Richard A. Dean

ELEMENTOS DE ÁLGEBRA ABSTRATA

ELEMENTOS DE ÁLGEBRA ABSTRATA

Richard A. Dean
California Institute of Technology

Tradução: **Carlos Alberto A. de Carvalho**
Professor do Instituto Militar de Engenharia
Professor da Universidade Veiga de Almeida

LIVROS TÉCNICOS E CIENTÍFICOS EDITORA S.A.
Rio de Janeiro — GB/1974

PREFÁCIO

Este livro é um desenvolvimento do curso introdutório de álgebra dado no California Institute of Technology. O curso, e de modo mais completo este livro-texto, deve ser entendido como uma introdução aos tópicos e técnicas da álgebra abstrata que encontram sempre maiores aplicações em matemática e em ciências aplicadas. Este livro serve também para introduzir o estudante na espécie de matemática que, pela abstração e generalidade, pela aplicação do método axiomático, e pelo estudo de uma demonstração como um meio de compreender matemática, mais se assemelha à pesquisa matemática honesta do que o faz o curso típico de cálculo. Entretanto os pré requisitos formais são apenas os equivalentes de um programa moderno de matemática elementar. Naturalmente, a experiência adicional, fornecida por qualquer curso de matemática mais sério é incalculável.

Escrevendo este livro simplesmente desejei estabelecer meu plano para um tratamento introdutório da álgebra e gozar do luxo, nem sempre permitido em um curso, de incluir alguns tópicos tratados com pouca freqüência neste nível, e de excluir outros tópicos que têm sido tratados extensivamente.

Neste espírito o livro não contém nenhum desenvolvimento de álgebra linear e determinantes, tão pouco contém o desenvolvimento dos inteiros a partir dos postulados de Peano, nem dos números reais a partir dos racionais, nem de aritmética transfinita. Apesar destes serem, naturalmente, tópicos importantes, não são exigidos para o material contido neste livro.

Se este livro tem um tema, é o conceito de grupo. O conceito de grupo é o mais central de todos os conceitos algébricos; na verdade, as técnicas empregadas em teoria dos grupos têm servido amplamente como modelo para outros tópicos da álgebra. Se este livro tem um objetivo, é a teoria de Galois para corpos de característica zero e uma demonstração completa do critério de que os zeros de um polinômio podem ser expressos por radicais.

O Capítulo 1 é uma introdução aos grupos. Este capítulo é o mais longo do livro porque inclui um grande número de exemplos, notadamente grupos cíclicos, grupos de permutação e grupos diedrais. Desenvolve as noções chave de subgrupo, homomorfismo e grupo quociente, e produto direto. Compreendi que é valioso o tempo usado em sala de aula para tratar

este material com um justo detalhe e esperar que a classe se torne razoavelmente capaz de manipular os conceitos relativos a grupos. A facilidade com abstração ganha aqui, paga belos dividendos durante o restante do curso. Assim, o Capítulo 2, Anéis, segue facilmente porque muitos dos teoremas aparecem como análogos naturais dos teoremas sobre grupos. Neste tratamento os primeiros teoremas sobre sistemas com duas operações binárias tornam-se rotina.

Tenho rejeitado a tese de que uma introdução a álgebra deve começar com um estudo dos inteiros. Enquanto uma discussão informal de teoria dos números é útil e interessante ela não prepara um estudante para a abstração subseqüente de um tratamento axiomático de grupos, anéis e espaços vetoriais. Por outro lado, um desenvolvimento dos postulados de Peano é um tedioso **tour de force** que usualmente produz uma pouco útil teoria dos números.

O Capítulo 3, Os Inteiros, constitui uma abordagem médio-básica para a teoria dos números. Os inteiros são apresentados como um domínio de integridade ordenado no qual a ordem realiza a boa-ordenação dos elementos positivos. O fato de que este sistema de axiomas é categórico é um resultado muito importante para ser ignorado e muito significativo para se passar por cima com uma prova de "faz-de-conta". A sutileza crucial é um teorema dando condições suficientes para um esquema indutivo definir uma função. Esta seção e este resultado bastante técnico podem, naturalmente, ser omitidos sem prejudicar a continuidade do livro como um todo. Na realidade, exceto pelos resultados sobre aritmética dos inteiros (Seç. 3.6), o capítulo inteiro pode ser omitido, desde que o leitor se disponha a aceitar as propriedades mais elementares dos domínios de integridade ordenados e dos conjuntos bem-ordenados. Mesmo a aritmética é essencialmente repetida no contexto mais geral de um domínio euclideano no Capítulo 5.

Os capítulos subseqüentes sobre corpos, domínio euclideano, polinômios, e espaços vetoriais seguem de maneira direta. No Capítulo 8, Extensão de Corpos, o principal resultado é a existência e unicidade de um corpo decomponível para um polinômio. A incursão lateral através de corpos finitos e o teorema de Wedderburn sobre anéis de divisão finitos podem ser incluídos ou excluídos, dependendo do interesse do leitor. O material do Capítulo 9, Grupos Finitos, pode também ser selecionado deste modo. Tudo o que aí está contido é essencial para um domínio efetivo da teoria dos grupos, e em particular as seções sobre grupos solúveis são indispensáveis para a teoria de Galois. Não fiz concessões no sentido de "abrandar" o tratamento do teorema de base clássico para grupos abelianos finitamente gerados. A demonstração que aparece no Capítulo 9 é completamente construtiva para grupos abelianos finitamente apresentados. Ao longo do livro tenho tentado fazer todas as provas construtivas e dar problemas utilizando as construções. A tendência pedagógica deste livro-texto é a de que a teoria adquire significado maior quando são resolvidos problemas concretos. Para a parte de unicidade do teorema de base usei a prova de P. Cohn da lei do cancelamento para fatores diretos cíclicos de um grupo abeliano. Deste teorema segue de um modo simples uma demonstração muito natural para a unicidade.

Finalmente, o livro termina com um capítulo sobre teoria de Galois. A teoria de Galois serve não apenas como exemplo de uma bela teoria matemática, mas também como um significativo instrumento pedagógico; ligando teoria dos grupos e teoria dos corpos o entendimento de cada um destes tópicos é ampliado. Por mais belo que seja o teorema sobre a correspondência de Galois, quando isolado, é provavelmente um erro começar este capítulo — a menos que o leitor esteja preparado para enfrentar os detalhes surpreendentemente complicados dos teoremas sobre as soluções de equações por radicais. Acredito, e em geral sigo, a máxima atribuída a Tchekhov: "Não traga um canhão à cena a menos que esteja preparado para dispará-lo."

Uma palavra sobre o Capítulo 0. O Capítulo 0 deve ser percorrido muito rapidamente apenas para nos informarmos do que contém. Não pretende ser uma parte real do livro e

por esta razão não contém exercícios. Passe ao Capítulo 1 tão rápido quanto possível! O Capítulo 0 deveria ser usado como um apêndice e um glossário de notação e terminologia. Entretanto, a sua precedência é justificada por fornecer um vocabulário e incluir alguns resultados indispensáveis. Haverá ocasião em que será necessário voltar ao Capítulo 0 para maior clareza. Em tais ocasiões será útil fazer uma leitura mais cuidadosa das seções partinentes, talvez mesmo construir alguns exemplos adicionais e inventar algum problema.

Como sempre, os exercícios desempenham um papel-chave para a compreensão do material do texto. Foram incluídos mais de 350 problemas. Propositadamente, os resultados de alguns dos problemas serão usados subseqüentemente no livro. Em tais ocasiões darei um breve esquema da solução. Alguns problemas são pouco razoáveis; são os marcados com asterisco. Tais problemas servem melhor como problemas de discussão em classe.

O esquema de numeração para teoremas e lemas é o padrão. Dentro de um capítulo os teoremas são numerados consecutivamente de 1 a **n**. Os lemas são numerados independentemente de 1 a **m**. Se, por exemplo, no Capítulo 5 citamos o Teorema 8 do Capítulo 2 o referiremos simplesmente como Teorema 2.8. No alto de páginas alternadas estão os títulos da seção correspondente e os números dos teoremas e lemas em sua forma decimal completa. Definições não foram numeradas numa tentativa de encorajar o estudante a aprender as definições à medida que elas ocorrem e a evitar o mar de números que resultaria. Todas as definições são claramente anotadas no índice; a página na qual a definição aparece está em negrito.

Sou profundamente agradecido aos meus colegas e estudantes do California Institute of Technology. Durante os quatro anos de evolução e preparação deste manuscrito seus comentários e críticas incisivas resultaram em um vasto número de melhoramentos e modificações. As melhores demonstrações são deles. Gostaria de agradecer particularmente a ajuda do falecido Morgan Ward cujos escritos abundam em muitas das provas e exercícios. Sou também grato aos Professores Peter Hilton, Robert Stoll e J. Dean Swift que leram cuidadosamente uma redação final do manuscrito e cujas críticas permitiram remover um grande número de imprecisões e deselegâncias. A menção dos seus nomes não constitui um endosso e, naturalmente, os erros e mal julgamentos que restam são meus.

Também agradeço a John Wiley and Sons por sua paciência e habilidade em reproduzir as 85 figuras, algumas das quais aparecem em duas cores.

RICHARD A. DEAN

Pasadena, California
Janeiro, 1966

SÍMBOLOS ESPECIAIS E NOTAÇÃO

I; o conjunto dos inteiros, 1
$|$, $a|b$; a divide b, 1
$\in$, $A \in B$; pertinência, 4
$\notin$, $A \notin B$; não-pertinência, 4
$=$, $A = B$; igualdade de conjuntos, 5
$\{a\}$; conjunto de um elemento, 5
$\varnothing$; conjunto vazio, 5
$|A|$; número cardinal de elementos do conjunto A, 5
$\subseteq$, $A \subseteq B$; inclusão de subconjuntos, 5
$-$, $A - B$; conjunto diferença, 6
$\cup$, $A \cup B$, $\bigcup A$; conjunto união, 6
$\cap$, $A \cap B$, $\bigcap A$; conjunto interseção, 6
(a, b); par ordenado, 7
$\times$, $A \times B$; produto cartesiano, 7
produto direto de grupos A e B, 65
$\mathscr{D}_T$; domínio da relação T, 8
$\mathscr{R}_T$; contradomínio da relação T, 8
ι; iota, a função identidade, 11
$c_S(\chi)$; função característica, 11
$f: A \to B$; função de A em B, 12
$\binom{n}{k}$; símbolo combinatório, 16
$\langle S, \circ \rangle$; Grupo com operação, 24
a^{-1}; inverso de a, em um grupo (multiplicativo), 30
$\mathscr{S}_n$; grupo simétrico sobre n símbolos, 37
$\langle g \rangle$; grupo cíclico com gerador g, 40
ideal principal com gerador g, 78
Sb, bS; classes laterais do subgrupo S, 47
$[G:S]$; índice do subgrupo S no grupo G, 48
$\vee$, $A \vee B$; supremo de subgrupos, 51
supremo de subanéis, 75
supremo de subespaços, 188

$\langle S \rangle$; subgrupo gerado pelo subconjunto S, 52
$A \cdot B$; complexo em um grupo 55
$\mathscr{A}_n$; grupo alternado sobre n símbolos, 55, 296
Z; centro de grupo, 56, 233
N_a; normalizador (=centralizador do elemento a em um grupo, 230
N_S; normalizador do conjunto S em um grupo, 56, 234
G/K; grupo cociente, 59
anel cociente, 80
$\langle A +, \cdot \rangle$; anel, 70
D_p; números racionais $a|b$, onde $b = p^k$, 76
$\widehat{D}_p$; números racionais $a|b$, onde $p \nmid b$, 76
I_d; $I/\langle d \rangle$, 81
$\equiv$, $a \equiv b \pmod K$; relação de congruência, 82
$\sim$, $a \sim b$; a é associado a b, em um anel, 87
(b, c), MDC (b, c); maior divisor comum, 87, 105
$[b, c]$, MMC (b, c); menor múltiplo comum, 87, 105
$\langle D, +, \cdot, \leq \rangle$; domínio de integridade ordenado, 92
E_+; conjunto de elementos positivos, 97
$|a|$; valor absoluto, 93
φ; função φ de Euler, 107
$[r]$; função maior inteiro, 108
Q; corpo de cocientes, 110
Ra; corpo dos números racionais, 112
(K); característica de K, 115
$S(a_1, \ldots, a_n)$, $S(A)$; menor subcorpo contendo $S \cup A$, 115
Re; corpo dos números reais, 121
C; corpo dos números complexos, 122
i; o número complexo $(0, 1)$, um zero de $x^2 + 1$, 123
$\overline{\alpha}$; complexo conjugado α, 126
$|\alpha|$; módulo do número complexo α, 123
$\langle D, +, \cdot, v \rangle$; domínio euclideano, 129
G; o anel dos inteiros gaussianos, 129
$A[x]$; o anel de polinômios com coeficientes em A, 147
x; indeterminada, 147
f'; derivada formal do polinômio f, 160
DFU; domínio de fatoração única, 162
$A(x)$; corpo de cocientes de $A[x]$, 169
$V_n(K)$; espaço vetorial dos n-uplas sobre K, 174
$V_\infty(K)$; espaço vetorial de seqüências infinitas de K, 175
$\dim(V)$; dimensão do espaço vetorial V, 182
$\mathscr{L}(V)$; grupo linear completo, 189
$\underset{\sim}{c}$, $a \underset{\sim}{c} b$; a e b são conjugados em F sobre K, 209
$[F : K]$; grau da extensão de corpo F sobre K, 212
$\mathscr{G}(F/K)$; grupo de automorfismos da extensão de corpo F sobre K, 215
$W_p(d)$; número de polinômios mônicos irredutíveis de grau d em $CG(p)[x]$, 221
μ; função μ de Möbius, 222
$\Phi_n(x)$; polinômio ciclotômico, 227
$\underset{\sim}{s}$, $D \underset{\sim}{s} E$; D e E são conjuntos conjugados em G, 235
p-SS; um p-subgrupo de Sylow, 238
G'; grupo derivado (comutador) do grupo G, 248
$\mathscr{S}(L)$; grupo de automorfismos de $F \supseteq L$ fixando cada elemento de L, 265
$I(\mathscr{H})$; corpo de elementos fixados por $\mathscr{H} \subseteq \mathscr{G}(F/K)$, 265
TFTG; teorema fundamental da teoria de Galois, 271
$\lambda(\epsilon, a)$; resolvente de Lagrange, 278
Δ; discriminante, 287, 296
$s_k = \Sigma t_1 \ldots t_k$; o k-ésimo polinômio simétrico elementar, 293

CONTEÚDO

Símbolos e Notações, XI

Capítulo 0, 1

0.1. Aritmética, 1
0.2. Conjuntos, 4
0.3. Relações, 7
0.4. Funções e Aplicações, 10
0.5. Operações e Operadores, 13
0.6. Combinatória, 16

Prólogo, 19

Capítulo 1 Grupos, 23

1.1. Introdução, 23
1.2. Axiomas de grupo, 23
1.3. Exemplos, 24
Exercício 1, 27
1.4. Lemas Básicos, 28
Exercício 2, 33
1.5. Isomorfismo, 34
Exercício 3, 35

1.6. Grupos de permutação, 36
Exercício 4, 39
1.7. Grupos cíclicos, 40
1.8. Grupos diedrais, 42
1.9. Subgrupos, 45
Exercício 5, 55
1.10. Homomorfismos, 56
Exercício 6, 64
1.11. Produtos diretos, 65
Exercício 7, 69

Capítulo 2 Anéis, 70

2.1. Definições, 70
2.2. Lemas Básicos, 74
2.3. Subanéis, 75
Exercício 1, 76
2.4. Homomorfismos, 77
Exercício 2, 85
2.5. Domínios de integridade, 86
Exercício 3, 89

