

ALGEBRA PENTRU INFORMATICA

GEORGE CIPRIAN MODOI

CUPRINS

Bibliografie	2
1. Mulțimi, Funcții, Relații	3
1.1. Preliminarii logice	3
Exerciții la Preliminarii logice	3
1.2. Mulțimi	3
Operații cu mulțimi	4
Exerciții la Mulțimi	6
1.3. Funcții	6
Injectivitate, surjectivitate, bijectivitate	8
Cardinalul unei mulțimi	9
Produsul cartezian	9
Operații	10
Exerciții la funcții	11
1.4. Relații	13
Relații de echivalență	15
Relații de ordine	16
Exerciții la Relații	18
2. Grupuri, inele, corpuri	20
2.1. Grupuri	20
Subgrupuri	21
Homomorfisme de grupuri	22
Grupuri ciclice și ordinul unui element	23
Acțiuni ale grupurilor pe mulțimi	23
Grupul simetric	24
Exerciții la grupuri	25
2.2. Inele și corpuri	28
Subinele și subcorpuri	29
Homomorfisme	30
Elemente speciale într-un inel	31
Exerciții la inele și corpuri	32
3. Algebra liniara	33
3.1. Spații vectoriale și aplicații liniare	34
Subspații vectoriale	35
Suma și suma directă a subspațiilor	36
Aplicații liniare	37
Exerciții la spații vectoriale	38
3.2. Baza unui spațiu vectorial	39
Independență liniară	39

Baze și coordonate	40
Dimensiunea unui spațiu vectorial	42
Proprietatea de universalitate a bazei unui spațiu vectorial	42
Formule legate de dimensiune	43
Lema substituției	43
Exerciții la Baze	44
3.3. Aplicații liniare și matrici	45
Matricea unei liste de vectori	45
Matricea unei aplicații liniare	46
Exerciții la Aplicații liniare și matrici	47
3.4. Diagonalizarea unui endomorfism de spații vectoriale	47
Ideea algoritmului Page Ranking	49
Exerciții la Diagonalizare	49

BIBLIOGRAFIE

- [1] M. Artin, *Algebra*, Prentice Hall, 1991.
- [2] N. Both, S. Crivei, *Culegere de probleme de algebră*, Lito UBB, 1996.
- [3] S. Breaz, T. Coconet, C. Conțiu, *Lecții de Algebră*, Editura Eikon, Cluj, 2010.
- [4] P. M. Cohn, *Elements of Linear Algebra*, Springer Verlag, N.Y.-Berlin-Heidelberg, 1994.
- [5] I. D. Ion, N. Radu, *Algebra*, Editura Did. Ped. București, 1970.
- [6] I. D. Ion, N. Radu, C. Niță, D. Popescu, *Probleme de algebră*, Ed. Did. Ped., București, 1970.
- [7] B. Külshammer, *Lineare Algebra und Analytische Geometrie*, Vorlesungsskripte, <https://www.minet.uni-jena.de//algebra//skripten/skripten.html>.
- [8] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, 1986.
- [9] C. Năstăsescu, C. Niță, M. Brandiburu, D. Joița, *Exerciții și probleme de algebră*, Ed. Did. Ped. București, 1983.
- [10] I. Purdea, I. Pop, *Algebră*, Ed. Gill, Zalău, 2007.
- [11] C. Pelea, I. Purdea, *Probleme de algebră*, Editura EFES, Cluj, 2005.
- [12] G. Pic, I. Purdea, *Tratat de algebră modernă*, Editura Academiei, București, 1977.
- [13] A. E. Schroth, *Algebra für die Studierende der Informatik*, Vorlesungsskripte, http://www.carsten-buschmann.de/skripte/Algebra_fuer_Informatiker.pdf.

1. MULTIMI, FUNCȚII, RELAȚII

1.1. Preliminarii logice. Propozițiile logice sunt numai acele propoziții care pot fi adevărate sau false; celelalte propoziții gramaticale precum întrebarile, exclamațiile etc., care nu pot fi adevărate sau false, nu sunt incluse printre propozițiile logice. Propozițiile sunt conectate de operatori, dintre care noi vom folosi următorii:

- Negare \neg
- și logic \wedge
- sau logic (neexclusiv) \vee
- sau exclusiv \oplus
- implicația logică \Rightarrow
- echivalența logică \Leftrightarrow

Acești operatori sunt definiți prin următoarele tabele de avedări: (aici p și q sunt propoziții, iar 0 și 1 înseamnă fals, respectiv adevărat):

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \Rightarrow q$	$p \Leftrightarrow q$
0	0	1	0	0	0	1	1
0	1	1	0	1	1	1	0
1	0	0	0	1	1	0	0
1	1	0	1	1	0	1	1

Exerciții la Preliminarii logice.

Exercițiu 1.1.1. Să se arate că următoarele formule propoziționale sunt tautologii, adică ele sunt întotdeauna adevărate, indiferent de valoarea de adevăr a propozițiilor p, q, r :

- (a) $((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$
- (b) $((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$ *v este asociativ*
- (c) $(p \vee q) \Leftrightarrow (q \vee p)$
- (d) $(p \wedge q) \Leftrightarrow (q \wedge p)$
- (e) $(p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$
- (f) $(p \vee (q \wedge r)) \Leftrightarrow ((p \vee q) \wedge (p \vee r))$
- (g) $(p \vee (p \wedge q)) \Leftrightarrow p$
- (h) $(p \wedge (p \vee q)) \Leftrightarrow p$
- (i) $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$
- (j) $p \Rightarrow p$
- (k) $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$.

1.2. Multimi. Multimea este o colecție de obiecte distințe și bine determinate (care obiecte sunt numite *elemente*). Multimile pot fi date în mod direct prin enumerarea explicită a elementelor lor (altfel spus *sintetic*) sau prin precizarea unei condiții (proprietăți) pe care trebuie să o îndeplinească (adică *analitic*). Vom scrie $x \in A$ (și vom spune că "x aparține multimii A") pentru a exprima faptul ca x este un element al multimii A. De notat că noțiunile "multime" și "apartenență" sunt primare, adică ele nu se definesc.

- Exemplu 1.2.1.** a) $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, $C = \{?, ?, ?, \vee\}$, $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
 b) $Z = \{x \mid x \in \mathbb{N} \text{ și } 0 \leq x < 10\}$, $[-3, 8) = \{x \mid x \in \mathbb{R} \text{ și } -3 \leq x < 8\}$.
 c) Alte exemple ...

Definiție 1.2.2. Două multimi sunt egale exact atunci când ele conțin aceleși elemente.

Denumirea 1.28

(a) $\varphi: "x \in A"$

$\varphi \Rightarrow \varphi$

		$\varphi \Rightarrow \varphi$
		0
		1
0		
1		1

Deci $A \subseteq A$

(b) $p: "x \in A"$, $q: "x \in B"$, $r: "x \in C"$

Pf. să demonstrezi $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$
verificare cu tabloul de adevară

$$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$$

(c) De fel ca (b)

(d) $p: "x \in \emptyset"$, $q: "x \in A"$

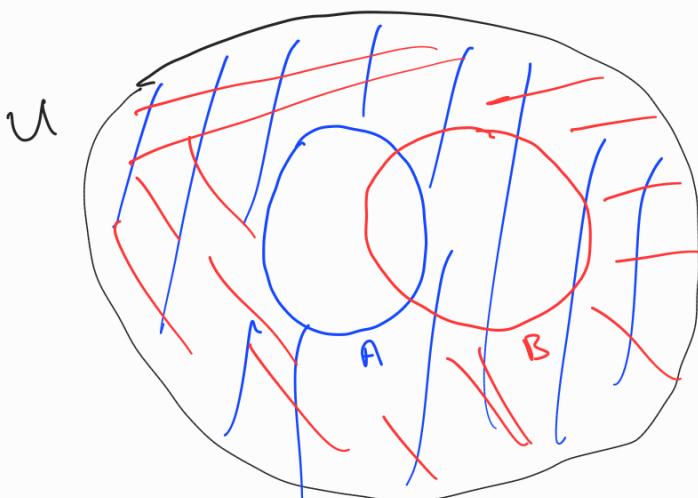
$p = 1$ (contradicție = într-o enunțare falsă)

Fără implicății sau deci

$p \Rightarrow q$ este adevarat.

(e) Fie φ și φ' două multimi videte.

$$\text{cf (d)} \quad \left. \begin{array}{l} \varphi \subseteq \varphi' \\ \varphi' \subseteq \varphi' \end{array} \right\} \stackrel{(c)}{\Rightarrow} \varphi = \varphi'.$$



$$C_u(A \cup B) \approx C_u A \cap C_u B$$

Exemplu 1.2.3. $\{1, 2, 3\} = \{x \in \mathbb{N} \mid 1 \leq x \leq 3\} = \{x \in \mathbb{Z} \mid 0 < x < 4\}$,
 $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$.

Observație 1.2.4. a) Elementele unei mulțimi nu sunt ordonate în nici un fel:
 $\{1, 2\} = \{2, 1\}$ sau $\{a, b, c\} = \{b, c, a\} = \{a, c, b\} = \{b, a, c\} = \{c, a, b\} = \{c, b, a\}$.

b) Într-o mulțime un element apare numai o dată: $\{1, 2\}$ și NU $\{1, 2, 2, 1\}$.

c) Definirea analitică a unei mulțimi necesită precauții suplimentare. De exemplu construcția: $R = \{x \mid x \notin x\}$ conduce la un paradox. Mai precis, amândouă propozițiile $R \in R$ și $R \notin R$ conduc la o contradicție (paradoxul lui Russell). Aici $x \notin A$ este negația propoziției $x \in A$. Nu ne vom ocupa prea mult de problemelor de acest tip, și vom evita paradoxurile lucrând "local", anume, când considerăm o proprietate P (Predicat) definim $A = \{x \in U \mid P(x)\}$ și nu $A = \{x \mid P(x)\}$, și U este o mulțime suficient de cuprinzătoare (Universul discursului).

Exemplu 1.2.5. Mulțimi de numere:

Numere naturale: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, $\mathbb{N}^* = \{1, 2, 3, \dots\}$.

Numere întregi: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

Numere raționale: $\mathbb{Q} = \{\frac{m}{n} \mid n, m \in \mathbb{Z}, n \neq 0\}$.

Numere reale: \mathbb{R} ($\mathbb{R} = ?$).

Numere complexe: $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ și $i^2 = -1$.

Definiție 1.2.6. Considerăm două mulțimi A și B . Spunem că A este o *submulțime* a lui B , dacă $x \in A$ implică $x \in B$. Scriem $A \subseteq B$.

Definiție 1.2.7. Mulțimea vidă notată cu \emptyset este mulțimea care nu conține nici un element.

Propoziție 1.2.8. Următoarele afirmații sunt valabile pentru orice mulțimi A , B și C :

- (a) $A \subseteq A$ (reflexivitate).
- (b) Dacă $A \subseteq B$ și $B \subseteq C$ atunci $A \subseteq C$ (tranzitivitate).
- (c) $A=B$ dacă $A \subseteq B$ și $B \subseteq A$ (antisimetrie).
- (d) $\emptyset \subseteq A$.
- (e) Multimea vidă este unică determinată.

Demonstrație. □

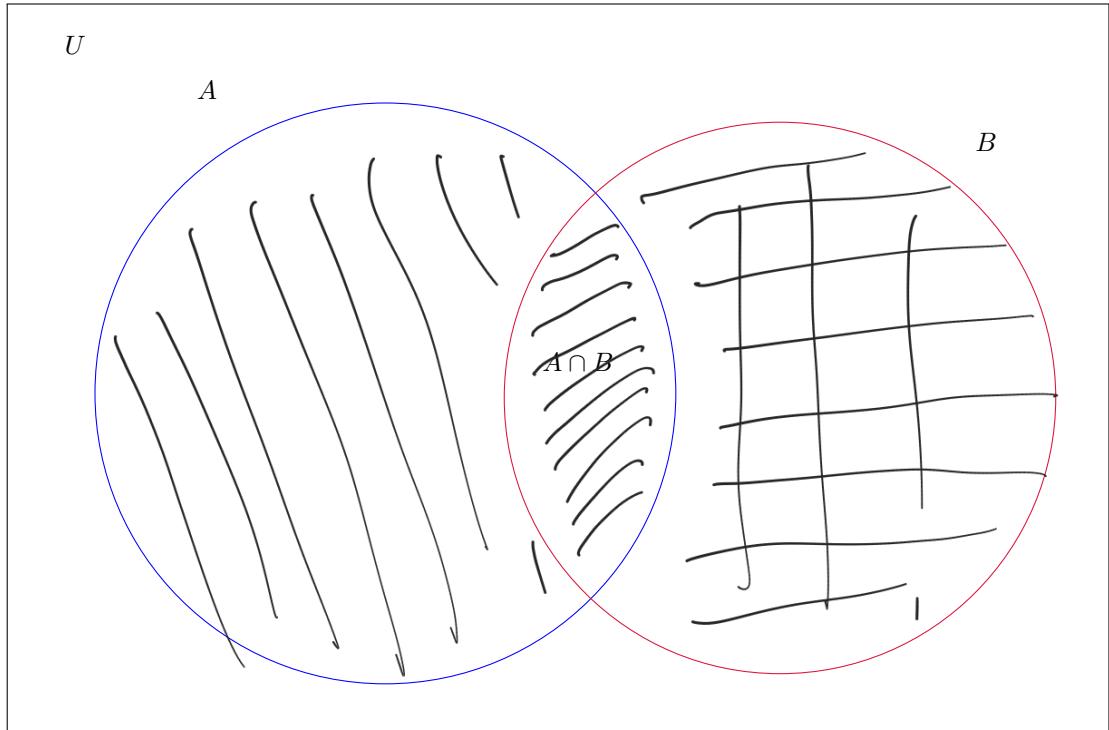
Operații cu mulțimi.

Definiție 1.2.9. Fie A și B mulțimi. Se definește:

- (a) Reuniunea dintre A și B prin $A \cup B = \{x \mid x \in A \vee x \in B\}$.
- (b) Intersecția dintre A și B prin $A \cap B = \{x \mid x \in A \wedge x \in B\}$.
- (c) Diferența dintre A și B prin $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

În cazul $A \subseteq U$ se numește complementara lui A în U mulțimea $\mathbf{C}_U A = U \setminus A$.

Observație 1.2.10. Mulțimile pot fi reprezentate prin aşa numitele diagrame Euler-Venn. De exemplu:



Teoremă 1.2.11. Fie A, B, C, U mulțimi, așa încât $A, B, C \subseteq U$.

- (a) $(A \cup B) \cup C = A \cup (B \cup C)$ și $(A \cap B) \cap C = A \cap (B \cap C)$ (asociativitate).
- (b) $A \cup B = B \cup A$ și $A \cap B = B \cap A$ (comutativitate).
- (c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ și $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (dublă distributivitate).
- (d) $A \cup A = A = A \cap A$ (idempotentă).
- (e) $A \cup (A \cap B) = A = A \cap (A \cup B)$ (absorbție).
- (f) $\mathbf{C}_U(A \cup B) = \mathbf{C}_U A \cap \mathbf{C}_U B$ și $\mathbf{C}_U(A \cap B) = \mathbf{C}_U A \cup \mathbf{C}_U B$ (regulile lui de Morgan).

Demonstrație.

□

Definiție 1.2.12. Fie A o mulțime. Mulțimea putere a mulțimii A este mulțimea tuturor submulțimilor lui A , adică:

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

Observație 1.2.13. Definiția mulțimii tuturor submulțimilor necesită precauții suplimentare: care univers trebuie folosit? De notat: paradoxul lui Cantor este construit cu ajutorul mulțimii tuturor submulțimilor.

Definiție 1.2.14. Pentru două mulțimi A și B , se definește *produsul cartezian* ca fiind:

$$A \times B = \{(a, b) \mid a \in A \text{ și } b \in B\}.$$

Aici (a, b) este o *pereche* (ceea ce înseamnă o mulțime ordonată), care din perspectiva teoriei mulțimilor poate fi definită prin

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

$$(a, b) \neq (b, a)$$

$$\{a, b\} \neq \{b, a\}$$

$$(A_1 \times A_2) \times A_3 = A_1 \times A_2 \times A_3 = \{(a_1, a_2, a_3) \mid a_i \in A_i \text{ for } i=1,2,3\}$$

$$(a_1, a_2, a_3) = ((a_1, a_2), a_3)$$

Observație 1.2.15. Inductiv se poate defini produsul cartezian a unui număr finit de mulțimi:

$$A_1 \times A_2 \times \dots \times A_{n-1} \times A_n = (\underbrace{A_1 \times A_2 \times \dots \times A_{n-1}}_{\text{produsul cartezian}}) \times A_n$$

Pentru o mulțime A avem $A^1 = A$ și $A^n = A^{n-1} \times A$, pentru orice $n > 1$.

Exerciții la Mulțimi.

Exercițiu 1.2.16. Să se determine $A \cup B$, $A \cap B$, $A \setminus B$, $\mathbf{C}_{\mathbb{N}}(A)$, $A \times B$, unde

$$A = \{n \in \mathbb{N} \mid \frac{3n+5}{n+1} \in \mathbb{N}\} \text{ și } B = \{x \in \mathbb{Z} \mid x \text{ este par și } -2 \leq x < 3\}.$$

Exercițiu 1.2.17. Să se determine $\mathcal{P}(\emptyset)$, $\mathcal{P}(\{\emptyset\})$, $\mathcal{P}(\{\emptyset, \{\emptyset\}\})$.

1.3. Funcții.



Definiție 1.3.1. O *funcție* (sau *aplicație*) este un triplet (A, B, f) care este format din două mulțimi A și B și o lege de corespondență f , astfel încât fiecărui element din A îi corespunde un singur element din B . Mulțimile A și B se numesc domeniul de definiție (sau simplu domeniul), respectiv domeniul de valori (sau codomeniul) funcției. Se scrie $f : A \rightarrow B$ sau $A \xrightarrow{f} B$. Pentru $a \in A$ se notează $f(a)$ unicul element din B care îi corespunde lui a prin f (numit și *imaginăria lui a prin f*). Se notează cu B^A mulțimea tuturor funcțiilor de la A la B , adică

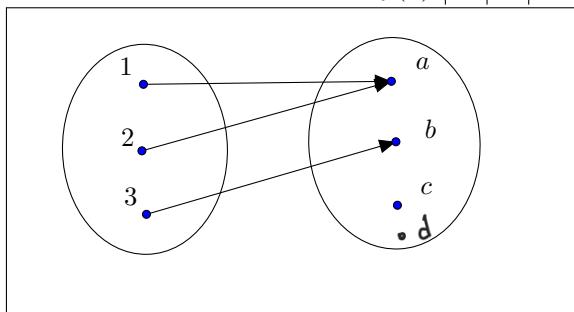
$$B^A = \{f : A \rightarrow B \mid f \text{ este o funcție}\}. \quad \checkmark$$

Observație 1.3.2. Două funcții $f : A \rightarrow B$ și $f' : A' \rightarrow B'$ sunt egale dacă $A = A'$, $B = B'$ și $f(x) = f'(x')$ pentru orice $x \in A$.

dacă și numai
dacă

Observație 1.3.3. Funcțiile pot fi definite în mai multe moduri:

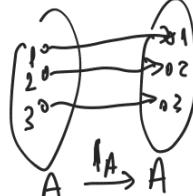
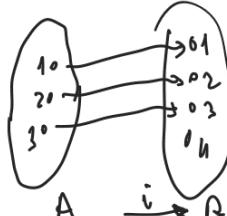
- (a) Prin indicarea directă a imaginii fiecărui element din domeniul, de exemplu $f : \{1, 2, 3\} \rightarrow \{a, b, c, d\}$, $f(1) = f(2) = a$ și $f(3) = b$. Variante (pentru aceeași funcție): Printr-un tabel:
$$\begin{array}{c|ccc} x & 1 & 2 & 3 \\ \hline f(x) & a & a & b \end{array}$$
 sau printr-o diagramă:



- (b) Printr-o formulă de calcul a imaginii fiecărui element, de exemplu $f : \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = x + 1$ pentru orice $x \in \mathbb{N}$. Intrebare: Orice formulă conduce la o funcție bine definită?

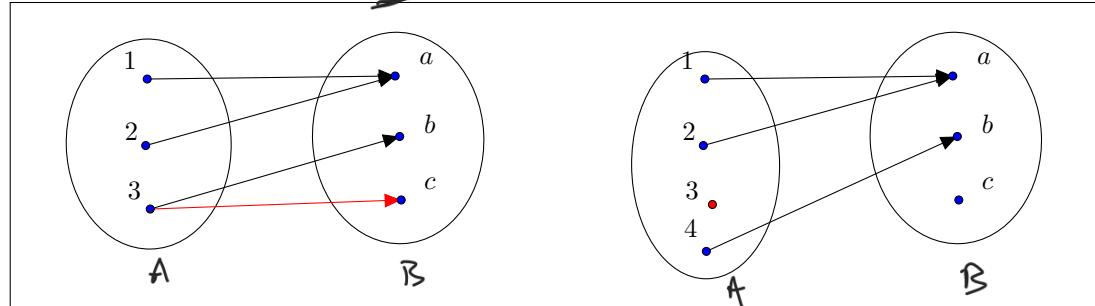
Exemplu 1.3.4. (a) Pentru orice mulțime A se definește *funcția identitate* prin $1_A : A \rightarrow A$, $1_A(x) = x$ pentru orice $x \in A$. Se notează uneori ~~$1_A = id_A$~~

(b) Dacă A și B sunt mulțimi, astfel încât $A \subseteq B$, se definește funcția *inclusiune* prin $i = i_{A,B} : A \rightarrow B$, $i(x) = x$, pentru orice $x \in A$. De notat că $i_{A,B} = 1_A$ dacă $A = B$, altfel $i_{A,B} \neq 1_A$.



(c) Dacă A, B, C sunt multimi, aşa încât $C \subseteq A$ și $f : A \rightarrow B$ este o funcție se construiește *funcția restricție* a lui f la C , prin $f|_C : C \rightarrow B$, $f|_C(x) = f(x)$ pentru orice $x \in C$.

(d) Următoarele corespondențe nu sunt funcții:



Definiție 1.3.5. Fie $f : A \rightarrow B$ o funcție și fie $X \subseteq A$, $Y \subseteq B$ două submulțimi (a lui A respectiv B). Se definește:

(a) Imaginea lui X prin f , ca fiind

$$f(X) = \{f(x) \mid x \in X\} = \{y \in B \mid \exists x \in X \text{ astfel încât } f(x) = y\}.$$

În cazul $X = A$ vom vorbi despre imaginea funcției f , și anume $f(A) = \text{Im } f$.

(b) Contraimagea (imaginea inversă) lui Y prin f , ca fiind

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}.$$

Definiție 1.3.6. Dacă $f : A \rightarrow B$ și $g : B \rightarrow C$ sunt funcții, atunci *componerea* lor este definită astfel: $g \circ f : A \rightarrow C$, $(g \circ f)(x) = g(f(x))$ pentru orice $x \in A$.

Teoremă 1.3.7. Atunci când este definită componerea funcțiilor este asociativă, adică pentru $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ avem $(h \circ g) \circ f = h \circ (g \circ f)$. Funcția identitate acționează ca element neutru pentru componerea funcțiilor, adică pentru $A \xrightarrow{f} B$ avem $f = f \circ 1_A = 1_B \circ f$.

Demonstrație. □

Definiție 1.3.8. O funcție $f : A \rightarrow B$ se numește *inversabilă* dacă există o altă funcție $f' : B \rightarrow A$ astfel încât $f' \circ f = 1_A$ și $f \circ f' = 1_B$.

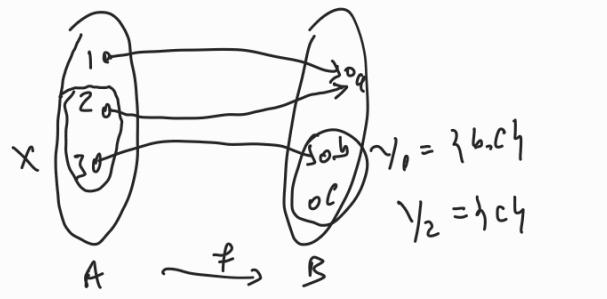
Propoziție 1.3.9. Dacă $f : A \rightarrow B$ este inversabilă, atunci există o singură funcție $f' : B \rightarrow A$ cu proprietatea $f' \circ f = 1_A$ și $f \circ f' = 1_B$. Notăm cu f^{-1} această funcție și o numim inversa funcției f . De asemenea avem $(f^{-1})^{-1} = f$.

Demonstrație. □

Exemplu 1.3.10. $\exp : \mathbb{R} \rightarrow (0, \infty)$, $\exp(x) = e^x$ este inversabilă și are inversa $\ln : (0, \infty) \rightarrow \mathbb{R}$. A se observă legătura dintre inversabilitatea funcțiilor și soluția (eventual unică) a ecuațiilor!

Propoziție 1.3.11. Dacă $A \xrightarrow{f} B \xrightarrow{g} C$ sunt două funcții inversabile, atunci tot așa este și $g \circ f$; mai mult avem $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Demonstrație. □

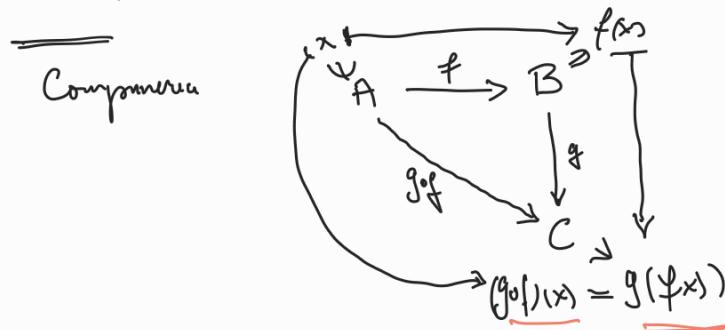


$$x = \{2, 3\} \quad f(x) = \{a, b\}$$

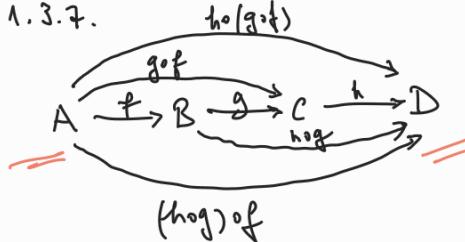
$$A \subseteq A \quad f(A) = \{a, b\}$$

$$f(A) = \underbrace{\{f(x) \mid x \in A\}}_{\text{Def}} = \{f(2), f(3)\} = \{a, b\}$$

$$f^{-1}(N_1) = \{3\} \quad f^{-1}(N_2) = \emptyset$$



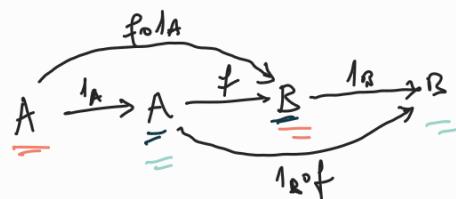
Denum 1.3.7.



Fie $x \in A$

$$(h \circ (g \circ f))(x) = h(g(f(x))) = h(g(f(x)))$$

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) \quad \square$$



Obe Dacă $A \neq B$ atunci nu există $f \circ 1_A = 1_B \circ f$

Dacă $A = B$ atunci $1_A = 1_B$ este elem. neutru -

Avem în același mod $f \circ 1_A = f = 1_B \circ f$ or

$$x \in A \quad (f \circ 1_A)(x) = f(1_A(x)) = f(x)$$

$$(1_B \circ f)(x) = 1_B(f(x)) = f(x) \quad \forall x \in A$$

1.3.8. Dacă

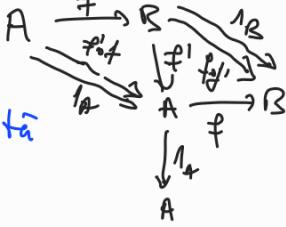
fiind $f: A \rightarrow B$ și presupunând că există $f': f'': B \rightarrow A$ astfel încât

$$f' \circ f = 1_A \quad \text{și} \quad f \circ f' = 1_B$$

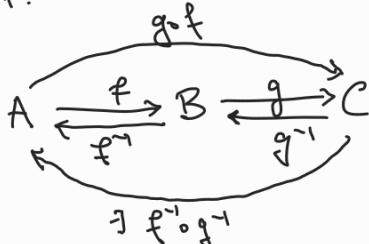
$$f'' \circ f = 1_A \quad \text{și} \quad f \circ f'' = 1_B$$

$$f' = 1_A \circ f = (f'' \circ f) \circ f' = f'' \circ (f' \circ f)$$

$$f'' \circ 1_B = f'', \quad \square$$



Dacă 1.3.11.

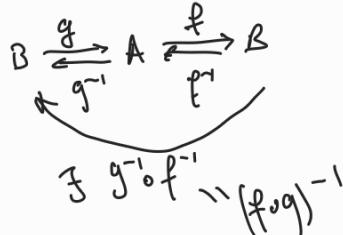
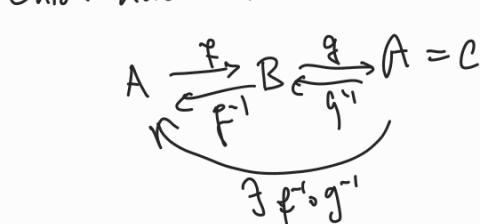


$$f' \circ f = 1_A \quad f \circ f' = 1_B$$
$$g^{-1} \circ g = 1_B \quad g \circ g^{-1} = 1_C$$

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g \circ g^{-1}) \circ f = f^{-1} \circ 1_B \circ f = f^{-1} \circ f = 1_A$$
$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ 1_B \circ g^{-1} = g \circ g^{-1} = 1_C$$
$$\Rightarrow (g \circ f)^{-1} = f^{-1} \circ g^{-1}, \quad \square$$

Obiceiul (1) dacă $A \neq C$ atunci nu există $g'' \circ f'$! !

