

Adelina-Loredana MANEA

FUNDAMENTELE ALGEBRICE ALE INFORMATICII PRIN EXERCITII



Editura
Universității
Transilvania
din Brașov

2025

EDITURA UNIVERSITĂȚII TRANSILVANIA DIN BRAȘOV

Adresa: Str. Iuliu Maniu nr. 41A
500091 Brașov
Tel.: 0268 476 050
Fax: 0268 476 051
E-mail: editura@unitbv.ro

Editură recunoscută CNCSIS, cod 81.

Copyright © Autorul, 2025

Lucrarea a fost avizată de Departamentul de Matematică și Informatică, Facultatea de Matematică și informatică a Universității Transilvania din Brașov.

Descrierea CIP a Bibliotecii Naționale a României

MANEA, ADELINA LOREDANA

Fundamentele algebrice ale informaticii prin exerciții / Adelina-Loredana Manea. - Brașov : Editura Universității "Transilvania" din Brașov, 2025

Conține bibliografie

ISBN 978-606-19-1826-3

004

51

Cuprins

1	Mulțimi. Relații. Funcții	3
1.1	Mulțimi	3
1.1.1	Breviar de teorie	3
1.1.2	Aplicații	4
1.2	Relații	10
1.2.1	Breviar teoretic	10
1.2.2	Aplicații	10
1.3	Relații de echivalență	13
1.3.1	Breviar teoretic	13
1.3.2	Aplicații	14
1.4	Funcții	25
1.4.1	Breviar teoretic	25
1.4.2	Aplicații	26
2	Monoizi	37
2.1	Monoid	37
2.1.1	Breviar teoretic	37
2.1.2	Aplicații	39
2.2	Monoidul liber generat de o mulțime	46
2.2.1	Breviar teoretic	46
2.2.2	Aplicații	47
2.3	Elemente de teoria codificării	54
2.3.1	Breviar teoretic	54
2.3.2	Aplicații	55
3	Grupuri	61
3.1	Grupuri. Morfisme de grupuri	61
3.1.1	Breviar teoretic	61
3.1.2	Aplicații	62

3.2	Subgrup	74
3.2.1	Breviar teoretic	74
3.2.2	Aplicații	75
3.3	Teorema lui Lagrange. Grup factor	85
3.3.1	Breviar teoretic	85
3.3.2	Aplicații	86
3.4	Ordinul unui element	90
3.4.1	Breviar teoretic	90
3.4.2	Aplicații	90
3.5	Grupuri ciclice	100
3.5.1	Breviar teoretic	100
3.5.2	Aplicații	101
3.6	Aplicație în criptografie: Logaritmul discret	108
3.6.1	Breviar teoretic	108
3.6.2	Aplicații	109
4	Inele și corpuri	111
4.1	Inele. Elemente speciale în inele	111
4.1.1	Breviar teoretic	111
4.1.2	Aplicații	113
4.2	Subinel, subcorp, ideal	127
4.2.1	Breviar de teorie	127
4.2.2	Aplicații	128
4.3	Morfisme de inele și morfisme de corpuri. Inel factor	133
4.3.1	Breviar teoretic	133
4.3.2	Aplicații	134
5	Spații vectoriale	143
5.1	Spații vectoriale	143
5.1.1	Breviar teoretic	143
5.1.2	Aplicații	144
5.2	Subspații vectoriale	148
5.2.1	Breviar teoretic	148
5.2.2	Aplicații	149
5.3	Bază și dimensiune	163
5.3.1	Breviar teoretic	163
5.3.2	Aplicații	164
5.4	Matricea schimbării de bază	173
5.4.1	Breviar teoretic	173

