# GRUPO DE ESTUDOS DO ENSINO DA MATEMÁTICA G. E. E. M. — SÃO PAULO

SÉRIE PROFESSOR N.º 6

# INICIAÇÃO ÀS ESTRUTURAS ALGÉBRICAS

L. H. JACY MONTEIRO

# GRUPO DE ESTUDOS DO ENSINO DA MATEMÁTICA G. E. E. M. — São Paulo

Série Professor N.o 6

Prof. Alternir A. R. Avaldi

# INICIAÇÃO ÀS ESTRUTURAS ALGÉBRICAS

7ª Edição

DISTRIBUIÇÃO



LIVRARIA NOBEL S. A.
EDITORA - DISTRIBUIDORA
MATRIZ: RUA MARIA ANTONIA, 108
TELEFONES 256-7081 - 256-6100 - 256-0054
FILIAL: R. DA CONSOLAÇÃO, 49 - TEL. 35-0783
CAIXA POSTAL 2373 - 01,222 SÃO PAULO

### APRESENTAÇÃO

1ª edição

O Grupo de Estudos do Ensino da Matemática, de São Paulo, no cumprimento de sua programação editorial, tem o prazer de lançar, dentro da *Série Professor*, o Volume de nº 6— "Iniciação às Estruturas Algébricas", de autoria de seu membro L.H.Jacy Monteiro.

Tal volume, mais que um livro de rico conteúdo, é um guia a todo professor secundário interessado no aspecto atual da Matemática, abrangendo áreas pertencentes ao 1º e 2º ciclos da escola média.

O Capítulo I trata de *Relações* que, desde a 1ª série ginasial, participam de toda programação de Matemática da escola secundária. No Capítulo II é feito o estudo geral das *Aplicações* e o III é o Capítulo destinado às *Operações*, com as respectivas propriedades estruturais.

Finalmente no Capítulo IV são estudados os *Grupos, Anéis* e *Corpos*, com aplicações. Atente-se para a ênfase dada ao tratamento da importante estrutura de *Grupo*, cujo estudo até o Teorema de Lagrange, é recomendado a todo professor secundário de Matemática.

O Departamento de Publicações do GEEM espera, com este novo volume de sua coleção, continuar contribuindo para o aprimoramento do professorado secundário brasileiro.

Outrossim, aproveita o ensejo para agradecer ao seu membro Renate G. Watanabe pela leitura dos originais, incluindo valiosas sugestões, bem como a todos que colaboraram para que este volume chegasse a termo num mínimo de tempo.

São Paulo, janeiro de 1968

## INTRODUÇÃO

- Utilizaremos nestas notas a teoria dos conjuntos que está exposta no volume 3 desta mesma série de publicações (ver [3], pp.21-66). Suporemos que o leitor conheça as propriedades elementares dos seguintes conjuntos:
- N conjunto dos números naturais  $(0 \in N)$ ;
- Z conjunto dos números inteiros;
- Q conjunto dos números racionais;
- R conjunto dos números reais.
- 2. Faremos, a seguir, um resumo das propriedades relativas à Aritmética do anel **Z** dos números inteiros que serão freqüentemente utilizadas neste livro.

#### 2,1 - Axioma de indução finita

Se S é um subconjunto qualquer do conjunto N dos números naturais e se S satisfaz as condições

- a) 0 ES;
- b)  $n \in S \Longrightarrow n + 1 \in S$ ;

então S = N.

O axioma de indução finita nos mostra que o único subconjunto de  $\, N \,$  que satisfaz as condições a) e b) é o próprio  $\, N \,$ .

#### 2,2 - Princípio do menor número natural

Todo conjunto não vazio de números naturais possui um mínimo.