(2) Chiar dacă $A = C$ atunci .



Dacă $A \neq B$ nu este posibil ca

$$(g \circ f)^{-1}: A \rightarrow B \quad g^{-1} \circ f^{-1}: B \rightarrow B$$
$$C \quad \text{să fie egale.}$$

(3) Chiar și în cazul în care $A = B = C$

nu este posibil ca $(g \circ f)^{-1} \neq g^{-1} \circ f^{-1}$. În unele situații particularmente posibile și egaleitatea

Injectivitate, surjectivitate, bijectivitate.

Definiție 1.3.12. O funcție $f : A \rightarrow B$ se numește:

- (a) *injectivă* dacă pentru $x_1, x_2 \in A$, $x_1 \neq x_2$ implică $f(x_1) \neq f(x_2)$.
- (b) *surjectivă* dacă pentru orice $y \in B$ există $x \in A$ așa încât $f(x) = y$.
- (c) *bijectivă* dacă f atât injectivă cât și surjectivă.

Observație 1.3.13. În mod echivalent o funcție $f : A \rightarrow B$ este

- (a) injectivă dacă $x_1, x_2 \in A$, $f(x_1) = f(x_2)$ implică $x_1 = x_2$.
- (b) surjectivă dacă $f(A) = B$.

Observație 1.3.14. O funcție $f : A \rightarrow B$ este injectivă, surjectivă sau bijectivă dacă pentru orice $y \in B$ ecuația $f(x) = y$ are cel mult, cel puțin, respectiv exact o soluție $x \in A$.

Propoziție 1.3.15. Următoarele propoziții sunt adevărate pentru două funcții $A \xrightarrow{f} B \xrightarrow{g} C$:

- (a) Dacă f și g sunt injective, atunci așa este și $g \circ f$.
- (b) Dacă f și g sunt surjective, atunci așa este și $g \circ f$.
- (c) Dacă f și g sunt bijective, atunci așa este și $g \circ f$.
- (d) Dacă $g \circ f$ este injectivă, atunci așa este și f .
- (e) Dacă $g \circ f$ este surjectivă, atunci așa este și g .
- (f) Dacă $g \circ f$ este bijectivă, atunci f este injectivă și g este surjectivă.

Demonstrație. □

Propoziție 1.3.16. Fie $f : A \rightarrow B$ o funcție cu $A \neq \emptyset$. Următoarele afirmații sunt echivalente:

- (i) f este injectivă.
- (ii) f are o inversă la stânga, adică există $g : B \rightarrow A$, astfel încât $g \circ f = 1_A$.
- (iii) f este simplificabilă la stânga, adică dacă $h_1, h_2 : A' \rightarrow A$ sunt funcții atunci $f \circ h_1 = f \circ h_2$ implică $h_1 = h_2$.

Demonstrație. □

Propoziție 1.3.17. Fie $g : B \rightarrow A$ o funcție. Următoarele afirmații sunt echivalente:

- (i) g este surjectivă.
- (ii) g are o inversă la dreapta, adică există $f : A \rightarrow B$ astfel încât $g \circ f = 1_A$.
- (iii) g este simplificabilă la dreapta, adică dacă $k_1, k_2 : A' \rightarrow A$ sunt funcții atunci $k_1 \circ g = k_2 \circ g$ implică $k_1 = k_2$.

Demonstrație. □

Teoremă 1.3.18. Fie $f : A \rightarrow B$ o funcție. Următoarele afirmații sunt echivalente:

- (i) f este bijectivă.
- (ii) f este inversabilă.
- (iii) f este inversabilă la stânga și inversabilă la dreapta.

Demonstrație. □

(iv) f este simplificabilă la stânga și la dreapta. □

Dem. 1.3.15



a) f, g inj.

Fie $x_1, x_2 \in A$ a.i. $(g \circ f)(x_1) = (g \circ f)(x_2)$
 $g(f(x_1)) = g(f(x_2))$
 $f(x_1) = f(x_2)$
 $x_1 = x_2$.

Dacă $g \circ f$ este inj.

b) f, g surj.

Fie $z \in C \xrightarrow{\text{surj.}} \exists y \in B: g(y) = z$

$\xrightarrow{\text{surj.}} \exists x \in A: f(x) = y$

Amenajare: $(g \circ f)(x) = g(f(x)) = g(y) = z$.

Dacă $g \circ f$ surj.

c) $g \circ f$ este inj.

Fie $x_1, x_2 \in A$ a.i. $f(x_1) = f(x_2) \xrightarrow{\text{f surj.}} g(f(x_1)) = g(f(x_2))$

$(g \circ f)(x_1) = (g \circ f)(x_2) \xrightarrow{\text{g of inj.}} x_1 = x_2$.

Dacă f este inj.

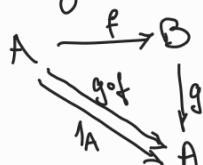
d) $g \circ f$ este surj.

Fie $z \in C \xrightarrow{\text{g of surj.}} \exists x \in A: (g \circ f)(x) = z \Rightarrow g(f(x)) = z$

Notă: $y = f(x) \in B$ $g(y) = z$. Dacă g surj. \square

Dem. 1.3.16. $A \xrightarrow{f} B$, $A \neq \emptyset$

(i) \Rightarrow (ii). Caut $g: B \rightarrow A$ a.i. $g \circ f = 1_A$



$g \circ f = 1_A \Rightarrow (g \circ f)(x) = 1_A(x), \forall x \in A \Rightarrow g(f(x)) = x, \forall x \in A$. (1)

Fie $y \in B$

Dacă $y \notin f(A) \xrightarrow{\text{finj.}} \exists ! x \in A: f(x) = y$

Pentru $g(y) = x$

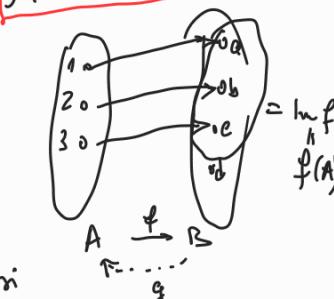
Dacă $y \notin f(A)$ atunci $A \neq \emptyset$ și

permite să alegem un elem. $a \in A$ și

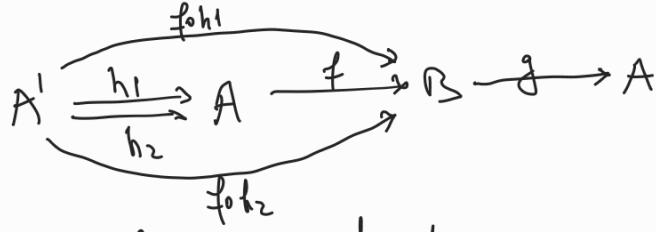
definim $g(y) = a$.

Dacă $g: B \rightarrow A$ $g(y) = \begin{cases} x, & \text{x este unic a.c. } f(x) = y \text{ pt } y \in f(A) \\ a, & y \notin f(A) \end{cases}$

Fie să se verifice că g este inversă a f deci $g \circ f = 1_A$.



(ii) \Rightarrow (iii)



Dim (i) $\exists g: B \rightarrow A$ a.i. $g \circ f = 1_A$

Stim $f \circ h_1 = f \circ h_2 \Rightarrow g \circ (f \circ h_1) = g \circ (f \circ h_2) \Rightarrow$

$$(g \circ f) \circ h_1 = (g \circ f) \circ h_2 \Rightarrow 1_A \circ h_1 = 1_A \circ h_2 \Rightarrow h_1 = h_2.$$

(iii) \Rightarrow (i). Fie $x_1, x_2 \in A$ a.i. $f(x_1) = f(x_2)$

Definim $A' = \{0\}$, $h_1, h_2: A' \rightarrow A$, $h_1(0) = x_1$, $h_2(0) = x_2$
 $f \circ h_1: A' \rightarrow B$, $f \circ h_2: A' \rightarrow B$

$$\left. \begin{aligned} (f \circ h_1)(0) &= f(h_1(0)) = f(x_1) = f(x_2) = f(h_2(0)) = (f \circ h_2)(0) \\ 0 &\text{ este singular elem. din } A' \end{aligned} \right\} \Rightarrow$$

$$f \circ h_1 = f \circ h_2 \xrightarrow{(iii)} h_1 = h_2 \Rightarrow x_1 = h_1(0) = h_2(0) = x_2.$$

Dici f este inj. \square .

1.3.17. Defin $g: B \rightarrow A$

Dim Def. 1.3.16.

(i) \Rightarrow (ii). g surj.

Cant $f: A \rightarrow B$ a.i. $g \circ f = 1_A$ sau echiv. (1) este valabilă.

Fie $x \in A$ surj. există elem. $\exists y$

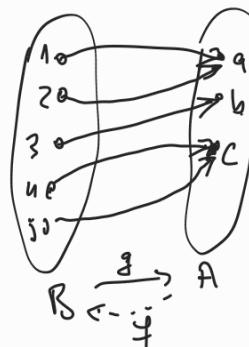
$y \in B$ a.i. $g(y) = x$ (sau

echiv. ec. $g(y) = x$ sau w unde $w \in B$).

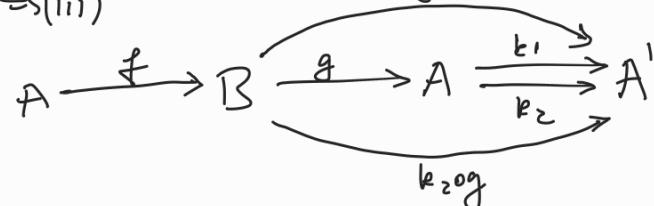
Aleg $y = y_x \in B$ a.i. $g(y) = x$ și

definesc $f(x) = y_x$.

Atunci (1) este valabilă dci $g \circ f = 1_A$.



(iii) \Rightarrow (ii)



$$k_1 \circ g = k_2 \circ g$$

Stim că $\exists f: A \rightarrow B$ a.i. $g \circ f = 1_A$ } \Rightarrow

$$(k_1 \circ g) \circ f = (k_2 \circ g) \circ f \Rightarrow k_1 \circ (g \circ f) = k_2 \circ (g \circ f) \Rightarrow k_1 \circ 1_A = k_2 \circ 1_A \Rightarrow k_1 = k_2.$$

(iii) \Rightarrow (i) Przypomnij co g nu wie mniej. \Rightarrow jest a.i.

$$g(y) \neq a, \forall y \in B$$

Abyg $A' = \{0, 1\}$ i definiuj $k_1, k_2: A \rightarrow A'$

$$k_1(x) = 0, \forall x \in A$$

$$k_2(x) = \begin{cases} 0 & \forall x \in A \setminus \{a\} \\ 1 & x = a \end{cases}$$

Ahunc: $k_1 \circ g, k_2 \circ g: B \rightarrow A'$

$$(k_1 \circ g)(y) = k_1(g(y)) = 0, \forall y \in B.$$

$$(k_2 \circ g)(y) = k_2(g(y)) = \underset{\#}{\underset{a}{0}}, \forall y \in B$$

Deci $k_1 \circ g = k_2 \circ g$ dan $k_1 \neq k_2$. \square .

Cardinalul unei mulțimi.

Definiție 1.3.19. Spunem că două mulțimi A și B au același cardinal dacă există o bijecție $f : A \rightarrow B$. O mulțime A este finită dacă $A = \emptyset$ sau există $n \in \mathbb{N}^*$ astă încât A și $\{1, 2, \dots, n\}$ au același cardinal. În ultimul caz, numarul natural n este unic determinat, deoarece nu există o bijecție $\{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}$ pentru $n \neq m$; spunem că A are cardinalul n , și scriem $|A| = n$ sau $\#A = n$. Mulțimea vidă nu are elemente, deci cardinalul ei este zero; scriem $|\emptyset| = 0$.

$$\boxed{\exists \phi \vdash |\emptyset| = 0}$$

Observație 1.3.20. Pentru mulțimile finite cardinalul este simplu numarul de elemente. Dar cardinalul se definește și pentru mulțimile infinite, așadar există o masură cu ajutorul căreia putem compara "mărimea" acestor mulțimi.

Propoziție 1.3.21. Fie A o mulțime finită. Următoarele afirmații sunt echivalente pentru o funcție $f : A \rightarrow A$:

- (i) f este injectivă.
- (ii) f este surjectivă.
- (iii) f este bijectivă.

Demonstrație. ~~temă~~

□

Observație 1.3.22. O mulțime infinită A poate fi caracterizată prin proprietatea că există o funcție injectivă (sau surjectivă) $f : A \rightarrow A$ care nu este bijectivă.

Definiție 1.3.23. Pentru o submulțime X a unei mulțimi A se definește funcția caracteristică $\chi_X : A \rightarrow \{0, 1\}$ a lui X (în raport cu A) prin

$$\chi_X(x) = \begin{cases} 1 & \text{dacă } x \in X \\ 0 & \text{dacă } x \notin X \end{cases} = \text{valoarea de aderare a proprietății "x \in X"}$$

Lemă 1.3.24. Pentru orice mulțime A funcția $\chi : \mathcal{P}(A) \rightarrow \{0, 1\}^A$, $\chi(X) = \chi_X$ este bijectivă.

Demonstrație. ~~temă~~

□

Corolar 1.3.25. Pentru orice mulțime A avem $|\mathcal{P}(A)| = |\{0, 1\}^A|$ și mulțimile A și $\mathcal{P}(A)$ nu au același cardinal.

Demonstrație. ~~temă~~

$$|\mathcal{P}(A)| = 2^n \Rightarrow |\mathcal{P}(\mathcal{P}(A))| = 2^{2^n}$$

□

Produsul cartezian.

Propoziție 1.3.26. Considerăm mulțimile A_1, A_2, \dots, A_n , unde $n \in \mathbb{N}^*$. Să se arate că

$$\phi : A_1 \times A_2 \times \dots \times A_n \rightarrow (A_1 \cup A_2 \cup \dots \cup A_n)^{\{1, 2, \dots, n\}} \text{ unde}$$

$$\phi(a_1, a_2, \dots, a_n)(i) = a_i, \text{ pentru orice } i \in I$$

este o funcție injectivă, a cărei imagine este:

$$\text{Im}\phi = \{f \in (A_1 \cup A_2 \cup \dots \cup A_n)^{\{1, 2, \dots, n\}} \mid f(i) \in A_i \text{ pentru orice } i \in I\}.$$

Așadar ϕ induce o bijecție

$$A_1 \times A_2 \times \dots \times A_n \rightarrow \text{Im}\phi, (a_1, a_2, \dots, a_n) \mapsto \phi(a_1, a_2, \dots, a_n).$$

Demonstrație.

□

$$I = \{a_1, a_2, a_3\} \quad A = \{b_1, b_2, b_3, b_4\}$$

$f: I \rightarrow A$ | f function

x	a_1	a_2	a_3	$A^I = A \times A \times A$
$f_1(x)$	(b_1, b_1, b_1)			
$f_2(x)$	(b_1, b_1, b_2)			
$f_3(x)$	(b_1, b_1, b_3)			
$f_4(x)$	(b_1, b_2, b_4)			
$f_5(x)$	b_1, b_2, b_1			
\vdots	---			
$f_8(x)$	b_1, b_2, b_n			
	$\Rightarrow a \cdot n \cdot d$			

$$\prod_{i \in I} A_i \Rightarrow (a_i)_{i \in I}, \text{ și multime posibil infinită}$$

$$f: I \rightarrow \bigcup_{i \in I} A_i, \quad a_i := f(i) \in A_i, \quad \forall i \in I$$

10 GEORGE CIPRIAN MODOI

Propoziția anterioară ne oferă posibilitatea de a extinde definiția produsului cartezian din cazul familiilor finite de mulțimi (a se vedea Observația 1.2.15) pentru o familie oarecare (posibil infinită).

Definiție 1.3.27. Se consideră familia de mulțimi A_i cu $i \in I$. Prin definiție *produsul cartezian* a acestei familii este:

$$\prod_{i \in I} A_i = \left\{ f : I \rightarrow \bigcup_{i \in I} A_i \mid f(i) \in A_i \text{ pentru orice } i \in I \right\}.$$

Observație 1.3.28. (1) Dacă în definiția anterioară avem $A_i = A$ pentru orice $i \in I$ gilt, atunci:

$$A^I = \prod_{i \in I} A_i = \{f : I \rightarrow A \mid f \text{ este o funcție}\}$$

(a se compara cu notația B^A din definiția 1.3.1).

(2) Existența produsului cartezian necesită o axiomă specială a teoriei mulțimilor, și anume Axioma Alegerii. Deși intuitiv este clar, din punct de vedere formal nu este posibil ca în lipsa acestei axiome să construim o funcție $f : I \rightarrow \bigcup_{i \in I} A_i$ așa încât $f(i) \in A_i$ pentru orice $i \in I$ (adică să alegem elementele $f(i) \in A_i, i \in I$).

Operații.

Definiție 1.3.29. Fie A o mulțime. O *operație (binară)* pe A este o funcție $* : A \times A \rightarrow A$. Adesea se scrie $a * b$ în loc de $*(a, b)$.

Definiție 1.3.30. O operație $* : A \times A \rightarrow A$ pe A se numește:

- (a) *asociativă* dacă $a * (b * c) = (a * b) * c$ pentru orice $a, b, c \in A$.
- (b) *comutativă* dacă $a * b = b * a$ pentru orice $a, b \in A$.

Un element $e \in A$ cu proprietatea $e * a = a * e = a$ pentru orice $a \in A$ se numește *element neutru* pentru $*$. Dacă operația $*$ are un element neutru e , atunci un element $x \in A$ se numește *inversabil* dacă există $x' \in A$ așa încât $x * x' = e = x' * x$.

Propoziție 1.3.31. Dacă o operație $* : A \times A \rightarrow A$ are un element neutru, atunci el este unic.

Demonstrație. $e, e' \in A$ neutre $\begin{cases} e * e' = e' \\ e * e' = e \end{cases} \Rightarrow e = e'$ \square

Propoziție 1.3.32. Se consideră o operație asociativă $* : A \times A \rightarrow A$ care are un element neutru e .

- (a) Dacă $x \in A$ este inversabil, atunci elementul $x' \in A$ cu proprietatea $x * x' = e = x' * x$ este unic. El se notează cu x^{-1} și se numește inversul (sau simetricul) lui x . Mai mult, avem $(x^{-1})^{-1} = x$.
- (b) Dacă $x, y \in A$ sunt inversabile, atunci $x * y$ este de asemenea inversabil și avem $(xy)^{-1} = y^{-1}x^{-1}$. $(x * y)^{-1} = y^{-1} * x^{-1}$.

Demonstrație. \square

Definiție 1.3.33. Un *monoid* este o pereche (structură) $(M, *)$ care consistă dintr-o mulțime M împreună cu o operație asociativă $* : M \times M \rightarrow M$, care are un element neutru. Pentru doi monoizi $(M, *)$ și (N, \circ) se numește *homomorfism de monoizi* o funcție $f : M \rightarrow N$ cu proprietatea $f(x * y) = f(x) \circ f(y)$ pentru orice $x, y \in M$.

a se vedea de la pd. funcții

Exemplu 1.3.34. (1). Următoarele perechi sunt monoizi: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , $(\mathbb{Q}, +)$, (\mathbb{Q}, \cdot) , $(\mathbb{R}, +)$, (\mathbb{R}, \cdot) , $(\mathbb{C}, +)$, (\mathbb{C}, \cdot) .

(2) Dacă $(M, *)$ și $(N, *)$ sunt monoizi, atunci $1_M : M \rightarrow M$ și $\bar{e} : M \rightarrow N$, $\bar{e}(x) = e$ pentru orice $x \in M$ sunt homomorfisme de monoizi.

Exerciții la funcții.

Exercițiu 1.3.35. Se consideră funcțiile:

- (1) $f_1 : \mathbb{R} \rightarrow \mathbb{R}$, $f_1(x) = x^2$
- (2) $f_2 : [0, \infty) \rightarrow \mathbb{R}$, $f_2(x) = x^2$
- (3) $f_3 : \mathbb{R} \rightarrow [0, \infty)$, $f_3(x) = x^2$
- (4) $f_4 : [0, \infty) \rightarrow [0, \infty)$, $f_4(x) = x^2$.

Să se studieze pentru fiecare dintre ele injectivitatea, surjectivitatea și bijectivitatea. În cazul existenței inversei să se determine această.

Exercițiu 1.3.36. Același exercițiu ca și 1.3.35 pentru funcțiile:

- (1) $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = \begin{cases} 2x + 1 & \text{dacă } x \leq 1 \\ x + 2 & \text{dacă } 1 < x \end{cases}$
- (2) $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = \begin{cases} x^2 + 1 & \text{dacă } x \leq 0 \\ -x + 2 & \text{dacă } 0 < x \end{cases}$
- (3) $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = \begin{cases} 2x + 1 & \text{dacă } x \leq 0 \\ x + 2 & \text{dacă } 0 < x \end{cases}$

Exercițiu 1.3.37. Să se precizeze dacă următoarele compuneri $f \circ g$ și $g \circ f$ sunt definite, și în caz afirmativ să se determine funcția compusă:

- (1) $f, g : \mathbb{R} \rightarrow \mathbb{R}$ $f(x) = \begin{cases} x^2 - 1 & \text{dacă } x \leq -1 \\ x - 1 & \text{dacă } -1 < x \end{cases}$ și $g(x) = \begin{cases} -x + 1 & \text{dacă } x < 3 \\ x - 2 & \text{dacă } 3 \leq x \end{cases}$
- (2) $f : \mathbb{R} \rightarrow [0, \infty)$, $f(x) = |x|$ și $g : \mathbb{N}^* \rightarrow \mathbb{R}$, $g(x) = 1/x$.
- (3) $f : \mathbb{R} \rightarrow [0, \infty)$, $f(x) = x^2 + 1$ și $g : [0, \infty) \rightarrow \mathbb{R}$, $g(x) = \sqrt{x}$.

Exercițiu 1.3.38. Fie A, B, C trei mulțimi așa încât $C \subseteq A$ și fie $f : A \rightarrow B$ o funcție. Să se arate că $f|_C : f \circ i$, unde $i : C \rightarrow A$ este funcția de incluziune.

Exercițiu 1.3.39. Fie $f : A \rightarrow B$ o funcție inversabilă și fie $Y \subseteq B$. Atunci prin $f^{-1}(Y)$ putem înțelege fie contraimaginea lui Y prin f sau imaginea Y prin f^{-1} . Să se arate că cele două interpretări nu intră în conflict (conduc la aceeași mulțime).

Exercițiu 1.3.40. Să se găsească un exemplu de două funcții $f, g : \mathbb{N} \rightarrow \mathbb{N}$ așa încât $g \circ f \neq f \circ g$. (Deși compunerea este definită bilateral, ea nu este comutativă).

Exercițiu 1.3.41. Să se arate că orice funcție $f : A \rightarrow B$ poate fi scrisă ca o compunere $f = i \circ p$ unde $i = i_f$ este injectivă iar $p = p_f$ este surjectivă.

Exercițiu 1.3.42. Să se găsească un exemplu care constă dintr-o funcție $f : A \rightarrow B$, așa încât:

- (1) f este injectivă dar nu are o inversă la stânga.
- (2) f are exact o inversă la stânga, dar nu este bijectivă.
- (3) f are exact două inverse la stânga.
- (4) f are o infinitate de inverse la stânga.

Exercițiu 1.3.43. Să se găsească un exemplu care constă dintr-o funcție $g : B \rightarrow A$, așa încât:

- (1) g are exact două inverse la dreapta.

(2) g are o infinitate de inverse la dreapta.

Să se arate că g are exact o inversă la dreapta dacă g este bijectivă.

Exercițiu 1.3.44. Să se găsească un exemplu care constă din două funcții $A \xrightarrow{f} B \xrightarrow{g} C$, aşa încât:

- (1) $g \circ f$ este injectivă, dar g nu este injectivă.
- (2) $g \circ f$ este surjectivă, dar f nu este surjectivă.
- (3) $g \circ f$ este bijectivă, dar g nu este injectivă și f nu este surjectivă.

Exercițiu 1.3.45. Fie $f : A \rightarrow B$ o funcție, și fie $X, X_1, X_2 \subseteq A$ și $Y, Y_1, Y_2 \subseteq B$ submulțimi. Să se arate:

- (1) $X \subseteq f^{-1}(f(X))$.
- (2) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.
- (3) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$.
- (4) $f(f^{-1}(Y)) \subseteq Y$.
- (5) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.
- (6) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

Exercițiu 1.3.46. Următoarele afirmații sunt echivalente, pentru o funcție $f : A \rightarrow B$:

- (i) f este injectivă.
- (ii) $X = f^{-1}(f(X))$ pentru orice submulțime $X \subseteq A$.
- (iii) $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$ pentru orice două submulțimi $X_1, X_2 \subseteq A$.

Să se găsească un exemplu care să arate că injectivitatea lui f este necesară pentru amândouă egalitățile (2) și (3). (ii) și (iii)

Exercițiu 1.3.47. Următoarele afirmații sunt echivalente, pentru o funcție $f : A \rightarrow B$:

- (i) f este surjectivă.
- (ii) $f(f^{-1}(Y)) = Y$ pentru orice submulțime $Y \subseteq B$.

Să se găsească un exemplu care să arate că surjectivitatea lui f este necesară pentru egalitatea (ii).

Exercițiu 1.3.48. Fie A și B două mulțimi finite cu $|A| = n$ și $|B| = m$. Să se determine $|B^A|$. Indicație: Se arată prin inducție după n că $|B^A| = m^n$.

Exercițiu 1.3.49. Fie A și B mulțimi finite cu $|A| = n$ și $|B| = m$. Să se determine numărul tuturor funcțiilor injective de la A la B . Indicație: Numărul căutat este $A_m^n = \frac{m!}{(m-n)!}$.

Exercițiu 1.3.50. Fie A o mulțime finită cu $|A| = n$. Să se determine numărul tuturor funcțiilor bijective $f : A \rightarrow A$ (adică numărul tuturor permutărilor lui A).

Exercițiu 1.3.51. Fie B o mulțime finită cu $|B| = m$. Să se determine numărul tuturor submulțimilor lui B cu n elemente. Indicație: Numărul căutat este $\binom{m}{n} = \frac{m!}{n!(m-n)!}$.

Exercițiu 1.3.52. Să se arate că $\sum_{i=0}^n \binom{m}{i} = 2^m$.

Exercițiu 1.3.53. (Principiul incluziei și al excluderii) Fie A_1, A_2, \dots, A_n mulțimi finite, unde $n \in \mathbb{N}^*$. Atunci:

$$\begin{aligned}|A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\&\quad - \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|.\end{aligned}$$

$$\begin{aligned}|A_1 \cap A_2 \cap \dots \cap A_n| &= \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cup A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cup A_j \cup A_k| \\&\quad - \dots + (-1)^{n-1} |A_1 \cup A_2 \cup \dots \cup A_n|.\end{aligned}$$

Exercițiu 1.3.54. Fie A și B mulțimi, cu $|A| = n$ și $|B| = m$. Să se găsească numărul tuturor funcțiilor surjective $f : A \rightarrow B$.

Exercițiu 1.3.55. Să se arate că mulțimile $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ au același cardinal.

Exercițiu 1.3.56. Să se arate că mulțimile \mathbb{N} și \mathbb{R} nu au același cardinal. Indicație: Se arată că $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Exercițiu 1.3.57. Fie A o mulțime finită cu $|A| = n$.

- (1) Câte operații se pot defini pe A ?
- (2) Câte dintre ele sunt comutative?
- (3) Câte dintre ele au un element neutru?

Exercițiu 1.3.58. Se consideră operația $* : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, dată prin $x * y = xy + 2ax + by$, pentru orice $x, y \in \mathbb{R}$. Să se determine $a, b \in \mathbb{R}$, astfel încât $*$ să fie asociativă și comutativă.

Exercițiu 1.3.59. Fie A o mulțime (numită *alfabet*), și fie $W = W(A) = \bigcup_{n \in \mathbb{N}} A^n$ (*mulțimea tuturor cuvintelor peste A*). Aici $A^0 = \{\lambda\}$, unde λ este cuvântul vid și $A^n = \{x_1 x_2 \dots x_n \mid x_1, x_2, \dots, x_n \in A\}$. Ca o excepție de la regula generală vom nota în acest context $x_1 x_2 \dots x_n$ și nu (x_1, x_2, \dots, x_n) un element din A^n , aşadar A^n este mulțimea tuturor cuvintelor de lungime n . Să se arate că (W, \cdot) este un monoid, unde

$$(x_1 x_2 \dots x_n) \cdot (y_1 y_2 \dots y_m) = x_1 x_2 \dots x_n y_1 y_2 \dots y_m \in A^{n+m}$$

este concatenarea (juxtapunerea) cuvintelor. Cum $A^1 = A$, putem privi A ca o submulțime a lui W . Să se arate că (W, \cdot) este *monoidul liber* peste A , ceea ce înseamnă că pentru orice monoid $(M, *)$ și pentru orice funcție $f : A \rightarrow M$, există un unic homomorfism de monoizi $\bar{f} : W \rightarrow M$, astfel încât $\bar{f}|_A = f$.