5.4.2	Aplicații	173
5.5	Corpuri-spații vectoriale	177
5.5.1	Breviar teoretic	177
5.5.2	Aplicații	178
5.6	Produs scalar. Ortogonalitate.	181
5.6.1	Breviar teoretic	181
5.6.2	Aplicații	183
5.7	Morfisme liniare	192
5.7.1	Breviar teoretic	192
5.7.2	Aplicații	193
6	Coduri liniare	201
6.1	Codificare liniară	201
6.1.1	Breviar teoretic	201
6.1.2	Aplicații	202
6.2	Matrice de control. Sindromul unui vector.	207
6.2.1	Breviar teoretic	207
6.2.2	Aplicații	208
6.3	Corectarea erorilor	211
6.3.1	Breviar teoretic	211
6.3.2	Aplicații	212
6.4	Coduri Hamming	227
6.4.1	Breviar teoretic	227
6.4.2	Aplicații	227
7	Anexe	229
7.1	Anexa 1- Grupuri de permutări	229
7.2	Anexa 2: Inele de matrice	236
7.3	Anexa 3: Rezolvarea sistemelor de ecuații liniare	245
7.4	Anexa 4: Inele de polinoame	256

Prefață

Studiul matematicii în pregătirea unui informatician reprezintă o bază necesară înțelegerii conceptelor cu care urmează să lucreze în zona de dezvoltare creativă a domeniului său de specialitate.

Acest studiu este cu atât mai eficient cu cât implicarea personală este mai mare. Acesta este motivul elaborării volumului de față care este conceput pentru studiu individual. Fiecare paragraf are un breviar teoretic minimal, cu definiții, eventual exemple și câteva proprietăți, urmat de aplicații care îmbină elemente de înțelegere a noțiunilor enunțate cu elemente practice și teoretice de construcție a altor exemple și proprietăți. Totul este conceput ca exercițiu, deci permite o redescoperire de către cititor atât a elementelor teoretice care derivă din definițiile date, cât și a unor situații punctuale, practice, care ancorează conceptele într-un cadru concret.

Primul capitol trimite cititorul în zona de fundament absolut al conceptelor matematice, fiind o invitație la reactualizarea cunoștințelor despre mulțimi și funcții din liceu, dar și la completarea acestora cu noțiunile de relație între două mulțimi și partiție a unei mulțimi. Aceste concepte sunt utile oricărei persoane care utilizează raționament matematic, logic, indiferent de specializarea sa.

Următoarele patru capitole prezintă graduat structurile algebrice în care multe concepte informatice se construiesc. Sunt structuri abstracte definite de mulțimi dotate cu legi de compoziție care verifică anumite axiome pe baza cărora se stabilesc tehnici de calcul care conduc la modele matematice aplicabile în domenii tehnice și în informatică.

Astfel, capitolul doi este dedicat structurii algebrice de monoid, ultimul paragraf al acestui capitol fiind despre cele mai simple codificări bazate pe monoidul liber generat de o mulțime numită alfabet.

Capitolul al treilea, în care este dezvoltată structura de grup cu proprietăți specifice, are ca element aplicativ elemente de criptografie cu chei publice și private. Capitolul al patrulea introduce structuri

algebrice cu două legi de compoziție interne, numite inele și corpuri. Aceste structuri sunt necesare, prin tehnicile de calcul specifice, în capitolul al cincilea care este dedicat spațiilor vectoriale. Această ultimă structură algebrică crează cadrul teoretic pentru ultimul capitol în care se introduc codurile liniare.

Volumul are prevăzute și patru anexe în care se prezintă grupurile de permutări, inelele de matrice, metodele de rezolvare a sistemelor de ecuații liniare și inelele de polinoame studiate în liceu, acestea fiind noțiuni necesare în parcurgerea exercițiilor. Cititorul care nu este bine familiarizat din programul preuniversitar parcurs cu aceste noțiuni este invitat să își actualizeze cunoștințele consultând aceste anexe.

Autoarea

Capitolul 1

Mulțimi. Relații. Funcții

1.1 Mulțimi

1.1.1 Breviar de teorie

Considerăm cunoscute noțiunile de mulțime, submulțime, relațiile între mulțimi (incluziune, egalitate) și operațiile cu mulțimi: intersecția, reuniunea, diferența, diferența simetrică, produsul cartezian. Egalitatea a două mulțimi se demonstrează prin dublă incluziune. Notăm cu Φ mulțimea vidă.

