.

O espaço normado $\overset{\leftrightarrow}{\mathcal{L}}_{|||}(\mathbb{E})$ das transformações lineares contínuas invertíveis que preservam a norma é um subgrupo de $\overset{\leftrightarrow}{\mathcal{L}}(\mathbb{E})$, chamado *grupo linear de isometrias de \mathbb{E}* . Esse grupo é geralmente chamado de *grupo ortogonal* e denotado $O(\mathbb{E})$ e, se $\mathbb{E} = C^d$, C o corpo de escalares, denota-se $O_d(C)$.

O conjunto das transformações de $\overset{\leftrightarrow}{\mathcal{L}}_{|||}(\mathbb{E})$ que têm determinante unitário é um subgrupo, pois se $\det(f) = \det(f') = 1$, então $\det(f' \circ f) = \det(f') \det(f) = 1$. Esse grupo é geralmente chamado de *grupo ortogonal especial* e denotado $SO(\mathbb{E})$ e, se $\mathbb{E} = C^d$, C o corpo de escalares, denota-se $SO_d(C)$.

Temos que

$$\begin{aligned}SL(\mathbb{E}) &\subseteq GL(\mathbb{E}) \\ O(\mathbb{E}) &\subseteq GL(\mathbb{E}) \\ SO(\mathbb{E}) &\subseteq O(\mathbb{E}) \\ SO(\mathbb{E}) &\subseteq SL(\mathbb{E})\end{aligned}$$

17.3 Espaços Normados de Dimensão Finita

Espaços lineares de dimensão finita E sobre um corpo C podem ser identificados com C^d , que que d é a dimensão de E . Nesses casos, a menos que seja mencionado

o contrário, sempre consideraremos a base canônica

$$e_i = (0, \dots, 0, \underbrace{1}_i, 0, \dots, 0)$$

em \mathbf{C}^d e todo vetor $v \in \mathbf{C}^d$ será representado como $v = (v_0, \dots, v_{d-1})$.

Definição 17.9. Sejam \mathbf{E} um espaço linear finito sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$ e $p \in [1, \infty[$. A p -norma em \mathbf{E} é a função

$$\begin{aligned} \|\cdot\|_p : E &\longrightarrow \mathbb{R} \\ v &\longmapsto \left(\sum_{i=0}^{d-1} |v_i|^p \right)^{\frac{1}{p}}. \end{aligned}$$

A ∞ -norma em \mathbf{E} é a função

$$\begin{aligned} \|\cdot\|_\infty : E &\longrightarrow \mathbb{R} \\ v &\longmapsto \max_{i \in [d]} |v_i|. \end{aligned}$$

Pode-se verificar que $\lim_{p \rightarrow \infty} \|v\|_p = \|v\|_\infty$.

Proposição 17.7. Para todo $p \in [1, \infty]$, a p -norma em \mathbf{E} é uma norma.

Definição 17.10. Seja \mathbf{E} um espaço linear. Normas *equivalentes* em \mathbf{E} são normas $\|\cdot\|, \|\cdot\|'$ em \mathbf{E} para as quais existem $c, C \in]0, \infty[$ tais que, para todo $v \in E$,

$$c \|v\|' \leq \|v\| \leq C \|v\|'.$$

Proposição 17.8. Equivalência de normas é uma relação de equivalência.

Proposição 17.9. Sejam \mathbf{E} um espaço vetorial finito sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$. Então todas normas em \mathbf{E} são equivalentes.

Demonstração. Vamos mostrar que toda norma em \mathbf{E} é equivalente a $\|\cdot\|_1$ e, como equivalência de normas é uma relação de equivalência, seguirá que todas normas são equivalentes em \mathbf{E} . Seja $\|\cdot\|$ uma norma em \mathbf{E} . Para todo $v \in E$, definindo $C := \max_{0 \leq i < d} \|e_i\|$, em que $\{e_i\}_{0 \leq i < d}$ é a base canônica de \mathbf{E} , segue que

$$\|v\| = \left\| \sum_{i=0}^{d-1} v_i e_i \right\| \leq \sum_{i=0}^{d-1} |v_i| \|e_i\| \leq C \|v\|_1.$$

A outra parte da equivalência segue do fato de que toda todo conjunto fechado e limitado em \mathbb{R} é sequencialmente compacto. ■

Proposição 17.10. *Normas equivalentes geram a mesma topologia.*

Demonstração. Basta notar que as bolas de uma norma sempre têm uma bola da outra norma contida nelas. ■

Pelas proposições anteriores, concluímos que um espaço linear normado de dimensão finita tem uma única topologia determinada por norma. Portanto todas noções topológicas relacionadas a espaços normados são independentes da norma escolhida.

17.4 Funções Multilineares

Proposição 17.11. *Sejam $\mathbf{E}_0, \dots, \mathbf{E}_{n-1}, \mathbf{E}$ espaços normados e $L: E_0 \times \dots \times E_{n-1} \rightarrow E$ uma função n -linear. São equivalentes*

1. L é contínua;
2. L é contínua em 0;
3. Existe real $C > 0$ tal que, para todos $v_0 \in E_0, \dots, v_{n-1} \in E_{n-1}$,

$$\|L(v_0, \dots, v_{n-1})\| \leq C \|v_0\| \cdots \|v_{n-1}\|;$$

Proposição 17.12. *Sejam $\mathbf{E}_1, \dots, \mathbf{E}_{n-1}$ espaços normados de dimensão finita, \mathbf{E} um espaço normado e $L: E_1 \times \dots \times E_{n-1} \rightarrow E$ uma função n -linear. Então existe real $C > 0$ tal que, para todos $v_1 \in E_1, \dots, v_n \in E_n$,*

$$\|L(v_1, \dots, v_{n-1})\| \leq C \|v_1\| \cdots \|v_{n-1}\|.$$

Demonstração. Para todo $i \in [n]$, sejam $d_i := \dim E_i$ e $(b_j^{(i)})_{j \in [d_i]}$ uma base ordenada de E_i . Todas normas em E_i são equivalentes, portanto usaremos a norma $\|\cdot\|_\infty$. Assim, para todos $v_1 \in E_1, \dots, v_{n-1} \in E_{n-1}$,

$$\begin{aligned} \|L(v_0, \dots, v_{n-1})\| &= \left\| \sum_{\substack{0 \leq k_0 < d_0 \\ \dots \\ 0 \leq k_{n-1} < d_{n-1}}} v_{(0)}^{k_0} \cdots v_{(n-1)}^{k_{n-1}} L(b_{k_0}^{(0)}, \dots, b_{k_{n-1}}^{(n-1)}) \right\| \\ &\leq \sum_{\substack{0 \leq k_0 < d_0 \\ \dots \\ 0 \leq k_{n-1} < d_{n-1}}} |v_{(0)}^{k_0}| \cdots |v_{(n-1)}^{k_{n-1}}| \|L(b_{k_0}^{(0)}, \dots, b_{k_{n-1}}^{(n-1)})\| \\ &\leq \|v_0\| \cdots \|v_{n-1}\| \sum_{\substack{0 \leq k_0 < d_0 \\ \dots \\ 0 \leq k_{n-1} < d_{n-1}}} \|L(b_{k_0}^{(0)}, \dots, b_{k_{n-1}}^{(n-1)})\|. \end{aligned}$$

Definindo

$$C := \sum_{\substack{0 \leq k_0 < d_0 \\ \dots \\ 0 \leq k_{n-1} < d_{n-1}}} \|L(b_{k_0}^{(0)}, \dots, b_{k_{n-1}}^{(n-1)})\|,$$

segue que

$$\|L(v_0, \dots, v_{n-1})\| \leq C \|v_0\| \cdots \|v_{n-1}\|. \quad \blacksquare$$

17.5 Norma de Funções Multilineares

Capítulo 18

Espaços Lineares com Produto Interno

18.1 Produto Interno

Definição 18.1. Seja \mathbf{V} um espaço linear sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$ invariante por conjugação complexa¹. Um *produto interno* em \mathbf{V} é uma função $\langle \cdot, \cdot \rangle : \mathbf{V} \times \mathbf{V} \rightarrow \mathbf{C}$ que satisfaz

1. (Linearidade na primeira entrada)

- (a) Para todos $v_0, v_1, v \in V$,

$$\langle v_0 + v_1, v \rangle = \langle v_0, v \rangle + \langle v_1, v \rangle;$$

- (b) Para todos $v, v' \in V$ e $c \in C$,

$$\langle cv, v' \rangle = c \langle v, v' \rangle;$$

2. (Simetria conjugada) Para todos $v, v' \in V$,

$$\langle v, v' \rangle = \overline{\langle v', v \rangle};$$

3. (Positividade) Para todo $v \in V$, $\langle v, v \rangle \in [0, \infty[$;

4. (Definição positiva) Para todo $v \in V$, se $\langle v, v \rangle = 0$, então $v = 0$.

Definição 18.2. Um *espaço com produto interno* é um par $(\mathbf{V}, \langle \cdot, \cdot \rangle)$ em que \mathbf{V} é um espaço linear sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$ invariante por conjugação complexa e $\langle \cdot, \cdot \rangle : \mathbf{V} \times \mathbf{V} \rightarrow \mathbf{C}$ é um produto interno em \mathbf{V} .

¹Um corpo $\mathbf{C} \subseteq \mathbb{C}$ tal que, para todo $c \in C$, temos $\bar{c} \in C$.

Proposição 18.1 (Propriedades de Produto Interno). *Seja $(\mathbf{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$. Então*

1. (Linearidade conjugada na segunda entrada)

(a) Para todos $v_0, v_1, v \in V$,

$$\langle v, v_0 + v_1 \rangle = \langle v, v_0 \rangle + \langle v, v_1 \rangle;$$

(b) Para todos $v, v' \in V$ e $c \in C$,

$$\langle v', cv \rangle = \bar{c} \langle v', v \rangle;$$

2. Para todos $v_0, \dots, v_n, v \in V$ e $c_0, \dots, c_n \in C$,

$$\left\langle \sum_{i=0}^n c_i v_i, v \right\rangle = \sum_{i=0}^n c_i \langle v_i, v \rangle$$

$$e \quad \left\langle v, \sum_{i=0}^n c_i v_i \right\rangle = \sum_{i=0}^n \bar{c}_i \langle v, v_i \rangle.$$

3. (Desigualdade de Cauchy-Schwarz) Para todos $v, v' \in V$,

$$|\langle v, v' \rangle|^2 \leq \langle v, v \rangle \langle v', v' \rangle$$

e a igualdade ocorre se, e somente se, um vetor é múltiplo do outro.

Demonstração. 1. Exercício simples.

2. Exercício simples.

3. Se existe $c \in C$ tal que $v' = cv$, então

$$|\langle v, v' \rangle|^2 = |\langle v, cv \rangle|^2 = |c|^2 |\langle v, v \rangle|^2 = c\bar{c} |\langle v, v \rangle|^2 = \langle v, v \rangle \langle cv, cv \rangle = \langle v, v \rangle \langle v', v' \rangle.$$

Caso contrário, se $v' - cv = 0$ para todo $c \in C$, então para $c = \frac{\langle v', v \rangle}{\langle v, v \rangle}$ segue que

$$\begin{aligned} 0 &< \langle v' - cv, v' - cv \rangle \\ &= \langle v', v' \rangle - c \langle v, v' \rangle - \bar{c} \langle v', v \rangle + |c|^2 \langle v, v \rangle \\ &= \langle v', v' \rangle - c \bar{c} \langle v', v \rangle - \bar{c} \langle v', v \rangle + |c|^2 \langle v, v \rangle \\ &= \langle v', v' \rangle - \frac{|\langle v, v' \rangle|^2}{\langle v, v \rangle} - \frac{|\langle v, v' \rangle|^2}{\langle v, v \rangle} + \frac{\langle v, v' \rangle^2}{\langle v, v \rangle} \\ &= \langle v', v' \rangle - \frac{|\langle v, v' \rangle|^2}{\langle v, v \rangle}, \end{aligned}$$

o que implica

$$|\langle v, v' \rangle|^2 < \langle v, v \rangle \langle v', v' \rangle.$$

■

Proposição 18.2. Sejam \mathbf{V} um espaço linear sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$ invariante por conjugação complexa e $(b_i)_{i \in I}$ uma base ordenada de \mathbf{V} . Existe único produto interno $\langle \cdot, \cdot \rangle$ em \mathbf{V} tal que, para todos $i, j \in I$, $\langle b_i, b_j \rangle = \delta_{i,j}$.

18.2 Norma Induzida, Ortogonalidade e Ângulo

18.2.1 Norma

Definição 18.3. Seja $(\mathbf{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$. A *norma* (induzida pelo produto interno) de \mathbf{V} é a função

$$\begin{aligned}\|\cdot\| : V &\longrightarrow \mathbb{R} \\ v &\longmapsto \langle v, v \rangle^{\frac{1}{2}}.\end{aligned}$$

Em termos da norma, a desigualdade de Cauchy-Schwarz fica

$$|\langle v, v' \rangle| \leq \|v\| \|v'\|.$$

Proposição 18.3. Seja $(\mathbf{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$. A função $\|\cdot\|$ é uma norma em \mathbf{V} .

Demonstração. 1. (Separação) Seja $v \in V$ tal que $\|v\| = 0$. Então $\langle v, v \rangle^{\frac{1}{2}} = 0$, portanto $\langle v, v \rangle = 0$, o que implica $v = 0$.

2. (Homogeneidade absoluta) Sejam $c \in C$ e $v \in V$. Então

$$\|cv\| = \langle cv, cv \rangle^{\frac{1}{2}} = (c\bar{c} \langle v, v \rangle)^{\frac{1}{2}} = |c| \|v\|.$$

3. (Subaditividade) Para todos $v, v' \in V$,

$$\begin{aligned}\|v + v'\|^2 &= \langle v + v', v + v' \rangle \\ &= \langle v, v \rangle + \langle v, v' \rangle + \langle v', v \rangle + \langle v', v' \rangle \\ &= \|v\|^2 + \langle v, v' \rangle + \overline{\langle v, v' \rangle} + \|v'\|^2 \\ &= \|v\|^2 + 2\Re(\langle v, v' \rangle) + \|v'\|^2 \\ &\leq \|v\|^2 + 2|\langle v, v' \rangle| + \|v'\|^2 \\ &= \|v\|^2 + 2\|v\| \|v'\| + \|v'\|^2 \\ &= (\|v\| + \|v'\|)^2.\end{aligned}$$
■

Proposição 18.4. Seja $(\mathbf{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno. Então, para todos $v, v' \in V$,

1. (*Regra do Paralelogramo*) $\|v + v'\|^2 + \|v - v'\|^2 = 2(\|v\|^2 + \|v'\|^2)$;

2. Se a característica de \mathbf{C} é diferente de 2,

$$\Re(\langle v, v' \rangle) = \frac{1}{4} (\|v + v'\|^2 - \|v - v'\|^2),$$

$$\Im(\langle v, v' \rangle) = \frac{i}{4} (\|v + iv'\|^2 - \|v - iv'\|^2),$$

e

$$\langle v, v' \rangle = \frac{1}{4} ((\|v + v'\|^2 - \|v - v'\|^2) + i(\|v + iv'\|^2 - \|v - iv'\|^2)).$$

Proposição 18.5 (Polarização). *Seja $(V, \|\cdot\|)$ um espaço normado tal que, para todos $v, v' \in V$,*

$$\|v + v'\|^2 + \|v - v'\|^2 = 2(\|v\|^2 + \|v'\|^2).$$

Então existe produto interno $\langle \cdot, \cdot \rangle$ em V tal que $\|v\| = \langle v, v \rangle$ para todo $v \in V$.

Demonstração. Se $\mathbf{C} \subseteq \mathbb{R}$, tome

$$\langle v, v' \rangle = \frac{1}{4} (\|v + v'\|^2 - \|v - v'\|^2).$$

Caso contrário, tome

$$\langle v, v' \rangle = \frac{1}{4} ((\|v + v'\|^2 - \|v - v'\|^2) + i(\|v + iv'\|^2 - \|v - iv'\|^2)). \quad \blacksquare$$

De fato, a segunda identidade se reduz à primeira quando v, v' são reais.

18.2.2 Perpendicularidade e Paralelismo

Definição 18.4. Seja $(V, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $\mathbf{C} \subseteq \mathbb{C}$. Vetores *paralelos* são vetores $v, v' \in V$ para os quais existe $c \in C \setminus \{0\}$ satisfazendo $v' = cv$. Denota-se $v \parallel v'$.

Vetores *perpendiculares* (ou *ortogonais*) são vetores $v, v' \in V$ que satisfazem $\langle v, v' \rangle = 0$. Denota-se $v \perp v'$.

Um conjunto *perpendicular* (ou *ortogonal*) é um conjunto $U \subseteq V$ tal que, para todos $u, u' \in U$, $u \perp u'$, e um conjunto *ortonormal* é um conjunto ortogonal U tal que, para todo $u \in U$, $\|u\| = 1$. O *complemento perpendicular* (ou *ortogonal*) de um conjunto $U \subseteq V$ é o conjunto

$$U^\perp := \{v \in V \mid \forall_{u \in U} v \perp u\}.$$

Proposição 18.6 (Propriedades de \parallel e \perp). *Seja $(V, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $C \subseteq \mathbb{C}$.*

1. A relação de paralelismo \parallel é uma equivalência;
2. A relação de perpendicularidade \perp é simétrica;
3. Para todos $u, v, v' \in V \setminus \{0\}$, se $v \parallel v'$ e $v \perp u$, então $v' \perp u$.
4. Para todos $v, v' \in V \setminus \{0\}$, $v \parallel v'$ se, e somente se, $\{v, v'\}$ é linearmente dependente.
5. Para todos $v, v' \in V \setminus \{0\}$, se $v \perp v'$, então $\{v, v'\}$ é linearmente independente.
6. Para todo $v \in V$, se $v \parallel 0$ então $v = 0$; para todo $v \in V$, $v \perp 0$.

Proposição 18.7 (Propriedades de complemento perpendicular). *Seja $(V, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $C \subseteq \mathbb{C}$.*

1. Para todo $U \subseteq V$, U^\perp é um subespaço linear de V .
2. $V^\perp = \{0\}$.
3. Para todo subespaço linear $U \subseteq V$, $U(U^\perp)^\perp = U$.

Demonstração. Primeiro notamos que $0 \in U^\perp$, pois para todo $u \in U$, $0 \perp u$. Segundo, sejam $v, v' \in U^\perp$ e $c \in C$. Então, para todo $u \in U$, $\langle v, u \rangle = \langle v', u \rangle = 0$, logo

$$\langle cv + v', u \rangle = c \langle v, u \rangle + \langle v', u \rangle = 0,$$

o que mostra que $cv + v' \in U^\perp$. ■

Definição 18.5. Sejam $(V, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $C \subseteq \mathbb{C}$ e $u \in V$. A projeção paralela² de V sobre u é

$$\begin{aligned} p_{\parallel u}: V &\longrightarrow V \\ v &\longmapsto \begin{cases} \frac{\langle v, u \rangle}{\|u\|^2}u, & u \neq 0 \\ 0, & u = 0. \end{cases} \end{aligned}$$

A projeção perpendicular de V sobre u é

$$\begin{aligned} p_{\perp u}: V &\longrightarrow V \\ v &\longmapsto v - p_{\parallel u}(v). \end{aligned}$$

²Essa projeção é conhecida como *projeção ortogonal* de V sobre u , mas aqui adotaremos as nomenclatura de paralela, já que definimos também a projeção perpendicular, e essa pode ser confundida com a ortogonal.

Proposição 18.8 (Propriedades das projeções). *Seja $(V, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $C \subseteq \mathbb{C}$.*

1. $p_{\parallel 0} = 0$ e $p_{\perp 0} = \text{Id}$;
2. Para todo $u \in V$, as projeções $p_{\parallel u}: V \rightarrow V$ e $p_{\perp u}: V \rightarrow V$ são lineares e idempotentes.
3. Para todos $u, v \in V$,
 - (a) se $u \not\perp v$, então $p_{\parallel u}(v) \parallel u$;
 - (b) $p_{\perp u}(v) \perp u$;
 - (c) se $v \parallel u$, então $p_{\parallel u}(v) = v$ (ou seja, $p_{\parallel u}|_{\langle u \rangle} = \text{Id}$);
 - (d) se $v \perp u$, então $p_{\perp u}(v) = v$ (ou seja, $p_{\perp u}|_{\langle u \rangle^\perp} = \text{Id}$);
4. Para todos $u, v \in V \setminus \{0\}$, $\{u, v\}$ é linearmente independente se, e somente se, $p_{\perp u}(v) \neq 0$.

Demonstração. 1. Direto da definição.

2. O caso em que $u = 0$ é consequência do item anterior, pois 0 e Id são lineares e idempotentes. Consideremos $u \in V \setminus \{0\}$.

(Linearidade) Sejam $v, v' \in V$ e $c \in C$.

$$p_{\parallel u}(cv + v') = \frac{\langle cv + v', u \rangle}{\|u\|^2}u = \frac{c\langle v, u \rangle + \langle v', u \rangle}{\|u\|^2}u = cp_{\parallel u}(v) + p_{\parallel u}(v').$$

(Idempotência) Seja $v \in V$.

$$p_{\parallel u}(p_{\parallel u}(v)) = \frac{\left\langle \frac{\langle v, u \rangle}{\|u\|^2}u, u \right\rangle}{\|u\|^2}u = \frac{\langle v, u \rangle}{\|u\|^2} \frac{\langle u, u \rangle}{\|u\|^2}u = \frac{\langle v, u \rangle}{\|u\|^2}u = p_{\parallel u}(v).$$

(Linearidade) Sejam $v, v' \in V$ e $c \in C$.

$$p_{\perp u}(cv + v') = cv + v' - p_{\parallel u}(cv + v') = cv + v' - cp_{\parallel u}(v) + p_{\parallel u}(v') = cp_{\perp u}(v) + p_{\perp u}(v').$$

(Idempotência) Seja $v \in V$.

$$\begin{aligned} p_{\perp u}(p_{\perp u}(v)) &= v - p_{\parallel u}(v) - p_{\parallel u}(v - p_{\parallel u}(v)) \\ &= v - p_{\parallel u}(v) - p_{\parallel u}(v) + p_{\parallel u}(p_{\parallel u}(v)) \\ &= v - p_{\parallel u}(v) - p_{\parallel u}(v) + p_{\parallel u}(v) \\ &= v - p_{\parallel u}(v) \\ &= p_{\perp u}(v). \end{aligned}$$

3. (a) Se $u \neq v$, $\langle u, v \rangle \neq 0$, o que implica que $u \neq 0$ e $\frac{\langle v, u \rangle}{\|u\|^2} \neq 0$. Como por definição $p_{\parallel u}(v) = \frac{\langle v, u \rangle}{\|u\|^2}u$, segue que $p_{\parallel u}(v) \parallel u$.

- (b) Se $u = 0$, $p_{\perp u}(v) \perp u$. Se $u \neq 0$,

$$\left\langle p_{\parallel u}(v), u \right\rangle = \left\langle \frac{\langle v, u \rangle}{\|u\|^2}u, u \right\rangle = \frac{\langle v, u \rangle}{\|u\|^2} \langle u, u \rangle = \langle v, u \rangle,$$

portanto

$$\langle p_{\perp u}(v), u \rangle = \langle v - p_{\parallel u}(v), u \rangle = \langle v, u \rangle - \langle p_{\parallel u}(v), u \rangle = 0,$$

o que mostra que $p_{\perp u}(v) \perp u$.

- (c) Se $v \parallel u$, existe $c \in C \setminus \{0\}$ tal que $v = cu$. Se $u = 0$, então $v = 0$, logo $p_{\parallel u}(v) = p_{\parallel 0}(0) = 0 = v$. Se $u \neq 0$, então

$$p_{\parallel u}(v) = \frac{\langle v, u \rangle}{\|u\|^2}u = \frac{\langle cu, u \rangle}{\|u\|^2}u = cu = v.$$

- (d) Se $v \perp u$, então $\langle u, v \rangle = 0$. Se $u = 0$, então $p_{\perp u} = \text{Id}$, logo $p_{\perp u}(v) = v$. Se $u \neq 0$,

$$p_{\perp u}(v) = v - \frac{\langle v, u \rangle}{\|u\|^2}u = v.$$

■

Todo v pode ser decomposto como $v = p_{\parallel u}(v) + p_{\perp u}(v)$.

