ALGEBRA PENTRU INFORMATICĂ

GEORGE CIPRIAN MODOI

Cuprins

Bibliografie	2
1. Mulţimi, Funcţii, Relaţii	3
1.1. Preliminarii logice	3
Exerciţii la Preliminarii logice	3
1.2. Mulţimi	3
Operaţii cu mulţimi	4
Exerciţii la Mulţimi	6
1.3. Funcţii	6
Injectivitate, surjectivitate, bijectivitate	8
Cardinalul unei mulţimi	9
Produsul cartezian	9
Operaţii	10
Exerciţii la funcţii	11
1.4. Relaţii	13
Relaţii de echivalenţă	15
Relaţii de ordine	16
Exerciţii la Relaţii	18
2. Grupuri, inele, corpuri	20
2.1. Grupuri	20
Subgrupuri	21
Homomorfisme de grupuri	22
Grupuri ciclice şi ordinul unui element	23
Acţiuni ale grupurilor pe mulţimi	23
Grupul simetric	24
Exerciţii la grupuri	25
2.2. Inele şi corpuri	28
Subinele şi subcorpuri	29
Homomorfisme	30
Elemente speciale într-un inel	31
Exerciţii la inele şi corpuri	32
3. Algebra liniara	33
3.1. Spaţii vectoriale si aplicaţii liniare	34
Subspaţii vectoriale	35
Suma şi suma directă a subspaţiilor	36
Aplicaţii liniare	37
Exerciţii la spaţii vectoriale	38
3.2. Baza unui spaţiu vectorial	39
Independenţă liniară	39

Baze şi coordonate 40
Dimensiune unui spaţiu vectorial 42
Proprietatea de universalitate a bazei unui spaţiu vectorial 42
Formule legate de dimensiune 43
Lema substituţiei 43
Exerciţii la Baze 44
3.3. Aplicaţii liniare şi matrici 45
Matricea unei liste de vectori 45
Matricea unei aplicaţii liniare 46
Exerciţii la Aplicatii liniare si matrici 47
3.4. Diagonalizarea unui endomorfism de spaţii vectoriale 47
Ideea algoritmului Page Ranking 49
Exerciţii 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. Coconeţ, C. Conţiu, *Lecţii 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, *Algbera*, Editura Did. Ped. Bucureşti, 1970.
[6] I. D. Ion, N. Radu, C. Niţă, D. Popescu, *Probleme de algebră*, Ed. Did. Ped., Bucureşti, 1970.
[7] B. Külshammer, *Lineare Algebra und Analytische Geometrie*, Vorlesungsskripte, `https://www.minet.uni-jena.de//algebra//skripten/skripten.html`.
[8] C. Năstăsescu, C. Niţă, C. Vraciu, Bazele algebrei, Ed. Academiei, 1986.
[9] C. Năstăsescu, C. Niţă, M. Brandiburu, D. Joiţa, *Exerciţii şi probleme de algebră*, Ed. Did. Ped. Bucureşti, 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, Bucureşti, 1977.
[13] A. E. Schroth, *Algebra für die Studierende der Informatik*, Vorlesungsskripte, `http://www.carsten-buschmann.de/skripte/Algera_fuer_Informatiker.pdf`.

1. Mulţimi, Funcţii, Relaţii

1.1. **Preliminarii logice.** Propoziţiile logice sunt numai acele propoziţii care pot fi adevărate sau false; celelalte propoziţii gramaticale precum întrebarile, exclamaţiile etc., care nu pot fi adevarate sau false, nu sunt incluse printre propoziţiile logice. Propoziţiile sunt conectate de operatori, dintre care noi vom folosi următorii:

- Negare $\neg$
- şi logic $\wedge$
- sau logic (neexclusiv) $\vee$
- sau exclusiv $\oplus$
- implicaţia logică $\Rightarrow$
- echivalenţa logică $\Leftrightarrow$

Acestri operatori sunt definiţi prin următoarele tabele de avedăr: (aici p şi q sunt propoziţii, iar 0 şi 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

Exerciţii la Preliminarii logice.

Exerciţiu 1.1.1. Să se arate că urmatoarele formule propoziţionale sunt tautologii, adică ele sunt întotdeauna adevărate, indiferent de valoarea de adevăr a propoziţiilor p, q r:

(a) $((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$
(b) $((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$ $\vee$ 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. **Mulţimi.** Mulţimea este o colecţie de obiecte distincte si bine determinate (care obiecte sunt numite *elemente*). Mulţimile pot fi date în mod direct prin enumerarea explicită a elementelor lor (altfel spus *sintetic*) sau prin precizarea unei condiţii (proprietăţi) pe care trebuie să o îndeplinească (adică *analitic*). Vom scrie $x \in A$ (şi vom spune că "x aparţine mulţimii A) pentru a exprima faptul ca x este un element al mulţimii A. De notat că noţiunile "mulţime" şi "apartenenţă" sunt primare, adică ele nu se definesc.

Exemplu 1.2.1. a) $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, $C = \{?, 7, *, \vee\}$, $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.
b) $Z = \{x \mid x \in \mathbb{N}$ şi $0 \leq x < 10\}$, $[-3, 8) = \{x \mid x \in \mathbb{R}$ şi $-3 \leq x < 8\}$.
c) Alte exemple ...

Definiţie 1.2.2. Două mulţimi sunt egale exact atunci când ele conţin aceleaşi elemente.

Dem 1.28

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

$p \Rightarrow p$

p	$p \Rightarrow p$
0	1
1	1

Deci $A \subseteq A$

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

Pt. a demonstra $A \subseteq B$ și $B \subseteq C \Rightarrow A \subseteq C$

verificăm cu tabela de adevăr

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

(c) la fel ca (b)

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

$p = \perp$ (contradicție = întotdeauna false)

Falsul implică orice deci

$p \Rightarrow q$ este adevărată.

(e) Fie $\emptyset$ și $\emptyset'$ două mulțimi vide.

Cf (d) $\left.\begin{array}{l} \emptyset \subseteq \emptyset' \\ \emptyset' \subseteq \emptyset' \end{array}\right\} \overset{(c)}{\Longrightarrow} \emptyset = \emptyset'$.

