ELEMENTOS DE MATEMÁTICA

Pedro G. Mattos

Sumário

Introdução **ix**

1 Conjuntos 1

1 Os Axiomas e as Construções Essenciais **2**
1.1 Preliminares de Lógica 2
1.1.1 Lógica de Ordem 0 3
1.1.2 Lógica de Ordem 1 5
1.1.3 Conjunto e Pertencimento 10
1.2 Axiomas do Vazio e da Extensão 11
1.2.1 Vazio e Igualdade 11
1.2.2 Subconjuntos 12
1.3 Axioma da Especificação 13
1.4 Axioma das Partes 14
1.5 Axioma do Par 15
1.6 Axioma da União 16
1.6.1 União de um Conjunto 16
1.6.2 Interseção de um Conjunto 17
1.7 Axioma do Infinito 18
1.8 Axioma da Escolha 19
1.9 Axiomas da Fundação e Substituição 21

2 Famílias e Propriedades de Conjuntos **23**
2.1 Famílias e Indexações 23
2.2 Propriedades de União e Interseção 25
2.3 Produto de Conjuntos 27
2.4 Coproduto de Conjuntos 28
2.4.1 Propriedades de Produto e Coproduto 29
2.5 Complementares e Diferença Simétrica 30
2.5.1 Propriedades 30

2.6 Coberturas e Partições 31
2.6.1 Refinamento de Partições 31

3 Funções **34**
3.1 Definição e Propriedades Básicas 34
3.2 Composição de Funções 36
3.3 Função Inversa, Injetividade e Sobrejetividade 37
3.4 Imagem Inversa de Função e Propriedades 38
3.5 Propriedades de Imagem e Imagem Inversa 39
3.6 Os Funtores Imagem e Imagem Inversa 41

4 Relações Binárias **43**
4.1 Relações de Equivalência 43
4.2 Relações de Ordem 44
4.2.1 Ordens Parciais, Estritas e Totais 44
4.2.2 Conjuntos Parcialmente Ordenados 46
4.2.3 Funções Monótonas 48
4.2.4 Cadeias e Lema de Zorn 49
4.2.5 Pré-Ordens 49
4.2.6 Conjunto Direcionado 50
4.2.7 Reticulados 50
4.2.8 Álgebras Booleanas 51

5 Cardinalidade de Conjuntos **55**
5.1 Relações 55
5.1.1 Igualdade de Cardinais 55
5.1.2 Ordenação de Cardinais 56
5.2 Operações 57
5.2.1 Cardinalidade de Soma (ou União Disjunta) 57

6 Conjuntos Numéricos **60**
6.1 Números Naturais 60
6.1.1 Adição 61
6.1.2 Multiplicação 63
6.1.3 Ordenação 66
6.1.4 Bases 69
6.2 Números Inteiros 71
6.2.1 Adição e Subtração 72
6.2.2 Multiplicação 73
6.2.3 Ordenação 74

2 Álgebra 75

1 Operações Binárias e Estruturas Básicas 76
1.1 Operações Binárias . . . 76
1.2 Magma . . . 77
1.3 Semigrupo . . . 78
1.4 Homomorfismo de Semigrupos . . . 80
1.5 Monoide . . . 80
1.6 Homomorfismos de Monoides . . . 83

2 Grupos 84
2.1 Construções Algébricas . . . 84
2.1.1 Grupo e Subgrupo . . . 84
2.1.2 Coclasses e Índice de Subgrupo . . . 88
2.1.3 Subgrupo Normal e Grupo Quociente . . . 90
2.1.4 Homomorfismo de Grupo . . . 92
2.1.5 Núcleo, Imagem e Isomorfismo . . . 94
2.1.6 Teoremas de Isomorfismo . . . 96
2.2 Construções Categóricas . . . 98
2.2.1 Produto de Grupos . . . 98
2.2.2 Grupo Livre . . . 99
2.2.3 Coproduto de Grupos . . . 101
2.3 Construções Específicas . . . 103
2.3.1 Grupo Simples e Subgrupo Normal Maximal . . . 103
2.3.2 Sequência subnormal . . . 104
2.3.3 Conjunto gerador . . . 104
2.3.4 Grupos Simétricos e Alternados . . . 104
2.3.5 Grupos Cíclicos . . . 109
2.3.6 Grupos Diedrais . . . 109
2.4 Ação de Grupos . . . 110
2.4.1 Órbitas e Estabilizadores . . . 111
2.5 Grupo Linear Geral . . . 111
2.6 Representação de Grupos . . . 112

3 Anéis 113
3.1 Construções Algébricas . . . 113
3.1.1 Anel e Subanel . . . 113
3.1.2 Ideais e Anéis Quocientes . . . 116
3.1.3 Homomorfismos de Anéis . . . 120
3.1.4 Teoremas de Isomorfismo . . . 127
3.2 Construções Categóricas . . . 131

3.2.1 Anel de Polinômios 131
3.2.2 Produto de Anéis 135
3.3 Construções Específicas 136
3.3.1 Domínios e Corpos 136
3.3.2 Divisão e Associação em Anéis 137
3.3.3 Irredutíveis, Primos e Fatoração 142
3.3.4 Ideais Primos e Ideais Maximais 149
3.3.5 Domínios Euclidianos 151
3.3.6 Raízes de Polinômios 152
3.4 Corpos 153
3.4.1 Extensões de Corpos 153
3.4.2 Extras 157
3.5 Matrizes 158
3.5.1 Soma de Matrizes 159
3.5.2 Produto de Matrizes e Produto Por Escalar 160
3.5.3 Matrizes Quadradas 162
3.5.4 Traço e Determinante 162

4 Corpos 164
4.1 Corpo e Subcorpo 164
4.2 Corpo de Frações 164
4.2.1 Os Números Racionais $\mathbb{Q}$ 168
4.2.2 Funções de Arredondamento 168

5 Espaços Lineares 171
5.1 Módulos 171
5.2 Espaço e Subespaço Lineares 174
5.3 Combinação Linear de Vetores 180
5.4 Soma de Subespaços Vetoriais 184
5.5 Bases de Espaços Vetoriais 186
5.6 Funções Lineares 189
5.7 Produto e Coproduto de Espaços Vetoriais 191
5.7.1 Produto 191
5.7.2 Coproduto (Soma) 193
5.8 Projeções Lineares 194
5.9 Funções Multilineares 196
5.9.1 Simetria, Antissimetria e Alternância 198
5.10 Formas Multilineares 200
5.10.1 Produto Tensorial de Formas Multilineares 201
5.10.2 Produto Alternado de Formas Multilineares 201
5.10.3 Formas Puxadas e Determinante 203

5.10.4 Extras . . . 205
5.11 Produto Tensorial de Espaços Lineares . . . 206
5.11.1 Tensores . . . 209

6 Álgebras sobre Corpos 210
6.1 Álgebra e Ação Adjunta . . . 210
6.2 Derivação . . . 211
6.3 Álgebra de Derivação Adjunta . . . 213
6.4 As Álgebras Reais $\mathbb{R}$, $\mathbb{R}^2$ e $\mathbb{R}^4$ . . . 215
6.4.1 Complexos . . . 215
6.4.2 Quatérnios . . . 217

7 Ordem em Estruturas Algébricas 224
7.1 Corpos Ordenados . . . 224
7.1.1 Imersão dos Inteiros e Racionais . . . 228
7.1.2 Cones Positivos . . . 228
7.1.3 Corpos Ordenados Completos . . . 231
7.1.4 Corpos Ordenados Infinitesimais . . . 232
7.1.5 Valor Absoluto e Distância . . . 232
7.1.6 Conicidade . . . 234
7.1.7 Convexidade . . . 235

3 Topologia e Geometria 236

1 Topologia 237
1.1 Espaços Topológicos . . . 237
1.1.1 Topologia, Abertos e Fechados . . . 237
1.1.2 Topologias Geradas, Bases e Sub-bases . . . 244
1.1.3 Funções Contínuas . . . 245
1.1.4 Topologias Induzidas . . . 246
1.2 Separação . . . 253
1.2.1 Noções de Separação de Conjuntos . . . 253
1.2.2 Espaços Distinguíveis . . . 254
1.2.3 Espaços Acessíveis . . . 255
1.2.4 Espaços Separados . . . 256
1.2.5 Espaços Regulares . . . 256
1.2.6 Espaços Completamente Regulares . . . 257
1.2.7 Espaços Normais . . . 257
1.3 Convergência . . . 259
1.3.1 Redes . . . 259

1.4 Conexidade e Compacidade 261
1.4.1 Conexidades 261
1.4.2 Compacidades 264
1.4.3 Contabilidades 266
1.5 Homotopia e Grupo Fundamental 267
1.5.1 Homotopia 267
1.5.2 Equivalência Homotópica 268
1.5.3 Caminhos e Laços 268
1.5.4 Homotopia de Caminhos 269
1.5.5 Grupo Fundamental 274
1.6 Topologia de Ordem 275
1.6.1 Topologia de um Corpo Ordenado 275

2 Espaços Métricos 278
2.1 Os Espaços Métricos 278
2.1.1 Métricas 278
2.1.2 Diâmetro, Bolas e Conjuntos e Funções Limitadas 282
2.2 Topologia dos Espaços Métricos 284
2.2.1 Interior e Pontos Interiores 284
2.2.2 Limites e Convergência de Sequências 285
2.2.3 Fecho e Pontos Aderentes 287
2.2.4 Conjuntos Densos 288
2.2.5 Conjuntos Compactos 289
2.2.6 Continuidade 289
2.2.7 Ponto Limite e Conjunto Derivado 291
2.2.8 Distância e Bolas de Conjuntos e Separação Métrica 291
2.3 Estrutura Uniforme 293
2.3.1 Sequências Aproximantes 293
2.3.2 Continuidade Uniforme 295
2.3.3 Espaços Métricos Completos 295
2.3.4 Limitação Uniforme (ou Total) 297
2.4 Funções que Preservam Distância 299
2.4.1 Funções Métricas (ou Subsemelhanças) 299
2.4.2 Homometrias e Isometrias 301
2.4.3 Contrações 302
2.4.4 Semelhanças 303

3 Grupos Topológicos 304
3.1 Grupo Topológico 304
3.2 Topologia em Grupos 306
3.3 Distância em Grupos 307

3.4 Homomorfismos Contínuos 307
3.5 Subgrupos Topológicos 308
3.6 Conexidade em Grupos Topológicos 308
3.7 Espaço de Homeomorfismos 309
3.8 Ação Contínua 309

4 Espaços Lineares Topológicos 311
4.1 Anéis e Corpos Topológicos 311
4.2 Espaço Linear Topológico 311
4.3 Espaço de Funções a Valores Vetoriais 311
4.4 Funções Lineares Contínuas 314
4.5 Espaço Dual Contínuo 314
4.6 Teoremas de Representação de Riesz 315
4.6.1 Representação Linear de Produto Interno 315
4.6.2 Representação Contínua de Medida 316

5 Espaços Normados 317
5.1 Norma em Corpos (Valor Absoluto) 317
5.2 Normas 320
5.2.1 Seminormas 320
5.2.2 Normas, Espaços Normados e Métricas Lineares 322
5.2.3 Bolas e Esferas Unitárias e Topologia 325
5.2.4 Equivalência de Normas 326
5.3 Funções Limitadas e Norma de Funções Lineares 327
5.4 Espaços Normados Completos 329
5.4.1 Sequências Absolutamente Somáveis 331
5.4.2 Espaços Normados de Dimensão Finita 332
5.4.3 Espaços de Funções Absolutamente Somáveis 334
5.4.4 Espaços de Funções Absolutamente Integráveis 336
5.4.5 Dualidade e Mergulho de Espaços Absolutamente Integráveis 346
5.5 Isometrias Lineares 347
5.5.1 Os Grupos Lineares Geral e Especial de Transformações e de Isometrias 347
5.6 Funções Multilineares 348
5.7 Álgebras Normadas 349
5.7.1 Função Exponencial 349

6 Espaços Lineares com Produto Interno 353
6.1 Produto Interno 353
6.2 Norma Induzida, Ortogonalidade e Ângulo 355
6.2.1 Norma 355

6.2.2 Perpendicularidade e Paralelismo 356
6.2.3 Projeções Paralela e Perpendicular 358
6.2.4 Projeções Ortogonais 360
6.2.5 Ângulo 361
6.2.6 Espaço Projetivo 365
6.2.7 Funções Ortogonais e Conformes 368
6.3 Espaço de Funções Quadrado Somáveis 371

7 Medida 372
7.1 Espaço Mensurável 372
7.1.1 Sigma-Álgebras e Sub-Sigma-Álgebras 372
7.1.2 Sigma-Álgebras Geradas 374
7.1.3 Limites de Conjuntos 374
7.2 Funções Mensuráveis 375
7.2.1 Sigma-Álgebras Puxadas e Empurradas 376
7.3 Produto de Espaços Mensuráveis 377
7.4 Espaços Mensuráveis com Estrutura Adicional 379
7.4.1 Espaços Mensuráveis Topológicos 379
7.4.2 Funções Mensuráveis com Valores Vetoriais 379
7.4.3 Funções Mensuráveis com Valores em Espaços Métricos . . . 379
7.5 Medida e Espaço de Medida 381
7.5.1 Medidas 381
7.5.2 Medida Exterior 383
7.6 Medida em Espaços Topológicos 386
7.6.1 Medidas Regulares 386
7.6.2 Medidas Localmente Finitas 386
7.7 Medidas em Grupos Topológicos 387
7.8 Medida em Espaços Métricos 387
7.8.1 Medidas Exteriores Métricas 387
7.8.2 Medidas por Coberturas Métricas 389
7.8.3 Dimensão Métrica e Fractais 393
7.9 Espaço Linear de Medidas 393
7.10 Quase 395
7.10.1 Quase Todo 395
7.10.2 Quase Igualdade de Conjuntos 396
7.10.3 Quase Igualdade de Funções 399

8 Integração 403
8.1 Integral de Funções Mensuráveis Simples 403
8.2 Integral de Funções Mensuráveis Positivas 408
8.3 Integral de Funções Mensuráveis 408

8.4 Teoremas de Convergências 408
8.5 Mudança de Variáveis na Integração 408
8.6 Integral em Espaços Normados Completos 410
8.6.1 Funções Simples 410
8.7 Desintegração de Medida 412

9 Diferenciação 414
9.1 Diferenciabilidade 414
9.1.1 Diferenciais de Ordem Superior 418
9.2 Derivadas Direcionais e a Geometria da Diferenciabilidade 420
9.3 Os Teoremas Fundamentais 421
9.3.1 Teorema da Função Inversa 421
9.3.2 Teorema da Função Implícita 421
9.3.3 Forma Local da Imersão 421
9.3.4 Forma Local da Submersão 422
9.3.5 Teorema do Posto 422
9.4 Cálculo em Espaços Normados de Dimensão Finita 423
9.4.1 Diferencial 423

10 Variedades 426
10.1 Variedades Topológicas e Diferenciais 426
10.1.1 Cartas e Atlas 426
10.1.2 Variedades e Estrutura Topológica e Diferencial 429
10.1.3 Exemplos de Variedades 431
10.1.4 Propriedades Topológicas 434
10.2 Funções Diferenciáveis 436
10.2.1 Funções Diferenciáveis 436
10.2.2 Funções Separadoras e Partições da Unidade 437
10.3 Espaço Tangente 439
10.3.1 Álgebra dos Campos Escalares 439
10.3.2 Espaço Tangente e a Diferencial 440
10.3.3 Fibrado Tangente 445
10.3.4 Curvas Equivelozes 446
10.4 Subvariedades 448
10.4.1 Imersão 448
10.4.2 Submersão 448
10.4.3 Mergulho 448
10.4.4 Subvariedades Imersas e Mergulhadas 448
10.5 Transversalidade 448
10.5.1 Conjuntos Nulos 448
10.5.2 Valor Regular 450

10.5.3 Ponto Crítico 450
10.5.4 Transversalidade 450
10.6 Campos Tensoriais 452
10.6.1 Campos Tensoriais, Vetoriais, e Derivações 452
10.6.2 Derivações e Colchete de Campos Vetoriais 453
10.6.3 Álgebra de Campos Tensoriais 456
10.6.4 Fluxo de Campos Vetoriais 456
10.6.5 Espaço Cotangente 460
10.6.6 Formas Diferenciáveis 460
10.6.7 Derivada Exterior 463
10.6.8 Derivada de Lie 467
10.7 Orientação 467
10.7.1 Orientação de Espaços Lineares 467
10.7.2 Orientação de Variedades 470
10.8 Grupos Diferenciais 471
10.9 Folheações 471
10.9.1 Cartas e Atlas Folheados 471
10.9.2 Componentes Tangencial e Transversal da Carta 473
10.9.3 Folheação 474

11 Fibrados **476**
11.1 Fibrados Topológicos 476
11.2 Fibrados Vetorias 477
11.2.1 Seções Locais e Globais 489
11.2.2 Grupo Estrutural 491
11.2.3 Referenciais Locais e Globais 491
11.3 Fibrados Principais 492
11.4 Conexões em Fibrados Vetoriais 494
11.4.1 Espaços Verticais e Horizontais 494
11.4.2 Conexão/Derivada Covariante 495

Licença do Livro (Inglês) **499**
.1 Definitions 499
.2 Scope 500
.3 License Conditions 501
.4 Sui Generis Database Rights 502
.5 Disclaimer of Warranties and Limitation of Liability 503
.6 Term and Termination 503
.7 Other Terms and Conditions 504
.8 Interpretation 504

Parte 1

Conjuntos

Capítulo 1

Os Axiomas e as Construções Essenciais

1.1 Preliminares de Lógica

Alguns conceitos da lógica formal serão brevemente introduzidos nesta seção para que a abordagem nas próximas seções façam sentido. Comentaremos sobre lógicas de ordem 0 e de ordem 1, tradicionalmente chamadas de lógica proposicional e lógica de predicados.

As teorias da lógica formal costumam ter axiomas, sentenças assumidas válidas a partir das quais deve-se inferir todas as outras sentenças da teoria. Ao longo do livro, os axiomas, as definições e as proposições serão enunciados, não como sentenças simbólicas, mas como sentenças em português, como se faz tradicionalmente na matemática. Isso facilita o entendimento e a naturalidade das sentenças. No entanto, ao longo das seções que seguem essas sentenças serão enunciadas também formalmente, para estimular o pensamento e a manipulação formais.

Alguns símbolos lógicos frequentemente facilitam e deixam mais claros os enunciados de sentenças na matemática. O símbolo

$$\bigwedge$$

será usados para substituir as expressões "para todo/a", "para todos/as", "para qualquer", "para quaisquer" e outras possíveis flexões gramaticais. O símbolo

$$\bigvee$$

será usados para substituir as expressões "para algum/ma", "para alguns/mas", "existe", "existem" e outras possíveis flexões gramaticais. Eles indicam que uma propriedade vale para todo/algum conjunto. O símbolo $\bigvee!$ significa que existe e é

único. Além desses, serão usados também os símbolos lógicos

$$\leftarrow \qquad \rightarrow \qquad \leftrightarrow$$

e as versões informais matemáticas

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

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

$$\wedge \qquad \vee$$

e as versões informais matemáticas

e ou

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

1.1.1 Lógica de Ordem 0

Na lógica de ordem 0, existem contáveis *proposições simples* (ou *variáveis proposicionais*). Elas são representadas por símbolos especificados e no que segue serão representadas pela letra P ou por P seguida de uma quantidade finita de $'$ (apóstrofes), como P' ou P''''.

Além disso, existem os *operadores lógicos*, que são os símbolos

$$\neg \qquad \wedge \qquad \vee \qquad \rightarrow \qquad \leftrightarrow$$

respectivamente chamados de *negação*, *conjunção*, *disjunção*, *implicação* e *equivalência*. Podem-se considerar também os símbolos

$$\top \qquad \bot$$

que são chamados de *verdade* e *falsidade*, mas não adotaremos eles neste livro. Os símbolos $\top$ e $\bot$ são operadores 0-ários, o símbolo $\neg$ é um operador 1-ário e os operadores $\wedge$, $\vee$, $\rightarrow$ e $\leftrightarrow$ são operadores 2-ários.

Os conectivos lógicos podem ser combinados com as proposições atômicas para formar outras proposições. Para isso, usam-se os símbolos

$$(\qquad)$$

que são os *parênteses inicial* e *final*, respectivamente. As regras de formação aceitas são que, se P e P' são proposições (atômicas ou não), então também são proposições

$$\neg P \qquad (P \wedge P') \qquad (P \vee P') \qquad (P \to P') \qquad (P \leftrightarrow P')$$

e os parênteses podem ser omitidos quando for claro o que se pretende dizer. Qualquer fórmula formada indutivamente por esses passos é uma proposição da linguagem.

Além disso, existem as regras de inferência ou dedução sintática, as regras que nos permitem, a partir de um conjunto de proposições Γ, deduzir outra proposição P. Denota-se isso por

$$\Gamma \vdash P$$

Adotaremos as seguintes regras. Para quaisquer proposições P, P' e P'', valem as seguintes deduções.

Introdução da Negação:

$$(P \to P'), (P \to \neg P') \vdash (\neg P)$$

Eliminação da Negação:

$$(\neg P) \vdash (P \to P')$$

Eliminação da Dupla-Negação:

$$(\neg\neg P) \vdash P$$

Introdução da Conjunção:

$$P, P' \vdash (P \wedge P')$$

Eliminações da Conjunção:

$$(P \wedge P') \vdash P$$

$$(P \wedge P') \vdash P'$$

Introduções da Disjunção:

$$P \vdash (P \vee P')$$

$$P' \vdash (P \vee P')$$

Eliminação da Disjunção:

$$(P \vee P'), (P \to P''), (P' \to P'') \vdash P''$$

Introdução da Equivalência:

$$(P \to P'), (P' \to P) \vdash (P \leftrightarrow P')$$

Eliminações da Equivalência:

$$(P \leftrightarrow P') \vdash (P \to P')$$

$$(P \leftrightarrow P') \vdash (P' \to P)$$

Introdução da Implicação:

$$(P \vdash P') \vdash (P \to P')$$

Eliminação da Implicação:

$$P, (P \to P') \vdash P'$$

A partir de um conjunto de proposições Γ, *deduzimos* uma proposição P com uma sequência finita de proposições obtidas de Γ usando as regras de inferência enunciadas.

1.1.2 Lógica de Ordem 1

A lógica de ordem 1 é uma linguagem formal. O *alfabeto* é composto por

1. letras latinas (em diferentes fontes e tamanhos)

$$a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z$$

$$A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z$$

2. letras gregas

$$\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta, \iota, \kappa, \lambda, \mu, \nu, \xi, o, \pi, \rho, \sigma, \tau, \upsilon, \phi, \chi, \psi, \omega$$

$$\Gamma, \Delta, \Theta, \Lambda, \Xi, \Pi, \Sigma, \Upsilon, \Phi, \Psi, \Omega$$

3. numerais arábicos
$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

4. símbolos lógicos (ou *operadores*)
$$\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \bigwedge, \bigvee$$

5. outros símbolos gráficos
$$(,), [,], \{, \}, |, ', ,$$

A *expressões básicas* podem ser

1. as *variáveis*, (em uma quantidade contável), representadas aqui por letras dos alfabetos latino e grego, possivelmente indexadas por outras letras ou numerais, ou pelo apóstrofe ';

2. as *constantes (individuais)* (em uma quantidade contável), representadas aqui por letras dos alfabetos latino e grego, possivelmente indexadas por outras letras ou numerais, ou pelo apóstrofe ', ou representadas por símbolos específicos;

3. para cada número natural n, os *predicados* n-ários (em uma quantidade contável), representadas aqui por letras dos alfabetos latino e grego, possivelmente indexadas por outras letras ou numerais, ou pelo apóstrofe ', ou representadas por símbolos específicos. Os predicados 0-ários são as *proposições* (ou *letras sentenciais*), os predicados 1-ários são as *propriedades* e os predicados 2-ários são as *relações*.

Não restringiremos quais letras representam o que, isso sempre ficará claro pelo contexto. De fato, a quantidade de símbolos de uma linguagem é finita, mas expressões formadas por eles são contáveis, mas não especificaremos esses detalhes aqui.

As *expressões bem formadas* da linguagem são

1. Os *termos*, que são as variáveis ou constantes individuais;

2. As *fórmulas*, expressões definidas recursivamente por

   (a) (Fórmulas simples ou atômica) Para um predicado n-ário P e termos $t_1, \cdots, t_n$, $P(t_1, \cdots, t_n)$ é uma fórmula;

   (b) (Fórmulas moleculares) Para fórmulas F e F', $\neg F$, $(F \wedge F')$, $(F \vee F')$, $(F \rightarrow F')$ e $(F \leftrightarrow F')$ são fórmulas. As fórmulas F e F' são *subfórmulas* dessas fórmulas;

(c) (Fórmulas gerais) Para fórmula F e variável v que ocorre em F, $(\bigwedge vF)$ e $(\bigvee vF)$ são fórmulas. A fórmula F é uma *subfórmula* dessas fórmulas;

(d) Nenhuma outra exressão é uma fórmula.

Uma *variável livre* de uma fórmula é definida recursivamente como

1. Para uma fórmula simples F e v uma variável, v é livre em F se, e somente se, v ocorre em F;

2. Para uma fórmula F da forma $\neg F'$, $(F' \wedge F'')$, $(F' \vee F'')$, $(F' \to F'')$, $(F' \leftrightarrow F'')$, e v uma variável, v é livre em F se, e somente se, é livre em F' ou em F'';

3. Para uma fórmula composta F da forma $\bigwedge v'F'$ ou $\bigvee v'F'$ e v uma variável, v é livre em F se, e somente se, v é livre em F' e v é diferente de v'. No caso em que v é livre em F' mas v é igual a v', a variável v está *ligada* ao quantificador $\bigwedge$ ou $\bigvee$, respectivamente.

Uma *sentença* (ou *fórmula fechada*) é uma fórmula sem variáveis livres. Uma *fórmula aberta* é uma fórmula que não é uma sentença.

Abreviações

Por simplicidade, os parênteses de fórmulas moleculares e gerais podem ser omitidos sempre que possível. Fórmulas gerais da forma $\bigwedge vF$ podem ser abreviadas por

$$\bigwedge_v F$$

e fórmulas gerais da forma $\bigvee vF$ podem ser abreviadas por

$$\bigvee_v F.$$

Ainda, para fórmulas F e F' e variável v livre em alguma das fórmulas, proposições categóricas do tipo

$$\bigwedge v(F \to F')$$

podem ser abriviadas por

$$\bigwedge_{v|F} F'$$

e proposições categóricas do tipo

$$\bigvee v(F \wedge F')$$

podem abreviadas por

$$\bigvee_{v|F} F'.$$

Esse é o modo em que pensamos nessas afirmações na linguagem natural e em matemática.

Regras de Inferência

As seguintes regras de inferência são definidas para fórmulas F e F', definimos as seguintes regras.

1. *Introdução da Negação*:

$$(F \to F'), (F \to \neg F') \vdash (\neg F)$$

2. *Eliminação da Negação*:

$$(\neg F) \vdash (F \to F')$$

3. *Eliminação da Dupla-Negação*:

$$(\neg\neg F) \vdash F$$

4. *Introdução da Conjunção*:

$$F, F' \vdash (F \wedge F')$$

5. *Eliminações da Conjunção*:

$$(F \wedge F') \vdash F$$

$$(F \wedge F') \vdash F'$$

6. *Introduções da Disjunção*:

$$F \vdash (F \vee F')$$

$$F' \vdash (F \vee F')$$

7. *Eliminação da Disjunção*:

$$(F \vee F'), (F \to F''), (F' \to F'') \vdash F''$$

8. *Introdução da Equivalência*:

$$(F \to F'), (F' \to F) \vdash (F \leftrightarrow F')$$

9. *Eliminações da Equivalência*:

$$(F \leftrightarrow F') \vdash (F \rightarrow F')$$

$$(F \leftrightarrow F') \vdash (F' \rightarrow F)$$

10. *Introdução da Implicação*:

$$(F \vdash F') \vdash (F \rightarrow F')$$

11. *Eliminação da Implicação*:

$$F, (F \rightarrow F') \vdash F'$$

Para uma fórmula F, uma variável v e um termo t tal que, ao substituirmos cada ocorrência livre de v em F por t, o termo t não é ligado a nenhum quantificador de F, denotamos a *substituição* de v por t na fórmula F por

$$F{\downarrow}_t^v\,,$$

comumente denotado $F[v/t]$.

1. *Introdução do Quantificador Universal*: Para fórmula F, variável v e termo t, t não ocorrente em premissa ou hipótese vigente,

$$F{\downarrow}_t^v \vdash \bigwedge vF$$

2. *Eliminação do Quantificador Universal*: Para fórmula F, variável v e termo t,

$$\bigwedge vF \vdash F{\downarrow}_t^v$$

3. *Introdução do Quantificador Particular*: Para fórmula F, variável v e termo t,

$$F{\downarrow}_t^v \vdash \bigvee vF$$

4. *Eliminação do Quantificador Particular*: Para fórmulas F e F', variável v e termo t, t não ocorrente em premissa ou hipótese vigente e t não ocorre em F',

$$(\bigvee vF), (F{\downarrow}_t^v \vdash F') \vdash F'$$

Os detalhes sobre essas regras de inferênncia não serão comentados, mas elas simplesmente formalizam as regras de inferência usuais na prática de matemática.

Igualdade e Unicidade

O predicado 2-ário mais importante em linguagens de lógica de ordem 1 é a *igualdade* $=$. Os detalhes sobre a definição e uso da igualdade não serão especificados aqui, mas basicamente para termos t e t', $t = t'$ é uma fórmula, e sempre que vale $t = t'$, pode-se substituir todos os t por t' em uma fórmula que ainda se tem uma fórmula equivalente. O símbolo *desigualdade* é uma abreviação para uma fórmula de negação de uma igualdade. Para termos t e t', a expressão

$$t \neq t'$$

abrevia a fórmula

$$\neg(t = t').$$

Com o conceito de igualdade, podemos definir o que significa que uma *única* constante c satisfaz uma propriedade P. Para uma propriedade P e uma variável v, a expressão

$$\bigvee! v P v$$

significa

$$\bigvee v(Pv \wedge \bigwedge v'(Pv' \to v' = v)).$$

Algumas definições equivalentes são

$$\bigvee v \bigwedge v'(Pv' \leftrightarrow v' = v),$$

que é mais breve, mas na prática mais difícil de se usar em demonstrações, e

$$\bigvee v(Pv \wedge \neg \bigvee v'(Pv' \wedge v' \neq v)),$$

e

$$\bigvee v P v \wedge \bigwedge v \bigwedge v'((Pv \wedge Pv') \to v = v').$$

1.1.3 Conjunto e Pertencimento

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 parcialmente formal, parcialmente 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 C pertence ao conjunto C'" ou "o conjunto C é elemento do conjunto C'" é denotada por

$$C \in C'.$$

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

Isso quer dizer que a teoria de conjuntos é uma teoria da lógica de ordem 1 com igualdade $=$ e um predicado 2-ário $\in$.

1.2 Axiomas do Vazio e da Extensão

1.2.1 Vazio e Igualdade

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.

Definição 1.1. Um conjunto *vazio* é um conjunto que não possui elementos.

Axioma 0 (Vazio)**.** Algum conjunto é vazio.

$$\bigvee C \bigwedge x(x \notin C)$$

O axioma não estabelece explicitamente a unicidade desse conjunto, mas ele é de fato único e é denotado $\emptyset$. Como o conjunto vazio não possui elementos, sempre que se conclui que existe um elemento em $\emptyset$, ou seja, que existe $x \in \emptyset$, chega-se em uma contradição e a conclusão é que o que se assumiu para chegar na contradição é falso. Essa é uma forma padrão de se demonstrarem diversas proposições na lógica e na matemática.

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

Axioma 1 (Extensão)**.** Sejam C e C' conjuntos. Os conjuntos C e C' são *iguais* se, e somente se, todo elemento de C pertence a C' e todo elemento de C' pertence a C. Denota-se $C = C'$.

$$\bigwedge C \bigwedge C'(C = C' \leftrightarrow \bigwedge x(x \in C \leftrightarrow x \in C'))$$

Caso contrário, denota-se $C \neq C'$.

$$\bigwedge C \bigwedge C'(C \neq C' \leftrightarrow \neg(C = C'))$$

O axioma da extensão nos permite provar a proposição afirmada anteriormente de que um único conjunto é vazio.

Proposição 1.1. *Um único conjunto é vazio.*

$$\bigvee! C \bigwedge x(x \notin C)$$

Demonstração. Sejam C e C' conjuntos vazios. Se $C \neq C'$, então (pelo axioma da extensão) para algum conjunto Y, $Y \in C$ e $Y \notin C'$, ou $Y \in C'$ e $Y \notin C$. O primeiro caso leva à contradição $Y \in C$ e o segundo caso leva à contradição $Y \in C'$, pois C e C' são vazios, não possuem elementos. Logo $C = C'$. ■

Definição 1.2. O único conjunto vazio é denotado $\emptyset$.

$$\bigwedge C(C = \emptyset \leftrightarrow \bigwedge x(x \notin C))$$

1.2.2 Subconjuntos

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 1.3. Seja C um conjunto. Um *subconjunto* (ou uma *parte*) de C é um conjunto C' tal que, para todo $x \in C'$, $x \in C$. Denota-se $C' \subseteq C$.

$$\bigwedge C \bigwedge C'(C' \subseteq C \leftrightarrow \bigwedge x(x \in C' \rightarrow x \in C))$$

Caso contrário, denota-se $Y \nsubseteq X$.

$$\bigwedge C \bigwedge C'(C' \nsubseteq C \leftrightarrow \neg C' \subseteq C)$$

Um subconjunto *próprio* de C é um subconjunto $C' \subseteq C$ tal que $C' \neq C$. Denota-se $C' \subset C$.

$$\bigwedge C \bigwedge C'(C' \subset C \leftrightarrow C' \subseteq C \wedge C' \neq C)$$

Com essa definição, o axioma da extensão pode ser reenunciado como

$$\bigwedge C \bigwedge C'(C = C' \leftrightarrow C \subseteq C' \wedge C' \subseteq C)$$

Proposição 1.2. *Para todo conjunto C,*

1. *O conjunto vazio é subconjunto de todo conjunto.*

$$\bigwedge C(\emptyset \subseteq C)$$

2. *O único subconjunto do conjunto vazio é ele mesmo.*

$$\bigwedge C(C \subseteq \emptyset \rightarrow C = \emptyset)$$

Demonstração. 1. Suponha que $\emptyset$ não é subconjunto de C. Então existe $x \in \emptyset$ tal que $x \notin C$. Mas $x \in \emptyset$ é uma contradição, o que mostra que $\emptyset \subseteq C$.

2. Exercício.

■

1.3 Axioma da Especificação

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

Axioma 2 (Especificação (Esquema))**.** Seja f uma fórmula com variáveis livres $x, C, v_0, \cdots, v_n$. Para todos $v_0, \cdots, v_n$ e todo conjunto C, algum conjunto S tem como seus únicos elementos os elementos de C tais que vale $f(x, C, v_0, \cdots, v_n)$.

$$\bigwedge v_0, \cdots, v_n \bigwedge C \bigvee S \bigwedge x(x \in S \leftrightarrow (x \in C \wedge f(x, C, v_0, \cdots, v_n)))$$

Proposição 1.3 (Unicidade da Especificação)**.** *Seja f uma fórmula com variáveis livres $x, C, v_0, \cdots, v_n$. Para todos $v_0, \cdots, v_n$ e todo conjunto C, um único conjunto S tem como seus únicos elementos os elementos de C tais que vale $f(x, C, v_0, \cdots, v_n)$.*

$$\bigwedge v_0, \cdots, v_n \bigwedge C \bigvee! S \bigwedge x(x \in S \leftrightarrow (x \in C \wedge f(x, C, v_0, \cdots, v_n)))$$

Demonstração. Sejam f, $x, C, v_0, \cdots, v_n$ como no enunciado. Pelo axioma da especificação, algum conjunto S tem como seus únicos elementos os elementos de C tais que vale $f(x, C, v_0, \cdots, v_n)$. Sejam S, S' conjuntos com essas propriedades. Mostraremos que $S = S'$. Seja x um conjunto. Então $x \in S$ é equivalente a $x \in C$ e $f(x, C, v_0, \cdots, v_n)$, o que é equivalente $x \in S'$. Pelo axioma da extensão, $S = S'$. ■

Definição 1.4. Seja f uma fórmula com variáveis livres $x, C, v_0, \cdots, v_n$. Para todos $v_0, \cdots, v_n$ e todo conjunto C, o único conjunto S que tem como seus únicos elementos os elementos de C tais que vale $f(x, C, v_0, \cdots, v_n)$ é denotado

$$\{x \in C \mid f(x, C, v_0, \cdots, v_n)\} := S.$$

Proposição 1.4. *Seja f uma fórmula com variáveis livres $x, C, v_0, \cdots, v_n$.*

$$\{x \in C \mid f(x, C, v_0, \cdots, v_n)\} \subseteq C.$$

Demonstração. Se $x \in S$, então $x \in C$ e $f(x, C, v_0, \cdots, v_n)$, logo $x \in C$, o que mostra que $S \subseteq C$. ■

1.4 Axioma das Partes

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

Axioma 3 (Partes)**.** Para todo conjunto C, algum conjunto tem todos os subconjuntos de C como elementos.

$$\bigwedge C \bigvee P \bigwedge p(p \subseteq C \to p \in P)$$

O conjunto cujos elementos precisamente pelos subconjuntos de um conjunto X é chamado de conjunto das partes de X e denotado $\mathsf{P}(X)$. O axioma das partes não estabelece explicitamente sua existência, mas podemos mostrar que ele existe usando o axioma da especificação, e mais precisamente mostrar que ele é único pela unicidade da especificação.

Proposição 1.5 (Conjuntos das Partes)**.** *Para todo conjunto C, um único conjunto tem exatamente os subconjuntos de C como elementos.*

$$\bigwedge C \bigvee! P \bigwedge p(p \subseteq C \leftrightarrow p \in P)$$

Demonstração. Seja C um conjunto. Pelo axioma das partes, algum conjunto Q satisfaz que, para todo $p \subseteq C$, $p \in Q$. Consideremos a fórmula $p \subseteq C$. Pela unicidade da especificação, existe único P definido como

$$P := \{p \in Q \mid p \subseteq C\}.$$ ■

O conjunto P não depende de Q pela unicidade da especificação.

Definição 1.5. Para todo conjunto C, o *conjunto das partes* de C é o único conjunto cujos elementos são os subconjuntos de C. Denota-se

$$\mathsf{P}(C) = \{p \mid p \subseteq C\}\,.$$

Proposição 1.6. *O conjunto das partes de um subconjunto de um conjunto é subconjunto do conjunto das partes do conjunto.*

$$\bigwedge C \bigwedge C'(C \subseteq C' \to \mathsf{P}(C) \subseteq \mathsf{P}(C'))$$

1.5 Axioma do Par

O próximo axioma garante, a partir da existência de dois conjuntos, 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 4 (Par)**.** Para todos conjuntos C e C', algum conjunto P tem como elementos C e C'.

$$\bigwedge C \bigwedge C' \bigvee P(C \in P \wedge C' \in P)$$

Como o axioma do conjunto vazio, o axioma da especificação e o axioma das partes, esse conjunto P não é explicitamente único pelo axioma do par. Devemos derivar a unicidade de um conjunto que tem exatamente os dois conjuntos como elementos a partir da unicidade da especificação.

Proposição 1.7. *Para todos conjuntos C e C', um único conjunto P tem como seus únicos elementos C e C'.*

$$\bigwedge C \bigwedge C' \bigvee! P \bigwedge x(x \in P \leftrightarrow x = C \vee x = C')$$

Demonstração. Pelo axioma do par, algum conjunto Q tem como elementos os conjunto C e C'. pela unicidade da especificação, definimos

$$P := \{x \in Q \mid x = C \vee x = C'\}\,. \qquad \blacksquare$$

Definição 1.6. Para todos conjuntos C e C', o *par* de C e C' é o único conjunto que tem como seus únicos elementos C e C'. Denota-se

$$\{C, C'\} = \{x \mid x = C \vee x = C'\}\,.$$

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 1.7. Seja C um conjunto. O *conjunto unitário* de elemento C é o par de C e C. Denota-se

$$\{C\} := \{C, C\}.$$

1.6 Axioma da União

1.6.1 União de um Conjunto

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

Axioma 5 (União)**.** Para todo conjunto C, algum conjunto tem como elementos os elementos que pertencem a algum elemento de C.

$$\bigwedge C \bigvee U \bigwedge x(\bigvee X(X \in C \wedge x \in X) \to x \in U)$$

Novamente, a unicidade de um conjunto que tem exatamente esses elementos segue do unicidade da especificação.

Proposição 1.8. *Para todo conjunto C, um único conjunto tem como seus únicos elementos os elementos que pertencem a algum elemento de C.*

$$\bigwedge C \bigvee! U \bigwedge x(\bigvee X(X \in C \wedge x \in X) \leftrightarrow x \in U)$$

Demonstração. Pelo axioma da união, existe V cujos elementos são os elementos que pertencem a algum elemento de C. Pela unicidade da especificação, definimos

$$U := \{x \in V \mid \bigvee X(X \in C \wedge x \in X)\}. \qquad \blacksquare$$

Definição 1.8. Para todo conjunto C, a *união* de C é o único conjunto que tem como seus únicos elementos os elementos que pertencem a algum elemento de C. Denota-se

$$\bigcup C = \{x \mid \bigvee X(X \in C \wedge x \in X)\}.$$

A união do par $\{C, C'\}$ e denotada $C \cup C'$.

Proposição 1.9. *1. A união do conjunto vazio é o conjunto vazio.*

$$\bigcup \emptyset = \emptyset$$

2. *A união de um subconjunto de um conjunto é subconjunto da união do conjunto.*

$$\bigwedge C \bigwedge C'(C \subseteq C' \to \bigcup C \subseteq \bigcup C')$$

3. *Todo elemento de um conjunto é subconjunto da união do conjunto.*

$$\bigwedge C \bigwedge X(X \in C \to X \subseteq \bigcup C)$$

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

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

1.6.2 Interseção de um Conjunto

A interseção de um conjunto não vazio de conjuntos denotado C é o conjunto cujos elementos pertencem a todos conjuntos que pertencem C. O conjunto interseção existe por consequêcia do axioma da especificação.

Proposição 1.10. *Para todo conjunto não vazio C, um único conjunto tem como elementos exatamente os elementos que pertencem a todos elementos de C.*

$$\bigwedge C \bigvee! I \bigwedge x(\bigwedge X(X \in C \to x \in X) \leftrightarrow x \in I)$$

Demonstração. Como C é não vazio, tome $X' \in C$. Pela unicidade da especificação, definimos

$$I := \{x \in X' \mid \bigwedge X(X \in C \to x \in X)\}. \qquad ■$$

Definição 1.9. Para todo conjunto não vazio C, a *interseção* de C é o único conjunto que tem como elementos exatamente os elementos que pertencem a todos elementos de C. Denota-se

$$\bigcap C = \{x \mid \bigwedge X(X \in C \to x \in X)\}.$$

A interseção do par $\{C, C'\}$ e denotada $C \cap C'$.

Proposição 1.11. *A interseção de um conjunto não vazio é subconjunto da interseção de um subconjunto não vazio do conjunto.*

$$\bigwedge C \bigwedge C'(C \neq \emptyset \wedge C' \neq \emptyset \wedge C \subseteq C' \to \bigcap C' \subseteq \bigcap C)$$

Demonstração. Seja $x \in \bigcap C'$. Então, para todo $X \in C'$, $x \in X$. Como $C \subseteq C'$, então todo para $X \in C$, $X \in C'$, logo $x \in \bigcap C$. ■

Proposição 1.12. *A interseção de um conjunto não vazio é subconjunto de todo elemento do conjunto.*

$$\bigwedge C \bigwedge X(C \neq \emptyset \wedge X \in C \to \bigcap C \subseteq X)$$

1.7 Axioma do Infinito

Definição 1.10. Seja C um conjunto. O *sucessor* de C é o conjunto

$$\vdash\!\!\dashv(C) := C \cup \{C\}.$$

Um conjunto *indutivo* é um conjunto que contém $\emptyset$ e contém o sucessor de cada um de seus elementos.

Axioma 6. Algum conjunto é indutivo.

$$\bigvee I(\emptyset \in I \wedge \bigwedge x \in I(\vdash\!\!\dashv(x) \in I))$$

Proposição 1.13. *Seja F um conjunto cujos elementos são conjuntos indutivos. $\bigcap F$ é indutivo.*

Demonstração. Como todo $C \in F$ é indutivo, para todo $C \in F$ vale $\emptyset \in C$, portanto $\emptyset \in \bigcap F$. Seja $x \in \bigcap F$. Então, para todo $C \in F$, $x \in C$ e, como C é indutivo, $\vdash\!\!\dashv(x) \in C$, logo $\vdash\!\!\dashv(x) \in \bigcap F$. Isso mostra que $\bigcap F$ é indutivo. ■

Proposição 1.14. *Um único conjunto indutivo é subconjunto de todo conjunto indutivo.*

Demonstração. Pelo axioma do infinito, algum conjunto I é indutivo. Consideremos o conjunto F dos subconjuntos indutivos de I:

$$F := \{C \in \mathsf{P}(I) \mid \emptyset \in C \wedge \bigwedge x \in C(\vdash\!\!\dashv(x) \in C)\}.$$

Definimos

$$\omega := \bigcap F.$$

O conjunto ω é indutivo pela proposição anterior. Mostremos que ω é subconjunto de todo conjunto indutivo. Seja J um conjunto indutivo. Consideremos o conjunto $\bigcap\{I, J\} = I \cap J$. Como I e J são indutivos, $I \cap J$ é indutivo pela proposição anterior; como $I \cap J \subseteq I$, $I \cap J \in F$, logo $\omega \subseteq I \cap J \subseteq J$. ■

Definição 1.11. O *conjunto dos números ordinais finitos* (ou *números naturais*) é o único conjunto indutivo que é subconjunto de todo conjunto indutivo. Denota-se esse conjunto por ω.

Proposição 1.15.

1. *(Princípio da Indução Finita) O único subconjunto indutivo de ω é ω;*
2. *Todo elemento de ω é o conjunto vazio ou o sucessor de um outro elemento.*

$$\bigwedge n(n \in \omega \to (n = \emptyset \vee \bigvee n'(n' \in \omega \wedge n = \vdash\!\!\dashv(n')))$$

Demonstração. Segue direto da definição de ω, pois se $I \subseteq \omega$ é indutivo, então $\omega \subseteq I$, logo $I = \omega$. ■

1.8 Axioma da Escolha

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

Pares Ordenados, Produto de Par e Função

Definição 1.12. Sejam X e Y conjuntos. O *par ordenado* com *primeira coordenada* X e *segunda coordenada* Y é o conjunto

$$(X, Y) := \{\{X\}, \{X, Y\}\} \in \mathsf{P}\left(\mathsf{P}\left(X \cup Y\right)\right).$$

Proposição 1.16. *Sejam X, Y, Z e W conjuntos. Então*

$$(X, Y) = (Z, W) \quad \Longleftrightarrow \quad X = Z \;\; e \;\; Y = W.$$

Definição 1.13. Sejam X e Y conjuntos. O *produto* de X por Y é o conjunto

$$X \times Y := \{(x, y) \in \mathsf{P}\left(\mathsf{P}\left(X \cup Y\right)\right) \mid x \in X \;\; \text{e} \;\; y \in Y\}.$$

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

Definição 1.14. Sejam X e Y conjuntos. Uma *função* de X para Y é um conjunto $f \subseteq X \times Y$ que satisfaz

$$\bigwedge x \in X \;\; \bigvee! y \in Y \qquad (x, y) \in f.$$

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

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

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

Proposição 1.17. *Seja $f : A \longrightarrow B$.*

1. $A = \emptyset \quad \Longleftrightarrow \quad f = \emptyset.$

2. $B = \emptyset \quad \Longrightarrow \quad A = \emptyset$.

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

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

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

■

O Axioma da Escolha e Produto de Conjuntos

Definição 1.15. Seja C um conjunto. O *produto* de C é o conjunto

$$\prod C := \left\{ f : C \longrightarrow \bigcup C \;\middle|\; \bigwedge X \in C \quad f(X) \in X \right\}.$$

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

Proposição 1.18. *Seja C um conjunto. Então*

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

Demonstração. 1. Como $C = \emptyset$, então $\bigcup \emptyset = \emptyset$. A função $\emptyset : \emptyset \longrightarrow \emptyset$ é uma função em $\prod C$, pois satisfaz por vacuidade que $\bigwedge X \in C \quad f(X) \in X$. 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 $f : C \longrightarrow \bigcup C$ satisfaz que $\bigwedge X \in C \quad f(X) \in X$. 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 $\prod C \neq \emptyset$.

1.9 Axiomas da Fundação e Substituição

Axioma 8 (Fundação)**.** Todo conjunto não vazio tem algum elemento com o qual sua interseção é vazia.

$$\bigwedge x(x \neq \emptyset \to \bigvee y(y \in x \wedge x \cap y = \emptyset))$$

Esse axioma é essencial na teoria de conjuntos, e também é conhecido como axioma da regularidade. Não estudaremos ele aqui.

Os axiomas da especificação e do par são consequência do axioma da substituição. Ele não será abordado aqui.

Propriedades Gerais

Contenção

Proposição 1.19. *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, $\bigwedge x \in X\ x \in Y$ e $\bigwedge y \in Y\ y \in X$, 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 1.20. *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 1.21. *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 1.22. *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 $F : I \longrightarrow C$. 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, $I = \{0, \ldots, n-1\}$ 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 simplesmennte 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 $F : C \longrightarrow C$ definida para todo $X \in C$ por $F(X) = X$. Desse modo, essa é uma indexação do conjunto X. Mas essa resposta não satisfaz a tradição de indexar um quantidade finita de conjuntos $\{X, Y\}$ com números naturais. A resposta menos óbvia é que todo conjunto pode ser bem ordenado e, dessa forma, existe uma função de um número ordinal para o conjunto, logo uma indexação desse conjunto por um número ordinal. Os números naturais são os números ordinais finitos, o que significa que essa resposta menos óbvia condiz com a idexação que se faz usualmente de uma quantidade finita de conjuntos. Esse tópicos, no entanto, não serão abordados nesse capítulo.

2.2 Propriedades de União e Interseção

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

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

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

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

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

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

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

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

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

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

■

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

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

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

1. $\displaystyle\bigcap_{i\in I} \mathsf{P}\,(C_i) = \mathsf{P}\left(\bigcap_{i\in I} C_i\right)$;

2. $\displaystyle\bigcup_{i\in I} \mathsf{P}\,(C_i) \subseteq \mathsf{P}\left(\bigcup_{i\in I} C_i\right)$.

2.3 Produto de Conjuntos

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

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

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

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

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).*

$$\begin{tikzcd} & \prod_{i\in I} C_i \arrow[d, "\pi_i"] \\ X \arrow[ur, dashed, "f"] \arrow[r, "f_i"'] & C_i \end{tikzcd}$$

Demonstração. Defina a função

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

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

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

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

2.4 Coproduto de Conjuntos

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

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

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

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

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).*

$$\begin{tikzcd} \bigsqcup_{i\in I} C_i \arrow[dr, dashed, "f"] & \\ C_i \arrow[u, "\iota_i"] \arrow[r, "f_i"'] & X \end{tikzcd}$$

Demonstração. Defina a função

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

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 $\overline{f} : \bigsqcup_{i\in I} C_i \longrightarrow X$ função tal que, para todo $i \in I$, $\overline{f} \circ \iota_i = f_i$. Seja $x \in \bigsqcup_{i\in I} C_i$. Existem $i \in I$ e $c \in C_i$ tais que $x = (i,c)$. Da propriedade comutativa de $\overline{f}$, segue que

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

Isso mostra que $\overline{f} = f$. ■

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

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

Demonstração. 1.

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

2.

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

■

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

Proposição 2.8. *Sejam X um conjunto, $(Y_i)_{i\in I}$ uma família de conjuntos, $(S_i)_{i\in I}$ uma família de subconjutos 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*

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

Demonstração. 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

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

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

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

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

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

$$S^{\complement} := X \setminus S.$$

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

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

2.5.1 Propriedades

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

1. $(X^{\complement})^{\complement} = X$;
2. $\emptyset^{\complement} = U$ *e* $U^{\complement} = \emptyset$;

3. $X \cap X^{\complement} = \emptyset$ *e* $X \cup X^{\complement} = U$*;*

4. $X \subseteq Y \iff Y^{\complement} \subseteq X^{\complement}$.

5. $(X \cup Y)^{\complement} = X^{\complement} \cap Y^{\complement}$ *e* $(X \cap Y)^{\complement} = X^{\complement} \cup Y^{\complement}$.

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 $\mathcal{P} \subseteq \mathsf{P}(X)$ 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 identidicamos um subconjunto de $\mathsf{P}(X)$ com uma família de sunconjuntos 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 $D \subseteq C_D$:

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

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

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

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 intergação de Riemmann. 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

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

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

$$\bigwedge a \in A \ \bigvee! b \in B \qquad (a, b) \in f.$$

Denota-se $f : A \longrightarrow B$. 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

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

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

Proposição 3.1. *Seja $f : A \longrightarrow B$ 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 $f : A \longrightarrow B$ e $g : A' \longrightarrow B'$. Então*

$$f = g \quad \Longleftrightarrow \quad A = A' \;\; e \;\; \bigwedge a \in A \quad f(a) = g(a).$$

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

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

O conjunto $f(A)$ é o *imagem* de f.

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

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

$$\begin{aligned} f|_{A'} \colon A' &\longrightarrow B \\ a &\longmapsto f(a). \end{aligned}$$

Proposição 3.4. *Sejam $f : A \longrightarrow B$, $A' \subseteq A$ 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 $f : A \longrightarrow B'$ e $g : B \longrightarrow C$ funções tais que $B' \subseteq B$. A *função composta* de g com f é a função

$$\begin{aligned} g \circ f \colon A &\longrightarrow C \\ a &\longmapsto g(f(a)). \end{aligned}$$

Proposição 3.5. *Sejam $f : A \longrightarrow B'$, $g : B \longrightarrow C'$ e $h : C \longrightarrow D$ 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 $f : A \longrightarrow B$. 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

$$\begin{aligned} \mathrm{I}_A \colon A &\longrightarrow A \\ a &\longmapsto a. \end{aligned}$$

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

$$f \circ \mathrm{I}_A = f \quad e \quad \mathrm{I}_B \circ f = f.$$

Demonstração. Primeiro, notemos que $f \circ \mathrm{I}_A$ e $\mathrm{I}_B \circ f$ 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 $\mathrm{I}_\emptyset = \emptyset$. 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, $f \circ \mathrm{I}_A$ é uma função de $\emptyset$ em B e, portanto, $f \circ \mathrm{I}_A = \emptyset = f$. Ainda, $\mathrm{I}_B \circ f$ é uma função de $\emptyset$ em B e, portanto, $\mathrm{I}_B \circ f = \emptyset = f$. Se $A \neq \emptyset$, seja $a \in A$. Então $(f \circ \mathrm{I}_A)(a) = f(\mathrm{I}_A(a)) = f(a) = \mathrm{I}_B(f(a)) = (\mathrm{I}_B \circ f)(a)$. ■

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

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

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

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

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 conjunto. 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 $g \circ f = \mathrm{I}_A$.*

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

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

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 $g : B \longrightarrow A$ para cada elemento de B como $g(b) := a$. Assim, segue que $g \circ f = \mathrm{I}_B$. ■

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

Proposição 3.11. *Sejam $f : A \longrightarrow B'$ e $g : B \longrightarrow C$ 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 $f : A \longrightarrow B$ e $g : B \longrightarrow C$ 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 $f : A \longrightarrow B$ 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 $f : A \longrightarrow B$ uma função, $B' \subseteq B$ e $(B_i)_{i \in I} \subseteq \mathsf{P}(B)$ uma família de subconjuntos de B. Então*

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

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

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

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

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

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

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

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

3.5 Propriedades de Imagem e Imagem Inversa

Proposição 3.14. *Sejam $f : D \longrightarrow C$ uma função e $(C_i)_{i\in I}$ uma família de subconjuntos de C. Então*

1. $f(\emptyset) = \emptyset$;

2. $f(D) \subseteq C$;

3. $f\left(\bigcup_{i\in I} C_i\right) = \bigcup_{i\in I} f(C_i)$;

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

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

3. Se $f\left(\bigcup_{i\in I} C_i\right) = \emptyset$, então $\bigcup_{i\in I} C_i = \emptyset$. Assim, segue que, para todo $i \in I$, $C_i = \emptyset$ e temos que $f(C_i) = \emptyset$. Portanto $\bigcup_{i\in I} f(C_i) = \emptyset$. Caso contrário, seja $d \in f\left(\bigcup_{i\in I} C_i\right)$. Então existe $c \in \bigcup_{i\in I} C_i$ tal que $f(c) = d$ e, consequentemente, existe $i \in I$ tal que $c \in C_i$. Assim, segue que $d = f(c) \in f(C_i) \subseteq \bigcup_{i\in I} f(C_i)$.

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

■

Proposição 3.15. *Sejam $f : D \longrightarrow C$ uma função, $X \subseteq D$ e $Y \subseteq C$. Então*

1. $X \subseteq f^{-1}(f(X))$.

2. $X = f^{-1}(f(X))$ *se f é injetiva.*

3. $f(f^{-1}(Y)) \subseteq Y$.

4. $f(f^{-1}(Y)) = Y$ *se f é sobrejetiva.*

Demonstração. 1. Seja $x \in X$. Então $f(x) \in f(X)$, o que implica que $x \in f^{-1}(f(X))$.

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

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

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

■

3.6 Os Funtores Imagem e Imagem Inversa

Podemos entender a imagem e a imagem inversa de funções como funções definidas no conjunto das partes do domínio de contradomínio da função, como a seguir.

Seja $f\colon C \longrightarrow C'$ uma função. A função imagem de f é a função

$$\begin{aligned} \mathsf{P}_\star(f)\colon \mathsf{P}(C) &\longrightarrow \mathsf{P}(C') \\ A &\longmapsto f(A) = \{f(a) \mid a \in A\} \end{aligned}$$

e a função imagem inversa de f é a função

$$\begin{aligned} \mathsf{P}^\star(f)\colon \mathsf{P}(C') &\longrightarrow \mathsf{P}(C) \\ B &\longmapsto f^{-1}(B) = \{c \in C \mid f(c) \in B\}\,. \end{aligned}$$

Sendo assim, elas satisfazem as seguintes propriedades funtoriais.

Proposição 3.16 (Imagem é funtor covariante)**.** *1. Para todo conjunto C,*

$$\mathsf{P}_\star(\mathrm{I}_C) = \mathrm{I}_{\mathsf{P}(C)};$$

2. Para todos conjuntos C, C', C'' e todas funções $f\colon C \longrightarrow C'$ e $f'\colon C' \longrightarrow C''$,

$$\mathsf{P}_\star(f' \circ f) = \mathsf{P}_\star(f') \circ \mathsf{P}_\star(f).$$

Demonstração. 1. Para todo $A \in \mathsf{P}(C)$,

$$\mathsf{P}_\star(\mathrm{I}_c)(A) = \{\mathrm{I}_C(a) \mid a \in A\} = \{a \mid a \in A\} = A,$$

portanto $\mathsf{P}_\star(\mathrm{I}_C) = \mathrm{I}_{\mathsf{P}(C)}$.

2. Para todo $A \in \mathsf{P}(C)$,

$$\begin{aligned} \mathsf{P}_\star(f' \circ f)(A) &= \{f' \circ f(a) \mid a \in A\} \\ &= \{f'(f(a)) \mid a \in A\} \\ &= \mathsf{P}_\star(f')(\{f(a) \mid a \in A\}) \\ &= \mathsf{P}_\star(f')(\mathsf{P}_\star(f)(A)) \\ &= (\mathsf{P}_\star(f') \circ \mathsf{P}_\star(f))(A), \end{aligned}$$

portanto $\mathsf{P}_\star(f' \circ f) = \mathsf{P}_\star(f') \circ \mathsf{P}_\star(f)$.

■

Proposição 3.17 (Imagem inversa é funtor contravariante)**.** *1. Para todo conjunto C,*

$$\mathsf{P}_\star(\mathrm{I}_C) = \mathrm{I}_{\mathsf{P}(C)};$$

2. *Para todos conjuntos C, C', C'' e todas funções $f\colon C \longrightarrow C'$ e $f'\colon C' \longrightarrow C''$,*

$$\mathsf{P}_\star(f' \circ f) = \mathsf{P}_\star(f) \circ \mathsf{P}_\star(f').$$

Demonstração. 1. Para todo $A \in \mathsf{P}(C)$,

$$\mathsf{P}^\star(\mathrm{I}_c)(A) = \{c \in C \mid \mathrm{I}_C(c) \in A\} = \{c \in C \mid c \in A\} = A,$$

portanto $\mathsf{P}^\star(\mathrm{I}_C) = \mathrm{I}_{\mathsf{P}(C)}$.

2. Para todo $A \in \mathsf{P}(C'')$,

$$\begin{aligned}
\mathsf{P}^\star(f' \circ f)(A) &= \{c \in C \mid f' \circ f(c) \in A\} \\
&= \{c \in C \mid f'(f(c)) \in A\} \\
&= \left\{c \in C \;\middle|\; f(c) \in \mathsf{P}^\star(f')(A)\right\} \\
&= \left\{c \in C \;\middle|\; c \in \mathsf{P}^\star(f)(\mathsf{P}^\star(f')(A))\right\} \\
&= \left\{c \in C \;\middle|\; c \in \mathsf{P}^\star(f) \circ \mathsf{P}^\star(f')(A)\right\} \\
&= \mathsf{P}^\star(f) \circ \mathsf{P}^\star(f')(A),
\end{aligned}$$

portanto $\mathsf{P}_\star(f' \circ f) = \mathsf{P}_\star(f') \circ \mathsf{P}_\star(f)$.

■

Proposição 3.18. *Seja $f\colon C \longrightarrow C'$ uma função.*

1. $\mathrm{I}_{\mathsf{P}(C)} \subseteq \mathsf{P}^\star \circ \mathsf{P}_\star(f)$;
2. $\mathrm{I}_{\mathsf{P}(C)} = \mathsf{P}^\star \circ \mathsf{P}_\star(f)$ *se f é injetiva;*
3. $\mathsf{P}_\star \circ \mathsf{P}^\star(f) \subseteq \mathrm{I}_{\mathsf{P}(C')}$;
4. $\mathsf{P}_\star \circ \mathsf{P}^\star(f) = \mathrm{I}_{\mathsf{P}(C')}$ *se f é sobrejetiva.*

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

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

4.1 Relações de Equivalência

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

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

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

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

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 $P := A/\sim$. Claramete, $\emptyset \nsubseteq P$. 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

$$\bigwedge a_1, a_2 \in A \qquad a_1 \sim a_2 \Leftrightarrow \bigvee Q \in P \quad a_1, a_2 \in Q,$$

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 $\mathsf{P}(A)$ é uma relação de ordem parcial em $\mathsf{P}(A)$.*

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

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

é uma relação de ordem parcial nos naturais.

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

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

é uma ordem parcial em X.

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

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

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

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

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

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

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

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

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

é uma ordem estrita em X.

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

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

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

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

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

é uma ordem parcial em X.

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

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

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

4.2.2 Conjuntos Parcialmente Ordenados

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

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

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

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

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

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

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

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

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

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

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

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

Dualmente, se Y e Z têm menor elemento,

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

Demonstração. Vamos mostrar que $\max Y \in \{\max Z\} \cup (Y \smallsetminus Z)$. Como $\max Y \in Y$, $\max Y \notin (Y \smallsetminus Z)$ 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 $\max Y \in \{\max Z\} \cup (Y \smallsetminus Z)$. Agora vamos mostrar que $\{\max Z\} \cup (Y \smallsetminus Z)$ tem maior elemento $\max Y$. Seja $y \in \{\max Z\} \cup (Y \smallsetminus Z)$. Se $y = \max Z$, como $Z \subseteq Y$, então $y \leq \max Y$. Se $y \in (Y \smallsetminus Z)$, como $(Y \smallsetminus Z) \in Y$, então $y \leq \max Y$. Portanto $\max Y = \max(\{\max Z\} \cup (Y \smallsetminus Z))$. ■

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

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

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

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

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

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

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

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

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

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

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

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

...

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

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

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

Dualmente, se Y e Z têm ínfimo,

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

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

4.2.3 Funções Monótonas

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

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

4.2.4 Cadeias e Lema de Zorn

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

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

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

Demonstração. ... ■

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

4.2.5 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 $x, x' \in X$,

$$x \sim x' \quad \Longleftrightarrow \quad x \preceq x' \ \text{ e } \ x' \preceq x.$$

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

$$[x] \leq [x'] \quad \Longleftrightarrow \quad x \preceq x'.$$

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 $x_0, \ldots, x_{n-1} \in X$. 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 $x_1, x_1 \in X$, o conjunto $\{x_1, x_2\}$ tem supremo e ínfimo, denotados, respectivamente, $x_1 \vee x_2$ e $x_1 \wedge x_2$.

Proposição 4.15. *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 $\mathcal{A} \subseteq \mathsf{P}(A)$ um conjunto de partes de A que satisfaz*

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

Então $(\mathcal{A}, \cup, \cap)$ é uma álgebra booleana.

Demonstração. Primeiramente, é necessário notar, embora os símbolos $\cup$ e $\cap$ não sejam funções propriamente ditas, ao fixarmos um conjunto A, podemos definir $\cup$ e $\cap$ como operações binárias em $\mathsf{P}(A)$, dadas por $(X, Y) \longmapsto X \cup Y$ e $(X, Y) \longmapsto X \cap Y$, respectivamente. Para $X, Y \in \mathcal{A}$, temos que $X \cup Y, X \cap Y \in \mathcal{A}$, o que mostra que as operações estão bem definidas.

Sendo assim, podemos prosseguir com a demonstração. Se $\mathcal{A}$ satisfaz as propriedades do enunciado, então $A = \emptyset^{\complement} \in \mathcal{A}$. O par $(\mathcal{A}, \cup)$ é um magma comutativo com elemento neutro $\emptyset$, pois a união de dois cojuntos é comutativa por definição e a união de um conjunto qualquer com o conjunto vazio dá o próprio conjunto. Da mesma forma, o par $(\mathcal{A}, \wedge)$ é um magma comutativo com elemento neutro A, pois a interseção de dois conjuntos é comutativa por definição e a interseção de qualquer conjunto com o conjunto A é o próprio conjunto. Ainda, vale que, para todo $X, Y, Z \in \mathcal{A}$, $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ e $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$;

ou seja, as operações binárias $\cup$ e $\cap$ são distributivas uma sobre a outra. Por fim, nota-se que, dado $X \in \mathcal{A}$, $X^{\complement} \in \mathcal{A}$ e vale $X \cup X^{\complement} = A$ e $X \cap X^{\complement} = \emptyset$. Logo $(\mathcal{A}, \cup, \cap)$ é uma álgebra booleana. ■

Proposição 4.19 (Princípio da Dualidade)**.** *Toda afirmação dudutível somente a partir da definição de álgebra booleana continua válida se são trocados entre si os símbolos* $\vee$ *e* $\wedge$ *e os símbolos* 0 *e* 1 *que aparecem na expressão.*

Demonstração. Todas as propriedades de uma álgebra booleana são definidas simetricaente e continuam iguais se trocamos entre si os símbolos $\vee$ e $\wedge$ e os símbolos 0 e 1. Logo isso também vale para qualquer afirmação dedutível dessas propriedades. ■

Como consequência do princípio da dualidade, qualquer afirmação dedutível das pripriedades de álbegra booleana tem uma afirmação associadad a ela ao trocarmos entre si os símbolos $\vee$ e $\wedge$ e os símbolos 0 e 1, que chamaremos que sua afirmação *dual*. Claramente, a afirmação dual da dual é a própria afirmação. Portanto só será necessário demonstrar a afirmação para demonstrar sua afirmação dual. Toda proposição, lema e teorema dessa seção exibirá sua proposição, lema e teorema dual, mas a afirmação dual não será demonstrada.

Teorema 4.20 (Identidades)**.** *Seja* $(A, \vee, \wedge)$ *uma álgebra booleana. Então*

$$\bigwedge a \in A \qquad a \vee 1 = 1$$

$$\bigwedge a \in A \qquad a \wedge 0 = 0$$

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

$$\bigwedge a, b \in A \qquad a \vee (a \wedge b) = a$$

$$\bigwedge a, b \in A \qquad a \wedge (a \vee b) = a$$

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

$$\bigwedge a \in A \qquad a \vee a = a$$

$$\bigwedge a \in A \qquad a \wedge a = a$$

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

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

$$(A, \vee) \text{ é associativo.}$$

$$(A, \wedge) \text{ é associativo.}$$

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*

$$\bigwedge a, b \in A \qquad (a \wedge b)' = a' \vee b'$$

$$\bigwedge a, b \in A \qquad (a \vee b)' = a' \wedge b'$$

Função Indicadora

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

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

A função indicadora é uma bijeção e mostra que os conjuntos $\mathsf{P}(X)$ e 2^X têm a mesma cardinalidade. De fato, sabemos que $(\mathsf{P}(X), \cap, \cup, \emptyset, X)$ é uma álgebra de conjuntos. Podemos também, usando a estrutura de álgebra em $\{0,1\}$, dada pelas operações mínimo e máximo $\wedge, \vee \colon \{0,1\} \times \{0,1\} \longrightarrow \{0,1\}$ 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 $\mathbf{1} \colon \mathsf{P}(X) \longrightarrow 2^X$ é um ismomorfismo de álgebras.

Proposição 4.28. *Seja* X *um conjunto. A função indicadora* $\mathbf{1} \colon \mathsf{P}(X) \longrightarrow 2^X$ *de* X *é um isomorfismo entre as álgebras* $(\mathsf{P}(X), \cap, \cup, \emptyset, X)$ *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 $C, C' \in \mathsf{P}(X)$, $\mathbf{1}_{C \cap C'} = \mathbf{1}_C \wedge \mathbf{1}_{C'}$, $\mathbf{1}_{C \cup C'} = \mathbf{1}_C \vee \mathbf{1}_{C'}$, 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. $\mathbf{1}_{A^{\complement}} = 1 - \mathbf{1}_A$;
2. $\mathbf{1}_{A \setminus B} = \mathbf{1}_A - \mathbf{1}_A \mathbf{1}_B$;
3. $\mathbf{1}_{A \triangle B} = \mathbf{1}_A + \mathbf{1}_B - 2\mathbf{1}_A \mathbf{1}_B$;
4. $\mathbf{1}_{\bigcap_{i \in [n]} A_i} = \bigtimes_{i \in [n]} \mathbf{1}_{A_i}$;
5. $\mathbf{1}_{\bigcup_{i \in [n]} A_i} = \bigplus_{\substack{S \subseteq [n] \\ S \neq \emptyset}} \left((-1)^{|S|-1} \bigtimes_{i \in S} \mathbf{1}_{A_i} \right)$;
6. $\mathbf{1}_{\triangle_{i \in [n]} A_i} = \bigplus_{\substack{S \subseteq [n] \\ S \neq \emptyset}} \left((-2)^{|S|-1} \bigtimes_{i \in S} \mathbf{1}_{A_i} \right)$;

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

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

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

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

Demonstração.

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

■

De certa forma, essa proposição mostra que a noção de cardinalidades iguais se comporta como uma relação de equivalência. Não podemos dizer que $=$ é, de fato, uma relação de equivalência porque nao existe um conjunto de todos os conjuntos no qual defini-la. Todas proposições sobre cardinalidades são, na verdade, proposições sobre funções entre conjutos e convém saber que as propriedades acima valem.

5.1.2 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 $C : X \longrightarrow Y$.

   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 $C : X \longrightarrow Y$.

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 $E : X \longrightarrow \mathbb{N}$ 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. $|X| \leq |Y|$ *e* $|Y| \leq |X| \Rightarrow |X| = |Y|$*;*

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

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

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

2. Teorema de Cantor-Schröder-Bernstein.

3. $|X| \leq |Y|$ e $|Y| \leq |Z|$, então existem funções injetivas $C_1 : X \longrightarrow Y$ e $C_2 : Y \longrightarrow Z$. Mas então $C_2 \circ C_1 : X \longrightarrow Z$ 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. $|X|^{|Y|} := \left|X^Y\right|$.

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

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

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 $c \in C_i$. ■

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 $f_i : C_i \longrightarrow C$ bijeção. Considere a função

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

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

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

■

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 $f_i : C \longrightarrow C_i$. Considere a função

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

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 $f_i : C_i \longrightarrow C$. Considere a função

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

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 $\boldsymbol{N} = (N, 0, \vdash\!\!\dashv)$ em que

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

O *um* de $\boldsymbol{N}$ é o elemento $1 := \vdash\!\!\dashv(0)$.

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

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

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

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

6.1.1 Adição

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

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

que satisfaz

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

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 $I := \{n \in N : \bigvee! n_3 \in N \quad n_1 + n = n_3\}$. 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 $\Vdash$ é função, $\Vdash(n_3) = \Vdash(n_1 + n) \in N$ é único e tomando $n_1 + \Vdash(n) = \Vdash(n_1 + n)$, concluímos que $\Vdash(n) \in I$ 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

$$n_1 +_1 \Vdash(n) = \Vdash(n_1 +_1 n) = \Vdash(n_1 +_2 n) = n_1 +_2 \Vdash(n),$$

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

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

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

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

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

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

Agora, seja $n \in I$. Então

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

o que implica $\mathrm{H}(n) \in I$. Logo $I = N$. ■

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

$$\bigwedge n \in N \qquad \mathrm{H}(n) = n + 1.$$

Demonstração. Seja $n \in N$. Então

$$\mathrm{H}(n) = \mathrm{H}(n + 0) = n + \mathrm{H}(0) = n + 1.$$

■

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

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

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

   $$0 + \mathrm{H}(n) = 0 + (n + 1) = (0 + n) + 1 = n + 1 = \mathrm{H}(n),$$

   o que implica que $\mathrm{H}(n) \in I$ 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

   $$1 + \mathrm{H}(n) = 1 + (n + 1) = (1 + n) + 1 = (n + 1) + 1 = \mathrm{H}(n) + 1,$$

   o que implica que $\mathrm{H}(n) \in I$ e, portanto, $I = N$.

■

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

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

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

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

Agora, seja $n \in I$. Então

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

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

6.1.2 Multiplicação

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

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

que satisfaz

1. *(M1)* $\bigwedge n \in N \qquad n \times 0 = 0$*;*
2. *(M2)* $\bigwedge n_1, n_2 \in N \qquad n_1 \times \vdash\!\!\dashv(n_2) = (n_1 \times n_2) + n_1.$

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 $I := \{n \in N : \bigvee! n_3 \in N \quad n_1 \times n = n_3\}$. Primeiro, notemos que $0 \in I$, pois $n_1 \times 0 = 0$ e, portanto, n_3 esxite e é único. Agora, seja $n \in I$. Então existe único $n_3 \in N$ tal que $n_1 \times n = n_3$ e, como $+$ é função, $n_3 + n_1 = n_1 \times n + n$ é único e tomando $n_1 \times \vdash\!\!\dashv(n) = n_1 \times n + n_1$, concluímos que

$\mathrm{H}(n) \in I$ e, portanto, $I = N$. Logo $\times$ está bem definida. Agora, devemos mostrar que $\times$ é única. Sejam $\times_1, \times_2 : N \times N \longrightarrow N$ 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

$$n_1 \times_1 \mathrm{H}(n) = n_1 \times_1 n + n_1 = n_1 \times_2 n + n_1 = n_1 \times_2 \mathrm{H}(n),$$

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

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

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

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

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

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

o que implica que $\mathrm{H}(k) \in I$ 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

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

o que implica que $\mathrm{H}(k) \in I$ e, portanto, que $I = N$.

■

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

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

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

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

Agora, seja $k \in I$. Então

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

o que implica que $\mathrm{H}(k) \in I$ e, portanto, que $I = N$. ■

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

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

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

$$0 \times \mathrm{H}(n) = (0 \times n) + 0 = 0 + 0 = 0,$$

o que mostra que $\mathrm{H}(n) \in N$ 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

$$1 \times \vdash\!\!\dashv(n) = (1 \times n) + 1 = n + 1 = \vdash\!\!\dashv(n),$$

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

■

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

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

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

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

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

6.1.3 Ordenação

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

1. $\bigwedge n, m, k \in N \qquad n + k = m + k \quad \Longrightarrow \quad n = m;$

2. $\bigwedge n, m \in N \qquad n + m = 0 \quad \Longrightarrow \quad n = m = 0.$

Demonstração. 1. Seja $I := \{k \in N : \bigwedge n, m \in N \quad n + k = m + k \quad \Longrightarrow \quad n = m\}$. 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 $n + \vdash\!\!\dashv(k) = m + \vdash\!\!\dashv(k)$, então $\vdash\!\!\dashv(n + k) = \vdash\!\!\dashv(m + k)$ e, como $\vdash\!\!\dashv$ é injetiva, $n + k = m + k$, o que implica que $n = m$ e, assim, temos que $\vdash\!\!\dashv(k) \in I$ 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 $m = \vdash\!\!\dashv(k)$ e segue que $n + m = n + \vdash\!\!\dashv(k) = \vdash\!\!\dashv(n + k) = 0$, o que é absurdo, pois $\vdash\!\!\dashv^{-1}(\{0\}) = \emptyset$. Logo $n = m = 0$.

■

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

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

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

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

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

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

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

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

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

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

então $I = N$*.*

Demonstração. Seja $I \subseteq N$ e suponha que $0 \in I$ e $\{m \in N : m < n\} \subseteq I \quad \Longrightarrow$ $\vdash\!\!\dashv(n) \in I$. Então ■

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

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

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

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

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

6.1.4 Bases

O número *zero*, representado por 0, é a constante definida na estrutura de $\boldsymbol{N} = (N, 0, \vdash\!\!\!\dashv)$. O número *um* (já definido anteriormente) e os números *dois*, *três*, *quatro*, *cinco*, *seis*, *sete*, *oito*, *nove*, *dez* e *onze*, são definidos, na ordem respectiva, por

$$\begin{aligned}
1 &:= \vdash\!\!\!\dashv(0)\\
2 &:= \vdash\!\!\!\dashv(1)\\
3 &:= \vdash\!\!\!\dashv(2)\\
4 &:= \vdash\!\!\!\dashv(3)\\
5 &:= \vdash\!\!\!\dashv(4)\\
6 &:= \vdash\!\!\!\dashv(5)\\
7 &:= \vdash\!\!\!\dashv(6)\\
8 &:= \vdash\!\!\!\dashv(7)\\
9 &:= \vdash\!\!\!\dashv(8)\\
\mathcal{Z} &:= \vdash\!\!\!\dashv(9)\\
\mathcal{E} &:= \vdash\!\!\!\dashv(\mathcal{Z}).
\end{aligned}$$

O número *doze* ou a *dúzia* é o número $\vdash\!\!\!\dashv(\mathcal{E})$. Esses são os caracteres usados na representação numérica de base doze, ou seja, a representação dos números naturais que define doze símbolos para representar os primeiros números:

$$\vdash\!\!\!\dashv(\mathcal{E}) = |\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathcal{Z}, \mathcal{E}\}|\,.$$

Para representar a dúzia, definimos $10 := \vdash\!\!\!\dashv(\mathcal{E})$. Note que isso é uma notação e não deve ser confundida, claro, com o produto 1×0. Formalmente, a representação é uma sequência $r \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathcal{Z}, \mathcal{E}\}^{\mathbb{N}}$ com finitas entradas diferentes de 0.

Evidentemente, a representação mais usual dos números naturais é a representação decimal, ou de base dez. Nesse caso $\mathcal{Z}$ é representado por 10 e existem somente dez símbolos, pois os símbolos $\mathcal{Z}$ e $\mathcal{E}$ não são usados para representar dez e onze.

Na base doze, os caracteres que usamos são:

A tabela de multiplicação é:

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

0	1	2	3	4	5	6	7	8	9	ƧƐ	ƐƐ	10
1	1	2	3	4	5	6	7	8	9	ƧƐ	ƐƐ	10
2	2	4	6	8	ƧƐ	10	12	14	16	18	21	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	ƧƐ	13	18	21	26	32	34	39	42	47	50
6	6	10	16	20	26	30	36	40	46	50	56	60
7	7	12	19	24	32	36	41	48	53	25	65	70
8	8	14	20	28	34	40	48	54	60	68	74	80
9	9	16	23	30	39	46	53	60	69	76	83	90
ƧƐ	ƧƐ	18	26	34	42	50	25	68	76	84	92	02
ƐƐ	ƐƐ	21	29	38	47	56	65	74	83	92	12	03
10	10	20	30	40	50	60	70	80	90	02	03	100

6.2 Números Inteiros

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

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

é uma relação de equivalência.

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

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

$$Z := {}^{N \times N}\big/_{\sim},$$

o *conjunto dos números inteiros.*

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

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

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

6.2.1 Adição e Subtração

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

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

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

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

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

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

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

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. ■

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

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

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

1. Como $(0, 0) \in 0$, então $(n_1, n_2) + (0, 0) = (n_1, n_2)$, logo $n + 0 = n$.
2. Notemos que

$$\begin{aligned} ((n_1, n_2) + (m_1, m_2)) + (k_1, k_2) &= (n_1 + m_1, n_2 + m_2) + (k_1, k_2) \\ &= (n_1 + m_1 + k_1, n_2 + m_2 + k_2) \\ &= (n_1, n_2) + (m_1 + k_1, m_2 + k_2) \\ &= (n_1, n_2) + ((m_1, m_2) + (k_1, k_2)), \end{aligned}$$

logo $(n + m) + k = n + (m + k)$.

3. Notemos que

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

logo $n + m = m + n$.

■

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned}
&(n_1m_1 + n_2m_2 + n_2'm_1' + n_1'm_2') + (n_1m_2' + n_2m_1' + n_1m_1' + n_2m_2') \\
&= n_1(m_1 + m_2') + n_2(m_2 + m_1') + (n_2' + n_1)m_1' + (n_1' + n_2)m_2' \\
&= n_1(m_1' + m_2) + n_2(m_2' + m_1) + (n_2 + n_1')m_1' + (n_1 + n_2')m_2' \\
&= (n_2m_1 + n_1m_2 + n_1'm_1' + n_2'm_2') + (n_1m_2' + n_2m_1' + n_1m_1' + n_2m_2'),
\end{aligned}$$

o que implica que

$$n_1m_1 + n_2m_2 + n_2'm_1' + n_1'm_2' = n_2m_1 + n_1m_2 + n_1'm_1' + n_2'm_2'$$

e, portanto, $(n_1m_1 + n_2m_2, n_2m_1 + n_1m_2) \sim (n_1'm_1' + n_2'm_2', n_2'm_1' + n_1'm_2')$, o que mostra que o produto $n \times m$ está bem definido. ■

6.2.3 Ordenação

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

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

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

Parte 2

Álgebra

Capítulo 1

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.

1.1 Operações Binárias

Definição 1.1. Seja X um conjunto não vazio. Uma *operação binária* em X é uma função

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

Proposição 1.1 (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 1.2. Seja X um conjunto. Uma operação binária *associativa* é uma operação binária $* : X \times X \longrightarrow X$ 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 $* : X \times X \longrightarrow X$ que satisfaz, para todos $x_1, x_2 \in X$

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

Definição 1.3. 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 $x_1, x_2, x_3 \in X$,

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

1.2 Magma

Definição 1.4. Um *magma* é um par $\boldsymbol{X} = (X, *)$ em que X é um conjunto não vazio e $*$ é uma operação binária em X.

Definição 1.5 (Identidade)**.** Seja $\boldsymbol{X} = (X, *)$ um magma. Uma *identidade* com respeito a $*$ é um elemento $\mathrm{I} \in X$ que satisfaz, para todo $x \in X$,

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

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

Proposição 1.2. *Seja $\boldsymbol{X} = (X, *)$ 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

$$\mathrm{I}_1 = \mathrm{I}_1 * \mathrm{I}_2 = \mathrm{I}_2.$$

■

Definição 1.6 (Operação com conjuntos)**.** Sejam $\boldsymbol{X}$ um magma, $A, B \subseteq X$ e $x \in X$. Definimos

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

1.3 Semigrupo

Definição 1.7. Um *semigrupo* é um magma $\boldsymbol{X} = (X, *)$ em que $*$ é associativa. Um semigrupo *comutativo* é um semigrupo em que $*$ é comutativa.

Definição 1.8. Seja $\boldsymbol{X} = (X, *)$ um semigrupo, $n \in \mathbb{N}^*$ e $(x_i)_{i\in[n]}$ elementos de X. O *operatório* desses elementos é

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

Notação. Costumamos denotar essa operação por

$$x_{n_1} * \cdots * x_0 := \mathop{\ast}_{i\in[n]} x_i = (x_{n-1} * (\cdots (x_1 * x_0)))$$

O símbolo usado para a soma $+$ é o *somatório* $\mathop{+}$ e o símbolo usado para o produto $\times$ é o *produtório* $\mathop{\times}$. 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 as ordens fossem devidamente trocadas.

Proposição 1.3. *Sejam $\boldsymbol{X} = (X, *)$ um semigrupo, $n, k \in \mathbb{N}^*$ e $(x_i)_{i\in[n+k]}$ elementos de X. Então*

$$\mathop{\ast}_{i\in[n+k]} x_i = \mathop{\ast}_{i\in[k]} x_{n+i} * \mathop{\ast}_{i\in[n]} x_i.$$

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

$$\mathop{\ast}_{i\in[n+1]} x_i = x_n * \mathop{\ast}_{i\in[n]} x_i = \mathop{\ast}_{i\in[1]} x_{n+i} * \mathop{\ast}_{i\in[n]} x_i.$$

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

$$\begin{aligned} \mathop{\ast}_{i\in[n+k+1]} x_i &= x_{n+k} * \mathop{\ast}_{i\in[n+k]} x_i \\ &= x_{n+k} * \left(\mathop{\ast}_{i\in[k]} x_{n+i} * \mathop{\ast}_{i\in[n]} x_i \right) \\ &= \left(x_{n+k} * \mathop{\ast}_{i\in[k]} x_{n+i} \right) * \mathop{\ast}_{i\in[n]} x_i \\ &= \mathop{\ast}_{i\in[k+1]} x_{n+i} * \mathop{\ast}_{i\in[n]} x_i. \end{aligned}$$

■

Proposição 1.4 (Associatividade Generalizada)**.** *Sejam* $\boldsymbol{X} = (X, *)$ *um semigrupo,* $n \in \mathbb{N}^*$*,* $(x_i)_{i\in[n]}$ *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*

$$\mathop{\ast}_{i\in[n]} x_i = \mathop{\ast}_{j\in[p]} \left(\mathop{\ast}_{i\in[k_j]} x_{i+k_0+\cdots+k_{j-1}} \right).$$

Demonstração. Segue por indução da proposição anterior. ■

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

$$\mathop{\ast}_{j\in[p]} \left(\mathop{\ast}_{i\in[k_j]} x_{i+k_0+\cdots+k_{j-1}} \right) = \left(\mathop{\ast}_{i\in[k_{p-1}]} x_{i+k_0+\cdots+k_{p-2}} \right) * \cdots * \left(\mathop{\ast}_{i\in[k_0]} x_i \right)$$

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

Proposição 1.5 (Comutatividade Generalizada)**.** *Sejam* $\boldsymbol{X} = (X, *)$ *um semigrupo comutativo e* $n \in \mathbb{N}^*$*. Então, para toda bijeção* $\psi\colon [n] \longrightarrow [n]$*,*

$$\mathop{\ast}_{i\in[n]} x_{\psi(i)} = \mathop{\ast}_{i\in[n]} x_i.$$

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 $\psi\colon [n+1] \longrightarrow [n+1]$ uma bijeção. Definamos $k = \psi^{-1}(n)$ e a bijeção

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

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

que

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

■

1.4 Homomorfismo de Semigrupos

Definição 1.9. Sejam $\boldsymbol{X}_1 = (X_1, *_1)$ e $\boldsymbol{X}_2 = (X_2, *_2)$ semigrupos. Um *homomorfismo de semigrupos* de $\boldsymbol{X}_1$ para $\boldsymbol{X}_2$ é uma função $h : X_1 \longrightarrow X_2$ que satisfaz, para todos $x, x' \in X_1$

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

Denota-se $h : \boldsymbol{X}_1 \longrightarrow \boldsymbol{X}_2$.

Proposição 1.6 (Composição de homomorfismos)**.** *Sejam $\boldsymbol{X}_1 = (X, *_1)$, $\boldsymbol{X}_2 = (X_2, *_2)$ e $\boldsymbol{X}_3 = (X_3, *_3)$ semigrupos e $h_1 : \boldsymbol{X}_1 \longrightarrow \boldsymbol{X}_2$ e $h_2 : \boldsymbol{X}_2 \longrightarrow \boldsymbol{X}_3$ homomorfismos de semigrupos. Então $h_2 \circ h_1 : \boldsymbol{X}_1 \longrightarrow \boldsymbol{X}_3$ é homomorfismo de semigrupos.*

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

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

■

1.5 Monoide

Definição 1.10. Um *monoide* é uma tripla $\boldsymbol{M} = (M, *, \mathrm{I})$ 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 $\boldsymbol{M}$ por I_M quando houver ambiguidade. Ainda, como existe identidade, definimos

$$\mathop{\ast}_{i\in[0]} x_i = \mathrm{I}.$$

Exemplo 1.1. *O conjunto* $\mathbb{N}$*, com a operação binária*

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

e a identidade 0*, formam um monoide comutativo.*

Definição 1.11 (Inverso)**.** Sejam $\boldsymbol{X} = (X, *)$ 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

$$\overline{x} * x = \mathrm{I} = x * \overline{x}.$$

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

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

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 iguadades da esquerda e da direita acima, mas não adotaremos essa distinção neste livro.

Proposição 1.7. *Seja* $(M, *, \mathrm{I})$ *um monoide. Se* $m \in M$ *tem inverso com respeito* $*$ *e* I*, ele é único.*

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

$$\overline{m} = \overline{m} * \mathrm{I} = \overline{m} * (m * \overline{\overline{m}}) = (\overline{m} * m) * \overline{\overline{m}} = \mathrm{I} * \overline{\overline{m}} = \overline{\overline{m}}. \qquad \blacksquare$$

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 1.8. *Seja* $(M, *, \mathrm{I})$ *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 1.12. Seja $\boldsymbol{M} = (M, *, \mathrm{I})$ um monoide. Um *submonoide* de $\boldsymbol{M}$ é um monoide $\boldsymbol{S} = (S, *_S, \mathrm{I}_S)$ em que $S \subseteq M$, $*_S = *|_{S\times S}$ e $\mathrm{I}_S = \mathrm{I}$. Denota-se $\boldsymbol{S} \leq \boldsymbol{M}$. Um submonoide *próprio* de $\boldsymbol{M}$ é um monoide $\boldsymbol{S} \leq \boldsymbol{M}$ em que S é um subconjunto próprio de M ($S \subset M$). Denota-se $\boldsymbol{S} < \boldsymbol{M}$.

Proposição 1.9. *Sejam $\boldsymbol{M} = (M, *, \mathrm{I})$ um monoide e $S \subseteq M$ um conjunto tal que*

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

Então $\boldsymbol{S} = (S, *|_{S\times S}, \mathrm{I})$ é um monoide. Ainda, se $\boldsymbol{M}$ é comutativo, então $\boldsymbol{S}$ é comutativo.

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

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 (1.1). (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 $\mathrm{I} \in S$, da identidade de $*$ segue que

$$\mathrm{I} \star s = \mathrm{I} * s = s = s * \mathrm{I} = s \star \mathrm{I}.$$

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

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

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

Logo $\star$ é comutativa. ■

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

1.6 Homomorfismos de Monoides

Definição 1.13. Sejam $\boldsymbol{M}_1 = (M_1, *_1, \mathrm{I}_1)$ e $\boldsymbol{M}_2 = (M_2, *_2, \mathrm{I}_2)$ monoides. Um *homomorfismo de monoides* de $\boldsymbol{M}_1$ para $\boldsymbol{M}_2$ é uma função $h : M_1 \longrightarrow M_2$ que satisfaz

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

Denota-se $h : \boldsymbol{M}_1 \longrightarrow \boldsymbol{N}_2$.

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

Demonstração.

1. Como homomorfismos de monoides são homomorfismos de semigrupos, o resultado segue da proposição na seção de semigrupos que afirma que composição de homomorfismos é homomorfismo (1.6).
2. Para mostrar que a identidade é preservada, basta notar que

$$(h_2 \circ h_1)(\mathrm{I}_1) = h_2(h_1(\mathrm{I}_1)) = h_2(\mathrm{I}_2) = \mathrm{I}_3.$$

■

Capítulo 2

Grupos

2.1 Construções Algébricas

2.1.1 Grupo e Subgrupo

Definição 2.1. Um *grupo* é uma quádrupla $\boldsymbol{G} = (G, *, \mathrm{I}, ^{-1})$ em que G é um conjunto, $* : G \times G \longrightarrow G$ é uma operação binária associativa, $\mathrm{I} \in G$ é uma identidade com respeito a $*$ e $^{-1} : G \longrightarrow G$ 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 $g \in G$,

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

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

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

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 $\boldsymbol{G} = (G, *, \mathrm{I}, ^{-1})$ em que $(G, *, \mathrm{I})$ é um monoide e $^{-1} : G \longrightarrow G$ é uma operação unária inversa com respeito a $*$ e I.

Definição 2.2. Sejam $\boldsymbol{G} = (G, *)$ um grupo, $g \in G$ e $n \in \mathbb{N}$. Definimos

$$g^n := \mathop{\ast}_{i=1}^{n} g \quad \text{e} \quad g^{-n} := \mathop{\ast}_{i=1}^{n} g^{-1}.$$

Proposição 2.1 (Leis de corte e inversão)**.** *Seja $\boldsymbol{G}$ um grupo. Então*

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

Demonstração. Se $gg_1 = gg_2$, então

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

A demonstração da segunda implicação é análoga. ■

Definição 2.3. Seja $\boldsymbol{G} = (G, *, \mathrm{I}, ^{-1})$ um grupo. Um *subgrupo* de $\boldsymbol{G}$ é um grupo $\boldsymbol{S} = (S, *_S, \mathrm{I}_S, ^{-1_S})$ em que $S \subseteq G$, $*_S = *|_{S\times S}$, $\mathrm{I}_S = \mathrm{I}$ e $^{-1} = {}^{-1_S}$. Denota-se $\boldsymbol{S} \leq \boldsymbol{G}$. Um subgrupo *próprio* de $\boldsymbol{G}$ é um subgrupo $\boldsymbol{S} \leq \boldsymbol{G}$ em que S é um conjunto próprio de G ($S \subset G$). Denota-se $\boldsymbol{S} < \boldsymbol{G}$.

Proposição 2.2. *Sejam $\boldsymbol{G}$ 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 $\boldsymbol{S} = (S, *|_{S\times S})$ é um grupo. Ainda, se $\boldsymbol{G}$ é comutativo, então $\boldsymbol{S}$ 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 (1.1). (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 $\mathrm{I} = s * s^{-1} \in S$ e, como I é identidade de $\boldsymbol{G}$, segue que, para todo $s \in S$,

$$\mathrm{I} \star s = \mathrm{I} * s = s = s * \mathrm{I} = s \star \mathrm{I}.$$

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

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

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

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

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

■

Proposição 2.3. *Sejam $\boldsymbol{G}$ um grupo e $\mathcal{G}$ o conjunto dos subgrupos de $\boldsymbol{G}$. Então $(\mathcal{G}, \leq)$ é um conjunto parcialmente ordenado.*

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

Proposição 2.4. *Seja $\boldsymbol{G}$ um grupo. Então $\{\mathrm{I}\}$ e $\boldsymbol{G}$ são subgrupos de $\boldsymbol{G}$.*

Proposição 2.5. *Sejam $\boldsymbol{G}$ um grupo, $(\boldsymbol{S}_i)_{i \in I}$ uma família de subgrupos de $\boldsymbol{G}$ e*

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

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

Demonstração. (SG1) Para todo $i \in I$, $\boldsymbol{S_i} \leq \boldsymbol{G}$, 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 $\boldsymbol{S_i} \leq \boldsymbol{G}$, segue que $s_1 s_2 \in S_i$, o que implica que $s_1 s_2 \in S$. (SG3) Seja $s \in S$. Para todo $i \in I$, $s \in S_i$ e, como $\boldsymbol{S_i} \leq \boldsymbol{G}$, segue que $s^{-1} \in S_i$, o que implica que $s^{-1} \in S$. ■

Proposição 2.6. *Sejam $\boldsymbol{G}$ um grupo, $(\boldsymbol{S}_i)_{i \in I}$ uma família superiormente dirigida de subgrupos de $\boldsymbol{G}$ (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 $\boldsymbol{S}$ é um subgrupo de $\boldsymbol{G}$.

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

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

Definição 2.4. Seja $\boldsymbol{M}$ um monoide. O conjunto dos elementos invertíveis de M é denotado por M^*.

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

Proposição 2.7. *Seja* $\boldsymbol{M} = (M, *, \mathrm{I})$ *um monoide. Então existe uma operação unária* $^{-1} : M^* \longrightarrow M^*$ *tal que* $\boldsymbol{M^*} = (M^*, *|_{M^* \times M^*}, \mathrm{I}, ^{-1})$ *é um grupo.*

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

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

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 $\mathrm{I} \in M^*$, pois $\mathrm{I} * \mathrm{I} = \mathrm{I}$. Como M^* é contém a identidade e fechado sob $*$, segue que $(M^*, *, \mathrm{I})$ é um monoide (1.9). Por fim, $\boldsymbol{M^*}$ é um grupo pois, por definição, todo elemento tem inverso e ele é único. ■

Definição 2.5. Sejam $\boldsymbol{G}$ um grupo e $g \in G$. A *conjugação* por g é a função

$$\begin{aligned} C_g \colon G &\longrightarrow G \\ h &\longmapsto ghg^{-1}. \end{aligned}$$

A *translação à direita* por g é a função

$$\begin{aligned} D_g \colon G &\longrightarrow G \\ h &\longmapsto hg. \end{aligned}$$

A *translação à esquerda* por g é a função

$$\begin{aligned} E_g \colon G &\longrightarrow G \\ h &\longmapsto gh. \end{aligned}$$

2.1.2 Coclasses e Índice de Subgrupo

Definição 2.6. Sejam $\boldsymbol{G}$ um grupo, $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo e $g \in G$. A *coclasse à esquerda* de $\boldsymbol{S}$ em $\boldsymbol{G}$ com *representante* g é o conjunto

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

A *coclasse à direita* de $\boldsymbol{S}$ em $\boldsymbol{G}$ 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 2.8. *Sejam $\boldsymbol{G}$ um grupos, $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo e $g_1 g_2 \in G$. Então*

1. $g_1(g_2S) = (g_1g_2)S$ *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 $\boldsymbol{S}$ é subgrupo, segue que $g_2^{-1}g_1 = s's^{-1} \in S$.

   ($\Rightarrow$) ($\subseteq$) Se $g_2^{-1}g_1 \in S$, existe $s \in S$ tal que $g_2^{-1}g_1 = s$, portanto $g_1 = g_2s$, logo $g_1 \in g_2S$. Assim, dado $g \in g_1S$, existe $s' \in S$ tal que $g = g_1s'$. Como $\boldsymbol{S}$ é subgrupo, $ss' \in S$, logo $g = g_2ss' \in g_2S$. ($\supseteq$) Da mesma forma, como $\boldsymbol{S}$ é subgrupo, $g_1^{-1}g_2 = (g_2^{-1}g_1)^{-1} = s^{-1} \in S$, o que implica que $g_2 = g_1s^{-1} \in g_1S$. Assim, dado $g \in g_2S$, existe $s' \in S$ tal que $g = g_2s'$. Como $\boldsymbol{S}$ é subgrupo, $s^{-1}s' \in S$, logo $g = g_1s^{-1}s' \in g_2S$.

■

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

$$|g_1 S| = |g_2 S|\,.$$

Demonstração. Considere a relação

$$\begin{aligned} f\colon g_1 S &\longrightarrow g_2 S \\ g &\longmapsto g_2 g_1^{-1} g. \end{aligned}$$

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

$$\begin{aligned} f^{-1}\colon g_2 S &\longrightarrow g_1 S \\ g &\longmapsto g_1 g_2^{-1} g, \end{aligned}$$

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

■

Proposição 2.10. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo. A relação binária $\sim$ em G definida por*

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

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

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

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

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

Definição 2.7. Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo. O *conjunto quociente* de $\boldsymbol{G}$ por $\boldsymbol{S}$ é o conjunto

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

Definição 2.8. Seja $\boldsymbol{G}$ um grupo e $\boldsymbol{S} \leq \boldsymbol{G}$ subgrupo. O *índice* de $\boldsymbol{S}$ em $\boldsymbol{G}$ é número cardinal

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

Proposição 2.11. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{S} \leq \boldsymbol{G}$ um subgrupo. Então*

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

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

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

Da segunda condição, temos por 5.3 que

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

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

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

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

2.1.3 Subgrupo Normal e Grupo Quociente

Definição 2.9. Seja $\boldsymbol{G}$ um grupo. Um subgrupo *normal* de $\boldsymbol{G}$ é um subgrupo $\boldsymbol{N} \leq \boldsymbol{G}$ que satsfaz

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

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

Proposição 2.12. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{N} \leq \boldsymbol{G}$ um subgrupo. São equivalentes:*

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

Proposição 2.13. *Seja* $\boldsymbol{G}$ *um grupo. Então* $\{\boldsymbol{e}\}$ *e* $\boldsymbol{G}$ *são subgrupos normais de* $\boldsymbol{G}$.

Proposição 2.14. *Sejam* $\boldsymbol{G}$ *um grupo,* $(\boldsymbol{N}_i)_{i\in I}$ *uma família de subgrupos normais de* $\boldsymbol{G}$ *e*

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

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

Demonstração. (Subgrupo) Como $(\boldsymbol{N}_i)_{i\in I}$ uma família de subgrupos de $\boldsymbol{G}$, segue que $\boldsymbol{N}$ é um subgrupo de $\boldsymbol{G}$ (2.5). (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 2.15. *Sejam* $\boldsymbol{G}$ *um grupo,* $(\boldsymbol{N}_i)_{i\in I}$ *uma família superiormente dirigida de subgrupos normais de* $\boldsymbol{G}$ *(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 $\boldsymbol{N}$ *é um subgrupo normal de* $\boldsymbol{G}$.

Demonstração. (Subgrupo) Como $(\boldsymbol{N}_i)_{i\in I}$ uma família superiormente dirigida de subgrupos de $\boldsymbol{G}$, segue que $\boldsymbol{N}$ é um subgrupo de $\boldsymbol{G}$ (2.6). (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 2.10. Seja $\boldsymbol{G}$ um grupo e $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ um subgrupo normal. O *grupo quociente* de $\boldsymbol{G}$ por $\boldsymbol{N}$ é a quádrupla $\boldsymbol{G/N} = (G/N, *, \mathrm{I}N, ^{-1})$, em que G/N é o conjunto quociente de G pela relação de equivalência induzida por N,

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

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

Uma notação um pouco mais cuidadosa ressaltaria que as operações binárias de $\boldsymbol{G}$ e de $\boldsymbol{G/N}$ não são a mesma e, se denotarmos a primeira como $*$ e a segunda como $\star$, teríamos a definição acima nos dando $g_1N \star g_2N := (g_1 * g_2)N$. No entanto, como $*$ de G/N está sempre relacionada a $*$ de G, mantemos a mesma notação para ambas e a mesma convenção de omiti-la quando possível. Vale notar, também, que pela associatividade da $*$ de $\boldsymbol{G}$, temos que $g_1g_2N = g_1(g_2N) = (g_1g_2)N$. O mesmo vale para $^{-1}$.

Proposição 2.16. *Seja $\boldsymbol{G}$ um grupo e $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ um subgrupo normal. Então $\boldsymbol{G/N}$ é um grupo.*

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

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

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

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

(identidade) Seja $g \in G$. Então

$$[\mathrm{I}][g] = [\mathrm{I}g] = [g] = [g\mathrm{I}] = [g][\mathrm{I}].$$

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

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

■

2.1.4 Homomorfismo de Grupo

Definição 2.11. Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos. Um *homomorfismo de grupos* de $\boldsymbol{G_1}$ para $\boldsymbol{G_2}$ é uma função $h : G_1 \longrightarrow G_2$ que satisfaz, para todos $g_1, g_2 \in G_1$,

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

Denota-se $h : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$. O conjunto desses homomorfismos é denotado $\mathcal{H}\mathrm{om}(\boldsymbol{G_1}, \boldsymbol{G_2})$.

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

Proposição 2.17 (Homomorfismos preservam a estrutura algébrica)**.** *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos $h : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$ um homomorfismo de grupos. Então*

1. $h(\mathrm{I}_1) = \mathrm{I}_2$;

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

Demonstração. Seja $g \in G_1$. Então

1.

$$\begin{aligned} h(\mathrm{I}_1) &= h(\mathrm{I}_1)\mathrm{I}_2 \\ &= h(\mathrm{I}_1)h(g)h(g)^{-1} \\ &= h(\mathrm{I}_1 g)h(g)^{-1} \\ &= h(g)h(g)^{-1} \\ &= \mathrm{I}_2. \end{aligned}$$

2.

$$\begin{aligned} h(g)^{-1} &= h(g)^{-1}\mathrm{I}_2 \\ &= h(g)^{-1}h(\mathrm{I}_1) \\ &= h(g)^{-1}h(gg^{-1}) \\ &= h(g)^{-1}h(g)h(g^{-1}) \\ &= \mathrm{I}_2 h(g^{-1}) \\ &= h(g^{-1}). \end{aligned}$$

■

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

Proposição 2.18 (Composição de homomorfismos)**.** *Sejam* $\boldsymbol{G_1}$, $\boldsymbol{G_2}$ *e* $\boldsymbol{G_3}$ *grupos e* $h_1 : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$ *e* $h_2 : \boldsymbol{G_2} \longrightarrow \boldsymbol{G_3}$ *homomorfismos de grupos. Então* $(h_2 \circ h_1) : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_3}$ *é um homomorfismo de grupos.*

Demonstração. Como um homomorfismo de grupos é um homomorfismo de semigrupos, o resultado segue da proposição na seção de semigrupos que afirma que composição de homomorfismos é homomorfismo (1.6). ■

Proposição 2.19. *Sejam* $\boldsymbol{G}$ *um grupo e* $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ *um subgrupo normal. A projeção canônica* $\pi : G \longrightarrow G/N$, *definida por*

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

é um homomorfismo de grupos sobrejetivo.

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

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

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

Proposição 2.20. *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$ um homomorfismo de grupos. Se $\boldsymbol{S} \leq \boldsymbol{G_2}$ é um subgrupo, então $\boldsymbol{h^{-1}(S)} \leq \boldsymbol{G_1}$ é um subgrupo, e se $\boldsymbol{N} \trianglelefteq \boldsymbol{G_2}$ é um subgrupo normal, então $\boldsymbol{h^{-1}(N)} \trianglelefteq \boldsymbol{G_1}$ é um subgrupo normal.*

Demonstração. (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 $\boldsymbol{S}$ é subgrupo, $h(s_1)h(s_2) \in S$. Logo, como h é homomorfismo, $h(s_1 s_2) = h(s_1)h(s_2) \in S$ e, portanto, $s_1 s_2 \in h^{-1}(S)$. (SG3) Seja $s \in h^{-1}(S)$. Então $h(s) \in S$ e, como $\boldsymbol{S}$ é subgrupo, $h(s)^{-1} \in S$. Como h é homomorfismo, segue que $h(s^{-1}) = h(s)^{-1} \in S$ e, portanto, $s^{-1} \in h^{-1}(S)$. (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 $\boldsymbol{N}$ é subgrupo normal, segue que $h(g)h(n)h(g)^{-1} \in N$. Logo $gng^{-1} \in h^{-1}(N)$. ■

Proposição 2.21. *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$ um homomorfismo de grupos. Se $\boldsymbol{S} \leq \boldsymbol{G_1}$, então $\boldsymbol{h(S)} \leq \boldsymbol{G_2}$, e se h é sobrejetivo e $\boldsymbol{N} \trianglelefteq \boldsymbol{G_1}$ um subgrupo normal, então $\boldsymbol{h(N)} \trianglelefteq \boldsymbol{G_2}$.*

Demonstração. (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 $\boldsymbol{S}$ é subgrupo, segue que $s_1' s_2' \in S$ e, como h é homomorfismo, segue que

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

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

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

■

2.1.5 Núcleo, Imagem e Isomorfismo

Definição 2.12. Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$ um homomorfismo de grupos. O *núcleo* de h é o conjunto

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

e a *imagem* de h é o conjunto

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

Proposição 2.22. *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$ um homomorfismo de grupos. Então h é injetiva se, e somente se,* $\mathrm{nuc}(h) = \{\mathrm{I}_1\}$.

Demonstração. ($\Rightarrow$) Suponha que h é injetiva. Seja $n \in \mathrm{nuc}(h)$. Então $h(n) = \mathrm{I}_2$. Mas $h(\mathrm{I}_1) = \mathrm{I}_2$ e, como h é injetiva, concluímos que $n = \mathrm{I}_1$.
($\Leftarrow$) Suponha que $\mathrm{nuc}(h) = \{\mathrm{I}_1\}$. Sejam $g_1, g_2 \in G_1$. Se $h(g_1) = h(g_2)$, temos que $h(g_1 g_2^{-1}) = h(g_1)h(g_2)^{-1} = \mathrm{I}_2$, o que implica que $g_1 g_2^{-1} = \mathrm{I}_1$, pois $\mathrm{nuc}(h) = \{\mathrm{I}_1\}$. Logo $g_1 = g_2$, e concluímos que h é injetiva. ■

Definição 2.13. Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos. Um *isomorfismo de grupos* é um homomorfismo de grupos invertível. O conjunto de todos esses ismorfismos é denotado por $\mathcal{I}\mathrm{so}(\boldsymbol{G_1}, \boldsymbol{G_2})$.

Proposição 2.23. *Sejam $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ grupos e $h : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$ um isomorfimo de grupos. Então $h^{-1} : \boldsymbol{G_2} \longrightarrow \boldsymbol{G_1}$ é um isomorfismo de grupos.*

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

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

■

Definição 2.14. Grupo *isomorfos* são grupos $\boldsymbol{G_1}$ e $\boldsymbol{G_2}$ para os quais existe isomorfismo $h : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$. Denota-se $\boldsymbol{G_1} \simeq \boldsymbol{G_2}$.

Proposição 2.24. *Sejam $\boldsymbol{G_1}$, $\boldsymbol{G_2}$ e $\boldsymbol{G_3}$ grupos. Então*

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

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

2. A inversa é um isomorfismo de grupos (2.23).

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.

2.1.6 Teoremas de Isomorfismo

Teorema 2.25 (1º teorema de isomorfismo)**.** *Sejam* $\boldsymbol{G_1}$ *e* $\boldsymbol{G_2}$ *grupos e* $h : \boldsymbol{G_1} \longrightarrow \boldsymbol{G_2}$ *um homomorfismo de grupos. Então* $\mathbf{nuc}\,(\boldsymbol{h}) \trianglelefteq \boldsymbol{G_1}$, $\mathbf{im}\,(\boldsymbol{h}) \leq \boldsymbol{G_2}$ *e*

$$\boldsymbol{G_1}\big/_{\mathbf{nuc}(\boldsymbol{h})} \simeq \mathbf{im}\,(\boldsymbol{h}).$$

Demonstração. Como $\mathrm{nuc}(h) = h^{-1}(e_2)$ e $\{\boldsymbol{e_2}\} \trianglelefteq \boldsymbol{G_2}$ (2.13), a proposição segue da proposição 2.20. Como $\mathrm{im}(h) = h^(G_1)$ e $\boldsymbol{G_1} \leq \boldsymbol{G_1}$ (2.13), a proposição segue da proposição 2.20. Por causa disso, $\boldsymbol{G_1}/\,\mathbf{nuc}\,(\boldsymbol{h})$ e $\mathbf{im}\,(\boldsymbol{h})$ são grupos. Consideremos a função

$$\begin{aligned} \eta\colon G_1/\,\mathrm{nuc}(h) &\longrightarrow \mathrm{im}(h) \\ g\,\mathrm{nuc}(h) &\longmapsto h(g). \end{aligned}$$

Primeiro mostremos que η é função. Sejam $g_1, g_2 \in G_1$ tais que $g_1\,\mathrm{nuc}(h) = g_2\,\mathrm{nuc}(h)$. Então $g_2^{-1}g_1 \in \mathrm{nuc}(h)$ (2.8), 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 $\eta(g_1\,\mathrm{nuc}(h)) = \eta(g_1\,\mathrm{nuc}(h))$.

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

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

Por fim, devemos mostrar que η é bijetivo. (Injetividade) Seja $[g] \in \mathrm{nuc}(\eta)$. Então $\eta([g]) = \mathrm{I}_2$, logo $h(a) = \mathrm{I}_2$. Mas isso implica que $g \in \mathrm{nuc}(h)$. Portanto $[g] = [\mathrm{I}_1]$, e segue que $\mathrm{nuc}(\eta) = \{[\mathrm{I}_1]\}$, o que é equivalente à injetividade (2.22). (Sobrejetividade) Para todo $g \in \mathrm{im}(h)$, existe $g' \in G_1$ tal que $g = h(g')$. Mas $h(g') = \eta(g'\,\mathrm{nuc}(h))$, e segue a sobrejetividade. ■

Teorema 2.26 (2º teorema de isomorfismo)**.** *Sejam* $\boldsymbol{G}$ *um grupo,* $\boldsymbol{S} \leq \boldsymbol{G}$ *um subgrupo e* $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ *um subgrupo normal. Então* $\boldsymbol{SN} \leq \boldsymbol{G}$, $\boldsymbol{S} \cap \boldsymbol{N} \trianglelefteq \boldsymbol{S}$ *e*

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

Teorema 2.27 (3º teorema de isomorfismo)**.** *Sejam* $\boldsymbol{G}$ *um grupo e* $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ *um subgrupo normal. Então*

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

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

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

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

2.2 Construções Categóricas

2.2.1 Produto de Grupos

Definição 2.15. Seja $(\boldsymbol{G_i})_{i\in I} = (G_i, *_i, \mathrm{I}_i, ^{-1})_{i\in I}$ uma família de grupos. O *produto* da família $(\boldsymbol{G_i})_{i\in I}$ é a quádrupla

$$\prod_{i\in I} \boldsymbol{G_i} := (G, *, \mathrm{I}, ^{-1}),$$

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

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

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

Proposição 2.28. *Seja $(\boldsymbol{G_i})_{i\in I}$ uma família de grupos. Então o produto $\prod_{i\in I} \boldsymbol{G_i}$ é um grupo. Se para todo $i \in I$ $\boldsymbol{G_i}$ é comutativo, então $\prod_{i\in I} \boldsymbol{G_i}$ é comutativo.*

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

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

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

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

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

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

(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 2.29. *Seja $(\boldsymbol{G_i})_{i\in I}$ 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 2.30 (Propriedade Universal)**.** *Sejam* $(\boldsymbol{G_i})_{i\in I}$ *uma família de grupos,* $\boldsymbol{X}$ *um grupo e, para todo* $i \in I$, $h_i : \boldsymbol{X} \longrightarrow \boldsymbol{G_i}$ *um homomorfismo de grupos. Então existe um único homomorfismo de grupos* $h : \boldsymbol{X} \longrightarrow \prod_{i\in I} \boldsymbol{G_i}$ *tal que, para todo* $i \in I$, $\pi_i \circ h = h_i$ *(o diagrama comuta).*

$$\begin{tikzcd}
 & \prod\limits_{i\in I} \boldsymbol{G_i} \arrow[d, "\pi_i"] \\
\boldsymbol{X} \arrow[ur, dashed, "h"] \arrow[r, "h_i"'] & \boldsymbol{G_i}
\end{tikzcd}$$

Demonstração. Defina a função

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

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,

$$h(x_1x_2) = (h_i(x_1x_2))_{i\in I} = (h_i(x_1)h_i(x_2))_{i\in I} = h(x_1)h(x_2).$$

■

2.2.2 Grupo Livre

Definição 2.16. 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 $(c_1, \ldots, c_n) \in C^n$. Denota-se $c_1 \cdots c_n$.

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

Definição 2.17. 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

$$p_1 \sim p_2 \quad \Longleftrightarrow \quad p_1p_2^{-1} \rightsquigarrow e.$$

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

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

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

A inclusão é definida.

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

Proposição 2.31 (Propriedade Universal)**.** *Seja C um conjunto, $\boldsymbol{X} = (X, \star)$ um grupo e $f : C \longrightarrow X$ uma função. Então existe um único homomorfismo de grupos $h : \langle \boldsymbol{C}\rangle \longrightarrow \boldsymbol{X}$ tal que $h \circ \iota = f$ (o diagrama comuta).*

$$\begin{tikzcd} \langle \boldsymbol{C}\rangle \arrow[dr, dashed, "h"] & \\ C \arrow[u, "\iota"] \arrow[r, "f"'] & \boldsymbol{X} \end{tikzcd}$$

Demonstração. Defina a função

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

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 $\overline{h} : \langle \boldsymbol{C} \rangle \longrightarrow \boldsymbol{X}$ um homomorfismo de grupos tal que $\overline{h} \circ \iota = f$. 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

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

o que implica que $\overline{h} = h$. ■

2.2.3 Coproduto de Grupos

Definição 2.18. Seja $(\boldsymbol{G_i})_{i \in I}$ uma família de grupos. O *coproduto* da família $(\boldsymbol{G_i})_{i \in I}$ é o par

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

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

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

Proposição 2.32 (Propriedade Universal)**.** *Sejam $(\boldsymbol{G_i})_{i \in I}$ uma família de grupos, $\boldsymbol{X} = (X, \star)$ um grupo e, para todo $i \in I$, $h_i : \boldsymbol{G_i} \longrightarrow \boldsymbol{X}$ um homomorfismo de grupos. Então existe um único homomorfismo de grupos $h : \bigsqcup_{i \in I} \boldsymbol{G_i} \longrightarrow \boldsymbol{X}$ tal que, para todo $i \in I$, $h \circ \iota_i = h_i$ (o diagrama comuta).*

$$\begin{tikzcd}
\bigsqcup_{i \in I} \boldsymbol{G_i} \arrow[dr, dashed, "h"] & \\
\boldsymbol{G_i} \arrow[u, "\iota_i"] \arrow[r, "h_i"'] & \boldsymbol{X}
\end{tikzcd}$$

Demonstração. Defina a função

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

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

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

■

2.3 Construções Específicas

2.3.1 Grupo Simples e Subgrupo Normal Maximal

Definição 2.19. Um *grupo simples* é um grupo não-trivial $\boldsymbol{G}$ cujos únicos subgrupos normais são $\boldsymbol{\{e\}}$ e $\boldsymbol{G}$.

Definição 2.20. Seja $\boldsymbol{G}$ um grupo. Um subgrupo normal *maximal* de $\boldsymbol{G}$ é um subgrupo normal próprio $\boldsymbol{M} \lhd \boldsymbol{G}$ que satisfaz

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

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

Proposição 2.33. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{M} \trianglelefteq \boldsymbol{G}$ um subgrupo normal. Então $\boldsymbol{M}$ é maximal se, e somente se, $\boldsymbol{G/M}$ é simples.*

Demonstração. Consideremos a projeção canônica

$$\begin{aligned} \pi \colon G &\longrightarrow {}^{G}\!/_{M} \\ g &\longmapsto gM. \end{aligned}$$

($\Rightarrow$) Suponhamos que $\boldsymbol{M}$ é maximal. Então $\boldsymbol{M}$ é um subgrupo próprio, o implica que $\boldsymbol{G/M}$ é não-trivial. Seja $\boldsymbol{N} \trianglelefteq \boldsymbol{G/M}$. Sabemos que $\boldsymbol{\pi^{-1}(N)} \trianglelefteq \boldsymbol{G}$ (2.20). Como $[e] \in N$, então $\pi^{-1}(e) \subseteq \pi^{-1}(N)$. Notando que $\pi^{-1}([e]) = \mathrm{nuc}(\pi) = M$, segue que $M \subseteq \pi^{-1}(N)$. Como $\boldsymbol{M}$ é maximal, segue que $\pi^{-1}(N) = N$ ou $\pi^{-1}(N) = G$. Notemos que $N = \pi(\pi^{-1}(N))$, pois π é sobrejetiva. No primeiro caso, $N = \pi(\pi^{-1}(N)) = \pi(M) = \{[e]\}$. No segundo caso, $N = \pi(\pi^{-1}(N)) = \pi(G) = G/M$. Portanto $\boldsymbol{G/M}$ é simples.
($\Leftarrow$) Suponhamos que $\boldsymbol{G/M}$ é simples. Seja $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ tal que $M \subseteq N$. Como π é homomorfismo de grupos sobrejetivo, ssegue que $\pi(N) \trianglelefteq \boldsymbol{G/M}$ (2.21). Como $\boldsymbol{G/M}$ é simples, então $\pi(N) = \{[e]\}$ ou $\pi(N) = G/M$. No primeiro caso, $N = \mathrm{nuc}(\pi) = M$. No segundo caso, $N = \pi^{-1}(\pi(N)) = \pi^{-1}(N) = G$. Logo $\boldsymbol{M}$ é maximal. ■

Conjectura 2.34. *Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{N} \lhd \boldsymbol{G}$ um subgrupo normal próprio. Então $\boldsymbol{G}$ tem subgrupo normal maximal.*

Demonstração. Usaremos o lema de Zorn. Seja $P \subseteq \mathsf{P}(G)$ o conjunto de todos os subconjuntos $S \subset G$ tais que $\boldsymbol{S} \lhd \boldsymbol{G}$. Então $(P, \subseteq)$ é um conjunto parcialmente ordenado com a contenção de conjuntos usual. Agora, seja $(C)_{i \in I}$ uma cadeia de $(P, \subseteq)$. Consideremos o conjunto $C := \bigcup_{i \in I} C_i$. Como

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

Então P tem elemento maximal. ■

2.3.2 Sequência subnormal

Definição 2.21. Seja $\boldsymbol{G}$ um grupo. Uma *sequência subnormal* de $\boldsymbol{G}$ é uma sequência finita $(\boldsymbol{N_i})_{i\in[n]}$ de subgrupos de $\boldsymbol{G}$ que satisfaz

$$\boldsymbol{\{e\} = N_0 \trianglelefteq \cdots \trianglelefteq N_{n-1} = G}.$$

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

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

$$\boldsymbol{\{e\} = N_0 \triangleleft \cdots \triangleleft N_{n-1} = G}.$$

O comprimento

2.3.3 Conjunto gerador

Definição 2.22. Seja $\boldsymbol{G}$ um grupo e $S \subseteq G$ um conjunto. O grupo *gerado* por S é o grupo $\boldsymbol{\langle S\rangle \leq G}$ em que

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

$$\langle S\rangle := \left\{ \mathop{\ast}_{i\in[n]} s_i \;\middle|\; n \in \mathbb{N},\ s_i \in S \ \text{ ou } \ s_i^{-1} \in S \right\}.$$

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

2.3.4 Grupos Simétricos e Alternados

Definição 2.23. Seja C um conjunto. O *grupo simétrico* de C é o par $\boldsymbol{\mathfrak{S}(C)} = (\mathfrak{S}(C), \circ)$, em que

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

é o conjunto de todas as bijeções entre C e C, e $\circ$ é a composição de funções. Seja α um número cardinal. Para $C = \alpha$, usa-se a notação $\mathfrak{S}_\alpha := \mathfrak{S}(\alpha)$.

Proposição 2.35. *Seja C um conjunto. O grupo simétrico $\boldsymbol{\mathfrak{S}(C)}$ é um grupo.*

Demonstração. Se $C = \emptyset$, então $\mathfrak{S}(C) = \{\emptyset\}$. Assim, como $\emptyset\circ\emptyset = \emptyset$, segue que $\circ$ é operação binária em $\{\emptyset\}$. Ainda, segue que $\circ$ é associativa, pois $(\emptyset\circ\emptyset)\circ\emptyset = \emptyset\circ(\emptyset\circ\emptyset)$; tem elemeno neutro $\emptyset$, pois $\emptyset\circ\emptyset = \emptyset$, e que todo elemento tem inverso, pois $\emptyset^{-1} = \emptyset$.