Capítulo 3 Os Inteiros, 90

3.1. Introdução, 90
3.2. Ordem, 91
3.3. Ordem em Domínios de Integridade, 92
Exercício 1, 95
3.4. Conjuntos Bem-Ordenados, 95
Exercício 2, 96
3.5. Inteiros, 97
Exercício 3, 102
3.6. Aritmética nos Inteiros, 103
Exercício 4, 107

Capítulo 4 Corpos, 109

4.1. Introdução, 109
4.2. Corpo de Quocientes, 109
Exercício 1, 113
4.3. Subcorpos, 113
4.4. Homomorfismos de Corpos, 115
Exercício 2, 116
4.5. Os Números Reais, 117
Exercício 3, 121

4.6. Os Números Complexos, 121
Exercício 4, 126

Capítulo 5 Domínios Euclideanos, 128

5.1. Introdução, 128
5.2. O Algoritmo Euclideano, 130
Exercício 1, 133
5.3. Aritmética em Domínios de Integridade, 134
Exercício 2, 138
5.4. Aplicação aos Grupos, 139
Exercício 3, 141

Capítulo 6 Polinômios, 143

6.1. Introdução, 143
6.2. Anéis de Polinômios, 145
Exercício 1, 149
6.3. Polinômios sobre um Corpo, 150
Exercício 2, 153
6.4. Os Números Complexos, 154
Exercício 3, 156
6.5. Propriedades Especiais de **K** [**X**], 156
Exercício 4, 161
6.6. Factoração em $\mathscr{A}$[**X**], 161
Exercício 5, 168
6.7. Corpo de Quocientes de $\mathscr{A}$[**X**], 168
6.8. Polinômios em Várias Variáveis, 169
Exercício 6, 171

Capítulo 7 Espaços Vetoriais, 172

7.1. Introdução, 172
7.2. Definições e Exemplos, 173
Exercício 1, 176
7.3. Subespaços, 176
Exercício 2, 178
7.4. Dependência e Base, 178
Exercício 3, 185
7.5. Transformações Lineares, 185
Exercício 4, 190
7.6. Soluções de Sistemas de Equações Lineares, 191
Exercício 5, 195
7.7. Álgebras, 196
Exercício 6, 201

Capítulo 8 Extensões de Corpos e Corpos Finitos, 203

8.1. Construção de Extensões de Corpos, 203
Exercício 1, 210
8.2. Classificação de Extensões, 210
8.3. Extensões Transcendentes, 212
8.4. Extensões Algébricas, 214
Exercício 2, 218
8.5. Corpos Finitos, 218
Exercício 3, 223
8.6. Extensões Simples, 224
8.7. Raízes da Unidade, 225
8.8. Teorema de Wedderburn, 229
Exercício 4, 232

Capítulo 9 Grupos Finitos, 233

9.1. Teorema de Cauchy, 233
9.2. **p**-Grupos, 235
Exercício 1, 238
9.3. Os Teoremas de Sylow, 238
Exercício 2, 243
9.4. Grupos Solúveis, 244
Exercício 3, 250
9.5. Grupos Abelianos, 251
Exercício 4, 263

Capítulo 10 Teoria de Galois, 265

10.1. Teorema Fundamental da Teoria de Galois, 265
Exercício 1, 275
10.2. Corpos Ciclotômicos e Extensões Cíclicas, 276
10.3. Solução de Equações por Radicais, 279
10.4. Equações de 2.° e 3.° Graus, 286
Exercício 2, 291
10.5. O Polinômio Geral de **n**-ésimo Grau, 292
10.6. O Discriminante, 295
10.7. Polinômios Simétricos, 297
Exercício 3, 299

Respostas aos Exercícios, 300

Índice Alfabético, 309

Capítulo 0

Neste capítulo introdutório revisaremos alguns fatos sobre aritmética e reuniremos uns poucos conceitos básicos sobre conjuntos, relação e funções. A maioria destas noções é familiar, e este capítulo serve simplesmente para introduzir as notações e convenções usadas através do livro e selecionar dos muitos fatos matemáticos que já conhecemos aqueles que têm um especial significado para este livro. Por agora adotamos o ponto de vista de que podemos usar estes fatos bem aceitos da aritmética e da teoria dos conjuntos sem prova. Daremos, ocasionalmente, neste capítulo, curtos argumentos de suporte a um teorema na esperança de ampliar seu significado. Devemos fazer uma leitura rápida porém cuidadosa deste capítulo antes de passar ao Prólogo e ao início do próprio texto. Será provavelmente prudente voltar ao Cap. 0 de tempos em tempos para recordar definições e notações à medida que surjam.

0.1. ARITMÉTICA

Neste capítulo e nos dois capítulos seguintes faremos uso dos inteiros como uma fonte de exemplos. Serão usados para provar teoremas e estabelecer definições. As propriedades que necessitaremos serão familiares, e não tentaremos até o Cap. 3 um tratamento cuidadoso dos inteiros como uma teoria axiomática. Suporemos que inteiros podem ser adicionados, subtraídos, multiplicados, e que são ordenados por "maior do que" e "menor do que". Designaremos o conjunto dos inteiros por I.

Teorema 1. Se a e b são inteiros positivos e se a divide b então $a \leq b$.

Adotamos a notação usual que emprega a barra vertical para designar divisão. Escrevemos $a|b$ se, e somente se, a divide b. Se a não divide b escreveremos $a \nmid b$. Assim, $2|4$, $3|12$, mas $2 \nmid 5$.

Teorema 2. Se a é um inteiro positivo e b é qualquer inteiro, então existem inteiros q e r tais que

$$b = a \cdot q + r \text{ onde } 0 \leq r < a.$$

Se $0 \leq b < a$ podemos tomar $q = 0$ e $r = b$. Se $b \geq a$ então o Teorema 2 diz, na linguagem da aritmética elementar, que a divide b (este é o caso $r = 0$) ou se dividirmos b por a obteremos um resto que é menor que a.

Definição. Um inteiro p distinto de 0 e de $\pm$ 1 é chamado *primo* se, para todos os inteiros a e b, sempre que $p \mid ab$, então $p \mid a$ ou $p \mid b$. Um inteiro distinto de 0 e de $\pm$ 1 e que não é primo é chamado *composto*.

Teorema 3. Seja p um inteiro tal que $p \neq 0, \pm 1$. p é primo se, e somente se, para todos os inteiros a e b, verifica-se o seguinte: se $p = ab$, então $p = \pm a$ ou $p = \pm b$.

É prática comum inverter as posições da definição de um primo e do Teorema 3. Nossa posição coincide com a definição, geralmente aceita, e que daremos no Cap. 2, de um elemento primo no contexto mais geral de um domínio de integridade arbitrário. No Cap. 2 um elemento que satisfaz a conclusão do Teorema 3 será chamado um elemento irredutível.

Teorema 4 (*Princípio de indução*). Uma asserção referente a um inteiro m pode ser provada para todos os inteiros m maiores ou iguais a um inteiro particular, digamos a_0, pelos dois passos seguintes:

A. Dar uma prova ou uma verificação de que a asserção vale para o inteiro a_0.

B. Provar o lema seguinte: Seja k um inteiro qualquer tal que $k \geq a_0$. *Se* a asserção é verdadeira para k *então* é verdadeira para o inteiro $(k + 1)$.

O passo (*B*) é chamado "passo indutivo", e a hipótese do lema é chamada "hipótese de indução". Dizemos que a asserção foi provada por "indução sobre m".

Há um outro modo de ver este princípio. Suponhamos que se tenha uma asserção que asseguramos ser verdadeira para todos os inteiros maiores ou iguais a a_0. Se alguma crítica diz que não é assim, então deve haver um menor inteiro h tal que $h \geq a_0$ para o qual a nossa asserção é falsa. Claramente $h \neq a_0$ porque foi provado em (*A*) que nosso resultado vale para a_0; logo $h > a_0$ e $(h - 1) \geq a_0$. Além disso, h tendo sido escolhido como o menor inteiro para o qual nossa asserção é falsa, ela deve ser verdadeira para $(h - 1)$. Então se pusermos $k = (h - 1)$ no lema *B*, que foi provado, e ao qual nossa crítica não faz objeção, concluímos

que a asserção é verdadeira para o inteiro $(k + 1)$, isto é, para h. Logo nossa crítica deve estar errada.

Um esquema análogo pode também ser usado para definir um conceito envolvendo inteiros.

A^*. Definimos explicitamente o conceito para um inteiro inicial a_0. (Na prática a_0 é usualmente 0, 1, ou 2.)

B^*. Seja k qualquer inteiro tal que $k \geq a_0$. O conceito é definido para $(k + 1)$ em termos do conceito para os inteiros m tais que $a_0 \leq m \leq k$. (Nesta passagem é apropriado tratar o conceito como completamente definido para inteiros entre a_0 e k.)

Exemplo 1. Definiremos exponenciação para potências inteiras não-negativas por indução. Seja r um número real.

A^*. $r^0 = 1$.

B^*. Se k é um inteiro não-negativo, então $r^{(k+1)} = r^k \cdot r$.

Freqüentemente vemos r^k "definido" por algum artifício de notação como $r^k = \underbrace{r \cdot \cdots \cdot r}_{k \text{ fatores}}$.

Apesar de ser este procedimento na melhor das hipóteses deselegante e na pior, sem sentido é o que transmite a noção da melhor maneira. A vantagem de usar indução para obter definições de conceitos matemáticos é que se pode então fazer demonstrações por indução que são precisas, elegantes e completas. Como um exemplo vamos provar por indução as leis de adição e multiplicação para a exponenciação usando a definição acima.

I. Se r é um número real, então para todos os inteiros não-negativos n e m,

$$r^n \cdot r^m = r^{n+m}.$$

Provemos por indução sobre m. A proposição é verdadeira quando $m = 0$ porque, pela definição A^*, $r^0 = 1$ e $r^n \cdot 1 = r^n = r^{n+0}$. Agora o lema B. As hipóteses particulares deste lema são que k é um inteiro positivo e que $r^n \cdot r^k = r^{n+k}$. Então $r^n \cdot r^{k+1} = r^n \cdot (r^k r)$ pela definição B^* enquanto, pela associatividade, $r^n \cdot (r^k r) = (r^n \cdot r^k) \cdot r$. Mas havíamos suposto $r^n \cdot r^k = r^{n+k}$ e assim $r^n \cdot r^{(k+1)} = r^{n+k} \cdot r$, o que, por definição, é $r^{(n+k)+1} = r^{n+(k+1)}$. Logo o lema B, o passo indutivo, foi estabelecido.

II. Se r é um número real, então para todos os inteiros não-negativos n e m,

$$(r^n)^m = r^{nm}.$$

Provemos por indução sobre m. A proposição vale quando $m = 0$ porque $(r^n)^0 = 1 = r^0$. As hipóteses indutivas supõem que $k \geq 0$ e que $(r^n)^k = r^{nk}$. Agora $(r^n)^{(k+1)} = (r^n)^k \cdot r^n$ pela definição B^* e da hipótese indutiva, $(r^n)^k = r^{nk}$. Logo $(r^n)^{(k+1)} = r^{nk} \cdot r^n$. De (I) e da lei distributiva para inteiros resulta $r^{nk} \cdot r^n = r^{nk+n} = r^{n(k+1)}$ e assim o passo indutivo foi estabelecido.

0.2. CONJUNTOS

Adotaremos uma atitude informal em relação à teoria dos conjuntos. Falaremos sobre conjunto e seus elementos; operaremos com conjuntos, considerando relações sobre conjuntos, funções de um conjunto para outro, e formando novos conjuntos por várias construções. Em nenhum lugar neste texto tentaremos construir um fundamento próprio para a teoria dos conjuntos. Nosso desenvolvimento supõe a teoria dos conjuntos como básica para a matemática e usa-a informalmente como uma linguagem para expressar idéias matemáticas. É, entretanto, nossa intenção, sermos cuidadosos com a apresentação da teoria dos conjuntos no sentido de que cada teorema poderia, de modo direto, ser incorporado em uma teoria formal. Tentaremos pôr em evidência aquelas ocasiões em que a formalização não seja possível por métodos rotineiros.

As noções de "conjunto" e "pertinência" serão aceitas como noções primitivas. Pertinência é uma asserção sobre dois conjuntos. Se A e B são conjuntos, A é um membro de B ou A não é um membro de B. A pertinência é designada pelo símbolo $\in$ e a escrita simbólica usual

$$A \in B$$

significa qualquer das sentenças sinônimas seguintes:

O conjunto A é um membro do conjunto B.

O conjunto A pertence ao conjunto B.

A está em B.

A notação $A \notin B$ significa que A não é um membro de B. Se $A \in B$ dizemos que A é um *elemento* de B.

Concebemos um conjunto como uma entidade independente que é uma coleção de seus elementos. Do nosso ponto de vista elementos são apenas outros conjuntos. "Conjunto" é um coletivo no mesmo sentido em que o são "bando" e "teoria". Um "bando" é uma coleção de "gansos", uma "teoria" é uma coleção de "teoremas", e um "conjunto" é uma coleção de "elementos". Freqüentemente fazemos a distinção relativa entre um conjunto e seus elementos usando letras minúsculas para os elementos de um conjunto e uma letra maiúscula para o conjunto. Assim "$a \in A$" será uma notação típica neste livro.

O símbolo de igualdade (=) é usado entre dois símbolos denotando conjuntos como uma escrita simbólica para assegurar que os dois símbolos são nomes para o mesmo conjunto. Assim $2 = 1 + 1$ assegura que 2 e $1 + 1$ são nomes para o mesmo inteiro; designam o mesmo conjunto.

Mas que significa dizer que dois conjuntos são o "mesmo"? Intuitivamente, seria natural concordar que dois conjuntos são o mesmo se têm os mesmos elementos. Na realidade, adotamos, como um axioma, o critério seguinte para decidir quando dois conjuntos são o mesmo. O axioma é enunciado em termos dos conceitos primitivos.

Axioma de Extensão

$A = B$ se, e somente se, para todos os conjuntos x, se $x \in A$ então $x \in B$ e se $x \in B$ então $x \in A$.

Este axioma estabelece que um conjunto é determinado pelos seus elementos. Quando conveniente listamos os elementos que são membros de um conjunto A e mostramos que esta lista designa o conjunto colocando-a entre chaves. Por exemplo, $\{0, 1\}$ designa o conjunto cujos elementos são 0 e 1. Note que $\{0, 1\} = \{1, 0\}$ e $\{0, 0\} = \{0\}$.

Um conjunto $S = \{a\}$ contém um único membro. O conjunto que não contém membros será referido como o *conjunto vazio* ou o *conjunto nulo* e será denotado por $\varnothing$.

Uma listagem é impossível para conjuntos infinitos e inconveniente para outros conjuntos. Nestes casos freqüentemente empregamos a chamada notação construtiva. Um exemplo dará a idéia. Suponhamos que se deseje designar o conjunto R de números reais entre 0 e 1. Escolhemos um símbolo para um elemento, digamos r. Se r é um membro de R, então r é um número real e $0 \leq r \leq 1$. O conjunto R é designado na notação construtiva do seguinte modo:

$$\{r : r \text{ é um número real e } 0 \leq r \leq 1\}.$$

Lê-se, "o conjunto de todos os r tais que r é um número real e 0 é menor ou igual a r e r é menor ou igual a 1".

De modo mais geral, um conjunto é com freqüência determinado pelas condições que seus elementos devem satisfazer. Se por brevidade chamamos estas condições C então designamos o conjunto determinado por estas condições por

$$\{x : x \text{ satisfaz as condições } C\}.$$

Estamos agora vendo um conjunto como determinado por uma condição ou propriedade. O conjunto consiste de precisamente aqueles elementos satisfazendo uma condição ou condições específicas. As condições podem ser muito complexas e na realidade pode não ser sempre possível decidir se um elemento satisfaz as condições dadas.