1.4. Relații.

Definiție 1.4.1. O *relație* este un triplet (A, B, R) , unde A și B sunt două mulțimi oarecare, iar $R \subseteq A \times B$. Uneori notăm $r = (A, B, R)$ și scriem *arb* în loc de $(a, b) \in R$, altori scriem numai $R \subseteq A \times B$ pentru a desemna o relație. Ca și în cazul funcțiilor A și B se numesc *domeniu* respectiv *codomeniu*. Dacă $A = B$ atunci relația $R \subseteq A \times A$ se zice *omogenă* (pe A).

Observație 1.4.2. Funcțiile pot fi privite ca fiind cazuri speciale de relații, și anume o funcție $f : A \rightarrow B$ este o relație $f = (A, B, F)$ cu proprietatea suplimentară că pentru orice $x \in A$ există un singur element $y \in B$ astfel încât xy . În acest caz $F = \{(a, f(a)) \mid a \in A\}$ este graficul funcției f .

$$F = \{(a, f(a)) \mid a \in A\} \subseteq A \times B$$

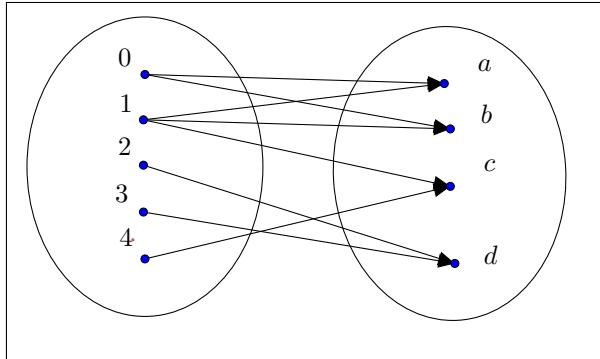
functii

- Exemplu 1.4.3.** Urătoarele exemple sunt relații care nu sunt funcții:
- (1) Relația uzuală mai mic sau egal este o relație omogenă pe \mathbb{N} , \mathbb{Z} , \mathbb{Q} sau \mathbb{R} .
 - (2) Divizibilitatea $a|b$ dacă există c astăncă $b = ac$ este o relație omogenă pe \mathbb{N} sau \mathbb{Z} .
 - (3) Fie $n \in \mathbb{N}$, $n > 1$. Congruența modulo n este o relație omogenă pe \mathbb{Z} . Reamintim: Congruența modulo n este definită prin $x \equiv y \pmod{n}$ dacă $n|(x-y)$.
 - (4) Pentru orice mulțime A apartenența este o relație între A și $\mathcal{P}(A)$.

Exemplu 1.4.4. Pentru orice mulțime A , egalitatea este o relație omogenă pe A . Se observă că această relație este și o funcție, mai precis funcția identitate a lui A .

Observație 1.4.5. Ca și în cazul funcțiilor, există mai multe moduri în care poate fi dată o relație:

- (1) Prin indicarea directă a perechilor care sunt în relație, de ex. dacă $A = \{0, 1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ și $R = \{(0, a), (0, b), (1, a), (1, b), (1, c), (2, d), (3, d), (4, c)\}$, atunci (A, B, R) este o relație. Diagramele vin și aici în ajutor:



- (2) Printr-o matrice cu intrări în mulțimea $\{0, 1\}$: Se consideră două mulțimi finite $A = \{a_1, a_2, \dots, a_m\}$ și $B = \{b_1, b_2, \dots, b_n\}$ și o relație $R \subseteq A \times B$. Această relație poate fi reprezentată printr-o matrice $M(R) = (m_{i,j}) \in \mathbb{M}_{m \times n}(\{0, 1\})$, unde

$$m_{i,j} = \begin{cases} 1 & \text{dacă } (a_i, b_j) \in R \\ 0 & \text{dacă } (a_i, b_j) \notin R \end{cases}$$

De exemplu matricea relației anterioare este:

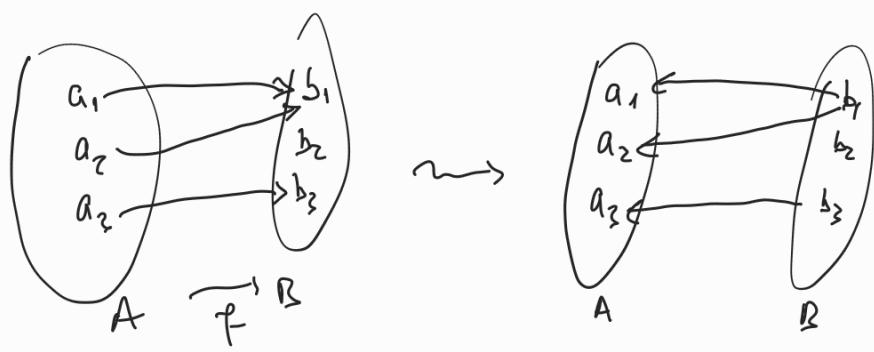
$$\begin{array}{c} \xrightarrow{0} \\ \xrightarrow{1} \\ \xrightarrow{2} \\ \xrightarrow{3} \\ \xrightarrow{4} \end{array} \left[\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array} \right]$$

Aici prin $\mathbb{M}_{m \times n}(\{0, 1\})$ se notează mulțimea tuturor matricilor (adică tabele dreptunghice) cu m linii și n coloane și cu intrări din $\{0, 1\}$.

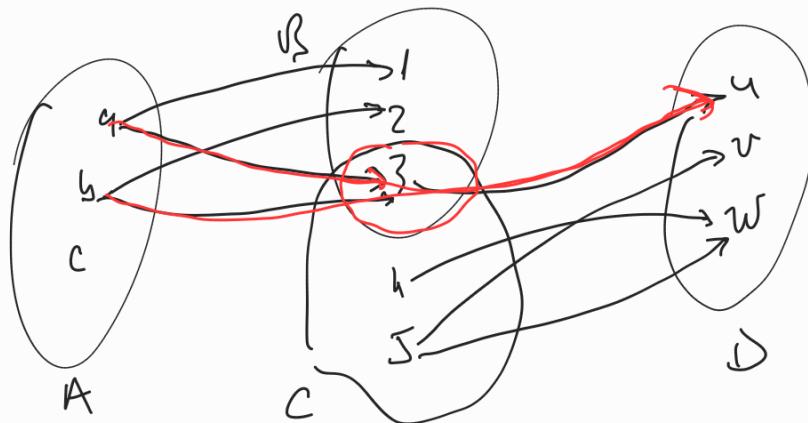
- (3) Printr-o proprietate pe care trebuie să o satisfacă toate elementele care se află în relație, ca în Exemplul 1.4.3 (2), (3). .

Definiție 1.4.6. Pentru orice relație (A, B, R) se definește *relația inversă* ca fiind (B, A, R^{-1}) , unde $(b, a) \in R^{-1}$ dacă $(a, b) \in R$ pentru orice pereche $(a, b) \in A \times B$.

Observație 1.4.7. Relația inversă se poate defini pentru orice relație, în particular pentru orice funcție privită ca relație. Dar relația inversă a unei funcții este exact atunci o funcție când funcția de la care pornim este bijectivă.



$f = (A, B, f)$ $\rightsquigarrow \exists (B, A, f^{-1})$
 $f^{-1} = \{(b_1, a_1), (b_2, a_2), (b_3, a_3)\}$
 relatie dan \cong en functie



$n = (A, B, R)$ $n = (C, D, S)$
 $R = \{(a_1, 1), (a_1, 3), (a_2, 2), (a_2, 3)\}$
 $S = \{(b_1, u), (b_1, v), (b_2, u), (b_2, w)\}$

$$S \circ R = (A, D, S \circ R)$$

$$S \circ R = \{(a_1, u), (a_2, u)\}$$

$\text{Ob} \quad \text{Dacă } B \cap C = \emptyset \Rightarrow S \circ R = (A, D, \emptyset)$
 $\emptyset \subseteq A \times D$

$$f: A \rightarrow B \text{ funcție} \quad f(X) = \{y \in B \mid \exists x \in X : f(x) = y\}$$

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$$

Definiție 1.4.8. Fie $r = (A, B, R)$ o relație și $X \subseteq A$, $Y \subseteq B$ submulțimi. Se definesc: $r(X) = \{y \in B \mid \text{există } x \in X \text{ așa încât } xry\}$ și $r^{-1}(Y) = \{x \in A \mid \text{există } y \in Y \text{ așa încât } xry\}$.

Observație 1.4.9. Pentru o relație $r = (A, B, R)$ și o submulțime $Y \subseteq B$ avem $(r^{-1})(Y) = r^{-1}(Y)$.

Definiție 1.4.10. Fie (A, B, R) și (C, D, S) două relații. Componerea celor două relații este definită prin: $(A, D, S \circ R)$ unde

$$S \circ R = \{(a, d) \mid \text{există } x \in B \cap C \text{ așa încât } (a, x) \in R \text{ și } (x, d) \in S\}.$$

Observație 1.4.11. Spre deosebire de cazul funcțiilor, compunerea este definită oricând fără a fi necesară coincidența dintre codomeniul primei relații cu domeniul celei de-a două.

Definiție 1.4.12. O relație omogenă $r = (A, A, R)$ se numește:

- (a) reflexivă dacă $a \sim a$ pentru orice $a \in A$.
- (b) tranzitivă dacă pentru orice $a, b, c \in A$ din $a \sim b$ și $b \sim c$ rezultă $a \sim c$.
- (c) simetrică dacă pentru orice $a, b \in A$ din $a \sim b$ rezultă $b \sim a$.
- (d) antisimetrică dacă pentru orice $a, b \in A$ din $a \sim b$ și $b \sim a$ rezultă $a = b$.

Se numește preordine o relație omogenă care este reflexivă și tranzitivă.

Relații de echivalență.

Definiție 1.4.13. Fie A o mulțime. O relație de echivalență (sau pe scurt echivalență) pe A este o preordine care este de asemenea simetrică, adică o relație omogenă pe A care este reflexivă, tranzitivă și simetrică.

Exemplu 1.4.14. Următoarele relații sunt echivalențe:

- (1) Relația de egalitate pe o mulțime arbitrară.
- (2) Congruența triunghiurilor (pe mulțimea tuturor triunghiurilor din plan).
- (3) Asemănarea triunghiurilor (pe mulțimea tuturor triunghiurilor din plan).

Definiție 1.4.15. Fie \equiv o relație de echivalență pe o mulțime A . Pentru un element $a \in A$ se notează

$$[a] = [a]_{\equiv} = \{x \in A \mid a \equiv x\}$$

clasa de echivalență a lui a . Se numește mulțimea factor a lui A modulo \equiv mulțimea tuturoe claselor de echivalență, adică

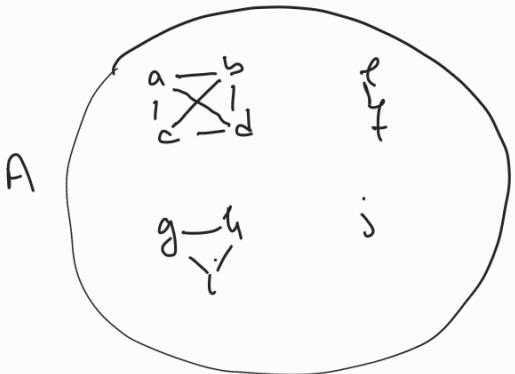
$$A/\equiv = \{[a] \mid a \in A\}.$$

Funția $p = p_{\equiv} : A \rightarrow A/\equiv$ dată prin $p(x) = [x]$ se numește proiecția canonica atașată relației de echivalență \equiv .

Observație 1.4.16. În definiția formală a mulțimii factor este posibil, și chiar foarte probabil, ca anumite elemente să apară de mai multe ori. Noi știm că într-o mulțime un element apare o singură dată, și presupunem automat că se elemină repetițiile. Totuși această presupunere necesită precauții suplimentare, căci o folosire greșită poate conduce la funcții care nu sunt bine definite și, prin urmare, la contradicții.

Propoziție 1.4.17. Fie (A, A, \equiv) o relație de echivalență pe o mulțime A , și $a, b \in A$. Avem:

- (a) $a \in [a]$, așadar $[a] \neq \emptyset$.



$$(A, \mathcal{R}, \equiv)$$

$$\equiv = \{ (a, a), (b, b), (a, c), (a, d), (b, a), (b, b),$$

$$(b, c), (b, d), (c, a), (c, b), (c, d), (d, a),$$

$$(d, b), (d, c), (d, d), (e, f), (f, e),$$

$$(f, f), (g, h), (g, i), (g, j), (h, i), (h, j), (i, j),$$

$$(j, i) \}$$

$$[a]_{\equiv} = \{ a, b, c, d \} = [b] = [c] = [d]$$

$$[e] = \{ e, f \} = [f], [g] = [i] = [j] = \{ g, h, i, j \}, [i] = \{ j \}.$$

$$A/\equiv = \{ [x] \mid x \in A \} = \{ [a], [b], [c], [d], [e], [f], [g], [h], [i], [j] \}$$

$$= \{ \{ a, b, c, d \}, \{ e, f \}, \{ g, h, i, j \}, \{ i \} \}$$

4.4.17. Dem (a) $a \equiv a$ dim reflex. $\Rightarrow a \in [a]$.

$$(b) \Rightarrow " \text{ Stim } [a] = [b] \Rightarrow b \in [a] \Rightarrow a \equiv b.$$

Dim (a) schinen $b \in [b]$

$$\left. \begin{array}{l} \text{" Stim } a \equiv b \stackrel{(a)}{\Rightarrow} b \equiv a \Rightarrow b \equiv x \Rightarrow x \in [b]. \text{ Dem } [a] \subseteq [b]. \\ \text{Re } x \in [a] \Rightarrow a \equiv x \end{array} \right\} \Rightarrow b \equiv x \Rightarrow x \in [b].$$

$$\text{fie } x \in [b] \Rightarrow b \equiv x \Rightarrow a \equiv x \Rightarrow x \in [a]. \text{ Dem } [b] \subseteq [a].$$

Also $[a] = [b]$.

$$(c) \Leftarrow ". \text{ Stim } [a] = [b] \Rightarrow [a] \cap [b] = \{ \underset{\alpha}{a} \} = [b] \neq \emptyset.$$

$$\Rightarrow " \text{ Stim } [a] \cap [b] \neq \emptyset \Rightarrow \exists c \in [a] \cap [b]$$

$$\Rightarrow \left\{ \begin{array}{l} c \in [a] \Rightarrow a \equiv c \\ c \in [b] \Rightarrow b \equiv c \stackrel{(a)}{\Rightarrow} c \equiv b \end{array} \right\} \stackrel{(T)}{\Rightarrow} a \equiv b \stackrel{(b)}{\Rightarrow} [a] = [b].$$

$$(d) [x] \subseteq A, \forall x \in A \Rightarrow \bigcup_{x \in A} [x] \subseteq A.$$

$$\text{Fie } a \in A \stackrel{(a)}{\Rightarrow} a \in [a] \Rightarrow a \in \bigcup_{x \in A} [x]. \text{ Dem } A \subseteq \bigcup_{x \in A} [x]$$

$$A = \bigcup_{x \in A} [x]. \quad \square$$

- (b) $[a] = [b]$ dacă $a \equiv b$.
- (c) $[a] \cap [b] \neq \emptyset$ dacă $[a] = [b]$.
- (d) $\bigcup_{x \in A} [x] = A$.

Demonstrație.

□

Definiție 1.4.18. Fie A o mulțime. O *partiție* a mulțimii A este o submulțime $\pi \subseteq \mathcal{P}(A)$ a mulțimii putere a lui A (adică o mulțime a cărei elemente sunt submulțimi ale lui A), aşa încât:

- (a) $\emptyset \notin \pi$.
- (b) Pentru $X, Y \in \pi$ dacă $X \cap Y \neq \emptyset$ atunci $X = Y$.
- (c) $\bigcup_{X \in \pi} X = A$.

Teoremă 1.4.19. Fie A o mulțime.

- (1) Dacă (A, A, \equiv) este o relație de echivalență pe A , atunci A/\equiv este o partiție a mulțimii A .
- (2) Dacă $\pi \subseteq \mathcal{P}(A)$ este o partiție a lui A , atunci (A, A, \equiv_π) este o relație de echivalență, unde pentru orice $a, b \in A$ avem

$$(*) \quad a \equiv_\pi b \text{ dacă există } X \in \pi \text{ aşa încât } a, b \in X.$$

- (3) Procedeele de la (1) și (2) descriu două funcții inverse una celeilalte între Mulțimea tuturor echivalențelor pe A și mulțimea tuturor partițiilor pe A .

Demonstrație.

□

Relații de ordine.

Definiție 1.4.20. Fie A o mulțime. O *relație de ordine* (sau pe scurt *ordine*) pe A este o preordine care este și antisimetrică, adică o relație omogenă pe A care este reflexivă, tranzitivă și antisimetrică. *Antisimetria:* $a \neq b \Rightarrow a = b$.

Adesea se notează o relație de ordine cu \leq și se spune că (A, \leq) este o mulțime ordonată. În acest caz notăm $x < y$ relația $x \leq y$ și $x \neq y$. (A, \leq)

Exemplu 1.4.21. Următoarele relații sunt de ordine:

- (1) Relația de egalitate pe o mulțime arbitrară.
- (2) Relația obișnuită de mai mic sau egal pe $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ sau \mathbb{R} .
- (3) Incluziunea pe o mulțime a căror elemente sunt mulțimi, de exemplu $(\mathcal{P}(A), \subseteq)$ este o mulțime ordonată, unde A este o mulțime oarecare.

De notat că în (\mathbb{R}, \leq) avem $x \leq y$ sau $y \leq x$ pentru orice $x, y \in \mathbb{R}$ (aceasta înseamnă (\mathbb{R}, \leq) este un *lanț* sau *sir*). În general acest lucru nu este adevărat pentru o mulțime ordonată oarecare, de exemplu $(\mathcal{P}(A), \subseteq)$ nu este un lanț când A are cel puțin două elemente, pentru că există $X, Y \in \mathcal{P}(A)$ astfel încât $X \not\subseteq Y$ și $Y \not\subseteq X$.

Definiție 1.4.22. Fie (A, \leq) o mulțime ordonată. Un element $a \in A$ se numește:

- (a) *minimal* dacă pentru orice $x \in A$ din $x \leq a$ rezultă $x = a$.
- (b) *maximal* dacă pentru orice $x \in A$ din $a \leq x$ rezultă $x = a$.
- (c) *cel mai mic element* a lui A dacă $a \leq x$ pentru orice $x \in A$.
- (d) *cel mai mare element* a lui A dacă $x \leq a$ pentru orice $x \in A$.

Observație 1.4.23. Fie (A, \leq) o mulțime ordonată. Se notează $\geq = \leq^{-1}$, adică $x \geq y$ dacă $y \leq x$. Este ușor de a verifica că \geq este de asemenea o relație de ordine (vezi Exercițiu 1.4.48). Se poate observa că $a \in A$ este minimal sau cel

$$x \leq y \Leftrightarrow y \geq x$$

1.4.19. Denum (n) rezultă din 1.4.17.

(2)(A). Fie $a \in A$. Dacă $A = \bigcup_{X \in \pi} X \Rightarrow \exists X \in \pi : a \in X \Rightarrow a \equiv_{\pi} a$.

(T). Fie $a, b, c \in A$ $a \equiv_{\pi} b, b \equiv_{\pi} c$.

$$a \equiv_{\pi} b \xrightarrow{(*)} \exists X \in \pi : a, b \in X \xrightarrow{(*)} b \in X \cap X' \Rightarrow X \cap X' \neq \emptyset$$
$$b \equiv_{\pi} c \xrightarrow{(*)} \exists X' \in \pi : b, c \in X'$$

$$\Rightarrow X = X' \Rightarrow a, c \in X \Rightarrow a \equiv_{\pi} c.$$

(S) Fie $a, b \in A$: $a \equiv_{\pi} b \Rightarrow \exists X \in \pi : a, b \in X \Rightarrow b \equiv_{\pi} a$.

Dacă (A, A, \equiv_{π}) este o rel. de echivalență.

(3)

$$\left\{ (A, A, \equiv) \mid \text{rel. de echiv.} \right\} \xrightarrow{(1)} \left\{ \pi \subseteq P(A) \mid \text{partitie} \right\} \xrightarrow{(2)} \left\{ (A, A, \equiv) \mid \text{rel. de echiv.} \right\}$$
$$(A, A, \equiv) \longmapsto A/\equiv \xrightarrow{(*)} (A, A, \equiv_{(A/\equiv)})$$

De asemenea: $(A, A, \equiv) = (A, A, \equiv_{(A/\equiv)})$. (3)

$$\left\{ \pi \subseteq P(A) \mid \pi \text{ partitie} \right\} \xrightarrow{(2)} \left\{ (A, A, \equiv) \mid \text{rel. de echiv.} \right\} \xrightarrow{(1)} \left\{ \pi \subseteq P(A) \mid \text{partitie} \right\}$$
$$\pi \longmapsto (A, A, \equiv_{\pi}) \longmapsto A/\equiv_{\pi}$$

De asemenea $\widehat{\pi} = A/\equiv_{\pi}$ (4)

Pr. (3):

$$(a, b) \in A \times A \text{ a.i. } a \equiv b \Rightarrow [a] = [b] \in A/\equiv$$

Dacă $\exists X = [a] = [b] \in A/\equiv$ a.i. $a, b \in X \Rightarrow a \equiv_{(A/\equiv)} b$.

Reciproc dacă $a \equiv_{(A/\equiv)} b \xrightarrow{(*)} \exists X \in A/\equiv \text{ a.i. } a, b \in X \Rightarrow [x] \mid x \in A$

$\exists c \in A : X = [c]$.

Dacă $a \in [c] \Rightarrow c \equiv a \xrightarrow{(*)} a \equiv c \xrightarrow{(T)} a \equiv b$, ceea ce arăta (3).

La (4) se procedă astfel:

$(P(A), \subseteq)$ este o multime ordonată = poset

$\forall X \in P(A) : X \subseteq X$

$\forall X, Y, Z \in P(A) : X \subseteq Y \wedge Y \subseteq Z \Rightarrow X \subseteq Z$

$\forall X, Y \in P(A) : X \subseteq Y \wedge Y \subseteq X \Rightarrow X = Y$.

$\exists X, Y \in P(A) \text{ a.i. } X \neq Y \wedge Y \neq X$.

$$A = \{a, b, c\}$$

$$\mathcal{P}(A) = \{ \emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\} \}$$

$(\mathcal{P}(A), \subseteq)$

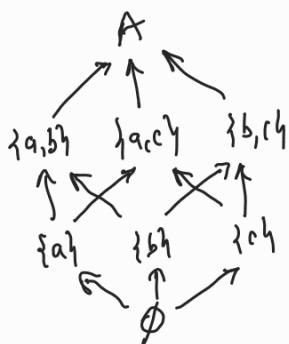
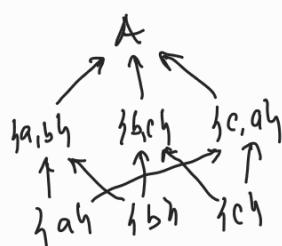


diagramma Hasse

$$\begin{aligned} & \{a\} \not\subseteq \{b\} \quad \left. \begin{array}{l} \{a\} \not\subseteq \{b\} \\ \{b\} \not\subseteq \{a\} \end{array} \right\} \text{ sunt incomparabile} \\ & \{a\} \subseteq \{a\} \quad \checkmark \quad \{a, b\} \subseteq \{a, b\} \end{aligned}$$

↓
3
2
1
0



$(\mathcal{P}(A) \setminus \{\emptyset\}, \subseteq)$

(\mathbb{N}, \leq)

Denum. 1. h.zu. (A, \leq) m.o.

Stim ca $\exists a \in A$ $a = u$ mai mic elem.

Fie $x \in A$ a.i. $x \leq a$ $\left. \begin{array}{l} a \text{ este ul mai mic} \Rightarrow a \leq x \end{array} \right\} \xrightarrow{\text{H1}} x = a$. Daca a e minimal.

Fie $a' \in A$ un elem. minimal $\left. \begin{array}{l} a' \text{ minimal} \\ \text{Cum } a \text{ e ul mai mic} \Rightarrow a \leq a' \end{array} \right\} \xrightarrow{\text{H1}} a = a'$. \otimes

Denum 1. h.zu Fie $a, a' \in A$ cumbe verifica prop. de a fi ul mai mic elem. $\xrightarrow{\text{H1}}$ a este unul elem. minimal

$a' \xrightarrow{\text{H1}} u$

$\Rightarrow a = a'$. \otimes .

mai mic element în (A, \leq) dacă a este maximal, respectiv cel mai mare element în (A, \geq) și invers. Această observație se poate extinde pentru toate noțiunile și afirmațiile referitoare la mulțimi ordonate și este așa numitul principiu al dualității.

Lemă 1.4.24. Fie (A, \leq) o mulțime ordonată. Dacă A are un cel mai mic (mare) element, atunci acest element este unicul element minimal (respectiv maximal).

Corolar 1.4.25. Cel mai mic (mare) element al unei mulțimi ordonate, dacă există, este unic.

Demonstrație.

Teoremă 1.4.26. Următoarele afirmații sunt echivalente pentru o mulțime ordonată (A, \leq) :

- (i) Orice submulțime nevidă a lui A are un element minimal (condiția minimalității).
- (ii) Orice lanț descrescător de elemente din A este finit, adică dacă $a_0 \geq a_1 \geq a_2 \dots$ cu $a_0, a_1, a_2, \dots \in A$, atunci există $n \in \mathbb{N}$ așa încât $a_n = a_{n+1} = \dots$ (condiția lanțurilor descrescătoare).
- (iii) Dacă $B \subseteq A$ are proprietățile
 - (a) B conține toate elementele minime ale lui A ;
 - (b) pentru $a \in A$ dacă $\{x \in A \mid x < a\} \subseteq B$ atunci $a \in B$;
 atunci $B = A$ (condiția inductivității).

Demonstrație. $\forall n \in \mathbb{N} : P(n)$.

Definiție 1.4.27. Fie (A, \leq) o mulțime ordonată și $X \subseteq A$. O margine inferioară (superioară) pentru X este un element $a \in A$ așa încât, $a \leq x$ (respectiv $x \leq a$) pentru orice $x \in X$. Se numește infimum (supremum) a lui X în A cea mai mare (mică) margine inferioară (respectiv superioară) a lui X , adică

$$\inf X = a \in A \text{ dacă } \begin{cases} a \leq x \text{ pentru orice } x \in X \\ \text{dacă } a' \in A \text{ așa încât } a' \leq x \text{ pentru orice } x \in X \text{ atunci } a' \leq a. \end{cases}$$

$$\sup X = a \in A \text{ dacă } \begin{cases} x \leq a \text{ pentru orice } x \in X \\ \text{dacă } a' \in A \text{ așa încât } x \leq a' \text{ pentru orice } x \in X \text{ atunci } a \leq a'. \end{cases}$$

Observație 1.4.28. Fie (A, \leq) o mulțime ordonată și $X \subseteq A$.

- (1) Dacă există $\inf X$ și $\sup X$ sunt unice.
- (2) Dacă există cel mai mic (mare) element a a lui X atunci $a = \inf X$ ($a = \sup X$).

Exemplu 1.4.29. (1) În (\mathbb{R}, \leq) avem $\inf(0, 1) = \inf[0, 1] = 0$, $\sup\{x \in \mathbb{R} \mid x^2 < 2\} = \sqrt{2}$, nu există $\inf \mathbb{Z}$ și nu există $\sup(0, \infty)$.

(2) În (\mathbb{Q}, \leq) nu există $\sup\{x \in \mathbb{Q} \mid x^2 < 2\}$.

(3) Într-o mulțime ordonată (A, \leq) există $\inf \emptyset$ ($\sup \emptyset$) exact atunci când A are cel mai mare (respectiv mic) element a , și avem $\inf \emptyset = a = \sup A$ ($\sup \emptyset = a = \inf A$).

Definiție 1.4.30. O latice este o mulțime ordonată (L, \leq) cu proprietatea că există $\inf\{x, y\}$ și $\sup\{x, y\}$ pentru orice două elemente $x, y \in L$. Notăm $x \vee y = \sup\{x, y\}$ și $x \wedge y = \inf\{x, y\}$. Laticea L se zice completă dacă există $\inf(X)$ și $\sup(X)$ pentru orice submulțime $X \in L$.

$$\{x \in \mathbb{R} \mid x^2 < 2\} = (-\sqrt{2}, \sqrt{2})$$

$$\{x \in \mathbb{Q} \mid x^2 < 2\} = (-\sqrt{2}, \sqrt{2}) \cap \mathbb{Q}.$$

Dem. 1-h.2b (i) \Rightarrow (iii). Presupunem condiția falsă că ei există

$B \subseteq A$ care verifică (a) și (b) dar $B \neq A \Rightarrow A \setminus B \neq \emptyset$

Din (ii) rezultă că $\exists a \in A \setminus B$ minimal în $A \setminus B$

Dacă a minimal în $A \Leftrightarrow a \notin B$ imposibil.