Isto é, se  $S \subset \mathbb{N}$  e se  $S \neq \emptyset$  então existe m $\in S$  tal que m $\leq x$  para todo x em S (m é o m/nimo de S),

#### 2,3 - Princípio do menor número inteiro

Todo subconjunto S, de Z, que é não vazio e minorado, possui um mínimo. Isto é, se  $S \subset Z$ , com  $S \neq \emptyset$ , e se existe  $b \in Z$  tal que  $b \leq x$  para todo x em S (b é

um *minorante* de S), então existe um número inteiro m tal que: 1) m $\in$ S; 2) m $\leqslant$ x para todo x em S (m é o *mínimo* de S).

#### 2.4 - Algoritmo da divisão

Se a e b são dois números inteiros e se b  $\neq$ 0, então existe um único par (q,r), de números inteiros, tal que

$$a = bq + r$$
  $e \quad 0 \leqslant r \leqslant |b|$ .

#### 2.5 - Máximo divisor comum

Diz-se que um número inteiro d é o *máximo divisor comum* de dois números inteiros a e b se, e somente se, são válidas as seguintes condições

Di. dia e dib,

D2: para todo inteiro d', se d' a e d' b, então d' d.

Demonstra-se que dados dois números inteiros a e b existe um único de**Z** que satisfaz as condições D0, D1 e D2; além disso, existem números inteiros r e s tais que

$$d = ra + sb.$$

O máximo divisor comum de a e b é indicado pela notação mdc(a,b), Notemos que mdc(0,0)=0.

#### 2.6 - Números primos

Diz-se que um número inteiro p é *primo* se, e somente se, p satisfaz as seguintes condições

- 1)  $p \neq 0$  e  $p \neq \pm 1$ ;
- 2) os únicos divisores de p são -1, 1, p e -p.

Com o auxílio do último teorema enunciado acima demonstra-se que se p é um nú-mero primo e se p | (ab), com a e b inteiros, então p | a ou p | b. De um modo mais geral temos: se m | (ab) (onde a, b e m são números inteiros) e se mdc(m, a) = 1 (isto é, se a e m são primos entre si), então m | b.

#### 2.7 - Teorema fundamental da Aritmética

Todo número inteiro n, com n≠0, e n≠±1, é igual a um produto de números pri-

mos; além disso, se

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$$

são duas decomposições de n como produtos de números primos, então s=t e usando-se uma notação conveniente temos:  $p_i=\pm\,q_i$  para  $i=1,2,\ldots,s$ .

Uma conseqüência imediata do teorema acima é a seguinte: para todo número inteiro n, com  $n \neq 0$  e  $n \neq \pm 1$ , existem números primos positivos

$$p_1, p_2, \ldots, p_r$$

tais que

$$n = \pm p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

onde  $a_1, a_2, \ldots, a_r$  são números naturais não nulos; além disso, esta decomposição de n é única a menos da ordem dos fatores.

# ÍNDICE

		pág,			
Apresentação					
INTRODUÇÃO					
,		7			
CAPÍTULO I	: RELAÇÕES				
§ 1.	Introdução	13			
§ 2.	Exemplos	13			
§ 3.	Relações binárias	20			
§ 4.	Composição de relações	24			
§ 5.	Relações recíprocas ou inversas	29			
§ 6.	Relações reflexivas, simétricas e transitivas	32			
§ 7.	Relações de equivalência	36			
§ 8.	Classes de equivalência	40			
§ 9.	Partições	45			
§10.	Relações de ordem	49			
RESU	IMO DO CAPÍTULO I	56			
		00			
CAPÍTULO II: APLICAÇÕES					
§ 1.	Introdução	58			
§ 2.	Aplicações	58			
§ 3.	Composição de aplicações	66			
§ 4.	Aplicações sobrejetoras	70			
§ 5.	Aplicações injetoras	73			
§ 6.	Aplicações bijetoras	78			
RESU	IMO DO CAPÍTULO II	85			
CAPÍTULO II	II: OPERAÇÕES				
§ 1.	Introdução	88			
§ 2.	Exemplos	88			
§ 3.	Leis de composição internas	90			
§ 4.	Elemento neutro	100			
§ 5.	Semigrupos e monóides	105			