O conjunto vazio é um conjunto tal que $x \notin \varnothing$ para todos os conjuntos x. Temos também $\varnothing = \{x : x \neq x\}$.

Empregamos também uma outra conveniência de notação na designação de conjuntos. Listando um conjunto podemos dar uns poucos membros típicos e segui-los com três pontos (...) para indicar que o conjunto pode ter mais elementos que não tomamos o cuidado de descrever. Assim poderíamos denotar os inteiros positivos como $\{1, 2, 3, \ldots\}$. Esta notação é muito pouco satisfatória posto que os elementos do conjunto devem ser efetivamente determinados do contexto da situação; em particular, devemos poder decidir se o conjunto é finito ou infinito.

Apresentamos aqui algumas abreviaturas especiais: $|A|$ designa o número cardinal dos elementos de A. Escrevemos $A \subseteq B$ se, e somente se, $x \in B$ sempre que $x \in A$. Logo $A \subseteq B$ significa que cada elemento de A é um elemento de B.

$A \subseteq B$ é freqüentemente lido: "A está contido em B" ou "A está incluído em B" e dizemos que A é um *subconjunto* de B. Claramente $A = B$ se, e somente se, $A \subseteq B$ e $B \subseteq A$. Note que $\varnothing \subseteq A$ e $A \subseteq A$ para todos os conjuntos A. A e $\varnothing$ são chamados subconjuntos *impróprios* de A; todos os outros subconjuntos de A são chamados subconjuntos *próprios*. Escrevemos $A \subset B$ se $A \subseteq B$ e $A \neq B$.

$$A - B = \{x : x \in A \text{ e } x \notin B\}.$$
$$A \cup B = \{x : x \in A \text{ ou } x \in B\}.$$

A palavra "ou", é aqui usada no sentido inclusivo de "e/ou". Um exemplo é $\{0, 1, 2\} \cup \{0, 3\} = \{0, 1, 2, 3\}$.

$$A \cap B = \{x : x \in A \text{ e } x \in B\}.$$

Se A é um conjunto escreveremos $\bigcup A$ para o conjunto $\{x :$ existe um $a \in A$ tal que $x \in a\}$. $\bigcup A$ é chamado o conjunto união dos conjuntos em A. Analogamente escrevemos $\bigcap A$ para o conjunto $\{x : x \in a$ para todo $a \in A\}$. $\bigcap A$ é chamado o conjunto interseção dos conjuntos em A. Note que se $A = \{a_1, a_2\}$, então $\bigcup A = a_1 \cup a_2$.

Empregaremos dois tipos de diagramas para mostrar as várias relações entre conjuntos. Um deles é o familiar diagrama de Venn com regiões designando conjuntos. Tomemos por exemplo,

$$\begin{aligned} A &= \{\text{todos os inteiros}\}, \\ B &= \{\text{todos os inteiros múltiplos de } 6\}, \\ C &= \{\text{todos os inteiros múltiplos de } 15\}, \\ B \cap C &= \{\text{todos os inteiros múltiplos de } 30\}. \end{aligned}$$

A Fig. 1 ilustra esta técnica.

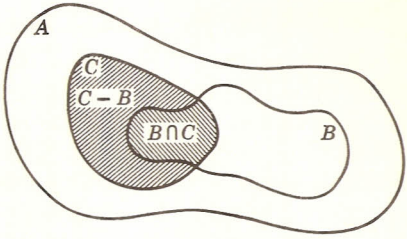


Fig. 1

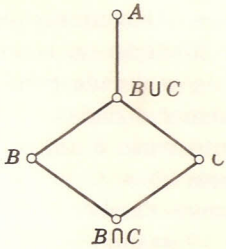


Fig. 2

Um outro tipo de diagrama usa um ponto para designar um conjunto. Se um conjunto B é um subconjunto de um conjunto A, então o ponto para A é desenhado mais alto do que o ponto para B e traçamos uma linha de um para o outro ponto. A Fig. 2 ilustra esta técnica para o exemplo acima. Nossa convenção não exige que se trace uma linha distinta de B para A porque os segmentos de reta de B para $B \cup C$ e de $B \cup C$ para A fornecem uma indicação de que B é um subconjunto de A. Uma outra linha seria supérflua. Na linguagem da seção

seguinte a relação de inclusão ($\subseteq$) é uma relação transitiva sobre os subconjuntos de um conjunto e exploramos isto no diagrama.

Dizemos que os membros de um conjunto A são *mutuamente disjuntos* se para quaisquer dois conjuntos distintos a e b em A, $a \cap b = \varnothing$.

Exemplo 2. Seja a o conjunto dos inteiros ímpares e b o conjunto dos inteiros pares. Então $A = \{a, b\}$ tem membros mutuamente disjuntos. Se c é o conjunto dos múltiplos de 3 e $B = \{a, b, c\}$, então os elementos de B não são mutuamente disjuntos. Note que $\cup A = \cup B$.

Temos uma necessidade constante de usar o conceito de um "par ordenado" de elementos. Por exemplo, em geometria analítica um ponto do plano é dado por dois números — suas ordenadas. Concordamos em escrever primeiro a coordenada x do ponto e então sua coordenada y. Deste modo o ponto com coordenadas (1, 2) é distinguido do ponto (2, 1). A distinção é feita pelo nosso esquema de notação; a coordenada x aparece como o número da esquerda. Podemos nos livrar da dependência do esquema de notação de "esquerda" e "direita" usando uma definição introduzida por Norbert Wiener e C. Kuratowski:

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Assim o par ordenado (a, b) é um conjunto consistindo de no máximo dois elementos, o conjunto $\{a\}$ e o conjunto $\{a, b\}$. É claro que, se $a \neq b$, então $(a, b) \neq (b, a)$. Na realidade, $(a, b) = (b, a)$ se, e somente se, $a = b$. Note que $(a, a) = \{\{a\}\}$, o conjunto de um elemento cujo único elemento é o conjunto $\{a\}$. De modo geral, $(a, b) = (c, d)$ se, e somente se, $a = c$ e $b = d$. $A \times B$ designa o conjunto $\{(a, b) : a \in A \text{ e } b \in B\}$. $A \times B$ é chamado o *produto cartesiano* de A e B.

0.3. RELAÇÕES

Sejam A e B dois conjuntos. Havendo uma razão para associar certos elementos de A a certos elementos de B, usamos a palavra "relação" e dizemos que os elementos associados estão relacionados. Assim se A é o conjunto de todos os homens vivos e B é o conjunto de todas as mulheres vivas poderíamos dizer que o homem a está relacionado a mulher b se a foi alguma vez casado com b. Este relacionamento pode naturalmente ser muito complexo! A noção importante é que estamos escolhendo certos pares ordenados (a, b) de $A \times B$ e dizendo que os pares ordenados escolhidos, a e b estão relacionados. A escolha dos pares ordenados constitui, é claro, uma forma de definição para qualquer propósito desejado, e é a essência da definição matemática formal de relação.

Definição. Uma *relação binária* entre os conjuntos A e B é um subconjunto T do produto cartesiano $A \times B$.

Como um exemplo, seja A o conjunto dos inteiros positivos e B o conjunto dos inteiros negativos. Seja $T = \{(a, b) : a + b = 0\}$. Assim, T contém os pares $(1, -1)$, $(2, -2)$, e assim por diante. Freqüentemente empregamos um símbolo especial, digamos τ, escrevendo $a \tau b$ se, e somente se, $(a, b) \in T$. Analogamente

escrevemos $a \not T b$ se, e somente se, $(a, b) \notin T$. Se $A = B$ falamos de uma *relação binária* sobre A.

Exemplo 3. Seja A o conjunto dos inteiros não-negativos. Seja $T = \{(a, b): a$ divide $b\}$. Aqui o símbolo de relação é a barra vertical mencionada anteriormente.

Um subconjunto especial de A de importância na discussão de uma relação T é o domínio $\mathscr{D}_T$ da relação T:

$$\mathscr{D}_T = \{a : \text{existe } b \in B \text{ tal que } (a, b) \in T\}.$$

Analogamente o contradomínio $\mathscr{R}_T$ de T é um subconjunto de B:

$$\mathscr{R}_T = \{b : \text{existe } a \in A \text{ tal que } (a, b) \in T\}.$$

Exemplo 4. Seja $A = B$ o conjunto de todos os números reais. Seja

$$T = \{(x, y) : x^2 + (y - 1)^2 = 1\}.$$

Temos:

$$\mathscr{D}_T = \{x : -1 \leq x \leq 1\} \qquad \text{e} \qquad \mathscr{R}_T = \{y : 0 \leq y \leq 2\}.$$

Os pontos do plano cujas coordenadas cartesianas correspondem a esta relação estão sobre um círculo de raio 1 e centro (0, 1).

Uma classe especial de relação sobre um conjunto A que desempenham um papel fundamental em matemática consiste daquelas relações chamadas relações de equivalência.

Definição. Uma relação binária E sobre um conjunto A é chamada uma *relação de equivalência* sobre A se são válidas as três propriedades seguintes:

1. Para todo $a \in A$, $(a, a) \in E$.
2. Para todo a e b em A, se $(a, b) \in E$, então $(b, a) \in E$.
3. Para todo a, b e c em A, se $(a, b) \in E$ e $(b, c) \in E$, então $(a, c) \in E$.

Uma relação que satisfaz (1) é chamada *reflexiva*.
Uma relação que satisfaz (2) é chamada *simétrica*.
Uma relação que satisfaz (3) é chamada *transitiva*.

Introduzindo o símbolo especial ($\sim$) para uma relação de equivalência E, as propriedades poderão ser enunciadas como se segue:

1*. Para todo $a \in A$, $a \sim a$.
2*. Para todo a e b em A, se $a \sim b$, então $b \sim a$.
3*. Para todo a, b e c em A, se $a \sim b$ e $b \sim c$, então $a \sim c$.

É freqüente pensar que simetria e transitividade implicam reflexividade argumentando que (2*) dá $a \sim b$ e $b \sim a$ e então (3*) dá $a \sim a$. Entretanto, o exemplo seguinte mostra que este não é o caso.

Exemplo 5. Seja $A = \{x, y\}$ e $R = \{(y, y)\}$.

Assim $y \sim y$ é a única relação! (1*) não vale porque $x \not\sim x$; entretanto, (2*) e (3*) são válidos. A dificuldade com o argumento errôneo dado acima é que x pode não estar relacionado a nenhum elemento, como no caso do Ex. 5. Se

x fosse relacionado a algum elemento, então o argumento seria válido e mostraria que $x \sim x$.

Exemplos de Relações de Equivalência

1. Seja A o conjunto das figuras geométricas planas. Seja $a \sim b$ se, e somente se, a é congruente a b.

2. Seja A o mesmo conjunto em (1). Seja $a \sim b$ se, e somente se, a é semelhante a b.

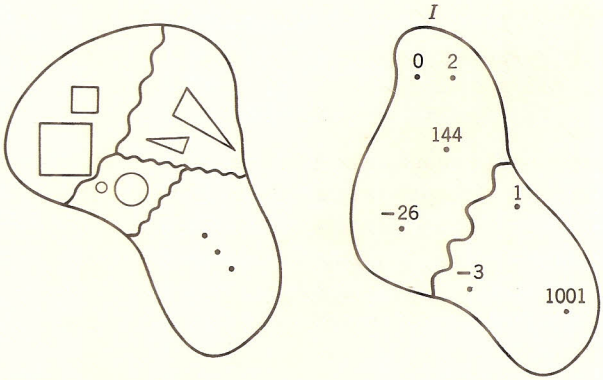
3. Seja A o conjunto dos automóveis existentes no mundo no dia de hoje. Seja $a \sim b$ se, e somente se, a e b são feitos pelo mesmo fabricante.

4. Seja A o conjunto de todos os inteiros. Seja $a \sim b$ se, e somente se, 2 divide $a - b$.

5. Seja A o conjunto de todas as funções contínuas sobre o intervalo fechado $[0, 1] = \{x : 0 \leq x \leq 1\}$. Seja $a(x) \sim b(x)$ se, e somente se, $\int_0^1 a(x)dx = \int_0^1 b(x)\, dx$.

A mais importante propriedade de uma relação de equivalência sobre um conjunto é que ela particiona o conjunto em subconjuntos mutuamente disjuntos chamadas classes de equivalência. Uma classe de equivalência contendo um elemento x consiste precisamente dos elementos equivalentes a x. No exemplo (4) acima há duas classes de equivalência, os números ímpares e os números pares. Em (1) acima há muitas classes de equivalência, uma delas é o conjunto de todos os quadrados de lado 1 cm. As classes de equivalência de (2) e (4) são ilustradas na Fig. 3. A situação geral é estabelecida no teorema seguinte.

Teorema 5. Seja A um conjunto não-vazio e designemos por σ uma relação de equivalência sobre A. Para todo $x \in A$ seja $S_x = \{y : y \sigma x\}$. A é o conjunto soma do conjunto de subconjuntos S_x não-vazios e mutuamente disjuntos; $A = \cup \{S_x : x \in A\}$. S_x é chamada uma *classe de equivalência* de A sob σ. Reciprocamente, se A é o con-



Exemplo (2) Exemplo (4)

Fig. 3

junto soma de um conjunto T de subconjuntos de A não-vazios e mutuamente disjuntos, então pode ser definida uma relação de equivalência τ sobre A de modo que os elementos de T sejam as classes de equivalência de A sob τ.

DEMONSTRAÇÃO. *Parte I.* Indiquemos com σ uma relação de equivalência sobre o conjunto não-vazio A. Para cada $x \in A$, seja S_x o subconjunto de A definido no teorema. Como σ é reflexiva, $x \in S_x$ e assim S_x é não-vazio. Segue de $x \in S_x \in A$ que $A = \bigcup \{x : x \in A\} \subseteq \bigcup \{S_x : x \in A\} \subseteq A$.

Agora suponhamos que $S_x \cap S_y \neq \varnothing$ e seja $z \in S_x \cap S_y$. Temos por definição $z \sigma x$ e $z \sigma y$, logo $x \sigma y$ e $y \sigma x$ seguem da transitividade e da simetria de σ. Mas se $v \in S_x$, então $v \sigma x$ e como $x \sigma y$, novamente por transitividade, temos $v \sigma y$. Logo $S_x \subseteq S_y$. Analogamente concluímos que $S_y \subseteq S_x$ e então que $S_x = S_y$. Portanto as classes de equivalência de A sob σ formam um conjunto mutuamente disjunto de subconjuntos não-vazios de A. Temos efetivamente $S_x = S_y$ se, e somente se, $x = y$.

Parte II. Seja $A = \bigcup T$ onde T é um conjunto de subconjuntos de A não-vazios e mutuamente disjuntos. Recordemos que um elemento t de T é um subconjunto de A. Definimos uma relação E sobre A como segue: $(x, y) \in E$ se, e somente se, x e y pertencem ao mesmo subconjunto $t \in T$. E é trivialmente reflexiva e simétrica. Vemos facilmente que E é também transitiva, e então E é uma relação de equivalência que denotaremos por τ. Devemos agora provar que se $t \in T$, então existe um $x \in T$ tal que $t = \{y : y \in A \text{ e } y \tau x\}$. Por hipótese, t é um subconjunto não-vazio de A, e seja $x \in t$. Agora, por definição, para todo $y \in A$ temos $y \tau x$ se, e somente se, y pertence a t. Logo, $t = \{y : y \in A \text{ e } y \tau x\}$.

0.4. FUNÇÕES E APLICAÇÕES

Um dos conceitos mais centrais de toda a matemática é o conceito de *função*. Em sua forma básica uma função é um tipo especial de relação.