Espaço Projetivo

A relação de paralelismo \parallel é uma equivalência. Além disso, ela não depende do produto interno, está definida para qualquer espaço linear \mathbf{V} sobre um corpo \mathbf{C} qualquer. Isso permite que se quociente V por \parallel , e esse é o *espaço projetivo de \mathbf{V}*

$$\mathbb{P}V := V / \parallel.$$

18.2.3 Ângulo

Definiremos agora a noção de ângulo induzida pelo produto interno. Pela desigualdade de Cauchy-Schwarz, sabemos que, para todos $v, v' \in V$,

$$|\langle v, v' \rangle| \leq \|v\| \|v'\|.$$

Disso segue que, para todos $v, v' \in V \setminus \{0\}$,

$$\frac{|\langle v, v' \rangle|}{\|v\| \|v'\|} \leq 1.$$

Se o produto interno for real, então

$$-1 \leq \frac{\langle v, v' \rangle}{\|v\| \|v'\|} \leq 1.$$

Isso significa que a função $\cos^{-1}: [-1, 1] \rightarrow [0, \frac{\pi}{2}]$ está definida para esses valores, portanto podemos definir a função ângulo como a seguir. No caso em que o produto interno não é real, ainda se pode definir o ângulo considerando o valor de \cos^{-1} para $\frac{|\langle v, v' \rangle|}{\|v\| \|v'\|} \in [0, 1]$, e com imagem $[0, \frac{\pi}{4}]$, mas não estudaremos esse caso aqui.

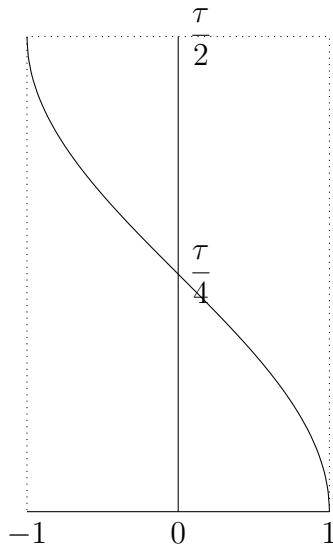


Figura 18.1: Gráfico da função $\cos^{-1}: [-1, 1] \rightarrow [0, \frac{\pi}{2}]$.

Definição 18.6. Sejam $(V, \langle \cdot, \cdot \rangle)$ um espaço com produto interno real e $v, v' \in V \setminus \{0\}$. O ângulo entre v e v' é

$$\sphericalangle(v, v') := \cos^{-1} \left(\frac{\langle v, v' \rangle}{\|v\| \|v'\|} \right).$$

A função ângulo de V é a função

$$\begin{aligned} \sphericalangle(\cdot, \cdot): V \setminus \{0\} \times V \setminus \{0\} &\longrightarrow \left[0, \frac{\pi}{2}\right] \\ (v, v') &\longmapsto \sphericalangle(v, v'). \end{aligned}$$

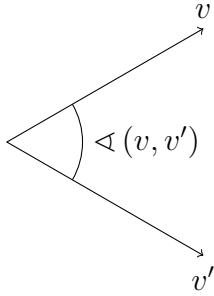


Figura 18.2: Representação de vetores e o ângulo entre eles.

Proposição 18.9 (Propriedades de Ângulo). *Seja $(V, \langle \cdot, \cdot \rangle)$ um espaço com produto interno real.*

1. Para todos $v, v' \in V \setminus \{0\}$,

$$\langle v, v' \rangle = \|v\| \|v'\| \cos(\alpha(v, v'));$$

2. Para todos $v, v' \in V \setminus \{0\}$ e $cc' \in \mathbb{R} \setminus \{0\}$,

$$\alpha(cv, c'v') = \begin{cases} \alpha(v, v'), & cc' > 0 \\ \frac{\pi}{2} - \alpha(v, v'), & cc' < 0; \end{cases}$$

3. Para todos $v, v' \in V \setminus \{0\}$,

$$v \parallel v' \iff \alpha(v, v') \in \{0, \frac{\pi}{2}\}.$$

Se existe $c \in]0, \infty[$ tal que $v' = cv$, então $\alpha(v, v') = 0$, e se existe $c \in]-\infty, 0[$ tal que $v' = cv$, então $\alpha(v, v') = \frac{\pi}{2}$;

4. Para todos $v, v' \in V \setminus \{0\}$,

$$v \perp v' \iff \alpha(v, v') = \frac{\pi}{4}.$$

Demonstração. 1. Segue diretamente da definição.

2. Da igualdade

$$\alpha(v, v') = \cos^{-1} \left(\frac{\langle v, v' \rangle}{\|v\| \|v'\|} \right)$$

segue que, para todos $c, c' \in \mathbb{R} \setminus \{0\}$

$$\begin{aligned}\sphericalangle(cv, c'v') &= \cos^{-1} \left(\frac{\langle cv, c'v' \rangle}{\|cv\| \|c'v'\|} \right) \\ &= \cos^{-1} \left(\frac{cc' \langle v, v' \rangle}{|c| |c'| \|v\| \|v'\|} \right) \\ &= \cos^{-1} \left(\frac{cc'}{|cc'|} \frac{\langle v, v' \rangle}{\|v\| \|v'\|} \right).\end{aligned}$$

Nesse caso, se $cc' > 0$, então

$$\sphericalangle(cv, c'v') = \cos^{-1} \left(1 \frac{\langle v, v' \rangle}{\|v\| \|v'\|} \right) = \sphericalangle(v, v'),$$

e, se $cc' < 0$, então

$$\sphericalangle(cv, c'v') = \cos^{-1} \left(-1 \frac{\langle v, v' \rangle}{\|v\| \|v'\|} \right) = \frac{\pi}{2} - \sphericalangle(v, v').$$

3. Notemos que, para todo $v \in V \setminus \{0\}$,

$$\sphericalangle(v, v) = \cos^{-1} \left(\frac{\langle v, v \rangle}{\|v\| \|v\|} \right) = \cos^{-1}(1) = 0.$$

Notemos também que $\cos^{-1}: [-1, 1] \longrightarrow \left[0, \frac{\pi}{2}\right]$ é uma bijeção tal que $\cos^{-1}(1) = 0$ e $\cos^{-1}(-1) = \frac{\pi}{2}$.

Suponhamos agora que existe $c \in \mathbb{R} \setminus \{0\}$ tal que $v' = cv$. Nesse caso, pelo item anterior segue que, relacionando $\sphericalangle(v, v')$ com $\sphericalangle(v, v)$,

$$\sphericalangle(v, v') = \sphericalangle(v, cv) = \begin{cases} 0, & c > 0 \\ \frac{\pi}{2}, & c < 0. \end{cases}$$

Reciprocamente, suponhamos que $\sphericalangle(v, v') = 0$. Da bijetividade de \cos^{-1} segue que $\frac{\langle v, v' \rangle}{\|v\| \|v'\|} = 1$, logo $|\langle v, v' \rangle| = \|v\| \|v'\|$ e pela desigualdade de Cauchy-Schwarz existe $c \in \mathbb{R} \setminus \{0\}$ tal que $v' = cv$. Como $0 = \sphericalangle(v, v') = \sphericalangle(v, cv)$, $c \in]0, \infty[$. Suponhamos então que $\sphericalangle(v, v') = \frac{\pi}{2}$. Da bijetividade de \cos^{-1} segue que $\frac{\langle v, v' \rangle}{\|v\| \|v'\|} = -1$, logo $|\langle v, v' \rangle| = \|v\| \|v'\|$ e pela desigualdade de Cauchy-Schwarz existe $c \in \mathbb{R} \setminus \{0\}$ tal que $v' = cv$. Como $\frac{\pi}{2} = \sphericalangle(v, v') = \sphericalangle(v, cv)$, $c \in]-\infty, 0[$.

4. Segue diretamente da bijetividade de \cos^{-1} , pois $\sphericalangle(v, v') = \frac{\pi}{4}$ se, e somente se, $\frac{\langle v, v' \rangle}{\|v\|\|v'\|} = 0$, o que ocorre se, e somente se, $\langle v, v' \rangle = 0$. \blacksquare

Se quocientamos o intervalo $[0, \frac{\pi}{2}]$ identificando suas extremidades de modo a obter $\frac{\pi}{2}\mathbb{T}^1$, temos que

$$\sphericalangle(cv, v') = \pm_c \sphericalangle(v, v'),$$

pois em $\frac{\pi}{2}\mathbb{T}^1$ vale a igualdade $\frac{\pi}{2} - \sphericalangle(v, v') = -\sphericalangle(v, v')$. Isso é uma curiosidade interessante.

18.2.4 Funções Ortogonais e Conformes

Definição 18.7. Sejam $(\mathbf{V}, \langle \cdot, \cdot \rangle)$ e $(\mathbf{V}', \langle \cdot, \cdot \rangle')$ espaços com produto interno. Uma função *ortogonal* de \mathbf{V} para \mathbf{V}' é uma função linear $f: V \rightarrow V'$ tal que, para todos $v, v' \in V$,

$$\langle f(v), f(v') \rangle' = \langle v, v' \rangle.$$

O conjunto dessas funções é $\mathcal{L}_{\langle \cdot, \cdot \rangle}(\mathbf{V}, \mathbf{V}')$.

Uma função *conforme* de \mathbf{V} para \mathbf{V}' é uma função linear $f: V \rightarrow V'$ tal que, para todos $v, v' \in V$,

$$\sphericalangle'(f(v), f(v')) = \sphericalangle(v, v').$$

O conjunto dessas funções é $\mathcal{L}_{\sphericalangle}(\mathbf{V}, \mathbf{V}')$.

Note que, na definição de uma função conforme, está implícito que $\sphericalangle'(f(v), f(v'))$ existe, portanto $f(v) \neq 0$ para todo $v \in V \setminus \{0\}$, o que significa que f é injetiva.

Proposição 18.10. Sejam $(\mathbf{V}, \langle \cdot, \cdot \rangle)$ e $(\mathbf{V}', \langle \cdot, \cdot \rangle')$ espaços com produto interno sobre um corpo \mathbf{C} de característica diferente de 2 e $f: V \rightarrow V'$ uma função linear.

1. f é ortogonal se, e somente se, é uma isometria local:

$$\mathcal{L}_{\langle \cdot, \cdot \rangle}(\mathbf{V}, \mathbf{V}') = \mathcal{L}_{\parallel\parallel}(\mathbf{V}, \mathbf{V}');$$

2. f é conforme se, e somente se, existe $c \in]0, \infty[$ tal que, para todos $v, v' \in V$,

$$\langle f(v), f(v') \rangle' = c \langle v, v' \rangle.$$

Demonstração. 1. Se f é ortogonal, então para todo $v \in V$,

$$\|f(v)\|' = \langle f(v), f(v) \rangle'^{\frac{1}{2}} = \langle v, v \rangle^{\frac{1}{2}} = \|v\|.$$

Reciprocamente, como a característica de \mathbf{C} é diferente de 2, vale que, para todos $v, v' \in V$,

$$\langle v, v' \rangle = \frac{1}{4} \left((\|v + v'\|^2 - \|v - v'\|^2) + i (\|v + iv'\|^2 - \|v - iv'\|^2) \right).$$

Se f é isometria local, então, para todos $v, v' \in V$,

$$\begin{aligned} \langle f(v), f(v') \rangle &= \frac{1}{4} \left(\|f(v) + f(v')\|^2 - \|f(v) - f(v')\|^2 \right) \\ &\quad + \frac{i}{4} \left(\|f(v) + if(v')\|^2 - \|f(v) - if(v')\|^2 \right) \\ &= \frac{1}{4} \left(\|f(v + v')\|^2 - \|f(v - v')\|^2 \right) \\ &\quad + \frac{i}{4} \left(\|f(v + iv')\|^2 - \|f(v - iv')\|^2 \right) \\ &= \frac{1}{4} \left((\|v + v'\|^2 - \|v - v'\|^2) + i (\|v + iv'\|^2 - \|v - iv'\|^2) \right) \\ &= \langle v, v' \rangle. \end{aligned}$$

2. Se f é conforme, para todos $v, v' \in V$ vale

$$\sphericalangle'(f(v), f(v')) = \sphericalangle(v, v').$$

Como \cos^{-1} é bijeção, então

$$\frac{\langle f(v), f(v') \rangle'}{\|f(v)\|' \|f(v')\|'} = \frac{\langle v, v' \rangle}{\|v\| \|v'\|},$$

o que implica

$$\langle f(v), f(v') \rangle' = \frac{\|f(v)\|' \|f(v')\|'}{\|v\| \|v'\|} \langle v, v' \rangle.$$

Resta mostrar que $\frac{\|f(v)\|' \|f(v')\|'}{\|v\| \|v'\|}$ é constante. Note que isso ocorre se, e somente se, $N(v) := \frac{\|f(v)\|'}{\|v\|}$ é constante. Para mostrar que essa função é constante, vamos mostrar que sua diferencial é nula. Sejam $v \in V \setminus \{0\}$ e $h \in V$.

Como f é linear e $D\|v\|(h) = \frac{\langle v, h \rangle}{\|v\|}$ é a diferencial³ de N ,

$$\begin{aligned} DN|_v(h) &= \frac{\|v\| D\|f(v)\|'(h) - \|f(v)\|' D\|v\|(h)}{\|v\|^2} \\ &= \frac{\frac{\|v\|}{\|f(v)\|'} \langle f(v), Df(v)(h) \rangle' - \frac{\|f(v)\|'}{\|v\|} \langle v, h \rangle}{\|v\|^2} \\ &= \frac{\|v\|^2 \langle f(v), f(h) \rangle' - \|f(v)\|'^2 \langle v, h \rangle}{\|f(v)\|' \|v\|^3}. \end{aligned}$$

Notemos que, como f preserva ângulo, então se $v \perp v'$ segue que $f(v) \perp f(v')$. Escrevendo $h = p_{\|v\|}(h) + p_{\perp v}(h) = h^{\parallel} + h^{\perp}$, temos que $h^{\perp} \perp v$, e $h^{\parallel} \parallel v$ ou $h^{\parallel} = 0$, logo

$$DN|_v(h) = DN|_v(h^{\parallel} + h^{\perp}) = DN|_v(h^{\parallel}) + DN|_v(h^{\perp}).$$

Calculemos $DN|_v(h^{\parallel})$. Como $h^{\parallel} = cv$, com $c = \frac{\langle h, v \rangle}{\|v\|^2}$, segue que

$$\begin{aligned} DN|_v(h^{\parallel}) &= \frac{\|v\|^2 \langle f(v), f(cv) \rangle' - \|f(v)\|'^2 \langle v, cv \rangle}{\|f(v)\|' \|v\|^3} \\ &= \frac{c \|v\|^2 \langle f(v), f(v) \rangle' - c \|f(v)\|'^2 \langle v, v \rangle}{\|f(v)\|' \|v\|^3} \\ &= \frac{c \|v\|^2 \|f(v)\|'^2 - c \|f(v)\|'^2 \|v\|^2}{\|f(v)\|' \|v\|^3} \\ &= 0. \end{aligned}$$

Calculemos agora $DN|_v(h^{\perp})$. Como $\langle h^{\perp}, v \rangle = 0$, então $\langle f(v), f(h^{\perp}) \rangle = 0$, logo

$$DN|_v(h^{\perp}) = \frac{\|v\|^2 \langle f(v), f(h^{\perp}) \rangle' - \|f(v)\|'^2 \langle v, h^{\perp} \rangle}{\|f(v)\|' \|v\|^3} = 0.$$

Assim, concluímos que $DN|_v(h) = DN|_v(h^{\parallel}) + DN|_v(h^{\perp}) = 0$, ou seja, $DN|_v = 0$ para todo $v \in V \setminus \{0\}$, o que implica que existe $c' \in \mathbb{R}$ tal que, para todo $v \in V \setminus \{0\}$, $N(v) = \frac{\|f(v)\|}{\|v\|} = c'$. Como f preserva ângulos, é injetiva, portanto $f(v) = 0$ se, e somente se, $v = 0$, o que significa que $c' \neq 0$. Definindo $c := (c')^2$, segue que $c \in]0, \infty[$, portanto

$$\langle f(v), f(v') \rangle' = \frac{\|f(v)\|' \|f(v')\|'}{\|v\| \|v'\|} \langle v, v' \rangle = (c')^2 \langle v, v' \rangle = c \langle v, v' \rangle.$$

³Não tenho certeza, mas acredito que isso dependa da característica de C ser diferente de 2, pois quando calculamos a diferencial pela regra da cadeia cancelamos fatores de 2.

Reciprocamente, se existe $c \in]0, \infty[$ tal que

$$\langle f(v), f(v') \rangle' = c \langle v, v' \rangle,$$

então $\|f(v)\| = \langle f(v), f(v) \rangle^{\frac{1}{2}} = c^{\frac{1}{2}} \langle v, v' \rangle^{\frac{1}{2}} = c^{\frac{1}{2}} \|v\|$ e segue que

$$\begin{aligned} \sphericalangle'(f(v), f(v')) &= \cos^{-1} \left(\frac{\langle f(v), f(v') \rangle'}{\|f(v)\|' \|f(v')\|'} \right) \\ &= \cos^{-1} \left(\frac{c \langle v, v' \rangle}{c \|v\| \|v'\|} \right) \\ &= \sphericalangle(v, v'). \end{aligned}$$

■

Capítulo 19

Cálculo Diferencial

O espaço real \mathbb{E} estudado neste capítulo será o espaço vetorial normado $(\mathbb{R}^d, +, \cdot)$ sobre \mathbb{R} . A base canônica de \mathbb{R}^d será representada pelos vetores $\{\mathbf{e}_0, \dots, \mathbf{e}_{d-1}\}$. Um vetor $x \in \mathbb{R}^d$ será também representado por $x = (x_0, \dots, x_{d-1})$ e uma função $f : \mathbb{R}^{d_0} \rightarrow \mathbb{R}^{d_1}$ será também representada por $f = (f_0, \dots, f_{d_1-1})$, de modo que $f_i := \pi_i \circ f$, sendo π_i a i -ésima projeção de \mathbb{R}^{d_1} em \mathbb{R} . Como todas normas em \mathbb{R}^d são equivalentes, não será feita referência à norma utilizada, apenas será usado o fato de que \mathbb{R}^d é um espaço vetorial normado (e completo). Se necessário, a norma utilizada será explicitada e, quando não for, a norma usada será $\|\cdot\|_2$. O estudo da diferenciabilidade em espaços de dimensão maior que 1 envolve o uso de funções contínuas e transformações lineares, e também de funções de um espaço real em um espaço de transformações lineares. Por esse motivo, a notação pode ser confusa. Para simplificar a notação, uma transformação linear T aplicada a um vetor v será sempre denotada por $T \cdot v$. Desenvolveremos, a seguir, a teoria de diferenciabilidade de funções entre espaços reais, e as funções consideradas serão sempre da forma

$$f : \mathbb{R}^d \rightarrow \mathbb{R}^c,$$

mas toda teoria poderia ser desenvolvida para funções definidas em abertos de \mathbb{R}^d . O tratamento que adotaremos, no entanto, não prejudica a generalidade, pois todas propriedades desenvolvidas podem ser compreendidas localmente.

19.1 Diferenciabilidade

A ideia por trás dessa definição de diferenciabilidade é a de que a função f pode ser aproximada em uma vizinhança de um ponto p por seu valor no ponto mais o valor de uma transformação linear aplicada num vetor v de variação que mede quanto afastou-se do ponto p . Ser aproximada, nesse sentido, quer dizer que o erro da aproximação será da ordem da norma do vetor variação v , de modo que a

razão entre os dois vá a zero quando a variação vai a zero. A definição de função contínua, de fato, pode ser pensada como um caso análogo: a função f numa vizinhança do ponto p pode ser aproximada por seu valor em p , e aproximada aqui quer dizer que a norma da diferença vai a zero quando o vator variação vai a zero. Mais à frente, as k -ésimas diferenciais da função f serão definidas analogamente, considerando nesses casos funções multilineares.

Definição 19.1. Sejam $p \in \mathbb{R}^d$ e $f : \mathbb{R}^d \rightarrow \mathbb{R}^c$ uma função. Uma *diferencial* de f em p é uma transformação linear $T : \mathbb{R}^d \rightarrow \mathbb{R}^c$ que satisfaz

$$\lim_{v \rightarrow 0} \frac{f(p + v) - f(p) - T \cdot v}{\|v\|} = 0.$$

Uma função *diferenciável* em p é uma função que tem diferencial em p .

É válido notar que são equivalentes a essa condição

$$\lim_{x \rightarrow p} \frac{f(x) - f(p) - T \cdot (x - p)}{\|x - p\|} = 0.$$

e

$$\lim_{v \rightarrow 0} \frac{\|f(p + v) - f(p) - T \cdot v\|}{\|v\|} = 0.$$

Proposição 19.1 (Diferenciabilidade implica continuidade). *Sejam $p \in \mathbb{R}^d$ e $f : \mathbb{R}^d \rightarrow \mathbb{R}^c$ uma função. Se f é diferenciável em p , então f é contínua em p .*

Demonstração. Se f é diferenciável em p , então, como $\lim_{v \rightarrow 0} T \cdot v = 0$,

$$\begin{aligned} \lim_{v \rightarrow 0} (f(p + v) - f(p)) &= \lim_{v \rightarrow 0} (f(p + v) - f(p) - T \cdot v) \\ &= \lim_{v \rightarrow 0} \|v\| \frac{f(p + v) - f(p) - T \cdot v}{\|v\|} \\ &= 0, \end{aligned}$$

logo f é contínua em p . ■

Proposição 19.2 (Unicidade da diferencial). *Sejam $p \in \mathbb{R}^d$ e $f : \mathbb{R}^d \rightarrow \mathbb{R}^c$ uma função diferenciável em p . Então existe uma única diferencial de f em p .*

Demonstração. Sejam $T, S : \mathbb{R}^d \rightarrow \mathbb{R}^c$ diferenciais de f em p . Nesse caso, temos que

$$\begin{aligned} \lim_{v \rightarrow 0} \frac{T \cdot v - S \cdot v}{\|v\|} &= \\ &= \lim_{v \rightarrow 0} \frac{T \cdot v - (f(p + v) - f(p)) + (f(p + v) - f(p)) - S \cdot v}{\|v\|} \\ &= - \lim_{v \rightarrow 0} \frac{f(p + v) - f(p) - T \cdot v}{\|v\|} + \lim_{v \rightarrow 0} \frac{f(p + v) - f(p) - S \cdot v}{\|v\|} \\ &= 0. \end{aligned}$$

Como T e S são transformações lineares, sabemos que $T \cdot 0 = S \cdot 0 = 0$. Para todo $v \in \mathbb{R}^d \setminus \{0\}$, temos que, quando $t \rightarrow 0$, $tv \rightarrow 0$. Ainda, como T e S são transformações lineares, $T \cdot (tv) = t(T \cdot v)$ e $S \cdot (tv) = t(S \cdot v)$, e segue que

$$\begin{aligned} 0 &= \lim_{tv \rightarrow 0} \frac{\|T \cdot (tv) - S \cdot (tv)\|}{\|tv\|} \\ &= \lim_{t \rightarrow 0} \frac{|t| \|T \cdot v - S \cdot v\|}{|t| \|v\|} \\ &= \frac{\|T \cdot v - S \cdot v\|}{\|v\|}, \end{aligned}$$

o que implica $T \cdot v = S \cdot v$, pois $\|v\| \neq 0$. Portanto $T = S$. \blacksquare

Notaçāo. Sejam $p \in \mathbb{R}^d$ e $f : \mathbb{R}^d \rightarrow \mathbb{R}^c$ uma função diferenciável em p . A diferencial de f em p é denotada $Df(p) : \mathbb{R}^d \rightarrow \mathbb{R}^c$ e satisfaz

$$\lim_{v \rightarrow 0} \frac{f(p + v) - f(p) - Df(p) \cdot v}{\|v\|} = 0.$$

Podemos ver que, se f é diferenciável, então $Df : \mathbb{R}^d \rightarrow L(\mathbb{R}^d, \mathbb{R}^c)$ é uma função que leva $p \in \mathbb{R}^d$ na diferencial $Df(p)$ de f em p .