			pág.
	§ 6. § 7. § 8. § 9. §10.	Elementos simetrizáveis.  Operações comutativas  Distributividade  Leis de composição externas  Relação compatível com uma operação.  MO DO CAPÍTULO III	113 118 122 128 143 144
CAPITU	LO I	V: GRUPOS, ANÉIS E CORPOS	
		lução	153
	\$ 1. \$ 2. \$ 3. \$ 4. \$ 5. \$ 6. \$ 7. \$ 8. \$ 9. \$10. \$11.	Definições  Exemplos de grupos.  Propriedades elementares de um grupo Isomorfismos.  Subgrupos Grupos cíclicos  Teorema de Lagrange  Relações de eqüivalência associadas a um subgrupo  Subgrupos normais e grupos quocientes Homomorfismos.  Teorema do homomorfismo  IMO DA PRIMEIRA PARTE	154 158 164 169 175 179 186 191 196 201 205 209
	\$12. \$13. \$14. \$15. \$16. \$17. \$18. \$19. \$20.	Definição de anel, exemplos Propriedades elementares de um anel Divisores do zero, elementos regulares Anéis de integridade. Corpos comutativos Subanéis e subcorpos Ideais e anéis quocientes Homomorfismos Característica de um anel	213 220 224 230 232 236 241 252 258
ÍNDICE ALFABÉTICO			

### ÍNDICE ALFABÉTICO

#### A

Adição 91 Adição módulo m 137 Anel 213 Anel com elemento unidade 213 Anel comutativo 213 Anel comutativo com elemento unidade 213 Anel das aplicações de X em A 216 Anel de Boole 216 Anel de integridade 230 Anel dos inteiros módulo m 215 Anel dos números inteiros 215 Anel nulo 215 Anel-produto 219 Anel trivial 216 Anel quociente 244 Anel unitário 213 Aplicação 58 Aplicação injetora 76 Aplicação canônica 63 Aplicação constante 63 Aplicação injetora 73 Aplicação idêntica 63 Aplicação inversa ou recíproca 78 Aplicação sobrejetora 70 Automorfismo (de anel) 252 Automorfismo (de grupo) 175

Automorfismo interno 175

Base 130
Bijeção 76
Binômio de Newton 222

#### C

Característica de um anel 259 Característica diferente de zero 259 Característica zero 259 Centro de um grupo 208 Classe de equivalência 40 Classe lateral à direita 186 Classe lateral à esquerda 186 Composição 91 Composta de duas aplicações 66 Composta de duas relações 25 Composto de uma n-upla 111 Congruência módulo m 38 Conjunto de chegada (de uma relação) 21 Conjunto de partida (de uma relação) Conjunto ordenado 49 Conjunto parcialmente ordenado 49 Conjunto quociente 41 Conjunto totalmente ordenado 49 Contra-domínio 59 Corpo 233 Corpo comutativo 232 Corpo dos inteiros módulo p 234 Corpo dos números racionais 234 Corpo dos números reais 234 Corpo dos quatérnios 233 Corpo primo 260

#### D

Denominador 235

Diferença 169

Diferença simétrica 94

Distributiva 123

Divisão 167, 235

Divisor do zero 226

Divisor próprio do zero 226

Domínio de uma aplicação 59

Domínio de uma relação 21

#### E

Elemento central 122
Elemento inversível 114, 223
Elemento neutro 101
Elemento regular 226
Elemento simetrizável 113
Elemento unidade 102
Elementos permutáveis 118
Endomorfismo (de anel) 252
Epimorfismo (de anéis) 252
Epimorfismo (de grupos) 201
Eqüipolência 38
Expoente 130