Definição. Uma *função* f é uma relação entre conjuntos A e B tal que:

$$\text{Se } (a, b) \in f \text{ e } (a, c) \in f, \text{ então } b = c.$$

Esta definição simplesmente assegura que o segundo membro de um par ordenado pertencente a f é univocamente determinado pelo primeiro membro. Quando a relação f é uma função é costume escrever o par ordenado como $(a, f(a))$. Note, também, que nos temos afastado da nossa convenção de usar letras maiúsculas para conjuntos porque a notação usual para uma função é uma letra minúscula. Veremos mais tarde que é conveniente usar letras gregas minúsculas para denotar certas funções.

Definição. Se f é uma função entre A e B, A é chamado a *fonte* e B a *meta* de f. Se f é tal que $\mathscr{D}_f = A$ dizemos que f é uma função *de A em B*. Se $\mathscr{D}_f = A$ e $\mathscr{R}_f = B$, então dizemos que f é uma função *de A sobre B*.

A distinção entre as palavras *em* e *sobre* é crucial! É claro que cada função de A sobre B é também uma função de A em B e qualquer função é uma função do seu domínio sobre seu co-domínio. É usual dizer que uma função f de A sobre B é uma função *sobrejetiva* ou que f é uma *sobrejeção* de A para B.

Nos Exs. 6 a 8 a seguir, a fonte A é o conjunto de todos os números reais e $A = B$.

Exemplo 6. $f = \{(x, y) : y = x^2\}$, $\mathscr{D}_f = A$ e $\mathscr{R}_f = \{x : 0 \leq x\}$. f é uma função de A em A.

Exemplo 7. $g = \{(x, y) : y^2 = x^2\}$ não é uma função porque, por exemplo, $(1, 1)$ e $(1, -1)$ pertencem a g. $\mathscr{D}_g = \mathscr{R}_g = A$.

Exemplo 8. $h = \{(x, y) : y = \sqrt{1 - x^2}\}$, $\mathscr{D}_h = \{x : |x| \leq 1\}$ e $\mathscr{R}_h = \{y : 0 \leq y \leq 1\}$. h é uma função de fonte e meta A.

Exemplo 9. Sejam $A = \{a_1, a_2, a_3, a_4\}$ e $B = \{b_1, b_2, b_3, \ldots\}$. Seja $k = \{(a_1, b_1), (a_2, b_1), (a_3, b_3)\}$. $\mathscr{D}_k = \{a_1, a_2, a_3\}$ e $\mathscr{R}_k = \{b_1, b_3\}$. k é uma função de fonte A e meta B.

Exemplo 10. Seja A um qualquer conjunto. A função identidade de A sobre A é $\{(x, x) : x \in A\}$; isto é, $\iota(x) = x$, para todo $x \in A$.

Exemplo 11. Sejam A e B dois quaisquer conjuntos. Seja b um elemento fixado de B. A função constante f_b é $\{(x, b) : x \in A\}$; isto é, $f_b(x) = b$ para todo $x \in A$.

Exemplo 12. Seja A um qualquer conjunto. Seja S qualquer subconjunto de A. Seja $B = \{0, 1\}$. A *função característica* c_S é a função $\{(x, 1) : x \in S\} \cup \{(x, 0) : x \notin S\}$; isto é,

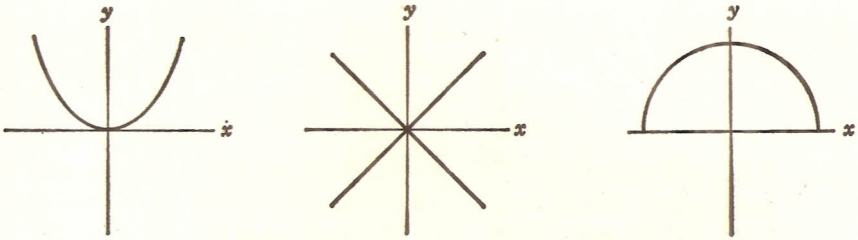
$$c_S(x) = \begin{cases} 1 \text{ se } x \in S \\ 0 \text{ se } x \notin S \end{cases}$$

Exemplo 13. Uma *seqüência* é uma função especial. Seja A um subconjunto dos inteiros não-negativos $\{0, 1, 2, \ldots\}$. Seja B qualquer conjunto. Uma sucessão ou seqüência é uma função s de A em B. Denotamos usualmente o segundo elemento do par ordenado $(i, b) \in s$ por s_i e indicamos então a seqüência por $\{s_i : i \in A\}$. Se $A = \{0, 1, \ldots\}$ escrevemos usualmente $\{s_0, s_1, \ldots\}$.

Definição. Seja A o conjunto finito de inteiros positivos $\{1, 2, \ldots, n\}$. Seja B um qualquer conjunto. Uma *n-upla* de elementos de B é uma seqüência de A em B. Uma n-upla será designada por $(b_1, \ldots, b_n)$.

Um par ordenado (a, b) pode ser identificado com uma 2-upla e $A \times B$ pode ser identificado com o conjunto de todas as 2-uplas (s_1, s_2) que são funções de $\{1, 2\}$ em $A \cup B$ tais que $s_1 \in A$ e $s_2 \in B$. $A_1 \times \ldots \times A_n$ denotará todas as n-uplas $(a_1, \ldots, a_n)$ de $A_1 \cup \ldots \cup A_n$ tais que $a_i \in A_i$ para $i = 1, \ldots, n$.

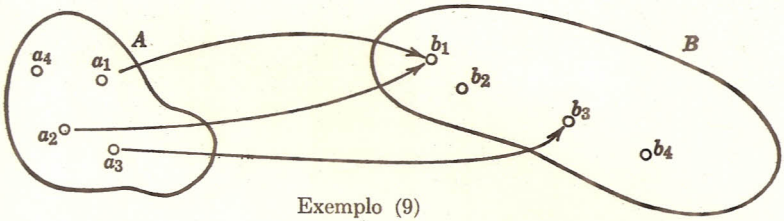
Em geometria analítica aprendemos a representar os pontos (x, y) satisfazendo uma relação sobre os números reais para construir um gráfico. Os Exs. 6, 7 e 8 são representados graficamente na Fig. 4.



Exemplo (6) Exemplo (7) Exemplo (8)

Fig. 4

Representaremos o Ex. 9 de maneira diferente. Exploramos a noção de que uma função associa a um elemento particular de um conjunto A no máximo um elemento de um conjunto B. A palavra "aplicação" é sugestiva e é usada como um sinônimo de função. Se $(a, b) \in f$, então b é chamado a *imagem* de a sob f, e a é chamada a pré-imagem ou imagem inversa de b sob f. Note que um elemento de B pode ter muitas pré-imagens ou nenhuma pré-imagem sob f. Assim uma função aplica certos elementos de A em elementos de B. Para visualizar isto, é conveniente desenhar um conjunto simbólico A e um conjunto simbólico B e ligá-los por setas para indicar esta aplicação. A Fig. 5 é uma visualização desta espécie para o Ex. 9.



Exemplo (9)

Fig. 5

Em geral usamos uma representação simbólica como a que é mostrada na Fig. 6. Escrevemos simbolicamente $f : A \to B$ quando f é uma aplicação de A em B.

Definição. Seja $A \subseteq A_1$ e $B \subseteq B_1$. Se $f : A \to B$ e $g : A_1 \to B_1$, dizemos que g é uma *extensão* de f se $f \subseteq g$. Se $f : A \to B$ e se $S \subseteq A$, dizemos que $h : S \to B$ é a *restrição* de f a S se $\mathscr{D}_h = S \cap \mathscr{D}_f$ e $h \subseteq f$.

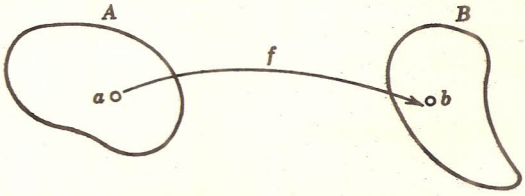


Fig. 6

Exemplo 14. Seja $A = B = \{$números racionais$\}$. Seja $f : A \to B$ a função $\{(r, r^2) : r \in A\}$. Seja $A_1 = B_1 = \{$números reais$\}$. Seja $g = \{(r, r^2): r \in A\} \cup \cup \{(x, 0) : x \in A_1 - A\}$. Então g é uma extensão de f. Seja $S = \{x : x$ é racional e $0 \leq x \leq 1\}$. Seja $h : S \to S$ a função $\{(r, r^2): r \in S\}$. h é aqui a restrição de f a S.

Definição. Uma aplicação $f : A \to B$ é chamada injetiva ou é uma *injeção* de A em B, se sempre que (a, b) e (c, b) estão em f então $a = c$. Se f é injetiva e sobrejetiva diremos que f é *bijetiva* ou é uma *bijeção* de A sobre B.

É apenas um exercício de vocabulário ver que uma função é injetiva se, e somente se, cada elemento em seu co-domínio tem uma única pré-imagem em A.

Definição. *Composição de aplicações.* Seja $f : A \to B$ uma aplicação de A em B e seja $g : B \to C$ uma aplicação de B em C. A aplicação $h : A \to C$ de A em C dada por $h = \{(a, g(f(a))) : a \in A\}$ é chamada a composta de f e g. Escrevemos $h = gf$. A Fig. 7 ilustra este processo.

tal que $f(A) \subset D_g$

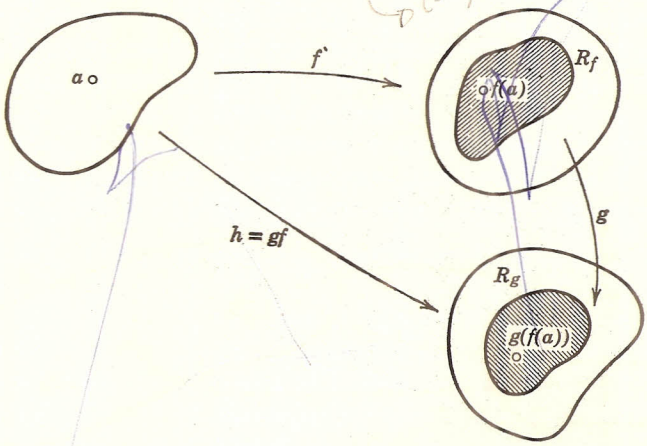


Fig. 7

É importante realizar que nossa notação escreve as aplicações da direita para a esquerda. gf significa aplicar primeiro a aplicação f e então a aplicação g. Isto é consistente com a notação habitual para as funções. Assim sen $2x$ representa a composição da função f dada por $f(x) = 2x$ e da função g dada por $g(y) =$ sen y, enquanto 2 sen x representa fg.

Teorema 6. Se f é uma injeção de A em B, então existe uma sobrejeção g de B para A tal que gf é a função identidade sobre A. A função g é univocamente determinada se, e somente se, $|A| = 1$ ou f é uma bijeção de A sobre B.

0.5. OPERAÇÕES E OPERADORES

Definição. Uma *operação binária* sobre um conjunto A é uma aplicação de $A \times A$ em A.

Em termos mais vivos, porém ligeiramente menos precisos, uma operação binária é uma regra que nos diz como combinar um par de elementos para obter um elemento do conjunto A. Adição, subtração, multiplicação e divisão fornecem exemplos tirados de nossas primeiras experiências matemáticas. Na realidade poderíamos apresentar a tábua de adição na forma seguinte:

$$+ = \{((1, 1), 2), ((1, 2), 3), ((2, 1), 3), \ldots\}.$$

Com auxílio de uma notação que deve ser usada circularmente poderíamos escrever:

$$+ = \{((a, b), c) : a + b = c\}!$$

Podemos sem perda de precisão, ver uma operação binária m sobre A como um conjunto de triplas ordenadas (3-uplas) de A. Podemos considerar m como o conjunto $\{(a, b, c) : ((a, b), c) \in m\}$. Por exemplo, $(1, 2, 3) \in +$.

Se m é uma operação binária sobre A usaremos com freqüência um novo símbolo, digamos $(*)$, escrevendo $a * b = c$ se $((a, b), c)$ pertence a m. Na maioria das vezes simplesmente justapomos a e b, escrevendo $ab = c$. Esta é a prática usual para a multiplicação em álgebra enquanto $(\times)$ ou $(\cdot)$ é usualmente empregado para a multiplicação de números reais. Assim é que vemos $2 \times 3 = 6$ ou $2 \cdot 3 = 6$.

Exemplo 15. Seja S um conjunto; A consiste de todas as aplicações de S em S. A composição de aplicações é uma operação binária sobre A.

Definição. Denotemos por $(*)$ uma operação binária sobre A. A operação é chamada *associativa* se para todo a, b e c em A, $(a * b) * c = a * (b * c)$. A operação é dita *comutativa* se para todo a e b em A, $a * b = b * a$.

Se $(*)$ designa uma operação binária sobre A ainda não foi definido o que deve significar o símbolo $a_1 * a_2 * \ldots * a_n$. Por exemplo, se a operação é $(+)$ sobre os inteiros o que designa $6 + 4 + 1$? 11, naturalmente! Entretanto se a operação binária é a subtração $(-)$ sobre o conjunto dos inteiros então o símbolo $6 - 4 - 1$ é ambíguo.

Definição. Seja $m : A \times A \to A$ uma operação binária sobre um conjunto A que será denotada por $(*)$. Indicaremos com $a_1 * a_2 * a_3$ a imagem sob m do par ordenado $(a_1 * a_2, a_3)$. Isto é, $a_1 * a_2 * a_3$ é o elemento obtido primeiro determinando $(a_1 * a_2)$ e então $(a_1 * a_2) * a_3$. Na realidade é costume usar parênteses para indicar que vamos primeiro determinar $a_1 * a_2$ $(= a_4)$ e então $a_4 * a_3$. Definimos por indução $a_1 * a_2 * \ldots * a_{n-1} * a_n = (a_1 * \ldots * a_{n-1}) * a_n$.

Esta convenção para a notação é referida como associação à esquerda. Se a lei associativa vale para $(*)$ então pode ser provado que cada modo de inserir parênteses no símbolo $a_1 * \ldots * a_n$ para reduzir seu cálculo a uma seqüência de operações binárias resulta sempre no mesmo elemento de A.

Para ser preciso, estamos aqui definindo, por indução, uma função φ do conjunto de todas as n-uplas, $n = 2, 3 \ldots$, em A como segue:

$$\varphi(a_1, a_2) = a_1 * a_2$$
$$\varphi(a_1, a_2, \ldots, a_n, a_{n+1}) = \varphi(a_1, a_2, \ldots, a_n) * a_{n+1}$$

Existe um hiato neste ponto porque não sabemos realmente que função, no sentido preciso de nossa definição anterior, foi definida. Com efeito, qual é o conjunto de pares ordenados que constitui a função? Removeremos esta lacuna no Cap. 3 onde estabelecemos um esquema geral para definir uma função por indução. Por agora, nos basearemos em nossa intuição e na suposição feita na Seç. 0.1 de que podemos dar uma tal definição.

Teorema 7. Suponhamos que A consiste de todas as aplicações de um conjunto S em S. A operação binária de composição definida sobre A é associativa.

Demonstração. Sejam f, g e h aplicações de S em S. Devemos provar que $(hg)f = h(gf)$. Não há dúvida de que $(hg)f$ e $h(gf)$ são funções de S em S porque, como foi observado, a composição é uma operação binária sobre A. Temos somente que provar que são a mesma função, isto é, que os conjuntos de pares ordenados que constituem as duas funções são iguais. Para fazer isto é claramente suficiente mostrar que a imagem de cada $x \in S$ é a mesma sob $(hg)f$ e $h(gf)$. Temos $(hg)f\,(x) = (hg)(f(x)) = h(g(f(x)))$, enquanto $h(gf)(x) = h(gf(x)) = h(g(f(x)))$. Logo a imagem de x sob cada função é $h(g(f(x)))$. A Fig. 8 ilustra a situação.