$C_U(A \cup B) = C_U A \cap C_U B$

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

Observaţie 1.2.4. a) Elementele unei mulţimi 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 mulţime un element apare numai o dată: $\{1,2\}$ şi NU $\{1,2,2,1\}$.

c) Definirea analitică a unei mulţimi necesită precauţii suplimentare. De exemplu construcţia: $R = \{x \mid x \notin x\}$ conduce la un paradox. Mai precis, amândouă propoziţiile $R \in R$ şi $R \notin R$ conduc la o contradicţie (paradoxul lui das Russell). Aici $x \notin A$ este negaţia propoziţiei $x \in A$. Nu ne vom ocupa prea mult de problemem de acest tip, şi vom evita paradoxurile lucrând "local", anume, când considerăm o proprietate P (Predicat) definim $A = \{x \in U \mid P(x)\}$ şi nu $A = \{x \mid P(x)\}$, şie U este o mulţime suficient de cuprinzătoare (Universul discursului).

Exemplu 1.2.5. Mulţimi de numere:

Numere naturale: $\mathbb{N} = \{0,1,2,3,\ldots\}$, $N^* = \{1,2,3\ldots\}$.
Numere întregi: $\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$.
Numere raţionale: $\mathbb{Q} = \{\frac{m}{n} \mid n,m \in \mathbb{Z}, n \neq 0\}$.
Numere reale: $\mathbb{R}$ ($\mathbb{R}$ =?).
Numere complexe: $\mathbb{C} = \{a + ib \mid a,b \in \mathbb{R}\}$ şie $i^2 = -1$.

Definiţie 1.2.6. Considerăm două mulţimi A şi B . Spunem că A este o *submulţime* a lui B, dacă $x \in A$ implică $x \in B$. Scriem $A \subseteq B$.

Definiţie 1.2.7. Mulţimea vidă notată cu $\emptyset$ este mulţimea care nu conţine nici un element.

Propoziţie 1.2.8. *Următoarele afirmaţii sunt valabile pentru orice mulţimi A, B şi C:*

(a) $A \subseteq A$ *(reflexivitate).*
(b) *Dacă* $A \subseteq B$ *şi* $B \subseteq C$ *atunci* $A \subseteq C$ *(tranzitivitate).*
(c) A=B *ddacă* $A \subseteq B$ *şi* $B \subseteq A$ *(antisimetrie).*
(d) $\emptyset \subseteq A$.
(e) *Multimea vidă este unic determinată.*

Demonstraţie. □

Operaţii cu mulţimi.

Definiţie 1.2.9. Fie A şi B muljmi. Se defineşte:

(a) *Reuniunea* dintre A şi B prin $A \cup B = \{x \mid x \in A \vee x \in B\}$.
(b) *Intersectia* dintre A şi B prin $A \cap B = \{x \mid x \in A \wedge x \in B\}$.
(c) *Diferenţa* dintre A şi B prin $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

În cazul $A \subseteq U$ se numeşte *complementara* lui A în U mulţimea $\mathbf{C}_U A = U \setminus A$.

Observaţie 1.2.10. Mulţimile pot fi reprezentate prin aşa numitele diagrame Euler-Venn. De exemplu:

Teoremă 1.2.11. *Fie A, B, C, U mulţimi, aşa încât $A, B, C \subseteq U$.*

(a) $(A \cup B) \cup C = A \cup (B \cup C)$ *şi* $(A \cap B) \cap C = A \cap (B \cap C)$ *(asociativitate).*
(b) $A \cup B = B \cup A$ *şi* $A \cap B = B \cap A$ *(comutativitate).*
(c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *şi* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(dublă distributivitate).*
(d) $A \cup A = A = A \cap A$ *(idempotenţă).*
(e) $A \cup (A \cap B) = A = A \cap (A \cup B)$ *(absorbţie).*
(f) $\mathbf{C}_U(A \cup B) = \mathbf{C}_U A \cap \mathbf{C}_U B$ *şi* $\mathbf{C}_U(A \cap B) = \mathbf{C}_U A \cup \mathbf{C}_U B$ *(regulile lui de Morgan).*

Demonstraţie. □

Definiţie 1.2.12. Fie A o mulţime. *Mulţimea putere a* mulţimii A este mulţimea tuturor submulţimilor lui A, adică:

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

Observaţie 1.2.13. Definiţia mulţimii tuturor submulţimior necesită precauţii suplimentare: care univers trebuie folosit? De notat: paradoxul lui Cantor este construit cu ajutorul mulţimii tuturor submulţimilor.

Definiţie 1.2.14. Pentru două mulţimi A şi B, se defineşte *produsul cartezian* ca fiind:

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

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

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

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

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

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

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

Observaţie 1.2.15. Inductiv se poate defini produsul cartezian a unui număr finit de mulţimi:

$$A_1 \times A_2 \times \ldots A_{n-1} \times A_n = (A_1 \times A_2 \times \ldots A_{n-1}) \times A_n.$$

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

Exerciţii la Mulţimi.

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

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

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

$\{\emptyset\}$

1.3. Funcţii.

Definiţie 1.3.1. O *funcţie* (sau *aplicaţie*) este un triplet (A, B, f) care este format din două mulţimi A şi B şi o lege de corespondenţă f, aşa încât fiecărui element din A îi corespunde un singur element din B. Mulţimile A şi B se numesc domeniul de definiţie (sau simplu domeniul), respectiv domeniul de valori (sau codomeniul) funcţiei. Se scrie $f : A \to B$ 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 şi *imaginea lui a prin f*). Se notează cu B^A mulţimea tuturor funcţiilor de la A la B, adică

$$B^A = \{f : A \to B \mid f \text{ este o funcţie}\}.$$

Observaţie 1.3.2. Două func tii $f : A \to B$ şi $f' : A' \to B'$ sunt egale ddacă $A = A'$, $B = B'$ şi $f(x) = f(x')$ pentru orice $x \in A$.

dacă şi numai dacă

Observaţie 1.3.3. Funcţiile pot fi definite în mai multe moduri:

(a) Prin indicarea directa a imaginii fiecărui element din domeniu, de exemplu $f : \{1, 2, 3\} \to \{a, b, c, d\}$, $f(1) = f(2) = a$ şi $f(3) = b$. Variante (pentru aceeaşi funcţie): Printr-un tabel:

x	1	2	3
$f(x)$	a	a	b

sau printr-o diagramă:

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

Exemplu 1.3.4. (a) Pentru orice mulţime A se defineşte *funcţia identitate* prin $1_A : A \to A$, $1_A(x) = x$ pentru orice $x \in A$. Se notează uneori $1_A = id_A$

(b) Dacă A şi B sunt mulţimi, aşa încât $A \subseteq B$, se defineşte funcţia *incluziune* prin $i = i_{A,B} : A \to B$, $i(x) = x$, pentru orice $x \in A$. De notat că $i_{A,B} = 1_A$ ddacă $A = B$, altfel $i_{A,B} \neq 1_A$.