#### F

Fração 235
Fatores de um produto 91
Função 60

Gerador 180

Gráfico de uma relação 22

Grupo 154

Grupo aditivo 155

Grupo aditivo dos inteiros módulo m 159, 160

Grupo aditivo dos inteiros 159

Grupo aditivo dos números racionais 159

Grupo cíclico 180

Grupo cíclico de ordem 4 171

Grupo cíclico finito 180

Grupo cíclico infinito 180

Grupo comutativo ou abeliano 155

Grupo de Klein 170

Grupo das simetrias de um quadrado 162

Grupo dos automorfismo 175

Grupo dos automorfismos internos 175

Grupos dos elementos inversíveis de um anel 223

Grupo dos elementos simetrizáveis de um monóide 160

Grupo finito 155

Grupo infinito 155

Grupo multiplicativo 155

Grupo multiplicativo de um corpo 235

Grupo multiplicativo dos números racionais 159

Grupo multiplicativo dos números reais 159

Grupo multiplicativo dos números reais positivos 159

Grupo-produto 157

Grupo quociente 198

Grupo simétrico 160

Grupo-soma 157

Grupos isomorfos 173

Homomorfismo (de anéis) 252
Homomorfismo (de grupos) 201
Homomorfismo canônico (de anel) 244, 253
Homomorfismo canônico (de grupo) 202
Homomorfismo nulo 253

#### 1

Ideal 242 Ideal à direita 242 Ideal à esquerda 242 Ideal bilateral 242 Ideal bilateral associado a uma relação de equivalência 242 Ideal maximal 251 Ideal primo 249 Ideal principal 246 Imagem de um elemento 59 Imagem de uma aplicação 59 Imagem de uma relação 21 Imagem recíproca 84 Indicador de Euler 228 Índice de um subgrupo 190 Injeção 73 Intersecção 93 Inverso 114, 223 Isomorfismo (de anéis) 252 Isomorfismo (de grupos) 172 Isomorfismo recíproco ou inverso 172, 256

#### L

Lei de composição associativa 105 Lei de composição externa 129 Lei de composição interna 90

Lei de tricotomia 53

Lei do anulamento do produto (LAP) 231

Lei do cancelamento da multiplicação (LCM) 231

Lei do cancelamento da adição (LCA) 165

Lei geral de associatividade 112

Lei geral de comutatividade 120

Lei ou propriedade associativa 105

Lei ou propriedade comutativa 118

Leis restritas do cancelamento da multiplicação 224

#### M

Monóide 105

Monóide aditivo 106

Monóide comutativo 119

Monóide multiplicativo 106

Monomorfismo (de anéis) 252

Monomorfismo (de grupos) 201

Multiplicação 91

Multiplicação módulo m 139

Múltiplo 130

#### N

Notação aditiva 91

Notação de composição 91

Notação multiplicativa 91

Núcleo de um homomorfismo (de anéis) 252

Núcleo de um homomorfismo (de grupos) 203

Numerador 235

Operação associativa 105
Operação comutativa 118
Operação distributiva em relação à outra operação 123
Operação externa 129
Operação induzida 135
Operação interna 90
Oposto 114
Ordem 49
Ordem de um elemento 181
Ordem de um grupo 155
Ordem estrita 53
Ordem estrita total 53
Ordem oposta 50
Ordem parcial 49
Ordem total 49