Proposiçāo 19.3 (Regra da cadeia). *Sejam $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ diferenciável em $p \in \mathbb{R}^n$ e $g : \mathbb{R}^m \rightarrow \mathbb{R}^l$ diferenciável em $f(p)$. Então $g \circ f : \mathbb{R}^n \rightarrow \mathbb{R}^l$ é diferenciável em p e*

$$D(g \circ f)(p) = Dg(f(p)) \circ Df(p).$$

Demonstraçāo. Definamos

$$r_1(v) := f(p + v) - f(p) - Df(p) \cdot v$$

e

$$r_2(v) := g(f(p) + v) - g(f(p)) - Dg(f(p)) \cdot v,$$

de modo que da diferenciabilidade de f em p e de g em $f(p)$ segue

$$\lim_{v \rightarrow 0} \frac{r_1(v)}{\|v\|} = \lim_{v \rightarrow 0} \frac{r_2(v)}{\|v\|} = 0.$$

Calculando $(g \circ f)(p + v)$, obtemos

$$\begin{aligned} (g \circ f)(p + v) &= g(f(p + v)) = g(f(p) + Df(p) \cdot v + r_1(v)) \\ &= g(f(p)) + Dg(f(p)) \cdot (Df(p) \cdot v + r_1(v)) \\ &\quad + r_2(Df(p) \cdot v + r_1(v)) \\ &= (g \circ f)(p) + (Dg(f(p)) \circ Df(p)) \cdot v + Dg(f(p)) \cdot r_1(v) \\ &\quad + r_2(Df(p) \cdot v + r_1(v)). \end{aligned}$$

Portanto

$$\begin{aligned}(g \circ f)(p + v) - (g \circ f)(p) - (\text{D}g(f(p)) \circ \text{D}f(p)) \cdot v \\ = \text{D}g(f(p)) \cdot r_1(v) + r_1(\text{D}f(p) \cdot v + r_1(v)).\end{aligned}$$

Como $\text{D}g(f(p)) \circ \text{D}f(p)$ é uma transformação linear de \mathbb{R}^n para \mathbb{R}^l , basta mostrar que a expressão acima, dividida por $\|v\|$, vai a zero. Mas

$$\lim_{v \rightarrow 0} \frac{\text{D}g(f(p)) \cdot r_1(v)}{\|v\|} = \lim_{v \rightarrow 0} \text{D}g(f(p)) \cdot \frac{r_1(v)}{\|v\|} = 0$$

e, como $\lim_{v \rightarrow 0} \text{D}f(p) \cdot v + r_1(v) = 0$ e $\text{D}f(p) \cdot \frac{v}{\|v\|}$ é limitado,

$$\begin{aligned}\lim_{v \rightarrow 0} \frac{r_1(\text{D}f(p) \cdot v + r_1(v))}{\|v\|} \\ = \lim_{v \rightarrow 0} \frac{r_1(\text{D}f(p) \cdot v + r_1(v))}{\|\text{D}f(p) \cdot v + r_1(v)\|} \frac{\|\text{D}f(p) \cdot v + r_1(v)\|}{\|v\|} \\ = \lim_{v \rightarrow 0} \frac{r_1(\text{D}f(p) \cdot v + r_1(v))}{\|\text{D}f(p) \cdot v + r_1(v)\|} \left\| \text{D}f(p) \cdot \frac{v}{\|v\|} + \frac{r_1(v)}{\|v\|} \right\| = 0.\end{aligned}$$

Logo

$$\lim_{v \rightarrow 0} \frac{(g \circ f)(p + v) - (g \circ f)(p) - (\text{D}g(f(p)) \circ \text{D}f(p)) \cdot v}{\|v\|} = 0,$$

e concluímos que $\text{D}g(f(p)) \circ \text{D}f(p)$ é a diferencial de $g \circ f$ em p . ■

Proposição 19.4 (Regra da cadeia iterada). *Sejam $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ 2-diferenciável em $p \in \mathbb{R}^n$ e $g : \mathbb{R}^m \rightarrow \mathbb{R}^l$ diferenciável em $f(p)$. Então $g \circ f : \mathbb{R}^n \rightarrow \mathbb{R}^l$ é diferenciável em p e*

$$\text{D}^2(g \circ f)(p, p) = \text{D}^2g(f(p), f(p)) \circ \text{D}f(p) + \text{D}g(f(p)) \circ \text{D}^2f(p)$$

Proposição 19.5. *Sejam $f, g : \mathbb{R}^n \rightarrow \mathbb{R}^m$ diferenciáveis em $p \in \mathbb{R}^n$. Então*

1. $D(f + g)(p) = Df(p) + Dg(p);$
2. $D(f \cdot g) = Df(p) \cdot g(p) + f(p) \cdot Dg(p);$
3. Se $g(a) \neq 0$,

$$D\left(\frac{f}{g}\right)(p) = \frac{g(p) \cdot Df(a) - Dg(a) \cdot f(p)}{g(p)^2}$$

19.1.1 Diferenciais de Ordem Superior

Generalizamos, agora, a ideia de uma diferencial para uma r -diferencial. Para isso, denotaremos um vetor (v, \dots, v) com k entradas por $(v)^{\otimes k}$.

Definição 19.2. Seja $p \in \mathbb{R}^d$. Uma função r -diferenciável em p é uma função $f: \mathbb{R}^d \rightarrow \mathbb{R}^c$ tal que, para todo $k \in [r+1]$, existe uma função k -linear simétrica

$$L_k: \mathbb{R}^d \times \cdots \times \mathbb{R}^d \rightarrow \mathbb{R}^c$$

satisfazendo

$$\lim_{v \rightarrow 0} \frac{f(p+v) - f(p) - \sum_{k=1}^r \frac{1}{k!} L_k \cdot (v)^{\otimes k}}{\|v\|^r} = 0.$$

Uma função L_k como acima é uma *diferencial de ordem k* (ou k -ésima *diferencial*) da f em p .

Proposição 19.6. Sejam $p \in \mathbb{R}^d$ e $f: \mathbb{R}^d \rightarrow \mathbb{R}^c$ uma função k -diferenciável em p . Então f é $(k-1)$ -diferenciável em p .

Demonstração. Primeiro notemos que

$$\lim_{v \rightarrow 0} \frac{L_r \cdot (v)^{\otimes r}}{\|v\|^{r-1}} \leq \lim_{v \rightarrow 0} \frac{\|L_r\| \|v\|^r}{\|v\|^{r-1}} = \lim_{v \rightarrow 0} \|L_r\| \|v\| = 0.$$

Portanto segue que

$$\begin{aligned} & \lim_{v \rightarrow 0} \frac{f(p+v) - f(p) - \sum_{k=1}^{r-1} \frac{1}{k!} L_k \cdot (v)^{\otimes k}}{\|v\|^{r-1}} \\ &= \lim_{v \rightarrow 0} \frac{f(p+v) - f(p) - \sum_{k=1}^{r-1} \frac{1}{k!} L_k \cdot (v)^{\otimes k} - \frac{1}{r!} L_r \cdot (v)^{\otimes r}}{\|v\|^{r-1}} \\ &= \lim_{v \rightarrow 0} \|v\| \frac{f(p+v) - f(p) - \sum_{k=1}^r \frac{1}{k!} L_k \cdot (v)^{\otimes k}}{\|v\|^r} \\ &= 0. \end{aligned}$$

■

Proposição 19.7. Sejam $p \in \mathbb{R}^d$ e $f: \mathbb{R}^d \rightarrow \mathbb{R}^c$ uma função r -diferenciável em p . Então as k -ésimas diferenciais de f em p são únicas.

Demonstração. Mostraremos por indução em r . Para $r = 1$, temos a definição de função diferenciável, portanto a diferencial de f em p é única. Para o passo indutivo, suponhamos que toda função $(r - 1)$ -diferenciável tem únicas i -ésimas diferenciais para $0 \leq i \leq r - 1$. Consideremos uma função $f: \mathbb{R}^d \rightarrow \mathbb{R}^c$ r -diferenciável em p . Então ela é $(r - 1)$ -diferenciável em p pela proposição anterior e segue que, para todo $k \in [r]$, existe uma única função k -linear simétrica

$$L_k: \mathbb{R}^d \times \cdots \times \mathbb{R}^d \rightarrow \mathbb{R}^c$$

satisfazendo

$$\lim_{v \rightarrow 0} \frac{f(p + v) - f(p) - \sum_{k=1}^{r-1} \frac{1}{k!} L_k \cdot (v)^{\otimes k}}{\|v\|^r} = 0.$$

Agora, sejam L, S diferenciais de ordem r de f em p e definamos

$$A(v) := f(p + v) - f(p) - \sum_{k=1}^{r-1} \frac{1}{k!} L_k \cdot (v)^{\otimes k}.$$

Segue que

$$\begin{aligned} & \lim_{v \rightarrow 0} \frac{L \cdot (v)^{\otimes r} - S \cdot (v)^{\otimes r}}{\|v\|^r} \\ &= r! \lim_{v \rightarrow 0} \frac{\frac{1}{r!} L \cdot (v)^{\otimes r} - A(v) + A(v) - \frac{1}{r!} S \cdot (v)^{\otimes r}}{\|v\|^r} \\ &= -r! \lim_{v \rightarrow 0} \frac{\frac{1}{r!} L \cdot (v)^{\otimes r} - A(v)}{\|v\|^r} + r! \lim_{v \rightarrow 0} \frac{A(v) - \frac{1}{r!} S \cdot (v)^{\otimes r}}{\|v\|^r} \\ &= 0. \end{aligned}$$

Como L e S são transformações r -lineares, sabemos que $L \cdot (0)^{\otimes r} = S \cdot (0)^{\otimes r} = 0$. Para $v \in (\mathbb{R}^d)^r \setminus \{(0)^{\otimes r}\}$, temos que, quando $t \rightarrow 0$, $(tv)^{\otimes r} \rightarrow (0)^{\otimes r}$. Ainda, como L e S são r -lineares, $L \cdot (tv)^{\otimes r} = t^r L \cdot (v)^{\otimes r}$ e $S \cdot (tv)^{\otimes r} = t^r S \cdot (v)^{\otimes r}$, e segue que

$$\begin{aligned} 0 &= \lim_{tv \rightarrow 0} \frac{L \cdot (tv)^{\otimes r} - S \cdot (tv)^{\otimes r}}{\|tv\|^r} \\ &= \lim_{t \rightarrow 0} \frac{(t)^r (L \cdot (v)^{\otimes r} - S \cdot (v)^{\otimes r})}{|t|^r \|v\|^r} \\ &= \pm \frac{(L \cdot (v)^{\otimes r} - S \cdot (v)^{\otimes r})}{\|v\|^r} \end{aligned}$$

o que implica $L \cdot (v)^{\otimes r} = S \cdot (v)^{\otimes r}$, pois $\|v\| \neq 0$. Por fim, essa relação e a simetria de L e S implicam que elas são iguais em todos os pontos, portanto $L = S$. ■

Notação. Sejam $p \in \mathbb{R}^d$ e $f: \mathbb{R}^d \rightarrow \mathbb{R}^c$ uma função r -diferenciável em p . A diferencial de ordem r de f em p é denotada $D^r f(p): \mathbb{R}^d \times \cdots \times \mathbb{R}^d \rightarrow \mathbb{R}^c$ e, se definimos $D^0 f(p) := f(p)$, as diferenciais satisfazem

$$\lim_{v \rightarrow 0} \frac{f(p + v) - \sum_{k=0}^r \frac{1}{k!} D^k f(p) \cdot (v)^{\otimes k}}{\|v\|^r} = 0.$$

O polinômio

$$P(v) = \sum_{k=0}^r \frac{1}{k!} D^k f(p) \cdot (v)^{\otimes k}$$

é o *polinômio diferencial de ordem r* de f em p .

19.2 Derivadas Direcionais e a Geometria da Diferenciabilidade

A partir dessa seção, consideraremos funções $f: A \rightarrow \mathbb{R}^c$, em que $A \subseteq \mathbb{R}^d$ é um aberto. Toda a discussão feita na seção anterior considerou a diferenciabilidade em pontos do domínio. Agora, consideraremos a diferenciabilidade em conjuntos. A definição de diferenciabilidade da seção anterior pode ser facilmente adaptada para funções $f: A \rightarrow \mathbb{R}^c$ pois essa função pode ser definida em \mathbb{R}^d todo escolhendo qualquer valor para f em A^c . Como as definições e resultados trataram de pontos, isso não é um problema. Os abertos serão necessários agora pois consideraremos curvas numa vizinhança de um ponto e relacionaremos as derivadas por essas curvas com derivadas parciais da função f .

Definição 19.3. Sejam $A \subseteq \mathbb{R}^n$ um aberto, $p \in A$, $v \in \mathbb{R}^d$ tal que $p + v \in A$ e $f: A \rightarrow \mathbb{R}^c$. A *derivada direcional* de f em p na direção de v é

$$\frac{\partial f}{\partial v}(p) := \lim_{t \rightarrow 0} \frac{f(p + tv) - f(p)}{t}.$$

Como A é aberto, existe ε tal que $p + tv \in A$ para todo $t \in]-\varepsilon, \varepsilon[$. Tomemos então a curva

$$\begin{aligned} \gamma:]-\varepsilon, \varepsilon[&\longrightarrow A \\ t &\longmapsto p + tv, \end{aligned}$$

de modo que temos $\gamma(0) = p$ e $\gamma'(0) = v$. Então, pela regra da cadeia,

$$\frac{\partial f}{\partial v}(p) = D(f \circ \gamma)(0) = Df(\gamma(0)) \cdot \gamma'(0) = Df(p) \cdot v.$$

Disso concluímos que a derivada direcional de f em p na direção de v é a imagem de v sob a transformação linear $Df(p)$. Portanto definindo as derivadas direcionais $\partial_i f(x) := Df(x) \cdot e_i$ temos que

$$Df(x) \cdot v = \sum_{i=0}^{d-1} v^i \partial_i f(x).$$

19.3 Os Teoremas Fundamentais

19.3.1 Teorema da Função Inversa

Proposição 19.8. *Sejam $p \in \mathbb{R}^d$ e $f: \mathbb{R}^d \rightarrow \mathbb{R}^d$ uma função \mathcal{C}^r -diferenciável ($r \geq 1$) numa vizinhança aberta $A \subseteq \mathbb{R}^d$ de p . Se $Df(p): \mathbb{R}^d \rightarrow \mathbb{R}^d$ é invertível, então existe uma vizinhança aberta $V \subseteq \mathbb{R}^d$ de p tal que $f: V \rightarrow f(V)$ é invertível, $f^{-1}: f(V) \rightarrow V$ é \mathcal{C}^r -diferenciável e*

$$D(f^{-1})(f(p)) = (Df(p))^{-1}.$$

19.3.2 Teorema da Função Implícita

Proposição 19.9. *Sejam $p = (x_0, y_0) \in \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ e $f: \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \rightarrow \mathbb{R}^{d_1}$ uma função \mathcal{C}^r -diferenciável ($r \geq 1$) numa vizinhança aberta $A \subseteq \mathbb{R}^{d_0+d_1}$ de p tal que $f(p) = 0$. Se $Df(p): \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \rightarrow \mathbb{R}^{d_1}$ é sobrejetiva, então existem vizinhanças abertas $V_0 \subseteq \mathbb{R}^{d_0}$ de x_0 e $V_1 \subseteq \mathbb{R}^{d_1}$ de y_0 e única função \mathcal{C}^r -diferenciável $g: V_0 \subseteq \mathbb{R}^{d_0} \rightarrow V_1 \subseteq \mathbb{R}^{d_1}$ satisfazendo*

1. $g(x_0) = y_0$;
2. Para todos $(x, y) \in V_0 \times V_1$, $f(x, y) = 0$ se, e somente se, $y = g(x)$.

Observação: $Df(p): \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \rightarrow \mathbb{R}^{d_1}$ é sobrejetiva se, e somente se,

$$\begin{aligned} Df(p) \circ \iota_1: \mathbb{R}^{d_1} &\rightarrow \mathbb{R}^{d_1} \\ y &\mapsto D(f)(p) \cdot (0, y) \end{aligned}$$

é invertível (em que $\iota_1: \mathbb{R}^{d_1} \rightarrow \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$). Note que $D_1 f(p)$ também pode ser vista como essa função.

19.3.3 Forma Local da Imersão

Proposição 19.10. *Sejam $p \in \mathbb{R}^{d_0}$ e $f: \mathbb{R}^{d_0} \rightarrow \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ uma função \mathcal{C}^r -diferenciável ($r \geq 1$) numa vizinhança aberta $A \subseteq \mathbb{R}^{d_0}$ de p . Se $Df(p): \mathbb{R}^{d_0} \rightarrow$*

$\mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ é injetiva, então existem vizinhanças abertas $V_0 \subseteq \mathbb{R}^{d_0}$ de p , $V_1 \subseteq \mathbb{R}^{d_1}$ de 0 e $V \subseteq \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ de $f(p)$ e \mathcal{C}^r -difeomorfismo $g: V \rightarrow V_0 \times V_1$ tal que, para todo $x \in V_0$,

$$g \circ f(x) = (x, 0).$$

(ou seja, $g \circ f = \iota_0: V_0 \subseteq \mathbb{R}^{d_0} \rightarrow \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$).

Observação: A diferencial $Df(p): \mathbb{R}^{d_0} \rightarrow \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ é injetiva se, e somente se,

$$\begin{aligned} Df(p) \circ \pi_0: \mathbb{R}^{d_0} &\rightarrow \mathbb{R}^{d_0} \\ y &\mapsto (D(f)(p) \cdot y)|_{\mathbb{R}^{d_0}} \end{aligned}$$

é invertível.

19.3.4 Forma Local da Submersão

Proposição 19.11. Sejam $p = (x_0, y_0) \in \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ e $f: \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \rightarrow \mathbb{R}^{d_1}$ uma função \mathcal{C}^r -diferenciável ($r \geq 1$) numa vizinhança aberta $A \subseteq \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ de p . Se $Df(p): \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \rightarrow \mathbb{R}^{d_1}$ é sobrejetiva, então existem vizinhanças abertas $V \subseteq \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ de p , $V_0 \subseteq \mathbb{R}^{d_0}$ de x_0 e $V_1 \subseteq \mathbb{R}^{d_1}$ de $f(p)$ e \mathcal{C}^r -difeomorfismo $g: V_0 \times V_1 \rightarrow V$ tal que, para todo $(x, y) \in V_0 \times V_1$,

$$f \circ g(x, y) = y.$$

(ou seja, $f \circ g = \pi_1: V_0 \times V_1 \subseteq \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \rightarrow \mathbb{R}^{d_1}$).

Observação: A diferencial $Df(p): \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \rightarrow \mathbb{R}^{d_1}$ é sobrejetiva se, e somente se,

$$\begin{aligned} Df(p) \circ \iota_1: \mathbb{R}^{d_1} &\rightarrow \mathbb{R}^{d_1} \\ y &\mapsto D(f)(p) \cdot (0, y) \end{aligned}$$

é invertível. Note que $D_1 f(p)$ também pode ser vista como essa função.

19.3.5 Teorema do Posto

Proposição 19.12. Seja $f: \mathbb{R}^d \times \mathbb{R}^{d_0} \rightarrow \mathbb{R}^d \times \mathbb{R}^{d_1}$ uma função \mathcal{C}^r -diferenciável ($r \geq 1$) num aberto $A \subseteq \mathbb{R}^d \times \mathbb{R}^{d_0}$. Se $Df(p): \mathbb{R}^d \times \mathbb{R}^{d_0} \rightarrow \mathbb{R}^d \times \mathbb{R}^{d_1}$ tem o mesmo posto para todo $p \in A$ (f tem posto constante em A), então, para todo $p \in A$, existem vizinhanças abertas $V_0 \subseteq \mathbb{R}^d \times \mathbb{R}^{d_0}$ de p e $V_1 \subseteq \mathbb{R}^d \times \mathbb{R}^{d_1}$ de $f(p)$ e \mathcal{C}^r -difeomorfismos $g_0: V_0 \rightarrow g_0(V_0) \subseteq \mathbb{R}^d \times \mathbb{R}^{d_0}$ e $g_1: V_1 \rightarrow g_1(V_1) \subseteq \mathbb{R}^d \times \mathbb{R}^{d_1}$ tais que, para todo $(x, y) \in V_0$,

$$g_1 \circ f \circ g_0^{-1}(x, y) = (x, 0).$$

(ou seja, $g_1 \circ f \circ g_0^{-1} = \iota \circ \pi: \mathbb{R}^d \times \mathbb{R}^{d_0} \rightarrow \mathbb{R}^d \times \mathbb{R}^{d_1}$).

19.4 Cálculo em Espaços Normados de Dimensão Finita

19.4.1 Diferencial

Definição 19.4. Sejam \mathbb{E}_0 e \mathbb{E}_1 espaços normados de dimensão finita, $p \in \mathbb{E}_0$, $A \subseteq E_0$ uma vizinhança aberta de p e $f: A \rightarrow \mathbb{E}_1$ uma função. Uma *diferencial* de f em p é uma função linear $L: \mathbb{E}_0 \rightarrow \mathbb{E}_1$ que satisfaz

$$\lim_{v \rightarrow 0} \frac{f(p+v) - f(p) - L \cdot v}{\|v\|} = 0.$$

Uma função *diferenciável* em p é uma função definida numa vizinhança aberta de p que tem diferencial em p . Uma função diferenciável em um conjunto $C \subseteq \mathbb{E}_0$ é uma função diferenciável em todo $p \in C$, ou seja, uma função definida numa vizinhança aberta de C e diferenciável em todos seus pontos.

Relembremos que a norma escolhida para o espaço linear é irrelevante, já que elas são todas equivalentes quando a dimensão do espaço normado é finita. A necessidade de definirmos a função em uma vizinhança aberta do ponto é para que a noção de limite esteja bem definida. A diferencial é única quando existe, como mostraremos na proposição a seguir. Isso permite que denotemos essa função linear de um jeito específico que será definido depois da demonstração da proposição.