Suponhamos, então, que $C \neq \emptyset$ e sejam $p_1, p_2 \in \mathfrak{S}(C)$. 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 $\boldsymbol{\mathfrak{S}(C)}$, pois, para todo $p \in \mathfrak{S}(C)$, vale $p \circ \mathrm{I}_C = \mathrm{I}_C \circ p = p$ (3.7). Por fim, como p é uma bijeção, existe função inversa $p^{-1} : C \longrightarrow C$ que é bijeção entre C e C (3.8 e 3.9); logo existe $p^{-1} \in \mathfrak{S}(C)$ tal que $p \circ p^{-1} = p^{-1} \circ p = \mathrm{I}_C$. Portanto concluímos que $\boldsymbol{\mathfrak{S}(C)}$ é um grupo. ■

Proposição 2.36. *Sejam A e B conjuntos tais que $|A| = |B|$. Então*

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

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

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

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

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

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

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

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

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

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

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

Essa proposição mostra que podemos estudar somente os grupos simétricos dos números cardinais, pois isso será equivalente a estudar qualquer grupo simétrico. Em particular, para todo conjunto finito, podemos estudar seu grupo simétrico considerando somente o grupo simétrico $\boldsymbol{\mathfrak{S}}_n$, em que n é o número de elementos do conjunto. A partir de agora, as proposições serão considerando esses grupos $\boldsymbol{\mathfrak{S}}_n$.

Proposição 2.37. *Seja $n \in \mathbb{N}$. Então $|\mathfrak{S}_n| = n!$.*

Teorema 2.38. *Seja $\boldsymbol{G}$ um grupo. Então*

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

Demonstração. Consideremos a função

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

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 $x \in G$,

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

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

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

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

$$g * x = h(g)(x) = \mathrm{I}_G(x) = x,$$

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

Esse teorema é um teorema muito importante, pois ele mostra que, de certa forma, todo grupo é um subconjunto de permutações. Por causa disso que grupos são pensados como os objetos algébricos que modelam a simetria.

Permutações e Órbitas

Definição 2.24. Seja $n \in \mathbb{N}$. Uma *permutação* de n objetos é um elemento $p \in \mathfrak{S}_n$, denotado por

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

Notação. Seja $n \in \mathbb{N}$. A composição de duas permutações $p_1, p_2 \in \mathfrak{S}_n$, quando representadas na notação acima, é denotada

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

Definição 2.25. Sejam $n \in \mathbb{N}$ e $p \in \mathfrak{S}_n$. A *matriz de permutação* de p é a matriz $[p] \in \mathbb{M}_n(\mathbb{Z})$ cujas entradas são dadas por

$$[p]_{i,j} = \delta_{i,p(j)} = \begin{cases} 1 & i = p(j) \\ 0 & i \neq p(j). \end{cases}$$

O *conjunto das matrizes de permutação* de $\mathfrak{S}_n$ é o conjunto

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

Proposição 2.39. *Seja $n \in \mathbb{N}$. Então o par $[\mathfrak{S}_n] = ([\mathfrak{S}_n], \cdot)$, em que $\cdot$ é o produto de matrizes, é um grupo, e*

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

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

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

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

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

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

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

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

Note que que h é homomorfismo, pois, para todos $p, q \in \mathfrak{S}_n$,

$$h(pq) = [pq] = [p][q] = h(p)h(q).$$

Ainda, h ■

Definição 2.26. Sejam $n \in \mathbb{N}$, $p \in \mathfrak{S}_n$ e $m \in [n]$. A *órbita de m sob p* é o conjunto

$$\mathcal{O}_p(m) := \left\{ p^k(m) \;\middle|\; k \in \mathbb{Z} \right\}.$$

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 2.40. *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, $\emptyset \nsubseteq \mathcal{O}_p$. 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 $[n] \subseteq \bigcup_{m\in[n]}$ 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 2.27. Sejam $n, k \in \mathbb{N}$. Um *ciclo* de $\mathfrak{S}_n$ é um elemento $c \in \mathfrak{S}_n$ para o qual existe $m \in [n]$ 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

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

Proposição 2.41. *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 2.42 (Fatoração de Permutação)**.** *Seja $n \in \mathbb{N}$ e $p \in \mathfrak{S}_n$. Então existem únicos ciclos $c_1, \ldots, c_k \in \mathfrak{S}_n$ disjuntos dois a dois tais que $p = c_1 \circ \cdots \circ c_k$.*

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

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

■

2.3.5 Grupos Cíclicos

2.3.6 Grupos Diedrais

2.4 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 2.28. Sejam $\boldsymbol{G}$ um grupo e X um conjunto. Uma *ação* de $\boldsymbol{G}$ em X é um homomorfismo de grupos

$$\begin{aligned} A\colon G &\longrightarrow \mathfrak{S}(X) \\ g &\longmapsto g_{\blacksquare} : X \longrightarrow X \\ & \qquad\qquad x \longmapsto g_{\blacksquare}\, x. \end{aligned}$$

Denota-se $A\colon \boldsymbol{G} \curvearrowright X$. Diz-se que o grupo $\boldsymbol{G}$ *age* no conjunto X, e denota-se $\boldsymbol{G} \curvearrowright X$, se, e somente se, existe ação de $\boldsymbol{G}$ 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 2.43. *Sejam X um conjunto e $\boldsymbol{G}$ um grupo. Então $\boldsymbol{G} \curvearrowright X$ se, e somente se, existe uma função*

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

que satisfaz

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

$$e_{\blacksquare}\, x = x;$$

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

$$(g_1 g_0)_{\blacksquare}\, x = g_{1\blacksquare}\, (g_{0\blacksquare}\, x).$$

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

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

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

Essa proposição é geralmente considerada a definição de uma ação *à esquerda* de $\boldsymbol{G}$ 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.

2.4.1 Órbitas e Estabilizadores

Definição 2.29. Sejam X um conjunto, $\boldsymbol{G}$ um grupo, $\boldsymbol{G} \curvearrowright X$ e $x \in X$. A *órbita* de x sob $\boldsymbol{G}$ é o conjunto

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

Definição 2.30. Sejam X um conjunto, $\boldsymbol{G}$ um grupo, $A : \boldsymbol{G} \curvearrowright X$ e $x \in X$. O *estabilizador* de x é

$$G_x = \{g \in G \mid g\boldsymbol{.}\, x = x\} = A^{-1}(\{\mathrm{I}\}) = \mathrm{nuc}(A).$$

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

2.5 Grupo Linear Geral

Definição 2.31. Sejam $\boldsymbol{C}$ um corpo e $n \in \mathbb{N}$. O *grupo linear geral* de $\boldsymbol{C}$ de ordem n é o conjunto

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

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

$$\mathrm{GL}(\boldsymbol{V}) := \mathrm{GL}_n(\boldsymbol{C}).$$

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

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

2.6 Representação de Grupos

Definição 2.33. Sejam $\boldsymbol{G}$ um grupo e $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Uma *representação* de $\boldsymbol{G}$ em $\boldsymbol{V}$ é um homomorfismo de grupos

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

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

Definição 2.34. Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$.

Capítulo 3

Anéis

3.1 Construções Algébricas

3.1.1 Anel e Subanel

Definição 3.1. Um *anel* é uma lista $\boldsymbol{A} = (A, +, -, 0, \times, 1)$ 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 $\boldsymbol{A}$;

2. $(A, \times, 1)$ é um monoide comutativo, em que $\times$ é a *multiplicação* e 1 é a *unidade* (ou o *um*) de $\boldsymbol{A}$;

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 substração, 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,

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

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 (1.7).

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 3.1. *Seja* $\boldsymbol{A}$ *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 3.2. Seja $\boldsymbol{A}$ um anel. O conjunto dos elementos invertíveis sob multiplicação de $\boldsymbol{A}$ é denotado por A^*.

Proposição 3.2. *Seja* $\boldsymbol{A}$ *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 3.3. Seja $\boldsymbol{A} = (A, +, -, 0, \times, 1)$ um anel. Um *subanel* de $\boldsymbol{A}$ é um anel $\boldsymbol{S} = (S, +_S, \times_S)$ em que $S \subseteq A$, $+_S = +|_{S\times S}$ e $\times_S = \times|_{S\times S}$. Denota-se $\boldsymbol{S} \leq \boldsymbol{A}$. Um subanel *próprio* de $\boldsymbol{A}$ é um subanel $\boldsymbol{S} \leq \boldsymbol{A}$ em que S é um conjunto próprio de A ($S \subset A$). Denota-se $\boldsymbol{S} < \boldsymbol{A}$.

Proposição 3.3. *Sejam $\boldsymbol{A} = (A, +, \times)$ um anel e $S \subseteq A$. Então*

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

é um anel com $1 \in S$ se, e somente se,

1. *$(S, +|_{S\times S})$ é um subgrupo comutativo de $(A, +)$:*
   (a) *(Não-vacuidade) $S \neq \emptyset$;*
   (b) *(Fechamento) $\bigwedge s_1, s_2 \in S \qquad s_1 + s_2 \in S$;*
   (c) *(Invertibilidade) $\bigwedge s \in S \qquad -s \in S$;*
2. *$(S, \times|_{S\times S})$ é um submonoide comutativo de $(A, \times)$ com $1 \in S$:*
   (a) *(Identidade) $1 \in S$;*
   (b) *(Fechamento) $\bigwedge s_1, s_2 \in S \qquad s_1 \times s_2 \in S$.*

Demonstração. ($\Rightarrow$) Suponhamos que $\boldsymbol{S}$ é um anel com $1 \in S$. (Subgrupo) Como $S \subseteq A$ e $(S, +|_{S\times S})$ um grupo comutativo, então é um subgrupo de $(A, +)$ por definição de subgrupo (o que é equivalente às propriedades listadas) e é comutativo (2.2)). (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 (1.9).

($\Leftarrow$) 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 $+\times_{S\times S}$. ■

3.1.2 Ideais e Anéis Quocientes

Definição 3.4. Seja $\boldsymbol{A}$ um anel. Um *ideal* de $\boldsymbol{A}$ é um conjunto não vazio $I \subseteq A$ tal que

1. $\bigwedge i_1, i_2 \in I \qquad i_1 - i_2 \in I$
2. $\bigwedge a \in A, i \in I \qquad ai \in I$

Denotamos que I é ideal de $\boldsymbol{A}$ por $I \trianglelefteq A$. Ainda, $I \triangleleft A$ significa que $I \neq A$ e $I \trianglelefteq A$.

É interessante observar que I é subgrupo de $(A, +)$. A definição de ideal difere da definição de subanel na propriedade 2.

Proposição 3.4. *Sejam $\boldsymbol{A}$ um anel e $I \trianglelefteq A$. Então*

1. $0 \in I$;
2. $\bigwedge i_1, i_2 \in I \qquad i_1 + i_2 \in I$;
3. $1 \in I \Rightarrow I = A$;
4. $\{0\}$ *e* A *são ideais de* A.

Demonstração. 1. Seja $i \in I$. Então $0 = i - i \in I$.

2. Sejam $i_1, i_2 \in I$. Pelo item anterior, sabemos que $0 \in I$, o que implica $-i_2 = 0 - i_2 \in I$. Logo $i_1 + i_2 = i_1 - (-i_2) \in I$.
3. Se $1 \in I \trianglelefteq A$, então, para todo $a \in A$, temos $a = a \cdot 1 \in A$. Logo $I = A$.
4. Consideremos $\{0\}$. Se $i \in \{0\}$, então $i = 0$. Portanto, para todo $a \in A$ e $i \in \{0\}$, temos $i - i = 0 \in \{0\}$ e $ai = 0 \in \{0\}$. Logo $\{0\} \trianglelefteq A$. Agora, consideremos A. Para todo $a_1, a_2 \in A$, temos $a_1 - a_2 \in A$ e $a_1 a_2 \in A$. Logo $A \trianglelefteq A$.

■

Proposição 3.5. *Sejam $\boldsymbol{A}$ um anel e $(I_j)_{j \in J}$ uma família de ideais de $\boldsymbol{A}$. Então*

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

é um ideal de $\boldsymbol{A}$.

Demonstração. Sejam $i_1, i_2 \in I$ e $a \in A$. Então, para todo $j \in J$, $i_1, i_2 \in I_j$ e, como I_j é ideal de $\boldsymbol{A}$, segue que $i_1 - i_2 \in I_j$ e que $ai_1 \in W_i$. Logo $i_1 - i_2 \in I$ e $ai_1 \in I$, o que mostra que I é ideal de $\boldsymbol{A}$. ■

Proposição 3.6. *Sejam* $\boldsymbol{A}$ *um anel e* $(I_j)_{n\in\mathbb{N}}$ *uma sequência crescente de ideais de* $\boldsymbol{A}$*; ou seja,* $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$*. Então*

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

é um ideal de $\boldsymbol{A}$*.*

Demonstração. Sejam $i_1, i_2 \in I$. Então existem $n, m \in \mathbb{N}$ tais que $i_1 \in I_n$ e $i_2 \in I_m$. Nesse caso, $I_n \subseteq I_m$ ou $I_m \subseteq I_n$. Sem perda de generalidade, suponhamos o primeiro caso. Então segue que $i_1 \in I_m$ e, portanto, $i_1 - i_2 \in I_m$, o que mostra que $i_1 - i_2 \in I$. Agora, seja $a \in A$ e notemos que, como I_n é ideal de $\boldsymbol{A}$, segue qque $ai_1 \in I_n$. Logo $ai_1 \in I$, o que mostra que I é ideal de $\boldsymbol{A}$. ■

Definição 3.5. Sejam $\boldsymbol{A}$ um anel e $a_1, \ldots, a_n \in A$. Definimos o conjunto

$$\mathop{+}_{i=1}^{n} a_i A = a_1 A + \ldots + a_n A := \left\{ \mathop{+}_{i=1}^{n} a_i b_i \;\middle|\; b_i \in A \right\}.$$

Proposição 3.7. *Sejam* $\boldsymbol{A}$ *um anel e* $a_1, \ldots, a_n \in A$*. Então*

$$I := \mathop{+}_{k=1}^{n} a_k A \trianglelefteq A.$$

Demonstração. Sejam $a \in A$ e $i_1, i_2 \in I$ tais que $i_1 = +_{k=1}^{n} a_i b_i$ e $i_2 = +_{k=1}^{n} a_i c_i$. Então

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

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

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

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

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

Definição 3.6. Seja $\boldsymbol{A}$ um anel. Um *ideal principal* de $\boldsymbol{A}$ é um ideal $I \trianglelefteq A$ tal que

1. $\bigvee a \in A \qquad I = aA.$

Proposição 3.8. *Seja* $\boldsymbol{A}$ *um anel. Então* $\boldsymbol{A}$ *é um corpo se, e somente se,* $\boldsymbol{A}$ *é um anel não-trivial cujos únicos ideais de* $\boldsymbol{A}$ *são* $\{0\}$ *e* A*.*

Demonstração. Suponha que $\boldsymbol{A}$ é um corpo. Então $(A \setminus \{0\}, \cdot)$ é um grupo e, portanto, $A \neq \emptyset$. Seja $I \trianglelefteq A$ e suponha que $I \neq \{0\}$. Então existe $i \in I \setminus \{0\}$. Como $\boldsymbol{A}$ é corpo, existe $i^{-1} \in A$. Portanto $1 = i^{-1}i \in I$. Logo $I = A$.

Por outro lado, suponha que os únicos ideais de A são $\{0\}$ e A. Como $\boldsymbol{A}$ é não-trivial, seja $a \in A \setminus \{0\}$ e consideremos o ideal $I = aA$. Notemos que $a = a \cdot 1 \in aA$, o que implica $I \neq \{0\}$. Portanto $I = A$. Mas então $1 \in aA$, o que significa que deve existir $b \in A$ tal que $1 = ab$; ou seja, todo $a \in A \setminus \{0\}$ tem inverso em A. Logo $\boldsymbol{A}$ é corpo. ■

Proposição 3.9. *Sejam $\boldsymbol{A}$ um anel e $I \trianglelefteq A$. A relação binária $\sim_I$ em A, definida por*

$$a \sim_I b \Leftrightarrow a - b \in I,$$

é uma relação de equivalência.

Demonstração. Vamos demonstrar as três propriedades de uma relação de equivalência.

1. (Reflexividade) Seja $a \in A$. Então $a - a = 0 \in I$. Logo $a \sim_I a$.

2. (Simetria) Sejam $a_1, a_2 \in A$ tais que $a_1 \sim_I a_2$. Então $(a_1 - a_2) \in I$. Mas $0 \in I$, o que implica $a_2 - a_1 = 0 - (a_1 - a_2) \in I$. Logo $a_2 \sim_I a_1$.

3. (Transitividade) Sejam $a_1, a_2, a_3 \in A$ tais que $a_1 \sim_I a_2$ e $a_2 \sim_I a_3$. Então $(a_1 - a_2), (a_2 - a_3) \in I$, o que implica $a_1 - a_3 = (a_1 - a_2) + (a_2 - a_3) \in I$. Logo $a_1 \sim_I a_3$.

■

Definição 3.7. Sejam $\boldsymbol{A}$ 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 3.10. *Sejam $(A, +, \cdot)$ um anel, $I \trianglelefteq A$ e $\sim_I$ a relação de equivalência definida na proposição anterior e $a \in A$. Então a classe de equivalência $[a] = \{b \in A : b \sim_I a\}$ é igual à classe lateral $a + I$ e, por consequência, o conjunto quociente $A/\sim_I$ é igual ao conjunto A/I.*

Demonstração. Seja $b \in [a]$. Então $b - a \in I$; ou seja, existe $i \in I$ tal que $b - a = i$. Mas isso implica $b = a + i$, que implica, por sua vez, que $b \in a + I$. Por outro lado, seja $b \in a + I$. Então existe $i \in I$ tal que $b = a + i$; ou seja, $b - a = i$, que implica $b - a \in I$ e, assim, $b \in [a]$. Disso, vem que $A/\sim_I = A/I$. ■

Uma consequência disso é que o conjunto A é particionado em classes laterais de I. Outra consequência é que duas classes laterais são iguais se, e somente se, a diferença entre seus representantes está em I.

Definição 3.8. Sejam $\boldsymbol{A}$ um anel, $I \trianglelefteq A$ e $a_1, a_2 \in A$. Então definimos as operações binárias $\oplus$ e $\odot$ em A/I por

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

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

Proposição 3.11. *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 $(a_1 b_1) + I = (a_2 b_2) + I$. ■

Proposição 3.12. *Sejam $\boldsymbol{A} = (A, +, \cdot)$ um anel e $I \trianglelefteq A$. Então $\boldsymbol{A/I} := (A/I, \oplus, \odot)$ 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

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

■

3.1.3 Homomorfismos de Anéis

Definição 3.9. Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ dois anéis. Um *homomorfismo de anéis* entre $\boldsymbol{A}$ e $\boldsymbol{B}$ é uma função $\phi : A \longrightarrow B$ que é

1. um homomorfismo de grupos entres $(A, +)$ e $(B, \oplus)$

   (a) $\bigwedge a_1, a_2 \in A \qquad \phi(a_1 + a_2) = \phi(a_1) \oplus \phi(a_2)$;

2. um homomorfismo de monoides entre $(A, \cdot)$ e $(B, \odot)$

(a) $\bigwedge a_1, a_2 \in A \qquad \phi(a_1 \cdot a_2) = \phi(a_1) \odot \phi(a_2)$;

(b) $\phi(1_A) = 1_B$.

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

Exemplo 3.1. *Seja $(A, +, \cdot)$ um anel e consideremos o anel dos números inteiros $(\mathbb{Z}, +, \cdot)$. Então*

$$\begin{aligned} \phi\colon \mathbb{Z} &\longrightarrow A \\ z &\longmapsto \begin{cases} \displaystyle\mathop{\mathbin{+}}_{i=1}^{z} 1_A & z > 0 \\ 0_A & z = 0 \\ -\phi(-z) & z > 0 \end{cases} \end{aligned}$$

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

$$\phi(z_1 + z_2) = \mathop{\mathbin{+}}_{i=1}^{z_1+z_2} 1_A = \mathop{\mathbin{+}}_{i=1}^{z_1} 1_A + \mathop{\mathbin{+}}_{i=z_1+1}^{z_1+z_2} 1_A = \mathop{\mathbin{+}}_{i=1}^{z_1} 1_A + \mathop{\mathbin{+}}_{i=1}^{z_2} 1_A = \phi(z_1) + \phi(z_2).$$

Se $z_1 < 0$ e $z_1 < 0$, então $z_1 + z_2 < 0$. Logo $-z_1$, $-z_2$ e $-(z_1 + z_2)$ são positivos e segue da equação anterior que

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

No caso que resta, z_1 e z_2 são um positivo e um negativo; sem perda de generalidade, suponhamos que $z_1 > 0$ nesse caso $-z_2 > 0$. Se tivermos $z_1 = -z_2$,

então

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

Se tivermos $z_1 > -z_2$, então

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

Por fim, se $-z_2 > z_1$, então $-z_1 < 0$ e $-z_2 >$ 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 3.10. Sejam $\boldsymbol{A}$ um anel e $n \in \mathbb{Z}$. O *número inteiro* n em $\boldsymbol{A}$ é o elemento

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

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

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

Proposição 3.13. *Sejam* $\boldsymbol{A}$ *um anel e* $a, b \in A$. *Então*

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

Exemplo 3.2. *Sejam* $\boldsymbol{A}$ *um anel e* $I \trianglelefteq A$. *Então a* projeção canônica *de* A *em* A/I, *definida por*

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

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 3.14 (Homomorfismos preservam a estrutura algébrica entre anéis)**.** *Sejam* $\boldsymbol{A} = (A, +, \cdot)$ *e* $\boldsymbol{B} = (B, \oplus, \odot)$ *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 entres $(A, +)$ e $(B, \oplus)$, sabemos que ϕ preserva a estrutura algébrica de grupo entre os grupos (2.17). ■

Corolário 3.15 (Composição de homomorfismos é homomorfismo)**.** *Sejam* $\boldsymbol{A_1} = (A_1, +_1, \cdot_1)$, $\boldsymbol{A_2} = (A_2, +_2, \cdot_2)$ *e* $\boldsymbol{A_3} = (A_3, +_3, \cdot_3)$ *três anéis e* $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A_1}, \boldsymbol{A_2})$ *e* $\psi \in \mathcal{H}\mathrm{om}(\boldsymbol{A_2}, \boldsymbol{A_3})$. *Então* $(\psi \circ \phi) \in \mathcal{H}\mathrm{om}(\boldsymbol{A_1}, \boldsymbol{A_3})$.

Demonstração. As duas propriedades de homomorfismo de anéis para $(\psi \circ \phi)$ seguem de propriedades análogas na seção de grupos e monoides.

1. Como ϕ é um homomorfismo de grupos entre $(A_1, +_1)$ e $(A_2, +_2)$ e ψ é homomorfismos de grupos entre $(A_2, +_2)$ e $(A_3, +_3)$, segue da proposição de composição de homomorfismos da seção de grupos (2.18) 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 (1.10) que $(\psi \circ \phi)$ é homomorfismo de monoides entre $(A_1, \cdot_1)$ e $(A_3, \cdot_3)$.

■

Proposição 3.16. *Sejam $\boldsymbol{A}$ e $\boldsymbol{B}$ anéis, $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$ e $I \trianglelefteq B$. Então $\phi^{-1}(I) \trianglelefteq A$.*

Demonstração. Sejam $i_1, i_2 \in \phi^{-1}(I)$ e $a \in A$. Então, como $\phi(i_1), \phi(i_2) \in I$, temos $\phi(i_1 - i_1) = \phi(i_1) - \phi(i_2) \in I$, o que implica que $i_1 - i_2 \in \phi^{-1}(I)$. Ainda, como $\phi(a) \in A$, temos que $\phi(ai_1) = \phi(a)\phi(i_1) \in I$, o que implica $ai_1 \in \phi^{-1}(I)$. Logo $\phi^{-1}(I) \trianglelefteq A$. ■

Proposição 3.17. *Sejam $\boldsymbol{A}$ e $\boldsymbol{B}$ anéis, $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$ sobrejetivo e $I \trianglelefteq A$. Então $\phi(I) \trianglelefteq B$.*

Demonstração. Sejam $j_1, j_2 \in \phi(I)$ e $b \in B$. Então existem $i_1, i_2 \in I$ tais que $\phi(i_1) = j_1$ e $\phi(i_2) = j_2$ e, como ϕ é sobrejetiva, existe $a \in A$ tal que $\phi(a) = b$. Então, como $I \trianglelefteq A$, temos que $i_1 - i_2 \in I$ e $ai_1 \in I$, o que implica $j_1 - j_2 = \phi(i_1) - \phi(i_2) = \phi(i_1 - i_2) \in \phi(I)$ e $bj_1 = \phi(a)\phi(i_1) = \phi(ai_1) \in \phi(I)$. Logo $\phi(I) \trianglelefteq B$. ■

Definição 3.11. Sejam $\boldsymbol{A}$ e $\boldsymbol{B}$ dois anéis e $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$. O *núcleo* de ϕ é o conjunto

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

e a *imagem* de ϕ é o conjunto

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

Proposição 3.18. *Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ dois anéis e seja $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$. Então*

1. $\mathrm{nuc}(\phi) \trianglelefteq A$;

2. $\mathrm{im}(\phi)$ *é subanel de* $\boldsymbol{B}$.

Demonstração. Demonstramos as afirmações separadamente.

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

■

Proposição 3.19. *Sejam* $\boldsymbol{A} = (A, +, \cdot)$ *e* $\boldsymbol{B} = (B, \oplus, \odot)$ *dois anéis e seja* $\phi \in \mathcal{H}\text{om}(\boldsymbol{A}, \boldsymbol{B})$. *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 (2.22), esta proposição está provada. ■

Definição 3.12. Sejam $\boldsymbol{A} = (A, +, \cdot)$ e $\boldsymbol{B} = (B, \oplus, \odot)$ dois anéis. Um isomorfismo de anéis é um homomorfismo de anéis $\phi \in \mathcal{H}\text{om}(\boldsymbol{A}, \boldsymbol{B})$ que é bijetivo. O conjunto de todos os homomorfismos de anéis entre $\boldsymbol{A}$ e $\boldsymbol{B}$ é denotado por $\mathcal{I}\text{so}(\boldsymbol{A}, \boldsymbol{B})$.

Proposição 3.20. *Sejam* $\boldsymbol{A} = (A, +, \cdot)$ *e* $\boldsymbol{B} = (B, \oplus, \odot)$ *anéis e* $\phi \in \mathcal{I}\text{so}(\boldsymbol{A}, \boldsymbol{B})$. *Então* $\phi^{-1} \in \mathcal{I}\text{so}(\boldsymbol{B}, \boldsymbol{A})$.

Demonstração. Como ϕ é bijetiva, sua inversa ϕ^{-1} também é bijetiva. Devemos provar que ϕ^{-1} é um homomorfismo de anéis. Sejam $b_1, b_1 \in B$. Primeiro, vamos provar que ϕ^{-1} é um homomorfismo de grupos entre $\boldsymbol{B}$ e $\boldsymbol{A}$. Como ϕ é isomorfismo, existem $a_1, a_2 \in A$ tais que $\phi(a_1) = b_1$ e $\phi(a_2) = b_2$. Então

$$\begin{aligned}
\phi^{-1}(b_1 \oplus b_2) &= \phi^{-1}(\phi(a_1) \oplus \phi(a_2)) \\
&= \phi^{-1}(\phi(a_1 + a_2)) \\
&= a_1 + a_2 \\
&= \phi^{-1}(b_1) \oplus \phi^{-1}(b_2)
\end{aligned}$$

e

$$\phi^{-1}(\ominus b_1) = \phi^{-1}(\phi(-a_1)) = -a_1 = \ominus\phi(b_1).$$

Agora, mostramos que ϕ^{-1} é homomorfismo de monoides entre $(B, \odot)$ e $(A, \cdot)$.

$$\begin{aligned}\phi^{-1}(b_1 \odot b_2) &= \phi^{-1}(\phi(a_1) \odot \phi(a_2)) \\ &= \phi^{-1}(\phi(a_1 \cdot a_2)) \\ &= a_1 \cdot a_2 \\ &= \phi^{-1}(b_1) \odot \phi^{-1}(b_2)\end{aligned}$$

e, como $\phi(1_A) = 1_B$, temos $\phi^{-1}(1_B) = 1_A$. ■

Definição 3.13. Sejam $\boldsymbol{A}$ e $\boldsymbol{B}$ dois anéis. Dizemos que $\boldsymbol{A}$ é *isomorfo* a $\boldsymbol{B}$, e denotamos isso por $\boldsymbol{A} \simeq \boldsymbol{B}$, sse existe $\phi \in \mathcal{I}\mathrm{so}(\boldsymbol{A}, \boldsymbol{B})$.

Proposição 3.21. *Sejam $\boldsymbol{A_1}$, $\boldsymbol{A_2}$ e $\boldsymbol{A_3}$ três anéis. Então*

1. *(Reflexividade) $\boldsymbol{A_1} \simeq \boldsymbol{A_1}$;*
2. *(Antissimetria) $\boldsymbol{A_1} \simeq \boldsymbol{A_2} \Rightarrow \boldsymbol{A_2} \simeq \boldsymbol{A_1}$;*
3. *(Transitividade) $\boldsymbol{A_1} \simeq \boldsymbol{A_2}$ e $\boldsymbol{A_2} \simeq \boldsymbol{A_3} \Rightarrow \boldsymbol{A_1} \simeq \boldsymbol{A_3}$.*

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

Demonstração. Vamos demonstrar as três propriedades separadamente.

1. Claramente, a função $\phi = Id_A : A \longrightarrow A$ é um isomorfismo de anéis. Logo $\boldsymbol{A_1} \simeq \boldsymbol{A_1}$
2. Se $\mathbf{A}_1 \simeq \boldsymbol{A_2}$, existe $\phi \in \mathcal{I}\mathrm{so}(\boldsymbol{A_1}, \boldsymbol{A_2})$. Pela proposição (3.20), ϕ^{-1} é um isomorfismo de anéis entre $\boldsymbol{A_2}$ e $\boldsymbol{A_1}$. Logo $\boldsymbol{A_2} \simeq \boldsymbol{A_1}$.
3. $\boldsymbol{A_1} \simeq \boldsymbol{A_2}$, existe $\phi \in \mathcal{I}\mathrm{so}(\boldsymbol{A_1}, \boldsymbol{A_2})$ e, como $\boldsymbol{A_2} \simeq \boldsymbol{A_3}$, existe $\psi \in \mathcal{I}\mathrm{so}(\boldsymbol{A_2}, \boldsymbol{A_3})$. Assim, pela proposição (3.15), sabemos que $(\psi \circ \phi) \in \mathcal{H}\mathrm{om}(\boldsymbol{A_1}, \boldsymbol{A_3})$. Ainda, como ϕ e ψ são bijeções, sua composição é uma bijeção. Portanto $(\psi \circ \phi) \in \mathcal{I}\mathrm{so}(\boldsymbol{A_1}, \boldsymbol{A_3})$, o que implica $\boldsymbol{A_1} \simeq \boldsymbol{A_3}$.

■

3.1.4 Teoremas de Isomorfismo

Teorema 3.22 (Primeiro Teorema de Isomorfismo)**.** *Sejam* $\boldsymbol{A} = (A, +, \cdot)$ *e* $\boldsymbol{B} = (B, \oplus, \odot)$ *dois anéis e* $\phi \in \mathcal{H}\mathrm{om}(\boldsymbol{A}, \boldsymbol{B})$*. Então*

$$\boldsymbol{A}\big/\mathbf{nuc}(\boldsymbol{\varphi}) \simeq \mathbf{im}\,(\boldsymbol{\varphi}).$$

Demonstração. Primeiro, vale notar que, como $\mathrm{im}(\phi) \trianglelefteq A$, o $\boldsymbol{A}/\,\mathbf{nuc}\,(\boldsymbol{\phi})$ é um anel. Agora, consideremos a função

$$\begin{aligned} \psi\colon A\big/\mathrm{nuc}(\phi) &\longrightarrow \mathrm{im}(\phi) \\ a + \mathrm{nuc}(\phi) &\longmapsto \phi(a). \end{aligned}$$

Notemos que a função ψ é bem definida. Para isso, sejam $a_1, a_2 \in A$ tais que $a_1 + \mathrm{nuc}(\phi) = a_2 + \mathrm{nuc}(\phi)$. Então $(a_1 - a_2) \in \mathrm{nuc}(\phi)$, o que implica $\phi(a_1 - a_2) = 0$. Como ϕ é homomorfismo de anéis, segue que $\phi(a_1) = \phi(a_2)$. Então $\psi(a_1 + \mathrm{nuc}(\phi)) = \psi(a_2 + \mathrm{nuc}(\phi))$.

Vamos mostrar que essa função é um isomorfismo de anéis. Primeiro, vamos mostrar que ψ é homomorfismo de anéis. Para isso, vamos denotar $a + \mathrm{nuc}(\phi) \in A/\,\mathrm{nuc}(\phi)$ por $[a]$ para facilitar a demonstração. Sejam $[a_1], [a_2] \in A/\,\mathrm{nuc}(\phi)$. Vemos que ψ é homomosfismo de grupos entre $(A/\,\mathrm{nuc}(\phi), +)$ e $(\mathrm{im}(\phi), \oplus)$, pois

$$\psi([a_1] + [a_2]) = \psi([a_1 + a_2]) = \phi(a_1 + a_2) = \phi(a_1) \oplus \phi(a_2) = \psi([a_1]) \oplus \psi([a_2]).$$

Agora, vemos que ψ é homomosfismo de monoides entre $(A/\,\mathrm{nuc}(\phi), \cdot)$ e $(\mathrm{im}(\phi), \odot)$, pois

$$\psi([a_1] \cdot [a_2]) = \psi([a_1 \cdot a_2]) = \phi(a_1 \cdot a_2) = \phi(a_1) \odot \phi(a_2) = \psi([a_1]) \odot \psi([a_2])$$

e $\psi([1_A]) = \phi(1_A) = 1_B$.

Por fim, devemos mostrar que ψ é bijetiva. Primeiro, mostramos que ψ é injetiva. Seja $[a] \in \mathrm{nuc}(\psi)$. Então $\psi([a]) = 0_B$, o que implica $\phi(a) = 0_B$. Mas isso implica $a \in \mathrm{nuc}(\phi)$; ou seja, $[a] = [0_A]$. Logo $\mathrm{nuc}(\psi) = \{[0_A]\}$, que quer dizer que ψ é injetiva (3.19). Agora, notamos que ψ é sobrejetiva por construção, pois tem como contradomínio $\mathrm{im}(\phi)$. ■

Proposição 3.23 (Teorema Chinês do Resto)**.** *Sejam* $m_1, \ldots, m_n \in \mathbb{N} \smallsetminus \{0, 1\}$ *dois a dois coprimos entre si. Então*

$$\mathbb{Z}\big/(m_1 m_2 \ldots m_n \mathbb{Z}) \simeq \left(\mathbb{Z}\big/m_1\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}\big/m_n\mathbb{Z}\right).$$

Definição 3.14.

$$B + I := \{b + i : b \in B, i \in I\}$$

Teorema 3.24 (Segundo Teorema de Isomorfismo)**.** *Sejam $\boldsymbol{A}$ um anel, B um subanel de $\boldsymbol{A}$ e $I \trianglelefteq A$. Então*

1. *$B + I$ é subanel de $\boldsymbol{A}$;*

2. *$B \cap I \trianglelefteq B$;*

3. $$\boldsymbol{B}\big/\boldsymbol{B \cap I} \simeq \boldsymbol{B + I}\big/\boldsymbol{I}.$$

Demonstração. 1. Para mostrar que $B + I$ é subanel de $\boldsymbol{A}$, primeiro notamos que $B + I$ não é vazio, pois B não é vazio e I não é vazio. Ainda, notamos que $B + I \subseteq A$, pois $B \subseteq A$ e $I \subseteq A$. Agora, mostramos as pripriedades de subanel. Sejam $b_1, b_2 \in B$ e $i_1, i_2 \in I$. Primeiro, mostraremos que $B + I$ é subgrupo de $(A, +)$. Note que $(b_1 + i_1) - (b_2 + i_2) \in B + I$, pois, como B é subgrupo de $(A, +)$, $b_1 - b_2 \in B$ e, como $I \trianglelefteq A$, $i_1 - i_2 \in A$, o que implica $(b_1 + i_1) - (b_2 + i_2) = (b_1 - b_2) + (i_1 - i_2) \in B + I$. Mostremos agora que $B + I$ é submonoide de $(A, \cdot)$. Note que

$$(b_1 + i_1)(b_2 + i_2) = b_1b_2 + b_1i_2 + i_1b_2 + i_1i_2.$$

Como B é submonoide de $(A, \cdot)$, $b_1b_2 \in B$ e, como $i \trianglelefteq A$, $b_1i_2, i_1b_2, i_1i_2 \in I$, o que implica $b_1i_2 + i_1b_2 + i_1i_2 \in I$. Logo $(b_1 + i_1)(b_2 + i_2) = (b_1b_2) + (b_1i_2 + i_1b_2 + i_1i_2) \in B + I$. Ainda, $1 \in B$ e $0 \in I$. Logo $1 = 1 + 0 \in B + I$.

2. Para mostrar que $B \cap I \trianglelefteq B$, notemos primeiro que $B \cap I$ não é vazio. De fato, como B é subanel de $\boldsymbol{A}$, segue que $0 \in B$ e, como $I \trianglelefteq A$, também segue que $0 \in I$, o que implica $0 \in B \cap I$. Claramente, $B \cap I \subseteq A$. Então basta provar as propriedades de ideal. Sejam $b_1, b_2 \in B \cap I$. Como B é subanel de $\boldsymbol{A}$, temos $b_1 - b_2 \in B$ e, como $I \trianglelefteq A$, temos $b_1 - b_2 \in I$. Logo $b_1 - b_2 \in B \cap I$. Seja $b \in B$. Como B é subanel de $\boldsymbol{A}$, temos $bb_1 \in B$ e, como $I \trianglelefteq A$, temos $bb_1 \in I$. Logo $bb_1 \in B \cap I$.

3. O isomorfismo só faz sentido se os dois quocientes fazem sentido. O primeiro faz sentido pelo item anterior. O segundo faz sentido pois, pela definição de ideal, segue direto que $I \trianglelefteq B + I$, pois $I \subseteq B + I \subseteq A$. Então devemos exibir um isomorfismo de anéis entre os dois anéis. Considere a função

$$\begin{aligned} \phi\colon B &\longrightarrow B + I\big/I \\ b &\longmapsto b + I. \end{aligned}$$

Essa função é um homomorfismo de anéis. Sejam $b_1, b_2 \in B$. Então $\phi(b_1 + b_2) = (b_1 + b_2) + I = (b_1 + I) + (b_1 + I) = \phi(b_1) + \phi(b_2)$. Ainda, vale $\phi(b_1b_2) = (b_1b_2) + I = (b_1 + I)(b_1 + I) = \phi(b_1)\phi(b_2)$. Por fim, $\phi(1) = 1 + I$.

Agora, notemos que $\mathrm{nuc}(\phi) = B \cap I$. Seja $b \in B$. Então

$$b \in \mathrm{nuc}(\phi) \Leftrightarrow \phi(b) = 0 \Leftrightarrow b + I = I \Leftrightarrow b \in I.$$

Por fim, notemos que $\mathrm{im}(\phi) = B + I/I$, 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 (3.22) que

$$\boldsymbol{B}\big/\boldsymbol{B \cap I} = \boldsymbol{B}\big/\mathbf{nuc}(\boldsymbol{\phi}) \simeq \mathbf{im}\,(\boldsymbol{\phi}) = \boldsymbol{B + I}\big/\boldsymbol{I}.$$

■

Lema 3.25. *Sejam $\boldsymbol{A}$ um anel e $I \trianglelefteq A$. Então*

1. *Se B é subanel de $\boldsymbol{A}$ tal que $I \subseteq B$, então B/I é subanel de $\boldsymbol{A/I}$. Por outro lado, todo subanel de $\boldsymbol{A/I}$ é da forma B/I para algum B subanel de $\boldsymbol{A}$ tal que $I \subseteq B$.*

2. *Se $J \trianglelefteq A$ tal que $I \subseteq J$, então $J/I \trianglelefteq A/I$. Por outro lado, todo ideal de A/I é da forma J/I para algum $J \trianglelefteq A$, tal que $I \subseteq J$.*

Demonstração. 1. Seja B um subanel de $\boldsymbol{A}$ tal que $I \subseteq B$. Para mostrar que o conjunto B/I é subanel de $\boldsymbol{A/I}$, 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 $\boldsymbol{A/I}$.

Seja agora C um subanel de $\boldsymbol{A/I}$. Como C é subconjunto não vazio de $\boldsymbol{A/I}$, 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 $\boldsymbol{A}$. Sejam $b_1, b_2 \in B$. Como B/I é subanel de $\boldsymbol{A/I}$, 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 $a j_1 \in J$. Então $(j_1 + I) - (j_2 + I) = (j_1 - j_2) + I \in J/I$ e $(a + I)(j_1 + I) = (a j_1) + I \in J/I$.

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 $(a + I)(j_1 + I) = (a j_1) + I \in J/I$. Então $j_1 - j_2 \in J$ e $a j_1 \in J$, e a demonstração está completa.

■

Teorema 3.26 (Terceiro Teorema de Isomorfismo)**.** *Sejam* $\boldsymbol{A}$ *um anel,* $I \trianglelefteq A$ *e* $J \trianglelefteq A$ *tais que* $I \subseteq J$*. Então*

$$\boldsymbol{(A/I)}\big/\boldsymbol{(J/I)} \simeq \boldsymbol{A}\big/\boldsymbol{J}.$$

Demonstração. Consideremos a função

$$\begin{aligned} \phi\colon A\big/I &\longrightarrow A\big/J \\ a+I &\longmapsto a+J. \end{aligned}$$

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

$$\begin{aligned} \phi((a_1+I)(a_2+I)) &= \phi((a_1a_2)+I) \\ &= (a_1a_2)+J \\ &= (a_1+J)(a_2+J) \\ &= \phi(a_1)\phi(a_2). \end{aligned}$$

Por fim, notamos que $\phi(1+I) = 1+J$. Assim, provamos que ϕ é homomorfismo de anéis.

Agora, notemos que

$$\mathrm{nuc}(\phi) = \{a+I : \phi(a+I) = 0+J\} = \{a+I : a \in J\} = J\big/I,$$

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, $\mathrm{im}(\phi) = A/J$. Logo, pelo primeiro teorema de isomorfismo (3.22), temos que

$$\boldsymbol{(A/I)}\big/\boldsymbol{(J/I)} = \boldsymbol{(A/I)}\big/\mathbf{nuc}(\boldsymbol{\phi}) \simeq \mathbf{im}\,(\boldsymbol{\phi}) = \boldsymbol{A}\big/\boldsymbol{J}.$$

■

3.2 Construções Categóricas

3.2.1 Anel de Polinômios

Definição 3.15. Seja $\boldsymbol{A}$ um anel. O *anel de polinômios* em $\boldsymbol{A}$ é o conjunto

$$A[x] := \left\{ p \in A^{\mathbb{N}} \;\middle|\; |\mathrm{supp}(p)| < |\mathbb{N}| \right\}.$$

Os elementos de $A[x]$ são os *polinômios* em $\boldsymbol{A}$.

Defininimos os polinômios em $\boldsymbol{A}$ como as sequências em A com suporte finito. O suporte da sequência $p\colon \mathbb{N} \longrightarrow A$, 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

$$p = \mathop{\mathbin{+}}_{i=0}^{n} p_i x^i.$$

Antes disso, mostraremos que $A[x]$ é um anel, o que justifica seu nome.

Definição 3.16. Seja $\boldsymbol{A}$ um anel. Definimos em $A[x]$ as operações e as constantes

$$\begin{aligned} +_{A[x]}\colon A[x] \times A[x] &\longrightarrow A[x] \\ (p, q) &\longmapsto (p_n + q_n)_{n\in\mathbb{N}} \end{aligned}$$

$$\begin{aligned} -_{A[x]}\colon A[x] &\longrightarrow A[x] \\ p &\longmapsto (-p_n)_{n\in\mathbb{N}} \end{aligned}$$

$$\begin{aligned} 0_{A[x]}\colon \mathbb{N} &\longrightarrow A \\ n &\longmapsto 0 \end{aligned}$$

$$\begin{aligned} \cdot_{A[x]}\colon A[x] \times A[x] &\longrightarrow A[x] \\ (p, q) &\longmapsto \left(\mathop{\mathbin{+}}_{i=0}^{n} p_i q_{n-i} \right)_{n\in\mathbb{N}}. \end{aligned}$$

$$\begin{aligned} 1_{A[x]}\colon \mathbb{N} &\longrightarrow A \\ n &\longmapsto \begin{cases} 1, & n = 0 \\ 0, & n \neq 0. \end{cases} \end{aligned}$$

Os sub-índices $A[x]$ serão suprimidos quando possível.

Proposição 3.27. *Seja* $\boldsymbol{A}$ *um anel. Então* $\boldsymbol{A[x]} = (A[x], +, -, 0, \cdot, 1)$ *é um anel.*

Demonstração. 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 $p, q, r \in A[x]$,

$$\begin{aligned}
(pq)r &= \left(\mathop{\Large +}_{i=0}^{n} (pq)_i r_{n-i}\right)_{n\in\mathbb{N}} \\
&= \left(\mathop{\Large +}_{i=0}^{n} \left(\mathop{\Large +}_{j=0}^{i} p_j q_{i-j}\right) r_{n-i}\right)_{n\in\mathbb{N}} \\
&= \left(\mathop{\Large +}_{i=0}^{n} \mathop{\Large +}_{j=0}^{i} p_j q_{i-j} r_{n-i}\right)_{n\in\mathbb{N}} \\
&= \left(\mathop{\Large +}_{0\le j\le i\le n} p_j q_{i-j} r_{n-i}\right)_{n\in\mathbb{N}} \\
&= \left(\mathop{\Large +}_{i=0}^{n} \mathop{\Large +}_{j=0}^{n-i} p_i q_j r_{n-i-j}\right)_{n\in\mathbb{N}} \\
&= \left(\mathop{\Large +}_{i=0}^{n} p_i \left(\mathop{\Large +}_{j=0}^{n-i} q_j r_{n-i-j}\right)\right)_{n\in\mathbb{N}} \\
&= \left(\mathop{\Large +}_{i=0}^{n} p_i (qr)_{n-i}\right)_{n\in\mathbb{N}} \\
&= p(qr);
\end{aligned}$$

2. (Unidade) Para todo $p \in A[x]$,

$$1p = \left(\left(1p_n + \mathop{\Large +}_{i=1}^{n} p_i 0\right)\right)_{n\in\mathbb{N}} = (p_n)_{n\in\mathbb{N}} = p.$$

3. (Comutatividade) Para todos $p, q \in A[x]$,

$$pq = \left(\mathop{\Large +}_{i=0}^{n} p_i q_{n-i}\right)_{n\in\mathbb{N}} = \left(\mathop{\Large +}_{i=0}^{n} q_i p_{n-i}\right)_{n\in\mathbb{N}} = qp.$$

Por fim, mostremos que vale a distributividade. Para todos $p, q, r \in A[x]$,

$$\begin{aligned}
p(q+r) &= \left(\bigplus_{i=0}^{n} p_i(q+r)_{n-i}\right)_{n\in\mathbb{N}} \\
&= \left(\bigplus_{i=0}^{n} p_i(q_{n-i}+r_{n-i})\right)_{n\in\mathbb{N}} \\
&= \left(\bigplus_{i=0}^{n} (p_i q_{n-i}+p_i r_{n-i})\right)_{n\in\mathbb{N}} \\
&= \left(\bigplus_{i=0}^{n} p_i q_{n-i} + \bigplus_{i=0}^{n} p_i r_{n-i}\right)_{n\in\mathbb{N}} \\
&= \left(\bigplus_{i=0}^{n} p_i q_{n-i}\right)_{n\in\mathbb{N}} + \left(\bigplus_{i=0}^{n} p_i r_{n-i}\right)_{n\in\mathbb{N}} \\
&= pq + pr.
\end{aligned}$$

■

Definição 3.17. Seja $\boldsymbol{A}$ um anel. O *grau* de $p \in A[x] \smallsetminus \{0\}$ é o número

$$\operatorname{gr}(p) := \max \operatorname{supp}(p)$$

(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 3.18. Seja $\boldsymbol{A}$ um anel. A *variável* de $A[x]$ é a função

$$\begin{aligned}
x\colon \mathbb{N} &\longrightarrow A \\
n &\longmapsto \begin{cases} 1, & n = 1 \\ 0, & n \neq 1. \end{cases}
\end{aligned}$$

Notemos que, para todo $k \in \mathbb{N}$, x^k é a função

$$\begin{aligned}
x^k\colon \mathbb{N} &\longrightarrow A \\
n &\longmapsto \begin{cases} 1, & n = k \\ 0, & n \neq k \end{cases}
\end{aligned}$$

e assim podemos escrever todo polinômio $p \in A[x]$ como uma soma finita

$$p = \mathop{\mathbin{+}}_{i=0}^{\mathrm{gr}(p)} p_i x^i.$$

Proposição 3.28. *Sejam $\boldsymbol{A}$ um domínio e $p, q \in A[x] \smallsetminus \{0\}$. Então*

$$\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q).$$

Demonstração. Seja $k := \mathrm{gr}(p) + \mathrm{gr}(q)$. O produto pq terá coeficientes $\mathop{\mathbin{+}}_{i=0}^{n} p_i q_{n-i}$, com $n \in \{0, \ldots, k\}$. Notemos que, para $k = \mathrm{gr}(p) + \mathrm{gr}(q)$,

$$\mathop{\mathbin{+}}_{i=0}^{k} p_i q_{k-i} = p_{\mathrm{gr}(p)} q_{\mathrm{gr}(q)}.$$

Isso ocorre porque todos os termos desse somatório se anulam, menos quando $i = \mathrm{gr}(p)$. Se $i > \mathrm{gr}(p)$, temos $p_i = 0$; se $i < \mathrm{gr}(p)$, então $k - i > \mathrm{gr}(p) + \mathrm{gr}(q) - \mathrm{gr}(p) = \mathrm{gr}(q)$, e temos $q_{k-i} = 0$. Em ambos os casos, $p_i q_{k-i} = 0$. Por definição, $p_{\mathrm{gr}(p)} \neq 0$ e $q_{\mathrm{gr}(q)} \neq 0$ e, como $\boldsymbol{A}$ é um domínio, isso implica que $p_{\mathrm{gr}(p)} q_{\mathrm{gr}(q)} \neq 0$. Logo $pq \neq 0$ e $\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q)$. ■

Proposição 3.29. *Seja $\boldsymbol{A}$ um anel. Então $\boldsymbol{A}$ é um domínio se, e somente se, $\boldsymbol{A}[\boldsymbol{x}]$ é um domínio.*

Demonstração. Suponha que $\boldsymbol{A}$ é um domínio e sejam $p_0, p_1 \in A[x] \smallsetminus \{0\}$. Então $\mathrm{gr}(p_0 p_1) = \mathrm{gr}(p_1) + \mathrm{gr}(p_1)$, o que mostra que $p_0 p_1 \neq 0$. Logo $\boldsymbol{A}[\boldsymbol{x}]$ é um domínio. Reciprocamente, suponha que $\boldsymbol{A}[\boldsymbol{x}]$ é um domínio e sejam $a_0, a_1 \in A \smallsetminus \{0\}$. Então $a_0, a_1 \in A[x] \smallsetminus \{0\}$ e, portanto, $a_0 a_1 \neq 0$. Logo $\boldsymbol{A}$ é um domínio. ■

Podemos ver que $\boldsymbol{A}[\boldsymbol{x}]$ nunca é um corpo, pois x não tem inverso.

Anel de Polinômios Multivariados

Definição 3.19. Sejam $\boldsymbol{A}$ um anel e $n \in \mathbb{N}$. O *anel de polinômios* em n variáveis em $\boldsymbol{A}$ é o conjunto

$$A[x_0, \ldots, x_{n-1}] := \left\{ p \in A^{\mathbb{N}^n} \;\middle|\; |\mathrm{supp}(p)| < |\mathbb{N}| \right\}.$$

Os elementos de $A[x]$ são os *polinômios em n variáveis* em $\boldsymbol{A}$.

3.2.2 Produto de Anéis

Definição 3.20. Seja $(\boldsymbol{A_i})_{i\in I} = (A_i, +_i, \times_i)_{i\in I}$ uma família de anéis. O *produto* da família $(\boldsymbol{A_i})_{i\in I}$ é a tripla

$$\prod_{i\in I} \boldsymbol{A_i} := (A, +, \times)$$

em que $A = \prod_{i\in I} A_i$ é o produto de conjuntos,

$$\begin{aligned} +\colon A \times A &\longrightarrow A \\ (a, b) &\longmapsto (a_i +_i b_i)_{i\in I} \end{aligned}$$

e

$$\begin{aligned} \times\colon A \times A &\longrightarrow A \\ (a, b) &\longmapsto (a_i \times_i b_i)_{i\in I}. \end{aligned}$$

Denotaremos as operações $+_i$ todas por $+$ e as operações $\times_i$ todas por $\times$ quando não existir ambiguidade.

Proposição 3.30. *Seja $(\boldsymbol{A_i})_{i\in I} = (A_i, +_i, \times_i)_{i\in I}$ uma família de anéis. Então o produto $\prod_{i\in I} \boldsymbol{A_i}$ 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 popriedades 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

$$\begin{aligned} a \times (b + c) &= a \times (b_i +_i c_i)_{i \in I} \\ &= (a_i \times_i (b_i +_i c_i))_{i \in I} \\ &= ((a_i \times_i b_i) +_i (a_i \times_i c_i))_{i \in I} \\ &= (a_i \times_i b_i)_{i \in I} + (a_i \times_i c_i)_{i \in I} \\ &= (a \times b) + (a \times c). \end{aligned}$$

■

3.3 Construções Específicas

3.3.1 Domínios e Corpos

Definição 3.21. Um *domínio de integridade* (ou *domínio*) é um anel $\boldsymbol{A}$ tal que, para todos $a_0, a_1 \in A$,

$$a_0 \cdot a_1 = 0 \quad \Longrightarrow \quad a_0 = 0 \ \text{ ou } \ a_1 = 0.$$

Definição 3.22. Um *corpo* é um anel $\boldsymbol{A}$ tal que, para todo $a \in A \smallsetminus \{0\}$, existe a^{-1}, de modo que $(A \smallsetminus \{0\}, \times, ^{-1}, 1)$ é um grupo.

Proposição 3.31. *Todo corpo $\boldsymbol{A}$ é um domínio.*

Demonstração. Sejam $a_1, a_2 \in A$ tais que $a_1 \cdot a_2 = 0$. Suponhamos que $a_2 \neq 0$. Então existe $a_2^{-1} \in A$ e temos

$$\begin{aligned} a_1 &= a_1 \cdot 1 \\ &= a_1 \cdot (a_2 \cdot a_2^{-1}) \\ &= (a_1 \cdot a_2) \cdot a_2^{-1} \\ &= 0 \cdot a_2^{-1} \\ &= 0. \end{aligned}$$

Logo, se $a_1 \cdot a_2 = 0$, $a_1 = 0$ ou $a_2 = 0$. ■

Proposição 3.32 (Lei do corte em domínios)**.** *Sejam $\boldsymbol{A}$ um domínio e $a, a_1, a_2 \in A$, $a \neq 0$. Então*

$$aa_1 = aa_2 \quad \Longrightarrow \quad a_1 = a_2$$

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 $\boldsymbol{A}$ 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 $\boldsymbol{A}$ ser um corpo, se $\mathbf{A}$ for um domínio, vale a lei do corte da multiplicação para elementos de $A \setminus \{0\}$.

3.3.2 Divisão e Associação em Anéis

Divisão

Definição 3.23. Sejam $\boldsymbol{A}$ um anel e $a, a' \in A$. O elemento a *divide* o elemento a' em $\boldsymbol{A}$ se, e somente se, existe $q \in A$ tal que $aq = a'$. O elemento a é um *divisor* de a' em $\boldsymbol{A}$, o elemento a' é um *múltiplo* de a em $\boldsymbol{A}$ e denota-se $a \preceq_{\boldsymbol{A}} a'$. A relação $\preceq_{\boldsymbol{A}}$ é a relação de *divisão* em $\boldsymbol{A}$. Sempre que possível, o subíndice de $\preceq_{\boldsymbol{A}}$ será omitido.

Proposição 3.33. *Seja $\boldsymbol{A}$ 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 3.34. *Seja $\boldsymbol{A}$ 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 3.35. *Sejam $\boldsymbol{A}$ 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 implicação invertidas. ■

Definição 3.24. Sejam $\boldsymbol{A}$ um anel e $Q \subseteq A$. Um *divisor comum* de Q em $\boldsymbol{A}$ é um elemento $d \in A$ que satisfaz, para todo $q \in Q$,
$$d \preceq q.$$
O conjunto dos divisores comuns de Q em $\boldsymbol{A}$ é $\mathrm{Div}_{\boldsymbol{A}}(Q)$. O subíndice $\boldsymbol{A}$ será omitido sempre que possível.

Dualmente, um *múltiplo comum* de Q em $\boldsymbol{A}$ é um elemento $m \in A$ que satisfaz, para todo $q \in Q$,
$$q \preceq m.$$
O conjunto dos múltiplos comuns de Q em $\boldsymbol{A}$ é $\mathrm{Mul}_{\boldsymbol{A}}(Q)$. O subíndice $\boldsymbol{A}$ será omitido sempre que possível.

Proposição 3.36. *Sejam $\boldsymbol{A}$ um anel e $Q \subseteq A$. Então*

1. $\mathrm{Div}(A) = \mathrm{Div}(A^*) = A^*$ *e* $\mathrm{Div}(\emptyset) = \mathrm{Div}(\{0\}) = A$;

2. $A^* \subseteq \mathrm{Div}(Q) \subseteq A$*;*

3. $\{0\} \cap \mathrm{Div}(Q) \neq \emptyset \Leftrightarrow Q \subseteq \{0\} \Leftrightarrow \mathrm{Div}(Q) = A$.

Dualmente,

1. $\mathrm{Mul}(A) = \mathrm{Mul}(\{0\}) = \{0\}$ *e* $\mathrm{Mul}(\emptyset) = \mathrm{Mul}(A^*) = A$*;*

2. $\{0\} \subseteq \mathrm{Mul}(Q) \subseteq A$*;*

3. $A^* \cap \mathrm{Mul}(Q) \neq \emptyset \Leftrightarrow Q \subseteq A^* \Leftrightarrow \mathrm{Mul}(Q) = A$.

Demonstração. 1. Seja $u \in A^*$. Então $u \preceq a$ para todo $a \in A$. Logo $u \in \mathrm{Div}(A)$. Por outro lado, seja $d \in \mathrm{Div}(A)$. 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 $u \in \mathrm{Div}(A^*)$. Por outro lado, seja $d \in \mathrm{Div}(A^*)$. Então $d \preceq u$ para todo $u \in A^*$. Logo $d \in A^*$.

Seja $a \in A$. Se $a \notin \mathrm{Div}(\emptyset)$, existe $q \in \emptyset$ tal que $a \not\preceq q$, o que é absurdo. Logo $a \in \mathrm{Div}(\emptyset)$.

Seja $a \in A$. Então $a \preceq 0$, o que implica $a \in \mathrm{Div}(\{0\})$. A inclusão contrária é óbvia pela definição do conjunto dos divisores comuns.

2. Se $Q = \emptyset$, então $\mathrm{Div}(Q) = A$. Se $Q \neq \emptyset$, sejam $q \in Q$ e $u \in A^*$. Então $u \preceq q$. Logo $u \in \mathrm{Div}(Q)$. A inclusão $\mathrm{Div}(Q) \subseteq A$ é óbvia pela definição do conjunto de divisores comuns;

3. Suponhamos que $\{0\} \cap \mathrm{Div}(Q) \neq \emptyset$. Então $0 \in \mathrm{Div}(Q)$. 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 $\mathrm{Div}(Q) = A$.

   Suponhamos que $\mathrm{Div}(Q) = A$. Então $\{0\} \cap \mathrm{Div}(Q) = \{0\} \neq \emptyset$.

Dualmente,

1. Note que $a \preceq 0$ para todo $a \in A$. Logo $0 \in \mathrm{Mul}(A)$. Por outro lado, seja $m \in \mathrm{Mul}(A)$. 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 $0 \in \mathrm{Mul}(\{0\})$. Por outro lado, seja $m \in \mathrm{Mul}(\{0\})$. Então $0 \preceq m$, o que implica $m = 0$.

   Seja $a \in A$. Se $a \notin \mathrm{Mul}(\emptyset)$, existe $q \in \emptyset$ tal que $q \not\preceq a$, o que é absurdo. Logo $a \in \mathrm{Mul}(\emptyset)$.

   Sejam $a \in A$ e $u \in A^*$. Então $u \preceq a$, o que implica $a \in \mathrm{Mul}_{bmA}(A^*)$. A inclusão contrária é óbvia pela definição do conjunto dos múltiplos comuns.

2. Se $Q = \emptyset$, então $\mathrm{Mul}(Q) = A$. Se $Q \neq \emptyset$, seja $q \in Q$. Então $q \preceq 0$, o que implica $\{0\} \in \mathrm{Mul}(Q)$. A inclusão $\mathrm{Mul}(Q) \subseteq A$ é óbvia pela definição do conjunto dos múltiplos comuns;

3. Suponhamos que $A^* \cap \mathrm{Mul}(Q) \neq \emptyset$. Seja $m \in A^* \cap \mathrm{Mul}(Q)$. Se $Q = \emptyset$, então $Q \subseteq A^*$. Caso contrário, seja $q \in Q$. Como $q \preceq m$, pois $m \in \mathrm{Mul}(Q)$, 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 $\mathrm{Mul}(Q) = A$. Caso contrário, sejam $q \in Q$ e $a \in A$. Então $q \in A^*$ e segue que $q \preceq a$. Logo $a \in \mathrm{Mul}(Q)$. Por outro lado, a inclusão $\mathrm{Mul}(Q) \subseteq A$ é óbvia pela definição do conjunto de múltiplos comuns;

   Suponhamos que $\mathrm{Mul}(Q) = A$. Então $A^* \cap \mathrm{Mul}(Q) = A^*$. Como $1 \in A^*$, segue que $A^* \cap \mathrm{Mul}(Q) \neq \emptyset$. ■

Definição 3.25. Sejam $\boldsymbol{A}$ um anel e $Q \subseteq A$. Um *máximo divisor comum* de Q em $\boldsymbol{A}$ é um elemento $d \in A$ que satisfaz

1. $d \in \mathrm{Div}(Q)$;

2. Para todo $d' \in \mathrm{Div}(Q)$, $d' \preceq d$.

O conjunto dos máximos divisores comuns de Q em $\boldsymbol{A}$ é $\mathrm{mdc}_{\boldsymbol{A}}(Q)$. Se Q é um conjunto finito $Q = \{a_1, \ldots, a_n\}$, denota-se $\mathrm{mdc}_{\boldsymbol{A}}(Q) = \mathrm{mdc}_{\boldsymbol{A}}(a_1, \ldots, a_n)$ ou $\mathrm{mdc}_{\boldsymbol{A}}(Q) = (a_1, \ldots, a_n)$. O subíndice $\boldsymbol{A}$ será omitido sempre que possível.

Dualmente, um *mínimo múltiplo comum* de Q em $\boldsymbol{A}$ é um elemento $m \in A$ que satisfaz

1. $m \in \mathrm{Mul}_{\boldsymbol{A}}(Q)$;

2. Para todo $m' \in \mathrm{Mul}(Q)$, $m \preceq m'$.

O conjunto dos mínimos múltiplos comuns de Q em $\boldsymbol{A}$ é $\mathrm{mmc}_{\boldsymbol{A}}(Q)$. Se Q é um conjunto finito $Q = \{a_1, \ldots, a_n\}$, denota-se $\mathrm{mmc}_{\boldsymbol{A}} = \mathrm{mmc}_{\boldsymbol{A}}(a_1, \ldots, a_n)$ ou $\mathrm{mmc}_{\boldsymbol{A}}(Q) = [a_1, \ldots, a_n]$. O subíndice $\boldsymbol{A}$ será omitido sempre que possível.

Proposição 3.37. *Sejam $\boldsymbol{A}$ um anel e $Q \subseteq A$. Então*

1. $Q \subseteq \{0\} \Leftrightarrow \mathrm{mdc}(Q) = \{0\}$;

2. $A^* \cap Q \neq \emptyset \Rightarrow \mathrm{mdc}(Q) = A^*$.

Dualmente,

1. $Q \subseteq A^* \Leftrightarrow \mathrm{mmc}(Q) = A^*$;

2. $\{0\} \cap Q \neq \emptyset \Rightarrow \mathrm{mmc}(Q) = \{0\}$.

Demonstração. 1. Suponha que $Q \subseteq \{0\}$. Então $A = \mathrm{Div}(Q)$. Em particular, $0 \in \mathrm{Div}(Q)$. Ainda, para todo $d \in \mathrm{Div}(Q)$, vale que $d \preceq 0$, pois $d \in A$. Logo $0 \in \mathrm{mdc}(Q)$. Ainda, se $d \in \mathrm{mdc}(Q)$, então $0 \preceq d$, pois $0 \in \mathrm{Div}(Q)$ e $d \in \mathrm{mdc}(Q)$. Portanto $d = 0$. Reciprocamente, se $\mathrm{mdc}(Q) = \{0\}$, então $0 \in \mathrm{Div}(Q)$; ou seja, $\{0\} \cap \mathrm{Div}(Q) \neq \emptyset$, 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 $u \in \mathrm{Div}(Q)$. Ainda, se $d \in \mathrm{Div}(Q)$, então, em particular, $d \preceq a$. Mas como $a \in A^*$, segue que $d \in A^*$. Logo $d \preceq u$, o que mostra que $u \in \mathrm{mdc}(Q)$. Por outro lado, se $d \in \mathrm{mdc}(Q)$, então $d \preceq a$. Como $a \in A^*$, então $d \in A^*$, e concluímos que $A^* = \mathrm{mdc}(Q)$.

Dualmente,

1. Suponha que $Q \subseteq A^*$. Então $A = \mathrm{Mul}(Q)$. Seja $u \in A^*$. Então $u \in \mathrm{Mul}(Q)$. Ainda, para todo $m \in \mathrm{Mul}(Q)$, vale que $u \preceq m$, pois $m \in A$. Logo $u \in \mathrm{mmc}(Q)$. Ainda, se $m \in \mathrm{mmc}(Q)$, então $m \preceq u$, pois $u \in \mathrm{Mul}(Q)$ e $m \in \mathrm{mmc}(Q)$. Portanto $m \in A^*$. Reciprocamente, se $\mathrm{mmc}(Q) = A^*$, então $1 \in \mathrm{Mul}(Q)$; ou seja, $A^* \cap \mathrm{Mul}(Q) \neq \emptyset$, o que implica $Q \subseteq A^*$.

2. Como $\{0\} \cap Q \neq \emptyset$, então $0 \in Q$. Note que $0 \in \mathrm{Mul}(Q)$. Ainda, se $m \in \mathrm{Mul}(Q)$, então $0 \preceq m$. Então segue que $0 \in \mathrm{mmc}(Q)$. Por outro lado, se $m \in \mathrm{mmc}(Q)$, então $0 \preceq m$, o que implica $m = 0$, e concluímos que $\mathrm{mmc}(Q) = \{0\}$. ■

Relação de Associação

Definição 3.26. Sejam $\boldsymbol{A}$ um anel e $a, a' \in A$. O elemento a é *associado* ao elemento a' em $\boldsymbol{A}$ se, e somente se, $a \preceq_{\boldsymbol{A}} a'$ e $a' \preceq_{\boldsymbol{A}} a$. Denota-se $a \sim_{\boldsymbol{A}} a'$. A relação $\sim_{\boldsymbol{A}}$ é a relação de *associação* em $\boldsymbol{A}$. Sempre que possível, o subíndice de $\sim_{\boldsymbol{A}}$ 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 3.38. *Sejam $\boldsymbol{A}$ 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 $\boldsymbol{A}$ 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 $a \sim a'$. ■

Proposição 3.39. *Seja* $\boldsymbol{A}$ *um anel.*

1. *Para todos* $a_0, \ldots, a_{n-1}, a'_0, \ldots, a'_{n-1} \in A$, *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 $a_0, \ldots, a_{n-1}, a'_0, \ldots, a'_{n-1} \in A$ 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
$$\bigtimes_{i\in[n]} a_i \sim \bigtimes_{i\in[n]} a'_i.$$
■

Proposição 3.40. *Sejam* $\boldsymbol{D}$ *um domínio e* $d_0, \ldots, d_{n-1} \in D$ *não todos nulos. Se* d, d' *são máximos divisores comuns de* $d_0, \ldots, d_{n-1}$, *então* $d \sim d'$.

Demonstração. Como d é máximo divisor comum de $d_0, \ldots, d_{n-1}$ e d' é divisor comum de $d_0, \ldots, d_{n-1}$, então $d' \preceq d$. Analogamente, $d \preceq d'$. Portanto $d \sim d'$. ■

3.3.3 Irredutíveis, Primos e Fatoração

Definição 3.27. Seja $\boldsymbol{D}$ um domínio. Um elemento *irredutível* em $\boldsymbol{D}$ é um elemento $i \in D \smallsetminus (D^* \cup \{0\})$ que satisfaz, para todos $d, d' \in D$ tais que $i = dd'$,
$$d \in D^* \quad \text{ou} \quad d' \in D^*.$$

Proposição 3.41. *Sejam* $\boldsymbol{D}$ *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 $\boldsymbol{D}$ 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 $u^{-1}d' \neq 0$. Logo segue que $i = (u^{-1}d)d'$, uma contradição porque i é irredutível. ■

Definição 3.28. Seja $\boldsymbol{D}$ um domínio. Um elemento *primo* em $\boldsymbol{D}$ é um elemento $p \in D \smallsetminus (D^* \cup \{0\})$ que satisfaz, para todos $d, d' \in D$ tais que $p \preceq dd'$,
$$p \preceq d \quad \text{ou} \quad p \preceq d'.$$

Proposição 3.42. *Sejam $\boldsymbol{D}$ um domínio e p primo.*

1. *Para todo $p' \in D$ tal que $p \sim p'$, p' é primo;*
2. *Para todos $d_0, \ldots, d_{n-1}$ 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 irredutível.*

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 $\boldsymbol{D}$ 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 propridade 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 $\boldsymbol{D}$ é domínio, $1 = qd'$. Logo $d' \in D^*$. Analogamente, se $p \preceq d'$, segue que $d \in D^*$ (usamos a comutatividade). Portanto p é irredutível.

■

Proposição 3.43. *Seja $\boldsymbol{D}$ um domínio euclidiano que não é um corpo e ϕ uma função euclidiana em $\boldsymbol{D}$. Então $d_0 \in D$ tal que*

$$\phi(d_0) = \min \{\phi(d) \mid d \in D \smallsetminus (D^* \cup \{0\})\}$$

é um elemento irredutível em $\boldsymbol{D}$.

Demonstração. Primeiro, definamos $m := \min \{\phi(d) \mid d \in D \smallsetminus (D^* \cup \{0\})\}$ 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 $d_0 = d_1 d_2$, com $d_1, d_2 \in D$. Como $\boldsymbol{D}$ é um domínio, então $d_1 \neq 0$ e $d_2 \neq 0$. Suponha que $d_1, d_2 \notin D^*$. Então $\phi(d_1) \geq m = \phi(d_1 d_2) \geq \phi(d_1)$ e $\phi(d_2) \geq m = \phi(d_1 d_2) \geq \phi(d_2)$. Logo $\phi(d_1) = \phi(d_1 d_2)$ e $\phi(d_2) = \phi(d_1 d_2)$, o que implica $d_1, d_2 \in D^*$, que é absurdo. ■

Fatoração

Definição 3.29. Sejam $\boldsymbol{D}$ um domínio, $a \in D \smallsetminus \{0\}$ 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 exite 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 $a \in D \smallsetminus \{0\}$ 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 3.44. *Seja $\boldsymbol{D}$ 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 3.30. Um *domínio de fatoração única* é um domínio $\boldsymbol{D}$ que satisfaz

1. (Existência de Fatoração) Todo elemento $d \in D \smallsetminus \{0\}$ tem fatoração;
2. (Unicidade de Fatoração) Todas fatorações de $d \in D \smallsetminus \{0\}$ são associadas.

Domínios de fatoração única também são chamados de domínios fatoriais. Antes de demosntrar a próxima proposição, enunciamos um lema simples que usaremos na demonstração.

Lema 3.45. *Para todo $k \in [n]$, a função*

$$\begin{aligned} f_k \colon [n-1] &\longrightarrow [n] \smallsetminus \{k\} \\ i &\longmapsto \begin{cases} i, & i < k \\ i+1, & i \geq k. \end{cases} \end{aligned}$$

é bijetiva e sua inversa é

$$\begin{aligned} {f_k}^{-1} \colon [n] \smallsetminus \{k\} &\longrightarrow [n-1] \\ i &\longmapsto \begin{cases} i, & i < k \\ i-1, & i > k \end{cases} \end{aligned}$$

Para toda permutação $\sigma' \colon [n-1] \longrightarrow [n-1]$, a função

$$\begin{aligned} \sigma \colon [n] &\longrightarrow [n] \\ i &\longmapsto \begin{cases} f_k \circ \sigma'(i), & i < n-1 \\ k, & i = n-1, \end{cases} \end{aligned}$$

é uma permutação.

A proposição a seguir relaciona duas noções da teoria de fatoação em anéis. A primeira é a unicidade de fatoração e a segunda é a relação entre elementos irredutíveis e primos.

Proposição 3.46. *Seja $\boldsymbol{D}$ um domínio tal que todo elemento não nulo tem fatoração. Então as fatorações de $d \in D \smallsetminus \{0\}$ são todas associadas se, e somente se, todo elemento irredutível de $\boldsymbol{D}$ é primo.*

Demonstração. Suponhamos, primeiro, que todas fatorações de $d \in D \smallsetminus \{0\}$ são associadas. Sejam p irredutível 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 $d, d \in D \smallsetminus \{0\}$, 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

$$p \bigtimes_{i\in[m]} q_i \sim pq \sim \left(\bigtimes_{i\in[n]} p_i\right)\left(\bigtimes_{i\in[n']} p'_i\right).$$

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 irredutível de $\boldsymbol{D}$ é primo. Sejam $d \in D \smallsetminus \{0\}$, e $(p_i)_{i\in[n]}$ e $(p'_i)_{i\in[n']}$ fatorações de d, de modo que

$$\bigtimes_{i\in[n]} p_i \sim d \sim \bigtimes_{i\in[n']} p'_i.$$

Todos os irredutíveis $p_0, \ldots, p_{n-1}$ e $p'_0, \ldots, p'_{n'-1}$ 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 $d \in D \smallsetminus \{0\}$ 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 irredutíveis, então $q \in D^*$. Portanto segue que

$$\begin{aligned}\left(\bigtimes_{i\in[n-1]} p_i\right) p_{n-1} &\sim \left(\bigtimes_{i\in[k]} p'_i\right) p_{n-1} \left(\bigtimes_{i\in[n'-k-1]} p'_{i+k+1}\right)\\ &= \left(\bigtimes_{i\in[k]} p'_i\right)\left(\bigtimes_{i\in[n'-k-1]} p'_{i+k+1}\right) p_{n-1}.\end{aligned}$$

Como $\boldsymbol{D}$ é domínio e $p_{n-1} \neq 0$, então

$$\bigtimes_{i\in[n-1]} p_i \sim \left(\bigtimes_{i\in[k]} p'_i\right)\left(\bigtimes_{i\in[n'-k-1]} p'_{i+k+1}\right).$$

Considerando a bijeção (3.45)

$$\begin{aligned} f_k \colon [n-1] &\longrightarrow [n] \smallsetminus \{k\}\\ i &\longmapsto \begin{cases} i, & i < k\\ i+1, & i \geq k\end{cases}\end{aligned}$$

e definindo, para todo $i \in [n'] \smallsetminus \{k\}$, $q_i := p'_{f_k(i)}$, temos uma sequência de irredutíveis $(q_i)_{i\in[n'-1]}$ 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 (3.45)

$$\begin{aligned} \sigma\colon [n] &\longrightarrow [n] \\ i &\longmapsto \begin{cases} f_k \circ \sigma'(i), & i < n-1 \\ k, & i = n-1, \end{cases} \end{aligned}$$

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. ■

Definição 3.31. Sejam $\boldsymbol{D}$ um domínio, $a \in D \smallsetminus \{0\}$ 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 irredutíveis 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 3.47. *Seja $\boldsymbol{D}$ um domínio de fatoração única. Então*

1. *(Existência de Fatoração Reduzida) Todo $d \in D \smallsetminus \{0\}$ tem fatoração reduzida;*
2. *(Unicidade de Fatoração Reduzida) Para todo $d \in D \smallsetminus \{0\}$, 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 $d \in D \smallsetminus \{0\}$. Como $\boldsymbol{D}$ é domínio de fatoração única, existe fatoração $(p'_i)_{i\in[n']}$ de d em irredutíveis tais que

$$d \sim \bigtimes_{i\in[n']} p'_i.$$

Vamos considerar os conjuntos $I_i := \left\{ j \in [n'] \;\middle|\; p'_j \sim p'_i \right\}$ 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 $P_0, \ldots, P_{n-1}$ 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 irredutível 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 3.48. *Seja $\boldsymbol{D}$ um domínio de fatoração única. Então, para todos $a, b \in D \smallsetminus \{0\}$, existe $d \in \operatorname{mdc}(a, b)$.*

Demonstração. Se $\{a, b\} \cap D^* \neq \emptyset$, então $\operatorname{mdc}(a, b) = D^*$. Suponhamos, então, que $\{a, b\} \notin D \smallsetminus (D^* \cup \{0\})$. Como $\boldsymbol{D}$ 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 $\mathrm{mdc}(a, b) = D^*$. Para isso, mostraremos que $1 \in \mathrm{mdc}(a, b)$. Notamos que $1 \in D^* \subseteq \mathrm{Div}(a, b)$. Agora, seja $d \in \mathrm{Div}(a, b)$. Como $0 \notin \{a, b\}$, então $0 \notin \mathrm{Div}(a, b)$. Se $d \in D^*$, então $d \preceq 1$, logo $1 \in \mathrm{mdc}(a, b)$. Se $d \in D \smallsetminus (D^* \cup \{0\})$, então existe p irredutível tal que $p \preceq d$, portanto $p \preceq a$ e $p \preceq b$. Como $\boldsymbol{D}$ 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 elementoss são irredutíveis, $p \sim p_i$ e $p \sim q_j$, portanto $p_i \sim q_j$, o que é uma constradição. Logo $1 \in \mathrm{mdc}(a, b)$. Como todos os máximos divisores comuns são associados, então $D^* = \mathrm{mdc}(a, b)$.

Se $k \geq 1$, mostraremos que $p_1 \cdots p_k \in \mathrm{mdc}(a, b)$. 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 trasitividade de $\preceq$, segue que $p_1 \cdots p_k \preceq b$. Logo $p_1 \cdots p_k \in \mathrm{Div}(a, b)$. Então, seja $d \in \mathrm{Div}(a, b)$. Se $d \in D^*$, então $d \preceq p_1 \cdots p_k$. Logo $p_1 \cdots p_k \in \mathrm{mdc}(a, b)$. Se $d \in D \smallsetminus (D^* \cup \{0\})$, então existem $r_1, \ldots, r_l$ irredutíveis tais que $d = r_1 \cdots r_l$. Por $\boldsymbol{D}$ ser domínio, $r_1, \ldots, r_l$ são primos. Como $d \preceq a$, então $r_1 \preceq p_1 \cdots p_k$. Como r_1 é primo, existe $i_1 \in \{1, \ldots, k\}$ 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 $\boldsymbol{D}$ é domínio. Repetindo o processo indutivamente, conclui-se que existem $i_1, \ldots, i_m$ tais que $r_j \sim p_{i_j}$ para todo $j \in \{1, \ldots, l\}$. Da mesma forma, conclui-se que que existem $i'_1, \ldots, i'_m$ tais que $r_j \sim q_{i'_j}$ para todo $j \in \{1, \ldots, l\}$. Portanto, da reflexividade e transitividade de $\sim$, segue que $p_{i_j} \sim q_{i'_j}$ para todo i, j. Então $d \sim p_{i_1} \cdots p_{i_m} \sim q_{i'_1} \cdots q_{i'_m}$. Como $p_{i_1} \cdots p_{i_m} \preceq p_1 \cdots p_k$ e $q_{i'_1} \cdots q_{i'_m} \preceq q_1 \cdots q_k$, então $d \preceq p_1 \cdots p_k$. ■

3.3.4 Ideais Primos e Ideais Maximais

Definição 3.32. Seja $\boldsymbol{A}$ um anel. Um *ideal primo* de $\boldsymbol{A}$ é um ideal $I \trianglelefteq A$ tal que

1. $\bigwedge a, b \in A \qquad ab \in I \Rightarrow a \in I \;\text{ ou }\; b \in I.$

Teorema 3.49. *Seja $\boldsymbol{A}$ um anel e $I \trianglelefteq A$. Então I é um ideal primo de $\boldsymbol{A}$ se, e somente se, $\boldsymbol{A/I}$ é um domínio.*

Demonstração. Vamos demonstrar as duas implicações ao mesmo tempo. Sejam $a, b \in A$ e $\alpha, \beta \in A/I$ tais que $\alpha = a + I$ e $\beta = b + I$. Note que $\boldsymbol{A/I}$ é um domínio se, e somente se,

$$\bigwedge \alpha, \beta \in A/I \qquad \alpha\beta = 0_{A/I} \Rightarrow \alpha = 0_{A/I} \;\text{ ou }\; \beta = 0_{A/I}.$$

Mas $\alpha\beta = (a + I)(b + I) = ab + I$ e $0_{A/I} = 0 + I$. Ainda, para qualquer $a' \in A$, $a' + I = 0 + I$ se, e somente se, $a' \in I$. Logo segue que a implicação acima é equivalente a

$$\bigwedge a, b \in A \qquad ab = 0 \Rightarrow a = 0 \;\text{ ou }\; b = 0,$$

que é a definição de ideal primo. ■

Definição 3.33. Seja $\boldsymbol{A}$ um anel. Um *ideal maximal* de $\boldsymbol{A}$ é um ideal $I \lhd A$ tal que

$$\bigwedge J \in \mathsf{P}(A) \qquad I \subseteq J \;\text{ e }\; J \trianglelefteq A \Rightarrow J = I \;\text{ ou }\; J = A.$$

Teorema 3.50. *Seja $\boldsymbol{A}$ um anel e $I \lhd A$. Então I é um ideal maximal de $\boldsymbol{A}$ se, e somente se, $\boldsymbol{A/I}$ é um corpo.*

Demonstração. Em ambas implicações, usaremos o fato que um anel é um corpo se, e somente se, seus únicos ideais são o anel trivial e o anel todo (3.8).

$\Leftarrow$ Suponha que I é um ideal maximal de $\boldsymbol{A}$. Vamos mostrar que os únicos ideais de $\boldsymbol{A/I}$ são $\{0+I\}$ e A/I. Seja $L \trianglelefteq A/I$ e consideremos a projeção canônica

$$\begin{aligned} \pi\colon A &\longrightarrow {}^{A}\!/_{I} \\ a &\longmapsto a + I. \end{aligned}$$

Sabemos que $\pi^{-1}(L) = \{a \in A : \pi(a) \in L\} \trianglelefteq A$ (3.16). Como $0+I = 0_{A/I} \in L$, isso implica que $\pi^{-1}(0+I) \subseteq \pi^{-1}(L)$. Notando que $\pi^{-1}(0+I) = \mathrm{nuc}(\phi) = I$, 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 $\boldsymbol{A/I}$ 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 $\pi(J) \trianglelefteq A/I$ (3.17). Como $\boldsymbol{A/I}$ é corpo, $\pi(J) = 0_{A/I}$ ou $\pi(J) = A/I$. No primeiro caso, $J = \mathrm{nuc}(\pi) = I$. No segundo caso, $J = \pi^{-1}(\pi(J)) = \pi^{-1}(A/I) = A$. Logo I é ideal maximal de A.

■

Proposição 3.51. *Seja $\boldsymbol{A}$ um anel e $I \lhd A$ um ideal maximal. Então I é ideal primo.*

Demonstração. A demonstração é simples. Sabemos que, se I é ideal maximal, então A/I é um corpo (3.50). Mas isso implica que A/I é um domínio (3.31). Concluímos, portanto, que I é um ideal primo (3.49). ■

3.3.5 Domínios Euclidianos

Definição 3.34. Seja $\boldsymbol{D}$ um domínio. Uma *função euclidiana* em $\boldsymbol{D}$ é uma função $\phi : D \smallsetminus \{0\} \longrightarrow \mathbb{N}$ que satisfaz

1. Para todos $a \in D$ e $b \in D \smallsetminus \{0\}$, existem $q, r \in D$ tais que
   (a) $a = qb + r$;
   (b) $r = 0$ ou $\phi(r) < \phi(b)$;
2. Para todos $a, b \in D \smallsetminus \{0\}$, $\phi(a) \leq \phi(ab)$.

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 3.52. *Sejam $\boldsymbol{D}$ um domínio e $\phi : D \smallsetminus \{0\} \longrightarrow \mathbb{N}$ uma função que satisfaz*

1. *Para todos $a \in D$ e $b \in D \smallsetminus \{0\}$, 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 $\boldsymbol{D}$.

Proposição 3.53. *Sejam $\boldsymbol{D}$ um domínio, ϕ uma função euclidiana em $\boldsymbol{D}$ e $a, b \in D$.*

Definição 3.35. Um *domínio euclidiano* é um domínio em que existe uma função euclidiana.

Proposição 3.54. *Os anéis $\mathbb{Z}$ e $\mathbb{Z}[i]$ são domínios euclidianos.*

Proposição 3.55. *Seja $\boldsymbol{C}$ um corpo. Então $\boldsymbol{C}[\boldsymbol{x}]$ é um domínio euclidiano.*

Definição 3.36. Um *domínio principal* é um domínio em que todo ideal é principal.

Proposição 3.56. *Seja $\boldsymbol{D}$ um domínio euclidiano. Então $\boldsymbol{D}$ é um domínio principal.*

Demonstração. Seja ϕ uma função euclidiana em $\boldsymbol{D}$ e $I \trianglelefteq D$. Se $I = \{0\}$, então $I = 0I$. Se $I \neq 0$, seja $a \in I \smallsetminus \{0\}$ tal que $\phi(a) = \min\{\phi(i) \mid a \in I \smallsetminus \{0\}\}$. 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 $\phi(a) = \min\{\phi(i) \mid a \in I \smallsetminus \{0\}\}$. Logo $r = 0$, o que implica $b = aq$; ou seja, $I \subseteq aD$. Como a inclusão inversa sempre vale, então $I = aD$. ■

Proposição 3.57. *Sejam $\boldsymbol{D}$ um domínio eucidiano, ϕ uma função euclidiana em $\boldsymbol{D}$ e $d_1, d_2 \in D \smallsetminus \{0\}$. Então $d_1 \in D^*$ se, e somente se, $\phi(d_2) = \phi(d_1 d_2)$.*

Demonstração. Se $d_1 \in D^*$, então existe $d_1^{-1} \in D$. Assim, temos que $\phi(d_1 d_2) \leq \phi(d_1 d_2 d_1^{-1}) = \phi(d_2)$. Por outro lado, sempre vale $\phi(d_2) \leq \phi(d_1 d_2)$. Logo $\phi(d_1 d_2) = \phi(d_2)$. Por outro lado, suponha $\phi(d_1 d_1) = \phi(d_2)$. Existem $q, r \in D$ tais que $d_2 = d_1 d_2 q + r$. Se $r \neq 0$, então, como $r = d_2 - d_1 d_2 q = d_2(1 - d_1 q)$ e $\boldsymbol{D}$ é domínio, segue que $1 - qa \neq 0$. Logo $\phi(r) = \phi(d_2(1 - d_1 q)) \geq \phi(d_2) = \phi(d_1 d_2)$, contradição. Logo $r = 0$ e temos $d_2 = d_1 d_2 q$. Como $d_2 \neq 0$ e $\boldsymbol{D}$ é domínio, então $d_1 q = 1$, o que implica $d_1 \in D^*$. ■

Proposição 3.58. *Seja $\boldsymbol{D}$ um domínio euclidiano e ϕ uma função eucliana em $\boldsymbol{D}$. Então*

$$D^* = \{d \in D \mid \phi(d) = \phi(1)\}.$$

Demonstração. Tome $d_2 = 1$ na proposição anterior. ■

3.3.6 Raízes de Polinômios

Proposição 3.59. *Seja $\boldsymbol{A}$ um anel e $f, g \in A[x]$. Se g é mônico, então existem $q, r \in A[x]$ tais que $f = qg + r$ e $r = 0$ ou $\operatorname{gr}(r) < \operatorname{gr}(g)$.*

Demonstração. Sejam $n := \operatorname{gr}(f)$, $m := \operatorname{gr}(g)$,

$$f = \mathop{\bigplus}_{i=0}^{n} a_i x^i \quad \text{e} \quad g = \mathop{\bigplus}_{i=0}^{m-1} b_i x^i + x^m$$

Se $m \leq n$, definimos $q(x) := a_n x^{n-m}$ e $r := f - qg$ e temos

$$\begin{aligned}
r(x) &= f(x) - q(x)g(x) \\
&= \mathop{\bigplus}_{i=0}^{n} a_i x^i - a_n x^{n-m} \left(\mathop{\bigplus}_{i=0}^{m-1} b_i x^i + x^m \right) \\
&= \mathop{\bigplus}_{i=0}^{n} a_i x^i - \left(\mathop{\bigplus}_{i=0}^{m-1} a_n b_i x^{n-m+i} + a_n x^n \right) \\
&= \mathop{\bigplus}_{i=0}^{n-1} a_i x^i - \mathop{\bigplus}_{i=n-m}^{n-1} a_n b_{i-n+m} x^i \\
&= \mathop{\bigplus}_{i=0}^{n-m-1} a_i x^i + \mathop{\bigplus}_{i=n-m}^{n-1} (a_i - a_n b_{i-n+m}) x^i.
\end{aligned}$$

Daí, segue que, se $r \neq 0$, $\operatorname{gr}(r) \leq n - 1 < m \leq \operatorname{gr}(g)$.

... TERMINAR, USEI ISSO NUMA DEMONSTRAÇÃOMAIS A FRENTE, TENHO QUE DEMMONSTRAR. ■

Definição 3.37. Sejam $\boldsymbol{A}$ 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

$$p(a) := \mathop{+}_{i=0}^{n} p_i a^i \in A.$$

Definição 3.38. Sejam $\boldsymbol{A}$ um anel e $p \in A[x]^* = A[x] \smallsetminus A$. Uma *raiz* de p é um elemento $r \in A$ tal que $p(r) = 0$.

Proposição 3.60. *Sejam $\boldsymbol{A}$ um anel, $p \in A[x]^*$ e $r \in A$. Então r é raiz de p se, e somente se, existe $q \in A[x]$ tal que $p(x) = (x - r)q(x)$.*

Demonstração. Primeiro, notemos que, se existe $q \in A[x]$ tal que $p(x) = (x - r)q(x)$, então $p(r) = (r - r)q(r) = 0q(r) = 0$. Reciprocamente, suponhamos que r é raiz de p.

... ■

3.4 Corpos

3.4.1 Extensões de Corpos

Definição 3.39. Seja $\boldsymbol{C}$ um corpo. Uma *extensão* de $\boldsymbol{C}$ é um corpo $\boldsymbol{E}$ tal que $\boldsymbol{C}$ é um subcorpo de $\boldsymbol{E}$.

Proposição 3.61. *Sejam $\boldsymbol{C}$ um corpo e $\boldsymbol{E} = (E, +, \cdot)$ uma extensão de $\boldsymbol{C}$. Então $(E, \oplus, \odot)$ é um espaço vetorial sobre $\boldsymbol{C}$, em que $\oplus := +$ e $\odot := \cdot|_{C \times E}$.*

Demonstração. Como $\boldsymbol{E}$ é um anel, então $(E, \oplus) = (E, +)$ é um grupo comutativo com elemento neutro 0 do corpo. Agora, como $\odot$ é a restrição de $\cdot$ a $C \times E$, então, para todo $e \in E$, $1 \odot e = 1e = e$ e, para todos $c_1, c_2 \in C$, $(c_1 \cdot c_2) \odot e = c_1 c_2 e = c_1 \odot (c_2 \odot e)$. Por fim, como $\cdot$ é distributiva sobre $+$, segue que, para todos $c \in C$ e $e_1, e_2 \in E$, $c \odot (e_1 \oplus e_2) = c(e_1 + e_2) = ce_1 + ce_2 = c \odot e_1 \oplus c \odot e_2$ e, para todos $c_1, c_2 \in C$ e $e \in E$, $(c_1 + c_2) \odot e = (c_1 + c_2)e = c_1 e + c_2 e = c_1 odote \oplus c_2 \odot e$. Por tanto, concluímos que $(E, \oplus, \odot)$ é um espaço vetorial sobre $\boldsymbol{C}$. ■

Notação. Nesse caso, quando não houver ambiguidade, denotaremos $\oplus$ como $+$ e $\odot$ como $\cdot$, bem como todas outras notações relacionadas às operações do espaço veorial.

Definição 3.40. Sejam $\boldsymbol{C}$ um corpo e $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$. Então a *dimensão* da extensão $\boldsymbol{E}$ com respeito a $\boldsymbol{C}$ é a dimensão do espaço vetorial $\boldsymbol{E}$ sobre $\boldsymbol{C}$. A extensão $\boldsymbol{E}$ é *finita* de sua dimensão é finita e *infitina* se sua dimensão é infinita.

Definição 3.41. Sejam $\boldsymbol{C}$ um corpo e $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$. Um *elemento algébrico* sobre $\boldsymbol{C}$ é um elemento $\alpha \in E$ que é raiz de um polinômio em $C[x]^*$.

Proposição 3.62. *Sejam $\boldsymbol{C}$ um corpo e $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$. Então*

1. *Todo elemento de C é algébrico sobre $\boldsymbol{C}$;*
2. *Se $\alpha \in E \smallsetminus \{0\}$ é um elemento algébrico sobre $\boldsymbol{C}$, então existem $c_0, \ldots, c_n \in C$ tais que $c_0 \neq 0$ e*
$$\mathop{+}_{i=0}^{n} c_i \alpha^i = 0.$$

Demonstração. 1. Seja $\alpha \in C$. Então $\alpha \in E$, pois $C \subseteq E$. Tomando $p(x) = x - \alpha$, temos que $p(\alpha) = \alpha - \alpha = 0$.

2. Sejam $\alpha \in E$ um elemento algébrico sobre $\boldsymbol{C}$ e $c'_0, \ldots, c'_m \in C$ tais que
$$\mathop{+}_{i=0}^{m} c'_i \alpha^i = 0.$$
Como $c'_0, \ldots, c'_m$ não são todos nulos, seja $k := \min\{i \in \{0, \ldots, m\} : c'_i \neq 0\}$. Então, para todo $i < k$, $c'_i = 0$, e segue que
$$0 = \mathop{+}_{i=0}^{m} c'_i \alpha^i = \mathop{+}_{i=k}^{m} c'_i \alpha^i = \alpha^k \mathop{+}_{i=k}^{m} c'_i \alpha^{i-k}$$
e, como E é corpo e $\alpha \neq 0$, podemos dividir por α^k em ambos lados e temos
$$\mathop{+}_{i=k}^{m} c'_i \alpha^{i-k} = 0.$$
Fazendo, $n := m - k$ e, para todo $i \in \{0, \ldots, n\}$, $c_i := c'_{k+i}$, temos que $c_0, \ldots, c_n \in E$ — com $c_0 = c'_k \neq 0$ e, portanto, não todos nulos — tais que
$$\mathop{+}_{i=0}^{n} c_i \alpha^i = \mathop{+}_{i=0}^{n} c'_{k+i} \alpha^i = \mathop{+}_{i=k}^{m} c'_i \alpha^{i-k} = 0.$$

■

Definição 3.42. Sejam $\boldsymbol{C}$ um corpo, $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$ e $\alpha \in E$ um elemento algébrico sobre $\boldsymbol{C}$. Um *polinômio minimal* de α sobre $\boldsymbol{C}$ é um polinômio $p \in C[x]$ que satisfaz

1. $p(\alpha) = 0$;
2. p é mônico;
3. $\mathrm{gr}(p) = \min\{\mathrm{gr}(f) : f \in C[x]^*, f(\alpha) = 0 \text{ e } f \text{ é mônico}\}$.

Proposição 3.63. *Sejam $\boldsymbol{C}$ um corpo, $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$ e $\alpha \in E$ um elemento algébrico sobre $\boldsymbol{C}$. Então existe um único polinômio minimal de α sobre $\boldsymbol{C}$.*

Demonstração. Pela definição de elemento algébrico, existe $p \in C[x]^*$ tal que $p'(\alpha) = 0$. Seja $n := \mathrm{gr}(p')$ e $p'(x) = +_{i=0}^{n} a'_i x^i$. Como $\boldsymbol{C}$ é corpo e $a'_n \neq 0$, existe $(a'_n)^{-1} \in C$. Definindo

$$p := (a'_n)^{-1} p = \mathop{+}_{i=0}^{n-1} (a'_n)^{-1} a_i x^i + x^n,$$

segue que $p \in C[x]^*$, $\mathrm{gr}(p) = n$, $p(\alpha) = (a'_n)^{-1} p'(\alpha) = 0$ e p é mônico. Portanto $\{\mathrm{gr}(f) : f \in C[x]^*, f(\alpha) = 0 \text{ e } f \text{ é mônico}\}$ não é vazio, e, como é subconjunto de $\mathbb{N}$, admite mínimo, o que mostra que existe polinômio minimal de α sobre $\boldsymbol{C}$.

Para mostrar a unicidade, suponhamos que p_1 e p_2 são polinômios minimais de α sobre $\boldsymbol{C}$. Pela primeira propriedade de polinômio minimal, $(p_1 - p_2)(\alpha) = p_1(\alpha) - p_2(\alpha) = 0$. Pela terceira propriedade de polinômio minimal, $\mathrm{gr}(p_1) = \mathrm{gr}(p_2)$. Seja $n := \mathrm{gr}(p_1)$ 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

$$(p_1 - p_2)(x) = \mathop{+}_{i=0}^{n-1} (a_i - b_i) x^i,$$

e conclui-se que $\mathrm{gr}(p_1 - p_2) < n$. Se $p_1 \neq p_2$, existe $i \in \{0, \ldots, n-1\}$ tal que $a_i \neq b_i$. Então seja $k := \max\{i \in \{0, \ldots, n-1\} : a_i \neq b_i\}$. Assim, para todo $i > k$, $a_i = b_i$, o que implica $a_i - b_i = 0$, e temos que $\mathrm{gr}(p_1 - p_2) = k$ e

$$(p_1 - p_2)(x) = \mathop{+}_{i=0}^{k} (a_i - b_i) x^i.$$

Como $\boldsymbol{C}$ é corpo e $a_k - b_k \neq 0$, existe $(a_k - b_k)^{-1} \in C$. Definindo

$$p := (a_k - b_k)^{-1}(p_1 - p_2) = \mathop{+}_{i=0}^{k-1} (a_k - b_k)^{-1}(a_i - b_i) x^i + x^k,$$

segue que $p \in C[x]^*$, $\mathrm{gr}(p) = k$, $p(\alpha) = (a_k - b_k)^{-1}(p_1 - p_2)(\alpha) = (a_k - b_k)^{-1}(p_1(\alpha) - p_2(\alpha)) = 0$ e p é mônico. Mas $\mathrm{gr}(p) = k < n = \mathrm{gr}(p_1) = \mathrm{gr}(p_2)$, o que contradiz a minimalidade do grau de p_1 e p_2. Portanto $p_1 = p_2$ e está provada a unicidade. ■

Proposição 3.64. *Seja $\boldsymbol{C}$ um corpo e $p \in C[x]^*$. Se p é mônico e redutível, então existem $p_1, p_2 \in C[x]^*$ tais que $p = p_1 p_2$ e p_1 e p_2 são mônicos.*

Demonstração. Como p é redutível, existem $p_1', p_2' \in C[x]^*$ tais que $p = p_1'p_2'$. Sejam $n := \mathrm{gr}(p_1)$, $p_1 = +_{i=0}^{n} a_i x^i$, e $m := \mathrm{gr}(p_2)$, $p_2 = +_{i=0}^{m} b_i x^i$. Pela definição de produto, sabemos que $a_n b_m = 1$, pois p é mônico. Como $\boldsymbol{C}$ é um corpo, existem $(a_n)^{-1}, (b_m)^{-1} \in C$. Definindo

$$p_1 := (a_n)^{-1}p_1' = \mathop{+}_{i=0}^{n-1}(a_n)^{-1}a_i x^i + x^n \quad \text{e} \quad p_2 := (b_m)^{-1}p_2' = \mathop{+}_{i=0}^{m-1}(b_m)^{-1}b_i x^i + x^m,$$

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 3.65. *Sejam $\boldsymbol{C}$ um corpo, $\boldsymbol{E}$ uma extensão de $\boldsymbol{C}$, $\alpha \in E$ um elemento algébrico sobre $\boldsymbol{C}$ e $p \in C[x]^*$ um polinômio mônico tal que $p(\alpha)$. Então p é o polinômio minimal de α sobre $\boldsymbol{C}$ se, e somente se, p é irredutível em $\boldsymbol{C}[x]$.*

Demonstração. Suponhamos que p é polinômio minimal de α sobre $\boldsymbol{C}$. Se p não é irredutível em $C[x]$, como p é mônico, então existem $p_1, p_2 \in C[x]^*$ mônicos tais que $0 < \mathrm{gr}(p_i) < \mathrm{gr}(p)$ para todo $i \in \{1, 2\}$. Como $p(\alpha) = p_1(\alpha)p_2(\alpha) = 0$ e $\boldsymbol{C}$ é corpo, segue que $p_1(\alpha) = 0$ ou $p_2(\alpha) = 0$. No primeiro caso, $p_1 \in C[x]^*$ é um polinômio mônico, $p_1(\alpha) = 0$ e $\mathrm{gr}(p_1) < \mathrm{gr}(p)$, o que contradiz a minimalidade de p. No segundo caso, $p_2 \in C[x]^*$ é um polinômio mônico, $p_2(\alpha) = 0$ e $\mathrm{gr}(p_2) < \mathrm{gr}(p)$, o que também contradiz a minimalidade de p, e temos um absurdo. Portanto p é irredutível em $\boldsymbol{C}[x]$.

Reciprocamente, suponhamos que p é irredutível em $\boldsymbol{C}[x]$. Por hipótese, $p(\alpha) = 0$ e p é mônico. Seja $p_\alpha \in C[x]^*$ o polinômio minimal de α sobre $\boldsymbol{C}$. Então $\mathrm{gr}(p_\alpha) \leq \mathrm{gr}(p)$. Como p_α é mônico, exitem $q, r \in C[x]$ 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 $\mathrm{gr}(r) < \mathrm{gr}(p_\alpha)$. Seja $n := \mathrm{gr}(r)$. Como $r(\alpha) = 0$, segue que $\mathrm{gr}(r) > 0$. Então seja $r(x) = +_{i=0}^{n} a_i x^i$. Como $\boldsymbol{C}$ é corpo, existe $(a_n)^{-1} \in C$. Assim, definindo

$$p' := (a_n)^{-1}r = \mathop{+}_{i=0}^{n-1}(a_n)^{-1}a_i x^i + x^n,$$

e segue que $p' \in C[x]^*$, $p'(\alpha) = (a_n)^{-1}p'(\alpha) = 0$ e p' é mônico. Mas $\mathrm{gr}(p') = n = \mathrm{gr}(r) < \mathrm{gr}(p_\alpha)$, o que contradiz a minimalidade do grau de p_α. Então $r \neq 0$. Se $r = 0$, então $p = qp_\alpha$. Mas p é irredutível, e $p_\alpha \in C[x]^*$, o que implica $q \in C$. Como p e p_α são mônicos, segue que $q = 1$ e, portanto, $p = p_\alpha$. ■

3.4.2 Extras

Teorema 3.66. *Seja $k \subseteq K$ uma estensão de corpos, $\overline{k}$ fecho algébrico de k. Então as seguintes condições são equivalentes:*

1. *DIAGRAMA COMUTATIVO*

$$\begin{tikzcd} k \arrow[r, "\cdot"] \arrow[d, "\cdot"'] & \overline{k} \\ K \arrow[ur, "\sigma"'] & \end{tikzcd}$$

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 $c \in k \setminus \{0\}$.*

Definição 3.43. Uma extensão de corpos $k \subseteq K$ é uma *extensão normal* se ela satisfaz uma das três condições do teorema acima.

OBS: Se $k \subseteq \overline{k}$ é uma extensão algébrica, então todo $\beta \in \overline{k}$ é algébrico sobre k vale para $\beta \in K$, então $k \subseteq K$ é extensão algébrica.

Se $k \subseteq K$ é extensão algébrica, então $k \subseteq K \subseteq \overline{K}$ são extensões algébricas, então $k \subseteq \overline{K}$ é extensão algébrica. Então $\overline{k} \sim \overline{K}$ é fecho algébrico de k.

Proposição 3.67. *Seja $k \subseteq K$ um extensão algébrica e $\sigma : K \longrightarrow K$ um homomorfismo de cropos que satisfaz $\sigma|_k = id|_k$. Então σ é um isomorfismo de corpos.*

Definição 3.44. Seja $E \subseteq F$ uma extensão algébrica e $\sigma : E \longrightarrow L$ um homomorfismo de corpos tal que L é algebricamente fechaado, $\sigma(E) \subseteq L$ é uma extensão algébrica (L é fecho algébrico de $\sigma(E)$)

$$S_\sigma := \{\mu : \mu : F \longrightarrow L \text{ homomorfismo de corpos}, \mu|_E = \sigma\}.$$

Lema 3.68. *$|S_\sigma|$ depende de $E \subseteq F$, mas não depende de σ nem de L.*

Definição 3.45. 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 3.69. 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

$$[F : E]_S \leq [F : E]$$

Definição 3.46. Seja $E \subseteq K$ uma extensão finita. Ela é *separável* se $[K : E]_S = [K : E]$.

Corolário 3.70. *Sejam $E \subseteq F \subseteq K$ extensões de corpos, $[K : E] < \infty$, $E \subseteq K$ separável. Então $E \subseteq F$ e $F subseteq K$ 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. ■

3.5 Matrizes

Definição 3.47. Seja $\boldsymbol{A}$ um anel e $l, c \in \mathbb{N}$. Uma *matriz* de dimensão $l \times c$ sobre $\boldsymbol{A}$ é uma função $M : [l] \times [c] \longrightarrow A$. 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 $\boldsymbol{A}$ é denotado por $\mathbb{M}_{l\times c}(\boldsymbol{A})$.

Definição 3.48. Seja $\boldsymbol{A}$ um anel e $d \in \mathbb{N}$. Uma *matriz quadrada* de dimensão d sobre $\boldsymbol{A}$ é uma matriz $M \in \mathbb{M}_{d\times d}(\boldsymbol{A})$. O conjunto de todas as matrizes quadradas de dimensão d sobre $\boldsymbol{A}$ é denotado por $\mathbb{M}_d(\boldsymbol{A})$.

Definição 3.49. Sejam $\boldsymbol{A}$ um anel e $M \in \mathbb{M}_{l\times c}(\boldsymbol{A})$. A *matriz transposta* de M é a matriz $M^\intercal \in \mathbb{M}_{c\times l}(\boldsymbol{A})$ definida por

$$(M^\intercal)(i, j) := m_{j,i}.$$

3.5.1 Soma de Matrizes

Definição 3.50. Sejam $\boldsymbol{A}$ um anel e $M, N \in \mathbb{M}_{l\times c}(\boldsymbol{A})$. A *matriz soma* das matrizes M e N é a matriz $(M+N) \in \mathbb{M}_{l\times c}(\boldsymbol{A})$ definida por

$$(M+N)(i,j) := m_{i,j} + n_{i,j}.$$

Definição 3.51. Sejam $\boldsymbol{A}$ um anel e 0 o elemento neutro da soma de $\boldsymbol{A}$.

1. A *matriz nula* de dimensão $l \times c$ sobre $\boldsymbol{A}$ é a matriz $\mathbb{O}_{l\times c} \in \mathbb{M}_{l\times c}(\boldsymbol{A})$, definida por
$$\mathbb{O}_{l\times c}(i,j) := 0.$$
2. Se $M \in \mathbb{M}_{l\times c}$, a *matriz negativa* de M é a matriz $-M \in \mathbb{M}_{l\times c}(\boldsymbol{A})$, definida por
$$(-M)(i,j) := -m_{i,j}.$$

Proposição 3.71. *Seja $\boldsymbol{A}$ um anel e $+$ a operação binária em $\mathbb{M}_{l\times c}(\boldsymbol{A})$ definida por*

$$\begin{aligned} +\colon \mathbb{M}_{l\times c}(\boldsymbol{A}) \times \mathbb{M}_{l\times c}(\boldsymbol{A}) &\longrightarrow \mathbb{M}_{l\times c}(\boldsymbol{A}) \\ (M,N) &\longmapsto M+N. \end{aligned}$$

Então $(\mathbb{M}_{l\times c}(\boldsymbol{A}), +)$ é um grupo com elemento neutro $\mathbb{O}_{l\times c}$. Se $\boldsymbol{A}$ é comutativo, então $(\mathbb{M}_{l\times c}(\boldsymbol{A}), +)$ é comutativo.

Demonstração. Sejam $M, N, P \in \mathbb{M}_{l\times c}(\boldsymbol{A})$. Primeiro, notemos que $+$ é associativa, pois, como a soma no anel é associativa, segue que

$$(m_{i,j} + n_{i,j}) + p_{i,j} = m_{i,j} + (n_{i,j} + p_{i,j})$$

e, portanto, $(M+N)+P = M+(N+P)$. Então, notemos que $\mathbb{O}$ é elemento neutro de $+$. Como 0 é elemento neutro da soma da anel, segue que

$$m_{i,j} + 0 = 0 + m_{i,j} = m_{i,j}$$

e, portanto, $M + \mathbb{O} = \mathbb{O} + M = M$. Ainda, notemos que, como $-m_{i,j}$ é o inverso aditivo de $m_{i,j}$ no anel, segue que

$$m_{i,j} + (-m_{i,j}) = (-m_{i,j}) + m_{i,j} = 0$$

e, portanto, $M + (-M) = (-M) + M = \mathbb{O}$. Assim, concluímos que $(\mathbb{M}_{l\times c}(\boldsymbol{A}), +)$ é um anel. Por fim, notemos que, se $\boldsymbol{A}$ é comutativo, então $+$ é comutativa, pois, como a soma no anel é comutativa, segue que

$$m_{i,j} + n_{i,j} = n_{i,j} + m_{i,j}$$

e, portanto, $M + N = N + M$. Assim, concluímos que, se $\boldsymbol{A}$ é comutativo, então $(\mathbb{M}_{l\times c}(\boldsymbol{A}), +)$ é comutativo. ■

3.5.2 Produto de Matrizes e Produto Por Escalar

Definição 3.52. Sejam $\boldsymbol{A}$ um anel e $M \in \mathbb{M}_{l\times d}(\boldsymbol{A})$ e $N \in \mathbb{M}_{d\times c}(\boldsymbol{A})$. A *matriz produto* das matrizes M e N é a matriz $(MN) \in \mathbb{M}_{l\times c}(\boldsymbol{A})$ definida por

$$(MN)(i,j) := \mathop{\Large +}_{k=1}^{d} m_{i,k}n_{k,j}.$$

Proposição 3.72. *Sejam $\boldsymbol{A}$ um anel e $M \in \mathbb{M}_{l\times d_1}(\boldsymbol{A})$, $N \in \mathbb{M}_{d_1\times d_2}(\boldsymbol{A})$ e $P \in \mathbb{M}_{d_2\times c}(\boldsymbol{A})$. Então*

$$(MN)P = M(NP).$$

Demonstração. Um elemento de MN é dado por

$$(mn)_{i,j} = \mathop{\Large +}_{k_1=1}^{d_1} m_{i,k_1}n_{k_1,j}.$$

Logo, um elemento de $(MN)P$ é dado por

$$((mn)p)_{i,j} = \mathop{\Large +}_{k_2=1}^{d_2} (mn)_{i,k_2}p_{k_2,j} = \mathop{\Large +}_{k_2=1}^{d_2} \left(\mathop{\Large +}_{k_1=1}^{d_1} m_{i,k_1}n_{k_1,k_2} \right) p_{k_2,j}.$$

Analogamente, um elemento de $M(NP)$ é dado por

$$(m(np))_{i,j} = \mathop{\Large +}_{k_1=1}^{d_1} m_{i,k_1}(np)_{k_1,j} = \mathop{\Large +}_{k_1=1}^{d_1} m_{i,k_1} \left(\mathop{\Large +}_{k_2=1}^{d_2} n_{k_1,k_2}p_{k_2,j} \right).$$

Mas então, como $\boldsymbol{A}$ é um anel, segue que

$$\begin{aligned}
((mn)p)_{i,j} &= \mathop{\Large +}_{k_2=1}^{d_2} \left(\mathop{\Large +}_{k_1=1}^{d_1} m_{i,k_1}n_{k_1,k_2} \right) p_{k_2,j} \\
&= \mathop{\Large +}_{k_2=1}^{d_2} \left(\mathop{\Large +}_{k_1=1}^{d_1} m_{i,k_1}n_{k_1,k_2}p_{k_2,j} \right) \\
&= \mathop{\Large +}_{k_1=1}^{d_1} \left(\mathop{\Large +}_{k_2=1}^{d_2} m_{i,k_1}n_{k_1,k_2}p_{k_2,j} \right) \\
&= \mathop{\Large +}_{k_1=1}^{d_1} m_{i,k_1} \left(\mathop{\Large +}_{k_2=1}^{d_2} n_{k_1,k_2}p_{k_2,j} \right) \\
&= (m(np))_{i,j}.
\end{aligned}$$

■

Definição 3.53. Sejam $\boldsymbol{A}$ um anel e 0 e 1 os elementos neutros da soma e da multiplicação de $\boldsymbol{A}$ respectivamente. A *matriz identidade* de dimensão d sobre $\boldsymbol{A}$ é a matriz $\mathrm{I}_d \in \mathbb{M}_d(\boldsymbol{A})$ definida por

$$\mathrm{I}_d(i,j) := \delta_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j, \end{cases}$$

Essa função δ é conhecida como delta de Kronecker.

Proposição 3.73. *Seja $\boldsymbol{A}$ um anel e $\cdot$ a operação binária em $\mathbb{M}_d(\boldsymbol{A})$ definida por*

$$\begin{aligned} \cdot \colon \mathbb{M}_d(\boldsymbol{A}) \times \mathbb{M}_d(\boldsymbol{A}) &\longrightarrow \mathbb{M}_d(\boldsymbol{A} \\ (M,N) &\longmapsto MN. \end{aligned}$$

Então $(\mathbb{M}_d(\boldsymbol{A}), \cdot)$ é um monoide com elemento neutro I_d.

Demonstração. Sejam $M, N, P \in \mathbb{M}_d(\boldsymbol{A})$. Pela proposição anterior, sabemos que vale $(MN)P = M(NP)$ e que, portanto, $\cdot$ é associativa. Agora, notemos que um elemento de $M\mathrm{I}_d$ é da forma

$$\mathop{\mathbin{+}}_{k=0}^{d-1} m_{i,k}\delta_{k,j}.$$

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

$$\mathop{\mathbin{+}}_{k=1}^{d} m_{i,k}\delta_{k,j} = m_{i,j}.$$

Assim, concluímos que $M\mathrm{I}_d = M$. Analogamente, mostra-se que $\mathrm{I}_d M = M$, e concluímos que I_d é elemento neutro de $\cdot$. Isso mostra que $(\mathbb{M}_d(\boldsymbol{A}), \cdot)$ é um monoide. ■

Definição 3.54. Seja $\boldsymbol{A}$ um anel. Uma *matriz invertível* é uma matriz $M \in \mathbb{M}_d(\boldsymbol{A})$ que é invertível com respeito ao produto do monoide $(\mathbb{M}_d(\boldsymbol{A}), \cdot)$. A matriz inversa de M é denotada M^{-1}.

Definição 3.55. Seja $\boldsymbol{A}$ um anel, $a \in A$ e $M \in \mathbb{M}_{l\times c}(\boldsymbol{A})$. O *produto por escalar* de a e M é a matriz $aM \in \mathbb{M}_{l\times c}$ definida por

$$(aM)(i,j) := am_{i,j}.$$

3.5.3 Matrizes Quadradas

Definição 3.56. Seja $\boldsymbol{A}$ um anel.

1. Uma *matriz triangular superior* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que satisfaz
$$\bigwedge i, j \in [d] \qquad i > j \Rightarrow m_{i,j} = 0.$$

2. Uma *matriz triangular inferior* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ sobre $\boldsymbol{A}$ que satisfaz
$$\bigwedge i, j \in [d] \qquad i < j \Rightarrow m_{i,j} = 0.$$

3. Uma *matriz triangular superior* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que satisfaz
$$\bigwedge i, j \in [d] \qquad i > j \Rightarrow m_{i,j} = 0.$$

4. Uma *matriz triangular* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que é triangular superior ou triangular inferior.

5. Uma *matriz diagonal* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que é triangular superior e triangular inferior; ou seja, que satisfaz
$$\bigwedge i, j \in [d] \qquad i \neq j \Rightarrow m_{i,j} = 0.$$

6. Uma *matriz simétrica* uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que é igual a sua transposta
$$M = M^{\intercal}.$$

7. Uma *matriz antissimétrica* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ que é igual à negativa da sua transposta
$$M = -M^{\intercal}.$$

8. Uma *matriz ortogonal* é uma matriz quadrada $M \in \mathbb{M}_d(\boldsymbol{A})$ cuja transposta é igual à sua inversa
$$M^{\intercal} = M^{-1}.$$

3.5.4 Traço e Determinante

Definição 3.57. Sejam $\boldsymbol{A}$ um anel e $M \in \mathbb{M}_d(\boldsymbol{A})$. O *traço* de M é o elemento $\operatorname{tr}(M) \in A$ definido por
$$\operatorname{tr}(M) := \mathop{\mathbin{+}}_{i=1}^{d} m_{i,i}.$$

Proposição 3.74. *Sejam* $\boldsymbol{A}$ *um anel,* $a \in A$ *e* $M, N \in \mathbb{M}_d(\boldsymbol{A})$*. Então*

1. $\operatorname{tr}(M^\intercal) = \operatorname{tr}(M)$;
2. $\operatorname{tr}(MN) = \operatorname{tr}(NM)$;
3. $\operatorname{tr}(M+N) = \operatorname{tr}(M) + \operatorname{tr}(N)$;
4. $\operatorname{tr}(aM) = a\operatorname{tr}(M)$.

Demonstração. 1.

$$\operatorname{tr}(M) = \mathop{\bigplus}_{i=1}^{d} m_{i,i} = \operatorname{tr}(M^\intercal).$$

2.

$$\begin{aligned}
\operatorname{tr}(MN) &= \mathop{\bigplus}_{i=1}^{d} \left(\mathop{\bigplus}_{k=1}^{d} m_{i,k} n_{k,i} \right) \\
&= \mathop{\bigplus}_{i=1}^{d} \left(\mathop{\bigplus}_{k=1}^{d} n_{k,i} m_{i,k} \right) \\
&= \mathop{\bigplus}_{k=1}^{d} \left(\mathop{\bigplus}_{i=1}^{d} n_{k,i} m_{i,k} \right) \\
&= \operatorname{tr}(NM).
\end{aligned}$$

3.

$$\begin{aligned}
\operatorname{tr}(M+N) &= \mathop{\bigplus}_{i=1}^{d} (m_{i,i} + n_{i,i}) \\
&= \mathop{\bigplus}_{i=1}^{d} m_{i,i} + \mathop{\bigplus}_{i=1}^{d} n_{i,i} \\
&= \operatorname{tr}(M) + \operatorname{tr}(N).
\end{aligned}$$

4.

$$\operatorname{tr}(aM) = \mathop{\bigplus}_{i=1}^{d} a m_{i,i} = a \mathop{\bigplus}_{i=1}^{d} m_{i,i} = a\operatorname{tr}(M).$$

■

Capítulo 4

Corpos

4.1 Corpo e Subcorpo

Já demos a definição de um corpo no capítulo de anéis, mas agora pretendemos ressaltar essa definição.

Definição 4.1. Um *corpo* é uma lista $\boldsymbol{C} = (C, +, -, 0, \times, ^{-1}, 1)$ tal que

1. $(C, +, -, 0, \times, 1)$ é um anel;
2. $(C \setminus \{0\}, \times, ^{-1}, 1)$ é um grupo (comutativo).

4.2 Corpo de Frações

Definição 4.2. Seja $\boldsymbol{D}$ um domínio. A *equivalência de frações* em $D \times D \setminus \{0\}$ é a relação definida por: para todos $(n, d), (n', d') \in D \times D*$,

$$(n, d) \sim (n', d') \Leftrightarrow nd' = dn'.$$

Proposição 4.1. *Seja $\boldsymbol{D}$ um domínio. A* equivalência de frações *em $D \times D \setminus \{0\}$ é uma equivalência.*

Demonstração. (Reflexividade) Segue direto de $nd = dn$ para todo $(n, d) \in D \times D \setminus \{0\}$.

(Simetria) Segue direto de $nd' = dn'$ se, e somente se, $dn' = nd'$ para todos $(n, d), (n', d') \in D \times D*$.

(Transitividade) Sejam $(n, d), (n', d'), (n'', d'') \in D \times D \setminus \{0\}$ tais que $(n, d) \sim (n', d')$ e $(n', d') \sim (n'', d'')$. Isso significa que $nd' = dn'$ e $n'd'' = d'n''$. Então segue que

$$d'(nd'') = nd'd'' = dn'd'' = dd'n'' = d'(dn'')$$

logo, como $d \neq 0$, segue da propriedade de cancelamento que

$$nd'' = dn'',$$

o que significa que $(n, d) \sim (n'', d'')$. ■

Note que a transitividade exige que valha a prorpiedade de cancelamente, por isso precisamos de um domínio, e também exige a comutatividade da multiplicação. Como essa relação é uma equivalência, podemos considerar o quociente desse conjunto pela relação, e obtemos o que se chama corpo de frações.

Definição 4.3. Seja $\boldsymbol{D}$ um domínio. O *corpo de frações* de $\boldsymbol{D}$ é o conjunto

$$Q(D) := D \times D \smallsetminus \{0\} \big/ \sim .$$

Os elementos de $Q(D)$ são *frações* e são denotadas

$$\frac{n}{d} := [(n, d)].$$

A *adição de frações* é a função

$$\begin{aligned} +\colon Q(D) \times Q(D) &\longrightarrow Q(D) \\ \left(\frac{n}{d}, \frac{n'}{d'}\right) &\longmapsto \frac{nd' + dn'}{dd'} \end{aligned}$$

A *inversa da adição de frações* é a função

$$\begin{aligned} -\colon Q(D) &\longrightarrow Q(D) \\ \frac{n}{d} &\longmapsto \frac{-n}{d} \end{aligned}$$

A *nulidade de frações* é a fração

$$0 := \frac{0}{1}.$$

A *multiplicação de frações* é a função

$$\begin{aligned} +\colon Q(D) \times Q(D) &\longrightarrow Q(D) \\ \left(\frac{n}{d}, \frac{n'}{d'}\right) &\longmapsto \frac{nn'}{dd'}; \end{aligned}$$

A *inversa da multiplicação de frações* é a função

$$\begin{aligned} {}^{-1}\colon Q(D) \smallsetminus \{0\} &\longrightarrow Q(D) \smallsetminus \{0\} \\ \frac{n}{d} &\longmapsto \frac{d}{n}; \end{aligned}$$

A *unidade de frações* é a fração

$$1 := \frac{1}{1}.$$

Definição 4.4. Seja $\boldsymbol{D}$ um domínio. A lista $(Q(D), +, -, 0, \times, ^{-1}, 1)$ é um corpo.