Dacă a nu e minimal în $A \Rightarrow \exists x \in A \mid x < a \wedge x \in B \neq \emptyset$.

Fie $x \in A \mid x < a$. Dacă presupunem $x \notin B$ atunci

$x \in A \setminus B$ ceea ce contrazice minimalitatea lui a în $A \setminus B$.

Intreanună că $x \in B$. Dacă $\exists x \in A \mid x < a \subseteq B$ este imposibil conform prop. (b) având $a \in B$, ceea ce este imposibil.

Având (iii) este aderată.

(iii) \Rightarrow (ii). $B = \{x \in A \mid a = a_0 \geq a_1 \geq \dots\} \Rightarrow \exists n \in \mathbb{N} : a_n = a_{n+1} = \dots$ $\forall x \in A$

Fie $a \in A$ un elem. minimal (există pt. că $A \subseteq A$, $A \neq \emptyset$).

Fie $a = a_0 \geq a_1 \geq a_2 \geq \dots \xrightarrow{\text{a minimal}} a = a_0 = a_1 = a_2 = \dots$ deci $a = u$.

Dacă $a \in B$ de unde rezultă că B satisfac cond. (a).

Fie $a \in A$ cu prop. $\exists x \in A \mid x < a \subseteq B$.

Considerăm un lant $a = a_0 \geq a_1 \geq a_2 \geq \dots$

Cat. I. $a = a_0 = a_1 = a_2 = \dots \Rightarrow$ lantul este staționar.

Cat. II $\Rightarrow k \geq 0$ a.i. $a_k > a_{k+1}$. Atunci $a = a_0 \geq a_k > a_{k+1}$

$\Rightarrow a_{k+1} \in \{x \in A \mid x < a\} \subseteq B \quad \left. \begin{array}{l} \Rightarrow \exists n \in \mathbb{N}, n \geq k+1 \text{ a.i.} \\ a_{k+1} \geq a_{k+2} \geq \dots \text{ lant descend.} \end{array} \right\}$

$a_n = a_{n+1} = \dots$
(este staționar).

Atunci:

$a = a_0 \geq a_1 \geq \dots \geq a_k \geq a_{k+1} \geq \dots \geq a_n \geq a_{n+1} \geq \dots$ este staționar.

($>$) ($=$) ($=$) \dots

Atunci $a \in B$, deci B satisfac (b)

Conform condiției (iii) care este ipoteză acum rezultă $B = A$,

deci rezultă (ii).

(ii) \Rightarrow (i). Fie $B \subseteq A$, $B \neq \emptyset \Rightarrow \exists a_0 \in B$

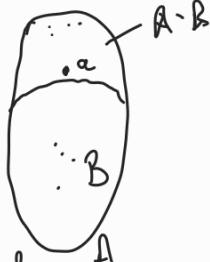
Dacă a_0 e minimal în B atunci stop; sau găsit ocază să continuăm.

Dacă a_0 nu e minimal atunci $\exists a_1 \in B : a_1 < a_0$.

Dacă a_1 e minimal în B atunci stop ...

Dacă nu $\Rightarrow \exists a_2 \in B : a_2 < a_1$.

S-a-n-d. Condiția (ii) care este ipoteză nu spune algoritmul de mai sus trebuie să se oprească doar $\exists n \in \mathbb{N} : a_n \in B$ este minimal în B . \square .



Teorema 1.4.31. Într-o lattice (L, \leq) sunt valabile proprietățile:

- (a) $x \vee (y \vee z) = (x \vee y) \vee z$ și $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (asociativitate).
- (b) $x \vee y = y \vee x$ și $x \wedge y = y \wedge x$ (comutativitate).
- (c) $x \vee (x \wedge y) = x = x \wedge (x \vee y)$ (absorbție).

Invers, dacă L este o mulțime împreună cu două operații $\vee, \wedge : L \times L \rightarrow L$ așa încât sunt valabile proprietățile (a), (b), (c) de mai sus, atunci L este o mulțime ordonată în raport cu relația $x \leq y$ dacă $x \wedge y = x$; mai mult (L, \leq) este chiar o lattice în care $\inf\{x, y\} = x \wedge y$ și $\sup\{x, y\} = x \vee y$, pentru orice $x, y \in L$.

Demonstrație. □

Propoziție 1.4.32. O mulțime ordonată (L, \leq) este o lattice completă dacă există $\inf X$ pentru orice $X \subseteq L$. există

Demonstrație. □

Exerciții la Relații.

Exercițiu 1.4.33. Fie $f : A \rightarrow B$ și $g : B \rightarrow C$ două funcții. Să se arate că funcția compusă $g \circ f$ este același lucru ca și relația compusă $g \circ f$.

Exercițiu 1.4.34. Fie $r = (A, B, R)$ o relație și notăm cu δ_A și δ_B relațiile de egalitate pe A respectiv B .

- (1) Să se arate că $r \circ \delta_A = r = \delta_B \circ r$, adică relația de egalitate acționează ca element neutru pentru compunerea relațiilor.
- (2) Să se arate că relația inversă $r^{-1} = (B, A, R^{-1})$ nu este în mod necesar inversă îr aport cu compunerea relațiilor, adică să se construiască un exemplu de relația r așa încât $r^{-1} \circ r \neq \delta_A$.

Exercițiu 1.4.35. Fie $r = (A, B, R)$ și $s = (B, C, S)$ două relații, unde A, B și C sunt mulțimi finite cu $|A| = m$, $|B| = n$ și $|C| = p$. Se ordenează elementele din A, B și C și se consideră matricile $M(r) \in \mathbb{M}_{m \times n}(\{0, 1\})$ și $M(s) \in \mathbb{M}_{n \times p}(\{0, 1\})$. Să se determine $M(r^{-1})$ și $M(s \circ r)$ în funcție de $M(r)$ și $M(s)$. Să se scrie un algoritm care citește $M(r)$ și $M(s)$ și calculează $M(r^{-1})$, $M(s \circ r)$.

Exercițiu 1.4.36. Să se arate că divizibilitatea pe \mathbb{Z} este o preordine care nu este nici simetrică și nici antisimetrică.

Exercițiu 1.4.37. Să se determine toate relațiile de echivalență care se pot defini pe $A = \{a, b, c\}$.

Exercițiu 1.4.38. Să se arate că următoarele relații sunt echivalențe și să se calculeze respectivele mulțimi factor:

- (1) $(\mathbb{C}, \mathbb{C}, \equiv)$ dată prin $x \equiv y$ dacă $|x| = |y|$.
- (2) $(\mathbb{C}^*, \mathbb{C}^*, \equiv)$ dată prin $x \equiv y$ dacă $\arg(x) = \arg(y)$.

Exercițiu 1.4.39. Să se arate că relația dată prin

$$(a, b) \sim (c, d) \text{ dacă } ad = cb$$

este o echivalență pe $\mathbb{Z} \times \mathbb{Z}^*$ și să se determine mulțimea factor

$$(\mathbb{Z} \times \mathbb{Z}^*)/\sim.$$

1.4.32. (L, \leq) m.t.
 (L, \leq) latiu kompletu $\Rightarrow \forall x \in L \quad f(\inf(x)) \in L$
 $f(\sup(x)) \in L$.

Reciproce presupunem \bar{w} pt. din multimea $X \subseteq L$ $f(\inf(X)) \in L$.
 Consideram $M = \{a \in L \mid \forall x \in X : x \leq a\} \subseteq L$ (multimea marginicelor superioare pt. X).

Conform ipotezei $\exists m = \inf(M) \in L$.

Te $x \in X \Rightarrow \underbrace{x \leq a}_{x \text{ marginime inf. pt. } M} \Rightarrow x \leq m$. (pt. că inf. este cea mai mare marginime inf. pt. M).

Aadar $m \in M$.
 Dar $\forall a \in M$ avem $m \leq a$ $\left(\begin{array}{l} \text{pt. că } m = \inf(M) \\ \text{cel mai mic element din } M \end{array} \right)$ $\Rightarrow m$ este

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b > 0, \gcd(a, b) = 1 \right\}$$

$$\frac{1}{2} = \frac{1}{2} = \frac{2}{4} \quad f\left(\frac{1}{2}\right) = \frac{1+0}{2^2} = \frac{2}{4} = \frac{1}{2} \quad \text{! ! ! } \quad f\left(\frac{2}{4}\right) = \frac{2+1}{4^2} = \frac{3}{16}$$

ALGEBRA PENTRU INFORMATICĂ

$$g\left(\frac{a}{b}\right) = \frac{2a + 3b}{b} = \frac{2a}{b} + \frac{3b}{b} = 2\left(\frac{a}{b}\right) + 3$$

$$g(x) = 2x + 3, \forall x \in \mathbb{Q}.$$

Exercițiu 1.4.40. Sunt bine definite următoarele funcții

NU $f : \mathbb{Q} \rightarrow \mathbb{Q}, f\left(\frac{a}{b}\right) = \frac{a+1}{b^2}$ pentru orice $a, b \in \mathbb{Z}, b \neq 0$,

DA $g : \mathbb{Q} \rightarrow \mathbb{Q}, g\left(\frac{a}{b}\right) = \frac{2a + 3b}{b}$ pentru orice $a, b \in \mathbb{Z}, b \neq 0$,

Nu $h : \mathbb{Z} \rightarrow \mathbb{Z}, h(x) = \frac{x}{2}$ pentru orice $x \in \mathbb{Z}$, $h\left(\frac{1}{2}\right) \notin \mathbb{Z}$

Nu $k : \mathbb{Z} \rightarrow \mathbb{Q}, k(x) = \frac{1}{x}$ pentru orice $x \in \mathbb{Z}$? $k(0) = \frac{1}{0}$ nu e definit

Exercițiu 1.4.41. Considerăm mulțimea $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ ca în Exercițiu 1.4.39.

Să se arate că $+, \cdot : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ sunt bine definite, unde:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ și } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

pentru orice $a, b, c, d \in \mathbb{Z}, b \neq 0, d \neq 0$.

Exercițiu 1.4.42. Fie $n \in \mathbb{N}, n \geq 2$. Să se arată că:

- (1) Congruența modulo n , și anume $(\mathbb{Z}, \mathbb{Z}, \equiv_n)$ dată de $x \equiv_n y$ (sau $x \equiv y \pmod{n}$) ddacă $n|(x - y)$ este o relație de echivalență.
- (2) Mulțimea factor corespunzătoare este mulțimea tuturor claselor de resturi modulo n : $\mathbb{Z}_n = \mathbb{Z}/\equiv_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$.
- (3) Operațiile următoare sunt bine definite:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n \text{ unde } [x]_n + [y]_n = [x + y]_n \text{ pentru orice } x, y \in \mathbb{Z} \text{ și}$$

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n \text{ unde } [x]_n \cdot [y]_n = [xy]_n \text{ pentru orice } x, y \in \mathbb{Z}.$$

Exercițiu 1.4.43. Fie A o mulțime și $r = (A, A, R)$ o preordine pe A . Să se arate că $r \cap r^{-1}$ unde $x(r \cap r^{-1})y$ ddacă xry și yrx este o relație de echivalență pe A și pe mulțimea factor $A/(r \cap r^{-1})$ relația r induce o ordine: $[x] \leq_r [y]$ ddacă xry . Să se studieze cazul particular când $A = \mathbb{Z}$ și preordinea este divizibilitatea (vezi Exercițiu 1.4.36).

Exercițiu 1.4.44. Fie $f : A \rightarrow B$ o funcție. Nucleul funcției f este o relație omogenă pe A notată cu $\ker f$ și definită prin $a(\ker f)b$ ddacă $f(a) = f(b)$. Să se arate că $\ker f$ este o relație de echivalență pe A . Invers, pentru orice relație de echivalență (A, A, \equiv) să se găsească o funcție $f : A \rightarrow B$, astfel încât \equiv este nucleul lui f .

Exercițiu 1.4.45. Să se găsească numărul tuturor relațiilor de echivalență care se pot defini pe o mulțime A cu n elemente.

Exercițiu 1.4.46. Să se determine toate relațiile de ordine care se pot defini pe $A = \{a, b, c\}$. În fiecare caz să se precizeze elementele minime, maxime, cel mai mic și/sau cel mai mare element.

Exercițiu 1.4.47. Să se construiască un exemplu de mulțime ordonată cu un singur element minimal, dar care nu are un cel mai mic element.

Exercițiu 1.4.48. Dacă (A, \leq) este o mulțime ordonată, atunci tot așa este și (A, \geq) .

Exercițiu 1.4.49. Orice latice finită este completă.

Exercițiu 1.4.50. Orice lanț este o latice. Este orice lanț o latice completă?

Exercițiu 1.4.51. Orice latice completă are cel mai mic și un cel mai mare element.

Exercițiu 1.4.52. $(\mathbb{N}, |)$ este o latice (aici cu $|$ se notează divizibilitatea). Este $(\mathbb{N}, |)$ completă?

Exercițiu 1.4.53. Arătați că (\mathbb{N}, \leq) este o latice care nu este completă. Explicați de ce acest exemplu nu contrazice Propoziția 1.4.32.

Exercițiu 1.4.54. $(\mathcal{P}(A), \subseteq)$ este o latice completă pentru orice mulțime A .

Exercițiu 1.4.55. Pe mulțimea \mathcal{L} a tuturor propozițiilor logice se definește relația $p \preceq q$ dacă $p \rightarrow q$ este o tautologie. Să se arate că \preceq este o preordine. Să se determine relația de echivalență asociată $\equiv = (\preceq \cap \preceq^{-1})$ (vezi Exercițiu 1.4.35) și mulțimea factor \mathcal{L}/\equiv (această mulțime este numită *algebra Lindenbaum-Tarski*). Să se arate că \mathcal{L}/\equiv este o latice completă.

2. GRUPURI, INELE, CORPURI

2.1. Grupuri.

Definiție 2.1.1. Un *grup* este o pereche (G, \cdot) care constă dintr-o mulțime G împreună cu o operație $\cdot : G \times G \rightarrow G$, astfel încât \cdot este asociativă, are un element neutru și fiecare element din G este inversabil în raport cu \cdot . În cazul în care \cdot este și comutativă atunci G se numește *abelian* sau *comutativ*.

Exemplu 2.1.2. Următoarele perechi sunt grupuri (abeliene):

- (a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.
- (b) (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) , (\mathbb{C}^*, \cdot) .
- (c) $(\mathbb{M}_{m \times n}(\mathbb{Z}), +)$, $(\mathbb{M}_{m \times n}(\mathbb{Q}), +)$, $(\mathbb{M}_{m \times n}(\mathbb{R}), +)$, $(\mathbb{M}_{m \times n}(\mathbb{C}), +)$

Exemplu 2.1.3. Următoarele perechi sunt monoizi dar nu grupuri:

- (a) $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , (\mathbb{Z}^*, \cdot)
- (b) (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) , (\mathbb{C}, \cdot) .
- (c) $(\mathbb{M}_{n \times n}(\mathbb{Z}), \cdot)$, $(\mathbb{M}_{n \times n}(\mathbb{Q}), \cdot)$, $(\mathbb{M}_{n \times n}(\mathbb{R}), \cdot)$, $(\mathbb{M}_{n \times n}(\mathbb{C}), \cdot)$

Nu există asa ceea ce
 $(\mathbb{M}_{n \times n}(\mathbb{R}), \cdot)$ nu este un grup

Observație 2.1.4. Cel mai adesea operația unui grup oarecare este notată multiplikativ, adică (G, \cdot) . În acest caz elementul neutru este notat 1 și pentru $x \in G$ notăm cu x^{-1} elementul invers. Pentru un grup abelian însă operația este adesea notată aditiv, adică $(G, +)$. În acest caz, elementul neutru se notează 0, iar pentru $x \in G$ notăm $-x$ elementul opus.

Propoziție 2.1.5. Fie (M, \cdot) un monoid și considerăm

$$\begin{aligned} M^\times &= \{x \in M \mid x \text{ este inversabil în } M\} \\ &= \{x \in M \mid \exists x^{-1} \in M \text{ astfel încât } xx^{-1} = 1 = x^{-1}x\} \subseteq M \end{aligned}$$

Să se arate că operația \cdot induce pe M^\times , iar M^\times împreună cu operația indușă formează un grup.

Demonstrație.

□

Corolar 2.1.6. Următoarele construcții conduc la grupuri neabeliene:

- (1) Dacă A este o mulțime, atunci $S(A) = \{\sigma : A \rightarrow A \mid \sigma \text{ este bijectivă}\}$ este un grup împreună cu compunerea funcțiilor; acest grup nu este abelian pentru $|A| \geq 3$. Grupul $S(A)$ se numește grupul simetric al mulțimii A .

2.1.5. Dem (M, \cdot) monoid

$$M^x = \{x \in M \mid \exists x^{-1} \in M : x \cdot x^{-1} = 1 = x^{-1} \cdot x\}.$$

• Adunarea cu M^x este parțial stabilită: ✓

$$x, y \in M^x \Rightarrow \exists x^{-1}, \exists y^{-1}$$

$$\left. \begin{array}{l} x \cdot y \in M \\ (xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1 \\ (y^{-1}x^{-1})(x \cdot y) = y^{-1}(x^{-1}x)y = y^{-1} \cdot 1 \cdot y = y^{-1} \cdot y = 1 \end{array} \right\} \Rightarrow$$

$$\exists (x \cdot y)^{-1} = y^{-1} \cdot x^{-1} \in M \Rightarrow x \cdot y \in M^x.$$

$$\bullet 1 \in M^x \text{ pt. c}\bar{\text{o}} \quad 1^{-1} = 1 \in M.$$

• asociativitatea înmulțirii din M^x nu mai trebuie verificată

deoarece "restenșează" din M .

$$\bullet x \in M^x \Rightarrow \exists x^{-1} \in M : \dots \Rightarrow (x^{-1})^{-1} = x \in M \Rightarrow x^{-1} \in M^x.$$

Deci (M^x, \cdot) este grup.

$$2.1.6. (1) M = A^A = \{ f: A \rightarrow A \mid f \text{ este funcție} \}$$

(A^A, \circ) monoid. - compativitatea este asociativă
- $1_A: A \rightarrow A$ este elem. neutru

$$(A^A)^x = \{ \sigma \in A^A \mid \sigma \text{ inversabil} \} = \{ \sigma: A \rightarrow A \mid \sigma \text{ bij} \} = S(A)$$

$(S(A), \circ)$ este grup.

$$S_n = S(\{1, 2, \dots, n\}).$$

$$\sigma = \begin{pmatrix} a & b & c & \dots & x & \dots \\ \downarrow & \downarrow & \downarrow & \dots & \downarrow & \dots \\ b & c & a & \dots & x & \dots \end{pmatrix} \quad T = \begin{pmatrix} a & b & c & \dots & x & \dots \\ a & c & b & \dots & x & \dots \end{pmatrix}$$

$$\sigma \cdot T = \begin{pmatrix} a & b & c & \dots & x & \dots \\ b & c & a & \dots & x & \dots \end{pmatrix} \neq T \cdot \sigma = \begin{pmatrix} a & b & c & \dots & x & \dots \\ c & a & b & \dots & x & \dots \end{pmatrix}.$$

$$(2) (M, \cdot) = (M_{n \times n}(K), \cdot) \text{ monoid}$$

- înmulțirea este asociativă. În elev. vîntură.

$$\begin{aligned} M_{n \times n}(K)^x &= \{ A \in M_{n \times n}(K) \mid \exists A^{-1} \text{ astfel încât } A \cdot A^{-1} = I_n = A \cdot A^{-1} \} \\ &= \{ A \in M_{n \times n}(K) \mid \det A \neq 0 \} = GL_n(K) \end{aligned}$$

grup.

Termenul verificării că $GL_n(K)$ este necomutativ nu se poate.

Obs. (R, \cdot) , (Q, \cdot) , (C, \cdot) monoidi comunități.

$$R^x = R^* = R \setminus \{0\}, \quad Q^x = Q^*, \quad C^x = C^*$$

(2) Fie $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ și $n \in \mathbb{N}^*$. Multimea $GL_n(K) = \{A \in M_{n \times n}(K) \mid \det(A) \neq 0\}$ împreună cu înmulțirea matricilor formează un grup, care nu este comutativ pentru $n \geq 2$. Grupul $GL_n(K)$ se numește grupul linear general de rang n peste K .

Demonstrație.

□

Subgrupuri.

operație

Definiție 2.1.7. Fie (G, \cdot) un grup. Un subgrup a lui G este o submulțime $H \subseteq G$, astfel încât operația pe G induce o opereție bine definită pe H (i. e. $x, y \in H \Rightarrow xy \in H$; se spune de asemenea că H este o parte stabilă a lui G), și H împreună cu operația indușă formează un grup. Se scrie $H \leq G$.

Exemplu 2.1.8. (1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ (cu adunarea). $\cdot : H \times H \rightarrow H$

(2) $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$ (cu înmulțirea).

(3) $\mathbb{R}_+^* \leq \mathbb{R}^*$, unde $\mathbb{R}_+^* = (0, \infty)$.

(4) Orice grup G are aşa numitele subgrupuri triviale i. e. $\{1\}$ și G .

Propoziție 2.1.9 (Teorema de caracterizare a subgrupurilor). Fie (G, \cdot) un grup și fie $H \subseteq G$ o submulțime. Următoarele afirmații sunt echivalente:

- (i) $H \leq G$.
- (ii) (a) $1 \in H$.
 - (b) $x, y \in H \Rightarrow xy \in H$.
 - (c) $x \in H \Rightarrow x^{-1} \in H$.
- (iii) (a) $1 \in H$.
 - (b) $x, y \in H \Rightarrow xy^{-1} \in H$.

Demonstrație.

□

Propoziție 2.1.10. Fie (G, \cdot) un grup. Dacă $H_i \leq G$, cu $i \in I$, atunci $\bigcap_{i \in I} H_i \leq G$.

Demonstrație.

□

Observație 2.1.11. Reuniunea a două sau mai multe subgrupuri nu este cu nevoie subgrup (Übung 2.1.58).

Definiție 2.1.12. Fie (G, \cdot) un grup și $X \subseteq G$ o submulțime a lui G . Subgrupul generat de X este definit prin

$$\langle X \rangle = \bigcap \{H \leq G \mid X \subseteq H\} = \bigcap_{X \subseteq H \leq G} H$$

Dacă $X = \{x_1, x_2, \dots, x_n\}$ este o mulțime finită atunci scriem $\langle x_1, x_2, \dots, x_n \rangle$ în loc de $\langle \{x_1, x_2, \dots, x_n\} \rangle$. $\langle \{x_1, x_2, \dots, x_n\} \rangle$ $\langle x_1, x_2, \dots, x_n \rangle$

Lemă 2.1.13. Fie (G, \cdot) un grup și $X \subseteq G$ o submulțime a lui G . Atunci:

- (a) $\langle X \rangle \leq G$.
- (b) $X \subseteq \langle X \rangle$ și $X = \langle X \rangle$ dacă $X \leq G$.
- (c) $\langle X \rangle$ este cel mai mic subgrup a lui G care conține submulțimea X , adică

$$H = \langle X \rangle \text{ dacă } \begin{cases} H \leq G \\ X \subseteq H \\ \text{dacă } K \leq G \text{ astfel încât } X \subseteq K \text{ atunci } H \leq K \end{cases}$$

- (d) ~~Cit~~ $X \subseteq Y \subseteq G$ ~~se~~ ~~gilt~~ ~~auch~~ $\langle X \rangle \leq \langle Y \rangle \leq G$.

Dacă atunci

$$\begin{matrix} \uparrow \\ H \subseteq K \end{matrix}$$

$$\text{Sub}(G) = \{H \subseteq G \mid H \leq G\}$$

Denumirea (i) \Rightarrow (ii) pt. că asociativitatea este o prop. evidentă
 Mai precis dacă $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, și $x, y, z \in G$, iar $H \subseteq G$ astfel
 că atât mai mult $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, și $x, y, z \in H$.

(ii) \Rightarrow (iii). $1 \in H$ din ipoteză

$$\text{Fie } x, y \in H \xrightarrow{\text{def}} x, y^{-1} \in H \xrightarrow{\text{(iiib)}} x \cdot y^{-1} \in H \quad \checkmark$$

(iii) \Rightarrow (ii). $1 \in H$ din ipoteză

$$\text{Fie } x \in H; \text{ stim } 1, x \in H \xrightarrow{\text{(iiib)}} 1 \cdot x \in H \Rightarrow x \in H.$$

$$\text{Fie } x, y \in H; \text{ stim } x, y^{-1} \in H \xrightarrow{\text{(iiib)}} x \cdot (y^{-1})^{-1} \in H \Rightarrow x \cdot y \in H. \quad \square.$$

Oblig. (i) $(\mathbb{Z}_{\geq 1}, +)$ Nu există asoc uval! (! ! !)

Dacă $x, y, z \in \mathbb{Z}_{\geq 1}$: $(x+y) + z = x + (y+z)$ asociativitate.

(ii) (\mathbb{N}^*, \cdot) dar $0 \notin \mathbb{N}^*$ (\mathbb{N}, \cdot) punct stabil
 punct stabilă \Rightarrow operatii binare definite $0 \in \mathbb{N}$
 $\mathbb{N} \neq \mathbb{Z}$.

2.1.10. Denumire. Notă $H = \bigcap_{i \in I} H_i = \{x \in G \mid x \in H_i, \forall i \in I\}$.

$$\left. \begin{array}{l} 1 \in G \\ H_i \leq G \end{array} \right\} \Rightarrow 1 \in H_i, \forall i \in I \Rightarrow 1 \in H. \quad (*)$$

$$\text{Fie } x, y \in H \Rightarrow x, y \in H_i, \forall i \in I \xrightarrow[\text{pt. } H_i \leq G]{\text{(iiib)}} x \cdot y^{-1} \in H_i, \forall i \in I \Rightarrow x \cdot y^{-1} \in H \quad (**).$$

$$\text{Din } (*) \text{ și } (**), \xrightarrow[\text{pt. } H]{\text{(iiib)}} H \leq G.$$

Exemplu. (\mathbb{C}^*, \cdot)

$$\begin{aligned} z \in \mathbb{C}^* & \quad \langle z \rangle = \{z, z^2, z^3, z^4, \dots, z^n, \dots, 1 = z^0, z^{-1} = \frac{1}{z}, z^{-2}, \dots\} \\ & = \{z^n \mid n \in \mathbb{Z}\} \leq \mathbb{C}^* \end{aligned}$$

$$i \in \mathbb{C} \quad \langle i \rangle = \{i, i^2 = -1, i^3 = -i, i^4 = 1\} \leq \mathbb{C}^*$$

Denumirea. Notă

$$H = \{x_1 x_2 \dots x_n \mid n \in \mathbb{N}, x_1, x_2, \dots, x_n \in X \cup X^{-1}\}$$

Astăzi că $H \leq G$ (1) OR.

- $1 \in H$ pt. că pt. $n=0$ produsul fără factori este $1 \in H$.
- Fie $x, y \in H \Rightarrow x = x_1 x_2 \dots x_n, y = y_1 y_2 \dots y_m, x_1, \dots, x_n \in X \cup X^{-1}$
 $y_1, \dots, y_m \in X \cup X^{-1}$

Astăzi $x \cdot y = x_1 x_2 \dots x_n y_1 y_2 \dots y_m \in H$

• Fie $x \in H \Rightarrow x = x_1 x_2 \dots x_n$, $x_1, x_2, \dots, x_n \in X \cup X^{-1}$. Atunci

$$x' = (x_1 x_2 \dots x_n)' = x_n' \dots x_2' x_1' \in H$$

Astăzi $X \subseteq H$ (2) ✓

Fie $x \in X$; not. $x_1 = x \in X$, pt $n=1$ obtin $x = x_1 \in H$. (produs cu un singur factor)

Astăzi că $K \leq G$, $X \subseteq K \Rightarrow H \subseteq K$. (3) ✓

Fie $K \leq G$ cu prop. $X \subseteq K \xrightarrow{K \leq G} X^{-1} \subseteq K \xrightarrow{K \leq G} x, x_2, \dots, x_n \in K$

Fie $x \in H \Rightarrow x = x_1 x_2 \dots x_n$, $x_1, x_2, \dots, x_n \in X \cup X^{-1} \xrightarrow{\text{p-alea.}} \downarrow x \in K$.

Deri $H \subseteq K$.

Din (1), (2), (3) $\Rightarrow H = \langle X \rangle$.

Dem. (a) $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \xrightarrow{\text{f}(1) \neq 1} 1 = f(1)$.

2.1.19. Dacă $f(1) \in H \Rightarrow f(1)^{-1} \in H$

(b) Fie $x \in G \Rightarrow \exists x' \in G: x \cdot x' = 1 = x' \cdot x \Rightarrow$

$$f(x \cdot x') = f(1) = f(x' \cdot x) \xrightarrow[\text{morf.}]{\text{f}}$$

$$\left. \begin{array}{l} f(x) \cdot f(x') = 1 = f(x') \cdot f(x) \\ f(x), f(x') \in H \end{array} \right\} \Rightarrow f(x)^{-1} = f(x'). \quad \square$$

Dacă 2.1.20. $G \xrightarrow{f} H$ f, g morfisme de gr. $\xrightarrow{\text{f}} \xrightarrow{\text{g}}$ $g \circ f$ morf.