Proposição 19.13 (Unicidade da Diferencial). *Sejam \mathbb{E}_0 e \mathbb{E}_1 espaços normados de dimensão finita, $A \subseteq E_0$ um aberto, $p \in A$ e $f: A \rightarrow \mathbb{E}_1$ uma função diferenciável em p . Então existe uma única diferencial de f em p .*

Demonstração. Sejam $L, \bar{L}: \mathbb{E}_0 \rightarrow \mathbb{E}_1$ diferenciais de f em p . Nesse caso, temos que

$$\begin{aligned} & \lim_{v \rightarrow 0} \frac{L \cdot v - \bar{L} \cdot v}{\|v\|} = \\ &= \lim_{v \rightarrow 0} \frac{L \cdot v - (f(p+v) - f(p)) + (f(p+v) - f(p)) - \bar{L} \cdot v}{\|v\|} \\ &= - \lim_{v \rightarrow 0} \frac{f(p+v) - f(p) - L \cdot v}{\|v\|} + \lim_{v \rightarrow 0} \frac{f(p+v) - f(p) - \bar{L} \cdot v}{\|v\|} \\ &= 0. \end{aligned}$$

Como L e \bar{L} são transformações lineares, sabemos que $L \cdot 0 = \bar{L} \cdot 0 = 0$. Para todo $v \in \mathbb{E}_0 \setminus \{0\}$, temos que, quando $t \rightarrow 0$, $tv \rightarrow 0$. Ainda, como L e \bar{L} são

transformações lineares, $L \cdot (tv) = t(L \cdot v)$ e $\bar{L} \cdot (tv) = t(\bar{L} \cdot v)$, e segue que

$$\begin{aligned} 0 &= \lim_{tv \rightarrow 0} \frac{\|L \cdot (tv) - \bar{L} \cdot (tv)\|}{\|tv\|} \\ &= \lim_{t \rightarrow 0} \frac{|t| \|L \cdot v - \bar{L} \cdot v\|}{|t| \|v\|} \\ &= \frac{\|L \cdot v - \bar{L} \cdot v\|}{\|v\|}, \end{aligned}$$

o que implica $L \cdot v = \bar{L} \cdot v$, pois $\|v\| \neq 0$. Portanto $L = \bar{L}$. ■

Notaçāo. Sejam \mathbb{E}_0 e \mathbb{E}_1 espaços normados de dimensão finita, $A \subseteq E_0$ um aberto, $p \in A$ e $f: A \rightarrow \mathbb{E}_1$ uma função diferenciável em p . A diferencial de f em p é denotada $Df(p) : \mathbb{E}_0 \rightarrow \mathbb{E}_1$ e satisfaz

$$\lim_{v \rightarrow 0} \frac{f(p + v) - f(p) - Df(p) \cdot v}{\|v\|} = 0.$$

Proposição 19.14 (Diferenciabilidade implica Continuidade). *Sejam \mathbb{E}_0 e \mathbb{E}_1 espaços normados de dimensão finita, $A \subseteq E_0$ um aberto, $p \in A$ e $f: A \rightarrow \mathbb{E}_1$ uma função diferenciável em p . Então f é contínua em p .*

Demonstração. Se f é diferenciável em p , como vale $\lim_{v \rightarrow 0} Df(p) \cdot v = 0$, segue que

$$\begin{aligned} \lim_{v \rightarrow 0} (f(p + v) - f(p)) &= \lim_{v \rightarrow 0} (f(p + v) - f(p) - Df(p) \cdot v) \\ &= \lim_{v \rightarrow 0} \|v\| \frac{f(p + v) - f(p) - Df(p) \cdot v}{\|v\|} \\ &= 0, \end{aligned}$$

o que implica que f é contínua em p . ■

Proposição 19.15 (Regra da Cadeia). *Sejam $\mathbb{E}_0, \mathbb{E}_1$ e \mathbb{E}_2 espaços normados de dimensão finita, $A_0 \subseteq E_0$ e $A_1 \subseteq E_1$ abertos e $f_0: A_0 \rightarrow \mathbb{E}_1$ e $f_1: A_1 \rightarrow \mathbb{E}_2$ funções. Se f_0 é diferenciável em $p \in A_0$ e f_1 é diferenciável em $f_0(p) \in A_1$, então $f_1 \circ f_0$ é diferenciável em p e*

$$D(f_1 \circ f_0)(p) = Df_1(f_0(p)) \circ Df_0(p).$$

Demonstração. Definamos

$$r_0(v) := f_0(p + v) - f_0(p) - Df_0(p) \cdot v$$

e

$$r_1(v) := f_1(f_0(p) + v) - f_1(f_0(p)) - Df_1(f_0(p)) \cdot v,$$

de modo que da diferenciabilidade de f_0 em p e de f_1 em $f_0(p)$ segue

$$\lim_{v \rightarrow 0} \frac{r_0(v)}{\|v\|} = \lim_{v \rightarrow 0} \frac{r_1(v)}{\|v\|} = 0.$$

Calculando $(f_1 \circ f_0)(p + v)$, obtemos

$$\begin{aligned} (f_1 \circ f_0)(p + v) &= f_1(f_0(p + v)) = f_1(f_0(p) + Df_0(p) \cdot v + r_0(v)) \\ &= f_1(f_0(p)) + Df_1(f_0(p)) \cdot (Df_0(p) \cdot v + r_0(v)) \\ &\quad + r_1(Df_0(p) \cdot v + r_0(v)) \\ &= (f_1 \circ f_0)(p) + (Df_1(f_0(p)) \circ Df_0(p)) \cdot v + Df_1(f_0(p)) \cdot r_0(v) \\ &\quad + r_1(Df_0(p) \cdot v + r_0(v)). \end{aligned}$$

Portanto

$$\begin{aligned} (f_1 \circ f_0)(p + v) - (f_1 \circ f_0)(p) - (Df_1(f_0(p)) \circ Df_0(p)) \cdot v \\ = Df_1(f_0(p)) \cdot r_0(v) + r_1(Df_0(p) \cdot v + r_0(v)). \end{aligned}$$

Como $Df_1(f_0(p)) \circ Df_0(p)$ é uma transformação linear de \mathbb{R}^n para \mathbb{R}^l , basta mostrar que a expressão acima, dividida por $\|v\|$, vai a zero. Mas

$$\lim_{v \rightarrow 0} \frac{Df_1(f_0(p)) \cdot r_0(v)}{\|v\|} = \lim_{v \rightarrow 0} Df_1(f_0(p)) \cdot \frac{r_0(v)}{\|v\|} = 0$$

e, como $\lim_{v \rightarrow 0} Df_0(p) \cdot v + r_0(v) = 0$ e $Df_0(p) \cdot \frac{v}{\|v\|}$ é limitado,

$$\begin{aligned} &\lim_{v \rightarrow 0} \frac{r_1(Df_0(p) \cdot v + r_0(v))}{\|v\|} \\ &= \lim_{v \rightarrow 0} \frac{r_1(Df_0(p) \cdot v + r_0(v))}{\|Df_0(p) \cdot v + r_0(v)\|} \frac{\|Df_0(p) \cdot v + r_0(v)\|}{\|v\|} \\ &= \lim_{v \rightarrow 0} \frac{r_1(Df_0(p) \cdot v + r_0(v))}{\|Df_0(p) \cdot v + r_0(v)\|} \left\| Df_0(p) \cdot \frac{v}{\|v\|} + \frac{r_0(v)}{\|v\|} \right\| = 0. \end{aligned}$$

Logo

$$\lim_{v \rightarrow 0} \frac{(f_1 \circ f_0)(p + v) - (f_1 \circ f_0)(p) - (Df_1(f_0(p)) \circ Df_0(p)) \cdot v}{\|v\|} = 0,$$

e concluímos que $Df_1(f_0(p)) \circ Df_0(p)$ é a diferencial de $f_1 \circ f_0$ em p . ■

Capítulo 20

Variedades

20.1 Estrutura Topológica e Diferencial

20.1.1 Cartas e Atlas

Definição 20.1. Sejam V um conjunto e $d \in \mathbb{N}$. Uma *carta d -dimensional* de V é um par (A, x) em que $A \subseteq V$ é um conjunto e $x: A \rightarrow \mathbb{R}^d$ é uma função injetiva tal que $x(A)$ é um aberto de \mathbb{R}^d . O *domínio* de (A, x) é A , o domínio de x , e o *mapa de coordenadas* de (A, x) é a função x . A i -ésima *coordenada* da carta (A, x) é a função $x^i := \pi^i \circ x: A \rightarrow \mathbb{R}$.

Definição 20.2. Sejam V um conjunto e $(A, x), (\bar{A}, \bar{x})$ cartas d -dimensionais de V . A *transição de coordenadas* de (A, x) para (\bar{A}, \bar{x}) é a função

$$\bar{x} \circ x^{-1}: x(A \cap \bar{A}) \rightarrow \bar{x}(A \cap \bar{A}).$$

A composição $\bar{x} \circ x^{-1}$ não está necessariamente definida em todo $x(A)$, mas somente na interseção do domínio de x^{-1} com a imagem inversa do domínio de \bar{x} por x^{-1} . Para ver que esse é o conjunto acima, basta notar que da injetividade de x segue

$$x(A) \cap (x^{-1})^{-1}(\bar{A}) = x(A \cap \bar{A}).$$

Da mesma forma definimos o contradomínio como acima.

Definição 20.3. Seja V um conjunto. Cartas \mathcal{C}^k -compatíveis de V são cartas (A, x) e (\bar{A}, \bar{x}) tais que $x(A \cap \bar{A})$ e $\bar{x}(A \cap \bar{A})$ são abertos e a transição de coordenadas

$$\bar{x} \circ x^{-1}: x(A \cap \bar{A}) \rightarrow \bar{x}(A \cap \bar{A})$$

é um difeomorfismo \mathcal{C}^k . Para $k = 0$, as cartas são *topologicamente compatíveis*, para $k > 0$, são *diferencialmente compatíveis*, sendo para $k = \infty$ *suavemente compatíveis*.

A relação de compatibilidade entre cartas não é uma relação de equivalência, mas a compatibilidade de atlas, uma noção associada a ela, é. A seguir, definimos o que é um atlas. A primeira condição, além de aparentemente necessária para que todos os pontos de V tenham cartas, será uma hipótese essencial para que a compatibilidade de atlas seja uma relação de equivalência. Isso é um resultado muito simples, mas que indica que nossa axiomatização é boa, de certa forma, pois ao termos a estrutura de um atlas do conjunto, não temos simplesmente várias cartas, mas cartas que se comportam de acordo com certa relação de equivalência. Essa relação de equivalência nos permitirá definir um objeto abstrato chamado atlas maximal, que na prática nunca é calculado, mas que como objeto teórico é belo e conveniente.

Definição 20.4. Seja V um conjunto. Um *atlas \mathcal{C}^k d-dimensional* de V é um conjunto \mathcal{A} de cartas d -dimensionais de V tal que

1. (Cobertura) O conjunto V é coberto pelos domínios das cartas de \mathcal{A}

$$V = \bigcup_{(A,x) \in \mathcal{A}} A;$$

2. (Compatibilidade) Todas cartas $(A, x), (\bar{A}, \bar{x}) \in \mathcal{A}$ são \mathcal{C}^k -compatíveis.

Para $k = 0$, \mathcal{A} é um atlas *topológico*, para $k > 0$, um atlas *diferencial*, sendo para $k = \infty$ um atlas *suave*.

Na definição de atlas, se não especificássemos que todas cartas devem ser d -dimensionais, poderíamos ter partes do conjunto V que fossem mapeadas em espaços reais de dimensão diferente. No entanto, nas cartas $(A, x), (\bar{A}, \bar{x}) \in \mathcal{A}$ em que $A \cap \bar{A} \neq \emptyset$, teríamos ao menos um homeomorfismo entre os conjuntos $x(A \cap \bar{A})$ e $\bar{x}(A \cap \bar{A})$, de modo que as cartas poderiam ser restritas a espaços reais de mesma dimensão; se $k \geq 1$, diferenciando a transição de coordenadas $\bar{x} \circ x^{-1}$ teríamos um homeomorfismo linear entre os espaços reais, garantindo a mesma dimensão. Isso mostra que, a menos de cartas que não tenham interseção no domínio, teríamos que ter espaços reais de mesma dimensão modelando o conjunto V . A partir de agora, sempre consideraremos que os atlases têm a mesma dimensão, e a dimensão de um atlas só será mencionada quando necessário.

Definição 20.5. Seja V um conjunto. Atlases \mathcal{C}^k -compatíveis de V são atlases \mathcal{C}^k \mathcal{A} e $\bar{\mathcal{A}}$ de V tais que todas as cartas $(A, x) \in \mathcal{A}$ e $(\bar{A}, \bar{x}) \in \bar{\mathcal{A}}$ são \mathcal{C}^k -compatíveis.

Essa definição é equivalente a dizer que $\mathcal{A} \cup \bar{\mathcal{A}}$ é um atlas \mathcal{C}^k .

Proposição 20.1. Seja V um conjunto. A relação de \mathcal{C}^k -compatibilidade de atlases de V é uma relação de equivalência.

Demonstração. A reflexividade e a simetria são evidentes, pois valem entre cartas. Para conferir a transitividade, sejam $\mathcal{A}, \bar{\mathcal{A}}$ e $\{(A_i, x_i)\}_{i \in I}$ atlas de V e sejam $(A, x) \in \mathcal{A}$ e $(\bar{A}, \bar{x}) \in \bar{\mathcal{A}}$ cartas. Como \mathcal{A} e $\bar{\mathcal{A}}$ são compatíveis com $\{(A_i, x_i)\}_{i \in I}$, segue que para todo $i \in I$, $x(A \cap A_i)$ e $x_i(A_i \cap \bar{A})$ são abertos de \mathbb{R}^d e as transições de coordenadas

$$x_i \circ x^{-1} : x(A \cap A_i) \longrightarrow x_i(A_i \cap \bar{A}).$$

e

$$\bar{x} \circ x_i^{-1} : x_i(A_i \cap \bar{A}) \longrightarrow \bar{x}(A_i \cap \bar{A}).$$

são difeomorfismos \mathcal{C}^k . Compondo essas transições de coordenada, e notando que

$$x(A \cap A_i) \cap (x_i \circ x^{-1})^{-1}(x_i(A_i \cap \bar{A})) = x(A \cap A_i \cap \bar{A})$$

(e analogamente para $\bar{x}(A \cap A_i \cap \bar{A})$), concluímos que

$$(\bar{x} \circ x_i^{-1}) \circ (x_i \circ x^{-1}) : x(A \cap A_i \cap \bar{A}) \longrightarrow \bar{x}(A \cap A_i \cap \bar{A})$$

e é um difeomorfismo \mathcal{C}^k .

Agora, notemos que o conjunto $x(A \cap A_i \cap \bar{A})$ é um aberto de \mathbb{R}^d já que $x(A \cap A_i)$ e $x_i(A_i \cap \bar{A})$ são abertos e $x_i \circ x^{-1}$ é contínua. Como

$$V = \bigcup_{i \in I} A_i,$$

segue que

$$\bigcup_{i \in I} x(A \cap A_i \cap \bar{A}) = x \left(A \cap \bigcup_{i \in I} A_i \cap \bar{A} \right) = x(A \cap \bar{A}),$$

então $x(A \cap \bar{A})$ é aberto de \mathbb{R}^d . Analogamente, o contradomínio de $\bar{x} \circ x^{-1}$ é $\bar{x}(A \cap \bar{A})$ e é aberto de \mathbb{R}^d . Portanto $\bar{x} \circ x^{-1}$ é uma função bem definida em $x(A \cap \bar{A})$ e segue que

$$\bar{x} \circ x^{-1} : x(A \cap \bar{A}) \longrightarrow \bar{x}(A \cap \bar{A}).$$

é um difeomorfismo \mathcal{C}^k , o que mostra que (A, x) e (\bar{A}, \bar{x}) são \mathcal{C}^k -compatíveis, e finalmente \mathcal{A} e $\bar{\mathcal{A}}$ são \mathcal{C}^k -compatíveis. ■

Isso implica, em particular, que os atlas $\mathcal{C}^k d$ -dimensionais de V podem ser particionados em classes de equivalência. Além disso, segue da proposição anterior que se dois atlas são compatíveis, sua união é um atlas, o que motiva a próxima definição.

Definição 20.6. Seja V um conjunto. Um atlas *maximal* \mathcal{C}^k (ou uma *estrutura diferencial* \mathcal{C}^k) d -dimensional de V é a união de todos os atlas de uma classe de equivalência de atlas $\mathcal{C}^k d$ -dimensionais de V .

Como comentado acima, o atlas maximal é um atlas, pois é uma união de atlas compatíveis. Com essa definição, podemos finalmente definir uma variedade.

20.2 Variedades e Topologia

Definição 20.7. Uma variedade \mathcal{C}^k d -dimensional é um par $\mathbf{V} = (V, \mathcal{A})$ em que V é um conjunto e \mathcal{A} é um atlas maximal \mathcal{C}^k d -dimensional de V . Para $k = 0$, a variedade \mathbf{V} é uma variedade *topológica* e, para $k > 0$, é uma variedade *diferencial*, sendo para $k = \infty$ uma variedade *suave*.

Quando não for necessário explicitar detalhes, uma variedade \mathcal{C}^k d -dimensional será simplesmente referida como uma variedade. Denotamos ainda a dimensão da variedade por um expoente: \mathbf{V}^d . É possível mostrar que toda variedade diferencial tem um subatlas maximal suave, de modo que não há perda de informação quando se separam as variedades apenas em topológicas e diferenciais, mas isso não será feito aqui.

Definição 20.8. Seja \mathbf{V} uma variedade. A *topologia* de \mathbf{V} é o conjunto

$$\mathcal{T} := \left\langle \bigcup_{(A,x) \in \mathcal{A}} x^*(\mathcal{T}_{\mathbb{R}^d}) \right\rangle,$$

em que $\mathcal{T}_{\mathbb{R}^d}$ é a topologia de \mathbb{R}^d .

Na notação acima, $\langle C \rangle$ denota a topologia gerada pelo conjunto $C \subseteq \mathcal{P}(V)$ e $x^*(\mathcal{T})$ denota a topologia puxada de \mathcal{T} pela função x , ou seja, o conjunto de imagens inversas por x de abertos da topologia \mathcal{T} . Essa é a menor topologia tal que todos os mapas de coordenadas x das cartas do atlas maximal são contínuos, a topologia inicial com respeito aos mapas de coordenadas do atlas da variedade. Pode-se ver que essa é a topologia cuja base são os domínios das cartas do atlas maximal. Ainda, vale notar que essa é a mesma topologia da gerada pelas topologias puxadas de $\mathcal{T}|_{x(A)}$, a topologia induzida de \mathcal{T} em $x(A)$. Isso ocorre porque os mapas de coordenadas x são bijeções no seu domínio, logo puxam qualquer subconjunto de $x(A)^c$ no vazio. De fato, há várias definições equivalentes de como induzir uma topologia em uma variedade, e a acima parece ser a mais bem definida em questão de teoria; no entanto, em geral só conseguimos conhecer um atlas de uma variedade, e não o atlas maximal todo, portanto saber gerar a topologia sem precisar do atlas maximal seria uma ferramenta muito boa, essencial às vezes. É isso que as proposições a seguir oferecem. A primeira afirma que, se gerarmos uma topologia a partir de uma atlas, qualquer carta compatível com esse atlas terá um mapa de coordenadas contínuo, o que implica, em particular, que as topologias geradas pelo atlas maximal e as geradas por qualquer subatlas são a mesma.

Proposição 20.2. Sejam V um conjunto, $\mathcal{A} = \{(A_i, x_i)\}_{i \in I}$ um atlas de V e

$$\mathcal{T} := \left\langle \bigcup_{i \in I} x_i^*(\mathcal{T}_{\mathbb{R}^d}) \right\rangle.$$

Se (A, x) é uma carta compatível com \mathcal{A} , então x é uma função contínua.

Demonstração. Seja U um aberto de \mathbb{R}^d . Para todo $i \in I$, definamos $U_i := (x \circ x_i^{-1})(x_i(A_i))$ e $S := \mathbb{R}^d \setminus \bigcup_{i \in I} U_i$. Então

$$U = U \cap \mathbb{R}^d = \bigcup_{i \in I} (U \cap U_i) \cup (U \cap S).$$

Como $V = \bigcup_{i \in I} A_i$ e, para todo $i \in I$, $x^{-1}(U_i) = A \cap A_i$, então

$$\begin{aligned} x^{-1}(S) &= x^{-1}(\mathbb{R}^d) \cap x^{-1}\left(\left(\bigcup_{i \in I} U_i\right)^c\right) \\ &= A \cap \left(\bigcup_{i \in I} x^{-1}(U_i)\right)^c \\ &= A \cap \left(\bigcup_{i \in I} A \cap A_i\right)^c \\ &= A \cap (A \cap V)^c = A \cap (A)^c = \emptyset. \end{aligned}$$

Disso, segue que $x^{-1}(U \cap S) = \emptyset$ e, portanto,

$$\begin{aligned} x^{-1}(U) &= \bigcup_{i \in I} x^{-1}(U \cap U_i) \cup x^{-1}(U \cap S) \\ &= \bigcup_{i \in I} (A \cap A_i) \cup (A \cap \emptyset) \\ &= \bigcup_{i \in I} A \cap A_i. \end{aligned}$$

Mostraremos, agora, que $A \cap A_i$ é aberto para todo $i \in I$, e com isso concluiremos que x^{-1} é aberto. Para isso, notemos que

$$x_i(A \cap A_i) = x_i(A_i) \cap (x_i \circ x^{-1})(x(A)).$$

Como $x(A)$ é aberto, pois (A, x) é carta, e $x \circ x_i^{-1}$ é difeomorfismo, pois (A, x) é compatível com \mathcal{A} , então $(x_i \circ x^{-1})(x(A))$ é aberto e, portanto, $x_i(A \cap A_i)$ é aberto, o que implica que $x_i^{-1}(x_i(A \cap A_i)) = A \cap A_i$ é aberto. Assim, concluímos que $x^{-1}(U)$ é aberto de \mathcal{T} , portanto x é contínua. \blacksquare

Proposição 20.3. *Sejam $\mathbf{V} = (V, \mathcal{A})$ uma variedade e $\bar{\mathcal{A}}$ um atlas compatível com o atlas maximal \mathcal{A} . A topologia*

$$\bar{\mathcal{T}} := \left\langle \bigcup_{(A,x) \in \bar{\mathcal{A}}} x^*(\mathcal{T}_{\mathbb{R}^d}) \right\rangle,$$

é igual à topologia \mathcal{T} de \mathbf{V} .

Demonstração. Por definição da topologia de \mathbf{V} , temos imediatamente que $\bar{\mathcal{T}} \subseteq \mathcal{T}$. Para a inclusão contrária, a proposição anterior mostra que toda carta de \mathcal{A} tem mapa de coordenadas contínuo em $\bar{\mathcal{T}}$, o que implica que $\mathcal{T} \subseteq \bar{\mathcal{T}}$. ■

Uma consequência óbvia das definições é que qualquer subconjunto aberto de \mathbb{R}^d é uma variedade. Antes de continuar a discussão sobre as propriedades topológicas de variedades, um comentário importante é que alguns autores definem uma variedade a partir de um espaço topológico desde o início, exigindo que os mapas de coordenadas sejam homeomorfismos com sua imagem no espaço real. A partir dessa definição, a topologia da variedade já existe desde o começo e não é induzida pelas cartas.

20.2.1 Exemplos de Variedades

A Esfera

Definição 20.9. A *esfera d-dimensional* é o conjunto

$$\mathbb{S}^d := \left\{ x \in \mathbb{R}^{d+1} \mid \|x\| = 1 \right\}.$$

A partir dessa notação de esfera unitária, podemos escrever facilmente qualquer n -esfera de raio $r \in \mathbb{R}$ e centro $c \in \mathbb{R}^{d+1}$ em \mathbb{R}^{d+1} como $c + r\mathbb{S}^d$ usando a notação de adição e multiplicação de um elemento de um anel com um subconjunto do anel.

Vamos considerar, na esfera, um atlas com apenas duas cartas: as *projeções estereográficas* focadas no norte e no sul.

Definição 20.10. O *pólo norte* de \mathbb{S}^d é o ponto $N := (0, \dots, 0, 1)$ e a *projeção estereográfica norte* de \mathbb{S}^d é a função

$$\begin{aligned} \pi_N: \mathbb{S}^d \setminus \{N\} &\longrightarrow \mathbb{R}^d \\ x &\longmapsto \frac{1}{1 - x_d}(x_0, \dots, x_{d-1}). \end{aligned}$$

O *pólo sul* de \mathbb{S}^d é o ponto $S := -N = (0, \dots, 0, -1)$ e a *projeção estereográfica sul* de \mathbb{S}^d é a função

$$\begin{aligned} \pi_S: \mathbb{S}^d \setminus \{S\} &\longrightarrow \mathbb{R}^d \\ x &\longmapsto \frac{1}{1 + x_d}(x_0, \dots, x_{d-1}). \end{aligned}$$

Proposição 20.4. Sejam π_N e π_S as projeções estereográficas norte e sul de \mathbb{S}^d . O conjunto

$$\mathcal{A} := \{(\mathbb{S}^d \setminus \{N\}, \pi_N), (\mathbb{S}^d \setminus \{S\}, \pi_S)\}$$

é um atlas de \mathbb{S}^d .