Demonstração. Exercício simples. ■

Definição 4.5. Seja $\boldsymbol{D}$ um domínio. A *inclusão canônica* de D em $Q(D)$ é a função

$$\begin{aligned} \iota\colon D &\longrightarrow Q(D) \\ a &\longmapsto \frac{a}{1}. \end{aligned}$$

Proposição 4.2. *Seja $\boldsymbol{D}$ um domínio. A inclusão $\iota\colon D \longrightarrow Q(D)$ é um homomorfismo injetivo de anéis.*

Proposição 4.3 (Propriedade Universal)**.** *Sejam $\boldsymbol{D}$ um domínio, $\boldsymbol{C}$ um corpo e $h\colon D \longrightarrow C$ um homomorfismo injetivo de anel. Existe um único homomorfismo injetivo de anel $\bar{h}\colon Q(D) \longrightarrow C$ tal que $\bar{h} \circ \iota = h$ (o diagrama comuta).*

$$\begin{tikzcd} \boldsymbol{Q(D)} \arrow[dr, dashed, "\bar{h}"] & \\ \boldsymbol{D} \arrow[u, "\iota"] \arrow[r, "h"'] & \boldsymbol{C} \end{tikzcd}$$

Demonstração. Definimos

$$\begin{aligned} \bar{h}\colon Q(D) &\longrightarrow C \\ \frac{n}{d} &\longmapsto h(n)h(d)^{-1}. \end{aligned}$$

Mostremos primeiro que essa função está bem definida. Primeiro, note que, como h é injetiva e $d \neq 0$, então $h(d) \neq 0$, portanto existe $h(d)^{-1} \in C$. Agora, sejam $(n, d), (n', d') \in D \times D \smallsetminus \{0\}$ tais que $\frac{n}{d} = \frac{n'}{d'}$. Então $nd' = dn'$, e segue da injetividade de h vale que $h(nd') = h(dn')$. Mas então $h(n)h(d') = h(d)h(n')$, o que implica que $h(n)h(d)^{-1} = h(n')h(d')^{-1}$, e segue que

$$\bar{h}\left(\frac{n}{d}\right) = h(n)h(d)^{-1} = h(n')h(d')^{-1} = \bar{h}\left(\frac{n'}{d'}\right).$$

Agora mostremos que $\bar{h}$ é homomorfismo de anel. (Homomorfismo de grupo) Sejam $\frac{n}{d}, \frac{n'}{d'} \in Q(D)$. Então

$$\begin{aligned}
\bar{h}\left(\frac{n}{d}+\frac{n'}{d'}\right) &= \bar{h}\left(\frac{nd'+dn'}{dd'}\right) \\
&= h(nd'+dn')h(dd')^{-1} \\
&= (h(n)h(d')+h(d)h(n'))h(d)^{-1}h(d')^{-1} \\
&= h(n)h(d)^{-1}+h(n')h(d')^{-1} \\
&= \bar{h}\left(\frac{n}{d}\right)+\bar{h}\left(\frac{n'}{d'}\right).
\end{aligned}$$

(Homomorfismo de monoide) Sejam $\frac{n}{d}, \frac{n'}{d'} \in Q(D)$. Então

$$\begin{aligned}
\bar{h}\left(\frac{n}{d}\frac{n'}{d'}\right) &= \bar{h}\left(\frac{nn'}{dd'}\right) \\
&= h(nn')h(dd')^{-1} \\
&= h(n)h(n')h(d)^{-1}h(d')^{-1} \\
&= h(n)h(d)^{-1}h(n')h(d')^{-1} \\
&= \bar{h}\left(\frac{n}{d}\right)\bar{h}\left(\frac{n'}{d'}\right).
\end{aligned}$$

Ainda, como h é homomorfismo de anel, $h(1)=1$, logo

$$\bar{h}\left(\frac{1}{1}\right) = h(1)h(1)^{-1} = 1.$$

(Injetividade) Sejam $\frac{n}{d}, \frac{n'}{d'} \in Q(D)$ tais que $\bar{h}(\frac{n}{d}) = \bar{h}(\frac{n'}{d'})$. Então

$$\begin{aligned}
0 &= \bar{h}\left(\frac{n}{d}\right)-\bar{h}\left(\frac{n'}{d'}\right) \\
&= \bar{h}\left(\frac{n}{d}-\frac{n'}{d'}\right) \\
&= \bar{h}\left(\frac{nd'-dn'}{dd'}\right) \\
&= h(nd'-dn')h(dd')^{-1}.
\end{aligned}$$

Como $d \neq 0$ e $d' \neq 0$, segue que $h(nd'-dn')=0$, e da injetividade de h segue que $nd'-dn'=0$, logo $nd'=dn'$, o que significa que $\frac{n}{d}=\frac{n'}{d'}$.

■

4.2.1 Os Números Racionais $\mathbb{Q}$

Essa construção, aplicada ao anel dos números inteiro, é o conjunto dos números racionais.

Definição 4.6. $\mathbb{Q} := Q(\mathbb{Z})$.

4.2.2 Funções de Arredondamento

Chão e teto

Definição 4.7. A função *chão* é a função

$$\begin{aligned} \lfloor \cdot \rfloor : \mathbb{R} &\longrightarrow \mathbb{Z} \\ x &\longmapsto \max \{ i \in \mathbb{Z} \mid i \leq x \} . \end{aligned}$$

A função *teto* é a função

$$\begin{aligned} \lceil \cdot \rceil : \mathbb{R} &\longrightarrow \mathbb{Z} \\ x &\longmapsto \min \{ i \in \mathbb{Z} \mid i \geq x \} . \end{aligned}$$

Proposição 4.4. *Para todo $x \in \mathbb{R}$,*

1. *(Conjugação)*

$$\begin{aligned} -\lfloor x \rfloor &= \lceil -x \rceil \\ -\lceil x \rceil &= \lfloor -x \rfloor ; \end{aligned}$$

2. *(Idempotência)*

$$\begin{aligned} \lfloor \lfloor x \rfloor \rfloor &= \lfloor x \rfloor \\ \lceil \lceil x \rceil \rceil &= \lceil x \rceil ; \end{aligned}$$

Proposição 4.5. *Para todo $x, x' \in \mathbb{R}$ e todo $i \in \mathbb{Z}$,*

1.

$$\begin{aligned} \lfloor x + i \rfloor &= \lfloor x \rfloor + i \\ \lceil x + i \rceil &= \lceil x \rceil + i; \end{aligned}$$

2.

$$\begin{aligned} \lfloor x \rfloor + \lfloor x' \rfloor \leq \lfloor x + x' \rfloor &\leq \lfloor x \rfloor + \lfloor x' \rfloor + 1 \\ -1 + \lceil x \rceil + \lceil x' \rceil \leq \lceil x + x' \rceil &\leq \lceil x \rceil + \lceil x' \rceil ; \end{aligned}$$

Proposição 4.6. *Para todos $x, x' \in \mathbb{R}$, $x' > 0$ e todos $i, i' \in \mathbb{Z}$, $i > 0$,*

1.
$$\left\lfloor \frac{\lfloor x \rfloor + i'}{i} \right\rfloor = \left\lfloor \frac{x + i'}{i} \right\rfloor$$
$$\left\lceil \frac{\lceil x \rceil + i'}{i} \right\rceil = \left\lceil \frac{x + i'}{i} \right\rceil;$$

2.
$$\left\lceil \frac{i'}{i} \right\rceil - 1 = \left\lfloor \frac{i' - 1}{i} \right\rfloor$$
$$\left\lfloor \frac{i'}{i} \right\rfloor + 1 = \left\lceil \frac{i' + 1}{i} \right\rceil;$$

3.
$$\left\lfloor \frac{\lfloor x \mathbin{/} x' \rfloor}{i} \right\rfloor = \left\lfloor \frac{x}{x'i} \right\rfloor$$
$$\left\lceil \frac{\left\lceil \frac{x}{x'} \right\rceil}{i} \right\rceil = \left\lceil \frac{x}{x'i} \right\rceil.$$

Resto e parte fracionária

Definição 4.8. Sejam $x, y \in \mathbb{R}$, $x' \neq 0$. O *resto* de x com respeito a x' é

$$\{x\}_{x'} := x - x' \left\lfloor \frac{x}{x'} \right\rfloor.$$

A *parte fracionária* de x é o resto de x com respeito a 1:

$$\{x\} := \{x\}_1.$$

Proposição 4.7. *Sejam $x, x' \in \mathbb{R}$, $x' \neq 0$.*

1. *Se $x' > 0$,*
$$0 \leq \{x\}_{x'} < x';$$

2. *Se $x' < 0$,*
$$x' < \{x\}_{x'} \leq 0;$$

Proposição 4.8. *Seja $x \in \mathbb{R}$,*

$$\lceil \{x\} \rceil = \lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0, & x \in \mathbb{Z} \\ 1, & x \notin \mathbb{Z}. \end{cases}$$

Proposição 4.9. *Sejam $x \in \mathbb{R}$, $i \in \mathbb{Z}$, $i > 0$.*

$$\left\lceil \left\{ \frac{x}{i} \right\} \right\rceil = \left\lceil \frac{x}{i} \right\rceil - \left\lfloor \frac{x}{i} \right\rfloor = \begin{cases} 0, & x \in i\mathbb{Z} \\ 1, & x \notin i\mathbb{Z}. \end{cases}$$

Arredondamento

Definição 4.9. A função *arredondamento meio para baixo* é a função

$$\begin{aligned} \lceil \cdot \rfloor \colon \mathbb{R} &\longrightarrow \mathbb{Z} \\ x &\longmapsto \left\lceil x - \frac{1}{2} \right\rceil. \end{aligned}$$

A função *arredondamento meio para cima* é a função

$$\begin{aligned} \lfloor \cdot \rceil \colon \mathbb{R} &\longrightarrow \mathbb{Z} \\ x &\longmapsto \left\lfloor x + \frac{1}{2} \right\rfloor. \end{aligned}$$

Capítulo 5

Espaços Lineares

5.1 Módulos

Definição 5.1. Seja $\boldsymbol{A} = (A, +, -, 0, \cdot, 1)$ um anel. Um *módulo (à esquerda)* sobre $\boldsymbol{A}$ é um par $(\boldsymbol{M}, \cdot)$ em que $\boldsymbol{M} = (M, \boldsymbol{+}, \boldsymbol{-}, \boldsymbol{0})$ é um grupo comutativo e $\cdot\colon \boldsymbol{A} \curvearrowright \boldsymbol{M}$ é uma ação de anel ($\cdot\colon \boldsymbol{A} \longrightarrow \mathrm{End}(\boldsymbol{M})$ é um homomorfismo de anel); ou seja,

1. Para todo $a \in A$, a função $a\cdot\colon \boldsymbol{M} \longrightarrow \boldsymbol{M}$ é um homomorfismo de grupo:

   (a) Para todos $m_0, m_1 \in M$,

   $$a \cdot (m_0 \boldsymbol{+} m_1) = a \cdot m_0 \boldsymbol{+} a \cdot m_1.$$

2. $\cdot\colon A \times M \longrightarrow M$ 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 $\boldsymbol{A}$ e da ação $\cdot$ serão suprimidos (e parênteses desnecessários relacionados a elas também), e os símbolos das operações $+, -$ de $\boldsymbol{A}$ e $\boldsymbol{+}, \boldsymbol{-}$ de $\boldsymbol{M}$ não serão diferenciadas em notação, nem os das constantes $0 \in A$ e $\boldsymbol{0} \in M$.

Na definição usamos o fato de que $\mathrm{End}(\boldsymbol{M})$ 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 $\boldsymbol{G}$ 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 $\mathrm{End}(\boldsymbol{G})$ de endomorfismos de grupo de $\boldsymbol{G}$ é um subanel de G^G.

Proposição 5.1. *Sejam X um conjunto e $\boldsymbol{G}$ um grupo comutativo. Então*

$$(G^X, +, -, 0, \circ, \mathrm{I})$$

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. $(G^X, \circ, \mathrm{I})$ 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 $x \in X$,

$$(\mathrm{I} \circ f)(x) = \mathrm{I}(f(x)) = f(x) = f(\mathrm{I}(x)) = (f \circ \mathrm{I})(x).$$

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 5.2. *Seja $\boldsymbol{G}$ um grupo comutativo. Então*

$$(\mathrm{End}(G), +, -, 0, \circ, \mathrm{I})$$

é um anel.

Demonstração. Como $\mathrm{End}(\boldsymbol{G}) \subseteq G^G$, basta mostrar que $\mathrm{End}(\boldsymbol{G})$ é subanel de G^G.

1. $\mathrm{End}(\boldsymbol{G})$ é subgrupo.

   (a) Para todos $h_0, h_1 \in \mathrm{End}(\boldsymbol{G})$ 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 $h \in \mathrm{End}(\boldsymbol{G})$ 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. $\mathrm{End}(\boldsymbol{G})$ é submonoide.

   (a) Para todos $h_0, h_1 \in \mathrm{End}(\boldsymbol{G})$ 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 $g_0, g_1 \in G$,

$$\mathrm{I}(g_0 + g_1) = g_0 + g_1 = \mathrm{I}(g_0) + \mathrm{I}(g_1).$$

■

5.2 Espaço e Subespaço Lineares

Definição 5.2. Seja $\boldsymbol{C} = (C, +, -, 0, \cdot, 1)$ um corpo. Um *espaço linear* sobre $\boldsymbol{C}$ é um módulo $(\boldsymbol{V}, \cdot)$ sobre $\boldsymbol{C}$; ou seja,

1. Para todo $c \in C$, a função $c\cdot\colon \boldsymbol{V} \longrightarrow \boldsymbol{V}$ 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 $\boldsymbol{C}$ e da ação $\cdot$ serão suprimidos (e parênteses desnecessários relacionados a elas também), e os símbolos das operações $+, -$ de $\boldsymbol{C}$ e $+, -$ de $\boldsymbol{V}$ não serão diferenciadas em notação. Um espaço linear será denotado como $\boldsymbol{V}$ quando não for relevante explicitar a ação $\cdot$.

Proposição 5.3. *Seja $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$. Para todos $\boldsymbol{v} \in V$ e $c \in C$,*

1. $c\boldsymbol{v} = \mathbf{0} \Leftrightarrow c = 0$ *ou* $\boldsymbol{v} = \mathbf{0}$;
2. $-(c\boldsymbol{v}) = (-c)\boldsymbol{v} = c(-\boldsymbol{v})$;
3. $c\boldsymbol{v} = (-c)(-\boldsymbol{v})$.

Demonstração. Sejam $\boldsymbol{v} \in V$ e $c \in C$.

1. Primeiro, notemos que
$$\begin{aligned} 0\boldsymbol{v} &= 0\boldsymbol{v} + \mathbf{0} \\ &= 0\boldsymbol{v} + (0\boldsymbol{v} - 0\boldsymbol{v}) \\ &= (0\boldsymbol{v} + 0\boldsymbol{v}) - 0\boldsymbol{v} \\ &= (0 + 0)\boldsymbol{v} - 0\boldsymbol{v} \\ &= 0\boldsymbol{v} - 0\boldsymbol{v} \\ &= \mathbf{0}. \end{aligned}$$
   Agora, notemos que
$$\begin{aligned} c\mathbf{0} &= c\mathbf{0} + \mathbf{0} \\ &= c\mathbf{0} + (c\mathbf{0} - c\mathbf{0}) \\ &= (c\mathbf{0} + c\mathbf{0}) - c\mathbf{0} \\ &= c(\mathbf{0} + \mathbf{0}) - c\mathbf{0} \\ &= c\mathbf{0} - c\mathbf{0} \\ &= \mathbf{0}. \end{aligned}$$

Portanto, se $c = 0$ ou $\boldsymbol{v} = \mathbf{0}$, então $c\boldsymbol{v} = \mathbf{0}$. Agora, suponhamos que $c\boldsymbol{v} = \mathbf{0}$. Se $c \neq 0$, como $\boldsymbol{C}$ é corpo, segue da demonstração anterior que

$$\boldsymbol{v} = c^{-1}c\boldsymbol{v} = c^{-1}\mathbf{0} = \mathbf{0}.$$

2. Basta notar que

$$\begin{aligned}
-(c\boldsymbol{v}) &= -(c\boldsymbol{v}) + \mathbf{0} \\
&= -(c\boldsymbol{v}) + (0\boldsymbol{v}) \\
&= -(c\boldsymbol{v}) + (c - c)\boldsymbol{v} \\
&= -(c\boldsymbol{v}) + (c\boldsymbol{v} + (-c)\boldsymbol{v}) \\
&= (-(c\boldsymbol{v}) + c\boldsymbol{v}) + (-c)\boldsymbol{v} \\
&= \mathbf{0} + (-c)\boldsymbol{v} \\
&= (-c)\boldsymbol{v}
\end{aligned}$$

e que

$$\begin{aligned}
-(c\boldsymbol{v}) &= -(c\boldsymbol{v}) + \mathbf{0} \\
&= -(c\boldsymbol{v}) + (c\mathbf{0}) \\
&= -(c\boldsymbol{v}) + c(\boldsymbol{v} - \boldsymbol{v}) \\
&= -(c\boldsymbol{v}) + (c\boldsymbol{v} + c(-\boldsymbol{v})) \\
&= (-(c\boldsymbol{v} + c\boldsymbol{v}) + c(-\boldsymbol{v}) \\
&= \mathbf{0} + c(-\boldsymbol{v}) \\
&= c(-\boldsymbol{v}).
\end{aligned}$$

3. Do item anterior, segue que

$$c\boldsymbol{v} = (-(-c))\boldsymbol{v} = (-c)(-\boldsymbol{v}).$$ ■

Proposição 5.4. *Seja $\boldsymbol{C}$ um corpo e n um natural positivo. Então $(C^n, +, \cdot)$, em que*

$$\begin{aligned}
\cdot\colon C \times C^n &\longrightarrow C^n \\
(c, (c_1, \ldots, c_n)) &\longmapsto (c \cdot c_1, \ldots, c \cdot c_n),
\end{aligned}$$

é um espaço vetorial sobre $\boldsymbol{C}$.

Demonstração. Claramente $(C^n, +)$ é um grupo comutativo com elemento neutro $(0, \ldots, 0)$. Note que, para todos $(c_1, \ldots, c_n) \in C^n$ e $c, c' \in C$,

$$1 \cdot (c_1, \ldots, c_n) = (1 \cdot c_1, \ldots, 1 \cdot c_n) = (c_1, \ldots, c_n)$$

e

$$\begin{aligned}(c \cdot c') \cdot (c_1, \ldots, c_n) &= ((c \cdot c') \cdot c_1, \ldots, (c \cdot c') \cdot c_n) \\ &= ((c \cdot (c' \cdot c_1), \ldots, (c \cdot (c' \cdot c_n)) \\ &= c \cdot (c' \cdot c_1, \ldots, c' \cdot c_n) \\ &= c \cdot (c' \cdot (c_1, \ldots, c_n)).\end{aligned}$$

Ainda, note que, para todos $(c_1, \ldots, c_n), (c'_1, \ldots, c'_n) \in C^n$ e $c, c' \in C$,

$$\begin{aligned}c \cdot ((c_1, \ldots, c_n) + (c'_1, \ldots, c'_n)) &= c \cdot (c_1 + c'_1, \ldots, c_n + c'_n) \\ &= (c \cdot (c_1 + c'_1), \ldots, c \cdot (c_n + c'_n)) \\ &= (c \cdot c_1 + c \cdot c'_1, \ldots, c \cdot c_n + c \cdot c'_n) \\ &= (c \cdot c_1, \ldots, c \cdot c_n) + (c \cdot c'_1, \ldots, c \cdot c'_n) \\ &= c \cdot (c_1, \ldots, c_n) + c \cdot (c'_1, \ldots, c'_n)\end{aligned}$$

e

$$\begin{aligned}(c + c') \cdot (c_1, \ldots, c_n) &= ((c + c')c_1, \ldots, (c + c')c_n) \\ &= (c \cdot c_1 + c' \cdot c_1, \ldots, c \cdot c_n + c' \cdot c_n)_{i \in I} \\ &= (c \cdot c_1, \ldots, c \cdot c_n) + (c' \cdot c_1, \ldots, c' \cdot c_n) \\ &= c \cdot (c_1, \ldots, c_n) + c' \cdot (c_1, \ldots, c_n).\end{aligned}$$

■

Para generalizar esse resultado, lembremos que o produto de uma família $(C_i)_{i \in I}$ de conjuntos é $\prod_{i \in I} C_i$ 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 5.5. *Sejam I um conjunto e $\boldsymbol{C}$ um corpo. Então $\boldsymbol{C^I} = (C^I, +, \cdot)$, em que*

$$\begin{aligned}+ \colon C^I &\longrightarrow C^I \\ (\boldsymbol{c}, \boldsymbol{c'}) &\longmapsto (c_i + c'_i)_{i \in I}\end{aligned}$$

e

$$\begin{aligned}\cdot \colon C \times C^I &\longrightarrow C^I \\ (a, \boldsymbol{c}) &\longmapsto (a \cdot c_i)_{i \in I}\end{aligned}$$

é um espaço vetorial sobre $\boldsymbol{C}$.

Esse exemplo pode ser ainda mais generalizado como a seguir.

Proposição 5.6 (Espaço de Funções)**.** *Sejam X um conjunto e $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Então $\boldsymbol{V}^{\boldsymbol{X}} = (V^X, +, \cdot)$, em que*

$$\begin{aligned} +\colon V^X \times V^X &\longrightarrow V^X \\ (\boldsymbol{f}_1, \boldsymbol{f}_2) &\longmapsto \boldsymbol{f}_1 + \boldsymbol{f}_2 \colon X \longrightarrow V \\ & \qquad\qquad x \longmapsto \boldsymbol{f}_1(x) + \boldsymbol{f}_2(x). \end{aligned}$$

e

$$\begin{aligned} \cdot\colon C \times V^X &\longrightarrow V^X \\ (c, \boldsymbol{f}) &\longmapsto c\boldsymbol{f} \colon X \longrightarrow V \\ & \qquad\qquad x \longmapsto c\boldsymbol{f}(x), \end{aligned}$$

é um espaço vetorial sobre $\boldsymbol{C}$.

Demonstração. Primeiro, sabemos que $(V^X, +)$ é um grupo comutativo com identidade $0\colon V^X \times V^X \longrightarrow V^X$ definida por $0(x) = 0$. Devemos então mostrar que $\cdot\colon C \times V^X \longrightarrow V^X$ satisfaz os itens da definição de espaço vetorial. Primeiro, seja $\boldsymbol{f} \in V^X$. Então, para todo $x \in X$, $(1\boldsymbol{f})(x) = 1\boldsymbol{f}(x) = \boldsymbol{f}(x)$, o que mostra que $1\boldsymbol{f} = \boldsymbol{f}$. Agora, sejam $c_1, c_2 \in C$ e $\boldsymbol{f} \in V^X$. Então, para todo $x \in X$,

$$((c_1c_2)\boldsymbol{f})(x) = (c_1c_2)\boldsymbol{f}(x) = c_1(c_2\boldsymbol{f}(x)) = c_1(c_2\boldsymbol{f})(x) = (c_1(c_2\boldsymbol{f}))(x),$$

o que mostra que $(c_1c_2)\boldsymbol{f} = c_1(c_2\boldsymbol{f})$.

Por fim, devemos mostrar as propriedades distributivas. Sejam $c \in C$ e $\boldsymbol{f}_1, \boldsymbol{f}_2 \in V^X$. Então, para todo $x \in X$,

$$\begin{aligned} (c(\boldsymbol{f}_1 + \boldsymbol{f}_2))(x) &= c(\boldsymbol{f}_1 + \boldsymbol{f}_2)(x) \\ &= c(\boldsymbol{f}_1(x) + \boldsymbol{f}_2(x)) \\ &= c\boldsymbol{f}_1(x) + c\boldsymbol{f}_2(x) \\ &= (c\boldsymbol{f}_1)(x) + (c\boldsymbol{f}_2)(x) \\ &= (c\boldsymbol{f}_1 + c\boldsymbol{f}_2)(x), \end{aligned}$$

o que mostra que $c(\boldsymbol{f}_1 + \boldsymbol{f}_2) = c\boldsymbol{f}_1 + c\boldsymbol{f}_2$. Agora, sejam $c_1, c_2 \in C$ e $\boldsymbol{f} \in V^X$. Então, para todo $x \in X$,

$$\begin{aligned} ((c_1 + c_2)\boldsymbol{f})(x) &= (c_1 + c_2)\boldsymbol{f}(x) \\ &= c_1\boldsymbol{f}(x) + c_2\boldsymbol{f}(x) \\ &= (c_1\boldsymbol{f})(x) + (c_2\boldsymbol{f})(x) \\ &= (c_1\boldsymbol{f} + c_2\boldsymbol{f})(x), \end{aligned}$$

o que mostra que $(c_1 + c_2)\boldsymbol{f} = c_1\boldsymbol{f} + c_2\boldsymbol{f}$. Assim, concluímos que $(V^X, +, \cdot)$ é um espaço vetorial sobre $\boldsymbol{C}$. ■

Definição 5.3. Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Um *subespaço vetorial* de $\boldsymbol{V}$ é um conjunto não vazio $W \subseteq V$ tal que

1. $\bigwedge \boldsymbol{w}_1, \boldsymbol{w}_2 \in W \qquad \boldsymbol{w}_1 + \boldsymbol{w}_2 \in W$;
2. $\bigwedge c \in C \ \bigwedge \boldsymbol{w} \in W \qquad c\boldsymbol{w} \in W$.

Proposição 5.7. *Seja $\boldsymbol{V} = (V, +, \cdot)$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Então um conjunto não vazio $W \subseteq V$ é um subespaço vetorial de $\boldsymbol{V}$ se, e somente se, $\boldsymbol{W} = (W, +|_{W\times W}, \cdot|_{C\times W})$ é um espaço vetorial sobre $\boldsymbol{C}$.*

Proposição 5.8. *Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e W um subespaço vetorial de $\boldsymbol{V}$. Então*

1. $\mathbf{0} \in W$;
2. $\{\mathbf{0}\}$ *e* V *são subespaços vetoriais de* $\boldsymbol{V}$.

Demonstração. 1. Como W não é vazio, seja $\boldsymbol{w} \in W$. Então $0\boldsymbol{w} = \mathbf{0} \in W$.

2. Seja $W = \{\mathbf{0}\}$. Se $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$, $\boldsymbol{w}_1 = \mathbf{0}$ e $\boldsymbol{w}_2 = \mathbf{0}$, e segue que $\boldsymbol{w}_1 + \boldsymbol{w}_2 = \mathbf{0} + \mathbf{0} = \mathbf{0}$. Ainda, para todo $c \in C$, segue que $c\boldsymbol{w}_1 = c\mathbf{0} = \mathbf{0} \in W$. Seja $W = V$. Como $\boldsymbol{V}$ é espaço vetorial, então V é subespaço vetorial de $\boldsymbol{V}$ pala proposição anterior. ■

Proposição 5.9. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $(W_i)_{i\in I}$ uma família de subespaços vetoriais de $\boldsymbol{V}$. Então*

$$W := \bigcap_{i\in I} W_i$$

é um subespaço vetorial de $\boldsymbol{V}$.

Demonstração. Como, para todo $i \in I$, $\mathbf{0} \in W_i$, segue que $\mathbf{0} \in W$ e, portanto, W não é vazio. Agora, sejam $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$ e $c \in C$. Então, para todo $i \in I$, $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W_i$ e, como W_i é subespaço vetorial de $\boldsymbol{V}$, segue que $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W_i$ e que $c\boldsymbol{w}_1 \in W_i$. Logo $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W$ e $c\boldsymbol{w}_1 \in W$, o que mostra que W é subespaço vetorial de $\boldsymbol{V}$. ■

Proposição 5.10. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $\{W_i\}_{i\in I}$ uma cadeia de subespaços vetoriais de $\boldsymbol{V}$ (ou seja, para todos $I, j \in I$, $W_I \subseteq W_j$ ou $W_j \subseteq W_i$). Então*

$$W := \bigcup_{i\in I} W_i$$

é um subespaço vetorial de $\boldsymbol{V}$.

Demonstração. Como, para todo $i \in I$, $\mathbf{0} \in W_i$, pois W_i é subespaço vetoriasl de $\boldsymbol{V}$, segue que $\mathbf{0} \in W$ e, portanto, W não é vazio. Agora, sejam $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$. Então existem $i, j \in I$ tais que $\boldsymbol{w}_1 \in W_i$ e $\boldsymbol{w}_2 \in W_j$. Nesse caso, $W_i \subseteq W_j$ ou $W_j \subseteq W_i$. Sem perda de generalidade, suponhamos o primeiro caso. Então segue que $\boldsymbol{w}_1 \in W_j$ e, portanto, $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W_j$, o que mostra que $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W$. Agora, seja $c \in C$ e notemos que, como W_i é subespaço vetorial de $\boldsymbol{V}$, segue que $c\boldsymbol{w}_1 \in W_i$. Logo $c\boldsymbol{w}_1 \in W$, o que mostra que W é subespaço vetorial de $\boldsymbol{V}$. ■

Definição 5.4. Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$, $W \subseteq V$ e $(W_i)_{i \in I}$ uma indexação do conjunto de todos subespaços vetoriais de $\boldsymbol{V}$ dos quais W é subconjunto. O *subespaço vetorial gerado por* W em $\boldsymbol{V}$ é o subespaço vetorial

$$\langle W \rangle := \bigcap_{i \in I} W_i.$$

Nesse caso, dizemos que W é um *conjunto gerador* de $\langle W \rangle$ ou que W gera $\langle W \rangle$.

Proposição 5.11. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Então $\langle \emptyset \rangle = \{\mathbf{0}\}$.*

Demonstração. Como $\{\mathbf{0}\}$ é um subespaço vetorial de V e $\emptyset \subseteq \{\mathbf{0}\}$, segue que, se $\boldsymbol{v} \in \langle \emptyset \rangle$, então $\boldsymbol{v} \in \{\mathbf{0}\}$, o que implica $\boldsymbol{v} = \mathbf{0}$ e, portanto, que $\langle \emptyset \rangle = \{\mathbf{0}\}$. ■

5.3 Combinação Linear de Vetores

Definição 5.5. Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$ um conjunto finito tal que $W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$. Uma *combinação linear* de W em $\boldsymbol{V}$ é um vetor $\boldsymbol{v} \in V$ tal que existem $c_1, \ldots, c_n \in C$ satisfazendo

$$\boldsymbol{v} = \mathop{\mathbin{+}}_{i=1}^{n} c_i \boldsymbol{w}_i.$$

Se W é um conjunto infinito, uma *combinação linear* de W é uma combinação linear de um subconjunto finito de W.

O vetor $\mathbf{0}$ é combinação linear de qualquer conjunto, pois é a soma vazia.

Teorema 5.12. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$ não vazio. Então $\langle W \rangle$ é o conjunto de todas as combinações lineares de W em $\boldsymbol{V}$.*

Demonstração. Consideremos, primeiro, o caso em que $W = \emptyset$. Nesse caso, $\langle W \rangle = \{\mathbf{0}\}$, e a única combinação linear de W é a soma vazia $\mathbf{0}$, o que mostra a igualdade dos conjuntos.

Agora, assumamos que $W \neq \emptyset$ e seja $(W_j)_{j\in J}$ uma indexação do conjunto de todos subespaços de $\boldsymbol{V}$ que contêm W. Primeiro, mostraremos que uma combinação linear de W em $\boldsymbol{V}$ está em $\langle W\rangle$. Seja $\boldsymbol{v} := +_{i=1}^{n} c_i\boldsymbol{w}_i$ uma combinação linear de W em $\boldsymbol{V}$. Para todo $j \in J$, W_j é um subespaço vetorial de $\boldsymbol{V}$. Portanto, para todo $i \in [n]$, segue que $c_i\boldsymbol{w_i} \in W_j$ e, então, que $\boldsymbol{v} \in W_j$. Logo $\boldsymbol{v} \in \langle W\rangle$.

Reciprocamente, mostraremos que o conjunto de todas combinações lineares de W em $\boldsymbol{V}$ é um subespaço vetorial de $\boldsymbol{V}$. Primeiro, notemos que $\mathbf{0}$ é uma combinação linear de W, pois, para todo $\boldsymbol{w} \in W$, vale $\mathbf{0} = 0\boldsymbol{w}$. Agora, sejam $\boldsymbol{v}_1 = +_{i=1}^{n} c_i\boldsymbol{w}_i$ e $\boldsymbol{v}_2 = +_{i=1}^{m} c'_i\boldsymbol{w}'_i$ combinações lineares de W em $\boldsymbol{V}$ e $c \in C$. Então, se definirmos, para todo $i \in [m]$, $\boldsymbol{w}_{n+i} := \boldsymbol{w}'_i$ e $c_{n+i} := c'_i$ e, para todo $i \in [n]$, $\overline{c}_i := cc_i$, segue que

$$\boldsymbol{v}_1 + \boldsymbol{v}_2 = \mathop{+}_{i=1}^{n} c_i\boldsymbol{w}_i + \mathop{+}_{i=1}^{m} c'_i\boldsymbol{w}'_i = \mathop{+}_{i=1}^{n+m} c_i\boldsymbol{w}_i$$

e

$$c\boldsymbol{v}_1 = \mathop{+}_{i=1}^{n} (cc_i)\boldsymbol{w}_i = \mathop{+}_{i=1}^{n} \overline{c}_i\boldsymbol{w}_i$$

são combinações lineares de W em $\boldsymbol{V}$, o que implica que o conjunto de todas combinações lineares de W em $\boldsymbol{V}$ é um subespaço de $\boldsymbol{V}$. Assim, como $\langle W\rangle$ é subconjunto de todo conjunto que é subespaço vetorial de $\boldsymbol{V}$ contendo W, segue que o conjunto de todas combinações lineares de W em $\boldsymbol{V}$ é igual ao subespaço gerado por W. ■

Proposição 5.13. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$, $W \subseteq V$ e $\boldsymbol{v} \in \langle W\rangle$. Então existem $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in W$ distintos e $c_1, \ldots, c_n \in C$ tais que*

$$\boldsymbol{v} = \mathop{+}_{i=1}^{n} c_i\boldsymbol{w}_i.$$

Demonstração. Como $\boldsymbol{v} \in \langle W\rangle$, existem $\boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_m \in W$ e $c'_1, \ldots, c'_m \in C$ tais que $\boldsymbol{v} = +_{i=1}^{m} c'_i\boldsymbol{w}'_i$. Vamos particionar o conjunto dos índices $[m]$ com a seguinte relação de equivalência: para todo $i, j \in [m]$, $i \sim j$ se, e somente se, $\boldsymbol{w}'_i = \boldsymbol{w}'_j$. Essa relação é de equivalência pois a igualddade de vetores é uma relação de equivalência. Agora, seja n o número de classes de equivalências dessa relação. Para cada $i \in [n]$, seja $j \in P_i$ e definimos os vetores $\boldsymbol{w}_i := \boldsymbol{w}'_j$. Notemos que os vetores $\boldsymbol{w}_i$ estão bem definidos, não dependem do j, pois, se $k \in P_i$, então $\boldsymbol{w}_i = \boldsymbol{w}'_j = \boldsymbol{w}'_k$. Ainda, definimos os coeficientes $c_i := +_{j\in P_i} c'_j$. Desse modo, segue que

$$\boldsymbol{v} = \mathop{+}_{i=1}^{m} c'_i\boldsymbol{w}'_i = \mathop{+}_{i=1}^{n} \mathop{+}_{j\in P_i} c'_j\boldsymbol{w}'_j = \mathop{+}_{i=1}^{n} \mathop{+}_{j\in P_i} c'_j\boldsymbol{w}_i = \mathop{+}_{i=1}^{n} c_i\boldsymbol{w}_i.$$

Por fim, notemos que os $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$ são distintos por definição, já que, se $\boldsymbol{w}_i = \boldsymbol{w}_j$ para $i, j \in [n]$, então existem $k, l \in [m]$ tais que $k \in P_i$, $l \in P_j$ e $\boldsymbol{w}_i = \boldsymbol{w}'_k$, $\boldsymbol{w}_j = \boldsymbol{w}'_l$. Mas isso implica $\boldsymbol{w}'_k = \boldsymbol{w}'_l$, o que implica $P_i = P_j$ e, portanto, $i = j$. ■

Definição 5.6 (Dependência Linear)**.** Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$. Dizemos que W é *linarmente dependente* em $\boldsymbol{V}$ se existem $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in W$ distintos e $c_1, \ldots, c_n \in C$ não nulos tais que

$$\mathbf{0} = \mathop{\mathbin{+}}_{i=1}^{n} c_i \boldsymbol{w}_i.$$

Caso contrário, dizemos que W é *linearmente independente* em $\boldsymbol{V}$.

Proposição 5.14. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$. Então W é linearmente dependente se, e somente se, existe $\boldsymbol{w} \in W$ que é combinação linear de $W \smallsetminus \{\boldsymbol{w}\}$ em $\boldsymbol{V}$.*

Demonstração. Suponhamos que W é linearmente dependente. Então existem vetores $\boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_n \in W$ distintos e $c'_1, \ldots, c'_n \in C$ não nulos tais que

$$\mathbf{0} = \mathop{\mathbin{+}}_{i=1}^{n} c'_i \boldsymbol{w}'_i.$$

Como $c'_1, \ldots, c'_n$ são não nulos, então existe $j \in [n]$ tal que $c'_j \neq 0$. Definindo $\boldsymbol{w}_i := \boldsymbol{w}'_i$ se $1 \leq i < j$ e $\boldsymbol{w}_i := \boldsymbol{w}'_{i-1}$ 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

$$\boldsymbol{w}'_j = \mathop{\mathbin{+}}_{i=1}^{j-1} (c'_j)^{-1}(-c'_i)\boldsymbol{w}'_i + \mathop{\mathbin{+}}_{i=j+1}^{n} (c'_j)^{-1}(-c'_i)\boldsymbol{w}'_i = \mathop{\mathbin{+}}_{i=1}^{n-1} c_i \boldsymbol{w}_i.$$

Por tanto, como $\boldsymbol{w}_i \in W \smallsetminus \{\boldsymbol{w}'_j\}$ e $c_i \in C$ para todo $i \in [n-1]$, $\boldsymbol{w}'_j$ é combinação linear de $W \smallsetminus \{\boldsymbol{w}'_j\}$ em $\boldsymbol{V}$.

Reciprocamente, suponhamos que existe $\boldsymbol{w} \in W$ que é combinação linear de $W \smallsetminus \{\boldsymbol{w}\}$ em $\boldsymbol{V}$. Então existem $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in W \smallsetminus \{\boldsymbol{w}\}$ distintos e $c_1, \ldots, c_n \in C$ tais que

$$\boldsymbol{w} = \mathop{\mathbin{+}}_{i=1}^{n} c_i \boldsymbol{w}_i.$$

Definindo $\boldsymbol{w}_{n+1} := \boldsymbol{w}$ e $c_{n+1} := -1$, segue que

$$\mathbf{0} = \mathop{\mathbin{+}}_{i=1}^{n} c_i \boldsymbol{w}_i - \boldsymbol{w} = \mathop{\mathbin{+}}_{i=1}^{n+1} c_i \boldsymbol{w}_i.$$

Então, como $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n+1}$ são distintos e $c_{n+1} = -1 \neq 0$, segue que W é linearmente dependente. ■

Proposição 5.15. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$. Então*

1. *$\emptyset$ é linearmente independente em $\boldsymbol{V}$;*
2. *Se $\mathbf{0} \in W$, então W é linearmente dependente em $\boldsymbol{V}$;*
3. *Se $W = \{\boldsymbol{v}\} \neq \{\mathbf{0}\}$, então W é linearmente independente em $\boldsymbol{V}$.*
4. *Sejam $\boldsymbol{v}, \boldsymbol{v}' \neq 0$. $W = \{\boldsymbol{v}, \boldsymbol{v}'\}$ é linearmente dependente se, e somente se, existe $c \in C \setminus \{0\}$ tal que $\boldsymbol{v}' = c\boldsymbol{v}$.*

Demonstração. 1. Suponha, por absurdo, que $\emptyset$ não é linearmente independente. Então existem $\boldsymbol{w_1}, \ldots, \boldsymbol{w_n} \in \emptyset$ distintos e $c_1, \ldots, c_n \in C$ não nulos tais que

$$\mathbf{0} = \mathop{\mathbin{+}}_{i=1}^{n} c_i \boldsymbol{w_i}.$$

Mas $\boldsymbol{w_1}, \ldots, \boldsymbol{w_n} \in \emptyset$ é um absurdo.

2. Seja $c \in C \setminus \{0\}$. Então, como $\mathbf{0} = c\mathbf{0}$, segue que W é linearmente dependente em $\boldsymbol{V}$.

3. Se $\mathbf{0} = c\boldsymbol{v}$, como $\boldsymbol{v} \neq \mathbf{0}$, segue que $c = 0$, o que mostra que W é linearmente independente em $\boldsymbol{V}$.

4. Se W é linearmente dependente, então existem $c, c' \in C \setminus \{0\}$ tais que $0 = c\boldsymbol{v} + c'\boldsymbol{v}'$, o que implica que

$$\boldsymbol{v}' = -\frac{c}{c'}\boldsymbol{v}.$$

Reciprocamente, se existe $c \in C \setminus \{0\}$ tal que $\boldsymbol{v}' = c\boldsymbol{v}$, então

$$0 = -c\boldsymbol{v} + c\boldsymbol{v} = -c\boldsymbol{v} + \boldsymbol{v}',$$

o que mostra que W é linearmente dependente.

■

Proposição 5.16. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W \subseteq V$. Então W é linearmente independente em $\boldsymbol{V}$ se, e somente se, para toda combinação linear $\boldsymbol{v} = +_{i=1}^{n} c_i \boldsymbol{w}_i \neq \mathbf{0}$ de W em $\boldsymbol{V}$ tal que $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$ são distintos e não nulos, então $c_1, \ldots, c_n$ são únicos.*

Demonstração. Primeiro, suponhamos que W é linearmente dependente em $\boldsymbol{V}$. Então existem $\boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_{n'} \in W$ distintos e $c'_1, \ldots, c'_{n'} \in C$ não nulos tais que

$$\mathbf{0} = \mathop{+}_{i=1}^{n'} c'_i \boldsymbol{w}'_i.$$

Nesse caso, seja $\boldsymbol{v} \in \langle W \rangle$. Se $\boldsymbol{v} = \mathbf{0}$, então segue que
..... . Se $\boldsymbol{v} \neq \mathbf{0}$

■

Proposição 5.17. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $\{W_i\}_{i \in I}$ uma cadeia de conjuntos linearmente independentes em $\boldsymbol{V}$ (ou seja, para todos $i, j \in I$, $W_i \subseteq W_j$ ou $W_j \subseteq W_i$). Então*

$$W := \bigcup_{i \in I} W_i$$

é um conjunto linearmente independente em $\boldsymbol{V}$.

Demonstração. Como, para todo $i \in I$, $\mathbf{0} \in W_i$, segue que $\mathbf{0} \in W$ e, portanto, W não é vazio. Agora, sejam $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$. Então existem $i, j \in I$ tais que $\boldsymbol{w}_1 \in W_i$ e $\boldsymbol{w}_2 \in W_j$. Nesse caso, $W_i \subseteq W_j$ ou $W_j \subseteq W_i$. Sem perda de generalidade, suponhamos o primeiro caso. Então segue que $\boldsymbol{w}_1 \in W_j$ e, portanto, $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W_j$, o que mostra que $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in W$. Agora, seja $c \in C$ e notemos que, como W_i é subespaço vetorial de $\boldsymbol{V}$, segue que $c\boldsymbol{w}_1 \in W_i$. Logo $c\boldsymbol{w}_1 \in W$, o que mostra que W é subespaço vetorial de $\boldsymbol{V}$. ■

5.4 Soma de Subespaços Vetoriais

Definição 5.7. Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $(W_i)_{i \in I}$ uma família de subespaços vetoriais de $\boldsymbol{V}$. A *soma* de $(W_i)_{i \in I}$ é o subespaço vetorial gerado pela união de W_i. Denotamos

$$\mathop{+}_{i \in I} W_i := \left\langle \bigcup_{i \in I} W_i \right\rangle.$$

Caso $(W_i)_{i \in I}$ seja uma família finita, escrevemos $W_1 + \cdots + W_n$.

Definição 5.8. Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Uma *soma direta* é a soma de uma família $(W_i)_{i \in I}$ de subespaços vetoriais de $\boldsymbol{V}$ tal que $W_i \cap W_j = \{\mathbf{0}\}$ 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 5.18. *Seja* $\boldsymbol{V}$ *um espaço vetorial sobre um corpo* $\boldsymbol{C}$ *e* $W_1, \ldots, W_n$ *subespaços vetoriais de* $\boldsymbol{V}$ *tais que* $V = +_{i=1}^{n} W_i$. *Então*

$$V = \bigoplus_{i=1}^{n} W_i$$

se, e somente se, para todo $\boldsymbol{v} \in V$, *existem únicos* $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_n \in W_n$ *tais que*

$$\boldsymbol{v} = \mathop{+}_{i=1}^{n} \boldsymbol{w}_i.$$

Demonstração. Mostraremos, primeiro, que se V é soma direta de $W_1, \ldots, W_n$, então todo vetor de V é soma única de vetores de $W_1, \ldots, W_n$. A demontração será por indução em n. O caso base é trivial, pois, se $V = W_1$, então, para todo $\boldsymbol{v} \in V$, $\boldsymbol{v} \in W_1$. Agora, suponhamos que a proposição vale para todo natural menor ou igual a n. Sejam $W_1, \ldots, W_{n+1}$ subespaços vetoriais de V tais que $V = +_{i=1}^{n+1} W_i$. Então existem $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_{n+1} \in W_{n+1}$ tais que

$$\boldsymbol{v} = \mathop{+}_{i=1}^{n+1} \boldsymbol{w}_i.$$

Suponhamos que existam $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_{n+1} \in W_{n+1}$ tais que

$$\boldsymbol{v} = \mathop{+}_{i=1}^{n+1} \boldsymbol{w}'_i.$$

Então

$$\boldsymbol{v} = \mathop{+}_{i=1}^{n+1} \boldsymbol{w}_i = \mathop{+}_{i=1}^{n+1} \boldsymbol{w}'_i,$$

o que implica

$$\mathop{+}_{i=1}^{n} (\boldsymbol{w}_i - \boldsymbol{w}'_i) = \boldsymbol{w}'_{n+1} - \boldsymbol{w}_{n+1}.$$

Como, para todo $i \in [n+1]$, $w_i, w'_i \in W_i$, segue que $\boldsymbol{w}_i - \boldsymbol{w}'_i \in W_i$. Definamos $W := \bigcup_{i=1}^{n} W_i$. Assim, segue que

$$\mathop{+}_{i=1}^{n} (\boldsymbol{w}_i - \boldsymbol{w}'_i) \in \langle W \rangle$$

e

$$\boldsymbol{w}'_{n+1} - \boldsymbol{w}_{n+1} \in W_{n+1}.$$

Ainda, como V é soma direta de $W_1, \ldots, W_{n+1}$, então segue que $W \cap W_{n+1} = \{\boldsymbol{0}\}$. Portanto concluímos que

$$\mathop{+}_{i=1}^{n} (\boldsymbol{w}_i - \boldsymbol{w}'_i) = \boldsymbol{w}'_{n+1} - \boldsymbol{w}_{n+1} = \boldsymbol{0}.$$

Assim, concluímos que $\boldsymbol{w}'_{n+1} = \boldsymbol{w}_{n+1}$ e que

$$\mathop{\mathbin{+}}_{i=1}^{n} \boldsymbol{w}_i = \mathop{\mathbin{+}}_{i=1}^{n} \boldsymbol{w}'_i.$$

Mas notemos que

$$\langle \boldsymbol{W} \rangle = (\langle W \rangle, +|_{\langle W \rangle \times \langle W \rangle}, \cdot|_{\langle W \rangle \times \langle W \rangle})$$

é um espaço vetorial e $W_1, \ldots, W_n$ são subespaços vetoriais de $\langle \boldsymbol{W} \rangle$ tais que $\langle W \rangle = \mathop{\mathbin{+}}_{i=1}^{n} W_i$. Portanto, pela hipótese de indução, segue que, para todo $i \in [n]$, $\boldsymbol{w}_i = \boldsymbol{w}'_i$ e, portanto, concluímos que existem únicos $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_{n+1} \in W_{n+1}$ tais que

$$\boldsymbol{v} = \mathop{\mathbin{+}}_{i=1}^{n+1} \boldsymbol{w}_i.$$

Suponhamos, então, que todo vetor de V é soma de únicos vetores de W_1, ..., W_n. Sejam $i, j \in [n]$, $i \neq j$, e $\boldsymbol{v} \in W_i \cap W_j$. Como $\boldsymbol{v} \in V$, segue que existem únicos $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_n \in W_n$ tais que

$$\boldsymbol{v} = \mathop{\mathbin{+}}_{k=1}^{n} \boldsymbol{w}_k.$$

Sem perda de generalidade, suponhamos $i < j$. Notemos que

$$\boldsymbol{v} = \mathop{\mathbin{+}}_{i=1}^{n} \boldsymbol{w}_i = \mathop{\mathbin{+}}_{k=1}^{i-1} \boldsymbol{w}_k + (\boldsymbol{w}_i + \boldsymbol{v}) + \mathop{\mathbin{+}}_{k=i+1}^{j-1} \boldsymbol{w}_k + (\boldsymbol{w}_j - \boldsymbol{v}) + \mathop{\mathbin{+}}_{k=j+1}^{n} \boldsymbol{w}_k.$$

Como $\boldsymbol{v} \in W_i \cap W_j$, segue que $(\boldsymbol{w}_i + \boldsymbol{v}) \in W_i$ e $(\boldsymbol{w}_j - \boldsymbol{v}) \in W_j$ e, portanto, como $\boldsymbol{w}_1 \in W_1, \ldots, \boldsymbol{w}_n \in W_n$ são únicos, segue que $(\boldsymbol{w}_i + \boldsymbol{v}) = \boldsymbol{w}_i$ e $(\boldsymbol{w}_j - \boldsymbol{v}) = \boldsymbol{w}_j$; ou seja, $\boldsymbol{v} = \boldsymbol{0}$. Logo V é soma direta de $W_1, \ldots, W_n$. ■

5.5 Bases de Espaços Vetoriais

Definição 5.9. Seja $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Uma *base* de $\boldsymbol{V}$ é um conjunto $B \subseteq V$ linearmente independente em $\boldsymbol{V}$ que gera V; ou seja, $V = \langle B \rangle$. Uma base de um subespaço vetorial W de $\boldsymbol{V}$ é uma base do espaço vetorial $\boldsymbol{W} = (W, +|_{W \times W}, \cdot|_{W \times W})$.

Teorema 5.19. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Então existe base B de $\boldsymbol{V}$ e, se L é um conjunto linearmente independente em $\boldsymbol{V}$, existe uma base B de $\boldsymbol{V}$ tal que $L \subseteq B$.*

Demonstração. A afirmação de que todo espaço vetorial tem uma base é consequência da segunda afirmação porque, tomando $L = \emptyset$, sabemos que L é linearmente independente e, portanto, existe base B de $\boldsymbol{V}$ que contém $\emptyset$. Demonstraremos a segunda afirmação.

Sejam L um conjunto linearmente independente em $\boldsymbol{V}$ e P o conjunto dos subconjuntos $S \subseteq V$ tais que $L \subseteq S$ e S é linearmente independente em $\boldsymbol{V}$. Então $(P, \subseteq)$ é um conjunto parcialmente ordenado com a contenção de conjuntos usual. Agora, seja $(S_i)_{i \in I}$ uma cadeia de $(P, \subseteq)$. Consideremos o conjunto $S := \bigcup_{i \in I} S_i$. Como $L \subseteq S_i$ para todo $i \in I$, então $L \subseteq S$. Devemos mostrar que S é um conjunto linearmente independente em $\boldsymbol{V}$. Para isso, seja $M \subseteq S$ subconjunto finito de S. Como $(S_i)_{i \in I}$ é uma cadeia, existe $i \in I$ tal que $M \subseteq S_i$. Mas, como S_i é linearmente independente, então M também o é e, portanto, S é linearmente independente. Logo S é um limitante superior da cadeia. Concluímos, portanto, que existe um elemento maximal B de $(P, \subseteq)$ que, por definição de P, é linearmente independente e $L \subseteq B$.

Vamos mostrar que B é base de $\boldsymbol{V}$. Devemos mostrar que B gera V, ou seja, que $V = \langle B \rangle$. Seja $\boldsymbol{v} \in V$ e suponhamos, por absurdo, que $\boldsymbol{v} \notin \langle B \rangle$. Então, em particular, $\boldsymbol{v} \notin B$; logo $B \subset B \cup \{\boldsymbol{v}\}$. Concluiremos que $B \cup \{\boldsymbol{v}\}$ é linearmente independente, o que constradiz a maximalidade de B. Seja S um subconjunto finito de $B \cup \{\boldsymbol{v}\}$. Se $\boldsymbol{v} \notin S$, então $S \subseteq B$ e, portanto, é linearmente independente, pois B o é; se $\boldsymbol{v} \in S$, sejam $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} := S \smallsetminus \{\boldsymbol{v}\} \subseteq B$ e $c, c_1, \ldots, c_n \in C$ tais que

$$c_1 \boldsymbol{v}_1 + \cdots + c_n \boldsymbol{v}_n - c\boldsymbol{v} = \boldsymbol{0}.$$

Como $\boldsymbol{v} \notin \langle B \rangle$, então $c = 0$, pois, caso contrário, teríamos

$$\boldsymbol{v} = \frac{c_1}{c} \boldsymbol{v}_1 + \cdots + \frac{c_n}{c} \boldsymbol{v}_n.$$

Assim, segue que $c_1 \boldsymbol{v}_1 + \cdots + c_n \boldsymbol{v}_n = \boldsymbol{0}$. Mas $S \smallsetminus \{\boldsymbol{v}\} \subseteq B$ é linearmente independente, pois B o é, o que implica que $c_1 = \cdots = c_n = 0$ e, portanto, S é linearmente independente. Com isso, concluímos que $B \cup \{\boldsymbol{v}\}$ é linearmente independente, pois todo subconjunto finito é, e isso contradiz a maximalidade de B. Por esse absurdo, segue que $\boldsymbol{v} \in \langle B \rangle$ e, portanto, que $V = \langle B \rangle$. Concluímos que B é uma base de $\boldsymbol{V}$ que contém L. ■

Proposição 5.20. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $W, W' \subseteq V$ conjuntos finitos. Se W é linearmente independente em $\boldsymbol{V}$ e W' gera V, então $|W| \leq |W'|$.*

Demonstração. Se $W = \emptyset$, então $0 = |W'| \leq |W|$. Caso contrário, seja $|W| = n$ e $(\boldsymbol{w}_i)_{i \in [n]}$ uma indexação de W. Suponhamos, por absurdo, que $W' = \emptyset$. Então, como W' gera V e $\langle W' \rangle = \{\boldsymbol{0}\}$, segue que $V = \{\boldsymbol{0}\}$, o que é absurdo, pois isso

implica que $W = \{\mathbf{0}\}$, que é um conjunto linearmente dependente. Então $W' \neq \emptyset$. Seja $|W'| = m$ e $(\boldsymbol{w}'_i)_{i\in[m]}$ uma indexação de W'. Queremos mostrar que $n \leq m$. Suponhamos, por absurdo, que $m < n$. Como W é linearmente independente, então, para todo $i \in [n]$, $\boldsymbol{w}_i \neq \mathbf{0}$. Como W' gera V, existem $c_1, \ldots, c_m \in C$ tais que

$$\boldsymbol{w}_1 = \mathop{\mathbin{+}}_{i=1}^{m} c_i \boldsymbol{w}'_i,$$

e os $c_1, \ldots, c_m \in C$ não são todos nulos pois, caso contrário, teríamos $\boldsymbol{w}_1 = \mathbf{0}$. Assim, suponhamos, sem perda de generalidade, que $c_1 \neq 0$. Então

$$\boldsymbol{w}'_1 = c_1^{-1}\boldsymbol{w}_1 - \mathop{\mathbin{+}}_{i=2}^{m} c_1^{-1} c_i \boldsymbol{w}'_i.$$

Seja $W_1 := \{\boldsymbol{w}_1, \boldsymbol{w}'_2, \ldots, \boldsymbol{w}'_m\}$. Como W' gera V e todo elemento de W' pode ser escrito como combinação linear de W_1, W_1 gera V. Assim, analogamente, podemos escrever $\boldsymbol{w}_2$ como combinação linear de W_1, como $\boldsymbol{w}_2 \neq \mathbf{0}$, segue que nem todo os coeficientes da combinação linear são nulos. Mais ainda, se somente o coeficiente de $\boldsymbol{w}_1$ é não nulo, então $\boldsymbol{w}_2$ é múltiplo de $\boldsymbol{w}_1$, o que contradiz a independência linear de W. Portanto, deve existir um coeficiente dos $\boldsymbol{w}'_2, \ldots, \boldsymbol{w}'_m$ não nulo. Assim, sem perda de generalidade, suponhamos que o coeficiente de $\boldsymbol{w}'_2$ é não nulo. Então, como no caso anterior, $\boldsymbol{w}'_2$ pode ser escrito como combinação linear de $\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}'_3, \ldots, \boldsymbol{w}'_m$ e segue que o conjunto $W_2 := \{\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}'_3, \ldots, \boldsymbol{w}'_m\}$ gera V. Repetindo o processo, que termina porque $m < n$ são finitos, achamos o conjunto $W_m := \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$, que gera V e é um subconjunto próprio de W, pois $m < n$. Mas isso implica que $\boldsymbol{w}_{m+1} \in W$ é uma combinação linear de W_m em $\boldsymbol{V}$, o que implica que W é linearmente dependente, uma contradição. Logo $m \leq n$. ■

Teorema 5.21. *Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$. Se $B, B' \subseteq V$ são bases de $\boldsymbol{V}$, então $|B| = |B'|$.*

Demonstração. Primeiro, vamos mostrar que não ocorre o caso de uma base ser um conjunto finito e outra ser um conjunto infinito. Suponhamos, sem perda de generalidade, que B é um conjunto finito com $|B| = n$, $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\} := B$, e B' é um conjunto infinito. Seja $i \in [n]$. Como $\boldsymbol{b}_i \in V$ e B' gera V, segue que existem $\boldsymbol{b}_{i,1}, \ldots, \boldsymbol{b}_{i,n_i} \in B'$ e $c_{i,1}, \ldots, c_{i,n_i} \in C$ tais que

$$\boldsymbol{b}_i = \mathop{\mathbin{+}}_{j=1}^{n_i} c_{i,j} \boldsymbol{b}_{i,j}.$$

Notemos que o conjunto de todos esses $\boldsymbol{b}_{i,j}$ é $B'' := \bigcup_{i=1}^{n} \{\boldsymbol{b}_{i,j} : j \in [n_i]\}$, que é um subconjunto finito de B' e, portanto, um subconjunto próprio. Assim, como

$B'' \subset B'$, existe $\boldsymbol{b} \in B' \smallsetminus B''$. Como $\boldsymbol{b} \in V$ e B é base, segue que existem $c_1, \ldots, c_n \in C$ tais que $\boldsymbol{b} = +_{i=1}^{n} c_i \boldsymbol{b}_i$. Mas então

$$\boldsymbol{b} = \mathop{+}_{i=1}^{n} c_i \boldsymbol{b}_i = \mathop{+}_{i=1}^{n} c_i \mathop{+}_{j=1}^{n_i} c_{i,j} \boldsymbol{b}_{i,j} = \mathop{+}_{i=1}^{n} \mathop{+}_{j=1}^{n_i} c_i c_{i,j} \boldsymbol{b}_{i,j},$$

o que mostra que $\boldsymbol{b} \in B'$ pode ser escrito como uma combinação linear de $B' \smallsetminus \{\boldsymbol{b}\}$ em $\boldsymbol{V}$; ou seja, B' não é linearmente independente, o que é um absurdo. Assim, existem dois casos a serem considereados; o primeiro em que ambas as bases são conjuntos finitos e o outro em que ambas são conjuntos infinitos.

Suponhamos, no primeiro caso, que B e B' são conjuntos finitos com $|B| = n$ e $|B'| = m$. Como B é linearmente independente e B' gera V, segue que $|B| \leq |B'|$. Reciprocamente, como B' é linearmente independente e B gera V, segue que $|B'| \leq |B|$. Assim, segue que $|B| = |B'|$. Agora, suponhamos que B e B' são conjuntos infinitos.

TERMINAR ■

Definição 5.10. Sejam $\boldsymbol{V}$ um espaço vetorial sobre um corpo $\boldsymbol{C}$ e $B \subseteq V$ uma base $\boldsymbol{V}$. A *dimensão* de $\boldsymbol{V}$ é o número ordinal $\dim \boldsymbol{V} := |B|$.

5.6 Funções Lineares

Definição 5.11. Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços lineares sobre um corpo $\boldsymbol{C}$. Uma função *linear* de $\boldsymbol{V}$ para $\boldsymbol{W}$ é uma função $L\colon V \longrightarrow W$ que satisfaz

1. (Aditividade) Para todos $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$,

$$L(\boldsymbol{v}_1 + \boldsymbol{v}_2) = L(\boldsymbol{v}_1) + L(\boldsymbol{v}_2);$$

2. (Homogeneidade) Para todos $c \in C, \bigwedge \boldsymbol{v} \in V$,

$$L(c\boldsymbol{v}) = cL(\boldsymbol{v}).$$

Denota-se $L\colon \boldsymbol{V} \longrightarrow \boldsymbol{W}$. O conjunto das funções lineares de $\boldsymbol{V}$ para $\boldsymbol{W}$ é denotado $\mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$ e o conjunto das funções lineares de $\boldsymbol{V}$ para $\boldsymbol{V}$ é denotado $\mathcal{L}(\boldsymbol{V})$.

É imediato da definição que as duas propriedades são equivalentes à seguinte propriedade

1. (Linearidade) Para todos $c_1, c_2 \in C$ e $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$,

$$L(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1 L(\boldsymbol{v}_1) + c_2 L(\boldsymbol{v}_2).$$

Proposição 5.22. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços lineares sobre um corpo $\boldsymbol{C}$ e $L \in \mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$. Então*

1. *(Linearidade generalizada) Para todos $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in V$ e $c_1, \ldots, c_n \in C$,*

$$L\left(\mathop{+}_{i=1}^{n} c_i \boldsymbol{v}_i\right) = \mathop{+}_{i=1}^{n} c_i L(\boldsymbol{v}_i).$$

2. *$L(\mathbf{0}) = \mathbf{0}$;*

3. *$L(-\boldsymbol{v}) = -L(\boldsymbol{v})$.*

Proposição 5.23. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços lineares sobre um corpo $\boldsymbol{C}$. O espaço linear $\mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$ é um subespaço linear de $\boldsymbol{W}^{\boldsymbol{V}}$.*

Demonstração. Primeiro, sejam $L_1, L_2 \in \mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$. Então, para todos $c \in C$ e $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$,

$$\begin{aligned}
(L_1 + L_2)(\boldsymbol{v}_1 + c\boldsymbol{v}_2) &= L_1(\boldsymbol{v}_1 + c\boldsymbol{v}_2) + L_2(\boldsymbol{v}_1 + c\boldsymbol{v}_2) \\
&= L_1(\boldsymbol{v}_1) + cL_1(\boldsymbol{v}_2) + L_2(\boldsymbol{v}_1) + cL_2(\boldsymbol{v}_2) \\
&= L_1(\boldsymbol{v}_1) + L_2(\boldsymbol{v}_1) + cL_1(\boldsymbol{v}_2) + cL_2(\boldsymbol{v}_2) \\
&= (L_1 + L_2)(\boldsymbol{v}_1) + c(L_1 + L_2)(\boldsymbol{v}_2).
\end{aligned}$$

Agora, sejam $c' \in C$ e $L \in \mathcal{L}(\boldsymbol{V}; \boldsymbol{W})$. Então

$$\begin{aligned}
(c'L)(\boldsymbol{v}_1 + c\boldsymbol{v}_2) &= c'L(\boldsymbol{v}_1 + c\boldsymbol{v}_2) \\
&= c'(L(\boldsymbol{v}_1) + cL(\boldsymbol{v}_2)) \\
&= c'L(\boldsymbol{v}_1) + c'cL(\boldsymbol{v}_2) \\
&= (c'L)(\boldsymbol{v}_1) + c(c'L)(\boldsymbol{v}_2).
\end{aligned}$$

Portanto concluímos que $\mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$ é um subespaço linear de $\boldsymbol{W}^{\boldsymbol{V}}$. ■

Proposição 5.24. *Sejam $\boldsymbol{V}_1$, $\boldsymbol{V}_2$ e $\boldsymbol{V}_3$ espaços lineares sobre um corpo $\boldsymbol{C}$. Se $L_1 \in \mathcal{L}(\boldsymbol{V}_1, \boldsymbol{V}_2)$, $L_2 \in \mathcal{L}(\boldsymbol{V}_2, \boldsymbol{V}_3)$, então $L_2 \circ L_1 \in \mathcal{L}(\boldsymbol{V}_1, \boldsymbol{V}_3)$.*

Demonstração. Sejam $c \in C$ e $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$. Então

$$\begin{aligned}
(L_2 \circ L_1)(\boldsymbol{v}_1 + c\boldsymbol{v}_2) &= L_2(L_1(\boldsymbol{v}_1 + c\boldsymbol{v}_2)) \\
&= L_2(L_1(\boldsymbol{v}_1) + cL_1(\boldsymbol{v}_2)) \\
&= L_2(L_1(\boldsymbol{v}_1)) + cL_2(L_1(\boldsymbol{v}_2)) \\
&= (L_2 \circ L_1)(\boldsymbol{v}_1) + c(L_2 \circ L_1)(\boldsymbol{v}_2),
\end{aligned}$$

o que mostra que $L_2 \circ L_1$ é linear. ■

Proposição 5.25. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços lineares sobre um corpo $\boldsymbol{C}$ e $L \in \mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$. Se L é invertível, então $L^{-1} \in \mathcal{L}(\boldsymbol{W}, \boldsymbol{V})$.*

Demonstração. Seja $L \in \mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$. Se L é invertível, $L^{-1} \in V^W$ e, para todos $c \in C$ e $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$, existem $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ tais que $L(\boldsymbol{v}_1) = \boldsymbol{w}_1$ e $L(\boldsymbol{v}_2) = \boldsymbol{w}_2$ e segue que

$$\begin{aligned} L^{-1}(\boldsymbol{w}_1 + c\boldsymbol{w}_2) &= L^{-1}(L(\boldsymbol{v}_1) + cL(\boldsymbol{v}_2)) \\ &= L^{-1}(L(\boldsymbol{v}_1 + c\boldsymbol{v}_2)) \\ &= \boldsymbol{v}_1 + c\boldsymbol{v}_2 \\ &= L^{-1}(\boldsymbol{w}_1) + cL^{-1}(\boldsymbol{w}_2), \end{aligned}$$

o que mostra que L^{-1} é linear. ■

Proposição 5.26. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços lineares sobre um corpo $\boldsymbol{C}$, $B_V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ base de $\boldsymbol{V}$, $B_W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$ base de $\boldsymbol{W}$ e $L \in \mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$. Então, para todo $\boldsymbol{v} \in V$, existem únicos $c_1, \ldots, c_m \in C$ tais que*

$$L(\boldsymbol{v}) = \mathop{\mathbin{+}}_{i=1}^{m} c_j \boldsymbol{w}_j.$$

Demonstração. Primeiro demonstraremos a existência. Sabemos que, como B_V é base de V, então existem únicos $a_1, \ldots, a_n \in C$ tais que $\boldsymbol{v} = +_{i=1}^{n} a_i \boldsymbol{v}_i$. Mas, como L é linear, então

$$L(\boldsymbol{v}) = L\left(\mathop{\mathbin{+}}_{i=1}^{n} a_i \boldsymbol{v}_i\right) = \mathop{\mathbin{+}}_{i=1}^{n} a_i L(\boldsymbol{v}_i).$$

Agora, como B_W é base de $\boldsymbol{W}$, para cada $i \in \{1, \ldots, n\}$ existem únicos

$$b_{i1}, \ldots, b_{im} \in C$$

tais que $L(\boldsymbol{v}_i) = +_{j=1}^{m} b_{ij} \boldsymbol{w}_j$. Assim, definindo $c_j := +_{i=1}^{n} a_i b_{ij}$, segue que

$$L(\boldsymbol{v}) = \mathop{\mathbin{+}}_{i=1}^{n} a_i \left(\mathop{\mathbin{+}}_{j=1}^{m} b_{ij} \boldsymbol{w}_j\right) = \mathop{\mathbin{+}}_{j=1}^{m} \left(\mathop{\mathbin{+}}_{i=1}^{n} a_i b_{ij}\right) \boldsymbol{w}_j = \mathop{\mathbin{+}}_{j=1}^{m} c_j \boldsymbol{w}_j.$$

■

5.7 Produto e Coproduto de Espaços Vetoriais

5.7.1 Produto

Definição 5.12. Seja $(\boldsymbol{V_i})_{i \in I} = ((V_i, +_i, \cdot_i))_{i \in I}$ uma família de espaços vetoriais sobre um corpo $\boldsymbol{C}$. O *produto categórico* de $(\boldsymbol{V_i})_{i \in I}$ é a tripla

$$\prod_{i \in I} \boldsymbol{V_i} = (V, +, \cdot),$$

em que $V = \prod_{i\in I} V_i$,

$$\begin{aligned} +\colon V \times V &\longrightarrow V \\ (v_1, v_2) &\longmapsto ((v_1)_i +_i (v_2)_i)_{i\in I} \end{aligned}$$

e

$$\begin{aligned} \cdot\colon C \times V &\longrightarrow V \\ (c, v) &\longmapsto (c \cdot_i v_i)_{i\in I}. \end{aligned}$$

Proposição 5.27. *Seja* $(\boldsymbol{V_i})_{i\in I} = ((V_i, +_i, \cdot_i))_{i\in I}$ *uma família de espaços vetoriais sobre um corpo* $\boldsymbol{C}$. *Então* $\prod_{i\in I} \boldsymbol{V_i} = (V, +, \cdot)$ *é um espaço vetorial sobre* $\boldsymbol{C}$.

Demonstração. 1. $(V, +)$ é um grupo pois tem a mesma operação do produto de grupos (2.28).

2. Seja $v \in V$. Então
$$1v = (1v_i)_{i\in I} = (v_i)_{i\in I} = v.$$
Sejam $c_1, c_2 \in C$ e $v \in V$. Então
$$\begin{aligned} (c_1c_2)v &= ((c_1c_2)v_i)_{i\in I} \\ &= (c_1(c_2v_i))_{i\in I} \\ &= c_1(c_2v_i)_{i\in I} \\ &= c_1(c_2v). \end{aligned}$$

3. (Distributividades) Sejam $c \in C$ e $v, v' \in V$. Então
$$\begin{aligned} c(v + v') &= c(v_i + v'_i)_{i\in I} \\ &= (c(v_i + v'_i))_{i\in I} \\ &= (cv_i + cv'_i)_{i\in I} \\ &= (cv_i)_{i\in I} + (cv'_i)_{i\in I} \\ &= cv + cv'. \end{aligned}$$
Sejam $c_1, c_2 \in C$ e $v \in V$. Então
$$\begin{aligned} (c_1 + c_2)v &= ((c_1 + c_2)v_i)_{i\in I} \\ &= (c_1v_i + c_2v_i)_{i\in I} \\ &= (c_1v_i)_{i\in I} + (c_2v_i)_{i\in I} \\ &= c_1v + c_2v. \end{aligned}$$
■

Proposição 5.28. *Seja* $(\boldsymbol{V_i})_{i\in I} = ((V_i, +_i, \cdot_i))_{i\in I}$ *uma família de espaços vetoriais sobre um corpo* $\boldsymbol{C}$*. Para todo* $i \in I$*, a projeção canônica* $\pi_i : \prod_{i\in I} \boldsymbol{V_i} \longrightarrow \boldsymbol{V_i}$ *é uma função linear.*

Demonstração. Sejam $c \in C$ e $v, v' \in \prod_{i\in I} V_i$. Então

$$\pi_i(v + cv') = \pi_i((v_i + cv'_i)_{i\in I}) = v_i + cv'_i = \pi_i(v) + c\pi_i(v'). \qquad \blacksquare$$

Proposição 5.29 (Propriedade Universal)**.** *Sejam* $(\boldsymbol{V_i})_{i\in I}$ *uma família de espaços vetoriais sobre um corpo* $\boldsymbol{C}$*,* $\boldsymbol{X}$ *um espaço vetorial sobre* $\boldsymbol{C}$ *e, para todo* $i \in I$*,* $L_i : \boldsymbol{X} \longrightarrow \boldsymbol{V_i}$ *uma função linear. Então existe única função linear* $L : \boldsymbol{X} \longrightarrow \prod_{i\in I} \boldsymbol{V_i}$ *tal que, para todo* $i \in I$*,* $\pi_i \circ L = L_i$ *(o diagrama comuta).*

$$\begin{tikzcd}
 & \prod\limits_{i\in I} \boldsymbol{V_i} \arrow[d, "\pi_i"] \\
\boldsymbol{X} \arrow[ur, dashed, "L"] \arrow[r, "L_i"'] & \boldsymbol{V_i}
\end{tikzcd}$$

Demonstração. Defina a função

$$\begin{aligned} L\colon X &\longrightarrow \prod_{i\in I} V_i \\ x &\longmapsto (L_i(x))_{i\in I}. \end{aligned}$$

Da propriedade universal para conjuntos, L é a única função de X para $\bigtimes_{i\in I} \boldsymbol{V_i}$ tal que, para todo $i \in I$, $\pi_i \circ L = L_i$. Falta mostrar que L é função linear. Sejam $c \in C$ e $x_1, x_2 \in V$. Então

$$\begin{aligned} L(x_1 + cx_2) &= (L_i(x_1 + cx_2))_{i\in I} \\ &= (L_i(x_1) + cL_i(x_2))_{i\in I} \\ &= (L_i(x_1))_{i\in I} + c(L_i(x_2))_{i\in I} \\ &= L(x_1) + cL(x_2). \end{aligned} \qquad \blacksquare$$

5.7.2 Coproduto (Soma)

Definição 5.13. Seja $(\boldsymbol{V_i})_{i\in I} = ((V_i, +_i, \cdot_i))_{i\in I}$ uma família de espaços vetoriais. A *soma categórica* de $(\boldsymbol{V_i})_{i\in I}$ é

$$\bigsqcup_{i\in I} \boldsymbol{V_i} = (V, +, \cdot),$$

em que

$$V = \left\{ v = (v_i)_{i\in I} \in \prod_{i\in I} V_i \;\middle|\; |\mathrm{supp}(v)| < |\mathbb{N}| \right\},$$

$$\begin{aligned} +\colon V \times V &\longrightarrow V \\ (v, v') &\longmapsto (v_i +_i v'_i)_{i\in I} \end{aligned}$$

e

$$\begin{aligned} \cdot\colon C \times V &\longrightarrow V \\ (c, v) &\longmapsto (cv_i)_{i\in I}. \end{aligned}$$

Observe que, se $|I| < |\mathbb{N}|$, então $\prod_{i\in I} \boldsymbol{V_i} = \bigsqcup_{i\in I} \boldsymbol{V_i}$.

Proposição 5.30 (Propriedade Universal)**.** *Sejam $(\boldsymbol{V_i})_{i\in I}$ uma família de espaços vetoriais sobre um corpo $\boldsymbol{C}$, $\boldsymbol{X}$ um espaço vetorial sobre $\boldsymbol{C}$ e, para todo $i \in I$, $L_i : \boldsymbol{V_i} \longrightarrow \boldsymbol{X}$ uma função linear. Então existe única função linear $L : \boldsymbol{X} \longrightarrow \bigsqcup_{i\in I} \boldsymbol{V_i}$ tal que, para todo $i \in I$, $L \circ \iota_i = L_i$ (o diagrama comuta).*

$$\begin{tikzcd} \boldsymbol{V_i} \arrow[r, "L_i"] \arrow[d, "\iota_i"'] & \boldsymbol{X} \\ \bigsqcup_{i\in I} \boldsymbol{V_i} \arrow[ur, dashed, "L"'] & \end{tikzcd}$$

O coproduto de espaços vetoriais é também chamado de *soma* ou *soma direta* e denotado

$$\bigoplus_{i\in I} \boldsymbol{V_i}.$$

5.8 Projeções Lineares

Definição 5.14. Seja $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$. Uma *projeção linear* em $\boldsymbol{V}$ é uma função linear $p\colon V \longrightarrow V$ idenpotente: $p^2 = p$.

Proposição 5.31. *Sejam $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$ e $p\colon V \longrightarrow V$ uma projeção linear.*

1. $p|_{p(V)} = \mathrm{I}|_{p(V)}$;

2. $(\mathrm{I}-p)\colon V \longrightarrow V$ *é uma projeção linear em* $\boldsymbol{V}$*;*

3. $(\mathrm{I}-p)^{-1}(0) = p(V)$ *e* $(\mathrm{I}-p)(V) = p^{-1}(0)$*;*

4. $V = p(V) \oplus p^{-1}(0) = p(V) \oplus (\mathrm{I}-p)(V)$*;*

5. *Para todo* $\lambda \in C \smallsetminus \{0,1\}$*,*

$$(\lambda\mathrm{I}-p)^{-1} = \frac{1}{\lambda}\mathrm{I} + \frac{1}{\lambda(1-\lambda)}p$$

   portanto $\mathrm{Esp}(p) \subseteq \{0,1\}$*;*

6. p *é invertível se, e somente se,* $p = \mathrm{I}$*.*

7. *Se* $p \neq 0$*, seu polinômio mínimo é* $x^2 - x = x(x-1)$*, logo* p *é diagonalizável pois tem raízes distintas.*

Demonstração. 1. Seja $v \in p(V)$. Então existe $v' \in V$ tal que $v = p(v')$, logo

$$p(v) = p(p(v')) = p^2(v') = p(v') = v.$$

2. A função $\mathrm{I}-p$ é linear pois é uma diferença de funções lineares. Basta mostrar que ela é idempotente. Basta notar que

$$(\mathrm{I}-p)^2 = \mathrm{I} - p - p + p^2 = \mathrm{I} - p - p + p = \mathrm{I} - p.$$

3. Seja $v \in (\mathrm{I}-p)^{-1}(0)$. Então $(\mathrm{I}-p)(v) = 0$, logo $v = p(v)$, o que implica que $v \in p(V)$. Reciprocamente, seja $v \in p(V)$. Então do item 1 segue que $p(v) = v$, logo $(\mathrm{I}-p)(v) = v - p(v) = v - v = 0$.

   A outra relação segue de $(\mathrm{I}-p)$ ser projeção e $p = \mathrm{I} - (\mathrm{I}-p)$.

4. Seja $v \in p(V) \cap p^{-1}(0)$. Então $p(v) = 0$ e $p(v) = v$, o que implica que $v = p(v) = 0$. Assim temos que $p(V) \cap p^{-1}(0) = \{0\}$.

   Seja $v \in V$. Então $p(v) \in p(V)$ e $(\mathrm{I}-p)(v) \in p^{-1}(0)$ (pois $(\mathrm{I}-p)(V) = p^{-1}(0)$), logo $v = p(v) + (\mathrm{I}-p)(v)$, o que mostra que $V = p(V) + p^{-1}(V)$.

5. Note que

$$\frac{1}{1-\lambda} - \frac{1}{\lambda} - \frac{1}{\lambda(1-\lambda)} = \frac{\lambda - (\lambda-1) - 1}{\lambda(1-\lambda)} = 0,$$

logo

$$\begin{aligned}(\lambda \mathrm{I} - p) \circ \left(\frac{1}{\lambda}\mathrm{I} + \frac{1}{\lambda(1-\lambda)}p\right) &= \mathrm{I} + \frac{1}{1-\lambda}p - \frac{1}{\lambda}p - \frac{1}{\lambda(1-\lambda)}p^2 \\ &= \mathrm{I} + \left(\frac{1}{1-\lambda} - \frac{1}{\lambda} - \frac{1}{\lambda(1-\lambda)}\right)p \\ &= \mathrm{I}.\end{aligned}$$

e

$$\left(\frac{1}{\lambda}\mathrm{I} + \frac{1}{\lambda(1-\lambda)}p\right) \circ (\lambda \mathrm{I} - p) = \mathrm{I} - \frac{1}{\lambda}p + \frac{1}{1-\lambda}p - \frac{1}{\lambda(1-\lambda)}p^2 = \mathrm{I}.$$

6. Se p é invertível, $V = p(V)$, logo

$$p = p|_V = p|_{p(V)} = \mathrm{I}|_{p(V)} = \mathrm{I}|_V = \mathrm{I}.$$

A recíproca é evidente.

7. Evidente.

■

5.9 Funções Multilineares

Definição 5.15. Sejam $\boldsymbol{V_0}, \cdots, \boldsymbol{V_{k-1}}$ e $\boldsymbol{W}$ espaços lineares sobre um corpo $\boldsymbol{C}$ e $k \in \mathbb{N}$. Uma função *k-linear* de $(\boldsymbol{V_0}, \ldots, \boldsymbol{V_{k-1}})$ para $\boldsymbol{W}$ é uma função

$$L\colon V_0 \times \cdots \times V_{k-1} \longrightarrow W$$

qua satisfaz

1. (Multilinearidade) Para todos $i \in [k]$ e

$$(v_0, \ldots, v_{i-1}, v_{i+1}, \ldots, v_{k-1}) \in V_0 \times \cdots \times V_{i-1} \times V_{i+1} \times \cdots \times V_{k-1},$$

a função

$$\begin{aligned} L(v_0, \ldots, v_{i-1}, \boldsymbol{\cdot}, v_{i+1}, \ldots, v_{k-1})\colon \boldsymbol{V_i} &\longrightarrow \boldsymbol{W} \\ v &\longmapsto L(v_0, \ldots, v_{i-1}, v, v_{i+1}, \ldots, v_{k-1}) \end{aligned}$$

é uma função linear.

O conjunto dessas funções é denotado

$$\mathcal{L}(V_0, \ldots, V_{k-1}; W)$$

e, quando todos os espaços $\boldsymbol{V_i}$ são iguais, denota-se

$$\mathcal{L}^k(V, W) := \mathcal{L}(\underbrace{V, \ldots, V}_{k}; W)$$

Proposição 5.32. *Sejam $\boldsymbol{V_0}, \cdots, \boldsymbol{V_{k-1}}$ e $\boldsymbol{W}$ espaços lineares sobre um corpo $\boldsymbol{C}$ 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 $\boldsymbol{V_i}$. Toda função k-linear $L \in \mathcal{L}(V_0, \ldots, V_{k-1}; W)$ está determinada pelos seus valores em $(b_{j_0}^{(0)}, \ldots, b_{j_{k-1}}^{(k-1)})_{(j_0, \ldots, j_{k-1}) \in [d_0] \times \cdots \times [d_{k-1}]}$.*

Demonstração. Sejam $v_0, \ldots, v_{m-1} \in V_k$, $c^0, \ldots, c^{m-1} \in C$, e, para todo $i \in [k] \smallsetminus \{k\}$, $v_i' \in V_i$. Como consequência da propriedade de linearidade generalizada para funções lineares,

$$L\left(v_0', \ldots, \mathop{+}_{i \in [m]} c^i v_i, \ldots, v_{k-1}'\right) = \mathop{+}_{i \in [m]} c^i L\left(v_0', \ldots, v_i, \ldots, v_{k-1}'\right).$$

Sendo assim, para cada $i \in [k]$, sejam $v_i \in V_i$ e $v_{(i)}^0, \ldots, v_{(i)}^{d_i} \in C$ os coeficientes de v_i na base $b^{(i)}$, de modo que

$$v_i = \mathop{+}_{j \in [d_i]} v_{(i)}^j b_j^{(i)}.$$

Pela linearidade em cada entrada, temos que

$$\begin{aligned}
L(v_0, \ldots, v_{k-1}) &= L\left(\mathop{+}_{j_0 \in [d_0]} v_{(0)}^{j_0} b_{j_0}^{(0)}, \ldots, \mathop{+}_{j_{k-1} \in [d_{k-1}]} v_{(k-1)}^{j_{k-1}} b_{j_{k-1}}^{(k-1)}\right) \\
&= \mathop{+}_{j_0 \in [d_0]} v_{(0)}^{j_0} L\left(b_{j_0}^{(0)}, \ldots, \mathop{+}_{j_{k-1} \in [d_{k-1}]} v_{(k-1)}^{j_{k-1}} b_{j_{k-1}}^{(k-1)}\right) \\
&\vdots \qquad\qquad\qquad\qquad \vdots \\
&= \mathop{+}_{j_0 \in [d_0]} \cdots \mathop{+}_{j_{k-1} \in [d_{k-1}]} v_{(0)}^{j_0} \cdots v_{(k-1)}^{j_{k-1}} L\left(b_{j_0}^{(0)}, \ldots, b_{j_{k-1}}^{(k-1)}\right) \\
&= \mathop{+}_{(j_0, \ldots, j_{k-1}) \in [d_0] \times \cdots \times [d_{k-1}]} v_{(0)}^{j_0} \cdots v_{(k-1)}^{j_{k-1}} L\left(b_{j_0}^{(0)}, \ldots, b_{j_{k-1}}^{(k-1)}\right).
\end{aligned}$$

Portanto a função L está determinada pelos valores que tem nos elementos

$$(b_{j_0}^{(0)}, \ldots, b_{j_{k-1}}^{(k-1)})_{(j_0, \ldots, j_{k-1}) \in [d_0] \times \cdots \times [d_{k-1}]}.$$

■

Proposição 5.33. *Sejam* $\boldsymbol{V_0}, \cdots, \boldsymbol{V_{k-1}}$ *e* $\boldsymbol{W}$ *espaços lineares sobre um corpo* $\boldsymbol{C}$*. Então*

$$\mathcal{L}(\boldsymbol{V_0}, \ldots, \boldsymbol{V_{k-1}}; \boldsymbol{W}) := (\mathcal{L}(V_0, \ldots, V_{k-1}; W), +, \cdot),$$

em que $+$ *e* $\cdot$ *são a soma e o produto escalar pontuais induzidos por* $\boldsymbol{W}$*, é um espaço linear sobre* $\boldsymbol{C}$*.*

5.9.1 Simetria, Antissimetria e Alternância

Definição 5.16. Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços lineares sobre um corpo $\boldsymbol{C}$. Uma função k-linear de $\boldsymbol{V}$ para $\boldsymbol{W}$

1. *simétrica* é uma função $f \in \mathcal{L}^k(\boldsymbol{V}, \boldsymbol{W})$ tal que, para toda permutação $p \in \mathfrak{S}_k$ e todos v_0, ..., $v_{k-1} \in V$,

$$f(v_{p(0)}, \ldots, v_{p(k-1)}) = f(v_0, \ldots, v_{k-1});$$

   O conjunto das funções k-lineares simétricas é denotado $\mathcal{S}^k(\boldsymbol{V}, \boldsymbol{W})$.

2. *antissimétrica* é uma função $f \in \mathcal{L}^k(\boldsymbol{V}, \boldsymbol{W})$ tal que, para toda permutação $p \in \mathfrak{S}_k$ e todos $v_0, \ldots, v_{k-1} \in V$,

$$f(v_{p(0)}, \ldots, v_{p(k-1)}) = \epsilon(p) f(v_0, \ldots, v_{k-1});$$

3. *alternada* é uma função $f \in \mathcal{L}^k(\boldsymbol{V}, \boldsymbol{W})$ tal que, para todos $v_0, \ldots, v_{k-1} \in V$ linearmente dependentes,

$$f(v_0, \ldots, v_{k-1}) = 0.$$

   O conjunto das funções k-lineares alternadas é denotado $\mathcal{A}^k(\boldsymbol{V}, \boldsymbol{W})$.

Proposição 5.34. *Sejam* $\boldsymbol{V}$ *e* $\boldsymbol{W}$ *espaços lineares sobre um corpo* $\boldsymbol{C}$ *e* $f \in \mathcal{L}^k(\boldsymbol{V}, \boldsymbol{W})$*.*

1. *A função* f *é alternada se, e somente se, para todos* v_0, ..., $v_{k-1} \in V$ *tais que existem* $i, j \in [k]$ *distintos satizfazendo* $v_i = v_j$*,*

$$f(v_0, \ldots, v_{k-1}) = 0.$$

2. *Se* f *é alternada, então é antissimétrica. Se* $\operatorname{car}(\boldsymbol{C}) \neq 2$ *e* f *é antissimétrica, então é alternada.*

3. *Se* $\operatorname{car}(\boldsymbol{C}) = 2$*, então* f *é antissimétrica se, e somente se, é simétrica.*

Demonstração. 1. Se f é alternada, então, para todos $v_0, \ldots, v_{k-1} \in V$ tais que $v_i = v_j$ para dois $i, j \in [k]$ distintos, o conjunto $\{v_0, \ldots, v_{k-1}\}$ é linearmente dependente, portanto $f(v_0, \ldots, v_{k-1}) = 0$. Reciprocamente, suponha que f satisfaz a propriedade e sejam $v_0, \ldots, v_{k-1} \in V$ linearmente dependentes. Então existe $i \in [k]$ tal que v_i é combinação linear dos outros v_j: existem $c_j \in C$, com $j \in [k] \smallsetminus \{i\}$, tais que

$$v_i = \mathop{+}_{j \in [k] \smallsetminus \{i\}} c_j v_j.$$

Assim, segue da k-linearidade e da propriedade enunciada que

$$\begin{aligned} f(v_0, \ldots, v_{k-1}) &= f\left(v_0, \ldots, \mathop{+}_{j \in [k] \smallsetminus \{i\}} c_j v_j, \ldots, v_{k-1}\right) \\ &= \mathop{+}_{j \in [k] \smallsetminus \{i\}} c_j f(v_0, \ldots, v_j, \ldots, v_{k-1}) \\ &= \mathop{+}_{j \in [k] \smallsetminus \{i\}} c_j 0 = 0. \end{aligned}$$

2. Suponha f alternada e sejam $v_0, \ldots, v_{k-1} \in V$. Então segue da k-linearidade e da alternância de f que

$$\begin{aligned} 0 =& f(v_0, \ldots, v_i + v_j, \ldots, v_i + v_j, \ldots, v_{k-1}) \\ =& f(v_0, \ldots, v_i, \ldots, v_i, \ldots, v_{k-1}) + f(v_0, \ldots, v_i, \ldots, v_j, \ldots, v_{k-1}) \\ &+ f(v_0, \ldots, v_j, \ldots, v_i, \ldots, v_{k-1}) + f(v_0, \ldots, v_j, \ldots, v_j, \ldots, v_{k-1}) \\ =& f(v_0, \ldots, v_i, \ldots, v_j, \ldots, v_{k-1}) + f(v_0, \ldots, v_j, \ldots, v_i, \ldots, v_{k-1}), \end{aligned}$$

portanto

$$f(v_0, \ldots, v_i, \ldots, v_j, \ldots, v_{k-1}) = -f(v_0, \ldots, v_j, \ldots, v_i, \ldots, v_{k-1}).$$

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 $p \in \mathfrak{S}_k$,

$$f(v_{p(0)}, \ldots, v_{p(k-1)}) = (-1)^N f(v_0, \ldots, v_{k-1}) = \epsilon(p) f(v_0, \ldots, v_{k-1}).$$

Suponha que $\operatorname{car}(\boldsymbol{C}) \neq 2$. Sejam $f \in \mathcal{L}^k(\boldsymbol{V}, \boldsymbol{W})$ antissimétrica e v_0, …, $v_{k-1} \in V$ tais que $v_i = v_j$ para dois $i, j \in [k]$ distintos. Considerando a permutação $(i \quad j) \in \mathfrak{S}_k$, segue da antissimetria de f e de $\epsilon((i \quad j)) = -1$ que

$$\begin{aligned} f(v_0, \ldots, v_i, \ldots, v_j, \ldots, v_{k-1}) &= f(v_0, \ldots, v_j, \ldots, v_i, \ldots, v_{k-1}) \\ &= -f(v_0, \ldots, v_i, \ldots, v_j, \ldots, v_{k-1}), \end{aligned}$$

portanto
$$2f(v_0, \ldots, v_{k-1}) = 0.$$
Como $\mathrm{car}(\boldsymbol{C}) \neq 2$, segue que $f(v_0, \ldots, v_{k-1}) = 0$. Do item 1 segue que f é alternada.

3. Se $\mathrm{car}(\boldsymbol{C}) = 2$, 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 $f\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$ dada por

$$\begin{aligned} f\colon \mathbb{Z}_2 \times \mathbb{Z}_2 &\longrightarrow \mathbb{Z}_2 \\ (0,0) &\longmapsto 0 \\ (0,1) &\longmapsto 0 \\ (1,0) &\longmapsto 0 \\ (1,1) &\longmapsto 1 \end{aligned}$$

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 $p\colon [k] \longrightarrow [k]$, 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 $p\colon [k] \longrightarrow [k]$,

$$f(v_{p(0)}, \ldots, v_{v_{k-1}}) = \epsilon(p) f(v_0, \ldots, v_{k-1}).$$

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 5.35. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ espaços lineares sobre um corpo $\boldsymbol{C}$. Os espaços $\mathcal{S}^k(\boldsymbol{V}, \boldsymbol{W})$ e $\mathcal{A}^k(\boldsymbol{V}, \boldsymbol{W})$ são subespaços lineares de $\mathcal{L}^k(\boldsymbol{V}, \boldsymbol{W})$.*

5.10 Formas Multilineares

Definição 5.17. Seja $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$. Uma *forma k-linear* em $\boldsymbol{V}$ é uma função $f \in \mathcal{L}^k(\boldsymbol{V}; \boldsymbol{C})$, ou seja, um funcional k-linear em $(\boldsymbol{V}, \ldots, \boldsymbol{V})$.

O conjunto das formas k-lineares simétricas é denotado $\mathcal{S}^k(\boldsymbol{V})$ e o das alternadas é denotado $\mathcal{A}^k(\boldsymbol{V})$.

Temos que $\mathcal{S}^1(\boldsymbol{V}) = \mathcal{A}^1(\boldsymbol{V}) = \mathcal{L}^k(\boldsymbol{V})$ e $\mathcal{S}^0(\boldsymbol{V}) = \mathcal{A}^0(\boldsymbol{V}) = \mathcal{L}^0(\boldsymbol{V}) = C$.

5.10.1 Produto Tensorial de Formas Multilineares

Definição 5.18. Sejam $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$, $f \in \mathcal{L}^k(V)$, $f' \in \mathcal{L}^{k'}(V)$ e $v_0, \ldots, v_{k+k'-1} \in V$. O *produto tensorial* de f e f' em $(v_0, \ldots, v_{k+k'-1})$ é

$$(f \otimes f')(v_0, \ldots, v_{k+k'-1}) := f(v_0, \ldots, v_{k-1}) f'(v_k, \ldots, v_{k+k'-1}).$$

Sejam $n \in \mathbb{N}$ e $(f_i)_{i\in[n]}$ formas multilineares em $\boldsymbol{V}$. 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 5.36. *Seja $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$.*

1. *Para todas formas $f \in \mathcal{L}^k(\boldsymbol{V})$ e $f' \in \mathcal{L}^{k'}(\boldsymbol{V})$, a função $f \otimes f'$ é uma forma $k + k'$-linear.*

2. *(Bilinearidade) A função*

$$\begin{aligned} \otimes \colon \mathcal{L}^k(\boldsymbol{V}) \times \mathcal{L}^{k'}(\boldsymbol{V}) &\longrightarrow \mathcal{L}^{k+k'}(\boldsymbol{V}) \\ (f, f') &\longmapsto f \otimes f' \end{aligned}$$

   é bilinear.

3. *(Associatividade) Para todas formas $f \in \mathcal{L}^k(\boldsymbol{V})$, $f' \in \mathcal{L}^{k'}(\boldsymbol{V})$ e $f'' \in \mathcal{L}^{k''}(\boldsymbol{V})$,*

$$(f \otimes f') \otimes f'' = f \otimes (f' \otimes f'').$$

5.10.2 Produto Alternado de Formas Multilineares

Definição 5.19. Sejam $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$, $f \in \mathcal{A}^k(\boldsymbol{V})$, $f' \in \mathcal{A}^{k'}(\boldsymbol{V})$ e $v_0, \ldots, v_{k+k'-1} \in \boldsymbol{V}$. O *produto alternado* (ou *exterior*) de f e f' em $(v_0, \ldots, v_{k+k'-1})$ é

$$(f \wedge f')(v_0, \ldots, v_{k+k'-1}) := \frac{1}{k!k'!} \bigplus_{p\in\mathfrak{S}_{k+k'}} \epsilon(p)(f \otimes f')(v_{p(i)})_{i\in[k+k']}.$$

Sejam $n \in \mathbb{N}$ e $(f_i)_{i\in[n]}$ formas multilineares em $\boldsymbol{V}$. 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 5.37. *Seja $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$.*

1. *Para todas formas $f \in \mathcal{L}^k(\boldsymbol{V})$ e $f' \in \mathcal{L}^{k'}(\boldsymbol{V})$, a função $f \wedge f'$ é uma forma $k + k'$-linear alternada.*

2. *(Bilinearidade) A função*

$$\begin{aligned} \wedge\colon \mathcal{A}^k(\boldsymbol{V}) \times \mathcal{A}^{k'}(\boldsymbol{V}) &\longrightarrow \mathcal{A}^{k+k'}(\boldsymbol{V}) \\ (f, f') &\longmapsto f \wedge f' \end{aligned}$$

   é bilinear.

3. *(Associatividade) Para todas formas alternadas $f \in \mathcal{A}^k(\boldsymbol{V})$, $f' \in \mathcal{A}^{k'}(\boldsymbol{V})$ e $f'' \in \mathcal{A}^{k''}(\boldsymbol{V})$,*

$$(f \wedge f') \wedge f'' = f \wedge (f' \wedge f'').$$

4. *Para todas formas $f \in \mathcal{A}^k(\boldsymbol{V})$ e $f' \in \mathcal{A}^{k'}(\boldsymbol{V})$*

$$f' \wedge f = (-1)^{kk'} f \wedge f'.$$

Demonstração. 1. Seja $v_0, \ldots, v_{k+k'-1} \in V$ e $\bar{p} \in \mathfrak{S}_{k+k'}$. Então

$$\begin{aligned} (f \wedge f')(v_{\bar{p}(i)})_{i\in[k+k']} &= \frac{1}{k!k'!} \bigplus_{p\in\mathfrak{S}_{k+k'}} \epsilon(p)(f \otimes f')(v_{p(\bar{p}(i))})_{i\in[k+k']} \\ &= \frac{1}{k!k'!} \bigplus_{p\in\mathfrak{S}_{k+k'}} \epsilon(\bar{p}^{-1}p)(f \otimes f')(v_{p(i)})_{i\in[k+k']} \\ &= \frac{1}{k!k'!} \bigplus_{p\in\mathfrak{S}_{k+k'}} \epsilon(\bar{p}^{-1})\epsilon(p)(f \otimes f')(v_{p(i)})_{i\in[k+k']} \\ &= \epsilon(\bar{p}^{-1})\frac{1}{k!k'!} \bigplus_{p\in\mathfrak{S}_{k+k'}} \epsilon(p)(f \otimes f')(v_{p(i)})_{i\in[k+k']} \\ &= \epsilon(\bar{p})(f \wedge f')(v_i)_{i\in[k+k']}. \end{aligned}$$

2.

■

Proposição 5.38. *Sejam $\boldsymbol{V}$ um espaço linear de dimensão finita d sobre um corpo $\boldsymbol{C}$, $(b_i)_{i\in[d]}$ um base ordenada de $\boldsymbol{V}$ e $({b_i}^*)_{i\in[d]}$ a base dual de $\boldsymbol{V}^*$. Então $\mathcal{A}^k(\boldsymbol{V})$ é um espaço linear sobre $\boldsymbol{C}$ de dimensão $\binom{d}{k}$ e o conjunto*

$$\left\{b^*_{i_0} \wedge \cdots \wedge b^*_{i_{k-1}} \;\middle|\; i_0 < \cdots < i_{k-1} \in [d]\right\}$$

de formas alternadas k-lineares em $\boldsymbol{V}$ é uma base para $\mathcal{A}^k(\boldsymbol{V})$.

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*.

Definição 5.20. Seja $d \in \mathbb{N}$. O *determinante* em $\mathbb{R}^d$ é a forma d-linear

$$\det := {e_0}^* \wedge \ldots \wedge {e_{d-1}}^*.$$

Como comentado, essa é a única forma d-linear em $\mathbb{R}^d$ tal que

$$\det(e_0, \ldots, e_{d-1}) = 1.$$

Na seção seguinte, definiremos o conceito de determinante de modo mais geral e independente de base.

5.10.3 Formas Puxadas e Determinante

Definição 5.21. Sejam $\boldsymbol{V}$ e $\boldsymbol{V'}$ espaços lineares sobre um corpo $\boldsymbol{C}$, $L\colon V \longrightarrow V'$ uma função linear e $f \in \mathcal{L}^k(V')$. A *forma k-linear puxada* por L de f é a função

$$\begin{aligned} L^*f\colon V^k &\longrightarrow C \\ (v_0, \ldots, v_{k-1}) &\longmapsto f(L(v_0), \ldots, L(v_{k-1})). \end{aligned}$$

A função *k-adjunta* induzida por L é a função linear

$$\begin{aligned} L^*\colon \mathcal{L}^k(V') &\longrightarrow \mathcal{L}^k(V) \\ f &\longmapsto L^*f. \end{aligned}$$

A notação é ambígua porque, para cada $k \in [d+1]$, a função L^* é uma função diferente. De fato, para $f \in \mathcal{L}^k(V')$,

$$L^*f = f \circ L^{\otimes k},$$

o que quer dizer que

$$L^* = (L^{\otimes k})^\star$$

Proposição 5.39. *Sejam $\boldsymbol{V}$, $\boldsymbol{V}'$ e $\boldsymbol{V}''$ espaços lineares sobre um corpo $\boldsymbol{C}$ e $L\colon V \longrightarrow V'$ e $L'\colon V' \longrightarrow V''$ funções lineares. Então*

$$(L' \circ L)^* = L^* \circ L'^*.$$

Demonstração. Seja $f \in \mathcal{L}^k(V)$ tal que $f \neq 0$. Então

$$\begin{aligned}(L' \circ L)^* f(v_0, \ldots, v_{k-1}) &= f((L' \circ L)(v_0), \ldots, (L' \circ L)(v_{k-1})) \\ &= f(L'(L(v_0)), \ldots, L'(L(v_{k-1}))) \\ &= L'^* f(L(v_0), \ldots, L(v_{k-1})) \\ &= L^*(L'^* f)(v_0, \ldots, v_{k-1}) \\ &= (L^* \circ L'^*) f(v_0, \ldots, v_{k-1}).\end{aligned}$$

■

Essas funções 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 linear d-dimensional $\boldsymbol{V}$, o espaço $\mathcal{A}^d(\boldsymbol{V})$ 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 é seu d-adjunto.

Definição 5.22. Sejam $\boldsymbol{V}$ um espaço linear d-dimensional sobre um um corpo $\boldsymbol{C}$, $L\colon V \longrightarrow V$ uma função linear e $L^*\colon \mathcal{A}^d(V) \longrightarrow \mathcal{A}^d(V)$. O *determinante* de L é a constante $\det(L) \in C$ tal que, para todas formas $f \in \mathcal{A}^d(\boldsymbol{V})$,

$$L^* f = \det(L) f.$$

Isso nos dá por definição a igualdade

$$f(L(v_0), \ldots, L(v_{d-1})) = \det(L) f(v_0, \ldots, v_{d-1}).$$

Proposição 5.40. *Sejam $\boldsymbol{V}$ um espaço linear d-dimensional sobre um um corpo $\boldsymbol{C}$ e $L, L' \in \mathcal{L}(V, V)$. Então*

$$\det(L' \circ L) = \det(L) \det(L').$$

Demonstração. Seja $f \in \mathcal{A}^n(V)$ tal que $f \neq 0$. Então

$$\det(L' \circ L) f = (L' \circ L)^* f = (L^* \circ L'^*) f = \det(L) \det(L') f.$$

■

Proposição 5.41. *Sejam $\boldsymbol{V}$ um espaço linear d-dimensional sobre um um corpo $\boldsymbol{C}$ e $L\colon V \longrightarrow V$ uma função linear. Então L é invertível se, e somente se,* $\det(L) \neq 0$.

Demonstração. Basta notar que L é invertível se, e somente se, leva base em base e $f \in \mathcal{A}^d(V)$ é nula em um conjunto linearmente independente de vetores. ■

5.10.4 Extras

Definimos

$$[d]^{\uparrow k} := \left\{ (i_0, \ldots, i_{k-1}) \in [d]^k \;\middle|\; i_0 < \cdots < i_{k-1} \right\}.$$

Note que

$$\left| [d]^{\uparrow k} \right| = \left| \binom{[d]}{k} \right| = \binom{d}{k},$$

em que $\binom{[d]}{k} = \{I \subseteq [d] \mid |I| = k\}$.

5.11 Produto Tensorial de Espaços Lineares

Definição 5.23. Sejam X um conjunto, $\boldsymbol{C}$ um corpo e $f : X \longrightarrow C$ uma função. O *suporte* de f é o conjunto

$$\operatorname{supp}(f) := f^{-1}\left(\{0\}^{\complement}\right) = \{x \in X \mid f(x) \neq 0\}.$$

Definição 5.24. Sejam I um conjunto e $\boldsymbol{C}$ um corpo. O *espaço linear livre em I* sobre $\boldsymbol{C}$ é o conjunto

$$\mathcal{F}(I) := \left\{v \in C^I \;\middle|\; |\operatorname{supp}(v)| < |\mathbb{N}|\right\}.$$

Os elementos de $\mathcal{F}(I)$ são as *combinações lineares formais* de elementos de I sobre $\boldsymbol{C}$.

A *inclusão* de I em $\mathcal{F}(I)$ é a função

$$\begin{aligned} \iota \colon I &\longrightarrow \mathcal{F}(I) \\ v &\longmapsto \delta_v \colon I \longrightarrow C \\ & \qquad\qquad i \longmapsto \begin{cases} 1, & i = v \\ 0, & i \neq v. \end{cases} \end{aligned}$$

Denotaremos os elementos δ_v por v quando não houver necessidade de diferenciá-los.

Note que $\mathcal{F}(I) = \bigsqcup_{i \in I} \boldsymbol{C}$ e, portanto,

$$\boldsymbol{\mathcal{F}(I)} := (\mathcal{F}(I)), +, \cdot),$$

em que $+$ e $\cdot$ são a soma e o produto escalar pontuais induzidos por $\boldsymbol{W}$, é um espaço linear sobre $\boldsymbol{C}$ com base $\{\delta_v \mid v \in I\}$. Por isso, definido $c_i := v(i) \in C$, uma função $v : I \longrightarrow C$ de suporte finito é uma soma

$$v = \mathop{\boldsymbol{+}}_{i \in I} c_i \delta_i = \mathop{\boldsymbol{+}}_{i \in I} c_i v_i,$$

que é uma soma finita porque $\operatorname{supp}(v)$ é finito, ou seja, somente uma quantidade finita dos c_i é não nulo.

Proposição 5.42 (Propriedade Caracterítica dos Espaços Lineares Livres)**.** *Sejam I um conjunto, $\boldsymbol{C}$ um corpo e $\boldsymbol{V}$ um espaço linear sobre $\boldsymbol{C}$. Para toda função $f : I \longrightarrow V$, existe uma única função linear $\bar{f} : \mathcal{F}(I) \longrightarrow V$ tal que $\bar{f} \circ \iota = f$ (o diagrama comuta).*

$$\begin{tikzcd}
\boldsymbol{\mathcal{F}(I)} \arrow[dr, dashed, "\bar{f}"] & \\
I \arrow[u, "\iota"] \arrow[r, "f"'] & \boldsymbol{V}
\end{tikzcd}$$

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

$$\bar{f}\left(\mathop{+}_{v_i\in I} c_i v_i\right) := \mathop{+}_{v_i\in I} c_i f(v_i)$$

A função é única pois está definida da base δ_v. ■

Definição 5.25. Sejam $\boldsymbol{C}$ um corpo e $V_0, \ldots, V_{n-1}$ conjuntos. Consideremos o conjunto $\mathcal{R}$ gerado por vetores de $\mathcal{F}(V_0 \times \cdots \times V_{n-1})$ da forma

$$(v_0, \ldots, v_i + v_i', \ldots, v_{n-1}) - (v_0, \ldots, v_i, \ldots, v_{n-1}) - (v_0, \ldots, v_i', \ldots, v_{n-1}),$$

$$(v_0, \ldots, cv_i, \ldots, v_{n-1}) - c(v_0, \ldots, v_i, \ldots, v_{n-1}),$$

em que $v_i, v_i' \in V_i$ para todo $i \in [n]$ e $c \in C$. O *produto tensorial* de $V_0, \ldots, V_{n-1}$ é o espaço linear

$$\boldsymbol{V_0} \otimes \cdots \otimes \boldsymbol{V_{n-1}} := \mathcal{F}(\boldsymbol{V_0} \times \cdots \times \boldsymbol{V_{n-1}}) \big/ \boldsymbol{\mathcal{R}}$$

A classe de equivalência de $(v_0, \ldots, v_{n-1}) \in V_0 \times \cdots \times V_{n-1}$ em $V_0 \otimes \cdots \otimes V_{n-1}$ é denotada $v_0 \otimes \cdots \otimes v_{n-1}$ e o *mapa tensorial canônico* é a função $\otimes := \pi \circ \iota \colon V_0 \times \cdots \times V_{n-1} \longrightarrow V_0 \otimes \cdots \otimes V_{n-1}$, em que $\pi \colon \mathcal{F}(V_0 \times \cdots \times V_{n-1}) \longrightarrow \mathcal{R}$ é a projeção do quociente de espaços lineares.

Proposição 5.43 (Propriedade Característica de Produto Tensorial)**.** *Sejam* $\boldsymbol{V}_0$, $\ldots$, $\boldsymbol{V}_{n-1}$, $\boldsymbol{W}$ *espaços lineares sobre um corpo* $\boldsymbol{C}$.

1. *O mapa tensorial canônico*

$$\otimes \colon \boldsymbol{V_0} \times \cdots \times \boldsymbol{V_{n-1}} \longrightarrow \boldsymbol{V_0} \otimes \cdots \otimes \boldsymbol{V_{n-1}}$$

é uma função multilinear.

2. *Para toda função multilinear* $L\colon \boldsymbol{V_0} \times \cdots \times \boldsymbol{V_{n-1}} \longrightarrow \boldsymbol{W}$*, existe única função linear* $\bar{L}\colon \boldsymbol{V_0} \otimes \cdots \otimes \boldsymbol{V_{n-1}} \longrightarrow \boldsymbol{W}$ *tal que* $\bar{L} \circ \otimes = L$ *(o diagrama comuta).*

$$\begin{tikzcd}
\boldsymbol{V_0} \otimes \cdots \otimes \boldsymbol{V_{n-1}} \arrow[dr, dashed, "\bar{L}"] & \\
\boldsymbol{V_0} \times \cdots \times \boldsymbol{V_{n-1}} \arrow[u, "\otimes"] \arrow[r, "L"'] & \boldsymbol{W}
\end{tikzcd}$$

Demonstração. 1. Vale por definição.

2. Pela propriedade característica de espaços lineares livres, existe única função linear $\tilde{L} : \mathcal{F}(V_0 \times \cdots \times V_{n-1}) \longrightarrow W$ 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 $c \in C$,

$$\begin{aligned}
\tilde{L}(v_0, \ldots, v_i + v_i', \ldots, v_{n-1}) &= L(v_0, \ldots, v_i + v_i', \ldots, v_{n-1}) \\
&= L(v_0, \ldots, v_i, \ldots, v_{n-1}) + L(v_0, \ldots, v_i', \ldots, v_{n-1}) \\
&= \tilde{L}(v_0, \ldots, v_i, \ldots, v_{n-1}) + \tilde{L}(v_0, \ldots, v_i', \ldots, v_{n-1}) \\
&= \tilde{L}((v_0, \ldots, v_i, \ldots, v_{n-1}) + (v_0, \ldots, v_i', \ldots, v_{n-1}))
\end{aligned}$$

e

$$\begin{aligned}
\tilde{L}(v_0, \ldots, cv_i, \ldots, v_{n-1}) &= L(v_0, \ldots, cv_i, \ldots, v_{n-1}) \\
&= cL(v_0, \ldots, v_i, \ldots, v_{n-1})) \\
&= c\tilde{L}(v_0, \ldots, v_i, \ldots, v_{n-1}) \\
&= \tilde{L}(c(v_0, \ldots, v_i, \ldots, v_{n-1})).
\end{aligned}$$

Isso implica que existe função linear $\bar{L} : V_0 \otimes \cdots \otimes V_{n-1} \longrightarrow W$ 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:

$$\mathcal{L}(\boldsymbol{V_0}, \ldots, \boldsymbol{V_{n-1}}; \boldsymbol{W}) \simeq \mathcal{L}(\boldsymbol{V_0} \otimes \cdots \otimes \boldsymbol{V_{n-1}}; \boldsymbol{W}).$$

5.11.1 Tensores

Definição 5.26. Seja $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$. A *k-potência tensorial* de $\boldsymbol{V}$ é o espaço

$$V^{\otimes k} := \bigotimes_{i\in[k]} V = \underbrace{V \otimes \cdots \otimes V}_{k}.$$

Um k-vetor de $\boldsymbol{V}$ é um elemento de $V^{\otimes k}$ e um k-covetor de $\boldsymbol{V}$ é um elemento de $(V^*)^{\otimes k}$.

A *(p,q)-potência tensorial* de $\boldsymbol{V}$ é o espaço

$$V^{\otimes(p,q)} := V^{\otimes p} \otimes (V^*)^{\otimes q}.$$

Um (p,q)-tensor de $\boldsymbol{V}$ é um elemento de $V^{\otimes(p,q)}$. A *álgebra tensorial* de $\boldsymbol{V}$ 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 6

Álgebras sobre Corpos

6.1 Álgebra e Ação Adjunta

Definição 6.1. Seja $\boldsymbol{C}$ um corpo. Uma *álgebra* sobre $\boldsymbol{C}$ é um par $(\boldsymbol{A}, \cdot)$ em que $\boldsymbol{A}$ é um espaço vetorial sobre $\boldsymbol{C}$ e $\cdot\colon A \times A \longrightarrow A$ 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 6.2. Sejam $(\boldsymbol{A}, \cdot)$ uma álgebra sobre um corpo $\boldsymbol{C}$ e $a \in A$. A *ação adjunta* em $\boldsymbol{A}$ baseada em a é a função linear

$$\begin{aligned} \mathrm{ad}_a\colon A &\longrightarrow A \\ a' &\longmapsto a \cdot a'. \end{aligned}$$

Proposição 6.1. *Seja $(\boldsymbol{A}, \cdot)$ uma álgebra sobre um corpo $\boldsymbol{C}$. Então $(\mathcal{L}(A, A), \circ)$ é uma álgebra associativa sobre $\boldsymbol{C}$.*

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. ■

Proposição 6.2. *Sejam $(\boldsymbol{A}, \cdot)$ uma álgebra sobre um corpo $\boldsymbol{C}$ e I um conjunto. Então $(A^I, \cdot)$, em que $\cdot\colon A^I \times A^I \longrightarrow A^I$ é o produto entrada a entrada, é uma álgebra sobre $\boldsymbol{C}$. 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, $(1)_{in\in I}$ é identidade do produto de A^I.*

Demonstração. Sabemos que A^I é um espaço linear sobre $\boldsymbol{C}$. 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. ■

Proposição 6.3. *Seja $(\boldsymbol{A}, \cdot)$ uma álgebra sobre um corpo $\boldsymbol{C}$. A álgebra $\boldsymbol{A}$ é associativa se, e somente se, para todos $a, a' \in A$,*

$$\mathrm{ad}_{a\cdot a'} = \mathrm{ad}_a \circ \mathrm{ad}_{a'}\,.$$

6.2 Derivação

Definição 6.3. Seja $(\boldsymbol{A}, \cdot)$ uma álgebra sobre um corpo $\boldsymbol{C}$. Uma *derivação* em $\boldsymbol{A}$ é uma função linear $D\colon A \longrightarrow A$ 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 $\mathrm{Der}(A)$.

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 6.4. *Sejam $(\boldsymbol{A}, \cdot)$ uma álgebra sobre um corpo $\boldsymbol{C}$ e $D\colon A \longrightarrow A$ uma derivação em $\boldsymbol{A}$.*

1. *Para todos $a_0, \ldots, a_{n-1} \in A$,*

$$D(a_0 \cdots a_{n-1}) = \mathop{\bigplus}_{i \in [n]} a_0 \cdots D(a_i) \cdots a_{n-1};$$

2. *Se $\cdot$ é comutativo, então, para todos $a \in A$ e $n \in \mathbb{N}^*$,*

$$D(a^n) = na^{n-1}D(a);$$

3. *Se existe identidade $1 \in A$ do produto, então*

$$D(1) = 0.$$

4. *(Regra do produto de ordem superiror) Para todos $a, a' \in A$ e $n \in \mathbb{N}$,*

$$D^n(aa') = \mathop{\bigplus}_{i \in [n+1]} \binom{n}{i} D^{n-i}(a) D^i(a').$$

Definição 6.4. Seja $(\boldsymbol{A}, \cdot)$ uma álgebra sobre um corpo $\boldsymbol{C}$. O *colchete comutador* de $(\boldsymbol{A}, \cdot)$ é a função

$$\begin{aligned} [\cdot, \cdot]\colon A \times A &\longrightarrow A \\ (a, a') &\longmapsto a \cdot a' - a' \cdot a. \end{aligned}$$

Proposição 6.5. *Seja $(\boldsymbol{A}, \cdot)$ uma álgebra sobre um corpo $\boldsymbol{C}$. Então*

1. *$(A, [\cdot, \cdot])$ é uma álgebra antissimétrica sobre $\boldsymbol{C}$;*

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 $a, a' \in A$,

$$aa' = aa' + 0 = aa' + [a', a] = aa' + a'a - aa' = a'a.$$

■

6.3 Álgebra de Derivação Adjunta

Proposição 6.6. *Sejam* $(\boldsymbol{A}, \cdot)$ *uma álgebra sobre um corpo* $\boldsymbol{C}$ *e* $a \in A$. *A função adjunta* ad_a *é uma derivação em* $\boldsymbol{A}$ *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 6.5. Seja $\boldsymbol{C}$ um corpo. Uma *álgebra de derivação adjunta*[1] sobre $\boldsymbol{C}$ é um par $(\boldsymbol{A}, [\cdot, \cdot])$ em que $[\cdot, \cdot] \colon A \times A \longrightarrow A$ é um produto alternado tal que, para todo $a \in A$, ad_a é uma derivação em $\boldsymbol{A}$. O produto $[\cdot, \cdot]$ é o *colchete de derivação*.

[1] Essas 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 $[\cdot,\cdot]\colon A\times A\longrightarrow A$ são equivalentes a

1. (Linearidade na 2ª 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 $\partial_a := \mathrm{ad}_a$, 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 $\mathrm{Der}(A)$ das derivações em uma álgebra associativa $(\boldsymbol{A},\cdot)$. O espaço $\mathrm{Der}(A)$ é um subespaço linear de $\mathcal{L}(A,A)$. Para mostrar isso, mostraremos que $\mathrm{Der}(A)$ é fechado pela soma e pelo produto por escalar pontuais. Soma: para todas derivações $D, D'\in\mathrm{Der}(A)$, 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 derivaãço $D\in\mathrm{Der}(A)$ 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 $\mathrm{Der}(A)$ é subespaço linear de $\mathcal{L}(A,A)$.

No entanto, $\mathrm{Der}(A)$ não é uma subálgebra de $\mathcal{L}(A, A)$ com o produto de composição de funções, pois, para todos $D, D' \in \mathrm{Der}(A)$ 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 6.7. *Seja* $(\boldsymbol{A}, \cdot)$ *uma álgebra sobre um corpo* $\boldsymbol{C}$. *Então* $(\mathrm{Der}(A), [\cdot, \cdot])$ *é uma subálgebra de* $(\mathcal{L}(A, A), [\cdot, \cdot])$.

6.4 As Álgebras Reais $\mathbb{R}$, $\mathbb{R}^2$ e $\mathbb{R}^4$

6.4.1 Complexos

O espaço linear $\mathbb{R}$ é um álgebra com o produto de corpo usual. Consideremos o espaço linear $\mathbb{R}^2$ e o produto

$$\begin{aligned}\times : \mathbb{R}^2 \times \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (x_0y_0 - x_1y_1, x_0y_1 + x_1y_0)\end{aligned}$$

Primeiro notemos que o produto é comutativo, pois para todos $x, y \in \mathbb{R}^2$,

$$x \times y = (x_0y_0 - x_1y_1, x_0y_1 + x_1y_0) = (y_0x_0 - y_1x_1, y_0x_1 + y_1x_0) = y \times x.$$

Assim, para mostrar que $\times$ é bilinear, basta mostrar que é linear na primeira entrada. Para todos $x, x', y \in \mathbb{R}^2$ e todo $c \in \mathbb{R}$,

$$\begin{aligned}(cx + x') \times y &= ((cx_0 + x'_0)y_0 - (cx_1 + x'_1)y_1, (cx_0 + x'_0)y_1 + (cx_1 + x'_1)y_0) \\ &= (cx_0y_0 + x'_0y_0 - cx_1y_1 - x'_1y_1, cx_0y_1 + x'_0y_1 + cx_1y_0 + x'_1y_0) \\ &= c(x_0y_0 - x_1y_1, x_0y_1 + x_1y_0) + (x'_0y_0 - x'_1y_1, x'_0y_1x'_1y_0) \\ &= c(x \times y) + x' \times y.\end{aligned}$$

Ainda, $\times$ é associativo, pois para todos $x, y, z \in \mathbb{R}^2$,

$$\begin{aligned}(x \times y) \times z &= (x_0y_0 - x_1y_1, x_0y_1 + x_1y_0) \times z \\ &= ((x_0y_0 - x_1y_1)z_0 - (x_0y_1 + x_1y_0)z_1, (x_0y_0 - x_1y_1)z_1 + (x_0y_1 + x_1y_0)z_0) \\ &= (x_0(y_0z_0 - y_1z_1) - x_1(y_0z_1 + y_1z_0), x_0(y_0z_1 + y_1z_0) + x_1(y_0z_0 - y_1z_1)) \\ &= x \times (y_0z_0 - y_1z_1, y_0z_1 + y_1z_0) \\ &= x \times (y \times z).\end{aligned}$$

Definindo $\mathbf{1} := (1, 0)$, notemos que $\mathbf{1}$ é uma unidade de $\times$, pois para todo $x \in \mathbb{R}^2$,

$$\mathbf{1} \times x = (1x_0 - 0x_1, 1x_1 + 0x_0) = (x_0, x_1) = x.$$

Definindo $\mathbf{i} := (0, 1)$, notemos que

$$\mathbf{i} \times \mathbf{i} = (00 - 11, 01 + 10) = (-1, 0) = -\mathbf{1}.$$

Todo $x \in \mathbb{R}^2$ pode ser escrito como $x_0\mathbf{1} + x_1\mathbf{i}$, de modo que o produto $\times$ nessa notação é o produto dos números usual dos números complexos

$$x \times y = (x_0\mathbf{1} + x_1\mathbf{i}) \times (y_0\mathbf{1} + y_1\mathbf{i}) = (x_0y_0 - x_1y_1)\mathbf{1} + (x_0y_1 + x_1y_0)\mathbf{i}.$$

Para simplificar a notação, a partir de agora passaremos a escrever 1 e i para $\mathbf{1}$ e $\mathbf{i}$ e escreveremos todos $x \in \mathbb{R}^2$ na notação de números complexos.

O produto $\times$ pode também ser visto como uma ação de $\mathbb{R}^2$ aditivo sobre $\mathbb{R}^2$ aditivo. Cada $x \in \mathbb{R}^2$ pode ser identificado com uma transformação linear $x\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$. Os elementos $x \in \mathbb{S}^1 \subseteq \mathbb{R}^2$ são as rotações: se $x \in \mathbb{S}^1$, então existe $\alpha \in [0, \tau[$ tal que

$$x = (\cos(\alpha), \operatorname{sen}(\alpha)) = \cos(\alpha) + \mathrm{i}\operatorname{sen}(\alpha).$$

Isso ocorre porque, se $x \in \mathbb{S}^1$, então $\|x\| = 1$, logo $({x_0}^2 + {x_1}^2)^{\frac{1}{2}} = 1$, portanto ${x_0}^2 + {x_1}^2 = 1$. Então $|x_0| \leq 1$, ou seja, $-1 \leq x_0 \leq 1$. Definido $\alpha' := \cos^{-1}(x_0) \in \left[0, \frac{\tau}{2}\right]$, temos que ${x_1}^2 = 1 - \cos(\alpha)^2$, logo $|x_1| = (1 - \cos(\alpha)^2)^{\frac{1}{2}}$, então $x_1 = \pm\operatorname{sen}(\alpha)$. Tomamos $\alpha := \alpha'$ se $x_1 > 0$ e $\alpha := \tau - \alpha'$ se $x_1 < 0$. No caso $x_1 = 0$, tomamos $\alpha = 0$ se $x_0 = 1$ e $\alpha = \frac{\tau}{2}$ se $x_0 = -1$.