(c) Dacă A, B, C sunt mulţimi, aşa încât $C \subseteq A$ şi $f : A \to B$ este o funcţie se construieşte *funcţia restricţie* a lui f la C, prin $f|_C : C \to B$, $f|_C(x) = f(x)$ pentru orice $x \in C$.

(d) Următoarele corespondenţe nu sunt funcţii:

Definiţie 1.3.5. Fie $f : A \to B$ o funcţie şi fie $X \subseteq A$, $Y \subseteq B$ două submulţimi (a lui A respectiv B). Se defineşte:

(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 funcţiei f, şi anume $f(A) = \mathrm{Im} f$.

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

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

Definiţie 1.3.6. Dacă $f : A \to B$ şi $g : B \to C$ sunt funcţii, atunci *compunerea* lor este definită astfel: $g \circ f : A \to C$, $(g \circ f)(x) = g(f(x))$ pentru orice $x \in A$.

Teoremă 1.3.7. *Atunci când este definită compunerea funcţiilor este asociativă, adică pentru $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ avem $(h \circ g) \circ f = h \circ (g \circ f)$. Funcţia identitate acţionează ca element neutru pentru compunerea funcţiilor, adică pentru $A \xrightarrow{f} B$ avem $f = f \circ 1_A = 1_B \circ f$.*

Demonstraţie. □

Definiţie 1.3.8. O funcţie $f : A \to B$ se numeşte *inversabilă* dacă există o altă funcţie $f' : B \to A$ astfel încât $f' \circ f = 1_A$ şi $f \circ f' = 1_B$.

Propoziţie 1.3.9. *Dacă $f : A \to B$ este inversabilă, atunci există o singură funcţie $f' : B \to A$ cu proprietatea $f' \circ f = 1_A$ şi $f \circ f' = 1_B$. Notăm cu f^{-1} această funcţie şi o numim* inversa *funcţiei f. De asemenea avem $(f^{-1})^{-1} = f$.*

Demonstraţie. □

Exemplu 1.3.10. $\exp : \mathbb{R} \to (0, \infty)$, $\exp(x) = e^x$ este inversabilă şi are inversa $\ln : (0, \infty) \to \mathbb{R}$. A se observa legătura dintre inversabilitatea funţiilor şi soluţia (eventual unică) a ecuaţiilor!

Propoziţie 1.3.11. *Dacă $A \xrightarrow{f} B \xrightarrow{g} C$ sunt doă funcţii inversabile, atunci tot aşa este şi $g \circ f$; mai mult avem $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Demonstraţie. □

$X = \{2,3\}$ $\qquad f(X) = \{a, b\}$

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

$f(A) = \{f(x), x \in A\} = \{\underset{a}{f(1)}, \underset{\cancel{c}}{f(2)}, \underset{b}{f(3)}\} = \{a, b\}$

$f^{-1}(Y_1) = \{3\}$ $\qquad f^{-1}(Y_2) = \emptyset$

Compunerea

Dem 1.3.7.

Fie $x \in A$

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

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

Obs Dacă $A \neq B$ atunci NU există $f \circ 1_B$

— " — $1_A \circ f$

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

Vrem să arătăm că $f \circ 1_A = f = 1_B \circ f$ OK

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

$(1_B \circ f)(x) = 1_B(\underset{y \in B}{f(x)}) = \underset{y}{f(x)}$

1.3.9. Dem

Fie $f: A \to B$ și presup. că $\exists\, f', f'': B \to A$ a.î.

Inflexivă $f' \circ f = 1_A$, $f \circ f' = 1_B$

$f'' \circ f = 1_A$, $f \circ f'' = 1_B$ Inflexivă

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, shift left, "f'\circ f"] \arrow[dr, shift right, "1_A"'] & B \arrow[d, shift right, "f'"'] \arrow[dr, shift left, "1_B"] \arrow[dr, shift right, "f''"'] & \\
& A \arrow[r, "f"] \arrow[d, "1_A"] & B \\
& A &
\end{tikzcd}$$

$$f' = 1_A \circ f' = (f'' \circ f) \circ f' \overset{\text{asoc}}{=} f'' \circ (f \circ f') = f'' \circ 1_B = f''. \quad \boxtimes$$

Dem 1.3.11.

$$\begin{tikzcd}
A \arrow[r, shift left, "f"] \arrow[rr, bend left, "g\circ f"] & B \arrow[l, shift left, "f^{-1}"] \arrow[r, shift left, "g"] & C \arrow[l, shift left, "g^{-1}"] \arrow[ll, bend left, "\exists\, f^{-1}\circ g^{-1}"]
\end{tikzcd}$$

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

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

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ 1_B \circ f = f^{-1} \circ f = 1_A$$

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ 1_B \circ g^{-1} = g \circ g^{-1} = 1_C$$

$$\Rightarrow \exists\, (g \circ f)^{-1} = f^{-1} \circ g^{-1}. \quad \boxtimes$$

Obs (1) Dacă $A \neq C$ atunci nu există $g^{-1} \circ f^{-1}$!!!

$B \xrightarrow{f^{-1}} A \quad C \xrightarrow{g^{-1}} B$ nu se pot prelungi în egalitate!

(2) Chiar dacă $A = C$ atunci

$$\begin{tikzcd}
A \arrow[r, shift left, "f"] \arrow[rr, bend left] & B \arrow[l, shift left, "f^{-1}"] \arrow[r, shift left, "g"] & A = C \arrow[l, shift left, "g^{-1}"] \arrow[ll, bend left, "\exists\, f^{-1}\circ g^{-1}"]
\end{tikzcd}
\qquad
\begin{tikzcd}
B \arrow[r, shift left, "g"] & A \arrow[l, shift left, "g^{-1}"] \arrow[r, shift left, "f"] & B \arrow[l, shift left, "f^{-1}"] \arrow[ll, bend left, "\exists\, g^{-1}\circ f^{-1} = (f\circ g)^{-1}"]
\end{tikzcd}$$

Dacă $A \neq B$ nu este posibil ca

$(g \circ f)^{-1}: \underset{\underset{C}{\parallel}}{A} \to B \qquad g^{-1} \circ f^{-1}: B \to B$

să fie egale.