Demonstração. As inversas de π_N e π_S são dadas por

$$\begin{aligned}\pi_N^{-1} : \mathbb{R}^d &\longrightarrow \mathbb{S}^d \\ x &\longmapsto \frac{1}{\|x\|^2 + 1} (2x_0, \dots, 2x_{d-1}, \|x\|^2 - 1)\end{aligned}$$

e

$$\begin{aligned}\pi_S^{-1} : \mathbb{R}^d &\longrightarrow \mathbb{S}^d \\ x &\longmapsto \frac{-1}{\|x\|^2 + 1} (2x_0, \dots, 2x_{d-1}, \|x\|^2 - 1).\end{aligned}$$

A transição de coordenadas entre as cartas é dada por

$$\begin{aligned}\pi_N \circ \pi_S^{-1} : \mathbb{R}^d \setminus \{0\} &\longrightarrow \mathbb{R}^d \setminus \{0\} \\ x &\longmapsto \frac{1}{\|x\|^2} x.\end{aligned}$$

Claramente, todas as funções são suaves. ■

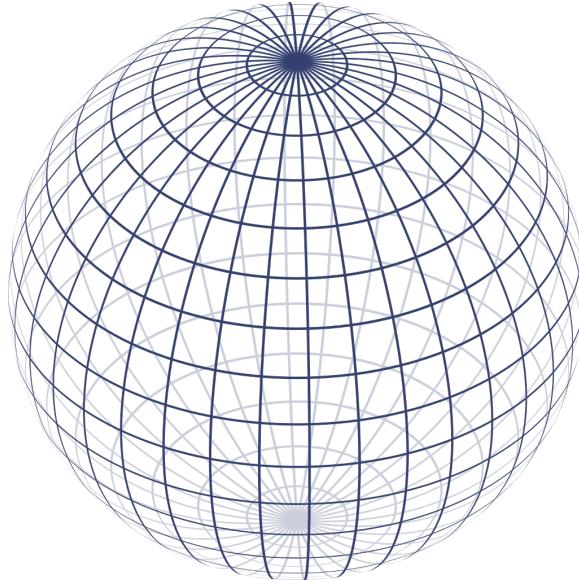


Figura 20.1: Esfera 2-dimensional

O Espaço Projetivo

Definição 20.11. Sejam $x, y \in \mathbb{R}^d \setminus \{0\}$. A relação de *equivalência homogênea* entre os pontos é definida por

$$x : y \iff \exists t \in \mathbb{R}^* \quad x = ty.$$

Essa relação é realmente uma relação de equivalência, pois tomando $t = 1$ temos a reflexividade, tomando $\bar{t} = t^{-1}$ temos a simetria e tomando $t_1 t_0$ temos a transitividade. A classe de equivalência de um ponto $x \in \mathbb{R}^d$ é a reta sem a origem de \mathbb{R}^d que passa pela origem e por x , e é denotada por $[x_0 : \dots : x_{d-1}] := [x]$.

Definição 20.12. O *espaço projetivo real d-dimensional* é o conjunto

$$\mathbb{PR}^d := \left\{ [x_0 : \dots : x_d] \mid x \in \mathbb{R}^{d+1} \right\}.$$

Considerando os conjuntos

$$A_i := \left\{ [x_0 : \dots : x_d] \in \mathbb{PR}^d \mid x_i \neq 0 \right\}.$$

e as funções

$$\begin{aligned} \varphi_i: A_i &\longrightarrow \mathbb{R}^d \\ [x_0 : \dots : x_d] &\longmapsto \frac{1}{x_i}(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_d), \end{aligned}$$

cujas inversas são

$$\begin{aligned} \varphi_i^{-1}: \mathbb{R}^d &\longrightarrow A_i \\ x &\longmapsto [x_0 : \dots, x_{i-1} : 1 : x_i : \dots : x_{d-1}]. \end{aligned}$$

Uma descrição equivalente é

$$\mathbb{PR}^d := \mathbb{S}^d / \mathbb{S}^0 = \left\{ \{x, -x\} \mid x \in \mathbb{S}^d \right\}.$$

Essa construção considera a ação de \mathbb{S}^0 em \mathbb{S}^d , a saber,

$$\begin{aligned} \times: \mathbb{S}^0 \times \mathbb{S}^d &\longrightarrow \mathbb{S}^d \\ (u, x) &\longmapsto ux. \end{aligned}$$

O espaço $\mathbb{S}^0 = \{1, -1\} \subseteq \mathbb{R}$ tem estrutura de grupo com a multiplicação de \mathbb{R} e pode ser identificado com o grupo \mathbb{Z}_2 pelo isomorfismo de grupos

$$\begin{aligned} h: (\mathbb{Z}_2, +) &\longrightarrow (\mathbb{S}^0, \times) \\ n &\longmapsto (-1)^n, \end{aligned}$$

que é homomorfismo pois $(-1)^{n+n'} = (-1)^n(-1)^{n'}$ e é claramente bijeção.

O Toro

Definição 20.13. O *toro d-dimensional* é o conjunto

$$\mathbb{T}^d := \mathbb{R}^d / \mathbb{Z}^d.$$

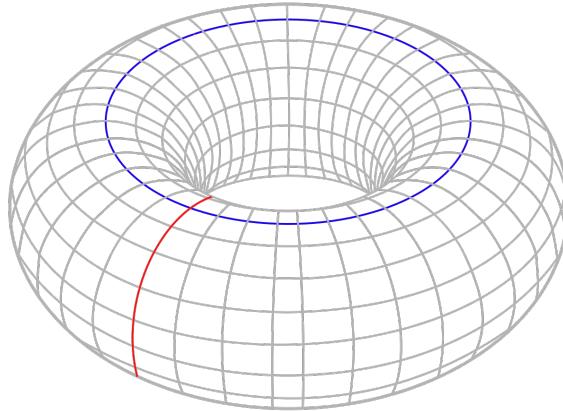


Figura 20.2: Toro

Hiperboloide

Definição 20.14. O *hiperboloide d-dimensional* é o conjunto

$$\mathbb{H}^d := \left\{ (x, t) \in \mathbb{R}^d \times \mathbb{R} = \mathbb{R}^{d+1} \mid \|x\|^2 + 1 = t^2 \text{ e } t > 0 \right\}.$$

20.2.2 Propriedades Topológicas

Uma variedade definida como acima não precisa necessariamente ser um espaço separado (T_2), ou seja, espaço cujos pontos distintos são separados por vizinhanças. Em geral, na definição de variedade consideram-se espaços separados, mas ainda não faremos essa distinção. Ainda, outra hipótese comum é que a topologia admita base enumerável. Isso é equivalente, para uma variedade, a existir um subatlas enumerável.

Proposição 20.5. *Seja \mathbf{V} uma variedade. Então*

1. \mathbf{V} é um espaço topológico acessível (T_1);
2. \mathbf{T} tem base enumerável se, e somente se, existe um subatlas enumerável de \mathcal{A} .
3. Cada componente conexa de \mathbf{V} é conexa por caminhos.

Demonstração. 1. Sejam p, \bar{p} pontos distintos de V . Queremos mostrar que existe vizinhança de cada um que não contém o outro. Para isso, tomamos carta (A, x) em p . Se A não contém \bar{p} , então A é vizinhança de p que não contém \bar{p} ; caso contrário, como $x(p)$ e $x(\bar{p})$ são distintos, pois x é injetiva,

segue que existe vizinhança U de $x(p)$ que não contém $x(\bar{p})$, pois \mathbb{R}^d é acessível, logo $x^{-1}(p)$ é uma vizinhança de p que não contém \bar{p} . Analogamente, mostramos o mesmo para \bar{p} , portanto V eles são separados e concluímos que \mathbf{V} é um espaço topológico acessível.

2. (\Rightarrow) Como \mathcal{T} tem base enumerável, então toda cobertura de V tem subcobertura enumerável. Sendo assim, dada a cobertura por abertos das cartas de \mathcal{A} , tomamos uma subcobertura enumerável e segue que esse é um subatlas enumerável de \mathcal{A} .

(\Leftarrow) Seja $\bar{\mathcal{A}}$ um subatlas enumerável de \mathcal{A} . Para cada $(A, x) \in \bar{\mathcal{A}}$, consideramos as bolas $\odot_r(x) \subseteq x(A) \subseteq \mathbb{R}^d$ tais que $r \in \mathbb{Q}$ e $x \in \mathbb{Q}^d$. A união das imagens inversas dessas bolas pelos mapas de coordenadas é o conjunto enumerável

$$\bar{\mathcal{B}} = \bigcup_{(A,x) \in \bar{\mathcal{A}}} \left\{ x^{-1}(\odot_r(x)) \mid \odot_r(x) \subseteq x(A), r \in \mathbb{Q}, x \in \mathbb{Q}^d \right\}.$$

Esse conjunto é uma base de \mathbf{V} : (1) O conjunto $\bar{\mathcal{B}}$ cobre V , pois os domínios das cartas de $\bar{\mathcal{A}}$ cobrem V e as imagens inversas das bolas de centro e raio racionais cobrem o domínio de cada carta de $\bar{\mathcal{A}}$; (2) Sejam A_1 e $A_2 \in \bar{\mathcal{B}}$. Então $A_1 \cap A_2$ é aberto e, para todo $p \in A_1 \cap A_2$, existem $r \in \mathbb{Q}$ e $x \in \mathbb{Q}^d$ tais que $x_1(p) \in \odot_r(x) \subseteq x_1(A_1 \cap A_2)$, logo $p \in x_1^{-1}(\odot_r(x)) \subseteq A_1 \cap A_2$.

3. Sejam $C(p)$ uma componente conexa de \mathbf{V} em p e U o conjunto de todos pontos de $C(p)$ ligados por um caminho a p . Mostraremos que U é aberto e fechado, portanto igual a $C(p)$. Mostremos primeiro que U é aberto. Seja $q \in C(p)$ e A uma vizinhança de q homeomorfa a uma bola de \mathbb{R}^d . Como a bola é conexa por caminhos e homeomorfa a A , segue que A é conexa por caminhos. Portanto todo ponto de A está em $C(p)$, já que existe caminho do um ponto de A a q e caminho de q a p . Isso mostra que U é aberto. Agora, seja $q \in U^c$. Novamente, tomamos uma vizinhança A de q homeomorfa a uma bola de \mathbb{R}^d e segue que A é conexa por caminhos. Nesse caso, nenhum ponto de A está em $C(p)$, caso contrário existiria caminho ligando q a p , o que contradiz a hipótese. Isso mostra que U^c é fechado, portanto U aberto. Assim, como U é aberto e fechado, $C(p)$ é conexo e $p \in U$, segue que $C(p) = U$.

■

20.3 Funções Diferenciáveis e Espaço Tangente

20.3.1 Funções Diferenciáveis

Definição 20.15. Sejam \mathbf{V}_0 e \mathbf{V}_1 \mathcal{C}^k -variedades de dimensões d_0 e d_1 , respectivamente. Uma função \mathcal{C}^k -diferenciável de \mathbf{V}_0 para \mathbf{V}_1 é uma função $F: V_0 \rightarrow V_1$ que satisfaz: para todo $p \in V_0$, existem cartas $(A_0, x_0) \in \mathcal{A}_0$ em p e $(A_1, x_1) \in \mathcal{A}_1$ em $F(p)$ tais que $F(A_0) \subseteq A_1$ e

$$x_1 \circ F \circ x_0^{-1}: x_0(A_0) \rightarrow x_1(A_1)$$

é uma função \mathcal{C}^k -diferenciável de $x_0(A_0) \subseteq \mathbb{R}^{d_0}$ para $x_1(A_1) \subseteq \mathbb{R}^{d_1}$.

Denota-se $F: \mathbf{V}_0 \rightarrow \mathbf{V}_1$. O conjunto de todas essas funções é denotado $\mathcal{C}^k(\mathbf{V}_0, \mathbf{V}_1)$. Quando $V_1 = \mathbb{R}$, denota-se simplesmente $\mathcal{C}^k(\mathbf{V}_0)$.

A diferenciabilidade independe da carta escolhida no seguinte sentido.

Demonstração. Sejam $(A_0, x_0), (\bar{A}_0, \bar{x}_0)$ cartas em p e $(A_1, x_1), (\bar{A}_1, \bar{x}_1)$ cartas em $f(p)$ tais que $F(A_0) \subseteq A_1$ e $F(\bar{A}_0) \subseteq \bar{A}_1$. Então $F(A_0 \cap \bar{A}_0) \subseteq A_1 \cap \bar{A}_1$, $p \in A_0 \cap \bar{A}_0$ e $F(p) \in A_1 \cap \bar{A}_1$. Restringindo domínios adequadamente,

$$\bar{x}_1 \circ F \circ \bar{x}_0^{-1} = (\bar{x}_1 \circ x_1^{-1}) \circ (x_1 \circ F \circ x_0^{-1}) \circ (x_0 \circ \bar{x}_0^{-1})$$

Como as transições de coordenadas $(\bar{x}_1 \circ x_1^{-1})$ e $(x_0 \circ \bar{x}_0^{-1})$ são \mathcal{C}^k -difeomorfismos, então $(x_1 \circ F \circ x_0^{-1})$ é \mathcal{C}^k -diferenciável se, e somente se, $(\bar{x}_1 \circ F \circ \bar{x}_0^{-1})$ o é. ■

Como uma \mathcal{C}^k -variedade é também uma \mathcal{C}^l -variedade para todo $l \leq k$, sempre se pode definir entre \mathcal{C}^k e \mathcal{C}^l -variedade funções \mathcal{C}^m -diferenciáveis para qualquer $m \leq \min\{k, l\}$.

Proposição 20.6. Sejam \mathbf{V}_0 e \mathbf{V}_1 \mathcal{C}^k -variedades e $F_0: \mathbf{V}_0 \rightarrow \mathbf{V}_1$ uma função \mathcal{C}^k -diferenciável. Então F é uma função contínua.

Proposição 20.7. Sejam \mathbf{V}_0 , \mathbf{V}_1 e \mathbf{V}_2 \mathcal{C}^k -variedades e $F_0: \mathbf{V}_0 \rightarrow \mathbf{V}_1$ e $F_1: \mathbf{V}_1 \rightarrow \mathbf{V}_2$ funções \mathcal{C}^k -diferenciáveis. Então $F_1 \circ F_0: \mathbf{V}_0 \rightarrow \mathbf{V}_2$ é uma função \mathcal{C}^k -diferenciável.

Casos particulares relevantes são quando uma das duas variedades é um subconjunto de \mathbb{R}^d . Toma-se assim a carta trivial nesse subconjunto. Um desses casos é evidenciado a seguir.

Definição 20.16. Sejam \mathbf{V} uma \mathcal{C}^k -variedade e $I \subseteq \mathbb{R}$ um intervalo aberto. Uma \mathcal{C}^k -curva em \mathbf{V} é uma função $\gamma: I \rightarrow \mathbf{V}$ \mathcal{C}^k -diferenciável.

Isso é equivalente a dizer que, para todo $p \in \gamma(V)$ existe carta (A, x) em p tal que

$$x \circ \gamma: I \rightarrow x(A)$$

é uma função \mathcal{C}^k -diferenciável, ao escolher acima a função identidade.

20.3.2 Espaço Tangente e a Diferencial

A partir desta seção, não estudaremos mais com detalhes os casos de variedades \mathcal{C}^k -diferenciais para cada $k \in \mathbb{N} \cup \{\infty\}$. Nos referiremos somente a *variedades* ou *variedades diferenciais*, sendo que o primeiro termo se refere a qualquer variedade topológica e o segundo a variedades suaves, isto é, \mathcal{C}^∞ -diferenciais, e a mesma nomenclatura será usada para funções diferenciáveis.

Álgebra dos Campos Escalares

Dada uma variedade diferencial \mathbf{V} , um *campos escalares* em \mathbf{V} são funções do espaço $\mathcal{C}^\infty(V, \mathbb{R})$ das funções diferenciáveis de V para \mathbb{R} . Esse espaço será denotado $\mathfrak{T}^0(V)$ ¹. O espaço $\mathfrak{T}^0(V)$ é um espaço vetorial sobre \mathbb{R} com as operações de soma e produto por escalar induzidas pontualmente de \mathbb{R} : a soma dada por

$$\begin{aligned} +: \mathfrak{T}^0(V) \times \mathfrak{T}^0(V) &\longrightarrow \mathfrak{T}^0(V) \\ (f, f') &\longmapsto f + f': V \longrightarrow \mathbb{R} \\ p &\longmapsto f(p) + f'(p) \end{aligned}$$

e o produto por escalar é dado por

$$\begin{aligned} \cdot: \mathbb{R} \times \mathfrak{T}^0(V) &\longrightarrow \mathfrak{T}^0(V) \\ (c, f) &\longmapsto cf: V \longrightarrow \mathbb{R} \\ p &\longmapsto cf(p). \end{aligned}$$

Ainda, pode-se definir um produto em $\mathfrak{T}^0(V)$ também induzido pontualmente de \mathbb{R} , dado por

$$\begin{aligned} \times: \mathfrak{T}^0(V) \times \mathfrak{T}^0(V) &\longrightarrow \mathfrak{T}^0(V) \\ (f, f') &\longmapsto ff': V \longrightarrow \mathbb{R} \\ p &\longmapsto f(p)f'(p). \end{aligned}$$

Esse produto é bilinear com respeito à estrutura linear de $\mathfrak{T}^0(V)$ e, portanto, faz desse espaço uma álgebra associativa e comutativa. Essa álgebra é a *álgebra de campos escalares* em \mathbf{V} . É simples ver que essas operações geram funções diferenciáveis de $\mathfrak{T}^0(V)$.

Proposição 20.8. *Seja \mathbf{V} uma variedade diferencial.*

¹Usualmente denota-se esse espaço por $\mathcal{C}^\infty(V)$, mas adotaremos essa notação por motivos que ficarão mais claros na seção de campos tensoriais mais à frente; em resumo, campos escalares são campos tensoriais de tipo $(0, 0)$

1. $(\mathfrak{T}^0(V), +, -, 0, \times, 1)$ é um anel, em que as operações são as operações pontuais induzidas de \mathbb{R} .
2. $(\mathfrak{T}^0(V), +, -, 0, \times, 1, \cdot)$ é uma álgebra associativa, comutativa e com unidade sobre \mathbb{R} , em que as operações são as operações pontuais induzidas de \mathbb{R} .

Derivações em Pontos

Definição 20.17. Sejam V uma variedade diferencial e $p \in V$. Uma *derivação* em p é um funcional linear $D: \mathfrak{T}^0(V) \rightarrow \mathbb{R}$ que satisfaz, para todas $f, f' \in \mathfrak{T}^0(V)$,

$$D(f f') = D(f)f'(p) + f(p)D(f').$$

O *espaço tangente* a V em p é o conjunto $TV|_p$ de todas derivações em p e os *vetores tangentes* a V em p são os elementos de $TV|_p$.

O espaço tangente $TV|_p$ é um espaço vetorial. Para mostrar isso, devemos mostrar que ele é um subespaço vetorial do espaço dos funcionais lineares $\mathcal{L}(\mathfrak{T}^0(V), \mathbb{R})$.

Proposição 20.9. *Sejam V uma variedade diferencial e $p \in V$. O espaço tangente a V em p é um subespaço vetorial de $\mathcal{L}(\mathfrak{T}^0(V), \mathbb{R})$.*

Demonstração. Para isso, primeiro notamos que claramente $TV|_p$ não é vazio, pois o funcional nulo que leva toda função diferenciável em $0 \in \mathbb{R}$ é uma derivação em p . Agora, para todos $v, v' \in TV|_p$ e $c \in \mathbb{R}$, e todos $f, f' \in \mathfrak{T}^0(V)$,

$$\begin{aligned} (v + v')(f f') &= v(f f') + v'(f f') \\ &= v(f)f'(p) + f(p)v(f') + v'(f)f'(p) + f(p)v'(f') \\ &= (v(f) + v'(f))f'(p) + f(p)(v(f') + v'(f')) \\ &= (v + v')(f)f'(p) + f(p)(v + v')(f') \end{aligned}$$

e

$$\begin{aligned} (cv)(f f') &= c(v(f f')) \\ &= c(v(f)f'(p) + f(p)v(f')) \\ &= cv(f)f'(p) + cf(p)v(f') \\ &= (cv)(f)f'(p) + f(p)(cv)(f'), \end{aligned}$$

o que mostra que $v + v'$ e cv são derivações em p . ■

Assim temos um espaço vetorial $TV|_p$ associado a cada ponto p da variedade. As seguintes propriedades serão utilizadas na demonstração de algumas proposições mais à frente.

Proposição 20.10. Sejam \mathbf{V} uma variedade diferencial, $p \in V$ e $v \in TV|_p$.

1. Para toda função constante $f \in \mathfrak{T}^0(V)$,

$$v(f) = 0.$$

2. Para todas funções $f, f' \in \mathfrak{T}^0(V)$ tais que $f(p) = f'(p) = 0$,

$$v(ff') = 0.$$

Demonstração. 1. Se f é constante, existe $c \in \mathbb{R}$ $f(p) = c$ para todo $p \in V$, portanto $f = c1_V$, em que 1_V é a função constante igual a 1. Notemos que

$$v(1_V) = v((1_V)^2) = v(1_V)1_V(p) + 1_V(p)v(1_V) = 2v(1_V),$$

o que implica $v(1_V) = 0$, portanto $v(f) = cv(1_V) = 0$.

2. Basta ver que

$$v(ff') = v(f)f'(p) + f(p)v(f') = 0. \quad \blacksquare$$

A Diferencial de uma Função Diferenciável

Definição 20.18. Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais, $F: V \rightarrow V'$ uma função diferenciável e $p \in V$. A *diferencial* de F em p é a função

$$\begin{aligned} DF|_p: TV|_p &\longrightarrow TV'|_{F(p)} \\ v &\longmapsto DF|_p v: \mathfrak{T}^0(V') \longrightarrow \mathbb{R} \\ f &\longmapsto v(f \circ F). \end{aligned}$$

Pode-se denotar DF_p por simplicidade.

A diferencial $DF|_p$ aplicada em um vetor tangente v é uma derivação em $F(p)$ de $\mathfrak{T}^0(V')$. Para mostrar isso, sejam $f, f' \in \mathfrak{T}^0(V')$ e $c \in \mathbb{R}$. Como v é linear,

$$\begin{aligned} (DF|_p v)(f + f') &= v((f + f') \circ F) \\ &= v((f \circ F) + (f' \circ F)) \\ &= v(f \circ F) + v(f' \circ F) \\ &= (DF|_p v)(f) + (DF|_p v)(f') \end{aligned}$$

e

$$\begin{aligned} (DF|_p v)(cf) &= v((cf) \circ F) \\ &= v(c(f \circ F)) \\ &= cv(f \circ F) \\ &= c(DF|_p v)(f), \end{aligned}$$

o que mostra que $DF|_p v$ é linear; como v é derivação em p ,

$$\begin{aligned}(DF|_p v)(ff') &= v((ff') \circ F) \\&= v((f \circ F)(f' \circ F)) \\&= v(f \circ F)(f' \circ F)(p) + (f \circ F)(p)v(f' \circ F) \\&= v((f \circ F))f'(F(p)) + f(F(p))v(f' \circ F) \\&= (DF|_p v)(f)f'(F(p)) + f(F(p))(DF|_p v)(f')\end{aligned}$$

o que mostra que $DF|_p v$ é derivação em $F(p)$.