Sendo assim, para todo $\cos(\alpha) + \mathrm{i}\operatorname{sen}(\alpha) \in \mathbb{S}^1$, e todo $x \in \mathbb{R}^2$,

$$(\cos(\alpha) + \mathrm{i}\operatorname{sen}(\alpha)) \times x = (\cos(\alpha)x_0 - \operatorname{sen}(\alpha)x_1) + \mathrm{i}(\cos(\alpha)x_1 + \operatorname{sen}(\alpha)x_0).$$

Definimos $|x| := ({x_0}^2 + {x_1}^2)^{\frac{1}{2}}$ e $\angle(x) := \alpha$. Os elementos $x \in \mathbb{R} \subseteq \mathbb{R}^2$ são as expansões e contrações. Os elementos de $\mathbb{R}^2$ podem ser decompostos como

$$x = |x|\,(\cos(\angle(x)) + \mathrm{i}\operatorname{sen}(\angle(x))).$$

6.4.2 Quatérnios

O Produto Quaterniônico

Consideremos o espaço linear $\mathbb{R}^4$. Definamos $\mathbf{1} := (1,0,0,0)$, $\mathbf{i} := (0,1,0,0)$, $\mathbf{j} := (0,0,1,0)$ e $\mathbf{k} := (0,0,0,1)$. Consideremos o produto

$$\begin{aligned} \cdot : \mathbb{R}^4 \times \mathbb{R}^4 &\longrightarrow \mathbb{R}^4 \\ (x,y) &\longmapsto \quad (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3)\mathbf{1} \\ &\qquad +(x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)\mathbf{i} \\ &\qquad +(x_0y_2 - x_1y_3 + x_2y_0 + x_3y_1)\mathbf{j} \\ &\qquad +(x_0y_3 + x_1y_2 - x_2y_1 + x_3y_0)\mathbf{k}. \end{aligned}$$

Pode-se mostrar (as contas são trabalhosas, embora simples) que $\cdot$ é um produto bilinear associativo, mas não comutativo, preservado pela norma, que $\mathbf{1}$ é identidade de $\cdot$ e que

$$\mathbf{ijk} = \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}.$$

Dessas relações, deduzem-se

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \qquad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \qquad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

De fato, em vez da expressão explícita para $\cdot$ em termos das entradas de x e y, poderíamos somente definir o produto entre os elementos de uma base, no caso $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, e o produto se estenderia linearmente. Essa definição seria dada como nas relações acima.

Com essas relações e representando os elementos $x \in \mathbb{R}^4$ como

$$x = x_0\mathbf{1} + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k},$$

pode-se calcular o produto $\cdot$ em $\mathbb{R}^4$ facilmente. Esse produto é o produto usual dos números quatérnios.

Vamos denotar a álgebra de $\mathbb{R}^4$ com esse produto por $\mathbb{H}$.

Definição 6.6. Seja $x \in \mathbb{H}$. A *componente escalar* de x é o número real

$$\dot{x} := x_0 \in \mathbb{R}$$

e a *componente vetorial* de x é o vetor real

$$\vec{x} := (x_1, x_2, x_3) \in \mathbb{R}^3.$$

Denota-se

$$x = \dot{x} + \vec{x},$$

em que $\dot{x}$ é entendido como $x_0\mathbf{1}$ e $\vec{x}$ é entendido como $x_1\mathbf{i}+x_2\mathbf{j}+x_3\mathbf{k}$. Os subespaços vetorias de escalares e vetores são denotados, respectivamente, $\dot{\mathbb{H}}$ e $\vec{\mathbb{H}}$, e temos portanto

$$\mathbb{H} = \dot{\mathbb{H}} \oplus \vec{\mathbb{H}} \simeq \mathbb{R} \oplus \mathbb{R}^3.$$

O *conjugado* de x é

$$\overline{x} := \dot{x} - \vec{x}.$$

Um *versor* é um quatérnio $u \in \mathbb{H}$ tal que $\dot{u} = 0$ e $\|\vec{u}\| = 1$.

Os Produtos Escalar e Vetorial

Definição 6.7. O *produto escalar* em $\vec{\mathbb{H}}$ é a função

$$\begin{aligned} \cdot\colon \vec{\mathbb{H}} \times \vec{\mathbb{H}} &\longrightarrow \mathbb{R} \\ (\vec{x}, \vec{y}) &\longmapsto \vec{x} \cdot \vec{y} := x_1y_1 + x_2y_2 + x_3y_3. \end{aligned}$$

O *produto vetorial* em $\vec{\mathbb{H}}$ é a função

$$\begin{aligned} \times\colon \vec{\mathbb{H}} \times \vec{\mathbb{H}} &\longrightarrow \vec{\mathbb{H}} \\ (\vec{x}, \vec{y}) &\longmapsto \vec{x} \times \vec{y} := (x_2y_3 - x_3y_2)\mathbf{i} \\ &\qquad + (-x_1y_3 + x_3y_1)\mathbf{j} \\ &\qquad + (x_1y_2 - x_2y_1)\mathbf{k} \end{aligned}$$

Esses são o produto interno e o produto vetorial usuais em $\mathbb{R}^3$.

► **Exercício 6.1.** 1. O produto escalar $\cdot\colon \vec{\mathbb{H}} \times \vec{\mathbb{H}} \longrightarrow \mathbb{R}$ é um produto interno no subespaço vetorial $\vec{\mathbb{H}}$;

2. O produto vetorial $\times\colon \vec{\mathbb{H}} \times \vec{\mathbb{H}} \longrightarrow \vec{\mathbb{H}}$ é uma função bilinear alternada tal que, para todos $\vec{x}, \vec{y} \in \vec{\mathbb{H}}$,

   (a) $(\vec{x} \times \vec{y}) \cdot \vec{x} = (\vec{x} \times \vec{y}) \cdot \vec{x} = 0$;

   (b) $(\vec{x} \times \vec{y}) \cdot (\vec{x} \times \vec{y}) = \begin{vmatrix} \vec{x} \cdot \vec{x} & \vec{x} \cdot \vec{y} \\ \vec{y} \cdot \vec{x} & \vec{y} \cdot \vec{y} \end{vmatrix}$.

3. A função

$$\begin{aligned} \cdot \circ \times\colon \vec{\mathbb{H}} \times \vec{\mathbb{H}} \times \vec{\mathbb{H}} &\longrightarrow \vec{\mathbb{H}} \\ (\vec{x}, \vec{y}, \vec{z}) &\longmapsto (\vec{x} \times \vec{y}) \cdot \vec{z} \end{aligned}$$

   é uma função trilinear alternada.

Proposição 6.8. *1. Para todos $\vec{x}, \vec{y} \in \vec{\mathbb{H}}$ ($\dot{x} = \dot{y} = 0$),*

$$\vec{x}\vec{y} = -\vec{x} \cdot \vec{y} + \vec{x} \times \vec{y};$$

2. Para todos $x, y \in \mathbb{H}$,

$$xy = \dot{x}\dot{y} - \vec{x} \cdot \vec{y} + \dot{x}\vec{y} + \dot{y}\vec{x} + \vec{x} \times \vec{y}$$

3. Para todos $x, y \in \mathbb{H}$, $xy = yx$ se, e somente se, $\vec{x} \parallel \vec{y}$ (ou seja, $\vec{x} \times \vec{y} = 0$);

4. Para todo $x \in \mathbb{H} \setminus \{0\}$,

$$x^{-1} = \frac{\overline{x}}{\|x\|^2};$$

5. Um quatérnio $u \in \mathbb{H}$ é um versor se, e somente se, $u^2 = -1$;

6. Para todo $x \in \mathbb{H} \setminus \{0\}$, existem único versor $u \in \mathbb{H}$ e único ângulo $\alpha \in [0, \tau[$ tais que

$$x = \|x\| \left(\cos(\alpha) + \operatorname{sen}(\alpha) u\right).$$

Demonstração. 1. Como $x_0 = y_0 = 0$,

$$\begin{aligned} xy = &- (x_1y_1 + x_2y_2 + x_3y_3) \\ &+ (x_2y_3 - x_3y_2)\mathbf{i} \\ &+ (-x_1y_3 + x_3y_1)\mathbf{j} \\ &+ (x_1y_2 - x_2y_1)\mathbf{k} \\ = &- \vec{x} \cdot \vec{y} + \vec{x} \times \vec{y}. \end{aligned}$$

2. Segue da bilinearidade do produto e de $\vec{x}$ e $\vec{y}$ serem puramente vetoriais que

$$\begin{aligned} xy &= (\dot{x} + \vec{x})(\dot{y} + \vec{y}) \\ &= \dot{x}\dot{y} + \dot{x}\vec{y} + \dot{y}\vec{x} + \vec{x}\vec{y} \\ &= \dot{x}\dot{y} + \dot{x}\vec{y} + \dot{y}\vec{x} + (-\langle \vec{x}, \vec{y} \rangle + \vec{x} \times \vec{y}) \\ &= \left(\dot{x}\dot{y} - \vec{x} \cdot \vec{y}\right) + \left(\dot{x}\vec{y} + \dot{y}\vec{x} + \vec{x} \times \vec{y}\right). \end{aligned}$$

3. Para todos $x, y \in \mathbb{H}$,

$$\begin{aligned} xy - yx &= \dot{x}\dot{y} - \vec{x} \cdot \vec{y} + \dot{x}\vec{y} + \dot{y}\vec{x} + \vec{x} \times \vec{y} \\ &\quad - \dot{y}\dot{x} + \vec{y} \cdot \vec{x} - \dot{y}\vec{x} - \dot{x}\vec{y} - \vec{y} \times \vec{x} \\ &= \vec{x} \times \vec{y} - \vec{y} \times \vec{x}. \end{aligned}$$

Isso implica que $xy - yx = 0$ se, e somente se, $\vec{x} \times \vec{y} - \vec{y} \times \vec{x} = 0$, o que ocorre se, e somente se, $\vec{x} \times \vec{y} = 0$, que por sua vez é equivalente a $\vec{x} \parallel \vec{y}$.

4. Para todo $x \in \mathbb{H} \setminus \{0\}$,

$$\begin{aligned} xx^{-1} &= (\dot{x} + \vec{x}) \|x\|^{-2} (\dot{x} - \vec{x}) \\ &= \|x\|^{-2} (\dot{x}^2 - \vec{x} \cdot (-\vec{x}) + \dot{x}(-\vec{x}) + \dot{x}\vec{x} + \vec{x} \times (-\vec{x})) \\ &= \|x\|^{-2} (\dot{x}^2 + \vec{x} \cdot \vec{x} - \dot{x}\vec{x} + \dot{x}\vec{x} - \vec{x} \times \vec{x}) \\ &= \|x\|^{-2} \|x\|^2 \\ &= 1 \end{aligned}$$

e, como $\vec{x} \times (-\vec{x}) = 0$, $x^{-1}x = xx^{-1} = 1$.

5. Para todo $u \in \mathbb{H}$,

$$\begin{aligned} u^2 &= \dot{u}\dot{u} - \vec{u} \cdot \vec{u} + \dot{u}\vec{u} + \dot{u}\vec{u} + \vec{u} \times \vec{u} \\ &= \dot{u}^2 - \|\vec{u}\|^2 + 2\dot{u}\vec{u}. \end{aligned}$$

Segue que $\dot{u} = 0$ e $\|\vec{u}\| = 1$ se, e somente se, $u^2 = -1$.

6. Exercício.

■

Sejam $x, y \in \mathbb{H} \setminus \{0\}$ tais que $xy \in \dot{\mathbb{H}}$. Então

$$0 = \dot{x}\vec{y} + \dot{y}\vec{x} + \vec{x} \times \vec{y}.$$

Isso implica que $(\vec{x}, \vec{y}, \vec{x} \times \vec{y})$ não é uma base de $\vec{\mathbb{H}}$, pois caso contrário

$$\dot{x}\vec{y} + \dot{y}\vec{x} + \vec{x} \times \vec{y} \neq 0,$$

já que $(\dot{x}, \dot{y}, 1) \neq (0, 0, 0)$. Mas a tripla não é base se, e somente se, $\vec{x} = 0$ ou $\vec{y} = 0$ ou $\vec{x} \times \vec{y} = 0$, porque sempre vale $\vec{x} \cdot (\vec{x} \times \vec{y}) = \vec{y} \cdot (\vec{x} \times \vec{y}) = 0$. No primeiro caso, segue que $\vec{x} \times \vec{y} = 0$,

$$0 = \dot{x}\vec{y},$$

e, no segundo caso, analogamente segue que

$$0 = \dot{y}\vec{x}.$$

No terceiro caso, segue que

$$\dot{y}\vec{x} = -\dot{x}\vec{y},$$

e que $\vec{x} \parallel \vec{y}$.

Nos primeiros dois casos, $\langle \vec{x}, \vec{y} \rangle = 0$, logo

$$(\dot{xy}) = \dot{x}\dot{y} - \langle \vec{x}, \vec{y} \rangle = \dot{x}\dot{y}.$$

No terceiro caso, $\langle \vec{x}, \vec{y} \rangle = \|\vec{x}\| \|\vec{y}\|$, logo

$$(\dot{xy}) = \dot{x}\dot{y} - \langle \vec{x}, \vec{y} \rangle = \dot{x}\dot{y} - \|\vec{x}\| \|\vec{y}\|.$$

Em ambos os casos,

$$(\dot{xy}) = \dot{x}\dot{y} - \|\vec{x}\| \|\vec{y}\|.$$

Rotações em $\mathbb{R}^3$ por Quatérnios

A rotação de $v \in \mathbb{R}^3$ por um ângulo θ em torno de um vetor unitário $u \in \mathbb{R}^3$ é dada por

$$R_u^\theta(v) = \mathrm{p}_{\|u}(v) + \cos(\theta)\mathrm{p}_{\perp u}(v) + \mathrm{sen}(\theta)u \times v.$$

Note que genericamente $(\mathrm{p}_{\|u}(v), \mathrm{p}_{\perp u}(v), u \times v)$ é uma base de $\mathbb{R}^3$. Isso significa que

$$R_u^\theta = \mathrm{p}_{\|u} + \cos(\theta)\mathrm{p}_{\perp u} + \mathrm{sen}(\theta)u\times.$$

As funções $\mathrm{p}_{\|u}$, $\mathrm{p}_{\perp u}$ e $u\times$ são funções lineares e, na base canônica de $\mathbb{R}^3$, são dadas pelas matrizes

$$[\mathrm{p}_{\|u}] = \begin{bmatrix} {u_1}^2 & u_1u_2 & u_1u_3 \\ u_1u_2 & {u_2}^2 & u_2u_3 \\ u_1u_3 & u_2u_3 & {u_3}^2 \end{bmatrix}$$

$$[\mathrm{p}_{\perp u}] = \begin{bmatrix} 1-{u_1}^2 & -u_1u_2 & -u_1u_3 \\ -u_1u_2 & 1-{u_2}^2 & -u_2u_3 \\ -u_1u_3 & -u_2u_3 & 1-{u_3}^2 \end{bmatrix}$$

e

$$[u\times] = \begin{bmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{bmatrix}$$

Os quatérnios unitários são os elementos de $\mathbb{S}^3 \subseteq \mathbb{R}^4$ e $SO(3)$ é o grupo de rotações de $\mathbb{R}^3$. Definimos a função

$$\begin{aligned} R\colon \mathbb{S}^3 &\longrightarrow SO(3) \\ q &\longmapsto R_q\colon \mathbb{R}^3 \longrightarrow \mathbb{R}^3 \\ &\qquad\qquad v \longmapsto qvq^{-1}. \end{aligned}$$

Mostremos que essa função está bem definida. Precisamos mostrar que $qvq^{-1} \in \mathbb{R}^3$ e que R_q é uma rotação. Primeiro, seja $q \in \mathbb{S}^3$. Então, como $\|q\| = 1$,

$$q^{-1} = \dot{q} - \vec{q}.$$

Como $v \in \mathbb{R}^3$ é um quatérnio vetorial puro, temos

$$\dot{(vq^{-1})} = \dot{v}\dot{q} - \langle \vec{v}, -\vec{q} \rangle = \langle \vec{v}, \vec{q} \rangle\,,$$

$$\vec{(vq^{-1})} = \dot{v}(-\vec{q}) + \dot{q}\vec{v} + \vec{v} \times (-\vec{q}) = \dot{q}\vec{v} - \vec{v} \times \vec{q},$$

e, portanto,

$$\begin{aligned}
(qv\dot{q^{-1}}) &= \dot{q}(v\dot{q^{-1}}) - \left\langle \vec{q}, (v\vec{q^{-1}}) \right\rangle \\
&= \dot{q}\,\langle \vec{v}, \vec{q}\rangle - \langle \vec{q}, \dot{q}\vec{v} - \vec{v}\times\vec{q}\rangle \\
&= \dot{q}\,\langle \vec{v}, \vec{q}\rangle - \dot{q}\,\langle \vec{q}, \vec{v}\rangle + \langle \vec{q}, \vec{v}\times\vec{q}\rangle \\
&= \dot{q}\,\langle \vec{v}, \vec{q}\rangle - \dot{q}\,\langle \vec{v}, \vec{q}\rangle \\
&= 0,
\end{aligned}$$

o que mostra que $qvq^{-1} \in \mathbb{R}^3$, ou seja, é um quatérnio vetorial puro.

Para cada $q \in \mathbb{S}^3$, essa função é linear, pois, para todos $c \in \mathbb{R}$ e $v, v' \in \mathbb{R}^3$, segue da bilinearidade e da associatividade do produto e da comutatividade com escalares que

$$\begin{aligned}
R_q(cv + v') &= q(cv + v')q^{-1} \\
&= q(cvq^{-1} + v'q^{-1}) \\
&= qcvq^{-1} + qv'q^{-1} \\
&= cqvq^{-1} + qv'q^{-1} \\
&= cR_q(v) + R_q(v').
\end{aligned}$$

A função R_q é uma isometria, pois

$$\|R_q(v)\| = \left\|qvq^{-1}\right\| = \|q\|\,\|v\|\,\left\|q^{-1}\right\| = \|q\|\,\|q\|^{-1}\,\|v\| = \|v\|\,.$$

Por fim, notemos que

$$\begin{aligned}
qvq^{-1} &= (q\vec{vq^{-1}}) \\
&= \dot{q}(v\vec{q^{-1}}) + (v\dot{q^{-1}})\vec{q} + \vec{q}\times(v\vec{q^{-1}}) \\
&= \dot{q}(\dot{q}\vec{v} - \vec{v}\times\vec{q}) + \langle \vec{v}, \vec{q}\rangle\,\vec{q} + \vec{q}\times(\dot{q}\vec{v} - \vec{v}\times\vec{q}) \\
&= \dot{q}\dot{q}\vec{v} - \dot{q}\vec{v}\times\vec{q} + \langle \vec{v}, \vec{q}\rangle\,\vec{q} + \dot{q}\vec{q}\times\vec{v} - \vec{q}\times(\vec{v}\times\vec{q}) \\
&= \dot{q}\dot{q}\vec{v} + 2\dot{q}\vec{q}\times\vec{v} + \langle \vec{v}, \vec{q}\rangle\,\vec{q} - \langle \vec{q}, \vec{q}\rangle\,\vec{v} + \langle \vec{q}, \vec{v}\rangle\,\vec{q} \\
&= (\dot{q}\dot{q} - \langle \vec{q}, \vec{q}\rangle)\vec{v} + 2\dot{q}\vec{q}\times\vec{v} + 2\,\langle \vec{v}, \vec{q}\rangle\,\vec{q}.
\end{aligned}$$

Como $\|q\|^2 = \dot{q}^2 + \|\vec{q}\|^2$, podemos tomar $\theta \in \mathbb{S}^1$ tal que

$$\dot{q} = \cos(\theta/2)$$

e

$$\|\vec{q}\| = \operatorname{sen}(\theta/2).$$

Definindo

$$u := \vec{q}/\operatorname{sen}(\theta/2),$$

temos $\|u\| = 1$ e

$$q = \cos(\theta/2) + \operatorname{sen}(\theta/2)u = \mathrm{e}^{(\theta/2)u}.$$

Temos assim

$$\begin{aligned}
qvq^{-1} &= (\cos(\theta/2)^2 - \operatorname{sen}(\theta/2)^2)v + 2\cos(\theta/2)\operatorname{sen}(\theta/2)u \times v + 2\operatorname{sen}(\theta/2)^2 \langle v, u\rangle u \\
&= \cos(\theta)v + \operatorname{sen}(\theta)u \times v + (1 - \cos(\theta)) \langle v, u\rangle u \\
&= \langle v, u\rangle u + \cos(\theta)(v - \langle v, u\rangle u) + \operatorname{sen}(\theta)u \times v \\
&= \mathrm{p}_{\|u}(v) + \cos(\theta)\mathrm{p}_{\perp u}(v) + \operatorname{sen}(\theta)u \times v \\
&= R_u^\theta(v).
\end{aligned}$$

Matricialmente, $[R_q]$ é dada por

$$\begin{bmatrix} {u_1}^2 & u_1u_2 & u_1u_3 \\ u_1u_2 & {u_2}^2 & u_2u_3 \\ u_1u_3 & u_2u_3 & {u_3}^2 \end{bmatrix} + \cos(\theta) \begin{bmatrix} 1-{u_1}^2 & -u_1u_2 & -u_1u_3 \\ -u_1u_2 & 1-{u_2}^2 & -u_2u_3 \\ -u_1u_3 & -u_2u_3 & 1-{u_3}^2 \end{bmatrix} + \operatorname{sen}(\theta) \begin{bmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{bmatrix}$$

ou

$$(1 - \cos(\theta)) \begin{bmatrix} {u_1}^2 & u_1u_2 & u_1u_3 \\ u_1u_2 & {u_2}^2 & u_2u_3 \\ u_1u_3 & u_2u_3 & {u_3}^2 \end{bmatrix} + \cos(\theta)\mathrm{I} + \operatorname{sen}(\theta) \begin{bmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{bmatrix}$$

Capítulo 7

Ordem em Estruturas Algébricas

7.1 Corpos Ordenados

Nesta seção, pretendemos formalizar a ideia de elementos positivos e negativos em um corpo, e para isso usaremos o conceito de ordem. Uma ordem, também chamada de ordem total, ordem linear ou cadeia, é uma relação reflexiva, antissimétrica, transitiva e total em um conjunto X. As três primeiras propriedades definem uma ordem parcial, e a quarta, também chamada de conexidade, significa existe relação entre qualquer par de elementos. De fato, as três úmtimas implicam a reflexividade, mas definimos assim para podermos dizer que uma ordem total é uma ordem parcial que satisfaz a totalidade.

Um corpo é um conjunto em que existe adição, subtração, multiplicação e divisão. Para unir os dois conceitos de modo que as estruturas de corpo e de ordem se relacionem, devemos exigir que elas satisfaçam algumas propriedades. Para isso, devemos relembrar dos conceitos de função monótona, de translação e de expansão. Uma função monótona crescente entre conjuntos ordenados é uma função f tal que, se dois elementos do domínio x, x' têm uma certa relação de ordem $x \leq x'$ (um é menor ou igual ao outro), então suas imagens têm a mesma relação de ordem, $f(x) \leq f(x')$. Isso quer dizer que a função preserva a ordem dos conjuntos. Uma função monótona decrescente inverte a relação de ordem, de modo que se dois elementos têm uma relação de ordem $x \leq x'$, suas imagens têm a relação de ordem dual, ou invertida, $f(x') \leq f(x)$. Lembremos ainda que, em uma ordem total, definimos para cada $e \in X$ os seguintes intervalos

$$
\begin{aligned}
[e, \infty[&= \{e \in X \mid e \leq x\} \\
]e, \infty[&= \{e \in X \mid e < x\} \\
]\infty, e] &= \{e \in X \mid x \leq e\} \\
]\infty, e[&= \{e \in X \mid x < e\}\,.
\end{aligned}
$$

Claramente, supomos que ∞ não é um símbolo usado para representar um elemento de X, de modo a não gerar confusão.

Para entrelaçar as estruturas de corpo e de ordem, usamos as translações e expansões em corpos e exigimos que elas sejam monótonas. Seja $\boldsymbol{C}$ um corpo e $c \in C$. A translação em C por c é a função

$$\begin{aligned} T_c \colon C &\longrightarrow C \\ c' &\longmapsto c + c' \end{aligned}$$

e a expansão de C por c é a função

$$\begin{aligned} E_c \colon C &\longrightarrow C \\ c' &\longmapsto cc'. \end{aligned}$$

Aqui assumimos que os corpos são comutativos, por isso não é necessário considerar translações e expansões à esquerda e à direita.

Pedir que as fuções sejam monónotas é bem natural para preservar a estrutura de ordem do corpo. No entanto, se escolhemos ter translação monótona, não podemos ter qualquer expansão monótona, já que se E_{-1} fosse monótona, seguiria que, para todos $c, c' \in C$,

$$c \leq c' \Rightarrow -c \leq -c'$$

e da monotonicidade da adição seguiria que

$$c' = (c' + c) + (-c) \leq (c' + c) + (-c') = c.$$

Como $c \leq c'$ e $c' \leq c$, seguiria então da antissimetria da ordem que $c = c'$. Como a ordem é total, isso implicaria ainda que todos elementos são iguais, já que quaisquer dois elementos podem ser comparados. Isso nos sugere, então, a imitar a relação de ordem nos números racionais e reais, e exigir que a expansão por elementos positivos sejam crescente e por elementos negativos seja decrescente. Claro, isso nos obriga a definir o que é ser positivo ou negativo. Positivo significa simplesmente ser maior ou igual a 0, e negativo significa ser menor ou igual a 0. A definição de 0 como positivo ou negativo é, na maioria dos casos, irrelevante, mas em geral é mais conveniente considerá-lo ambos, em vez de nenhum dos dois.

Definição 7.1. Um *corpo ordenado* é um par $(\boldsymbol{C}, \leq)$ em que $\boldsymbol{C}$ é um corpo e $\leq$ é uma ordem em C que satisfaz:

1. (Monotonicidade da translação) Para todo $c \in C$, a translação $T_c \colon C \longrightarrow C$ é uma função monótona crescente: para todos $c', c'' \in C$

$$c' \leq c'' \Rightarrow c + c' \leq c + c'';$$

2. (Monotonicidade da expansão) Para todo $c \in [0, \infty[$ ($c \in C$ tal que $c \geq 0$), a expansão $E_c \colon C \longrightarrow C$ é uma função monótona crescente: para todos $c', c'' \in C$
$$c' \leq c'' \Rightarrow cc' \leq cc''.$$

Os elementos *positivos*, *negativos*, *estritamente positivos* e *estritamente negativos* de C são os elementos $c \in C$ tais que $c \geq 0$, $c \leq 0$, $c > 0$ e $c < 0$, respectivamente. O conjuntos desses elementos são denotados, respectivamente, $C_{\geq 0} := [0, \infty[$, $C_{\leq 0} :=]\infty, 0]$, $C_{>0} :=]0, \infty[$ e $C_{<0} :=]\infty, 0[$.

Poderia-se perguntar por que devemos ter uma ordem total, por que não só uma ordem parcial. Se queremos definir o conceito de positividade e negatividade, devemos garantir que todos os elementos sejam relacioonados com o 0. Suponhamos então que temos uma ordem parcial tal que todos elementos são relacionados com 0 e mostremos que essa ordem é total. Para todos $c, c' \in C$, consideremos então $c' - c \in C$. Como todos elementos podem ser comparados com 0, segue que $c' - c \geq 0$ ou $c' - c \leq 0$. Da monotonicidade crescente da translação por c, segue que $c' \geq c$ ou $c' \leq c$, portanto a ordem é total. O conceito de monotonicidade da expansão ser crescente ou decrescente de acordo com a positividade do elemento pelo qual se multiplica exige, em si, que todos elementos sejam relacionados com 0. Nas seções seguintes veremos como o conceito de cone positivo se relaciona com o de ordem em corpos.

Proposição 7.1. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado.*

1. *Para todo $c \in C$, $c \in C_{\geq 0}$ se, e somente se, $-c \in C_{\leq 0}$;*

2. *Para todo $c \in C_{\leq 0}$, a expansão $E_c \colon C \longrightarrow C$ é uma função monótona decrescente: para todos $c', c'' \in C$*
$$c' \leq c'' \Rightarrow cc'' \leq cc'.$$

3. *Para todos $c, c' \in C$,*
   (a) *se $c, c' \in C_{\geq 0}$, então $c + c' \in C_{\geq 0}$;*
   (b) *se $c, c \in C_{\leq 0}$, então $c + c' \in C_{\leq 0}$;*

4. *Para todos $c, c' \in C$, $cc' \in C_{\geq 0}$ se, e somente se, $c, c' \in C_{\geq 0}$ ou $c, c' \in C_{\leq 0}$;*

5. *A inversa da adição $- \colon C \longrightarrow C$ é descrescente: para todos $c, c' \in C$ tais que $c \leq c'$, $-c' \leq -c$;*

6. *A inversa da multiplicação ${}^{-1} \colon C \smallsetminus \{0\} \longrightarrow C \smallsetminus \{0\}$ é descrecente: para todos $c, c' \in C \smallsetminus \{0\}$ tais que $c \leq c'$, $c'^{-1} \leq c^{-1}$;*

7. *Para todo* $c \in C$, $c^2 \geq 0$;

8. $-1 \leq 0 \leq 1$;

9. *Para todos* $c, c', d, d' \in C$ *tais que* $c \leq c'$ *e* $d \leq d'$, $c + d \leq c' + d'$;

Demonstração. 1. Seja $c \in C_{\geq 0}$. Isso significa que $c \geq 0$. Pela monotonicidade crescente da translação por $-c$, segue que

$$-c = -c + 0 \leq -c + c = 0,$$

portanto $-c \in C_{\leq 0}$. A recíproca segue direto de $c = -(-c)$.

2. Sejam $c \in C_{\leq 0}$ e $c', c'' \in C$ tais que $c' \leq c''$. Então temos que $-c \in C_{\leq 0}$, portanto

$$-cc' \leq -cc''$$

e somando $cc' + cc''$, segue que

$$cc'' = (cc' + cc'') - cc' \leq (cc' + cc'') - cc'' = cc'.$$

3.

4. Se $c, c' \in C_{\geq 0}$, então $c \geq 0$ e $c' \geq 0$, logo da monotonicidade crescente de E_c segue que $cc' \geq c0 = 0$. Se $c, c' \in C_{\leq 0}$, então $c \leq 0$ e $c' \leq 0$, logo da monotonicidade decrescente de E_c segue que $cc' \geq c0 = 0$.

   Reciprocamente, se $c \in C_{\geq 0}$ e $c' \in C_{\leq 0}$, então $c \geq 0$ e $c' \leq 0$, logo da monotonicidade crescente de E_c segue que $cc' \leq c0 = 0$. O caso em que $c \in C_{\leq 0}$ e $c' \in C_{\geq 0}$ é o mesmo, trocando c e c'.

■

Proposição 7.2 (Relação de ordem e ciclicidade)**.** *Seja* $(\boldsymbol{C}, \leq)$ *um corpo ordenado. Se* $\mathrm{car}(\boldsymbol{C}) \neq 0$, *então* $\boldsymbol{C}$ *é o corpo trivial* ($C = \{0\}$).

Demonstração. Seja $\mathrm{car}(C) = n \in \mathbb{N} \setminus \{0\}$. Consideremos $0, 1, n_C \in C$. Pela monotonicidade da adição, segue que,

$$0 \leq 1 \leq 1 + 1 \leq \ldots \leq n_C = 0,$$

o que implica, pela antissimetria da ordem, que $1 = 0$. ■

7.1.1 Imersão dos Inteiros e Racionais

Lembremos que a função

$$\begin{aligned} h\colon \mathbb{Z} &\longrightarrow C \\ n &\longmapsto \begin{cases} +_{i\in[n]} 1_C, & n > 0 \\ 0_C, & n = 0 \\ +_{i\in[-n]}(-1_C), & n < 0 \end{cases} \end{aligned}$$

é um homomorfismo de anel. Como $(\boldsymbol{C}, \leq)$ é um corpo ordenado não trivial, ele não tem torção, logo h é injetivo e sua imagem é $\mathbb{Z}_C$. A função

$$\begin{aligned} \bar{h}\colon \mathbb{Q} &\longrightarrow C \\ \frac{n}{d} &\longmapsto h(n)h(d)^{-1} \end{aligned}$$

é um homomorfismo de corpo injetivo cuja imagem é $\mathbb{Q}_C$. O homomorfismo $\bar{h}$ é o único homomorfismo injetivo que extende h, de acordo com a propriedade universal dos corpos de frações 4.3. Assim, todo corpo sem torção, em particular um corpo ordenado não trivial, tem um subcorpo isomorfo aos racionais. Note que $\bar{h}$ é crescente, pois $\mathbb{Q}_C$ tem a mesma relação de ordem que $\mathbb{Q}$.

Proposição 7.3. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado não trivial. Para todo $\frac{n}{d}, \frac{n'}{d'} \in \mathbb{Q}_C$,*

$$\frac{p}{q} \leq \frac{p'}{q'} \Leftrightarrow pq' \leq qp'$$

Demonstração. Tomemos $q, q' \geq 0$ sem perda de generalidade. Suponhamos que $\frac{p}{q} \leq \frac{p'}{q'}$. Da monotonicidade crescente de $E_{qq'}$, segue que

$$pq' = qq'\frac{p}{q} \leq qq'\frac{p'}{q'} = qp'.$$

A recírpoca é evidente. ■

7.1.2 Cones Positivos

Apresentamos brevemente uma definição alternativa de ordem em corpos.

Definição 7.2. Seja $\boldsymbol{C}$ um corpo. Um *cone pré-positivo* em C é um conjunto $P \subseteq C$ tal que

1. (Fechamento da adição) Para todos $p, p' \in P$, $p + p' \in P$;

2. (Fechamento da multiplicação) Para todos $p, p' \in P$, $pp' \in P$;
3. (Positividade do quadrado) Para todo $c \in C$, $c^2 \in P$;
4. (Não-positividade do oposto da unidade) $-1 \notin P$.

Um *cone positivo* é um cone pré-positivo $P \subseteq C$ tal que $C = P \cup -P$.

Proposição 7.4. *Sejam $\boldsymbol{C}$ um corpo e $P \subseteq C$ um cone pré-positivo.*

1. $0, 1 \in P$;
2. *Para todo $p \in P \smallsetminus \{0\}$, $p^{-1} \in P$;*
3. $P \cap -P = \{0\}$;
4. *$P \cup -P$ é um subcorpo de C.*

Demonstração. 1. Pela positividade do quadrado, segue que $0 = 0^2 \in P$ e $1 = 1^2 \in P$.

2. Exercício.
3. Seja $p \in P \cap -P$. Então $p, -p \in P$. Se $p \neq 0$, então $p^{-1} \in P$ e segue que $-1 = -pp^{-1} \in P$, o que é uma contradição. Logo $p = 0$.
4. Exercício.

■

Proposição 7.5. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. O conjunto $C_{\geq 0}$ de elementos positivos de C é um cone positivo.*

Demonstração. Segue direto das proposições anteriores. ■

Definição 7.3. Sejam $\boldsymbol{C}$ um corpo e $P \subseteq C$ um cone pré-positivo. A *ordem* induzida por P é a relação $\leq_P$ definida por: para todos $c, c' \in C$, $c \leq c'$ se, e somente se, $c' - c \geq 0$.

Proposição 7.6. *Sejam $\boldsymbol{C}$ um corpo e $P \subseteq C$ um cone pré-positivo.*

1. *A ordem $\leq_P$ induzida por P é uma ordem parcial em C;*
2. *Para todo $c \in C$, a translação $T_c \colon C \longrightarrow C$ é monótona crescente;*
3. *Para todo $c \in C$,*
   (a) *se $c \in P$, a expansão $E_c \colon C \longrightarrow C$ é monótona crescente;*

(b) se $c \in -P$, a expansão $E_c \colon C \longrightarrow C$ é monótona decrescente.

Demonstração. 1. (Reflexividade) Seja $c \in C$. Isso significa que $c - c = 0 \in P$, logo $c \leq_P c$.

(Antissimetria) Sejam $c, c' \in C$ tais que $c \leq_P c'$ e $c' \leq_P c$. Isso significa que $c' - c \in P$ e $c - c' = -(c' - c) \in P$, o que implica que $c' - c = 0$, logo $c = c'$.

(Transitividade) Sejam $c, c', c'' \in C$ tais que $c \leq_P c'$ e $c' \leq_P c''$. Isso significa que $c' - c \in P$ e $c'' - c' \in P$, logo $(c'' - c') + (c' - c) = c'' - c \in P$, portanto $c \leq_P c''$.

2. Sejam $c \in C$ e $c', c'' \in C$ tais que $c' \leq_P c''$. Isso significa que $c'' - c \in P$, portanto
$$(c + c'') - (c + c') = c'' - c' \in P,$$
o que significa que $c + c' \leq_P c + c''$. Isso mostra que T_c é monótona crescente.

3. Sejam $c \in C$ e $c', c'' \in C$ tais que $c' \leq_P c''$. Isso significa que $c'' - c' \in P$.

   (a) Se $c \in P$, segue do fechamento por multiplicação que
   $$cc'' - cc' = c(c'' - c') \in P,$$
   o que significa que $cc' \leq_P cc''$. Isso mostra que E_c é monótona crescente.

   (b) Se $c \in -P$, então $-c \in P$, e segue do fechamento por multiplicação que
   $$cc' - cc'' = -c(c'' - c') \in P,$$
   o que significa que $cc'' \leq_P cc'$. Isso mostra que E_c é monótona decrescente.

■

No entanto, para elementos $c \in C$ que não estão em $P \cup -P$, não podemos garantir a monotonicidade da expansão por ele. Note que $C \neq P \cup -P$ é equivalente a termos elementos que não são relacionados com 0.

Proposição 7.7. *Sejam $\boldsymbol{C}$ um corpo e $P \subseteq C$ um cone positivo. O par $(\boldsymbol{C}, \leq_P)$ é um corpo ordenado.*

Demonstração. Pela proposição anterior, $\leq_P$ é uma ordem parcial. Basta mostrar a totalidade. Sejam $c, c' \in C$. Como $C = P \cup -P$, então $c' - c \in P \cup -P$. Isso implica que $c' - c \in P$ ou $c' - c \in -P$, logo $c \leq_P c'$ ou $c' \leq_P c$. Assim concluímos que $\leq_P$ é uma ordem.

Pela proposição anterior, a translação é monótona. Como $C = P \cup -P$, então $c \geq_P 0$ se, e somente se, $c \in P$ e $c \leq_P 0$ se, e somente se, $c \in -P$, e segue da proposição anterior que, se $c \geq_P 0$, a expansão E_c é monótona crescente e, se $c \leq_P 0$, a expansão E_c é monótona decrescente. ■

Proposição 7.8. *Seja $\boldsymbol{C}$ um corpo. Existe uma bijeção entre as ordens em $\boldsymbol{C}$ tais que $(\boldsymbol{C}, \leq)$ é um corpo ordenado e os cones positivos de $\boldsymbol{C}$.*

Demonstração. Usando os resultados anteriores, essa demonstração fica simples. A bijeção é dada por $\leq \longmapsto C_{\geq 0}$ e sua inversa é $P \longmapsto \leq_P$. ■

7.1.3 Corpos Ordenados Completos

Definição 7.4. Um corpo ordenado *completo* é um corpo ordenado $(\boldsymbol{C}, \leq)$ tal que todo conjunto não-vazio limitado superiormente admite supremo: para todo $A \subseteq C$ não-vazio imitado superiormente, existe $s \in C$ tal que

$$s = \sup A.$$

Proposição 7.9. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado completo (não-trivial). Existe isomorfismo de corpos crescente $h\colon \mathbb{R} \longrightarrow C$.*

Demonstração. Definimos h como

$$\begin{aligned} h\colon \mathbb{R} &\longrightarrow C \\ x &\longmapsto \sup\left\{ \frac{i_C}{j_C} \;\middle|\; (i,j) \in \mathbb{Z} \times \mathbb{Z} \smallsetminus \{0\}, \frac{i}{j} \leq x \right\}. \end{aligned}$$

Definamos $L(x) := \{q \in \mathbb{Q} \mid q \leq x\}$. Mostremos que h é uma bijeção. (Injetividade) Sejam $x, x' \in \mathbb{R}$ tais que $x \neq x'$. Da totalidade da ordem, $x < x'$ ou $x' < x$, logo $\sup L(x) < \sup L(x')$ ou $\sup L(x') < \sup L(x)$. No primeiro caso, segue que $h(x) < h(x')$, e no segundo $h(x') < h(x)$, portanto $h(x) \neq h(x')$. (Sobrejetividade) Seja $c \in C$. Então $c = \sup\{q \in \mathbb{Q}_C \mid q \leq c\}$, portanto definindo $x := \sup\left\{ \frac{i_C}{j_C} \;\middle|\; (i,j) \in \mathbb{Z} \times \mathbb{Z} \smallsetminus \{0\}, \frac{i_C}{j_C} \leq c \right\}$, temos que $h(x) = y$.

Agora, mostremos que h é isomorfismo de corpos. (Homomorfismo de grupo aditivivo) Sejam $x, x' \in \mathbb{R}$. Então $x + x' = \sup L(x + x')$, logo

$$h(x + x') = h(\sup L(x + x')) = \sup h(L(x + x')) = h(x) + h(x').$$

(Homomorfismo de grupo multiplicativo) Sejam $x, x' \in \mathbb{R}$. Então $xx' = \sup L(xx')$, logo

$$h(xx') = h(\sup L(xx')) = \sup h(L(xx')) = h(x)h(x').$$

Os detalhes podem ser completados pelo leitor.

O ismorfismo h é crescente pois, se $x \leq x'$, então $L(x) \subseteq L(x')$, logo $h(L(x)) \subseteq h(L(x'))$, o que implica $h(x) \leq h(x')$. ■

Essa proposição mostra que corpos ordenados completos são, basicamente, cópias de $\mathbb{R}$. Isso nos permite usar $\mathbb{R}$ sempre que quisermos usar algum corpo que seja ordenado e completo, e tira um pouco a arbitrariedade algébrica de usar o corpo dos números reais.

7.1.4 Corpos Ordenados Infinitesimais

Definição 7.5. Um *corpo não-infinitesimal* (ou *arquimediano*) é um corpo ordenado $(\boldsymbol{C}, \leq)$ tal que $\mathbb{N}_C$ é ilimitado superiormente: para todo $c \in C$, existe $n \in \mathbb{N}_C$ tal que $c < n$.

Proposição 7.10. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. São equivalentes:*

1. *$(\boldsymbol{C}, \leq)$ é arquimediano;*
2. *Para todos $c \in C_{>0}$ e $c' \in C$, existe $n \in \mathbb{N}_C$ tal que $nc > c'$;*
3. *Para todo $c \in C_{>0}$, existe $n \in \mathbb{N}_C$ tal que $0 < \frac{1}{n} < c$;*
4. *Para todo $c \in C_{>0}$, existe $n \in \mathbb{N}_C$ tal que $0 < \frac{1}{2^n} < c$.*
5. *Para todos $c, c' \in C$ tais que $c < c'$, existe $q \in \mathbb{Q}_C$ tal que $c < q < c'$.*

7.1.5 Valor Absoluto e Distância

Definição 7.6. Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. O *valor absoluto* de C é a função

$$\begin{aligned} |\cdot| \colon C &\longrightarrow C_{\geq 0} \\ c &\longmapsto \begin{cases} c, & c \in C_{\geq 0} \\ -c, & c \in C_{\leq 0}. \end{cases} \end{aligned}$$

Proposição 7.11. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. O valor absoluto satisfaz*

1. *(Separação) Para todo $c \in C$, $|c| = 0$ se, e somente se, $c = 0$;*
2. *(Multiplicatividade) Para todos $c, c' \in C$, $|cc'| = |c|\,|c'|$;*
3. *(Subaditividade) Para todos $c, c' \in C$, $|c + c'| \leq |c| + |c'|$;*
4. *Para todo $c \in C$, $|-c| = |c|$;*
5. *Para todo $c \in C \smallsetminus \{0\}$, $|c^{-1}| = |c|^{-1}$.*

Demonstração. 1. Como $0 \in C_{\geq 0}$, $|0| = 0$. Reciprocamente, se $|c| = 0$, então $c = 0$ ou $-c = 0$. Ambos os casos implicam $c = 0$.

2. Sejam $c, c' \in C$. Consideramos quatro casos. Se $c, c' \in C_{\geq 0}$, então $cc' \in C_{\geq 0}$, logo
$$|cc'| = cc' = |c|\,|c'|\,.$$

Se $c, c' \in C_{\leq 0}$, então $cc' \in C_{\geq 0}$, logo

$$|cc'| = cc' = (-c)(-c') = |c|\,|c'|\,.$$

Se $c \in C_{\geq 0}$ e $c \in C_{\leq 0}$, então $cc' \in C_{\leq 0}$, logo

$$|cc'| = -cc' = |c|\,|c'|\,.$$

O caso em que $c \in C_{\leq 0}$ e $c \in C_{\geq 0}$ é o mesmo, trocando c e c'.

3. Sejam $c, c' \in C$. Consideramos quatro casos. Se $c, c' \in C_{\geq 0}$, então $c + c' \in C_{\geq 0}$, logo
$$|c + c'| = c + c' = |c| + |c'|\,.$$
Se $c, c' \in C_{\leq 0}$, então $c + c' \in C_{\leq 0}$, logo
$$|c + c'| = -(c + c') = (-c) + (-c') = |c| + |c'|\,.$$
Se $c \in C_{\geq 0}$ e $c' \in C_{\leq 0}$, então $-c \leq c$ e $c' \leq -c'$. Consideramos dois casos. Se $c + c' \in C_{\geq 0}$, então
$$|c + c'| = c + c' \leq c + (-c') = |c| + |c'|$$
Se $c + c' \in C_{\leq 0}$, então
$$|c + c'| = -(c + c') = (-c) + (-c') \leq c + (-c') = |c| + |c'|$$

4. Seja $c \in C$. Se $c \in C_{\geq 0}$, então $|c| = c$ e $-c \in C_{\leq 0}$, logo $|-c| = c = |c|$; se $c \in C_{\leq 0}$, então $|c| = -c$ e $-c \in C_{\geq 0}$, logo $|-c| = -c = |c|$.

5. Seja $c \in C \smallsetminus \{0\}$. Então
$$\left|c^{-1}\right| = \left|c^{-1}\right| |c|\,|c|^{-1} = \left|c^{-1}c\right| |c|^{-1} = |1|\,|c|^{-1} = |c|^{-1}\,.$$

■

Definição 7.7. Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. A *distância* de C é a função

$$\begin{aligned} |\cdot,\cdot| \colon C \times C &\longrightarrow C_{\geq 0} \\ (c, c') &\longmapsto |c' - c|\,. \end{aligned}$$

Proposição 7.12. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. A distância $|\cdot,\cdot| : C \times C \longrightarrow C_{\geq 0}$ satisfaz:*

1. *(Separação) Para todos $c, c' \in C$,*
$$|c, c'| = 0 \quad \Longleftrightarrow \quad c = c';$$

2. *(Simetria) Para todos* $c, c' \in C$,

$$|c, c'| = |c', c|\,;$$

3. *(Desigualdade Triangular) Para todos* $c, c', c'' \in C$,

$$|c, c''| \leq |c, c'| + |c', c''|\,;$$

4. *(Invariância por Translação) Para todos* $c, c', c'' \in C$,

$$|c + c', c + c''| = |c', c''|\,;$$

5. *(Homogeneidade Absoluta) Para todos* $c, c', c'' \in C$,

$$|cc', cc''| = |c|\,|c', c''|\,.$$

6. *Para todos* $c, c' \in C$,

$$|-c, -c'| = |c, c'|\,;$$

7. *Para todo* $c \in C$,

$$|c| = |0, c|\,.$$

7.1.6 Conicidade

Definição 7.8 (Cone)**.** Seja $\boldsymbol{V}$ um espaço linear sobre um corpo ordenado $(\boldsymbol{C}, \leq)$. Um *cone* (ou *conjunto cônico*) em V é um conjunto $X \subseteq V$ tal que, para todo $c \in C_{\geq 0}$,

$$cX \subseteq X.$$

Isso é equivalente a, para todos $c \in C_{\geq 0}$ e $x \in X$, $cx \in X$.

Definição 7.9 (Combinação cônica)**.** Sejam $\boldsymbol{V}$ um espaço linear sobre um corpo ordenado $(\boldsymbol{C}, \leq)$ e $v_0, \cdots, v_{n-1} \in V$. Uma *combinação cônica* de $v_0, \cdots, v_{n-1}$ é um vetor $v \in V$ para o qual existem $c_0, \cdots, c_{n-1} \in C_{\geq 0}$ tais que

$$v = \mathop{\bigplus}_{i \in [n]} c_i v_i.$$

Um *cone agudo* é um cone X tal que $X \cap -X = \{0\}$.

Proposição 7.13. *Sejam* $\boldsymbol{V}$ *um espaço linear sobre um corpo ordenado* $(\boldsymbol{C}, \leq)$ *e* $X \subseteq V$ *um cone.*

1. *Se* $X \neq \emptyset$, *então* $0 \in X$;

2. $X \cap -X$ é o maior subespaço linear contido em X.

Definição 7.10. Sejam X um conjunto e $(\boldsymbol{C}, \leq)$ um corpo ordenado. Uma *função positiva* de X para C é uma função de X para $C_{\geq 0}$; ou seja, uma função $f\colon X \longrightarrow C$ tal que, para todo $x \in X$, $f(x) \geq 0$. O espaço de funções positivas de X para C é $C^X_{\geq 0}$.

Proposição 7.14. *Sejam X um conjunto e $(\boldsymbol{C}, \leq)$ um corpo ordenado. O espaço $C^X_{\geq 0}$ de funções positivas é um cone em C^X.*

Demonstração. Sejam $c \in C_{\geq 0}$ e $f \in C^X_{\geq 0}$. Então, para todo $x \in X$, $f(x) \geq 0$, portanto $cf(x) \geq 0$, logo $cf \geq 0$. ■

7.1.7 Convexidade

Definição 7.11 (Conjunto convexo)**.** Seja $\boldsymbol{V}$ um espaço linear sobre um corpo ordenado $(\boldsymbol{C}, \leq)$. Um *conjunto convexo* em V é um conjunto $X \subseteq V$ tal que, para todo $c \in [0, 1]$,

$$(1 - c)X + cX \subseteq X.$$

Isso é equivalente a dizer que, para todos $x, x' \in X$ e $c \in [0, 1]$,

$$(1 - c)x + cx' \in X.$$

Uma combinação convexa é uma combinação cônica cuja soma dos coeficientes é 1.

Definição 7.12 (Combinação convexa)**.** Sejam $\boldsymbol{V}$ um espaço linear sobre um corpo ordenado $(\boldsymbol{C}, \leq)$ e $v_0, \cdots, v_{n-1} \in V$. Uma *combinação convexa* de $v_0, \cdots, v_{n-1}$ é um vetor $v \in V$ para o qual existem $c_0, \cdots, c_{n-1} \in C_{\geq 0}$ tais que $+_{i \in [n]} c_i = 1$ e

$$v = \mathop{+}_{i \in [n]} c_i v_i.$$

Um conjunto convexo é um conjunto fechado por combinações convexas.

Proposição 7.15. *Seja $\boldsymbol{V}$ um espaço linear sobre um corpo ordenado $(\boldsymbol{C}, \leq)$ e X um conjunto convexo em V. Para todos $c_0, \cdots, c_{n-1} \in C_{\geq 0}$ tais que $+_{i \in [n]} c_i = 1$,*

$$\mathop{+}_{i \in [n]} c_i X \subseteq X.$$

Parte 3

Topologia e Geometria

Capítulo 1

Topologia

1.1 Espaços Topológicos

1.1.1 Topologia, Abertos e Fechados

A noção de topologia que será abordada nesta parte do livro é a topologia baseada em teoria dos conjuntos.

Definição 1.1. Seja X um conjunto. Uma *topologia* de X é um conjunto $\mathcal{T} \subseteq \mathsf{P}(X)$ 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 1.1. *Seja X um conjunto.*

1. *(Topologia trivial) $\{\emptyset, X\}$ é uma topologia de X;*
2. *(Topologia discreta) $\mathsf{P}(X)$ 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 seguda 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 $\mathcal{T} = \mathsf{P}(X)$. ■

Definição 1.2. 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 complemenar em X é um aberto de $(X, \mathcal{T})$. O conjunto dos fechados de $(X, \mathcal{T})$ é denotado $\mathsf{C}(\mathcal{T})$.

Proposição 1.2 (Dualidade de abertos e fechados)**.** *Seja X um conjunto. Então*

1. *Vazio e conjunto todo são fechados.*
$$\emptyset, X \in \mathsf{C}(\mathcal{T})$$
2. *Interseção de fechados é fechado.*
$$(F_i)_{i\in I} \subseteq \mathsf{C}(\mathcal{T}) \Rightarrow \bigcap_{i\in I} F_i \in \mathsf{C}(\mathcal{T})$$
3. *União finita de fechados é fechado.*
$$(F_i)_{i\in[n]} \subseteq \mathsf{C}(\mathcal{T}) \Rightarrow \bigcup_{i=0}^{n-1} F_i \in \mathsf{C}(\mathcal{T})$$

Demonstração. Todas as demonstrações dependem de propriedades básicas de teoria de conjuntos.

1. Como $\emptyset, X \in \mathcal{T}$, $\emptyset^{\mathsf{C}} = X$ e $X^{\mathsf{C}} = \emptyset$, segue que $\emptyset, X \in \mathsf{C}(\mathcal{T})$.
2. Seja $(F_i)_{i\in I} \subseteq \mathsf{C}(\mathcal{T})$. Então $((F_i)^{\mathsf{C}})_{i\in I} \subseteq \mathcal{T}$, o que implica que $\bigcup_{i\in I}(F_i)^{\mathsf{C}} \in \mathcal{T}$. Para concluir a demonstração, basta notar que
$$\left(\bigcup_{i\in I}(F_i)^{\mathsf{C}}\right)^{\mathsf{C}} = \bigcap_{i\in I} F_i.$$
3. Seja $(F_i)_{i\in[n]} \subseteq \mathsf{C}(\mathcal{T})$. Então $((F_i)^{\mathsf{C}})_{i\in[n]} \subseteq \mathcal{T}$, o que implica que $\bigcap_{i=0}^{n-1}(F_i)^{\mathsf{C}} \in \mathcal{T}$. Para concluir a demonstração, basta notar que
$$\left(\bigcap_{i=0}^{n-1}(F_i)^{\mathsf{C}}\right)^{\mathsf{C}} = \bigcup_{i=0}^{n-1} F_i.$$

■

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 froteira 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 particilar, em algum aberto. Seguem abaixo a definição formal de interior de um conjunto e, em seguida, algumas propriedades básicas.

Definição 1.3. Sejam $\boldsymbol{X}$ 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 defínção, 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 $\mathcal{I} : \mathsf{P}(X) \longrightarrow \mathsf{P}(X)$ que leva $C \longmapsto C^\circ$. 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 $\mathsf{P}(X)$ 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 1.3. *Sejam* $\boldsymbol{X}$ *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 $j \in I$ 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 1.4. *Sejam* X *um conjunto e* $\mathcal{I} : \mathsf{P}(X) \longrightarrow \mathsf{P}(X)$ *uma função que satisfaz, para todos* $A, B \subseteq X$,

1. $\mathcal{I}(X) = X$;

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,

$$\begin{aligned}
\mathcal{I}\left(\bigcap_{i=0}^{k} A_i\right) &= \mathcal{I}\left(\left(\bigcap_{i=0}^{k-1} A_i\right) \cap A_k\right) \\
&= \mathcal{I}\left(\bigcap_{i=0}^{k-1} A_i\right) \cap \mathcal{I}\left(A_k\right) \\
&= \bigcap_{i=0}^{k-1} A_i \cap A_k \\
&= \bigcap_{i=0}^{k} A_i,
\end{aligned}$$

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 1.5. *Sejam $(X, \mathcal{T})$ um espaço topológico e $C \subseteq X$. Então*

$$C^\circ = \{x \in X \mid \bigvee A \in \mathcal{T} \quad x \in A \subseteq C\}$$

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 1.4. 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 1.6. *Seja $\boldsymbol{X}$ 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 1.7. *Sejam X um conjunto e $\mathcal{F} : \mathsf{P}(X) \longrightarrow \mathsf{P}(X)$ uma função que satisfaz, 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 $\complement(\mathcal{T}) := \{C \subseteq X \mid C = \mathcal{F}(C)\}$ 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 1.8. *Sejam $\boldsymbol{X}$ um espaço topológico e $A \subseteq X$. Então*

1. $(\overline{A})^{\complement} = (A^{\complement})^{\circ}$;
2. $(A^{\circ})^{\complement} = \overline{(A^{\complement})}$.

Demonstração. 1.

2.

■

Fronteira

Definição 1.5. Sejam $\boldsymbol{X}$ um espaço topológico e $C \subseteq X$. A *fronteira* de C é o conjunto

$$\partial C := \overline{C} \smallsetminus C^{\circ}.$$

Proposição 1.9. *Sejam $\boldsymbol{X}$ um espaço topológico e $C \subseteq X$. Então*

1. *O fecho é a união disjunta de interior e fronteira.*

$$\overline{C} = C^{\circ} \cup \partial C \quad e \quad C^{\circ} \cap \partial C = \emptyset$$

2. *A fronteira é a interseção dos fechos do conjunto e de seu complementar.*

$$\partial C = \overline{C} \cap \overline{C^{\complement}}$$

3. *Um conjunto é aberto se, e somente se, não contém pontos da fronteira.*

$$C \in \mathcal{T} \Leftrightarrow \partial C \cap C = \emptyset$$

4. *Um conjunto é fechado se, e somente se, contém todos pontos da fronteira.*

$$C \in \complement(\mathcal{T}) \Leftrightarrow \partial C \subseteq C$$

5. *A fronteira de um conjunto é fechada.*

$$\partial C \in \complement(\mathcal{T})$$

6. $\partial(\partial(\partial C)) = \partial(\partial C)$.

Demonstração. 1.

$$\partial C = \overline{C} \setminus C^\circ \Leftrightarrow \overline{C} = C^\circ \cup \partial C$$

2.

3.

$$\partial C = \overline{C} \setminus C^\circ = \overline{C} \cap (C^\circ)^\complement = \overline{C} \cap \overline{C^\complement}$$

■

1.1.2 Topologias Geradas, Bases e Sub-bases

Topologias Finas e Grossas e Topologias Geradas

Definição 1.6. 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 1.10. *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 1.7. Sejam X um conjunto, $G \subseteq \mathsf{P}(X)$ 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

1.1.3 Funções Contínuas

Definição 1.8. Sejam $\boldsymbol{X} = (X, \mathcal{T}_X)$ e $\boldsymbol{Y} = (Y, \mathcal{T}_Y)$ espaços topológicos. Uma *função contínua* de $\boldsymbol{X}$ para $\boldsymbol{Y}$ é uma função $f : X \longrightarrow Y$ tal que, para todo $A \in \mathcal{T}_Y$,

$$f^{-1}(A) \in \mathcal{T}_X.$$

Denota-se $f : \boldsymbol{X} \longrightarrow \boldsymbol{Y}$. O conjunto dessas funções é denotado por $\mathscr{C}(\boldsymbol{X}, \boldsymbol{Y})$.

Proposição 1.11. (Propriedades categóricas).

1. *(Identidade) Seja $\boldsymbol{X}$ um espaço topológico. A função $\mathrm{I}_X : X \longrightarrow X$ é uma função contínua.*

2. *(Associatividade) Sejam $\boldsymbol{X_0}$, $\boldsymbol{X_1}$ e $\boldsymbol{X_2}$ espaços topológicos e $f_0 : \boldsymbol{X_0} \longrightarrow \boldsymbol{X_1}$ e $f_1 : \boldsymbol{X_1} \longrightarrow \boldsymbol{X_2}$ funções contínuas. Então $f_1 \circ f_0 : \boldsymbol{X_0} \longrightarrow \boldsymbol{X_2}$ é uma função contínua.*

$$\begin{tikzcd} \boldsymbol{X_0} \arrow[r, "f_0"] \arrow[rr, bend right, "f_1 \circ f_0"'] & \boldsymbol{X_1} \arrow[r, "f_1"] & \boldsymbol{X_2} \end{tikzcd}$$

Demonstração. 1. Seja $A \in \mathcal{T}$. Então $\mathrm{I}_X^{-1}(A) = A \in \mathcal{T}$, logo I_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.

■

Suporte de Funções Vetoriais

Definição 1.9. Sejam $\boldsymbol{X}$ um espaço topológico, $\boldsymbol{L}$ um espaço linear topológico e $f\colon X \longrightarrow L$ uma função contínua. O *suporte fechado* de f é o conjunto

$$\overline{\operatorname{supp}}(f) := \overline{\operatorname{supp}(f)} = \overline{f^{-1}(L \smallsetminus \{0\})}.$$

1.1.4 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 quado 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 1.10. Sejam X um conjunto, $\boldsymbol{Y} = (Y, \mathcal{T}_Y)$ um espaço topológico e $f : X \longrightarrow Y$ uma função. A *topologia puxada* por f de $\boldsymbol{Y}$ para X é

$$f^\star(\mathcal{T}_Y) := \left\{ f^{-1}(A) \;\middle|\; A \in \mathcal{T}_Y \right\}.$$

Proposição 1.12. *Sejam X um conjunto, $\boldsymbol{Y} = (Y, \mathcal{T}_Y)$ um espaço topológico e $f : X \longrightarrow Y$ uma função. Então $f^\star(\mathcal{T}_Y)$, a topologia puxada por f de $\boldsymbol{Y}$ para X, é uma topologia de X.*

Demonstração. (1) Notemos que, como $\emptyset \in \mathcal{T}_Y$ e $\emptyset = f^{-1}(\emptyset)$, temos que $\emptyset \in f^\star(\mathcal{T}_Y)$. (2) Seja $(A_i)_{i\in I}$ uma família de conjuntos em $f^\star(\mathcal{T}_Y)$. 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 $\bigcup_{i\in I} A_i \in f^\star(\mathcal{T}_Y)$. (3) Seja $(A_i)_{i=1}^n$ uma família de conjuntos em $f^\star(\mathcal{T}_Y)$. 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 $\bigcap_{i=1}^n A_i \in f^\star(\mathcal{T}_Y)$. ■

Proposição 1.13. *Sejam $\boldsymbol{X} = (X, \mathcal{T}_X)$ e $\boldsymbol{Y} = (Y, \mathcal{T}_Y)$ espaços topológicos. Uma função $f : X \longrightarrow Y$ é função contínua de $\boldsymbol{X}$ para $\boldsymbol{Y}$ se, e somente se, a topologia $f^\star(\mathcal{T}_Y)$ puxada por f de $\boldsymbol{Y}$ para X é uma subtopologia de $\mathcal{T}_X$.*

$$f \in \mathscr{C}(\boldsymbol{X}, \boldsymbol{Y}) \quad \Longleftrightarrow \quad f^\star(\mathcal{T}_Y) \subseteq \mathcal{T}_X.$$

Demonstração. Suponha que $f \in \mathscr{C}(\boldsymbol{X}, \boldsymbol{Y})$ e seja $B \in f^\star(\mathcal{T}_Y)$. 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, $f^\star(\mathcal{T}_Y) \subseteq \mathcal{T}_X$. Reciprocamente, suponha que $f^\star(\mathcal{T}_Y) \subseteq \mathcal{T}_X$. Então, para todo $A \in \mathcal{T}_Y$, $f^{-1}(A) \in f^\star(\mathcal{T}_Y)$, portanto $f^{-1}(A) \in \mathcal{T}_X$, o que mostra que $f \in \mathscr{C}(\boldsymbol{X}, \boldsymbol{Y})$. ■

Definição 1.11. Sejam $\boldsymbol{X}$ um conjunto, $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{T}_i)_{i\in I}$ uma família de espaços topológicos e, para todo $i \in I$, $f_i : X \longrightarrow X_i$ 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 1.14. *Sejam $\boldsymbol{X}$ um conjunto, $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{T}_i)_{i\in I}$ uma família de espaços topológicos e, para todo $i \in I$, $f_i : X \longrightarrow X_i$ uma função. A topologia inicial de X com respeito à família $(f_i)_{i\in I}$ é a topologia*

$$\left\langle \bigcup_{i\in I} {f_i}^\star(\mathcal{T}_i) \right\rangle.$$

Demonstração. Seja $\mathcal{T}$ uma topologia de X tal que, para todo $i \in I$, $f_i : X \longrightarrow X_i$ é contínua. Então, para todo $i \in I$, ${f_i}^\star(\mathcal{T}_i) \subseteq \mathcal{T}$ (1.13), o que implica que $\bigcup_{i\in I} {f_i}^\star(\mathcal{T}_i) \subseteq \mathcal{T}$ e, portanto, $\langle \bigcup_{i\in I} {f_i}^\star(\mathcal{T}_i) \rangle \subseteq \mathcal{T}$. ■

Topologias Empurrada e Final

Definição 1.12. Sejam $\boldsymbol{X} = (X, \mathcal{T}_X)$ um espaço topológico, Y um conjunto e $f : X \longrightarrow Y$ uma função. A *topologia empurrada* por f de $\boldsymbol{X}$ para Y é

$$f_\star(\mathcal{T}_X) := \left\{ A \subseteq Y \;\middle|\; f^{-1}(A) \in \mathcal{T}_X \right\}.$$

Proposição 1.15. *Sejam $\boldsymbol{X} = (X, \mathcal{T}_X)$ um espaço topológico, Y um conjunto e $f : X \longrightarrow Y$ uma função. Então $\mathcal{T}_Y := f_\star(\mathcal{T}_X)$, a topologia empurrada por f de $\boldsymbol{X}$ para Y, é uma topologia de Y.*

Demonstração. (1) Como $f^{-1}(\emptyset) = \emptyset$ e $f^{-1}(Y) = X$, segue que $\emptyset, Y \in f_\star(\mathcal{T}_X)$. (2) Seja $(A_i)_{i\in I}$ uma família de conjuntos de $f_\star(\mathcal{T}_X)$. 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 $\bigcup_{i\in I} A_i \in f_\star(\mathcal{T}_X)$. (3) Seja $(A_i)_{i=1}^n$ uma família de conjuntos de $f_\star(\mathcal{T}_X)$. 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 $\bigcap_{i=1}^n A_i \in f_\star(\mathcal{T}_X)$. ■

Definição 1.13. Sejam $\boldsymbol{X}$ um conjunto, $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{T}_i)_{i\in I}$ uma família de espaços topológicos e, para todo $i \in I$, $f_i : X_i \longrightarrow X$ 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 1.16. *Sejam $\boldsymbol{X}$ um conjunto, $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{T}_i)_{i\in I}$ uma família de espaços topológicos e, para todo $i \in I$, $f_i : X_i \longrightarrow X$ uma função. A topologia final de X com respeito à família $(f_i)_{i\in I}$ é a topologia*

$$\bigcap_{i\in I} f_{i\star}(\mathcal{T}_i).$$

Demonstração. Seja $\mathcal{T}$ uma topologia de X tal que, para todo $i \in I$, $f_i : X_i \longrightarrow X$ 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 $A \in f_{i\star}(\mathcal{T}_i)$, portanto $A \in \bigcap_{i\in I} f_{i\star}(\mathcal{T}_i)$. Isso mostra que $\mathcal{T} \subseteq \bigcap_{i\in I} f_{i\star}(\mathcal{T}_i)$, e como interseção de topologiaas é topologia, segue o procurado. ■

Produto de Espaços Topológicos

Definição 1.14. Seja $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{T}_i)_{i\in I}$ uma família de espaços topológicos. O *produto* da família $(\boldsymbol{X_i})_{i\in I}$ é o par

$$\prod_{i\in I} \boldsymbol{X_i} := \left(\prod_{i\in I} X_i, \left\langle \bigcup_{i\in I} {\pi_i}^\star(\mathcal{T}_i) \right\rangle\right).$$

A topologia $\langle \bigcup_{i\in I} {\pi_i}^\star(\mathcal{T}_i) \rangle$ é a *topologia produto* de $\prod_{i\in I} X_i$.

Proposição 1.17. *Sejam* $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{T}_i)_{i\in I}$ *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* $i \in I \smallsetminus J$*.*

Demonstração. Como $\pi_i = \pi_i \circ \mathrm{I}_X$, segue de uma propriedades básica de imagem inversa de produto (2.8) que

$$\prod_{i\in I} A_i = \mathrm{I}_X^{-1}\left(\prod_{i\in I} A_i\right) = \bigcap_{i\in I} \pi_i^{-1}(A_i)$$

Para todo $i \in I \smallsetminus J$, $A_i = X_i$, então $\pi_i^{-1}(A_i) = X$ e, portanto,

$$\bigcap_{i\in I\smallsetminus J} \pi_i^{-1}(A_i) = \bigcap_{i\in I\smallsetminus J} X = X.$$

Isso implica que

$$\bigcap_{i\in I} \pi_i^{-1}(A_i) = \left(\bigcap_{i\in I\smallsetminus J} \pi_i^{-1}(A_i)\right) \cap \left(\bigcap_{j\in J} \pi_j^{-1}(A_j)\right) = \bigcap_{j\in J} \pi_j^{-1}(A_j)$$

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. ■

Proposição 1.18 (Propriedade Universal)**.** *Sejam* $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{T}_i)_{i\in I}$ *uma família de espaços topológicos,* $\boldsymbol{T} = (T, \mathcal{T}_T)$ *um espaço topológico e, para todo* $i \in I$*,* $f_i : \boldsymbol{T} \longrightarrow \boldsymbol{X_i}$ *uma função contínua. Então existe uma única função contínua* $f : \boldsymbol{T} \longrightarrow \prod_{i\in I} \boldsymbol{X_i}$ *tal que, para todo* $i \in I$*,* $\pi_i \circ f = f_i$ *(o diagrama comuta).*

$$\begin{tikzcd}
 & \prod_{i\in I} \boldsymbol{X_i} \arrow[d, "\pi_i"] \\
\boldsymbol{T} \arrow[ur, dashed, "f"] \arrow[r, "f_i"'] & \boldsymbol{X_i}
\end{tikzcd}$$

Definição 1.15. Defina a função

$$\begin{aligned} f\colon T &\longrightarrow \prod_{i\in I} X_i \\ x &\longmapsto (f_i(x))_{i\in I}. \end{aligned}$$

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 $i \in I \smallsetminus J_k$, $A_{ki} = X_i$. 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 $i \in I \smallsetminus J_k$, $A_{ki} = X_i$, 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 impica 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 1.16. Seja $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{T}_i)_{i\in I}$ uma família de espaços topológicos. O *coproduto* da família $(\boldsymbol{X_i})_{i\in I}$ é o par

$$\bigsqcup_{i\in I} \boldsymbol{X_i} := \left(\bigsqcup_{i\in I} X_i, \bigcap_{i\in I} \iota_{i\star}(\mathcal{T}_i)\right).$$

A topologia $\bigcap_{i\in I} \pi_{i\star}(\mathcal{T}_i)$ é a *topologia coproduto* de $\bigsqcup_{i\in I} X_i$.

Proposição 1.19 (Propriedade Universal)**.** *Sejam $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{T}_i)_{i\in I}$ uma família de espaços topológicos, $\boldsymbol{T} = (T, \mathcal{T}_T)$ um espaço topológico e, para todo $i \in I$, $f_i : \boldsymbol{X_i} \longrightarrow \boldsymbol{T}$ uma função contínua. Então existe uma única função contínua $f : \bigsqcup_{i\in I} \boldsymbol{X_i} \longrightarrow \boldsymbol{T}$ tal que, para todo $i \in I$, $f \circ \iota_i = f_i$ (o diagrama comuta).*

$$\begin{tikzcd}
\bigsqcup_{i\in I} \boldsymbol{X_i} \arrow[dr, dashed, "f"] & \\
\boldsymbol{X_i} \arrow[u, "\iota_i"] \arrow[r, "f_i"'] & \boldsymbol{T}
\end{tikzcd}$$

Subespaços Topológicos

Definição 1.17. 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 1.20. *Sejam $(X, \mathcal{T})$ um espaço topológico e $S \subseteq X$ um subconjunto. A topologia induzida por $\mathcal{T}$ em S é o conjunto*

$$\mathcal{T}|_S = \iota_\star(\mathcal{T}),$$

a maior topologia tal que a inclusão $\iota : S \longrightarrow X$ é contínua.

Proposição 1.21. *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 1.22 (Propriedade característica)**.** *Sejam $\boldsymbol{X} = (X, \mathcal{T}_X)$ e $(Y, \mathcal{T}_Y)$ espaços topológicos e $\boldsymbol{S} \subseteq \boldsymbol{X}$ um subespaço. Uma função $f : Y \longrightarrow S$ é contínua se, e somente se, $\iota \circ f : Y \longrightarrow X$ é contínua (o diagrama comuta).*

$$\begin{tikzcd} & \boldsymbol{X} \\ \boldsymbol{T} \arrow[ur, "\iota \circ f"] \arrow[r, "f"'] & \boldsymbol{S} \arrow[u, "\iota"'] \end{tikzcd}$$

Proposição Restrição de função contínua é contínua na topologia induzida.

Proposição 1.23 (Colagem por abertos)**.** *Sejam $\boldsymbol{X}$ e $\boldsymbol{Y}$ espaços topológicos, $f : X \longrightarrow Y$ uma função e $(X_i)_{i\in I}$ uma cobertura de X por conjuntos abertos tal que, para todo $i \in I$, $f|_{X_i} : X_i \longrightarrow Y$ é contínua. Então $f : X \longrightarrow Y$ é contínua.*

Proposição 1.24 (Colagem por fechados)**.** *Sejam $\boldsymbol{X}$ e $\boldsymbol{Y}$ espaços topológicos, $f : X \longrightarrow Y$ uma função e $(X_i)_{i=1}^n$ uma cobertura de X por conjuntos fechados tal que, para todo $1 \leq i \leq n$, $f|_{X_i} : X_i \longrightarrow Y$ é contínua. Então $f : X \longrightarrow Y$ é contínua.*

Quociente de Espaços Topológicos

Definição 1.18. Sejam $\boldsymbol{X} = (X, \mathcal{T})$ um espaço topológico e $\sim$ uma relação de equivalência em X. O *espaço quociente* com respeito a $\sim$ é o espaço topológico

$$\boldsymbol{X}\big/\!\sim \;:= \left(X\big/\!\sim, \pi^\star(\mathcal{T})\right),$$

em que $\pi : X \longrightarrow X/\!\sim$ é a projeção canônica de equivalências.

É fácil notar que os abertos de $\boldsymbol{X}/\!\sim$ são conjuntos de classes de equivalência cuja união é um aberto de $\boldsymbol{X}$. Notemos, ainda, que se $f : X \longrightarrow Y$ 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 1.25 (Propriedade característica)**.** *Sejam $\boldsymbol{X} = (X, \mathcal{T}_X)$ e $(Y, \mathcal{T}_Y)$ espaços topológicos e $\boldsymbol{Q}$ um espaço quociente de $\boldsymbol{X}$. Uma função $f : Q \longrightarrow Y$ é contínua se, e somente se, $f \circ \pi : X \longrightarrow Y$ é contínua (o diagrama comuta).*

$$\begin{tikzcd} \boldsymbol{X} \arrow[d, "\pi"'] \arrow[dr, "f \circ \pi"] & \\ \boldsymbol{Q} \arrow[r, "f"'] & \boldsymbol{Y} \end{tikzcd}$$

1.2 Separação

1.2.1 Noções de Separação de Conjuntos

Nesta seção são apresentadas algumas noções de como dois conjuntos de um espaço topológico podem ser separados. As duas noções mas 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 1.19. Sejam $\boldsymbol{X}$ um espaço topológico e $A, B \subseteq X$. Definimos as seguintes relações entre A e B:

1. (*Separação*) Cada conjunto é disjunto do feixo 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 cosiderar, 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 1.26. *Sejam $\boldsymbol{X}$ 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.*

1.2.2 Espaços Distinguíveis

Definição 1.20. Seja $\boldsymbol{X}$ um espaço topológico. Pontos *topologicamente indistinguíveis* em $\boldsymbol{X}$ são pontos $x, y \in X$ tais que $\mathcal{V}_x = \mathcal{V}_y$. Pontos *topologicamente disntinguíveis em $\boldsymbol{X}$* são pontos que não são topologicamente indistinguíveis.

Proposição 1.27. *Seja $\boldsymbol{X}$ um espaço topológico. A relação binária de indistinguibilidade 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 indisntinguível. Para isso, basta considerar o espaço quociente definido pela relação. de indistinguibilidade topológica. Espaços com essa propriedade são definidos a seguir.

Definição 1.21 (T_0)**.** Um espaço topológico *distinguível* é um espaço topológico $\boldsymbol{X}$ em que todo par de pontos distintos é topologicamente distinguível:

$$\bigwedge x, y \in X \quad x \neq y \quad \Rightarrow \quad \mathcal{V}_x \neq \mathcal{V}_y.$$

Proposição 1.28. *Seja $\boldsymbol{X}$ um espaço topológico. São equivalentes as seguites propriedades:*

1. $\boldsymbol{X}$ *é dinstinguível.*
2. $\bigwedge x, y \in X \quad x \neq y \quad \Rightarrow \quad \mathcal{V}_x \nsubseteq \mathcal{V}_y$ *ou* $\mathcal{V}_y \nsubseteq \mathcal{V}_x$.
3. $\bigwedge x, y \in X \quad x \neq y \quad \Rightarrow \quad x \notin \overline{\{y\}}$ *ou* $y \notin \overline{\{x\}}$.
4. $\bigwedge x, y \in X \quad x \neq y \quad \Rightarrow \quad \overline{\{x\}} \neq \overline{\{y\}}$.

Proposição 1.29. *Sejam* $\boldsymbol{X}$ *um espaço topológico distinguível e* $Y \subseteq X$. *Então* $\boldsymbol{Y}$ *é um espaço topológico distinguível.*

Proposição 1.30. *Seja* $(X_i)_{i \in I}$ *uma família não vazia de espaços topológicos não vazios. O espaço produto* $\prod_{i \in I} \boldsymbol{X_i}$ *é distinguível se, e somente se, todos os espaços* $\boldsymbol{X}_i$ *são distinguíveis.*

1.2.3 Espaços Acessíveis

Definição 1.22 (T_1)**.** Um espaço topológico *acessível* é um espaço topológico $\boldsymbol{X}$ em que

$$\bigwedge x, y \in X \quad x \neq y \quad \Rightarrow \quad \mathcal{V}_x \nsubseteq \mathcal{V}_y \text{ e } \mathcal{V}_y \nsubseteq \mathcal{V}_x.$$

Proposição 1.31 ($T_1 \Rightarrow T_0$)**.** *Seja* $\boldsymbol{X}$ *um espaço topológico. Se* $\boldsymbol{X}$ *é acessível, então* $\boldsymbol{X}$ *é dintinguível.*

Demonstração. Se $\boldsymbol{X}$ é acessível, então, para todos $x, y \in X$ tais que $x \neq y$, temos que $\mathcal{V}_x \nsubseteq \mathcal{V}_y$ e $\mathcal{V}_y \nsubseteq \mathcal{V}_x$. Mas isso implica que $\mathcal{V}_x \nsubseteq \mathcal{V}_y$ ou $\mathcal{V}_y \nsubseteq \mathcal{V}_x$, o que é equivalente a $\mathcal{V}_x \neq \mathcal{V}_y$. Logo $\boldsymbol{X}$ é dintinguível. ■

Proposição 1.32. *Seja* $\boldsymbol{X}$ *um espaço topológico. São equivalentes as seguintes propriedades:*

1. $\boldsymbol{X}$ *é acessível.*
2. *Todo par de pontos distintos é separado:*

$$\bigwedge x, y \in X \quad x \neq y \quad \Rightarrow \quad x \notin \overline{\{y\}} \text{ e } y \notin \overline{\{x\}}.$$

3. $\bigwedge x, y \in X \quad x \neq y \quad \Rightarrow \quad \bigvee U \in \mathcal{V}_x,\ V \in \mathcal{V}_y \qquad y \notin U$ *e* $x \notin V$.
4. $\bigwedge x \in X \quad \overline{\{x\}} = \{x\}$.

Proposição 1.33. *Sejam* $\boldsymbol{X}$ *um espaço topológico acessível e* $Y \subseteq X$. *Então* $\boldsymbol{Y}$ *é um espaço topológico acessível.*

Proposição 1.34. *Seja* $(X_i)_{i \in I}$ *uma família não vazia de espaços topológicos não vazios. O espaço produto* $\prod_{i \in I} \boldsymbol{X_i}$ *é acessível se, e somente se, todos os espaços* $\boldsymbol{X}_i$ *são acessíveis.*

1.2.4 Espaços Separados

Definição 1.23 (T_2)**.** Um espaço topológico *separado (por vizinhanças)* é um espaço topológico $\boldsymbol{X}$ em que todo par de pontos distintos é separado por vizinhanças:

$$\bigwedge x, y \in X \quad x \neq y \quad \Rightarrow \quad \bigvee U \in \mathcal{V}_x,\ V \in \mathcal{V}_y \quad U \cap V = \emptyset.$$

Esses espaços também são conhecidos como espaços de Hausdorff.

Proposição 1.35 ($T_2 \Rightarrow T_1$)**.** *Seja $\boldsymbol{X}$ um espaço topológico. Se $\boldsymbol{X}$ é separado, então $\boldsymbol{X}$ é acessível.*

Proposição 1.36. *Seja $\boldsymbol{X}$ um espaço topológico. São equivalentes as seguintes propriedades:*

1. *$\boldsymbol{X}$ é separado.*
2. *Toda rede convergente em $\boldsymbol{X}$ tem limite único.*
3. *Todo filtro convergente em $\boldsymbol{X}$ tem limite único.*

Proposição 1.37. *Sejam $\boldsymbol{X}$ um espaço topológico separado e $Y \subseteq X$. Então $\boldsymbol{Y}$ é um espaço topológico separado.*

Proposição 1.38. *Seja $(\boldsymbol{X}_i)_{i \in I}$ uma família não vazia de espaços topológicos não vazios. O espaço produto $\prod_{i \in I} \boldsymbol{X_i}$ é separado se, e somente se, todos os espaços $\boldsymbol{X}_i$ são separados.*

Proposição 1.39. *Sejam $\boldsymbol{X}$ um espaço topológico, $\boldsymbol{Y}$ um espaço topológico separado, $D \subseteq X$ um subconjunto denso em X e $f, g : X \longrightarrow Y$ funções contínuas tais que $f|_D = g|_D$. Então $f = g$.*

1.2.5 Espaços Regulares

Definição 1.24. 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 seprados regulares são também chamados de T_3.

Proposição 1.40. *Seja $\boldsymbol{X}$ um espaço topológico regular. Então $\boldsymbol{X}$ 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 $\boldsymbol{X}$ 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 $\boldsymbol{X}$, 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 $\boldsymbol{X}$ é separado por vizinhanças. ■

Proposição 1.41. *Seja $\boldsymbol{X}$ um espaço topológico. São equivalentes as seguintes propriedades:*

1. *$\boldsymbol{X}$ 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 1.42. *Sejam $\boldsymbol{X}$ um espaço topológico regular e $Y \subseteq X$. Então $\boldsymbol{Y}$ é um espaço topológico regular.*

Proposição 1.43. *Seja $(X_i)_{i \in I}$ uma família não vazia de espaços topológicos não vazios. O espaço produto $\prod_{i \in I} \boldsymbol{X_i}$ é regular se, e somente se, todos os espaços $\boldsymbol{X}_i$ são regulares.*

1.2.6 Espaços Completamente Regulares

Definição 1.25. 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 1.44. *Seja $\boldsymbol{X}$ um espaço topológico. Se $\boldsymbol{X}$ é completamente regular, então $\boldsymbol{X}$ é regular.*

Proposição 1.45. *Sejam $\boldsymbol{X}$ um espaço topológico completamente regular e $Y \subseteq X$. Então $\boldsymbol{Y}$ é um espaço topológico completamente regular.*

Proposição 1.46. *Seja $(X_i)_{i \in I}$ uma família não vazia de espaços topológicos não vazios. O espaço produto $\prod_{i \in I} \boldsymbol{X_i}$ é completamente regular se, e somente se, todos os espaços $\boldsymbol{X}_i$ são completamente regulares.*

1.2.7 Espaços Normais

Definição 1.26. 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 1.47. *Seja $\boldsymbol{X}$ um espaço topológico normal. Então $\boldsymbol{X}$ 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 $\boldsymbol{X}$ 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 $\boldsymbol{X}$ existem $V_x \in \mathcal{V}_x$ e $V_y \in \mathcal{V}_y$ tais que $V_x \cap V_y = \emptyset$; ou seja, $\boldsymbol{X}$ é separado por vizinhanças. ■

Proposição 1.48. *Sejam $\boldsymbol{X}$ um espaço topológico normal e $Y \subseteq X$ fechado. Então $\boldsymbol{Y}$ é um espaço topológico normal.*

Proposição 1.49. *Seja $\boldsymbol{X}$ um espaço topológico. São equivalentes as seguintes propriedades:*

1. *$\boldsymbol{X}$ 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 1.50 (Lema de Urysohn)**.** *Um espaço topológico $\boldsymbol{X}$ é normal se, e somente se, todo par de conjuntos fechados disjuntos é separado por função contínua.*

Demonstração. Se todo par de cojuntos fechados é separado por função contínua, segue da proposição 1.26 que eles são separados por vizinhanças.

Para demonstrar a recíproca, suponhamos que $\boldsymbol{X}$ 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 $A_1 := {F_1}^{\complement}$ e notamos que $F_0 \subseteq A_1$, pois F_0 e F_1 são disjuntos. Como $\boldsymbol{X}$ 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 $Q_n := \{r(k) \mid k \in \{0, \ldots, n\}\}$ 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

$$\begin{aligned} f \colon X &\longrightarrow [0,1] \\ x &\longmapsto \inf \{q \in Q \mid x \in A_q\}. \end{aligned}$$

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 $A_q \subseteq A_1 = F_1^{\complement}$, 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 $\{q \in Q \mid x \in A_q\}\ \mathbb{Q} \cap [0, q[$ 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 $A := A_q \smallsetminus \overline{A_p}$. 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. ■

1.3 Convergência

1.3.1 Redes

Proposição 1.51. *Sejam $\boldsymbol{X}$ 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 1.27. Sejam X um conjunto e $(\Lambda, \leq)$ um conjunto direcionado. Uma *rede* de elementos de X indexados por Λ é uma função $x : \Lambda \longrightarrow X$. 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 1.28 (Limite e convergência)**.** Sejam $\boldsymbol{X}$ um espaço topológico e $(x_\lambda)_{\lambda\in\Lambda}$ uma rede de X. Um *limite* de $(x_\lambda)_{\lambda\in\Lambda}$ em $\boldsymbol{X}$ 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 $(x_\lambda)_{\lambda\in\Lambda} \to \ell$. Uma rede *convergente* é uma rede que tem limite.

Proposição 1.52. *Um espaço topológio $\boldsymbol{X}$ 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 $\boldsymbol{X}$ 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 $(\Lambda, \leq)$ 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 $\boldsymbol{X}$ 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 1.53. *Sejam $\boldsymbol{X}_0$ e $\boldsymbol{X}_1$ espaços topológicos e $f : X_0 \longrightarrow X_1$ 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 1.54. *Sejam $(\boldsymbol{X}_i)_{i\in I}$ uma família de espaços topológicos e $(x_\lambda)_{\lambda\in\Lambda}$ uma rede de $\boldsymbol{X} = \prod_{i\in I} \boldsymbol{X}_i$. Então $(x_\lambda)_{\lambda\in\Lambda} \to \ell \in X$ se, e somente se, para todo $i \in I$, $(\pi_i(x_\lambda))_{\lambda\in\Lambda} \to \pi_i(\ell) \in X_i$.*

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 $((x_{i,\lambda})_{i\in I})_{\lambda\in\Lambda} \to (\ell_i)_{i\in I}$. ■

1.4 Conexidade e Compacidade

1.4.1 Conexidades

Definimos o conceito de desconexo antes por ele ser mais intuitivo de ser enunciado. Ser desconexo é ter como separar o espaço $\boldsymbol{X}$ 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 1.29. Um espaço topológico *desconexo* é um espaço topológico $\boldsymbol{X}$ 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 $\boldsymbol{\emptyset}$ 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 1.55. *Um espaço topológico $\boldsymbol{X}$ 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 $\boldsymbol{X}$ é desconexo, os conjuntos que formam sua partição por abertos são ambos abertos e fechados. Reciprocamente, se $A \subseteq X$ é não tricial, aberto e fechado, $A^{\complement}$ também

é não trivial e aberto (e fechado), logo $\{A, A^{\complement}\}$ 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 1.56. *Seja $\boldsymbol{X}$ um espaço topológico. Então $S \subseteq X$ é conexo se, e somente se, não existem conjuntos não triviais separados em $\boldsymbol{X}$ cuja união é S.*

Demonstração. Se S é desconexo, existe uma partição $\{A, B\}$ de S por abertos de $\boldsymbol{S}$. 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, similamente, $\overline{A}^X \cap B = \emptyset$, o que mostra que A e B são separados em $\boldsymbol{X}$. Reciprocamente, se existem $A, B \subseteq X$ conjuntos não triviais separados em $\boldsymbol{X}$ 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 $\boldsymbol{S}$, o que mostra que $\boldsymbol{S}$ 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 1.57. *Sejam $\boldsymbol{X}$ um espaço topológico, e $\boldsymbol{\{0,1\}}$ espaço topológico com a topologia discreta. Então $\boldsymbol{X}$ é conexo se, e somente se, toda função contínua $f : \boldsymbol{X} \longrightarrow \boldsymbol{\{0,1\}}$ é constante.*

Demonstração. Demonstraremos a ida e a volta pela contrapositiva. Se $\boldsymbol{X}$ é desconexo, seja $\{A_0, A_1\}$ uma partição de X por dois conjuntos abertos. Definamos

$$\begin{aligned} f\colon X &\longrightarrow \{0,1\} \\ x &\longmapsto \begin{cases} 0, & x \in A_0 \\ 1, & x \in A_1. \end{cases} \end{aligned}$$

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 $f : X \longrightarrow \{0,1\}$ 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 $\boldsymbol{X}$ é desconexo. ■

Proposição 1.58. *Sejam $\boldsymbol{X}$ e $\boldsymbol{Y}$ espaços topológicos e $f : \boldsymbol{X} \longrightarrow \boldsymbol{Y}$ uma função contínua. Se $\boldsymbol{X}$ é conexo, então $\boldsymbol{Y}$ é conexo.*

Demonstração. Se $\boldsymbol{Y}$ 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 $\boldsymbol{X}$. ■

Componentes Conexas

Proposição 1.59. *Seja $\boldsymbol{X}$ 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 1.30. Sejam $\boldsymbol{X}$ um espaço topológico, $p \in X$ e $(C_i)_{i\in I}$ uma indexação dos conjuntos conexos que contêm p. A *componente conexa* de $\boldsymbol{X}$ em p é o conjunto conexo

$$\Gamma_p := \bigcup_{i\in I} C_i.$$

O conjunto Γ_p é conexo pela proposição 1.59, 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 1.60. *As componentes conexas de um espaço topológico $\boldsymbol{X}$ 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

1.4.2 Compacidades

As propriedade de compacidade de um espaço topológico são propriedades relacionadas a coberturas de um espaço.

Compacidade

Definição 1.31. Um espaço topológico *compacto* é um espaço topológico $\boldsymbol{X}$ em que toda cobertura aberta $\mathcal{C}$ de $\boldsymbol{X}$ tem subcobertura finita. Um subconjunto *compacto* de $\boldsymbol{X}$ é um conjunto $C \subseteq X$ que é compacto com a topologia de subespaço.

Proposição 1.61. *Seja $\boldsymbol{X}$ um espaço topológico. São equivalentes*

1. *$\boldsymbol{X}$ é compacto;*
2. *Toda rede em $\boldsymbol{X}$ tem sub-rede convergente.*

Proposição 1.62. *Seja $\boldsymbol{X}$ um espaço topológico. Se $C \subseteq X$ é compacto e $F \subseteq C$ é fechado, então F é compacto.*

Proposição 1.63. *Seja $\boldsymbol{X}$ um espaço topológico separado. Para todo compacto $C \subseteq X$ e todo ponto $x \in X \smallsetminus C$, existem vizinhanças abertas V' de C e V de x que são disjuntas.*

Demonstração. Como $\boldsymbol{X}$ é separado, para todo $c \in C$ existem vizinhanças abertas V'_c de c e V_c de x que são disjuntas. Como C é compacto e $\{V'_c\}_{c \in C}$ é cobertura de C, existem $c_0, \cdots, c_{n-1} \in C$ tais que

$$C \subseteq \bigcup_{i \in [n]} V'_{c_i}$$

Definindo $V' := \bigcup_{i \in [n]} V'_{c_i}$ e $V := \bigcap_{i \in [n]} V_{c_i}$, segue que V' e V são vizinhanças abertas de C e x, respectivamente, e $V' \cap V = \emptyset$. ■

Proposição 1.64. *Seja $\boldsymbol{X}$ um espaço topológico separado.*

1. *Se $C \subseteq X$ é compacto, então é fechado;*
2. *Se $C \subseteq X$ é compacto e $F \subseteq X$ é fechado, então $C \cap F$ é compacto.*

Proposição 1.65. *Sejam $\boldsymbol{X}_0$ e $\boldsymbol{X}_1$ espaços topológicos e $f \colon X_0 \longrightarrow X_1$ uma função contínua. Se $\boldsymbol{X}_0$ é compacto, então $f(\boldsymbol{X}_0)$ é compacto.*

Demonstração. Seja $(C_I)_{i\in I}$ uma cobertura aberta de $f(\boldsymbol{X}_0)$. A família $(f^{-1}(C_i))_{i\in I}$ é uma cobertura de X_1, 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 $\boldsymbol{X}_0$ é compacto, existem $i_0, \ldots, i_{n-1} \in I$ tal que $(f^{-1}(A_{i_k}))_{k\in[n]}$ é uma cobertura aberta de $\boldsymbol{X}_0$. Então $(A_{i_k})_{k\in[n]}$ é uma cobertura aberta de $f(\boldsymbol{X}_0)$, 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 $f(\boldsymbol{X}_0)$ é compacto. ■

Definição 1.32. Sejam $\boldsymbol{X}$ um espaço topológico e $\boldsymbol{L}$ um espaço linear topológico. O espaço das funções contínuas de $\boldsymbol{X}$ para $\boldsymbol{L}$ com suporte compacto é denotado $\mathscr{C}_c(X, L)$.

Compacidade Contável (Lindelöf)

Definição 1.33. Um espaço topológico *contavelmente compacto* (*Lindelöf*) é um espaço topológico $\boldsymbol{X}$ em que toda cobertura aberta $\mathcal{C}$ de $\boldsymbol{X}$ tem subcobertura contável.

Alguns autores definem compacidade contável como a propriedade de que toda cobertura aberta contável admite subcobertura finita.

Compacidade Local

Definição 1.34. Um espaço topológico *localmente compacto* é um espaço topológico $\boldsymbol{X}$ em que todo ponto $x \in X$ tem uma vizinhança compacta.

Proposição 1.66. *Seja $\boldsymbol{X}$ um espaço topológico localmente compacto. Se $\boldsymbol{X}$ é separado, então todo ponto $x \in X$ tem uma vizinhança aberta com fecho compacto.*

Proposição 1.67. *Seja $\boldsymbol{X}$ um espaço topológico separado e localmente compacto. Para todo compacto $C \subseteq X$ e toda vizinhança aberta $A \subseteq X$ de C, existe aberto $V \subseteq X$ com fecho compacto tal que*

$$C \subseteq V \subseteq \overline{V} \subseteq A.$$

Proposição 1.68. *Seja $\boldsymbol{X}$ um espaço topológico separado e localmente compacto. Para todo compacto C e todo aberto A de X, existe função $f \in \mathscr{C}_c(X, [0,1])$ que separa C e $A^{\complement}$.*

Paracompacidade

Definição 1.35. Um espaço topológico *paracompacto* é um espaço topológico $\boldsymbol{X}$ em que toda cobertura aberta $\mathcal{C}$ de $\boldsymbol{X}$ tem refinamento aberto localmente finito.

Compacidade Sequencial

1.4.3 Contabilidades

Base de Vizinhanças Contável (1º Contável)

Base Contável (2º Contável)

1.5 Homotopia e Grupo Fundamental

1.5.1 Homotopia

Definição 1.36. Sejam $\boldsymbol{X}$ e $\boldsymbol{X}'$ espaços topológicos e $f, f' \in \mathscr{C}(X, X')$ funções contínuas. Uma *homotopia* de f para f' é uma função contínua

$$\begin{aligned} H\colon [0,1] \times X &\longrightarrow X' \\ (t,x) &\longmapsto H^t(x) \end{aligned}$$

tal que $H^0 = f$ e $H^1 = f'$. As funções f e f' são *homotópicas* e denota-se $f \approx g$.

Proposição 1.69. *Sejam $\boldsymbol{X}$ e $\boldsymbol{X}'$ espaços topológicos. A relação de homotopia é uma equivalência no conjunto $\mathscr{C}(X, X')$ das funções contínuas de $\boldsymbol{X}$ para $\boldsymbol{X}'$.*

Demonstração.

1. (Reflexiviade) Seja $f \in \mathscr{C}(X, X')$. Consideremos a função

$$\begin{aligned} H\colon [0,1] \times X &\longrightarrow X' \\ (t,x) &\longmapsto f(x) \end{aligned}$$

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 $f, f' \in \mathscr{C}(X, X')$ tais que $f \approx f'$ e $H\colon [0,1] \times X \longrightarrow X'$ uma homotopia de f para f'. Consideremos a função

$$\begin{aligned} H'\colon [0,1] \times X &\longrightarrow X' \\ (t,x) &\longmapsto H^{1-t}(x). \end{aligned}$$

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 $f, f', f'' \in \mathscr{C}(X, X')$ tais que $f \approx f'$ e $f' \approx f''$ e $H\colon [0,1] \times X \longrightarrow X'$ uma homotopia de f para f' e $H'\colon [0,1] \times X \longrightarrow X'$ uma homotopia de f' para f''. Consideremos a função

$$\begin{aligned} H''\colon [0,1] \times X &\longrightarrow X' \\ (t,x) &\longmapsto \begin{cases} H^{2t}(x), & t \in \left[0, \frac{1}{2}\right] \\ H'^{2t-1}(x), & t \in \left[\frac{1}{2}, 1\right] \end{cases}. \end{aligned}$$

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 1.70. *Sejam $\boldsymbol{X}$, $\boldsymbol{X}'$ e $\boldsymbol{X}''$ espaços topológicos, $f, f' \in \mathscr{C}(X, X')$ e $g, g' \in \mathscr{C}(X', X'')$ funções contínuas tais que $f \approx f'$ e $g \approx g'$. Então*

$$(g \circ f) \approx (g' \circ f').$$

Demonstração. Sejam $H\colon [0,1] \times X \longrightarrow X'$ uma homotopia de f para f' e $H' : [0,1] \times X' \longrightarrow X''$ uma homotopia de g para g'. Consideremos a função

$$\begin{aligned} H''\colon [0,1] \times X &\longrightarrow X'' \\ (t, x) &\longmapsto H'^t \circ H^t(x). \end{aligned}$$

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 $g' \circ f'$. ■

1.5.2 Equivalência Homotópica

Definição 1.37. Sejam $\boldsymbol{X}$ e $\boldsymbol{X}'$ espaços topológicos. Uma *equivalência homotópica* entre $\boldsymbol{X}$ e $\boldsymbol{X}'$ é uma par $(f, f') \in \mathscr{C}(X, X') \times \mathscr{C}(X', X)$ de funções contínuas tais que $f' \circ f \approx \mathrm{I}_X$ e $f \circ f' \approx \mathrm{I}_{X'}$. Os espaços $\boldsymbol{X}$ e $\boldsymbol{X}'$ são *homotopicamente equivalentes* e denota-se $X \approx X'$.

1.5.3 Caminhos e Laços

Definição 1.38 (Caminho e laço)**.** Seja $\boldsymbol{X}$ um espaço topológico. Um *caminho* em X é uma função contínua $c\colon [0,1] \longrightarrow X$. Um *laço* em X é uma função contínua $\ell : \mathbb{S}^1 \longrightarrow X$ 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 1.39. Seja X um espaço métrico e $c : [0,1] \longrightarrow X$ um caminho em X. O *caminho inverso* de c é o caminho

$$\begin{aligned} c^{-1} : [0,1] &\longrightarrow X \\ s &\longmapsto c(1-s). \end{aligned}$$

Definição 1.40. 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 1.41. 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

$$\begin{aligned} (c_1 \cdot c_2) : [0,1] &\longrightarrow X \\ s &\longmapsto \begin{cases} c_1(2s) & \text{se } 0 \leq s \leq \frac{1}{2} \\ c_2(2s-1) & \text{se } \frac{1}{2} \leq s \leq 1. \end{cases} \end{aligned}$$

1.5.4 Homotopia de Caminhos

Definição 1.42. 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 1.1: Ilustração de uma homotopia de caminhos.

Proposição 1.71. *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. Reflexiviade: $l_1 \approx l_1$.
   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 $t \in [0,1]$, $H(0,t) = H(1,t) = l(0)$, 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 $H : S^1 \times [0,1] \longrightarrow X$ uma homotopia de laços entre l_1 e l_2. Então consideremos a função

$$\begin{aligned} H' : S^1 \times [0,1] &\longrightarrow X \\ (x,t) &\longmapsto H(x, 1-t). \end{aligned}$$

Sabemos que H é uma homotopia entre l_2 e l_1. Basta notar que, para todo $t \in [0,1]$, $H'(0,t) = H(0,1-t) = l(0) = H(1,1-t) = H'(1,t)$, 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 $H_1 : S^1 \times [0,1] \longrightarrow X$ uma homotopia entre l_1 e l_2 e $H_2 : S^1 \times [0,1] \longrightarrow X$ uma homotopia entre l_2 e l_3. Então consideremos a função

$$\begin{aligned} H : S^1 \times [0,1] &\longrightarrow X \\ (x,t) &\longmapsto \begin{cases} H_1(x, 2t) & \text{se } 0 \leq t \leq \frac{1}{2} \\ H_2(x, 2t-1) & \text{se } \frac{1}{2} \leq t \leq 1. \end{cases} \end{aligned}$$

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 1.72. *Seja X um espaço métrico e $c_1, c_2, c_3 : [0,1] \longrightarrow X$ 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 $\phi : [0,1] \longrightarrow [0,1]$

$$\phi(s) = \begin{cases} 2s & \text{se } s \in [0, \frac{1}{4}] \\ s + \frac{1}{4} & \text{se } s \in [\frac{1}{4}, \frac{1}{2}] \\ \frac{s}{2} + \frac{1}{2} & \text{se } s \in [\frac{1}{2}, 1]. \end{cases}$$

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

$$\begin{aligned} H : [0,1] \times [0,1] &\longrightarrow X \\ (s,t) &\longmapsto (c_1 \cdot c_2) \cdot c_3((1-t)s + t\phi(s)). \end{aligned}$$

Analogamente aos itens anteriorrs, mostra-se que H é homotopia de caminhos.

■

Proposição 1.73. *Sejam X um espaço métrico, $x_0 \in X$ e $c_1, c_2, c_1', c_2' : [0,1] \longrightarrow X$ 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

$$\begin{aligned} H : [0,1] \times [0,1] &\longrightarrow X \\ (s,t) &\longmapsto \begin{cases} H_1(2s,t) & \text{se } 0 \leq s \leq \frac{1}{2} \\ H_2(2s-1,t) & \text{se } \frac{1}{2} \leq s \leq 1. \end{cases} \end{aligned}$$

Primeiro, notemos que H é uma homotopia entre c_1 e c_2. Pa 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 $(c_1')^{-1}$.

■

1.5.5 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 1.43. 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 1.44. 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 1.73.

Teorema 1.74. *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 1.72 e 1.73. ■

1.6 Topologia de Ordem

Lembremos que, se $(X, \leq)$ é um conjunto (totalmente) ordenado e $e, e' \in X$, o intervalo aberto de extremos inferior e e superior e' é o conjunto

$$]e, e'[= \{x \in X \mid e < x < e'\}.$$

As semirretas abertas são os intervalos

$$]e, \infty[:= \{x \in X \mid e < x\}$$

e

$$]-\infty, e[:= \{x \in X \mid x < e\}.$$

Definição 1.45. Seja $(X, \leq)$ um conjunto ordenado. A *topologia de ordem* sobre X é a topologia gerada pelas semirretas abertas de $(X, \leq)$. Denotamos essa topologia por $\mathcal{T}_{\leq}$ (ou simplesmente $\mathcal{T}$ se for claro pelo contexto).

Proposição 1.75. *Seja $(X, \leq)$ um conjunto ordenado. O par $(X, \mathcal{T}_{\leq})$ é um espaço topológico hereditariamente normal com base de intervalos abertos.*

1.6.1 Topologia de um Corpo Ordenado

Lembremos que, se $(X, \leq)$ é um espaço ordenado, a topologia $\mathcal{T}_{\leq}$ induzida por $\leq$ é a topologia gerada pelas semirretas abertas $]x, \infty[$ e $]\infty, x[$, e o conjunto de intervalos abertos $]x, x'[$ é uma base de $\mathcal{T}_{\leq}$.

Note que

$$\bigcup_{i \in I}]e_i, e_i'[= \left]\inf_{i \in I} e_i, \sup_{i \in I} e_i'\right[$$
$$\bigcap_{i \in I} [e_i, e_i'] = \left[\sup_{i \in I} e_i, \inf_{i \in I} e_i'\right].$$

Proposição 1.76. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. O par $(\boldsymbol{C}, \mathcal{T}_{\leq})$ é um corpo topológico.*

Demonstração. Precisamos mostrar que $+$, $-$, $\times$ e $^{-1}$ são contínuas. Para isso, basta mostrar que elas puxam abertos geradores para abertos. Seja $e \in C$ e consideremos as semirretas $]e, \infty[$ e $]-\infty, e[$. Para mostrar que $+$ é contínua, notamos que, se $c + c' > e$, então $c' > e - c$, logo

$$+^{-1}\big(]e, \infty[\big) = \bigcup_{c \in C} \big(]c, \infty[\times]e - c, \infty[\big)$$

e, analogamente,

$$+^{-1}\Big(\,]-\infty, e[\,\Big) = \bigcup_{c\in C}\Big(\,]-\infty, c[\,\times\,]-\infty, e-c[\,\Big),$$

que são abertos pois são uniões de abertos, o que implica que $+$ é contínua. Para mostrar que $-$ é contínua, notamos que

$$-^{-1}\Big(\,]e, \infty[\,\Big) = \,]-\infty, -e[$$

e

$$-^{-1}(]-\infty, e[) = \,]-e, \infty[\,,$$

que são ambos abertos, o que mostra que $-$ é contínua.

Para mostrar que $\times$ é contínua, consideramos dois casos.

(1) Se $e = 0$ e $c \times c' > e = 0$, então $c \neq 0$, logo se $c > 0$ então $c' > 0$ e, se $c < 0$, então $c' < 0$, logo

$$\times^{-1}\Big(\,]0, \infty[\,\Big) = \Big(\,]0, \infty[\,\times\,]0, \infty[\,\Big) \cup \Big(\,]-\infty, 0[\,\times\,]-\infty, 0[\,\Big)$$

e, analogamente,

$$\times^{-1}\Big(\,]-\infty, 0[\,\Big) = \Big(\,]0, \infty[\,\times\,]-\infty, 0[\,\Big) \cup \Big(\,]-\infty, 0[\,\times\,]0, \infty[\,\Big),$$

que são ambos abertos; o caso (2) em que $e \neq 0$ é análogo, embora um pouco mais trabalhoso. Isso mostra que $\times$ é contínua. Mostrar que $^{-1}$ é contínua também é trabalhoso, mas segue direto de modo análogo. ■

Proposição 1.77. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. O grupo topológico $(\boldsymbol{C}, \mathcal{T}_{\leq})$ é separado.*

Demonstração. Sejam $c, c' \in C$ tais que $c \neq c'$. Então $c < c'$ ou $c' < c$. Sem perda de generalidade, considere que $c < c'$. Então as vizinhanças

$$\left]-\infty, \frac{c+c'}{2}\right[\qquad \text{e} \qquad \left]\frac{c+c'}{2}, \infty\right[$$

de c e c', respectivamente, separam c e c'. ■

Consideremos em $C_{\geq 0}$ a topologia induzida.

Proposição 1.78. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. As funções valor absoluto $|\cdot| : C \longrightarrow C_{\geq 0}$ e distância $|\cdot,\cdot| : C \times C \longrightarrow C_{\geq 0}$ são contínuas.*

Demonstração. (Valor absoluto) Seja $c \in C_{\geq 0}$ e consideremos os abertos $]c, \infty[$ e $[0, c[$. Então

$$|\cdot|^{-1}\Big(]c, \infty[\Big) =]-\infty, -c[\cup]c, \infty[$$

e

$$|\cdot|^{-1}\Big([0, c[\Big) =]-c, 0] \cup [0, c[=]-c, c[\,,$$

que são ambos abertos, o que mostra que $|\cdot|$ é contínua.

(Distância) Como $|\cdot, \cdot|$ é composição de $|\cdot|$, $+$, $-$, p_0 e p_1, que são todas contínuas, segue que ela é contínua. ■

Proposição 1.79. *Seja $(\boldsymbol{C}, \leq)$ um corpo ordenado. O corpo $\boldsymbol{C}$ é não-infinitesimal se, e somente se, $\mathbb{Q}_C$ é denso em C.*

Capítulo 2

Espaços Métricos

2.1 Os Espaços Métricos

2.1.1 Métricas

Definição 2.1. Seja M um conjunto. Uma *métrica* sobre M é uma função

$$|\cdot,\cdot| : M \times M \longrightarrow [0,\infty[$$

que satisfaz

1. (Separação) Para todos $p, p' \in M$,

$$|p,p'| = 0 \quad \Longleftrightarrow \quad p = p';$$

2. (Simetria) Para todos $p, p' \in M$

$$|p,p'| = |p',p|\,;$$

3. (Desigualdade Triangular) Para todos $p, p', p'' \in M$,

$$|p,p''| \leq |p,p'| + |p',p''|\,.$$

A *distância* entre p e p' é o número real $|p,p'|$.

Na definição, enunciamos 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 2.2. Um *espaço métrico* é um par $\boldsymbol{M} = (M,d)$ em que M é um conjunto e d é uma métrica em M. Os elementos de M são *pontos*. Um *subespaço métrico* de $\boldsymbol{M}$ é o par $\boldsymbol{S} = (S, d|_{S\times S})$.

Proposição 2.1. *Seja* $\boldsymbol{M}$ *um espaço métrico. Então*

1. *(Positividade) Para todos* $p, p' \in M$, $d(p, p') \geq 0$.
2. *(Desigualdade Triangular Generalizada) Para todos* $p_0, \ldots, p_n \in M$,

$$d(p_0, p_n) \leq \mathop{\mathbin{+}}_{i=1}^{n-1} d(p_i, p_{i+1})$$

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 $\mathop{\mathbin{+}}_{i=1}^{0} d(p_i, p_{i+1}) = 0$, pois a soma é vazia. Para $n = 2$, sejam $p_1, p_2 \in M$; então $d(p_1, p_2)$ e $\mathop{\mathbin{+}}_{i=1}^{1} d(p_i, p_{i+1}) = d(p_1, p_2)$, e vale a propriedade. Para $n = 3$, sejam $p_1, p_2, p_3 \in M$; então a propriedade é a desigualdade triangulal. Agora, sejam $n \geq 4$, $p_1, \ldots, p_n \in M$ e assumamos que a propriedade vale para todo $k \in \mathbb{N}$, tal que $3 \leq k \leq n - 1$. Então

$$d(p_1, p_n) \leq \mathop{\mathbin{+}}_{i=1}^{n-3} d(p_i, p_{i+1}) + d(p_{n-2}, p_n),$$

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,

$$\begin{aligned} d(p_1, p_n) &\leq \mathop{\mathbin{+}}_{i=1}^{n-3} d(p_i, p_{i+1}) + d(p_{n-2}, p_n) \\ &\leq \mathop{\mathbin{+}}_{i=1}^{n-3} d(p_i, p_{i+1}) + d(p_{n-2}, p_{n-1}) + d(p_{n-1}, p_n) \\ &= \mathop{\mathbin{+}}_{i=1}^{n-1} d(p_i, p_{i+1}). \end{aligned}$$

■

Alguns exemplos de métricas seguem.

Proposição 2.2. *Seja* M *um conjunto.*

1. *A* métrica discreta

$$\begin{aligned} d\colon M \times M &\longrightarrow [0, \infty[\\ (p, p') &\longmapsto \begin{cases} 0, & p = p' \\ 1, & p \neq p' \end{cases} \end{aligned}$$

é uma métrica sobre M.

Mostramos agora que podem-se definir distâncias a partir de distâncias já conhecidas no espaço.

Proposição 2.3. *Sejam M um conjunto e $d_0, \ldots, d_{n-1}$ métricas em M. Então a função*

$$\begin{aligned} d\colon M \times M &\longrightarrow \mathbb{R} \\ (p, p') &\longmapsto \mathop{\mathbin{+}}_{i=0}^{n-1} d_i(p, p') \end{aligned}$$

é uma métrica sobre M.

Demonstração. 1. (Separação) Sejam $p, p' \in M$. Suponhamos que

$$d(p, p') = \mathop{\mathbin{+}}_{i=0}^{n} d_i(p, p') = 0.$$

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

$$d(p, p') = \mathop{\mathbin{+}}_{i=0}^{n-1} 0 = 0.$$

2. (Simetria) Sejam $p, p' \in M$. Então, pela simetria de d_i para todo $i \in [n]$,

$$d(p, p') = \mathop{\mathbin{+}}_{i=0}^{n-1} d_i(p, p') = \mathop{\mathbin{+}}_{i=1}^{n-1} d_i(p, p') = d(p, p').$$

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

$$\begin{aligned} d(p,p'') &= \mathop{\mathbin{+}}_{i=0}^{n-1} d_i(p,p'') \\ &\leq \mathop{\mathbin{+}}_{i=0}^{n-1} (d_i(p,p') + d_i(p',p'')) \\ &= \mathop{\mathbin{+}}_{i=0}^{n-1} d_i(p,p') + \mathop{\mathbin{+}}_{i=0}^{n-1} d_i(p',p'') \\ &= d(p,p') + d(p',p''). \end{aligned}$$

■

Proposição 2.4. *Sejam M um conjunto não vazio e $d_0, \ldots, d_{n-1}$ métricas em M. Então a função*

$$\begin{aligned} d\colon M \times M &\longrightarrow \mathbb{R} \\ (p,p') &\longmapsto \max\{d_i(p,p') \mid i \in [n]\} \end{aligned}$$

é uma métrica sobre 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 segudo caso, segue que

$$d(p,p'') = d_2(p,p'') \leq d_2(p,p') + d_2(p',p'') \leq d(p,p') + d(p',p''). \qquad ■$$

▶ **Exercício 2.1** (Métrica Limitada)**.** Seja (M, d) um espaço métrico. A função

$$\begin{aligned} d \wedge 1 \colon M \times M &\longrightarrow \mathbb{R} \\ (p, p') &\longmapsto \min\{d(x, y), 1\} \end{aligned}$$

é uma métrica sobre M, a *métrica limitada induzida por* d.

▶ **Exercício 2.2** (Métricas p)**.** Sejam $\boldsymbol{M}$ e $\boldsymbol{M'}$ espaços métricos e $p \in [1, \infty[$. A função

$$\begin{aligned} (d^p + d'^p)^{\frac{1}{p}} \colon (M \times M') \times (M \times M') &\longrightarrow \mathbb{R} \\ ((x, x'), (y, y')) &\longmapsto (d(p, q)^p + d'(p', q')^p)^{\frac{1}{p}} \end{aligned}$$

é uma métrica sobre $M \times M'$.

Definição 2.3. Seja $d \in \mathbb{N}$. A *métrica reta* sobre $\mathbb{R}^d$ é a função

$$\begin{aligned} |\cdot, \cdot|_{\mathbb{R}^d} \colon \mathbb{R}^d &\longrightarrow \mathbb{R}^d \\ (x, x') &\longmapsto \left(\mathop{+}_{i \in [d]} |x_i - x'_i|^2 \right)^{\frac{1}{2}}. \end{aligned}$$

2.1.2 Diâmetro, Bolas e Conjuntos e Funções Limitadas

Definição 2.4. Sejam $\boldsymbol{M}$ 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* $\boldsymbol{M}$ 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

$$\begin{aligned} \varnothing \colon \mathsf{P}(M) &\longrightarrow [0, \infty] \\ C &\longmapsto \varnothing(C). \end{aligned}$$

Definição 2.5. Sejam $\boldsymbol{M}$ 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

$$\mathrm{B}_r(c) := \{p \in M \mid |c, p| < r\}.$$

A *bola fechada* de centro c e raio r em M é o conjunto

$$\overline{\mathrm{B}}_r(c) := \{p \in M \mid |c, p| \leq r\}.$$

Figura 2.1: Bolas aberta e fechada de centro c e raio r, respectivamente.

Proposição 2.5. *Sejam $\boldsymbol{M}$ um espaço métrico e $C \subseteq M$ um conjunto. Então C é um conjunto limitado se, e somente se, existe bola $\overline{\mathrm{B}}_r(c)$ tal que $C \subseteq \overline{\mathrm{B}}_r(c)$.*

Demonstração. Se C é limitado, basta tomar $r = \varnothing(C)$ e $c \in C$. Reciprocamente, se existe bola $\overline{\mathrm{B}}_r(c)$ tal que $C \subseteq \overline{\mathrm{B}}_r(c)$, 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 $\varnothing(C) \leq 2r \in [0, \infty[$. ■

▶ **Exercício 2.3.** Seja $\boldsymbol{M}$ um espaço métrico.

1. Para todos $C, C' \subseteq M$ tais que $C \subseteq C'$,
$$\varnothing(C) \leq \varnothing(C').$$
2. Para todos $C, C' \subseteq M$,
$$\varnothing(C \cup C') = \max\{\varnothing(C), \varnothing(C'), \sup\{|p, p'| \mid p \in C, p' \in C'\}\}.$$
3. Para todos $C, C' \subseteq M$,
$$\varnothing(C \cup C') \leq \min\{\varnothing(C), \varnothing(C')\};$$
4. Para todo $r \in [0, \infty[$ e todo $p \in M$.
$$\varnothing(\mathrm{B}_r(p)) \leq 2r.$$

Note que o diâmetro da bola de raio r não necessariamente é $2r$, por exemplo para $r = 2$ na métrica discreta.

▶ **Exercício 2.4.** Sejam M um conjunto, d uma métrica em M e $d \wedge 1$ a métrica limitada sobre M. Todo subconjunto de M é limitado com respeito a $d \wedge 1$.

Definição 2.6. Seja $\boldsymbol{M}$ um espaço métrico. Uma função *limitada* em $\boldsymbol{M}$ é uma função $f\colon X \longrightarrow M$ de um conjunto X para M cuja imagem $f(X)$ é limitada.

2.2 Topologia dos Espaços Métricos

2.2.1 Interior e Pontos Interiores

Definição 2.7. Sejam $\boldsymbol{M}$ 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 $\mathrm{B}_r(p) \subseteq C$. O *interior* de C é o conjunto C° de todos pontos interiores de C. Um *conjunto aberto* de $\boldsymbol{M}$ é um conjunto $A \subseteq M$ tal que $A = A^\circ$. O conjunto dos conjuntos abertos de $\boldsymbol{M}$ é denotado $\mathcal{T}_{\boldsymbol{M}}$.

Proposição 2.6. *Seja $\boldsymbol{M} = (M, d)$ um espaço métrico. Então*

1. *Para todo $c \in M$ e para todo número real $r > 0$, a bola aberta $\mathrm{B}_r(c)$ é um conjunto aberto;*

2. *O conjunto $\mathcal{T}_{\boldsymbol{M}}$ é uma topologia de M.*

Demonstração. 1. Sejam $c \in M$ e $r \in \,]0, \infty[$. Queremos mostrar que $\mathrm{B}_r(c)$ é aberto. Para isso, seja $p \in \mathrm{B}_r(c)$. 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 $p' \in \mathrm{B}_{r-d}(p)$. 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 $p' \in \mathrm{B}_r(c)$ e que, portanto, $\mathrm{B}_s(p) \subseteq \mathrm{B}_r(c)$. Assim, mostramos que $\mathrm{B}_r(p)$ 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 $\mathrm{B}_r(p) \subseteq A$, o que é absurdo. Para mostrar que M é aberto, sejam $p \in M$ e $r \in \,]0, \infty[$. Então $\mathrm{B}_r(p) \subseteq M$, pois qualquer bola aberta é subconjunto de M. Portanto M é aberto.

   (b) Seja $(A_i)_{i \in I}$ uma família de abertos em $\boldsymbol{M}$ 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 $\mathrm{B}_r(p) \subseteq A_k$. Como $A_k \subseteq (A_i)_{i \in I}$, segue que $\mathrm{B}_r(p) \subseteq (A_i)_{i \in I}$ e que, portanto, $(A_i)_{i \in I}$ é aberto.

   (c) Seja $(A_i)_{i \in [n]}$ uma sequência de abertos em $\boldsymbol{M}$ 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 $\mathrm{B}_{r_k}(p) \subseteq A_k$, Seja $r := \min\{r_k : k \in [n]\}$. Então, para todo $k \in [n]$, vale $\mathrm{B}_r(p) \subseteq \mathrm{B}_{r_k}(p)$, e segue que $\mathrm{B}_r(p) \subseteq A_k$ e, portanto, $\mathrm{B}_r(p) \subseteq (A_i)_{i \in [n]}$, o que mostra que $(A_i)_{i \in [n]}$ é aberto.

■

► **Exercício 2.5.** Sejam M um conjunto e d uma métrica em M. A métrica limitada $d \wedge 1$ sobre M induz a mesma topologia que d sobre M.

2.2.2 Limites e Convergência de Sequências

Definição 2.8. Sejam $\boldsymbol{M}$ 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

$$\bigwedge n \in \mathbb{N} \qquad n \geq N \Rightarrow p_n \in \mathrm{B}_\varepsilon(p).$$

Denota-se $(p_n)_{n\in\mathbb{N}} \to p$. 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 2.7. *Todo espaço métrico $\boldsymbol{M}$ 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 $\mathrm{B}_r(p) \cap \mathrm{B}_r(p') = \emptyset$. 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 $p'' \in \mathrm{B}_r(p) \cap \mathrm{B}_r(p')$. 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 $\mathrm{B}_r(p) \cap \mathrm{B}_r(p') = \emptyset$. ■

Corolário 2.8. *Toda sequência convergente em um espaço métrico $\boldsymbol{M}$ 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 $p_n \in \mathrm{B}_\varepsilon(p)$, e existe $N_2 \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, se $n \geq N_2$, então $p_n \in \mathrm{B}_\varepsilon(p')$. 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 $p_n \in \mathrm{B}_\varepsilon(p)$ e $p_n \in \mathrm{B}_\varepsilon(p')$; ou seja, $p_n \in \mathrm{B}_\varepsilon(p) \cap \mathrm{B}_\varepsilon(p')$, mas isso é absurdo, pois $\mathrm{B}_\varepsilon(p) \cap \mathrm{B}_\varepsilon(p') = \emptyset$. Portanto $p = p'$. ■

Essa proposição nos permite tratar o limite de uma sequência como um número único e, por isso, podemos usar a notação $\lim\limits_{n\in\mathbb{N}} p_n = p$ para quando $(p_n)_{n\in\mathbb{N}} \to p$.

Proposição 2.9. *Uma sequência de em um espaço métrico $\boldsymbol{M}$ é convergente se, e somente se, todas suas subsequências são convergentes.*

Demonstração. Suponhamos que $(p_n) \to p$ 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 $(p_n) \to p$, existe $N \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, se $n \geq N$, então $p_n \in \mathrm{B}_\varepsilon(p)$; 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

$$k \geq K \Rightarrow n_k \geq N \Rightarrow p_{n_k} \in \mathrm{B}_\varepsilon(p)$$

e, portanto, $(p_{n_k}) \longrightarrow p$. 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, $(p_n) \to p$. ■

Proposição 2.10. *Toda sequência convergente em um espaço métrico* $\boldsymbol{M}$ *é limitada.*

Demonstração. Seja $(p_n)_{n\in\mathbb{N}}$ uma sequência de pontos em M tal que $(p_n) \to p$. Então, para $\varepsilon = 1$, existe $N \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, se $n \geq N$, então $p_n \in \mathrm{B}_1(p)$. Assim, seja $l \in \mathbb{R}$ tal que

$$l > \max(\{1\} \cup \{d(p, p_n) : n \in [N]\}),$$

seque que, para todo $n \in \mathbb{N}$, $p_n \in \mathrm{B}_l(p)$ pois, se $0 \leq n \leq N$, $d(p, p_n) < l$ pela definição de l e, se $n \geq N$, então $p_n \in \mathrm{B}_1(p) \subseteq B_l(p)$, pois $1 < l$. Logo $(p_n)_{n\in\mathbb{N}}$ é limitada. ■

Proposição 2.11. *Sejam* $\boldsymbol{M}$ *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* $\varepsilon > 0$*,* $C \cap \mathrm{B}_\varepsilon(p) \neq \emptyset$*.*

Demonstração. Suponhamos que exista uma sequência $(p_n)_{n\in\mathbb{N}}$ de pontos em C tal que $(p_n) \to p$. 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 $p_n \in \mathrm{B}_\varepsilon(p)$. Mas isso implica que $p_n \in C \cap \mathrm{B}_\varepsilon(p)$. Reciprocamente, suponhamos que, para todo número real $\varepsilon > 0$, $C \cap \mathrm{B}_\varepsilon(p) \neq \emptyset$. Então, em particular, para todo $n \in \mathbb{N}$, escolhamos $p_n \in C \cap \mathrm{B}_{\frac{1}{n}}(p)$. Assim, temos a sequência $(p_n)_{n\in\mathbb{N}}$. Para mostrar que $(p_n) \to p$, 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, $(p_n) \to p$. ■

Proposição 2.12. *Sejam* $\boldsymbol{M}$ *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

$$\bigwedge n \in \mathbb{N} \qquad n \geq N_1 \Rightarrow d(p, p_n) < \tfrac{\varepsilon}{2}$$

e

$$\bigwedge n \in \mathbb{N} \qquad n \geq N_2 \Rightarrow d(q, q_n) < \tfrac{\varepsilon}{2}.$$

Fazendo $N_3 := \max\{N_1, N_2\}$, segue que

$$\bigwedge n \in \mathbb{N} \qquad n \geq N_3 \Rightarrow d(p_n, q_n) \leq d(p_n, p) + d(p, q) + d(q, q_n) < d(p, q) + \varepsilon;$$

ou seja, $d(p_n, q_n) - d(p, q) < \varepsilon$. Analogamente, achamos $N_6 \in \mathbb{N}$ tal que

$$\bigwedge n \in \mathbb{N} \qquad n \geq N_3 \Rightarrow d(p_n, q_n) \leq d(p_n, p) + d(p, q) + d(q, q_n) < d(p, q) + \varepsilon$$

e fazendo $n := \max\{N_3, N_6\}$, segue que

$$\bigwedge n \in \mathbb{N} \qquad n \geq N \Rightarrow |d(p, q) - d(p_n, q_n)| < \varepsilon,$$

o que mostra que $(d(p_n, q_n)) \to d(p, q)$ em $\mathbb{R}$.