(3) Chiar și în cazul în care $A = B = C$ este posibil ca $(g \circ f)^{-1} \neq g^{-1} \circ f^{-1}$. În unele cazuri particulare este posibilă și egalitatea.

Injectivitate, surjectivitate, bijectivitate.

Definiţie 1.3.12. O funcţie $f : A \to B$ se numeşte:

(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 $x \in A$ aşa încât $f(x) = y$.
(c) *bijectivă* dacă f atât injectivă cât şi surjectivă.

Observaţie 1.3.13. În mod echivalent o funcţie $f : A \to B$ este

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

Observaţie 1.3.14. O funcţie $f : A \to B$ este injectivă, surjectivă sau bijecktivă ddacă pentru orice $y \in B$ ecuaţia $f(x) = y$ are cel mult, cel puţin, respectiv exact o soluţie $x \in A$.

Propoziţie 1.3.15. *Următoarele propoziţii sunt adevărate pentru două funcţii* $A \xrightarrow{f} B \xrightarrow{g} C$*:*

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

Demonstraţie. □

Propoziţie 1.3.16. *Fie $f : A \to B$ o funcţie cu $A \neq \emptyset$. Următoarele afirmaţii sunt echivalente:*

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

Demonstraţie. □

Propoziţie 1.3.17. *Fie $g : B \to A$ o funcţie. Următoarele afirmaţii sunt echivalente:*

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

Demonstraţie. □

Teoremă 1.3.18. *Fie $f : A \to B$ o funcţie. Următoarele afirmaţii sunt echivalente:*

(i) *f este bijectivă.*
(ii) *f este inversabilă.*
(iii) *f este inversabilă la stânga şi inversabilă la dreapta.*

~~*Demonstraţie.*~~ □

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

Dem 1.3.15 $\quad A \xrightarrow{f} B \xrightarrow{g} C$, $\quad A \xrightarrow{g\circ f} C$

a) f, g inj

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

$$g(f(x_1)) = g(f(x_2)) \xRightarrow{g \text{ inj}}$$
$$f(x_1) = f(x_2) \xRightarrow{f \text{ inj}}$$
$$x_1 = x_2.$$

Deci $g\circ f$ este inj.

b) f, g surj.

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

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

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

Deci $g\circ f$ surj.

d) $g\circ f$ este inj.

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

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

Deci f este inj.

e) $g\circ f$ este surj.

Fie $z \in C \xRightarrow{g\circ f \text{ surj}} \exists x \in A \quad (g\circ f)(x) = z \Rightarrow g(f(x)) = z$

Not $y = f(x) \in B \quad g(y) = z$. Deci g surj. $\boxtimes$

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

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, shift left, "g\circ f"] \arrow[dr, shift right, "1_A"'] & B \arrow[d, "g"] \\ & A \end{tikzcd}$$

$g\circ f = 1_A \iff (g\circ f)(x) = 1_A(x), \forall x \in A \iff \boxed{g(f(x)) = x, \forall x \in A. \ (1)}$

Fie $y \in B$

Dacă $y \in \operatorname{Im} f \xRightarrow{f \text{ inj}} \exists! x \in A: f(x) = y$

Punem $g(y) = x$

Dacă $y \notin \operatorname{Im} f$ atunci $A \neq \emptyset$ ne permite să alegem un elem. $a \in A$ și definim $g(y) = a$.

Ex

Deci $g: B \to A \quad g(y) = \begin{cases} x, & x \text{ sol. unică a ec. } f(x) = y \text{ pt } y \in \operatorname{Im} f \\ a, & y \notin \operatorname{Im} f. \end{cases}$

Este clar că (1) este verificată de g deci $g\circ f = 1_A$.

(ii) $\Rightarrow$ (iii)

$$\begin{tikzcd} A' \arrow[r, shift left, "h_1"] \arrow[r, shift right, "h_2"'] \arrow[rr, bend left, "f\circ h_1"] \arrow[rr, bend right, "f\circ h_2"'] & A \arrow[r, "f"] & B \arrow[r, "g"] & A \end{tikzcd}$$

Din (i) $\exists\, g: B \to A$ a.î. $g\circ f = 1_A$

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.î. $f(x_1) = f(x_2)$

Definim $A' = \{0\}$, $h_1, h_2 : A' \to A$, $h_1(0) = x_1$, $h_2(0) = x_2$

$f\circ h_1 : A' \to B$, $f\circ h_2 : A' \to B$

$(f\circ h_1)(0) = f(h_1(0)) = f(x_1) = f(x_2) = f(h_2(0)) = (f\circ h_2)(0)$ $\Big\}\Rightarrow$

0 este singurul elem. din A'

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

Deci f este inj. $\boxtimes$.

1.3.17. Dem $g: B \to A$

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

Caut $f: A \to B$ a.î. $g\circ f = 1_A$ sau echiv. (1) este valabilă. din Dem. 1.3.16.

Fie $x \in A$ $\xRightarrow{g \text{ surj}}$ există elem. $y \in B$ a.î. $g(y) = x$ (sau echiv. ec. $g(y) = x$ are soluții $y \in B$).

Ex

Alg $y = y_x \in B$ a.î. $g(y) = x$ și definesc $f(x) = y_x$.

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

(ii) $\Rightarrow$ (iii)

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] \arrow[rr, bend left, "k_1\circ g"] \arrow[rr, bend right, "k_2\circ g"'] & A \arrow[r, shift left, "k_1"] \arrow[r, shift right, "k_2"'] & A' \end{tikzcd}$$

$k_1\circ g = k_2\circ g$

Stim că $\exists\, f: A \to B$ a.î. $g\circ f = 1_A$ $\Big\}\Rightarrow$

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

(iii) $\Rightarrow$ (i) Presupunem că g nu este surj. $\Rightarrow \exists\, a \in A$ a.î.