Pentru o mulțime A notăm cu $P(A)$ mulțimea tuturor submulțimilor sale, numită *mulțimea părților lui A* .

Notăm cu $|A|$ cardinalul mulțimii A . Considerăm cunoscut faptul că numărul elementelor reuniunii a două mulțimi disjuncte este suma cardinalelor celor două mulțimi.

Fie M o mulțime și A o submulțime a sa. Diferența $M - A$ se mai numește *complementara* mulțimii A și se notează $C_M A$ sau simplu $\bar{A}$ dacă mulțimea M se subînțelege din context.

Un instrument util în demonstrații este *Inducția matematică*. Aceasta este un procedeu prin care se demonstrează afirmații matematice referitoare la orice număr natural $n \geq n_0$.

Există mai multe variante ale inducției matematice, dintre care amintim inducția simplă și inducția completă.

Fie $P(n)$ o afirmație matematică și $n_0 \in \mathbb{N}$ un număr natural fixat. Se cere să se arate că $P(n)$ este adevărată pentru orice $n \geq n_0$.

Inducția matematică constă în doi pași: *verificarea* și *etapa de demonstrație*, numită și *etapa inductivă*.

Inducția simplă:

- Verificăm $P(n_0)$ adevărat.
- Presupunem $P(k)$ adevărat și demonstrăm $P(k + 1)$ adevărat.

Inducția completă:

- Verificăm $P(n_0)$ adevărat.
- Presupunem $P(k)$ adevărat pentru orice $n_0 \leq k \leq n$ și demonstrăm $P(n + 1)$ adevărat.

1.1.2 Aplicații

Exercițiul 1.1.1. a) Fie $A = \{1, 2\}$. Scrieți mulțimile $P(A)$ și $P(P(A))$.

b) Arătați că dacă A este o mulțime finită cu $|A| = m$, atunci $|P(A)| = 2^m$.

Rezolvare: Mulțimile cerute sunt:

$$P(A) = \{\Phi, \{1\}, \{2\}, \{1, 2\}\},$$

Elementele mulțimii $P(P(A))$ sunt:

$$\begin{aligned} &\Phi, \{\Phi\}, \{\{1\}\}, \{\{2\}\}, \{\{1, 2\}\}, \{\Phi, \{1\}\}, \{\Phi, \{2\}\}, \{\Phi, \{1, 2\}\}, \\ &\{\{1\}, \{2\}\}, \{\{1\}, \{1, 2\}\}, \{\{2\}, \{1, 2\}\}, \{\Phi, \{1\}, \{2\}\}, \\ &\{\Phi, \{1\}, \{1, 2\}\}, \{\Phi, \{2\}, \{1, 2\}\}, \{\{1\}, \{2\}, \{1, 2\}\}, P(A). \end{aligned}$$

b) Vom demonstra prin inducție matematică, după m , afirmația din enunț.

Pas 1. Dacă $m = 0$ atunci $A = \Phi$ și $P(A) = \{\Phi\}$, deci $|P(A)| = 2^0$.

Pas 2. Presupunem că orice mulțime cu $m - 1$ elemente are exact 2^{m-1} submulțimi și fie A cu m elemente. Vom demonstra că A are 2^m submulțimi.

Fie $x \in A$, fixat arbitrar, iar $A' = A - \{x\}$. Toate submulțimile lui A care nu conțin elementul x sunt submulțimi ale lui A' , în număr de 2^{m-1} , conform ipotezei de inducție. Submulțimile lui A care conțin x sunt de forma $B \cup \{x\}$, cu $B \subseteq A'$, deci tot 2^{m-1} . Avem deci

$$P(A) = P(A') \cup \{B \cup \{x\} \mid B \in P(A')\}.$$