■

2.2.3 Fecho e Pontos Aderentes

Definição 2.9. Sejam $\boldsymbol{M}$ 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 $\boldsymbol{M}$ é um conjunto $F \subseteq M$ tal que $F = \overline{F}$.

Proposição 2.13. *Sejam $\boldsymbol{M}$ um espaço métrico e $F \subseteq M$. Então F é um conjunto fechado se, e somente se, $F^{\complement}$ é um conjunto aberto.*

Demonstração. Suponhamos que F é um conjunto fechado. Se $F^{\complement} = \emptyset$, Mas $\emptyset$ é aberto pois, caso contrário, existe $p \in \emptyset$ para o qual não há número real $\varepsilon > 0$ tal que $\mathrm{B}_\varepsilon(p) \subseteq \emptyset$, mas isso é absurdo. Se $F^{\complement} \neq \emptyset$, seja $p \in F^{\complement}$. Se não existe número real $\varepsilon > 0$ tal que $\mathrm{B}_\varepsilon(p) \subseteq F^{\complement}$, então, para todo número real $\varepsilon > 0$, $F \cap \mathrm{B}_\varepsilon(p) \neq \emptyset$. Mas isso implica que existe uma sequência $(p_n)_{n\in\mathbb{N}}$ de pontos em F tal que $(p_n) \to p$. Como F é fechado, isso implica $p \in F$, o que é uma contradição. Então existe número real $\varepsilon > 0$ tal que $\mathrm{B}_\varepsilon(p) \subseteq F^{\complement}$, e isso mostra que $F^{\complement}$ é aberto.

Reciprocamente, suponhamos que $F^{\complement}$ 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 $p \in F^{\complement}$ e, como $F^{\complement}$ é aberto, existe um número real $\varepsilon > 0$ tal que $\mathrm{B}_\varepsilon(p) \subseteq F^{\complement}$. Como $(p_n) \to p$, existe $N \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, se $n \geq N$, então $p_n \in \mathrm{B}_\varepsilon(p)$. Mas isso implica que $p_N \in \mathrm{B}_\varepsilon(p) \subseteq F^{\complement}$, o que é absurdo, pois $p_n \in F$. Portanto $p \in F$ e isso mostra que F é fechado. ■

Proposição 2.14. *Seja $\boldsymbol{M}$ um espaço métrico. Então, para todo $c \in M$ e para todo número real $r > 0$, a bola fechada $\bar{\mathrm{B}}_r(c)$ é um conjunto fechado.*

Demonstração. Basta notar que $\bar{\mathrm{B}}_r(c)^{\complement}$ é aberto. ■

2.2.4 Conjuntos Densos

Definição 2.10. Sejam $\boldsymbol{M}$ 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 2.15. *Sejam $\boldsymbol{M} = (M, d)$ 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 $\boldsymbol{M}$, $A \cap C \neq \emptyset$ implica $A \cap D \neq \emptyset$.*

Demonstração. Suponhamos que D é denso em C. Sejam A um conjunto aberto de $\boldsymbol{M}$ 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 $\mathrm{B}_\varepsilon(p) \subseteq A$. Então, como $(p_n) \to p$, existe um número natural N tal que, para todo natural $n \geq N$, $p_n \in \mathrm{B}_\varepsilon(p)$. Mas isso implica que $p_n \in A \cap D$.

Reciprocamente, suponhamos que, para todo conjunto aberto A de $\boldsymbol{M}$, $A \cap C \neq \emptyset$ 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 $\mathrm{B}_{\frac{1}{n}}(p)$ é um conjunto aberto que contém p. Mas então $\mathrm{B}_{\frac{1}{n}}(p) \cap C \neq \emptyset$, o que implica $\mathrm{B}_{\frac{1}{n}}(p) \cap D \neq \emptyset$. Para cada $n \in \mathbb{N}$, escolhamos $p_n \in B_{\frac{1}{n}}(p) \cap D$. 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

$$\bigwedge n \in \mathbb{N} \qquad n \geq N \Rightarrow \tfrac{1}{n} \leq \tfrac{1}{N} \leq \varepsilon \Rightarrow p_n \in \mathrm{B}_{\frac{1}{n}}(p) \subseteq \mathrm{B}_{\frac{1}{N}}(p) \subseteq \mathrm{B}_\varepsilon(p).$$

Isso mostra que $p \in \overline{D}$ e, portanto, que $C \subseteq \overline{D}$. ■

Proposição 2.16. *Sejam $\boldsymbol{M}_1$ e $\boldsymbol{M}_2$ espaços métricos e $f, g \colon M_1 \longrightarrow M_2$ 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

$$(f(p_n)) \to f(p) \ \text{ e } \ (g(p_n)) \to g(p).$$

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 2.17. *Sejam $\boldsymbol{M}_1$ e $\boldsymbol{M}_2$ espaços métricos, $f, g : M_1 \longrightarrow M_2$ 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 $f|_C = g|_C$. ■

2.2.5 Conjuntos Compactos

Proposição 2.18. *Sejam $\boldsymbol{M}$ um espaço métrico e $C \subseteq M$. Se C é compacto, então é limitado.*

Demonstração. Seja $p \in M$ e consideremos a cobertura $\{\mathrm{B}_r(p) \mid r \in]0, \infty[\}$ de C. Pela compacidade, existe subcobertura finita $\{\mathrm{B}_{r_0}(p), \ldots, \mathrm{B}_{r_{n-1}}(p)\}$ de C. Tomando $r := \max\{r_i \mid i \in [n]\}$, segue que $\mathrm{B}_{r_i}(p) \subseteq \mathrm{B}_r(p)$ para todo $i \in [n]$, logo $C \subseteq \mathrm{B}_r(p)$, 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 métrico[1].

2.2.6 Continuidade

Definição 2.11. Sejam $\boldsymbol{M}$ e $\boldsymbol{M}'$ espaços métricos e $p \in M$. Uma função *contínua em p* é uma função $f\colon M \longrightarrow M'$ que satisfaz: para todo $\varepsilon \in]0, \infty[$, existe $\delta\,]0, \infty[$ tal que, para todo $x \in M$

$$x \in \mathrm{B}_\delta(p) \Rightarrow f(x) \in \mathrm{B}_\varepsilon(f(p)).$$

Uma função *descontínua* em p é uma função que não é contínua em p.

[1]Para mais detalhes, conferir `https://math.stackexchange.com/questions/674982/difference-between-closed-bounded-and-compact-sets`.

Denotamos as bolas abertas em $\boldsymbol{M}$ e em $\boldsymbol{M}'$ por B, mas deve-se perceber que elas são relativas a métricas possivelmente diferentes.

Proposição 2.19. *Sejam $\boldsymbol{M}_1$ e $\boldsymbol{M}_2$ espaços métricos, $f : M_1 \longrightarrow M_2$ 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 $p_n \in \mathrm{B}_\delta(p)$ implica $f(p_n) \in \mathrm{B}_\varepsilon(f(p))$. Mas, como $(p_n) \to p$, existe $N \in \mathbb{N}$ tal que

$$\bigwedge n \in \mathbb{N} \qquad n \geq N \Rightarrow p_n \in \mathrm{B}_\delta(p) \Rightarrow f(p_n) \in \mathrm{B}_\varepsilon(f(p))$$

o que mostra que $(f(p_n)) \to f(p)$.

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 $x \in \mathrm{B}_\delta(p)$, mas $f(x) \notin \mathrm{B}_\varepsilon(f(p))$. 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 $f(p_n) \notin \mathrm{B}_\varepsilon(f(p))$. Seja $n \in \mathbb{N}$ e tomemos $\delta = \frac{1}{n}$. Então existe $x \in M_1$ tal que $x \in \mathrm{B}_{\frac{1}{n}}(p)$, mas $f(x) \notin \mathrm{B}_\varepsilon(f(p))$. 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

$$\bigwedge n \in \mathbb{N} \qquad n \geq N \Rightarrow \tfrac{1}{n} \leq \tfrac{1}{N} \leq \varepsilon' \Rightarrow p_n \in \mathrm{B}_{\frac{1}{n}}(p) \subseteq \mathrm{B}_{\frac{1}{N}}(p) \subseteq \mathrm{B}_{\varepsilon'}(p).$$

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, $f(p_N) \notin \mathrm{B}_\varepsilon(f(p))$ 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 2.12. Sejam $\boldsymbol{M}_1$ e $\boldsymbol{M}_2$ espaços métricos, $D \subseteq M_1$ e $f : D \longrightarrow M_2$ 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.

2.2.7 Ponto Limite e Conjunto Derivado

Definição 2.13. Sejam $\boldsymbol{M}$ 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 $C \smallsetminus \{p\}$ que converge para p. O *derivado* de C é o conjunto de todos os pontos limites de C.

Da definição, segue que $C' \subseteq \overline{C}$. A inclusão contrária caracteriza a seção a seguir.

Definição 2.14. Sejam $\boldsymbol{M}$ 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 $p \in \overline{C} \smallsetminus C'$.

2.2.8 Distância e Bolas de Conjuntos e Separação Métrica

Definição 2.15. Sejam $\boldsymbol{M}$ um espaço métrico e $C, C' \subseteq M$. A *distância* entre C e C' é

$$|C, C'| := \inf \{|c, c'| \mid c \in C, c' \in C'\}.$$

Para todo $p \in M$, denotam-se $|C, p| := |C, \{p\}|$ e $|p, C| := |\{p\}, C|$.

Essa definição, em particular, estabelece a distância de pontos para conjuntos também. Existem outras definições de distâncias entre conjuntos, mas elas não serão tratadas aqui.

Definição 2.16. Sejam $\boldsymbol{M}$ um espaço métrico e $C \subseteq M$ e $r \in \,]0, \infty[$. A *r-vizinhança* de C é o conjunto

$$\mathrm{B}_r(C) := \{p \in M \mid |C, p| < r\}.$$

A *r-vizinhança fechada* de C é o conjunto

$$\overline{\mathrm{B}}_r(C) := \{p \in M \mid |C, p| \leq r\}.$$

Note que excluímos $r = 0$ da definição pois basicamente teríamos $\mathrm{B}_0(C) = \emptyset$ e $\overline{\mathrm{B}}_0(C) = \overline{C}$.

► **Exercício 2.6.** Sejam $\boldsymbol{M}$ um espaço métrico e $C \subseteq M$ e $r \in \,]0, \infty[$.

1. A vizinhança $\mathrm{B}_r(C)$ é um conjunto aberto e

$$\mathrm{B}_r(C) = \bigcup_{c\in C} \mathrm{B}_r(c);$$

2. Para todo $r' \in]0, \infty[$ tais que $r \leq r'$,
$$C \subseteq \mathrm{B}_r(C) \subseteq \mathrm{B}_{r'}(C);$$
3. A vizinhança fechada $\overline{\mathrm{B}}_r(C)$ é um conjunto fechado e
$$\overline{\mathrm{B}}_r(C) \supseteq \bigcup_{c \in C} \overline{\mathrm{B}}_r(c);$$
4. Para todo $r' \in]0, \infty[$ tais que $r \leq r'$,
$$\overline{C} \subseteq \overline{\mathrm{B}}_r(C) \subseteq \overline{\mathrm{B}}_{r'}(C);$$
5. Para $r \in]0, \infty[$,
$$\overline{\mathrm{B}}_r(C) = \overline{\mathrm{B}_r(C)}$$

Demonstração. 1. Primeiro, mostramos a igualdade dos conjuntos. ($\supseteq$) Seja $p \in \bigcup_{c \in C} \mathrm{B}_r(c)$. Então existe $c \in C$ tal que $|c, p| < r$, o que implica que
$$|C, p| = \inf \{|c, p| \mid c \in C\} \leq |c, p| < r,$$
logo $p \in \mathrm{B}_r(C)$.

($\subseteq$) Seja $p \in \mathrm{B}_r(C)$. Então
$$|C, p| = \inf \{|c, p| \mid c \in C\} < r.$$
Isso significa que existe sequência $(c_n)_{n \in \mathbb{N}}$ em C tal que $\lim_{n \to \infty} |c, p| < r$, o que implica existe $n \in \mathbb{N}$ tal que $|c_n, p| < r$, logo $p \in \bigcup_{c \in C} \mathrm{B}_r(c)$.

Como as bolas $\mathrm{B}_r(c)$ são abertas, segue que $\mathrm{B}_r(C) = \bigcup_{c \in C} \mathrm{B}_r(c)$ é aberto. ■

Definição 2.17. Seja $\boldsymbol{M}$ um espaço métrico. Conjuntos *metricamente separados* são conjuntos $C, C' \subseteq M$ tais que
$$|C, C'| > 0.$$

Proposição 2.20. *Sejam $\boldsymbol{M}$ um espaço métrico e $C, C' \subseteq M$ conjuntos metricamente separados. Então C e C' são separados por vizinhanças.*

Demonstração. Seja $\delta := |C, C'|$. Pela separação métrica, $\delta > 0$. Então $C \subseteq \mathrm{B}_{\frac{\delta}{2}}(C)$ e $C' \subseteq \mathrm{B}_{\frac{\delta}{2}}(C')$ e $\mathrm{B}_{\frac{\delta}{2}}(C) \cap \mathrm{B}_{\frac{\delta}{2}}(C') = \emptyset$, já que, se existe $p \in \mathrm{B}_{\frac{\delta}{2}}(C) \cap \mathrm{B}_{\frac{\delta}{2}}(C')$, então existem $c \in C$ e $c' \in C'$ tais que $|c, p| < \frac{\delta}{2}$ e $|c', p| < \frac{\delta}{2}$, portanto
$$|c, c'| \leq |c, p| + |c', p| < \frac{\delta}{2} + \frac{\delta}{2} = \delta,$$
o que implica que $|C, C'| < \delta$, contradição. ■

Isso implica, em particular, que conjuntos metricamente separados são, além de separados por vizinhanças, separados, disjuntos e, claro, distintos.

Proposição 2.21. *Todo espaço métrico* $\boldsymbol{M}$ *é um espaço topológico normal.*

Demonstração. Sejam $F, F' \subseteq M$ fechados disjuntos. Mostraremos que F e F' são separados por vizinhanças, o que mostrará que o espaço é normal.

Para todo $f \in F$, existe $\delta_f \in]0, infty[$ tal que

$$\mathrm{B}_{\delta_f}(f) \cap F' = \emptyset,$$

pois F' é fechado e $f \notin F'$. Definimos

$$V := \bigcup_{f \in F} \mathrm{B}_{\frac{\delta_f}{2}}(f).$$

Esse conjunto é uma vizinhança aberta de F. Analogamente, definimos V' uma vizinhança aberta de F'. Claramente $V \cap V' =$, pois caso contrário, se existe $p \in V \cap V'$, então existem $f \in F$e $f' \in F'$ tais que

$$p \in \mathrm{B}_{\frac{\delta_f}{2}}(f) \cap \mathrm{B}_{\frac{\delta_{f'}}{2}}(f'),$$

portanto se $\delta_f \leq \delta_{f'}$, então $f \in \mathrm{B}_{\frac{\delta_{f'}}{2}}(f')$ e, se $\delta_{f'} \leq \delta_f$, então $f' \in \mathrm{B}_{\frac{\delta_f}{2}}(f)$, ambos contradições. ■

2.3 Estrutura Uniforme

2.3.1 Sequências Aproximantes

Definição 2.18. Seja $\boldsymbol{M}$ um espaço métrico. Uma sequência *aproximante* em $\boldsymbol{M}$ 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

$$\bigwedge n, m \in \mathbb{N} \qquad n, m \geq N \Rightarrow d(p_n, p_m) < \varepsilon.$$

Essa 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 2.22. *Toda sequência convergente em um espaço métrico* $\boldsymbol{M}$ *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 $n \geq N$, $p_n \in \mathrm{B}_{\frac{1}{2}\varepsilon}(p)$. Assim, segue que

$$\bigwedge n, m \in \mathbb{N} \qquad n, m \geq N \Rightarrow d(p_n, p_m) \leq d(p_n, p) + d(p, p_m) < \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon,$$

o que mostra que $(p_n)_{n\in\mathbb{N}}$ é uma sequência aproximante. ■

Proposição 2.23. *Toda sequência aproximante em um espaço métrico $\boldsymbol{M}$ 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

$$\bigwedge n, m \in \mathbb{N} \qquad n, m \geq N \Rightarrow d(p_n, p_m) < \tfrac{\varepsilon}{2}.$$

Como $(p_{n_k})_{k\in\mathbb{N}}$ é uma subsequência convergente, existe $K_1 \in \mathbb{N}$ tal que

$$\bigwedge k \in \mathbb{N} \qquad k \geq K_1 \Rightarrow d(p, p_{n_k}) < \tfrac{\varepsilon}{2}.$$

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

$$\bigwedge n \in \mathbb{N} \qquad n \geq N \Rightarrow d(p_n, p) \leq d(p_n, p_{n_k}) + d(p_{n_k}, p) < \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon.$$

■

Proposição 2.24. *Toda sequência aproximante em um espaço métrico $\boldsymbol{M}$ é limitada.*

Demonstração. Seja $(p_n)_{n\in\mathbb{N}}$ uma sequência aproximante em $\boldsymbol{M}$. Então, para $\varepsilon = 1$, existe $N \in \mathbb{N}$ tal que

$$\bigwedge n, m \in \mathbb{N} \qquad n, m \geq N \Rightarrow d(p_n, p_m) < 1.$$

Definamos $P := \{p_n : n \in \mathbb{N}\}$. Então segue que

$$\begin{aligned} \varnothing(P) &= \sup\{d(p_n, p_m) \mid n, m \in \mathbb{N}\} \\ &= \max\{1 \cup \{d(p_n, p_m) \mid 0 \leq n, m \leq N\}\} \in \mathbb{R}, \end{aligned}$$

o que mostra que $(p_n)_{n\in\mathbb{N}}$ é limitada. ■

2.3.2 Continuidade Uniforme

Definição 2.19. Sejam $\boldsymbol{M}_1$ e $\boldsymbol{M}_2$ espaços métricos. Uma função *uniformemente contínua* é uma função $f : M_1 \longrightarrow M_2$ tal que, para todo número real $\varepsilon > 0$, existe um número real $\delta > 0$ tal que

$$\bigwedge p_1, p_2 \in M_1 \qquad d_1(p_1, p_2) < \delta \Rightarrow d_2(f(p_1), f(p_2)) < \varepsilon.$$

Proposição 2.25. *Sejam $\boldsymbol{M}_1$ e $\boldsymbol{M}_2$ espaços métricos, $f : M_1 \longrightarrow M_2$ 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

$$\bigwedge n, m \in \mathbb{N} \qquad n, m \geq N \Rightarrow d_1(p_n, p_m) < \delta.$$

Mas, da continuidade uniforme de f, isso implica que

$$\bigwedge n, m \in \mathbb{N} \qquad n, m \geq N \Rightarrow d_1(p_n, p_m) < \delta \Rightarrow d_2(f(p_n), f(p_m)) < \varepsilon,$$

e isso mostra que $(f(p_n))_{n\in\mathbb{N}}$ é uma sequênca aproximante. ■

2.3.3 Espaços Métricos Completos

Definição 2.20. Um espaço métrico *completo* é um espaço métrico em que todas sequências aproximantes convergem.

Proposição 2.26. *Seja $\boldsymbol{M}$ um espaço métrico. Todo subespaço completo de $\boldsymbol{M}$ é um conjunto fechado em $\boldsymbol{M}$.*

Demonstração. Sejam $\boldsymbol{C} \subseteq \boldsymbol{M}$ subsepaço 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 2.27. *Sejam $\boldsymbol{M}$ um espaço métrico, $\boldsymbol{C} \subseteq \boldsymbol{M}$ um subespaço completo e $F \subseteq C$ um conjunto fechado em $\boldsymbol{M}$. Então $\boldsymbol{F}$ 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 2.28. *Seja $\boldsymbol{M}$ um espaço métrico. Então $\boldsymbol{M}$ é completo se, e somente se, para toda sequência descrescente $(F_n)_{n\in\mathbb{N}}$ de conjuntos não vazios e fechados em $\boldsymbol{M}$ tais que $(\varnothing(F_n))_{n\in\mathbb{N}} \to 0$ em $\mathbb{R}$, vale que*

$$\bigcap_{n\in\mathbb{N}} A_n \neq \emptyset.$$

Teorema 2.29. *Sejam $\boldsymbol{M}_1$ um espaço métrico, $\boldsymbol{M}_2$ espaço métrico completo, $D \subseteq M_1$ um conjunto denso em M_1 e $f : D \longrightarrow M_2$ uma função uniformemente contínua. Então f tem uma única extensão para uma função uniformemente contínua $f^* : M_1 \longrightarrow M_2$. 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 $f(p_n) \to f(p)$, 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

$$\bigwedge p, p' \in M_1 \qquad d_1(p, p') < \delta \Rightarrow d_2(f(p), f(p')) < \tfrac{\varepsilon}{2}.$$

Assim, sejam $p, q \in M_1$ tais que $d_1(p, q) < \delta$. Quremos mostrar que $d_2(f(p), f(p')) < \varepsilon$. Sejam $(p_n)_{n\in\mathbb{N}}$ e $(q_n)_{n\in\mathbb{N}}$ sequências que convergem para p e q, respectivamente. Então $d_1(p_n, q_n) \to d_1(p, q)$ 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 2.21. Seja $\boldsymbol{M}_1$ um espaço métrico. Um *completamento* de $\boldsymbol{M}$ é um espaço métrico $\boldsymbol{M}_2$ completo tal que M_1 é denso em M_2.

Proposição 2.30. *Seja $\boldsymbol{M}$ um espaço métrico e $\boldsymbol{M}_1$ e $\boldsymbol{M}_2$ completamentos de $\boldsymbol{M}$. Então existe uma isometria entre $\boldsymbol{M}_1$ e $\boldsymbol{M}_2$ que é a função identidade quando restrita a M.*

Demonstração. Seja f a função identidade em M. Pela proposição anterior, existe uma única extensãouniformemente contínua de f^* em M_1 ...

... ■

Proposição 2.31. *Sejam $K \subseteq M$ compacto e $f : M \longrightarrow \bar{M}$ 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 absudo. ■

2.3.4 Limitação Uniforme (ou Total)

Sejam (M, d) um espaço métrico e $\mathcal{T}$ a topologia induzida por d. A métrica limitada $d \wedge 1$ induz a mesma topologia $\mathcal{T}$ que d sobre M, mas com respeito a $d \wedge 1$ todos conjuntos são limitados, enquanto que com respeito a d isso nem sempre é verdade (somente nos casos em que o espaço inteiro é limitado). Isso mostra que o conceito de limitação não está sempre relacionado à topologia do espaço.

A convergência de sequências em $(M, \mathcal{T})$ independe da métrica que a gera e, portanto, concluímos que não pode existir um análogo ao teorema de Bolzano - Weierstrass usando o conceito de limitação, pois todas sequências em $(M, d\wedge 1)$ são limitadas, mas não necessariamente têm subsequência convergente. Definiremos a seguir um conceito distinto de limitação em espaços métricos que está mais relacionado à estrutura uniforme do espaço.

Definição 2.22. Um espaço métrico *uniformemente limitado* (ou *totalmente limitado*) é um espaço métrico $\boldsymbol{M}$ em que, para todo $\varepsilon \in]0, \infty[$, existe uma ε-cobertura finita de M. Um conjunto *uniformemente limitado* é um conjunto que é uniformemente limitado com a estrutura métrica induzida.

Proposição 2.32. *Seja $\boldsymbol{M}$ um espaço métrico.*

1. *$\boldsymbol{M}$ é uniformemente limitado se, e somente se, para todo $\varepsilon \in]0, \infty[$, existem $p_0, \cdots, p_{n-1}$ tais que*
$$M \subseteq \bigcup_{i \in [n]} \mathrm{B}_\varepsilon(p);$$

2. *Se $\boldsymbol{M}$ é uniformemente limitado, então é limitado.*

Demonstração. 1. ($\Rightarrow$) Seja $\varepsilon \in]0, \infty[$. Como M é uniformemente limitado, existe uma $\frac{\varepsilon}{2}$-cobertura finita $\{C_i\}_{i \in [n]}$ de M. Tome, para cada $i \in [n]$, $c_i \in C_i$. Então $\varnothing(\mathrm{B}_{\frac{\varepsilon}{2}}(c_i)) \leq \varepsilon$ e $C_i \subseteq \mathrm{B}_{\frac{\varepsilon}{2}}(c_i)$, portanto
$$M \subseteq \bigcup_{i \in [n]} C_i \subseteq \bigcup_{i \in [n]} \mathrm{B}_{\frac{\varepsilon}{2}}(c_i).$$

($\Leftarrow$) Reciprocamente, seja $\varepsilon \in]0, \infty[$. Existem existem $p_0, \cdots, p_{n-1}$ tais que
$$M \subseteq \bigcup_{i \in [n]} \mathrm{B}_{\frac{\varepsilon}{2}}(p_i);$$

Como, para todo $i \in [n]$, $\varnothing(\mathrm{B}_{\frac{\varepsilon}{2}}(p)) \leq \varepsilon$, segue que $(\mathrm{B}_{\frac{\varepsilon}{2}}(p_i))_{i \in [n]}$ é uma ε-cobertura de M, portanto M é uniformemente limitado.

2. Seja $(C_i)_{i \in [n]}$ uma cobertura 1-precisa de M. Então, como para todo $i \in [n]$, $\varnothing(C_i) < \infty$, e a cobertura é finita, $\varnothing(M) < \infty$.

■

▶ **Exercício 2.7.** Seja $d \in \mathbb{N}$ e consideremos $\mathbb{R}^d$ com a métrica reta usual. Um subconjunto de $\mathbb{R}^d$ é limitado se, e somente se, é uniformemente limitado.

Lema 2.33. *Sejam $\boldsymbol{M}$ um espaço métrico e $(x_n)_{n \in \mathbb{N}}$ uma sequência em M.*

1. *Se $(x_n)_{n \in \mathbb{N}}$ é aproximante, então sua imagem $x(\mathbb{N}) \subseteq M$ é uniformemente limitada;*

2. *Se $x(\mathbb{N})$ é uniformemente limitada, $(x_n)_{n \in \mathbb{N}}$ tem subsequência aproximante.*

Demonstração. 1. Seja $\varepsilon \in]0, \infty[$. Como $(x_n)_{n\in\mathbb{N}}$ é aproximante, existe $N \in \mathbb{N}$ tal que, para todos $n, n' \in \mathbb{N}$, se $n \geq N$ e $n' \geq N$, então $|x_n, x_{n'}| < \varepsilon$, portanto

$$\varnothing \{x_n \mid n \in \mathbb{N}, n \geq N\} \leq \varepsilon,$$

portanto

$$(\{x_0\}, \cdots, \{x_{N-1}\}, \{x_n \mid n \in \mathbb{N}, n \geq N\})$$

é uma cobertura ε-precisa finita de $x(\mathbb{N})$.

2. Se $x(\mathbb{N})$ for finito, então $(x_n)_{n\in\mathbb{N}}$ tem subsequência constante, logo aproximante. Suponhamos o caso em que $x(\mathbb{N})$ é infinito.

■

Proposição 2.34. *Seja $\boldsymbol{M}$ um espaço métrico. O espaço $\boldsymbol{M}$ é uniformemente limitado se, e somente se, toda sequência tem subsequência aproximante.*

Demonstração. ($\Rightarrow$) Suponha que $\boldsymbol{M}$ é uniformemente limitado. Seja ffl ■

Proposição 2.35. *Seja $\boldsymbol{M}$ um espaço métrico. O espaço $\boldsymbol{M}$ é compacto se, e somente se, é completo e uniformemente limitado.*

2.4 Funções que Preservam Distância

2.4.1 Funções Métricas (ou Subsemelhanças)

Definição 2.23. Sejam $\boldsymbol{M}_0$ e $\boldsymbol{M}_1$ espaços métricos e $c \in [0, \infty[$. Uma função *métrica*[2] de $\boldsymbol{M}_0$ para $\boldsymbol{M}_1$ (com constante c) é uma função $f\colon M_0 \longrightarrow M_1$ que satisfaz, para todos $p, p' \in M_0$,

$$d_1(f(p), f(p')) \leq c d_0(p, p').$$

Para $0 \leq c < 1$, a função f é uma *contração*; para $c = 1$, é uma *homometria*[3].

Proposição 2.36. *Sejam $\boldsymbol{M}_0, \boldsymbol{M}_1$ e $\boldsymbol{M}_2$ espaços métricos, $f_0\colon M_0 \longrightarrow M_1$ uma função métrica (com constante c_0) e $f_1\colon M_1 \longrightarrow M_2$ uma função métrica (com constante c_1). Então $f_1 \circ f_0\colon M_0 \longrightarrow M_2$ é uma função métrica (com constante $c_1 c_0$). 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.*

[2]Essas funções são conhecidas geralmente como funções 'Lipschitz' contínuas.

[3]Essas 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

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 2.37. *Sejam $\boldsymbol{M}_0$ e $\boldsymbol{M}_1$ espaços métricos e $f\colon M_0 \longrightarrow M_1$ 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

$$d_1(f(p), f(p')) \leq c d_0(p, p') \leq c\frac{\varepsilon}{c} = \varepsilon.$$ ■

Proposição 2.38. *Sejam $\boldsymbol{M}_0$ e $\boldsymbol{M}_1$ espaços métricos e $f\colon M_0 \longrightarrow M_1$ 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 $p, p' \in M_0$,*

$$c^{-1} d_0(p, p') \leq d_1(f(p), f(p')) \leq c d_0(p, p').$$

Demonstração. Se f tem inversa à esquerda c-métrica, então, para todos $q, q' \in M_1$,

$$d_0(f^{-1}(q), f^{-1}(q')) \leq c d_1(q, q').$$

Assim, para todos $p, p' \in M_0$,

$$d_0(p, p') = d_0(f^{-1}(f(p)), f^{-1}(f(p'))) \leq c d_1(f(p), f(p')),$$

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 $d_0(p, p') \leq c d_1(f(p), f(p'))$, 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

$$\begin{aligned} d_0(f^{-1}(q), f^{-1}(q')) &= d_0(f^{-1}(f(p)), f^{-1}(f(p'))) \\ &= d_0(p, p') \leq c d_1(f(p), f(p')) \\ &= c d_1(q, q'), \end{aligned}$$

o que mostra que f^{-1} é c-métrica.

■

2.4.2 Homometrias e Isometrias

Definição 2.24. Sejam $\boldsymbol{M_0}$ e $\boldsymbol{M_1}$ espaços métricos. Uma *isometria local* ou (*imersão isométrica*) de $\boldsymbol{M_0}$ para $\boldsymbol{M_1}$ é uma função $f\colon M_0 \longrightarrow M_1$ 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 2.39. *Sejam $\boldsymbol{M_0}$ e $\boldsymbol{M_1}$ espaços métricos e $f\colon M_0 \longrightarrow M_1$ 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 2.40. *Sejam $\boldsymbol{M_0}$ e $\boldsymbol{M_1}$ espaços métricos e $f\colon M_0 \longrightarrow M_1$ 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 2.41. *Sejam $\boldsymbol{M_0}$ e $\boldsymbol{M_1}$ espaços métricos e $f\colon M_0 \longrightarrow M_1$ 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. ■

2.4.3 Contrações

Proposição 2.42 (Ponto Fixo para Contrações)**.** *Sejam $\boldsymbol{M}$ um espaço métrico completo e $f\colon M \longrightarrow M$ uma contração. Existe único ponto fixo $\bar{p} \in M$ para f e, para todo $p \in M$,*

$$\lim_{n\longrightarrow\infty} f^n(p) = \bar{p}.$$

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,

$$d(f^k(p), f^{k+1}(p)) \leq cd(f^{k-1}(p), f^k(p)) \leq cc^{k-1}d(p, f(p)) = c^k d(p, f(p)).$$

Agora, notemos que, para todos $n, p \in \mathbb{N}$, segue da desigualdade triangular generalizada que

$$\begin{aligned} d(f^n(p), f^{n+p}(p)) &\leq \mathop{\mathop{+}\limits_{i=0}}^{p-1} d(f^{n+i}(p), f^{n+i+1}(p)) \\ &\leq \mathop{\mathop{+}\limits_{i=0}}^{p-1} c^{n+i} d(p, f(p)) \\ &= c^n \frac{1 - c^p}{1 - c} d(p, f(p)) \\ &\leq \frac{c^n}{1 - c} d(p, f(p)), \end{aligned}$$

pois $c \geq 0$ implica $1 - c^p < 1$. Como $c < 1$, então $\lim_{n\longrightarrow\infty} \frac{c^n}{1-c} = 0$, portanto, para todos $n, p \in \mathbb{N}$,

$$\lim_{n\longrightarrow\infty} d(f^n(p), f^{n+p}(p)) = 0,$$

o que mostra que $(f^n(p))_{n\in\mathbb{N}}$ é uma sequência aproximante e, como $\boldsymbol{M}$ é completo, converge para $\bar{p} \in M$. Como f é contínua,

$$f(\bar{p}) = f\left(\lim_{n\longrightarrow\infty} f^n(p)\right) = \lim_{n\longrightarrow\infty} f^{n+1}(p) = \bar{p},$$

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 $\bar{p} = p$. ■

2.4.4 Semelhanças

Definição 2.25. Sejam $\boldsymbol{M_0}$ e $\boldsymbol{M_1}$ espaços métricos e $c \in [0, \infty[$. Uma *c-semelhança local* ou (*imersão c-semelhante*) de $\boldsymbol{M_0}$ para $\boldsymbol{M_1}$ é uma função $f\colon M_0 \longrightarrow M_1$ 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.

Capítulo 3

Grupos Topológicos

3.1 Grupo Topológico

Definição 3.1. Um *grupo topológico* é uma quádrupla $\boldsymbol{G} = ((G, \mathcal{T}), \times, ^{-1}, e)$ em que $(G, \mathcal{T})$ é um espaço topológico, $(G, \times, ^{-1}, \mathrm{I})$ é um grupo e as operações

$$\times \colon G^2 \longrightarrow G \qquad \text{e} \qquad ^{-1} \colon G \longrightarrow G$$

são funções contínuas.

Note que não é necessária nenhuma condição sobre $\mathrm{I} \in G$, pois se visto como operações zerária $\mathrm{I} \colon \{0\} \longrightarrow G$, ela é contínua em qualquer topologia de G, pois $\{0\}$ só admite a topologia trivial.

Lembremos que para um grupo $\boldsymbol{G}$ e $g \in G$, a conjugação por g é a função

$$\begin{aligned} C_g \colon G &\longrightarrow G \\ h &\longmapsto ghg^{-1}, \end{aligned}$$

a translação à direita por g é a função

$$\begin{aligned} D_g \colon G &\longrightarrow G \\ h &\longmapsto hg \end{aligned}$$

e a translação à esquerda por g é a função

$$\begin{aligned} E_g \colon G &\longrightarrow G \\ h &\longmapsto gh. \end{aligned}$$

Proposição 3.1. *Seja $\boldsymbol{G}$ 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. ■

Exemplo 3.1. *Seja* $\boldsymbol{X}$ *um espaço topológico e* $\boldsymbol{G}$ *um grupo topológico. Consideremos o conjunto* $\mathscr{C}(X, G)$ *das funções contínuas de* $\boldsymbol{X}$ *para* $\boldsymbol{G}$ *e as operações induzidas pontualmente de* G *em* $\mathscr{C}(X, G)$ *por* $(f \times g)(x) := f(x) \times g(x)$, $(f^{-1})(x) := (f(x))^{-1}$ *e* $\mathrm{I}(x) := \mathrm{I}$. *A quádrupla* $(\mathscr{C}(X, G), \times, ^{-1}, \mathrm{I})$ *é um grupo. Consideramos agora a topologia* compacto-aberto $\mathcal{T}$ *gerada pelos conjuntos*

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

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

Proposição 3.2. *Seja* $\boldsymbol{G}$ *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 e $gA = E_g(A)$, $Ag = D_g(A)$.
2. Segue do fato de que E_g e D_g são homeomorfismos e $gA = E_g(A)$, $Ag = D_g(A)$.
3. Segue do fato de que
$$AC = \bigcup_{c \in C} Ac \quad \text{e} \quad CA = \bigcup_{c \in C} cA$$
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.

■

3.2 Topologia em Grupos

Uma peculiaridade dos grupos topológico é que, como temos homeomorfismo do grupo para ele mesmo que levam qualquer elemento para a identidade, segue que basta estudar as vizinhanças abertas da identidade para entender a topologia do grupo. Isso fica mais claro com os resultados a seguir.

Definição 3.2. Seja $\boldsymbol{G}$ um grupo. Um *sistema de vizinhanças da identidade* em $\boldsymbol{G}$ é um conjunto $\mathcal{V}$ de subconjuntos de G tal que

1. Para todo $A \in \mathcal{V}$, $\mathrm{I} \in A$;
2. Para todos $A, A' \in \mathcal{V}$, $A \cap A' \in \mathcal{V}$;
3. Para todo $A \in \mathcal{V}$, existe $B \in \mathcal{V}$ tal que $B^2 \subseteq A$;
4. Para todo $A \in \mathcal{V}$, $A^{-1} \in \mathcal{V}$;
5. Para todos $A \in \mathcal{V}$, $g \in G$, $gAg^{-1} \in \mathcal{V}$.

Denotaremos por $\mathcal{V} := \mathcal{V}_{\mathrm{I}}^{\circ}$ as vizinhanças abertas da identidade I.

Proposição 3.3. *Seja $\boldsymbol{G}$ um grupo topológico. O conjunto $\mathcal{V}$ de vizinhanças abertas de I é um sistema de vizinhanças da identidade.*

Definição 3.3. Seja $\boldsymbol{G}$ um grupo. Uma topologia *invariante por translação à esquerda* em $\boldsymbol{G}$ é uma topologia $\mathcal{T}$ em G tal que, para todos $A \in \mathcal{T}$ e $g \in G$, $gA \in \mathcal{T}$. Uma topologia *invariante por translação à direita* em $\boldsymbol{G}$ é uma topologia $\mathcal{T}$ em G tal que, para todos $A \in \mathcal{T}$ e $g \in G$, $Ag \in \mathcal{T}$.

Proposição 3.4. *Sejam $\boldsymbol{G}$ um grupo e $\mathcal{T}$ uma topologia em G.*

1. *Se $\mathcal{T}$ é invariante por translação à esquerda em $\boldsymbol{G}$ então a topologia produto $\mathcal{T}^2$ em $G \times G$ é invariante por translação à esquerda em $\boldsymbol{G} \times \boldsymbol{G}$;*
2. *Se $\mathcal{T}$ é invariante por translação à direita em $\boldsymbol{G}$ então a topologia produto $\mathcal{T}^2$ em $G \times G$ é invariante por translação à direita em $\boldsymbol{G} \times \boldsymbol{G}$.*

Proposição 3.5. *Seja $\boldsymbol{G}$ um grupo e $\mathcal{T}$ uma topologia invariante por translação à esquerda e à direita em $\boldsymbol{G}$. Então $((G, \mathcal{T}), \times, ^{-1}, \mathrm{I})$ é um grupo topológico se, e somente se,*

1. *$\times$ é contínua em (I, I);*
2. *$^{-1}$ é contínua em I.*

Proposição 3.6. *Sejam $\boldsymbol{G}$ um grupo e $\mathcal{V}$ um sistema de vizinhanças da identidade em $\boldsymbol{G}$. Existe uma única topologia $\mathcal{T}$ em G tal que $((G,\mathcal{T}),\times,^{-1},\mathrm{I})$ é um grupo topológico e $\mathcal{V}$ é um sistema fundamental de vizinhanças de I em $(G,\mathcal{T})$.*

Proposição 3.7. *Seja $\boldsymbol{G}$ um grupo topológico. São equivalentes:*

1. *$(G,\mathcal{T})$ é separado;*
2. *$\{\mathrm{I}\}$ é fechado;*
3. *$\bigcap_{A\in\mathcal{V}} A = \{\mathrm{I}\}$.*

3.3 Distância em Grupos

Definição 3.4. Seja $\boldsymbol{G}$ um grupo. Uma distância *invariante por translação à esquerda* em $\boldsymbol{G}$ é uma distância $|\cdot,\cdot| : G\times G \longrightarrow [0,\infty[$ em G tal que, para todo $g\in G$, a translação à esquerda E_g é uma isometria local em $(G,|\cdot,\cdot|)$. Uma distância *invariante por translação à direita* em $\boldsymbol{G}$ é uma distância em G tal que, para todo $g\in G$, a translação à direita D_g é uma isometria local. Uma distância *invariante por translação* em $\boldsymbol{G}$ é uma distância invariante à esquerda e à direita em $\boldsymbol{G}$.

No caso da invariância à esquerda, isso quer dizer que, para todos $g, g_0, g_1 \in G$,

$$|gg_0, gg_1| = |g_0, g_1|\,.$$

O caso à direita é análogo.

Proposição 3.8. *Seja $\boldsymbol{G}$ um grupo topológico e $\mathcal{V}$ um sistema de vizinhanças da identidade enumerável. Existem distâncias $|\cdot,\cdot|_E$ e $|\cdot,\cdot|_D$ em G invariantes por translação à esquerda e à direita em $\boldsymbol{G}$, respectivamente, e compatíveis com a topologia de $\boldsymbol{G}$.*

3.4 Homomorfismos Contínuos

Proposição 3.9. *Sejam $\boldsymbol{G}$ e $\boldsymbol{H}$ grupos topológicos e $h : G \longrightarrow H$ um homomorfismo de grupos. Então ϕ é contínuo se, e somente se, ϕ é contínuo na identidade $\mathrm{I}\in G$.*

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 $g = E_g(\mathrm{I})$. ■

3.5 Subgrupos Topológicos

Definição 3.5. Seja $\boldsymbol{G} = ((G, \mathcal{T}), \times, ^{-1}, \mathrm{I})$ um grupo topológico. Um *subgrupo topológico* de $\boldsymbol{G}$ é uma quádrupla $\boldsymbol{S} = ((S, \mathcal{T}_S), \times|_S, ^{-1}|_S, \mathrm{I})$ em que $(S, \mathcal{T}|_S)$ é um subespaço topológico de $(G, \mathcal{T})$ e $(S, \times|_S, ^{-1}|_S, \mathrm{I})$ é um subgrupo de $(G, \times, ^{-1}, \mathrm{I})$.

Proposição 3.10. *Seja $\boldsymbol{G}$ um grupo topológico e $\boldsymbol{S}$ um subgrupo de $\boldsymbol{G}$. Então $\boldsymbol{S}$ é um grupo topológico.*

Demonstração. Temos que mostrar que as operações $\times|_S$ e $^{-1}|_S$ são contínuas. ($\times|_S$ é contínua) Seja $C \subseteq G$,

$$\times|_S^{-1}(C \cap S) = \times^{-1}(C) \cap (S \times S),$$

portanto para todo aberto $A \cap S$ de S, com $A \subseteq G$ aberto de G, segue que $\times|_S^{-1}(A \cap S) = \times^{-1}(A) \cap (S \times S)$ é aberto em $S \times S$, logo $\times|_S$ é contínua.

($^{-1}|_S$ é contínua) Análogo ao caso do produto. ■

Proposição 3.11. *Seja $\boldsymbol{G}$ um grupo topológico. Se $\boldsymbol{S}$ é subgrupo topológico de $\boldsymbol{G}$, então $\overline{\boldsymbol{S}}$ é um subgrupo topológico de $\boldsymbol{G}$. Se $\boldsymbol{N}$ é subgrupo topológico normal de $\boldsymbol{G}$, então $\overline{\boldsymbol{N}}$ é um subgrupo topológico normal de $\boldsymbol{G}$.*

Proposição 3.12. *Sejam $\boldsymbol{G}$ um grupo topológico e $\boldsymbol{S}$ é subgrupo topológico de $\boldsymbol{G}$.*

1. *$\overline{\boldsymbol{S}}$ é um subgrupo topológico de $\boldsymbol{G}$;*
2. *Se $\boldsymbol{S}$ é um subgrupo normal, então $\overline{\boldsymbol{S}}$ é um subgrupo topológico normal de $\boldsymbol{G}$;*
3. *Se $S^\circ \neq \emptyset$, então S é aberto;*
4. *Se S é aberto, então S é fechado.*

3.6 Conexidade em Grupos Topológicos

Definição 3.6. Seja $\boldsymbol{G}$ um grupo topológico. A componente conexa de I é denotada G_{I}.

Proposição 3.13. *Seja $\boldsymbol{G}$ um grupo topológico. Então $\boldsymbol{G}_{\mathrm{I}}$ é um subgrupo topológico normal e fechado de $\boldsymbol{G}$ e existe bijeção entre as componentes conexas de $\boldsymbol{G}$ e as classes laterais de G_{I}.*

Proposição 3.14. *Seja $\boldsymbol{G}$ um grupo topológico.*

1. *Se $\boldsymbol{G}$ é localmente conexo, então G_{I} é aberta;*
2. *Se $\boldsymbol{G}$ é conexo, para toda vizinhança A de I,*

$$G = \bigcup_{n \in \mathbb{N}} A^n.$$

3.7 Espaço de Homeomorfismos

Sej $\boldsymbol{X}$ um espaço topológico. O espaço $\overset{\leftrightarrow}{\mathscr{C}}(X) = \overset{\leftrightarrow}{\mathscr{C}}(X, X)$ dos homeomorfismos de $\boldsymbol{X}$ para $\boldsymbol{X}$ é um grupo com produto de composição $\circ$, a inversa de função $^{-1}$ e a função identidade I. A topologia de $\overset{\leftrightarrow}{\mathscr{C}}(X)$ é a topologia produto. A composição de funções é contínua com respeito a essa topologia, bem como a inversa de funções.

Proposição 3.15. *Seja $\boldsymbol{X}$ um espaço topológico. O espaço do homeomorfismos*

$$\left(\left(\overset{\leftrightarrow}{\mathscr{C}}(X), \mathcal{T}|_{\overset{\leftrightarrow}{\mathscr{C}}(X)}\right), \circ, ^{-1}, \mathrm{I}\right)$$

é um grupo topológico.

Demonstração. Para qualquer conjunto X, o espaço de bijeções $\left(\overset{\leftrightarrow}{\mathcal{F}}(X), \circ, ^{-1}, \mathrm{I}\right)$ é um grupo. No caso de $\boldsymbol{X}$ ser um espaço topológico, temos que $\overset{\leftrightarrow}{\mathscr{C}}(X) \subseteq \mathscr{C}$, pois todo homeomorfismo é uma bijeção. Devemos mostrar que $\overset{\leftrightarrow}{\mathscr{C}}(X)$ é um subgrupo. Para isso, notemos que, para todas $f, f' \in \overset{\leftrightarrow}{\mathscr{C}}(X)$, $f' \circ f$ é contínua, pois é composta de contínuas, e tem inversa contínua, pois

$$(f' \circ f)^{-1} = f^{-1} \circ (f')^{-1},$$

que é contínua porque é composta das contínuas f^{-1} e $(f')^{-1}$. Ainda, para toda $f \in \overset{\leftrightarrow}{\mathscr{C}}(X)$, por definição temos $f^{-1} \in \overset{\leftrightarrow}{\mathscr{C}}(X)$. Por fim, claramente I é contínua, o que mostra que $\overset{\leftrightarrow}{\mathscr{C}}(X)$ é um subgrupo de $\overset{\leftrightarrow}{\mathcal{F}}(X)$.

A topologia de $\overset{\leftrightarrow}{\mathscr{C}}(X)$ é a topologia de subconjunto induzida da topologia produto de $\overset{\leftrightarrow}{\mathcal{F}}(X)$. Devemos mostrar que as operações $\circ$ e $^{-1}$ são contínuas. ■

3.8 Ação Contínua

Definição 3.7. Sejam $\boldsymbol{G}$ um grupo topológico e $\boldsymbol{X}$ um espaço topológico. Uma *ação contínua* de $\boldsymbol{G}$ em $\boldsymbol{X}$ é uma ação $\boldsymbol{.} : G \times X \longrightarrow X$ que é uma função contínua[1]

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

que satisfaz

[1] Com respeito à topologia produto de $G \times X$

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

$$\mathbf{1}_{\blacksquare}\, x = x;$$

2. (Compatibilidade) Para todos $g, g' \in G$ e $x \in X$,

$$(g'g)_{\blacksquare}\, x = g'_{\blacksquare}\, (g_{\blacksquare}\, x).$$

Denota-se $\blacksquare : \boldsymbol{G} \curvearrowright \boldsymbol{X}$. O grupo $\boldsymbol{G}$ *age continuamente* em $\boldsymbol{X}$.

Para cada $g \in G$, ação $\blacksquare$ induz uma função contínua

$$\begin{aligned} g_{\blacksquare} : X &\longrightarrow X \\ x &\longmapsto g_{\blacksquare}\, x. \end{aligned}$$

Nesse caso, temos um ismorfismo de grupos topológicos (isomorfismo de grupo e homeomorfismo)

$$\begin{aligned} \blacksquare : G &\longrightarrow \overset{\leftrightarrow}{\mathscr{C}}(X) \\ g &\longmapsto g_{\blacksquare} : X \longrightarrow X \\ & \qquad\qquad x \longmapsto g_{\blacksquare}\, x \end{aligned}$$

Capítulo 4

Espaços Lineares Topológicos

4.1 Anéis e Corpos Topológicos

Definição 4.1. Um *anel topológico* é uma lista $\boldsymbol{A} = ((A, \mathcal{T}), +, -, 0, \times, 1)$ em que $(A, \mathcal{T})$ é um espaço topológico, $(A, +, -, 0, \times, 1)$ é um anel e as operações $+$, $-$ e $\times$ são contínuas.

Um *corpo topológico* é uma lista $\boldsymbol{C} = ((C, \mathcal{T}), +, -, 0, \times, ^{-1}, 1)$ em que $(C, \mathcal{T})$ é um espaço topológico, $(C, +, -, 0, \times, ^{-1}, 1)$ é um corpo e as operações $+$, $-$, $\times$ e $^{-1}$ são contínuas.

Note que, como no caso dos grupos topológicos, não é necessária nenhuma condição sobre 0 e 1, pois se vistos como operações zerárias, são contínuas em qualquer topologia.

Nesta seção deixamos somente as definições de anel e corpo topológico para referência, não exploraremos a teoria de aneis e corpos topológicos.

4.2 Espaço Linear Topológico

Definição 4.2. Um *espaço linear topológico* é um espaço linear $\boldsymbol{L} = (L, \cdot)$ sobre um corpo topológico $\boldsymbol{C}$ em que L é um grupo topológico e $\cdot \colon \boldsymbol{C} \curvearrowright \boldsymbol{L}$ é uma ação contínua.

4.3 Espaço de Funções a Valores Vetoriais

Primeiro relembremos que, se X é um conjunto e $(L, +, 0, -, \cdot)$ é um espaço linear sobre um corpo C, o espaço L^X de funções de X para L é um espaço linear com

a adição pontual

$$\begin{aligned} +\colon L^X \times L^X &\longrightarrow L^X \\ (f, f') &\longmapsto f + f' \colon X \longrightarrow L \\ &\qquad\qquad x \longmapsto f(x) + f'(x), \end{aligned}$$

a função nula

$$\begin{aligned} 0\colon X &\longrightarrow L \\ x &\longmapsto 0, \end{aligned}$$

a inversa pontual da adição

$$\begin{aligned} -\colon L^X &\longrightarrow L^X \\ f &\longmapsto -f \colon X \longrightarrow L \\ &\qquad\qquad x \longmapsto -(f(x)) \end{aligned}$$

e a multiplicação pontual por escalar

$$\begin{aligned} \cdot\colon C \times L^X &\longrightarrow L^X \\ (c, f') &\longmapsto cf \colon X \longrightarrow L \\ &\qquad\qquad x \longmapsto c(f(x)). \end{aligned}$$

Proposição 4.1. *Sejam X um conjunto e $\boldsymbol{L}$ um espaço linear topológico sobre um corpo topológico $\boldsymbol{C}$. O espaço de funções L^X é um espaço linear topológico com a topologia produto.*

Demonstração. Temos que mostrar que as operações algébricas em L^X são contínuas. As projeções da topologia produto de $L^X = \prod_{x \in X} L$ são as funções avaliação para cada $x \in X$

$$\begin{aligned} \mathrm{p}_x\colon L^X &\longrightarrow L \\ f &\longmapsto f(x). \end{aligned}$$

Notemos que

$$\begin{aligned} \mathrm{p}_x \circ + &= + \circ (\mathrm{p}_x, \mathrm{p}_x), \\ \mathrm{p}_x \circ - &= - \circ \mathrm{p}_x. \\ \mathrm{p}_x \circ \cdot &= \cdot \circ (\mathrm{I}, \mathrm{p}_x), \end{aligned}$$

em que as operações à esquerda são as operações em L^X e as à direita, as em L. Nesse caso, segue que as operações algébricas em L^X são contínuas pela

propriedade universal do produto de espaços topológicos. No caso da adição $+\colon L^X \times L^X \longrightarrow L^X$, o seguinte diagrama comuta:

$$\begin{tikzcd}
 & L^X \arrow[d, "\mathrm{p}_x"] \\
L^X \times L^X \arrow[ur, dashed, "+"] \arrow[r, "+ \circ (\mathrm{p}_x, \mathrm{p}_x)"'] & L.
\end{tikzcd}$$

Como p_x é contínua para cada $x \in X$ pela definição da topologia produto, segue que $(\mathrm{p}_x, \mathrm{p}_x)\colon L^X \times L^X \longrightarrow L \times L$ também é contínua, logo da continuidade de $+\colon L \times L \longrightarrow L$ segue que $+ \circ (\mathrm{p}_x, \mathrm{p}_x)\colon L^X \times L^X \longrightarrow L$ é contínua. Pela propriedade universal, $+\colon L^X \times L^X \longrightarrow L^X$ é a única função contínua tal que o diagrama comuta. A demonstração da continuidade das outras operações algébricas é análoga. Os seguintes diagramas comutam:

$$\begin{tikzcd}
 & L^X \arrow[d, "\mathrm{p}_x"] \\
L^X \arrow[ur, dashed, "-"] \arrow[r, "- \circ \mathrm{p}_x"'] & L
\end{tikzcd}
\qquad
\begin{tikzcd}
 & L^X \arrow[d, "\mathrm{p}_x"] \\
C \times L^X \arrow[ur, dashed, "\cdot"] \arrow[r, "\cdot \circ (\mathrm{I}, \mathrm{p}_x)"'] & L.
\end{tikzcd}$$

■

Proposição 4.2. *Sejam $\boldsymbol{X}$ um espaço topológico e $\boldsymbol{L}$ um espaço linear topológico sobre um corpo topológico $\boldsymbol{C}$. O espaço de funções contínuas $\mathscr{C}(\boldsymbol{X}, \boldsymbol{L})$ é espaço linear topológico.*

Demonstração. Para mostrar isso, basta mostrar que $\mathscr{C}(X, L)$ é um subespaço linear de L^X. (Fechado pela adição) Para todas $f, f' \in \mathscr{C}(X, L)$, $(f, f')\colon X \times X \longrightarrow L \times L$ é contínua. Como $+\colon L^X \times L^X \longrightarrow L^X$ é contínua, segue que

$$f + f' = + \circ (f, f')$$

é contínua, pois é composição de contínuas.

(Fechado pela multiplicação por escalar) Para todos $c \in C$, $f \in \mathscr{C}(X, L)$, $(c, f)\colon \{0\} \times X \longrightarrow C \times L$ é contínua, em que c é interpretado como uma função $c\colon \{0\} \longrightarrow C$. Como $\cdot$ é contínua, segue que

$$cf = \cdot \circ (c, f)$$

é contínua, pois é composição de contínuas. Isso mostra que $\mathscr{C}(X, L)$ é subespaço linear de L^X, portanto é um espaço linear. ■

4.4 Funções Lineares Contínuas

Definição 4.3. Sejam $\boldsymbol{L}, \boldsymbol{L}'$ espaços lineares topológicos. Uma *função linear contínua* de $\boldsymbol{L}$ para $\boldsymbol{L}'$ é uma função $f\colon L \longrightarrow L'$ que é linear com respeito à estrutura de espaço linear de $\boldsymbol{L}$ e $\boldsymbol{L}'$ e contínua com respeito à estrutura de espaço topológico de $\boldsymbol{L}$ e $\boldsymbol{L}'$. O conjunto dessas funções é denotado $\mathscr{L}(\boldsymbol{L}, \boldsymbol{L}')$.

Isso é o mesmo que dizer que

$$\mathscr{L}(\boldsymbol{L}, \boldsymbol{L}') = \mathcal{L}(\boldsymbol{L}, \boldsymbol{L}') \cap \mathscr{C}(\boldsymbol{L}, \boldsymbol{L}').$$

4.5 Espaço Dual Contínuo

No estudo de espaços lineares, um objeto importante é o espaço linear dual, o espaço dos funcionais lineares em um espaço linear. No caso de espaços lineares topológicos, um subespaço do espaço linear dual mostra-se mais interessante, o espaço dos funcionais lineares contínuos. No caso de espaço lineares topológico de dimensão finita, todo funcional linear é contínuo, mas no caso geral devemos nos restringir aos contínuos para que a teoria tenha propriedades mais desejáveis e interessantes.

Definição 4.4. Seja L um espaço linear topológico sobre um corpo topológico C. O *espaço linear dual contínuo* de L é o espaço linear

$$L^{\circledast} := \mathscr{L}(L, C).$$

Como o espaço $L^* = \mathcal{L}(L, C)$ dos funcionais lineares em L e o espaço $\mathscr{C}(L, C)$ dos funcionais contínuos em L são espaços lineares, o espaço

$$L^{\circledast} = L^* \cap \mathscr{C}(L, C),$$

dos funcionais lineares contínuos em L é um espaço linear.

Definição 4.5. Sejam L um espaço linear topológico sobre um corpo topológico C e $v \in L$. A *evaluação* em v é o funcional linear

$$\begin{aligned} e_v \colon L^{\circledast} &\longrightarrow C \\ f &\longmapsto f(v). \end{aligned}$$

A *topologia*[1] *de* $L^{\circledast}$ é a topologia inicial com respeito à família $\{e_v\}_{v \in L}$

A topologia definida é a menor topologia em $L^{\circledast}$ tal que, para todo $v \in L$, a evaluação $e_v \colon L^{\circledast} \longrightarrow C$ é contínua; ou seja, é a topologia

$$\mathcal{T} := \left\langle \bigcup_{v \in L} {e_v}^{\star}(\mathcal{T}_C) \right\rangle,$$

em que $\mathcal{T}_C$ é a topologia de C.

Em $\mathbb{R}$, essa é a mesma topologia que a gerada pelos abertos

$$B_{\varepsilon}^{v}(f) := \{f' \in L^* \mid |f'(v) - f(v)| < \varepsilon\},$$

para cada $v \in L$, $\varepsilon \in]0, \infty[$ e $f \in L^*$. Basta notar que, para cada $v \in V$,

$$|e_v(f') - e_v(f)| = |f'(v) - f(v)| < \varepsilon,$$

ou seja, essa é a condição para e_v ser contínua.

4.6 Teoremas de Representação de Riesz

4.6.1 Representação Linear de Produto Interno

Proposição 4.3. *Seja* $\boldsymbol{L}$ *um espaço linear com produto interno completo. A função*

$$\begin{aligned} I \colon L &\longrightarrow L^{\circledast} \\ v &\longmapsto I_v \colon V \longrightarrow \mathbb{R} \\ & \qquad\quad v' \longmapsto \langle v, v' \rangle \end{aligned}$$

é um isomorfismo de espaços lineares com produto interno.

[1] Chamada topologia fraca ou topologia fraca $*$ (lido 'estrela') de $L^{\circledast}$.

4.6.2 Representação Contínua de Medida

Lembremos que, para todo espaço topológico $\boldsymbol{X} = (X, \mathcal{T})$, o conjunto $\mathcal{M}_{\mathcal{T}}$ é a álgebra de mensuráveis em X gerada pelos abertos de $\mathcal{T}$. O conjunto $\mathfrak{M}_r(X, \mathcal{M}_{\mathcal{T}})$ é o conjunto das medidas (positivas ou não) completas regulares, o que nesse contexto quer dizer que são finitas em compactos, interiormente regulares em abertos e mensuráveis com medida finita, e exteriormente regulares em mensuráveis.

Proposição 4.4. *Seja $\boldsymbol{X}$ um espaço topológico separado e localmente compacto. A função*

$$\begin{aligned} I\colon \mathfrak{M}_{\mathcal{T}}(X) &\longrightarrow \mathscr{C}_c(X, \mathbb{R})^{\circledast} \\ m &\longmapsto I_m\colon \mathscr{C}_c(X, \mathbb{R}) \longrightarrow \mathbb{R} \\ & \qquad\qquad\qquad\quad f \longmapsto \int_X f \mathrm{d}m \end{aligned}$$

é um isomorfismo de espaços lineares normados. Se restrito às medidas positivas, I é um isomorfismo entre as medidas positivas e os funcionais positivos.

Capítulo 5

Espaços Normados

5.1 Norma em Corpos (Valor Absoluto)

Consideremos um corpo $\boldsymbol{C}$. Queremos definir uma função $|\cdot| : C \longrightarrow [0, \infty[$ que satisfaça a propriedade de multiplicatividade para todos $c, c' \in C$,

$$|cc'| = |c|\,|c'|\,.$$

Nesse caso, temos

$$|0| = |0c| = |0|\,|c|\,.$$

Se $|0| \neq 0$, então $|c| = 1$ para todo $c \in C$ (inclusive $|0| = 1$), o que mostra que $|\cdot|$ é uma função trivial e, portanto, não tem comportamento tão interessante. É natural então assumir que $|0| = 0$. Nesse caso, não concluímos da multiplicatividade que $|c| = 1$ para todo $c \in C$. No entanto, temos

$$|1| = |1 \cdot 1| = |1|\,|1|\,.$$

Então $|1| = 0$ ou $|1| = 1$. No primeiro caso, segue que, para todo $c \in C$, $|c| = |1c| = |1|\,|c| = 0\,|c| = 0$, logo $|c| = 0$ para todo $c \in C$, o que mostra que $|\cdot|$ novamente é uma função trivial. É natural, assim, assumir que $|1| \neq 0$, e portanto $|1| = 1$. Assumiremos, no entanto, que para todo $c \in C$, se $|c| = 0$ então $c = 0$, o que implica $|\cdot|$ é um homomorfismo de grupos entre o grupo multiplicativo de $\boldsymbol{C}$ e o grupo multiplicativo $]0, \infty[$. Notemos ainda que

$$1 = |1| = |(-1)(-1)| = |-1|\,|-1|\,,$$

portanto $|-1| = 1$, já que $|-1| \in [0, \infty[$. Disso segue que

$$|-c| = |-1|\,|c| = |c|\,.$$

Ainda, para todo $c \in C$ segue que

$$\left|c^{-1}\right| = \left|c^{-1}\right| |c| \, |c|^{-1} = \left|c^{-1}c\right| |c|^{-1} = |1| \, |c|^{-1} = |c|^{-1} .$$

Além da multiplicatividade, uma segunda propriedade desejável é a subaditividade: para todos $c, c' \in C$,

$$|c + c'| \leq |c| + |c'| .$$

Note que não adotamos a propriedade mais forte de aditividade. Isso ocorre porque queremos que $|\cdot|$ se comporte de fato como o valor absoluto em $\mathbb{R}$, e também porque queremos que $|\cdot|$ tenha valores positivos, o que a aditividade não permitiria pois de $|0| = 0$ e $|1| = 1$ seguiria que $|-1| = -1$.

Definição 5.1. Seja $\boldsymbol{C}$ um corpo. Uma *norma* (ou *valor absoluto*) em $\boldsymbol{C}$ é uma função $|\cdot| : C \longrightarrow [0, \infty[$ que satisfaz

1. (Separação) Para todo $c \in C$, $|c| = 0$ se, e somente se, $c = 0$;
2. (Multiplicatividade) Para todos $c, c' \in C$,
$$|cc'| = |c| \, |c'| ;$$
3. (Subaditividade) Para todos $c, c' \in C$,
$$|c + c'| \leq |c| + |c'| .$$

Proposição 5.1 (Propriedades da Norma)**.** *Sejam $\boldsymbol{C}$ um corpo e $|\cdot|$ uma norma em $\boldsymbol{C}$.*

1. $|1| = |-1| = 1$;
2. *Para todo $c \in C$, $|-c| = |c|$;*
3. *Para todo $c \in C$, $|c| \geq 0$;*
4. *(Subaditividade generalizada) Para todos $c_0, \ldots, c_{n-1} \in C$,*
$$\left| \mathop{+}_{i \in [n]} c_i \right| \leq \mathop{+}_{i \in [n]} |c_i| ;$$
5. *Para todos $c, c' \in C$, $||c'| - |c|| \leq |c' - c|$.*

Demonstração. 1. Notemos que

$$|1| = \left|1^2\right| = |1|^2 ,$$

logo $|1| = 0$ ou $|1| = 1$. Da separação de $|\cdot|$, segue que $|1| = 1$.

2. Para todo $c \in C$,

$$|-c| = |-1|\,|c| = |c| .$$

3. Seja $c \in C$. Temos que

$$0 = |0| = |c - c| \leq |c| + |-c| = 2\,|c| ,$$

logo $|c| \geq 0$

4. Segue por indução da subaditividade de $|\cdot|$.

5. Da subaditividade, segue que

$$|c'| = |(c' - c) + c| \leq |c' - c| + |c| ,$$

portanto

$$|c'| - |c| \leq |c' - c| .$$

Simetricamente obtém-se $|c| - |c'| \leq |c' - c|$, e segue que

$$||c'| - |c|| \leq |c' - c| .$$

■

Definição 5.2. Um *corpo normado* é um par $(\boldsymbol{C}, |\cdot|)$ em que $\boldsymbol{C}$ é um corpo e $|\cdot|$ é uma norma em $\boldsymbol{C}$.

Uma norma em $\boldsymbol{C}$ induz uma métrica e essa métrica, por sua vez, induz uma topologia em C.

Definição 5.3. Seja $(\boldsymbol{C}, |\cdot|)$ um corpo normado. A *métrica* (induzida pela norma) de $\boldsymbol{C}$ é a função

$$\begin{aligned} |\cdot,\cdot| \colon C \times C &\longrightarrow [0, \infty[\\ (c, c') &\longmapsto |c' - c| . \end{aligned}$$

Proposição 5.2. *Seja $(\boldsymbol{C}, |\cdot|)$ um corpo normado. A métrica $|\cdot,\cdot|$ induzida pela norma de $\boldsymbol{C}$ é uma métrica em C.*

Proposição 5.3. *Seja $(\boldsymbol{C}, |\cdot|)$ um corpo normado.*

1. *A norma* $|\cdot| : C \longrightarrow [0, \infty[$ *é uma função contínua;*

2. $\boldsymbol{C}$ *é um corpo topológico.*

Demonstração. 1. Segue direta da propriedade de que, para todos $c, c' \in C$, $||c'| - |c|| \leq |c' - c|$, pois dado $\varepsilon > 0$, tomando $\delta = \varepsilon$ temos que, se $|c, c'| = |c' - c| \leq \delta$, então

$$||c|, |c'|| = ||c'| - |c|| \leq |c' - c| \leq \delta = \varepsilon.$$

2. Para mostrar a continuidade de $+$, podemos usar qualquer norma em $C \times C$; escolhemos a norma

$$\begin{aligned} |\cdot|_{C\times C} \colon C \times C &\longrightarrow [0, \infty[\\ (c, c') &\longmapsto |c| + |c'|\,. \end{aligned}$$

Agora, basta notarmos que, dados $(c_0, c_1), (c_0', c_1') \in C \times C$,

$$\begin{aligned} |(c_0' + c_1') - (c_0 + c_1)| &= |(c_0' - c_0) + (c_1' - c_1)| \\ &\leq |c_0' - c_0| + |c_1' - c_1| \\ &= |(c_0' - c_0, c_1' - c_1)|_{C\times C} \\ &= |(c_0', c_1') - (c_0, c_1)|_{C\times C}\,, \end{aligned}$$

portanto, dado $\varepsilon > 0$, basta tomarmos $\delta = \varepsilon$ e segue que, se $|(c_0', c_1') - (c_0, c_1)|_{C\times C} < \delta$, então

$$|(c_0' + c_1') - (c_0 + c_1)| \leq |(c_0', c_1') - (c_0, c_1)|_{C\times C} < \delta = \varepsilon.$$

A continuidade das outras operações é análoga.

■

5.2 Normas

5.2.1 Seminormas

Definição 5.4. Seja $\boldsymbol{L}$ um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$. Uma *seminorma* em $\boldsymbol{L}$ é uma função $p \colon L \longrightarrow \mathbb{R}$ que satisfaz

1. (Homogeneidade absoluta) Para todos $c \in C$ e $v \in L$,

$$p(cv) = |c|\, p(v);$$

2. (Subaditividade) Para todos $v, v' \in L$,

$$p(v + v') \leq p(v) + p(v').$$

Proposição 5.4. *Sejam $\boldsymbol{L}$ um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$ e $p\colon L \longrightarrow C$ uma seminorma em $\boldsymbol{L}$.*

1. *$p(0) = 0$;*
2. *Para todo $v \in L$, $p(v) \geq 0$;*
3. *Para todo $v, v' \in L$, $|p(v) - p(v')| \leq p(v - v')$.*

Definição 5.5. Seja $\boldsymbol{L}$ um espaço linear sobre um corpo $(\boldsymbol{C}, \leq)$ ordenado. Um conjunto *absorvedor* em L é um conjunto $A \subseteq L$ tal que, para todo $v \in L$, existe $c \in C_{>0}$ tal que $v \in cA$.

Proposição 5.5. *Sejam L um espaço linear sobre um corpo $(\boldsymbol{C}, \leq)$ ordenado e $A \subseteq L$ um conjunto absorvedor.*

1. *$0 \in A$;*
2. *Para todo $v \in L$, existe $\inf\{c > 0 \mid v \in cA\}$.*

Definição 5.6. Sejam $\boldsymbol{L}$ um espaço linear real[1] e $A \subseteq L$ um conjunto absorvedor. O *calibre*[2] de A é a função

$$\begin{aligned} p_A\colon L &\longrightarrow \mathbb{R} \\ v &\longmapsto \inf\{c > 0 \mid v \in cA\}. \end{aligned}$$

A função está bem definida pois A é absorvedor (proposição anterior).

Proposição 5.6. *Sejam $\boldsymbol{L}$ um espaço linear real e $A \subseteq L$ um conjunto absorvedor.*

1. *Para todos $v \in L$ e $c \in]0, \infty[$,*

$$p_A(cv) = cp_A(v);$$

2. *Se A é convexo, então p_A é subaditivo: para todos $v, v' \in L$,*

$$p_A(v + v') \leq p_A(v) + p_A(v');$$

[1]Mais geralmente, poderiam ser considerados corpos ordenados normados $(\boldsymbol{C}, \leq, |\cdot|)$, mas os detalhes não serão feitos aqui.

[2]Essas funções são conhecidas comoo funcionais de Minkowski

3. *Se A é convexo e balanceado, p_A é uma seminorma;*

4. *Definindo $A^\circ := \{v \in L \mid p_A(v) < 1\}$ e $\overline{A} := \{v \in L \mid p_A(v) \leq 1\}$, vale $A^\circ \subseteq A \subseteq \overline{A}$ e $p_{A^\circ} = p_A = p_{\overline{A}}$.*

Demonstração. 1. Sejam $v \in L$ e $c \in]0, \infty[$. Então

$$\begin{aligned} p_A(cv) &= \inf\{c' > 0 \mid cv \in c'A\} \\ &= \\ &= \\ &= c \inf\{c' > 0 \mid v \in c'A\} \\ &= cp_A(v). \end{aligned}$$

■

5.2.2 Normas, Espaços Normados e Métricas Lineares

Definição 5.7. Seja $\boldsymbol{E}$ um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$. Uma *norma* em $\boldsymbol{E}$ é uma função $\|\cdot\| : E \longrightarrow \mathbb{R}$ que satisfaz

1. (Separação) Para todo $v \in E$, se $\|v\| = 0$, então $v = 0$.

2. (Homogeneidade absoluta[3]) Para todos $c \in C$ e $v \in E$,

$$\|cv\| = |c| \, \|v\| \, ;$$

3. (Subaditividade[4]) Para todos $v, v' \in E$,

$$\|v + v'\| \leq \|v\| + \|v'\| \, .$$

Uma norma é uma seminorma separada. Claramente $|\cdot| : \mathbb{C} \longrightarrow \mathbb{R}$ é uma norma em $\mathbb{C}$.

Proposição 5.7 (Propriedades da Norma)**.** *Sejam $\boldsymbol{E}$ um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$ e $\|\cdot\|$ uma norma em $\boldsymbol{E}$.*

1. *$\|0\| = 0$;*

2. *Para todo $v \in E$, $\|-v\| = \|v\|$;*

3. *Para todo $v \in E$, $\|v\| \geq 0$.*

[3]Esta propriedade recebe diferentes nomes, incluindo 'Dilatação'.
[4]Esta propriedade recebe diferentes nomes, incluindo 'Desigualdade Triangular'.

4. *(Subaditividade generalizada) Para todos* $v_0, \ldots, v_{n-1} \in E$,

$$\left\| \mathop{+}_{i\in[n]} v_i \right\| \leq \mathop{+}_{i\in[n]} \|v_i\| .$$

5. *Para todos* $v, v' \in E$, $|\|v'\| - \|v\|| \leq \|v' - v\|$.

Definição 5.8. Um *espaço normado* é um par $\mathbb{E} = (\boldsymbol{E}, \|\cdot\|)$ em que $\boldsymbol{E}$ é um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$ e $\|\cdot\|$ é uma norma em $\boldsymbol{E}$. A dimensão de $\mathbb{E}$ é a dimensão do espaço linear $\boldsymbol{E}$.

Definição 5.9. Seja $\boldsymbol{E}$ um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$. Uma *métrica linear* em $\boldsymbol{E}$ é uma métrica[5] $|\cdot,\cdot| : E \times E \longrightarrow \mathbb{R}$ em E que satisfaz

1. (Invariância por translação) Para todos $v, v', w \in E$,

$$|v + w, v' + w| = |v, v'| .$$

2. (Homogeneidade absoluta) Para todos $v, v' \in E$ e $c \in C$,

$$|cv, cv'| = |c|\, |v, v'| ;$$

Definição 5.10. Seja $\mathbb{E}$ um espaço normado. A *métrica* (induzida pela norma) de $\mathbb{E}$ é a função

$$\begin{aligned} |\cdot,\cdot| \colon E \times E &\longrightarrow \mathbb{R} \\ (v, \bar{v}) &\longmapsto \|v - \bar{v}\| . \end{aligned}$$

A *topologia de* $\mathbb{E}$ é a topologia de $(E, |\cdot,\cdot|)$.

Para que essa definição seja boa, mostramos a seguir a proposição.

Proposição 5.8. *Seja* $\mathbb{E}$ *um espaço normado. A função*

$$\begin{aligned} |\cdot,\cdot| \colon E \times E &\longrightarrow \mathbb{R} \\ (v_0, v_1) &\longmapsto \|v_0 - v_1\| . \end{aligned}$$

é uma métrica linear em E.

Demonstração. Primeiro mostramos que $|\cdot,\cdot|$ é uma métrica.

[5] Adotamos aqui a notação $|x, x'|$ em vez da notação mais usual $d(x, x')$.

1. (Separação) Sejam $v, \bar{v} \in E$. Se $v = \bar{v}$, então segue da positividade que

$$|v, \bar{v}| = |v, v| = \|v - v\| = \|v - v\| = \|0\| = 0.$$

Reciprocamente, se $|v, \bar{v}| = 0$, 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

$$|v, \bar{v}| = \|v - \bar{v}\| = \|-1(\bar{v} - v)\| = |-1| \, \|\bar{v} - v\| = |\bar{v}, v| \, .$$

3. (Desigualdade triangular) Sejam $v_0, v_1, v_2 \in E$. Então segue da subaditividade que

$$\begin{aligned} |v_0, v_2| &= \|v_0 - v_2\| \\ &= \|v_0 - v_1 + v_1 - v_2\| \\ &\leq \|v_0 - v_1\| + \|v_1 - v_2\| \\ &= |v_0, v_1| + |v_1, v_2| \, . \end{aligned}$$

Agora, mostremos que $|\cdot, \cdot|$ é métrica linear.

1. (Invariância por translação) Sejam $v, v', w \in E$. Então

$$|v + w, v' + w| = \|(v + w) - (v' + w)\| = \|v - v'\| = |v, v'| \, .$$

2. (Homogeneidade absoluta) Sejam $v, v' \in E$ e $c \in C$. Então

$$|cv, cv'| = \|cv - cv'\| = \|c(v - v')\| = |c| \, \|v - v'\| = |c| \, |v, v'| \, . \qquad \blacksquare$$

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 5.9. *Sejam $\boldsymbol{E}$ um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$ e $|\cdot, \cdot|$ uma métrica linear em $\boldsymbol{E}$. A função*

$$\begin{aligned} \|\cdot\| \colon E &\longrightarrow \mathbb{R} \\ v &\longmapsto |v, 0| \end{aligned}$$

é uma norma em $\boldsymbol{E}$ e a métrica induzida por essa norma é $|\cdot, \cdot|$.

Demonstração. Mostremos primeiro que a função é uma norma.

1. (Separação) Seja $v \in E$. Então $\|v\| = |v, 0| = 0$, logo da separação de $|\cdot, \cdot|$ segue que $v = 0$.

2. (Homogeneidade absoluta) Sejam $c \in C$ e $v \in E$. Então segue da homogeneidade absoluta de $|\cdot, \cdot|$ que

$$\|cv\| = |cv, 0| = |c|\,|v, 0| = |c|\,\|v\|\,.$$

3. (Subaditividade) Sejam $v, v' \in E$. Então da invariância por translação, da simetria e da desigualdade triangular de $|\cdot, \cdot|$ que

$$\begin{aligned}\|v + v'\| &= |v + v', 0| \\ &= |v, -v'| \\ &\leq |v, 0| + |0, -v'| \\ &\leq |v, 0| + |v', 0| \\ &= \|v\| + \|v'\|\,.\end{aligned}$$

Agora, mostremos que a métrica $|\cdot, \cdot|'$ induzida por essa norma é a métrica original $|\cdot, \cdot|$. Sejam $v, v' \in E$. Então da invariância por translação de $|\cdot, \cdot|$ segue que

$$|v, v'|' = \|v - v'\| = |v - v', 0| = |v, v'|\,. \qquad \blacksquare$$

5.2.3 Bolas e Esferas Unitárias e Topologia

Definição 5.11. 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, $\mathbb{B} = \overline{\mathrm{B}}_1(0)$. Com essa notação para a bola unitária, podemos representar qualquer bola de centro c e raio r como $c + r\mathbb{B}$, pois

$$\begin{aligned}c + r\mathbb{B} &= \{c + rv \mid v \in \mathbb{B}\} \\ &= \{c + rv \mid \|v\| \leq 1\} \\ &= \left\{v \;\middle|\; \left\|\frac{v - c}{r}\right\| \leq 1\right\} \\ &= \{v \mid \|v - c\| \leq r\} \\ &= \overline{\mathrm{B}}_r(c).\end{aligned}$$

Proposição 5.10. *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. ■

A topologia de um espaço normado é dada pela sua norma, através da base de abertos formadas pelas bolas. Essa é a topologia dada pela métrica induzida pela norma.

Proposição 5.11. *Seja $\mathbb{E}$ um espaço normado.*

1. *A norma $\|\cdot\| : E \longrightarrow \mathbb{R}$ é uma função contínua.*
2. *$\boldsymbol{E}$ é um espaço linear topológico.*

5.2.4 Equivalência de Normas

Definição 5.12. Seja $\boldsymbol{E}$ um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$. Normas (*topologicamente*) *equivalentes* em $\boldsymbol{E}$ são normas $\|\cdot\|, \|\cdot\|'$ em $\boldsymbol{E}$ que induzem a mesma topologia em E.

Proposição 5.12. *Seja $\boldsymbol{E}$ um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$. Normas $\|\cdot\|, \|\cdot\|'$ em $\boldsymbol{E}$ são equivalentes se, e somente se, existem $c, C \in]0,\infty[$ tais que, para todo $v \in E$,*

$$c\|v\|' \leq \|v\| \leq C\|v\|'.$$

Demonstração. Demonstraremos a volta pois a ida é evidente. Basta mostrar que as bases de bolas são equivalentes. Para isso, mostramos primeiro que uma bola de uma topologia contém uma bola de outra. Sejam $\|\cdot\|, \|\cdot\|'$ normas equivalentes em $\boldsymbol{E}$. Tomemos uma bola $\mathrm{B}_r(v)$ da norma $\|\cdot\|$. Como existe $C \in]0,\infty[$ tal que, para todo $v \in E$, $\|v\| \leq C\|v\|'$, segue que

$$\mathrm{B}'_{rC^{-1}}(v) \subseteq \mathrm{B}_r(v),$$

pois se $v' \in \mathrm{B}'_{rC^{-1}}(v)$, então $\|v' - v\| < rC^{-1}$, logo $C\|v' - v\| < r$, o que implica que $\|v' - v\| < r$, portanto $v' \in \mathrm{B}_r(v)$.

Sendo assim, tomemos uma bola $\mathrm{B}_r(v)$ da norma $\|\cdot\|$ e $x \in \mathrm{B}_r(v)$. Então temos que $\mathrm{B}_{r-\|x-v\|}(x) \subseteq \mathrm{B}_r(v)$ e portanto temos que, pelo argumento do parágrafo anterior, $\mathrm{B}'_{(r-\|x-v\|)C^{-1}}(x) \subseteq \mathrm{B}_{r-\|x-v\|}(x)$, logo

$$\mathrm{B}'_{(r-\|x-v\|)C^{-1}}(x) \subseteq \mathrm{B}_r(v).$$

Simetricamente, mostra-se que

$$\mathrm{B}_{(r-\|x-v\|')c}(x) \subseteq \mathrm{B}'_r(v),$$

portanto as bases de bolas são equivalentes, o que quer dizer que as topologias são a mesma. ■

5.3 Funções Limitadas e Norma de Funções Lineares

Definição 5.13. Sejam $\mathbb{E}$ e $\mathbb{E}'$ espaços normados. Uma função linear *limitada* é uma função linear $L\colon E \longrightarrow E'$ para a qual existe $c \in [0, \infty[$ satisfazendo, para todo $v \in E$,

$$\|L(v)\|' \leq c\,\|v\|\,.$$

Proposição 5.13. *Sejam $\mathbb{E}$ e $\mathbb{E}'$ espaços normados e $L\colon E \longrightarrow E'$ uma função linear. Então L é limitada se, e somente se, é contínua.*

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 $v \in \mathbb{E} \smallsetminus \{0\}$. Então, como $\left\|\delta \frac{v}{\|v\|}\right\| = \delta$, 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 5.14. Sejam $\mathbb{E}$ e $\mathbb{E}'$ espaços normados e $L \in \mathscr{L}(\mathbb{E}, \mathbb{E}')$ uma função linear contínua. A *norma* de L é

$$\|L\| := \inf\left\{c \in [0, \infty[\mid \bigwedge_{v \in \mathbb{E}} \|L(v)\| \leq c\,\|v\|\right\}.$$

Proposição 5.14. *Sejam $\mathbb{E}$ e $\mathbb{E}'$ espaços normados e $L \in \mathscr{L}(\mathbb{E}, \mathbb{E}')$ uma função linear contínua.*

1. *Para todo $v \in E$,*
$$\|Lv\| \leq \|L\| \, \|v\| \, ;$$

2.
$$\begin{aligned} \|L\| &= \sup \left\{ \frac{\|L(v)\|}{\|v\|} \;\middle|\; v \in \mathbb{E} \smallsetminus \{0\} \right\} \\ &= \sup \left\{ \frac{\|L(v)\|}{\|v\|} \;\middle|\; v \in \mathbb{B} \right\} \\ &= \sup \left\{ \|L(v)\| \mid v \in \mathbb{S} \right\}. \end{aligned}$$

Demonstração. 1. Segue direto da definição.

2. Como L é linear, segue que, para todo $v \in E \smallsetminus \{0\}$,
$$\|L(v)\| = \left\| \|v\| \, L\left(\frac{v}{\|v\|}\right) \right\| = \|v\| \left\| L\left(\frac{v}{\|v\|}\right) \right\|,$$
portanto $\|L(v)\| \leq c \, \|v\|$ se, e somente se, $\left\| L\left(\frac{v}{\|v\|}\right) \right\| \leq c$. Isso implica que
$$\|L\| = \sup \left\{ \|L(v)\| \mid v \in \mathbb{S} \right\}.$$

■

Proposição 5.15. *Sejam $\mathbb{E}$ e $\mathbb{E}'$ espaços normados. A função*
$$\begin{aligned} \|\cdot\| \colon \mathscr{L}(\mathbb{E}, \mathbb{E}') &\longrightarrow \mathbb{R} \\ L &\longmapsto \|L\| \end{aligned}$$
é uma norma em $\mathscr{L}(\mathbb{E}, \mathbb{E}')$.

Demonstração. 1. (Separação) Seja $0 \in \mathscr{L}(\mathbb{E}, \mathbb{E}')$. Para todo $v \in E$,
$$\|0(v)\| = \|0\| = 0 \, \|v\| \, ,$$
portanto $\|0\| = 0$.

2. (Homogeneidade absoluta) Sejam $c \in C$ e $L \in \mathscr{L}(\mathbb{E}, \mathbb{E}')$. 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 $L, L' \in \mathscr{L}(\mathbb{E}, \mathbb{E}')$. 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 $\|L + L'\| \leq \|L\| + \|L'\|$. ■

5.4 Espaços Normados Completos

Espaços normados completos são espaços normados que são completos com respeito à métrica induzida pela sua norma. Esses espaços são comumente chamados de 'Espaços de Banach'[6]. Aqui adotaremos simplesmente a nomenclatura de espaços normados completos. Os espaços normados completos mais comuns são os espaços lineares finitos com a norma p, sendo $p \in [1, \infty]$. Além desses espaços, um tipo de espaço mais geral (que inclui esses) são os chamados espaços de funções absolutamente p-somáveis. Esses espaços serão descritos nas seções a seguir.

Proposição 5.16. *Sejam $\boldsymbol{E}$ um espaço linear sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$ e $\|\cdot\|\,, \|\cdot\|'$ normas equivalentes em $\boldsymbol{E}$. O espaço $(\boldsymbol{E}, \|\cdot\|)$ é completo se, e somente se, $(\boldsymbol{E}, \|\cdot\|')$ é completo.*

Essa proposição mostra que, além de induzirem a mesma topologia, a propriedade completude — que faz parte da estrutura uniforme, e não topológica, do espaço — também é induzida por normas equivalentes.

Proposição 5.17. *Sejam $\boldsymbol{X}$ um espaço topológico separado compacto e $(\boldsymbol{C}, |\cdot|)$ um corpo normado. A função*

$$\begin{aligned}\|\cdot\| \colon \mathscr{C}(X, C) &\longrightarrow [0, \infty[\\ f &\longmapsto \sup_{x \in X} |f(x)| = \max_{x \in X} |f(x)|\end{aligned}$$

[6]Em homenagem ao matemático polonês *Stefan Banach* (30/03/1892 – 31/08/1945).

é uma norma em $\mathscr{C}(\boldsymbol{X}, \boldsymbol{C})$ e, se $(\boldsymbol{C}, |\cdot|)$ é completo, o espaço $(\mathscr{C}(\boldsymbol{X}, \boldsymbol{C}), \|\cdot\|)$ é completo.

Proposição 5.18. *Sejam $\boldsymbol{X}$ um espaço topológico compacto e $(\boldsymbol{L}, |\cdot|)$ um espaço linear normado. A função*

$$\begin{aligned} \|\cdot\| \colon \mathscr{C}(X, L) &\longrightarrow [0, \infty[\\ f &\longmapsto \max_{x \in X} |f(x)| \,. \end{aligned}$$

é uma norma no espaço de funções contínuas $\mathscr{C}(\boldsymbol{X}, \boldsymbol{L})$ que induz a mesma topologia do espaço. Se $(\boldsymbol{L}, |\cdot|)$ é completo, $\mathscr{C}(\boldsymbol{X}, \boldsymbol{L})$ é completo.

Demonstração. Primeiro temos que mostrar que a função $\|\cdot\|$ está bem definida, ou seja, que para toda $f \in \mathscr{C}(X, L)$ existe $m \in [0, \infty[$ tal que $m = \max_{x \in X} |f(x)|$. Como X é compacto, para toda $f \in \mathscr{C}(X, L)$ a imagem $f(X) \subseteq L$ é compacta, portanto $|f(X)| \subseteq [0, \infty[$ é compacto e $\max_{x \in X} |f(x)| \in [0, \infty[$.

Mostremos agora que $\|\cdot\|$ é uma norma em $\mathscr{C}(X, L)$: (Separação) Para toda $f \in \mathscr{C}(X, L)$, se $\|f\| = 0$, então $|f(x)| \leq 0$ para todo $x \in X$, logo $|f(x)| = 0$ para todo $x \in X$, e segue pela separação de $|\cdot|$ que $f(x) = 0$, portanto $f = 0$.

(Homogeneidade absoluta) Para todos $c \in C$ e $f \in \mathscr{C}(X, L)$,

$$\|cf\| = \max_{x \in X} |cf(x)| = \max_{x \in X} |c|\,|f(x)| = |c| \max_{x \in X} |f(x)| = |c|\,\|f\| \,.$$

(Desigualdade triangular) Para todas $f, f' \in \mathscr{C}(X, L)$,

$$\begin{aligned} \|f + f'\| &= \max_{x \in X} |f(x) + f'(x)| \\ &\leq \max_{x \in X} (|f(x)| + |f'(x)|) \\ &= \max_{x \in X} |f(x)| + \max_{x \in X} |f'(x)| \\ &= \|f\| + \|f'\| \,. \end{aligned}$$

Por fim, mostremos que $\mathscr{C}(X, L)$ é completo. Seja $\{f_n\}_{n \in \mathbb{N}}$ uma sequência acumulante[7] em $\mathscr{C}(X, L)$. Notemos que, para cada $x \in X$, $\{f_n(x)\}_{n \in \mathbb{N}}$ é uma sequência acumulante em L, portanto uma sequência convergente, já que L é completo. Isso significa que existe $f \in L^X$ que é o limite pontual de $\{f_n\}_{n \in \mathbb{N}}$: para todo $x \in X$,

$$f(x) = \lim_{n \longrightarrow \infty} f_n(x).$$

Basta mostrar agora que $\{f_n\}_{n \in \mathbb{N}}$ converge para f em $\mathscr{C}(X, L)$, pois isso mostra também que $f \in \mathscr{C}(X, L)$. Seja $\varepsilon \in]0, \infty[$. Então existe $N \in \mathbb{N}$ tal que, para todos $n, n' \in \mathbb{N}$ tais que $n, n' \geq N$,

$$\|f_{n'} - f_n\| \leq \varepsilon.$$

[7] Sequência de Cauchy.

Logo, para todo $x \in X$,

$$|f(x) - f_n(x)| = \lim_{n' \longrightarrow \infty} |f_{n'} - f_n| \leq \varepsilon,$$

o que implica que

$$\|f - f_n\| = \max_{x \in X} |f(x) - f_n(x)| \leq \varepsilon.$$

Isso mostra que $f_n \to f$ em $\mathscr{C}(X, L)$. ■

5.4.1 Sequências Absolutamente Somáveis

Definição 5.15. Seja $\boldsymbol{L}$ um espaço linear topológico sobre um corpo topológico $\boldsymbol{C}$. Uma *sequência somável* em $\boldsymbol{L}$ é uma sequência $(v_n)_{n \in \mathbb{N}}$ em L tal que a sequência

$$\left(\mathop{+}_{k \in [n]} v_k \right)_{n \in \mathbb{N}}$$

é convergente.

Definição 5.16. Sejam $(\boldsymbol{E}, \|\cdot\|)$ um espaço normado sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$. Uma *sequência absolutamente somável* em $\boldsymbol{E}$ é uma sequência $(v_n)_{n \in \mathbb{N}}$ em E tal que a sequência

$$\left(\mathop{+}_{k \in [n]} \|v_k\| \right)_{n \in \mathbb{N}}$$

é convergente.

Proposição 5.19. *Sejam $(\boldsymbol{E}, \|\cdot\|)$ um espaço normado sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$. O espaço $(\boldsymbol{E}, \|\cdot\|)$ é completo se, e somente se, toda sequência absolutamente $(v_n)_{n \in \mathbb{N}}$ é somável.*

Demonstração. Suponha que $(\boldsymbol{E}, \|\cdot\|)$ é completo. Seja $(v_n)_{n \in \mathbb{N}}$ um sequência absolutamente somável. Defina a sequência

$$s_n := \left(\mathop{+}_{k \in [n]} v_k \right)_{n \in \mathbb{N}}$$

em E. Para $m > 1$,

$$\|s_m - s_n\| = \left\| \mathop{+}_{k=n}^{m-1} v_k \right\| \leq \mathop{+}_{k=n}^{m-1} \|v_k\| .$$

Como as somas parciais de $+_{n \in \mathbb{N}} \|v_n\|$ formam uma sequência convergente (e portanto aproximante), pois $(v_n)_{n \in \mathbb{N}}$ é absolutamente somável, $+_{k=n}^{m-1} \|v_k\| \to 0$

quando $n, m \to \infty$. Isso mostra que $(s_n)_{n\in\mathbb{N}}$ é aproximante, e da completude de $(\boldsymbol{E}, \|\cdot\|)$ segue que é convergente, o que significa que $(v_n)_{n\in\mathbb{N}}$ é somável.

Reciprocamente, suponha que toda sequência absolutamente somável em $(\boldsymbol{E}, \|\cdot\|)$ é somável. Seja $(v_n)_{n\in\mathbb{N}}$ uma sequência aproximante. Para mostrar que essa sequência converge, basta achar uma subsequência que converge. Escolha $(v_{n_k})_{k\in\mathbb{N}}$ tal que, para todo $k \in \mathbb{N}$, $\left\|v_{n_{k+1}} - v_{n_k}\right\| < 2^{-k}$. Então $+_{k\in\mathbb{N}} \left\|v_{n_{k+1}} - v_{n_k}\right\|$ converge, o que implica que $+_{k\in\mathbb{N}} \left(v_{n_{k+1}} - v_{n_k}\right)$ converge, já que toda sequência absolutamente somável é somável. Isso implica que a sequência $v_{n_m} = v_{n_0} + +_{k\in[m]} \left(v_{n_{k+1}} - v_{n_k}\right)$ converge. Portanto $(v_n)_{n\in\mathbb{N}}$ converge. ■

5.4.2 Espaços Normados de Dimensão Finita

Espaços lineares $\boldsymbol{E}$ de dimensão finita $d \in \mathbb{N}$ sobre um corpo podem ser identificados com $\boldsymbol{C}^{\boldsymbol{d}}$. Nesses casos, a menos que seja mencionado o contrário, sempre consideraremos a base canônica

$$e_i = (0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0)$$

em $\boldsymbol{C}^{\boldsymbol{d}}$ e todo vetor $v \in \boldsymbol{C}^{\boldsymbol{d}}$ será representado como $v = (v_0, \ldots, v_{d-1})$.

Definição 5.17. Sejam $\boldsymbol{E}$ um espaço linear finito d-dimensional sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$ e $p \in [1, \infty[$. A *norma* p em $\boldsymbol{E}$ é a função

$$\begin{aligned} \|\cdot\|_p \colon E &\longrightarrow \mathbb{R} \\ v &\longmapsto \left(\mathop{+}_{i=0}^{d-1} |v_i|^p \right)^{\frac{1}{p}}. \end{aligned}$$

A *norma* ∞ em $\boldsymbol{E}$ é a função

$$\begin{aligned} \|\cdot\|_\infty \colon E &\longrightarrow \mathbb{R} \\ v &\longmapsto \max_{i\in[d]} |v_i|. \end{aligned}$$

Pode-se verificar que $\lim\limits_{p\to\infty} \|v\|_p = \|v\|_\infty$.

Proposição 5.20. *Sejam $\boldsymbol{E}$ um espaço linear finito d-dimensional sobre um corpo normado $(\boldsymbol{C}, |\cdot|)$ e $p \in [1, \infty[$.*

1. *A norma p em $\boldsymbol{E}$ é uma norma;*

2. *Para todo $v \in E$,*
$$\|v\|_\infty \leq \|v\|_p \leq d^{p^{-1}} \|v\|_\infty.$$

Proposição 5.21. *Sejam $\boldsymbol{E}$ um espaço vetorial sobre um corpo normado completo $(\boldsymbol{C}, |\cdot|)$.*

1. *A bola $\mathbb{B}$ é compacta se, e somente se, a dimensão de $\boldsymbol{E}$ é finita.*
2. *Se a dimensão de $\boldsymbol{E}$ é finita, todas normas em $\boldsymbol{E}$ são equivalentes;*
3. *Se a dimensão de $\boldsymbol{E}$ é finita, todas as normas fazem de $\boldsymbol{E}$ um espaço completo.*

Demonstração. 1. Será demonstrado mais adiante.

2. Vamos mostrar que toda norma em $\boldsymbol{E}$ é equivalente a $\|\cdot\|_1$ e, como equivalência de normas é uma relação de equivalência, seguirá que todas normas são equivalentes em $\boldsymbol{E}$. Seja $\|\cdot\|$ uma norma em $\boldsymbol{E}$. Para todo $v \in E$, definindo $c := \max_{i\in[d]} \|e_i\|$, em que $\{e_i\}_{i\in[d]}$ é a base canônica de $\boldsymbol{E}$, segue que

$$\|v\| = \left\| \bigplus_{i=0}^{d-1} v_i e_i \right\| \leq \bigplus_{i=0}^{d-1} |v_i| \, \|e_i\| \leq c \, \|v\|_1 .$$

A outra parte da equivalência segue do fato de que todo conjunto fechado e limitado em $\mathbb{C}$ é sequencialmente compacto.

Suponha, por absurdo, que não exista $C \in]0, \infty[$ tal que, para todo $v \in E$, $C^{-1} \|v\|_1 \leq \|v\|$. Assim, para todo $n \in \mathbb{N}$, existe $v_n \in E$ com $\|v_n\|_1 = 1$ e $1 = \|v_n\|_1 > N \|v_n\|$. Como $\mathbb{S}$ é compacta, já que a dimensão é finita, existe subsequência $(v_{n_k})_{k\in\mathbb{N}}$ convergindo a v' em $(\boldsymbol{E}, \|\cdot\|_1)$. Como a norma é contínua, segue que $\|v'\|_1 = 1$. Pela desigualdade anterior, tem-se

$$\|v'\| \leq \|v' - v_{n_k}\| + \|v_{n_k}\| \leq c \, \|v' - v_{n_k}\|_1 + \frac{1}{n_k},$$

que converge para 0 quando $k \to \infty$; ou seja, $\|v'\| = 0$ e portanto $v' = 0$, o que contradiz $\|v'\|_1 = 1$.

3. Como todas as normas são equivalentes, basta provar para $\|\cdot\|_1$. Seja $(v_n)_{n\in\mathbb{N}} = (\bigplus_{i\in[d]} v_n^i e_i)_{n\in\mathbb{N}}$ uma sequência aproximante em $(\boldsymbol{E}, \|\cdot\|_1)$. Como

$$\bigplus_{i\in[d]} \left| v_n^i - v_{n'}^i \right| = \|v_n - v_{n'}\|_1 ,$$

segue que, para todo $i \in [d]$, a sequência $(v_n^i)_{n\in\mathbb{N}}$ é aproximante em $\boldsymbol{C}$ e então, da completude de $\boldsymbol{C}$, converge para algum $v_\infty^i \in C$. Definindo $v_\infty := \bigplus_{i\in[d]} v_\infty^i e_i$ em $\boldsymbol{E}$, segue que

$$\lim_{n\to\infty} \|v_n - v_\infty\|_1 = \lim_{n\to\infty} \bigplus_{i\in[d]} \left| v_n^i - v_\infty^i \right| = 0,$$

ou seja, $(v_n)_{n\in\mathbb{N}} \to v_\infty$ e o espaço é completo.

■

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.

5.4.3 Espaços de Funções Absolutamente Somáveis

Definição 5.18. Sejam X um conjunto, $(\boldsymbol{C}, |\cdot|)$ um corpo normado e $p \in [0, \infty[$. Uma função *absolutamente p-somável* (ou *absolutamente somável na potência p*) é uma função $f\colon X \longrightarrow C$ tal que

$$\mathop{+}_{x\in X} |f(x)|^p < \infty.$$

O conjunto das funções absolutamente p-somáveis é denotado $\mathscr{S}^p(X, C)$.

Uma função *absolutamente ∞-somável* (ou *absolutamente somável na potência* ∞, ou ainda *essencialmente absolutamente somável*) é uma função $f\colon X \longrightarrow C$ tal que

$$\sup_{x\in X} |f(x)| < \infty.$$

O conjunto das funções absolutamente ∞-somáveis é denotado $\mathscr{S}^\infty(X, C)$.

Note que as definições implicam que, para todo $p \in [0, \infty]$, as funções $f \in \mathscr{S}^p(X, C)$ são nulas a menos de um subconjunto contável de X; ou seja, têm suporte contável: $|\mathrm{supp}(f)| \leq |\mathbb{N}|$. O conjunto $\mathscr{S}^0(X, C)$ é, de fato, o conjunto de funções com suporte finito, pois a soma será finita se, e somente se, a função tiver uma quantidade finita de valores. O conjunto $\mathscr{S}^\infty(X, C)$ é o conjunto das funções de valor absoluto (ou norma) limitado. Quando $X = \mathbb{N}$ ou $X = \mathbb{Z}$, os espaços são espaços de sequências infinitas unilaterais ou bilaterais, respectivamente. Esses espaços são todos subespaços lineares do espaço C^X de funções $f\colon X \longrightarrow C$, que é espaço linear já que o corpo $\boldsymbol{C}$ é um espaço linear sobre si mesmo.

Proposição 5.22. *Sejam X um conjunto, $(\boldsymbol{C}, |\cdot|)$ um corpo normado e $p \in [0, \infty[$. O espaço $\mathscr{S}^p(X, C)$ é subespaço linear de C^X.*

Demonstração. Consideramos dois casos. (1) Seja $p \in [1, \infty[$. Para todos $c \in C$ e

$f, f' \in \mathscr{S}^p(X, C)$,

$$\begin{aligned}
\mathop{\text{+}}_{x\in X} |(cf + f')(x)|^p &= \mathop{\text{+}}_{x\in X} |cf(x) + f'(x)|^p \\
&\leq \mathop{\text{+}}_{x\in X} (|c|\,|f(x)| + |f'(x)|)^p \\
&\leq 2^{p-1} \left(|c|^p \mathop{\text{+}}_{x\in X} |f(x)|^p + \mathop{\text{+}}_{x\in X} |f'(x)|^p \right) \\
&< \infty,
\end{aligned}$$

pois $\text{+}_{x\in X} |f(x)|^p < \infty$ e $\text{+}_{x\in X} |f'(x)|^p < \infty$. Isso mostra que $cf + f' \in \mathscr{S}^p(X, C)$, portanto que $\mathscr{S}^p(X, C)$ é um espaço linear, subespaço de C^X.

(2) Para todos $c \in C$ e $f, f' \in \mathscr{S}^\infty(X, C)$,

$$\sup_{x\in X} |(cf + f')(x)| \leq |c| \sup_{x\in X} |f(x)| + \sup_{x\in X} |f'(x)| < \infty,$$

pois $\sup_{x\in X} |f(x)| < \infty$ e $\sup_{x\in X} |f'(x)| < \infty$. Isso mostra que $cf + f' \in \mathscr{S}^\infty(X, C)$, portanto que $\mathscr{S}^\infty(X, C)$ é um espaço linear, subespaço de C^X. ■

Embora esses espaços possam ser definidos para quaisquer $p \in [0, \infty]$ e sejam espaços lineares em todos os casos, nem todos esses espaços admitem os mesmos tipos de estrutura além da de espaço linear.

Definição 5.19. Sejam X um conjunto e $(\boldsymbol{C}, |\cdot|)$ um corpo normado.

1. Para todo $p \in [0, 1[$, a *distância* p entre $f, f' \in \mathscr{S}^p(X, C)$ é
$$|f, f'|_p := \mathop{\text{+}}_{x\in X} |f'(x) - f(x)|^p .$$

2. Para todo $p \in [1, \infty[$, a *norma* p de $f \in \mathscr{S}^p(X, C)$ é
$$\|f\|_p := \left(\mathop{\text{+}}_{x\in X} |f(x)|^p \right)^{p^{-1}} .$$

   A *norma* ∞ de $f \in \mathscr{S}^\infty(X, C)$ é
$$\|f\|_\infty := \sup_{x\in X} |f(x)| .$$

A função $\|\cdot\|_p$ é uma norma em $\mathscr{S}^p(X, C)$, a *norma* p, e p pode ser descrito como a *potência* da norma e do espaço. Quando X é finito, esse espaço é simplesmente o espaço vetorial finito C^X definido anteriormente e as p-normas definidas para espaços de dimensão finita coincidem com essas. Quando $X = \mathbb{N}$ ou $X = \mathbb{Z}$, os espaços são espaços de sequências infinitas unilaterais ou bilaterais, respectivamente.

Proposição 5.23. *Sejam X um conjunto e $(\boldsymbol{C}, |\cdot|)$ um corpo normado completo.*

1. *Para todo $p \in [0,1[$, o espaço $(\mathscr{S}^p(X,C), |\cdot,\cdot|_p)$ é um espaço métrico completo;*

2. *Para todo $p \in [1,\infty]$, o espaço $(\mathscr{S}^p(X,C), \|\cdot\|_p)$ é um espaço normado completo.*

5.4.4 Espaços de Funções Absolutamente Integráveis

Consideraremos funções de um espaço de medida $\boldsymbol{X}$ para um corpo normado $\boldsymbol{C}$. Esse corpo deve ser entendido, em geral, como $\mathbb{R}$ ou $\mathbb{C}$, pois alguns detalhes não serão especificados, por exemplo qual a estrutura de espaço de medida de um corpo normado qualquer, ou ainda um problema maior, o que é a integral de uma função com valores em um corpo qualquer.

Lembremos que o conjunto de funções mensuráveis de $\boldsymbol{X}$ para $\boldsymbol{C}$ é denotadas $\mathscr{M}(\boldsymbol{X},\boldsymbol{C})$ e o conjunto das quase funções (classe de equivalência de funções que são iguais a menos de um conjunto de medida nula) mensuráveis é denotado $\mathscr{M}_{\doteq}(\boldsymbol{X},\boldsymbol{C})$.

Antes da definição a seguir, ressaltamos dois comentários. Primeiro, definimos que elevar um número positivo a 0 dará o seguinte resultado:

$$\begin{aligned}(\cdot)^0 \colon [0,\infty[&\longrightarrow [0,\infty[\\ x &\longmapsto \begin{cases} 0, & x = 0\\ 1, & x \neq 0.\end{cases}\end{aligned}$$

Isso faz com que, para toda função $f \colon X \longrightarrow C$,

$$|f|^0 = \mathbf{1}_{\operatorname{supp}(f)}.$$

Segundo, lembremos que o supremo essencial de uma função f é definido por

$$\sup \operatorname{ess}(f) := \inf \left\{ t \in]0,\infty[\;\middle|\; \mathring{\bigwedge}_{x\in X} f(x) \leq t \right\},$$

em que $\mathring{\bigwedge}$ é 'para quase todo', ou seja, existe conjunto nulo N tal que, para todo $x \in X \smallsetminus N$, a propriedade vale.

Definição 5.20. Sejam $\boldsymbol{X}$ um espaço de medida, $(\boldsymbol{C}, |\cdot|)$ um corpo normado e $p \in [0,\infty[$. Uma função *absolutamente p-integrável*[8] de $\boldsymbol{X}$ para $\boldsymbol{C}$ é uma função

[8]Essas funções não recebem esse nome usualmente. O espaço $\mathscr{I}^p(\boldsymbol{X},\boldsymbol{C})$ é geralmente chamado de espaço $L^p(\boldsymbol{X},\boldsymbol{C})$, 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`).

$f \in \mathscr{M}(\boldsymbol{X}, \boldsymbol{C})$ tal que

$$\int |f|^p \, \mathrm{d}m < \infty.$$

O conjunto das quase funções absolutamente p-integráveis é denotado $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$.

Uma função *absolutamente ∞-integrável* é uma função $f \in \mathscr{M}(\boldsymbol{X}, \boldsymbol{C})$ tal que

$$\sup \operatorname{ess}(|f|) < \infty.$$

O conjunto das quase-funções absolutamente ∞-integráveis é denotado $\mathscr{I}^\infty(\boldsymbol{X}, \boldsymbol{C})$.

Note que, os espaços $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ são espaços de quase funções, ou seja, espaços de classes de equivalência de funções, cuja equivalência é ser igual a menos de um conjunto de medida nula. Na prática, trataremos essas quase funções como funções, mas esse detalhe tem que estar sempre claro para o leitor.

Por definição, para todo $p \in [0, \infty]$, vale que

$$\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}) \subseteq \mathscr{M}_{\doteq}(\boldsymbol{X}, \boldsymbol{C}),$$

pois $\mathscr{M}_{\doteq}(\boldsymbol{X}, \boldsymbol{C})$ é o espaço de quase-funções mensuráveis. As inclusões não são somente de conjuntos, no entanto. De fato, como $\mathscr{M}_{\doteq}(\boldsymbol{X}, \boldsymbol{C})$ é um espaço linear, os espaços $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ herdam uma estrutura de espaço linear e pode-se mostrar que eles são subespaços lineares de $\mathscr{M}_{\doteq}(\boldsymbol{X}, \boldsymbol{C})$. Inclusões relacionando diferentes espaços $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ e $\mathscr{I}^q(\boldsymbol{X}, \boldsymbol{C})$ não são tão óbvias e não serão abordadas por enquanto. O caso em que $p = 0$ nos dá que $\mathscr{I}^0(\boldsymbol{X}, \boldsymbol{C})$ é o conjunto das funções cujo suporte tem medida finita.

Esta proposição auxiliará a demonstração da proposição seguinte.

Proposição 5.24. *Sejam $a, b \in [0, \infty]$.*

1. *Para todo $p \in [0, 1]$,*
$$(a + b)^p \leq a^p + b^p;$$

2. *Para todo $p \in [1, \infty[$,*
$$(a + b)^p \leq 2^{p-1}(a^p + b^p).$$

Demonstração. 1. Para $p \in [0, 1]$, como a função

$$\begin{aligned} (\cdot)^p \colon [0, \infty[&\longrightarrow [0, \infty[\\ t &\longmapsto t^p \end{aligned}$$

é côncava[9] e $0^p = 0 \geq 0$, segue que ela é subaditiva[10].

[9] Inclusive para $p = 0$ e $p = 1$.

[10] A demonstração é simples e pode ser conferida em `https://en.wikipedia.org/wiki/Subadditivity`

2. Para $p \in [1, \infty[$, como a função

$$\begin{aligned}(\cdot)^p \colon [0, \infty[&\longrightarrow [0, \infty[\\ t &\longmapsto t^p\end{aligned}$$

é convexa[11], segue que

$$(a+b)^p = 2^p(2^{-1}a + 2^{-1}b)^p \leq 2^p\left(2^{-1}a^p + 2^{-1}b^p\right) = 2^{p-1}(a^p + b^p).$$

■

Proposição 5.25. *Sejam $\boldsymbol{X}$ um espaço de medida, $\boldsymbol{C}$ um corpo normado e $p \in [0, \infty]$. O espaço $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ é um espaço linear.*

Demonstração. Demonstraremos que os espaços $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ são espaços lineares mostrando que são subespaços lineares de $\mathscr{M}_{\doteq}(\boldsymbol{X}, \boldsymbol{C})$. Sejam $c \in C$ e $f, f' \in \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$. Consideramos três casos.

1. Seja $p \in [0, 1[$. Segue de 5.24 e da homogeneidade absoluta e subaditividade de $|\cdot|$ que

$$|cf + f'|^p \leq ||cf| + |f'||^p \leq |c|^p\,|f|^p + |f'|^p\,.$$

Como $\int |f|^p \,\mathrm{d}m < \infty$ e $\int |f'|^p \,\mathrm{d}m < \infty$,

$$\begin{aligned}\int |cf + f'|^p \,\mathrm{d}m &\leq \int \left(|c|^p\,|f|^p + |f'|^p\right) \mathrm{d}m \\ &= |c|^p \int |f|^p \,\mathrm{d}m + \int |f'|^p \,\mathrm{d}m \\ &< \infty,\end{aligned}$$

o que mostra que $cf + f' \in \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$.

2. Seja $p \in [1, \infty[$. Segue de 5.24 e da homogeneidade absoluta e subaditividade de $|\cdot|$ que

$$|cf + f'|^p \leq ||cf| + |f'||^p \leq 2^{p-1}\left(|c|^p\,|f|^p + |f'|^p\right).$$

Como $\int |f|^p \,\mathrm{d}m < \infty$ e $\int |f'|^p \,\mathrm{d}m < \infty$, segue dessa desigualdade que

$$\begin{aligned}\int |cf + f'|^p \,\mathrm{d}m &\leq \int 2^{p-1}\left(|c|^p\,|f|^p + |f'|^p\right) \mathrm{d}m \\ &= 2^{p-1}\left(|c|^p \int |f|^p \,\mathrm{d}m + \int |f'|^p \,\mathrm{d}m\right) \\ &< \infty,\end{aligned}$$

o que mostra que $cf + f' \in \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$.

[11] Note que vale também para $p = 1$.

3. Para $p = \infty$, é claro que, como $|cf + f'| \leq |c|\,|f| + |f'|$,

$$\sup\operatorname{ess}(|cf + f'|) \leq |c| \sup\operatorname{ess}(|f|) + \sup\operatorname{ess}(|f'|) < \infty,$$

pois $\sup\operatorname{ess}(|f|) < \infty$ e $\sup\operatorname{ess}(|f'|) < \infty$, o que mostra que $cf + f' \in \mathscr{I}^{\infty}(\boldsymbol{X}, \boldsymbol{C})$. ■

Definição 5.21. Sejam $\boldsymbol{X}$ um espaço de medida e $(\boldsymbol{C}, |\cdot|)$ um corpo normado.

1. Para todo $p \in [0, 1[$, a *distância* p entre $f, f' \in \mathscr{M}_{\doteq}(\boldsymbol{X}, \boldsymbol{C})$ é

$$|f, f'|_p := \int |f' - f|^p \,\mathrm{d}m.$$

2. Para todo $p \in [1, \infty[$, a *norma* p de $f \in \mathscr{M}_{\doteq}(\boldsymbol{X}, \boldsymbol{C})$ é

$$\|f\|_p := \left(\int |f|^p \,\mathrm{d}m\right)^{p^{-1}}.$$

3. A *norma* ∞ de $f \in \mathscr{M}_{\doteq}(\boldsymbol{X}, \boldsymbol{C})$ é

$$\|f\|_{\infty} := \sup\operatorname{ess}(|f|).$$

Esses valores nem sempre são menores que ∞ para qualquer quase-função mensurável. As distâncias p são de fato distâncias quando restritas a $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$, $p \in [0, 1[$, e as normas p são de fato normas quando restritas a $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$, $p \in [1, \infty]$, mas ainda não demonstraremos isso. Para essas demonstrações, precisamos primeiro estabelecer algumas desigualdade clássicas que envolvem esses valores. Essas normas serão avaliadas mais à frente em quase-funções mensuráveis quaisquer,

Desigualdades das Normas p

Nesta seção, trabalharemos com pares de números $p, q \in [1, \infty]$ tais que

$$p^{-1} + q^{-1} = 1.$$

Esses números p e q são às vezes chamados de 'conjugados de Hölder'. Como $p^{-1} + q^{-1} = 1$, segue que $q = \frac{p}{p-1}$. Além disso, esses são os pares de números cuja média hamônica é igual a 2, já que

$$H(p, q) = \frac{2}{p^{-1} + q^{-1}} = 2.$$

Por causa disso, chamaremos esses números de *duais harmônicos*[12]. O fato de 2 ser o dual de 2 será relevante na teoria de espaços com produto interno completos. Sob essa perspectiva, 2 está no 'meio da caminho' entre 1 e ∞. Deve-se comentar a respeito de $p = 1$ ou $p = \infty$. Consideraremos que 1 e ∞ são duais harmônicos, como se tivéssemos $\infty^{-1} = 0$, de modo que $1^{-1} + \infty^{-1} = 1$. Em geral, no entanto, tomaremos cuidado para não realizarmos operações mal definidas com 0 e ∞, e na prática bastará a afirmação de que 1 e ∞ são conjugados.

Definição 5.22. A função *dual harmônico* em $[1, \infty]$ é

$$\begin{aligned} {}^*\colon [1,\infty] &\longrightarrow [1,\infty] \\ p &\longmapsto p^* = \begin{cases} \infty, & p = 1 \\ \dfrac{p}{p-1}, & p \in \,]1,\infty[\\ 1, & p = \infty \end{cases}. \end{aligned}$$

Figura 5.1: Gráfico da função ${}^*\colon [1,\infty] \longrightarrow [1,\infty]\,, p \longmapsto \frac{p}{p-1}$.

Proposição 5.26 ([13])**.** *Sejam $a, b \in [0, \infty[$ e $p \in \,]1, \infty[$. Então*

$$ab \leq a^p p^{-1} + b^{p^*} p^{*-1}$$

e a igualdade vale se, e somente se, $a^p = b^{p^*}$.

[12] A escolha do termo *dual* ficará clara mais adiante, quando forem analisadas as propriedades do espaço dual de $\mathscr{L}^p$

[13] Essa desiguldade é conhecida como 'desigualdade de produtos de Young', em homenagem ao matemático inglês *William Henry Young* (20/10/1863 – 07/07/1942). `https://en.wikipedia.org/wiki/Young%27s_inequality_for_products`.

Demonstração. Para $a = 0$ ou $b = 0$, a afirmação é claramente verdadeira. Considere $a \neq 0$ e $b \neq 0$. Como $p^{-1} + p^{*-1} = 1$, da concavidade da função logarítmica segue que

$$\llcorner(ab) = \llcorner(a) + \llcorner(b) = p^{-1}\llcorner(a^p) + p^{*-1}\llcorner(b^{p^*}) \leq \llcorner(p^{-1}a^p + p^{*-1}b^{p^*}).$$

e a igualdade vale se, e somente se, $a^p = b^{p^*}$. Como a função exponencial é crescente, conclui-se que $ab \leq a^p p^{-1} + b^{p^*} p^{*-1}$. ■

Essa desigualdade será usada na próxima demonstração.

Proposição 5.27 ([14]). *Sejam $\boldsymbol{X}$ um espaço de medida, $(\boldsymbol{C}, |\cdot|)$ um corpo normado e $p \in [1, \infty]$. Para todas funções $f, f' \in \mathscr{M}_{\doteq}(\boldsymbol{X}, \boldsymbol{C})$,*

$$\|ff'\|_1 \leq \|f\|_p \|f'\|_{p^*}.$$

Demonstração. Primeiro, tratamos de alguns casos triviais. Se $\|f\|_p = 0$, então $f = 0$, portanto $ff' = 0$ e segue que $\|ff'\|_1 = 0$, logo a desigualdade vale. O mesmo vale para $\|f'\|_{p^*} = 0$, portanto assumimos que $\|f\|_p \neq 0$ e $\|f'\|_{p^*} \neq 0$. Se $\|f\|_p = \infty$ ou $\|f'\|_{p^*} = \infty$, então $\|f\|_p \|f'\|_{p^*} = \infty$, logo a desigualdade vale. Portanto assumimos também que $\|f\|_p \neq \infty$ e $\|f'\|_{p^*} \neq \infty$. Se $p = \infty$ e $p^* = 1$, então $|ff'| \leq \|f\|_\infty |f'|$ quase sempre, e a desigualdade segue da monotonicidade da integral. O mesmo vale para $p = 1$ e $p^* = \infty$, portanto podemos assumir ainda que $p, p^* \in]1, \infty[$.

Pela desigualdade de produtos 5.26, segue que, para todo $x \in X$,

$$\left|\frac{f(x)}{\|f\|_p}\frac{f'(x)}{\|f'\|_{p^*}}\right| \leq \left|\frac{f(x)}{\|f\|_p}\right|^p p^{-1} + \left|\frac{f'(x)}{\|f'\|_{p^*}}\right|^{p^*} p^{*-1}.$$

Integrando ambos os lados, segue que

$$\frac{\|ff'\|_1}{\|f\|_p \|f'\|_{p^*}} \leq \frac{\|f\|_p^p}{\|f\|_p^p} p^{-1} + \frac{\|f'\|_{p^*}^{p^*}}{\|f'\|_{p^*}^{p^*}} p^{*-1} = p^{-1} + p^{*-1} = 1,$$

portanto $\|ff'\|_1 \leq \|f\|_p \|f'\|_{p^*}$, o que demonstra a proposição. ■

[14] Essa desigualdade é conhecida como 'desigualdade de Hölder', em homenagem ao matemático alemão *Otto Ludwig Hölder* (22/12/1859 – 29/08/1937). `https://en.wikipedia.org/wiki/H%C3%B6lder%27s_inequality`.

Os espaços de funções absolutamente integráveis são normados (e completos)

Para todo $p \in [0, \infty]$, os espaços $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ são espaços lineares, pois são subespaços de $\mathscr{M}_{\hat{=}}(\boldsymbol{X}, \boldsymbol{C})$. Além disso, para $p \in [1, \infty]$, a norma p é de fato uma norma em $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ e, se o corpo normado $\boldsymbol{C}$ for completo, a distância induzida pela norma faz de $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ um espaço normado completo[15]. O ponto mais difícil da demonstração é a subaditividade[16] da norma p.

Para $p \in [0, 1[$, não se pode definir uma norma desse mesmo modo, pois a subaditividade falha, mas a distância p é de fato uma distância em $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ e, se o corpo normado $\boldsymbol{C}$ for completo, $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ é completo.

Proposição 5.28. *Sejam $\boldsymbol{X}$ um espaço de medida e $(\boldsymbol{C}, |\cdot|)$ um corpo normado.*

1. *Para todo $p \in [0, 1[$, o espaço $(\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}), |\cdot, \cdot|_p)$ é um espaço métrico invariante por translação. Se $(\boldsymbol{C}, |\cdot|)$ é completo, então $(\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}), |\cdot, \cdot|_p)$ é completo.*

2. *Para todo $p \in [1, \infty]$. O espaço $(\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}), \|\cdot\|_p)$ é um espaço normado. Se $(\boldsymbol{C}, |\cdot|)$ é completo, então $(\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}), \|\cdot\|_p)$ é completo.*

Demonstração. 1. Exercício.

2. (Separação) Seja $f \in \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ tal que $\|f\|_p = 0$. Então $|f|^p = 0$, portanto $f = 0$.