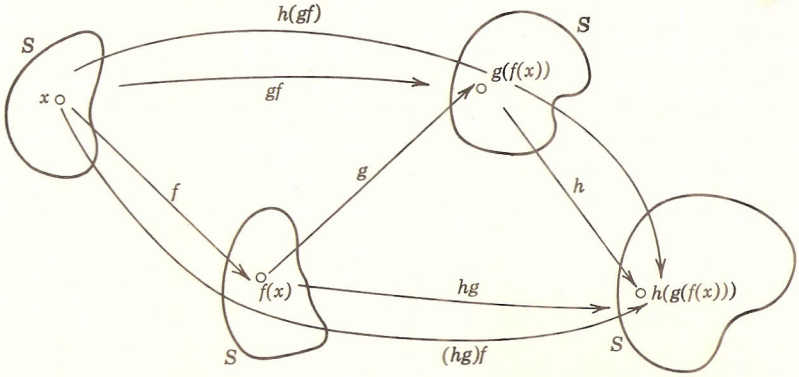


Fig. 8

Definição. Uma *operação n-ária* sobre um conjunto A é uma aplicação do conjunto de todas as n-uplas de A em A.

Exemplo 16. Seja A o conjunto dos inteiros. Uma operação ternária (3-ária) sobre A é definida aplicando a 3-upla (a, b, c) em $ab + c$.

Como no caso de uma operação binária podemos pensar numa operação n-ária como um conjunto de $(n + 1)$-uplas.

Uma operação unária (1-ária) sobre A é exatamente uma função de A em A. Não teremos ocasião de considerar outras operações senão operações unárias e binárias.

Definição. Seja $(*)$ uma operação binária definida sobre um conjunto S. Um subconjunto $T \subseteq S$ é dito *fechado sob* $(*)$ se a restrição de $(*)$ a $T \times T$ é uma operação sobre T.

Assim $T \subseteq S$ é fechado sob uma operação binária $(*)$ se para todo $(t_1, t_2) \in \in T \times T$, então $t_1 * t_2 \in T$.

Exemplo 17. Se I é o conjunto de todos os inteiros e $I_+ = \{x : x \in I, x > 0\}$, então I_+ é fechado sob a adição mas não sob a subtração.

O conceito de uma operação binária pode ser generalizado de modo útil para a noção de um conjunto de operadores sobre um conjunto.

Definição. Um conjunto B é dito um conjunto de *operadores para A por M* se M é uma aplicação de $B \times A$ em A.

O efeito desta aplicação é que há uma regra que nos diz como combinar um elemento de B e um elemento de A para obter um elemento de A.

Exemplo 18. Se M é uma operação binária sobre A, então A é um conjunto de operadores para A. Deste modo, por exemplo, poderíamos ver $2 +$ não como um inteiro mas como a operação ("efeito") de adicionar 2 a cada inteiro.

Exemplo 19. Seja A o conjunto das funções contínuas de valores reais sobre $[0, 1]$. Seja B o conjunto dos números reais. Então se $f \in A$ e $r \in B$ podemos definir $M(r, f)$ como a função f^r, isto é, $(r \cdot f)(x) = (f(x))^r = f^r(x)$. Assim B é um conjunto de operadores (operadores exponenciais) para A.

Exemplo 20. Sejam S um qualquer conjunto e A o conjunto de todas as aplicações de S em S. Para $(f, x) \in A \times S$, definimos $M(f, x) = f(x)$. Então A é um conjunto de operadores para S.

0.6. COMBINATÓRIA

Necessitaremos fazer de tempos em tempos umas poucas contas sobre o número de elementos de um conjunto finito. Aqui estão alguns dos resultados básicos.

Teorema 8. Se S é um conjunto de n elementos então

1. O número total de subconjuntos de S é 2^n.
2. Se $n \geq 1$, o número de subconjuntos de S com um número par de elementos é o mesmo que o número de subconjuntos com um número ímpar de elementos. Este número é 2^{n-1}.
3. Se $\binom{n}{k}$ designa o número de subconjuntos com k elementos então $\binom{n}{k} = \binom{n}{n-k}$ e para $n > k \geq 1$, $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$.
4. Para $n \geq k \geq 0$, $\binom{n}{k} = n!/k!\,(n-k)!$ (Seguimos a convenção de que $0! = 1$.)

5. Para números a, b temos a fórmula binomial: $(a + b)^n = \sum_{k=0}^{k=n} \binom{n}{k} a^k b^{n-k}$.

DEMONSTRAÇÃO. As conclusões (1), (2) e (3) são provadas simultaneamente por indução sobre n. Para $n = 0$ a conclusão (1) é óbvia e as outras duas valem por estarem supondo $n > 0$. (É também fácil verificar estas conclusões para $n = 1$ e $n = 2$.) Assim o passo A de nossa prova por indução está completo. A hipótese indutiva para o passo B estabelece que (1), (2) e (3) valem para todos os conjuntos com $n - 1$ elementos. Provaremos agora, com base nesta suposição, que valem para um conjunto com n elementos. Seja S um conjunto com n elementos onde suporemos, para evitar trivialidades, $n \geq 2$. Seja x um elemento particular de S que mantemos fixado ao longo de nossa discussão. Seja $S' = S - \{x\}$. Notamos que S' tem $n - 1$ elementos e que se A é um subconjunto de S, então se $x \notin A$ segue $A \subseteq S'$, mas se $x \in A$, então existe um único conjunto $A' \subseteq S'$ tal que $A = A' \cup \{x\}$; com efeito, $A' = A - \{x\}$. Seja K o número de subconjuntos de S' com um número par de elementos (ou um número ímpar de elementos). Temos $2K = 2^{n-1}$. Acrescentamos agora o elemento x a cada subconjunto de S'. É claro que, se $E' \subseteq S'$ e E' tem um número par de elementos, então $E = E' \cup \{x\}$ tem um número ímpar de elementos, enquanto que se $O' \subseteq S'$ tem um número ímpar de elementos, então $O = O' \cup \{x\}$ tem um número par de elementos. Assim para contar o número de subconjuntos de S, com um número par de elementos, temos K subconjuntos que têm um número par de elementos e são subconjuntos de S' e K mais da forma $O' \cup \{x\}$. Posto que cada subconjunto A de S tem, como foi observado, uma única expressão de forma A' ou $A' \cup \{x\}$ com $A' \subseteq S'$ é agora claro que existam exatamente $2K$ subconjuntos de S com um número par de elementos. Analogamente existem $2K$ subconjuntos de S com um número ímpar de elementos, um total de $4K = 2^n$ subconjuntos de S. Assim estabelecemos (1) e (2). Para provar (3) observamos de início que $\binom{n}{k} = \binom{n}{n-k}$ notando que a correspondência de cada subconjunto com seu complemento é injetiva e que se $A \subseteq S$ tem k elementos então seu complemento deve ter $n - k$ elementos. A segunda parte de (3) segue de modo análogo ao de (2). Se $A \subseteq S$ tem k elementos e $k \geq 1$, então $A = A' \subseteq S'$ ou $A = A' \cup \{x\}$ dependendo de $x \notin A$ ou $x \in A$. Logo o número de subconjuntos de S tendo k elementos deve ser a soma do número de subconjuntos de S' tendo k elementos e do número de subconjuntos de S' tendo $k - 1$ elementos (aos quais acrescentamos x para obter um conjunto com k elementos que contêm x). Isto é, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

A conclusão (4) segue por muito conhecida indução sobre n; deixamos os detalhes para o leitor. (5) tem também uma prova padrão por indução, entretanto é mais direto partir da observação de que um termo $a^k b^{n-k}$ aparece no produto $(a + b)^n$ escolhendo o termo a de k dos fatores $(a + b)$ e b dos restantes $n - k$

fatores. Logo o coeficiente de $a^k b^{n-k}$ é simplesmente o número de subconjuntos de $\{1, \ldots, n\}$ tendo k elementos. (1) pode naturalmente ser provado de (3), (4) e (5): tomamos $a = b = 1$. (2) também segue de (3), (4) e (5); basta tomar $a = 1$ e $b = -1$. (3) é precisamente a lei que governa a formação do triângulo de Pascal.

* * *

Um segundo lema combinatório é o clássico princípio do "pombo-correio" atribuído a P. G. L. Dirichlet (1805-1859).

Teorema 9. Se um conjunto de n elementos distintos é particionado em k subconjuntos onde $0 < k < n$, então algum subconjunto deve conter pelo menos dois elementos.

Este teorema assegura simplesmente que se n "cartas" devem ser colocadas em k "caixas de pombos-correio" onde $n > k > 0$, então pelo menos duas cartas devem estar na mesma caixa. Matematicamente falando, um conjunto finito não pode ser posto em correspondência injetiva com um seu subconjunto próprio.

Este princípio é freqüentemente usado em jogos de salão; por exemplo, se uma gaveta contém somente meias brancas e pretas, quantas meias devem ser retiradas da gaveta para assegurar que se obtém pelo menos um par casado? Dirichlet usou este princípio para mostrar que se r é um número real positivo e N é qualquer inteiro positivo então existem inteiros a e b com $0 < b \leq N$ tal que $|br - a| \leq 1/N$. (A parte sutil deste resultado é o limite para b: $0 < b \leq N$.) Notamos que cada número positivo r tem a forma $r = r_0 + r_1$, onde r_0 é inteiro não-negativo e $0 \leq r_1 < 1$. Chamamos r_1 a parte fracionária de r e a denotamos por $\{r\}$. Observamos também que o intervalo unidade $[0, 1]$ é claramente dividido em N intervalos da forma $[t/N, (t + 1)/N]$, $0 \leq t < N$; cada intervalo de comprimento $1/N$. Estas são as "caixas de pombos-correio". Dirichlet agora argumenta que $\{0\}, \{r\}, \{2r\}, \ldots, \{Nr\}$ são $N + 1$ números no intervalo unidade $[0, 1]$. Estas são as "cartas". Logo pelo menos duas devem estar na mesma caixa, isto é, no mesmo intervalo. Assim para algum par de inteiros, $0 \leq p < q \leq N$, devemos ter $|\{pr\} - \{qr\}| \leq 1/N$.

Agora se $pr = u + \{pr\}$ e $qr = v + \{qr\}$, onde u e v são inteiros, temos $|\{qr\} - \{pr\}| = |(q - p)r - (v - u)| \leq 1/N$ e realmente, $0 < q - p \leq N$.

LEITURA SUPLEMENTAR

P. R. Halmos, *Naive Set Theory*, Princeton, N. J.: Van Nostrand (1960).

L. Henkin, On mathematical induction, *American Mathematical Monthly*, **67** (1960), 323–338.

I. Niven e H. S. Zuckerman, *An Introduction to the Theory of Numbers*, New York: John Wiley e Sons (1960).

R. R. Stoll, *Set Theory and Logic*, San Francisco: W. H. Freeman (1963).

Prólogo

Para dar alguma idéia do que tentaremos fazer neste livro necessitamos compreender o termo "álgebra abstrata". Provavelmente a álgebra abstrata que nos é mais familiar é a dos inteiros embora não os tenhamos chamado nem de "abstratos" nem de "álgebra". Há em primeiro lugar o conjunto dos inteiros e provavelmente sentimos saber o que são inteiros; sabemos mesmo compará-los com pontos sobre uma reta. Temos durante anos usado as operações binárias de adição, subtração e multiplicação. Sabemos que tipos de leis estas operações obedecem. Além disso, sabemos estabelecer alguns teoremas verdadeiros sobre os inteiros. O termo "álgebra abstrata" aplicado aos inteiros compreende o conjunto dos inteiros, as operações binárias de adição, subtração e multiplicação definidas sobre este conjunto, uma lista de axiomas básicos que estas operações satisfazem, uma relação que ordena os inteiros, uma lista de axiomas que a relação de ordem satisfaz e finalmente um conjunto completo de teoremas que descrevem o comportamento dos inteiros sob estas operações e relações. Alguns destes teoremas são fáceis conseqüências dos axiomas, outros são extremamente difíceis, exigindo técnicas e conhecimento de outros sistemas matemáticos, e naturalmente muitas questões permanecem abertas. Tradicionalmente o estudo deste sistema matemático é chamado teoria dos números.

O principal objetivo de um tal estudo é obter uma descrição da estrutura dos inteiros. Poderíamos evidentemente encher livrarias com fatos especiais sobre inteiros especiais. Isto não seria provavelmente apenas sem sentido, mas para empregar uma metáfora pitoresca, perderíamos a visão da floresta pelas árvores. Como podemos ver a floresta? Podemos estabalecer teoremas válidos para todos os inteiros, ou mesmo teoremas válidos para certos subconjuntos de inteiros. Podemos olhar para subconjuntos com propriedades especiais e podemos descobrir relações sobre os inteiros que exibem propriedades-chave. Podemos estudar as funções dos inteiros em inteiros. Teremos, naturalmente, de selecionar de todas as possíveis funções aquelas que nos dizem alguma coisa dos inteiros como um todo. Precisamente que relações e funções são frutíferas para estudo é uma questão

de visão mais profunda. Julgamos a efetividade das técnicas por quanto nos dizem sobre questões particulares.

Em geral uma álgebra abstrata é um sistema formado por um conjunto S de elementos e um certo número de operações e relações sobre S. É bom recordar que estas operações e relações são precisamente conjuntos de n-uplas. Estudar uma álgebra abstrata é aprender alguma coisa sobre o comportamento individual dos elementos, descobrir alguns teoremas sobre o sistema e encontrar algumas propriedades que descrevam o sistema. Fazemos isto isolando subconjuntos distinguidos de S, determinando como estes subconjuntos de S interagem sob as operações e relações e, mais importante, estudando funções sobre S.

Se pensarmos um minuto sobre isso veremos que, com o propósito de estudar a estrutura de uma álgebra abstrata, não é tão importante conhecer todas as triplas ordenadas que constituem uma operação binária sobre S quanto é saber as propriedades que a operação satisfaz. Por exemplo, não é tão importante conhecer a expansão decimal do produto de 84.927 e 101.110.112 como é saber que a multiplicação e a adição são associativas, comutativas, e que a multiplicação distribui sobre a adição.

Portanto, descrevendo uma álgebra abstrata usualmente não tentaremos dar e realmente, se S é infinito não poderemos dar, uma lista completa das $(n + 1)$-uplas correspondentes a cada operação n-ária. Podemos dar uma regra que nos permitirá computar a operação se os elementos de S são dados sob uma certa forma, ou podemos definir uma operação por indução. É usual assegurar que existe uma operação n-ária sobre S quando ela satisfaz uma lista prefixada de propriedades-axiomas. Este procedimento nos permite uma grande economia. Se S e T são conjuntos diferentes, os sistemas matemáticos relativos a S e T serão, *a priori* diferentes, posto que as n-uplas correspondentes às operações serão conjuntos diferentes. Entretanto, acontece com freqüência que S e T possuem as mesmas espécies de operações e relações no sentido de que os mesmos axiomas são aceitos sobre uma operação sobre S e uma correspondente operação sobre T. Se é este o caso então nosso estudo das duas álgebras abstratas pode ser mais produtivo se destacamos aquelas operações comuns a S e T e estudamos um sistema com operações que têm estes axiomas. Porque, então, cada teorema provado neste sistema geral estabelecerá um fato válido para todas as álgebras abstratas tendo operações e relações correspondentes a essas e satisfazendo esses axiomas. Em particular serão válidos em S e T.