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

Alg $A' = \{0,1\}$ și definim $k_1, k_2 : A \longrightarrow A'$

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

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

Atunci $k_1 \circ g, k_2 \circ g : B \longrightarrow A'$

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

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

Deci $k_1 \circ g = k_2 \circ g$ dar $k_1 \neq k_2$. $\boxtimes$.

Cardinalul unei mulţimi.

Definiţie 1.3.19. Spunem că două mulţimi A şi B *au acelaşi cardinal* dacă există o bijecţie $f : A \to B$. O mulţime A este *finită* dacă $A = \emptyset$ sau există $n \in \mathbb{N}^*$ aşa încât A şi $\{1, 2, \ldots, n\}$ au acelaşi cardinal. În ultimul caz, numarul natural n este unic determinat, deoarece nu există o bijecţie $\{1, 2 \ldots, n\} \to \{1, 2, \ldots, m\}$ pentru $n \neq m$; spunem că A are cardinalul n, şi scriem $|A| = n$ sau $\sharp A = n$. Mulţimea vidă nu are elemente, deci cardinalul ei este zero; scriem $|\emptyset| = 0$. $|\{\emptyset\}| = 1$

Observaţie 1.3.20. Pentru mulţimile finite cardinalul este simplu numarul de elemente. Dar cardinalul se defineşte şi pentru mulţimile infinite, aşadar există o masură cu ajutorul căreia putem compara "mărimea" acestor mulţimi.

Propoziţie 1.3.21. *Fie A o mulţime finită. Următoarele afirmaţii sunt echivalente pentru o funcţie $f : A \to A$:*

(i) *f ist injectivă.*
(ii) *f ist surjectivă.*
(iii) *f ist bijctivă.*

$f : \mathbb{Z} \to 2\mathbb{Z}$, $f(x) = 2x$

Demonstraţie. temă. □

Observaţie 1.3.22. O mulţime infinită A poate fi caracterizată prin proprietatea că există o funcţie injectivă (sau surjectivă) $f : A \to A$ care nu este bijectivă.

Definiţie 1.3.23. Pentru o submulţime X a unei mulţimi A se defineşte *funcţia caracteristică* $\mathrm{ch}_X : A \to \{0, 1\}$ a lui X (în rapurt cu A) prin

$$\mathrm{ch}_X(x) = \begin{cases} 1 \text{ dacă } x \in X \\ 0 \text{ dacă } x \notin X \end{cases}$$ = valoarea de adevăr a propoziţiei "$x \in X$"

Lemă 1.3.24. *Pentru orice mulţime A funcţia $\mathrm{ch} : \mathcal{P}(A) \to \{0, 1\}^A$, $\mathrm{ch}(X) = \chi_X$ este bijectivă.*

Demonstraţie. temă. □

Corolar 1.3.25. *Pentru orice mulţime A avem $|\mathcal{P}(A)| = |\{0, 1\}^A|$ şi mulţimile A şi $\mathcal{P}(A)$ nu au acelaşi cardinal.*

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

Demonstraţie. ✓ □

Produsul cartezian.

Propoziţie 1.3.26. *Considerăm mulţimile $A_1, A_2, \ldots, A_n$, unde $n \in \mathbb{N}^*$. Să se arate că*

$$\phi : A_1 \times A_2 \times \ldots \times A_n \to (A_1 \cup A_2 \cup \ldots \cup A_n)^{\{1,2,\ldots,n\}} \text{ unde}$$
$$\phi(a_1, a_2, \ldots, a_n)(i) = a_i, \text{ pentru orice } i \in I$$

este o funcţie injectivă, a cărei imagine este:

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

Aşadar ϕ induce o bijecţie

$$A_1 \times A_2 \times \ldots \times A_n \to \mathrm{Im}\phi, \ (a_1, a_2, \ldots, a_n) \mapsto \phi(a_1, a_2, \ldots, a_n).$$

Demonstraţie. □

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

$A^I = \{ f : I \to A \mid f \text{ funkcje} \}$

x	a_1	a_2	a_3
$f_1(x)$	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_4

$A^I = A \times A \times A$

n.a.m.d.

$\prod_{i\in I} A_i \ni (a_i)_{i\in I}$, I mulțime posibil infinită

$\updownarrow$

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

Propoziţia anterioară ne oferă posibilitatea de a extinde definiţia produsului cartezian din cazul familiilor finite de mulţimi (a se vedea Observaţia 1.2.15) pentru o familie oarecare (posibil infinită).

Definiţie 1.3.27. Se consideră familia de mulţimi A_i cu $i \in I$. Prin definiţie *produsul cartezian* a acestei familii este:

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

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

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

(a se compara cu notaţia B^A din definiţia 1.3.1).

(2) Existenţa produsului cartezian necesită o axiomă specială a teoriei mulţimilor, şi anume Axioma Alegerii. Deşi intuitiv este clar, din punct de vedere formal nu este posibil ca în lipsa acestei axiome să construim o funcţie $f : I \to \bigcup_{i\in I} A_i$ aşa încât $f(i) \in A_i$ pentru orice $i \in I$ (adică să alegem elementele $f(i) \in A_i, i \in I$).

Operaţii.

Definiţie 1.3.29. Fie A o mulţime. O *operaţie (binară)* pe A este o func tie $* : A \times A \to A$. Adesea se scrie $a * b$ în loc de $*(a, b)$.

Definiţie 1.3.30. O operatţie $* : A \times A \to A$ pe A se numeşte:

(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 numeşte *element neutru* pentru $*$. Dacă operaţia $*$ are un element neutru e, atunci un element $x \in A$ se numeţe *inversabil* dacă exsită $x' \in A$ aşa încât $x * x' = e = x' * x$.

Propoziţie 1.3.31. *Dacă o operaţie $* : A \times A \to A$ are un element neutru, atunci el este unic.*

$e, e' \in A$ neutre

$e * e' \overset{e \text{ neutru}}{=} e'$
$e * e' \overset{e' \text{ neutru}}{=} e$ $\Big\} \Rightarrow e = e'$

Demonstraţie. □

Propoziţie 1.3.32. *Se consideră o operaţie asociativă $* : A \times A \to A$ 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} şi se numeşte* 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 şi avem* $\cancel{(xy)^{-1} = y^{-1}x^{-1}}$. $(x * y)^{-1} = y^{-1} * x^{-1}$.

a se vedea dem. pt. funcții

Demonstraţie. □

Definiţie 1.3.33. Un *monoid* este o pereche (structură) $(M, *)$ care consistă dintr-o mulţime M împreună cu o operaţie asociativă $* : M \times M \to M$, care are un element neutru. Pentru doi monoizi $(M, *)$ şi $(N, *)$ se numeşte *homomorfism de monoizi* o funcţie $f : M \to N$ cu proprietatea $f(x * y) = f(x) * f(y)$ pentru orice $x, y \in M$.