   (Homogeneidade absoluta) Sejam $c \in C$ e $f \in \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$. Então

$$\begin{aligned}
\|cf\|_p &= \left(\int |cf|^p \, \mathrm{d}m\right)^{p^{-1}} \\
&= \left(|c|^p \int |f|^p \, \mathrm{d}m\right)^{p^{-1}} \\
&= |c| \left(\int |f|^p \, \mathrm{d}m\right)^{p^{-1}} \\
&= |c| \, \|f\|_p .
\end{aligned}$$

[15] Esse resultado de completude é conhecido por 'teorema de Riesz–Fischer', em homenagem ao matemático húngaro *Frigyes Riesz* (22/01/1880 – 28/02/1956) e ao matemático austríaco *Ernst Sigismund Fischer* (12/07/1875 – 14/11/1954). `https://en.wikipedia.org/wiki/Riesz%E2%80%93Fischer_theorem`

[16] A subaditividade para normas p é conhecida como 'desigualdade de Minkowski', em homenagem ao matemático alemão *Hermann Minkowski* (22/06/1864 – 12/01/1909). `https://en.wikipedia.org/wiki/Minkowski_inequality`.

(Subaditividade) Sejam $f, f' \in \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$. Se $\|f + f'\|_p = 0$, então claramente $\|f + f'\|_p = 0 \leq \|f\|_p + \|f'\|_p$. Assumamos então que $\|f + f'\|_p \neq 0$. Pela subaditividade de $|\cdot|$ e pela desigualdade 5.27, segue que

$$\begin{aligned}
\|f + f'\|_p^p &= \int |f + f'|^p \, \mathrm{d}m \\
&= \int |f + f'| \, |f + f'|^{p-1} \, \mathrm{d}m \\
&\leq \int (|f| + |f'|) \, |f + f'|^{p-1} \, \mathrm{d}m \\
&= \int |f| \, |f + f'|^{p-1} \, \mathrm{d}m + \int |f'| \, |f + f'|^{p-1} \, \mathrm{d}m \\
&= \left\| |f| \, |f + f'|^{p-1} \right\|_1 + \left\| |f'| \, |f + f'|^{p-1} \right\|_1 \\
&\leq \||f|\|_p \left\| |f + f'|^{p-1} \right\|_{p^*} + \||f'|\|_p \left\| |f + f'|^{p-1} \right\|_{p^*} \\
&= \left(\|f\|_p + \|f'\|_p \right) \left\| |f + f'|^{p-1} \right\|_{p^*} \\
&= \left(\|f\|_p + \|f'\|_p \right) \left(\int |f + f'|^{(p-1)p(p-1)^{-1}} \, \mathrm{d}m \right)^{p^{-1}(p-1)} \\
&= \left(\|f\|_p + \|f'\|_p \right) \left(\int |f + f'|^p \, \mathrm{d}m \right)^{p^{-1}(p-1)} \\
&= \left(\|f\|_p + \|f'\|_p \right) \left(\|f + f'\|_p \right)^{p-1} .
\end{aligned}$$

Multiplicando por $\left(\|f + f'\|_p \right)^{1-p}$ em ambos os lados, conclui-se que

$$\|f + f'\|_p \leq \|f\|_p + \|f'\|_p .$$

Isso mostra que $(\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}), \|\cdot\|_p)$ é um espaço normado.

Suponhamos agora que $(\boldsymbol{C}, |\cdot|)$ é completo. Para mostrar que $(\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}), \|\cdot\|_p)$ é completo, basta mostrar toda sequência absolutamente somável é somável (5.19). Seja $(f_n)_{n \in \mathbb{N}}$ uma sequência absolutamente somável em $(\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}), \|\cdot\|_p)$. Consideramos dois casos.

(a) Para $p \in [1, \infty[$. Notemos que, para todo $k \in \mathbb{N}$, f_k é mensurável, portanto $+_{k \in [n]} |f_k|$ e $\left(+_{k \in [n]} |f_k| \right)^p$ também são mensuráveis. Como

$$0 \leq \mathop{+}_{k \in [n]} |f_k| \leq \mathop{+}_{k \in [n+1]} |f_k| ,$$

e

$$0 \leq \left(\mathop{+}_{k \in [n]} |f_k| \right)^p \leq \left(\mathop{+}_{k \in [n+1]} |f_k| \right)^p ,$$

segue que do Teorema da Convergência Monótona que o limite $\bigplus_{k\in\mathbb{N}} |f_k|$ é mensurável e que

$$\begin{aligned}
\left\| \bigplus_{k\in\mathbb{N}} |f_k| \right\|_p &= \left(\int \left(\lim_{n\longrightarrow\infty} \bigplus_{k\in[n]} |f_k| \right)^p \mathrm{d}m \right)^{p^{-1}} \\
&= \left(\int \lim_{n\longrightarrow\infty} \left(\bigplus_{k\in[n]} |f_k| \right)^p \mathrm{d}m \right)^{p^{-1}} \\
&= \left(\lim_{n\longrightarrow\infty} \int \left(\bigplus_{k\in[n]} |f_k| \right)^p \mathrm{d}m \right)^{p^{-1}} \\
&= \lim_{n\longrightarrow\infty} \left(\int \left(\bigplus_{k\in[n]} |f_k| \right)^p \mathrm{d}m \right)^{p^{-1}} \\
&= \lim_{n\longrightarrow\infty} \left\| \bigplus_{k\in[n]} |f_k| \right\|_p \\
&\leq \lim_{n\longrightarrow\infty} \bigplus_{k\in[n]} \|f_k\|_p \\
&< \infty,
\end{aligned}$$

em que a segunda igualdade segue da continuidade de $(\cdot)^p$, a terceira segue do Teorema da Convergência Monótona, a quarta segue da continuidade de $(\cdot)^{p^{-1}}$ e a sexta da subaditividade de $\|\cdot\|_p$.
Isso mostra que $\bigplus_{k\in\mathbb{N}} |f_k| \in \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ e, portanto, que para quase todo ponto $x \in X$, $\bigplus_{k\in\mathbb{N}} |f_k(x)| \in [0, \infty[$. Assim, para quase todo $x \in X$, a sequência $(f_k(x))_{n\in\mathbb{N}}$ é absolutamente somável em $\boldsymbol{C}$ e, da completude de $\boldsymbol{C}$, segue que é somável e está definido o limite pontual

$$s(x) := \bigplus_{k\in\mathbb{N}} f_k(x).$$

A função s está definida para quase todo $x \in X$ e é mensurável. Para todo $n \in \mathbb{N}$, segue da continuidade e da subaditividade de $|\cdot|$ que

$$|s| = \lim_{n\longrightarrow\infty} \left| \bigplus_{k\in[n]} f_k \right| \leq \lim_{n\longrightarrow\infty} \bigplus_{k\in[n]} |f_k| \leq \bigplus_{k\in\mathbb{N}} |f_k|,$$

portanto

$$\|s\|_p = \left(\int |s|^p \,\mathrm{d}m \right)^{p^{-1}} \leq \left(\int \left| \bigplus_{k\in\mathbb{N}} |f_k| \right|^p \mathrm{d}m \right)^{p^{-1}} = \left\| \bigplus_{k\in\mathbb{N}} |f_k| \right\|_p,$$

o que mostra que $s \in \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$.

Temos que

$$\begin{aligned}\left|s - \mathop{+}_{k\in[n]} f_k(x)\right|^p &= \left|\mathop{+}_{k\in\mathbb{N}} f_{n+k}(x)\right|^p \\ &= \left(\mathop{+}_{k\in\mathbb{N}} |f_{n+k}(x)|\right)^p \\ &\leq 2^p \left(\mathop{+}_{k\in\mathbb{N}} |f_k|\right)^p .\end{aligned}$$

Como a função do lado direito é integrável e, para quase todo $x \in X$, $\left|s(x) - +_{k\in[n]} f_k(x)\right|^p \to 0$, do Teorema da Convergência Dominada segue que

$$\int \left|s - \mathop{+}_{k\in[n]} f_k\right|^p \mathrm{d}m \longrightarrow 0,$$

portanto $\left\|s - +_{k\in[n]} f_k\right\|_p^p \longrightarrow 0$, o que implica que $\left\|s - +_{k\in[n]} f_k\right\|_p \longrightarrow 0$.

(b) Para $p = \infty$, a demonstração se reduz a uma questão de convergência fora de conjuntos quase vazios.

■

O caso anterior de espaços de funções absolutamente somáveis

Os espaços $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ da subseção anterior são casos particulares dos espaços absolutamente p-integráveis. Consideramos o espaço de medida $(X, \mathsf{P}(X), \#)$, em que X é um conjunto qualquer, o conjunto das partes $\mathsf{P}(X)$ é a sigma-álgebra de X, e $\#$ é a medida de contagem

$$\begin{aligned}\#\colon \mathsf{P}(X) &\longrightarrow [0, \infty] \\ C &\longmapsto \begin{cases} |M|, & |M| < |\mathbb{N}| \\ \infty, & |M| \geq |\mathbb{N}| . \end{cases}\end{aligned}$$

Notemos que todas as funções $f \in C^X$ são mensuráveis nesse caso, pois $\mathsf{P}(X)$ é a maior sigma-álgebra em X. Ainda, temos que

$$\int_X |f|^p \,\mathrm{d}\# = \mathop{+}_{x\in X} |f(x)|^p$$

e

$$\sup \operatorname{ess}(|f|) = \sup_{x \in X} |f(x)| .$$

Também segue que, se $\|f\|_p < \infty$, então $|\operatorname{supp}(f)| \leq |\mathbb{N}|$.

Como o único conjunto de medida nula na medida de contagem é o conjunto vazio, segue que as funções são quase-iguais se, e somente se, elas são iguais, portanto funções e quase-funções representam o mesmo objeto. Sendo assim, as definições dos espaços de funções absolutamente somáveis e de funções absolutamente integráveis coincidem nesse caso, e por isso têm a mesma notação.

5.4.5 Dualidade e Mergulho de Espaços Absolutamente Integráveis

Novamente, consideramos $(\boldsymbol{C}, |\cdot|)$ como $\mathbb{R}$ ou $\mathbb{C}$.

Proposição 5.29. *Sejam $\boldsymbol{X}$ um espaço de medida e $(\boldsymbol{C}, |\cdot|)$ um corpo normado.*

1. *Para todo $p \in]1, \infty[$,*

$$\mathscr{I}^{p^*}(\boldsymbol{X}, \boldsymbol{C}) \simeq \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})^*.$$

O isomorfismo de espaços normados é

$$\begin{aligned} I_p \colon \mathscr{I}^{p^*}(\boldsymbol{X}, \boldsymbol{C}) &\longrightarrow \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})^* \\ f &\longmapsto I_p(f) \colon \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}) \longrightarrow C \\ & \qquad\qquad\qquad\qquad f' \longmapsto \int f f' \mathrm{d}m. \end{aligned}$$

2. *Se $\boldsymbol{X}$ é σ-finito,*

$$\mathscr{I}^{\infty}(\boldsymbol{X}, \boldsymbol{C}) \simeq \mathscr{I}^1(\boldsymbol{X}, \boldsymbol{C})^*.$$

Demonstração. Os detalhes da demonstração não serão explicados aqui, mas a ideia geral é a seguinte. A função I_p é linear e, pela desigualdade 5.27 ela é uma isometria local. Pelo teorema de Radon-Nikodym, pode-se mostrar que essa isometria é sobrejetiva e, portanto, um isomorfismo de espaços normados. ■

A escolha do termo *dual* para p^* fica mais clara agora, já que temos a relação

$$\mathscr{I}^{p^*} \simeq (\mathscr{I}^p)^*.$$

O dual de $\mathscr{I}^{\infty}(\boldsymbol{X}, \boldsymbol{C})$ é um caso mais complicado e não será abordado aqui.

Para $p, q \in [1, \infty]$ tais que $p < q$, devemos entender $\mathscr{I}^p$ como um espaço de funções que estão mais concentradas na origem, que são mais localmente singulares, enquanto as funções de $\mathscr{I}^q$ é um espaço de funções que são mais espalhadas.

Proposição 5.30. *Seja* $\boldsymbol{X}$ *um espaço de medida e* $(\boldsymbol{C}, |\cdot|)$ *um corpo normado (completo) e* $p, q \in]0, \infty]$ *tais que* $p < q$.

1. $\mathscr{I}^q(\boldsymbol{X}, \boldsymbol{C}) \subset \mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C})$ *se, e somente se,* X *não contém conjuntos de medida finita mas arbitrariamente grande;*

2. $\mathscr{I}^p(\boldsymbol{X}, \boldsymbol{C}) \subset \mathscr{I}^q(\boldsymbol{X}, \boldsymbol{C})$ *se, e somente se,* X *não contém conjuntos de medida não nula mas arbitrariamente pequena.*

5.5 Isometrias Lineares

Definição 5.23. Sejam $\mathbb{E}$ e $\mathbb{E}'$ espaços normados. Uma *isometria linear local* de $\mathbb{E}$ para $\mathbb{E}'$ é uma função linear $L\colon E \longrightarrow E'$ tal que, para todo $v \in E$,

$$\|L(v)\|' = \|v\| .$$

O conjunto dessas funções é $\mathscr{L}_{\|\|}(\mathbb{E}, \mathbb{E}')$. 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 $v, v' \in E$,

$$|L(v), L(v')| = \|L(v) - L(v')\| = \|L(v - v')\| = \|v - v'\| = |v, v'| .$$

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 as funções lineares limitadas.

5.5.1 Os Grupos Lineares Geral e Especial de Transformações e de Isometrias

O espaço normado $\overset{\leftrightarrow}{\mathscr{L}}(\mathbb{E})$ 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 $\overset{\leftrightarrow}{\mathscr{L}}(\mathbb{E})$ 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 $\overset{\leftrightarrow}{\mathscr{L}}_{\|\|}(\mathbb{E})$ das transformações lineares contínuas invertíveis que preservam a norma é um subgrupo de $\overset{\leftrightarrow}{\mathscr{L}}(\mathbb{E})$, 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 $\overset{\leftrightarrow}{\mathscr{L}}_{\|\|}(\mathbb{E})$ 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

$$\begin{aligned} SL(\mathbb{E}) &\subseteq GL(\mathbb{E}) \\ O(\mathbb{E}) &\subseteq GL(\mathbb{E}) \\ SO(\mathbb{E}) &\subseteq O(\mathbb{E}) \\ SO(\mathbb{E}) &\subseteq SL(\mathbb{E}) \end{aligned}$$

5.6 Funções Multilineares

Proposição 5.31. *Sejam* $\boldsymbol{E_0}, \ldots, \boldsymbol{E_{n-1}}, \boldsymbol{E}$ *espaços normados e* $L\colon E_0 \times \cdots \times E_{n-1} \longrightarrow E$ *uma função n-linear. São equivalentes*

1. *T é contínua;*
2. *T é contínua em 0;*
3. *Existe real $C > 0$ tal que, para todos $v_0 \in E_0$, …, $v_{n-1} \in E_{n-1}$,*

$$\|L(v_0, \ldots, v_{n-1})\| \leq C \|v_0\| \cdots \|v_{n-1}\| ;$$

Proposição 5.32. *Sejam* $\boldsymbol{E_1}, \ldots, \boldsymbol{E_{n-1}}$ *espaços normados de dimensão finita,* $\boldsymbol{E}$ *um espaço normado e* $L\colon E_1 \times \cdots \times E_{n-1} \longrightarrow E$ *uma função n-linear. Então existe real $C > 0$ tal que, para todos $v_1 \in E_1$, …, $v_n \in E_n$,*

$$\|L(v_1, \ldots, v_{n-1})\| \leq C \|v_1\| \cdots \|v_{n-1}\| .$$

Demonstração. Para todo $i \in [n]$, sejam $d_i := \dim E_i$ e $(b_j^{(i)})_{j \in [d_i]}$ uma base ordenada de $\boldsymbol{E_i}$. Todas normas em $\boldsymbol{E_i}$ são equivalentes, portanto usaremos a norma

$\|\cdot\|_\infty$. Assim, para todos $v_1 \in E_1$, ..., $v_{n-1} \in E_{n-1}$,

$$\begin{aligned}
\|L(v_0, \ldots, v_{n-1})\| &= \left\| \mathop{+}_{\substack{0 \le k_0 < d_0 \\ \cdots \\ 0 \le k_{n-1} < d_{n-1}}} v_{(0)}^{k_0} \cdots v_{(n-1)}^{k_{n-1}} L\left(b_{k_0}^{(0)}, \cdots, b_{k_{n-1}}^{(n-1)}\right) \right\| \\
&\le \mathop{+}_{\substack{0 \le k_0 < d_0 \\ \cdots \\ 0 \le k_{n-1} < d_{n-1}}} \left|v_{(0)}^{k_0}\right| \cdots \left|v_{(n-1)}^{k_{n-1}}\right| \left\|L\left(b_{k_0}^{(0)}, \cdots, b_{k_{n-1}}^{(n-1)}\right)\right\| \\
&\le \|v_0\| \cdots \|v_{n-1}\| \mathop{+}_{\substack{0 \le k_0 < d_0 \\ \cdots \\ 0 \le k_{n-1} < d_{n-1}}} \left\|L\left(b_{k_0}^{(0)}, \cdots, b_{k_{n-1}}^{(n-1)}\right)\right\|.
\end{aligned}$$

Definindo

$$C := \mathop{+}_{\substack{0 \le k_0 < d_0 \\ \cdots \\ 0 \le k_{n-1} < d_{n-1}}} \left\|L\left(b_{k_0}^{(0)}, \cdots, b_{k_{n-1}}^{(n-1)}\right)\right\|,$$

segue que

$$\|L(v_0, \ldots, v_{n-1})\| \le C \|v_0\| \cdots \|v_{n-1}\|.$$

■

5.7 Álgebras Normadas

Definição 5.24. Uma *álgebra normada* é um par $\mathbb{A} = (\boldsymbol{A}, \|\cdot\|)$ em que $\boldsymbol{A} = (A, \cdot)$ é uma álgebra sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$ e $\|\cdot\| : A \longrightarrow \mathbb{R}$ é uma norma em $\boldsymbol{A}$ satisfazendo, para todos $a, a' \in A$,

$$\|a \cdot a'\| \le \|a\| \|a'\|;$$

Uma *álgebra normada unitária* é uma álgebra normada $\mathbb{A} = (\boldsymbol{A}, \|\cdot\|)$ tal que $\boldsymbol{A} = (A, \cdot, 1)$ é uma álgebra unitária e

$$\|1\| = 1.$$

5.7.1 Função Exponencial

Consideremos uma álgebra normada unitária completa $\mathbb{A}$. Para todo $x \in A$, a sequência

$$e_n(x) := \mathop{+}_{i=0}^{n} \frac{x^i}{i!}$$

é uma sequência aproximante[17], já que, para todos $n, n' \in \mathbb{N}^*$ com $n' > n$,

$$\|e_{n'}(x) - e_n(x)\| = \left\| \mathop{+}_{i=n+1}^{n'} \frac{x^i}{i!} \right\| \leq \mathop{+}_{i=n+1}^{n'} \frac{\|x\|^i}{i!}.$$

Como a álgebra é completa, isso significa que $e_n(x)$ converge para um elemento

$$\mathrm{e}^x :=: \daleth(x) := \lim_{n \longrightarrow \infty} e_n(x) = \mathop{+}_{n \in \mathbb{N}} \frac{x^n}{n!}.$$

Definição 5.25. Seja $\mathbb{A}$ uma álgebra normada unitária completa. A *função exponencial* em $\mathbb{A}$ é a função

$$\begin{aligned} \daleth \colon A &\longrightarrow A \\ x &\longmapsto \mathop{+}_{n \in \mathbb{N}} \frac{x^n}{n!}. \end{aligned}$$

Proposição 5.33. *Seja $\mathbb{A}$ uma álgebra normada unitária completa.*

1. *Para todo $x \in A$, $\left\|\daleth(x)\right\| \leq \mathrm{e}^{\|x\|}$;*
2. *A função exponencial $\daleth \colon A \longrightarrow A$ é contínua;*
3. *$\daleth(0) = 1$;*
4. *Para todos $x, y \in A$ tais que $xy = yx$,*
$$\daleth(x + y) = \daleth(x)\daleth(y);$$
5. *Para todo $x \in A$, $\daleth(x)^{-1} = \daleth(-x)$;*
6. *Para todo $x \in A$, $\lim_{n \longrightarrow \infty} \left(1 + \frac{x}{n}\right)^n$.*

Demonstração. 1. Basta notar que, para todos $x \in A$ e $n \in \mathbb{N}$,

$$\|e_n(x)\| = \left\| \mathop{+}_{i=0}^{n} \frac{x^i}{i!} \right\| \leq \mathop{+}_{i=0}^{n} \frac{\|x\|^i}{i!} = e_n(\|x\|),$$

logo $\left\|\daleth(x)\right\| \leq \mathrm{e}^{\|x\|}$.

[17] Sequência de Cauchy.

2. Primeiro notamos que, para todos $x, y \in A$,

$$\begin{aligned}\|y^n - x^n\| &= \left\| \mathop{\bigplus}_{i=1}^{n-1} y^{n-i}(y-x)x^i \right\| \\ &\leq n \max(\|x\|, \|y\|)^{n-1} \|y-x\|,\end{aligned}$$

portanto

$$\begin{aligned}\left\| \daleth(y) - \daleth(x) \right\| &= \left\| \mathop{\bigplus}_{n=1}^{\infty} \frac{y^n - x^n}{n!} \right\| \\ &\leq \mathop{\bigplus}_{n=1}^{\infty} \frac{\|y^n - x^n\|}{n!} \\ &\leq \mathop{\bigplus}_{n=1}^{\infty} \frac{n \max(\|x\|, \|y\|)^{n-1}}{n!} \|y-x\| \\ &= \mathrm{e}^{\max(\|x\|, \|y\|)} \|y-x\|,\end{aligned}$$

o que mostra que $\daleth$ é contínua.

3. Segue de

$$\daleth(0) = \mathop{\bigplus}_{n\in\mathbb{N}} \frac{0^n}{n!} = 1 + \mathop{\bigplus}_{n\in\mathbb{N}^*} \frac{0^n}{n!} = 1.$$

4. Sejam $n \in \mathbb{N}$ e

$$s_n := e_{2n}(x+y) - e_n(x)e_n(y) = \mathop{\bigplus}_{k=0}^{2n} \frac{(x+y)^k}{k!} - \left(\mathop{\bigplus}_{i=1}^{n} \frac{x^i}{i!} \right) \left(\mathop{\bigplus}_{j=1}^{n} \frac{y^j}{j!} \right).$$

Como $xy = yx$,

$$\frac{(x+y)^k}{k!} = \frac{1}{k!} \mathop{\bigplus}_{i=0}^{k} \frac{k!}{i!(k-i)!} x^i y^{k-i} = \mathop{\bigplus}_{i+j=k} \frac{x^i y^j}{i!j!}.$$

Portanto

$$\begin{aligned}s_n &= \mathop{\bigplus}_{0\leq i+j\leq 2n} \frac{x^i y^j}{i!j!} - \mathop{\bigplus}_{0\leq i\leq n, 0\leq j\leq n} \frac{x^i y^j}{i!j!} \\ &= \mathop{\bigplus}_{k=0}^{n-1} \frac{x^k}{k!} \mathop{\bigplus}_{n+1}^{2n-k} \frac{y^j}{j!} + \mathop{\bigplus}_{k=0}^{n-1} \frac{y^k}{k!} \mathop{\bigplus}_{n+1}^{2n-k} \frac{x^j}{j!},\end{aligned}$$

o que implica que

$$\begin{aligned}
\|s_n\| &\leq \mathop{\mathbin{+}}_{k=0}^{n-1} \frac{\|x\|^k}{k!} \mathop{\mathbin{+}}_{n+1}^{2n-k} \frac{\|y\|^j}{j!} + \mathop{\mathbin{+}}_{k=0}^{n-1} \frac{\|y\|^k}{k!} \mathop{\mathbin{+}}_{n+1}^{2n-k} \frac{\|x\|^j}{j!} \\
&= \mathop{\mathbin{+}}_{k=0}^{2n} \frac{(\|x\| + \|y\|)^k}{k!} - \left(\mathop{\mathbin{+}}_{i=1}^{n} \frac{\|x\|^i}{i!} \right) \left(\mathop{\mathbin{+}}_{j=1}^{n} \frac{\|y\|^j}{j!} \right) \\
&= e_{2n}(\|x\| + \|y\|) - e_n(\|x\|)e_n(\|y\|).
\end{aligned}$$

Assim segue que

$$\left\| \daleth(x+y) - \daleth(x)\daleth(y) \right\| \leq \mathrm{e}^{\|x\|\|y\|} - \mathrm{e}^{\|x\|}\mathrm{e}^{\|y\|} = 0.$$

5. Basta notar que, como $x(-x) = (-x)x$,

$$\daleth(x)\daleth(-x) = \daleth(x-x) = \daleth(0) = 1. \qquad \blacksquare$$

6. Exercício.

Capítulo 6

Espaços Lineares com Produto Interno

6.1 Produto Interno

Definição 6.1. Seja $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$ invariante por conjugação complexa[1]. Um *produto interno* em $\boldsymbol{V}$ é uma função $\langle \cdot, \cdot \rangle : V \times V \longrightarrow C$ 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 6.2. Um *espaço com produto interno* é um par $(\boldsymbol{V}, \langle \cdot, \cdot \rangle)$ em que $\boldsymbol{V}$ é um espaço linear sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$ invariante por conjugação complexa e $\langle \cdot, \cdot \rangle : \boldsymbol{V} \times \boldsymbol{V} \longrightarrow C$ é um produto interno em $\boldsymbol{V}$.

[1] Um corpo $\boldsymbol{C} \subseteq \mathbb{C}$ tal que, para todo $c \in C$, temos $\overline{c} \in C$.

Proposição 6.1 (Propriedades de Produto Interno)**.** *Seja* $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ *um espaço com produto interno sobre um corpo* $\boldsymbol{C} \subseteq \mathbb{C}$*. 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* $c \in C$*,*
   $$\langle v', cv\rangle = \overline{c}\,\langle v', v\rangle\,;$$

2. *Para todos* $v_0, \ldots, v_n, v \in V$ *e* $c_0, \ldots, c_n \in C$*,*
   $$\left\langle \mathop{+}_{i=0}^{n} c_i v_i, v \right\rangle = \mathop{+}_{i=0}^{n} c_i \langle v_i, v\rangle$$
   e
   $$\left\langle v, \mathop{+}_{i=0}^{n} c_i v_i \right\rangle = \mathop{+}_{i=0}^{n} \overline{c_i}\,\langle v, v_i\rangle\,.$$

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
   $$|\langle v, v'\rangle|^2 = |\langle v, cv\rangle|^2 = |c|^2\,|\langle v, v\rangle|^2 = c\overline{c}\,|\langle v, v\rangle|^2 = \langle v, v\rangle\,\langle cv, cv\rangle = \langle v, v\rangle\,\langle v', v'\rangle\,.$$
   Caso contrário, se $v' - cv \neq 0$ para todo $c \in C$, então para $c = \frac{\langle v', v\rangle}{\langle v, v\rangle}$ segue que
   $$\begin{aligned}
   0 &< \langle v' - cv, v' - cv\rangle \\
   &= \langle v', v'\rangle - c\,\langle v, v'\rangle - \overline{c}\,\langle v', v\rangle + |c|^2\,\langle v, v\rangle \\
   &= \langle v', v'\rangle - c\overline{\langle v', v\rangle} - \overline{c}\,\langle v', v\rangle + |c|^2\,\langle v, v\rangle \\
   &= \langle v', v'\rangle - \frac{|\langle v, v'\rangle|^2}{\langle v, v\rangle} - \frac{|\langle v, v'\rangle|^2}{\langle v, v\rangle} + \frac{\langle v, v'\rangle^2}{\langle v, v\rangle} \\
   &= \langle v', v'\rangle - \frac{|\langle v, v'\rangle|^2}{\langle v, v\rangle},
   \end{aligned}$$
   o que implica
   $$|\langle v, v'\rangle|^2 < \langle v, v\rangle\,\langle v', v'\rangle\,.$$

■

Proposição 6.2. *Sejam $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$ invariante por conjugação complexa e $(b_i)_{i\in I}$ uma base ordenada de $\boldsymbol{V}$. Existe único produto interno $\langle \cdot, \cdot \rangle$ em $\boldsymbol{V}$ tal que, para todos $i, j \in I$, $\langle b_i, b_j \rangle = \delta_{i,j}$.*

6.2 Norma Induzida, Ortogonalidade e Ângulo

6.2.1 Norma

Definição 6.3. Seja $(\boldsymbol{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$. A *norma* (induzida pelo produto interno) de $\boldsymbol{V}$ é a função

$$\begin{aligned} \|\cdot\| \colon V &\longrightarrow \mathbb{R} \\ v &\longmapsto \langle v, v \rangle^{\frac{1}{2}} . \end{aligned}$$

Em termos da norma, a desigualdade de Cauchy-Schwarz fica

$$|\langle v, v' \rangle| \leq \|v\| \, \|v'\| .$$

Proposição 6.3. *Seja $(\boldsymbol{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$. A função $\|\cdot\|$ é uma norma em $\boldsymbol{V}$.*

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

$$\|cv\| = \langle cv, cv \rangle^{\frac{1}{2}} = (c\overline{c} \, \langle v, v \rangle)^{\frac{1}{2}} = |c| \, \|v\| .$$

3. (Subaditividade) Para todos $v, v' \in V$,

$$\begin{aligned} \|v + v'\|^2 &= \langle v + v', v + v' \rangle \\ &= \langle v, v \rangle + \langle v, v' \rangle + \langle v', v \rangle + \langle v', v' \rangle \\ &= \|v\|^2 + \langle v, v' \rangle + \overline{\langle v, v' \rangle} + \|v'\| \\ &= \|v\|^2 + 2\Re(\langle v, v' \rangle) + \|v'\| \\ &\leq \|v\|^2 + 2 \, |\langle v, v' \rangle| + \|v'\| \\ &= \|v\|^2 + 2 \, \|v\| \, \|v'\| + \|v'\|^2 \\ &= (\|v\| + \|v'\|)^2. \end{aligned}$$

■

Proposição 6.4. *Seja $(\boldsymbol{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno. Então, para todos $v, v' \in V$,*

1. *(Regra do Paralelogramo)* $\|v+v'\|^2 + \|v-v'\|^2 = 2\left(\|v\|^2 + \|v'\|^2\right)$;
2. *Se a característica de* $\boldsymbol{C}$ *é diferente de* 2,

$$\Re(\langle v, v'\rangle) = \frac{1}{4}\left(\|v+v'\|^2 - \|v-v'\|^2\right),$$

$$\Im(\langle v, v'\rangle) = \frac{\mathrm{i}}{4}\left(\|v+\mathrm{i}v'\|^2 - \|v-\mathrm{i}v'\|^2\right),$$

e

$$\langle v, v'\rangle = \frac{1}{4}\left(\left(\|v+v'\|^2 - \|v-v'\|^2\right) + \mathrm{i}\left(\|v+\mathrm{i}v'\|^2 - \|v-\mathrm{i}v'\|^2\right)\right).$$

Proposição 6.5 (Polarização)**.** *Seja* $(\boldsymbol{V}, \|\cdot\|)$ *um espaço normado tal que, para todos* $v, v' \in V$,

$$\|v+v'\|^2 + \|v-v'\|^2 = 2\left(\|v\|^2 + \|v'\|^2\right).$$

Então existe produto interno $\langle\cdot,\cdot\rangle$ *em* $\boldsymbol{V}$ *tal que* $\|v\| = \langle v, v\rangle$ *para todo* $v \in V$.

Demonstração. Se $\boldsymbol{C} \subseteq \mathbb{R}$, tome

$$\langle v, v'\rangle = \frac{1}{4}\left(\|v+v'\|^2 - \|v-v'\|^2\right).$$

Caso contrário, tome

$$\langle v, v'\rangle = \frac{1}{4}\left(\left(\|v+v'\|^2 - \|v-v'\|^2\right) + \mathrm{i}\left(\|v+\mathrm{i}v'\|^2 - \|v-\mathrm{i}v'\|^2\right)\right).$$

Os detalhes podem ser conferidos aqui[2]. ■

De fato, a segunda identidade se reduz à primeira quando v, v' são reais.

6.2.2 Perpendicularidade e Paralelismo

Definição 6.4. Seja $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$. Vetores *paralelos* são vetores $v, v' \in V$ para os quais existe $c \in C \smallsetminus \{0\}$ 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 $u \in U$, $\|v\| = 1$. O *complemento perpendicular* (ou *ortogonal*) de um conjunto $U \subseteq V$ é o conjunto

$$U^\perp := \{v \in V \mid \textstyle\bigwedge_{u\in U}\ v \perp u\}.$$

[2]https://math.stackexchange.com/questions/21792/norms-induced-by-inner-products-and-the-parallelogram-law

Proposição 6.6 (Propriedades de $\parallel$ e $\perp$)**.** *Seja* $(\boldsymbol{V}, \langle \cdot, \cdot \rangle)$ *um espaço com produto interno sobre um corpo* $\boldsymbol{C} \subseteq \mathbb{C}$.

1. *A relação de paralelismo* $\parallel$ *é uma equivalência;*
2. *A relação de perpendicularidade* $\perp$ *é simétrica;*
3. *Para todos* $u, v, v' \in V \smallsetminus \{0\}$*, se* $v \parallel v'$ *e* $v \perp u$*, então* $v' \perp u$.
4. *Para todos* $v, v' \in V \smallsetminus \{0\}$*,* $v \parallel v'$ *se, e somente se,* $\{v, v'\}$ *é linearmente dependente.*
5. *Para todos* $v, v' \in V \smallsetminus \{0\}$*, 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 6.7 (Propriedades de complemento perpendicular)**.** *Seja* $(\boldsymbol{V}, \langle \cdot, \cdot \rangle)$ *um espaço com produto interno sobre um corpo* $\boldsymbol{C} \subseteq \mathbb{C}$.

1. *Para todo* $U \subseteq V$*,* $U^\perp$ *é um subespaço linear de* V.
2. $V^\perp = \{0\}$.
3. *Para todo subespaço linear* $U \subseteq V$*,* $(U^\perp)^\perp = U$.

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 6.5. Seja $(\boldsymbol{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno. *Subespaços perpendiculares* em $\boldsymbol{V}$ são subespaços lineares $U, U' \subseteq V$ tais, para todos $u \in U$ e $u' \in U'$, $u \perp u'$. Denota-se $U \perp U'$.

6.2.3 Projeções Paralela e Perpendicular

Definição 6.6. Sejam $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$ e $u \in V$. A *projeção paralela*[3] de V sobre u é

$$\begin{aligned} \mathrm{p}_{\parallel u} \colon V &\longrightarrow V \\ v &\longmapsto \begin{cases} \dfrac{\langle v, u\rangle}{\|u\|^2} u, & u \neq 0 \\ 0, & u = 0. \end{cases} \end{aligned}$$

A *projeção perpendicular* de V sobre u é

$$\begin{aligned} \mathrm{p}_{\perp u} \colon V &\longrightarrow V \\ v &\longmapsto v - \mathrm{p}_{\parallel u}(v). \end{aligned}$$

Proposição 6.8 (Propriedades das projeções)**.** *Seja $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$.*

1. $\mathrm{p}_{\parallel 0} = 0$ *e* $\mathrm{p}_{\perp 0} = \mathrm{I}$*;*
2. *Para todo $u \in V$, as projeções $\mathrm{p}_{\parallel u} \colon V \longrightarrow V$ e $\mathrm{p}_{\perp u} \colon V \longrightarrow V$ são projeções lineares.*
3. *Para todos $u, v \in V$,*
   (a) *se $u \not\perp v$, então $\mathrm{p}_{\parallel u}(v) \parallel u$;*
   (b) $\mathrm{p}_{\perp u}(v) \perp u$*;*
   (c) *se $v \parallel u$, então $\mathrm{p}_{\parallel u}(v) = v$ (ou seja, $\mathrm{p}_{\parallel u}|_{\langle u\rangle} = \mathrm{I}$);*
   (d) *se $v \perp u$, então $\mathrm{p}_{\perp u}(v) = v$ (ou seja, $\mathrm{p}_{\perp u}|_{\langle u\rangle^\perp} = \mathrm{I}$);*
4. *Para todos $u, v \in V \smallsetminus \{0\}$, $\{u, v\}$ é linearmente independente se, e somente se, $\mathrm{p}_{\perp u}(v) \neq 0$.*

Demonstração. 1. Direto da definição.

2. O caso em que $u = 0$ é consequência do item anterior, pois 0 e I são lineares e idempotentes. Consideremos $u \in V \smallsetminus \{0\}$.

   (Linearidade) Sejam $v, v' \in V$ e $c \in C$.

$$\mathrm{p}_{\parallel u}(cv + v') = \frac{\langle cv + v', u\rangle}{\|u\|^2} u = \frac{c\,\langle v, u\rangle + \langle v', u\rangle}{\|u\|^2} u = c\mathrm{p}_{\parallel u}(v) + \mathrm{p}_{\parallel u}(v').$$

[3]Essa 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.

(Idempotência) Seja $v \in V$.

$$\mathrm{p}_{\parallel u}\left(\mathrm{p}_{\parallel u}(v)\right) = \frac{\left\langle \frac{\langle v,u\rangle}{\|u\|^2}u, u\right\rangle}{\|u\|^2}u = \frac{\langle v,u\rangle}{\|u\|^2}\frac{\langle u,u\rangle}{\|u\|^2}u = \frac{\langle v,u\rangle}{\|u\|^2}u = \mathrm{p}_{\parallel u}(v).$$

Segue direto da definição $\mathrm{p}_{\perp u} = \mathrm{I} - \mathrm{p}_{\parallel u}$ e de $\mathrm{p}_{\parallel u}$ ser projeção linear.

3. (a) Se $u \not\perp v$, $\langle u, v\rangle \neq 0$, o que implica que $u \neq 0$ e $\frac{\langle v,u\rangle}{\|u\|^2} \neq 0$. Como por definição $\mathrm{p}_{\parallel u}(v) = \frac{\langle v,u\rangle}{\|u\|^2}u$, segue que $\mathrm{p}_{\parallel u}(v) \parallel u$.

   (b) Se $u = 0$, $\mathrm{p}_{\perp u}(v) \perp u$. Se $u \neq 0$,

$$\left\langle \mathrm{p}_{\parallel u}(v), u\right\rangle = \left\langle \frac{\langle v,u\rangle}{\|u\|^2}u, u\right\rangle = \frac{\langle v,u\rangle}{\|u\|^2}\langle u,u\rangle = \langle v,u\rangle,$$

   portanto

$$\langle \mathrm{p}_{\perp u}(v), u\rangle = \left\langle v - \mathrm{p}_{\parallel u}(v), u\right\rangle = \langle v,u\rangle - \left\langle \mathrm{p}_{\parallel u}(v), u\right\rangle = 0,$$

   o que mostra que $\mathrm{p}_{\perp u}(v) \perp u$.

   (c) Se $v \parallel u$, existe $c \in C \smallsetminus \{0\}$ tal que $v = cu$. Se $u = 0$, então $v = 0$, logo $\mathrm{p}_{\parallel u}(v) = \mathrm{p}_{\parallel 0}(0) = 0 = v$. Se $u \neq 0$, então

$$\mathrm{p}_{\parallel u}(v) = \frac{\langle v,u\rangle}{\|u\|^2}u = \frac{\langle cu,u\rangle}{\|u\|^2}u = cu = v.$$

   (d) Se $v \perp u$, então $\langle u, v\rangle = 0$. Se $u = 0$, então $\mathrm{p}_{\perp u} = \mathrm{I}$, logo $\mathrm{p}_{\perp u}(v) = v$. Se $u \neq 0$,

$$\mathrm{p}_{\perp u}(v) = v - \frac{\langle v,u\rangle}{\|u\|^2} = v.$$

■

Todo v pode ser decomposto como $v = \mathrm{p}_{\parallel u}(v) + \mathrm{p}_{\perp u}(v)$.

Processo de Ortogonalização

Seja $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno sobre um corpo $\boldsymbol{C} \subseteq \mathbb{C}$ e $B = (v_i)_{i\in[d]}$ uma base finita de $\boldsymbol{V}$. A base $(u_i)_{i\in[d]}$, definida recursivamente por

$$u_i := \mathrm{p}_{\perp u_{i-1}} \circ \cdots \circ \mathrm{p}_{\perp u_0}(v_i) = v_i - \mathop{\bigplus}_{j\in[i]} \mathrm{p}_{\parallel u_j}(v_i)$$

é uma base ortogonal (perpendicular) de $\boldsymbol{V}$. A base $(e_i)_{i\in[d]}$ definida por $e_i := \frac{u_i}{\|u_i\|}$ é uma base ortonormal (ou perpendicular unitária) de $\boldsymbol{V}$.

6.2.4 Projeções Ortogonais

Lembremos que, para toda projeção linear $p\colon V \longrightarrow V$, vale que $(\mathrm{I}-p)$ é projeçãao linear, $p^{-1}(0) = (\mathrm{I}-p)(V)$ e

$$V = p(V) \oplus (\mathrm{I}-p)(V).$$

Definição 6.7. Seja $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno. Uma *projeção ortogonal* em $\boldsymbol{V}$ é uma projeção linear $p\colon V \longrightarrow V$ tal que $p(V) \perp (\mathrm{I}-p)(V)$.

Proposição 6.9. *Sejam $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno (completo) e $p\colon V \longrightarrow V$ uma projeção ortogonal em $\boldsymbol{V}$.*

1. *Para todos $v, v' \in V$,*

$$\langle p(v), v' - p(v')\rangle = \langle v - p(v), p(v')\rangle = 0;$$

2. *Para todos $v, v' \in V$,*

$$\langle p(v), v'\rangle = \langle p(v), p(v')\rangle = \langle v, p(v')\rangle\,;$$

Proposição 6.10. *Sejam $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno completo e $U \subseteq V$ um subespaço linear fechado. Existe projeção ortogonal $p\colon V \longrightarrow V$ tal que $p(V) = U$.*

Demonstração. Como U é fechado, é um subespaço completo. Seja $v \in V$. O conjunto

$$N := \{\|v-u\| \mid u \in U\}$$

tem ínfimo e, como U é completo, N tem mínimo. Definimos $p(v)$ como o ponto $u \in U$ tal que $\|v-u\| = \min N$. Mostremos que p é uma projeção ortogonal.

(Idempotência) Seja $v \in V$. Então, como $p(v) \in U$, segue que $p(p(v)) = p(v) \in U$, pois $\|p(v) - p(v)\| = 0$, logo $p^2 = p$.

(Ortogonalidade) Sejam $u \in U = p(V)$ e $v \in (\mathrm{I}-p)(V)$. Se $u = 0$, então $\langle v, u\rangle = \langle v, 0\rangle = 0$. Suponhamos $u \neq 0$. Temos que

$$\begin{aligned}
\left\|v - \mathrm{p}_{\|u}(v)\right\|^2 &= \|v\|^2 - 2\left\langle v, \mathrm{p}_{\|}(v)u\right\rangle + \left\|\mathrm{p}_{\|u}(v)\right\|^2 \\
&= \|v\|^2 - 2\frac{\langle v,u\rangle}{\|u\|^2}\langle v,u\rangle + \frac{\langle v,u\rangle^2}{\|u\|^4}\|u\|^2 \\
&= \|v\|^2 - 2\frac{\langle v,u\rangle^2}{\|u\|^2} + \frac{\langle v,u\rangle^2}{\|u\|^2} \\
&= \|v\|^2 - \frac{\langle v,u\rangle^2}{\|u\|^2}.
\end{aligned}$$

Seja $v' \in V$ tal que $(\mathrm{I} - p)(v') = v$. Então $(p(v') + \mathrm{p}_{\|u}(v)) \in U$, logo pela minimalidade de $p(v')$ segue que

$$\begin{aligned}
\|v\|^2 &= \|v' - p(v')\|^2 \\
&\leq \left\|v' - (p(v') + \mathrm{p}_{\|u}(v))\right\|^2 \\
&= \left\|v - \mathrm{p}_{\|u}(v)\right\|^2 \\
&= \|v\|^2 - \frac{\langle v, u\rangle^2}{\|u\|^2},
\end{aligned}$$

logo $\frac{\langle v,u\rangle^2}{\|u\|^2} = 0$, o que é equivalente a $\langle v, u\rangle = 0$.

(Linearidade) Sejam $v, v' \in V$ e $c \in C$. Então $(cv + v') - p(cv + v')$, $cv - p(cv)$ e $v' - p(v') \in (\mathrm{I} - p)(V)$. Da ortogonalidade de p, para todo $u \in U = p(V)$ temos

$$0 = \langle (cv + v') - p(cv + v'), u\rangle = \langle cv - cp(v), u\rangle = \langle v' - p(v'), u\rangle\,,$$

portanto

$$\begin{aligned}
0 &= \langle (cv + v') - p(cv + v'), u\rangle - \langle cv - cp(v), u\rangle - \langle v' - p(v'), u\rangle \\
&= \langle cp(v) + p(v') - p(cv + v'), u\rangle\,.
\end{aligned}$$

Tomando $u = cp(v) + p(v') - p(cv + v')$, temos que $u \in U$ e então

$$0 = \langle p(cv) + p(v') - p(cv + v'), cp(v) + p(v') - p(cv + v')\rangle\,,$$

o que implica $p(cv + v') = cp(v) + p(v')$. ■

Proposição 6.11. *Seja $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno. Toda projeção ortogonal $p\colon V \longrightarrow V$ em $\boldsymbol{V}$ é contínua.*

Demonstração. Basta notar que, pela desigualdade do produto interno, para todo $v \in V$,

$$\|p(v)\|^2 = \langle p(v), p(v)\rangle = \langle p(v), v\rangle \leq \|p(v)\|\,\|v\|\,,$$

logo $\|p(v)\| \leq \|v\|$. Isso mostra que p é limitada, o que é equivalente a ser contínua. ■

6.2.5 Ângulo

Definiremos agora a noção de ângulo induzida pelo produto interno. Pela desiguadade de Cauchy-Schwarz, sabemos que, para todos $v, v' \in V$,

$$|\langle v, v'\rangle| \leq \|v\|\,\|v'\|\,.$$

Disso segue que, para todos $v, v' \in V \smallsetminus \{0\}$,

$$\frac{|\langle v, v'\rangle|}{\|v\|\,\|v'\|} \leq 1.$$

Se o produto interno for real, então

$$-1 \leq \frac{\langle v, v'\rangle}{\|v\|\,\|v'\|} \leq 1.$$

Isso significa que a função $\cos^{-1}\colon [-1,1] \longrightarrow \left[0, \frac{\tau}{2}\right]$ está definida para esses valores, portanto podemos definir a função ângulo como a seguir. No caso em que o produto interno não é reaal, 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 $\left[0, \frac{\tau}{4}\right]$, mas não estudaremos esse caso aqui.

Figura 6.1: Gráfico da função $\cos^{-1}\colon [-1,1] \longrightarrow \left[0, \frac{\tau}{2}\right]$.

Definição 6.8. Sejam $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno real e $v, v' \in V \smallsetminus \{0\}$. 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 $\boldsymbol{V}$ é a função

$$\begin{aligned} \sphericalangle(\cdot,\cdot)\colon V \smallsetminus \{0\} \times V \smallsetminus \{0\} &\longrightarrow \left[0, \frac{\tau}{2}\right] \\ (v, v') &\longmapsto \sphericalangle(v, v'). \end{aligned}$$

Figura 6.2: Representação de vetores e o ângulo entre eles.

Proposição 6.12 (Propriedades de Ângulo)**.** *Seja* $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ *um espaço com produto interno real.*

1. *Para todos* $v, v' \in V \smallsetminus \{0\}$,
$$\langle v, v'\rangle = \|v\|\,\|v'\|\cos(\sphericalangle(v, v'));$$

2. *Para todos* $v, v' \in V \smallsetminus \{0\}$ *e* $cc' \in \mathbb{R} \smallsetminus \{0\}$,
$$\sphericalangle(cv, c'v') = \begin{cases} \sphericalangle(v, v'), & cc' > 0 \\ \dfrac{\tau}{2} - \sphericalangle(v, v'), & cc' < 0; \end{cases}$$

3. *Para todos* $v, v' \in V \smallsetminus \{0\}$,
$$v \parallel v' \iff \sphericalangle(v, v') \in \{0, \frac{\tau}{2}\}.$$
Se existe $c \in \,]0, \infty[$ *tal que* $v' = cv$*, então* $\sphericalangle(v, v') = 0$*, e se existe* $c \in \,]-\infty, 0[$ *tal que* $v' = cv$*, então* $\sphericalangle(v, v') = \frac{\tau}{2}$*;*

4. *Para todos* $v, v' \in V \smallsetminus \{0\}$,
$$v \perp v' \iff \sphericalangle(v, v') = \frac{\tau}{4}.$$

Demonstração. 1. Segue diretamente da definição.

2. Da igualdade
$$\sphericalangle(v, v') = \cos^{-1}\left(\frac{\langle v, v'\rangle}{\|v\|\,\|v'\|}\right)$$

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

$$\sphericalangle(cv, c'v') = \cos^{-1}\left(-1\frac{\langle v, v'\rangle}{\|v\|\,\|v'\|}\right) = \frac{\tau}{2} - \sphericalangle(v, v').$$

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 $\cos^{-1}\colon [-1, 1] \longrightarrow \left[0, \frac{\tau}{2}\right]$ é uma bijeção tal que $\cos^{-1}(1) = 0$ e $\cos^{-1}(-1) = \frac{\tau}{2}$.

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 $\sphericalangle(v, v)$,

$$\sphericalangle(v, v') = \sphericalangle(v, cv) = \begin{cases} 0, & c > 0 \\ \dfrac{\tau}{2}, & c < 0. \end{cases}$$

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 $\sphericalangle(v, v') = \frac{\tau}{2}$. 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 $\frac{\tau}{2} = \sphericalangle(v, v') = \sphericalangle(v, cv)$, $c \in \,]-\infty, 0[$.

4. Segue diretamente da bijetividade de $\cos^{-1}$, pois $\sphericalangle(v, v') = \frac{\tau}{4}$ se, e somente se, $\frac{\langle v, v\rangle}{\|v\|\|v\|} = 0$, o que ocorre se, e somente se, $\langle v, v'\rangle = 0$. ■

6.2.6 Espaço Projetivo

O espaço projetivo é o espaço de retas pela origem. Ele pode ser descrito de diferentes formas. Quando $V = \mathbb{R}^d$ (ou um espaço normado), podemos descrevê-lo como o quociente da esfera unitária pela antípoda $-\mathrm{I}$. Quando $\boldsymbol{V}$ é um espaço com produto interno, podemos induzir em $\mathbb{P}V$ uma distância, o ângulo entre as retas de V. De qualquer forma, esse espaço é um espaço topológico, como será também descrito a seguir.

Estrutura Topológica

A relação de paralelismo $\parallel$ é uma equivalência não só em V, mas em $V \smallsetminus \{0\}$. Além disso, ela não depende de produto interno, está definida para qualquer espaço linear $\boldsymbol{V}$ sobre um corpo $\boldsymbol{C}$ qualquer. Isso permite que se quociente $V \smallsetminus \{0\}$ por $\parallel$, e esse é o *espaço projetivo* de $\boldsymbol{V}$.

Definição 6.9. Seja $\boldsymbol{V}$ um espaço linear sobre um corpo $\boldsymbol{C}$. O *espaço projetivo* de $\boldsymbol{V}$ é o conjunto

$$\mathbb{P}V := (V \smallsetminus \{0\}) \big/ \parallel .$$

Os elementos de $\mathbb{P}V$ são as *retas* de $\boldsymbol{V}$.

Esse quociente pode ser entendido também como o quociente pela ação do grupo multiplicativo $C \smallsetminus \{0\}$. Desse modo, temos que

$$\mathbb{P}V = (V \smallsetminus \{0\}) \big/ (C \smallsetminus \{0\}) \cdot$$

O caso em que $\boldsymbol{V}$ é um espaço normado nos permite dar mais uma definição equivalente desse espaço. Lembremos que $\mathbb{S}^0 = \{1, -1\}$ é o grupo discreto multiplicativo com 2 elementos e é subgrupo do grupo multiplicativo $C \smallsetminus \{0\}$. Se $\boldsymbol{V}$ é um espaço normado, a esfera $\mathbb{S}V$ de $\boldsymbol{V}$ está definida. Nesse caso, $\mathbb{S}^0$ age em $\mathbb{S}V$ e o espaço quociente $\mathbb{S}/\mathbb{S}^0$ pode ser identificado com $\mathbb{P}V$ de um jeito bem natural, de modo que as estruturas definidas em um possam sempre ser passadas para o outro. Temos

$$\mathbb{P}V \simeq \mathbb{S}V \big/ \mathbb{S}^0 .$$

O isomorfismo é dado por

$$\begin{aligned} h \colon \mathbb{P}V &\longrightarrow \mathbb{S}V \big/ \mathbb{S}^0 \\ [v] &\longmapsto \left\{ \frac{v}{\|v\|}, -\frac{v}{\|v\|} \right\} \end{aligned}$$

com inversa

$$\begin{aligned} h^{-1} \colon \mathbb{S}V \big/ \mathbb{S}^0 &\longrightarrow \mathbb{P}V \\ \{u, -u\} &\longmapsto \{cu \mid c \in C \smallsetminus \{0\}\} . \end{aligned}$$

Estrutura Métrica

Quando o espaço linear tem um produto interno, a função ângulo pode ser usada para definir uma função distância no espaço projetivo.

Definição 6.10. Seja $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ um espaço com produto interno. O *ângulo* entre retas r e r' de $\boldsymbol{V}$ é o menor ângulo entre vetores de r e r'

$$\sphericalangle(r, r') := \min_{v\in r, v'\in r'} \sphericalangle(v, v').$$

Mostremos como achar uma expressão para $\sphericalangle(r, r')$, o que facilitará a demonstração de que essa função é de fato uma distância. Queremos mostrar que

$$\sphericalangle(r, r') = \cos^{-1}\left(\frac{|\langle v, v'\rangle|}{\|v\|\,\|v'\|}\right),$$

em que $v \in r, v' \in r'$. Para todos $\bar{v} \in r$ e $\bar{v}' \in r'$, existem escalares $c, c' \in C \setminus \{0\}$ tais que $\bar{v} = cv$ e $\bar{v}' = c'v'$. Portanto

$$\begin{aligned}\sphericalangle(r, r') &= \min_{\bar{v}\in r, \bar{v}'\in r'} \sphericalangle(\bar{v}, \bar{v}') \\ &= \min_{c,c'\in C\setminus\{0\}} \sphericalangle(cv, cv') \\ &= \min\left\{\sphericalangle(v, v'), \frac{\tau}{2} - \sphericalangle(v, v')\right\}.\end{aligned}$$

Como $\sphericalangle(v, v') \in \left[0, \frac{\tau}{2}\right]$, segue que

$$\min\left\{\sphericalangle(v, v'), \frac{\tau}{2} - \sphericalangle(v, v')\right\} \in \left[0, \frac{\tau}{4}\right].$$

Assim, escolhendo $v \in r$ e $v' \in r'$ tais que $\langle v, v'\rangle \geq 0$, temos $\sphericalangle(v, v') \in \left[0, \frac{\tau}{4}\right]$, o que implica que

$$\sphericalangle(r, r') = \min\left\{\sphericalangle(v, v'), \frac{\tau}{2} - \sphericalangle(v, v')\right\} = \cos^{-1}\left(\frac{|\langle v, v'\rangle|}{\|v\|\,\|v'\|}\right).$$

Podemos restringir ainda mais a escolha dos $v \in r$ e $v' \in r'$ notando que

$$\cos^{-1}\left(\frac{|\langle v, v'\rangle|}{\|v\|\,\|v'\|}\right) = \cos^{-1}\left(\left|\left\langle \frac{v}{\|v\|}, \frac{v'}{\|v'\|}\right\rangle\right|\right)$$

e que $\frac{v}{\|v\|}, \frac{v'}{\|v'\|} \in \mathbb{S}$. Como existe $u \in V$ tal que $r \cap \mathbb{S} = \{u, -u\}$, podemos tomar $u \in r \cap \mathbb{S}$ e $u' \in r' \cap \mathbb{S}$ e temos que

$$\sphericalangle(r, r') = \cos^{-1}(|\langle u, u'\rangle|).$$

Definição 6.11. Seja $(\boldsymbol{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno. A distância em $\mathbb{P}V$ é a função

$$\begin{aligned} \sphericalangle(\cdot,\cdot)\colon \mathbb{P}V \times \mathbb{P}V &\longrightarrow \left[0, \frac{\tau}{4}\right] \\ (r, r') &\longmapsto \sphericalangle(r, r')\,. \end{aligned}$$

Proposição 6.13. *Seja $(\boldsymbol{V}, \langle \cdot, \cdot \rangle)$ um espaço com produto interno. A função $\sphericalangle(\cdot,\cdot)$ é uma distância em $\mathbb{P}V$.*

Demonstração. (Separação) Sejam $r \in \mathbb{P}V$ e $v \in r$. Então

$$\sphericalangle(r, r) = \cos^{-1}\left(\frac{|\langle v, v\rangle|}{\|v\|\,\|v\|}\right) = \cos^{-1}(1) = 0.$$

Reciprocamente, sejam $r, r' \in \mathbb{P}V$, $v \in r$ e $v' \in r'$. Se $\sphericalangle(r, r') = 0$, então $\frac{|\langle v,v\rangle|}{\|v\|\|v\|} = 1$, o que implica que $v' = v$ ou $v' = -v$, logo $r = r'$. (Simetria) Sejam $r, r' \in \mathbb{P}V$, $v \in r$ e $v' \in r'$. Então

$$\sphericalangle(r, r') = \cos^{-1}\left(\frac{|\langle v, v'\rangle|}{\|v\|\,\|v'\|}\right) = \cos^{-1}\left(\frac{\left|\overline{\langle v', v\rangle}\right|}{\|v'\|\,\|v\|}\right) = \cos^{-1}\left(\frac{|\langle v', v\rangle|}{\|v'\|\,\|v\|}\right) = \sphericalangle(r', r)\,.$$

(Desigualdade Triangular) Sejam $r, r', r'' \in \mathbb{P}V$, $v \in r$, $v' \in r'$ e $v'' \in r''$. Queremos mostrar que

$$\sphericalangle(r, r'') \leq \sphericalangle(r, r') + \sphericalangle(r', r'')\,.$$

Consideremos a projeção $\bar{v}$ de v' no plano $\langle\{v, v''\}\rangle$.

Se mostrarmos que

$$|\langle u, u''\rangle| \geq |\langle u, u'\rangle| + |\langle u', u''\rangle|\,,$$

segue da monotonicidade decrescente de $\cos^{-1}$.

$$|\langle u, u'\rangle + \langle u', u''\rangle| \leq |\langle u, u'\rangle| + |\langle u', u''\rangle|$$

$$\langle u, u'\rangle + \langle u'', u'\rangle = \langle u + u'', u'\rangle$$

■

6.2.7 Funções Ortogonais e Conformes

Definição 6.12. Sejam $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ e $(\boldsymbol{V}', \langle\cdot,\cdot\rangle')$ espaços com produto interno. Uma função *ortogonal* de $\boldsymbol{V}$ para $\boldsymbol{V}'$ é uma função linear $f\colon V \longrightarrow V'$ tal que, para todos $v, v' \in V$,

$$\langle f(v), f(v')\rangle' = \langle v, v'\rangle\,.$$

O conjunto dessas funções é $\mathscr{L}_{\langle,\rangle}(\boldsymbol{V}, \boldsymbol{V}')$.

Uma função *conforme* de $\boldsymbol{V}$ para $\boldsymbol{V}'$ é uma função linear $f\colon V \longrightarrow V'$ tal que, para todos $v, v' \in V$,

$$\sphericalangle'(f(v), f(v')) = \sphericalangle\,(v, v')\,.$$

O conjunto dessas funções é $\mathscr{L}_{\sphericalangle}(\boldsymbol{V}, \boldsymbol{V}')$.

Note que, na definição de uma função conforme, está implícito que $\sphericalangle'(f(v), f(v'))$ existe, portanto $f(v) \neq 0$ para todo $v \in V \smallsetminus \{0\}$, o que significa que f é injetiva.

Proposição 6.14. *Sejam $(\boldsymbol{V}, \langle\cdot,\cdot\rangle)$ e $(\boldsymbol{V}', \langle\cdot,\cdot\rangle')$ espaços com produto interno sobre um corpo $\boldsymbol{C}$ de característica diferente de 2 e $f\colon V \longrightarrow V'$ uma função linear.*

1. *f é ortogonal se, e somente se, é uma isometria local:*

$$\mathscr{L}_{\langle,\rangle}(\boldsymbol{V}, \boldsymbol{V}') = \mathscr{L}_{\|\|}(\boldsymbol{V}, \boldsymbol{V}');$$

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 $\boldsymbol{C}$ é diferente de 2, vale que, para todos $v, v' \in V$,

$$\langle v, v'\rangle = \frac{1}{4}\left(\left(\|v+v'\|^2 - \|v-v'\|^2\right) + \mathrm{i}\left(\|v+\mathrm{i}v'\|^2 - \|v-\mathrm{i}v'\|^2\right)\right).$$

Se f é isometria local, então, para todos $v, v' \in V$,

$$\begin{aligned}
\langle f(v), f(v')\rangle &= \frac{1}{4}\left(\|f(v)+f(v'))\|^2 - \|f(v)-f(v'))\|^2\right) \\
&\qquad + \frac{\mathrm{i}}{4}\left(\|f(v)+\mathrm{i}f(v')\|^2 - \|f(v)-\mathrm{i}f(v')\|^2\right) \\
&= \frac{1}{4}\left(\|f(v+v')\|^2 - \|f(v-v')\|^2\right) \\
&\qquad + \frac{\mathrm{i}}{4}\left(\|f(v+\mathrm{i}v')\|^2 - \|f(v-\mathrm{i}v')\|^2\right) \\
&= \frac{1}{4}\left(\left(\|v+v'\|^2 - \|v-v'\|^2\right) + \mathrm{i}\left(\|v+\mathrm{i}v'\|^2 - \|v-\mathrm{i}v'\|^2\right)\right) \\
&= \langle v, v'\rangle .
\end{aligned}$$

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 $v \in V \smallsetminus \{0\}$ e $h \in V$. Como f é linear e $\mathrm{D}\,\|v\|\,(h) = \frac{\langle v,h\rangle}{\|v\|}$ é a diferencial[4] de $\|\cdot\|$, a diferencial de N é

$$\begin{aligned}
\mathrm{D}N|_v(h) &= \frac{\|v\|\,\mathrm{D}\,\|f(v)\|'\,(h) - \|f(v)\|'\,\mathrm{D}\,\|v\|\,(h)}{\|v\|^2} \\
&= \frac{\frac{\|v\|}{\|f(v)\|'}\langle f(v), \mathrm{D}f(v)(h)\rangle' - \frac{\|f(v)\|'}{\|v\|}\langle v, h\rangle}{\|v\|^2} \\
&= \frac{\|v\|^2\langle f(v), f(h)\rangle' - \|f(v)\|'^2\langle v, h\rangle}{\|f(v)\|'\,\|v\|^3}.
\end{aligned}$$

[4]Não tenho certeza, mas acredito que isso dependa de a característica de $\boldsymbol{C}$ ser diferente de 2, pois quando calculamos a diferencial pela regra da cadeia cancelamos fatores de 2.

Notemos que, como f preserva ângulo, então se $v \perp v'$ segue que $f(v) \perp f(v')$. Escrevendo $h = \mathrm{p}_{\|v}(h) + \mathrm{p}_{\perp v}(h) = h^{\|} + h^{\perp}$, temos que $h^{\perp} \perp v$, e $h^{\|} \parallel v$ ou $h^{\|} = 0$, logo

$$\mathrm{D}N|_v(h) = \mathrm{D}N|_v(h^{\|} + h^{\perp}) = \mathrm{D}N|_v(h^{\|}) + \mathrm{D}N|_v(h^{\perp}).$$

Calculemos $\mathrm{D}N|_v(h^{\|})$. Como $h^{\|} = cv$, com $c = \frac{\langle h,v\rangle}{\|v\|^2}$, segue que

$$\begin{aligned}
\mathrm{D}N|_v(h^{\|}) &= \frac{\|v\|^2 \langle f(v), f(cv)\rangle' - \|f(v)\|'^2 \langle v, cv\rangle}{\|f(v)\|' \|v\|^3} \\
&= \frac{c\,\|v\|^2 \langle f(v), f(v)\rangle' - c\|f(v)\|'^2 \langle v, v\rangle}{\|f(v)\|' \|v\|^3} \\
&= \frac{c\,\|v\|^2 \|f(v)\|'^2 - c\|f(v)\|'^2 \|v\|^2}{\|f(v)\|' \|v\|^3} \\
&= 0.
\end{aligned}$$

Calculemos agora $\mathrm{D}N|_v(h^{\perp})$. Como $\left\langle h^{\perp}, v\right\rangle = 0$, então $\left\langle f(v), f(h^{\perp})\right\rangle = 0$, logo

$$\mathrm{D}N|_v(h^{\perp}) = \frac{\|v\|^2 \left\langle f(v), f(h^{\perp})\right\rangle' - \|f(v)\|'^2 \left\langle v, h^{\perp}\right\rangle}{\|f(v)\|' \|v\|^3} = 0.$$

Assim, concluímos que $\mathrm{D}N|_v(h) = \mathrm{D}N|_v(h^{\|}) + \mathrm{D}N|_v(h^{\perp}) = 0$, ou seja, $\mathrm{D}N|_v = 0$ para todo $v \in V \smallsetminus \{0\}$, o que implica que existe $c' \in \mathbb{R}$ tal que, para todo $v \in V \smallsetminus \{0\}$, $N(v) = \frac{\|f(v)\|}{\|v\|} = c'$. 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

$$\langle f(v), f(v')\rangle' = \frac{\|f(v)\|' \|f(v')\|'}{\|v\| \|v'\|} \langle v, v'\rangle = (c')^2 \langle v, v'\rangle = c \langle v, v'\rangle .$$

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

$$\begin{aligned}
\sphericalangle' (f(v), f(v')) &= \cos^{-1}\left(\frac{\langle f(v), f(v')\rangle'}{\|f(v)\|' \|f(v')\|'}\right) \\
&= \cos^{-1}\left(\frac{c \langle v, v'\rangle}{c \|v\| \|v'\|}\right) \\
&= \sphericalangle (v, v') .
\end{aligned}$$

■

6.3 Espaço de Funções Quadrado Somáveis

Sejam X um conjunto e $\boldsymbol{C} \subseteq \mathbb{C}$. Para todo $p \in [1, \infty]$, o espaço $\mathscr{S}^p(\boldsymbol{X}, \boldsymbol{C})$ é um espaço normado completo, mas somente para $p = 2$ esse espaço admite um produto interno. As funções absolutamente 2-somáveis do espaço $Smvl^2(\boldsymbol{X}, \boldsymbol{C})$ são também chamadas de *funções quadrado somáveis*. Note que, diferente do caso mais geral de funções absolutamente p-somáveis, aqui fixamos um subcorpo dos números complexos para usar o conjugação complexa. A generalização do complexo conjugado é mais difícil e detalhada e não será feita aqui.

Definição 6.13. Sejam X um conjunto e $\boldsymbol{C} \subseteq \mathbb{C}$ um corpo. O *produto interno* entre $f, f' \in \mathscr{S}^2(\boldsymbol{X}, \boldsymbol{C})$ é

$$\langle f, f' \rangle := \left(\mathop{+}_{x \in X} f(x) \overline{f'(x)} \right)^{2^{-1}} .$$

Proposição 6.15. *Sejam X um conjunto e $\boldsymbol{C} \subseteq \mathbb{C}$ um corpo. O espaço $(\mathscr{S}^2(\boldsymbol{X}, \boldsymbol{C}), \langle \cdot, \cdot \rangle)$ é um espaço com produto interno completo.*

Capítulo 7

Medida

7.1 Espaço Mensurável

7.1.1 Sigma-Álgebras e Sub-Sigma-Álgebras

Definição 7.1. Seja X um conjunto. Uma *sigma-álgebra* sobre X é um conjunto $\mathcal{M} \subseteq \mathsf{P}(X)$ de subconjuntos X que satisfaz

1. (Vazio) $\emptyset \in \mathcal{M}$;
2. (Fechamento por complementação) Para todo $M \in \mathcal{M}$, $M^{\complement} \in \mathcal{M}$;
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 7.1. *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 $X = \emptyset^{\complement} \in \mathcal{M}$.

2. Da segunda propriedade, tem-se que, para todo $i \in \mathbb{N}$, $M_i^{\complement} \in \mathcal{M}$. Da terceira propriedade de $\mathcal{M}$, tem-se que $\bigcup_{i\in\mathbb{N}} M_i^{\complement} \in \mathcal{M}$. Das Leis de De Morgan (4.27), tem-se que

$$\left(\bigcap_{i\in\mathbb{N}} M_i\right)^{\complement} = \bigcup_{i\in\mathbb{N}} (M_i)^{\complement} \in \mathcal{M},$$

e conclui-se que $\bigcap\limits_{i\in\mathbb{N}} M_i \in \mathcal{M}$.

■

Exemplo 7.1. $\mathcal{M} = \{\emptyset, X\}$ *e* $\mathcal{M} = \mathsf{P}(X)$ *são sigma-álgebras sobre* X.

Definição 7.2. 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 7.3. 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 7.2. *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* $n \in \mathbb{N}^*$,

$$D_n := C_n \setminus M_n$$

é uma sequência disjunta de conjuntos;

3.

$$\bigcup_{n\in\mathbb{N}} C_n = \bigcup_{n\in\mathbb{N}} M_n = \bigcup_{n\in\mathbb{N}} D_n.$$

7.1.2 Sigma-Álgebras Geradas

Proposição 7.3. *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 $A^{\complement} \in \mathcal{M}_i$ para todo $i \in I$, o que implica $A^{\complement} \in \mathcal{M}$. 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 7.4. Seja X um conjunto e $\mathcal{C} \in \mathsf{P}(X)$ 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 7.2. *A sigma-álgebra sobre X gerada por $\emptyset$ é $\{\emptyset, X\}$.*

7.1.3 Limites de Conjuntos

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

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

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 7.4. *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 7.5. *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 7.6. Sejam X um conjunto e $(A_n)_{n\in\mathbb{N}}$ uma sequência de subconjuntos de X. Um *limite* de $(A_n)_{n\in\mathbb{N}}$ é um conjunto $\lim A_n$ tal que

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

7.2 Funções Mensuráveis

Definição 7.7. Sejam $\boldsymbol{X} = (X, \mathcal{M}_X)$ e $\boldsymbol{Y} = (Y, \mathcal{M}_Y)$ espaços mensuráveis. Uma *função mensurável* de $\boldsymbol{X}$ para $\boldsymbol{Y}$ é uma função $f\colon X \longrightarrow Y$ tal que, para todo $M \in \mathcal{M}$,

$$f^{-1}(M) \in \mathcal{M}_X.$$

Denota-se $f\colon \boldsymbol{X} \longrightarrow \boldsymbol{Y}$. O conjunto dessas funções é denotado $\mathscr{M}(\boldsymbol{X}, \boldsymbol{Y})$.

Proposição 7.6. *Seja $\boldsymbol{X}$ um espaço mensurável. A função $\mathrm{I}_X : X \longrightarrow X$ é uma função mensurável.*

Proposição 7.7. *Sejam $\boldsymbol{X_0}$, $\boldsymbol{X_1}$ e $\boldsymbol{X_2}$ espaços mensuráveis e $f_0 : \boldsymbol{X_0} \longrightarrow \boldsymbol{X_1}$ e $f_1 : \boldsymbol{X_1} \longrightarrow \boldsymbol{X_2}$ funções mensuráveis. Então $f_1 \circ f_0 : \boldsymbol{X_0} \longrightarrow \boldsymbol{X_2}$ é uma função mensurável.*

7.2.1 Sigma-Álgebras Puxadas e Empurradas

Definição 7.8. Sejam X um conjunto, $\boldsymbol{Y} = (Y, \mathcal{M}_Y)$ um espaço mensurável e $f : X \longrightarrow Y$ uma função. A *sigma-álgebra puxada* por f é

$$f^*(\mathcal{M}_Y) := \left\{ f^{-1}(M) \;\middle|\; M \in \mathcal{M}_Y \right\}.$$

Proposição 7.8. *Sejam X um conjunto, $\boldsymbol{Y} = (Y, \mathcal{M}_Y)$ um espaço mensurável e $f : X \longrightarrow Y$ 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 $A^{\complement} \in \mathcal{M}_Y$, o que implica $f^{-1}(A^{\complement}) \in \mathcal{M}_X$. Mas $(f^{-1}(A))^{\complement} = f^{-1}(A^{\complement})$ (3.13). Então $B^{\complement} \in \mathcal{M}_X$. 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 7.9. Sejam $\boldsymbol{X} = (X, \mathcal{M}_X)$ um espaço mensurável, Y um conjunto e $f : X \longrightarrow Y$ uma função. A *sigma-álgebra empurrada* por f é

$$f_*(\mathcal{M}_X) := \left\{ M \subseteq Y \;\middle|\; f^{-1}(M) \in \mathcal{M}_X \right\}.$$

Proposição 7.9. *Sejam $\boldsymbol{X} = (X, \mathcal{M}_X)$ um espaço mensurável, Y um conjunto e $f : X \longrightarrow Y$ 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 $(f^{-1}(A))^{\complement} \in \mathcal{M}_X$, pois $\mathcal{M}_X$ é sigma-álgebra. Mas $(f^{-1}(A))^{\complement} = f^{-1}(A^{\complement})$ (3.13), o que implica $f^{-1}(A^{\complement}) \in \mathcal{M}_X$ e, portanto, $A^{\complement} \in \mathcal{M}_Y$. 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 7.10. *Sejam $\boldsymbol{X} = (X, \mathcal{M}_X)$ e $\boldsymbol{Y} = (Y, \mathcal{M}_Y)$ espaços mensuráveis. Uma função $f : X \longrightarrow Y$ é função mensurável de $\boldsymbol{X}$ para $\boldsymbol{Y}$ se, e somente se, a sigma-álgebra $f^*(\mathcal{M}_Y)$ puxada por f é uma sub-sigma-álgebra de $\mathcal{M}_X$.*

$$f \in \mathscr{M}(\boldsymbol{X}, \boldsymbol{Y}) \iff f^*(\mathcal{M}_Y) \subseteq \mathcal{M}_X.$$

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. ■

7.3 Produto de Espaços Mensuráveis

Definição 7.10. Seja $(\boldsymbol{X_i})_{i\in I} = (X_i, \mathcal{M}_i)_{i\in I}$ uma família de espaços mensuráveis. O *produto* da família $(\boldsymbol{X}_i)_{i\in I}$ é o par

$$\prod_{i\in I} \boldsymbol{X_i} := (X, \mathcal{M})$$

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 7.11. *Seja $(\boldsymbol{X}_i)_{i\in I} = (X_i, \mathcal{M}_i)_{i\in I}$ uma família de espaços mensuráveis. Então o produto $\prod_{i\in I} \boldsymbol{X}_i$ 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-álgebras $\pi_i^*(\mathcal{M}_i)$ é a sigma-álgebras puxada por $\pi_i : X \longrightarrow X_i$, portanto uma sigma-álgebra sobre X. Assim, sendo, $\bigcup_{i\in I} \pi_i^*(\mathcal{M}_i) \subseteq \mathsf{P}(X)$ e, portanto, a sigma-álgebra $\mathcal{M}$ gerada por esse conjunto é uma sigma-álgebra sobre X. ■

Proposição 7.12. *Seja $(\boldsymbol{X}_i)_{i\in I} = (X_i, \mathcal{M}_i)_{i\in I}$ uma família de espaços mensuráveis. Para todo $i \in I$, a projeção canônica $\pi_i : \prod_{i\in I} X_i \longrightarrow X_i$ 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 7.13 (Propriedade Universal)**.** *Seja $(\boldsymbol{X}_i)_{i\in I} = (X_i, \mathcal{M}_i)_{i\in I}$ uma família de espaços mensuráveis, $\boldsymbol{Y} = (Y, \mathcal{M}_Y)$ um espaço mensurável e, para todo $i \in I$, $f_i : \boldsymbol{Y} \longrightarrow \boldsymbol{X_i}$ uma função mensurável. Então existe uma única função mensurável $f : \boldsymbol{Y} \longrightarrow \prod_{i\in I} \boldsymbol{X_i}$ tal que, para todo $i \in I$, $\pi_i \circ f = f_i$ (o diagrama comuta).*

$$\begin{tikzcd}
 & \prod_{i\in I} \boldsymbol{X_i} \arrow[d, "\pi_i"] \\
\boldsymbol{Y} \arrow[ur, dashed, "f"] \arrow[r, "f_i"'] & \boldsymbol{X_i}
\end{tikzcd}$$

Demonstração. Defina a função

$$\begin{aligned} f\colon Y &\longrightarrow \prod_{i\in I} X_i \\ y &\longmapsto (f_i(y))_{i\in I}. \end{aligned}$$

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 $(X, \mathcal{M}) := \prod_{i\in I} \boldsymbol{X_i}$. 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. ■

7.4 Espaços Mensuráveis com Estrutura Adicional

7.4.1 Espaços Mensuráveis Topológicos

Definição 7.11. Seja $\boldsymbol{X} = (X, \mathcal{T})$ um espaço topológico. A *σ-álgebra topológica* de $\boldsymbol{X}$ é

$$\mathcal{M}_{\mathcal{T}} := \langle \mathcal{T} \rangle ,$$

a σ-álgebra gerada pela topologia $\mathcal{T}$.

Essa σ-álgebra é comumente chamada de *σ-álgebra de Borel* e seus conjuntos mensuráveis de *borelianos* em homenagem ao matemático francês Émile Borel[1].

Proposição 7.14. *Sejam $\boldsymbol{X} = (X, \mathcal{T})$ um espaço topológico e $\mathcal{B} \subseteq \mathcal{T}$ uma base da topologia. Então*

$$\mathcal{M}_{\mathcal{T}} = \langle \mathcal{B} \rangle .$$

7.4.2 Funções Mensuráveis com Valores Vetoriais

Tratamos brevemente de funções mensuráveis a valores vetoriais. De fato poderíamos somente considerar espaços lineares mensuráveis (nos quais as operações do espaço linear são mensuráveis, mas esse caso é mais geral do que o necessário e não será definido). Pode-se perceber, no entanto, que a demonstração seria a mesma.

Proposição 7.15. *Sejam $\boldsymbol{X}$ um espaço mensurável e $\boldsymbol{L}$ um espaço linear topológico sobre um corpo $\boldsymbol{C}$. O espaço $\mathscr{M}(\boldsymbol{X}, \boldsymbol{L})$ de funções mensuráveis de $\boldsymbol{X}$ para $(L, \mathcal{M}_{\mathcal{T}})$ é um subespaço linear de $\boldsymbol{L}^X$.*

Demonstração. Sejam $c \in C$ e $f, f' \in \mathscr{M}(X, L)$. Como as operações $+$ e $\cdot$ do espaço linear são mensuráveis, pois são contínuas, e f, f' e a função constante c são mensuráveis, segue que cf e $f + f'$ são mensuráveis. ■

7.4.3 Funções Mensuráveis com Valores em Espaços Métricos

Proposição 7.16. *Sejam $\boldsymbol{X} = (X, \mathcal{M}_X)$ um espaço mensurável, $\boldsymbol{Y} = (Y, |\cdot, \cdot|)$ um espaço métrico e $(f_n)_{n \in \mathbb{N}}$ uma sequência de funções mensuráveis de $(X, \mathcal{M}_X)$ para $(Y, \mathcal{M}_{\mathcal{T}})$ que converge pontualmente para $f \colon X \longrightarrow Y$. Então f é mensurável.*

[1] Félix Édouard Justin Émile Borel (07/01/1871 – 03/02/1956)

Demonstração. Como a σ-álgebra topológica de Y é gerada por $\mathcal{T}$, basta mostrar que f puxa abertos para mensuráveis. Primeiro notemos que, se $A \subseteq Y$ é um conjunto aberto, então, para todo $x \in f^{-1}(A)$, existe $N \in \mathbb{N}$ tal que, para todo $n \geq N$, $x \in f_n^{-1}(A)$. Portanto, para todo $m \in \mathbb{N}$,

$$f^{-1}(A) \subseteq \bigcup_{n=m}^{\infty} {f_n}^{-1}(A)$$

e, consequentemente,

$$f^{-1}(A) \subseteq \bigcap_{m=0}^{\infty} \bigcup_{n=m}^{\infty} {f_n}^{-1}(A) = \limsup_{n\in\mathbb{N}} {f_n}^{-1}(A).$$

Segundo, seja $F \subseteq Y$ um conjunto fechado. Suponha que, para todo $m \in \mathbb{N}$, $x \in \bigcup_{n=m}^{\infty} {f_n}^{-1}(F)$. Então existe $N \in \mathbb{N}$ tal que, para todo $n \geq N$, $f_n(x) \in F$, portanto $f(x) \in F$ pois F é fechado. Segue então a inclusão contrária

$$\limsup_{n\in\mathbb{N}} {f_n}^{-1}(F) = \bigcap_{m=0}^{\infty} \bigcup_{n=m}^{\infty} {f_n}^{-1}(F) \subseteq f^{-1}(F).$$

Finalmente, seja agora $A \subseteq Y$ um conjunto aberto, e defina, para todo $n \in \mathbb{N}$, os conjuntos abertos

$$A_n := \left\{ y \in Y \;\middle|\; \left| y, A^{\complement} \right| > n^{-1} \right\}.$$

e os conjuntos fechados

$$F_n := \left\{ y \in Y \;\middle|\; \left| y, A^{\complement} \right| \geq n^{-1} \right\},$$

Claramente $A_n \subseteq F_n$ e

$$A = \bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} F_n.$$

Temos então as inclusões

$$f^{-1}(A) = \bigcup_{N\in\mathbb{N}} f^{-1}(F_N) \supseteq \bigcup_{N\in\mathbb{N}} \limsup_{n\in\mathbb{N}} {f_n}^{-1}(F_N) \supseteq \bigcup_{N\in\mathbb{N}} \limsup_{n\in\mathbb{N}} {f_n}^{-1}(A_N)$$

e

$$f^{-1}(A) = \bigcup_{N\in\mathbb{N}} f^{-1}(A_N) \subseteq \bigcup_{N\in\mathbb{N}} \limsup_{n\in\mathbb{N}} {f_n}^{-1}(A_N),$$

logo $f^{-1}(A) = \bigcup_{n\in\mathbb{N}} \limsup_{n\in\mathbb{N}} {f_n}^{-1}(A_N)$, e como f_n são mensuráveis e A_N são abertos, $f^{-1}(A)$ é mensurável. ■

7.5 Medida e Espaço de Medida

Comentário sobre o Monoide de Números Reais Positivos com Infinito Adotaremos nesta seção as definições de que, em $[0,\infty]$, a adição é definida por

$$\begin{aligned} +\colon [0,\infty]\times[0,\infty] &\longrightarrow [0,\infty] \\ (c,c') &\longmapsto \begin{cases} c+c, & c \neq \infty \ \text{ e } \ c \neq \infty \\ \infty, & c=\infty \ \text{ ou } \ c'=\infty \end{cases} \end{aligned}$$

e a multiplicação é definida por

$$\begin{aligned} \times\colon [0,\infty]\times[0,\infty] &\longrightarrow [0,\infty] \\ (c,c') &\longmapsto \begin{cases} 0, & c=0 \ \text{ ou } \ c'=0 \\ c\times c, & c\in\,]0,\infty[\ \text{ e } \ c'\in\,]0,\infty[\\ \infty, & (c=\infty \ \text{ e } \ c'\neq 0) \ \text{ ou } \ (c\neq 0 \ \text{ e } \ c'=\infty). \end{cases} \end{aligned}$$

7.5.1 Medidas

Isso faz de $[0,\infty]$ um monoide com operação binária de adição $+$ e identidade 0 e um monoide com operação binária de multiplicação $+$ e identidade 1.

Definição 7.12. Seja $\boldsymbol{X}=(X,\mathcal{M})$ um espaço mensurável. Uma *medida* sobre $\boldsymbol{X}$ é uma função $m\colon \mathcal{M}\longrightarrow[0,\infty]$ que satisfaz

1. $m(\emptyset)=0$;
2. Para toda sequência $(M_i)_{i\in\mathbb{N}}$ de conjuntos mensuráveis disjuntos aos pares,

$$m\left(\bigcup_{i\in\mathbb{N}} M_i\right) = \mathop{+}_{i\in\mathbb{N}} m(M_i).$$

Definição 7.13. Sejam X um conjunto e $\mathsf{P}(X)$ a σ-álgebra das partes de X. A *medida de contagem* sobre $(X,\mathsf{P}(X))$ é a função

$$\begin{aligned} \#\colon \mathsf{P}(X) &\longrightarrow [0,\infty] \\ C &\longmapsto \begin{cases} |M|, & |M|<|\mathbb{N}| \\ \infty, & |M|\geq|\mathbb{N}|. \end{cases} \end{aligned}$$

Definição 7.14. Sejam $\boldsymbol{X}$ um espaço mensurável e $x \in X$. A *medida atômica*[2] sobre $\boldsymbol{X}$ em x é a função

$$\begin{aligned} \mathbf{1}|_x \colon \mathcal{M} &\longrightarrow [0, \infty] \\ M &\longmapsto \begin{cases} 1, & x \in M \\ 0, & x \notin M. \end{cases} \end{aligned}$$

Em geral, a notação adotada é δ_x. Note que $\mathbf{1}|_x(M) = \mathbf{1}_M(x)$, portanto adotamos essa notação.

Exemplo 7.3. *Prove que as medida de contagem e atômica são medidas.*

Definição 7.15. 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 7.17. *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. $m(M_1) < +\infty \quad \Longrightarrow \quad m(M_2 \smallsetminus M_1) = m(M_2) - m(M_1)$.

Demonstração. Como $M_2 = M_1 \cup (M_2 \smallsetminus M_1)$ e $M_1 \cap (M_2 \smallsetminus M_1) = \emptyset$, segue que

$$m(M_2) = m(M_1) + m(M_2 \smallsetminus M_1).$$

1. Daí, como $m(M_2 \smallsetminus M_1) \geq 0$, segue que $m(M_2) \geq m(M_1)$.
2. Se $m(M_1) < +\infty$, então, subtraindo-a dos dois lados da equação, temos $m(M_2) - m(M_1) = m(M_2 \smallsetminus M_1)$.

■

Proposição 7.18. *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*

$$m\left(\bigcup_{n \in \mathbb{N}} M_n\right) = \lim_{n \longrightarrow +\infty} m(M_n);$$

2. *Se $(M_n)_{n \in \mathbb{N}}$ é decrescente e existe $n \in \mathbb{N}$ tal que $m(M_n) < +\infty$, então*

$$m\left(\bigcap_{n \in \mathbb{N}} M_n\right) = \lim_{n \longrightarrow +\infty} m(M_n).$$

[2]Essa medida é conhecida como 'medida de Dirac', em homenagem ao físico britânico *Paul Dirac* (08/08/1902 – 20/10/1984). `https://en.wikipedia.org/wiki/Dirac_measure`.

7.5.2 Medida Exterior

O conceito de medida exterior é um conceito mais abrangente que nos permite atribuir a cada subconjunto de um conjunto X um número real positivo. No entanto, nem sempre essa função será uma contavelmente aditiva, o que significa que ela nem sempre é uma medida. Mostraremos um jeito de restringir essa função a subconjuntos propícios de modo a termos uma sigma-álgebra de mensuráveis restrita à qual a medida exterior é uma medida. As medidas exteriores recebem esse nome exatamente porque medem conjuntos fora dessa sigma-álgebra, conjuntos não-mensuráveis.

Definição 7.16. Seja X um conjunto. Uma *medida exterior* sobre $\boldsymbol{X}$ é uma função $m\colon \mathsf{P}(X) \longrightarrow [0,\infty]$ que satisfaz

1. $m(\emptyset) = 0$;
2. Para todos $C, C' \subseteq X$ tais que $C \subset C'$,
$$m(C) \leq m(C');$$
3. Para toda sequência $(C_i)_{i\in\mathbb{N}}$ de subconjuntos de X,
$$m\left(\bigcup_{i\in\mathbb{N}} C_i\right) \leq \mathop{+}_{i\in\mathbb{N}} m(M_i).$$

Definição 7.17. Sejam X um conjunto e $m\colon \mathsf{P}(X) \longrightarrow [0,\infty]$ uma medida exterior sobre X. Um conjunto *mensurável* por m (ou *m-mensurável*) é um conjunto $M \subseteq X$ tal que, para todo conjunto $C \subseteq X$,
$$m(C) = m(C \cap M) + m(C \cap M^{\complement}).$$
O conjunto de conjuntos mensuráveis por m é denotado $\mathcal{M}_m$.

Proposição 7.19. *Sejam X um conjunto e $m\colon \mathsf{P}(X) \longrightarrow [0,\infty]$ uma medida exterior sobre X. A tripla $(X, \mathcal{M}_m, m|_{\mathcal{M}_m})$ é um espaço de medida.*

Esse método nos permite traduzir o problema de construir medida ao problema de construir medidas exteriores. Agora, vamos delinear um método de construir medidas exteriores em X usando somente um conjunto de subconjuntos de X em que uma função real positiva está definida. Essa medida é construída a partir de coberturas e por isso é chamada de medida exterior de cobertura.

Definição 7.18. Seja X um conjunto. Um *pré-sistema de medida* sobre X é um par $(\mathcal{E}, \rho)$, em que $\mathcal{E} \subseteq \mathsf{P}(X)$, $\emptyset \in \mathcal{E}$ e $\rho\colon \mathcal{E} \longrightarrow [0,\infty]$ é uma função tal que $\rho(\emptyset) = 0$.

Na definição seguinte, consideramos $\inf\{\emptyset\} = \infty$, pois o ínfimo é considerado no conjunto $[0, \infty]$.

Definição 7.19. Sejam X um conjunto e $(\mathcal{E}, \rho)$ um pré-sistema de medida sobre X. A *medida exterior de cobertura* induzida por $(\mathcal{E}, \rho)$ é a função

$$\begin{aligned} m^{(\mathcal{E},\rho)} \colon \mathsf{P}(X) &\longrightarrow [0, \infty] \\ C &\longmapsto \inf \left\{ \mathop{+}_{i\in\mathbb{N}} \rho(C_i) \;\middle|\; \{C_i\}_{i\in\mathbb{N}} \subseteq \mathcal{E},\ C \subseteq \bigcup_{i\in\mathbb{N}} C_i \right\}. \end{aligned}$$

Proposição 7.20. *Sejam X um conjunto e $(\mathcal{E}, \rho)$ um pré-sistema de medida sobre X. A medida exterior de cobertura $m^{(\mathcal{E},\rho)}$ induzida por $(\mathcal{E}, \rho)$ é a uma medida exterior sobre X.*

Demonstração. (Conjunto vazio) $m^{(\mathcal{E},\rho)}(\emptyset) = 0$, pois se tomamos a cobertura vazia $(\emptyset)_{i\in\mathbb{N}}$, temos que $\emptyset \subseteq \bigcup_{i\in\mathbb{N}} \emptyset$ e $\rho(\emptyset) = 0$;

(Monotonicidade crescente) Para todos $C, C' \subseteq M$ tais que $C \subseteq C'$, temos que uma cobertura de C' por conjuntos de $\mathcal{E}$ é uma cobertura de C por conjuntos de $\mathcal{E}$, logo $m^{(\mathcal{E},\rho)}(C) \leq m^{(\mathcal{E},\rho)}(C')$;

(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 por conjuntos de $\mathcal{E}$ tal que

$$\mathop{+}_{j\in\mathbb{N}} \rho(U_{i,j}) \leq m^{(\mathcal{E},\rho)}(C_i) + \frac{\varepsilon}{2^{i+1}}.$$

Essa cobertura existe porque $m^{(\mathcal{E},\rho)}(C_i)$ é um ínfimo. Então $(U_{i,j})_{(i,j)\in\mathbb{N}^2}$ é uma cobertura de $\bigcup_{i\in\mathbb{N}} C_i$ por conjuntos de $\mathcal{E}$ e segue que

$$\begin{aligned} m^{(\mathcal{E},\rho)}\left(\bigcup_{i\in\mathbb{N}} C_i\right) &\leq m^{(\mathcal{E},\rho)}\left(\bigcup_{(i,j)\in\mathbb{N}^2} U_{i,j}\right) \\ &\leq \mathop{+}_{(i,j)\in\mathbb{N}^2} \rho(U_{i,j}) \\ &\leq \mathop{+}_{i\in\mathbb{N}} \left(m^{(\mathcal{E},\rho)}(C_i) + \frac{\varepsilon}{2^{i+1}}\right) \\ &= \mathop{+}_{i\in\mathbb{N}} \left(m^{(\mathcal{E},\rho)}(C_i)\right) + \mathop{+}_{i\in\mathbb{N}} \frac{\varepsilon}{2^{i+1}} \\ &= \mathop{+}_{i\in\mathbb{N}} \left(m^{(\mathcal{E},\rho)}(C_i)\right) + \varepsilon. \end{aligned}$$

A primeira desigualdade vem da monotonicidade de $m^{(\mathcal{E},\rho)}$, a segunda de $m^{(\mathcal{E},\rho)}$ 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

$$m^{(\mathcal{E},\rho)}\left(\bigcup_{i\in\mathbb{N}} C_i\right) \leq \mathop{+}_{i\in\mathbb{N}} m^{(\mathcal{E},\rho)}(C_i). \qquad \blacksquare$$

Proposição 7.21. *Sejam X um conjunto e $(\mathcal{E},\rho)$ e $(\mathcal{E}',\rho')$ pré-sistemas de medida tais que $\mathcal{E}' \subseteq \mathcal{E}$ e $\rho \leq \rho'$. Então $m^{(\mathcal{E},\rho)} \leq m^{(\mathcal{E}',\rho')}$.*

Demonstração. Vamos mostrar que $m^{(\mathcal{E},\rho)} \leq m^{(\mathcal{E}',\rho)}$ e então que $m^{(\mathcal{E}',\rho)} \leq m^{(\mathcal{E}',\rho')}$. Seja $C \subseteq X$. Como toda cobertura de C por de $\mathcal{E}'$ é uma cobertura de C por conjuntos de $\mathcal{E}$. Isso implica que

$$\begin{aligned} m^{(\mathcal{E},\rho)}(C) &= \inf\left\{ \mathop{+}_{i\in\mathbb{N}} \rho(C_i) \;\middle|\; \{C_i\}_{i\in\mathbb{N}} \subseteq \mathcal{E},\ C \subseteq \bigcup_{i\in\mathbb{N}} C_i \right\} \\ &\leq \inf\left\{ \mathop{+}_{i\in\mathbb{N}} \rho(C_i) \;\middle|\; \{C_i\}_{i\in\mathbb{N}} \subseteq \mathcal{E}',\ C \subseteq \bigcup_{i\in\mathbb{N}} C_i \right\} \\ &= m^{(\mathcal{E}',\rho)}(C), \end{aligned}$$

o que mostra que $m^{(\mathcal{E},\rho)} \leq m^{(\mathcal{E}',\rho)}$.

Agora, como $\rho(C) \leq \rho'(C)$, segue que, para toda cobertura de C por conjuntos de $\mathcal{E}$,

$$\mathop{+}_{i\in\mathbb{N}} \rho(C_i) \leq \mathop{+}_{i\in\mathbb{N}} \rho'(C_i),$$

portanto

$$\begin{aligned} m^{(\mathcal{E}',\rho)}(C) &= \inf\left\{ \mathop{+}_{i\in\mathbb{N}} \rho(C_i) \;\middle|\; \{C_i\}_{i\in\mathbb{N}} \subseteq \mathcal{E}',\ C \subseteq \bigcup_{i\in\mathbb{N}} C_i \right\} \\ &\leq \inf\left\{ \mathop{+}_{i\in\mathbb{N}} \rho'(C_i) \;\middle|\; \{C_i\}_{i\in\mathbb{N}} \subseteq \mathcal{E}',\ C \subseteq \bigcup_{i\in\mathbb{N}} C_i \right\} \\ &= m^{(\mathcal{E}',\rho')}(C), \end{aligned}$$

o que mostra que $m^{(\mathcal{E}',\rho)} \leq m^{(\mathcal{E}',\rho')}$ e, finalmente, que

$$m^{(\mathcal{E},\rho)} \leq m^{(\mathcal{E}',\rho')}.$$

$\blacksquare$

7.6 Medida em Espaços Topológicos

Consideraremos nesta seção medidas em espaços topológicos. No entanto, em geral supomos que o espaço topológico é separado, isto é, T_2, pois isso garante um mínimo de propriedades de separação entre os pontos do espaço, a separação de pontos por vizinhanças abertas.

Consideraremos, em geral, σ-álgebras que contêm a topologia do espaço, o que é equivalente a dizer que contêm a σ-álgebra topológica do espaço, que é, por definição, a menor σ-álgebra que contém sua topologia.

7.6.1 Medidas Regulares

Definição 7.20. Sejam $\boldsymbol{X} = (X, \mathcal{T})$ um espaço topológico separado, $\mathcal{M}$ uma σ-álgebra sobre X que contém $\mathcal{T}$ e m uma medida sobre $(X, \mathcal{M})$. Um conjunto *interiormente regular* com respeito a m é um conjunto mensurável $M \subseteq X$ tal que

$$m(M) = \sup \{m(C) \mid C \subseteq M,\ C \text{ é compacto}\}.$$

Uma medida *interiormente regular* sobre $(X, \mathcal{M})$ é uma medida m sobre $(X, \mathcal{M})$ para a qual todo conjunto mensurável de X é interiormente regular com respeito a m.

Um conjunto *exteriormente regular* com respeito a m é um conjunto mensurável $M \subseteq X$ tal que

$$m(M) = \sup \{m(C) \mid C \subseteq M, M \in \mathcal{T}\}.$$

Uma medida *exteriormente regular* sobre $(X, \mathcal{M})$ é uma medida m sobre $(X, \mathcal{M})$ para a qual todo conjunto mensurável de X é exteriormente regular com respeito a m.

Um conjunto *regular* com respeito a m é um conjunto que é interior e exteriormente regular com respeito a m. Uma medida *regular* sobre $(X, \mathcal{M})$ é uma medida m sobre $(X, \mathcal{M})$ que é interiormente e exteriormente regular.

7.6.2 Medidas Localmente Finitas

Definição 7.21. Sejam $\boldsymbol{X} = (X, \mathcal{T})$ um espaço topológico separado e $\mathcal{M}$ uma σ-álgebra sobre X que contém $\mathcal{T}$. Uma medida *localmente finita* sobre $(X, \mathcal{M})$ é uma m sobre $(X, \mathcal{M})$ tal que, para todo $x \in X$, existe vizinhança aberta $A \subseteq X$ de x tal que $m(A) < \infty$.

7.7 Medidas em Grupos Topológicos

Definição 7.22. Sejam $\boldsymbol{G}$ um grupo topológico. Uma medida *invariante por translação à direita* sobre $(G, \mathcal{M}_{\mathcal{T}})$ é uma medida m sobre $(G, \mathcal{M}_{\mathcal{T}})$ tal que, para todo $g \in G$ e todo mensurável $M \subseteq G$,

$$m(gM) = m(M).$$

Uma medida *invariante por translação à esquerda* sobre $(G, \mathcal{M}_{\mathcal{T}})$ é uma medida m sobre $(G, \mathcal{M}_{\mathcal{T}})$ tal que, para todo $g \in G$ e todo mensurável $M \subseteq G$,

$$m(Mg) = m(M).$$

Proposição 7.22 ([3])**.** *Seja $\boldsymbol{G}$ um grupo topológico localmente compacto. Existe uma única (a menos de constante multiplicativa) medida não trivial sobre $(G, \mathcal{M}_{\mathcal{T}})$ que é*

1. *Invariante por translação à esquerda;*
2. *Finita em conjuntos compactos;*
3. *Exteriormente regular (em conjuntos mensuráveis);*
4. *Interiormente regular em conjuntos abertos.*

Se $\boldsymbol{G}$ é compacto, existe única medida como acima tal que $m(G) = 1$.

7.8 Medida em Espaços Métricos

7.8.1 Medidas Exteriores Métricas

Definição 7.23. Seja $\boldsymbol{M}$ um espaço métrico. Uma medida exterior *métrica* em $\boldsymbol{M}$ é uma medida exterior $m\colon \mathsf{P}(M) \longrightarrow [0, \infty]$ sobre M tal que, para todos $C, C' \subseteq M$ metricamente separados,

$$m(C \cup C') = m(C) + m(C').$$

Proposição 7.23. *Sejam $\boldsymbol{M}$ um espaço métrico, com σ-álgebra topológica $\mathcal{M}_{\mathcal{T}}$ e m uma medida exterior métrica em $\boldsymbol{M}$. Então todo $M \in \mathcal{M}_{\mathcal{T}}$ é m-mensurável.*

[3] Este teorema é conhecido como 'Teorema de Haar', em homenagem ao matemático húngaro *Alfréd Haar* (11/10/1885 – 16/03/1933). `https://en.wikipedia.org/wiki/Haar_measure`.

Demonstração. Para mostrar isso, mostraremos que todo conjunto fechado é m-mensurável. Basta mostrar que, para todo $C \subseteq M$ com $m(C) < \infty$ e todo fechado $F \subseteq M$,

$$m(C) \geq m(C \cap F) + m(C \cap F^{\complement}),$$

pois a desigualdade contrária sempre vale por subaditividade e a igualdade vale trivialmente se $m(C) = \infty$. Consideremos as vizinhanças fechadas

$$F_j := \overline{\mathrm{B}}_{\frac{1}{j}}(F) = \left\{ p \in M \;\middle|\; |F, p| \leq \frac{1}{j} \right\}.$$

Vale que $\left| C \cap F, C \cap F_j^{\complement} \right| > 0$, portanto

$$m(C) \geq m\left((C \cap F) \cup (C \cap F_j^{\complement}) \right) = m(C \cap F) + m(C \cap F_j^{\complement}).$$

Resta mostrar agora que $\lim_{j \to \infty} m(C \cap F_j^{\complement}) = m(C \cap F^{\complement})$. Como F é fechado, podemos escrever, para todo $j \in \mathbb{N}^*$,

$$C \cap F^{\complement} = \{ p \in C \mid |F, p| > 0 \} = (C \cap F_j^{\complement}) \cup \bigcup_{k=j}^{\infty} R_k,$$

em que $R_k := C \cap \overline{\mathrm{B}}_{\frac{1}{k}}(F) \smallsetminus \overline{\mathrm{B}}_{\frac{1}{k+1}}(F) = \left\{ p \in C \;\middle|\; \frac{1}{k+1} < |F, p| \leq \frac{1}{k} \right\}$. Pela subaditividade de m, segue que

$$m(C \cap F_j^{\complement}) \leq m(C \cap F^{\complement}) \leq m(C \cap F_j^{\complement}) + \mathop{\mathbin{+}}_{k=j}^{\infty} m(R_k).$$

Mas note que $\mathop{\mathbin{+}}_{k=1}^{\infty} m(R_k) < \infty$. Isso ocorre pois, para todo $j \geq i+2$, $|F_i, F_j| > 0$, portanto por indução em N segue que

$$\mathop{\mathbin{+}}_{k=1}^{N} m(R_{2k}) = m\left(\bigcup_{k=1}^{N} R_{2k} \right) \leq m(C) < \infty$$

e

$$\mathop{\mathbin{+}}_{k=1}^{N} m(R_{2k-1}) = m\left(\bigcup_{k=1}^{N} R_{2k-1} \right) \leq m(C) < \infty.$$

Portanto $\mathop{\mathbin{+}}_{k=1}^{\infty} m(R_k) < \infty$, o que implica que $\lim_{j \to \infty} m(C \cap F_j^{\complement}) = m(C \cap F^{\complement})$, e concluímos que F é m-mensurável, resultando que todo $M \in \mathcal{M}_{\mathcal{T}}$ é m-mensurável. ■

7.8.2 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 coincidam com as dimensões de espaços lineares como a reta, o plano, e de variedades.

Consideremos a função diâmetro em $\boldsymbol{M}$

$$\begin{aligned} \varnothing\colon \mathsf{P}(M) &\longrightarrow [0,\infty] \\ C &\longmapsto \varnothing(C). \end{aligned}$$

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 $d(C \times C) \subseteq d(D \times D)$, o que implica

$$\varnothing(C) \leq \varnothing(D);$$

No entanto, não satisfaz (3) Para todos $(C_i)_{i\in\mathbb{N}}$ subconjuntos de M,

$$\varnothing\left(\bigcup_{i\in\mathbb{N}} C_i\right) \leq \mathop{+}_{i\in\mathbb{N}} \varnothing\left(C_i\right).$$

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

$$\varnothing\left(\bigcup_{i\in\mathbb{N}} C_i\right) = 1 > \frac{1}{2} = \mathop{+}_{i\in\mathbb{N}} \varnothing\left(C_i\right).$$

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 $\boldsymbol{M}$ 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 7.24. Sejam $\boldsymbol{M}$ 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 7.25. Sejam $\boldsymbol{M}$ um espaço métrico, $C \subseteq M$, $d \in [0,\infty[$ e $\delta \in \,]0,\infty[$. A *medida d-dimensional δ-precisa* de C em $\boldsymbol{M}$ é

$$H^d_\delta(C) := \inf\left\{ \mathop{+}_{i\in\mathbb{N}} \varnothing(U_i)^d \;\middle|\; (U_i)_{i\in\mathbb{N}} \in \mathcal{C}_\delta(C) \right\}.$$

A *medida d-dimensional δ-precisa* em $\boldsymbol{M}$ é a função

$$\begin{aligned} H^d_\delta \colon \mathsf{P}(M) &\longrightarrow [0,\infty] \\ C &\longmapsto H^d_\delta(C). \end{aligned}$$

A sequência $(U_i)_{i\in\mathbb{N}}$ é uma *δ-cobertura* de C. Mostremos que H^d_δ é uma medida exterior em M.

Proposição 7.24. *Sejam $\boldsymbol{M}$ um espaço métrico, $d \in [0,\infty[$ e $\delta \in \,]0,\infty[$. A função $H^d_\delta \colon \mathsf{P}(M) \longrightarrow [0,\infty]$ é uma medida exterior sobre M.*

Demonstração. (Conjunto vazio) $H^d_\delta(\emptyset) = 0$, 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 $H^d_\delta(C) \leq H^d_\delta(C')$; (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

$$\mathop{+}_{j\in\mathbb{N}} \varnothing(U_{i,j})^d \leq H^d_\delta(C_i) + \frac{\varepsilon}{2^{i+1}}.$$

Essa cobertura existe porque $H^d_\delta(C_i)$ 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

$$\begin{aligned} H^d_\delta\left(\bigcup_{i\in\mathbb{N}} C_i\right) &\leq H^d_\delta\left(\bigcup_{(i,j)\in\mathbb{N}^2} U_{i,j}\right) \\ &\leq \mathop{+}_{(i,j)\in\mathbb{N}^2} \varnothing(U_{i,j})^d \\ &\leq \mathop{+}_{i\in\mathbb{N}} \left(H^d_\delta(C_i) + \frac{\varepsilon}{2^{i+1}}\right) \\ &= \mathop{+}_{i\in\mathbb{N}} \left(H^d_\delta(C_i)\right) + \mathop{+}_{i\in\mathbb{N}} \frac{\varepsilon}{2^{i+1}} \\ &= \mathop{+}_{i\in\mathbb{N}} \left(H^d_\delta(C_i)\right) + \varepsilon. \end{aligned}$$

A primeira desigualdade vem da monotonicidade de H^d_δ, a segunda de H^d_δ 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

$$H^d_\delta\left(\bigcup_{i\in\mathbb{N}} C_i\right) \leq \mathop{+}_{i\in\mathbb{N}} H^d_\delta(C_i). \qquad \blacksquare$$

Definimos agora a medida H^d que independe de δ. Notemos que, se $\delta \leq \delta'$, então $H^d_{\delta'}(C) \leq H^d_\delta(C)$, pois toda cobertura de C com diâmetro δ é uma cobertura com diâmetro δ'. Isso implica que existe em $[0,\infty]$ o limite

$$\lim_{\delta\to 0} H^d_\delta(C) = \sup_{\delta\in]0,\infty[} H^d_\delta(C).$$

Definição 7.26. Sejam $\boldsymbol{M}$ um espaço métrico e $d \in [0,\infty[$. A *medida d-dimensional* em $\boldsymbol{M}$ é a função

$$\begin{aligned} H^d\colon \mathsf{P}(M) &\longrightarrow [0,\infty] \\ C &\longmapsto H^d(C) := \sup_{\delta\in]0,\infty[} H^d_\delta(C). \end{aligned}$$

Proposição 7.25. *Sejam $\boldsymbol{M}$ um espaço métrico e $d \in [0,\infty[$. A função*

$$H^d\colon \mathsf{P}(M) \longrightarrow [0,\infty]$$

é uma medida exterior métrica em M.

Demonstração. (Conjunto vazio) $H^d(\emptyset) = 0$, pois $H^d_\delta(\emptyset) = 0$ para todo $\delta \in]0,\infty[$; (Monotonicidade) Para todos $C, C' \subseteq M$ tais que $C \subseteq C'$, temos que $H^d_\delta(C) \leq H^d_\delta(C')$ 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 $H^d_\delta(C_i) \leq H^d(C_i)$, segue que

$$H^d_\delta\left(\bigcup_{i\in\mathbb{N}} C_i\right) \leq \mathop{+}_{i\in\mathbb{N}} H^d_\delta(C_i) \leq \mathop{+}_{i\in\mathbb{N}} H^d(C_i).$$

Como isso vale para todo δ, segue que

$$H^d\left(\bigcup_{i\in\mathbb{N}} C_i\right) \leq \mathop{+}_{i\in\mathbb{N}} H^d\left(C_i\right).$$

Por fim, pode-se mostrar que, para todos conjuntos $C, C' \in M$ e para todo $\delta < d(C,C')$, tem-se

$$H^d_\delta(C \cup C') = H^d_\delta(C) + H^d_\delta(C'),$$

portanto, se $d(C,C') > 0$, tem-se

$$H^d(C \cup C') = H^d(C) + H^d(C'). \qquad \blacksquare$$

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 $C \in M$,

$$H^d(C) = H^d(C \cap E) + H^d(C \cap E^{\complement}).$$

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 (7.23) e H^d pode ser restringida para uma medida em M. Em geral, não se pode garantir o mesmo para as medidas exteriores[4] H^d_δ. Pode-se ainda mostrar a seguinte proposição.

Proposição 7.26. *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):*

$$H^n = \frac{2^n}{\mathrm{vol}^n(\mathbb{B}^n)}\,\mathrm{vol}^n\,.$$

Lembrando que

$$\mathrm{vol}^n(\mathbb{B}^n) = \frac{(\tau/2)^{\frac{n}{2}}}{(n/2)!}$$

em que $\tau = 6,28\ldots$ é a constante do círculo (razão da circunferência pelo raio) e a função fatorial ! é entendida como a extensão dada pela função Γ, definida $x! = \Gamma(x+1)$, ou mais explicitamente por

$$\begin{aligned} !\colon [0,\infty] &\longrightarrow [0,\infty] \\ x &\longmapsto \int_0^\infty t^x \mathrm{e}^{-t}\mathrm{d}t. \end{aligned}$$

Alguns casos particulares são

$$H^0 = \mathrm{vol}^0 = \# \qquad H^1 = \mathrm{vol}^1$$
$$H^2 = \frac{8}{\tau}\,\mathrm{vol}^2 \qquad H^3 = \frac{12}{\tau}\,\mathrm{vol}^3$$

O fator $\mathrm{vol}^n(\mathbb{B}^n)$ poderia ser evitado multiplicando-o na definição de H^n_δ, e o fator 2^n poderia ser evitado avaliando a soma de $\left(\frac{\varnothing(U_i)}{2}\right)^n$ em vez de somente $\varnothing(U_i)^n$. O número $\frac{\varnothing(C)}{2}$ pode ser naturalmente entendido como o *raio* do conjunto C.

[4] `https://web.stanford.edu/class/math285/ts-gmt.pdf`

7.8.3 Dimensão Métrica e Fractais

Seja $C \subseteq M$ um conjunto. A função

$$\begin{aligned} H^{(\cdot)}(C)\colon [0,\infty[&\longrightarrow [0,\infty] \\ d &\longmapsto H^d(C) \end{aligned}$$

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

$$\dim(C) := \inf \left\{ d \in [0,\infty[\;\middle|\; H^d(C) = 0 \right\}.$$

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 7.1. Exitem subconjuntos de $\mathbb{R}^d$ que têm dimensões não inteiras. Esses conjuntos são conhecidos como *fractais*.

Figura 7.1: Gráfico de $H^d(C)$ em função de d.

7.9 Espaço Linear de Medidas

Podemos expandir o conceito de medida para obtermos mais estrutura algébrica entre as medidas. Vamos modificar o conceito de medida para admitir valores negativos, mas em contrapartida temos que impedir que a medida de um conjunto seja infinita. Para isso, podemos definir a medida como uma função assumindo valores em $\mathbb{R}$ mas, de modo mais geral, basta considerarmos valores em um corpo topológico, o que permite que tenhamos medidas com valores em $\mathbb{C}$, ou podemos até mesmo generalizar para espaços lineares topológicos. A estrutura linear é o que garante que o espaço de medidas será também um espaço linear e a topologia é o que garante que podemos falar de convergência de uma sequência de elementos do

espaço linear, o que é necessário para que definamos a propriedade de σ-aditividade de uma medida.

Definição 7.27. Sejam $\boldsymbol{X} = (X, \mathcal{M})$ um espaço mensurável e $\boldsymbol{L}$ um espaço linear topológico sobre um corpo topológico $\boldsymbol{C}$. Uma *medida* sobre $\boldsymbol{X}$ a valores em $\boldsymbol{L}$ é uma função $m\colon \mathcal{M} \longrightarrow L$ que satisfaz:

1. $m(\emptyset) = 0$;
2. Para toda sequência $(M_i)_{i\in\mathbb{N}}$ de conjuntos mensuráveis disjuntos,

$$m\left(\bigcup_{i\in\mathbb{N}} M_i\right) = \mathop{+}_{i\in\mathbb{N}} m(M_i).$$

O conjunto das medidas sobre $\boldsymbol{X}$ a valores em $\boldsymbol{L}$ é denotado $\mathfrak{M}(\boldsymbol{X}, \boldsymbol{L})$. Caso não haja ambiguidade, denotamos $\mathfrak{M}$.

O conjunto $\mathfrak{M}(\boldsymbol{X})$ das medidas sobre $\boldsymbol{X}$ é um espaço de funções do conjunto $\mathcal{M}$ para o corpo (ou espaço linear) $\mathbb{R}$. Nesse sentido, podemos entender $\mathfrak{M}(\boldsymbol{X})$ como um subconjunto de $\mathbb{R}^{\mathcal{M}}$ e, de fato, esse conjunto forma um subespaço com respeito à adição e à multiplicação pontuais, bem como inversas e identidades de cada.

Proposição 7.27. *Seja $\boldsymbol{X}$ um espaço mensurável. O espaço $\mathfrak{M}(\boldsymbol{X})$ é um subespaço linear de $\mathbb{R}^{\mathcal{M}}$.*

Demonstração. Temos que mostrar que $\mathfrak{M}(\boldsymbol{X})$ é fechado pela adição e multiplicação. Sejam $c \in \mathbb{R}$ e $m, m' \in \mathfrak{M}(\boldsymbol{X})$. Então

1. $(cm + m')(\emptyset) = cm(\emptyset) + m'(\emptyset) = 0$;
2. Seja $(M_i)_{i\in\mathbb{N}}$ uma sequência de conjuntos mensuráveis disjuntos. Então

$$\begin{aligned}(cm + m')\left(\bigcup_{i\in\mathbb{N}} M_i\right) &= cm\left(\bigcup_{i\in\mathbb{N}} M_i\right) + m'\left(\bigcup_{i\in\mathbb{N}} M_i\right)\\ &= \mathop{+}_{i\in\mathbb{N}} cm(M_i) + \mathop{+}_{i\in\mathbb{N}} m'(M_i)\\ &= \mathop{+}_{i\in\mathbb{N}} (cm + m')(M_i).\end{aligned}$$

■

Quando $L = \mathbb{R}$, podemos quase recuperar a definição que tínhamos de medida finita considerando as *medidas positivas*. Esse é o conjunto das medida reais que só assumem valores em $\mathbb{R}_{\geq 0} = [0, \infty[$ e é denotado $\mathfrak{M}_{\geq 0}$. Note que $\mathfrak{M}_{\geq 0}$ é um cone em $\mathfrak{M}$, pois para todo $c \in \mathbb{R}_{\geq 0}$ e toda $m \in \mathfrak{M}_{\geq 0}$, temos $cm \in \mathfrak{M}_{\geq 0}$. Além disso, se $m \in \mathfrak{M}_{\geq 0} \cap -\mathfrak{M}_{\geq 0}$, então, para todo $M \in \mathcal{M}$, $m(M) \geq 0$ e $-m(M) \geq 0$, portanto $m = 0$, o que mostra que $\mathfrak{M}_{\geq 0}(\boldsymbol{X})$ é um cone agudo, ou seja, $\mathfrak{M}_{\geq 0}(\boldsymbol{X}) \cap -\mathfrak{M}_{\geq 0}(\boldsymbol{X}) = \{0\}$.

De modo mais geral, se temos um cone X em um espaço linear $\boldsymbol{L}$, então o espaço $\mathfrak{M}|_X$ é um cone e, se X é agudo, então $\mathfrak{M}$.

7.10 Quase

7.10.1 Quase Todo

A estrutura de medida nos permite definir um novo quantificador, que formaliza o conceito de que quase todo ponto satisfaz alguma propriedade, ou seja, de que, a menos de pontos em um conjunto de medida nula, todos os pontos satisfazem tal propriedade.

Definição 7.28. Seja $\boldsymbol{X}$ um espaço de medida. Uma propriedade P de elementos de X vale para *quase todo* ponto se existe um conjunto $M \in \mathcal{M}$ com $m(M) = 0$ tal que, para todo $x \in X \smallsetminus M$, vale a propriedade P:

$$\mathring{\bigwedge} x \mathrm{P} x \equiv \bigvee M \bigwedge x (M \in \mathcal{M} \wedge m(M) = 0 \wedge (x \in X \smallsetminus M \to \mathrm{P}x)).$$

A partir desse quantificador, podemos definir o quantificador *quase existe* da seguinte forma

$$\mathring{\bigvee} x \mathrm{P} x \equiv \neg \mathring{\bigwedge} x \neg \mathrm{P} x$$

$$\begin{aligned}
\neg \mathring{\bigwedge} x \neg \mathrm{P} x &\equiv \neg \bigvee M \bigwedge x (M \in \mathcal{M} \wedge m(M) = 0 \wedge (x \in X \smallsetminus M \to \neg \mathrm{P}x)) \\
&\equiv \bigwedge M \bigvee x (M \notin \mathcal{M} \vee m(M) > 0 \vee (x \in X \smallsetminus M \wedge \mathrm{P}x)) \\
&\equiv \bigwedge M \bigvee x (\neg (M \notin \mathcal{M} \vee m(M) > 0) \to (x \in X \smallsetminus M \wedge \mathrm{P}x)) \\
&\equiv \bigwedge M \bigvee x (M \in \mathcal{M} \wedge m(M) = 0 \to (x \in X \smallsetminus M \wedge \mathrm{P}x))
\end{aligned}$$

pois

$$\neg (A \to B) \equiv A \wedge \neg B$$

$$A \vee B \equiv \neg A \to B$$

Proposição 7.28. *Sejam $\boldsymbol{X}$ um espaço de medida e* P *e* Q *propriedades de elementos de X. Então*

1. $\overset{\circ}{\bigwedge} x\mathrm{P}x \wedge \overset{\circ}{\bigwedge} x\mathrm{Q}x \to \overset{\circ}{\bigwedge} x(\mathrm{P}x \wedge \mathrm{Q}x)$;

2. $\bigwedge x\mathrm{P}x \to \overset{\circ}{\bigwedge} x\mathrm{P}x$;

3. $\overset{\circ}{\bigvee} x\mathrm{P}x \to \bigvee x\mathrm{P}x$;

4. $\neg\overset{\circ}{\bigvee} x\neg\mathrm{P}x \equiv \overset{\circ}{\bigwedge} x\mathrm{P}x$;

Demonstração. 1. Sejam $M, N \in \mathcal{M}$ os conjuntos de medida 0 em cujos complementares P e Q falham, respectivamente. Então $M \cup N \in \mathcal{M}$ tem medida 0, portanto P e Q falham no complementar de $M \cup N$ e segue o teorema.

2. Tomando $M = \emptyset$, temos $X \setminus M = X$ e concluímo que para todo $x \in X \setminus M$ vale $\mathrm{P}x$.

3. Tomando $M = \emptyset$, temos $X \setminus M = X$ e concluímos que existe $x \in X$ tal que $\mathrm{P}x$.

4. Exercício.

■

7.10.2 Quase Igualdade de Conjuntos

Definição 7.29. Sejam $\boldsymbol{X} = (X, \mathcal{M}, m)$ um espaço de medida e $A \in \mathcal{M}$. Um conjunto *quase contido* em A com respeito a $\boldsymbol{X}$ é um conjunto $B \in \mathcal{M}$ tal que $m(B \setminus A) = 0$. Denota-se $B \overset{\circ}{\subseteq} A$.

Um conjunto *quase igual* a A com respeito a $\boldsymbol{X}$ é um conjunto $B \in \mathcal{M}$ tal que $B \overset{\circ}{\subseteq} A$ e $A \overset{\circ}{\subseteq} B$. Denota-se $B \overset{\circ}{=} A$. Conjuntos *quase vazios* em $\boldsymbol{X}$ são conjuntos quase iguais ao conjunto vazio ($A \overset{\circ}{=} \emptyset$) e conjuntos *quase totais* em $\boldsymbol{X}$ são conjuntos quase iguais a X ($A \overset{\circ}{=} X$).

Proposição 7.29. *Seja $\boldsymbol{X}$ um espaço de medida.*

1. *A relação $\overset{\circ}{\subseteq}$ em $\mathcal{M}$ é uma relação de ordem parcial (com respeito a $\overset{\circ}{=}$);*

2. *A relação $\overset{\circ}{=}$ em $\mathcal{M}$ é uma relação de equivalência.*

Demonstração. 1. (Reflexividade) Seja $A \in \mathcal{M}$. Então $A \overset{\circ}{\subseteq} A$, pois $m(A \setminus A) = m(\emptyset) = 0$. (Antissimetria) Sejam $A, B \in \mathcal{M}$ tais que $A \overset{\circ}{\subseteq} B$ e $B \overset{\circ}{\subseteq} A$. Então $A \overset{\circ}{=} B$ por definição. (Transitividade) Sejam $A, B, C \in \mathcal{M}$ tais que $A \overset{\circ}{\subseteq} B$ e $B \overset{\circ}{\subseteq} C$. Então $m(A \setminus B) = 0$ e $m(B \setminus C) = 0$. Mas $A \setminus C =$

$(A \cap B \setminus C) \cup (A \setminus (B \cup C))$; como $(A \cap B \setminus C) \subseteq B \setminus C$ e $(A \setminus (B \cup C)) \subseteq A \setminus B$, segue que

$$m(A \setminus C) = m(A \cap B \setminus C) + m(A \setminus (B \cup C)) \leq 0,$$

logo $A \overset{\circ}{\subseteq} C$;

2. (Reflexividade) Seja $A \in \mathcal{M}$. Então $A \overset{\circ}{=} A$, pois $A \overset{\circ}{\subseteq} A$. (Simetria) Sejam $A, B \in \mathcal{M}$ tais que $A \overset{\circ}{=} B$. Então $A \overset{\circ}{\subseteq} B$ e $B \overset{\circ}{\subseteq} A$, portanto $B \overset{\circ}{=} A$. (Transitividade) Sejam $A, B, C \in \mathcal{M}$ tais que $A \overset{\circ}{=} B$ e $B \overset{\circ}{=} C$. Então $A \overset{\circ}{\subseteq} B$ e $B \overset{\circ}{\subseteq} C$, portanto $A \overset{\circ}{\subseteq} C$. Analogamente, $C \overset{\circ}{\subseteq} A$, portanto $A \overset{\circ}{=} C$.