#### P

Parcelas 91

Parte fechada 96

Partição 45

Partição associada a uma relação de equivalência 46

Permutação 76

Potência 130

Potenciação 94

Produto 91

Produto de uma n-upla 111

Prolongamento de uma aplicação 63

Prolongamento de uma ordem 55

#### Q

Quociente 166, 235

Regra dos sinais 221

Relação 20

Relação compatível com uma operação 133

Relação composta 25

Relação de equivalência 36

Relação de equivalência associada a uma aplicação 83

Relação de equivalência associada à direita (à esquerda) a um subgrupo 194

Relação de equivalência associada a um ideal bilateral 243

Relação de equivalência associada a uma partição 46

Relação de equivalência compatível com a estrutura de anel 241

Relação de ordem 49

Relação recíproca ou inversa 29

Relação reflexiva 32

Relação simétrica 32

Relação transitiva 32

Representação gráfica da composta 26

Representante de uma classe de equivalência 40

Representante de uma classe lateral 186

Restrição de uma aplicação 63

Restrição de uma operação 96

Restrição de uma ordem 555

Reunião 93

S

Semigrupo 105

Semigrupo aditivo 105

Semigrupo comutativo 119

Semigrupo multiplicativo 105

Simétrico de um elemento 113

Sobrejeção 70

Soma 91

Soma de uma n-upla 11

Subanel 236

Subanel unitário 240
Subcorpo 237
Subgrupo 175
Subgrupo cíclico 180
Subgrupo invariante 201
Subgrupo normal 197
Subtração 167

#### T

Tábua de um grupo finito 156

Tábua de uma lei de composição 92

Teorema do homomorfismo (para anéis) 256

Teorema do homomorfismo (para grupos) 205

Teorema de Lagrange 189

Termos de um composto 91

Termos de um produto 91

Termos de uma soma 91

V

Vetor livre 44

Z

Zero 102

#### BIBLIOGRAFIA

- [1] BEAUMONT, R.A. PIERCE, R.S. *The Algebraic Foundations of Mathematics*, Addison-Wesley Publishing Company, Inc., Reading (1963)
- [2] CALAME, A. Mathématiques Modernes, volume I (1965), volume II (1966), Éditions du Griffon, Neuchâtel
- [3] CASTRUCCI, B. Elementos de teoria dos conjuntos, Grupo de Estudos do Ensino da Matemática, Série Professor, Nº 3, S. Paulo (1967)
- [4] DEAN, R.A. Elements of Abstract Algebra, John Wiley and Sons Inc., New York (1966)
- [5] JACY MONTEIRO, L.H. Elementos de Álgebra, Instituto de Matemática Pura e Aplicada, ao Livro Técnico S.A., Rio de Janeiro (1969)
- [6] PATTERSON, E.M. RUTHERFORD, D.E. Elementary Abstract Algebra, University Mathematical Texts, Oliver and Boyd Ltd., Londres (1965)
- [7] Um Programa Moderno de Matemática para o Ensino Secundário (Do Original: Un Programme Moderne de Mathématiques pour l'Enseignement Secondaire — O.E.C.E.), Grupo de Estudos do Ensino da Matemática, Série Professor Nº 2 (1965)
- [8] WHITESITT, J.E. Principles of Modern Algebra, Addison-Wesley Publishing Company, Inc., Reading (1964).

## PUBLICAÇÕES DO G. E. E. M. — SÃO PAULO

#### SÉRIE PROFESSOR

- N.º 1 MATEMÁTICA MODERNA PARA O ENSINO SECUNDÁRIO G. E. E. M.
- N.º 2 UM PROGRAMA MODERNO DE MATEMÁTICA PARA O ENSINO SECUNDÁRIO G. E. E. M.
- N.º 3 ELEMENTOS DA TEORIA DOS CONJUNTOS Benedito Castrucci
- N.º 4 INTRODUÇÃO À LÓGICA MATEMÁTICA Benedito Castrucci
- N.º 5 COMBINATÓRIA E PROBABILIDADES Ruy Madsen Barbosa
- N.º 7 POLINÔMIOS DIVISIBILIDADE L. H. Jacy Monteiro

#### SÉRIE ENSINO PRIMÁRIO

- N.º 1 INTRODUÇÃO DA MATEMÁTICA MODERNA NA ESCOLA
  PRIMÁRIA Anna Franchi e Manhucia P. Liberman (esgotado)
- N.º 2 UMA INICIAÇÃO À MATEMÁTICA

  Lucília Bechara Sanchez e Manhúcia Perelberg Liberman