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 $(M,*)$ şi $(N,*)$ sunt monoizi, atunci $1_M : M \to M$ şi $\overline{e} : M \to N$, $\overline{e}(x) = e$ pentru orice $x \in M$ sunt homomorfisme de monoizi.

Exerciţii la funcţii.

Exerciţiu 1.3.35. Se consideră funcţiile:
(1) $f_1 : \mathbb{R} \to \mathbb{R}$, $f_1(x) = x^2$
(2) $f_2 : [0,\infty) \to \mathbb{R}$, $f_2(x) = x^2$
(3) $f_3 : \mathbb{R} \to [0,\infty)$, $f_3(x) = x^2$
(4) $f_4 : [0,\infty) \to [0,\infty)$, $f_4(x) = x^2$.
Să se studieze pentru fircare dintre ele injectivitatea, surjectivitatea şi bijectivitatea. În cazul existenţei inversei să se determine această.

Exerciţiu 1.3.36. Acelaşi exerciţiu ca şi 1.3.35 pentru funţiile:
(1) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \begin{cases} 2x+1 \text{ dacă } x \leq 1 \\ x+2 \text{ dacă } 1 < x \end{cases}$
(2) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \begin{cases} x^2+1 \text{ dacă } x \leq 0 \\ -x+2 \text{ dacă } 0 < x \end{cases}$
(3) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \begin{cases} 2x+1 \text{ dacă } x \leq 0 \\ x+2 \text{ dacă } 0 < x \end{cases}$

Exerciţiu 1.3.37. Să se precizeze dauţ a următoarele compuneri $f \circ g$ şi $g \circ f$ sunt definite, şi în caz afirmativ să se determine funcţia compusă:
(1) $f, g : \mathbb{R} \to \mathbb{R}$ $f(x) = \begin{cases} x^2-1 \text{ dacă } x \leq -1 \\ x-1 \text{ dacă } -1 < x \end{cases}$ şi $g(x) = \begin{cases} -x+1 \text{ dacă } x < 3 \\ x-2 \text{ dacă } 3 \leq x \end{cases}$
(2) $f : \mathbb{R} \to [0,\infty), f(x) = |x|$ şi $g : \mathbb{N}^* \to \mathbb{R}, g(x) = 1/x$.
(3) $f : R \to [0,\infty), f(x) = x^2+1$ şi $g : [0,\infty) \to \mathbb{R}, g(x) = \sqrt{x}$.

Exerciţiu 1.3.38. Fie A, B, C trei mulţimi aşa încât $C \subseteq A$ şi fie $f : A \to B$ o funcţie. Să se arate că $f|_C : f \circ i$, unde $i : \cancel{A} \to \cancel{C}$ $C \to A$ este funcţia de incluziune.

Exerciţiu 1.3.39. Fie $f : A \to B$ o funcţie inversabilă şi fie $Y \subseteq B$. Atunci prin $f^{-1}(Y)$ putem înţelege 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 aceeaşi mulţime.

Exerciţiu 1.3.40. Să se găsească un exemplu de două funcţii $f, g : \mathbb{N} \to \mathbb{N}$ aşa încât $g \circ f \neq f \circ g$. (Deşi compunerea este definită bilateral, ea nu este comutativă).

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

Exerciţiu 1.3.42. Să se găsească un exemplu care constă dintr-o funcţie $f : A \to B$, aşa 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.

Exerciţiu 1.3.43. Să se găsească un exemplu care constă dintr-o funcţie $g : B \to A$, aşa 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 ddacă g este bijectivă.

Exerciţiu 1.3.44. Să se găsească un exemplu care constă din două funcţii $A \xrightarrow{f} B \xrightarrow{g} C$, 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 şi f nu este surjectivă.

Exerciţiu 1.3.45. Fie $f : A \to B$ o funcţie, şi fie $X, X_1, X_2 \subseteq A$ şi $Y, Y_1, Y_2 \subseteq B$ submulţimi. 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) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

Exerciţiu 1.3.46. Următoarele afirmaţii sunt echivalente, pentru o funcţie $f : A \to B$:

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

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

Exerciţiu 1.3.47. Următoarele afirmaţii sunt echivalente, pentru o funcţie $f : A \to B$:

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

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

Exerciţiu 1.3.48. Fie A şi B două mulţimi finite cu $|A| = n$ şi $|B| = m$. Să se determine $|B^A|$. ~~Indicaţie: Se arată prin inducţie după n că $|B^A| = m^n$~~.

Exerciţiu 1.3.49. Fie A şi B mulţimi finite cu $|A| = n$ şi $|B| = m$. Să se determine numărul tuturor funcţiilor injective de la A la B. Indicaţie: Numărul căutat este $A_m^n = \frac{m!}{(m-n)!}$.

Exerciţiu 1.3.50. Fie A o mulţime finită cu $|A| = n$. Să se determine numărul tuturor funcţiilor bijective $f : A \to A$ (adică numărul tuturor permutărilor lui A).

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

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

Exerciţiu 1.3.53. (Principiul includerii şi al excluderii) Fie $A_1, A_2, \ldots, A_n$ mulţimi finite, unde $n \in \mathbb{N}^*$. Atunci:

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n-1} |A_1 \cap A_2 \cap \ldots \cap A_n|.$$

$$|A_1 \cap A_2 \cap \ldots \cap A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cup A_j| + \sum_{1 \le i < j < k \le n} |A_i \cup A_j \cup A_k| - \ldots + (-1)^{n-1} |A_1 \cup A_2 \cup \ldots \cup A_n|.$$

Exerciţiu 1.3.54. Fie A şi B mulţimi, cu $|A| = n$ şi $|B| = m$. Să se găsească numărul tuturor funcţiilor surjective $f : A \to B$.

Exerciţiu 1.3.55. Să se arate că mulţimile $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ au acelaşi cardinal.