■

Proposição 7.30. *Sejam $\boldsymbol{X}$ um espaço de medida e $A, B \in \mathcal{M}$.*

1. *$A \overset{\circ}{=} B$ se, e somente se, $m(A \triangle B) = 0$;*
2. *Se $A \overset{\circ}{=} B$, então $m(A) = m(B)$;*
3. *Se $A \subseteq B$, então $A \overset{\circ}{=} B$ implica $m(A) = m(B)$; se $A \subseteq B$ e m é finita, então $m(A) = m(B)$ implica $A \overset{\circ}{=} B$;*
4. *$A \overset{\circ}{=} \emptyset$ se, e somente se, $m(A) = 0$;*
5. *$A \overset{\circ}{=} X$ se, e somente se, $m(A^{\complement}) = 0$. Se m é finita, $A \overset{\circ}{=} X$ se, e somente se, $m(A) = m(X)$;*
6. *$A \overset{\circ}{=} \emptyset$ se, e somente se, $A^{\complement} \overset{\circ}{=} X$;*
7. *Se $A \overset{\circ}{=} X$ e $B \overset{\circ}{=} X$, então $A \cap B \overset{\circ}{=} X$.*
8. *Se $A \overset{\circ}{=} X$ e m é finita, então, para todo $B \subseteq A$, vale $m(B) = m(A \cap B)$;*

Demonstração. 1. Como $A \setminus B$ e $B \setminus A$ são disjuntos, temos $m(A \triangle B) = m(A \setminus B) + m(B \setminus A)$, portanto $m(A \setminus B) = m(B \setminus A) = 0$ se, e somente se, $m(A \triangle B) = 0$;

2. Como $A \setminus B$ e $B \setminus A$ são disjuntos, temos $m(A \triangle B) = m(A \setminus B) + m(B \setminus A)$, portanto $m(A \setminus B) = m(B \setminus A) = 0$. Como $A = (A \cap B) \cup (A \setminus B)$ e $A \cap B$ e $A \setminus B$ são disjuntos, $m(A) = m(A \cap B) + m(A \setminus B) = m(A \cap B)$. Analogamente $m(B) = m(B \cap A)$, portanto $m(A) = m(B)$.

3. Como $A \subseteq B$, então $A \cup B = A$ e $A \cap B = B$, logo de $m(A \triangle B) = 0$ segue

$$m(A) = m(A \cup B) = m(A \cap B) + m(A \triangle B) = m(B).$$

Se m é finita, da mesma igualdade segue que

$$m(A \triangle B) = m(A \cup B) - m(A \cap B) = m(A) - m(B) = 0.$$

4. A ida segue do item acima. Como $A \cup \emptyset = A$ e $A \cap \emptyset = \emptyset$, segue que $A \triangle \emptyset = A$, logo $m(A \triangle \emptyset) = m(A)$. Assim segue de $m(A) = 0$ que $A \mathrel{\mathring{=}} \emptyset$.

5. A ida segue do item acima e de $m(X) = m(A) + m(A^{\complement})$. Como $A \cup X = X$ e $A \cap X = A$, segue que $A \triangle X = A^{\complement}$, logo $m(A \triangle X) = m(A^{\complement})$. Assim segue de $m(A^{\complement}) = 0$ que $A \mathrel{\mathring{=}} X$. Se m é finita, $m(A^{\complement}) = m(X) - m(A)$. Assim segue de $m(A) = m(X)$ se, e somente se, $m(A^{\complement}) = 0$.

6. Consequência dos itens anteriores.

7. Como $A \mathrel{\mathring{=}} X$ e $B \mathrel{\mathring{=}} X$, então $m(A^{\complement}) = m(B^{\complement}) = 0$, portanto

$$m\left((A \cap B)^{\complement}\right) = m\left(A^{\complement} \cup B^{\complement}\right) \leq m\left(A^{\complement}\right) + m\left(B^{\complement}\right) = 0,$$

o que mostra que $A \cap B \mathrel{\mathring{=}} X$.

8. Como $A \subseteq A \cup B$, então $m(A \cup B) = m(A \cap B) + m(A \triangle B) = 1$ e $m(A) = m(A \cap B) + m(A \smallsetminus B) = 1$, e, por m ser finita, igualando as expressões segue que

$$m(A \triangle B) = m(A \smallsetminus B).$$

Como

$$m(A \triangle B) = m(A \smallsetminus B) = m(B \smallsetminus A),$$

segue que $m(B \smallsetminus A) = 0$. Portanto, como

$$m(B) = m(B \cap A) + m(B \smallsetminus A)$$

concluímos que $m(B) = m(B \cap A)$.

■

Proposição 7.31. *Seja $\boldsymbol{X}$ um espaço de medida.*

1. *Os conjuntos $\{M \in \mathcal{M} \mid M \mathrel{\mathring{=}} \emptyset\}$ e $\{M \in \mathcal{M} \mid M \mathrel{\mathring{=}} X\}$ são fechados sob união e interseção enumeráveis;*

2. *O conjunto $\{M \in \mathcal{M} \mid M \mathrel{\mathring{=}} \emptyset \;\; ou \;\; M \mathrel{\mathring{=}} X\}$ é uma sigma-álgebra.*

Demonstração. 1. Seja $(M_i)_{i\in\mathbb{N}}$ uma sequência de conjuntos quase vazios. Então

$$m\left(\bigcup_{i\in\mathbb{N}} M_i\right) \leq \mathop{+}_{i\in\mathbb{N}} m(M_i) = 0$$

e, para algum $i \in \mathbb{N}$

$$m\left(\bigcap_{i\in\mathbb{N}} M_i\right) \leq m(M_i) = 0.$$

Seja $(M_i)_{i\in\mathbb{N}}$ uma sequência de conjuntos quase totais. O mesmo vale já que $M \mathrel{\mathring{=}} X$ se, e somente, $M^{\complement} \mathrel{\mathring{=}} \emptyset$.

2. Segue do item anterior, do fato que $M \mathrel{\mathring{=}} X$ se, e somente, $M^{\complement} \mathrel{\mathring{=}} \emptyset$, e de $\emptyset$ ser quase vazio.

■

7.10.3 Quase Igualdade de Funções

Existem dois modos de generalizar o conceito de função a partir de uma estrutura de medida, de modo a considerar equivalentes funções que diferem em um conjunto de medida zero. O método padrão consiste em construir classes de equivalência de funções definidas no espaço todo. O outro é considerar funções que não estão definidas no domínio todo do espaço. Descreveremos a abordagem padrão e numa subseção posterior esboçaremos algumas construções da segunda abordagem.

Definição 7.30. Sejam $\boldsymbol{X}$ espaço de medida e X' conjunto. Funções de $\boldsymbol{X}$ para X' *quase iguais* são funções (mensuráveis) $f\colon X \longrightarrow X'$ e $f'\colon X \longrightarrow X'$ tais que, para quase todo $x \in X$, $f(x) = f'(x)$. Denota-se $f \mathrel{\mathring{=}} f'$.

Explicitamente, a definição significa que existe $N \in \mathcal{M}$ tal que $N \mathrel{\mathring{=}} \emptyset$ e, para todo $x \in X \smallsetminus N$, $f(x) = f'(x)$; ou ainda, tal que $f|_{X\smallsetminus N} = f'|_{X\smallsetminus N}$.

Proposição 7.32. *Sejam $\boldsymbol{X}$ espaço de medida e X' conjunto. A relação $\mathring{=}$ de quase igualdade de funções é uma relação de equivalência no conjunto de funções de X para X'.*

Demonstração. Sejam $f, f', f''\colon X \longrightarrow X'$. (Reflexividade) Claramente, $f \mathrel{\mathring{=}} f$. (Simetria) Claramente $f \mathrel{\mathring{=}} f'$ implica $f' \mathrel{\mathring{=}} f$. (Transitividade) Se $f \mathrel{\mathring{=}} f'$ e $f' \mathrel{\mathring{=}} f''$, então existem conjuntos N e N' quase vazios tais que $f|_{X\smallsetminus N} = f'|_{X\smallsetminus N}$ e $f'|_{X\smallsetminus N'} = f'|_{X\smallsetminus N}$. Então, como $N \cap N'$ é quase vazio, segue que $f|_{X\smallsetminus(N\cap N')} = f'|_{X\smallsetminus(N\cap N')} = f''|_{X\smallsetminus(N\cap N')}$, portanto $f \mathrel{\mathring{=}} f''$. ■

Embora não seja necessário na definição que as funções sejam mensuráveis, consideraremos somente funções mensuráveis. Lembremos que, dados $\boldsymbol{X}$ e $\boldsymbol{X}'$ espaços de medida, $\mathscr{M}(\boldsymbol{X}, \boldsymbol{X}')$ é o conjunto de funções mensuráveis de $\boldsymbol{X}$ para $\boldsymbol{X}'$. Como $\overset{\circ}{=}$ é uma equivalência, podemos quocientar esse espaço pela equivalência, obtendo o conjunto de classes de equivalência de funções mensuráveis

Definição 7.31. Sejam $\boldsymbol{X}$ e $\boldsymbol{X}'$ espaços de medida. Uma *quase função* é uma classe de equivalência

$$[f] = \{f' \in \mathscr{M}(\boldsymbol{X}, \boldsymbol{X}') \mid f' \overset{\circ}{=} f\}.$$

O conjunto de *quase funções* de $\boldsymbol{X}$ para $\boldsymbol{X}'$ é o conjunto quociente

$$\mathscr{M}_{\overset{\circ}{=}}(\boldsymbol{X}, \boldsymbol{X}') := \mathscr{M}(\boldsymbol{X}, \boldsymbol{X}')\big/\overset{\circ}{=}.$$

Quando conveniente, denotaremos uma quase função $[f]$ cujo representante é f por f, para simplificar a notação.

Definição 7.32. Sejam $\boldsymbol{X}$, $\boldsymbol{X}'$ e $\boldsymbol{X}''$ espaços de medida. A *composição* de quase funções é definida como

$$\begin{aligned} \circ \colon \mathscr{M}_{\overset{\circ}{=}}(\boldsymbol{X}', \boldsymbol{X}'') \times \mathscr{M}_{\overset{\circ}{=}}(\boldsymbol{X}, \boldsymbol{X}') &\longrightarrow \mathscr{M}_{\overset{\circ}{=}}(\boldsymbol{X}, \boldsymbol{X}'') \\ ([f'], [f]) &\longmapsto [f' \circ f]. \end{aligned}$$

Proposição 7.33. *Sejam $\boldsymbol{X}$, $\boldsymbol{X}'$, $\boldsymbol{X}''$ e $\boldsymbol{X}'''$ espaços de medida.*

1. *Para toda $[f] \in \mathscr{M}_{\overset{\circ}{=}}(\boldsymbol{X}, \boldsymbol{X}')$,*

$$[\mathrm{I}_{X'}] \circ [f] = [f] = [f] \circ [\mathrm{I}_X];$$

2. *Para todas $[f] \in \mathscr{M}_{\overset{\circ}{=}}(\boldsymbol{X}, \boldsymbol{X}')$, $[f'] \in \mathscr{M}_{\overset{\circ}{=}}(\boldsymbol{X}', \boldsymbol{X}'')$ e $[f''] \in \mathscr{M}_{\overset{\circ}{=}}(\boldsymbol{X}'', \boldsymbol{X}''')$,*

$$[f''] \circ ([f'] \circ [f]) = ([f''] \circ [f']) \circ [f].$$

Abordagem Alternativa

Nesta subseção, definimos outros objetos com o nome de quase funções. Eles têm uma relação direta com as quase funções da seção anterior, mas fora desta seção, uma quase função sempre será entendida como uma classe de equivalência de funções que diferem somente em um conjunto de medida zero, como na seção anterior.

Definição 7.33. Sejam $\boldsymbol{X}_1$ e $\boldsymbol{X}_2$ espaços de medida. Uma *quase função* de $\boldsymbol{X}_1$ para $\boldsymbol{X}_2$ é uma função $f \colon C \longrightarrow X_2$ tal que $C \overset{\circ}{=} X_1$. Denota-se $f \colon \boldsymbol{X}_1 \overset{\circ}{\longrightarrow} \boldsymbol{X}_2$.

Definição 7.34. Sejam X_1, C_1, X_2, C_2 e X_3 conjuntos tais que $C_1 \subseteq X_1$ e $C_2 \subseteq X_2$, e $f_1 \colon C_1 \longrightarrow X_2$ e $f_2 \colon C_2 \longrightarrow X_3$ funções. A *composição* (generalizada) de f_1 com f_2 é a função

$$\begin{aligned} f_2 \circ f_1 \colon C_1 \cap {f_1}^{-1}(C_2) &\longrightarrow X_3 \\ x &\longmapsto f_2(f_1(x)). \end{aligned}$$

Proposição 7.34 (Composição de quase função)**.** *Sejam $\boldsymbol{X}_1$, $\boldsymbol{X}_2$ e $\boldsymbol{X}_3$ espaços de medida e $f_1 \colon \boldsymbol{X}_1 \xrightarrow{\circ} \boldsymbol{X}_2$ e $f_2 \colon \boldsymbol{X}_2 \xrightarrow{\circ} \boldsymbol{X}_3$ quase funções, com respectivos domínios C_1 e C_2, que preservam medida. Então $f_2 \circ f_1 \colon \boldsymbol{X}_1 \xrightarrow{\circ} \boldsymbol{X}_3$ é uma quase função, com domínio $C_1 \cap {f_1}^{-1}(C_2)$, que preserva medida.*

Demonstração. Como f_1 e f_2 preservam medida, $f_2 \circ f_1$ preserva medida. Basta mostrar que seu domínio é quase total. Como f_1 é quase função, $m_1({C_1}^{\complement}) = 0$, e como f_2 é quase função, $m_2({C_2}^{\complement}) = 0$. Assim, como f_1 preserva medida, $m_1({f_1}^{-1}((C_2)^{\complement})) = m_2((C_2)^{\complement}) = 0$. Por fim segue que

$$\begin{aligned} m_1\left(\left(C_1 \cap {f_1}^{-1}(C_2)\right)^{\complement}\right) &= m_1\left({C_1}^{\complement} \cup {f_1}^{-1}({C_2}^{\complement})\right) \\ &\leq m_1\left({C_1}^{\complement}\right) + m_1\left({f_1}^{-1}({C_2}^{\complement})\right) \\ &= 0 + 0 = 0, \end{aligned}$$

portanto $C_1 \cap {f_1}^{-1}(C_2) \mathrel{\mathring{=}} X_1$, e concluímos que $f_2 \circ f_1$ é uma quase função. ■

Proposição 7.35 (Associatividade)**.** *Sejam $\boldsymbol{X}_1$, $\boldsymbol{X}_2$, $\boldsymbol{X}_3$ e $\boldsymbol{X}_4$ espaços de medida e $f_1 \colon \boldsymbol{X}_1 \xrightarrow{\circ} \boldsymbol{X}_2$, $f_2 \colon \boldsymbol{X}_2 \xrightarrow{\circ} \boldsymbol{X}_3$ e $f_3 \colon \boldsymbol{X}_3 \xrightarrow{\circ} \boldsymbol{X}_4$ quase funções, com respectivos domínios C_1, C_2 e C_3, que preservam medida. Então*

$$f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1.$$

Demonstração. O domínio de $f_3 \circ (f_2 \circ f_1)$ é o conjunto

$$(C_1 \cap {f_1}^{-1}(C_2)) \cap (f_2 \circ f_1)^{-1}(C_3)$$

e o domínio de $(f_3 \circ f_2) \circ f_1$ é o conjunto

$$C_1 \cap {f_1}^{-1}(C_2 \cap {f_2}^{-1}(C_3)).$$

Vamos mostrar que esses conjuntos são iguais.

$$\begin{aligned} (C_1 \cap {f_1}^{-1}(C_2)) \cap (f_2 \circ f_1)^{-1}(C_3) &= C_1 \cap {f_1}^{-1}(C_2) \cap (f_2 \circ f_1)^{-1}(C_3) \\ &= C_1 \cap {f_1}^{-1}(C_2) \cap {f_1}^{-1}({f_2}^{-1}(C_3)) \\ &= C_1 \cap {f_1}^{-1}(C_2 \cap {f_2}^{-1}(C_3)). \end{aligned}$$

■

Definição 7.35. Sejam $\boldsymbol{X}_1$ e $\boldsymbol{X}_2$ espaços de medida. Quase funções de $\boldsymbol{X}_1$ para $\boldsymbol{X}_2$ *quase iguais* são quase funções $f_1\colon \boldsymbol{X}_1 \overset{\circ}{\longrightarrow} \boldsymbol{X}_2$ e $f_2\colon \boldsymbol{X}_1 \overset{\circ}{\longrightarrow} \boldsymbol{X}_2$ satisfazendo $f_1|_C = f_2|_C$ para algum conjunto $C \overset{\circ}{=} X_1$. Denota-se $f_1 \overset{\circ}{=} f_2$.

Proposição 7.36. *A relação $\overset{\circ}{=}$ de quase igualdade de quase funções é uma relação de equivalência.*

Demonstração. Sejam $f, f', f''\colon X \longrightarrow X'$. (Reflexividade) Claramente, $f \overset{\circ}{=} f$. (Simetria) Claramente $f \overset{\circ}{=} f'$ implica $f' \overset{\circ}{=} f$. (Transitividade) Se $f \overset{\circ}{=} f'$ e $f' \overset{\circ}{=} f''$, então existem conjuntos C e C' quase totais tais que $f|_C = f'|_C$ e $f'|_{C'} = f'|_{C'}$. Então, como $C \cap C'$ é quase total, segue que $f|_{C\cap C'} = f'|_{C\cap C'} = f''|_{C\cap C'}$, portanto $f \overset{\circ}{=} f''$. ■

Capítulo 8

Integração

8.1 Integral de Funções Mensuráveis Simples

Lembremos que a função indicadora de um conjunto X é a função

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

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 8.1. *Seja $(X, \mathcal{M})$ um espaço mensurável. Um conjunto $M \subseteq X$ é mensurável se, e somente se, $\mathbf{1}_M \in \mathscr{M}(\boldsymbol{X}, \{0,1\})$ é mensurável.*

Demonstração. Basta notar que $\mathbf{1}_M^{-1}(\{1\}) = M$ e $\mathbf{1}_M^{-1}(\{0\}) = M^{\complement}$. Se M é mensurável, então $M^{\complement}$ 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 $f\colon X \longrightarrow \mathbb{R}$ em um conjunto C se multiplicamos f por $\mathbf{1}_C$ (com a

multiplicação definida pontualmente). Nesse caso, temos a função

$$\begin{aligned} \mathbf{1}_C f \colon X &\longrightarrow \mathbb{R} \\ x &\longmapsto \mathbf{1}_C(x) f(x) = \begin{cases} f(x), & x \in C \\ 0, & x \notin C. \end{cases} \end{aligned}$$

Consideraremos primeiro funções que têm um número finito de valores. Essas funções são chamadas simples.

Definição 8.1. Seja $(X, \mathcal{M}, m)$ um espaço de medida. Uma função *simples* em X é uma função $f \colon X \longrightarrow \mathbb{R}$ 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 8.2. *Sejam $(X, \mathcal{M}, m)$ um espaço de medida e $f, f' \in \mathscr{M}(\boldsymbol{X}, [0, \infty])$ funções simples mensuráveis.*

1. *A partição por níveis $\mathcal{P}_f$ é uma partição por medida de X e*

$$f = \mathop{+}_{c \in f(X)} c \mathbf{1}_{f^{-1}(c)}.$$

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 8.2. Sejam $\boldsymbol{X} = (X, \mathcal{M}, m)$ um espaço de medida e $f \in \mathscr{M}(\boldsymbol{X}, [0, \infty])$ uma função simples mensurável. A *integral* de f em $\boldsymbol{X}$ é

$$\int f \mathrm{d}m := \mathop{+}_{c \in f(X)} c \; m(f^{-1}(c)).$$

Para todo conjunto mensurável $M \in \mathcal{M}$, a *integral* de f sobre M em $\boldsymbol{X}$ é

$$\int_M f \mathrm{d}m := \int \mathbf{1}_M f \mathrm{d}m.$$

Quando não for necessário explicitar a medida m, escreveremos

$$\int f.$$

Quando for necessário explicitar a variável da função f, escreveremos

$$\int f(x) \mathrm{d}m(x).$$

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

$$\mathop{+}_{i\in I} f_i.$$

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 8.3. *Sejam $\boldsymbol{X} = (X, \mathcal{M}, m)$ um espaço de medida.*

1. *Para todo $M \in \mathcal{M}$, $\int \mathbf{1}_M = m(M)$.*
2. *Para todo $M \in \mathcal{M}$ e toda função simples mensurável $f\colon X \longrightarrow \mathbb{R}$,*

$$\int_M f = \mathop{+}_{c\in f(X)} c\ m(M \cap f^{-1}(c)).$$

3. *Se $f \in \mathscr{M}(\boldsymbol{X}, [0,\infty])$ 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*

$$\int f = \mathop{+}_{P\in\mathcal{P}} c_P\ m(P).$$

Demonstração. 1. Como $\mathbf{1}_M(X) = \{0,1\}$, $\mathbf{1}_M^{-1}(1) = M$ e $\mathbf{1}_M^{-1}(0) = M^{\complement}$,

$$\int \mathbf{1}_M = \mathop{+}_{c\in\mathbf{1}_M(X)} c\ m(\mathbf{1}_M^{-1}(c)) = 1m(M) + 0m(M^{\complement}) = m(M).$$

■

Proposição 8.4. *Sejam $(X, \mathcal{M}, m)$ um espaço de medida, $M \in \mathcal{M}$ um conjunto mensurável $f\colon X \longrightarrow \mathbb{R}$ e $f'\colon X \longrightarrow \mathbb{R}$ 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

$$\int_M 0f = \mathop{+}_{c\in(0f)(X)} cm(M \cap (0f)^{-1}(c)) = 0m(M \cap X) = 0 = 0\int_M f.$$

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

$$\begin{aligned}\int_M af &= \mathop{+}_{c\in(af)(X)} cm(M \cap (af)^{-1}(c))\\ &= \mathop{+}_{c\in f(X)} acm(M \cap (af)^{-1}(ac))\\ &= \mathop{+}_{c\in f(X)} acm(M \cap f^{-1}(c))\\ &= a \mathop{+}_{c\in f(X)} cm(M \cap f^{-1}(c))\\ &= a\int_M f.\end{aligned}$$

2. Notemos que

$$\begin{aligned}(f + f')(X) &= \{f(x) + f'(x) \mid x \in X\}\\ &= \left\{c + c' \;\middle|\; (c, c') \in f(X) \times f'(X), f^{-1}(c) \cap (f')^{-1}(c') \neq \emptyset\right\}\\ &\subseteq f(X) + f'(X).\end{aligned}$$

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

$$f + f' = \mathop{+}_{c\in f(X)} \mathop{+}_{c'\in f(X)} (c + c')\mathbf{1}_{f^{-1}(c)\cap f^{-1}(c')},$$

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

$$\begin{aligned}
\int f+f' &= \mathop{+}_{c\in f(X)} \mathop{+}_{c'\in f(X)} (c+c')m\left(f^{-1}(c)\cap f^{-1}(c')\right)\\
&= \mathop{+}_{c\in f(X)} \mathop{+}_{c'\in f(X)} c\ m\left(f^{-1}(c)\cap f^{-1}(c')\right) + c'\ m\left(f^{-1}(c)\cap f^{-1}(c')\right)\\
&= \mathop{+}_{c\in f(X)} c\left(\mathop{+}_{c'\in f(X)} m\left(f^{-1}(c)\cap f^{-1}(c')\right)\right)\\
&\qquad\qquad + \mathop{+}_{c'\in f(X)} c'\left(\mathop{+}_{c\in f(X)} m\left(f^{-1}(c)\cap f^{-1}(c')\right)\right)\\
&= \mathop{+}_{c\in f(X)} c\ m(f^{-1}(c)) + \mathop{+}_{c'\in f'(X)} c'\ m((f')^{-1}(c'))\\
&= \int f + \int f'.
\end{aligned}$$

■

Demonstração. Sejam $f = +_{i=1}^{n} c_i\mathbf{1}_{P_i}$, $g = +_{j=1}^{m} d_j\mathbf{1}_{Q_j}$, $I := \{1,\cdots,n\}$ e $J := \{1,\cdots,m\}$.

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 $cf(X) = \{cc_1,\cdots,cc_n\}$ e as constantes $cc_1,\cdots,cc_n$ são todas distintas. Definindo, para todo $i\in I$, $R_i := \{x\in X \mid cf(x) = cc_i\}$, os conjuntos $R_1,\cdots,R_n$ 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

$$\int_M cf = \mathop{+}_{i=1}^{n} cc_i m(R_i\cap M) = c\mathop{+}_{i=1}^{n} c_i m(P_i\cap M) = c\int_M f.$$

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 $e_1,\cdots,e_l\in\mathbb{R}$ as constantes distintas tais que $(f+$

$g)(X) = \{e_1, \cdots, e_l\}$, $K := \{1, \cdots, l\}$ 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

$$f + g = \mathop{\mathbin{+}}_{k=1}^{l} e_k \mathbf{1}_{R_k}.$$

Por outro lado, temos

$$\begin{aligned}(f+g)(x) &= f(x) + g(x) \\ &= \mathop{\mathbin{+}}_{i=1}^{n} c_i \mathbf{1}_{P_i}(x) + \mathop{\mathbin{+}}_{j=1}^{m} d_j \mathbf{1}_{Q_j}(x) \\ &= \end{aligned}$$

$$f + g = \mathop{\mathbin{+}}_{i=1}^{n} \mathop{\mathbin{+}}_{j=1}^{m} (c_i + d_j) \mathbf{1}_{P_i \cap Q_j}.$$

Isso significa que os conjuntos

■

8.2 Integral de Funções Mensuráveis Positivas

8.3 Integral de Funções Mensuráveis

8.4 Teoremas de Convergências

8.5 Mudança de Variáveis na Integração

Lembremos que, se $T\colon (X, \mathcal{M}) \longrightarrow (X', \mathcal{M}')$ é uma função mensurável e m é uma medida sobre $(X, \mathcal{M})$, então a medida $T_\star m$ empurrada de m por T é a medida dada por

$$T_\star m = m \circ T^{-1}.$$

Ainda, se $f\colon X' \longrightarrow X''$ é uma função, a função puxada de f por T é a função $T^\star f\colon X \longrightarrow X''$ dada por

$$T^\star f = f \circ T.$$

Proposição 8.5. *Sejam $\boldsymbol{X} = (X, \mathcal{M}, m)$ e $\boldsymbol{X}' = (X', \mathcal{M}', m')$ espaços de medida e $T\colon X \longrightarrow X'$ uma função mensurável tal que $m' = T_\star m$. Para toda $f \in \mathscr{M}(X', \mathbb{R})$, $T^\star f \in \mathscr{I}^1(X, \mathbb{R})$ se, e somente se, $f \in \mathscr{I}^1(X', \mathbb{R})$ e, nesse caso,*

$$\int T^\star f \mathrm{d}m = \int f \mathrm{d}T_\star m.$$

Demonstração. A demonstração é evidente para funções simples, e pelo teorema da convergência monótona segue para qualquer função. Para qualquer conjunto mensurável $M \in \mathcal{M}'$, notemos que

$$T^\star \mathbf{1}_M = \mathbf{1}_M \circ T = \mathbf{1}_{T^{-1}(M)},$$

logo

$$\int T^\star \mathbf{1}_M \mathrm{d}m = \int \mathbf{1}_{T^{-1}(M)} \mathrm{d}m = m(T^{-1}(M)) = T_\star m(M) = \int \mathbf{1}_M \mathrm{d}T_\star m.$$

Da linearidade de $T^\star$, segue que para qualquer função simples $f\colon X' \longrightarrow \mathbb{R}$,

$$T^\star f = T^\star \left(\mathop{+}_{c \in f(X')} c\mathbf{1}_{f^{-1}(c)} \right) = \mathop{+}_{c \in f(X')} cT^\star \mathbf{1}_{f^{-1}(c)} = \mathop{+}_{c \in (T^\star f)(X)} c\mathbf{1}_{(T^\star f)^{-1}(c)}$$

é uma função simples. Da linearidade da integral segue então que

$$\begin{aligned}
\int T^\star f \mathrm{d}m &= \int \mathop{+}_{c \in (T^\star f)(X)} c\mathbf{1}_{(T^\star f)^{-1}(c)} \mathrm{d}m \\
&= \int \mathop{+}_{c \in f(X')} cT^\star \mathbf{1}_{f^{-1}(c)} \mathrm{d}m \\
&= \mathop{+}_{c \in f(X')} c \int T^\star \mathbf{1}_{f^{-1}(c)} \mathrm{d}m \\
&= \mathop{+}_{c \in f(X')} c \int \mathbf{1}_{f^{-1}(c)} \mathrm{d}T_\star m \\
&= \int \mathop{+}_{c \in f(X')} c\mathbf{1}_{f^{-1}(c)} \mathrm{d}T_\star m \\
&= \int f \mathrm{d}T_\star m.
\end{aligned}$$

Para uma função mensurável positiva $f\colon X' \longrightarrow [0, \infty[$, existe uma sequência crescente $(f_n)_{n \in \mathbb{N}}$ de funções mensuráveis simples positivas que converge para f. Segue que $(T^\star f_n)_{n \in \mathbb{N}}$ é uma sequência crescente de funções mensuráveis simples positivas que converge para $T^\star f$ e, pela convergência monótona da integral,

$$\int T^\star f \mathrm{d}m = \lim_{n \to \infty} \int T^\star f_n \mathrm{d}m = \lim_{n \to \infty} \int f_n \mathrm{d}T_\star m = \int f \mathrm{d}T_\star m.$$

Agora, para qualquer função mensurável $f\colon X' \longrightarrow \mathbb{R}$, vale que $(T^\star f)^+ = T^\star f^+$ e

$(T^\star f)^- = T^\star f^-$, portanto segue que

$$\begin{aligned}\int T^\star f \mathrm{d}m &= \int (T^\star f)^+ \mathrm{d}m - \int (T^\star f)^- \mathrm{d}m \\ &= \int T^\star f^+ \mathrm{d}m - \int T^\star f^- \mathrm{d}m \\ &= \int f^+ \mathrm{d}T_\star m - \int f^- \mathrm{d}T_\star m \\ &= \int f \mathrm{d}T_\star m.\end{aligned}$$

■

8.6 Integral em Espaços Normados Completos

Queremos definir o conceito de integração de funções de espaços de medida para espaços normados completos. Isso generaliza o caso de funções reais e complexas, pois de fato tudo que se precisa para integração são linearidade, norma e completude. Para estudar funções mensuráveis de um espaço de medida para um espaço normado, consideraremos no espaço normado a álgebra de mensuráveis topológica, gerada pelos abertos da topologia da norma. Começamos pelas funções simples.

8.6.1 Funções Simples

Definição 8.3. Sejam $\boldsymbol{X}$ um espaço de medida e $\mathbb{E}$ um espaço normado real. Uma *função simples* de $\boldsymbol{X}$ para $\boldsymbol{E}$ é uma função $f\colon X \longrightarrow E$ tal que $f(X)$ é finito. A *partição por níveis* de f é o conjunto

$$\mathcal{P}_f := \{f^{-1}(c)\}_{c\in f(X)}.$$

O conjunto das funções simples mensuráveis de X para E é denotado $\mathrm{Simp}(X, E)$.

Proposição 8.6. *Sejam $\boldsymbol{X}$ um espaço de medida, $\mathbb{E}$ um espaço normado real e $f, f'\colon X \longrightarrow E$ funções simples.*

1. *Uma função simples $f\colon X \longrightarrow E$ é mensurável se, e somente se, sua partição por níveis $\mathcal{P}_f$ é mensurável;*

2. *A função f pode ser decomposta em funções indicadoras como*

$$f = \mathop{\mathbin{+}}_{v\in f(X)} \mathbf{1}_{f^{-1}(v)} v$$

e, para toda partição $\mathcal{P} \geq \mathcal{P}_f$, definindo $\{v_P\} := f(P)$,

$$f = \mathop{\mathbin{+}}_{P\in\mathcal{P}} \mathbf{1}_P v_P;$$

3. *Para todas funções simples $f, f' \colon X \longrightarrow E$, a partição por níveis de $f + f'$ é mais grossa que o refinamento das partições por níveis de f e f':*

$$\mathcal{P}_{f+f'} \leq \mathcal{P}_f \vee \mathcal{P}_{f'}.$$

Demonstração. 1. Suponha que $f \colon X \longrightarrow E$ é uma função simples mensurável. Seja $v \in f(X)$. Como $\{v\}$ é fechado e f é mensurável, $f^{-1}(\{v\}) = f^{-1}(v)$ é mensurável.

Reciprocamente, seja $M \subseteq E$ um conjunto mensurável. Como $f(X)$ é finito, segue que $M \cap f(X)$ é finito. Seja $v_0, \cdots, v_{n-1} \in E$ tais que $M \cap f(X) = \bigcup_{i \in [n]} \{v_i\}$. Então

$$f^{-1}(M) = f^{-1}(M \cap f(X)) = f^{-1}\left(\bigcup_{i \in [n]} \{v_i\}\right) = \bigcup_{i \in [n]} f^{-1}(\{v_0\}).$$

Como $f^{-1}(\{v_i\})$ são mensuráveis, pois são elementos da partição por níveis de f, segue que $f^{-1}(M)$ é mensurável, pois é união de mensuráveis, o que mostra que f é mensurável.

2. Seja $x \in X$. Como $\mathcal{P}_f$ é partição de X, existe $v \in f(X)$ tal que $x \in f^{-1}(v)$. Nesse caso, $f(x) = v$, $\mathbf{1}_{f^{-1}(v)}(x) = 1$ e, para todo $v' \in f(X) \smallsetminus \{v\}$, $\mathbf{1}_{f^{-1}(v')}(x) = 0$, logo

$$f(x) = 1v = \mathbf{1}_{f^{-1}(v)}(x)v = \mathop{\bigplus}_{v \in f(X)} \mathbf{1}_{f^{-1}(v)}(x)v,$$

portanto $f = \bigplus_{v \in f(X)} \mathbf{1}_{f^{-1}(v)} v$. A outra igualdade é semelhante.

3. Exercício.

■

Proposição 8.7. *Sejam $\boldsymbol{X}$ um espaço de medida e $\mathbb{E}$ um espaço normado real. O conjunto* $\mathrm{Simp}(\boldsymbol{X}, \boldsymbol{E})$ *de funções simples mensuráveis é um subespaço linear real de $\mathscr{M}(\boldsymbol{X}, \boldsymbol{E})$. Se $f \colon X \longrightarrow E$ é uma função simples mensurável, então $\|f\| : X \longrightarrow \mathbb{R}$ também é.*

Demonstração. Para ver que $\mathrm{Simp}(\boldsymbol{X}, \boldsymbol{E})$ é um espaço linear, basta mostrar que ele subespaço linear de $\mathscr{M}(\boldsymbol{X}, \boldsymbol{E})$. Sejam $c \in \mathbb{R}$ e $f, f' \in \mathrm{Simp}(X, E)$. Como $f(X)$ e $f'(X)$ são finitos, e $(cf + f')(X) \subseteq cf(X) + f'(X)$, claramente $cf + f'$ é simples. Ainda, como f, f' são mensuráveis, segue que $cf + f'$ é mensurável, o que mostra que $cf + f' \in \mathrm{Simp}(X, E)$.

Para mostrar que $\|f\|$ é simples, basta notar que, como $f(X)$ é finito, claramente $\|f\|(X)$ é finito, e, como $\|\cdot\|$ é mensurável (pois é contínua), a composição $\|f\| = \|\cdot\| \circ f$ é mensurável. ■

Proposição 8.8. *Sejam $\boldsymbol{X}$ um espaço de medida e $\mathbb{E}$ um espaço normado real de dimensão finita. Uma função $f\colon X \longrightarrow E$ é mensurável se, e somente se, existe uma sequência $(f_n)_{n\in\mathbb{N}}$ de funções simples de $\operatorname{Simp}(X,E)$ que convergem pontualmente para f.*

Demonstração. Como $\mathbb{E}$ tem dimensão finita, basta mostrar a proposição para $\mathbb{R}$. Suponhamos que f é mensurável. Para cada $n \in \mathbb{N}^*$, particionamos o intervalo $[-n, n[$ em intervalos de tamanho $\frac{1}{n}$ e definimos, para cada $k \in [-n^2-1, n^2+1[\cap \mathbb{Z}$, os conjuntos

$$X_k := \begin{cases} f^{-1}\left(]\infty, -n[\right), & k = -n^2-1 \\ f^{-1}\left(\left[\dfrac{k}{n}, \dfrac{k+1}{n}\right[\right), & k \in [-n^2, n^2[\cap \mathbb{Z} \\ f^{-1}\left([n, \infty[\right), & k = n^2. \end{cases}$$

Os conjuntos $X_k \subseteq X$ são mensuráveis e particionam X. Definimos $f_0 := 0$ e, para cada $n \in \mathbb{N}^*$, as funções $f_n\colon X \longrightarrow \mathbb{R}$ por

$$f_n := \mathbf{1}_{X_{-n^2-1}}(-n) + \mathop{\bigplus}_{k=-n^2}^{n^2} \mathbf{1}_{X_k}\frac{k}{n}.$$

As funções f_n são funções simples e mensuráveis, e convergem pontualmente para f, o que termina a demonstração.

A recíproca é consequência de 7.16. ■

8.7 Desintegração de Medida

Seja $\boldsymbol{X} = (X, \mathcal{M}, m)$ um espaço de medida. Nessa seção consideraremos partições mensuráveis e partições por medida (contavelmente gerada). Dada uma partição $\mathcal{P}$ de $\boldsymbol{X}$, podemos induzir em $\mathcal{P}$ uma σ-álgebra e uma medida. Para isso, definimos a projeção

$$\begin{aligned} \mathrm{p}\colon X &\longrightarrow \mathcal{P} \\ x &\longmapsto [x] = P_x. \end{aligned}$$

Como $\mathcal{P}$ é partição por medida (contavelmente gerada), a projeção p não está definida para todo $x \in X$, as para quase todo, portanto é uma quase função. Agora, a σ-álgebra sobre $\mathcal{P}$ é $\mathrm{p}_\star\mathcal{M}$, a σ-álgebra empurrada por p, e a medida sobre $(\mathcal{P}, \mathrm{p}_\star\mathcal{M})$ é $\mathrm{p}_\star m$, a medida empurrada por p. A tripla $(\mathcal{P}, \mathrm{p}_\star\mathcal{M}, \mathrm{p}_\star m)$ é um espaço de medida. Usaremos esse espaço de medida para falar sobre desintegração de medidas.

Definição 8.4. Sejam $\boldsymbol{X} = (X, \mathcal{M}, m)$ um espaço de medida (finita) e $\mathcal{P}$ uma partição por medida (contavelmente gerada) de $\boldsymbol{X}$. Uma *desintegração* de μ relativa a $\mathcal{P}$ é uma família $(m_P)_{P\in\mathcal{P}}$ tal que

1. Para quase todo $P \in \mathcal{P}$,
$$m_P(P) = 1;$$

2. Para todo $M \in \mathcal{M}$, a função
$$\begin{aligned} m_{(\cdot)}(M)\colon \mathcal{P} &\longrightarrow \mathbb{R} \\ P &\longmapsto m_P(M) \end{aligned}$$
é mensurável;

3. Para todo $M \in \mathcal{M}$,
$$m(M) = \int m_P(M)\mathrm{dp}_\star m(P).$$
$$m(M) = \int_{P\in\mathcal{P}} m_P(M)\mathrm{dp}_\star m.$$

Proposição 8.9 (Unicidade de Desintegração)**.** *Sejam $\boldsymbol{X} = (X, \mathcal{M}, m)$ um espaço de medida (finita) e $\mathcal{P}$ uma partição por medida (contavelmente gerada) de $\boldsymbol{X}$. Se $(m_P)_{P\in\mathcal{P}}$ e $(m'_P)_{P\in\mathcal{P}}$ são desintegrações de m relativas a $\mathcal{P}$, então, para quase todo $P \in \mathcal{P}$, $m_P = m'_P$.*

Capítulo 9

Diferenciação

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 $\{\boldsymbol{e}_0, \ldots, \boldsymbol{e}_{d-1}\}$. Um vetor $x \in \mathbb{R}^d$ será também representado por $x = (x_0, \ldots, x_{d-1})$ e uma função $f : \mathbb{R}^{d_0} \longrightarrow \mathbb{R}^{d_1}$ será também representada por $f = (f_0, \ldots, f_{d_1-1})$, 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

$$f : \mathbb{R}^d \longrightarrow \mathbb{R}^c,$$

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.

9.1 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 vetor variação vai a zero. Mais à frente, as k-ésimas diferenciais da função f serão definidas analogamente, considerando nesses casos funções multilineares.

Definição 9.1. Sejam $p \in \mathbb{R}^d$ e $f : \mathbb{R}^d \longrightarrow \mathbb{R}^c$ uma função. Uma *diferencial* de f em p é uma transformação linear $T : \mathbb{R}^d \longrightarrow \mathbb{R}^c$ que satisfaz

$$\lim_{v \to 0} \frac{f(p+v) - f(p) - T \cdot v}{\|v\|} = 0.$$

Uma função *diferenciável* em p é uma função que tem diferencial em p.

É válido notar que são equivalentes a essa condição

$$\lim_{x \to p} \frac{f(x) - f(p) - T \cdot (x-p)}{\|x-p\|} = 0.$$

e

$$\lim_{v \to 0} \frac{\|f(p+v) - f(p) - T \cdot v\|}{\|v\|} = 0.$$

Proposição 9.1 (Diferenciabilidade implica continuidade)**.** *Sejam $p \in \mathbb{R}^d$ e $f : \mathbb{R}^d \longrightarrow \mathbb{R}^c$ uma função. Se f é diferenciável em p, então f é contínua em p.*

Demonstração. Se f é diferenciável em p, então, como $\lim_{v \to 0} T \cdot v = 0$,

$$\begin{aligned}
\lim_{v \to 0}(f(p+v) - f(p)) &= \lim_{v \to 0}(f(p+v) - f(p) - T \cdot v) \\
&= \lim_{v \to 0} \|v\| \, \frac{f(p+v) - f(p) - T \cdot v}{\|v\|} \\
&= 0,
\end{aligned}$$

logo f é contínua em p. ■

Proposição 9.2 (Unicidade da diferencial)**.** *Sejam $p \in \mathbb{R}^d$ e $f : \mathbb{R}^d \longrightarrow \mathbb{R}^c$ uma função diferenciável em p. Então existe uma única diferencial de f em p.*

Demonstração. Sejam $T, S : \mathbb{R}^d \longrightarrow \mathbb{R}^c$ diferenciais de f em p. Nesse caso, temos que

$$\begin{aligned}
&\lim_{v \to 0} \frac{T \cdot v - S \cdot v}{\|v\|} = \\
&= \lim_{v \to 0} \frac{T \cdot v - (f(p+v) - f(p)) + (f(p+v) - f(p)) - S \cdot v}{\|v\|} \\
&= -\lim_{v \to 0} \frac{f(p+v) - f(p) - T \cdot v}{\|v\|} + \lim_{v \to 0} \frac{f(p+v) - f(p) - S \cdot v}{\|v\|} \\
&= 0.
\end{aligned}$$

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 $t \to 0$, $tv \to 0$. 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

$$\begin{aligned} 0 &= \lim_{tv \to 0} \frac{\|T \cdot (tv) - S \cdot (tv)\|}{\|tv\|} \\ &= \lim_{t \to 0} \frac{|t| \, \|T \cdot v - S \cdot v\|}{|t| \, \|v\|} \\ &= \frac{\|T \cdot v - S \cdot v\|}{\|v\|}, \end{aligned}$$

o que implica $T \cdot v = S \cdot v$, pois $\|v\| \neq 0$. Portanto $T = S$. ■

Notação. Sejam $p \in \mathbb{R}^d$ e $f : \mathbb{R}^d \longrightarrow \mathbb{R}^c$ uma função diferenciável em p. A diferencial de f em p é denotada $\mathrm{D}f(p) : \mathbb{R}^d \longrightarrow \mathbb{R}^c$ e satisfaz

$$\lim_{v \to 0} \frac{f(p+v) - f(p) - \mathrm{D}f(p) \cdot v}{\|v\|} = 0.$$

Podemos ver que, se f é diferenciável, então $\mathrm{D}f : \mathbb{R}^d \longrightarrow L(\mathbb{R}^d, \mathbb{R}^c)$ é uma função que leva $p \in \mathbb{R}^d$ na diferencial $\mathrm{D}f(p)$ de f em p.

Proposição 9.3 (Regra da cadeia)**.** *Sejam $f : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ diferenciável em $p \in \mathbb{R}^n$ e $g : \mathbb{R}^m \longrightarrow \mathbb{R}^l$ diferenciável em $f(p)$. Então $g \circ f : \mathbb{R}^n \longrightarrow \mathbb{R}^l$ é diferenciável em p e*

$$\mathrm{D}(g \circ f)(p) = \mathrm{D}g(f(p)) \circ \mathrm{D}f(p).$$

Demonstração. Definamos

$$r_1(v) := f(p+v) - f(p) - \mathrm{D}f(p) \cdot v$$

e

$$r_1(v) := g(f(p) + v) - g(f(p)) - \mathrm{D}g(f(p)) \cdot v,$$

de modo que da diferenciabilidade de f em p e de g em $f(p)$ segue

$$\lim_{v \to 0} \frac{r_1(v)}{\|v\|} = \lim_{v \to 0} \frac{r_1(v)}{\|v\|} = 0.$$

Calculando $(g \circ f)(p+v)$, obtemos

$$\begin{aligned} (g \circ f)(p+v) &= g(f(p+v)) = g(f(p) + \mathrm{D}f(p) \cdot v + r_1(v)) \\ &= g(f(p)) + \mathrm{D}g(f(p)) \cdot (\mathrm{D}f(p) \cdot v + r_1(v)) \\ &\quad + r_1(\mathrm{D}f(p) \cdot v + r_1(v)) \\ &= (g \circ f)(p) + \Big(\mathrm{D}g(f(p)) \circ \mathrm{D}f(p)\Big) \cdot v + \mathrm{D}g(f(p)) \cdot r_1(v) \\ &\quad + r_1(\mathrm{D}f(p) \cdot v + r_1(v)). \end{aligned}$$

Portanto

$$\begin{aligned}(g\circ f)(p+v)-(g\circ f)(p)-\Big(\mathrm{D}g(f(p))\circ \mathrm{D}f(p)\Big)\cdot v\\ =\mathrm{D}g(f(p))\cdot r_1(v)+r_1(\mathrm{D}f(p)\cdot v+r_1(v)).\end{aligned}$$

Como $\mathrm{D}g(f(p))\circ \mathrm{D}f(p)$ 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

$$\lim_{v\to 0}\frac{\mathrm{D}g(f(p))\cdot r_1(v)}{\|v\|}=\lim_{v\to 0}\mathrm{D}g(f(p))\cdot\frac{r_1(v)}{\|v\|}=0$$

e, como $\lim_{v\to 0}\mathrm{D}f(p)\cdot v+r_1(v)=0$ e $\mathrm{D}f(p)\cdot\frac{v}{\|v\|}$ é limitado,

$$\begin{aligned}&\lim_{v\to 0}\frac{r_1(\mathrm{D}f(p)\cdot v+r_1(v))}{\|v\|}\\ &\quad=\lim_{v\to 0}\frac{r_1(\mathrm{D}f(p)\cdot v+r_1(v))}{\|\mathrm{D}f(p)\cdot v+r_1(v)\|}\frac{\|\mathrm{D}f(p)\cdot v+r_1(v)\|}{\|v\|}\\ &\quad=\lim_{v\to 0}\frac{r_1(\mathrm{D}f(p)\cdot v+r_1(v))}{\|\mathrm{D}f(p)\cdot v+r_1(v)\|}\left\|\mathrm{D}f(p)\cdot\frac{v}{\|v\|}+\frac{r_1(v)}{\|v\|}\right\|=0.\end{aligned}$$

Logo

$$\lim_{v\to 0}\frac{(g\circ f)(p+v)-(g\circ f)(p)-\Big(\mathrm{D}g(f(p))\circ \mathrm{D}f(p)\Big)\cdot v}{\|v\|}=0,$$

e concluímos que $\mathrm{D}g(f(p))\circ \mathrm{D}f(p)$ é a diferencial de $g\circ f$ em p. ■

Proposição 9.4 (Regra da cadeia iterada)**.** *Sejam $f:\mathbb{R}^n\longrightarrow\mathbb{R}^m$ 2-diferenciável em $p\in\mathbb{R}^n$ e $g:\mathbb{R}^m\longrightarrow\mathbb{R}^l$ diferenciável em $f(p)$. Então $g\circ f:\mathbb{R}^n\longrightarrow\mathbb{R}^l$ é diferenciável em p e*

$$\mathrm{D}^2(g\circ f)(p,p)=\mathrm{D}^2g(f(p),f(p))\circ \mathrm{D}f(p)+\mathrm{D}g(f(p))\circ \mathrm{D}^2f(p)$$

Proposição 9.5. *Sejam $f,g:\mathbb{R}^n\longrightarrow\mathbb{R}^m$ 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* $g(a)\neq 0$,
$$D\left(\frac{f}{g}\right)(p)=\frac{g(p)\cdot Df(a)-Dg(a)\cdot f(p)}{g(p)^2}$$

9.1.1 Diferenciais de Ordem Superior

Generalizamos, agora, a ideia de uma diferencial para uma r-diferencial. Para isso, denotaremos um vetor $(v, \ldots, v)$ com k entradas por $(v)^{\otimes k}$.

Definição 9.2. Seja $p \in \mathbb{R}^d$. Uma função *r-diferenciável* em p é uma função $f\colon \mathbb{R}^d \longrightarrow \mathbb{R}^c$ tal que, para todo $k \in [r+1]$, existe uma função k-linear simétrica

$$L_k\colon \mathbb{R}^d \times \cdots \times \mathbb{R}^d \longrightarrow \mathbb{R}^c$$

satisfazendo

$$\lim_{v\to 0} \frac{f(p+v) - f(p) - \displaystyle\mathop{+}_{k=1}^{r} \frac{1}{k!} L_k \cdot (v)^{\otimes k}}{\|v\|^r} = 0.$$

Uma função L_k como acima é uma *diferencial de ordem k* (ou *k-ésima diferencial*) da f em p.

Proposição 9.6. *Sejam $p \in \mathbb{R}^d$ e $f\colon \mathbb{R}^d \longrightarrow \mathbb{R}^c$ uma função k-diferenciável em p. Então f é $(k-1)$-diferenciável em p.*

Demonstração. Primeiro notemos que

$$\lim_{v\to 0} \frac{L_r \cdot (v)^{\otimes r}}{\|v\|^{r-1}} \leq \lim_{v\to 0} \frac{\|L_r\| \, \|v\|^r}{\|v\|^{r-1}} = \lim_{v\to 0} \|L_r\| \, \|v\| = 0.$$

Portanto segue que

$$\begin{aligned}
&\lim_{v\to 0} \frac{f(p+v) - f(p) - \displaystyle\mathop{+}_{k=1}^{r-1} \frac{1}{k!} L_k \cdot (v)^{\otimes k}}{\|v\|^{r-1}} \\
&= \lim_{v\to 0} \frac{f(p+v) - f(p) - \displaystyle\mathop{+}_{k=1}^{r-1} \frac{1}{k!} L_k \cdot (v)^{\otimes k} - \frac{1}{r!} L_r \cdot (v)^{\otimes r}}{\|v\|^{r-1}} \\
&= \lim_{v\to 0} \|v\| \, \frac{f(p+v) - f(p) - \displaystyle\mathop{+}_{k=1}^{r} \frac{1}{k!} L_k \cdot (v)^{\otimes k}}{\|v\|^{r}} \\
&= 0.
\end{aligned}$$

■

Proposição 9.7. *Sejam $p \in \mathbb{R}^d$ e $f\colon \mathbb{R}^d \longrightarrow \mathbb{R}^c$ 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 $f\colon \mathbb{R}^d \longrightarrow \mathbb{R}^c$ 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

$$L_k\colon \mathbb{R}^d \times \cdots \times \mathbb{R}^d \longrightarrow \mathbb{R}^c$$

satisfazendo

$$\lim_{v\to 0} \frac{f(p+v) - f(p) - \displaystyle\mathop{\mathbin{+}}_{k=1}^{r-1} \frac{1}{k!} L_k \cdot (v)^{\otimes k}}{\|v\|^r} = 0.$$

Agora, sejam L, S diferenciais de ordem r de f em p e definamos

$$A(v) := f(p+v) - f(p) - \mathop{\mathbin{+}}_{k=1}^{r-1} \frac{1}{k!} L_k \cdot (v)^{\otimes k}.$$

Segue que

$$\begin{aligned}
&\lim_{v\to 0} \frac{L\cdot(v)^{\otimes r} - S\cdot(v)^{\otimes r}}{\|v\|^r} \\
&= r! \lim_{v\to 0} \frac{\frac{1}{r!} L\cdot(v)^{\otimes r} - A(v) + A(v) - \frac{1}{r!} S\cdot(v)^{\otimes r}}{\|v\|^r} \\
&= -r! \lim_{v\to 0} \frac{\frac{1}{r!} L\cdot(v)^{\otimes r} - A(v)}{\|v\|^r} + r! \lim_{v\to 0} \frac{A(v) - \frac{1}{r!} S\cdot(v)^{\otimes r}}{\|v\|^r} \\
&= 0.
\end{aligned}$$

Como L e S são transformações r-lineares, sabemos que $L\cdot(0)^{\otimes r} = S\cdot(0)^{\otimes r} = 0$. Para $v \in (\mathbb{R}^d)^r \smallsetminus \{(0)^{\otimes r}\}$, temos que, quando $t \to 0$, $(tv)^{\otimes r} \to (0)^{\otimes r}$. 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

$$\begin{aligned}
0 &= \lim_{tv\to 0} \frac{L\cdot(tv)^{\otimes r} - S\cdot(tv)^{\otimes r}}{\|tv\|^r} \\
&= \lim_{t\to 0} \frac{(t)^r \Big(L\cdot(v)^{\otimes r} - S\cdot(v)^{\otimes r}\Big)}{|t|^r \, \|v\|^r} \\
&= \pm \frac{\Big(L\cdot(v)^{\otimes r} - S\cdot(v)^{\otimes r}\Big)}{\|v\|^r}
\end{aligned}$$

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 $f\colon \mathbb{R}^d \longrightarrow \mathbb{R}^c$ uma função r-diferenciável em p. A diferencial de ordem r de f em p é denotada $\mathrm{D}^r f(p)\colon \mathbb{R}^d \times \cdots \times \mathbb{R}^d \longrightarrow \mathbb{R}^c$ e, se definimos $D^0 f(p) := f(p)$, as diferenciais satisfazem

$$\lim_{v\to 0} \frac{f(p+v) - \displaystyle\mathop{+}_{k=0}^{r} \frac{1}{k!}\mathrm{D}^k f(p)\cdot (v)^{\otimes k}}{\|v\|^r} = 0.$$

O polinômio

$$P(v) = \mathop{+}_{k=0}^{r} \frac{1}{k!}\mathrm{D}^k f(p)\cdot (v)^{\otimes k}$$

é o *polinômio diferencial de ordem* r de f em p.

9.2 Derivadas Direcionais e a Geometria da Diferenciabilidade

A partir dessa seção, consideraremos funções $f : A \longrightarrow \mathbb{R}^c$, 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 parra funções $f : A \longrightarrow \mathbb{R}^c$ pois essa função pode ser definida em $\mathbb{R}^d$ todo escolhendo qualquer valor para f em $A^{\complement}$. 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 9.3. Sejam $A \subseteq \mathbb{R}^n$ um aberto, $p \in A$, $v \in \mathbb{R}^d$ tal que $p + v \in A$ e $f : A \longrightarrow \mathbb{R}^c$. A *derivada direcional* de f em p na direção de v é

$$\frac{\partial f}{\partial v}(p) := \lim_{t\to 0} \frac{f(p+tv) - f(p)}{t}.$$

Como A é aberto, existe ε tal que $p + tv \in A$ para todo $t \in \,]-\varepsilon, \varepsilon[$. Tomemos então a curva

$$\begin{aligned} \gamma\colon]-\varepsilon, \varepsilon[&\longrightarrow A \\ t &\longmapsto p + tv, \end{aligned}$$

de modo que temos $\gamma(0) = p$ e $\gamma'(0) = v$. Então, pela regra da cadeia,

$$\frac{\partial f}{\partial v}(p) = \mathrm{D}(f\circ\gamma)(0) = \mathrm{D}f(\gamma(0))\cdot\gamma'(0) = \mathrm{D}f(p)\cdot v.$$

Disso concluímos que a derivada direcional de f em p na direção de v é a imagem de v sob a transformação linear $\mathrm{D}f(p)$. Portanto definindo as derivadas direcionais $\partial_i f(x) := \mathrm{D}f(x) \cdot e_i$ temos que

$$\mathrm{D}f(x) \cdot v = \mathop{\mathop{+}}_{i=0}^{d-1} v^i \partial_i f(x).$$

9.3 Os Teoremas Fundamentais

9.3.1 Teorema da Função Inversa

Proposição 9.8. *Sejam $p \in \mathbb{R}^d$ e $f\colon \mathbb{R}^d \longrightarrow \mathbb{R}^d$ uma função $\mathscr{C}^r$-diferenciável ($r \geq 1$) numa vizinhança aberta $A \subseteq \mathbb{R}^d$ de p. Se $\mathrm{D}f(p)\colon \mathbb{R}^d \longrightarrow \mathbb{R}^d$ é invertível, então existe uma vizinhança aberta $V \subseteq \mathbb{R}^d$ de p tal que $f\colon V \longrightarrow f(V)$ é invertível, $f^{-1}\colon f(V) \longrightarrow V$ é $\mathscr{C}^r$-diferenciável e*

$$\mathrm{D}(f^{-1})(f(p)) = (\mathrm{D}f(p))^{-1}.$$

9.3.2 Teorema da Função Implícita

Proposição 9.9. *Sejam $p = (x_0, y_0) \in \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ e $f\colon \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \longrightarrow \mathbb{R}^{d_1}$ uma função $\mathscr{C}^r$-diferenciável ($r \geq 1$) numa vizinhança aberta $A \subseteq \mathbb{R}^{d_0+d_1}$ de p tal que $f(p) = 0$. Se $\mathrm{D}f(p)\colon \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \longrightarrow \mathbb{R}^{d_1}$ 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 $\mathscr{C}^r$-diferenciável $g\colon V_0 \subseteq \mathbb{R}^{d_0} \longrightarrow V_1 \subseteq \mathbb{R}^{d_1}$ 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: $\mathrm{D}f(p)\colon \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \longrightarrow \mathbb{R}^{d_1}$ é sobrejetiva se, e somente se,

$$\begin{aligned} \mathrm{D}f(p) \circ \iota_1 \colon \mathbb{R}^{d_1} &\longrightarrow \mathbb{R}^{d_1} \\ y &\longmapsto \mathrm{D}(f)(p) \cdot (0, y) \end{aligned}$$

é invertível (em que $\iota_1\colon \mathbb{R}^{d_1} \longrightarrow \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$). Note que $\mathrm{D}_1 f(p)$ também pode ser vista como essa função.

9.3.3 Forma Local da Imersão

Proposição 9.10. *Sejam $p \in \mathbb{R}^{d_0}$ e $f\colon \mathbb{R}^{d_0} \longrightarrow \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ uma função $\mathscr{C}^r$-diferenciável ($r \geq 1$) numa vizinhança aberta $A \subseteq \mathbb{R}^{d_0}$ de p. Se $\mathrm{D}f(p)\colon \mathbb{R}^{d_0} \longrightarrow$*

$\mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ 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 $\mathscr{C}^r$-difeomorfismo $g\colon V \longrightarrow V_0 \times V_1$ tal que, para todo $x \in V_0$,

$$g \circ f(x) = (x, 0).$$

(ou seja, $g \circ f = \iota_0\colon V_0 \subseteq \mathbb{R}^{d_0} \longrightarrow \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$).

Observação: A diferencial $\mathrm{D}f(p)\colon \mathbb{R}^{d_0} \longrightarrow \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ é injetiva se, e somente se,

$$\begin{aligned} \mathrm{D}f(p) \circ \pi_0\colon \mathbb{R}^{d_0} &\longrightarrow \mathbb{R}^{d_0} \\ y &\longmapsto \Big(\mathrm{D}(f)(p) \cdot y\Big) \restriction_{\mathbb{R}^{d_0}} \end{aligned}$$

é invertível.

9.3.4 Forma Local da Submersão

Proposição 9.11. *Sejam $p = (x_0, y_0) \in \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ e $f\colon \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \longrightarrow \mathbb{R}^{d_1}$ uma função $\mathscr{C}^r$-diferenciável ($r \geq 1$) numa vizinhança aberta $A \subseteq \mathbb{R}^{d_0} \times \mathbb{R}^{d_1}$ de p. Se $\mathrm{D}f(p)\colon \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \longrightarrow \mathbb{R}^{d_1}$ 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 $\mathscr{C}^r$-difeomorfismo $g\colon V_0 \times V_1 \longrightarrow V$ tal que, para todo $(x, y) \in V_0 \times V_1$,*

$$f \circ g(x, y) = y.$$

(ou seja, $f \circ g = \pi_1\colon V_0 \times V_1 \subseteq \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \longrightarrow \mathbb{R}^{d_1}$).

Observação: A diferencial $\mathrm{D}f(p)\colon \mathbb{R}^{d_0} \times \mathbb{R}^{d_1} \longrightarrow \mathbb{R}^{d_1}$ é sobrejetiva se, e somente se,

$$\begin{aligned} \mathrm{D}f(p) \circ \iota_1\colon \mathbb{R}^{d_1} &\longrightarrow \mathbb{R}^{d_1} \\ y &\longmapsto \mathrm{D}(f)(p) \cdot (0, y) \end{aligned}$$

é invertível. Note que $\mathrm{D}_1 f(p)$ também pode ser vista como essa função.

9.3.5 Teorema do Posto

Proposição 9.12. *Seja $f\colon \mathbb{R}^d \times \mathbb{R}^{d_0} \longrightarrow \mathbb{R}^d \times \mathbb{R}^{d_1}$ uma função $\mathscr{C}^r$-diferenciável ($r \geq 1$) num aberto $A \subseteq \mathbb{R}^d \times \mathbb{R}^{d_0}$. Se $\mathrm{D}f(p)\colon \mathbb{R}^d \times \mathbb{R}^{d_0} \longrightarrow \mathbb{R}^d \times \mathbb{R}^{d_1}$ 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 $\mathscr{C}^r$-difeomorfismos $g_0\colon V_0 \longrightarrow g_0(V_0) \subseteq \mathbb{R}^d \times \mathbb{R}^{d_0}$ e $g_1\colon V_1 \longrightarrow g_1(V_1) \subseteq \mathbb{R}^d \times \mathbb{R}^{d_1}$ tais que, para todo $(x, y) \in V_0$,*

$$g_1 \circ f \circ {g_0}^{-1}(x, y)) = (x, 0).$$

(ou seja, $g_1 \circ f \circ {g_0}^{-1} = \iota \circ \pi\colon \mathbb{R}^d \times \mathbb{R}^{d_0} \longrightarrow \mathbb{R}^d \times \mathbb{R}^{d_1}$).

9.4 Cálculo em Espaços Normados de Dimensão Finita

9.4.1 Diferencial

Definição 9.4. 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 $f\colon A \longrightarrow \mathbb{E}_1$ uma função. Uma *diferencial* de f em p é uma função linear $L\colon \mathbb{E}_0 \longrightarrow \mathbb{E}_1$ que satisfaz

$$\lim_{v \longrightarrow 0} \frac{f(p+v) - f(p) - L \cdot v}{\|v\|} = 0.$$

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 9.13 (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 $f\colon A \longrightarrow \mathbb{E}_1$ uma função diferenciável em p. Então existe uma única diferencial de f em p.*

Demonstração. Sejam $L, \bar{L}\colon \mathbb{E}_0 \longrightarrow \mathbb{E}_1$ diferenciais de f em p. Nesse caso, temos que

$$\begin{aligned}
&\lim_{v \to 0} \frac{L \cdot v - \bar{L} \cdot v}{\|v\|} = \\
&\quad = \lim_{v \to 0} \frac{L \cdot v - (f(p+v) - f(p)) + (f(p+v) - f(p)) - \bar{L} \cdot v}{\|v\|} \\
&\quad = -\lim_{v \to 0} \frac{f(p+v) - f(p) - L \cdot v}{\|v\|} + \lim_{v \to 0} \frac{f(p+v) - f(p) - \bar{L} \cdot v}{\|v\|} \\
&\quad = 0.
\end{aligned}$$

Como L e $\bar{L}$ são transformações lineares, sabemos que $L \cdot 0 = \bar{L} \cdot 0 = 0$. Para todo $v \in \mathbb{E}_0 \smallsetminus \{0\}$, temos que, quando $t \to 0$, $tv \to 0$. 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

$$\begin{aligned} 0 &= \lim_{tv \to 0} \frac{\left\| L \cdot (tv) - \bar{L} \cdot (tv) \right\|}{\|tv\|} \\ &= \lim_{t \to 0} \frac{|t| \left\| L \cdot v - \bar{L} \cdot v \right\|}{|t| \, \|v\|} \\ &= \frac{\left\| L \cdot v - \bar{L} \cdot v \right\|}{\|v\|}, \end{aligned}$$

o que implica $L \cdot v = \bar{L} \cdot v$, pois $\|v\| \neq 0$. Portanto $L = \bar{L}$. ■

Notação. Sejam $\mathbb{E}_0$ e $\mathbb{E}_1$ espaços normados de dimensão finita, $A \subseteq E_0$ um aberto, $p \in A$ e $f \colon A \longrightarrow \mathbb{E}_1$ uma função diferenciável em p. A diferencial de f em p é denotada $\mathrm{D}f(p) : \mathbb{E}_0 \longrightarrow \mathbb{E}_1$ e satisfaz

$$\lim_{v \to 0} \frac{f(p+v) - f(p) - \mathrm{D}f(p) \cdot v}{\|v\|} = 0.$$

Proposição 9.14 (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 $f \colon A \longrightarrow \mathbb{E}_1$ uma função diferenciável em p. Então f é contínua em p.*

Demonstração. Se f é diferenciável em p, como vale $\lim_{v \to 0} \mathrm{D}f(p) \cdot v = 0$, segue que

$$\begin{aligned} \lim_{v \to 0} (f(p+v) - f(p)) &= \lim_{v \to 0} (f(p+v) - f(p) - \mathrm{D}f(p) \cdot v) \\ &= \lim_{v \to 0} \|v\| \, \frac{f(p+v) - f(p) - \mathrm{D}f(p) \cdot v}{\|v\|} \\ &= 0, \end{aligned}$$

o que implica que f é contínua em p. ■

Proposição 9.15 (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 $f_0 \colon A_0 \longrightarrow \mathbb{E}_1$ e $f_1 \colon A_1 \longrightarrow \mathbb{E}_2$ 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*

$$\mathrm{D}(f_1 \circ f_0)(p) = \mathrm{D}f_1(f_0(p)) \circ \mathrm{D}f_0(p).$$

Demonstração. Definamos

$$r_0(v) := f_0(p+v) - f_0(p) - \mathrm{D}f_0(p) \cdot v$$

e

$$r_1(v) := f_1(f_0(p) + v) - f_1(f_0(p)) - \mathrm{D}f_1(f_0(p)) \cdot v,$$

de modo que da diferenciabilidade de f_0 em p e de f_1 em $f_0(p)$ segue

$$\lim_{v \to 0} \frac{r_0(v)}{\|v\|} = \lim_{v \to 0} \frac{r_1(v)}{\|v\|} = 0.$$

Calculando $(f_1 \circ f_0)(p + v)$, obtemos

$$\begin{aligned}
(f_1 \circ f_0)(p + v) &= f_1(f_0(p + v)) = f_1(f_0(p) + \mathrm{D}f_0(p) \cdot v + r_0(v)) \\
&= f_1(f_0(p)) + \mathrm{D}f_1(f_0(p)) \cdot (\mathrm{D}f_0(p) \cdot v + r_0(v)) \\
&\quad + r_1(\mathrm{D}f_0(p) \cdot v + r_0(v)) \\
&= (f_1 \circ f_0)(p) + \Big(\mathrm{D}f_1(f_0(p)) \circ \mathrm{D}f_0(p)\Big) \cdot v + \mathrm{D}f_1(f_0(p)) \cdot r_0(v) \\
&\quad + r_1(\mathrm{D}f_0(p) \cdot v + r_0(v)).
\end{aligned}$$

Portanto

$$\begin{aligned}
(f_1 \circ f_0)(p + v) - (f_1 \circ f_0)(p) - \Big(\mathrm{D}f_1(f_0(p)) \circ \mathrm{D}f_0(p)\Big) \cdot v \\
= \mathrm{D}f_1(f_0(p)) \cdot r_0(v) + r_1(\mathrm{D}f_0(p) \cdot v + r_0(v)).
\end{aligned}$$

Como $\mathrm{D}f_1(f_0(p)) \circ \mathrm{D}f_0(p)$ 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

$$\lim_{v \to 0} \frac{\mathrm{D}f_1(f_0(p)) \cdot r_0(v)}{\|v\|} = \lim_{v \to 0} \mathrm{D}f_1(f_0(p)) \cdot \frac{r_0(v)}{\|v\|} = 0$$

e, como $\lim_{v \to 0} \mathrm{D}f_0(p) \cdot v + r_0(v) = 0$ e $\mathrm{D}f_0(p) \cdot \frac{v}{\|v\|}$ é limitado,

$$\begin{aligned}
&\lim_{v \to 0} \frac{r_1(\mathrm{D}f_0(p) \cdot v + r_0(v))}{\|v\|} \\
&\quad = \lim_{v \to 0} \frac{r_1(\mathrm{D}f_0(p) \cdot v + r_0(v))}{\|\mathrm{D}f_0(p) \cdot v + r_0(v)\|} \frac{\|\mathrm{D}f_0(p) \cdot v + r_0(v)\|}{\|v\|} \\
&\quad = \lim_{v \to 0} \frac{r_1(\mathrm{D}f_0(p) \cdot v + r_0(v))}{\|\mathrm{D}f_0(p) \cdot v + r_0(v)\|} \left\| \mathrm{D}f_0(p) \cdot \frac{v}{\|v\|} + \frac{r_0(v)}{\|v\|} \right\| = 0.
\end{aligned}$$

Logo

$$\lim_{v \to 0} \frac{(f_1 \circ f_0)(p + v) - (f_1 \circ f_0)(p) - \Big(\mathrm{D}f_1(f_0(p)) \circ \mathrm{D}f_0(p)\Big) \cdot v}{\|v\|} = 0,$$

e concluímos que $\mathrm{D}f_1(f_0(p)) \circ \mathrm{D}f_0(p)$ é a diferencial de $f_1 \circ f_0$ em p. ■

Capítulo 10

Variedades

10.1 Variedades Topológicas e Diferenciais

10.1.1 Cartas e Atlas

Definição 10.1. 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 $x\colon A \longrightarrow \mathbb{R}^d$ 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 $x^i := \pi^i \circ x\colon A \longrightarrow \mathbb{R}$.

Definição 10.2. 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

$$\bar{x} \circ x^{-1} : x(A \cap \bar{A}) \longrightarrow \bar{x}(A \cap \bar{A}).$$

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 10.3. Seja V um conjunto. Cartas *$\mathscr{C}^k$-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

$$\bar{x} \circ x^{-1} : x(A \cap \bar{A}) \longrightarrow \bar{x}(A \cap \bar{A})$$

é um difeomorfismo $\mathscr{C}^k$. 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 10.4. Seja V um conjunto. Um *atlas* $\mathscr{C}^k$ 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 $(A, x), (\bar{A}, x) \in \mathcal{A}$ são $\mathscr{C}^k$-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 atlas têm a mesma dimensão, e a dimensão de um atlas só será mencionada quando necessário.

Definição 10.5. Seja V um conjunto. Atlas $\mathscr{C}^k$*-compatíveis* de V são atlas $\mathscr{C}^k$ $\mathcal{A}$ 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 $\mathscr{C}^k$-compatíveis.

Essa definição é equivalente a dizer que $\mathcal{A} \cup \bar{\mathcal{A}}$ é um atlas $\mathscr{C}^k$.

Proposição 10.1. *Seja V um conjunto. A relação de $\mathscr{C}^k$-compatibilidade de atlas 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

$$x_i \circ x^{-1} : x(A \cap A_i) \longrightarrow x_i(A \cap A_i).$$

e

$$\bar{x} \circ x_i^{-1} : x_i(A_i \cap \bar{A}) \longrightarrow \bar{x}(A_i \cap \bar{A}).$$

são difeomorfismos $\mathscr{C}^k$. 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 $\mathscr{C}^k$.

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 $\mathscr{C}^k$, o que mostra que (A, x) e $(\bar{A}, \bar{x})$ são $\mathscr{C}^k$-compatíveis, e finalmente $\mathcal{A}$ e $\bar{\mathcal{A}}$ são $\mathscr{C}^k$-compatíveis. ■

Isso implica, em particular, que os atlas $\mathscr{C}^k$ 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 10.6. Seja V um conjunto. Um atlas *maximal* $\mathscr{C}^k$ (ou uma *estrutura diferencial* $\mathscr{C}^k$) d-dimensional de V é a união de todos os atlas de uma classe de equivalência de atlas $\mathscr{C}^k$ 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.

10.1.2 Variedades e Estrutura Topológica e Diferencial

Definição 10.7. Uma *variedade* $\mathscr{C}^k$ d-dimensional é um par $\boldsymbol{V} = (V, \mathcal{A})$ em que V é um conjunto e $\mathcal{A}$ é um atlas maximal $\mathscr{C}^k$ d-dimensional de V. Para $k = 0$, a variedade $\boldsymbol{V}$ 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 $\mathscr{C}^k$ d-dimensional será simplesmente referida como uma variedade. Denotamos ainda a dimensão da variedade por um expoente: $\boldsymbol{V}^d$. 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 10.8. Seja $\boldsymbol{V}$ uma variedade. A *topologia* de $\boldsymbol{V}$ é o conjunto

$$\mathcal{T} := \left\langle \bigcup_{(A,x)\in\mathcal{A}} x^\star(\mathcal{T}_{\mathbb{R}^d}) \right\rangle,$$

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 $C \subseteq \mathsf{P}(V)$ e $x^\star(\mathcal{T})$ 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 $x(A)^\complement$ 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 10.2. *Sejam V um conjunto, $\mathcal{A} = \{(A_i, x_i)\}_{i\in I}$ um atlas de V e*

$$\mathcal{T} := \left\langle \bigcup_{i\in I} {x_i}^\star(\mathcal{T}_{\mathbb{R}^d}) \right\rangle.$$

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

$$\begin{aligned} x^{-1}(S) &= x^{-1}(\mathbb{R}^d) \cap x^{-1}\left(\left(\bigcup_{i \in I} U_i\right)^{\complement}\right) \\ &= A \cap \left(\bigcup_{i \in I} x^{-1}(U_i)\right)^{\complement} \\ &= A \cap \left(\bigcup_{i \in I} A \cap A_i\right)^{\complement} \\ &= A \cap (A \cap V)^{\complement} = A \cap (A)^{\complement} = \emptyset. \end{aligned}$$

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. ■

Proposição 10.3. *Sejam $\boldsymbol{V} = (V, \mathcal{A})$ uma variedade e $\bar{\mathcal{A}}$ um atlas compatível com o atlas maximal $\mathcal{A}$. A topologia*

$$\bar{\mathcal{T}} := \left\langle \bigcup_{(A,x) \in \bar{\mathcal{A}}} x^{\star}(\mathcal{T}_{\mathbb{R}^d}) \right\rangle,$$

é igual à topologia $\mathcal{T}$ de $\boldsymbol{V}$.

Demonstração. Por definição da topologia de $\boldsymbol{V}$, 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.

10.1.3 Exemplos de Variedades

A Esfera

Definição 10.9. A *esfera* d-dimensional é o conjunto

$$\mathbb{S}^d := \left\{ x \in \mathbb{R}^{d+1} \;\middle|\; \|x\| = 1 \right\}.$$

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 10.10. O *pólo norte* de $\mathbb{S}^d$ é o ponto $N := (0, \ldots, 0, 1)$ e a *projeção estereográfica norte* de $\mathbb{S}^d$ é a função

$$\begin{aligned} \pi_N \colon \mathbb{S}^d \smallsetminus \{N\} &\longrightarrow \mathbb{R}^d \\ x &\longmapsto \frac{1}{1 - x_d}(x_0, \ldots, x_{d-1}). \end{aligned}$$

O *pólo sul* de $\mathbb{S}^d$ é o ponto $S := -N = (0, \ldots, 0, -1)$ e a *projeção estereográfica sul* de $\mathbb{S}^d$ é a função

$$\begin{aligned} \pi_S \colon \mathbb{S}^d \smallsetminus \{S\} &\longrightarrow \mathbb{R}^d \\ x &\longmapsto \frac{1}{1 + x_d}(x_0, \ldots, x_{d-1}). \end{aligned}$$

Proposição 10.4. *Sejam π_N e π_S as projeções estereográficas norte e sul de $\mathbb{S}^d$. O conjunto*

$$\mathcal{A} := \{(\mathbb{S}^d \smallsetminus \{N\}, \pi_N), (\mathbb{S}^d \smallsetminus \{S\}, \pi_S)\}$$

é um atlas de $\mathbb{S}^d$.

Demonstração. As inversas de π_N e π_S são dadas por

$$\begin{aligned} \pi_N^{-1} \colon \mathbb{R}^d &\longrightarrow \mathbb{S}^d \\ x &\longmapsto \frac{1}{\|x\|^2 + 1}\left(2x_0, \ldots, 2x_{d-1}, \|x\|^2 - 1\right) \end{aligned}$$

e

$$\begin{aligned} \pi_S^{-1} \colon \mathbb{R}^d &\longrightarrow \mathbb{S}^d \\ x &\longmapsto \frac{-1}{\|x\|^2 + 1}\left(2x_0, \ldots, 2x_{d-1}, \|x\|^2 - 1\right). \end{aligned}$$

A transição de coordenadas entre as cartas é dada por

$$\begin{aligned} \pi_N \circ \pi_S^{-1} \colon \mathbb{R}^d \smallsetminus \{0\} &\longrightarrow \mathbb{R}^d \smallsetminus \{0\} \\ x &\longmapsto \frac{1}{\|x\|^2} x. \end{aligned}$$

Claramente, todas as funções são suaves. ■

Figura 10.1: Esfera 2-dimensional

O Espaço Projetivo

Definição 10.11. Sejam $x, y \in \mathbb{R}^d \smallsetminus \{0\}$. A relação de *equivalência homogênea* entre os pontos é definida por

$$x : y \quad \Longleftrightarrow \quad \bigvee t \in \mathbb{R}^* \qquad x = ty.$$

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 $[x_0 : \cdots : x_{d-1}] := [x]$.

Definição 10.12. O *espaço projetivo real* d-dimensional é o conjunto

$$\mathbb{PR}^d := \left\{ [x_0 : \cdots : x_d] \;\middle|\; x \in \mathbb{R}^{d+1} \right\}.$$

Considerando os conjuntos

$$A_i := \left\{ [x_0 : \cdots : x_d] \in \mathbb{PR}^d \;\middle|\; x_i \neq 0 \right\}.$$

e as funções

$$\begin{aligned} \varphi_i \colon A_i &\longrightarrow \mathbb{R}^d \\ [x_0 : \cdots : x_d] &\longmapsto \frac{1}{x_i}(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_d), \end{aligned}$$

cujas inversas são

$$\begin{aligned} \varphi_i^{-1} \colon \mathbb{R}^d &\longrightarrow A_i \\ x &\longmapsto [x_0 : \ldots, x_{i-1} : 1 : x_i :, \ldots : x_{d-1}]. \end{aligned}$$

Uma descrição equivalente é

$$\mathbb{PR}^d := \mathbb{S}^d \big/ \mathbb{S}^0 = \left\{ \{x, -x\} \;\middle|\; x \in \mathbb{S}^d \right\}.$$

Essa construção considera a ação de $\mathbb{S}^0$ em $\mathbb{S}^d$, a saber,

$$\begin{aligned} \times \colon \mathbb{S}^0 \times \mathbb{S}^d &\longrightarrow \mathbb{S}^d \\ (u, x) &\longmapsto ux. \end{aligned}$$

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

$$\begin{aligned} h \colon (\mathbb{Z}_2, +) &\longrightarrow (\mathbb{S}^0, \times) \\ n &\longmapsto (-1)^n, \end{aligned}$$

que é homomorfismo pois $(-1)^{n+n'} = (-1)^n(-1)^{n'}$ e é claramente bijeção.

O Toro

Definição 10.13. O *toro* d-dimensional é o conjunto

$$\mathbb{T}^d := \mathbb{R}^d / \mathbb{Z}^d.$$

Figura 10.2: Toro

Hiperboloide

Definição 10.14. O *hiperboloide* d-dimensional é o conjunto

$$\mathbb{H}^d := \left\{(x,t) \in \mathbb{R}^d \times \mathbb{R} = \mathbb{R}^{d+1} \;\middle|\; \|x\|^2 + 1 = t^2 \;\text{ e }\; t > 0\right\}.$$

▶ **Exercício 10.1.** Sejam $(\boldsymbol{V}_i)_{i\in[n]} = ((V_i, \mathcal{A}_i))_{i\in[n]}$ variedades $\mathscr{C}^k$ de dimensões $(d_i)_{i\in[n]}$, respectivamente. O par

$$\prod_{i\in[n]} V_i = \left(\prod_{i\in[n]} V_i, \prod_{i\in[n]} \mathcal{A}_i\right),$$

em que $\prod_{i\in[n]} V_i$ é o produto de conjuntos e

$$\prod_{i\in[n]} \mathcal{A}_i := \left\{\left(\prod_{i\in[n]} A_i, \prod_{i\in[n]} x_i\right) \;\middle|\; \bigwedge_{i\in[n]} (A_i, x_i) \in \mathcal{A}_i\right\}$$

é uma variedade $\mathscr{C}^k$ de dimensão $+_{i\in[n]} d_i$

10.1.4 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 10.5. *Seja $\boldsymbol{V} = (V, \mathcal{A})$ uma variedade. Então*

1. *$\boldsymbol{V}$ é um espaço topológico acessível (T_1);*

2. *$\boldsymbol{V}$ é um espaço topológico separado (T_2) se, e somente se, para todo $p, p' \in V$ distintos, existe $(A, x) \in \mathcal{A}$ tal que $p, p' \in A$ ou existem cartas $(A, x), (A', x) \in \mathcal{A}$ tais que $A \cap A' = \emptyset$, $p \in A$ e $p' \in A'$;*

3. *$\boldsymbol{V}$ tem base topológica enumerável se, e somente se, existe um subatlas enumerável de $\mathcal{A}$;*

4. *Cada componente conexa de $\boldsymbol{V}$ 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 $x(p)$, 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 $\boldsymbol{V}$ é um espaço topológico acessível.

2. Exercício.

3. ($\Rightarrow$) Como $\boldsymbol{V}$ 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 $\mathrm{B}_r(x) \subseteq x(A) \subseteq \mathbb{R}^d$ 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

$$\bar{\mathcal{B}} = \bigcup_{(A,x)\in\bar{\mathcal{A}}} \left\{ x^{-1}(\mathrm{B}_r(x)) \;\middle|\; \mathrm{B}_r(x) \subseteq x(A), r \in \mathbb{Q}, x \in \mathbb{Q}^d \right\}.$$

   Esse conjunto é uma base de $\boldsymbol{V}$: (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 $x_1(p) \in \mathrm{B}_r(x) \subseteq x_1(A_1 \cap A_2)$, logo $p \in {x_1}^{-1}(\mathrm{B}_r(x)) \subseteq A_1 \cap A_2$.

4. Sejam $C(p)$ uma componente conexa de $\boldsymbol{V}$ 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 $q \in U^{\complement}$. 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 $U^{\complement}$ é fechado, portanto U aberto. Assim, como U é aberto e fechado, $C(p)$ é conexo e $p \in U$, segue que $C(p) = U$.

■

10.2 Funções Diferenciáveis

10.2.1 Funções Diferenciáveis

Definição 10.15. Sejam $\boldsymbol{V_0}$ e $\boldsymbol{V_1}$ $\mathscr{C}^k$-variedades de dimensões d_0 e d_1, respectivamente. Uma função $\mathscr{C}^k$*-diferenciável* de $\boldsymbol{V_0}$ para $\boldsymbol{V_1}$ é uma função $F\colon V_0 \longrightarrow V_1$ 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

$$x_1 \circ F \circ x_0^{-1} : x_0(A_0) \longrightarrow x_1(A_1)$$

é uma função $\mathscr{C}^k$-diferenciável de $x_0(A_0) \subseteq \mathbb{R}^{d_0}$ para $x_1(A_1) \subseteq \mathbb{R}^{d_1}$.

Denota-se $F\colon \boldsymbol{V_0} \longrightarrow \boldsymbol{V_1}$. O conjunto de todas essas funções é denotado $\mathscr{C}^k(\boldsymbol{V_0}, \boldsymbol{V_1})$. Quando $V_1 = \mathbb{R}$, denota-se simplesmente $\mathscr{C}^k(\boldsymbol{V}_0)$.

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 $\mathscr{C}^k$-difeomorfismos, então $(x_1 \circ F \circ x_0^{-1})$ é $\mathscr{C}^k$-diferenciável se, e somente se, $(\bar{x}_1 \circ F \circ \bar{x}_0^{-1})$ o é. ■

Como uma $\mathscr{C}^k$-variedade é também uma $\mathscr{C}^l$-variedade para todo $l \leq k$, sempre se pode definir entre $\mathscr{C}^k$ e $\mathscr{C}^l$-variedade funções $\mathscr{C}^m$-diferenciáveis para qualquer $m \leq \min\{k, l\}$.

Proposição 10.6. *Sejam $\boldsymbol{V_0}$ e $\boldsymbol{V_1}$ $\mathscr{C}^k$-variedades e $F_0 : \boldsymbol{V_0} \longrightarrow \boldsymbol{V_1}$ uma função $\mathscr{C}^k$-diferenciável. Então F é uma função contínua.*

Proposição 10.7. *Sejam $\boldsymbol{V_0}$, $\boldsymbol{V_1}$ e $\boldsymbol{V_2}$ $\mathscr{C}^k$-variedades e $F_0 : \boldsymbol{V_0} \longrightarrow \boldsymbol{V_1}$ e $F_1 : \boldsymbol{V_1} \longrightarrow \boldsymbol{V_2}$ funções $\mathscr{C}^k$-diferenciáveis. Então $F_1 \circ F_0 : \boldsymbol{V_0} \longrightarrow \boldsymbol{V_1}$ é uma função $\mathscr{C}^k$-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 caso é evidenciado a seguir.

Definição 10.16. Sejam $\boldsymbol{V}$ uma $\mathscr{C}^k$-variedade e $I \subseteq \mathbb{R}$ um intervalo aberto. Uma *$\mathscr{C}^k$-curva* em $\boldsymbol{V}$ é uma função $\gamma : I \longrightarrow V$ $\mathscr{C}^k$-diferenciável.

Isso é equivalente a dizer que, para todo $p \in \gamma(V)$ existe carta (A, x) em p tal que

$$x \circ \gamma : I \longrightarrow x(A)$$

é uma função $\mathscr{C}^k$-diferenciável, ao escolher acima a função identidade.

10.2.2 Funções Separadoras e Partições da Unidade

Consideraremos inicialmente a função

$$\begin{aligned} f \colon \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \begin{cases} 0, & x \leq 0 \\ e^{-\frac{1}{x}}, & x > 0. \end{cases} \end{aligned}$$

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

$$\begin{aligned} h \colon \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{f(r_1 - x)}{f(x - r_0) - f(r_1 - x)}. \end{aligned}$$

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 $\mathrm{B}_{r_0}(0)$ e o complementar da bola fechada $\mathrm{B}_{r_1}(0)$. Basta usar a função h para definir a função

$$\begin{aligned} H \colon \mathbb{R}^d &\longrightarrow \mathbb{R} \\ x &\longmapsto h(\|x\|). \end{aligned}$$

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 $A^{\complement}$ e um compacto K. Essa funções sempre existem em espaços topológicos separados por vizinhanças (T_2) e localmente compactos.

Definição 10.17. Sejam $\boldsymbol{X}$ um espaço topológico e $f : X \longrightarrow \mathbb{R}$ uma função contínua. O *suporte fechado* de f é o conjunto

$$\overline{\mathrm{supp}}(f) := \overline{\mathrm{supp}(f)}.$$

Proposição 10.8. *Sejam $\boldsymbol{X}$ um espaço topológico separado por vizinhanças (T_2) e localmente compacto, $A \subseteq X$ um aberto e $K \subseteq A$ um compacto. Existe função $f : X \longrightarrow [0,1]$ tal que $\overline{\mathrm{supp}}(f) \subseteq A$ e $f(K) = \{1\}$.*

Notemos que tal função separa continuamente $A^{\complement}$ e K, pois

$$\mathrm{supp}(f) \subseteq \overline{\mathrm{supp}}(f) \subseteq A$$

implica $A^{\complement} \subseteq \mathrm{supp}(f)^{\complement}$, portanto $f(A^{\complement}) \subseteq f(\mathrm{supp}(f)^{\complement}) = \{0\}$.

Definição 10.18. Sejam $\boldsymbol{X}$ um espaço topológico (variedade suave) e $\mathcal{C} = (C_i)_{i\in I}$ uma cobertura aberta de $\boldsymbol{X}$. Uma *partição da unidade* (*suave*) subordinada a $\mathcal{C}$ é uma família de funções contínuas (suaves) $\psi_i \colon X \longrightarrow \mathbb{R}$ tal que

1. (Unidade) Para todos $i \in I$ e $x \in X$, $0 \leq \psi_i(x) \leq 1$;
2. (Partição) A família $(\overline{\mathrm{supp}}(\psi_i))_{i\in I}$ é localmente finita (todo ponto tem uma vizinhança que interseciona finitos dos conjuntos da família) e, para todo $x \in X$,
$$\mathop{+}_{i\in I} \psi_i(x) = 1.$$
3. (Subordinação) Para todo $i \in I$, $\overline{\mathrm{supp}}(\psi_i) \subseteq C_i$.

Proposição 10.9. *Sejam $\boldsymbol{V}$ uma variedade (suave) e $\mathcal{C} = (C_i)_{i\in I}$ uma cobertura aberta de $\boldsymbol{V}$. Existe partição da unidade (suave) $\psi_i \colon X \longrightarrow \mathbb{R}$ subordinada a $\mathcal{C}$.*

10.3 Espaço Tangente

A partir desta seção, não estudaremos mais com detalhes os casos de variedades $\mathscr{C}^k$-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, $\mathscr{C}^\infty$-diferenciais, e a mesma nomenclatura será usada para funções diferenciáveis.

10.3.1 Álgebra dos Campos Escalares

Dada uma variedade diferencial $\boldsymbol{V}$, um *campos escalares* em $\boldsymbol{V}$ são funções do espaço $\mathscr{C}^\infty(V, \mathbb{R})$ 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

$$\begin{aligned} +\colon \mathfrak{T}^0(V) \times \mathfrak{T}^0(V) &\longrightarrow \mathfrak{T}^0(V) \\ (f, f') &\longmapsto f + f' \colon V \longrightarrow \mathbb{R} \\ & \qquad\qquad p \longmapsto f(p) + f'(p) \end{aligned}$$

e o produto por escalar é dado por

$$\begin{aligned} \cdot\colon \mathbb{R} \times \mathfrak{T}^0(V) &\longrightarrow \mathfrak{T}^0(V) \\ (c, f) &\longmapsto cf \colon V \longrightarrow \mathbb{R} \\ & \qquad\qquad p \longmapsto cf(p). \end{aligned}$$

Ainda, pode-se definir um produto em $\mathfrak{T}^0(V)$ também induzido pontualmente de $\mathbb{R}$, dado por

$$\begin{aligned} \times\colon \mathfrak{T}^0(V) \times \mathfrak{T}^0(V) &\longrightarrow \mathfrak{T}^0(V) \\ (f, f') &\longmapsto ff' \colon V \longrightarrow \mathbb{R} \\ & \qquad\qquad p \longmapsto f(p)f'(p). \end{aligned}$$

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 $\boldsymbol{V}$. É simples ver que essas operações geram funções diferenciáveis de $\mathfrak{T}^0(V)$.

Proposição 10.10. *Seja $\boldsymbol{V}$ uma variedade diferencial.*

[1] Usualmente denota-se esse espaço por $\mathscr{C}^\infty(V)$, 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* $\mathbb{R}$.

10.3.2 Espaço Tangente e a Diferencial

Derivações em Pontos

Definição 10.19. Sejam $\boldsymbol{V}$ uma variedade diferencial e $p \in V$. Uma *derivação* em p é um funcional linear $D\colon \mathfrak{T}^0(V) \longrightarrow \mathbb{R}$ que satisfaz, para todas $f, f' \in \mathfrak{T}^0(V)$,

$$D(ff') = D(f)f'(p) + f(p)D(f').$$

O *espaço tangente* a $\boldsymbol{V}$ em p é o conjunto $\mathrm{T}V|_p$ de todas derivações em p e os *vetores tangentes* a V em p são os elementos de $\mathrm{T}V|_p$.

O espaço tangente $\mathrm{T}V|_p$ 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 10.11. *Sejam* $\boldsymbol{V}$ *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 $\mathrm{T}V|_p$ 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 $v, v' \in \mathrm{T}V|_p$ e $c \in \mathbb{R}$, e todos $f, f' \in \mathfrak{T}^0(V)$,

$$\begin{aligned}
(v + v')(ff') &= v(ff') + v'(ff') \\
&= v(f)f'(p) + f(p)v(f') + v'(f)f'(p) + f(p)v'(f') \\
&= (v(f) + v'(f))f'(p) + f(p)(v(f') + v'(f')) \\
&= (v + v')(f)f'(p) + f(p)(v + v')(f')
\end{aligned}$$

e

$$\begin{aligned}
(cv)(ff') &= c(v(ff')) \\
&= c(v(f)f'(p) + f(p)v(f')) \\
&= cv(f)f'(p) + cf(p)v(f') \\
&= (cv)(f)f'(p) + f(p)(cv)(f'),
\end{aligned}$$

o que mostra que $v + v'$ e cv são derivações em p. ■

Assim temos um espaço vetorial $\mathrm{T}V|_p$ associado a cada ponto p da variedade. As seguintes propriedades serão utilizadas na demonstração de algumas proposições mais à frente.

Proposição 10.12. *Sejam $\boldsymbol{V}$ uma variedade diferencial, $p \in V$ e $v \in \mathrm{T}V|_p$.*

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
$$v(ff') = v(f)f'(p) + f(p)v(f') = 0.$$
■

A Diferencial de uma Função Diferenciável

Definição 10.20. Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais, $F\colon V \longrightarrow V'$ uma função diferenciável e $p \in V$. A *diferencial* de F em p é a função
$$\begin{aligned} \mathrm{D}F|_p\colon \mathrm{T}V|_p &\longrightarrow \mathrm{T}V'|_{F(p)} \\ v &\longmapsto \mathrm{D}F|_p v\colon \mathfrak{T}^0(V') \longrightarrow \mathbb{R} \\ &\qquad\qquad\qquad f \longmapsto v(f \circ F). \end{aligned}$$

Pode-se denotar $\mathrm{D}F_p$ por simplicidade.

A diferencial $\mathrm{D}F|_p$ 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,
$$\begin{aligned} (\mathrm{D}F|_p v)(f + f') &= v((f + f') \circ F) \\ &= v((f \circ F) + (f' \circ F)) \\ &= v(f \circ F) + v(f' \circ F) \\ &= (\mathrm{D}F|_p v)(f) + (\mathrm{D}F|_p v)(f') \end{aligned}$$
e
$$\begin{aligned} (\mathrm{D}F|_p v)(cf) &= v((cf) \circ F) \\ &= v(c(f \circ F)) \\ &= cv(f \circ F) \\ &= c(\mathrm{D}F|_p v)(f), \end{aligned}$$

o que mostra que $\mathrm{D}F|_p v$ é linear; como v é derivação em p,

$$\begin{aligned}(\mathrm{D}F|_p v)(ff') &= v((ff')\circ F)\\ &= v((f\circ F)(f'\circ F))\\ &= v(f\circ F)(f'\circ F)(p) + (f\circ F)(p)v(f'\circ F)\\ &= v((f\circ F))f'(F(p)) + f(F(p))v(f'\circ F)\\ &= (\mathrm{D}F|_p v)(f)f'(F(p)) + f(F(p))(\mathrm{D}F|_p v)(f')\end{aligned}$$

o que mostra que $\mathrm{D}F|_p v$ é derivação em $F(p)$.

Proposição 10.13. *Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais e $F\colon V \longrightarrow V'$ uma função diferenciável e $p \in V$. A diferencial $\mathrm{D}F|_p\colon \mathrm{T}V|_p \longrightarrow \mathrm{T}V'|_{F(p)}$ é uma função linear.*

Demonstração. Sejam $v, v' \in \mathrm{T}V|_p$ e $c \in \mathbb{R}$. Então, para todo $f \in \mathfrak{T}^0(V)$,

$$\begin{aligned}(\mathrm{D}F|_p(v+v'))(f) &= (v+v')(f\circ F)\\ &= v(f\circ F) + v'(f\circ F)\\ &= (\mathrm{D}F|_p v)(f) + (\mathrm{D}F|_p v')(f)\end{aligned}$$

e

$$\begin{aligned}(\mathrm{D}F|_p(cv))(f) &= (cv)(f\circ F)\\ &= c(v(f\circ F))\\ &= (c\mathrm{D}F|_p v)(f),\end{aligned}$$

o que mostra que $\mathrm{D}F|_p(v+v') = \mathrm{D}F|_p v + \mathrm{D}F|_p v'$ e $\mathrm{D}F|_p(cv) = c\mathrm{D}F|_p v$. ■

Proposição 10.14 (Regra da Cadeia)**.** *Sejam $\boldsymbol{V}$, $\boldsymbol{V}'$ e $\boldsymbol{V}''$ variedades diferenciais, $F\colon V \longrightarrow V'$ e $F'\colon V' \longrightarrow V''$ funções diferenciáveis, e $p \in V$. Então*

$$\mathrm{D}(F'\circ F)|_p = \mathrm{D}F'|_{F(p)} \circ \mathrm{D}F|_p.$$

Demonstração. Para todos $v \in \mathrm{T}V|_p$ e $f \in \mathfrak{T}^0(V'')$,

$$\begin{aligned}(\mathrm{D}(F'\circ F)|_p v)(f) &= v(f\circ(F'\circ F))\\ &= v((f\circ F')\circ F))\\ &= (\mathrm{D}F|_p v)(f\circ F')\\ &= ((\mathrm{D}F'|_{F(p)})(\mathrm{D}F|_p v))(f)\\ &= ((\mathrm{D}F'|_{F(p)}\circ \mathrm{D}F|_p)v)(f),\end{aligned}$$

portanto $\mathrm{D}(F'\circ F)|_p v = (\mathrm{D}F'|_{F(p)}\circ \mathrm{D}F|_p)v$ para todo $v \in \mathrm{T}V|_p$, o que implica

$$\mathrm{D}(F'\circ F)|_p = \mathrm{D}F'|_{F(p)} \circ \mathrm{D}F|_p.$$ ■

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 $\mathrm{D}f|_p \colon \mathbb{R}^d \longrightarrow \mathbb{R}$. Essa diferencial pode ser aplicada no vetor canônico $e_i \in \mathbb{R}^d$, definindo

$$\partial_i|_p f := \mathrm{D}f|_p e_i.$$

A função $\partial_i|_p \colon \mathfrak{T}^0(\mathbb{R}^d) \longrightarrow \mathbb{R}$ 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

$$\begin{aligned}\partial_i|_p(cf + f') &= \mathrm{D}(cf + f')|_p e_i = (c\mathrm{D}f|_p + \mathrm{D}f'|_p)e_i \\ &= c\mathrm{D}f|_p e_i + \mathrm{D}f'|_p e_i \\ &= c\partial_i|_p(f) + \partial_i|_p(f'),\end{aligned}$$

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

$$\begin{aligned}\partial_i|_p(ff') &= \mathrm{D}(ff')|_p e_i \\ &= (\mathrm{D}f|_p f'(p) + f(p)\mathrm{D}f'|_p)e_i \\ &= \mathrm{D}f|_p f'(p)e_i + f(p)\mathrm{D}f'|_p e_i \\ &= \partial_i|_p(f)f'(p) + f(p)\partial_i|_p(f').\end{aligned}$$

A derivação direcional de f an direção de $v = +_{i\in[d]} c^i e_i$ é

$$\mathrm{D}_v|_p f := \mathrm{D}f|_p v.$$

Note que, para todo $f \in \mathfrak{T}^0(\mathbb{R}^d)$,

$$\mathrm{D}_v|_p(f) = \mathrm{D}f|_p v = \mathrm{D}f|_p \left(\mathop{+}_{i\in[d]} v^i e_i \right) = \mathop{+}_{i\in[d]} v^i \mathrm{D}f|_p e_i = \mathop{+}_{i\in[d]} v^i \partial_i|_p(f),$$

logo $\mathrm{D}_v|_p = +_{i\in[d]} v^i \partial_i|_p$. Mostraremos que essa função é um isomorfismo de espaço lineares.

Proposição 10.15. *Seja $d \in \mathbb{N}$. Para todo $p \in \mathbb{R}^d$, a função*

$$\begin{aligned}\mathrm{D}.|_p \colon \mathbb{R}^d &\longrightarrow \mathrm{T}\mathbb{R}^d|_p \\ v &\longmapsto \mathrm{D}_v|_p\end{aligned}$$

é um isomorfismo de espaços lineares.

Demonstração. Seja $v = +_{i\in[d]} v^i e_i$ e, portanto, $\mathrm{D}_v|_p = +_{i\in[d]} v^i \partial_i|_p$. 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 $\mathrm{D}f|_p$ que

$$\begin{aligned}
\mathrm{D}_{cv+v'}|_p f &= \mathrm{D}f|_p(cv + v') \\
&= c\mathrm{D}f|_p v + \mathrm{D}f|_p v' \\
&= c\mathrm{D}_v|_p f + \mathrm{D}_{v'}|_p f \\
&= (c\mathrm{D}_v + \mathrm{D}_{v'})f.
\end{aligned}$$

Agora, mostremos que ela é injetiva. Seja $v \in \mathbb{R}^d$ tal que $\mathrm{D}_v|_p = 0$. Então, para cada $i \in [d]$, como $\mathrm{D}\pi^i|_p = \pi^i$,

$$0 = \mathrm{D}_v|_p \pi^i = \mathrm{D}\pi^i|_p v = \pi^i(v) = v^i,$$

logo $v = 0$. Agora, mostremos que ela é sobrejetiva. Seja $D \in \mathrm{T}\mathbb{R}^d|_p$. Para cada $i \in [d]$, definimos $v^i := D(\pi^i)$ e $v := +_{i\in[d]} v^i e_i$. Mostraremos que $D = \mathrm{D}_v|_p$. Seja $f \in \mathfrak{T}^0(\mathbb{R}^d)$. Pela fórmula de Taylor, existem constantes $C_{i,j} \in \mathbb{R}$ tais que

$$f = f(p) + \mathop{+}_{i\in[d]} \partial_i f(p)(\pi^i - p^i) + \mathop{+}_{(i,j)\in[d]^2} C_{i,j}(\pi^i - p^i)(\pi^j - p^j).$$

Como $f(p)$ é constante, $D(f(p)) = 0$ (10.12), e, como as funções $(\pi^i - p^i)$ e $(\pi^j - p^j)$ se anulam em p, $D\left((\pi^i - p^i)(\pi^j - p^j)\right) = 0$ para todos $i, j \in [d]$ (10.12), logo

$$D\left(\mathop{+}_{(i,j)\in[d]^2} C_{i,j}(\pi^i - p^i)(\pi^j - p^j)\right) = \mathop{+}_{(i,j)\in[d]^2} C_{i,j} D\left((\pi^i - p^i)(\pi^j - p^j)\right) = 0,$$

o que implica que

$$\begin{aligned}
D(f) &= D\left(\mathop{+}_{i\in[d]} \partial_i f(p)(\pi^i - p^i)\right) \\
&= \mathop{+}_{i\in[d]} D\left(\partial_i f(p)(\pi^i - p^i)\right) \\
&= \mathop{+}_{i\in[d]} \left(\partial_i f(p) D(\pi^i - p^i)\right) \\
&= \mathop{+}_{i\in[d]} \partial_i f(p)(D(\pi^i) - D(p^i)) \\
&= \mathop{+}_{i\in[d]} \partial_i f(p) v^i \\
&= \mathrm{D}_v|_p f.
\end{aligned}$$

■

Essa proposição mostra que $(\partial_i|_p)_{i\in[d]}$ é uma base ordenada do espaço tangente $\mathrm{T}\mathbb{R}^d|_p$, o qual é isomorfo a $\mathbb{R}^d$ e deve ser visto como o espaço dos vetores tangentes a $\mathbb{R}^d$ em p.

10.3.3 Fibrado Tangente

Definição 10.21. Seja $\boldsymbol{V}$ um variedade diferencial. O *fibrado tangente* de $\boldsymbol{V}$ é

$$\mathrm{T}V := \bigsqcup_{p\in V} \mathrm{T}V|_p = \{(p,v) \mid p \in V, v \in \mathrm{T}V|_p\},$$

a união disjunta dos espaços tangentes a $\boldsymbol{V}$ 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

$$\begin{aligned}\frac{\partial}{\partial x^i}\bigg|_p : \mathfrak{T}^0(V) &\longrightarrow \mathbb{R}\\ f &\longmapsto \partial_i(f\circ x^{-1})|_{x(p)}\end{aligned}$$

são uma base ordenada de $\mathrm{T}V|_p$. Essas funções são lineares porque, para todas $f, f' \in \mathfrak{T}^0(V)$ e $c \in \mathbb{R}$,

$$\begin{aligned}\frac{\partial}{\partial x^i}\bigg|_p (cf+f') &= \partial_i((cf+f')\circ x^{-1})|_{x(p)}\\ &= \partial_i((cf\circ x^{-1}) + (f'\circ x^{-1}))|_{x(p)}\\ &= c\partial_i(f\circ x^{-1})|_{x(p)} + \partial_i(f'\circ x^{-1}))|_{x(p)}\\ &= c\,\frac{\partial}{\partial x^i}\bigg|_p f + \frac{\partial}{\partial x^i}\bigg|_p f,\end{aligned}$$

e são derivações porque, para todas $f, f' \in \mathfrak{T}^0(V)$,

$$\begin{aligned}\frac{\partial}{\partial x^i}\bigg|_p (ff') &= \partial_i((ff')\circ x^{-1})|_{x(p)}\\ &= \partial_i((f\circ x^{-1})(f'\circ x^{-1}))|_{x(p)}\\ &= (f\circ x^{-1})|_{x(p)}(\partial_i(f'\circ x^{-1})|_{x(p)}\\ &\qquad + (f'\circ x^{-1})|_{x(p)}(\partial_i(f\circ x^{-1})|_{x(p)}\\ &= f(p)\,\frac{\partial}{\partial x^i}\bigg|_p f + f'(p)\,\frac{\partial}{\partial x^i}\bigg|_p f'.\end{aligned}$$

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 $\mathrm{D}_i f(p)$) e

$$\partial_i f(p) = \mathrm{D}f(p) \cdot e_i.$$

A motivação da notação $\frac{\partial}{\partial x^i}$, além do uso histórico, vem da ideia de que vale a regra da cadeia

$$\partial_i (f \circ x^{-1})|_{x(p)} \text{`='} \partial_i f|_{x^{-1}(x(p))} \circ \partial_i (x^{-1})|_{x(p)} \text{`='} \partial_i f|_p \circ (\partial_i x|_p)^{-1} \text{`='} \left.\frac{\partial_i f}{\partial_i x}\right|_p.$$

A função

$$\begin{aligned} \frac{\partial}{\partial x^i} \colon A &\longrightarrow \mathrm{T}V|_A \\ p &\longmapsto \left.\frac{\partial}{\partial x^i}\right|_p \end{aligned}$$

é um campo vetorial em A — uma seção de $\mathrm{T}V|_A$ — e $\frac{\partial}{\partial x} = \left(\frac{\partial}{\partial x^i}\right)_{i \in [d]}$ é um referencial local de A.

10.3.4 Curvas Equivelozes

O espaço tangente pode ser alternativamente descrito com curvas.

Definição 10.22. Sejam $\boldsymbol{V}$ uma variedade diferencial e $p \in V$. Duas curvas $\gamma_0 \colon I_0 \longrightarrow V$ e $\gamma_1 \colon I_1 \longrightarrow V$ 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

$$\begin{aligned} (\bar{x} \circ \gamma_i)'(0) &= \mathrm{D}\Big((\bar{x} \circ x^{-1}) \circ (x \circ \gamma_i)\Big)(0) \\ &= \mathrm{D}(\bar{x} \circ x^{-1})(x \circ \gamma_i(0)) \circ (x \circ \gamma_i)'(0) \\ &= \mathrm{D}(\bar{x} \circ x^{-1})(x(p)) \circ (x \circ \gamma_i)'(0). \end{aligned}$$

Como $\bar{x} \circ x^{-1}$ é difeomorfismo, $\mathrm{D}(\bar{x} \circ x^{-1})(x(p))$ 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 10.23. Sejam $\boldsymbol{V}$ uma variedade diferencial, $p \in V$ e $\gamma : I \longrightarrow V$ uma curva iniciada em p. O *vetor tangente a* $\boldsymbol{V}$ *em* p, denotado $\gamma'(0)$, é a classe de equivalência de γ sob a relação $\asymp$ de equivelocidade de curvas.

O *espaço tangente* a $\boldsymbol{V}$ em p é o conjunto de vetores tangentes a $\boldsymbol{V}$ em p, denotado

$$\mathrm{T}V|_p := \{\gamma'(0) \mid \gamma \colon I \longrightarrow V, \gamma(0) = p\},$$

em que os I são intervalos abertos de $\mathbb{R}$ contendo o 0.

O *fibrado tangente* de $\boldsymbol{V}$ é a união disjunta dos espaços tangentes a $\boldsymbol{V}$ em todos pontos de V

$$\mathrm{T}V := \bigsqcup_{p \in V} \mathrm{T}V|_p = \{(p, v) \mid p \in V, v \in \mathrm{T}V|_p\}.$$

Os elementos do espaço tangente a $\boldsymbol{V}$ em um ponto $p \in V$ são chamados de vetores porque $\mathrm{T}_p\boldsymbol{V}$ é um espaço vetorial se definidas operações apropriadas. Isso que fazemos a seguir.

Para isso, vamos mostrar que $\mathrm{D}f(p) : \mathrm{T}_pV \longrightarrow \mathbb{R}^n$ é uma bijeção. Assim poderemos puxar as operações de espaço vetorial de $\mathbb{R}^n$ para T_pV.

Definição 10.24. Sejam $\boldsymbol{V}$ e $\bar{\boldsymbol{V}}$ variedades, $p \in V$ e $f : V \longrightarrow \bar{V}$ uma função diferenciável em p. A *diferencial* de f em p é a função

$$\begin{aligned} \mathrm{D}f(p) \colon \mathrm{T}_pV &\longrightarrow \mathrm{T}_{f(p)}\bar{V} \\ \gamma'(0) &\longmapsto (f \circ \gamma)'(0). \end{aligned}$$

Devemos mostrar que essa função está bem definida.

Tomando uma carta (A, x) em p, definimos a função

$$\begin{aligned} \mathrm{D}x(p) \colon \mathrm{T}_p\boldsymbol{V} &\longrightarrow \mathbb{R}^d \\ \gamma'(0) &\longmapsto (x \circ \gamma)'(0) \end{aligned}$$

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 $\mathrm{T}_p\boldsymbol{V}$, de modo que $\mathrm{T}_p\boldsymbol{V}$ é um espaço vetorial. Essas operações puxadas não dependem da carta (A, x) escolhida.

10.4 Subvariedades

10.4.1 Imersão

10.4.2 Submersão

10.4.3 Mergulho

10.4.4 Subvariedades Imersas e Mergulhadas

10.5 Transversalidade

10.5.1 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 10.25. 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

$$\mathrm{vol}^d(C) := |b_0 - a_0| \cdots |b_{d-1} - a_{d-1}| \,.$$

Admitimos nessa definição que $\emptyset$ é um intervalo aberto, portanto que é um cubo aberto, e temos que seu volume é 0.

Definição 10.26. 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

$$\mathop{+}_{n\in\mathbb{N}} \mathrm{vol}^d(C_n) < \varepsilon.$$

Denota-se $N \mathrel{\overset{\circ}{=}} \emptyset$.

O motivo da notação $N \mathrel{\overset{\circ}{=}} \emptyset$ ficará mais claro quando uma medida for definida.

Proposição 10.16. *Seja $d \in \mathbb{N}$. O conjunto de conjuntos nulos é um σ-ideal:*

1. $\emptyset \mathrel{\overset{\circ}{=}} \emptyset$;
2. *Se $S \subseteq N \subseteq \mathbb{R}^d$ e $N \mathrel{\overset{\circ}{=}} \emptyset$, então $S \mathrel{\overset{\circ}{=}} \emptyset$;*
3. *Para toda sequência $(N_n)_{n\in\mathbb{N}}$ de subconjuntos nulos em $\mathbb{R}^d$,*

$$\bigcup_{n\in\mathbb{N}} N_n \mathrel{\overset{\circ}{=}} \emptyset.$$

Demonstração. 1. Basta considerar a sequência de conjuntos vazios $(\emptyset)_{n\in\mathbb{N}}$. Essa sequência cobre $\emptyset$ e $\mathrm{vol}^d(\emptyset) = 0$. Portanto, para todo $\varepsilon > 0$,

$$\mathop{+}_{n\in\mathbb{N}} \mathrm{vol}^d(\emptyset) = 0 < \varepsilon,$$

o que mostra que $\emptyset \mathrel{\overset{\circ}{=}} \emptyset$.

2. Seja $\varepsilon > 0$. Como $N \mathrel{\overset{\circ}{=}} \emptyset$, existe cobertura $(C_n)_{n\in\mathbb{N}}$ de N por cubos tal que $\mathop{+}_{n\in\mathbb{N}} \mathrm{vol}^d(C_n) < \varepsilon$. Como $S \subseteq N$, essa cobertura é também uma cobertura de S, logo $S \mathrel{\overset{\circ}{=}} \emptyset$.

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 $\mathop{+}_{i\in\mathbb{N}} \mathrm{vol}^d(C_i^n) < \varepsilon 2^{-(n+1)}$, logo $(C_i^n)_{(n,i)\in\mathbb{N}^2}$ é uma cobertura de $(N_n)_{n\in\mathbb{N}}$ e

$$\mathop{+}_{(n,i)\in\mathbb{N}^2} \mathrm{vol}^d(C_i^n) < \mathop{+}_{n\in\mathbb{N}} \varepsilon 2^{-(n+1)} = \varepsilon. \qquad \blacksquare$$

Proposição 10.17. *Sejam $d \in \mathbb{N}$ e $C \subseteq \mathbb{R}^d$ um conjunto contável. Então $C \mathrel{\overset{\circ}{=}} \emptyset$.*

Demonstração. Basta mostrar que um conjunto unitário é nulo, pois C é uma união contável de conjunto 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

$$\mathrm{vol}^d(C_0) = \bigtimes_{i\in[d]} \left| p_i + \frac{(\alpha\varepsilon)^{\frac{1}{d}}}{2} - \left(p_i - \frac{(\alpha\varepsilon)^{\frac{1}{d}}}{2}\right)\right| = \left((\alpha\varepsilon)^{\frac{1}{d}}\right)^d = \alpha\varepsilon$$

e $\mathrm{vol}^d(\emptyset) = 0$, segue que

$$\mathop{+}_{n\in\mathbb{N}} \mathrm{vol}^d(C_n) = \alpha\varepsilon < \varepsilon,$$

logo $\{p\} \mathrel{\overset{\circ}{=}} \emptyset$. $\blacksquare$

Agora, definiremos conjuntos nulos em uma variedade $\boldsymbol{V}$.

Definição 10.27. Seja $\boldsymbol{V}$ uma variedade diferencial. Um conjunto *nulo* em $\boldsymbol{V}$ é um conjunto $N \subseteq V$ tal que, para toda carta (A, x) de $\boldsymbol{V}$, o conjunto $x(Q \cap A)$ é nulo em $\mathbb{R}^d$. Denota-se $N \mathrel{\overset{\circ}{=}} \emptyset$.

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 $\boldsymbol{V}$, vale para seu atlas maximal. Na próxima seção, enunciaremos proposições que envolvem conjuntos nulos.

10.5.2 Valor Regular

Definição 10.28. Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais e $F\colon V \longrightarrow V'$ uma função diferenciável. Um *valor regular* de F é um ponto $q \in V'$ tal que, para todo $p \in F^{-1}(q)$, $\mathrm{D}F|_p\colon \mathrm{T}V|_p \longrightarrow \mathrm{T}V'|_q$ é sobrejetiva.

Proposição 10.18. *Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais, $F\colon V \longrightarrow V'$ uma função diferenciável e $q \in V'$ um valor regular de F. Então $F^{-1}(q) \subseteq V$ é uma subvariedade diferencial de dimensão* $\dim(V) - \dim(V')$.

10.5.3 Ponto Crítico

Definição 10.29. Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais e $F\colon V \longrightarrow V'$ uma função diferenciável. Um *ponto crítico* de F é um ponto $p \in V$ tal que $\mathrm{D}F|_p\colon \mathrm{T}V|_p \longrightarrow \mathrm{T}V'|_{F(p)}$ não é sobrejetiva.

Ou seja, um valor regular é um ponto cujos pontos de sua imagem inversa não são críticos.

Proposição 10.19 (Teorema de Sard)**.** *Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais e $F\colon V \longrightarrow V'$ diferenciável. Se o conjunto $C \subseteq V$ de pontos críticos de F é nulo em $\boldsymbol{V}$, então $F(C) \subseteq V'$ é nulo em $\boldsymbol{V}'$.*

10.5.4 Transversalidade

Definição 10.30. Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais e $\boldsymbol{S} \subseteq \boldsymbol{V}'$ uma subvariedade. Uma função *transversal* a $\boldsymbol{S}$ é uma função diferenciável $F\colon V \longrightarrow V'$ tal que, para todo $p \in F^{-1}(S) \subseteq V$,

$$\mathrm{D}F|_p(\mathrm{T}V|_p) + \mathrm{T}S|_{F(p)} = \mathrm{T}V'|_{F(p)}.$$

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 $F(p) = q$, $\mathrm{T}S|_{F(p)} = \{0\}$ e a condição acima se torna $\mathrm{D}F|_p\mathrm{T}V|_p = \mathrm{T}V'|_{F(p)}$, o que é equivalente a $\mathrm{D}F|_p$ 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 10.20. *Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais, $\boldsymbol{S} \subseteq \boldsymbol{V}'$ uma subvariedade e $F\colon V \longrightarrow V'$ uma função diferenciável tal que $F \pitchfork S$. Então $F^{-1}(S) \subseteq V$ é uma subvariedade diferencial e* $\dim^{\complement}{}_V(F^{-1}(S)) = \dim^{\complement}{}_{V'}(S)$.

Demonstração. Consideremos $p \in U \subseteq V$, $q = F(p)$, $U' = F(U) \subseteq V'$, uma carta adaptada $\varphi\colon U' \subseteq V' \longrightarrow I^{\dim S} \times I^{\dim^{\complement}{}_{V'}S}$ tal que $\varphi(q) = 0$ e $\varphi(U \cap S) = I^{\dim S} \times \{0\}$, e a projeção $\pi\colon I^{\dim S} \times I^{\dim^{\complement}{}_{V'}S} \longrightarrow I^{\dim^{\complement}{}_{V'}S}$. Então

$$\pi \circ \varphi \circ F\colon V \longrightarrow I^{\dim^{\complement}{}_{V'}S}$$

é uma função diferenciável. Notemos agora que $0 \in I^{\dim^{\complement}{}_{V'}S}$ é um valor regular de $\pi \circ \varphi \circ F$, pois para todo $a \in F^{-1}(S)$, como $F \pitchfork S$,

$$\mathrm{T}V'|_{F(a)} = \mathrm{D}F|_p \mathrm{T}V|_a + \mathrm{T}S|_{F(a)},$$

portanto $\mathrm{D}\varphi|_{F(a)}\mathrm{T}S|_{F(a)} = \mathbb{R}^{\dim S} \times \{0\}$. Sendo assim, segue que $F^{-1}(S) = (\pi \circ \varphi \circ F)^{-1}(0)$, logo $F^{-1}(S)$ é uma subvariedade de V. ■

Um caso importante é quando tem-se uma variedade diferencial $\boldsymbol{V}$ e duas subvariedades diferenciais $\boldsymbol{S}$ e $\boldsymbol{S}'$ de $\boldsymbol{V}$. Se consideramos a inclusão $\iota\colon S \longrightarrow V$, a condição $p \in \iota^{-1}(S')$ é equivalente a $p \in S \cap S'$, pois $\iota(p) = p$. Nesse caso, $\mathrm{D}\iota|_p = \mathrm{I}$, portanto $\iota \pitchfork S'$ é equivalente a, para todo $p \in S \cap S'$,

$$\mathrm{T}S|_p + \mathrm{T}S'|_p = \mathrm{T}V|_p.$$

Claramente, essa condição é simétrica com relação a S e S'. Definimos assim a transversalidade entre subvariedades.

Definição 10.31. Seja $\boldsymbol{V}$ uma variedade diferencial. Duas subvariedades diferenciais $\boldsymbol{S}$ e $\boldsymbol{S}'$ de $\boldsymbol{V}$ são *transversais* se, e somente se, para todo $p \in S \cap S'$,

$$\mathrm{T}S|_p + \mathrm{T}S'|_p = \mathrm{T}V|_p.$$

Denota-se $S \pitchfork S'$.

Proposição 10.21. *Sejam $\boldsymbol{V}$ uma variedade diferencial e $\boldsymbol{S}$ e $\boldsymbol{S}'$ subvariedades diferenciais de $\boldsymbol{V}$ tais que $S \pitchfork S'$. Então $S \cap S'$ é uma subvariedade diferencial de V e*

$$\dim^{\complement}(S \cap S') = \dim^{\complement}(S) + \dim^{\complement}(S').$$

Demonstração. Corolário da proposição anterior. ■

Proposição 10.22. *Sejam $\boldsymbol{V}, \boldsymbol{V}'$ e $\boldsymbol{W}$ variedades diferenciais, $\boldsymbol{S} \subseteq \boldsymbol{V}'$ uma subvariedade diferencial e $F\colon V \times W \longrightarrow V''$, 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*

$$\begin{aligned} F_w\colon V &\longrightarrow V' \\ p &\longmapsto F(p, w). \end{aligned}$$

Exemplo 10.1. *Sejam* $f\colon \mathbb{R}^m \longrightarrow \mathbb{R}^n$ *suave e* $Z \subseteq \mathbb{R}^n$*. Defina*

$$\begin{aligned} f\colon \mathbb{R}^m \times \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ (x, v) &\longmapsto f(x) + v. \end{aligned}$$

$\mathrm{D}F_{(x_0,v_0)}(0, w) = \mathrm{D}(F_{x_0})_{v_0}(w) = w$*. 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 10.23. *Sejam* $S \subseteq N$ *subvariedade fechada. O conjunto*

$$\{f\colon M \longrightarrow N \mid f \pitchfork S\}$$

é aberto e denso.

10.6 Campos Tensoriais

10.6.1 Campos Tensoriais, Vetoriais, e Derivações

Definição 10.32. Seja $\boldsymbol{V}$ uma variedade diferencial. Um *campo tensorial* de tipo (k, l) em $\boldsymbol{V}$ é uma função

$$\begin{aligned} T\colon V &\longrightarrow \mathrm{T}V^{\otimes(k,l)} \\ p &\longmapsto T|_p \end{aligned}$$

tal que, para todo $p \in V$, $T|_p \in \mathrm{T}V^{\otimes(k,l)}|_p$. O conjunto dos campos tensoriais diferenciáveis[2] de tipo (k, l) em $\boldsymbol{V}$ 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 *campo vetorial* 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 $\mathrm{T}V|_p$: a soma é dada por

$$\begin{aligned} +\colon \mathfrak{T}^1(V) \times \mathfrak{T}^1(V) &\longrightarrow \mathfrak{T}^1(V) \\ (X, X') &\longmapsto X + X'\colon V \longrightarrow \mathrm{T}V \\ &\qquad\qquad\qquad\quad p \longmapsto X|_p + X'|_p. \end{aligned}$$

e o produto por escalar é dado por

$$\begin{aligned} \cdot\colon \mathbb{R} \times \mathfrak{T}^1(V) &\longrightarrow \mathfrak{T}^1(V) \\ (c, X) &\longmapsto cX\colon V \longrightarrow \mathrm{T}V \\ &\qquad\qquad\qquad\quad p \longmapsto cX|_p. \end{aligned}$$

[2] Aqui diferenciável quer dizer $\mathscr{C}^\infty$.

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:

$$\begin{aligned} \cdot\colon \mathfrak{T}^0(V) \times \mathfrak{T}^1(V) &\longrightarrow \mathfrak{T}^1(V) \\ (f, X) &\longmapsto fX\colon V \longrightarrow \mathrm{T}V \\ & \qquad\qquad p \longmapsto f(p)X|_p. \end{aligned}$$

Isso é uma ação do anel $\mathfrak{T}^0(V)$ que dá ao espaço $\mathfrak{T}^1(V)$ uma estrutura de módulo.