Proposição 20.11. *Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais e $F: V \rightarrow V'$ uma função diferenciável e $p \in V$. A diferencial $DF|_p: TV|_p \rightarrow TV'|_{F(p)}$ é uma função linear.*

Demonstração. Sejam $v, v' \in TV|_p$ e $c \in \mathbb{R}$. Então, para todo $f \in \mathfrak{T}^0(V)$,

$$\begin{aligned}(DF|_p(v + v'))(f) &= (v + v')(f \circ F) \\&= v(f \circ F) + v'(f \circ F) \\&= (DF|_p v)(f) + (DF|_p v')(f)\end{aligned}$$

e

$$\begin{aligned}(DF|_p(cv))(f) &= (cv)(f \circ F) \\&= c(v(f \circ F)) \\&= (cDF|_p v)(f),\end{aligned}$$

o que mostra que $DF|_p(v + v') = DF|_p v + DF|_p v'$ e $DF|_p(cv) = cDF|_p v$. ■

Proposição 20.12 (Regra da Cadeia). *Sejam \mathbf{V} , \mathbf{V}' e \mathbf{V}'' variedades diferenciais, $F: V \rightarrow V'$ e $F': V' \rightarrow V''$ funções diferenciáveis, $e p \in V$. Então*

$$D(F' \circ F)|_p = DF'|_{F(p)} \circ DF|_p.$$

Demonstração. Para todos $v \in TV|_p$ e $f \in \mathfrak{T}^0(V'')$,

$$\begin{aligned}(D(F' \circ F)|_p v)(f) &= v(f \circ (F' \circ F)) \\&= v((f \circ F') \circ F)) \\&= (DF|_p v)(f \circ F') \\&= ((DF'|_{F(p)})(DF|_p v))(f) \\&= ((DF'|_{F(p)} \circ DF|_p v))(f),\end{aligned}$$

portanto $D(F' \circ F)|_p v = (DF'|_{F(p)} \circ DF|_p v)$ para todo $v \in TV|_p$, o que implica

$$D(F' \circ F)|_p = DF'|_{F(p)} \circ DF|_p. ■$$

Vetores Tangentes e Espaços Tangentes a \mathbb{R}^d

Os vetores dos espaços tangentes a \mathbb{R}^d podem ser descritos como derivações. Seja $f \in \mathfrak{T}^0(\mathbb{R}^d)$ uma função escalar e consideremos sua diferencial $Df|_p: \mathbb{R}^d \rightarrow \mathbb{R}$. Essa diferencial pode ser aplicada no vetor canônico $e_i \in \mathbb{R}^d$, definindo

$$\partial_i|_p f := Df|_p e_i.$$

A função $\partial_i|_p: \mathfrak{T}^0(\mathbb{R}^d) \rightarrow \mathbb{R}$ assim definida é uma derivação em p . Ela é linear porque, para todas $f, f' \in \mathfrak{T}^0(\mathbb{R}^d)$ e $c \in \mathbb{R}$, segue da linearidade de D que

$$\begin{aligned}\partial_i|_p(cf + f') &= D(cf + f')|_p e_i = (cDf|_p + Df'|_p)e_i \\ &= cDf|_p e_i + Df'|_p e_i \\ &= c\partial_i|_p(f) + \partial_i|_p(f'),\end{aligned}$$

e é uma derivação em p porque, para todas $f, f' \in \mathfrak{T}^0(\mathbb{R}^d)$, segue da regra do produto de D que

$$\begin{aligned}\partial_i|_p(f f') &= D(f f')|_p e_i \\ &= (Df|_p f'(p) + f(p)Df'|_p)e_i \\ &= Df|_p f'(p)e_i + f(p)Df'|_p e_i \\ &= \partial_i|_p(f)f'(p) + f(p)\partial_i|_p(f').\end{aligned}$$

A derivação direcional de f an direção de $v = \sum_{i \in [d]} c^i e_i$ é

$$D_v|_p f := Df|_p v.$$

Note que, para todo $f \in \mathfrak{T}^0(\mathbb{R}^d)$,

$$D_v|_p(f) = Df|_p v = Df|_p \left(\sum_{i \in [d]} v^i e_i \right) = \sum_{i \in [d]} v^i Df|_p e_i = \sum_{i \in [d]} v^i \partial_i|_p(f),$$

logo $D_v|_p = \sum_{i \in [d]} v^i \partial_i|_p$. Mostraremos que essa função é um isomorfismo de espaço lineares.

Proposição 20.13. *Seja $d \in \mathbb{N}$. Para todo $p \in \mathbb{R}^d$, a função*

$$\begin{aligned}D.|_p: \mathbb{R}^d &\longrightarrow T\mathbb{R}^d|_p \\ v &\longmapsto D_v|_p\end{aligned}$$

é um isomorfismo de espaços lineares.

Demonstração. Seja $v = +_{i \in [d]} v^i e_i$ e, portanto, $D_v|_p = +_{i \in [d]} v^i \partial_i|_p$. Primeiro mostramos que essa função é linear. Sejam $v, v' \in \mathbb{R}^d$ e $c \in \mathbb{R}$. Então, para toda $f \in \mathfrak{T}^0(\mathbb{R}^d)$, segue da linearidade de $Df|_p$ que

$$\begin{aligned} D_{cv+v'}|_p f &= Df|_p(cv + v') \\ &= cDf|_p v + Df|_p v' \\ &= cD_v|_p f + D_{v'}|_p f \\ &= (cD_v + D_{v'})f. \end{aligned}$$

Agora, mostremos que ela é injetiva. Seja $v \in \mathbb{R}^d$ tal que $D_v|_p = 0$. Então, para cada $i \in [d]$, como $D\pi^i|_p = \pi^i$,

$$0 = D_v|_p \pi^i = D\pi^i|_p v = \pi^i(v) = v^i,$$

logo $v = 0$. Agora, mostremos que ela é sobrejetiva. Seja $D \in T\mathbb{R}^d|_p$. Para cada $i \in [d]$, definimos $v^i := D(\pi^i)$ e $v := +_{i \in [d]} v^i e_i$. Mostraremos que $D = D_v|_p$. Seja $f \in \mathfrak{T}^0(\mathbb{R}^d)$. Pela fórmula de Taylor, existem constantes $C_{i,j} \in \mathbb{R}$ tais que

$$f = f(p) + \sum_{i \in [d]} \partial_i f(p)(\pi^i - p^i) + \sum_{(i,j) \in [d]^2} C_{i,j}(\pi^i - p^i)(\pi^j - p^j).$$

Como $f(p)$ é constante, $D(f(p)) = 0$ (20.10), e, como as funções $(\pi^i - p^i)$ e $(\pi^j - p^j)$ se anulam em p , $D((\pi^i - p^i)(\pi^j - p^j)) = 0$ para todos $i, j \in [d]$ (20.10), logo

$$D \left(\sum_{(i,j) \in [d]^2} C_{i,j}(\pi^i - p^i)(\pi^j - p^j) \right) = \sum_{(i,j) \in [d]^2} C_{i,j} D((\pi^i - p^i)(\pi^j - p^j)) = 0,$$

o que implica que

$$\begin{aligned} D(f) &= D \left(\sum_{i \in [d]} \partial_i f(p)(\pi^i - p^i) \right) \\ &= \sum_{i \in [d]} D(\partial_i f(p)(\pi^i - p^i)) \\ &= \sum_{i \in [d]} (\partial_i f(p) D(\pi^i - p^i)) \\ &= \sum_{i \in [d]} \partial_i f(p) (D(\pi^i) - D(p^i)) \\ &= \sum_{i \in [d]} \partial_i f(p) v^i \\ &= D_v|_p f. \end{aligned}$$

■

Essa proposição mostra que $(\partial_i|_p)_{i \in [d]}$ é uma base ordenada do espaço tangente $T\mathbb{R}^d|_p$, o qual é isomorfo a \mathbb{R}^d e deve ser visto como o espaço dos vetores tangentes a \mathbb{R}^d em p .

20.3.3 Fibrado Tangente

Definição 20.19. Seja V um variedade diferencial. O *fibrado tangente* de V é

$$TV := \bigsqcup_{p \in V} TV|_p = \{(p, v) \mid p \in V, v \in TV|_p\},$$

a união disjunta dos espaços tangentes a V em todos pontos de V .

Referencial Local Coordenado

Dada uma carta (A, x) de V , as funções $\left(\frac{\partial}{\partial x^i}\Big|_p\right)_{i \in [d]}$, definidas por

$$\begin{aligned} \frac{\partial}{\partial x^i}\Big|_p : \mathfrak{T}^0(V) &\longrightarrow \mathbb{R} \\ f &\longmapsto \partial_i(f \circ x^{-1})|_{x(p)} \end{aligned}$$

são uma base ordenada de $TV|_p$. Essas funções são lineares porque, para todas $f, f' \in \mathfrak{T}^0(V)$ e $c \in \mathbb{R}$,

$$\begin{aligned} \frac{\partial}{\partial x^i}\Big|_p (cf + f') &= \partial_i((cf + f') \circ x^{-1})|_{x(p)} \\ &= \partial_i((cf \circ x^{-1}) + (f' \circ x^{-1}))|_{x(p)} \\ &= c\partial_i(f \circ x^{-1})|_{x(p)} + \partial_i(f' \circ x^{-1})|_{x(p)} \\ &= c \frac{\partial}{\partial x^i}\Big|_p f + \frac{\partial}{\partial x^i}\Big|_p f', \end{aligned}$$

e são derivações porque, para todas $f, f' \in \mathfrak{T}^0(V)$,

$$\begin{aligned} \frac{\partial}{\partial x^i}\Big|_p (ff') &= \partial_i((ff') \circ x^{-1})|_{x(p)} \\ &= \partial_i((f \circ x^{-1})(f' \circ x^{-1}))|_{x(p)} \\ &= (f \circ x^{-1})|_{x(p)}(\partial_i(f' \circ x^{-1})|_{x(p)} \\ &\quad + (f' \circ x^{-1})|_{x(p)}(\partial_i(f \circ x^{-1})|_{x(p)} \\ &= f(p) \frac{\partial}{\partial x^i}\Big|_p f + f'(p) \frac{\partial}{\partial x^i}\Big|_p f'. \end{aligned}$$

Vale lembrar que $\partial_i f(p)$ é a derivada direcional da função f na direção de e_i no ponto p (também identificada com a derivada parcial $D_i f(p)$) e

$$\partial_i f(p) = Df(p) \cdot e_i.$$

A motivação da notação $\frac{\partial}{\partial x^i}$, além do uso histórico, vem da ideia de que vale a regra da cadeia

$$\partial_i(f \circ x^{-1})|_{x(p)} = \partial_i f|_{x^{-1}(x(p))} \circ \partial_i(x^{-1})|_{x(p)} = \partial_i f|_p \circ (\partial_i x|_p)^{-1} = \left. \frac{\partial_i f}{\partial_i x} \right|_p.$$

A função

$$\begin{aligned} \frac{\partial}{\partial x^i} : A &\longrightarrow TV|_A \\ p &\longmapsto \left. \frac{\partial}{\partial x^i} \right|_p \end{aligned}$$

é um campo vetorial em A — uma seção de $TV|_A$ — e $\frac{\partial}{\partial x} = \left(\frac{\partial}{\partial x^i} \right)_{i \in [d]}$ é um referencial local de A .

20.3.4 Espaço Cotangente

Dada uma variedade diferencial \mathbf{V} e seu espaço

Definição 20.20. Sejam \mathbf{V} uma variedade diferencial e $p \in V$. O *espaço cotangente* a \mathbf{V} em p é

$$T^*V|_p := (TV|_p)^*,$$

o espaço linear dual do espaço tangente a \mathbf{V} em p . O *fibrado cotangente* de \mathbf{V} é

$$T^*V := \bigsqcup_{p \in V} T^*V|_p,$$

a união disjunta dos espaços tangentes a \mathbf{V} em todos os pontos de V .

Referencial Local Coordenado

Dada uma carta (A, x) de V , as funções $(dx^i|_p)_{i \in [d]}$, definidas por

$$\begin{aligned} dx^i|_p : TV|_p &\longrightarrow \mathbb{R} \\ v &\longmapsto v(x^i) \end{aligned}$$

são uma base ordenada de $T^*V|_p$. Essas funções são lineares porque, para todos $v, v' \in TV|_p$ e $c \in \mathbb{R}$,

$$\begin{aligned}\mathrm{d}x^i|_p(cv + v') &= (cv + v')(x^i) \\ &= cv(x^i) + v'(x^i) \\ &= c\mathrm{d}x^i|_p(v) + \mathrm{d}x^i|_p(v').\end{aligned}$$

A base $(\mathrm{d}x^i|_p)_{i \in [d]}$ de $T^*V|_p$ é a base dual de $\left(\frac{\partial}{\partial x^i}|_p\right)_{i \in [d]}$, pois

$$\mathrm{d}x^i|_p \left(\frac{\partial}{\partial x^j} \Big|_p \right) = \frac{\partial}{\partial x^j} \Big|_p x^i = \partial_j(x^i \circ x^{-1})|_{x(p)} = \partial_j(\pi^i)|_{x(p)} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

20.3.5 Curvas Equivelozes e Espaço Tangente

Definição 20.21. Sejam V uma variedade diferencial e $p \in V$. Duas curvas $\gamma_0 : I_0 \rightarrow V$ e $\gamma_1 : I_1 \rightarrow V$ iniciadas em p ($\gamma(0) = p$) são *equivelozes* se, e somente se, existe uma carta (A, x) em p tal que

$$(x \circ \gamma_0)'(0) = (x \circ \gamma_1)'(0).$$

Denota-se $\gamma_0 \asymp \gamma_1$.

A relação está bem definida, no sentido de que não depende da escolha de carta, e é uma relação de equivalência.

Demonstração. Sejam (A, x) , (\bar{A}, \bar{x}) cartas em p . Então, para $i = 0$ e $i = 1$,

$$\bar{x} \circ \gamma_i = (\bar{x} \circ x^{-1}) \circ (x \circ \gamma_i)$$

e, diferenciando essas funções em 0, obtemos pela regra da cadeia que

$$\begin{aligned}(\bar{x} \circ \gamma_i)'(0) &= D((\bar{x} \circ x^{-1}) \circ (x \circ \gamma_i))(0) \\ &= D(\bar{x} \circ x^{-1})(x \circ \gamma_i(0)) \circ (x \circ \gamma_i)'(0) \\ &= D(\bar{x} \circ x^{-1})(x(p)) \circ (x \circ \gamma_i)'(0).\end{aligned}$$

Como $\bar{x} \circ x^{-1}$ é difeomorfismo, $D(\bar{x} \circ x^{-1})(x(p))$ é invertível, portanto

$$(x \circ \gamma_0)'(0) = (x \circ \gamma_1)'(0)$$

se, e somente se,

$$(\bar{x} \circ \gamma_0)'(0) = (\bar{x} \circ \gamma_1)'(0).$$

■

Definição 20.22. Sejam \mathbf{V} uma variedade diferencial, $p \in V$ e $\gamma : I \rightarrow V$ uma curva iniciada em p . O *vetor tangente a \mathbf{V} em p* , denotado $\gamma'(0)$, é a classe de equivalência de γ sob a relação \asymp de equivelocidade de curvas.

O *espaço tangente* a \mathbf{V} em p é o conjunto de vetores tangentes a \mathbf{V} em p , denotado

$$TV|_p := \{\gamma'(0) \mid \gamma : I \rightarrow V, \gamma(0) = p\},$$

em que os I são intervalos abertos de \mathbb{R} contendo o 0.

O *fibrado tangente* de \mathbf{V} é a união disjunta dos espaços tangentes a \mathbf{V} em todos pontos de V

$$TV := \bigsqcup_{p \in V} TV|_p = \{(p, v) \mid p \in V, v \in TV|_p\}.$$

Os elementos do espaço tangente a \mathbf{V} em um ponto $p \in V$ são chamados de vetores porque $T_p \mathbf{V}$ é um espaço vetorial se definidas operações apropriadas. Isso que fazemos a seguir.

Para isso, vamos mostrar que $Df(p) : T_p V \rightarrow \mathbb{R}^n$ é uma bijeção. Assim poderemos puxar as operações de espaço vetorial de \mathbb{R}^n para $T_p V$.

Definição 20.23. Sejam \mathbf{V} e $\bar{\mathbf{V}}$ variedades, $p \in V$ e $f : V \rightarrow \bar{V}$ uma função diferenciável em p . A *diferencial* de f em p é a função

$$\begin{aligned} Df(p) : T_p V &\longrightarrow T_{f(p)} \bar{V} \\ \gamma'(0) &\longmapsto (f \circ \gamma)'(0). \end{aligned}$$

Devemos mostrar que essa função está bem definida.

Tomando uma carta (A, x) em p , definimos a função

$$\begin{aligned} Dx(p) : T_p \mathbf{V} &\longrightarrow \mathbb{R}^d \\ \gamma'(0) &\longmapsto (x \circ \gamma)'(0) \end{aligned}$$

de modo que a regra da composição é simulada. Essa função é uma bijeção e é usada para puxar as operações de \mathbb{R}^d para $T_p \mathbf{V}$, de modo que $T_p \mathbf{V}$ é um espaço vetorial. Essas operações puxadas não dependem da carta (A, x) escolhida.

20.4 Funções Separadoras e Partições da Unidade

Consideraremos inicialmente a função

$$f: \mathbb{R} \longrightarrow \mathbb{R}$$

$$x \longmapsto \begin{cases} 0, & x \leq 0 \\ e^{-\frac{1}{x}}, & x > 0. \end{cases}$$

Pode ser mostrado que essa função é suave, mas não faremos isso aqui. Sejam $r_0, r_1 \in \mathbb{R}$ tais que $r_0 < r_1$. Construímos a função

$$h: \mathbb{R} \longrightarrow \mathbb{R}$$

$$x \longmapsto \frac{f(r_1 - x)}{f(x - r_0) - f(r_1 - x)}.$$

Essa função é suave e tem a seguinte propriedade: $h(x) = 1$ para todo $x \leq r_0$, $0 < h(x) < 1$ para todo $x \in]r_0, r_1[$ e $h(x) = 0$ para todo $x \geq r_1$. Isso quer dizer que ela é uma função suave que separa (precisamente) os conjuntos $]-\infty, r_0]$ e $[r_1, +\infty[$. Em \mathbb{R}^d , podemos separar (precisamente) por função suave a bola fechada $\bigodot_{r_0}(0)$ e o complementar da bola fechada $\bigodot_{r_1}(0)$. Basta usar a função h para definir a função

$$H: \mathbb{R}^d \longrightarrow \mathbb{R}$$

$$x \longmapsto h(\|x\|).$$

Uma função suave que separa esses conjuntos é geralmente chamada de uma “bump function”, mas aqui a chamaremos de função separadora, pois ela separa (precisamente) os conjuntos. Em francês, essa função também é conhecida como uma “fonction plateau”, algo como “função planalto”. Essas funções são também chamadas de “funções teste”. Mais geralmente, uma função como essa é uma função para $[0, 1]$ com suporte em um aberto A que vale 1 em um compacto K , ou seja, uma função contínua que separa um fechado A^c e um compacto K . Essa funções sempre existem em espaços topológicos separados por vizinhanças (T_2) e localmente compactos.

Definição 20.24. Sejam X um espaço topológico e $f : X \longrightarrow \mathbb{R}$ uma função contínua. O *suporte fechado* de f é o conjunto

$$\overline{\text{supp}}(f) := \overline{\text{supp}(f)}.$$

Proposição 20.14. Sejam \mathbf{X} um espaço topológico separado por vizinhanças (T_2) e localmente compacto, $A \subseteq X$ um aberto e $K \subseteq A$ um compacto. Existe função $f : X \rightarrow [0, 1]$ tal que $\overline{\text{supp}}(f) \subseteq A$ e $f(K) = \{1\}$.

Notemos que tal função separa continuamente A^c e K , pois

$$\text{supp}(f) \subseteq \overline{\text{supp}}(f) \subseteq A$$

implica $A^c \subseteq \text{supp}(f)^c$, portanto $f(A^c) \subseteq f(\text{supp}(f)^c) = \{0\}$.

Definição 20.25. Sejam \mathbf{X} um espaço topológico (variedade suave) e $\mathcal{C} = (C_i)_{i \in I}$ uma cobertura aberta de \mathbf{X} . Uma *partição da unidade (suave)* subordinada a \mathcal{C} é uma família de funções contínuas (suaves) $\psi_i : X \rightarrow \mathbb{R}$ tal que

1. (Unidade) Para todos $i \in I$ e $x \in X$, $0 \leq \psi_i(x) \leq 1$;
2. (Partição) A família $(\overline{\text{supp}}(\psi_i))_{i \in I}$ é localmente finita (todo ponto tem uma vizinhança que intersecciona finitos dos conjuntos da família) e, para todo $x \in X$,

$$\sum_{i \in I} \psi_i(x) = 1.$$

3. (Subordinação) Para todo $i \in I$, $\overline{\text{supp}}(\psi_i) \subseteq C_i$.

Proposição 20.15. Sejam \mathbf{V} uma variedade (suave) e $\mathcal{C} = (C_i)_{i \in I}$ uma cobertura aberta de \mathbf{V} . Existe partição da unidade (suave) $\psi_i : X \rightarrow \mathbb{R}$ subordinada a \mathcal{C} .

20.5 Orientação

20.5.1 Orientação de Espaços Lineares

Denotaremos como $\mathcal{B}(L)$ o conjunto de bases ordenadas de \mathbf{L} , ou seja,

$$\mathcal{B}(L) := \left\{ b \in L^d \mid L = \langle b \rangle \right\}.$$

Definição 20.26. Seja \mathbf{L} um espaço linear finito sobre um corpo \mathbf{C} . Duas bases ordenadas $b, b' \in \mathcal{B}(L)$ são *coorientadas* se, e somente se,

$$\det[\text{Id}]_{b'}^b > 0,$$

em que $[\text{Id}]_{b'}^b$ é a mudança de base de b para b' .

Proposição 20.16. Seja \mathbf{L} um espaço linear finito sobre um corpo \mathbf{C} . A relação de coorientação de bases ordenadas em $\mathcal{B}(L)$ é uma relação de equivalência.

Demonstração. (Reflexividade) Seja b uma base ordenada de \mathbf{L} . Como $[\text{Id}]_b^b = \text{Id}$, segue que $\det[\text{Id}]_b^b = \det \text{Id} = 1 > 0$, portanto b é coorientada consigo mesma. (Simetria) Sejam b e b' bases ordenadas de \mathbf{L} tais que b e b' são coorientadas. Isso significa que $\det[\text{Id}]_{b'}^{b'} > 0$. Mas como $[\text{Id}]_b^{b'} = ([\text{Id}]_{b'}^{b'})^{-1}$, segue que

$$\det[\text{Id}]_b^{b'} = \det(([\text{Id}]_{b'}^{b'})^{-1}) = (\det[\text{Id}]_{b'}^{b'})^{-1} > 0,$$

portanto b' e b são coorientadas. (Transitividade) Sejam b , b' e b'' bases ordenadas de \mathbf{L} tais que b e b' são coorientadas e b' e b'' são coorientadas. Isso significa que $\det[\text{Id}]_b^b > 0$ e $\det[\text{Id}]_{b''}^{b''} > 0$. Como $[\text{Id}]_{b''}^{b''} = [\text{Id}]_{b'}^{b'} \circ [\text{Id}]_{b'}^{b''}$, segue que

$$\det[\text{Id}]_{b''}^{b''} = \det([\text{Id}]_{b'}^{b'} \circ [\text{Id}]_{b'}^{b''}) = \det[\text{Id}]_{b'}^{b'} \det[\text{Id}]_{b'}^{b''} > 0,$$

logo b e b'' são coorientadas. ■

Isso permite que se quociente o espaço de bases ordenadas de \mathbf{L} em classes de equivalências, e esse quociente é o conjunto de classes de bases coorientadas de \mathbf{L} , definido a seguir.

Definição 20.27. Sejam \mathbf{L} um espaço linear finito sobre um corpo \mathbf{C} e b uma base ordenada de \mathbf{L} . A *classe de orientação* gerada por b é o conjunto

$$[b] = \left\{ b' \in \mathcal{B}(L) \mid \det[\text{Id}]_{b'}^b > 0 \right\}.$$

O conjunto dessas classes de equivalência é denotado $[\mathcal{B}(L)]$. Uma *orientação* de \mathbf{L} é uma função injetiva

$$O: [\mathcal{B}(L)] \longrightarrow \{+1, -1\}$$

O conjunto de orientações de \mathbf{L} é denotado $\mathcal{O}(L)$.

Em geral, pode-se considerar que O está definida em $\mathcal{B}(L)$ por simplicidade de notação, pois teremos $O(b) \in \{+1, -1\}$ em vez de $O([b])\{+1, -1\}$.