Fie $x, y \in G$
 $(g \circ f)(x \cdot y) = g(f(x \cdot y)) \xrightarrow[\text{morf.}]{\text{f}} g(f(x) \cdot f(y)) \xrightarrow[\text{morf.}]{\text{g}} g(f(x)) \cdot g(f(y))$
 $(g \circ f)(x) \cdot (g \circ f)(y)$.

De acum stim că f este izomorfism adică (\forall) bij.

$\Rightarrow \exists f^{-1}: H \rightarrow G$ n.i. $f \circ f^{-1} = 1_H$, $f^{-1} \circ f = 1_G$. Mai mult f^{-1} este bij.

Fie $x', y' \in H$; not. $x = f(x') \in G$, $y = f(y') \in G$. Este clar

$$f(x) = x', f(y) = y'$$

$$f^{-1}(x' \cdot y') = f^{-1}(f(x) \cdot f(y)) \xrightarrow[\text{morf.}]{\text{f}} f^{-1}(f(x) \cdot f(y)) = 1_G(x \cdot y) = x \cdot y = f^{-1}(x') \cdot f^{-1}(y')$$

Deri f^{-1} este morf. \Rightarrow izomorfism. \square .

Demonstrație.

□

Propoziție 2.1.14. Fie (G, \cdot) un grup și $X \subseteq G$ o submulțime a lui G . Atunci:

$$\langle X \rangle = \{x_1 x_2 \dots x_n \mid n \in \mathbb{N}, x_1, x_2, \dots, x_n \in X \cup X^{-1}\},$$

unde $X^{-1} = \{x^{-1} \mid x \in X\}$. Această înseamnă că grupul generat de X conține toate elementele ~~din~~ G care se pot scrie ca un produs finit de elemente din $X \cup X^{-1}$. d.m.

Demonstrație.

□

Observație 2.1.15. Fie (G, \cdot) un grup și $x \in G$. Pentru orice $n \in \mathbb{Z}$ se definește:

$$x^n = \begin{cases} xx \dots x \text{ (n ori) dacă } n > 0 \\ 1 \text{ dacă } n = 0 \\ x^{-1} x^{-1} \dots x^{-1} \text{ (-n ori) dacă } n < 0 \end{cases}$$

Dacă operația este scrisă aditiv, adică $(G, +)$ atunci scriem

$$nx = \begin{cases} x + x + \dots + x \text{ (n ori) dacă } n > 0 \\ 0 \text{ dacă } n = 0 \\ (-x) + (-x) + \dots + (-x) \text{ (-n ori) dacă } n < 0 \end{cases}$$

Corolar 2.1.16. Fie (G, \cdot) un grup.

|n|

(a) Pentru $x \in G$ avem $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

 $x = \{x\}$

(b) Pentru $x, y \in G$ cu $xy = yx$ avem $\langle x, y \rangle = \{x^n y^m \mid n, m \in \mathbb{Z}\}$.

 $x = \{x, xy\}$

Homomorfisme de grupuri. = morfisme de grupuri

Definiție 2.1.17. Fie (G, \cdot) și (H, \cdot) două grupuri. Se numește *homomorfism (de grupuri)* între G și H o funcție $f : G \rightarrow H$ cu proprietatea $f(xy) = f(x)f(y)$ pentru orice $x, y \in G$. Se numește *izomorfism (de grupuri)* un homomorfism care este bijectiv. În acest caz grupurile se zic izomorfe și notăm $G \cong H$.

Exemplu 2.1.18. Pentru orice două grupuri G și H funcțiile 1_G și $e : G \rightarrow H$, $e(x) = 1$ sunt un izomorfism respectiv un homomorfism de grupuri. Dacă $G \leq H$ atunci funcția de incluziune $i : G \rightarrow H$ este un homomorfism. $1_G : G \rightarrow G$

Lemă 2.1.19. Dacă $f : G \rightarrow H$ este un homomorfism de grupuri atunci:

- (a) $f(1) = 1$.
- (b) $f(x^{-1}) = f(x)^{-1}$.

Demonstrație.

□

Lemă 2.1.20. Componerea a două homomorfisme este de asemenea un homomorfism. Funcția inversă a unui izomorfism de grupuri este de asemenea un izomorfism.

Demonstrație.

□

Definiție 2.1.21. Fie $f : G \rightarrow H$ un homomorfism. Numim *nucleul* respectiv *imaginăria* lui f mulțimile

$$\text{Ker } f = \{x \in G \mid f(x) = 1\} \text{ și } \text{Im } f = \{f(x) \mid x \in G\}.$$

Propoziție 2.1.22. Dacă $f : G \rightarrow H$ este un homomorfism, atunci:

Bew. 2.1.22. $f: G \rightarrow H$ inj.

(a) $\forall g \ni f(1) = 1 \in H \Rightarrow 1 \in \text{Ker } f$.

$\forall x, y \in \text{Ker } f \Rightarrow f(x) = 1 = f(y)$

$f(x \cdot y) = f(x) \cdot f(y) = 1 \cdot 1 = 1 \in H \Rightarrow xy \in \text{Ker } f$.

$\forall x \in \text{Ker } f \Rightarrow f(x) = 1$

$f(x^{-1}) = f(x)^{-1} = 1^{-1} = 1 \Rightarrow x^{-1} \in \text{Ker } f$

Deci $\text{Ker } f \leq G$.

(b) $\forall 1 = f(1) \in \text{Im } f$

$\forall x', y' \in \text{Im } f \Rightarrow \exists x, y \in G : f(x) = x', f(y) = y'$

$x' \cdot y' = f(x) \cdot f(y) \stackrel{\text{inj}}{\nmid} f(x \cdot y) \in \text{Im } f$.

$\forall x' \in \text{Im } f \Rightarrow \exists x \in G : f(x) = x'$

$(x')^{-1} = f(x)^{-1} = f\left(\frac{x}{1}\right) \in \text{Im } f$.

Deci $\text{Im } f \leq H$.

(c) " \Rightarrow " $\forall x \in \text{Ker } f \Rightarrow f(x) = 1 = f(1) \xrightarrow[\text{H}]{f \text{ inj}} x = 1$

Deci $\text{Ker } f = \{1\}$.

" \Leftarrow " Fie $x, y \in G$ u.i. $f(x) = f(y) \mid f(y)^{-1} \Rightarrow f(x) f(y)^{-1} = 1$
 $\exists f(y)^{-1} \in H$

$\Rightarrow f(x) f(y)^{-1} = 1 \Rightarrow f(x \cdot y^{-1}) = 1 \Rightarrow x \cdot y^{-1} \in \text{Ker } f$ $\left\{ \begin{array}{l} \text{Din ipotru } \text{Ker } f = \{1\} \\ \Rightarrow x \cdot y^{-1} = 1 \end{array} \right. \Rightarrow x = y$

Deci f este inj.

- (a) $\text{Ker } f \leq G$.
 (b) $\text{Im } f \leq H$.
 (c) f este injectiv dacă $\text{Ker } f = \{1\}$.
 (d) f este surjectiv dacă $\text{Im } f = H$ (*reformulare unor cunoscute pt. surjectivitate*)
- Demonstrație.* □

Grupuri ciclice și ordinul unui element.

Definiție 2.1.23. Un grup ciclic este un grup care este generat de un singur element al său.

Definiție 2.1.24. Fie (G, \cdot) un grup și $x \in G$. Se spune că x este de ordin finit dacă există $n \in \mathbb{N}^*$ astfel încât $x^n = 1$. În acest caz se numește ordinul lui x cel mai mic număr natural $n \in \mathbb{N}^*$ cu această proprietate; scriem $n = \text{ord}(x)$. Elementul x este de ordin infinit dacă el nu este de ordin finit, caz în care scriem $\text{ord}(x) = \infty$.

- Exemplu 2.1.25.** (1) În orice grup (G, \cdot) există un singur element de ordin 1, anume elementul neutru $\text{ord}(1) = 1$.
 (2) În $(\mathbb{Z}, +)$ avem $\text{ord}(2) = \text{ord}(3) = \infty$ și chiar $\text{ord}(x) = \infty$ pentru orice $x \neq 0$.
 (3) În (\mathbb{R}^*, \cdot) avem $\text{ord}(-1) = 2$ și $\text{ord}(2) = \text{ord}(-2) = \text{ord}(3) = \infty$; mai mult, $\text{ord}(x) = \infty$ pentru orice $x \in \mathbb{R} \setminus \{1, -1\}$.
 (4) În (\mathbb{C}^*, \cdot) avem $\text{ord}(i) = \text{ord}(-i) = 4$, $\text{ord}(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}) = 3$, $\text{ord}(2) = \text{ord}(-2) = \infty$; mai mult $\text{ord}(x) = \infty$ pentru orice $x \in \mathbb{C}^*$ cu $|x| \neq 1$.

Propoziție 2.1.26. Fie (G, \cdot) un grup, $x \in G$ și $n \in \mathbb{N}^*$. Avem:

$$\text{ord}(x) = n \text{ dacă } \begin{cases} x^n = 1 \\ \text{dacă } m \in \mathbb{Z} \text{ are proprietatea } x^m = 1 \text{ atunci } n|m \end{cases} .$$

Demonstrație. □

Propoziție 2.1.27. Fie (G, \cdot) un grup. Pentru orice $x \in G$ avem $\text{ord}(x) = |\langle x \rangle|$.

Demonstrație. □

(a) G ciclic $|G| > \infty \Rightarrow G \cong (\mathbb{Z}, +)$
(b) G ciclic $|G| = n \Rightarrow G \cong (\mathbb{Z}_n, +)$.

Acțiuni ale grupurilor pe mulțimi.

Definiție 2.1.28. Fie A o mulțime și (G, \cdot) un grup. Se numește *acțiune (la stânga)* a lui G pe A o funcție $\alpha : G \times A \rightarrow A$ cu proprietățile:

- (1) $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ pentru orice $g, h \in G$ și orice $x \in A$.
 (2) $\alpha(1, x) = x$ pentru orice $x \in A$.

Observație 2.1.29. Adesea funcția $\alpha : G \times A \rightarrow A$ este văzută ca o operație (înmulțire) externă, în sensul că operanții nu sunt luați din aceeași mulțime, și este notată prin $gx = \alpha(g, x)$. În acest caz, egalitățile (1) și (2) din definiția 2.1.28 devin:

$$g(hx) = (gh)x, \text{ respectiv } 1x = x, \text{ pentru orice } g, h \in G \text{ și orice } x \in A.$$

Teoremă 2.1.30. Fie A o mulțime și (G, \cdot) un grup.

- (a) Dacă $G \times A \rightarrow A$, $(g, x) \mapsto gx$ este o acțiune a lui G pe A , atunci $\phi : G \rightarrow S(A)$, $\phi(g) : A \rightarrow A$, $\phi(g) : x \mapsto gx$ este un homomorfism de grupuri.
 (b) Dacă $\phi : G \rightarrow S(A)$ este un homomorfism de grupuri, atunci $G \times A \rightarrow A$, $(g, x) \mapsto \phi(g)(x)$ este o acțiune a lui G pe A .

Denum. 2.1.26 (G, \cdot) grup $x \in G$, $n \in \mathbb{N}^*$

\Rightarrow "Stim $\text{ord}(x) = n$, Atunci $x^n = 1$

Tez $m \in \mathbb{Z}$ a.i. $x^m = 1$

Teorema importantă ca rest: $m = n \cdot q + r$, $q, r \in \mathbb{Z}$, $r \in \{0, 1, \dots, n-1\}$

$$x^m = x^{n \cdot q + r} = x^n \cdot x^r = x^n \cdot (x^n)^{-1} = 1 \cdot 1^{-1} = 1 \quad \left. \begin{array}{l} r \in \mathbb{N}, \quad r < n \\ n = \text{ul mai mic în } \mathbb{N}^* \text{ cu prop. } x^n = 1 \end{array} \right\} \Rightarrow r = 0.$$

Dacă $m = n \cdot q \Rightarrow m | m$.

\Leftarrow . $x^n = 1, n \in \mathbb{N}^*$ \Rightarrow x de ordin finit \Rightarrow nf $m = \text{ord}(x) \in \mathbb{N}^* \subseteq \mathbb{Z}$

Atunci $x^m = 1$ iar ipoteze ne spune că $n | m$ $\left. \begin{array}{l} n, m \in \mathbb{N}^* \\ n \leq m \end{array} \right\} \Rightarrow n \leq m$

P.e de altă parte din def. ordinului m este cel mai mic în \mathbb{N}^*

în prop. $x^m = 1$ deci $m \leq n$.

Prin urmare $n = m = \text{ord}(x)$. \square .

Denum. 2.1.27 (G, \cdot) grup $x \in G$.

$$(a) \langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}.$$

Cat I. $\text{ord}(x) = \infty$. Vom arăta că $x^k = x^t \Rightarrow k = t$.

$$\left. \begin{array}{l} x^k = x^t \quad | \cdot x^{-t} \Rightarrow x^{k-t} = 1 \Rightarrow x^{|k-t|} = 1 \\ |k-t| \in \mathbb{N} \\ \text{ord}(x) = \infty \end{array} \right\} \Rightarrow |k-t| = 0$$

$$\exists x^{-t} \in G$$

$$\Rightarrow k-t=0 \Rightarrow k=t.$$

$$|\langle x \rangle| = |\{x^m \mid m \in \mathbb{Z}\}| = |\mathbb{Z}| = \infty = \text{ord}(x).$$

Cat II $\text{ord}(x) = n$, $n \in \mathbb{N}^*$. Vom arăta că

$$\langle x \rangle = \{x^0, x^1, x^2, \dots, x^{n-1}\}$$

$\nexists x^m \in \langle x \rangle \quad (m \in \mathbb{Z})$

$$m = n \cdot q + r, \quad q, r \in \mathbb{Z} \quad r \in \{0, 1, \dots, n-1\}$$

$$\left. \begin{array}{l} x^m = x^{n \cdot q + r} = (x^n)^q \cdot x^r = 1^q \cdot x^r = 1 \cdot x^r = x^r \in \{1, x, x^2, \dots, x^{n-1}\} \\ k, t \in \{0, 1, \dots, n-1\} \quad x^k = x^t \quad | \cdot x^{-t} \Rightarrow x^{k-t} = 1 \Rightarrow n | (k-t) \end{array} \right\} \Rightarrow$$

$$\text{Dacă } k-t \in \{-n+1, -n+2, \dots, -1, 0, 1, \dots, n-1\}$$

$$k-t=0 \Rightarrow k=t.$$

$$\text{Deci } |\langle x \rangle| = |\underbrace{\{1, x, x^2, \dots, x^{n-1}\}}_{\text{două liste distincte}}| = n = \text{ord}(x).$$

(a) G ciclic $\Rightarrow \exists x \in G : G = \langle x \rangle \left\{ \begin{array}{l} (\alpha) \\ |G| = \infty \end{array} \right. \Rightarrow |\langle x \rangle| = \infty \Rightarrow$
 $\Rightarrow \text{ord}(x) = \infty$ (suntur := cauză I de dimensiune).

Definim $f: \mathbb{Z} \rightarrow G$, $f(m) = x^m$

Așa arătă în ceea ce că f este inj. $\left\{ \begin{array}{l} \Leftrightarrow f \text{ bij} \\ f \text{ este surj. pt. că } G = \langle x \rangle = \{x^m \mid m \in \mathbb{Z}\} \end{array} \right.$

$f(k+t) = x^{k+t} = x^k \cdot x^t = f(k) \cdot f(t)$ morf. de grupuri.

$$(G, \cdot) \cong (\mathbb{Z}, +).$$

Obl $\mathbb{Z} = \{n \cdot 1 \mid n \in \mathbb{Z}\} = \langle 1 \rangle$; sigur $\langle -1 \rangle = \mathbb{Z}$ ✓

(b) (G, \cdot) ciclic $G = \langle x \rangle$, $x \in G$ $\left\{ \begin{array}{l} |\langle x \rangle| = n \stackrel{(\alpha)}{\Leftrightarrow} \\ |G| = n, n \in \mathbb{N}^* \end{array} \right. \Rightarrow \text{ord}(x) = n$.

Suntur în ceea ce II.a.

$f: \mathbb{Z}_n \rightarrow G$, $f(\hat{k}) = x^k$, $\forall k \in \mathbb{Z}$

Bine definit $\hat{k} = \hat{m} \Leftrightarrow n \mid (k-m) \Rightarrow x^{k-m} = 1 \Rightarrow$
 $x^k \cdot x^{-m} = 1 \quad | \cdot x^m \Rightarrow x^k = x^m$. OK.

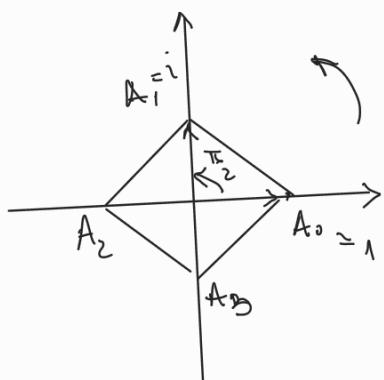
f este inj. cum au arătat în II.a)

f este surj. pt. că $G = \langle x \rangle = \{1, x, x^2, \dots, x^{n-1}\}$.

f morf. de grupuri $f(\hat{k} + \hat{t}) = f(\hat{k+t}) = x^{k+t} = x^k \cdot x^t = f(\hat{k}) \cdot f(\hat{t})$.

Deci $(\mathbb{Z}_n, +) \cong (G, \cdot)$. \square .

(\mathbb{C}^*, \cdot)



ϕ = rotație în sens trigonometric în jurul lui 0 cu $\frac{\pi}{2}$

$\left\{ \begin{array}{l} \phi = 1, \phi^{-1}, \phi^2, \phi^3 \\ \text{etc} \end{array} \right\} \cong (\mathbb{Z}_4, +)$

(c) Procedeele de la (a) și (b) descriu funcții mutual inverse între mulțimea tuturor acțiunilor lui G pe A și mulțimea tuturor homomorfismelor de grupuri $G \rightarrow S(A)$.

Demonstrație. □

Definiție 2.1.31. Fie $G \times A \rightarrow A$, $(g, x) \mapsto gx$ o acțiune a grupului (G, \cdot) pe mulțimea A . Se numește reprezentare prin permutări a acestei acțiuni homomorfismul de grupuri $\phi : G \rightarrow S(A)$ construit în Teorema 2.1.30. Acțiunea se zice *fidelă*, dacă reprezentarea ei prin permutări este un homomorfism injectiv.

Propoziție 2.1.32. Fie $G \times A \rightarrow A$, $(g, x) \mapsto gx$ o acțiune a grupului (G, \cdot) pe mulțimea A . Relația (A, A, \equiv) dată prin $x \equiv y$ dacă există $g \in G$ astfel încât $gx = y$, pentru orice $x, y \in A$ este o relație de echivalență, a carei clase de echivalență (numite orbite) se determină ca fiind $Gx = \{gx \mid g \in G\}$, mit $x \in A$.

Demonstrație. □

Corolar 2.1.33. Notăm cu $[A/\equiv]$ un sistem de reprezentanți pentru mulțimea tuturor orbitelor unei acțiuni $G \times A \rightarrow A$ a grupului (G, \cdot) pe mulțimea A . Atunci este valabilă egalitatea:

$$|A| = \sum_{Gx \in [A/\equiv]} |Gx|.$$

Demonstrație. □

Corolar 2.1.34. (Teorema lui Lagrange) Fie G un grup finit.

- (a) Dacă H este un subgrup al lui G atunci $|H|$ divide $|G|$.
- (b) Dacă $x \in G$ atunci $\text{ord}(x)$ divide $|G|$.

Demonstrație. □

Definiție 2.1.35. Ordinul unui grup (G, \cdot) este cardinalul $|G|$.

Grupul simetric.

Definiție 2.1.36. Fie n un număr natural și G un subgrup al grupului simetric $S_n = S(\{1, 2, \dots, n\})$. Acțiunea lui G pe $\{1, 2, \dots, n\}$ a cărei reprezentare prin permutări este funcția de inclusiune $i : G \rightarrow S_n$ este numită acțiunea canonica. Pentru $\sigma \in S_n$ se numesc σ -orbite orbitele acțiunii canonice a grupului $G = \langle \sigma \rangle$. O σ -orbită se zice trivială dacă ea conține un singur element. Un ciclu este o permutare care are o singură orbită netrivială. În acest caz, cardinalul acestei orbită (netriviale) este numită lungimea ciclului. Doă cicluri se zic disjuncte în cazul în care orbitele lor netriviale sunt disjuncte (ca mulțimi).

Observație 2.1.37. Fie $\sigma \in S_n$.

- (1) $\sigma = e$ (e este permutarea identică) ddacă toate σ -orbitele sunt triviale; Altfel spus e este un ciclu de lungime 1.
- (2) σ este un ciclu de lungime $1 < k \leq n$ ddacă există o submulțime $\{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$, astfel încât $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \dots, \sigma(i_n) = i_1$ și $\sigma(i) = i$ pentru $i \notin \{i_1, i_2, \dots, i_k\}$. În acest caz $\{i_1, i_2, \dots, i_k\}$ este singura orbită netrivială a lui σ și notăm $\sigma = (i_1 i_2 \dots i_k)$.

Teorema lui Lagrange

2.1.3h. (a). G grup, $H \leq G$

Definim relația f_H pe G prin $x f_H y \Leftrightarrow x^{-1}y \in H$, $\forall x, y \in G$.

(A) Arătăm că f_H este o relație echivalență

$$(R) \quad x \in G \quad x^{-1}x = 1 \in H \Rightarrow xf_H x$$

$$(T) \quad x, y, z \in G \quad x f_H y, y f_H z \Rightarrow x^{-1}y \in H, y^{-1}z \in H \xrightarrow{\text{p. stab.}} x^{-1}y^{-1}z \in H \Rightarrow xf_H z.$$

$$(S) \quad x, y \in G \quad x f_H y \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} \in H \Rightarrow y^{-1}x \in H \Rightarrow y f_H x.$$

(2) Vom arăta că pt. $x \in G$ clasa de echiv. a lui $x \in G$ este

$$xH = \{x \cdot h \mid h \in H\} \stackrel{x^{-1}}{=} \{y \in G \mid y f_H x\}$$

$$x^{-1}(xh) = x x^{-1}h = h \in H \Rightarrow xf_H(xh)$$

$$y \in G \quad y f_H x \Rightarrow x^{-1}y \in H; \text{ not. } h = x^{-1}y \in H \Rightarrow xh = x \cdot x^{-1}y = y$$

(3) Vom arăta că $\varphi_x: H \rightarrow xH$, $\varphi_x(h) = xh$ este o bij.

φ_x este inj. pt. că $xH = h \cdot x \mid h \in H$.

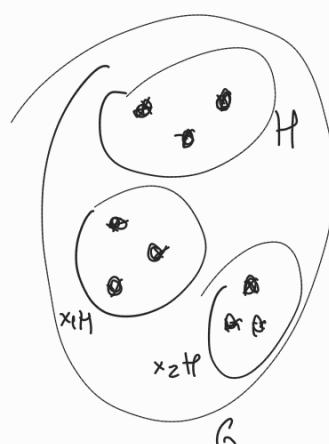
φ_x este surj. pt. că $xh = xk \Rightarrow h = k$ OR.
If inj. $\varphi_x(h) = \varphi_x(k)$, $h, k \in H \Rightarrow xh = xk \Rightarrow h = k$

$$\text{Obi} \quad NH = H$$

Amen $G = \bigcup_{x \in G} (xH)$ (prop. de
la partitii)

$$\text{și } |G| = \sum_{x \in G} |xH| = \sum |H|$$

Deci $|G| \leq \infty \Rightarrow |H| \mid |G|$. \square .



Lemă 2.1.38. Pentru $\sigma \in S_n$ și $i \in \{1, 2, \dots, n\}$ există un cel mai mic număr natural $k \leq 1$, astfel încât $\sigma^k(i) = i$. Acest număr k este lungimea orbitelor $\langle \sigma \rangle i$ și avem:

$$\langle \sigma \rangle i = \{i, \sigma(i), \dots, \sigma^{k-1}(i)\}.$$

Demonstrație. □

Lemă 2.1.39. Dacă σ_1 și σ_2 sunt cicluri disjuncte, atunci $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Demonstrație. □

Teoremă 2.1.40. Orice permutare se scrie ca un produs de cicluri netriviale și două câte două disjuncte. Mai mult, această descompunere este unică (abstracție făcând e ordinea factorilor).

Demonstrație. □

Observație 2.1.41. Se numește decompunerea lui σ ca produs de cicluri duoă câte două disjuncte dată în Teorema 2.1.40. Uneori această descompunere conține de asemenea și cicluri triviale $(i) = e$, unde $i \in \{1, 2, \dots, n\}$ cu proprietatea $\sigma(i) = i$, inclusiv cazul $\sigma = e$ din Teorema precedentă.

Definiție 2.1.42. O inversiune pentru $\sigma \in S_n$ este o pereche $(i, j) \in \{1, 2, \dots, n\}^2$, astfel încât $i < j$ și $\sigma(i) > \sigma(j)$. Se notează cu $m(\sigma)$ numărul de inversiuni și se definește semnul lui σ prin $\epsilon(\sigma) = (-1)^{m(\sigma)}$. Permutarea σ se zice *(im)pară* în cazul în care $m(\sigma)$ este (im)par.

Teoremă 2.1.43. (Cayley) Orice grup este izomorf cu un subgrup al unui grup de permutări.

Demonstrație. □

Exerciții la grupuri.

Exercițiu 2.1.44. Se consideră mulțimea

$$\mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C} \text{ (aici } i^2 = -1\text{).}$$

Să se arate că $\mathbb{Z} + i\mathbb{Z}$ este un monoid în raport cu înmulțirea numerelor complexe. Să se determine $(\mathbb{Z} + i\mathbb{Z})^\times$.

Exercițiu 2.1.45. Se consideră operația $* : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ gegeben durch $x * y = xy - 5x - 5y + 30$. Ist $(\mathbb{R}, *)$ eine Gruppe? Aber $(\mathbb{R} \setminus \{5\}, *)$, $((5, \infty), *)$ oder $((-\infty, 5), *)$?

Exercițiu 2.1.46. Man ziege, dass $(\mathbb{Z}_n, +)$ ($n \in \mathbb{N}$, $n \geq 2$) eine abelsche Gruppe ist, și $p_n : \mathbb{Z} \rightarrow \mathbb{Z}_n$, $p_n(x) = [x]_n$ ein surjektiver Gruppenhomomorphismus ist (siehe also Übung 1.4.42).

Exercițiu 2.1.47. Fie (G_i, \cdot) o familie de grupuri. Să se arate că $(\prod_{i \in I} G_i, \cdot)$ este un grup, unde

$$(x_i)_{i \in I} \cdot (y_i)_{i \in I} = (x_i y_i)_{i \in I} \text{ pentru orice } (x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} G_i.$$

Să se arate de asemenea că $p_j : \prod_{i \in I} \rightarrow G_j$, $p_j(x_i)_{i \in I} = x_j$ este un homomorfism surjectiv pentru orice $j \in I$.

Exercițiu 2.1.48. Fie G un grup. Să se arate că dacă pentru orice două elemente $x, y \in G$, există $k \in \mathbb{Z}$ astfel încât $(xy)^i = x^i y^i$ pentru $i = k - 1, k, k + 1$ atunci G este abelian.

Exercițiu 2.1.49. Să se arate că o parte stabilă finită a unui grup este întotdeauna un subgrup. Dar o parte stabilă infinită?

Exercițiu 2.1.50. Se consideră un grup (G, \cdot) , și se notează $\text{Sub}(G) = \{H \subseteq G \mid H \leq G\}$ mulțimea tuturor subgrupurilor. Să se arată că $(\text{Sub}(G), \leq)$ este o lattice.

Exercițiu 2.1.51. Fie $A_1 A_2 \dots A_n$ un poligon regulat (cu n vârfuri și n laturi) cu centrul O într-un plan α . (considerat ca o mulțime de puncte). O izometrie este o funcție $f : \alpha \rightarrow \alpha$ cu proprietatea că $|f(X)f(Y)| = |XY|$ pentru orice $X, Y \in \alpha$, unde prin $|XY|$ notăm distanța dintre X și Y . Se consideră mulțimea tuturor izometriilor care invariază poligonul $A_1 A_2 \dots A_n$ mai precis

$$\begin{aligned} D_n &= \{f : \alpha \rightarrow \alpha \mid f \text{ este o izometrie și} \\ &\quad f(A_1 A_2 \dots A_n) = A_1 A_2 \dots A_n\}. \end{aligned}$$

Notăm cu s rotația în jurul centrului O cu $\frac{2\pi}{n}$ radiani, (de la A_1 către A_2) și cu t simetria axială față de axa $A_1 O$. Să observăm că $s, t : \alpha \rightarrow \alpha$ sunt izometrii. Să se arate că

- (1) $s^n = 1 = t^2$ (aici $1 = 1_\alpha$ este funcția identitate a planului α).
- (2) $ts = s^{n-1}t$.
- (3) $D_n = \{1, s, \dots, s^{n-1}, t, st, \dots, s^{n-1}t\}$
- (4) D_n este un grup în raport cu compunerea funcțiilor (care este numit *grupul diedral*)
- (5) Să se determine $\langle s \rangle, \langle t \rangle, \langle s, t \rangle$

Să se construască tablele operațiilor D_3 și D_4 .