Exerciţiu 1.3.56. Să se arate că mulţimile $\mathbb{N}$ şi $\mathbb{R}$ nu au acelaşi cardinal. Indicaţie: Se arată că $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Exerciţiu 1.3.57. Fie A o mulţime finită cu $|A| = n$.

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

Exerciţiu 1.3.58. Se consideră operaţia $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, dată prin $x * y = xy + 2ax + by$, pentru orice $x, y \in \mathbb{R}$. Să se determine $a, b \in \mathbb{R}$, aşa încât $*$ să fie asociativă şi comutativă.

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

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

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

1.4. **Relaţii.**

Definiţie 1.4.1. O *relaţie* este un triplet (A, B, R), unde A şi B sunt două mulţimi oarecare, iar $R \subseteq A \times B$. Uneori notăm $r = (A, B, R)$ şi scriem arb în loc de $(a, b) \in R$, alteori scriem numai $R \subseteq A \times B$ pentru a desemna o relaţie. Ca şi în cazul funcţiilor A şi B se numesc *domeniu* respectiv *codomeniu*. Dacă $A = B$ atunci relaţia $R \subseteq A \times A$ se zice *omogenă* (pe A).

Observaţie 1.4.2. Funţiile pot fi privite ca fiind cazuri speciale de relaţii, şi anume o funcţie $f : A \to B$ este o relaţie $f = (A, B, F)$ cu prprietatea suplimentară că pentru orice $x \in A$ există un singur element $y \in B$ aşa încât xfy. În acest caz $F = \{(a, f(a)) \mid a \in A\}$ este graficul funcţiei f.

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

$a \leq b$

Exemplu 1.4.3. Urătoarele exemple sunt relaţii care nu sunt ~~func tii~~ funcţii:

(1) Relaţia uzuală mai mic sau egal este o relaţie omogenă pe $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ sau $\mathbb{R}$.
(2) Divizibilitatea $a|b$ ddacă există c aşa încât $b = ac$ este o relaţie omogenă pe $\mathbb{N}$ sau $\mathbb{Z}$.
(3) Fie $n \in \mathbb{N}$, $n > 1$. Congruenţa modulo n este o relaţie omogenă pe $\mathbb{Z}$. Reamintim: Congruenţa modulo n este definită prin $x \equiv y(\mod n)$ ddacă $n|(x-y)$.
(4) Pentru orice mulţime A apartenenţa $\in$ este o relaţie între A şi $\mathcal{P}(A)$.

Exemplu 1.4.4. Pentru orice mulţime A, egalitatea este o relaţie omogenă pe A. Se observă că această relaţie este şi o ~~funtie~~ funcţie, mai precis funcţia identitate a lui A.

Observaţie 1.4.5. Ca şi în cazul funcţiilor, există mai multe moduri în care poate fi dată o relaţie:

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

(2) Printr-o matrice cu intrări în mulţimea $\{0, 1\}$: Se consideră două mulţimi finite $A = \{a_1, a_2, \ldots, a_m\}$ şi $B = \{b_1, b_2, \ldots, b_n\}$ şi o relaţie $R \subseteq A \times B$. Această relaţie 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 matrice relaţiei anterioare este:
$$\begin{array}{c} 0 \rightarrow \\ 1 \rightarrow \\ 2 \rightarrow \\ 3 \rightarrow \\ 4 \rightarrow \\ \\ \end{array} \begin{array}{c} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\ a \quad b \quad c \quad d \end{array}$$
Aici prin $\mathbb{M}_{m\times n}(\{0, 1\})$ se notează mulţimea tuturor matricilor (adică tabele dreptunghice) cu m linii şi n coloane şi cu intrări din $\{0, 1\}$.

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

Definiţie 1.4.6. Pentru orice relaţie (A, B, R) se defineşte *relaţia inversă* ca fiind (B, A, R^{-1}), unde $(b, a) \in R^{-1}$ ddacă $(a, b) \in R$ pentru orice pereche $(a, b) \in A \times B$.

Observaţie 1.4.7. Relaţia inversă se poate defini pentru orice relaţie, î n particular pentru orice funcţie privită ca relaţie. Dar relaţia inversă a unei funcţii este exact atunci o funcţie când funcţia de la care pornim este bijectivă.

$f = (A, B, F) \rightsquigarrow \exists\, (B, A, F^{-1})$

$F^{-1} = \{(b_1, a_1), (b_1, a_2), (b_3, a_3)\}$

relații dar NU e funcție

$r = (A, B, R) \qquad s = (C, D, S)$

$R = \{(a,1), (a,3), (b,2), (b,3)\}$

$S = \{(3,u), (4,w), (5,v), (5,w)\}$

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

$S \circ R = \{(a,u), (b,u)\}$

Obs Dacă $B \cap C = \emptyset \Rightarrow s \circ r = (A, D, \emptyset)$

$\emptyset \subseteq A \times D$

$f: A \to B$ funcţie $\quad f(X) = \{y \in B \mid \exists x \in X : f(x) = y\}$

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

Definiţie 1.4.8. Fie $r = (A, B, R)$ o relaţie şi $X \subseteq A$, $Y \subseteq B$ submulţimi. Se definesc: $r(X) = \{y \in B \mid$ există $x \in \cancel{A}$ aşa încât $xry\}$ şi $r^{-1}(Y) = \{x \in A \mid$ există $y \in \cancel{B}$ aşa încât $xry\}$.

Observaţie 1.4.9. Pentru o relaţie $r = (A, B, R)$ şi o submulţime $Y \subseteq B$ avem $(r^{-1})(Y) = r^{-1}(Y)$.

Definiţie 1.4.10. Fie (A, B, R) şi (C, D, S) două relaţii. *Compunerea* celor două relaţii este definită prin: $(A, D, S \circ R)$ unde

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

Observaţie 1.4.11. Spre deosebire de cazul funcţiilor, compunerea este definită oricând fără a fi necesară coincidenţa dintre codomeniul primei relaţii cu domeniul celei de-a două.

Definiţie 1.4.12. O relaţie omogenă $r = (A, A, R)$ se numeşte:

(a) *reflexivă* dacă ara pentru orice $a \in A$.
(b) *tranzitivă* dacă pentru orice $a, b, c \in A$ din arb şi brc rezultă arc.
(c) *simetrică* dacă pentru orice $a, b \in A$ din arb rezultă bra.
(d) *antisimetrică* dacă pentru orice $a, b \in A$ din arb şi bra rezultă $a = b$.