Este procedimento é mais do que uma economia. Fixando nossa atenção sobre umas poucas propriedades temos uma chance de descobrir porque um certo teorema é verdadeiro. Tentamos tirar de um teorema e de sua demonstração tudo o que não é essencial. Tentamos reconhecer que condições mínimas são necessárias para a validade do teorema. Por exemplo, consideremos a lei de expoentes inteiros $(ab)^n = a^n b^n$ para números racionais. Que propriedades dos números racionais são necessárias para provar esta lei? Não precisamos saber, por exemplo, que entre cada dois números racionais existe um outro número racional; não precisamos saber que se $ab = 0$, então $a = 0$ ou $b = 0$. Necessitamos com

efeito apenas da associatividade e da comutatividade da operação de multiplicação. Realizando isto poderemos ver que $(ab)^n = a^n b^n$ e $n(a + b) = na + nb$ é a *mesma* lei apenas escrita com notações diferentes para operações diferentes. Podemos ver também que $\sqrt{2}\ (a + b) = \sqrt{2a} + \sqrt{2b}$ deve valer por razões muito diferentes.

Este procedimento é chamado o método axiomático. Para estudar um conjunto particular S com operações e relações específicas primeiro listamos as propriedades básicas de que gozam as operações e relações sobre S, que desejamos estudar. Então, por abstração, consideramos um conjunto arbitrário com operações e relações supostas definidas sobre ele que são caracterizados pelos axiomas correspondentes às propriedades básicas que foram escolhidas. Isto dá lugar a uma classe de álgebras abstratas. Uma álgebra abstrata é um membro da classe se o conjunto de elementos admite operações e relações que satisfazem os axiomas.

Uma classe de álgebras abstratas terá possivelmente muitos membros se o número de operações e relações consideradas e o número de axiomas forem pequenos. Naturalmente se existem muito poucos axiomas, a classe será tão grande que somente teoremas gerais de pouco interesse podem ser provados. Por outro lado, se uma classe de álgebras abstratas tem um grande número de operações, relações e axiomas, a classe pode ter apenas uns poucos membros, ou mesmo nenhum membro.

Na realidade, como veremos no Cap. 3, uma lista de aparência bastante inocente de operações, relações e axiomas acontece descrever uma classe de álgebras abstratas na qual qualquer dois membros são essencialmente o mesmo — de fato cada um é uma cópia exata dos inteiros.

Solucionaremos o problema, quando possível, de decidir se uma classe de álgebras abstratas tem pelo menos um membro — isto é, se um conjunto de axiomas relativos a certas operações e relações é consistente — encontrando um exemplo de um tal sistema e explicitamente verificando os axiomas.

Consideramos, por sua vez, as grandes classes de álgebras abstratas que são chamadas grupos, anéis, corpos e espaços vetoriais. Estas classes foram escolhidas porque um grande número de sistemas matemáticos diferentes e úteis podem ser vistos como membros de uma ou mais destas classes. Em cada caso encontraremos alguns teoremas que ajudarão a descrever a estrutura de qualquer tal sistema matemático particular. Quanto mais teoremas pudermos provar, melhor entenderemos o sistema. Nosso *modus operandi* será primeiro examinar as conseqüências imediatas dos axiomas, em seguida encontrar subconjuntos apropriados e ver como estes subconjuntos ajudam a descrever o sistema e então considerar as propriedades de aplicações de uma álgebra de uma classe sobre outra da mesma classe.

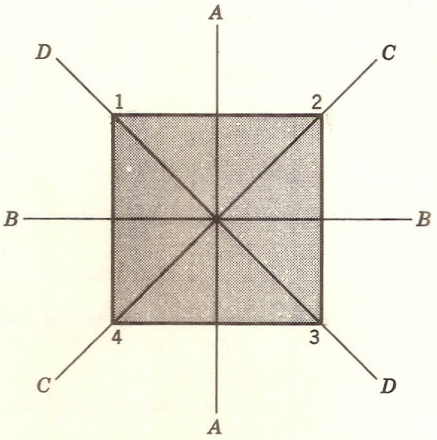
Em matemática a palavra "álgebra" refere-se a um sistema matemático no qual todas as operações sobre um conjunto são finitárias. É possível que exista um número infinito de operações, mas cada operação é uma operação n-ária para algum inteiro positivo n. Em contraste o cálculo estuda uma operação infinita — o limite. Um limite pode aplicar uma seqüência infinita de números reais em um

número real, enquanto para algumas seqüências não existe limite. Nenhum tal processo ocorre em uma álgebra, por definição. Isto não significa dizer que a álgebra não se relaciona com outras disciplinas matemáticas porque todos os ramos da matemática fazem intervir algumas operações finitárias, e quando isto acontece, métodos algébricos são as ferramentas apropriadas para pesquisa. Reciprocamente, algumas das mais difíceis questões algébricas têm sido solucionadas usando resultados obtidos por métodos não-algébricos. A forte independência entre os vários ramos da matemática é uma das principais características da matemática neste século. Este livro tenta dar uma introdução a alguns dos conceitos algébricos que são em interesse de toda a matemática.

Respostas

Exercício 1.1. Página 27

1. Sejam os vértices de um quadrado numerados como mostra a Fig. 1. Designemos por J, R, S, T rotações horárias de 0, 90, 180, 270 graus respectivamente. Sejam A, B, C, D, reflexões em torno das linhas assim designadas na Fig. 1. As simetrias do quadrado podem



então ser denotadas por:

$$J = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad R = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad C = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad D = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

4. $\{f_1(x) = x,\ f_2(x) = 1/x,\ g_2(x) = 1/(1-x),\ g_3(x) = (x-1)/x,\ g_4(x) = 1-x,$ $g_5(x) = x/(x-1)\}$.

6. G4.

10. G2, G3.

11. $\{J, R, S\}$ e $\{J, A\}$.

Exercício 1.2. Página 33

1.

	J	R	S	A	B	C
J	J	R	S	A	B	C
R	R	S	J	C	A	B
S	S	J	R	B	C	A
A	A	B	C	J	R	S
B	B	C	A	S	J	R
C	C	A	B	R	S	J

	J	R	S	T	A	B	C	D
J	J	R	S	T	A	B	C	D
R	R	S	T	J	C	D	B	A
S	S	T	J	R	B	A	D	C
T	T	J	R	S	D	C	A	B
A	A	D	B	C	J	S	T	R
B	B	C	A	D	S	J	R	T
C	C	A	D	B	R	T	J	S
D	D	B	C	A	T	R	S	J

4. $\varepsilon = (2, 0)$, $(a, b)^* = (2 - b, -b)$.

5. Não são tábuas de grupo porque $(ab)b \neq a(bb)$.

Exercício 1.3. Página 35

3. Não. No grupo aditivo dos racionais, para cada a existe um x tal que $x + x = a$. Isto não é verdadeiro para os inteiros.

5. Se $T = I$, então $\varphi(x) = x - 1$ aplica S isomorficamente sobre T.

Exercício 1.4. Página 39

3. (1): (1, 2, 3, 4), (2): (1, 4)(2, 3), (3): (1, 3, 2, 4), (4): (1, 3), (5): (2, 3, 4), (6): (1, 3)(2, 4), (7): (1), (2), (3), (4), (8): (1, 3, 4), (2, 5).

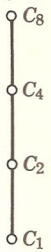
4. 1, 3, 4, 5, 7 são ciclos. 4 é uma transposição.

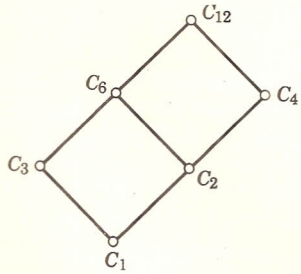
9. (1): (2 3), (2): (1 3)(4 5), (3): (1 2)(3 4), (4): (1 6 4)(2 5 3), (5): (1 4 6 2)(3 8 7), (6): $(a\ b)(c\ d)(f\ g)$.

Exercício 1.5. Página 55

1. Há 3 grupos cíclicos de ordem 4 e 4 grupos cada um deles isomorfo ao quatro-grupo.

4. Veja as Figs. 2 e 3.





5. Considere qualquer grupo cíclico infinito.

11. (ii) $|\mathscr{A}_4| = 12$. (iii) $1 = a^3 = b^3 = c^3 = d^3 = r^2 = s^2 = t^2$. (iv) $\{1, r, t, s\}$. (iv) $\{1, a, a^2\}$.

12. $\{1, a^2\}$ é o único que é subgrupo.

13. Um grupo de ordem 10 ou é cíclico ou é um grupo diedro.

Exercício 1.6. Página 64

3. $\{\iota, (12)(34), (13)(24), (14)(23)\}$ é o único subgrupo de ordem 4 em $\mathscr{S}_4$.

4. (iv) é normal; (v) não é.

10. A ordem de $\varphi(g)$ divide a ordem de g.

12. Seja $D_n = \{r, a : r^n = 1, a^2 = 1, ar = r^{-1}a\}$. Todo subgrupo de $\langle r \rangle$ é normal. Se n é ímpar, estes são os únicos; se n é par, então temos que $\langle a, r^2 \rangle$ e $\langle ar, r^2 \rangle$ são normais.

13. $(n + 1)!$ serve.

15. O grupo cíclico de ordem 5 é o subgrupo comutador.

Exercício 1.7. Página 69

2. $C_2 \times C_2$ é o quatro-grupo, $C_2 \times C_3 \cong C_6$, $C \times C_3 \cong C_{12}$.

3. $C_6 \times C_2 \cong V \times C_3$.

8. Considere $C_2 \times C_4 \times C_8 \times C_{16} \times \ldots$ e $C_4 \times C_8 \times C_{16} \times \ldots$

9. Veja (8).

Exercício 2.1. Página 76

1. $(-4) + (-1) \neq -(4 - 1)$.

3. (i) é um domínio de integridade, os outros não são anéis.

5. $D \times E$ é um anel comutativo com identidade.

7. Não existe nenhum domínio de integridade com 6 elementos.

Exercício 2.2. Página 85

1. $D \cong D^*$ via $\varphi(a) = a - 1$.

5. (i) 4, (ii) 3 e 7, (iii) 2 e 3, (iv) 5.

9. A soma dos dígitos, contando-se cada segundo dígito como negativo, deve ser divisível por 11.

10. $\{\bar{0}\}$, $\{\bar{0}, \bar{3}\}$, $\{\bar{0}, \bar{2}, \bar{4}\}$, $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

Exercício 2.3. Página 89

2. As unidades de D_p são números racionais da forma p^k, $k \in I$. As unidades de $\hat{D}_p$ são inteiros divisíveis por p e números racionais da forma $1/b$ onde p divide b.

6. A associatividade da multiplicação e a lei distributiva.

7. Associatividade da multiplicação, lei distributiva, inverso aditivo, sem divisores de zero.

9. Verdadeiro somente para $I/\langle 5 \rangle$.

10. $n = 6$: As unidades formam um grupo cíclico de ordem 2.
$n = 7$: As unidades formam um grupo cíclico de ordem 6.
$n = 8$: As unidades formam um quatro-grupo.

Exercício 3.1. Página 95

1. Uma classe de equivalência é da forma $\{a, -a\}$.

2. Somente se A é o conjunto vazio ou é o conjunto reduzido a um elemento.

3. Grupos cíclicos cujas ordens são potências primas.

4. Não. $A = \{\iota, (1\ 2)\ (3\ 4)\}$ é normal em $\{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ que é normal em $\mathscr{S}_4$ mas A não é normal em $\mathscr{S}_4$.

Exercício 3.2. Página 96

4. Sejam a/b, c/d escritos em seus menores termos ($0 = 0/1$). Uma possível ordem é $a/b \tau c/d$ se $a < c$ ou $a = c$ e $b \leq d$.

6. Uma possível ordem é $a \delta b$ se, e somente se, $b \leq a$.

Exercício 3.3. Página 102

1. $m \leq n(n-1)/2$.

6. $g(n, r) = r + a_{n+1}$, $A = R$, $f(1) = a = a_1$, $f(n) = \sum_{k=1}^{k=n} a_k$.

Exercício 3.4. Página 107

1. $104{,}976 = 3^8 2^4$, $857{,}375 = 5^3 19^3$, $97{,}344 = 2^6 3^2 13^2$.

2. \$1.00. Sim, sempre que w_1 mostra um número ímpar.

6. A ordem de p é n.

7. (iii) : $[a/b] = q$.

8. 3 tem expoente $33 + 11 + 3 + 1 = 48$; p tem expoente $[n/p] + [n/p^2] + \ldots + [n/p^k]$ onde $p^{k+1} > n$.

Exercício 4.1. Página 113

1. $\{a + b\sqrt{2} : a, b \in \mathrm{Ra}\}$.

2. O corpo de quocientes é isomorfo a Ra.

3. Não; $(\sqrt{2} + \sqrt{3})^2$ é irracional.

Exercício 4.2. Página 116

1. $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathrm{Ra}\}$ tem Ra, $\{a + b\sqrt{2} : a, b \in \mathrm{Ra}\}$, $\{a + c\sqrt{3} : a, c \in \mathrm{Ra}\}$ e $\{a + d\sqrt{6} : a, d \in \mathrm{Ra}\}$ como subcorpos próprios.

2. $S = D_p$.

3. Não se verifica!

10. $\bar{3}^{13} = \bar{3}$.

13. $G/H \cong \{M_a : M_a(x) = ax\} \cong \langle K - \{0\}, \cdot \rangle$.

Exercício 4.4. Página 127

6. (i) disco fechado; centro em a e raio r.

   (ii) O semiplano contendo a e determinado pelo bissetor perpendicular do segmento de reta (a, b).

   (iii) um círculo contendo a, ou se $r = 0$, o ponto a.

   (iv) elipse.

7. (i) $z = re^{i\theta}$ onde $r = \sqrt[n]{|c|}$ e $\theta = (1/n)$ argumento de $c + 2k\pi/n$.

   (ii) $z = -a \pm (\sqrt{2}/2)[(\sqrt{u^2 + v^2} + u)^{1/2} + (\sqrt{u^2 + v^2} - u)^{1/2} i]$ onde $a^2 - b = u + vi$ e $u, v \in \mathrm{Re}$.

9. (i) $\varphi^{-1}(x) = a^{-1}(x - b)$.

   (iii) $\varphi\theta\varphi^{-1}(x) = c(x - b) + ad + b$. Um subgrupo normal é $\{\varphi : \varphi(x) = cx,\ c \neq 0\}$.

13. $(-1)^{n+1}$.

Exercício 5.1. Página 133

3. $(6711,831) = 3 = 66 \cdot 6711 - 533 \cdot 831$.
4. $\alpha = \beta \cdot 1 + (-2 - 2i)$.
5. $(3 + 4i, 7 - i) = 1$.
7. Não.
11. Cada MDC(3/4, 7/2) é uma unidade.
12. $151{,}316 = 2^2 \cdot 11 \cdot 19 \cdot 181$.

Exercício 5.2. Página 138

2. $(4 + 11a)14 - (5 + 14a)11 = 1$. $c = 25$ é o menor inteiro com uma solução. $c = 924 = 6 \cdot 11 \cdot 14$ é o maior com cinco soluções.
3. $x \equiv 136$ mod. $(6 \cdot 5 \cdot 77)$.
4. $(m, n) \mid (a - b)$.
5. Cada membro de D_3 é uma solução!

Exercício 5.3. Página 142

5. Se $n = p_1^2 \ldots p_k^2 p_{k+1} \ldots p_r$ é a fatoração prima de n, então existem 2^k grupos abelianos de ordem n. Cada um deles tem a forma $C_d \times C_{n/d}$ onde $p_{k+1} \ldots p_r \mid d$ e $d \mid n$. (C_h é o grupo cíclico de ordem h.)