Exercițiu 2.1.52. Pe mulțimea $H = \{1, -1, i, -i, j, -j, k, -k\}$ se definește în felul următor o înmulțire:

- 1 este elementul neutru.
- Înmulțirea respectă regula semnelor: $(-x)y = x(-y) = -xy$ (altfel semnele + și - nu au încă vreun sens).
- $i^2 = j^2 = k^2 = -1$.
- $ij = k = -ji, jk = i = -kj, ki = j = -ik$.

Să se arate că (H, \cdot) este un grup (numit *grupul quaternionilor*).

Exercițiu 2.1.53. Să se arate că grupurile $(\mathbb{R}, +)$ și (\mathbb{R}_+^*, \cdot) sunt izomorfe.

Exercițiu 2.1.54. Să se arate că $f : \mathbb{C}^* \rightarrow \mathbb{R}$, $f(x) = \arg x$ este un homomorfism de grupuri între (\mathbb{C}^*, \cdot) și $(\mathbb{R}, +)$, și să se determine $\text{Ker } f$ și $\text{Im } f$.

Exercițiu 2.1.55. Să se arate că grupurile $(\mathbb{Z}, +)$ și $(\mathbb{Z}_n, +)$ ($n \in \mathbb{N}$, $n \geq 2$) sunt ciclice.

Exercițiu 2.1.56. Fie $n \in \mathbb{N}$, $n \geq 2$. Să se arate că

$$U_n = \{x \in \mathbb{C}^* \mid \text{există } n \in \mathbb{N} \text{ astfel încât } x^n = 1\}$$

este un subgrup a grupului (\mathbb{C}^*, \cdot) și că U_n este ciclic. Să se găsească un izomorfism între $(\mathbb{Z}_n, +)$ și (U_n, \cdot) .

Exercițiu 2.1.57. Să se găsească toate subgrupurile lui $(\mathbb{Z}, +)$. Indicație: Să se arate că

$$\text{Sub}(\mathbb{Z}, +) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}, \text{ unde } n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}.$$

Exercițiu 2.1.58. Să se găsească un exemplu de două subrupuri ale unui grup a căror reuniune nu este subgrup.

Exercițiu 2.1.59. Fie $(G, +)$ un grup abelian și $H, K \leq G$ două subgrupuri. Să se arate că $\langle H \cup K \rangle = H + K$, unde $H + K = \{x + y \mid x \in H, y \in K\}$.

Exercițiu 2.1.60. Fie (G, \cdot) un grup și $H, K \leq G$. Să se arate că $H \cup K \leq G$ dacă $H \subseteq K$ sau $K \subseteq H$.

Exercițiu 2.1.61. Fie $n, m \in \mathbb{Z}$. Să se arate că

- (a) $n\mathbb{Z} \subseteq m\mathbb{Z} \Leftrightarrow m|n$.
- (b) $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$, unde $k = \text{lcm}(n, m)$.
- (c) $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, unde $d = \gcd(n, m)$.

Exercițiu 2.1.62. Să se arate că pentru $n, m \in \mathbb{N}$ cu $d = \gcd(n, m)$, există două numere întregi $s, t \in \mathbb{Z}$, astfel încât $d = sn + tm$. Folosiți acest rezultat ca să arătați că $1 = \gcd(n, m)$ dacă există $s, t \in \mathbb{Z}$ astfel încât $1 = sn + tm$.

Exercițiu 2.1.63. Să se folosească algoritmul lui Euclid pentru ca plecând de la $m, n \in \mathbb{N}$ să determinăm numerele întregi s, t cu proprietatea că $\gcd(n, m) = sn + tm$ zu bestimmen.

Exercițiu 2.1.64. Să se găsească toate grupurile (până la un izomorfism) care se pot defini pe o mulțime cu 4 elemente.

Exercițiu 2.1.65. Fie (G, \cdot) un grup și $x, y \in G$ astfel încât $xy = yx$. Avem:

- (a) $\text{ord}(x^{-1}) = \text{ord}(x)$
- (b) $\text{ord}(xy) = \text{ord}(yx)$.

Exercițiu 2.1.66. Fie $f : G \rightarrow H$ un homomorfism de grupuri. Dacă $x \in G$ este de ordin finit, atunci tot aşa este și $f(x)$, și avem $\text{ord}(f(x)) | \text{ord}(x)$.

Exercițiu 2.1.67. Două grupuri ciclice infinite sunt izomorfe. Două grupuri ciclice finite sunt izomorfe dacă au același număr de elemente.

Exercițiu 2.1.68. Dacă G este un grup ciclic, atunci există un homomorfism surjectiv $\mathbb{Z} \rightarrow G$.

Exercițiu 2.1.69. Să se arată că următoarele perechi de grupuri nu sunt izomorfe: $(\mathbb{Z}_n, +)$ și $(\mathbb{Z}_m, +)$ și $n \neq m$; $(\mathbb{Z}, +)$ și $(\mathbb{Q}, +)$; $(\mathbb{Z}_8, +)$ și $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$ (pentru grupul produs vezi Übung 2.1.47).

Exercițiu 2.1.70. Fie $G \times A \rightarrow A$, $(g, x) \mapsto gx$ o acțiune a grupului (G, \cdot) pe mulțimea A . Să se arate că:

- (a) Pentru orice $x \in A$ submulțimea $\text{Stab}_G(x) = \{g \in G \mid gx = x\}$ formează un subgrup a lui G .
- (b) Mulțimea $K = \{g \in G \mid gx = x \text{ für alle } x \in A\}$ este un subgrup a lui G (acest subgrup este numit *nucleul* acțiunii). Mai mult avem: $K = \bigcap_{x \in A} \text{Stab}_G(x)$.
- (c) Acțiunea este fidelă dacă nucleul este trivial, adică $K = \{1\}$.

Exercițiu 2.1.71. Fie $N = \{1, x, x^2\}$ și $H = \{1, y, y^2, y^3\}$ două grupuri ciclice generate de elementele x și y cu $\text{ord}(x) = 3$, $\text{ord}(y) = 4$. Atunci:

- (a) Să se definească o acțiune netrivială a lui H pe N , (adică $\cdot : H \times N \rightarrow N$) așa încât $h \cdot 1 = h$ pentru orice $h \in H$.
 (b) Care este nucleul acestei acțiuni?
 (c) Pentru $h \in H$ se consideră $\phi_h : N \rightarrow N$, $\phi_h(n) = h \cdot n$. Să se arate că ϕ_h este un izomorfism.
 (d) Considerăm $G = N \times H$ ca mulțimi. Se definește o operație pe G prin

$$(n_1, h_1)(n_2, h_2) = (n_1(h_1 \cdot n_2), h_1 h_2).$$

Să se arate că G împreună cu această operație este un grup neabelian cu 12 elemente.

Exercițiu 2.1.72. Un grup de ordin prim este ciclic. Indicație: Se arată că un grup de ordin prim nu are subgrupuri netriviale (un astfel de grup se zice *simple*).

Exercițiu 2.1.73. Dacă mulțimile A și B au același cardinal, atunci grupurile $S(A)$ și $S(B)$ sunt izomorfe.

Exercițiu 2.1.74. Să se descompună $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 5 & 6 & 4 & 8 & 7 \end{pmatrix} \in S_8$ ca produs de cicluri două câte două disjuncte.

Exercițiu 2.1.75. Fie $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \in S_5$.

- (a) Să se descompună σ și τ ca produs de cicluri două câte două disjuncte.
 (b) Să se calculeze $\sigma\tau$, $\tau\sigma$, σ^{-1} , τ^2 .
 (c) Să se calculeze $\text{ord}(\sigma)$ și $\langle \sigma \rangle$.
 (d) Să se calculeze $\epsilon(\sigma)$ și $\epsilon(\tau)$.

Exercițiu 2.1.76. Să se arate că

- (a) $\epsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$ pentru orice $\sigma \in S_n$.
 (b) $\epsilon : S_n \rightarrow \{1, -1\} = U_2$ (vezi Exerțiul 2.1.56) este un homomorfism.
 (c) Kere = A_n , unde $A_n = \{\sigma \in S_n \mid \sigma \text{ este par}\}$.

Exercițiu 2.1.77. Un ciclu de lungime k este exact atunci o permutare pară când k este un număr impar. Orice permutare (im)pară se scrie ca un produs al unui număr (im)par de transpoziții, dar această descompunere nu mai este unică. Reamintim că o transpoziție este un ciclu de lungime 2.

Exercițiu 2.1.78. Fie $\sigma \in S_n$ un ciclu de lungime l . Să se arate:

- (a) Dacă $l = 2k + 1$ este impar, atunci σ^2 este un ciclu de lungime l .
 (b) Dacă $l = 2k$ este par, atunci σ^2 este un produs de două cicluri disjuncte amândouă de lungime k .
 (c) $\text{ord}(\sigma) = l$.

Exercițiu 2.1.79. Să se arate că $(12)(3456) \in S_6$ este o permutare para care nu este patratul nici unei alte permutări din S_6 .

2.2. Inele și corpuși.

Definiție 2.2.1. Un *inel* este un triplet $(R, +, \cdot)$, care constă dintr-o mulțime R împreună cu două operații $+$, $\cdot : R \times R \rightarrow R$, astfel încât

- (a) $(R, +)$ este un grup abelian.
 (b) \cdot este asociativă.

(c) · este distributivă bilateral în raport cu +, adică pentru orice $x, y, z \in R$ avem:

$$x(y+z) = xy + xz \text{ și } (y+z)x = yx + zx.$$

Inelul R se zice *comutativ* sau *unitar*, după cum operația · este și comutativă, respectiv are unitate.

Observație 2.2.2. Într-un inel R se notează cu 0 elementul neutru pentru + și cu 1 elementul neutru pentru · (dacă acesta din urmă există). Ordinea operațiilor este cea obișnuită, mai precis mai întâi acionează înmulțirea și pe urmă adunarea.

Exemplu 2.2.3. (a) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt inele comutative și unitare.

(b) Dacă R este un inel comutativ, atunci $(M_{n \times n}(R), +, \cdot)$ este de asemenea inel; totuși $(M_{n \times n}(R), +, \cdot)$ nu este în mod necesar comutativ. Dacă R este unitar atunci totașă este și $(M_{n \times n}(R), +, \cdot)$, iar elementul neutru pentru înmulțirea matricilor este totașă numita matrice unitate de rank n :

$$I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

- (c) Dacă $(R, +)$ este un grup abelian, atunci $(R, +, \cdot)$ este un inel unde $xy = 0$ pentru orice $x, y \in R$ (un astfel de inel se numește *de pătrat nul*. În particular $R = \{0\}$ este un inel (unitar!), unde $0 + 0 = 0 \cdot 0 = 0$ (acest inel se numește *inelul nul* și este notat $R = 0$).
- (d) Dacă $(R, +, \cdot)$ este un inel, atunci totașă este și $R^o, +, *$, unde $R^o = R$ și $x * y = yx$ pentru orice $x, y \in R$; R^o se numește *inelul opus* lui R .

Propoziție 2.2.4. (Reguli de calcul în inele) Fie R un inel și $x, y, z \in R$. Avem:

- (a) $x0 = 0x = 0$.
- (b) $x(-y) = (-x)y = -xy$.
- (c) $x(y - z) = xy - xz$ și $(y - z)x = yx - zx$.
- (d) Dacă $R \neq 0$ este un inel unitar, atunci $1 \neq 0$.

Demonstrație.

□

Definiție 2.2.5. Un *corp* este un inel unitar $(K, +, \cdot)$ cu proprietatea că oricare $x \in K^*$ este inversabil (în raport cu ·). (Aici și în continuare notăm $K^* = K \setminus \{0\}$)

Observație 2.2.6. În conformitate cu Propoziția 2.1.5, un inel unitar K este exact atunci un corp când (K^*, \cdot) este un grup.

Exemplu 2.2.7. (a) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt corpuri comutative.
(b) $(\mathbb{Z}, +, \cdot)$ nu este un corp.

Subinele și subcorpuri.

Definiție 2.2.8. Fie $(R, +, \cdot)$ un inel. Un *subinel* a lui R este o submulțime $S \subseteq R$, cu proprietatea că operațiile + și · din R induc operații bine definite pe S (adică $x, y \in S \Rightarrow x + y, xy \in S$; se mai spune că S este o *parte stabilă* în raport cu + și ·), iar cu operațiile induse S formează un inel. Se scrie $S \leq R$. Dacă $1 \in R$ atunci se zice *unitar* un subinel $S \leq R$ cu proprietatea $1 \in S$.

Exemplu 2.2.9. (1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$

- (2) $2\mathbb{Z} \leq \mathbb{Z}$ aber $1 \notin 2\mathbb{Z}$.
 (3) Orice inel R are aşa numitele subinele triviale, adică $\{0\}$ și R .

Propoziție 2.2.10 (Teorema de caracterizare a subinelelor). *Fie $(R, +, \cdot)$ un inel și fie $S \subseteq R$ o submulțime. Următoarele afirmații sunt echivalente :*

- (i) $S \leq R$.
- (ii) (a) $0 \in S$.
 - (b) $x, y \in S \Rightarrow x + y \in S$.
 - (c) $x \in S \Rightarrow -x \in S$.
 - (d) $x, y \in S \Rightarrow xy \in S$.
- (iii) (a) $0 \in S$.
 - (b) $x, y \in H \Rightarrow x - y \in H$.
 - (c) $x, y \in S \Rightarrow xy \in S$.

Demonstrație.

□

Propoziție 2.2.11. *Fie $(R, +, \cdot)$ un inel. Dacă $S_i \leq R$, cu $i \in I$, atunci avem $\bigcap_{i \in I} S_i \leq R$.*

Observație 2.2.12. Reuniunea a două sau mai multe subinele, nu este cu necesitate subinel (a se vedea și Observația 2.1.11), 2.1.11).

Definiție 2.2.13. Fie $(K, +, \cdot)$ un corp. Un *subcorp* a lui K este o submulțime $L \subseteq K$ cu proprietatea că operațiile $+$ și \cdot din R induc operații bine definite pe S , iar cu operațiile induse L formează un corp. Se scrie $L \leq K$.

Observație 2.2.14. Un subcorp este un subinel unitar

Propoziție 2.2.15 (Teorema de caracterizare a subcorpurilor). *Fie $(K, +, \cdot)$ un corp și fie $L \subseteq K$ o submulțime. Următoarele afirmații sunt echivalente:*

- (i) $L \leq K$.
- (ii) (a) $0, 1 \in L$.
 - (b) $x, y \in L \Rightarrow x + y \in L$.
 - (c) $x \in L \Rightarrow -x \in L$.
 - (d) $x, y \in L \Rightarrow xy \in L$.
 - (e) $x \in L^* \Rightarrow x^{-1} \in L$
- (iii) (a) $0, 1 \in L$.
 - (b) $x, y \in L \Rightarrow x - y \in L$.
 - (c) $x, y \in L^* \Rightarrow xy^{-1} \in S$.

Demonstrație.

□

Observație 2.2.16. Ca și în cazul grupurilor putem defini subinelul sau subcorpul generat.

Homomorfisme.

Definiție 2.2.17. Un *homomorfism* de inele (respectiv coruri) este o funcție $f : R \rightarrow S$ ($f : K \rightarrow L$), unde R și S (K și L) sunt două inele (coruri), astfel încât $f(x + y) = f(x) + f(y)$ și $f(xy) = f(x)f(y)$ pentru orice $x, y \in R$ ($x, y \in K$). Dacă inelele R și S sunt unitare, atunci un homomorfism $f : R \rightarrow S$ se zice *unitar* dacă $f(1) = 1$. Un homomorfism de inele (coruri) se numește *izomorfism* dacă el este și bijectiv; în acest caz, inelele (corurile) se zic izomorfe și scriem $R \cong S$ (sau $K \cong L$).

Exemplu 2.2.18. Pentru două inele (corpuri) R și S funcțiile $1_R : G \rightarrow H$, $0(x) = 0$ sunt un izomorfism, respectiv un homomorfism. Dacă $S \leq R$ atunci aplicația de incluziune $i : S \rightarrow R$ este un homomorfism.

Lemă 2.2.19. Un homomorfism de corpuri este sau unitar sau nul.

Demonstrație. □

Lemă 2.2.20. Componerea a două homomorfisme de inele (corpuri) este de asemenea un homomorfism. Funcția inversă a unui izomorfism de inele (corpuri) este de asemenea un izomorfism.

Demonstrație. □

ELEMENTE SPECIALE ÎNTR-UN INEL

Ca și în cazul monoizilor, pentru un inel unitar R notăm

$$R^\times = \{x \in R \mid x \text{ este inversabil (în raport cu înmulțirea)}\}.$$

Definiție 2.2.21. Fie R un inel. Un element $x \in R$ se numește:

- (1) *divizor al lui zero la stânga sau dreapta* dacă există $y \in R$, $y \neq 0$ astfel încât $xy = 0$ respectiv $yx = 0$. Elementul x este numit simplu *divizor al lui zero* dacă este un divizor al lui zero atât la stânga cât și la dreapta.
- (2) *idempotent* dacă este adevărată egalitatea $x^2 = x$.
- (3) *nilpotent* dacă există $n \in \mathbb{N}$, astfel încât $x^n = 0$.

Observație 2.2.22. Fie $R \neq 0$ un inel și fie $x \in R$.

- (a) În mod evident 0 este un divizor al lui zero. Se spune că 0 este divizorul trivial al lui zero. Un inel R se zice *fără divizori ai lui zero*, dacă R nu conține divizori netriviali ai lui zero.
- (b) 0 și 1 (dacă există $1 \in R$, ceea ce înseamnă R este unitar) sunt elemente idempotente; acești idempotenți sunt numiți triviali.
- (c) Dacă x este idempotent, atunci este valabilă egalitatea $x^n = x$, pentru orice $n \in \mathbb{N}^*$.
- (d) Dacă x este nilpotent și $x^n = 0$ pentru un $n \in \mathbb{N}$, atunci avem $x^{n+k} = 0$ pentru orice $k \in \mathbb{N}$.

Exemplu 2.2.23. Se consideră inelul $(\mathbb{Z}_{12}, +, \cdot)$.

- (1) $[3]_{12}$ este un divizor al lui zero, pentru că $[3]_{12}[4]_{12} = [4]_{12}[3]_{12} = [0]_{12}$.
- (2) $[4]_{12}$ este idempotent, pentru că $[4]_{12}^2 = [4]_{12}$.
- (3) $[6]_{12}$ este nilpotent, pentru că $[6]_{12}^2 = [0]_{12}$.

Propoziție 2.2.24. Fie R un inel unitar.

- (1) Dacă $x \in R^\times$ atunci x nu este un divizor al lui zero.
- (2) $x \in R$ nu este un divizor al lui zero la stânga (dreapta) dacă cu x se poate simplifica la stânga (dreapta).
- (3) Dacă $e \in R$ este un idempotent netrivial, atunci e este un divizor al lui zero.
- (4) Dacă $x \in R$ este nilpotent, atunci x este un divizor al lui zero.

Demonstrație. □

Definiție 2.2.25. Un domeniu de integritate este un inel comutativ, unitar și fără divizori ai lui zero.

Propoziție 2.2.26. *Un subinel unitar al unui corp comutativ este un domeniu de integritate.*

Demonstrație. □

Corolar 2.2.27. *Un corp comutativ este un domeniu de integritate.*

Examples 2.2.28. \mathbb{Q} , \mathbb{R} , \mathbb{C} sunt corpuri comutative, deci sunt și domenii de integritate. \mathbb{Z} este un domeniu de integritate care nu este corp.

Propoziție 2.2.29. *Un domeniu de interitate finit este un corp (comutativ).*

Demonstrație. □

Corolar 2.2.30. *Dacă p este un număr prim, atunci $(\mathbb{Z}_p, +, \cdot)$ este un corp comutativ.*

Exerciții la inele și corpuri.

Exercițiu 2.2.31. Să se verifice că $(\mathbb{Z}_n, +, \cdot)$ ($n \leq 2$) este un inel comutativ și unitar, unde $+$ și \cdot sunt definite ca în Exercițiul 1.4.42.

Exercițiu 2.2.32. Pentru un grup abelian $(G, +)$ se consideră

$$\text{End}(G) = \{f : G \rightarrow G \mid f \text{ este un homomorfism de grupuri}\}.$$

Să se arate că $(\text{End}(G), +, \circ)$ este un inel unitar, unde pentru $f, g \in \text{End}(G)$ se definește adunarea prin:

$$f + g : G \rightarrow G, (f + g)(x) = f(x) + g(x), \text{ pentru orice } x \in G.$$

$(\text{End}(G), +, \circ)$ este numit *inelul endomorfismelor* lui G .

Exercițiu 2.2.33. Se consideră o mulțime oarecare A și un inel R . Pe mulțimea $R^A = \{f : A \rightarrow R \mid f \text{ este o funcție}\}$ se definesc operațiile $+, \cdot : R^A \times R^A \rightarrow R^A$ prin $f + g, fg : A \rightarrow R$, $(f + g)(x) = f(x) + g(x)$ și $(fg)(x) = f(x)g(x)$ pentru orice $f, g \in R^A$ și orice $x \in A$. Să se arate că R^A este un inel, iar R^A exact atunci este comutativ sau unitar, când R are aceeași proprietate.

Exercițiu 2.2.34. Să se verifice că $(\mathbb{Q}, +, \cdot)$ este un corp, unde $+$ și \cdot sunt definite ca în Exercițiul 1.4.41.

Exercițiu 2.2.35. Se consideră grupul quaternionilor $H = \{\}$ (vezi Exercițiul Übung 2.1.52). Să se verifice că

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

este un corp necomutativ, unde

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k) = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i \\ + (ac' - bd' + ca' + db')j + (ad' + bc' - cb' + da')k$$

(adică înmulțirea în \mathbb{H} este indușă de înmulțirea în H).

Exercițiu 2.2.36. Fie R un inel comutativ și unitar. Să se verifice că mulțimea tuturor polinoamelor

$$R[X] = \{a_0 + a_1X + \dots + a_nX^n \mid n \in \mathbb{N}, a_i \in R \text{ pentru orice } 1 \leq i \leq n\}.$$

formează un inel comutativ și unitar împreună cu adunarea și înmulțirea bișnuită a polinoamelor. Să se arate de asemenea că R este un subinel al lui $R[X]$.

Exercițiu 2.2.37. Să se determine toate subinelele lui $(\mathbb{Z}, +, \cdot)$.

Exercițiu 2.2.38. Fie $n \in \mathbb{N}$, $n \geq 2$. Să se arate că $\mathbb{Z}_n^\times = \{[k]_n \mid \gcd(n, k) = 1\}$. Să se folosească acest rezultat pentru a arăta din nou că \mathbb{Z}_n este un corp dacă n este un număr prim.

Exercițiu 2.2.39. Să se rezolve următoarele ecuații în \mathbb{Z}_6 : $[4]_6x + [5]_6 = [1]_6$ și $[5]_6x + [3]_6 = [1]_6$

Exercițiu 2.2.40. Să se arate că $\mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z}\}$ este un subiel al lui \mathbb{C} . Să se arate că

$$R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$$

este un subiel al lui $(\mathbb{M}_{2 \times 2}(\mathbb{Z}), +, \cdot)$, și $R \cong \mathbb{Z} + i\mathbb{Z}$. Sunt $\mathbb{Z} + i\mathbb{Z}$ și/sau R domenii de integritate? Dar corpu?

Exercițiu 2.2.41. Să se determine $(\mathbb{Z} + i\mathbb{Z})^\times$.

Exercițiu 2.2.42. Să se arate că $R[X]^\times = R^\times$, pentru orice inel comutativ și unitar R .

Exercițiu 2.2.43. Fie R un inel comutativ și unitar. Să se arate că inelele $\mathbb{M}_{n \times n}(R)$ și $\mathbb{M}_{n \times n}(R)^\circ$ sunt izomorfe. De aici să se deducă echivalența următoarelor afirmații, pentru orice $A \in \mathbb{M}_{n \times n}(R)$:

- (i) A este inversabilă la stânga.
- (ii) A este inversabilă la dreapta.
- (iii) A este inversabilă.

Exercițiu 2.2.44. Să se arate că următoarele perechi de inele nu sunt izomorfe: \mathbb{Z} și \mathbb{Q} ; \mathbb{Z} și $\mathbb{M}_{2 \times 2}(\mathbb{Z})$.

Exercițiu 2.2.45. Să se arate că următoarele corpu nu sunt izomorfe: \mathbb{R} și \mathbb{C} .

Exercițiu 2.2.46. Să se arate că $\mathbb{Q} + i\mathbb{Q} = \{a + ib \mid a, b \in \mathbb{Q}\}$ este un subcorp al lui \mathbb{C} .

Exercițiu 2.2.47. Dacă R este un domeniu de integritate, atunci aceeași proprietate este valabilă pentru $R[X]$.

Exercițiu 2.2.48. Să se determine toate elementele idempotente din inelul \mathbb{Z}_n , unde $n \in \mathbb{N}$, $n \geq 2$.

Exercițiu 2.2.49. Să se determine toate elementele nilpotente din inelul \mathbb{Z}_n , unde $n \in \mathbb{N}$, $n \geq 2$.

3. ALGEBRA LINIARA

În acest capitol fixăm un corp comutativ $(K, +, \cdot)$. Exemple de corpu comutative sunt în special $K = \mathbb{R}$ sau $K = \mathbb{C}$ dar cazurile $K = \mathbb{Q}$ sau $K = \mathbb{Z}_p$, și $p \in \mathbb{N}$ este un număr prim sunt de asemenea posibile.

3.1. Spații vectoriale și aplicații liniare.

Definiție 3.1.1. Un spațiu vectorial peste K sau mai scurt K -spațiu vectorial este format dintr-un grup abelian $(V, +)$ împreună cu o operație externă $\cdot : K \times V \rightarrow V$ care satisfac următoarele axiome:

- (SV1) $\alpha(x + y) = \alpha x + \alpha y;$
- (SV2) $(\alpha + \beta)x = \alpha x + \beta x;$
- (SV3) $\alpha(\beta x) = (\alpha\beta)x;$
- (SV4) $1x = x$

pentru orice $x, y \in V$ și orice și orice $\alpha, \beta \in K$. Se scrie $_K V$. Elementele din V și K sunt numite *vectori* respectiv *scalar*. Adunarea în V și operația externă se numesc *adunarea vectorilor* respectiv *înmulțirea cu scalari*. Spațiile vectoriale sunt numite uneori *spații liniare*.

Exemplu 3.1.2. (1) $V = \{0\}$ este un spațiu vectorial, unde $0+0 = 0$ și $\alpha 0 = 0$ pentru orice $\alpha \in K$. Se notează cu 0 acest spațiu vectorial.

(2) K^n este un K -spațiu vectorial în raport cu adunarea vectorilor:

$$[x_1, x_2, \dots, x_n] + [y_1, y_2, \dots, y_n] = [x_1 + y_1, x_2 + y_2, \dots, x_n + y_n]$$

și cu înmulțirea cu scalari:

$$\alpha[x_1, x_2, \dots, x_n] = [\alpha x_1, \alpha x_2, \dots, \alpha x_n].$$

- (3) $M_{m \times n}(K)$ este un K -spațiu vectorial cu adunarea matricilor și cu înmulțirea unei matrici cu un scalar, adică pentru $A = [a_{i,j}]$ și $B = [b_{i,j}]$ și $\alpha \in K$, avem $A + B = [a_{i,j} + b_{i,j}]$ și $\alpha A = [\alpha a_{i,j}]$. ce obținem când punem $m = 1$? Dar pentru $n = 1$?
- (4) Dacă K este un corp și L este un subcorp, atunci L este un k -spațiu vectorial, unde adunarea vectorilor este adunarea în L , iar înmulțirea cu scalari este:

$$K \times L \rightarrow L, (\alpha, x) \mapsto \alpha x, \text{ pentru orice } x \in L, \alpha \in K.$$

(5) Multimea tuturor polinoamelor

$$K[X] = \{a_0 + a_1 X + \dots + a_n X^n \mid n \in \mathbb{N}, a_0, a_1, \dots, a_n \in K\}$$

este un K -spațiu vectorial în raport cu adunarea polinoamelor (vectori) și înmulțirea polinoamelor cu scalari din K .

- (6) Multimea tuturor vectorilor liberi din plan (sau din spațiu) în raport cu adunarea vectorilor liberi și die obișnuită înmulțire cu scalari este un \mathbb{R} -spațiu vectorial.

Propoziție 3.1.3. (Reguli de calcul în spații vectoriale) Fie V un K -spațiu vectorial, $x, y \in V$ și $\alpha, \beta \in K$. Avem:

- (a) $\alpha 0 = 0 = 0x$.
- (b) $\alpha(-x) = (-\alpha)x = -\alpha x$.
- (c) $\alpha(x - y) = \alpha x - \alpha y$ și $(\alpha - \beta)x = \alpha x - \beta x$.
- (d) $\alpha x = 0$ dacă $\alpha = 0$ sau $x = 0$.

Demonstrație. □

Subspații vectoriale.

Definiție 3.1.4. Fie V un K -spațiu vectorial. Un *subspațiu (vectorial)* a lui V este o submulțime $U \subseteq V$, cu proprietatea că adunarea vectorilor și înmulțirea cu scalari induc operații bine definite pe U (adică $x, y \in U, \alpha \in K \Rightarrow x + y, \alpha x \in U$), și U împreună cu operațiile restricționate fromează un spațiu vectorial. Se scrie $U \leq_K V$ sau simplu $U \leq V$.