Proposição 10.24. *Seja $\boldsymbol{V}$ 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 10.25. *Sejam $\boldsymbol{V}$ uma variedade diferencial e $X\colon V \longrightarrow \mathrm{T}V$ um campo vetorial. O campo vetorial X é diferenciável*[3] *em $\boldsymbol{V}$ se, e somente se, para toda $f \in \mathfrak{T}^0(V)$,*

$$\begin{aligned} \partial_X f\colon V &\longrightarrow \mathbb{R} \\ p &\longmapsto X|_p f \end{aligned}$$

é uma função escalar diferenciável.

10.6.2 Derivações e Colchete de Campos Vetoriais

A proposição da seção anterior é equivalente a dizer que X induz uma função

$$\begin{aligned} \partial_X\colon \mathfrak{T}^0(V) &\longrightarrow \mathfrak{T}^0(V) \\ f &\longmapsto \partial_X f. \end{aligned}$$

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

$$\partial_X(ff')(p) = X|_p(ff') = X|_p(f)f'(p) + f(p)X|_p(f') = (\partial_X(f)f' + f\partial_X(f'))(p).$$

[3] Aqui diferenciável quer dizer $\mathscr{C}^\infty$. Não consideraremos os detalhes relacionados ao grau de regularidade do campo, mas eles podem ser definidos e estudados de modo análogo, substituindo $\mathscr{C}^\infty$ por $\mathscr{C}^k$.

Pode-se mostrar que existe uma bijeção entre o conjunto dos campos vetoriais diferenciáveis $\mathfrak{T}^1(V)$ e o conjunto das derivações $\mathrm{Der}(\mathfrak{T}^0(V))$. 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 o 'colchete de Lie'. Esse colchete dará, como comentado anteriormente, uma estrutura de álgebra sobre $\mathbb{R}$ a $\mathfrak{T}^1(V)$. O conjunto $\mathrm{Der}(\mathfrak{T}^0(V))$ 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 $\mathrm{Der}(\mathfrak{T}^0(V))$ 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 $\partial_X, \partial_{X'} \in \mathrm{Der}(\mathfrak{T}^0(V))$, o produto

$$[\partial_X, \partial_{X'}] := \partial_X \circ \partial_{X'} - \partial_{X'} \circ \partial_X.$$

Esse produto é uma derivação pela proposição 6.7. 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 10.26 (Colchete em Coordenadas Locais)**.** *Sejam $\boldsymbol{V}$ uma variedade diferencial e $X, Y \in \mathfrak{T}^1(V)$ campos vetoriais. Para toda carta (A, x) de $\boldsymbol{V}$, 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*

$$[X, Y] = \mathop{+}_{(i,j)\in[d]^2} \left(X^i \frac{\partial Y^j}{\partial x^i} - Y^i \frac{\partial X^j}{\partial x^i} \right) \frac{\partial}{\partial x^j}.$$

Demonstração. Basta notar que, para toda $f \in \mathfrak{T}^0(V)$

$$\begin{aligned}
[X,Y]\,f &= \mathop{+}_{i\in[d]} X^i \frac{\partial}{\partial x^i}\left(\mathop{+}_{j\in[d]} Y^j \frac{\partial f}{\partial x^j}\right) - \mathop{+}_{j\in[d]} Y^j \frac{\partial}{\partial x^j}\left(\mathop{+}_{i\in[d]} X^i \frac{\partial f}{\partial x^i}\right) \\
&= \mathop{+}_{(i,j)\in[d]^2}\left(X^i \frac{\partial Y^j}{\partial x^i}\frac{\partial f}{\partial x^j} + X^i Y^j \frac{\partial^2 f}{\partial x^i \partial x^j} - Y^j \frac{\partial X^i}{\partial x^j}\frac{\partial f}{\partial x^i} - Y^j X^i \frac{\partial^2 f}{\partial x^j \partial x^i}\right) \\
&= \mathop{+}_{(i,j)\in[d]^2}\left(X^i \frac{\partial Y^j}{\partial x^i} - Y^i \frac{\partial X^j}{\partial x^i}\right)\frac{\partial f}{\partial x^j},
\end{aligned}$$

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 10.27. *Seja* $\boldsymbol{V}$ *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 6.7.

2. Para toda $g \in \mathfrak{T}^0(V)$,

$$\begin{aligned}
[fX, f'X']\,g &= (fX)(f'X')g - (f'X')(fX)g \\
&= (fX)(f'X'g) - (f'X')(fXg) \\
&= (fX)(f')(X'g) + f'((fX)(X'g)) \\
&\qquad - (f'X')(f)(Xg) - f((f'X')(Xg)) \\
&= ff'\,[X,X']\,(g) + f(Xf')X'(g) - f'(X'f)X(g) \\
&= (ff'\,[X,X'] + f(Xf')X' - f'(X'f)X)\,(g).
\end{aligned}$$

■

10.6.3 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 $\boldsymbol{V}$:

$$\left(\mathfrak{T}^1(V)\right)^{\otimes(k,l)} = \mathfrak{T}^{(k,l)}(V).$$

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 $\boldsymbol{V}$

$$\mathfrak{T}^{\otimes}(V) := \bigoplus_{(k,l)\in\mathbb{N}^2} \mathfrak{T}^{(k,l)}(V).$$

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.

10.6.4 Fluxo de Campos Vetoriais

As demonstrações dessa serão omitidas, mas podem ser encontradas em *Introduction to Smooth Manifolds*, *John M. Lee*, segunda edição.

Consideremos uma curva diferenciável $\gamma\colon I \longrightarrow V$ definida em um intervalo aberto I. Como, para todo $t \in I$, $\mathrm{T}I|_t \simeq \mathbb{R}$, segue que sua diferencial em $t \in I$ é uma função $\mathrm{D}\gamma|_t \longrightarrow \mathrm{T}V|_{\gamma(t)}$. Mas então $\mathrm{D}\gamma$

Definição 10.33. Sejam $\boldsymbol{V}$ um variedade diferencial e $X \in \mathfrak{T}^1(V)$. Uma *curva integral de* X é uma curva diferenciável $\gamma\colon I \longrightarrow V$ tal que, para todo $t \in I$,

$$\dot{\gamma}(t) = X|_{\gamma(t)}.$$

Se $0 \in I$, $\gamma(0) \in M$ é o *ponto inicial* de γ e γ é *iniciada* em $\gamma(0)$.

Em coordenadas locais (A, x), a condição $\dot{\gamma}(t) = X|_{\gamma(t)}$ se torna

$$\dot{\gamma}^i(t)\frac{\partial}{\partial x^i}|_{\gamma(t)} = X^i(\gamma(t))\frac{\partial}{\partial x^i}|_{\gamma(t)},$$

que se reduz a um sistema autônomo de equações diferenciais parciais: para todo $i \in [d]$,

$$\dot{\gamma}^i(t) = X^i(\gamma^0(t), \ldots, \gamma^{d-1}(t)).$$

O teorema de existência, unicidade e diferenciabilidade garante que o sistema anterior tem solução única e diferenciável. Isso implica a seguinte proposição.

Proposição 10.28. *Sejam* $\boldsymbol{V}$ *um variedade diferencial e* $X \in \mathfrak{T}^1(V)$*. Para todo* $p \in V$*, existem* $\varepsilon \in \,]0, \infty[$ *e curva diferenciável* $\gamma\colon \,]-\varepsilon, \varepsilon[\, \longrightarrow V$ *que é curva integral de* X *iniciada em* p*.*

Proposição 10.29. *Sejam* $\boldsymbol{V}$ *um variedade diferencial,* $X \in \mathfrak{T}^1(V)$ *e* $\gamma\colon I \longrightarrow V$ *uma curva integral de* X*.*

1. *Para todo* $c \in \mathbb{R}$*, a curva*

$$\begin{aligned} \gamma \circ T_c\colon T_{-c}I &\longrightarrow V \\ t &\longmapsto \gamma(c+t) \end{aligned}$$

   é uma curva integral de X*;*

2. *Para todo* $c \in \mathbb{R} \smallsetminus \{0\}$*, a curva*

$$\begin{aligned} \gamma \circ E_c\colon E_{c^{-1}}I &\longrightarrow M \\ t &\longmapsto \gamma(ct) \end{aligned}$$

   é uma curva integral de cX*.*

Lembremos que um fluxo em um conjunto V é uma ação de $\mathbb{R}$ em X, uma função

$$\begin{aligned} \Phi\colon \mathbb{R} \times V &\longrightarrow V \\ (t, p) &\longmapsto \Phi^t(p) \end{aligned}$$

tal que

1. Para todo $p \in V$, $\Phi^0(p) = p$;
2. Para todos $p \in V$ e $t, t' \in \mathbb{R}$, $\Phi^{t+t'}(p) = \Phi^t(\Phi^{t'}(p))$.

Quando V tem topologia, podemos considerar um fluxo contínuo, e quando V é uma variedade diferencial V, podemos considerar fluxos diferenciáveis. Para todo $t \in \mathbb{R}$, a translação por t ao longo de Φ é

$$\begin{aligned} \Phi^t\colon V &\longrightarrow V \\ p &\longmapsto \Phi^t(p) \end{aligned}$$

e, para todo $p \in V$, a curva de fluxo de Φ iniciada em p é

$$\begin{aligned} \Phi_{(p)}\colon \mathbb{R} &\longrightarrow V \\ t &\longmapsto \Phi^t(p). \end{aligned}$$

Note que $\Phi^t\colon V \longrightarrow V$ é um difeomorfismo e $\Phi_{(p)}\colon \mathbb{R} \longrightarrow V$ é uma curva diferenciável.

Definição 10.34. Sejam $\boldsymbol{V}$ um variedade diferencial e $\Phi\colon \mathbb{R}\times V \longrightarrow V$ um fluxo diferenciável em $\boldsymbol{V}$. O *gerador infinitesimal de* Φ é o campo vetorial

$$\begin{aligned} X\colon V &\longrightarrow \mathrm{T}V \\ p &\longmapsto \dot{\Phi}_{(p)}(0). \end{aligned}$$

Proposição 10.30. *Sejam $\boldsymbol{V}$ um variedade diferencial e $\Phi\colon \mathbb{R}\times V \longrightarrow V$ um fluxo diferenciável em $\boldsymbol{V}$. O gerador infinitesimal X de Φ é um campo vetorial diferenciável e cada curva $\Phi_{(p)}\colon \mathbb{R}\longrightarrow V$ é uma curva integral de X.*

No entanto, nem todo campo vetorial diferenciável gera um fluxo porque nem toda curva integral está definida para todo $\mathbb{R}$. Para permitir que exista uma forma de recíproca para essa proposição, devemos expandir o conceito de fluxo com o conceito de um fluxo local.

Definição 10.35. Seja $\boldsymbol{V}$ um variedade diferencial. Um *domínio de fluxo local* em $\boldsymbol{V}$ é um conjunto aberto $\mathscr{D}\subseteq \mathbb{R}\times V$ que satisfaz: para todo $p\in V$, existem $e_p\in\,]-\infty,0[$ e $\bar{e}_p\in\,]0,\infty[$ tais que

$$]e_p,\bar{e}_p[\,=\{t\in\mathbb{R}\mid (t,p)\in\mathscr{D}\}\,.$$

Em particular, $0\in\,]e_p,\bar{e}_p[$. Podemos escrever

$$\mathscr{D}=\bigcup_{p\in V}\,]e_p,\bar{e}_p[\,\times\{p\}.$$

Definição 10.36. Seja $\boldsymbol{V}$ um variedade diferencial. Um *fluxo local* em $\boldsymbol{V}$ é uma função $\Phi\colon \mathscr{D}\longrightarrow V$, em que $\mathscr{D}$ um domínio de fluxo local em $\boldsymbol{V}$, e valem

1. Para todo $p\in V$,
$$\Phi^0(p)=p;$$
2. Para todos $p\in V$, $t\in\,]e_p,\bar{e}_p[$ e $t'\in\,]e_{\Phi^t(p)},\bar{e}_{\Phi^t(p)}[$ tal que $t+t'\in\,]e_p,\bar{e}_p[$,
$$\Phi^{t+t'}(p)=\Phi^t(\Phi^{t'}(p)).$$

Para todo $p\in V$, a *curva de fluxo* de Φ iniciada em p é a curva

$$\begin{aligned} \Phi_{(p)}\colon\,]e_p,\bar{e}_p[\,&\longrightarrow V \\ t &\longmapsto \Phi^t(p). \end{aligned}$$

Para todo $t\in\mathbb{R}$, a *translação* por t ao longo de Φ é a função

$$\begin{aligned} \Phi^t\colon V_t &\longrightarrow V \\ p &\longmapsto \Phi^t(p), \end{aligned}$$

em que $V_t:=\{p\in V\mid (t,p)\in\mathscr{D}\}$.

Temos as relações

$$p \in V_t \quad \Longleftrightarrow \quad t \in \,]e_p, \bar{e}_p[\quad \Longleftrightarrow \quad (t,p) \in \mathscr{D}.$$

Para ressaltar a diferença conceitual, às vezes chama-se um fluxo de *fluxo global*. Claro que, se Φ é um fluxo é um fluxo local em que, para todos $p \in V$ e $t \in \mathbb{R}$, $]e_p, \bar{e}_p[\,= \mathbb{R}$ e $V_t = V$. Assim como no caso do fluxo, um fluxo local pode ser contínuo ou diferenciável.

Definição 10.37. Sejam $\boldsymbol{V}$ um variedade diferencial e $\Phi\colon \mathscr{D} \longrightarrow V$ um fluxo local diferenciável em $\boldsymbol{V}$. O *gerador infinitesimal de* Φ é o campo vetorial

$$\begin{aligned} X\colon V &\longrightarrow \mathrm{T}V \\ p &\longmapsto \dot{\Phi}_{(p)}(0). \end{aligned}$$

Proposição 10.31. *Sejam $\boldsymbol{V}$ um variedade diferencial e $\Phi\colon \mathscr{D} \longrightarrow V$ um fluxo local diferenciável em V. O gerador infinitesimal X de Φ é um campo vetorial diferenciável e cada curva $\Phi_{(p)}\colon \mathbb{R} \longrightarrow V$ é uma curva integral de X.*

Definição 10.38. Seja $\boldsymbol{V}$ uma variedade diferencial.

1. Um *fluxo local máximo* em $\boldsymbol{V}$ é um fluxo local em $\boldsymbol{V}$ que não admite extensão para um domínio de fluxo local maior.

2. Uma *curva integral máxima* é uma curva integral de um campo vetorial que não admite extensão para um intervalo maior.

Proposição 10.32. *Sejam $\boldsymbol{V}$ um variedade diferencial e $X \in \mathfrak{T}^1(V)$. Existe único fluxo diferencial máximo $\Phi\colon \mathscr{D} \longrightarrow V$ gerado por X e o fluxo Φ satisfaz*

1. *Para todo $p \in V$, a curva de fluxo $\Phi_{(p)}\colon \,]e_p, \bar{e}_p[\longrightarrow V$ é uma curva integral máxima de X iniciada em p;*

2. *Para todo $p \in V$ e todo $t \in \,]e_p, \bar{e}_p[$,*

$$]e_{\Phi^t(p)}, \bar{e}_{\Phi^t(p)}[\,= \,]e_p, \bar{e}_p[\,- t = \{t' - t \mid t' \in \,]e_p, \bar{e}_p[\}\,;$$

3. *Para todo $t \in \mathbb{R}$, V_t é aberto em V e $\Phi^t\colon V_t \longrightarrow V_{-t}$ é um difeomorfismo com inversa Φ^{-t}.*

10.6.5 Espaço Cotangente

Dada uma variedade diferencial $\boldsymbol{V}$ e seu espaço

Definição 10.39. Sejam $\boldsymbol{V}$ uma variedade diferencial e $p \in V$. O *espaço cotangente* a $\boldsymbol{V}$ em p é

$$\mathrm{T}^*V|_p := (\mathrm{T}V|_p)^*,$$

o espaço linear dual do espaço tangente a $\boldsymbol{V}$ em p. O *fibrado cotangente* de $\boldsymbol{V}$ é

$$\mathrm{T}^*V := \bigsqcup_{p \in V} \mathrm{T}^*V|_p,$$

a união disjunta dos espaço tangentes a $\boldsymbol{V}$ em todos pontos de V.

Referencial Local Coordenado

Dada uma carta (A, x) de V, as funções $(\mathrm{d}x^i|_p)_{i \in [d]}$, definidas por

$$\begin{aligned} \mathrm{d}x^i|_p \colon \mathrm{T}V|_p &\longrightarrow \mathbb{R} \\ v &\longmapsto v(x^i) \end{aligned}$$

são uma base ordenada de $\mathrm{T}^*V|_p$. Essas funções são lineares porque, para todos $v, v' \in \mathrm{T}V|_p$ 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 $\mathrm{T}^*V|_p$ é a base dual de $\left(\frac{\partial}{\partial x^i}\Big|_p\right)_{i \in [d]}$, pois

$$\mathrm{d}x^i|_p \left(\frac{\partial}{\partial x^j}\bigg|_p \right) = \frac{\partial}{\partial x^j}\bigg|_p x^i = \partial_j (x^i \circ x^{-1})|_{x(p)} = \partial_j (\pi^i)|_{x(p)} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

10.6.6 Formas Diferenciáveis

O fibrado de k-covetores (k-tensores covariantes) de uma variedade diferencial $\boldsymbol{V}$ é $\mathrm{T}^*V^{\otimes k}$, e o subfibrado de tensores alternados desse fibrado é denotado

$$\bigwedge^k \mathrm{T}^*V := \bigsqcup_{p \in V} \bigwedge^k \mathrm{T}^*V|_p.$$

Uma seção desse fibrado é um campo de funcionais k-lineares alternados sobre $\boldsymbol{V}$. A próxima definição consiste desses objetos.

Definição 10.40. Seja $\boldsymbol{V}$ uma variedade diferencial. Uma *k-forma* em $\boldsymbol{V}$ é uma função

$$\omega\colon V \longrightarrow \bigwedge^k \mathrm{T}^*V$$

tal que, para todo $p \in V$, $\omega|_p \in \bigwedge^k \mathrm{T}^*V|_p$ é um funcional k-linear alternado de $\mathrm{T}V|_p$. O conjunto de k-formas diferenciáveis[4] em $\boldsymbol{V}$ 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 $\boldsymbol{V}$. Para $k = 0$, $\omega\wedge\omega'$ é simplesmente $\omega\omega'$, uma k'-forma.

A soma direta desses espaços é o espaço das formas em $\boldsymbol{V}$, denotado

$$\Omega(V) := \bigoplus_{i\in[d]} \Omega^k(V).$$

Esse espaço linear com o produto exterior

$$\begin{aligned} \wedge\colon \Omega(V) \times \Omega(V) &\longrightarrow \Omega(V) \\ (\omega, \omega') &\longmapsto \omega \wedge \omega' \end{aligned}$$

é uma álgebra associativa, anticomutativa e graduada.

Representação Coordenada

Seja $\omega \in \Omega^k(V)$. Como $\omega|_p$ é um k-covetor de $\mathrm{T}V|_p$ para cada $p \in V$, podemos escrevê-lo com respeito a uma base de $\mathrm{T}^*V|_p$. Uma carta (A, x) de $\boldsymbol{V}$ induz uma base $(\mathrm{d}x^i|_p)_{i\in[d]}$ de $\mathrm{T}^*V|_p$ para cada $p \in A$. Em coordenadas locais, portanto, o funcional k-linear alternado $\omega|_p$ pode ser escrito

$$\omega|_p = \mathop{+}_{i\in[d]^{\uparrow k}} \omega_i(p)\mathrm{d}x^i|_p$$

em que $[d]^{\uparrow k} := \left\{(i_0, \ldots, i_{k-1})_{j\in[k]} \in [d]^k \;\middle|\; i_0 < \cdots < i_{k-1}\right\}$ é um conjunto de multi-índices crescentes e, para cada multi-índice $i = (i_0, \ldots, i_{k-1}) \in [d]^{\uparrow k}$,

$$\mathrm{d}x^i|_p = \mathrm{d}x^{i_0}|_p \wedge \cdots \wedge \mathrm{d}x^{i_{k-1}}|_p.$$

Isso ocorre porque $(\mathrm{d}x^i|_p)_{i\in[d]^{\uparrow k}}$ é uma base de $\bigwedge^k \mathrm{T}^*V|_p$. A k-forma ω restrita a A pode ser escrita

$$\omega|_A = \mathop{+}_{i\in[d]^{\uparrow k}} \omega_i \mathrm{d}x^i.$$

[4] Aqui diferenciável quer dizer $\mathscr{C}^\infty$.

Proposição 10.33. *Seja $\boldsymbol{V}$ uma variedade diferencial. Uma k-forma $\omega \in \Omega^k(V)$ é diferenciável se, e somente se, para toda carta (A, x) de $\boldsymbol{V}$, as funções $\omega_i \colon A \longrightarrow \mathbb{R}$ tais que*

$$\omega|_A = \mathop{+}_{i \in [d]^{\uparrow k}} \omega_i \mathrm{d}x^i$$

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 10.41. Seja $\boldsymbol{V}$ uma variedade diferencial d-dimensional. Uma *forma volume* em $\boldsymbol{V}$ é uma forma $\omega \in \Omega^d(V)$ tal que, para todo $p \in V$, $\omega|_p \neq 0$.

Proposição 10.34. *Seja $\boldsymbol{V}$ uma variedade diferenciável. Então $\boldsymbol{V}$ é orientável se, e somente se, existe uma forma volume $\omega \in \Omega^d(V)$.*

Formas Puxadas

Definição 10.42. Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais, $F \colon V \longrightarrow V'$ uma função diferencial e $\omega \in \Omega^k(V')$ uma k-forma em $\boldsymbol{V}'$. A k-forma *puxada* de ω por F é a a k-forma

$$\begin{aligned} F^\star\omega \colon V &\longrightarrow \bigwedge^k \mathrm{T}^*V \\ p &\longmapsto F^\star\omega|_p \colon \mathrm{T}V|_p \times \cdots \mathrm{T}V|_p \longrightarrow \mathbb{R} \\ &\qquad\qquad (v_0, \ldots, v_{k-1}) \longmapsto \omega|_{F(p)}(\mathrm{D}F|_p v_0, \ldots, \mathrm{D}F|_p v_{k-1}). \end{aligned}$$

em $\boldsymbol{V}$.

A definição é equivalente a, para todo $p \in V$,

$$(F^\star\omega)|_p := (\mathrm{D}F|_p)^\star \omega|_{F(p)}.$$

Proposição 10.35. *Sejam $\boldsymbol{V}$ e $\boldsymbol{V}'$ variedades diferenciais e $F \colon V \longrightarrow V'$ uma função diferencial.*

1. *$F^\star \colon \Omega^k(V') \longrightarrow \Omega^k(V')$ é uma função linear;*
2. *Para todas formas $\omega \in \Omega^k(V')$ e $\omega' \in \Omega^{k'}(V')$,*
$$F^\star(\omega \wedge \omega') = (F^\star\omega) \wedge (F^\star\omega');$$
3. *Para toda carta (A, x) de $\boldsymbol{V}'$ e toda forma $\omega \in \Omega^k(V')$,*
$$F^\star\left(\mathop{+}_{I \in [d]^{\uparrow k}} \omega_I \mathrm{d}x^I\right) = \mathop{+}_{I \in [d]^{\uparrow k}} (\omega_I \circ F)\mathrm{d}(x \circ F)^I = \mathop{+}_{I \in [d]^{\uparrow k}} (F^\star\omega_I)\mathrm{d}(F^\star x)^I.$$

10.6.7 Derivada Exterior

Formas no Espaço Real

Definiremos nesta seção a derivada exterior de formas. Primeiro definiremos a derivada exterior de formas em $\mathbb{R}^d$. Consideremos um campo escalar $\omega\colon A \subseteq \mathbb{R}^d \longrightarrow \mathbb{R}$, 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 $\mathrm{D}\omega|_p\colon \mathbb{R}^d \longrightarrow \mathbb{R}$ (que é um funcional 1-linear alternado em $\mathbb{R}^d$) dada por

$$\mathrm{D}\omega|_p = \mathop{+}_{i\in[d]} \partial_i\omega(p)\mathrm{d}\pi^i|_p,$$

em que $\mathrm{d}\pi^i|_p := \mathrm{D}\pi^i|_p$ é a diferencial de $\pi^i\colon A \subseteq \mathbb{R}^d \longrightarrow \mathbb{R}$ em p, que é a funcional linear $e^i\colon \mathbb{R}^d \longrightarrow \mathbb{R}$. (O funcional e^i é o mesmo funcional que π^i — as notações diferem somente por causa do contexto ser diferente — e $\mathrm{d}\pi^i|_p = \pi^i$, pois π^i é linear.) Isso significa que

$$\mathrm{D}\omega = \mathop{+}_{i\in[d]} \partial_i\omega\mathrm{d}\pi^i$$

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 $I = (i_0, \ldots, i_{k-1}) \in [d]^{\uparrow k}$, define-se

$$\mathrm{d}\pi^I = \mathrm{d}\pi^{i_0} \wedge \cdots \wedge \mathrm{d}\pi^{i_{k-1}}.$$

Com isso em mente, definimos a derivada exterior de formas em $\mathbb{R}^d$.

Definição 10.43. 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

$$\omega := \mathop{+}_{I\in[d]^{\uparrow k}} \omega_I\mathrm{d}\pi^I,$$

sendo, para todo $I \in [d]^{\uparrow k}$, $\omega_I \in \mathscr{C}^\infty(A)$. A *derivada exterior* de ω é a $(k+1)$-forma

$$\mathrm{d}\omega := \mathop{+}_{I\in[d]^{\uparrow k}} \mathrm{d}\omega_I \wedge \mathrm{d}\pi^I,$$

em que, para todo $I \in [d]^{\uparrow k}$, $\mathrm{d}\omega_I := \mathrm{D}\omega_I$ é a diferencial de ω_I.

Exemplo 10.2. *Como já comentado, a derivada exterior de uma* 0*-forma* $\omega\colon A \subseteq \mathbb{R}^d \longrightarrow \mathbb{R}$ *é dada por*

$$\mathrm{d}\omega = \mathop{+}_{i\in[d]} \partial_i\omega\mathrm{d}\pi^i.$$

Note também que a derivada exterior de uma 1*-forma* $\omega = +_{i\in[d]}\,\omega_i \mathrm{d}\pi^i$ *é dada por*

$$\begin{aligned}
\mathrm{d}\omega &= \mathop{+}_{i\in[d]} \mathrm{d}\omega_i \wedge \mathrm{d}\pi^i \\
&= \mathop{+}_{i\in[d]} \left(\mathop{+}_{j\in[d]} \partial_j \omega_i(p) \mathrm{d}\pi^j \right) \wedge \mathrm{d}\pi^i \\
&= \mathop{+}_{(i,j)\in[d]^2} \partial_j \omega_i(p) \mathrm{d}\pi^j \wedge \mathrm{d}\pi^i \\
&= \mathop{+}_{i<j} \partial_j \omega_i(p) \mathrm{d}\pi^j \wedge \mathrm{d}\pi^i + \mathop{+}_{i>j} \partial_j \omega_i(p) \mathrm{d}\pi^j \wedge \mathrm{d}\pi^i \\
&= \mathop{+}_{i<j} (\partial_i \omega_j - \partial_j \omega_i) \mathrm{d}\pi^i \wedge \mathrm{d}\pi^j.
\end{aligned}$$

Notemos que a derivada exterior acima definida para cada $k \in [d]$ é uma função

$$\begin{aligned}
\mathrm{d}\colon \Omega^k(A) &\longrightarrow \Omega^{k+1}(A) \\
\omega &\longmapsto \mathrm{d}\omega
\end{aligned}$$

e, portanto, é uma função

$$\begin{aligned}
\mathrm{d}\colon \Omega(A) &\longrightarrow \Omega(A) \\
\omega &\longmapsto \mathrm{d}\omega.
\end{aligned}$$

ao definirmos que, para todas $\omega \in \Omega^k(A)$ e $\omega' \in \Omega^{k'}(A)$,

$$\mathrm{d}(\omega + \omega') := \mathrm{d}\omega + \mathrm{d}\omega'.$$

A derivada exterior satisfaz as seguintes propriedades.

Proposição 10.36. *Sejam* $d \in \mathbb{N}$ *e* $A \subseteq \mathbb{R}^d$ *um aberto. A derivada exterior* $\mathrm{d}\colon \Omega(A) \longrightarrow \Omega(A)$ *satisfaz*

1. d *é linear sobre* $\mathbb{R}$*;*

2. *Para todas formas* $\omega \in \Omega^k(A)$ *e* $\omega' \in \Omega^{k'}(A)$*,*

$$\mathrm{d}(\omega \wedge \omega') = \mathrm{d}\omega \wedge \omega' + (-1)^k \omega \wedge \mathrm{d}\omega';$$

3. $\mathrm{d} \circ \mathrm{d} = 0$*;*

4. *Para toda função diferenciável* $F\colon A \subseteq \mathbb{R}^d \longrightarrow A' \subseteq \mathbb{R}^{d'}$ *e toda forma* $\omega \in \Omega^k(A')$*,*

$$F^\star(\mathrm{d}\omega) = \mathrm{d}(F^\star\omega).$$

Demonstração. 1. Sejam $\omega, \omega' \in \Omega^k(A)$ e $c \in \mathbb{R}$. Então

$$c\omega + \omega' = \mathop{+}_{I \in [d]^{\uparrow k}} (c\omega_I + \omega'_I) \wedge \mathrm{d}\pi^I,$$

portanto

$$\begin{aligned}
\mathrm{d}(c\omega + \omega') &= \mathrm{d}\left(\mathop{+}_{I \in [d]^{\uparrow k}} (c\omega_I + \omega'_I) \wedge \mathrm{d}\pi^I \right) \\
&= \mathop{+}_{I \in [d]^{\uparrow k}} \mathrm{d}(c\omega_I + \omega'_I) \wedge \mathrm{d}\pi^I \\
&= \mathop{+}_{I \in [d]^{\uparrow k}} (c\mathrm{d}\omega_I + \mathrm{d}\omega'_I) \wedge \mathrm{d}\pi^I \\
&= c \mathop{+}_{I \in [d]^{\uparrow k}} \mathrm{d}\omega_I \wedge \mathrm{d}\pi^I + \mathop{+}_{I \in [d]^{\uparrow k}} \mathrm{d}\omega'_I \wedge \mathrm{d}\pi^I \\
&= c\mathrm{d}\omega + \mathrm{d}\omega'.
\end{aligned}$$

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 $f\mathrm{d}\pi^i \in \Omega^k(A)$ e $f'\mathrm{d}\pi^{I'} \in \Omega^{k'}(A)$, em que $f, f' \in \mathscr{C}^\infty(A)$ são campos escalares, pois por linearidade a propriedade valerá para todas formas. Temos que mostrar que $\mathrm{d}(f\mathrm{d}\pi^I) = \mathrm{d}f \wedge \mathrm{d}\pi^I$ para todo multi-índice $I \in [d]^k$, não somente os crescentes $I \in [d]^{\uparrow k}$. Se I tem alguma entrada repetida, $\mathrm{d}\pi^I = 0$, portanto $\mathrm{d}(f\mathrm{d}\pi^I) = 0 = \mathrm{d}f \wedge \mathrm{d}\pi^I$. Caso contrário, existe permutação $\sigma \in [k]$ tal que $\sigma(I) = (i_{\sigma(0)}, \ldots, i_{\sigma(k-1)})$ é um multi-índice crescente, portanto

$$\mathrm{d}(f\mathrm{d}\pi^I) = \mathrm{d}(\epsilon(\sigma) f \mathrm{d}\pi^{\sigma(I)}) = \epsilon(\sigma)\mathrm{d}f \wedge \mathrm{d}\pi^{\sigma(I)} = \mathrm{d}f \wedge \mathrm{d}\pi^I.$$

Assim, segue que

$$\begin{aligned}
\mathrm{d}((f\mathrm{d}\pi^I) \wedge (f'\mathrm{d}\pi^{I'})) &= \mathrm{d}(ff'\mathrm{d}\pi^I \wedge \mathrm{d}\pi^{I'}) \\
&= \mathrm{d}(ff'\mathrm{d}\pi^I \wedge \mathrm{d}\pi^{I'}) \\
&= ((\mathrm{d}f)f' + f\mathrm{d}f') \wedge \mathrm{d}\pi^I \wedge \mathrm{d}\pi^{I'} \\
&= (\mathrm{d}f)f' \wedge \mathrm{d}\pi^I \wedge \mathrm{d}\pi^{I'} + f\mathrm{d}f' \wedge \mathrm{d}\pi^I \wedge \mathrm{d}\pi^{I'} \\
&= (\mathrm{d}f \wedge \mathrm{d}\pi^I) \wedge (f'\mathrm{d}\pi^{I'}) + (-1)^k (f\mathrm{d}\pi^I) \wedge (\mathrm{d}f' \wedge \mathrm{d}\pi^{I'}) \\
&= \mathrm{d}(f\mathrm{d}\pi^I) \wedge (f'\mathrm{d}\pi^{I'}) + (-1)^k (f\mathrm{d}\pi^I) \wedge \mathrm{d}(f'\mathrm{d}\pi^{I'}),
\end{aligned}$$

pois $\mathrm{d}f' \wedge \mathrm{d}\pi^I = (-1)^k \mathrm{d}\pi^I \wedge \mathrm{d}f'$.

3. Provaremos primeiros para 0-formas. Para $f \in \Omega^0(A)$,

$$\begin{aligned} \mathrm{d}(\mathrm{d}f) &= \mathrm{d}\left(\mathop{+}_{i\in[d]} \mathrm{D}_i f \mathrm{d}\pi^i \right) \\ &= \mathop{+}_{i<j} (\mathrm{D}_{i,j} f - \mathrm{D}_{j,i} f) \mathrm{d}\pi^i \wedge \mathrm{d}\pi^j \\ &= 0, \end{aligned}$$

pois $\mathrm{D}_{i,j} f = \mathrm{D}_{j,i} f$. Agora, para uma k-forma $\omega \in \Omega^k(A)$, segue do resultado anterior e do item anterior que

$$\begin{aligned} \mathrm{d}(\mathrm{d}\omega) &= \mathrm{d}\left(\mathop{+}_{I\in[d]^{\uparrow k}} \mathrm{d}\omega_I \wedge \mathrm{d}\pi^I \right) \\ &= \mathop{+}_{I\in[d]^{\uparrow k}} \mathrm{d}(\mathrm{d}\omega_I) \wedge \mathrm{d}\pi^I \\ &\quad + \mathop{+}_{I\in[d]^{\uparrow k}} \mathop{+}_{j\in[k]} (-1)^j \mathrm{d}\omega_I \wedge \mathrm{d}\pi^{i_0} \wedge \cdots \wedge \mathrm{d}(\mathrm{d}\pi^{i_j}) \wedge \cdots \wedge \mathrm{d}\pi^{i_{k-1}} \\ &= 0. \end{aligned}$$

4. Novamente, basta considerar $f\mathrm{d}\pi^I \in \Omega^k(A')$, pois $F^\star$ é linear. Da definição de forma puxada, segue que

$$\begin{aligned} F^\star(\mathrm{d}(f\mathrm{d}\pi^I)) &= F^\star(\mathrm{d}f \wedge \mathrm{d}\pi^I) \\ &= \mathrm{d}(f \circ F) \wedge \mathrm{d}(\pi^{i_0} \circ F) \wedge \cdots \mathrm{d}(\pi^{i_{k-1}} \circ F) \\ &= \mathrm{d}((f \circ F)\mathrm{d}(\pi^{i_0} \circ F) \wedge \cdots \mathrm{d}(\pi^{i_{k-1}} \circ F)) \\ &= \mathrm{d}(F^\star(f\mathrm{d}\pi^I)). \end{aligned}$$

■

Formas em Variedades Diferenciais

Estendemos agora a definição da derivada exterior de formas para variedades diferenciais quaisquer.

Proposição 10.37. *Seja* $\boldsymbol{V}$ *uma variedade diferencial. Existe única função*

$$\mathrm{d}\colon \Omega(V) \longrightarrow \Omega(V)$$

tal que

1. *Para todo* $k \in [\dim V]$, $\mathrm{d}\colon \Omega^k(V) \longrightarrow \Omega^{k+1}(V)$ *é linear sobre* $\mathbb{R}$*;*

2. *Para todas formas* $\omega \in \Omega^k(V)$ *e* $\omega' \in \Omega^{k'}(V)$,

$$\mathrm{d}(\omega \wedge \omega') = \mathrm{d}\omega \wedge \omega' + (-1)^k \omega \wedge \mathrm{d}\omega';$$

3. $\mathrm{d} \circ \mathrm{d} = 0$;

4. *Para todo campo escalar* $f \in \mathscr{C}^\infty(V) = \Omega^0(V)$, *a diferencial* $\mathrm{D}f$ *de* f *é a derivada exterior* $\mathrm{d}f$ *de* f, *dada por* $\mathrm{d}f(X) = \partial_X f$.

10.6.8 Derivada de Lie

10.7 Orientação

10.7.1 Orientação de Espaços Lineares

Denotaremos como $\mathcal{B}(L)$ o conjunto de bases ordenadas de $\boldsymbol{L}$, ou seja,

$$\mathcal{B}(L) := \left\{ b \in L^d \;\middle|\; L = \langle b \rangle \right\}.$$

Definição 10.44. Seja $\boldsymbol{L}$ um espaço linear finito sobre um corpo $\boldsymbol{C}$. Duas bases ordenadas $b, b' \in \mathcal{B}(L)$ são *coorientadas* se, e somente se,

$$\det[\mathrm{I}]^b_{b'} > 0,$$

em que $[\mathrm{I}]^b_{b'}$ é a mudança de base de b para b'.

Proposição 10.38. *Seja* $\boldsymbol{L}$ *um espaço linear finito sobre um corpo* $\boldsymbol{C}$. *A relação de coorientação de bases ordenadas em* $\mathcal{B}(L)$ *é uma relação de equivalência.*

Demonstração. (Reflexividade) Seja b uma base ordenada de $\boldsymbol{L}$. Como $[\mathrm{I}]^b_b = \mathrm{I}$, segue que $\det[\mathrm{I}]^b_b = \det \mathrm{I} = 1 > 0$, portanto b é coorientada consigo mesma. (Simetria) Sejam b e b' bases ordenadas de $\boldsymbol{L}$ tais que b e b' são coorientadas. Isso significa que $\det[\mathrm{I}]^b_{b'} > 0$. Mas como $[\mathrm{I}]^{b'}_b = ([\mathrm{I}]^b_{b'})^{-1}$, segue que

$$\det[\mathrm{I}]^{b'}_b = \det(([\mathrm{I}]^b_{b'})^{-1}) = (\det[\mathrm{I}]^b_{b'})^{-1} > 0,$$

portanto b' e b são coorientadas. (Transitividade) Sejam b, b' e b'' bases ordenadas de $\boldsymbol{L}$ tais que b e b' são coorientadas e b' e b'' são coorientadas. Isso significa que $\det[\mathrm{I}]^b_{b'} > 0$ e $\det[\mathrm{I}]^{b'}_{b''} > 0$. Como $[\mathrm{I}]^b_{b''} = [\mathrm{I}]^b_{b'} \circ [\mathrm{I}]^{b'}_{b''}$, segue que

$$\det[\mathrm{I}]^b_{b''} = \det([\mathrm{I}]^b_{b'} \circ [\mathrm{I}]^{b'}_{b''}) = \det[\mathrm{I}]^b_{b'} \det[\mathrm{I}]^{b'}_{b''} > 0,$$

logo b e b'' são coorientadas. ■

Isso permite que se quociente o espaço de bases ordenadas de $\boldsymbol{L}$ em classes de equivalências, e esse quociente é o conjunto de classes de bases coorientadas de $\boldsymbol{L}$, definido a seguir.

Definição 10.45. Sejam $\boldsymbol{L}$ um espaço linear finito sobre um corpo $\boldsymbol{C}$ e b uma base ordenada de $\boldsymbol{L}$. A *classe de orientação* gerada por b é o conjunto

$$[b] = \left\{ b' \in \mathcal{B}(L) \;\middle|\; \det[\mathrm{I}]_{b'}^{b} > 0 \right\}.$$

O conjunto dessas classes de equivalência é denotado $[\mathcal{B}(L)]$. Uma *orientação* de $\boldsymbol{L}$ é uma função injetiva

$$O\colon [\mathcal{B}(L)] \longrightarrow \{+1, -1\}$$

O conjunto de orientações de $\boldsymbol{L}$ 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 $\boldsymbol{L}$ 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 10.39. *Seja $\boldsymbol{L}$ um espaço linear finito sobre um corpo $\boldsymbol{C}$. 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 $\boldsymbol{L}$ 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 $b = (b_0, \ldots, b_{d-1})$ uma base ordenada de $\boldsymbol{L}$. Definimos a base $\bar{b} := (-b_0, \ldots, b_{d-1})$. Mostraremos que as únicas classes de orientação de $\boldsymbol{L}$ são $[b]$ e $[\bar{b}]$. Seja b' uma base de $\boldsymbol{L}$. Se

$\det[\mathrm{I}]^b_{b'} > 0$, então $[b'] = [b]$; caso contrário, $\det[\mathrm{I}]^b_{b'} < 0$. Mas

$$\begin{aligned}\det[\mathrm{I}]^b_{b'} &= \det\begin{bmatrix} \vdots & & \vdots \\ [b_0]_{b'} & \cdots & [b_{d-1}]_{b'} \\ \vdots & & \vdots \end{bmatrix} \\ &= -\det\begin{bmatrix} \vdots & & \vdots \\ [-b_0]_{b'} & \cdots & [b_{d-1}]_{b'} \\ \vdots & & \vdots \end{bmatrix} \\ &= -\det[\mathrm{I}]^{\bar{b}}_{b'},\end{aligned}$$

portanto $\det[\mathrm{I}]^{\bar{b}}_{b'} > 0$, o que mostra que $b' \in [\bar{b}]$. Isso implica que só existem duas orientações de $\boldsymbol{L}$, pois da injetividade segue que $O([b]) = +1$ e $O([\bar{b}]) = -1$, ou $O([b]) = -1$ e $O([\bar{b}]) = +1$. Logo $|\mathcal{O}(L)| = 2$. ■

A orientação canônica em $\mathbb{R}^d$ é a função O definida por $O([e_0, \ldots, e_{d-1}]) = +1$ e $O([-e_0, \ldots, e_{d-1}]) = -1$.

Aritmética de Orientações

Definimos a orientação de um isomorfismo linear $f\colon L \longrightarrow L$ por

$$O(f) := \frac{\det f}{|\det f|}.$$

Essa é uma função $O\colon \mathcal{L}(L) \longrightarrow \{+1, -1\}$. 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 $\boldsymbol{L}$ coorientadas e todo isomorfismo $f \in \mathcal{L}(L)$,

$$f[b_0, \ldots, b_{d-1}] := [f(b_0), \ldots, f(b_{d-1})].$$

Isso está bem definido. Assim, segue que, para toda base ordenada b de $\boldsymbol{L}$,

$$O(f[b]) = O(f)O([b]).$$

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 $(-1)^1 = -1$.

10.7.2 Orientação de Variedades

Definição 10.46. Seja $\boldsymbol{V}$ uma variedade diferencial. Uma *orientação* de $\boldsymbol{V}$ é uma função

$$O\colon V \longrightarrow \bigcup_{p\in V} \mathcal{O}(\mathrm{T}V|_p)$$

tal que

1. Para todo $p \in V$, $O|_p\colon [\mathcal{B}(\mathrm{T}V|_p)] \longrightarrow \{+1, -1\}$ é uma orientação de $\mathrm{T}V|_p$;
2. Para todo $\bar{p} \in V$, existe um referencial local diferenciável $(B_i)_{i\in[d]}$ de $\boldsymbol{V}$ em uma vizinhança $A \subseteq V$ de $\bar{p}$ tal que, para todos $p, p' \in A$,

$$O|_p([B_0|_p, \ldots, B_{d-1}|_p]) = O|_{p'}([B_0|_{p'}, \ldots, B_{d-1}|_{p'}]).$$

Uma variedade diferencial *orientável* é uma variedade diferencial que admite uma orientação $\mathcal{O}$.

Atlas Orientados

Definição 10.47. Seja $\boldsymbol{V}$ uma variedade diferencial. Duas cartas (A, x), (A', x') de $\boldsymbol{V}$ são *coorientadas* se, e somente se, para todo $p \in A \cap A'$,

$$\det(\mathrm{D}(x' \circ x^{-1})|_p) > 0.$$

Caso contrário, elas são *contraorientadas*, e existe $p \in A \cap A'$ tal que

$$\det(\mathrm{D}(x' \circ x^{-1})|_p) < 0.$$

O caso em que $\det(\mathrm{D}(x' \circ x^{-1})|_p) = 0$ não ocorre, pois as cartas são diferencialmente compatíveis, o que implica que a transição de coordenadas é um difeomorfismo, logo $\mathrm{D}(x' \circ x^{-1})(p)\colon \mathbb{R}^d \longrightarrow \mathbb{R}^d$ é invertível.

Definição 10.48. 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 atlas é uma relação de equivalência.

Proposição 10.40. *Seja $\boldsymbol{V}$ uma variedade diferencial orientável com n componentes conexas. Então*

$$|\mathcal{O}(V)| = 2^n.$$

10.8 Grupos Diferenciais

Definição 10.49. Um *grupo diferencial* é um par $(\boldsymbol{G}, \cdot)$ em que $\boldsymbol{G}$ é uma variedade diferencial, $(G, \cdot)$ é um grupo e as operações

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

são funções diferenciáveis.

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

10.9 Folheações

As definições e os principais resultados desta seção são baseados no livro *Foliations I*, Candel/Conlon.

10.9.1 Cartas e Atlas Folheados

Definição 10.50. Seja $d \in \mathbb{N}$. Um *retângulo aberto* d-dimensional é um conjunto $R \subseteq \mathbb{R}^d$ tal que, para intervalos abertos $I_0, \ldots, I_{d-1} \subseteq \mathbb{R}$,

$$R = I_0 \times \cdots \times I_{d-1}.$$

Definição 10.51. Sejam $\boldsymbol{V} = (V, \mathcal{A})$ uma variedade $\mathscr{C}^r$ d-dimensional e $k \in [d]$. Uma *carta k-folheada* (ou *k-dimensionalmente folheada*) de $\boldsymbol{V}$ é uma carta $(A, x) \in \mathcal{A}$ para a qual existem retângulos abertos $B_{\pitchfork} \subseteq \mathbb{R}^k$ e $B_{\pitchfork} \subseteq \mathbb{R}^{d-k}$ tais que

$$x(A) = B_{\pitchfork} \times B_{\pitchfork}.$$

Para todo $y \in B_{\pitchfork}$, a *placa* (*tangencial*) de (A, x) relativa a y é o conjunto $P_y = x^{-1}(B_{\pitchfork} \times \{y\}) \subseteq A$; para todo $x \in B_{\pitchfork}$, a (*seção*) *transversal* de (A, x) relativa a x é o conjunto $P_x = x^{-1}(\{x\} \times B_{\pitchfork}) \subseteq A$.

Os símbolos $\pitchfork$ e $\pitchfork$ são lidos *tangente* e *transverso*, respectivamente.

Proposição 10.41. *Seja $\boldsymbol{V} = (V, \mathcal{A})$ uma variedade $\mathscr{C}^r$ d-dimensional e $(A, x) \in \mathcal{A}$ uma carta k-folheada de $\boldsymbol{V}$. As placas $\{P_y\}_{y \in B_{\pitchfork}}$ são uma partição do domínio A de (A, x).*

Demonstração. Para mostrar isso, primeiro notamos que $P_y = x^{-1}(B_{\sqcap} \times \{y\}) \neq \emptyset$, pois x é sobrejetiva. Segundo, como $x(A) = B_{\sqcap} \times B_{\pitchfork}$, então

$$\begin{aligned} A &= x^{-1}(B_{\sqcap} \times B_{\pitchfork}) \\ &= x^{-1}\left(B_{\sqcap} \times \bigcup_{y \in B_{\pitchfork}} \{y\}\right) \\ &= \bigcup_{y \in B_{\pitchfork}} x^{-1}(B_{\sqcap} \times \{y\}) \\ &= \bigcup_{y \in B_{\pitchfork}} P_y. \end{aligned}$$

Por fim, notemos que, para todos $y, y' \in B_{\pitchfork}$, temos

$$\begin{aligned} P_y \cap P_{y'} &= x^{-1}(B_{\sqcap} \times \{y\}) \cap x^{-1}(B_{\sqcap} \times \{y'\}) \\ &= x^{-1}(B_{\sqcap} \times \{y\} \cap B_{\sqcap} \times \{y'\}) \\ &= x^{-1}(B_{\sqcap} \times (\{y\} \cap \{y'\})). \end{aligned}$$

portanto, se $y = y'$, $P_y = P_{y'}$ e, se $y \neq y'$, $P_y \cap P_{y'} = \emptyset$. ■

Definição 10.52. Seja $\boldsymbol{V} = (V, \mathcal{A})$ uma variedade $\mathscr{C}^r$ d-dimensional. Cartas folheadas de $\boldsymbol{V}$ *coerentemente folheadas* são cartas folheadas $(A, x), (A', x') \in \mathcal{A}$ tais que, para todas placas P de (A, x) e P' de (A', x'), a interseção $P \cap P'$ é aberta em P e em P'. Denota-se $(A, x) \approx (A', x')$.

Por definição, as cartas têm que ser ambas folheadas com placas de mesma dimensão caso tenham interseção não vazia, caso contrário a interseção de duas placas não seria aberta na placa de dimensão maior. Note que a relação de coerência de folheação é simétrica por definição e é reflexiva pois, para todos $y, y' \in B_{\pitchfork}$ com placas relativas $P_y, P_{y'} \subseteq A$ de uma carta folheada (A, x), temos $P_y = P_{y'}$, se, e somente se, $y = y'$, logo $P_y \cap P_{y'}$ é P_y se $y = y'$, ou $\emptyset$ se $y \neq y'$. Como P_y é aberto em si mesmo e $\emptyset$ é aberto, segue que (A, x) é coerentemente folheada consigo mesma. Para mostrar que a relação é transitiva, no entanto, precisamos de um atlas de cartas coerentemente folheadas.

Definição 10.53. Seja $\boldsymbol{V} = (V, \mathcal{A})$ uma variedade $\mathscr{C}^r$ d-dimensional. Um *atlas k-folheado*[5] de $\boldsymbol{V}$ é um subatlas $\mathcal{A}' \subseteq \mathcal{A}$ cujas cartas são cartas k-folheadas e coerentemente folheadas duas a duas.

Definição 10.54. Seja $\boldsymbol{V}$ uma variedade $\mathscr{C}^r$ d-dimensional. Atlas *coerentemente folheados* de $\boldsymbol{V}$ são atlas folheados $\mathcal{A}$ e $\mathcal{A}'$ de $\boldsymbol{V}$ tais que todas cartas $(A, x) \in \mathcal{A}$ e $(A', x') \in \mathcal{A}'$ são coerentemente folheadas. Denota-se $\mathcal{A} \approx \mathcal{A}'$.

[5] Novamente, ou *k-dimensionalmente folheado.*

Essa definição é equivalente a dizer que $\mathcal{A} \cup \mathcal{A}$ é um atlas folheado.

Proposição 10.42. *Seja $\boldsymbol{V}$ uma variedade $\mathscr{C}^r$ d-dimensional. A relação de coerência de folheação de atlas é uma relação de equivalência.*

Demonstração. A reflexividade e a simetria são evidentes, pois valem entre cartas folheadas. Para conferir a transitividade, basta mostrar que, se $\mathcal{A} = \{(A_i, x_i)\}_{i \in I}$ é um atlas k-folheado de $\boldsymbol{V}$ e $(A, x), (A', x')$ são cartas k-folheadas de $\boldsymbol{V}$ que são coerentemente folheadas com cada carta de $\mathcal{A}$, então as cartas (A, x) e (A', x') são coerentemente folheadas. Sejam P e P' placas de (A, x) e (A', x'), respectivamente. Se $P \cap P' = \emptyset$, $P \cap P'$ é aberto em P e em P'. Caso contrário, seja $p \in P \cap P'$. Como $\mathcal{A}$ é atlas, existe $i \in I$ tal que $p \in A_i$. Seja Q_p a placa de (A_i, x) tal que $p \in Q_p$. Como $(A, x) \approx (A_i, x_i)$, segue que $P \cap Q_p$ é aberto em P e em Q_p e, como $(A_i, x_i) \approx (A', x')$ que $Q_p \cap P'$ é aberto em Q_p e em P'. Assim, segue que $P \cap Q_p \cap P'$ é aberto em Q_p e, por uma mudança de parametrização, segue que é aberto em P e em P' também. Como

$$P \cap P' = \bigcup_{p \in P \cap P'} P \cap Q_p \cap P',$$

concluímos que $P \cap P'$ é aberto em P e em P', pois é união de abertos. Portanto $(A, x) \approx (A', x')$, o que mostra que $\mathcal{A} \approx \mathcal{A}'$. ■

10.9.2 Componentes Tangencial e Transversal da Carta

Definição 10.55. Sejam $\boldsymbol{V} = (V, \mathcal{A})$ uma variedade $\mathscr{C}^r$ d-dimensional e $(A, x) \in \mathcal{A}$ uma carta k-folheada de $\boldsymbol{V}$. A *projeção tangencial* de (A, x) é a projeção canônica $\mathrm{p}_{\pitchfork}\colon B_{\pitchfork} \times B_{\pitchfork} \longrightarrow B_{\pitchfork}$ e a *componente tangencial* de x é a função $x_{\pitchfork} := \mathrm{p}_{\pitchfork} \circ x\colon A \longrightarrow B_{\pitchfork}$. A *projeção transversal* de (A, x) é a projeção canônica $\mathrm{p}_{\pitchfork}\colon B_{\pitchfork} \times B_{\pitchfork} \longrightarrow B_{\pitchfork}$ e a *componente transversal* de x é a função $x_{\pitchfork} := \mathrm{p}_{\pitchfork} \circ x\colon A \longrightarrow B_{\pitchfork}$.

Mostraremos uma equivalência da definição de coerência de folheação que será útil.

Proposição 10.43. *Sejam $\boldsymbol{V} = (V, \mathcal{A})$ uma variedade $\mathscr{C}^r$ d-dimensional e (A, x), $(A', x') \in \mathcal{A}$ cartas k-folheadas de $\boldsymbol{V}$. As cartas são coerentemente folheadas se, e somente se, todo ponto $p \in A \cap A'$ tem vizinhança em que a transição de coordenadas*

$$x' \circ x^{-1}\colon x(A \cap A') \longrightarrow x'(A \cap A')$$

satisfaz, para todo $(p, q) \in x(A \cap A')$, com $p \in \mathbb{R}^k$ e $q \in \mathbb{R}^{d-k}$,

$$x' \circ x^{-1}(p, q) = (h_{\pitchfork}(p, q), h_{\pitchfork}(q)) \in \mathbb{R}^k \times \mathbb{R}^{d-k}.$$

Demonstração. (De Candel e Conlon) Suponhamos que as cartas são coerentemente folheadas. Consideremos em $x(A \cap A')$ a mudança de coordenadas

$$x' \circ x^{-1}(p,q) = (x'_{\pitchfork} \circ x^{-1}(p,q), x'_{\pitchfork} \circ x^{-1}(p,q)).$$

Sejam P placa de (A,x) e P' placa de (A',x'). Como as cartas são coerentemente folheadas, as componentes conexas de $P \cap A'$ estão contidas em placas de A', e o mesmo vale para P'. Equivalentemente, como as placas P e P' são conjuntos de nível de y e y', respectivamente, cada ponto em $A \cap A'$ tem vizinhança em que vale

$$x'_{\pitchfork} \circ x^{-1}(p,q) = x'_{\pitchfork} \circ x^{-1}(p',q),$$

ou seja, $x'_{\pitchfork} \circ x^{-1}$ independe de $B_{\pitchfork}$. Definindo $h_{\pitchfork}(p,q) := x'_{\pitchfork} \circ x^{-1}(p,q)$ e $h_{\pitchfork}(q) = x'_{\pitchfork} \circ x^{-1}(p,q)$ para qualquer p, segue o resultado. A recíproca fica como exercício. ■

10.9.3 Folheação

Definição 10.56. Seja $\boldsymbol{V}$ uma variedade $\mathscr{C}^r$ d-dimensional. Uma *k-folheação* de $\boldsymbol{V}$ é uma partição $\mathcal{F}$ de V em subvariedades k-dimensionais imersas[6] de V, as *folhas* de $\mathcal{F}$, para a qual existe atlas k-folheado $\mathcal{A}_{\mathcal{F}}$ de V satisfazendo que, para toda carta folheada $(A,x) \in \mathcal{A}_{\mathcal{F}}$ e toda $F \in \mathcal{F}$, $F \cap A$ é uma união de placas de $\mathcal{A}_{\mathcal{F}}$.

Proposição 10.44. *Sejam $\boldsymbol{V}$ uma variedade $\mathscr{C}^r$ d-dimensional e $\mathcal{F}$ uma k-folheação de $\boldsymbol{V}$. As folhas de $\mathcal{F}$ são conexas.*

Definições Alternativas

Folheações (Baseado em Camacho)

Definição 10.57. Seja $\boldsymbol{V}$ uma variedade $\mathscr{C}^r$ d-dimensional. Uma *folheação $\mathscr{C}^s$* k-dimensional de $\boldsymbol{V}$ (para $s \leq r$ e $k \leq d$) é um atlas $\mathscr{C}^s$ $\mathcal{F}$ de $\boldsymbol{V}$ que é maximal segundo as propriedades:

1. Para toda carta $(A,x) \in \mathcal{F}$, existem bolas abertas $B_{\pitchfork} \subseteq \mathbb{R}^k$ e $B_{\pitchfork} \subseteq \mathbb{R}^{d-k}$ tais que
$$x(A) = B_{\pitchfork} \times B_{\pitchfork};$$
2. Para todas cartas (A,x) e $(A',x') \in \mathcal{F}$, a transição de coordenadas
$$x' \circ x^{-1} \colon x(A \cap A') \longrightarrow x'(A \cap A')$$
satisfaz
$$x' \circ x^{-1}(x,y) = (h_{\pitchfork}(x,y), h_{\pitchfork}(y)) \in \mathbb{R}^k \times \mathbb{R}^{d-k}$$
para todo $(x,y) \in x(A \cap A')$, com $x \in \mathbb{R}^k$ e $y \in \mathbb{R}^{d-k}$.

[6] Isso quer dizer que a subvariedade é imagem de uma imersão injetiva em V.

Nesse caso, a variedade $\boldsymbol{V}$ é *folheada* por $\mathcal{F}$ e as cartas de $\mathcal{F}$ são *cartas de folheação.*

Definição 10.58. Sejam $\boldsymbol{V}$ uma variedade $\mathscr{C}^r$ d-dimensional, $\mathcal{F}$ uma folheação $\mathscr{C}^s$ k-dimensional de $\boldsymbol{V}$, $(A, x) \in \mathcal{F}$ uma carta de folheação e $x(A) = B_{\pitchfork} \times B_{\pitchfork}$. Uma *placa* de $\mathcal{F}$ baseada em (A, x) é um conjunto

$$P_c = x^{-1}(B_{\pitchfork} \times \{c\}),$$

em que $c \in B_{\pitchfork}$.

Proposição 10.45. *1. A função*

$$x^{-1}|_{B_{\pitchfork} \times \{c\}} \colon B_{\pitchfork} \times \{c\} \longrightarrow A$$

é um mergulho $\mathscr{C}^r$. Portanto as placas são subvariedades $\mathscr{C}^r$ k-dimensionais.

2. As placas baseadas em (A, x) são disjuntas duas a duas.

Folheações (Baseado em R. Bowen e B. Marcus, Unique Ergodicity for Horocycle Foliations)

Definição 10.59. Sejam X uma variedade topológica d-dimensional, $x \in X$ e $\mathcal{F}$ uma partição de X em subvariedades conexas de X. Um conjunto *k-transversal* a $\mathcal{F}$ em x é uma vizinhança compacta K de x (de $\dim^{\complement}{}_X(K) = n = d - k$) satisfazendo que

1. Existe uma função contínua injetiva $\phi \colon K \times \mathbb{B}^n \longrightarrow X$ tal que $\phi(K \times \mathbb{B}^n)$ é uma vizinhança[7] de x;

2. Para todo $y \in K$, existe folha $F \in \mathcal{F}$ tal que $\phi(y, 0) = y$ e $\phi(\{y\} \times \mathbb{B}^n) \subseteq F$.

Denota-se $K \pitchfork \mathcal{F}$.

Definição 10.60. Seja X uma variedade d-dimensional. Uma *folheação* k-dimensional de X é uma partição $\mathcal{F}$ de X em subvariedades conexas de X tal que, para todo $x \in X$, existe uma vizinhança compacta K de x $(d - k)$-transversal a $\mathcal{F}$ em x. As *folhas* de $\mathcal{F}$ são as partes de $\mathcal{F}$.

[7] Aqui aparece a dimensão $n = d - k$ das subvariedades.

Capítulo 11

Fibrados

11.1 Fibrados Topológicos

Definição 11.1. Sejam $\boldsymbol{X}$ e $\boldsymbol{F}$ espaços topológicos. Um *fibrado (topológico) de* $\boldsymbol{F}$ *sobre* $\boldsymbol{X}$ é um par $(\boldsymbol{E}, \mathrm{p})$, em que $\boldsymbol{E}$ é um espaço topológico e $\mathrm{p}\colon E \longrightarrow X$ é uma função contínua sobrejetiva que satisfaz: para todo $e \in E$, existem vizinhança $A \subseteq X$ de $\mathrm{p}(e)$ e, definindo $E|_A := \mathrm{p}^{-1}(A) \subseteq E$, homeomorfismo $h\colon E|_A \longrightarrow A \times F$ tais que $\mathrm{p}_A \circ h = \mathrm{p}$ (o diagrama comuta).

$$\begin{tikzcd}
E|_A \arrow[r, "h"] \arrow[d, "\mathrm{p}"'] & A \times F \arrow[dl, "\mathrm{p}_A"] \\
A &
\end{tikzcd}$$

O espaço $\boldsymbol{E}$ é o *espaço fibrado*, o espaço $\boldsymbol{X}$ é a *base*, o espaço $\boldsymbol{F}$ é a *fibra* e a função $\mathrm{p}\colon E \longrightarrow X$ é a *projeção fibrada* de $(\boldsymbol{E}, \mathrm{p})$. Para cada $x \in X$, a *fibra de* E *em* x é $E|_x := \mathrm{p}^{-1}(\{x\})$.

A definição significa que o espaço fibrado $\boldsymbol{E}$ é localmente um produto de sua base $\boldsymbol{X}$ e sua fibra $\boldsymbol{F}$. 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 11.1. *Sejam* $\boldsymbol{X}$ *e* $\boldsymbol{F}$ *espaços topológicos e* $(\boldsymbol{E}, \mathrm{p})$ *um fibrado de* $\boldsymbol{F}$ *sobre* $\boldsymbol{X}$.

1. *Para todo* $x \in X$*, a fibra* $E|_x$ *é homeomorfa a* F*;*

2. *A projeção fibrada* $\mathrm{p}\colon E \longrightarrow X$ *é aberta e a topologia de* $\boldsymbol{X}$ *é a topologia quociente de* $\boldsymbol{E}$ *por* p.

Proposição 11.2. *Sejam* $\boldsymbol{X}$ *e* $\boldsymbol{F}$ *espaços topológicos. O par* $(\boldsymbol{X} \times \boldsymbol{F}, \mathrm{p}_X)$ *é um fibrado de* $\boldsymbol{F}$ *sobre* $\boldsymbol{X}$.

Demonstração. Basta tomar $A = X$ e $h = \mathrm{I}\colon X \times F \longrightarrow X \times F$ e segue que h é homeomorfismo e $\mathrm{p}_X \circ \mathrm{I} = \mathrm{p}_X$. ■

Exemplo 11.1 (Faixa Torcida (Möbius))**.** *Consideremos em* $\mathbb{R}^2$ *a equivalência*

$$(x, y) \sim (x', y') \quad \Longleftrightarrow \quad \bigvee_{n\in\mathbb{Z}}(x', y') = (x + n, (-1)^n y).$$

Defina $E := \mathbb{R}^2/\!\sim$ *e denote por* $q\colon \mathbb{R}^2 \longrightarrow E$ *o mapa quociente. Consideremos o mapa* $\mathrm{p}_0\colon \mathbb{R}^2 \longrightarrow \mathbb{R}$ *a projeção na coordenada* 0 *e* $r\colon \mathbb{R} \longrightarrow \mathbb{S}^1$ *o recobrimento*

$$\begin{aligned} r\colon \mathbb{R} &\longrightarrow \mathbb{S}^1 \\ x &\longmapsto (\cos(\tau x), \operatorname{sen}(\tau x)). \end{aligned}$$

Como $r \circ \mathrm{p}_0\colon \mathbb{R}^2 \longrightarrow \mathbb{S}^1$ *é constante em cada classe de equivalência, existe única função contínua* $\mathrm{p}\colon E \longrightarrow \mathbb{S}^1$ *tal que* $q \circ \mathrm{p} = r \circ \mathrm{p}_0$ *(o diagrama comuta).*

$$\begin{tikzcd} \mathbb{R}^2 \arrow[r, "q"] \arrow[d, "\mathrm{p}_0"'] & E \arrow[d, dashed, "\mathrm{p}"] \\ \mathbb{R} \arrow[r, "r"'] & \mathbb{S}^1 \end{tikzcd}$$

O par $(\boldsymbol{E}, \mathrm{p})$ *é um fibrado de* $\mathbb{R}$ *sobre* $\mathbb{S}^1$*, chamado de* faixa torcida.

A faixa torcida é um importante objeto topológico e geométrico. Ela está intrinsecamente ligada ao fenômeno de não-orientabilidade de variedades diferenciais, como será demonstrado em capítulos mais à frente.

11.2 Fibrados Vetorias

Nessa seção, consideraremos espaços lineares reais de dimensão finita, ou seja, $\mathbb{R}^n$, mas poderíamos considerar espaços lineares topológicos $\boldsymbol{L}$.

Definição 11.2. Sejam $\boldsymbol{X}$ um espaço topológico e $n \in \mathbb{N}$. Um *fibrado vetorial de posto* n *sobre* $\boldsymbol{X}$ (ou *fibrado vetorial de* $\mathbb{R}^n$ *sobre* $\boldsymbol{X}$) é um par $(\boldsymbol{E}, \mathrm{p})$, em que $\boldsymbol{E}$ é um espaço topológico e $\mathrm{p}\colon E \longrightarrow X$ é uma função contínua sobrejetiva que, definido, para todo $A \subseteq X$ e todo $x \in X$, $E|_A := \mathrm{p}^{-1}(A) \subseteq E$ e $E|_x := E|_{\{x\}}$, satisfaz:

1. Para todo $x \in X$, $E|_x$ tem estrutura linear;
2. Para todo $e \in E$, existem vizinhança $A \subseteq X$ de $\mathrm{p}(e)$ e homeomorfismo $h\colon E|_A \longrightarrow A \times \mathbb{R}^n$ tais que
   (a) $\mathrm{p}_A \circ h = \mathrm{p}$ (o diagrama comuta).

$$\begin{tikzcd} E|_A \arrow[r, "h"] \arrow[d, "\mathrm{p}"'] & A \times \mathbb{R}^n \arrow[dl, "\mathrm{p}_A"] \\ A & \end{tikzcd}$$

   (b) Para todo $x \in A$, $h|_x\colon E|_x \longrightarrow \{x\} \times \mathbb{R}^n \simeq \mathbb{R}^n$ é um isomorfismo linear.

O espaço $\boldsymbol{E}$ é o *espaço fibrado*, o espaço $\boldsymbol{X}$ é a *base*, o espaço $\mathbb{R}^n$ é a *fibra* e a função $\mathrm{p}\colon E \longrightarrow X$ é a *projeção fibrada* de $\boldsymbol{E}$. Cada par (A, h) como acima é uma *trivialização local*. Para cada $x \in X$, a *fibra de E sobre x* é o espaço $E|_x = \mathrm{p}^{-1}(\{x\})$.

Um *fibrado vetorial diferencial* é um fibrado vetorial em que $\boldsymbol{E}$ e $\boldsymbol{X}$ são variedades diferenciais, p é diferenciável e existem cartas fibradas (A, h) como acima tais que h é difeomorfismo.

A seguinte proposição é evidente.

Proposição 11.3. *Sejam $\boldsymbol{X}$ um espaço topológico (variedade diferencial), $n \in \mathbb{N}$ e $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial (diferencial) de $\mathbb{R}^n$ sobre $\boldsymbol{X}$. O par $(\boldsymbol{E}, \mathrm{p})$ é um fibrado topológico de $\mathbb{R}^n$ sobre $\boldsymbol{X}$.*

Proposição 11.4 (Fibrado Tangente)**.** *Sejam $\boldsymbol{V}$ uma variedade diferencial d-dimensional. O par $(\mathrm{T}\boldsymbol{V}, \mathrm{p})$, em que $\mathrm{T}\boldsymbol{V}$ é o fibrado tangente, $\mathrm{p}\colon V \longrightarrow \mathrm{T}V$ é a projeção canônica e $\mathrm{T}V|_p$ tem a estrutura linear canônica, é um fibrado vetorial diferencial de posto d sobre $\boldsymbol{V}$.*

Demonstração. Sejam $p \in V$ e (A, x) uma carta de $\boldsymbol{V}$ em p. Definimos a função

$$\begin{aligned} h\colon \mathrm{T}V|_A &\longrightarrow A \times \mathbb{R}^d \\ \mathop{\mathbin{+}}_{i \in [d]} v^i \left.\frac{\partial}{\partial x^i}\right|_p &\longmapsto (p, (v^0, \ldots, v^{d-1})). \end{aligned}$$

Claramente $\mathrm{p}_A \circ h = \mathrm{p}$, e $h|_p\colon \mathrm{T}V|_p \longrightarrow \mathrm{T}V|_p$ é linear. Seja $(\mathrm{T}V|_A, \varphi)$ a carta de $\mathrm{T}V$ induzida de (A, x). Então temos que $\varphi = (x, \mathrm{I}) \circ h\colon \mathrm{T}V|_A \longrightarrow x(A) \times \mathbb{R}^d$. Como φ e (x, I) são difeomorfismos, h também é, o que mostra que (A, h) é uma trivialização local em p. Isso conclui a demonstração. ■

Funções de Transição

Relembremos que $\overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n)$ é o grupo de homeomorfismos lineares de $\mathbb{R}^n$ para $\mathbb{R}^n$.

Proposição 11.5. *Seja* $(\boldsymbol{E}, \mathrm{p})$ *um fibrado vetorial diferencial de* $\mathbb{R}^n$ *sobre uma variedade diferencial* $\boldsymbol{V}$. *Para todas trivializações locais* (A, h) *e* (A', h') *de* $\boldsymbol{E}$ *tais que* $A \cap A' \neq \emptyset$, *existe função diferenciável*

$$\begin{aligned} T^h_{h'} \colon A \cap A' &\longrightarrow \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n) \\ p &\longmapsto T^h_{h'}|_p. \end{aligned}$$

tal que, para todos $(p, v) \in (A \cap A') \times \mathbb{R}^n$,

$$h' \circ h^{-1}(p, v) = (p, T^h_{h'}|_p(v)).$$

Demonstração. Sejam (A, h) e (A', h') trivializações locais de $\boldsymbol{E}$ tais que $A \cap A' \neq \emptyset$. O seguinte diagrama comuta.

$$\begin{tikzcd} (A \cap A') \times \mathbb{R}^n \arrow[dr, "\mathrm{p}_A"'] & E|_{A\cap A'} \arrow[l, "h'"'] \arrow[r, "h"] \arrow[d, "\mathrm{p}"] & (A \cap A') \times \mathbb{R}^n \arrow[dl, "\mathrm{p}_A"] \\ & A & \end{tikzcd}$$

Segue que $\mathrm{p}_A \circ (h' \circ h^{-1}) = \mathrm{p}_A$, o que implica que existe função diferenciável $\sigma \colon (A \cap A') \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$ tal que, para todo $(p, v) \in$

$$h' \circ h^{-1}(p, v) = (p, \sigma(p, v)).$$

Para todo $p \in A \cap A'$, $T^h_{h'}|_p := \sigma(p, \cdot) \colon \mathbb{R}^n \longrightarrow \mathbb{R}^n$ é um homeomorfismo linear. Assim, a função

$$\begin{aligned} T^h_{h'} \colon A \cap A' &\longrightarrow \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n) \\ p &\longmapsto T^h_{h'}|_p \end{aligned}$$

é diferenciável e satisfaz o enunciado. ■

Definição 11.3. Seja $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$. Para todas trivializações locais (A, h) e (A', h') de $\boldsymbol{E}$ tais que $A \cap A' \neq \emptyset$, a *função de transição* de (A, h) para (A', h') é a função

$$\begin{aligned} T^h_{h'} \colon A \cap A' &\longrightarrow \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n) \\ p &\longmapsto T^h_{h'}|_p. \end{aligned}$$

No caso do fibrado tangente $\mathrm{T}\boldsymbol{V}$ de uma variedade diferencial $\boldsymbol{V}$, dadas cartas (A, x) e (A', x') de $\boldsymbol{V}$ tais que $A \cap A' \neq 0$, a função de transição das cartas $(\mathrm{T}V|_A, \varphi)$ e $(\mathrm{T}V|_{A'}, \varphi')$ de $\mathrm{T}\boldsymbol{V}$ induzidas por (A, x) e (A', x'), respectivamente, é a função

$$\begin{aligned} \mathrm{D}(x' \circ x^{-1})\colon A \cap A' &\longrightarrow \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n) \\ p &\longmapsto \mathrm{D}(x' \circ x^{-1})|_p. \end{aligned}$$

Proposição 11.6 (Construção por Atlas Fibrado)**.** *Sejam $\boldsymbol{V}$ uma variedade diferencial d-dimensional, $(E|_p)_{p \in V}$ uma família de espaços lineares reais n-dimensionais, $E := \bigsqcup_{p \in V} E|_p$, $\mathrm{p}\colon E \longrightarrow V$ uma função tal que $\mathrm{p}(E|_p) = \{p\}$ e $\mathcal{A}$ um conjunto de pares (A, h) tais que*

1. *$(A)_{(A,h) \in \mathcal{A}}$ é uma cobertura aberta de V;*
2. *Para toda $(A, h) \in \mathcal{A}$, com $E|_A := \mathrm{p}^{-1}(A)$, $h\colon E|_A \longrightarrow A \times \mathbb{R}^n$ é uma bijeção tal que $h \restriction_{E|_p}\colon E|_p \longrightarrow \{p\} \times \mathbb{R}^n \simeq \mathbb{R}^n$ é um isomorfismo linear;*
3. *Para todas $(A, h), (A', h') \in \mathcal{A}$, existe função diferenciável $T^h_{h'}\colon A \cap A' \longrightarrow \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n)$ tal que, para todo $(p, v) \in (A \cap A') \times \mathbb{R}^n$,*

$$h' \circ h^{-1}(p, v) = (p, T^h_{h'}|_p(v)).$$

Então existe única estrutura diferencial sobre E que o torna uma variedade diferencial $(d+n)$-dimensional de modo que $(\boldsymbol{E}, \mathrm{p})$ é um fibrado vetorial de $\mathbb{R}^n$ sobre $\boldsymbol{V}$.

Demonstração. Seja $p \in V$ e $(A, h) \in \mathcal{A}$ tal que $p \in A$. Seja (U_p, x_p) uma carta de V em p tal que $U_p \subseteq A$. Defina a função

$$\bar{x}_p := (x_p \times \mathrm{I}_{\mathbb{R}^n}) \circ h\colon E|_{U_p} \longrightarrow x_p(U_p) \times \mathbb{R}^n \subseteq \mathbb{R}^d \times \mathbb{R}^n.$$

Mostraremos que

$$\{(E|_{U_p}, \bar{x}_p)\}_{p \in V}$$

é um atlas diferencial $(d+n)$-dimensional de E.

1. (Cartas) Como (U_p, x_p) é carta, x_p é injetivo, portanto $(x_p \times \mathrm{I}_{\mathbb{R}^n})$ é injetivo; como h é injetivo, segue que $\bar{x}_p$ é injetivo.

   Como (U_p, x_p) é carta, $x_p(U_p)$ é aberto, logo

   $$\bar{x}_p(E|_{U_p}) = (x_p \times \mathrm{I}_{\mathbb{R}^n}) \circ h(E|_{U_p}) = (x_p \times \mathrm{I}_{\mathbb{R}^n})(U_p \times \mathbb{R}^n) = x_p(U_p) \times \mathbb{R}^n$$

   é aberto.

2. (Cobertura) Como $p \in U_p$, $E|_p \subseteq E|_{U_p} \subseteq E$, logo

$$E = \bigcup_{p \in V} E|_p \subseteq \bigcup_{p \in V} E|_{U_p} \subseteq E.$$

3. (Compatibilidade) Sejam $p, p' \in V$. Então

$$E|_{U_p} \cap E|_{U_{p'}} = \mathrm{p}^{-1}(U_p) \cap \mathrm{p}^{-1}(U_{p'}) = \mathrm{p}^{-1}(U_p \cap U_{p'}) = E|_{U_p \cap U'_p}.$$

Como (U_p, x_p) e (U_p, x_p) são compatíveis, então $x_p(U_p \cap U_{p'})$ e $x_{p'}(U_p \cap U_{p'})$ são abertos, logo

$$\bar{x}_p(E|_{U_p} \cap E|_{U_{p'}}) = \bar{x}_p(E|_{U_p \cap U'_p}) = x_p(U_p \cap U_{p'}) \times \mathbb{R}^n$$

e

$$\bar{x}_{p'}(E|_{U_p} \cap E|_{U'_p}) = \bar{x}_{p'}(E|_{U_p \cap U'_p}) = x_{p'}(U_p \cap U_{p'}) \times \mathbb{R}^n$$

são abertos.

Como $x_{p'}$ e x_p são difeomorfismos, $(x_{p'} \times \mathrm{I}_{\mathbb{R}^n})$ e $(x_p \times \mathrm{I}_{\mathbb{R}^n})$ são difeomorfismos; como $h' \circ h^{-1}$ é difeomorfismo, segue que

$$\bar{x}_{p'} \circ \bar{x}_p^{-1} = (x_{p'} \times \mathrm{I}_{\mathbb{R}^n}) \circ h' \circ h^{-1} \circ (x_p \times \mathrm{I}_{\mathbb{R}^n})^{-1}$$

é difeomorfismo.

Isso mostra que $\{(E|_{U_p}, \bar{x}_p)\}_{p \in V}$ é um atlas diferencial de E. Se $\boldsymbol{V}$ é segundo-contável, tem subatlas enumerável, e podemos tomar U_p nesse subatlas e $\{(E|_{U_p}, \bar{x}_p)\}_{p \in V}$ será um atlas enumerável, o que mostra que $\boldsymbol{E}$ é segundo contável. Se $\boldsymbol{V}$ é separado (T_2), note que pontos e, e' estão em um mesmo espaço $E|_p$ estão em uma mesma carta, enquanto que se esses pontos estão respectivamente em espaços $E|_p$ e $E|_{p'}$ distintos, podemos tomar U_p e $U_{p'}$ disjuntos, de modo que

$$E|_{U_p} \cap E|_{U_{p'}} = E|_{U_p \cap U_{p'}} = \emptyset,$$

que são vizinhanças abertas de e, e', o que mostra que E é separado.

A atlas maximal desse atlas define uma estrutura diferencial sobre E e temos uma variedade diferencial $\boldsymbol{E}$.

Para todo $(A, h) \in \mathcal{A}$, a função $h\colon E|_{U_p} \longrightarrow U_p \times \mathbb{R}^n$ é um difeomorfismo, pois sua representação coordenada com respeito às cartas $(E|_{U_p}, \bar{x}_p)$ de E e $(U_p \times \mathbb{R}^n, x_p \times \mathrm{I}_{\mathbb{R}^n})$ de $U_p \times \mathbb{R}^n$ é a identidade

$$(x_p \times \mathrm{I}_{\mathbb{R}^n}) \circ h \circ \bar{x}_p^{-1} = \mathrm{I}_{x_p(U_p) \times \mathbb{R}^n} := x_p(U_p) \times \mathbb{R}^n \longrightarrow x_p(U_p) \times \mathbb{R}^n,$$

um difeomorfismo.

A função $\mathrm{p}\colon E \longrightarrow V$ é diferenciável, pois sua representação coordenada com respeito às cartas $(E|_{U_p}, \bar{x}_p)$ de E e (U_p, x_p) de V é a projeção

$$x_p \circ \mathrm{p} \circ \bar{x}_p^{-1} = \mathrm{p}_{x_p(U_p)}\colon x_p(U_p) \times \mathbb{R}^n \longrightarrow x_p(U_p),$$

uma função diferenciável.

Mostremos que vale $\mathrm{p}_{U_p} \circ h = \mathrm{p}$. Seja $e \in E|_{U_p}$. Então existe $p' \in U_p$ tal que $e \in E|_{p'}$. Por hipótese, $\mathrm{p}(e) = p'$. Por outro lado, como $h(E|_p) = \{p\} \times \mathbb{R}^n$, existe $v \in \mathbb{R}^n$ tal que $h(e) = (p', v)$, portanto

$$\mathrm{p}_{U_p} \circ h(e) = p' = \mathrm{p}(e).$$

Por hipótese, $h \restriction_{E|_p}\colon E|_p \longrightarrow \{p\} \times \mathbb{R}^n \simeq \mathbb{R}^n$ é um isomorfismo linear. Isso mostra que h é uma trivialização local e, como $(A)_{(A,h)\in\mathcal{A}}$ cobre V, segue que $(\boldsymbol{E}, \pi)$ é um fibrado vetorial de $\mathbb{R}^n$ sobre $\boldsymbol{V}$.

A unicidade segue da estrutura diferencial segue do fato de que as funções $(h)_{(A,h)\in\mathcal{A}}$ devem ser difeomorfismos, portanto qualquer outra estrutura deve conter as cartas construídas e portanto será igual a essa estrutura. ■

As funções de transição $T^h_{h'}$ satisfazem as seguintes propriedades.

Proposição 11.7. *Seja $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$.*

1. *(Cociclicidade) Para todas trivializações locais (A, h), (A', h') e (A'', h'') de $\boldsymbol{E}$ e todo $p \in A \cap A' \cap A''$,*
$$T^h_{h''}|_p = T^{h'}_{h''}|_p \circ T^h_{h'}|_p.$$
2. *Para toda trivialização local (A, h) de $\boldsymbol{E}$ e todo $p \in A$,*
$$T^h_h|_p = \mathrm{I}_{\mathbb{R}^n};$$
3. *Para todas trivializações locais (A, h) e (A', h') de $\boldsymbol{E}$ e todo $p \in A \cap A'$,*
$$T^{h'}_h|_p = {T^h_{h'}|_p}^{-1};$$

Demonstração. 1. Como $h'' \circ h^{-1} = (h'' \circ h'^{-1}) \circ (h' \circ h^{-1})$, segue que, para todo $v \in \mathbb{R}^n$,

$$\begin{aligned}(p, T^h_{h''}|_p(v)) &= h'' \circ h^{-1}(p, v)\\ &= (h'' \circ h'^{-1}) \circ (h' \circ h^{-1})(p, v)\\ &= h'' \circ h'^{-1}(p, T^h_{h'}|_p(v))\\ &= (p, T^{h'}_{h''}|_p \circ T^h_{h'}|_p(v)),\end{aligned}$$

o que mostra que $T^h_{h''}|_p(v) = T^{h'}_{h''}|_p \circ T^h_{h'}|_p(v)$, logo $T^h_{h''}|_p = T^{h'}_{h''}|_p \circ T^h_{h'}|_p$.

2. Do item anterior segue que

$$T^h_h|_p = T^h_h|_p \circ T^h_h|_p,$$

o que mostra que

$$T^h_h|_p = T^h_h|_p \circ (T^h_h|_p)^{-1} = \mathrm{I}_{\mathbb{R}^n}.$$

■

Reciprocamente, a partir de uma família de mapas como acima, podemos construir o fibrado vetorial. No entanto, essa construção não é necessariamente única.

Proposição 11.8 (Construção por Funções de Transição)**.** *Sejam $\boldsymbol{V}$ uma variedade diferencial, $\mathcal{C} = (A_i)_{i\in I}$ uma cobertura aberta de V e $\{T^i_{i'}\}_{(i,i')\in I^2}$ um conjunto de funções diferenciáveis*

$$\begin{aligned} T^i_{i'}\colon A_i \cap A_{i'} &\longrightarrow \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n) \\ p &\longmapsto T^i_{i'}|_p \end{aligned}$$

tais que

1. *(Cociclicidade) Para todos $i, i', i'' \in I$ e todo $p \in A_i \cap A_{i'} \cap A_{i''}$,*

$$T^i_{i''}|_p = T^{i'}_{i''}|_p \circ T^i_{i'}|_p.$$

Existem variedade diferencial $\boldsymbol{E}$ e $\mathrm{p}\colon E \longrightarrow V$ função diferenciável sobrejetiva tal que $(\boldsymbol{E}, \mathrm{p})$ é um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre $\boldsymbol{V}$.

Demonstração. A construção é simples de se acompanhar, mas tem várias etapas. Construiremos o espaço E, os espaços $E|_p$, a projeção $\mathrm{p}\colon E \longrightarrow V$ e as funções h e usaremos a proposição 11.6 para mostrar a existência de estrutura diferencial para termos um fibrado vetorial.

Por simplicidade, para todos $i, i' \in I$, $p \in A_i \cap A_{i'}$ e $v \in \mathbb{R}^n$, denotaremos $T^i_{i'}|_p(v)$ por $T^i_{i'}|_p v$.

1. (Construir o espaço E) Definimos

$$E' := \bigsqcup_{i\in I}(A_i \times \mathbb{R}^n) = \{(i,(p,v)) \mid i \in I \ \text{ e } \ (p,v) \in A_i \times \mathbb{R}^n\}.$$

Por simplicidade, denotaremos $(i,(p,v)) \in E'$ por (i,p,v). Definimos a relação $\sim$ em E' por

$$(i,p,v) \sim (i',p',v') \quad \Longleftrightarrow \quad p = p' \ \text{ e } \ v' = T^i_{i'}|_p v.$$

Mostremos que $\sim$ é relação de equivalência.

(a) (Reflexividade) Primeiro notemos que, pelo mesmo argumento de 11.7, para todo $i \in I$ vale que $T_i^i|_p = \mathrm{I}_{\mathbb{R}^n}$. Seja $(i,p,v) \in E$. Disso segue que $T_i^i|_p v = v$, portanto $(i,p,v) \sim (i,p,v)$.

(b) (Simetria) Sejam $(i,p,v),(i',p',v') \in E'$ tais que $(i,p,v) \sim (i',p',v')$. Então $p = p'$ e $v' = T_{i'}^i|_p v$. Da cociclicidade de $\{T_{i'}^i\}_{(i,i')\in I^2}$ segue que

$$v = T_i^i|_p v = T_i^{i'}|_p \circ T_{i'}^i|_p v = T_i^{i'}|_p v'.$$

Como $p' = p$, segue que $(i',p',v') \sim (i,p,v)$.

(c) (Transitividade) Sejam $(i,p,v),(i',p',v'),(i'',p'',v'') \in E'$ tais que $(i,p,v) \sim (i',p',v')$ e $(i',p',v') \sim (i'',p'',v'')$. Então $p = p'$, $p' = p''$, $v' = T_{i'}^i|_p v$ e $v'' = T_{i''}^{i'}|_p v'$. Da cociclicidade de $\{T_{i'}^i\}_{(i,i')\in I^2}$ segue que

$$T_{i''}^i|_p v = T_{i''}^{i'}|_p \circ T_{i'}^i|_p v = T_{i''}^{i'}|_p v' = v''.$$

Como $p'' = p$, segue que $(i,p,v) \sim (i'',p'',v'')$.

Definimos então o espaço

$$E := {E'}\big/{\sim} = \{[(i,p,v)] \mid i \in I \ \text{ e } \ (p,v) \in A_i \times \mathbb{R}^n\}.$$

Por simplicidade, denotaremos $[(i,p,v)] \in E$ por $[i,p,v]$.

2. (Construir os espaços $E|_p$) Para todo $p \in V$, definimos

$$E|_p := \{[i,q,v] \in E \mid q = p\}.$$

Notemos que, para todos $p,p' \in V$, se $E|_p \cap E|_{p'} \neq \emptyset$, então $p = p'$, pois se $[i,q,v] \in E|_p \cap E|_{p'}$, então $q = p$ e $q = p'$, logo $p = p'$. Além disso, como $(A_i)_{i\in I}$ é cobertura de V,

$$E = \{[i,p,v] \mid i \in I \ \text{ e } \ (p,v) \in A_i \times \mathbb{R}^n\} = \bigcup_{p\in V} E|_p,$$

o que implica que

$$E \simeq \bigsqcup_{p\in V} E|_p.$$

Para todo $[j,p,u] \in E|_p$ e todo $i \in I$ tal que $p \in A_i$, existe único $v \in \mathbb{R}^n$ tal que $(i,p,v) \in [j,p,u]$. Para mostrar a existência, basta tomar $v = T_i^j|_p u$ e temos que

$$(j,p,u) \sim (i,p,T_i^j|_p u) = (i,p,v).$$

Agora, suponha que existem $v,v' \in \mathbb{R}^n$ tais que $(i,p,v),(i,p,v') \in [j,p,u]$. Então $(i,p,v) \sim (i,p,v')$, portanto $v' = T_i^i|_p v = v$. Sendo assim, a partir de agora podemos sempre tomar um representante de $[j,p,u] \in E|_p$ com um $i \in I$ conveniente, contanto que $p \in A_i$.

Vamos dar estrutura de grupo para $E|_p$.

(a) (+) A soma em $E|_p$ é a função

$$\begin{aligned} +\colon E|_p \times E|_p &\longrightarrow E|_p \\ ([i,p,v],[i,p,v']) &\longmapsto [i,p,v+v'], \end{aligned}$$

que está bem definida pois se $(i,p,v) \sim (j,p,u)$ e $(i,p,v') \sim (j,p,u')$, então $u = T^i_j|_p v$ e $u' = T^i_j|_p v'$, e segue da linearidade de $T^i_j|_p$ que

$$u + u' = T^i_j|_p v + T^i_j|_p v' = T^i_j|_p (v + v'),$$

o que implica que

$$[j,p,u+u'] = [j,p,T^i_j|_p(v+v')] = [i,p,v+v'].$$

A soma é associativa: para todos $[i,p,v],[i',p,v'],[i'',p,v''] \in E|_p$,

$$\begin{aligned} ([i,p,v]+[i,p,v']) + [i,p,v''] &= [i,p,v+v'] + [i,p,v''] \\ &= [i,p,v+v'+v''] \\ &= [i,p,v] + [i,p,v'+v''] \\ &= [i,p,v] + ([i,p,v']) + [i,p,v'']) \end{aligned}$$

A soma é comutativa: para todos $[i,p,v],[i,p,v'] \in E|_p$,

$$[i,p,v]+[i,p,v'] = [i,p,v+v'] = [i,p,v'+v] = [i,p,v'] + [i,p,v].$$

(b) (0) A identidade em $E|_p$ é

$$0 := [i,p,0],$$

que está bem definida pois, para todo $i' \in I$ tal que $p \in A_{i'}$, segue da linearidade de $T^i_{i'}|_p$ que

$$(i,p,0) \sim (i',p,T^i_{i'}|_p 0) = (i',p,0).$$

Ela é identidade de +: para todo $[i,p,v] \in E|_p$,

$$0 + [i,p,v] = [i,p,0] + [i,p,v] = [i,p,0+v] = [i,p,v].$$

(c) (−) A inversa em $E|_p$ é a função

$$\begin{aligned} -\colon E|_p &\longrightarrow E|_p \\ [i,p,v] &\longmapsto [i,p,-v], \end{aligned}$$

que está bem definida pois, se $(i,p,v) \sim (j,p,u)$, então $u = T^i_j|_p v$, e segue da linearidade de $T^i_j|_p$ que

$$-u = -T^i_j|_p v = T^i_j|_p(-v),$$

o que implica que

$$[j,p,-u] = [j,p,T^i_j|_p(-v)] = [i,p,-v].$$

Ela é inversa com respeito a + e 0: para todo $[(i,(p,v))] \in E|_p$,

$$-[i,p,v] + [i,p,v] = [i,p,-v] + [i,p,v] = [i,p,-v+v] = [i,p,0] = 0.$$

Isso mostra que $\boldsymbol{E|_p} := (E|_p, +, -, 0)$ é um grupo comutativo. Agora vamos construir a estrutura de espaço linear, ou seja, a ação de corpo de $\mathbb{R}$ sobre $E|_p$.

(a) $(\cdot)$ A ação de $\mathbb{R}$ sobre $E|_p$ é a função

$$\begin{aligned} \cdot\colon \mathbb{R} \times E|_p &\longrightarrow E|_p \\ (c,[i,p,v]) &\longmapsto [i,p,cv], \end{aligned}$$

que está bem definida pois se $(i,p,v) \sim (i',p,v')$, então $v' = T^i_{i'}|_p v$ e segue da linearidade de $T^i_{i'}|_p$ que

$$(i',p,cv') = (i',p,cT^i_{i'}|_p v) = (i',p,T^i_{i'}|_p(cv)) \sim (i,p,cv).$$

Para mostrar que $\cdot$ é ação de corpo, devemos mostrar o seguinte.

i. Seja $c \in \mathbb{R}$. Para todos $[i,p,v],[i,p,v'] \in E|_p$,

$$\begin{aligned} c([i,p,v]+[i,p,v']) &= c[i,p,v+v'] \\ &= [i,p,c(v+v')] \\ &= [i,p,cv+cv'] \\ &= [i,p,cv]+[i,p,cv'] \\ &= c[i,p,v]+c[i,p,v']. \end{aligned}$$

ii. Para todos $c,c' \in \mathbb{R}$ e $[i,p,v] \in E|_p$,

$$\begin{aligned} (c+c')[i,p,v] &= [i,p,(c+c')v] \\ &= [i,p,cv+c'v] \\ &= [i,p,cv]+[i,p,c'v] \\ &= c[i,p,v]+c'[i,p,v], \end{aligned}$$

$$\begin{aligned}(cc')[i,p,v] &= [i,p,(cc')v]\\ &= [i,p,c(c'v)]\\ &= c[i,p,c'v]\\ &= c(c'[i,p,v])\end{aligned}$$

e

$$1[i,p,v] = [i,p,1v] = [i,p,v].$$

Isso mostra que $(\boldsymbol{E}|_{\boldsymbol{p}},\cdot)$ é um espaço linear sobre $\mathbb{R}$. Esse espaço tem dimensão n, pois $([i,p,b_k])_{k\in[n]}$ é uma base de $E|_p$, em que $(b_k)_{k\in[n]}$ é uma base de $\mathbb{R}^n$. Isso ocorre pois, se $[i,p,v]\in E|_p$, então como $v\in\mathbb{R}^n$ e $(b_k)_{k\in[n]}$ gera $\mathbb{R}^n$, existe $(v^k)_{k\in[n]}\in\mathbb{R}^n$ tal que

$$v = \mathop{\mathbin{+}}_{k\in[n]} v^k b_k,$$

logo

$$[i,p,v] = [i,p,\mathop{\mathbin{+}}_{k\in[n]} v^k b_k] = \mathop{\mathbin{+}}_{k\in[n]} v^k[i,p,b_k],$$

o que mostra que $([i,p,b_k])_{k\in[n]}$ gera $E|_p$; se $(c^k)_{k\in[n]}\in\mathbb{R}^n$ são não nulos, então $\mathbin{+}_{k\in[n]} c^k b_k \neq 0$, pois $(b_k)_{k\in[n]}$ é linearmente independente, logo

$$\mathop{\mathbin{+}}_{k\in[n]} c^k[(i,(p,b_k))] = [(i,(p,\mathop{\mathbin{+}}_{k\in[n]} c^k b_k))] \neq 0,$$

o que mostra que $([i,p,b_k])_{k\in[n]}$ é linearmente independente, portanto base.

3. (Construir a projeção p) Definimos função

$$\begin{aligned}\mathrm{p}\colon E &\longrightarrow V\\ [i,p,v] &\longmapsto p,\end{aligned}$$

que está bem definida pois se $(i',p',v')\sim(i,p,v)\in E$, então $p=p'$. Claramente $\mathrm{p}(E|_p)=\{p\}$.

4. (Construir as trivializações locais h_i) Definimos, para todo $C\subseteq V$, $E|_C := \mathrm{p}^{-1}(C)$. Notemos que, para todo $p\in V$, $E|_p := E|_{\{p\}}$.

   Para todo $i\in I$, definimos a função

$$\begin{aligned}h_i\colon E|_{A_i} &\longrightarrow A_i\times\mathbb{R}^n\\ [i,p,v] &\longmapsto (p,v).\end{aligned}$$

Note que, para todo $[j,p,u] \in E|_{A_i}$, temos $p \in A_i$, o que garante que existe representante $(i,p,v) \in [j,p,u]$. Essa definição não é independente de representante.

A função h_i tem inversa

$$\begin{aligned} {h_i}^{-1} \colon A_i \times \mathbb{R}^n &\longrightarrow E|_{A_i} \\ (p,v) &\longmapsto [i,p,v], \end{aligned}$$

pois, para todo $[i,p,v] \in E|_{A_i}$ e todo $(p,v) \in A_i \times \mathbb{R}^n$,

$${h_i}^{-1} \circ h_i[i,p,v] = {h_i}^{-1}(p,v) = [i,p,v]$$

e

$$h_i \circ {h_i}^{-1}(p,v) = h_i[i,p,v] = (p,v).$$

Mostremos que, para todo $i \in I$ e todo $p \in A_i$, a função $h_i \restriction_{E|_p} \colon E|_p \longrightarrow \{p\} \times \mathbb{R}^n$ é isomorfismo linear. Primeiro notemos que o contradomínio de $h_i \restriction_{E|_p}$ é $\{p\} \times \mathbb{R}^n$, pois para todo $[i,p,v] \in E|_p$,

$$h_i[i,p,v] = (p,v) \in \{p\} \times \mathbb{R}^n.$$

Além disso, ${h_i}^{-1} \restriction_{\{p\}\times\mathbb{R}^n} \colon \{p\} \times \mathbb{R}^n \longrightarrow E|_p$ é a inversa de $h_i \restriction_{E|_p}$. Notemos que o contradomínio de ${h_i}^{-1} \restriction_{\{p\}\times\mathbb{R}^n}$ é $E|_p$, pois

$${h_i}^{-1}(p,v) = [i,p,v] \in E|_p.$$

Claramente ${h_i}^{-1} \restriction_{\{p\}\times\mathbb{R}^n} = {h_i \restriction_{E|_p}}^{-1}$.

Para mostrar a linearidade, sejam $[i,p,v], [i,p,v'] \in E|_p$ e $c \in \mathbb{R}$. Então

$$\begin{aligned} h_i(c[i,p,v] + [i,p,v']) &= h_i([i,p,cv+v']) \\ &= (p, cv+v') \\ &= c(p,v) + (p,v') \\ &= ch_i[i,p,v] + h_i[i,p,v']. \end{aligned}$$

5. Agora notemos que, para todos $i, i' \in I$ e $p \in A_i \cap A_{i'}$, temos que $(i,p,v) \sim (i', p, T^i_{i'}|_p v)$, logo

$$h_{i'} \circ {h_i}^{-1}(p,v) = h_{i'}([i,p,v]) = h_{i'}([i',p,T^i_{i'}|_p v]) = (p, T^i_{i'}|_p(v)),$$

o que mostra que $T^i_{i'}$ é a função de transição de (A_i, h_i) para $(A_{i'}, h_{i'})$.

Pela proposição 11.6, essa construção mostra que E tem única estrutura diferencial tal que $(\boldsymbol{E}, \mathrm{p})$ é um fibrado vetorial de $\mathbb{R}^n$ sobre $\boldsymbol{V}$. ■

Embora a proposição 11.6 garanta que a estrutura diferencial sobre E é única, aqui não necessariamente garantimos a unicidade da construção do fibrado porque não garantimos que as construções de E, p ou h_i são únicas. Mantendo as construções de E e p, mas tomando $L \in \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n)$ e definindo

$$\begin{aligned} h_i \colon E|_{A_i} &\longrightarrow A_i \times \mathbb{R}^n \\ [i,p,v] &\longmapsto (p, Lv) \end{aligned}$$

com inversa

$$\begin{aligned} {h_i}^{-1} \colon A_i \times \mathbb{R}^n &\longrightarrow E|_{A_i} \\ (p,v) &\longmapsto [i,p,L^{-1}v], \end{aligned}$$

ainda teríamos h_i uma bijeção que restrita às fibras é isomorfismo linear, e teríamos funções de transição

$$\begin{aligned} L \circ T^i_{i'} \circ L^{-1} \colon A_i \cap A_{i'} &\longrightarrow \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n) \\ p &\longmapsto L \circ T^i_{i'}|_p \circ L^{-1}, \end{aligned}$$

que é diferenciável porque $T^i_{i'}$ e L são, e $L \circ T^i_{i'}|_p \circ L^{-1} \in \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n)$ pois $T^i_{i'}|_p \in \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n)$ e $L \in \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n)$.

► **Exercício 11.1.** Verifique que a construção da proposição anterior com essa h_i que usa $L \in \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n)$ também gera uma estrutura de fibrado vetorial $(\boldsymbol{E}, \mathrm{p})$.

Essa estrutura alternativa é de fato equivalente à que construímos, num sentido de equivalência de fibrados que estudaremos adiante.

11.2.1 Seções Locais e Globais

Definição 11.4. Seja $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$. Uma *seção (global)* de $\boldsymbol{E}$ é uma função $s \colon V \longrightarrow E$ tal que

$$\mathrm{p} \circ s = \mathrm{I}_V.$$

Isso é equivalente a dizer que

$$\begin{aligned} s \colon V &\longrightarrow E \\ p &\longmapsto s|_p \end{aligned}$$

satisfaz, para todo $p \in V$, $s|_p \in E|_p$. O conjunto das seções diferenciáveis de $\boldsymbol{E}$ é denotado $\Gamma(E)$.

Seja $A \subseteq V$. Uma *seção local* de $\boldsymbol{E}$ sobre A é uma função $s \colon A \longrightarrow E$ tal que $\mathrm{p} \circ s = \mathrm{I}_A$. O conjunto das seções locais diferenciáveis de $\boldsymbol{E}$ sobre A é denotado $\Gamma(E)|_A$.

Definição 11.5. Sejam $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$ e $s \in \Gamma(E)$ uma seção. O *suporte* de s é o conjunto

$$\operatorname{supp}(s) := \overline{\{p \in V \mid s|_p \neq 0\}}.$$

O conjunto $\Gamma(E)$ é um espaço linear sobre $\mathbb{R}$ com a adição e o multiplicação por escalar induzidos pontualmente pela adição, zero, inversa da adição e multiplicação por escalar de $E|_p$. Além dessa operações, podemos multiplicar uma seção por uma função escalar diferenciável pontualmente e dar a $\Gamma(E)$ uma estrutura de módulo sobre $\mathscr{C}^\infty(V)$.

Definição 11.6. Seja $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$. A *adição* em $\Gamma(E)$ é

$$\begin{aligned} +\colon \Gamma(E) \times \Gamma(E) &\longrightarrow \Gamma(E) \\ (s, s') &\longmapsto s + s' \colon V \longrightarrow E \\ & \qquad\qquad p \longmapsto s|_p + s'|_p, \end{aligned}$$

a *seção zero* em $\Gamma(E)$ é a seção

$$\begin{aligned} 0\colon V &\longrightarrow E \\ p &\longmapsto 0_{E|_p}, \end{aligned}$$

a *inversa aditiva* de $\Gamma(E)$ é

$$\begin{aligned} -\colon \Gamma(E) &\longrightarrow \Gamma(E) \\ s &\longmapsto -s \colon V \longrightarrow E \\ & \qquad\qquad p \longmapsto -s|_p \end{aligned}$$

e o *produto por escalar* em $\Gamma(E)$ é

$$\begin{aligned} \cdot\colon \mathbb{R} \times \Gamma(E) &\longrightarrow \Gamma(E) \\ (c, s) &\longmapsto cs \colon V \longrightarrow E \\ & \qquad\qquad p \longmapsto cs|_p. \end{aligned}$$

A *multiplicação por função*

$$\begin{aligned} \cdot\colon \mathscr{C}^\infty(V) \times \Gamma(E) &\longrightarrow \Gamma(E) \\ (f, s) &\longmapsto fs \colon V \longrightarrow E \\ & \qquad\qquad p \longmapsto f(p)s|_p. \end{aligned}$$

Isso é uma ação do anel $\mathscr{C}^\infty(V)$ que dá ao espaço $\Gamma(E)$ uma estrutura de módulo.

▶ **Exercício 11.2.** Seja $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$.

1. O espaço de seções $\Gamma(E)$ é um espaço linear sobre $\mathbb{R}$ com respeito à adição e multiplicação por escalar pontuais.

2. O espaço de seções $\Gamma(E)$ é um módulo sobre $\mathscr{C}^\infty(V)$ com respeito à adição e multiplicação por função pontuais.

11.2.2 Grupo Estrutural

Definição 11.7. Sejam $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$ e $\boldsymbol{G} \subseteq \overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n)$ um grupo diferencial. Uma G-estrutura sobre $(\boldsymbol{E}, \mathrm{p})$ é uma coleção de funções de transição $\{T^i_{i'}\}_{(i,i')\in I^2}$ cujos domínios cobrem V tais que, para todos $i, i' \in I$ e $p \in A_i \cap A_{i'}$, $T^i_{i'}|_p \in G$. Um *grupo estrutural* de $\boldsymbol{E}$ é um grupo diferencial $\boldsymbol{G}$ para o qual existe uma G-estrutura.

Exemplo 11.2. *Seja $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$.*

1. *Se $G = \{\mathrm{I}\}$ é um grupo estrutural de $\boldsymbol{E}$, então $\boldsymbol{E}$ é trivial;*

2. *Uma $\overset{\leftrightarrow}{\mathscr{L}}(\mathbb{R}^n)^+$-estrutura sobre $\mathrm{T}V$ é equivalente a uma orientação de $\boldsymbol{V}$;*

3. *Uma $\overset{\leftrightarrow}{\mathscr{L}}_{\|\|}(\mathbb{R}^n)$-estrutura (também denotado $O(n)$ ou $O_n(\mathbb{R})$) sobre $\boldsymbol{E}$ é equivalente a um produto interno em cada fibra $E|_p$, dado por*

$$\langle v, v' \rangle |_p := v'^* T^i_{i'}|_p v.$$

11.2.3 Referenciais Locais e Globais

Definição 11.8. Sejam $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$ e $A \subseteq V$ um aberto. Uma k-tupla de seções locais sobre A *linearmente independente* é uma k-tupla $(s_i)_{i\in[k]}$ de seções locais $s_i \colon A \longrightarrow E$ de $\boldsymbol{E}$ sobre A tais que, para todo $p \in A$, $(s_i|_p)_{i\in[k]}$ é linearmente independente em $E|_p$.

Similarmente, uma k-tupla de seções locais sobre A que *gera* $\boldsymbol{E}$ é uma k-tupla $(s_i)_{i\in[k]}$ de seções locais $s_i \colon A \longrightarrow E$ de $\boldsymbol{E}$ sobre A tais que, para todo $p \in A$, $(s_i|_p)_{i\in[k]}$ gera $E|_p$.

Um *referencial local* de $\boldsymbol{E}$ sobre A é uma k-tupla de seções locais de $\boldsymbol{E}$ sobre A linearmente independente que *gera* $\boldsymbol{E}$. Um *referencial (global)* de $\boldsymbol{E}$ é um referencial local de $\boldsymbol{E}$ sobre V.

Lembremos que $(e_i)_{i\in[n]}$ é a base canônica de $\mathbb{R}^n$.

Proposição 11.9. *Sejam* $(\boldsymbol{E}, \mathrm{p})$ *um fibrado vetorial diferencial de* $\mathbb{R}^n$ *sobre uma variedade diferencial* $\boldsymbol{V}$ *e* (A, h) *uma trivialização local. A funções*

$$\begin{aligned} s_i \colon A &\longrightarrow E \\ p &\longmapsto h^{-1}(p, e_i). \end{aligned}$$

são seções locais de $\boldsymbol{E}$ *e* $(s_i)_{i\in[n]}$ *é um referencial local de* $\boldsymbol{E}$ *sobre* A.

Demonstração. As funções s_i são diferenciáveis porque h é difeomorfismo e de $\mathrm{p}_A \circ h = \mathrm{p}$ segue que, para todo $p \in A$,

$$\mathrm{p} \circ s_i(p) = \mathrm{p} \circ h^{-1}(p, e_i) = \mathrm{p}_A(p, e_i) = p,$$

logo $\mathrm{p} \circ s_i = \mathrm{I}_A$, o que mostra que s_i é uma seção local.

Para vermos que $(s_i)_{i\in[n]}$ é um referencial local, notemos que $h \colon E|_p \longrightarrow \{p\} \times \mathbb{R}^n$ é um isomorfismo e $h(s_i|_p) = (p, e_i)$, então leva $(s_i)_{i\in[n]}$ para a base canônica de $\{p\} \times \mathbb{R}^n$. ■

Definição 11.9. Sejam $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{V}$ e (A, h) uma trivialização local. O *referencial local associado a* h é o referencial local $(s_i)_{i\in[n]}$ de $\boldsymbol{E}$ sobre A, em que

$$\begin{aligned} s_i \colon A &\longrightarrow E \\ p &\longmapsto h^{-1}(p, e_i). \end{aligned}$$

► **Exercício 11.3.** Todo referencial local está associado a uma trivialização local.

11.3 Fibrados Principais

Lembremos o que é uma ação à direita de um grupo. Sejam X um conjunto e $\boldsymbol{G}$ um grupo. Uma ação à direita $X \curvearrowleft \boldsymbol{G}$ de G em X é uma função

$$\begin{aligned} A \colon X \times G &\longrightarrow X \\ (x, g) &\longmapsto x \centerdot g \end{aligned}$$

tal que

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

$$x \centerdot \mathrm{I} = x;$$

2. (Compatibilidade) Para todos $g, g' \in G$ e $x \in X$,

$$x \centerdot (gg') = (x \centerdot g) \centerdot g';$$

Além disso, consideraremos também a seguinte propriedade da ação.

1. (Livre) Para todo $g \in G$, se existe $x \in X$ tal que $x \centerdot g = x$, então $g = \mathrm{I}$;

Definição 11.10. Sejam $\boldsymbol{V}$ uma variedade diferencial e $\boldsymbol{G}$ um grupo diferencial. Um $\boldsymbol{G}$-fibrado principal diferencial sobre $\boldsymbol{V}$ é uma tripla $(\boldsymbol{E}, \pi, \centerdot)$ em que $\boldsymbol{P}$ é uma variedade diferencial, $\centerdot\colon E \times G \longrightarrow E$ é uma ação à direita diferenciável e livre, $V \simeq E/G$ e, para todo $x \in V$, existem vizinhança $A \subseteq V$ de x e difeomorfismo $\phi\colon E|_A := \mathrm{p}^{-1}(A) \longrightarrow A \times G$ tais que

1. $\mathrm{p}_A \circ \phi = \mathrm{p}$ (o diagrama comuta).

$$\begin{tikzcd}
E|_A \arrow[r, "\phi"] \arrow[d, "\mathrm{p}"'] & A \times G \arrow[dl, "\mathrm{p}_A"] \\
A &
\end{tikzcd}$$

2. (G-equivariância) Se $\phi(e) = (p, h)$, então $\phi(e \centerdot g) = (p, hg)$ — ou, equivalentemente, $\mathrm{p}_G \circ \phi \circ \centerdot g = \centerdot g \circ \mathrm{p}_G \circ \phi$ (o diagrama comuta).

$$\begin{tikzcd}
E|_A \arrow[r, "\centerdot g"] \arrow[d, "\mathrm{p}_G \circ \phi"'] & E|_A \arrow[d, "\mathrm{p}_G \circ \phi"] \\
G \arrow[r, "\centerdot g"'] & G
\end{tikzcd}$$

$$\phi^{-1}(p, h) \centerdot g = \phi^{-1}(p, hg)$$
$$(\centerdot g) \circ \phi^{-1}(p, h) = \phi^{-1}(p, hg)$$
$$(\centerdot g) \circ \phi^{-1}(p, h) = \phi^{-1}(p, (\centerdot g) \circ \mathrm{p}_G(e))$$

Proposição 11.10. *Seja* $(\boldsymbol{E}, \pi, \boldsymbol{.})$ *um fibrado principal diferencial de um grupo diferencial* $\boldsymbol{G}$ *sobre uma variedade diferencial* $\boldsymbol{V}$*. Para todas trivializações locais* (A, ϕ) *e* (A', ϕ') *de* $\boldsymbol{E}$*, a função de transição delas é a multiplicação à esquerda pela valor dela na identidade do grupo:*

$$\begin{aligned} T^{\phi}_{\phi'}|_p = E_{T^{\phi}_{\phi'}|_p \mathrm{I}} \colon G &\longrightarrow G \\ g &\longmapsto (T^{\phi}_{\phi'}|_p \mathrm{I})g. \end{aligned}$$

Demonstração. Sejam $g, h \in G$ e $e := \phi^{-1}(p, h)$. Da definição de função de transição,

$$\phi'(e) = \phi' \circ \phi^{-1}(p, h) = (p, T^{\phi}_{\phi'}|_p(h))$$

e, da equivariância,

$$(p, T^{\phi}_{\phi'}|_p(hg)) = \phi' \circ \phi^{-1}(p, hg) = \phi'(e \boldsymbol{.} g) = (p, (T^{\phi}_{\phi'}|_p(h))g),$$

o que implica que

$$T^{\phi}_{\phi'}|_p(hg) = (T^{\phi}_{\phi'}|_p h)g.$$

Tomando $h = \mathrm{I}$, segue que

$$T^{\phi}_{\phi'}|_p(g) = (T^{\phi}_{\phi'}|_p \mathrm{I})g.$$

■

Por simplicidade, identificaremos $T^{\phi}_{\phi'}|_p$ com $T^{\phi}_{\phi'}|_p \mathrm{I}$, de modo a termos $T^{\phi}_{\phi'}|_p \in G$. As funções de transição, que são da forma

$$T^{\phi}_{\phi'} \colon A \cap A' \longrightarrow \overset{\leftrightarrow}{\mathscr{C}}{}^{\infty}(G),$$

sob essa identificação podem ser entendidas como funções da forma

$$T^{\phi}_{\phi'} \colon A \cap A' \longrightarrow G.$$

11.4 Conexões em Fibrados Vetoriais

11.4.1 Espaços Verticais e Horizontais

Seja $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{B}$. Tomemos carta (A, x) de $\boldsymbol{B}$ e trivialização local (A, ϕ) de $\boldsymbol{E}$. Elas são funções

$$\begin{aligned} x \colon A &\longrightarrow x(A) \subseteq \mathbb{R}^d \\ b &\longmapsto x(b) \end{aligned}$$

e

$$\begin{aligned}\phi\colon E|_A &\longrightarrow A \times \mathbb{R}^n\\ e &\longmapsto (b, v).\end{aligned}$$

A função

$$\begin{aligned}\bar{x} = (x \times \mathrm{I}_{\mathbb{R}^n}) \circ \phi\colon E|_A &\longrightarrow x(A) \times \mathbb{R}^n \subseteq \mathbb{R}^d \times \mathbb{R}^n\\ e &\longmapsto (x(b), v),\end{aligned}$$

em que $\phi(e) = (b, v)$, é uma carta de $\boldsymbol{E}$. O referencial coordenado de $\mathrm{T}E|_A$ é

$$\left(\left.\frac{\partial}{\partial \bar{x}^i}\right|_e\right)_{i \in [d+n]}.$$

Mas notemos que, para $i \in [d]$,

$$\bar{x}^i = \mathrm{p}_i \circ \bar{x} = \mathrm{p}^i \circ x = x^i$$

e, para $j \in d + [n]$,

$$\bar{x}^i = \mathrm{p}_i \circ \bar{x} = \mathrm{p}^i \circ \phi = \phi^i,$$

portanto

$$\left(\left.\frac{\partial}{\partial \bar{x}^i}\right|_e\right)_{i \in [d+n]} = \left(\left.\frac{\partial}{\partial x^i}\right|_e, \left.\frac{\partial}{\partial \phi^j}\right|_e\right)_{i \in [d], j \in d+[n]}.$$

Consideremos a função diferenciável

$$\mathrm{D}\mathrm{p}|_e\colon \mathrm{T}E|_e \longrightarrow \mathrm{T}B|_b.$$

11.4.2 Conexão/Derivada Covariante

Definamos

$$\Omega^k_B(E) = \Omega^k(B) \otimes \Gamma(E).$$

Em particular,

$$\Omega^0_B(E) = \mathscr{C}^\infty(B) \otimes \Gamma(E) = \Gamma(E)$$

e

$$\Omega^1_B(E) = \Omega^1(B) \otimes \Gamma(E).$$

Definição 11.11. Seja $(\boldsymbol{E}, \mathrm{p})$ um fibrado vetorial diferencial de $\mathbb{R}^n$ sobre uma variedade diferencial $\boldsymbol{B}$. Uma *derivada covariante* em $\boldsymbol{E}$ é uma função linear sobre $\mathbb{R}$

$$\nabla\colon \Omega^0_B(E) \longrightarrow \Omega^1_B(E).$$

tal que, para todas $f \in \mathscr{C}^\infty(B)$ e $s \in \Gamma(E)$,

$$\nabla(fs) = \mathrm{d}f \otimes s + f\nabla s.$$

Equivalentemente, ∇ é uma função

$$\nabla\colon \Gamma(E) \longrightarrow \Omega^1(B) \otimes \Gamma(E)$$

que toma seções e retorna 1-formas a valores em seções.

Estendemos a derivada covariante $\nabla\colon \Omega^0_B(E) \longrightarrow \Omega^1_B(E)$ para uma função[1] linear sobre $\mathbb{R}$

$$\nabla\colon \Omega^k_B(E) \longrightarrow \Omega^{k+1}_B(E)$$

para todo k tal que, para todas $\omega \in \Omega^k(B)$ e $s \in \Gamma(E)$,

$$\nabla(\omega \otimes s) = \mathrm{d}\omega \otimes s + (-1)^k \omega \otimes \nabla s.$$

$$\begin{aligned} \nabla\colon \Omega^k_B(E) &\longrightarrow \Omega^{k+1}_B(E) \\ \sigma &\longmapsto \nabla\sigma\colon \text{ffl} \longrightarrow \text{ffl} \\ &\qquad\qquad\quad \text{ffl} \longmapsto \text{ffl} \end{aligned}$$

[1]Geralmente essa derivada estendida é denotada d_∇ e chamada de derivada exterior covariante, mas aqui adotaremos a simplicidade de manter ∇ para todos os casos.

A derivada covariante é a função $\mathbb{R}$-linear

$$\nabla\colon \Omega_B^k(E) \longrightarrow \Omega_B^{k+1}(E).$$

Localmente, temos

$$\nabla = \mathrm{d} + A.$$

A *curvatura* é a função $\mathscr{C}^\infty(B)$-linear

$$\nabla^2\colon \Omega_B^k(E) \longrightarrow \Omega_B^{k+2}(E).$$

Localmente, temos

$$\nabla^2 = \mathrm{d}A + A \wedge A.$$

Parametrização e Métrica da Esfera

$$\begin{aligned}
x_0 &= r\cos\phi_0\\
x_1 &= r\,\mathrm{sen}\,\phi_0\cos\phi_1\\
x_2 &= r\,\mathrm{sen}\,\phi_0\,\mathrm{sen}\,\phi_1.
\end{aligned}$$

$$\begin{aligned}
\mathrm{d}x_0 &= \cos\phi_0\mathrm{d}r - r\,\mathrm{sen}\,\phi_0\mathrm{d}\phi_0\\
\mathrm{d}x_1 &= \mathrm{sen}\,\phi_0\cos\phi_1\mathrm{d}r + r\cos\phi_0\cos\phi_1\mathrm{d}\phi_0 - r\,\mathrm{sen}\,\phi_0\,\mathrm{sen}\,\phi_1\mathrm{d}\phi_1\\
\mathrm{d}x_2 &= \mathrm{sen}\,\phi_0\,\mathrm{sen}\,\phi_1\mathrm{d}r + r\cos\phi_0\,\mathrm{sen}\,\phi_1\mathrm{d}\phi_0 + r\,\mathrm{sen}\,\phi_0\cos\phi_1\mathrm{d}\phi_1
\end{aligned}$$

$$\begin{aligned}
(\mathrm{d}x_0)^2 &= \cos^2\phi_0(\mathrm{d}r)^2 + r^2\,\mathrm{sen}^2\,\phi_0(\mathrm{d}\phi_0)^2 - 2r\,\mathrm{sen}\,\phi_0\cos\phi_0\mathrm{d}r\mathrm{d}\phi_0\\
(\mathrm{d}x_1)^2 &= \mathrm{sen}^2\,\phi_0\cos^2\phi_1(\mathrm{d}r)^2 + r^2\cos^2\phi_0\cos^2\phi_1(\mathrm{d}\phi_0)^2 + r^2\,\mathrm{sen}^2\,\phi_0\,\mathrm{sen}^2\,\phi_1(\mathrm{d}\phi_1)^2\\
&\quad + 2r\,\mathrm{sen}\,\phi_0\cos\phi_0\cos^2\phi_1\mathrm{d}r\mathrm{d}\phi_0 - 2r\,\mathrm{sen}^2\,\phi_0\,\mathrm{sen}\,\phi_1\cos\phi_1\mathrm{d}r\mathrm{d}\phi_1\\
&\quad - 2r^2\,\mathrm{sen}\,\phi_0\cos\phi_0\,\mathrm{sen}\,\phi_1\cos\phi_1\mathrm{d}\phi_0\mathrm{d}\phi_1\\
(\mathrm{d}x_2)^2 &= \mathrm{sen}^2\,\phi_0\,\mathrm{sen}^2\,\phi_1(\mathrm{d}r)^2 + r^2\cos^2\phi_0\,\mathrm{sen}^2\,\phi_1(\mathrm{d}\phi_0)^2 + r^2\,\mathrm{sen}^2\,\phi_0\cos^2\phi_1(\mathrm{d}\phi_1)^2\\
&\quad + 2r\,\mathrm{sen}\,\phi_0\cos\phi_0\,\mathrm{sen}^2\,\phi_1\mathrm{d}r\mathrm{d}\phi_0 + 2r\,\mathrm{sen}^2\,\phi_0\,\mathrm{sen}\,\phi_1\cos\phi_1\mathrm{d}r\mathrm{d}\phi_1\\
&\quad + 2r^2\,\mathrm{sen}\,\phi_0\cos\phi_0\,\mathrm{sen}\,\phi_1\cos\phi_1\mathrm{d}\phi_0\mathrm{d}\phi_1
\end{aligned}$$

$$\begin{aligned}
(\mathrm{d}x_0)^2 + (\mathrm{d}x_1)^2 + (\mathrm{d}x_2)^2 &= (\cos^2\phi_0 + \mathrm{sen}^2\,\phi_0)(\mathrm{d}r)^2\\
&\quad + r^2(\mathrm{sen}^2\,\phi_0 + \cos^2\phi_0\cos^2\phi_1 + \cos^2\phi_0\,\mathrm{sen}^2\,\phi_1)(\mathrm{d}\phi_0)^2\\
&\quad + r^2(\mathrm{sen}^2\,\phi_0\,\mathrm{sen}^2\,\phi_1 + \mathrm{sen}^2\,\phi_0\cos^2\phi_1)(\mathrm{d}\phi_1)^2\\
&\quad + 2r(-\mathrm{sen}\,\phi_0\cos\phi_0\\
&\qquad\qquad + \mathrm{sen}\,\phi_0\cos\phi_0\cos^2\phi_1 + \mathrm{sen}\,\phi_0\cos\phi_0\,\mathrm{sen}^2\,\phi_1)\mathrm{d}r\mathrm{d}\phi_0\\
&\quad + 2r(-\mathrm{sen}^2\,\phi_0\,\mathrm{sen}\,\phi_1\cos\phi_1 + \mathrm{sen}^2\,\phi_0\,\mathrm{sen}\,\phi_1\cos\phi_1)\mathrm{d}r\mathrm{d}\phi_1\\
&\quad + 2r^2(-\mathrm{sen}\,\phi_0\cos\phi_0\,\mathrm{sen}\,\phi_1\cos\phi_1\\
&\qquad\qquad + \mathrm{sen}\,\phi_0\cos\phi_0\,\mathrm{sen}\,\phi_1\cos\phi_1)\mathrm{d}\phi_0\mathrm{d}\phi_1\\
&= (\mathrm{d}r)^2 + r^2((\mathrm{d}\phi_0)^2 + \mathrm{sen}^2\,\phi_0(\mathrm{d}\phi_1)^2)\\
&= (\mathrm{d}r)^2 + r^2\mathrm{d}S^2.
\end{aligned}$$