Exercício 6.1. Página 149

2. Todos.
3. (i) -2, (ii) 0.

Exercício 6.2. Página 153

1. $x + 1$.
2. $f \equiv (1/2)(-x^2 - x + 1)$ mod. $(x^3 + 1)$.
3. $f \equiv x$ mod. $(x^2 + x + 1)$.
4. $x - 1$ não tem inverso; $x^2 - 1$ é redutível.
5. Sejam K um corpo e $f, g \in K[x]$. Se $(f, g) = d$ e nem f nem g são associados a d, então existem $a, b \in K[x]$ tais que $d = af + bg$ e grau $(a) <$ grau (g/d) e grau $(b) <$ grau (f/d).
7. $(1/4) \log (x + 1) - (1/4) \log (x - 1) - 1/[6(x - 1)] + (2/3\sqrt{3}) \operatorname{arctg} (2 + 1)/\sqrt{3}$.
10. Obtém-se um domínio de integridade.
11. Não.
12. Os polinômios "positivos" não são bem-ordenados.

Exercício 6.3. Página 156

1. Os elementos são $0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i$, onde $i^2 = -1 = 2$. Um gerador é $(1 + i)$.

Exercício 6.4. Página 161

1. Se $a \neq b$, então $r = ([f(a) - f(b)]/(a - b))x + [af(b) - bf(a)]/(a - b)$. Se $a = b$, então $r = f'(a)(x - a) + f(a)$.

2. $\lambda(1, 0, 0) = (31/3, 4/3, 10)$; $\lambda(0, 1, 0) = (47/3, 20/3, 19)$; $\lambda(0, 0, 1) = (-10, +1, -10)$.
3. $k = 2$.
4. Não há soluções. Base para o núcleo: $\{(2, 3, -1)\}$; imagem: $\{(1, 2, 2), (0, -2, -1)\}$.
6. Os inteiros a, b, c devem ser tais que $a + b = c - b$ e $3 \mid (a + b)$.

Exercício 8.1. Página 210

1. Os elementos são $0, 1, \theta, \theta + 1, \theta^2, \theta^2 + 1, \theta^2 + \theta, \theta^2 + \theta + 1$, onde $\theta^3 + \theta + 1 = 0$. Um cálculo típico dá $(\theta^2 + \theta)(\theta^2 + \theta + 1) = \theta^2$. $x^3 + x + 1 = (x + \theta)(x + \theta^2)(x + \theta^2 + \theta)$.
2. $(1 + \theta)^{-1} = (1 + 2\theta + 2\theta^2)/5$.
5. Uma condição suficiente é que $a \neq b$.

Exercício 8.2. Página 218

5. Se $\mathrm{car}(K) = p$, então $ax^p - ax + 1$ é fixado por σ. Generalize!

Exercício 8.3. Página 223

2. Se φ é a função φ de Euler então existem $\varphi(p^n - 1)/n$ polinômios.
3. Os polinômios irredutíveis de grau 4 sobre CG(2) são $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$ e $x^4 + x + 1$. Veja também o Probl. 6.
5. Se α é um zero de $x^3 - x + 1$ e β é um zero de $x^3 - x - 1$, então existe um automorfismo de $CG(3^3)$ levando α em $-\beta$.
6. Seja $\theta^4 = \theta + 1$. Os elementos de ordem 15 são θ, θ^2, $\theta^4 = \theta + 1$, $\theta^7 = \theta^3 + \theta + 1$, $\theta^8 = \theta^2 + 1$, $\theta^{11} = \theta^3 + \theta^2 + \theta$, $\theta^{13} = \theta^3 + \theta^2 + 1$ e $\theta^{14} = \theta^3 + 1$. Os elementos de ordem 5 são θ^3, $\theta^6 = \theta^3 + \theta^2$, $\theta^9 = \theta^3 + \theta$ e $\theta^{12} = \theta^3 + \theta^2 + \theta + 1$. Os elementos de ordem 3 são $\theta^5 = \theta^2, + \theta$ e $\theta^{10} = \theta^2 + \theta + 1$. $x^4 + x^2 + 1 = (x + \theta^2 + \theta)^2(x + \theta^2 + \theta + 1)^2$.

Exercício 8.4. Página 232

2. O conjunto dos elementos primitivos é $\{(ua + v)/(ra + s) : u, v, r, s \in K \text{ e } us - rv \neq 0\}$.

Exercício 9.1. Página 238

6. Os grupos de ordem 8 são C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, quatérnios, e o grupo diedro de ordem 8. Os grupos de ordem 9 são C_9 e $C_3 \times C_3$.
7. Há 14 grupos de ordem 16. Para um tratamento completo veja M. Hall, Jr. e J. K. Senior, *The Groups of Order* 2^n $(n \geq 6)$, New York: Macmillan (1964).

Exercício 9.2 Página 243

2. Existem 5 grupos de ordem 18 e cinco de ordem 20.
5. $S_q \cong C_q$ é normal. $S_p \cong C_p$ deve também ser normal. Uma condição necessária e suficiente é que $q \neq 1 + kp$.
6. Mostre que um grupo de ordem 30 deve ter um subgrupo cíclico de ordem 15. Há quatro grupos de ordem 30: C_{30}, $\mathscr{S}_3 \times C_5$, $D_{10} \times C_3$ e D_{30}. (Aqui D_k denota o grupo diedral de ordem k.)

Exercício 9.3. Página 250

5. Não verifica!

Exercício 9.4. Página 263

1. Existem 10 grupos abelianos de ordem 144: $C_{16} \times C_9$, $C_{16} \times C_3 \times C_3$, $C_2 \times C_8 \times C_9$, $C_2 \times C_8 \times C_3 \times C_3$, $C_2 \times C_2 \times C_4 \times C_9$, $C_2 \times C_2 \times C_4 \times C_3 \times C_3$, $C_2 \times C_2 \times C_2 \times C_2 \times C_9$, $C_2 \times C_2 \times C_2 \times C_2 \times C_3 \times C_3$, $C_4 \times C_4 \times C_9$, $C_4 \times C_4 \times C_3 \times C_3$.
2. O inteiro n não deve ser divisível por um quadrado distinto de 1.
3. $C_2 \times C_2 \times C_6 \times C_\infty$.
5. Não.

Exercício 10.1. Página 275

3. $G \cong \mathscr{S}_3$. $\mathrm{Ra}(d) = \mathrm{Ra}(\sqrt{-23})$.
4. (i) $\mathscr{S}_3 \times C_2$, (ii) C_4, (iii) quatro-grupo.
5. C_6. $\mathrm{Ra}(\sqrt{-3}, \sqrt[3]{2})$ e $\mathrm{Ra}(\sqrt{-3}, \sqrt{2})$.

Exercício 10.2. Página 291

1. O grupo de Galois é um grupo cíclico de ordem 3.
2. O grupo diedral de ordem 8.
5. Os graus possíveis são 1 e p.
6. (iii) 4, 4 e 2.
   (iv) $(u^3 + 2u^2 - 4u - 5)/(-9)$.
   (v) Não, Sim, Sim e Não.

Exercício 10.3. Página 299

2. $s_1{}^2 s_2{}^2 - 2s_3 s_1{}^2 + 4s_1 s_2 s_3 - 3s_3{}^2 - 2s_2{}^3$.
3. $N = (\Delta_n)^2(-1)^{(n-1)n/2}$.
6. (ii) c^2, $a^2 - 2b$ e $b^2 - 2ac$.
7. $(2q - 6pr + 18s)$ e 26.
8. $x^3 + 3x^2 - 2x = 9$.
10. Apenas (ii) e (iii).

ÍNDICE ALFABÉTICO

(Os números em negrito indicam a página onde aparece uma definição)

A

Abel, N.H., 27, 295
Abeliana, extensão, **272**
Abeliano, grupo, **27**, 140, 251
(grupo abeliano) livre, 252
Absoluto, valor, em domínios de integridade ordenados, **93**
em números complexos, **124**
Abstrata, álgebra, **20**, 128
Acréscimo em uma indeterminada, 122
Adição, 1, 16
de números complexos, **121**
de polinômios, **145**
no corpo de quocientes, **111**
operação de anel, 70
Aditivo, inverso, **74**
Albert, A.A., 202, 232
Álgebra, associativa, **197**
de grupo, **200**
dos quatérnios, **198**
linear, 202
teorema fundamental da, 123
Algébrica, extensão, 211, 214
independência, 213
Algebricamente fechado, corpo, **216**
Algébrico, elemento, **211**
fecho, **217**
inteiro, **299**
Algoritmo, da divisão, em um grupo abeliano, 556
euclideano, **131**
para fatorar um polinômio em I x, 167
para inteiros, 103
para obter uma base, 256
para polinômio, 150, 146
Alternado, grupo A_4, **55**, 245
A_n, **296**
Anel, **70**-89, 97
Automorfismo de, 77, 83-84
classes residuais de, 80
comutativo, **71**
de divisão, **70**
de fatoração única (DFU), **162**
de grupo, 200, **201**
de inteiros, 71, 83-84, **97**, 90-107
de polinômios, **146**
de transformações lineares, **197**
diferença, **80**
domínio de integridade, **70**
endomorfismo, **77**
euclideano, 128, **129**-138
fator ou quociente, **80**
homomorfismo de, **77**
nulo, **71**
Aplicação, 10, **11**, 25
(veja também Função, Permutação)
Apostol, Tom. M., 127
Apresentação finita, grupo abeliano de, 257, 258
Argumento de um número complexo, **125**
Aritmética, 1, 103, 238
em domínios euclideanos, 134
teorema fundamental da, 105
Artin, E., 299
Associados, elementos,
em domínios de integridade, **87**
Associativa, álgebra, 197
Associativa, operação, 14, 21

Automorfismo,
como grupo de permutação, 272
de um anel, **77**
de um corpo, 116
de um corpo F sobre K, **116**
de um corpo finito, 223
de um corpo fixado, 265
de um grupo, 65
Axiomas de extensão, **5**
Axiomas, para um
anel, **70**
anel de divisão, **70**
domínio de integridade, 70
domínio de integridade ordenado, **92**, 97
espaço vetorial, 173, 180
grupo, **23**

B

Ball, R.W., 69
Base, axioma para a existência da, **181**
para um espaço vetorial, **179**
para um grupo abeliano, **251**
teorema para grupos abelianos, 252
Bem ordenado, conjunto, 95, **96**
Bernays, P., 90, 108
Binária,
operação, **14**, 20
relação, **7**
Boa ordenação, 96
Bnck, R.C., 103, 108
Burnside, W., 12, 250, 264
problema de, 142

C

Cálculo, 21, 154, 160, 290
Cancelamento,
em anéis, 74
em domínios de integridade, 74
em grupos, 30, 33
lei para produtos diretos em grupos abelianos, 260
Cardano, fórmula de (H. Cardano), 289
Cartesiano, produto, 7
Cauchy, A.L., 23
Cauchy, teorema de grupo de, 69, 233
para grupos abelianos, 64
Cayley, A., 31, 200
Cayley, tábua para um grupo, 33, 45, 233
Característica, de um anel, **117**
de um corpo, **115**
zero, corpo de, 160, 265
Característica, função, **11**
Centro de um grupo, 56, 233
de um p-grupo, 238
de s_n, 238
Chinês, teorema do resto, 137
Cíclicas, extensões, **272**, 276
Cíclico, grupo, 40, 107, 128, 251
de raízes da unidade, 126, 127
gerador de, **40**
infinito, 41
Ciclo (permutação), 39
Ciclotômico,
Corpo, 279
polinômio, 227, 232
Classe, equação de,
para um grupo, **229**, 234, 239
Classes laterais, 47
Contradomínio, de uma transformação linear, 186, 190
de uma relação, 8
Coeficientes de um polinômio, 143, 145
Cohn, P.M., 260, 264
Combinatória, 16
Completo, grupo linear, 189
Completo, grupo simétrico (veja grupo simétrico)
Complexo conjugado, 123
Complexo, número, **121**, 154, 174, 211, 216
argumento de, **125**
corpo de, como espaço vetorial, 175
módulo de, **124**
Composto, número, **2**
Composição, **13**, 14
de função, 15
série de, 244
Comutador, 65, 248
subgrupo, **247**, 248
Comutativa, operação, 14, 21
Comutativo, anel, 70
Comutativo, grupo, 27
Congruência, sobre um anel, 82
solução de, em domínio euclideano, 138
Conjugação, classes de, **229**
Conjugados, elementos,
em um corpo, 238
em um grupo, 56, **229**
Conjugados, conjuntos,
em um grupo, **234**
Conjunto, 4-7
aplicações de, **15**
bem ordenado, **96**, **99**
disjuntos, **6**, **7**
enumerável, 216
interseção de, 6
limitado superiormente, 118
parcialmente ordenado, 91
união, **6**
vazio, **5**
Conjunto, fechado sob uma operação, **16**
Conjunto, notação para, **5**
Conjunto, teoria, 4, 18, 90
Consistente, conjunto de axiomas, 21
Contínua, função, 177
Contradomínio, de uma transformação linear, 186, 190
de uma relação, 8
Coprimo (primos relativos), **134**
Coordenada, **182**, 186
Corpo, 21, **70**, 109
algebricamente fechado, **216**, 219
automorfismo de, 116
característica de, 115
de automorfismo de F sobre K, 116
de característica zero, 115, 160, 225, 265
homomorfismo de, 116
Corpo decomponível, **205**, 267
existência do, 206
isomorfismo do, 208
de $x^n - 1$, 284
de $x^n - a$, 277, 278

Corpo, de números complexos, 121-127, 147-157
decomponível, 205, 267
de funções racionais, **168**
de números racionais, 112
de números reais, 117-121
de quocientes, 109, **112**, 168
Corpo, extensão de, **113**, 203
abeliana, **273**
algébrica, **211**
cíclica, **272**
finita, **212**, 266
grau de, **212**
simples, **224**
solúvel, **272**
transcendente, **216**, **212**
Corpos finitos, 74, 81, 150, 154, 176, 183, 218
existência e unidade de, 219
polinômios irredutíveis sobre CG(p)
Crivo, método, 106
Cúbico, polinômio, **145**
zeros de, 279, 288
Curtis, C.W., 200, 202

D

Decomponível, corpo, **205**, 267
existência e unidade, 219
isomorfismo de, 208
para $x^n - 278$
para $x^n - a$, 277, 278
Definição, por indução, 3, **99**
Dependência, 178
Dependente, conjunto de vetores, 178
Derivada, de um polinômio, **160**
Derivada, série, **248**
Derivado, subgrupo, 66, **247**, 248
Diagrama, 6
Diamante, teorema do, para homomorfismo de grupo, 239
Dickson, L.E., 200, 202
Diedrais, grupos, 42
de ordem, 6, 54
Diferença, anel, **80**
Dimensão de espaço vetorial, 182, 187, 189
Direto, produto, de grupos, 65
Dirichelet, P.G.L., 18, 106
Discriminante, **295**, 296
de um polinômio cúbico, **287**
Disjuntos, conjuntos, **7**
Distributivas, leis, 21, **70**
Divisão, 1, **86**, 228
em um domínio de integridade, 86
ordenação de inteiros por, 91
Divisão, algorítmo, 103
para polinômios, 150, 162
Divisão, anel, de, 70, 199, 229
Divisibilidade, critério de, 86
Divisores, de zero, **74**, 88, 200 201, 202
Domínio, de fatoração única, 162
de uma função, 8, 10
Dual, espaço, **191**