A classe de orientações gerada por uma base ordenada b é o conjunto de todas as bases ordenadas de \mathbf{L} que são coorientadas com essa base, a classe de equivalência dessa base com respeito à relação de coorientação.

A pergunta a ser feita então é: quantas orientações tem um espaço linear? A resposta intuitiva para \mathbb{R}^1 , \mathbb{R}^2 e \mathbb{R}^3 é 2, e essa é de fato a resposta para qualquer espaço linear finito. Uma orientação determina qual é a orientação positiva e qual é a orientação negativa. Mostraremos a seguir que, no caso de $d \geq 1$, essa função é uma bijeção e, no caso de $d = 0$, é uma escolha de +1 ou -1 para a orientação do ponto, pois \emptyset é a única base de $\{0\}$.

Proposição 20.17. *Seja \mathbf{L} um espaço linear finito sobre um corpo \mathbf{C} . Então*

$$|\mathcal{O}(L)| = 2.$$

Demonstração. Separamos a demonstração em dois casos: $\dim(L) = 0$ e $\dim(L) > 0$. No primeiro caso, a única base de \mathbf{L} é \emptyset , o que implica que existem duas funções injetivas do conjunto de classes de orientação de bases para $\{+1, -1\}$: a função $O(\emptyset) = +1$ e a função $O(\emptyset) = -1$. Portanto $|\mathcal{O}(L)| = 2$.

No segundo caso, se $\dim(L) > 0$, denotemos $d = \dim(L)$ e seja $b = (b_0, \dots, b_{d-1})$ uma base ordenada de \mathbf{L} . Definimos a base $\bar{b} := (-b_0, \dots, b_{d-1})$. Mostraremos que as únicas classes de orientação de \mathbf{L} são $[b]$ e $[\bar{b}]$. Seja b' uma base de \mathbf{L} . Se $\det[\text{Id}]_{b'}^b > 0$, então $[b'] = [b]$; caso contrário, $\det[\text{Id}]_{b'}^b < 0$. Mas

$$\begin{aligned}\det[\text{Id}]_{b'}^b &= \det \begin{bmatrix} \vdots & & \vdots \\ [b_0]_{b'} & \cdots & [b_{d-1}]_{b'} \\ \vdots & & \vdots \end{bmatrix} \\ &= - \det \begin{bmatrix} \vdots & & \vdots \\ [-b_0]_{b'} & \cdots & [b_{d-1}]_{b'} \\ \vdots & & \vdots \end{bmatrix} \\ &= - \det[\text{Id}]_{b'}^{\bar{b}},\end{aligned}$$

portanto $\det[\text{Id}]_{b'}^{\bar{b}} > 0$, o que mostra que $b' \in [\bar{b}]$. Isso implica que só existem duas orientações de \mathbf{L} , pois da injetividade segue que $O([b]) = +1$ e $O([\bar{b}]) = -1$, ou $O([b]) = -1$ e $O([\bar{b}]) = +1$. Logo $|\mathcal{O}(L)| = 2$. \blacksquare

A orientação canônica em \mathbb{R}^d é a função O definida por $O([e_0, \dots, e_{d-1}]) = +1$ e $O([-e_0, \dots, e_{d-1}]) = -1$.

Aritmética de Orientações

Definimos a orientação de um isomorfismo linear $f: L \rightarrow L$ por

$$O(f) := \frac{\det f}{|\det f|}.$$

Essa é uma função $O: \mathcal{L}(L) \rightarrow \{+1, -1\}$. Assim, segue que, para todos isomorfismos $f, f' \in \mathcal{L}(L)$,

$$O(f' \circ f) = O(f')O(f),$$

pois $\det(f' \circ f) = \det(f') \det(f)$.

Definimos, para toda classe de equivalência $[b]$ de bases ordenadas de \mathbf{L} coorientadas e todo isomorfismo $f \in \mathcal{L}(L)$,

$$f[b_0, \dots, b_{d-1}] := [f(b_0), \dots, f(b_{d-1})].$$

Isso está bem definido. Assim, segue que, para toda base ordenada b de \mathbf{L} ,

$$O(f[b]) = O(f)O([b]).$$

Vale notar que ambas as funções orientação, tanto a de isomorfismo como a de bases, define uma função com valores em $\{0, 1\}$, através do isomorfismo de grupos de $\{+1, -1\}$ para $\{0, 1\}$ definido por $(-1)^0 = +1$ e $(-1)^1 = -1$.

20.5.2 Orientação de Variedades

Definição 20.28. Seja \mathbf{V} uma variedade diferencial. Uma *orientação* de \mathbf{V} é uma função

$$O: V \longrightarrow \bigcup_{p \in V} \mathcal{O}(TV|_p)$$

tal que

1. Para todo $p \in V$, $O|_p: [\mathcal{B}(TV|_p)] \longrightarrow \{+1, -1\}$ é uma orientação de $TV|_p$;
2. Para todo $\bar{p} \in V$, existe um referencial local diferenciável $(B_i)_{i \in [d]}$ de \mathbf{V} em uma vizinhança $A \subseteq V$ de \bar{p} tal que, para todos $p, p' \in A$,

$$O|_p([B_0|_p, \dots, B_{d-1}|_p]) = O|_{p'}([B_0|_{p'}, \dots, B_{d-1}|_{p'}]).$$

Uma variedade diferencial *orientável* é uma variedade diferencial que admite uma orientação O .

Atlas Orientados

Definição 20.29. Seja \mathbf{V} uma variedade diferencial. Duas cartas (A, x) , (A', x') de \mathbf{V} são *coorientadas* se, e somente se, para todo $p \in A \cap A'$,

$$\det(D(x' \circ x^{-1})|_p) > 0.$$

Caso contrário, elas são *contraorientadas*, e existe $p \in A \cap A'$ tal que

$$\det(D(x' \circ x^{-1})|_p) < 0.$$

O caso em que $\det(D(x' \circ x^{-1})|_p) = 0$ não ocorre, pois as cartas são diferencialmente compatíveis, o que implica que a transição de coordenadas é um difeomorfismo, logo $D(x' \circ x^{-1})(p): \mathbb{R}^d \longrightarrow \mathbb{R}^d$ é invertível.

Definição 20.30. Um atlas diferencial *orientado* é um atlas cujas cartas são coorientadas duas a duas. Atlas diferenciais orientados *consistentes* são atlas diferenciais orientados cuja união é um atlas orientado.

Pode-se verificar que a relação de coorientabilidade de atlases é uma relação de equivalência.

Proposição 20.18. *Seja V uma variedade diferencial orientável com n componentes conexas. Então*

$$|\mathcal{O}(V)| = 2^n.$$

20.6 Conjuntos Nulos

Comentaremos nesta seção sobre o conceito de conjuntos nulos. Esses conceitos precedem o conceito mais amplo de uma medida de conjuntos, e podem ser definidos em \mathbb{R}^d independentemente das medidas mais usuais, como a de Borel e a de Lebesgue.

Definição 20.31. Seja $d \in \mathbb{N}$. Um *cubo d-dimensional* é um produto de d intervalos de \mathbb{R} . O *volume d-dimensional* de um cubo d -dimensional C cujo interior é $C^\circ =]a_0, b_0[\times \cdots \times]a_{d-1}, b_{d-1}[$ é o número real

$$\text{vol}^d(C) := |b_0 - a_0| \cdots |b_{d-1} - a_{d-1}|.$$

Admitimos nessa definição que \emptyset é um intervalo aberto, portanto que é um cubo aberto, e temos que seu volume é 0.

Definição 20.32. Seja $d \in \mathbb{N}$. Um conjunto *nulo* em \mathbb{R}^d é um conjunto $N \subseteq \mathbb{R}^d$ tal que, para todo $\varepsilon > 0$, existe cobertura $(C_n)_{n \in \mathbb{N}}$ de N por cubos d -dimensionais tal que

$$\sum_{n \in \mathbb{N}} \text{vol}^d(C_n) < \varepsilon.$$

Denota-se $N \doteq \emptyset$.

O motivo da notação $N \doteq \emptyset$ ficará mais claro quando uma medida for definida.

Proposição 20.19. Seja $d \in \mathbb{N}$. O conjunto de conjuntos nulos é um σ -ideal:

1. $\emptyset \doteq \emptyset$;
2. Se $S \subseteq N \subseteq \mathbb{R}^d$ e $N \doteq \emptyset$, então $S \doteq \emptyset$;
3. Para toda sequência $(N_n)_{n \in \mathbb{N}}$ de subconjuntos nulos em \mathbb{R}^d ,

$$\bigcup_{n \in \mathbb{N}} N_n \doteq \emptyset.$$

Demonstração. 1. Basta considerar a sequência de conjuntos vazios $(\emptyset)_{n \in \mathbb{N}}$. Essa sequência cobre \emptyset e $\text{vol}^d(\emptyset) = 0$. Portanto, para todo $\varepsilon > 0$,

$$\sum_{n \in \mathbb{N}} \text{vol}^d(\emptyset) = 0 < \varepsilon,$$

o que mostra que $\emptyset \doteq \emptyset$.

2. Seja $\varepsilon > 0$. Como $N \doteq \emptyset$, existe cobertura $(C_n)_{n \in \mathbb{N}}$ de N por cubos tal que $\sum_{n \in \mathbb{N}} \text{vol}^d(C_n) < \varepsilon$. Como $S \subseteq N$, essa cobertura é também uma cobertura de S , logo $S \doteq \emptyset$.

3. Seja $\varepsilon > 0$. Para cada $n \in \mathbb{N}$, existe cobertura $(C_i^n)_{i \in \mathbb{N}}$ de N_n por cubos tal que $\sum_{i \in \mathbb{N}} \text{vol}^d(C_i^n) < \varepsilon 2^{-(n+1)}$, logo $(C_i^n)_{(n,i) \in \mathbb{N}^2}$ é uma cobertura de $(N_n)_{n \in \mathbb{N}}$ e

$$\sum_{(n,i) \in \mathbb{N}^2} \text{vol}^d(C_i^n) < \sum_{n \in \mathbb{N}} \varepsilon 2^{-(n+1)} = \varepsilon. \quad \blacksquare$$

Proposição 20.20. *Sejam $d \in \mathbb{N}$ e $C \subseteq \mathbb{R}^d$ um conjunto contável. Então $C \stackrel{\circ}{=} \emptyset$.*

Demonstração. Basta mostrar que um conjunto unitário é nulo, pois C é uma união contável de conjuntos unitários, portanto nulo pela proposição anterior. Para isso, seja $p \in \mathbb{R}^d$ e $\epsilon > 0$. Tomando $\alpha \in]0, 1[$ e definindo os cubos

$$C_0 := \bigtimes_{i \in [d]} \left[p_i - \frac{(\alpha \varepsilon)^{\frac{1}{d}}}{2}, p_i + \frac{(\alpha \varepsilon)^{\frac{1}{d}}}{2} \right]$$

e, para todo $n \in \mathbb{N}^*$, $C_n := \emptyset$, segue que $p \in \bigcup_{n \in \mathbb{N}} C_n$, pois $p \in C_0$. Como

$$\text{vol}^d(C_0) = \bigtimes_{i \in [d]} \left| p_i + \frac{(\alpha \varepsilon)^{\frac{1}{d}}}{2} - \left(p_i - \frac{(\alpha \varepsilon)^{\frac{1}{d}}}{2} \right) \right| = ((\alpha \varepsilon)^{\frac{1}{d}})^d = \alpha \varepsilon$$

e $\text{vol}^d(\emptyset) = 0$, segue que

$$\sum_{n \in \mathbb{N}} \text{vol}^d(C_n) = \alpha \varepsilon < \varepsilon,$$

logo $\{p\} \stackrel{\circ}{=} \emptyset$. ■

Agora, definiremos conjuntos nulos em uma variedade \mathbf{V} .

Definição 20.33. Seja \mathbf{V} uma variedade diferencial. Um conjunto *nulo* em \mathbf{V} é um conjunto $N \subseteq V$ tal que, para toda carta (A, x) de \mathbf{V} , o conjunto $x(Q \cap A)$ é nulo em \mathbb{R}^d . Denota-se $N \stackrel{\circ}{=} \emptyset$.

Note que se (A, x) e (A', x') são cartas, a função $x' \circ x^{-1}$ preserva conjuntos nulos, pois é difeomorfismo. Isso significa, em particular, que se a propriedade vale para um atlas de \mathbf{V} , vale para seu atlas maximal. Na próxima seção, enunciaremos proposições que envolvem conjuntos nulos.

20.7 Valores Regulares, Pontos Críticos e Transversalidade

20.7.1 Valor Regular

Definição 20.34. Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais e $F: V \rightarrow V'$ uma função diferenciável. Um *valor regular* de F é um ponto $q \in V'$ tal que, para todo $p \in F^{-1}(q)$, $DF|_p: TV|_p \rightarrow TV'|_q$ é sobrejetiva.

Proposição 20.21. Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais, $F: V \rightarrow V'$ uma função diferenciável e $q \in V'$ um valor regular de F . Então $F^{-1}(q) \subseteq V$ é uma subvariedade diferencial de dimensão $\dim(V) - \dim(V')$.

20.7.2 Ponto Crítico

Definição 20.35. Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais e $F: V \rightarrow V'$ uma função diferenciável. Um *ponto crítico* de F é um ponto $p \in V$ tal que $DF|_p: TV|_p \rightarrow TV'|_{F(p)}$ não é sobrejetiva.

Ou seja, um valor regular é um ponto cujos pontos de sua imagem inversa não são críticos.

Proposição 20.22 (Teorema de Sard). *Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais e $F: V \rightarrow V'$ diferenciável. Se o conjunto $C \subseteq V$ de pontos críticos de F é nulo em \mathbf{V} , então $F(C) \subseteq V'$ é nulo em \mathbf{V}' .*

20.7.3 Transversalidade

Definição 20.36. Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais e $\mathbf{S} \subseteq \mathbf{V}'$ uma subvariedade. Uma função *transversal* a \mathbf{S} é uma função diferenciável $F: V \rightarrow V'$ tal que, para todo $p \in F^{-1}(S) \subseteq V$,

$$DF|_p(TV|_p) + TS|_{F(p)} = TV'|_{F(p)}.$$

Denota-se $F \pitchfork S$.

Um caso particular dessa definição é quando S é um conjunto unitário $\{q\}$. Nesse caso, para todo $p \in V$ tal que $F(p) = q$, $TS|_{F(p)} = \{0\}$ e a condição acima se torna $DF|_p TV|_p = TV'|_{F(p)}$, o que é equivalente a $DF|_p$ ser sobrejetiva, portanto $F \pitchfork \{p\}$ é equivalente a p ser valor regular de F . Segue da proposição análoga para valores regulares a seguinte proposição.

Proposição 20.23. Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais, $\mathbf{S} \subseteq \mathbf{V}'$ uma subvariedade e $F: V \rightarrow V'$ uma função diferenciável tal que $F \pitchfork S$. Então $F^{-1}(S) \subseteq V$ é uma subvariedade diferencial e $\text{codim}_V(F^{-1}(S)) = \text{codim}_{V'}(S)$.

Demonstração. Consideremos $p \in U \subseteq V$, $q = F(p)$, $U' = F(U) \subseteq V'$, uma carta adaptada $\varphi: U' \subseteq V' \rightarrow I^{\dim S} \times I^{\text{codim}_{V'} S}$ tal que $\varphi(q) = 0$ e $\varphi(U \cap S) = I^{\dim S} \times \{0\}$, e a projeção $\pi: I^{\dim S} \times I^{\text{codim}_{V'} S} \rightarrow I^{\text{codim}_{V'} S}$. Então

$$\pi \circ \varphi \circ F: V \rightarrow I^{\text{codim}_{V'} S}$$

é uma função diferenciável. Notemos agora que $0 \in I^{\text{codim}_{V'} S}$ é um valor regular de $\pi \circ \varphi \circ F$, pois para todo $a \in F^{-1}(S)$, como $F \pitchfork S$,

$$TV'|_{F(a)} = DF|_p TV|_a + TS|_{F(a)},$$

portanto $D\varphi|_{F(a)} TS|_{F(a)} = \mathbb{R}^{\dim S} \times \{0\}$. Sendo assim, segue que $F^{-1}(S) = (\pi \circ \varphi \circ F)^{-1}(0)$, logo $F^{-1}(S)$ é uma subvariedade de V . \blacksquare

Um caso importante é quando tem-se uma variedade diferencial \mathbf{V} e duas subvariedades diferenciais S e S' de \mathbf{V} . Se consideramos a inclusão $\iota: S \rightarrow V$, a condição $p \in \iota^{-1}(S')$ é equivalente a $p \in S \cap S'$, pois $\iota(p) = p$. Nesse caso, $D\iota|_p = \text{Id}$, portanto $\iota \pitchfork S'$ é equivalente a, para todo $p \in S \cap S'$,

$$TS|_p + TS'|_p = TV|_p.$$

Claramente, essa condição é simétrica com relação a S e S' . Definimos assim a transversalidade entre subvariedades.

Definição 20.37. Seja \mathbf{V} uma variedade diferencial. Duas subvariedades diferenciais S e S' de \mathbf{V} são *transversais* se, e somente se, para todo $p \in S \cap S'$,

$$TS|_p + TS'|_p = TV|_p.$$

Denota-se $S \pitchfork S'$.

Proposição 20.24. Sejam \mathbf{V} uma variedade diferencial e S e S' subvariedades diferenciais de \mathbf{V} tais que $S \pitchfork S'$. Então $S \cap S'$ é uma subvariedade diferencial de V e

$$\text{codim}(S \cap S') = \text{codim}(S) + \text{codim}(S').$$

Demonstração. Corolário da proposição anterior. \blacksquare

20.7.4 Mais Transversalidade

Proposição 20.25. Sejam \mathbf{V}, \mathbf{V}' e \mathbf{W} variedades diferenciais, $S \subseteq \mathbf{V}'$ uma subvariedade diferencial e $F: V \times W \rightarrow V''$, tal que $F \pitchfork S$. Então existe $\tilde{W} \subseteq W$ de medida total tal que $F_w \pitchfork S$ para todo $w \in \tilde{W}$ e

$$\begin{aligned} F_w: V &\longrightarrow V' \\ p &\longmapsto F(p, w). \end{aligned}$$

Exemplo 20.1. Sejam $f: \mathbb{R}^m \rightarrow \mathbb{R}^n$ suave e $Z \subseteq \mathbb{R}^n$. Defina

$$\begin{aligned} f: \mathbb{R}^m \times \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ (x, v) &\longmapsto f(x) + v. \end{aligned}$$

$DF_{(x_0, v_0)}(0, w) = D(F_{x_0})_{v_0}(w) = w$. Então $F \pitchfork Z$, e portanto $\tilde{S} \subseteq \mathbb{R}^n$ (como no teorema acima) tal que $F_{v_0}(x) = f(x) + v_0$ é $\pitchfork Z$.

Proposição 20.26. *Sejam $S \subseteq N$ subvariedade fechada. O conjunto*

$$\{f: M \rightarrow N \mid f \pitchfork S\}$$

é aberto e denso.

20.8 Campos Tensoriais

20.8.1 Campos Tensoriais, Vetoriais, e Derivações

Definição 20.38. Seja V uma variedade diferencial. Um de tipo (k, l) em V é uma função

$$\begin{aligned} T: V &\longrightarrow TV^{\otimes(k,l)} \\ p &\longmapsto T|_p \end{aligned}$$

tal que, para todo $p \in V$, $T|_p \in TV^{\otimes(k,l)}|_p$. O conjunto dos campos tensoriais diferenciáveis² de tipo (k, l) em V é denotado $\mathfrak{T}^{(k,l)}(V)$.

Um campo tensorial diferenciável de tipo $(k, 0)$ é também denotado $\mathfrak{T}^k(V)$ e um de tipo $(0, l)$ é também denotado $\mathfrak{T}^{*l}(V)$. Um é um campo tensorial de tipo $(1, 0)$.

O conjunto $\mathfrak{T}^1(V)$ é um espaço linear sobre \mathbb{R} com a soma e o produto por escalar induzidos pontualmente pela soma e produto por escalar de $TV|_p$: a soma é dada por

$$\begin{aligned} +: \mathfrak{T}^1(V) \times \mathfrak{T}^1(V) &\longrightarrow \mathfrak{T}^1(V) \\ (X, X') &\longmapsto X + X': V \longrightarrow TV \\ p &\longmapsto X|_p + X'|_p. \end{aligned}$$

e o produto por escalar é dado por

$$\begin{aligned} \cdot: \mathbb{R} \times \mathfrak{T}^1(V) &\longrightarrow \mathfrak{T}^1(V) \\ (c, X) &\longmapsto cX: V \longrightarrow TV \\ p &\longmapsto cX|_p. \end{aligned}$$

Mais adiante introduziremos um produto bilinear nesse espaço linear de modo a lhe dar uma estrutura de álgebra sobre \mathbb{R} . Além dessa operações, podemos multiplicar um campo vetorial por uma função escalar diferenciável pontualmente:

$$\begin{aligned} \cdot: \mathfrak{T}^0(V) \times \mathfrak{T}^1(V) &\longrightarrow \mathfrak{T}^1(V) \\ (f, X) &\longmapsto fX: V \longrightarrow TV \\ p &\longmapsto f(p)X|_p. \end{aligned}$$

Isso é uma ação do anel $\mathfrak{T}^0(V)$ que dá ao espaço $\mathfrak{T}^1(V)$ uma estrutura de módulo.

²Aqui diferenciável quer dizer \mathcal{C}^∞ .

Proposição 20.27. *Seja \mathbf{V} uma variedade diferencial.*

1. $(\mathfrak{T}^1(V), +, -, 0, \cdot)$ é um espaço linear sobre \mathbb{R} .
2. $(\mathfrak{T}^1(V), +, -, 0, \cdot)$ é um módulo sobre $\mathfrak{T}^0(V)$.

Proposição 20.28. *Sejam \mathbf{V} uma variedade diferencial e $X: V \rightarrow TV$ um campo vetorial. O campo vetorial X é diferenciável³ em \mathbf{V} se, e somente se, para toda $f \in \mathfrak{T}^0(V)$,*

$$\begin{aligned}\partial_X f: V &\longrightarrow \mathbb{R} \\ p &\longmapsto X|_p f\end{aligned}$$

é uma função escalar diferenciável.

20.9 Derivações e Colchete de Campos Vetoriais

A proposição da seção anterior é equivalente a dizer que X induz uma função

$$\begin{aligned}\partial_X: \mathfrak{T}^0(V) &\longrightarrow \mathfrak{T}^0(V) \\ f &\longmapsto \partial_X f.\end{aligned}$$

Essa função é linear na álgebra $\mathfrak{T}^0(V)$, pois

$$\partial_X(cf + f')(p) = X|_p(cf + f') = cX|_p f + X|_p f' = (c\partial_X f + \partial_X f')(p).$$

Além disso, ela é uma derivação em $\mathfrak{T}^0(V)$, pois

$$\partial_X(f f')(p) = X|_p(f f') = X|_p(f)f'(p) + f(p)X|_p(f') = (\partial_X(f)f' + f\partial_X(f'))(p).$$

Pode-se mostrar que existe uma bijeção entre o conjunto dos campos vetoriais diferenciáveis $\mathfrak{T}^1(V)$ e o conjunto das derivações $\text{Der}(\mathfrak{T}^0(V))$. Por esse motivo, ignora-se a notação $\partial_X f$ da derivação e denota-se simplesmente Xf . É importante notar, no entanto, que fX e Xf são objetos distintos, o primeiro sendo um elemento de $\mathfrak{T}^1(V)$, resultado da multiplicação de uma função escalar por um campo vetorial, uma operação da estrutura de $\mathfrak{T}^0(V)$ -módulo de $\mathfrak{T}^1(V)$, e a segunda é um elemento de $\mathfrak{T}^0(V)$, uma função escalar, resultado de uma derivação na álgebra $\mathfrak{T}^0(V)$.