Exemplu 3.1.5. Orice spațiu vectorial $_K V$ are două subspații așa zise *triviale*, anume $0 \leq_K V$ și $V \leq_K V$.

Propoziție 3.1.6 (de caracterizare a subspațiilor). *Fie V un K -spațiu vectorial și fie $U \subseteq V$ o submulțime. Următoarele afirmații sunt echivalente:*

- (i) $U \leq_K V$.
- (ii) (a) $0 \in U$.
 (b) $x, y \in U \Rightarrow x + y \in U$.
 (c) $x \in U, \alpha \in K \Rightarrow \alpha x \in U$.
- (iii) (a) $0 \in S$.
 (b) $x, y \in U \Rightarrow \alpha x + \beta y \in U$.

Demonstrație.

□

Propoziție 3.1.7. *Fie V un K -spațiu vectorial. Dacă $U_i \leq_K V$ sunt subspații, cu $i \in I$, atunci avem $\bigcap_{i \in I} U_i \leq_K V$.*

Demonstrație.

□

Observație 3.1.8. Reuniunea a două sau mai multe subspații nu este cu necesitate subspace (vezi de asemenea Observația 2.1.11).

Definiție 3.1.9. Fie V un K -spațiu vectorial și $X \subseteq V$ o submulțime a lui V . *Subspațiul generat de X* este definit prin

$$\langle X \rangle = \langle X \rangle_K = \bigcap_{X \subseteq U \leq_K V} U.$$

Dacă $X = \{x_1, x_2, \dots, x_n\}$ este o mulțime finită, scriem $\langle x_1, x_2, \dots, x_n \rangle_K$ în loc de $\langle \{x_1, x_2, \dots, x_n\} \rangle_K$.

Lemă 3.1.10. *Fie V un K -spațiu vectorial și $X \subseteq V$ o submulțime a lui V . Avem:*

- (a) $\langle X \rangle_K \leq_K V$.
- (b) $X \subseteq \langle X \rangle_K$ și $X = \langle X \rangle_K$ dacă $X \leq_K V$.
- (c) $\langle X \rangle_K$ este cel mai mic subspace a lui V care conține X i.e.

$$U = \langle X \rangle_K \text{ dacă } \begin{cases} U \leq_K V \\ X \subseteq U \\ \text{dacă } W \leq_K V \text{ astfel încât } X \subseteq W \text{ atunci } U \leq_K W \end{cases}.$$

- (d) Dacă $X \subseteq Y \subseteq G$ atunci $\langle X \rangle_K \leq \langle Y \rangle_K \leq V$.

Demonstrație.

□

Propoziție 3.1.11. *Fie V un K -spațiu vectorial și $X \subseteq V$ o submulțime a lui V . Avem:*

$$\langle X \rangle_K = \{\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n \mid n \in \mathbb{N}, x_1, x_2, \dots, x_n \in X \text{ și } \alpha_1, \alpha_2, \dots, \alpha_n \in K\}.$$

În particular, pentru $X = \{x_1, x_2, \dots, x_n\}$ avem:

$$\langle x_1, x_2, \dots, x_n \rangle_K = \{\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n \mid \alpha_1, \alpha_2, \dots, \alpha_n \in K\}.$$

Demonstrație. □

Definiție 3.1.12. Fie V un K -spațiu vectorial și $X \subseteq V$. Se numește *combinație liniară* a vectorilor din X o expresie de forma $\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$ cu $n \in \mathbb{N}$, $x_1, x_2, \dots, x_n \in X$ și $\alpha_1, \alpha_2, \dots, \alpha_n \in K$. În particular o combinație liniară a vectorilor $x_1, x_2, \dots, x_n \in V$ este o expresie de forma $\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$, $\alpha_1, \alpha_2, \dots, \alpha_n \in K$, și o combinație liniară a vectorilor $x, y \in V$ este $\alpha x + \beta y$, cu $\alpha, \beta \in K$.

Observație 3.1.13. Propoziția 3.1.11 spune că subspațiul generat de X conține toți vectorii care se pot scrie ca V care se pot scrie în formă de combinații liniare de elemente ale lui X .

Corolar 3.1.14. Fie V un K -spațiu vectorial.

- (a) Pentru $x \in V$ avem $\langle x \rangle_K = \{\alpha x \mid \alpha \in K\}$.
- (b) Pentru $x, y \in V$ avem $\langle x, y \rangle_K = \{\alpha x + \beta y \mid \alpha, \beta \in K\}$.

Suma și suma directă a subspațiilor.

Definiție 3.1.15. Fie V un K -spațiu vectorial și fie $S, T \leq_K V$ două subspații. Suma acestor subspații este definită ca fiind $S + T = \{x + y \mid x \in S, y \in T\}$.

Propoziție 3.1.16. Fie V un K -spațiu vectorial și fie $S, T \leq_K V$ două subspații. Atunci avem $\langle S \cup T \rangle_K = S + T$. În particular suma a două subspații este un subspațiu.

Demonstrație. □

Corolar 3.1.17. Într-un K -spațiu vectorial V notăm cu $\text{Sub}_K(V) = \{S \mid S \leq_K V\}$ multimea tuturor subspațiilor. Atunci $(\text{Sub}_K(V), \leq_K)$ este o lattice în care $\inf\{S, T\} = S \cap T$ și $\sup\{S, T\} = S + T$.

Demonstrație. □

Elementele unei sume $S + T$ a două subspații $S, T \leq_K V$ sunt vectorii care se pot scrie ca o sumă între un vector din S și un vector din T . Suntem interesați îndeosebi de cazul în care această scriere este unică.

Propoziție 3.1.18. Fie V un K -spațiu vectorial și fie $S, T \leq_K V$ două subspații. Următoarele afirmații sunt echivalente:

- (i) $S \cap T = 0$;
- (ii) Scrierea oricărui vector din $S + T$ ca o sumă dintre un vector din S și unul din T este unică, i. e. pentru $v \in S + T$ avem $v = x + y = s + t$ cu $x, s \in S$ și $y, t \in T$ implică $x = s$ și $y = t$.

Demonstrație. □

Definiție 3.1.19. Se numește *directă* o sumă $S + T$ a două subspații S și T care satisfac condițiile echivalente din Propoziția 3.1.18. În acest caz se scrie $S \oplus T = S + T$.

Observație 3.1.20. Fie V K -spațiu vectorial și fie $S, T \leq_K V$ două subspații. Atunci $V = S \oplus T$ dacă $S \cap T = 0$ și $S + T = V$.

Aplicații liniare.

Definiție 3.1.21. Fie V și W două K -spații vectoriale. Se numește *aplicație liniară* sau homomorfism de spații vectoriale între V și W o funcție $f : V \rightarrow W$ cu proprietățile $f(x+y) = f(x) + f(y)$ și $f(\alpha x) = \alpha f(x)$ pentru orice $x, y \in V$ și orice $\alpha \in K$. Se numește *isomorfism* o aplicație liniară care este și bijectivă. În acest caz spațiile vectoriale V și W se zic izomorfe și scriem $V \cong W$.

Exemplu 3.1.22. Pentru orice două K -spații vectoriale V și W aplicațiile 1_V și $0 : V \rightarrow W$, $0(x) = 0$ sunt liniare; mai mult 1_V este chiar un isomorfism. Dacă $V \leq_K W$ atunci aplicația de inclusiune $i : V \rightarrow W$ este liniară.

Notăție 3.1.23. Fie V și W două K -spații vectoriale. Vom nota

$\text{Hom}_K(V, W) = \{f : V \rightarrow W \mid f \text{ este liniar}\}$ și $\text{End}_K(V) = \text{Hom}_K(V, V)$ (o aplicație liniară $f : V \rightarrow V$ mai este numită și *endomorfism* a lui V).

Observație 3.1.24. Orice aplicație liniară $f : V \rightarrow W$ este și un morfism de grupuri, aşadar avem:

- (a) $f(0) = 0$.
- (b) $f(-x) = -f(x)$.

Propoziție 3.1.25. Fie V și W două K -spații vectoriale. O aplicație $f : V \rightarrow W$ este liniară dacă $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$, pentru orice $x, y \in V$ și orice $\alpha, \beta \in K$.

Demonstrație.

□

Observație 3.1.26. Prin inducție se poate arăta că o aplicație liniară păstrează combinațiile liniare, i. e. dacă $f : V \rightarrow W$ este liniară, $\alpha_1, \dots, \alpha_n \in K$ și $x_1, \dots, x_n \in V$ atunci avem:

$$f(\alpha_1 x_1 + \dots + \alpha_n x_n) = \alpha_1 f(x_1) + \dots + \alpha_n f(x_n).$$

Lemă 3.1.27. Componerea și adunarea a două aplicații liniare (dacă există) sunt de asemenea aplicații liniare. Înmulțirea unei aplicații liniare cu un scalar este o aplicație liniară. Funcția inversă a unui izomorfism este de asemenea un izomorfism.

Demonstrație.

□

Teoremă 3.1.28. Fie V și W două K -spații vectoriale. Atunci $\text{Hom}_K(V, W)$ este de asemenea un K -spațiu vectorial în raport cu adunarea vectorilor (a funcțiilor):

$$+ : \text{Hom}_K(V, W) \times \text{Hom}_K(V, W) \rightarrow \text{Hom}_K(V, W),$$

$$(f + g)(x) = f(x) + g(x) \text{ pentru orice } x \in V,$$

și cu înmulțirea cu scalari

$$\cdot : K \times \text{Hom}_K(V, W) \rightarrow \text{Hom}_K(V, W), (\alpha f)(x) = \alpha f(x), \text{ pentru orice } x \in V.$$

În particular $(\text{End}_K(V), +, \circ)$ este un inel unitar.

Demonstrație.

□

Definiție 3.1.29. Fie $f : V \rightarrow W$ o aplicație liniară. Numim *nucleul* respectiv *imaginăea* lui f mulțimile

$$\text{Ker} f = \{x \in V \mid f(x) = 0\} \text{ și } \text{Im} f = \{f(x) \mid x \in V\}.$$

Propoziție 3.1.30. Dacă $f : V \rightarrow W$ este o aplicație liniară atunci avem:

- (a) $\text{Ker } f \leq_K V$.
- (b) $\text{Im } f \leq_K W$.
- (c) f este injectivă dacă $\text{Ker } f = 0$.
- (d) f este surjectivă dacă $\text{Im } f = W$.

Demonstrație. □

Exerciții la spații vectoriale.

Exercițiu 3.1.31. Să se arate că $\mathbb{R}_+^* = (0, \infty)$ este un \mathbb{R} -spațiu vectorial în raport cu adunarea vectorilor:

$$\boxplus : \mathbb{R}_+^* \times \mathbb{R}_+^* \rightarrow \mathbb{R}_+^*, \quad x \boxplus y = xy, \quad \text{pentru orice } x, y \in \mathbb{R}_+^*,$$

și cu înmulțirea cu scalari

$$\boxdot : \mathbb{R} \times \mathbb{R}_+^* \rightarrow \mathbb{R}_+^*, \quad \alpha \boxdot x = x^\alpha \quad \text{pentru orice } x \in \mathbb{R}_+^*, \alpha \in \mathbb{R}.$$

Exercițiu 3.1.32. Să se verifice că operațiile:

$$\boxplus : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, \quad x \boxplus y = \sqrt[5]{x^5 + y^5}, \quad \text{pentru orice } x, y \in \mathbb{R},$$

$$\boxdot : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, \quad \alpha \boxdot x = \alpha \sqrt[5]{\alpha x} \quad \text{pentru orice } \alpha, x \in \mathbb{R}$$

definesc o structură de \mathbb{R} -spațiu vectorial pe \mathbb{R} .

Exercițiu 3.1.33. Care dintre următoarele submulțimi ale mulțimii \mathbb{R}^3 sunt \mathbb{R} -subspații:

- $A = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid 2x_1 + x_2 - x_3 = 0\}$.
- $B = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid 2x_1 + x_2 - x_3 = 1\}$.
- $C = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 = x_2 = x_3\}$.
- $D = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1^2 + x_2 = 0\}$.
- $E = \mathbb{R}^3 \setminus A$.
- $F = (\mathbb{R}^3 \setminus A) \cup \{0\}$.

Exercițiu 3.1.34. Fie $n \in \mathbb{N}$ fixat. Să se arate că $K_n[X] = \{f \in K[X] \mid \text{grad}(f) \leq n\}$ este un K -subspațiu a lui $K[X]$.

Exercițiu 3.1.35. Să se găsească ecuațiile care determină vectorii din următoarele subspații: $S = \langle [1, 2, -1] \rangle$ și $T = \langle [1, 2, 1], [-2, 1, -3] \rangle$ ale lui \mathbb{R}^3 (ecuațiile acestor subspații).

Exercițiu 3.1.36. Să se scrie subspațiile $S = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 - x_2 - x_3 = 0\}$ și $T = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 - x_2 - x_3 = x_3 - x_1\}$ ale lui \mathbb{R}^3 ca subspații generate (cu număr minimal de generatori).

Exercițiu 3.1.37. Se consideră submulțimile $S, T \subseteq \mathbb{R}^3$ date prin $S = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\}$ și $T = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 = x_2 = x_3\}$. Să se arate că $S, T \leq \mathbb{R}^3$ și $S \oplus T = \mathbb{R}^3$.

Exercițiu 3.1.38. Se consideră $S = \{\alpha I_2 \in \mathbb{M}_{2 \times 2}(\mathbb{R}) \mid \alpha \in \mathbb{R}\}$ și $T = \{A \in \mathbb{M}_{2 \times 2}(\mathbb{R}) \mid \text{Tr}(A) = 0\}$, unde $\text{Tr}(A)$ este suma intrărilor de pe diagonala principală a matricii A . Să se arate că $S, T \leq_{\mathbb{R}} \mathbb{M}_{2 \times 2}(\mathbb{R})$ și $S \oplus T = \mathbb{M}_{2 \times 2}(\mathbb{R})$.

Exercițiu 3.1.39. Se consideră o mulțime oarecare A și $\mathbb{R}^A = \{f : A \rightarrow \mathbb{R} \mid f \text{ este o funcție}\}$. Să se arate că \mathbb{R}^A este un \mathbb{R} -spațiu vectorial în raport cu adunarea vectorilor (a funcțiilor):

$$+ : \mathbb{R}^A \times \mathbb{R}^A \rightarrow \mathbb{R}^A, (f + g)(x) = f(x) + g(x), \text{ pentru orice } x \in A,$$

și cu înmulțirea cu scalari

$$\cdot : \mathbb{R} \times \mathbb{R}^A \rightarrow \mathbb{R}^A, (\alpha f)(x) = \alpha f(x), \text{ pentru orice } x \in A.$$

Exercițiu 3.1.40. Se consideră submulțimile $S = \{f \in \mathbb{R}^\mathbb{R} \mid f \text{ este pară}\}$ și $T = \{f \in \mathbb{R}^\mathbb{R} \mid f \text{ este impară}\}$ în $\mathbb{R}^\mathbb{R}$. Să se arate că $S, T \leq \mathbb{R}^\mathbb{R}$ și $S \oplus T = \mathbb{R}^\mathbb{R}$.

Exercițiu 3.1.41. Se consideră un număr prim $p \in N$. Să se arate că în orice \mathbb{Z}_p -spațiu vectorial este valabilă egalitatea $0 = x + x + \dots + x$ (p mal), pentru orice $x \in V$. Există o structură de \mathbb{Z}_p -spațiu vectorial pe grupul abelian $(\mathbb{Z}, +)$?

Exercițiu 3.1.42. Care dintre următoarele aplicații sunt liniare:

- (1) $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $f[x_1, x_2, x_3] = [x_1 - x_2, x_2 - x_3, x_3 - x_1]$.
- (2) $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $f[x_1, x_2, x_3] = [x_1 - 1, x_2 + 2, x_3 + 1]$.
- (3) $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$, $f[x_1, x_2, x_3] = [2x_1 - 3x_2 + x_3, -x_1 + x_2 + 3x_3, x_1 + x_2 + x_3]$.
- (4) $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$, $f[x_1, x_2] = [x_1 + x_2, x_1 - x_2, 2x_1 + x_2]$.
- (5) $f : \mathbb{R}^2 \rightarrow \mathbb{R}$, $f[x_1, x_2] = x_1^2 - x_2^2$.
- (6) $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $f[x_1, x_2] = [a_{1,1}x_1 + a_{2,1}x_2, a_{1,2}x_1 + a_{2,2}x_2]$, unde $a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2} \in \mathbb{R}$ sunt fixate.

Pentru aplicațiile care sunt liniare să se determine ecuațiile subspațiilor $\text{Ker } f$ și $\text{Im } f$.

3.2. Baza unui spațiu vectorial.

Independență liniară.

Definiție 3.2.1. Fie V un K -spațiu vectorial. Se numește *listă de vectori* un element $\mathbf{v} = [v_1, v_2, \dots, v_n]^t$ din $V^{n \times 1}$, unde $n \in \mathbb{N}$ este arbitrar. O listă de vectori $\mathbf{v} = [v_1, v_2, \dots, v_n]^t$ se zice *liniar independentă* dacă pentru $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ scalari avem $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n = 0 \Rightarrow \alpha_1 = \alpha_2 = \dots = \alpha_n = 0$. O listă se zice *liniar dependentă* dacă nu este liniar independentă. În acest caz o relație de dependență liniară este o egalitate de forma $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n = 0$ cu scalarii $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ nu toți nuli.

Observație 3.2.2. (1) Definiția liniar independentă unei liste $\mathbf{v} = [v_1, v_2, \dots, v_n]^t$ se poate scrie astfel:

$$[\alpha_1, \alpha_2, \dots, \alpha_n][v_1, v_2, \dots, v_n]^t = 0 \Rightarrow \alpha_1 = \alpha_2 = \dots = \alpha_n = 0.$$

Acesta este motivul pentru care luăm $[v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ în loc de $[v_1, v_2, \dots, v_n] \in V^n$.

- (2) Lista vidă de vectori este admisă (pentru $n = 0$). În particular lista vidă este liniar independentă.
- (3) O listă cu un singur element $[v_1]^t$ este exact atunci liniar independentă când $v_1 \neq 0$.
- (4) Dacă lista $[v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ conține vectorul nul $v_i = 0$, atunci ea este liniar dependentă, deoarece

$$0v_1 + \dots + 1v_i + \dots + 0v_n = 0.$$

- (5) Dacă lista $[v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ conține doi vectori egali $v_i = v_j$ cu $i \neq j$ atunci ea este liniar dependentă, deoarece

$$0v_1 + \dots + 1v_i + \dots + (-1)v_j + \dots + 0v_n = 0.$$

- (6) Uneori nu suntem interesați de ordinea vectorilor dintr-o lista $\mathbf{v} = [v_1, v_2, \dots, v_n]^t$ și spunem că vectorii v_1, v_2, \dots, v_n sunt liniar (in)dependenti în loc să spunem că lista de vectori are respectiva proprietate.

Exemplu 3.2.3. (1) Lista $[v_1, v_2, v_3]^t$ cu vectorii $v_1 = [1, 0, 1]$, $v_2 = [1, 2, 3]$ și $v_3 = v_1 + v_2 = [2, 2, 4]$ este liniar dependentă în \mathbb{R}^3 deoarece

$$1v_1 + 1v_2 + (-1)v_3 = v_1 + v_2 - v_3 = 0.$$

- (2) Lista $[e_1, e_2, e_3]^t$ cu vectorii $e_1 = [1, 0, 0]$, $e_2 = [0, 1, 0]$, $e_3 = [0, 0, 1]$ este liniar independentă în \mathbb{R}^3 .

Se spune că lista de vectori $[w_1, w_2, \dots, w_m]^t \in V^{m \times 1}$ este o sublistă a listei $[v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ dacă $\{w_1, w_2, \dots, w_m\} \subseteq \{v_1, v_2, \dots, v_n\}$. Cu alte cuvinte $[w_1, w_2, \dots, w_m]^t = [v_{i_1}, v_{i_2}, \dots, v_{i_m}]^t$, pentru anumiți indici $i_1, i_2, \dots, i_m \in \{1, \dots, n\}$.

Propoziție 3.2.4. Se consideră $\mathbf{w} = [v_{i_1}, v_{i_2}, \dots, v_{i_m}]^t \in V^{m \times 1}$ o sublistă a listei $\mathbf{v} = [v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$. Dacă \mathbf{w} este liniar dependentă, atunci tot așa este și \mathbf{v} . Echivalent, dacă \mathbf{v} este liniar independentă, atunci tot așa este și \mathbf{w} .

Demonstrație. □

Notăție 3.2.5. Fie $\mathbf{v} = [v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ o listă de vectori. Pentru $i_1, i_2, \dots, i_k \in \{1, 2, \dots, n\}$ notăm $\mathbf{v}^{\setminus i_1, i_2, \dots, i_k}$ sublistă care este obținută din \mathbf{v} prin eliminarea vectorilor $v_{i_1}, v_{i_2}, \dots, v_{i_k}$.

Pentru o listă de vectori $\mathbf{v} = [v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ scriem simplu $\langle \mathbf{v} \rangle = \langle b_1, b_2, \dots, b_n \rangle$ și vom vorbi despre spațiu generat de respectiva listă.

Propoziție 3.2.6. Fie $\mathbf{v} = [v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ o listă de vectori. Lista \mathbf{v} este exact atunci liniar dependentă când există $i \in \{1, 2, \dots, n\}$, astfel încât v_i este o combinație liniară a vectorilor din lista $\mathbf{v}^{\setminus i}$.

Demonstrație. □

Corolar 3.2.7. Fie $\mathbf{v} = [v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ o listă de vectori, astfel încât există $i \in \{1, 2, \dots, n\}$, cu proprietatea că v_i este o combinație liniară a vectorilor din lista $\mathbf{v}^{\setminus i}$ ist. Atunci $\langle \mathbf{v} \rangle = \langle \mathbf{v}^{\setminus i} \rangle$.

Demonstrație. □

Definiție 3.2.8. O submulțime finită $\{v_1, v_2, \dots, v_n\} \subseteq V$ se numește *liberă* dacă lista $[v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ este liniar independentă. O submulțime oarecare (posibil infinită) $B \subseteq V$ se numește *liberă* dacă fiecare submulțime finită a lui B este liberă.

Baze și coordinate.

Definiție 3.2.9. O bază (ordonată) a unui K -spațiu vectorial V este o listă de vectori $\mathbf{b} = [b_1, b_2, \dots, b_n]^t \in V^{n \times 1}$ astfel încât \mathbf{b} este liniar independentă și $\langle \mathbf{b} \rangle = V$ gilt (i. e. vectorii din această listă generează V).

Observație 3.2.10. (a) Adesea suntem interesați de baze care nu sunt ordonate, ceea ce înseamnă submulțimi

$$\{b_1, b_2, \dots, b_n\} \subseteq V$$

astfel încât $[b_1, b_2, \dots, b_n]^t$ este o bază (ordonată) în sensul Definiției 3.2.9.

(b) Cazul unei baze cu (posibil) o infinitate de elemente este de asemenea admis, chiar dacă noi nu îl vom studia. O bază a unui spațiu vectorial V este o submulțime $B \subseteq V$ astfel încât B este liberă și $\langle B \rangle = V$.

Exemplu 3.2.11. Lista $\mathbf{e} = [e_1, e_2, \dots, e_n]^t$ unde $e_1 = [1, 0, \dots, 0] \in K^n$, $e_2 = [0, 1, \dots, 0] \in K^n$, ..., $e_n = [0, 0, \dots, 1] \in K^n$ este o bază pentru K^n . Această bază se numește *baza canonică* a lui K^n . Baza canonică se poate scrie cu ajutorul acestor simboluri lui Kronecker:

$$e_i = [\delta_{i,j}]_{1 \leq j \leq n} \in K^n, \text{ unde } \delta_{i,j} = \begin{cases} 1 & \text{dacă } i = j \\ 0 & \text{dacă } i \neq j \end{cases} \text{ pentru orice } i \in \{1, \dots, n\}.$$

Propoziție 3.2.12. Fie V un K -spațiu vectorial și $\mathbf{b} = [b_1, b_2, \dots, b_n]^t \in V^{n \times 1}$. Următoarele afirmații sunt echivalente:

- (i) \mathbf{b} este o listă de vectori maximal liniar independentă, i. e. \mathbf{b} este liniar independentă și pentru orice $x \in V$ lista $\mathbf{b}' = [b_1, b_2, \dots, b_n, x]$ nu mai are aceeași proprietate.
- (ii) \mathbf{b} este o listă minimală cu proprietatea că generează V , i. e. $\langle \mathbf{b} \rangle = V$ și pentru oricare $i \in \{1, \dots, n\}$, avem $\langle \mathbf{b} \setminus i \rangle \neq V$.
- (iii) \mathbf{b} este o bază a lui V .

Demonstrație.

□

Definiție 3.2.13. Un K -spațiu vectorial V se numește *finit generat* dacă există o submulțime finită $\{b_1, b_2, \dots, b_n\} \subseteq V$ astfel încât $\langle b_1, b_2, \dots, b_n \rangle = V$.

Corolar 3.2.14. Orice spațiu vectorial finit generat are o bază.

Demonstrație.

□

Observație 3.2.15. Aici și în ce urmează, vom considera numai spații vectoriale finit generate. Totuși multe rezultate (de ex. Corolarul 3.2.14, Teorema 3.2.24, Corolarul 3.2.19 etc.) sunt valabile sau au un analog și în cazul spațiilor vectoriale care nu sunt finit generate.

Propoziție 3.2.16. Fie V un K -spațiu vectorial și $\mathbf{b} = [b_1, b_2, \dots, b_n]^t \in V^{n \times 1}$. Următoarele afirmații sunt echivalente:

- (i) \mathbf{b} este o bază a lui V .
- (ii) Pentru orice vector $x \in V$ există un unic sistem de scalari

$$\alpha = [\alpha_1, \dots, \alpha_n] \in K^n \text{ astfel încât } x = \alpha \mathbf{b} = \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_n b_n.$$

Demonstrație.

□

Definiție 3.2.17. Fie V un K -spațiu vectorial și $\mathbf{b} = [b_1, b_2, \dots, b_n]^t \in V^{n \times 1}$. Numim *coordonatele* unui vector $x \in V$ în raport cu \mathbf{b} scalari unic determinați $[\alpha_1, \dots, \alpha_n]$ cu proprietatea $x = \alpha_1 b_1 + \dots + \alpha_n b_n$.

Dimensiune unui spațiu vectorial.

Lemă 3.2.18. (Lema lui Steinitz) Se consideră două liste de vectori $\mathbf{v} = [v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ și $\mathbf{w} = [w_1, w_2, \dots, w_m]^t \in V^{m \times 1}$ într-un K -spațiu vectorial V , unde $n, m \in \mathbb{N}$. Dacă \mathbf{v} este liniar independentă și $\langle \mathbf{w} \rangle = V$, atunci avem $n \leq m$ și, după o eventuală renumerotare, $\langle v_1, \dots, v_n, w_{n+1}, \dots, w_m \rangle = V$.

Demonstrație. □

Corolar 3.2.19. Oricare două baze ale unui K -spațiu vectorial (finit generat) au același număr de elemente.

Demonstrație. □

Definiție 3.2.20. Prin definiție dimensiunea unui K -spațiu vectorial (finit generat) V este numărul elementelor unei baze a (prin urmare a tuturor bazelor) lui V . Se scrie $\dim_K V$ sau simplu $\dim V$. De acum nu vom mai vorbi despre spații finit generate, și vom folosi noțiunea echivalentă (dar mai elegantă) de spații finit dimensionale.

Exemplu 3.2.21. (1) $\dim 0 = 0$.

(2) $\dim_K K^n = n$; în particular $\dim_{\mathbb{R}} \mathbb{R} = 1$, $\dim_{\mathbb{R}} \mathbb{R}^2 = 2$, $\dim_{\mathbb{R}} \mathbb{R}^3 = 3$

Observație 3.2.22. Următoarele afirmații sunt adevărate arate într-un spațiu finit dimensional:

- (a) Orice listă liniar independentă se poate completa până la o bază.
- (b) Din orice listă care generază pe V se poate extrage o bază.
- (c) $\dim V$ este cel mai mare număr de vectori liniar independenti care există în V .
- (d) $\dim V$ este cel mai mic număr de elemente a unei liste care generează V .

Propoziție 3.2.23. Fie V un K -spațiu vectorial cu $\dim_K V = n$ și $\mathbf{b} = [b_1, b_2, \dots, b_n] \in V^{n \times 1}$ o listă de vectori. Următoarele afirmații sunt echivalente:

- (i) \mathbf{b} este liniar independentă.
- (ii) $\langle \mathbf{b} \rangle = V$.
- (iii) \mathbf{b} este o bază.

Demonstrație. □

Proprietatea de universalitate a bazei unui spațiu vectorial.

Teoremă 3.2.24. [Proprietatea de universalitate a bazei] Fie V și W două K -spații vectoriale și $\mathbf{v} = [v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ o bază a lui V . Pentru orice funcție $f : \{v_1, v_2, \dots, v_n\} \rightarrow W$ există o aplicație liniară unică $\bar{f} : V \rightarrow W$ astfel încât $\bar{f}(v_i) = f(v_i)$ pentru orice $1 \leq i \leq n$ (i. e. \bar{f} prelungește pe f sau f este o restricție a lui \bar{f}).