E

Eisenstein, critério de irredutibilidade de, 166
Elemento, **4**
Elementares, polinômios simétricos, 292, 297
Elementares, transformações, 185
Endomorfismo, de grupo, **62**, **65**
de um anel, **77**, 84
Equação de classe, **230**
do 2.º grau, 286
do 3.º grau, 286
solúvel por radicais, 265, 279
Equivalência, classe de, **9**
relação de, **8**, 210
Erathósthenes, 107
Erdos, P., 229, 232
Escalão, 173, **177**
multiplicação, 173
polinômio, 145
Euclides, 106
Euclideano, algoritmo, 128, **131**
domínio, **129**
Euler., L., 107
função de, 107, 138, 226, 227
Expoente, de um grupo, **141**
Exponenciação, 3, 16
Extensão de um corpo, **113**
algébrica, **211**, 214
como um espaço vetorial, 175
finita, **212**, 266
grau de, **212**
separável, 265
simples, 224
transcendente, **211**, 212
Extensão de:
uma função, 12
um homomorfismo, 150
um isomorfismo, 2, 10, 208, 212
Extensão, axioma de, 5
Extensão para uma base, 182
Externo, produto direto, 66

F

Fatoração em $A[x]$, 161
Fator, grupo, 59
anel, 80
Fefferman, S., 108, 117, 127, 232
Feit, W., 250
Fermat, Pierre de (1601-1665), 138
Fermat, pequeno teorema de, 83
Fixado, corpo, de um grupo, 265
Fixado, elemento, sob uma permutação, 37
Fluxo, diagrama de, para algoritmo de grupo abeliano, 256
Fração, 110
Fraenkel, A.A., 90, 108
Frobenius, G., 200
Função, **10**, 19
bijetiva, 13
característica, 11
como elemento de um anel, 71
como elemento de um espaço vetorial, 177
como elemento de um grupo, 24
composição de, **13**
e de Euler, 107, 139, 227, 231
extensão de, **12**
identidade, **11**
injetiva, sobrejetiva, **10**
n-upla de, 11
restrição a um subconjunto, **12**
seqüência de, **11**

Fundamental, teorema:
da álgebra, 123
da aritmética, 105
da teoria dos corpos, 203
da teoria de Galois (TFTG), 269
para grupos abelianos de geração finita, 252, 258

G

Galois, E., 23, 219, 281
Galois, corpos de, 219
Galois, grupo de, 272
de um polinômio geral, 293
Galois, teoria de, 265
Gauss, Karl Friedrich (1777-1855)
lema de, 164
Gaussianos, inteiros, 129
Gerador, conjunto, de vetores, 177
conjunto de, para um grupo, 51, 251
Geradores, para um grupo cíclico, 40
Godel, K., 217
Grau, de uma extensão de corpo, 212
de um polinômio, 145
Gray, E.L., 299
Grupo, 23, **24**-69, 127, 139-142, 200, 202, 220, 229, 233, 264
abeliano, **27**
alternado, 55, **296**
automorfismo de, **61**
axiomas de, 23
centro de, 56, 233
cíclico, **40**, 41, 49, 64
de ordens 1 e 2, 27
de ordem 3, 31
de ordem 4, 34
de ordem 6, 53
de ordem 8 e 9, 238
de ordem 10, 56
de ordem 12, 242
de ordem 15, 241
de ordens, 18, 20, 30, 244
de ordem p^2, 238
de ordem prima, 13
de permutações, **36**-40
de raízes da unidade, 127, 226
de um polinômio, 272
de unidades, 89
de unidades em I/n, 276, 277
diedral, 42-45
elemento identidade, **46**
expoente de, 141
fixado um subcorpo, **265**
homomorfismo de, 56-64, 239
inverso em, 23, 30
linear completo, **189**
quaterniônico, 56
quociente, 56
simples, 250
solúvel, 249

H

Hadamard, J., 106
Hall, Marshall, Jr., 69-142, 264
Hall, Philip, 238
Halmos, P.R., 18, 90, 108, 202
Hamilton, W.R., 200
Hardy, G.H., 106, 108
Henkin, L., 18
Herstein, I. N., 229, 232
Homomorfismo, de corpo, 115-116
de anel, **77**-85
de espaço vetorial, **185**
de grupo, **56**-65
núcleo de, **57**-77
Hopf, H., 200

I

Ideal, 77
em domínios euclideanos, 130-138
interseção de, **78**
maximal, 88, 89
no anel dos inteiros, 79-81
principal, **78**, 130
unidade, 78
zero, 78
Idempotente, elemento, **29**
Identidade, elemento, em um anel, 70, 74
em um grupo, 23, 29
Identidade, função, 11
Igualdade, **4**
Imagem, 12
pré-imagem, **12**
Independência, algébrica, **213**
linear, **178**
Independente, conjunto de vetores, **178**
Indeterminada, 148
Índice, de um subgrupo, **48**
Indução, definição por, 3, 99
princípio de, 2, 18, **98**
sobre m, 2
Indutiva, hipótese, 2
Indutivo, passo, 2
Infinito, grupo cíclico, 41
Injetiva, 13
Inteiros, 4, 20, 24, **97**, 128
módulo n, $I/\langle n \rangle$, n, 83-85, 138, 277
Integridade, domínio de, **70**, 74, 86-89
ordenado, **92**-95
Integridade, sistema de, **97**
Interno, produto direto, **66**
Inversa, aplicação, 13
Inverso, à direita, **24**
à esquerda, 13, 28, 30, 33
Inverso, elemento em um grupo, **23**
unicidade do, 30
Irracional, número, 127, 211
Irracionalidade de, 2, 117
Irredutível, elemento em:
anel de polinômios, **152**, 162-167, 221
domínio euclideano, 135
domínio de fatoração única, 162
domínio de integridade, **87**
inteiros, 2, 105
Isomorfismos de dois:
anéis, 77
grupos, **34**-35
sistemas de integridade, 101

J

Jacobson, N., 89, 127, 202, 299

K

Kaczynski, T.Y., 229, 232
Kervoire, M., 200
Knuth, D.E., 232
Kronecker, L., 23, 202
Kuratowski, C., 7

L

Lagrange, J.L., 48
  recíproca de, 233
  resolvente de, 278
  teorema (de grupo) de, 48, 212, 235
  teorema da interpolação de, 158
Lehmer, Emma, 228, 272
Lema de Gauss, 164
Landau, E., 117, 127
Le Yeque, W. J., 299
Lexicográfica, ordem, 96, 297
Linear:
  álgebra, 202
  equações, sistema de, 191-195-194-198
  espaço, nulo, **186**, **190**
  funcional, **191**, **194**
  imagem, **186**, **190**
  nulidade, **292**, **196**
  polinômio, **145**, **149**
    irredutibilidade de, **152**, **156**
  transformação, 185-190, 189-194
Livre, grupo abeliano, 252

M

Maior divisor comum (MDC), 87
  em domínios euclideanos, 128, 131
  em domínios de fatoração única, 162
  em inteiros, 104
  no anel de polinômios K[x], 152
Maior inteiro, função, 108
Maximal, ideal, **88**, 139
Maximal, princípio, **180**
Membro, 4
Menor múltiplo comum (MMC), **87**
  em domínios euclideanos, 138
  em sistemas de integridade, 104, 133
Migotti, A., 228
Milnor, J., 200
Möbius, A. F., 222
  fórmula de inversão, 222, 228
  função μ, **222**, 228
Módulo, 128
Módulo de número complexo, 124
Mônico, polinômio, **145**
Motzkin, T., 142
Mullin, R.C., 232
Múltiplos, zeros, 158-**161**
Multiplicação, como operação de anel, 70
  como operação de grupo, 30
  de números complexos, **121**
  no corpo de quocientes, **110**
Multiplicação de polinômios, **145**, 150

N

Não singular, transformação linear, **186**
Natural, homomorfismo, de grupo, **60**
  de anel, **80**
Niven, I., 18, 89, 108, 127, 202, 264
Normal, cadeia, **244**
Normal, extensão, **268**
Normal, subgrupo, **58**, 60, 244, 265, 270
Normalizador, em grupo, 56, **234**
Novikov, P. S., 142
n-upla, **11**, 21, 174
Núcleo de:
  homomorfismo de anel, **77**
  homomorfismo de grupo, **57**-65
  transformação linear, 186
Nulidade de transformação linear, **193**
Nulo, anel, **71**, 74
Nulo, conjunto, **5**
Número, teoria de, 18, **20**, 83, 84, 90-107, 221

O

Operação, **14**
  binária, **14**
  conjunto fechado sob, **16**
  n-ária, **16**
  ternária, **16**
  unária, **16**
Operadores, **16**, 172
Orbitais, 39
Ordem, de um grupo, **31**
  de um elemento de grupo, **46**
Ordenado, domínio de integridade, **92**, 128
Ordenado, par, 7

P

Parcial, ordenação, **91**
Parcialmente ordenado, conjunto, **91**
Pascal, triângulo de, 18
Permutação, **36**-40, 103
  centro de, 235
  ciclo, **39**
  grupo de, 36, 38
  grupo simétrico completo S_n, **37**
  ímpar, **296**
  órbitas, **39**
  par, **296**
  p-grupo, **235**
  transposição, 39
Pertinência, 4
Pombo correio, princípio dos, **18**
Polinômia, função, 138, 157
  coeficiente principal de, **145**
  de quarta ordem, **145**, 297
  de quinta ordem, **145**, 290, 294
  em várias variáveis, 168, **169**, 170
  geral de grau n, 294
  grupo de, **272**
  irredutível, **152**, 162-167, 204, 208, 215, 229
  irredutível sobre CG(p), 222
  linear, **145**, 152
  mônico, **145**
  primitivo, 164
  quadrático, 145, 157, 279
  sobre um corpo, 150-154
Polinômio, **145**, 143-170
  abeliano, **272**
  algoritmo euclideano para, 151
  algoritmo da divisão para, 151
  cíclico, **272**
  ciclotômico, **227**-228
  cúbico, **145**, 157, 279
  grau de, **145**

Polinômio, anel de, 146
decomposição de, 205
escalar, 145
simétrico, 292, **293**, 297
solúvel, **272**, 281
zeros de, 148, 157-160
Posto de uma transformação linear, 193
Pré-imagem, **12**
Primitiva, raiz da unidade, **126**, 127, 128
Primitivo, elemento, mod *b*, 277
de uma extensão de corpo, 99, **224**, 268, 272
Primitivo, polinômio, 164
Primo, elemento
coprimo, 134
de domínio de integridade, **87**
inteiro, 2, 105, 108
Primo, subcorpo, **114**, 115
Primos, teorema dos números, 106
Principal, ideal, **78**, 81
Próprio, subconjunto, **6**
Próprio, subgrupo, **46**, 49
p-subgrupo de Sylow (p-SS), 238
isomorfismo de, 241

Q

Quadrático, polinômio, **145**, 157, 289
Quarta ordem, polinômio, **145**
solubilidade de, 289
Quatérnios, álgebra dos, **198**
Quaterniônico, grupo, **56**
Quarto-grupo, **35**, 255
Quatro quadrados, teorema de, 200
Quinta ordem, polinômio, **145**
insolubilidade de, 294
Quociente
anel, **80**
grupo, **59**
Quocientes, corpo dos, **109**, **110**, 112

R

Racionais simétricas, funções, 293
Racional, números, corpo de 112, 114
polinômios sobre, 161, 164, 165
Raízes de uma equação, 148
da unidade, **126**, 225
múltiplas, **158**
solução para, por radicais, 279
torre de, 279
Reais, números, corpo de, 117, 121, 173, 174
Recíproca de Lagrange, 69, 233
para grupos abelianos, 233
Redheffer, R.M., 227
Reflexão, 25, 42, 73
Reflexiva, lei, **8**, 91
Relação, 7,11
anti-simétrica, **91**
binária, **7**
de equivalência, **8**, 9, 47, 87, 209, 279
reflexiva, **8**, 91
simétrica, **8**
transitiva, **8**
Relativos, primos, **134**
Resto, 2, 103, 129, 150
teorema do, 156
Representação, teorema de, para anéis, 84
para espaços vetoriais, 182
para grupos, 37
Residuais, classes, para anéis, 84
para espaços vetoriais, 183
para grupos, 37
Residuais, classes, para anéis, **80**
Restrição de funções, **12**
Reticulado, 128
Rogers, K., 232
Rotações, 25, 42, 44, 73
Rudin, W., 142
Ruffini, P., 295

S

Samuel, P., 127, 242
Sehveier, O., 212
Sehnider, Th., 212
Separável, polinômio, **265**
Seqüências, **11**
como elemento de espaço vetorial, 174
Simples, grupo, 250
Simples, zero, 156
Singular, transformação, 186
Sobrejetiva, função, **10**
Solução, de congruências, 137
de equações de 2.º e 3.º graus, **286**
de equações por radicais, 279, **280**
condições necessária e suficientes para, 281
Soluções, espaço de, **192**
para os Exercícios, 301
Solúvel, grupo, **245**, 265
Sperner, E., 202
Steinitz, E., 181
teorema de substituição de, **181**
Stoll, R. R., 18, 108
Subanel, 75
Subanéis, interseção de, 75
supremo de, 75
Subconjuntos, **6**
próprio, **6**
restrição de função a, 12
Subconjuntos, interseção de, **6**
união de, **6**
Subespaços, **176**
supremo de, 177
Subcorpo, **113**
de corpo finito, 219
primo, 114
próprio, 113
Subgrupo, **45**-55
comutador, 65, **247**
conjugado, **234**
classes laterais de, **47**
de grupo cíclico, 49, 50
de índice *p* em um *p* grupo, 237
derivado, 65, **247**
gerado por um conjunto, **52**
índice de, **48**
normal, 58
próprio, **46**
p-Sylow (p-SS), 238
Subgrupos, supremo de, **50**
interseção de, **50**
Subnormal, cadeia, 244
Supremo, 118, 121

Supremo de:
ideais, 78
subanéis, 75
subspaços, 177, 178
subgrupos, 50
Suppes, P., 90, 108
Sylow, L., 238
Simetria de um:
triângulo, 25
n-ágono regular, 42
Simetria, função, 293
relação, 8
Simétrico, grupo de permutações S_n, **37**, 39, 40, 41, 46, 57, 245
polinômio cujo grupo é S_p, 290
solubilidade de, 289
insolubilidade S_n ($n > 5$), 250
Simétrico, polinômio, 297
Sistema de equações lineares, 191, 195

T

Thompson, J., 250
Total, ordem, **91**
Totalmente ordenado, conjunto, 91
Transcendente, elemento, **211**
Transcendente, extensão, **211**, 212, 213
Transcendentes, números reais, 211
Transformação linear, **185**-189
Transitiva, Lei, **8**, **91**
para extensões algébricas do corpo, 215
Transposição, 39, 296
Triangular, desigualdade, 94, 127

U

União de conjuntos, **6**
Única, teorema de fatoração,
para inteiros, 105
para polinômios, 152
em domínios euclideanos, 136
Único, domínio de fatoração (DFU), **162**-167
Unidade, **86**
ideal, 78
em domínios euclideanos, 130
em inteiros gaussianos, 129
em sistemas de integridade, 97

V

Valle-Poussin, de la, 106
Van der Waerden, B. L., 117, 127, 142, 171, 299
Vazio, conjunto, **5**
Venn, diagrama de, 6
Vetores, 24, 172, **173**
Vetorial, espaço, 22, 172, **173**-202

W

Wahab, J. H., 171
Walker, E. A., 260, 264
Wedderburn, J. H. M., 25, 229
teorema de, sobre anéis de divisão finitos, 230
Wielaudt, H., 238
Wiener, N., 7
Wilson, teorema de, 84
Witt, E., 229, 232
Wright, E. M., 108

Z

Zariski, O., 127, 142, 232
Zassenhaus, H. J., 69
Zero, **70**
ideal, **78**
polinômio, **145**
vetor, **173**, 175
Zero, divisor de, **74**
Zero, de um polinômio, **148**
múltiplo, **158**, 160
simples, 159
Zukerman, H. S., 18, 89, 108, 202, 264