Definiremos agora a ‘derivada de Lie’. Essa derivada dará, como comentado anteriormente, uma estrutura de álgebra sobre \mathbb{R} a $\mathfrak{T}^1(V)$. O conjunto $\text{Der}(\mathfrak{T}^0(V))$

³Aqui diferenciável quer dizer \mathcal{C}^∞ . Não consideraremos os detalhes relacionados ao grau de regularidade do campo, mas eles podem ser definidos e estudados de modo análogo, substituindo \mathcal{C}^∞ por \mathcal{C}^k .

tem um produto \circ dado pela composição de funções, induzido do produto de composição de $\mathcal{L}(\mathfrak{T}^0, \mathbb{R})$. Esse produto é associativo, mas não faz de $\text{Der}(\mathfrak{T}^0(V))$ uma álgebra de Lie, pois nem é fechado; ou seja, a composição de quaisquer duas derivações não é uma derivação. Podemos formar uma álgebra de Lie a partir de uma álgebra associativa de um modo bem conhecido usando o colchete de Lie. Definamos, portanto, para duas derivações $\partial_X, \partial_{X'} \in \text{Der}(\mathfrak{T}^0(V))$, o produto

$$[\partial_X, \partial_{X'}] := \partial_X \circ \partial_{X'} - \partial_{X'} \circ \partial_X.$$

Esse produto é uma derivação pela proposição 12.7. Portanto existe um campo vetorial associado à derivação $[\partial_X, \partial_{X'}]$, que denotaremos por $[X, X'] \in \mathfrak{T}^1(V)$, de modo que

$$\partial_{[X, X']} = [\partial_X, \partial_{X'}].$$

O campo vetorial $[X, X']$ é chamado de ‘colchete de Lie’ dos campos $X, X' \in \mathfrak{T}^1(V)$. Em um ponto $p \in V$, e função $f \in \mathfrak{T}^0(V)$, o colchete é

$$[X, X']|_p(f) = X|_p(X'f) - X'|_p(Xf).$$

Proposição 20.29 (Colchete em Coordenadas Locais). *Sejam \mathbf{V} uma variedade diferencial e $X, Y \in \mathfrak{T}^1(V)$ campos vetoriais. Para toda carta (A, x) de \mathbf{V} , se $X = X^i \frac{\partial}{\partial x^i}$ e $Y = Y^i \frac{\partial}{\partial x^i}$ em A , então o colchete entre X e Y em A é*

$$[X, Y] = \bigoplus_{(i,j) \in [d]^2} \left(X^i \frac{\partial Y^j}{\partial x^i} - Y^i \frac{\partial X^j}{\partial x^i} \right) \frac{\partial}{\partial x^j}.$$

Demonstração. Basta notar que, para toda $f \in \mathfrak{T}^0(V)$

$$\begin{aligned} [X, Y]f &= \bigoplus_{i \in [d]} X^i \frac{\partial}{\partial x^i} \left(\bigoplus_{j \in [d]} Y^j \frac{\partial f}{\partial x^j} \right) - \bigoplus_{j \in [d]} Y^j \frac{\partial}{\partial x^j} \left(\bigoplus_{i \in [d]} X^i \frac{\partial f}{\partial x^i} \right) \\ &= \bigoplus_{(i,j) \in [d]^2} \left(X^i \frac{\partial Y^j}{\partial x^i} \frac{\partial f}{\partial x^j} + X^i Y^j \frac{\partial^2 f}{\partial x^i \partial x^j} - Y^j \frac{\partial X^i}{\partial x^j} \frac{\partial f}{\partial x^i} - Y^j X^i \frac{\partial^2 f}{\partial x^j \partial x^i} \right) \\ &= \bigoplus_{(i,j) \in [d]^2} \left(X^i \frac{\partial Y^j}{\partial x^i} - Y^i \frac{\partial X^j}{\partial x^i} \right) \frac{\partial f}{\partial x^j}, \end{aligned}$$

pois $\frac{\partial^2 f}{\partial x^i \partial x^j} = \frac{\partial^2 f}{\partial x^j \partial x^i}$. ■

Usando a notação de Einstein e simplificando a fórmula da proposição, temos

$$[X, Y] = (XY^i - YX^i) \frac{\partial}{\partial x^i}.$$

Em particular, temos que $\left[\frac{\partial}{\partial x^i}, \frac{\partial}{\partial x^j} \right] = 0$ para todos $i, j \in [d]$, fato essencial na demonstração da proposição anterior.

O colchete de Lie satisfaz as seguintes propriedades.

Proposição 20.30. *Seja \mathbf{V} uma variedade diferencial.*

1. $(\mathfrak{T}^1(V), [\cdot, \cdot])$ é uma álgebra de Lie sobre \mathbb{R} ;
2. Para todos $X, X' \in \mathfrak{T}^1(V)$ e $f, f' \in \mathfrak{T}^0(V)$,

$$[fX, f'X'] = ff' [X, X'] + f(Xf')X' - f'(X'f)X.$$

Demonstração. 1. Corolário de 12.7.

2. Para toda $g \in \mathfrak{T}^0(V)$,

$$\begin{aligned} [fX, f'X'] g &= (fX)(f'X')g - (f'X')(fX)g \\ &= (fX)(f'X'g) - (f'X')(fXg) \\ &= (fX)(f')(X'g) + f'((fX)(X'g)) \\ &\quad - (f'X')(f)(Xg) - f((f'X')(Xg)) \\ &= ff' [X, X'](g) + f(Xf')X'(g) - f'(X'f)X(g) \\ &= (ff' [X, X'] + f(Xf')X' - f'(X'f)X)(g). \end{aligned}$$

■

20.9.1 Álgebra de Campos Tensoriais

Assim como definimos produto tensorial de espaços lineares, podemos definir um produto tensorial de módulos sobre anéis comutativos. Pode-se mostrar que, nesse caso, o produto tensorial de tipo (k, l) do módulo $\mathfrak{T}^1(V)$ sobre o anel comutativo $\mathfrak{T}^0(V)$ é o espaço $\mathfrak{T}^{(k,l)}(V)$ de campos tensoriais de tipo (k, l) em \mathbf{V} :

$$(\mathfrak{T}^1(V))^{\otimes(k,l)} = \mathfrak{T}^{(k,l)}(V).$$

Desse modo, os campos tensoriais $T \in \mathfrak{T}^{(k,l)}(V)$ são tensores em si, e não somente tensores em cada ponto $p \in V$. Assim, podemos formar a *álgebra de campos tensoriais* em \mathbf{V}

$$\mathfrak{T}^\otimes(V) := \bigoplus_{(k,l) \in \mathbb{N}^2} \mathfrak{T}^{(k,l)}(V).$$

O espaço $\mathfrak{T}^\otimes(V)$ é uma álgebra sobre $\mathfrak{T}^0(V)$. A soma e o produto por escalar são definidos pontualmente e o produto tensorial também.

20.9.2 Fluxo de Campos Vetoriais

20.10 Formas Diferenciáveis

O fibrado de k -covetores (k -tensores covariantes) de uma variedade diferencial \mathbf{V} é $T^*V^{\otimes k}$, e o subfibrado de tensores alternados desse fibrado é denotado

$$\bigwedge^k T^*V := \bigsqcup_{p \in V} \bigwedge^k T^*V|_p.$$

Uma seção desse fibrado é um campo de funcionais k -lineares alternados sobre \mathbf{V} . A próxima definição consiste desses objetos.

ΑΒΕΔΕΦΓΗΤΓΚΛΜΝΩΡΩΣΤΥΨΩΧΨΞ

Definição 20.39. Seja \mathbf{V} uma variedade diferencial. Uma k -forma em \mathbf{V} é uma função

$$\omega: V \longrightarrow \bigwedge^k T^*V$$

tal que, para todo $p \in V$, $\omega|_p \in \bigwedge^k T^*V|_p$ é um funcional k -linear alternado de $TV|_p$. O conjunto de k -formas diferenciáveis⁴ em \mathbf{V} é denotado $\Omega^k(V)$.

O produto exterior de duas formas $\omega \in \Omega^k(V)$ e $\omega' \in \Omega^{k'}(V)$ é definido pontualmente,

$$(\omega \wedge \omega')|_p := \omega|_p \wedge \omega'|_p,$$

e é uma $(k+k')$ -forma em \mathbf{V} . Para $k = 0$, $\omega \wedge \omega'$ é simplesmente $\omega\omega'$, uma k' -forma.

A soma direta desses espaços é o espaço das formas em \mathbf{V} , denotado

$$\Omega(V) := \bigoplus_{i \in [d]} \Omega^k(V).$$

Esse espaço linear com o produto exterior

$$\begin{aligned} \wedge: \Omega(V) \times \Omega(V) &\longrightarrow \Omega(V) \\ (\omega, \omega') &\longmapsto \omega \wedge \omega' \end{aligned}$$

é uma álgebra associativa, anticomutativa e graduada.

⁴Aqui diferenciável quer dizer \mathcal{C}^∞ .

Representação Coordenada

Seja $\omega \in \Omega^k(V)$. Como $\omega|_p$ é um k -covetor de $TV|_p$ para cada $p \in V$, podemos escrevê-lo com respeito a uma base de $T^*V|_p$. Uma carta (A, x) de \mathbf{V} induz uma base $(dx^i|_p)_{i \in [d]}$ de $T^*V|_p$ para cada $p \in A$. Em coordenadas locais, portanto, o funcional k -linear alternado $\omega|_p$ pode ser escrito

$$\omega|_p = \bigoplus_{i \in [d]^{\uparrow k}} \omega_i(p) dx^i|_p$$

em que $[d]^{\uparrow k} := \{(i_0, \dots, i_{k-1})_{j \in [k]} \in [d]^k \mid i_0 < \dots < i_{k-1}\}$ é um conjunto de multi-índices crescentes e, para cada multi-índice $i = (i_0, \dots, i_{k-1}) \in [d]^{\uparrow k}$,

$$dx^i|_p = dx^{i_0}|_p \wedge \dots \wedge dx^{i_{k-1}}|_p.$$

Isso ocorre porque $(dx^i|_p)_{i \in [d]^{\uparrow k}}$ é uma base de $\wedge^k T^*V|_p$. A k -forma ω restrita a A pode ser escrita

$$\omega|_A = \bigoplus_{i \in [d]^{\uparrow k}} \omega_i dx^i.$$

Proposição 20.31. *Seja \mathbf{V} uma variedade diferencial. Uma k -forma $\omega \in \Omega^k(V)$ é diferenciável se, e somente se, para toda carta (A, x) de \mathbf{V} , as funções $\omega_i: A \rightarrow \mathbb{R}$ tais que*

$$\omega|_A = \bigoplus_{i \in [d]^{\uparrow k}} \omega_i dx^i$$

são diferenciáveis.

Diferenciabilidade independe da carta no sentido de que, se algum sub-atlas da variedade faz com que as funções a_i sejam todas diferenciáveis, então todas cartas compatíveis com esse atlas também farão.

Formas Volume

Definição 20.40. Seja \mathbf{V} uma variedade diferencial d -dimensional. Uma *forma volume* em \mathbf{V} é uma forma $\omega \in \Omega^d(V)$ tal que, para todo $p \in V$, $\omega|_p \neq 0$.

Proposição 20.32. *Seja \mathbf{V} uma variedade diferenciável. Então \mathbf{V} é orientável se, e somente se, existe uma forma volume $\omega \in \Omega^d(V)$.*

20.10.1 Formas Puxadas

Definição 20.41. Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais, $F: V \rightarrow V'$ uma função diferencial e $\omega \in \Omega^k(V')$ uma k -forma em \mathbf{V}' . A k -forma *pxuada* de ω por F é a

a k -forma

$$\begin{aligned} F^*\omega: V &\longrightarrow \bigwedge^k T^*V \\ p &\longmapsto F^*\omega|_p: TV|_p \times \cdots \times TV|_p \longrightarrow \mathbb{R} \\ (v_0, \dots, v_{k-1}) &\longmapsto \omega|_{F(p)}(DF|_p v_0, \dots, DF|_p v_{k-1}). \end{aligned}$$

em \mathbf{V} .

A definição é equivalente a, para todo $p \in V$,

$$(F^*\omega)|_p := (DF|_p)^*\omega|_{F(p)}.$$

Proposição 20.33. *Sejam \mathbf{V} e \mathbf{V}' variedades diferenciais e $F: V \longrightarrow V'$ uma função diferencial.*

1. $F^*: \Omega^k(V') \longrightarrow \Omega^k(V')$ é uma função linear;

2. Para todas formas $\omega \in \Omega^k(V')$ e $\omega' \in \Omega^{k'}(V')$,

$$F^*(\omega \wedge \omega') = (F^*\omega) \wedge (F^*\omega');$$

3. Para toda carta (A, x) de \mathbf{V}' e toda forma $\omega \in \Omega^k(V')$,

$$F^* \left(\bigoplus_{I \in [d]^{\uparrow k}} \omega_I dx^I \right) = \bigoplus_{I \in [d]^{\uparrow k}} (\omega_I \circ F) d(x \circ F)^I = \bigoplus_{I \in [d]^{\uparrow k}} (F^*\omega_I) d(F^*x)^I.$$

20.10.2 Derivada Exterior

Formas no Espaço Real

Definiremos nesta seção a derivada exterior de formas. Primeiro definiremos a derivada exterior de formas em \mathbb{R}^d . Consideraremos um campo escalar $\omega: A \subseteq \mathbb{R}^d \longrightarrow \mathbb{R}$, que é uma 0-forma em $A \subseteq \mathbb{R}^d$. A diferencial de ω em um ponto $p \in A$ é uma função linear $D\omega|_p: \mathbb{R}^d \longrightarrow \mathbb{R}$ (que é um funcional 1-linear alternado em \mathbb{R}^d) dada por

$$D\omega|_p = \bigoplus_{i \in [d]} \partial_i \omega(p) d\pi^i|_p,$$

em que $d\pi^i|_p := D\pi^i|_p$ é a diferencial de $\pi^i: A \subseteq \mathbb{R}^d \longrightarrow \mathbb{R}$ em p , que é a funcional linear $e^i: \mathbb{R}^d \longrightarrow \mathbb{R}$. (O funcional e^i é o mesmo funcional que π^i — as notações diferem somente por causa do contexto ser diferente — e $d\pi^i|_p = \pi^i$, pois π^i é linear.) Isso significa que

$$D\omega = \bigoplus_{i \in [d]} \partial_i \omega d\pi^i$$

é uma 1-forma em $A \subseteq \mathbb{R}^d$, ou seja, um campo de funcionais lineares alterados. Além disso, lembremos que, para todo multi-índice $I = (i_0, \dots, i_{k-1}) \in [d]^{\uparrow k}$, define-se

$$d\pi^I = d\pi^{i_0} \wedge \cdots \wedge d\pi^{i_{k-1}}.$$

Com isso em mente, definimos a derivada exterior de formas em \mathbb{R}^d .

Definição 20.42. Sejam $d \in \mathbb{N}$, $A \subseteq \mathbb{R}^d$ um aberto e $\omega \in \Omega^k(A)$ uma k -forma em A tal que

$$\omega := \bigoplus_{I \in [d]^{\uparrow k}} \omega_I d\pi^I,$$

sendo, para todo $I \in [d]^{\uparrow k}$, $\omega_I \in \mathcal{C}^\infty(A)$. A *derivada exterior* de ω é a $(k+1)$ -forma

$$d\omega := \bigoplus_{I \in [d]^{\uparrow k}} d\omega_I \wedge d\pi^I,$$

em que, para todo $I \in [d]^{\uparrow k}$, $d\omega_I := D\omega_I$ é a diferencial de ω_I .

Exemplo 20.2. Como já comentado, a derivada exterior de uma 0-forma $\omega: A \subseteq \mathbb{R}^d \rightarrow \mathbb{R}$ é dada por

$$d\omega = \bigoplus_{i \in [d]} \partial_i \omega d\pi^i.$$

Note também que a derivada exterior de uma 1-forma $\omega = \bigoplus_{i \in [d]} \omega_i d\pi^i$ é dada por

$$\begin{aligned} d\omega &= \bigoplus_{i \in [d]} d\omega_i \wedge d\pi^i \\ &= \bigoplus_{i \in [d]} \left(\bigoplus_{j \in [d]} \partial_j \omega_i(p) d\pi^j \right) \wedge d\pi^i \\ &= \bigoplus_{(i,j) \in [d]^2} \partial_j \omega_i(p) d\pi^j \wedge d\pi^i \\ &= \bigoplus_{i < j} \partial_j \omega_i(p) d\pi^j \wedge d\pi^i + \bigoplus_{i > j} \partial_j \omega_i(p) d\pi^j \wedge d\pi^i \\ &= \bigoplus_{i < j} (\partial_i \omega_j - \partial_j \omega_i) d\pi^i \wedge d\pi^j. \end{aligned}$$

Notemos que a derivada exterior acima definida para cada $k \in [d]$ é uma função

$$\begin{aligned} d: \Omega^k(A) &\longrightarrow \Omega^{k+1}(A) \\ \omega &\longmapsto d\omega \end{aligned}$$

e, portanto, é uma função

$$\begin{aligned} d: \Omega(A) &\longrightarrow \Omega(A) \\ \omega &\longmapsto d\omega. \end{aligned}$$

ao definirmos que, para todas $\omega \in \Omega^k(A)$ e $\omega' \in \Omega^{k'}(A)$,

$$d(\omega + \omega') := d\omega + d\omega'.$$

A derivada exterior satisfaz as seguintes propriedades.

Proposição 20.34. *Sejam $d \in \mathbb{N}$ e $A \subseteq \mathbb{R}^d$ um aberto. A derivada exterior $d: \Omega(A) \rightarrow \Omega(A)$ satisfaz*

1. d é linear sobre \mathbb{R} ;

2. Para todas formas $\omega \in \Omega^k(A)$ e $\omega' \in \Omega^{k'}(A)$,

$$d(\omega \wedge \omega') = d\omega \wedge \omega' + (-1)^k \omega \wedge d\omega';$$

3. $d \circ d = 0$;

4. Para toda função diferenciável $F: A \subseteq \mathbb{R}^d \rightarrow A' \subseteq \mathbb{R}^{d'}$ e toda forma $\omega \in \Omega^k(A')$,

$$F^*(d\omega) = d(F^*\omega).$$

Demonstração. 1. Sejam $\omega, \omega' \in \Omega^k(A)$ e $c \in \mathbb{R}$. Então

$$c\omega + \omega' = \bigoplus_{I \in [d]^{\uparrow k}} (c\omega_I + \omega'_I) \wedge d\pi^I,$$

portanto

$$\begin{aligned} d(c\omega + \omega') &= d \left(\bigoplus_{I \in [d]^{\uparrow k}} (c\omega_I + \omega'_I) \wedge d\pi^I \right) \\ &= \bigoplus_{I \in [d]^{\uparrow k}} d(c\omega_I + \omega'_I) \wedge d\pi^I \\ &= \bigoplus_{I \in [d]^{\uparrow k}} (cd\omega_I + d\omega'_I) \wedge d\pi^I \\ &= c \bigoplus_{I \in [d]^{\uparrow k}} d\omega_I \wedge d\pi^I + \bigoplus_{I \in [d]^{\uparrow k}} d\omega'_I \wedge d\pi^I \\ &= cd\omega + d\omega'. \end{aligned}$$

Para $\omega \in \Omega^k(A)$ e $\omega' \in \Omega^{k'}(A)$, segue da definição de d em $\Omega(A)$.

2. Basta considerar as formas $f d\pi^i \in \Omega^k(A)$ e $f' d\pi^{I'} \in \Omega^{k'}(A)$, em que $f, f' \in \mathcal{C}^\infty(A)$ são campos escalares, pois por linearidade a propriedade valerá para todas formas. Temos que mostrar que $d(f d\pi^I) = df \wedge d\pi^I$ para todo multiíndice $I \in [d]^k$, não somente os crescentes $I \in [d]^{\uparrow k}$. Se I tem alguma entrada

repetida, $d\pi^I = 0$, portanto $d(fd\pi^I) = 0 = df \wedge d\pi^I$. Caso contrário, existe permutação $\sigma \in [k]$ tal que $\sigma(I) = (i_{\sigma(0)}, \dots, i_{\sigma(k-1)})$ é um multi-índice crescente, portanto

$$d(fd\pi^I) = d(\epsilon(\sigma)fd\pi^{\sigma(I)}) = \epsilon(\sigma)df \wedge d\pi^{\sigma(I)} = df \wedge d\pi^I.$$

Assim, segue que

$$\begin{aligned} d((fd\pi^I) \wedge (f'd\pi^{I'})) &= d(f f' d\pi^I \wedge d\pi^{I'}) \\ &= d(f f' d\pi^I \wedge d\pi^{I'}) \\ &= ((df)f' + f df') \wedge d\pi^I \wedge d\pi^{I'} \\ &= (df)f' \wedge d\pi^I \wedge d\pi^{I'} + f df' \wedge d\pi^I \wedge d\pi^{I'} \\ &= (df \wedge d\pi^I) \wedge (f'd\pi^{I'}) + (-1)^k (fd\pi^I) \wedge (df' \wedge d\pi^{I'}) \\ &= d(fd\pi^I) \wedge (f'd\pi^{I'}) + (-1)^k (fd\pi^I) \wedge d(f'd\pi^{I'}), \end{aligned}$$

pois $df' \wedge d\pi^I = (-1)^k d\pi^I \wedge df'$.

3. Provaremos primeiros para 0-formas. Para $f \in \Omega^0(A)$,

$$\begin{aligned} d(df) &= d\left(\bigoplus_{i \in [d]} D_i f d\pi^i\right) \\ &= \bigoplus_{i < j} (D_{i,j} f - D_{j,i} f) d\pi^i \wedge d\pi^j \\ &= 0, \end{aligned}$$

pois $D_{i,j}f = D_{j,i}f$. Agora, para uma k -forma $\omega \in \Omega^k(A)$, segue do resultado anterior e do item anterior que

$$\begin{aligned} d(d\omega) &= d\left(\bigoplus_{I \in [d]^{\uparrow k}} d\omega_I \wedge d\pi^I\right) \\ &= \bigoplus_{I \in [d]^{\uparrow k}} d(d\omega_I) \wedge d\pi^I \\ &\quad + \bigoplus_{I \in [d]^{\uparrow k}} \bigoplus_{j \in [k]} (-1)^j d\omega_I \wedge d\pi^{i_0} \wedge \cdots \wedge d(d\pi^{i_j}) \wedge \cdots \wedge d\pi^{i_{k-1}} \\ &= 0. \end{aligned}$$

4. Novamente, basta considerar $fd\pi^I \in \Omega^k(A')$, pois F^\star é linear. Da definição

de forma puxada, segue que

$$\begin{aligned}
 F^*(d(fd\pi^I)) &= F^*(df \wedge d\pi^I) \\
 &= d(f \circ F) \wedge d(\pi^{i_0} \circ F) \wedge \cdots d(\pi^{i_{k-1}} \circ F) \\
 &= d((f \circ F)d(\pi^{i_0} \circ F) \wedge \cdots d(\pi^{i_{k-1}} \circ F)) \\
 &= d(F^*(fd\pi^I)).
 \end{aligned}$$

■

Formas em Variedades Diferenciais

Estendemos agora a definição da derivada exterior de formas para variedades diferenciais quaisquer.

Proposição 20.35. *Seja V uma variedade diferencial. Existe única função*

$$d: \Omega(V) \longrightarrow \Omega(V)$$

tal que

1. *Para todo $k \in [\dim V]$, $d: \Omega^k(V) \longrightarrow \Omega^{k+1}(V)$ é linear sobre \mathbb{R} ;*
2. *Para todas formas $\omega \in \Omega^k(V)$ e $\omega' \in \Omega^{k'}(V)$,*

$$d(\omega \wedge \omega') = d\omega \wedge \omega' + (-1)^k \omega \wedge d\omega';$$

3. $d \circ d = 0$;

4. *Para todo campo escalar $f \in \mathcal{C}^\infty(V) = \Omega^0(V)$, a diferencial Df de f é a derivada exterior df de f , dada por $df(X) = \partial_X f$.*