Demonstrație. □

Corolar 3.2.25. Fie V și W două K -spații vectoriale și $\mathbf{v} = [v_1, v_2, \dots, v_n]^t \in V^{n \times 1}$ o bază a lui V .

- (a) Dacă $f, g : V \rightarrow W$ sunt aplicații liniare astfel încât $f(v_i) = g(v_i)$ pentru orice $1 \leq i \leq n$, atunci $f = g$.
- (b) Dacă $\dim_K W = n$ atunci $V \cong W$.
- (c) $V \cong K^n$.

Formule legate de dimensiune.

Propoziție 3.2.26. Se consideră un K -spațiu vectorial V și $S, T \leq_K$ două subspații. Avem:

$$\dim S + \dim T = \dim(S + T) - \dim(S \cap T).$$

Demonstrație.

□

Corolar 3.2.27. Dacă V este un K -spațiu vectorial finit dimensional și $S \leq_K V$, atunci $\dim S \leq \dim V$. Mai mult, $\dim S = \dim V$ dacă $S = V$.

Demonstrație.

□

Propoziție 3.2.28. Fie $f : V \rightarrow W$ o aplicație liniară între două K -spații vectoriale V și W . Atunci:

$$\dim V = \dim \text{Ker } f + \dim \text{Im } f.$$

Demonstrație.

□

Corolar 3.2.29. Fie V și W două K -spații vectoriale cu $\dim V = \dim W$ și $f : V \rightarrow W$ o aplicație liniară. eine lineare Abbildung. Următoarele afirmații sunt echivalente:

- (i) f este injectivă.
- (ii) f este surjectivă.
- (iii) f este bijectivă.

Demonstrație.

□

Lema substituției.

Teoremă 3.2.30. (Lema substituției) Fie $\mathbf{b} = [b_1, b_2, \dots, b_n]^t$ o bază a K -spațiului vectorial V și $v \in V$ cu coordonatele $[\alpha_1, \alpha_2, \dots, \alpha_n]$ în raport cu baza \mathbf{b} (i. e. $v = \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_n b_n$). Considerăm lista de vectori $\mathbf{v}' = [b_1, \dots, v, \dots, b_n]$ care rezultă din \mathbf{v} prin înlocuirea (substituția) vectorului b_i cu v . Atunci:

- (a) \mathbf{b}' este o bază dacă $\alpha_i \neq 0$.
- (b) Dacă \mathbf{b}' este o bază și $x \in V$ are coordonatele $[x_1, x_2, \dots, x_n]$ în raport cu \mathbf{v}' și $[x'_1, x'_2, \dots, x'_n]$ în raport cu \mathbf{v}' atunci:

$$\begin{cases} x'_i = \alpha_i^{-1} x_i \\ x'_j = \alpha_i^{-1} (\alpha_i x_j - \alpha_j x_i) \text{ pentru } j \neq i \end{cases}.$$

Demonstrație.

□

Definiție 3.2.31. Se numește rangul unei liste de vectori $\mathbf{v} = [v_1, \dots, v_n]^t$ dimensiunea spațiului generat de \mathbf{v} , i. e. $\text{rank } \mathbf{v} = \dim \langle \mathbf{v} \rangle$.

Observație 3.2.32. Deoarece orice listă liniar independentă se poate completa până la o bază, se poate folosi lema substituției pentru a calcula rangul unei liste de vectori.

Exerciții la Baze.

Exercițiu 3.2.33. Să se arate că o listă cu doi vectori $[x, y]^t \in V^{2 \times 1}$ este exact atunci liniar dependentă când există $\alpha \in K$ astfel încât $x = \alpha y$ sau $y = \alpha x$. Să se găsească interpretarea geometrică în cazul $K = \mathbb{R}$, și $V = \mathbb{R}^3$. Când este o listă de vectori $[x, y, z]^t \in (\mathbb{R}^3)^{3 \times 1}$ liniar dependentă?

Exercițiu 3.2.34. Fie V un K -spațiu vectorial cu $\dim V = n$. Să se arate că pentru orice număr natural $m \leq n$ există un subspațiu $S \leq_K V$ astfel încât $\dim S = m$.

Exercițiu 3.2.35. Fie $f : V \rightarrow W$ o aplicație liniară și $X \subseteq V$. Să se arate că $f(\langle X \rangle) = \langle f(X) \rangle$.

Exercițiu 3.2.36. Să se arate că $\mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ este un \mathbb{Q} -spațiu vectorial și să se determine o bază și dimensiunea.

Exercițiu 3.2.37. Fie p un număr prim. Să se arate că

$$\mathbb{Q} + \mathbb{Q}\sqrt[3]{p} + \mathbb{Q}\sqrt[3]{p^2} = \{a + b\sqrt[3]{p} + \sqrt[3]{p^2} \mid a, b, c \in \mathbb{Q}\}$$

este un \mathbb{Q} -spațiu vectorial și să se determine o bază și dimensiunea.

Exercițiu 3.2.38. Fie $f : V \rightarrow W$ o aplicație liniară și $\mathbf{v} = [v_1, \dots, v_n]^t \in V^{n \times 1}$ o listă de vectori. Notăm $f(\mathbf{v}) = [f(v_1), \dots, f(v_n)]^t \in W^{n \times 1}$. Atunci:

- (a) dacă f este injectiv și \mathbf{v} este liniar independentă atunci $f(\mathbf{v})$ are aceeași proprietate.
- (b) Dacă f este surjectiv și $\langle \mathbf{v} \rangle = V$, atunci $\langle f(\mathbf{v}) \rangle = W$.
- (c) Dacă f este bijectiv și \mathbf{v} este o bază a lui V atunci $f(\mathbf{v})$ este de asemenea o bază (a lui W).

Exercițiu 3.2.39. Pentru un K -spațiu vectorial V cu $\dim V = n$ și $S \leq_K V$, să se arate că există $T \leq_K V$ astfel încât $S \oplus T = V$.

Exercițiu 3.2.40. Se consideră în \mathbb{R}^3 lista de vectori $\mathbf{v} = [v_1, v_2, v_3]^t$. Folosind două metode (definiția bazei respectiv lema substituției) să se găsească $a \in \mathbb{R}$ astfel încât \mathbf{v} este o bază a lui \mathbb{R}^3 , unde:

- (1) $v_1 = [1, -2, 0]$, $v_2 = [2, 1, 1]$, $v_3 = [0, a, 1]$.
- (2) $v_1 = [2, 1, -1]$, $v_2 = [0, 3, -1]$, $v_3 = [1, a, 1]$.

Exercițiu 3.2.41. Să se arate că $\mathbf{b} = [b_1, b_2, b_3, b_4]^t$ unde

$$b_1 = [1, 2, -1, 2], b_2 = [1, 2, 1, 4], b_3 = [2, 3, 0, -1], b_4 = [1, 3, -1, 0]$$

este o bază a lui \mathbb{R}^4 și să se determine coordonatele lui $x = [2, 3, 2, 10]$ în raport cu acea bază.

Exercițiu 3.2.42. Să se determine $a \in \mathbb{R}$ astfel încât lista $\mathbf{v} = [v_1, v_2, v_3]^t$ este o bază a lui \mathbb{R}^3 , unde:

$$v_1 = (a, 1, 1), v_2 = (1, a, 1), v_3 = (1, 1, a).$$

Exercițiu 3.2.43. Să se determine rangul listelor de vectori din \mathbb{R}^4 :

- (1) $[[0, 1, 3, 2], [1, 0, 5, 1], [-1, 0, 1, 1], [3, -1, -3, -4], [2, 0, 1, -1]]^t$;
- (2) $[[1, 2, 3, 0], [0, 1, -1, 1], [3, 7, 8, 1], [1, 3, 2, 1]]^t$;
- (3) $[[1, 2, -1, 2], [2, 3, 0, -1], [2, 4, 0, 6], [1, 2, 1, 4], [3, 6, -1, -1], [1, 3, -1, 0]]^t$.

Exercițiu 3.2.44. Se consideră subspațiile

$$S = \langle [2, 0, 1, -1], [0, 1, 2, 3], [-1, 0, 1, 1], [1, 1, 5, 2] \rangle$$

$$T = \langle [1, 0, 2, 0], [2, 1, -1, 2], [-1, -1, 3, -2] \rangle$$

ale spațiului vectorial real \mathbb{R}^4 . Să se folosească lema substituției pentru a determina dimensiunea și câte o bază în subspațiile S , T , $S + T$ și $S \cap T$.

Exercițiu 3.2.45. Folosind lema substituției să se calculeze dimensiunea și câte o bază a subspațiilor $\text{Ker } f$ și $\text{Im } f$, în cazurile:

- (1) $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ $f[x_1, x_2, x_3] = [x_1 + 2x_2, x_2 + x_3, x_1 - 2x_3]$.
- (2) $f : \mathbb{R}^4 \rightarrow \mathbb{R}^3$ $f[x_1, x_2, x_3, x_4] = [x_1 - x_2 - x_3, 3x_2 + x_4, 3x_1 - 3x_3 + x_4]$
- (3) $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ $f[x_1, x_2, x_3] = [-x_1 + 2x_2, x_1 - x_2 + x_3, x_2 + 2x_3]$.
- (4) $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ $f[x_1, x_2] = [x_1 - 3x_2, 2x_1, -x_1 + x_2]$.
- (5) $f : \mathbb{R}^4 \rightarrow \mathbb{R}^4$ $f[x_1, x_2, x_3, x_4] = [x_1 + 2x_2 + x_3 - x_4, x_1 + 2x_2 - x_3 + x_4, x_1 + 2x_2, x_3 - x_4]$.

3.3. Aplicații liniare și matrici.

Matricea unei liste de vectori. În cele ce urmează se consideră un K -spațiu vectorial V cu $\dim_K V = n$. Reamintim că dacă $\mathbf{b} = [b_1, b_2, \dots, b_n]^t$ o bază a lui V și $x \in V$, atunci coordonatele lui x în baza \mathbf{b} sunt scalarii unic determinați $[x_1, x_2, \dots, x_n] \in K^n$ cu proprietatea

$$x = x_1 b_1 + x_2 b_2 + \dots + x_n b_n = [x_1, x_2, \dots, x_n] [b_1, b_2, \dots, b_n]^t.$$

Notăm $[x]_{\mathbf{b}} = [x_1, x_2, \dots, x_n]$ și egalitatea de mai sus se scrie $x = [x]_{\mathbf{b}} \mathbf{b}$.

Definiție 3.3.1. Fie V un K -spațiu vectorial cu $\dim_K V = n$. Fie $\mathbf{b} = [b_1, b_2, \dots, b_n]^t$ o bază a lui V și $x \in V$. Coordonatele lui x în baza \mathbf{b} sunt scalarii $\mathbf{v} = [v_1, v_2, \dots, v_m]^t$ un sistem de vectori. Prin matricea listei \mathbf{v} în baza \mathbf{b} se înțelege:

$$[\mathbf{v}]_{\mathbf{b}} = [[v_1]_{\mathbf{b}}, [v_2]_{\mathbf{b}}, \dots, [v_m]_{\mathbf{b}}]^t \in \mathbb{M}_{m \times n}(K).$$

Cu alte cuvinte

$$[\mathbf{v}]_{\mathbf{b}} = \begin{bmatrix} [v_1]_{\mathbf{b}} \\ [v_2]_{\mathbf{b}} \\ \vdots \\ [v_m]_{\mathbf{b}} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

unde $v_i = a_{i1} b_1 + a_{i2} b_2 + \dots + a_{in} b_n$ pentru $1 \leq i \leq m$.

Propoziție 3.3.2. Fie V un K -spațiu vectorial cu $\dim_K V = n$. Fie $\mathbf{e} = [e_1, e_2, \dots, e_n]^t$ o bază și fie $\mathbf{b} = [b_1, b_2, \dots, b_n]$ un sistem de vectori în V . Atunci \mathbf{b} este bază dacă $[\mathbf{b}]_{\mathbf{e}} \in GL_n(K)$ (adică $[\mathbf{b}]_{\mathbf{e}}$ este inversabilă), și în acest caz pentru $x \in V$ avem

$$[x]_{\mathbf{b}} = [x]_{\mathbf{e}} [\mathbf{b}]_{\mathbf{e}}^{-1}.$$

În particular avem $[\mathbf{e}]_{\mathbf{b}} = [\mathbf{b}]_{\mathbf{e}}^{-1}$.

Demonstrație. □

Observație 3.3.3. Dacă $\mathbf{e} = [e_1, e_2, \dots, e_n]^t$ și $\mathbf{b} = [b_1, b_2, \dots, b_n]$ sunt baze, iar $\mathbf{v} = [v_1, v_2, \dots, v_m]$ este un sistem de vectori în V atunci

$$[\mathbf{v}]_{\mathbf{b}} = [\mathbf{v}]_{\mathbf{e}} [\mathbf{b}]_{\mathbf{e}}^{-1}.$$

Observație 3.3.4. Dacă $\mathbf{v} = [v_1, v_2, \dots, v_m]^t$ este un sistem de vectori iar $\mathbf{b} = [b_1, b_2, \dots, b_m]^t$ este o baza a K -spațiului vectorial V atunci:

$$\text{rank } \mathbf{v} = \text{rank}[\mathbf{v}]_{\mathbf{b}}.$$

Matricea unei aplicații liniare.

Definiție 3.3.5. Se consideră K -spațiile vectoriale V și W cu $\dim_K V = m$ și $\dim_K W = n$. Prin *matricea unei aplicații liniare* $f \in \text{Hom}_K(V, M)$ în raport cu perechea de baze $\mathbf{v} = [v_1, v_2, \dots, v_m]$ a lui V și $\mathbf{w} = [w_1, w_2, \dots, w_n]$ a lui W înțelegem

$$[f]_{\mathbf{v}, \mathbf{w}} = [f(\mathbf{v})]_{\mathbf{w}} \in \mathbb{M}_{m \times n}(K),$$

unde prin $f(\mathbf{v})$ am notat sistemul de vectori $[f(v_1), f(v_2), \dots, f(v_m)]^t$ în W . Cu alte cuvinte

$$[f]_{\mathbf{v}, \mathbf{w}} = \begin{bmatrix} [f(v_1)]_{\mathbf{w}} \\ [f(v_2)]_{\mathbf{w}} \\ \vdots \\ [f(v_m)]_{\mathbf{w}} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

unde $f(v_i) = a_{i1}w_1 + a_{i2}w_2 + \dots + a_{in}w_n$ pentru $1 \leq i \leq m$.

Propoziție 3.3.6. Se consideră K -spațiile vectoriale V , W și U cu $\dim_K V = m$, $\dim_K W = n$ și $\dim_K U = p$, împreună cu bazele $\mathbf{v} = [v_1, v_2, \dots, v_m]$, $\mathbf{w} = [w_1, w_2, \dots, w_n]$ și $\mathbf{u} = [u_1, u_2, \dots, u_p]$ în V , W , respectiv U . Dacă $\alpha \in K$, $f, f \in \text{Hom}_K(V, W)$ și $g \in \text{Hom}_K(W, U)$ atunci avem:

- (a) $[f + f']_{\mathbf{v}, \mathbf{w}} = [f]_{\mathbf{v}, \mathbf{w}} + [f']_{\mathbf{v}, \mathbf{w}}$.
- (b) $[\alpha f]_{\mathbf{v}, \mathbf{w}} = \alpha[f]_{\mathbf{v}, \mathbf{w}}$.
- (c) $[g \circ f]_{\mathbf{v}, \mathbf{u}} = [f]_{\mathbf{v}, \mathbf{w}} \cdot [g]_{\mathbf{w}, \mathbf{u}}$.

Demonstrație.

□

Teoremă 3.3.7. Se consideră K -spațiile vectoriale V și W cu $\dim_K V = m$, $\dim_K W = n$, împreună cu bazele $\mathbf{v} = [v_1, v_2, \dots, v_m]$ și $\mathbf{w} = [w_1, w_2, \dots, w_n]$. Atunci

- (a) Aplicația $\varphi : \text{Hom}_K(V, W) \rightarrow \mathbb{M}_{m \times n}(K)$, $\varphi(f) = [f]_{\mathbf{v}, \mathbf{w}}$ este un izomorfism de spații vectoriale.
- (b) Aplicația $\varphi : \text{End}_K(V) \rightarrow \mathbb{M}_{m \times n}(K)^o$, $\varphi(f) = [f]_{\mathbf{v}, \mathbf{v}}$ este un izomorfism de inele.

Demonstrație.

□

Observație 3.3.8. Pentru $f \in \text{End}_K(V)$ vom nota uneori $[f]_{\mathbf{v}} = [f]_{\mathbf{v}, \mathbf{v}}$ (ca și $\mathbb{M}_n(K)$ în loc de $\mathbb{M}_{n \times n}(K)$).

Teoremă 3.3.9 (Formula schimbării de bază). Se consideră K -spațiile vectoriale V și W cu $\dim_K V = m$, $\dim_K W = n$, împreună cu bazele $\mathbf{v} = [v_1, v_2, \dots, v_m]$, $\mathbf{v}' = [v'_1, v'_2, \dots, v'_m]$ în V și $\mathbf{w} = [w_1, w_2, \dots, w_n]$, $\mathbf{w}' = [w'_1, w'_2, \dots, w'_n]$ în W . Dacă $f \in \text{Hom}_K(V, W)$ atunci avem

$$[f]_{\mathbf{v}' \mathbf{w}'} = [\mathbf{v}']_{\mathbf{v}} \cdot [f]_{\mathbf{v}, \mathbf{w}} \cdot [\mathbf{w}']_{\mathbf{w}}^{-1}.$$

Demonstrație.

□

Exerciții la Aplicatii liniare si matrici.

Exercițiu 3.3.10. Fie $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$, $f[x_1, x_2, x_3] = [x_2, -x_1]$ și $\mathbf{v} = [[1, 1, 0], [0, 1, 1], [1, 0, 1]]^t$ și $\mathbf{w} = [[1, 1], [1, -2]]^t$.

- (a) Să se arate că $f \in \text{Hom}_{\mathbb{R}}(\mathbb{R}^3, \mathbb{R}^2)$.
- (b) Să se arate că \mathbf{v} și \mathbf{w} sunt baze în \mathbb{R}^3 , respectiv \mathbb{R}^2 și să se determine matricile $[f]_{\mathbf{v}, \mathbf{e}}$ și $[f]_{\mathbf{v}, \mathbf{w}}$, unde \mathbf{e} este baza canonica din \mathbb{R}^2 .
- (c) Să se determine dimensiunea și câte o bază în $\text{Ker}(f)$ și $\text{Im}(f)$.

Exercițiu 3.3.11. Fie $f : \mathbb{R}^4 \rightarrow \mathbb{R}^4$, $f[x_1, x_2, x_3, x_4] = [x_1 + 2x_2 + x_3 + x_4, 3x_1 + 7x_2 + 5x_3 + 2x_4, x_1 + 3x_2 + 3x_3, 4x_1 + 9x_2 + x_3 + 8x_4]$ și $\mathbf{e} = [e_1, e_2, e_3, e_4]^t$ baza canonica în \mathbb{R}^4 .

- (a) Să se arate că $f \in \text{End}_{\mathbb{R}}(\mathbb{R}^4)$.
- (b) să se determine matricea $[f]_{\mathbf{e}}$.
- (c) Să se arate că $\mathbf{b} = [b_1, b_2, b_3, b_4]^t$, unde $b_1 = e_1, b_2 = e_1 + e_2, b_3 = e_1 + e_2 + e_3, b_4 = e_1 + e_2 + e_3 + e_4$ este o bază în \mathbb{R}^4 , și să se determine $[f]_{\mathbf{b}}$ și $[v]_{\mathbf{b}}$ unde $v = [1, 2, -1, 0]$.
- (d) Să se determine dimensiunea și câte o bază în $\text{Ker}(f)$ și $\text{Im}(f)$.

3.4. Diagonalizarea unui endomorfism de spații vectoriale. În cele ce urmează fixăm un K -spațiu vectorial V , cu $\dim_K V = n \geq 1$, și un endomorfism $f \in \text{End}_K(V)$.

Propoziție 3.4.1. Pentru orice $\lambda \in K$, mulțimea $V(\lambda) = \{x \in V \mid f(x) = \lambda x\}$ este un subspațiu vectorial al lui V .

Demonstrație.

□

Observație 3.4.2. Avem $V(\lambda) = \text{Ker}(\lambda 1_V - f)$.

Spunem că $\lambda \in K$ este o *valoare proprie* pentru f dacă ecuația $f(x) = \lambda x$ are soluții nenule în V , cu alte cuvinte dacă $V(\lambda) \neq 0$. În acest caz, o soluție nenulă a acestei ecuații, adică un vector $0 \neq x \in V(\lambda)$ se numește *vector propriu* asociat valorii proprii λ . O matrice se zice *diagonală* dacă este de forma

$$\text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix}$$

Spunem că f este *diagonalizabil* dacă există o bază b a lui V astfel încât $[f]_b$ este diagonală.

Teoremă 3.4.3. Fie $b = [b_1, b_2, \dots, b_n]^t$ o bază a lui V . Atunci

$$[f]_b = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$$

dacă $\lambda_1, \lambda_2, \dots, \lambda_n$ sunt valori proprii ale lui f (nu neapărat distințe) iar b_i , $1 \leq i \leq n$ sunt vectori proprii corespunzători acestor valori proprii. Așadar $f \in \text{End}_K(V)$ este diagonalizabil dacă există o bază a lui V constituită din vectori proprii, cauză în care matricea lui f în această bază are pe diagonală valorile proprii respective.

Demonstrație.

□

Polinomul caracteristic al lui f este definit prin $p_f(t) = \det(tI_n - A)$ unde $A = [f]_e$ este matricea lui f într-o bază e a lui V .

Propoziție 3.4.4. *Polinomul caracteristic al lui f nu depinde de baza în care calculăm matricea lui f , mai precis dacă e și e' sunt baze pentru V și $A = [f]_e$, $A' = [f]_{e'}$, atunci $\det(tI_n - A) = \det(tI_n - A')$.*

Demonstrație. □

Exemplu 3.4.5. Pentru $n = 2$ și $[f]_e = A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ avem

$$p_f(t) = \begin{vmatrix} t-a & -b \\ -c & t-d \end{vmatrix} = t^2 - (a+d)t + (ad-bc) = t^2 - \text{trace}(A)t + \det(A).$$

Prinț-un ușor abuz de limbaj vorbim uneori de polinomul caracteristic al matricii $A = [f]_e$ în loc de polinomul catasteristic al endomorfismului f și scriem $p_A(t)$ în loc de $p_f(t)$. Același lucru este valabil și pentru vectori și valori proprii.

Observație 3.4.6. Avem:

- (a) $\deg p_f = n$.
- (b) Dacă $p_f(t) = p_0 + p_1t + \cdots + p_{n-1}t^{n-1} + p_nt^n$ atunci $p_n = 1$, $p_{n-1} = -\text{trace}(A)$, $p_0 = (-1)^n \det(A)$.

Propoziție 3.4.7. $\lambda \in K$ este valoare proprie a lui f dacă și numai dacă λ este rădăcină a polinomului caracteristic al lui f adică $p_f(\lambda) = 0$.

Demonstrație. □

Corolar 3.4.8. Endomorfismul f are cel mult n valori proprii distincte.

Numim *multiplicitate algebraică* a valorii proprii $\lambda \in K$ a lui f , multiplicitatea lui λ ca rădăcină a polinomului $p_f(t)$ și o notăm cu $m(\lambda)$. Numim *multiplicitate geometrică* a valorii proprii $\lambda \in K$ a lui f dimensiunea $d(\lambda) = \dim V(\lambda)$.

Observație 3.4.9. Pentru orice valoare proprie $\lambda \in K$ a lui f avem $1 \leq m(\lambda)$ și $m(\lambda)$ este cel mai mare exponent $m \in \mathbb{N}$ cu proprietatea $(t - \lambda)^m \mid p_f(t)$, adică $(t - \lambda)^{m(\lambda)} \mid p_f(t)$, iar $(t - \lambda)^{m(\lambda)+1} \nmid p_f(t)$.

Propoziție 3.4.10. Pentru orice valoare proprie $\lambda \in K$ a lui f avem

$$1 \leq d(\lambda) \leq m(\lambda).$$

Demonstrație. □

Lemă 3.4.11. Dacă $\lambda_1, \lambda_2, \dots, \lambda_r$ sunt valori proprii distincte pentru f și $0 \neq b_i \in V(\lambda_i)$, cu $1 \leq i \leq r$, sunt vectori proprii corespunzători, atunci b_1, b_2, \dots, b_n sunt liniar independenți.

Demonstrație. □

Teoremă 3.4.12. Următoarele afirmații sunt echivalente:

- (i) f este diagonalizabil.
- (ii) f are toate valorile proprii în K și pentru orice valoare proprie λ a lui f este valabilă egalitatea $d(\lambda) = m(\lambda)$.

în cazul în care f este diagonalizabil, matricea diagonală care îl reprezintă pe f are pe diagonală valorile proprii ale lui f , fiecare valoare proprie apărând de atâtea ori cât ordinul ei de multiplicitate.

Demonstrație.

□

Corolar 3.4.13. *Dacă f are n valori proprii distințe în K atunci f este diagonalizabil.*

Ideea algoritmului Page Ranking. (Larry Page - cofondator Google).

Înălțări: Cum se măsoară importanța unei pagini de internet? R: Importanța unei pagini de internet depinde de numărul de linkuri care trimit la aceea pagină, dar și de importanța paginilor care trimit linkuri către acea pagină. Într-un anume fel o pagină “moștenește” din importanța paginilor care trimit la ea.

Considerăm o rețea formată din paginile p_1, p_2, \dots, p_n . Căutăm o măsură a importanței de forma $I : \{p_1, p_2, \dots, p_n\} \rightarrow \mathbb{R}$, care crește direct proporțional cu importanța respectivei pagini. Dacă de la o pagină p_i pleacă l_i linkuri către paginile $p_{j_1}, p_{j_2}, \dots, p_{j_{l_i}}$ atunci fiecareia dintre aceste pagini își transferă o parte din importanța paginii p_i . Avem astăzi

$$I(p_j) = \sum \frac{I(p_i)}{l_i}$$

unde suma se face după toate paginile care trimit către p_j . Cu ajutorul numărului de linkuri (care se poate determina) se construiește matricea $L \in \mathbb{M}_{n \times n}(\mathbb{R})$ care are pe linia i exact l_i elemente egale cu $\frac{1}{l_i}$ corespunzătoare celor l_i pagini către care trimit pagina p_i , restul elementelor de pe linie fiind 0. Se observă că suma elementelor de pe linia i este 1. Egalitatea de mai sus se scrie matricial

$$[I(p_1), I(p_2), \dots, I(p_n)] = [I(p_1), I(p_2), \dots, I(p_n)]L,$$

adică $[I(p_1), I(p_2), \dots, I(p_n)]$ este un vector propriu al lui L corespunzător valorii proprii 1.

Ești așadar util să avem metode care să determine vectorii și valorile proprii ale unei matrici!

Exerciții la Diagonalizare.

Exercițiu 3.4.14. Să se diagonalizeze endomorfismul f (adică să se spună dacă f este diagonalizabil și în caz afirmativ să se găsească matricea diagonală care îl reprezintă pe f precum și baza în care f are această matrice) în următoarele cazuri:

(a) $f \in \text{End}_{\mathbb{R}}(\mathbb{R}^3)$, $f(x_1, x_2, x_3) = (3x_1 + x_2, -4x_1 - x_2, -4x_1 - 8x_2 - 2x_3)$.

(b) $f \in \text{End}_{\mathbb{R}}(\mathbb{R}^4)$ cu matricea (în baza canonică) $[f]_e = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$.

(c) $f \in \text{End}_{\mathbb{R}}(\mathbb{R}^3)$, $f(x_1, x_2, x_3) = (x_1 + 3x_3, x_2, 3x_1 - x_3)$. În acest caz să se calculeze f^n cu $n \in \mathbb{N}$.

(d) $f \in \text{End}_{\mathbb{R}}(\mathbb{R}^4)$ cu matricea (în baza canonică) $[f]_e = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

Exercițiu 3.4.15. Să se arate că o matrice cu proprietatea că suma elementelor de pe fiecare linie este 1 admite valoarea proprie 1.

Exercițiu 3.4.16. Fie $A \in \mathbb{M}_{n \times n}(\mathbb{C})$, cu valorile proprii $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{C}$.

(a) Să se arate că $\det(A) = 0$ dacă A are valoarea proprie $\lambda = 0$.

- (b) Să se determine valorile proprii ale matricilor A^m , unde $m \in \mathbb{N}$ și A^{-1} (dacă această matrice există).

Exercițiu 3.4.17. Pentru o matrice $A \in \mathbb{M}_{n \times n}(\mathbb{C})$, să se arate că următoarele afirmații sunt echivalente:

- (i) A este nilpotentă.
- (ii) $p_A(t) = t^n$.
- (iii) A are o singură valoare proprie $\lambda = 0$ cu ordinul de multiplicitate $m(0) = n$.

UNIVERSITATEA BABEŞ-BOLYAI, FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ, STR. MIHAIL KOGĂLNICEANU 1, 400084 CLUJ-NAPOCA, ROMÂNIA

E-mail address: cmodoi@math.ubbcluj.ro