Se numeşte *preordine* o relaţie omogenă care este reflexivă şi tranzitivă.

Relaţii de echivalenţă.

Definiţie 1.4.13. Fie A o mulţime. O *relaţie de echivalenţă* (sau pe scurt *echivalenţă*) pe A este o preordine care este de asemene simetrică, adică o relaţie omogenă pe A care este reflexivă, tranztivă şi simetrică.

Exemplu 1.4.14. Următoarele relaţii sunt echivalenţe:

(1) Relaţia de egalitate pe o mulţime arbitrară.
(2) Congruenţa triunghiurilor (pe mulţimea tuturor triunghiurilor din plan).
(3) Asemănarea triunghiurilor (pe mulţimea tuturor triunghiurilor din plan).

Definiţie 1.4.15. Fie $\equiv$ o relaţie de echivalenţă pe o mulţime A. Pentru un element $a \in A$ se notează

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

clasa de echivalenţă a lui a. Se numeşte *mulţimea factor* a lui A modulo $\equiv$ mulţimea tuturoe claselor de echivaleţă, adică

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

Funţia $p = p_{\equiv} : A \to A/_{\equiv}$ dată prin $p(x) = [x]$ se numeţe *proiecţia canonică* ataşată relaţiei de echivalenţă $\equiv$.

Observaţie 1.4.16. In definiţia formală a mulţimii factor este posibil, si chiar foarte probabil, ca anumite elemente să apară de mai multe ori. Noi ştim că într-o mulţime un element apare o singură dată, si presupunem automat că se eleimină repetiţiile. Totuşi această presupunere necesită precauţii suplimentare, căci o folosire greşită poate conduce la funcţii care nu sunt bine definite şi, prin urmare, la contradicţii.

Propoziţie 1.4.17. *Fie $(A, A, \equiv)$ o relaţie de echivalenţă pe omulţime A, şi $a, b \in A$. Avem:*

(a) $a \in [a]$, *aşadar* $[a] \neq \emptyset$.

$(A, A, \equiv)$

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

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

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

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

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

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

(b) "$\Rightarrow$" Stim $[a] = [b]$ $\Big\}$ $\Rightarrow b \in [a] \Rightarrow a \equiv b$.
Din (a) obținem $b \in [b]$

"$\Leftarrow$" Stim $a \equiv b \overset{(S)}{\Rightarrow} b \equiv a$ $\Big\}$ $\overset{T}{\Rightarrow} b \equiv x \Rightarrow x \in [b]$. Deci $[a] \subseteq [b]$.
Fie $x \in [a] \Rightarrow a \equiv x$

Fie $x \in [b] \Rightarrow b \equiv x$ $\Big\}$ $\overset{T}{\Rightarrow} a \equiv x \Rightarrow x \in [a]$. Deci $[b] \subseteq [a]$.
Deci $a \equiv b$

Așadar $[a] = [b]$.

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

"$\Rightarrow$" Stim $[a] \cap [b] \neq \emptyset \Rightarrow \exists\, c \in [a] \cap [b]$

$\Rightarrow \begin{cases} c \in [a] \Rightarrow a \equiv c \\ c \in [b] \Rightarrow b \equiv c \overset{(S)}{\Rightarrow} c \equiv b \end{cases} \Big\} \overset{(T)}{\Rightarrow} a \equiv b \overset{(b)}{\Rightarrow} [a] = [b]$.

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

Fie $a \in A \overset{(a)}{\Rightarrow} a \in [a] \Rightarrow a \in \bigcup_{x \in A} [x]$. Deci $A \subseteq \bigcup_{x \in A} [x]$ $\Big\} \Rightarrow$

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

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

Demonstraţie. □

Definiţie 1.4.18. Fie A o mulţime. O *partiţie* a mulţimii A este o submulţime $\pi \subseteq \mathcal{P}(A)$ a mulţimii putere a lui A (adică o mulţime a cărei elemente sunt submulţimi 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 mulţime.*
(1) *Dacă $(A, A, \equiv)$ este o relaţie de echivalenţă pe A, atunci $A/_{\equiv}$ este o partiţie a mulţimii A.*
(2) *Dacă $\pi \subseteq \mathcal{P}(A)$ este o partiţie a lui A, atunci $(A, A, \equiv_\pi)$ este o relaţie de echivalenţă, unde pentru orice $a, b \in A$ avem*

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

(3) *Procedeele de la (1) şi (2) descriu două funcţii inverse una celeilalte între Mulţimea tuturor echivalenţelor pe A şi mulţimea tuturor partiţiilor pe A.*

Demonstraţie. □

Relaţii de ordine.

Definiţie 1.4.20. Fie A o mulţime. O *relaţie de ordine* (sau pe scurt *ordine*) pe A este o preordine care este şi antisimetrică, adică o relaţie omogenă pe A care este reflexivă, tranzitivă şi antisimetrică. Antisim: $a \leq b$ şi $b \leq a \Rightarrow a = b$.

Adesea se notează o relaţie de ordine cu $\leq$ şi se spune că $(A, \leq)$ este o mulţime ordonată. În acest caz notăm $x < y$ relaţia $x \leq y$ şi $x \neq y$. $(A, A, \leq)$

Exemplu 1.4.21. Următoarele relaţii sunt de ordine:
(1) Relaţia de egalitate pe o mulţime arbitară.
(2) Relaţa obişnuită de mai mic sau egal pe $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ sau $\mathbb{R}$.
(3) Incluziunea pe o mulţime a căror elemente sunt mulţimi, de exemplu $(\mathcal{P}(A), \subseteq)$ este o mulţime ordonată, unde A este o mulţime 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 *lanţ* sau *şir*). În general acest lucru nu este adevărat pentru o mulţime ordonată oarecare, de exemplu $(\mathcal{P}(A), \subseteq)$ nu este un lanţ când A are cel puţin două elemente, pentru că există $X, Y \in \mathcal{P}(A)$ astfel încât $X \nsubseteq Y$ şi $Y \nsubseteq X$.

Definiţie 1.4.22. Fie $(A, \leq)$ o mulţime ordonată. Un element $a \in A$ se numeşte:
(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 $x \in A$.

Observaţie 1.4.23. Fie $(A, \leq)$ o mulţime ordonată. Se notează $\geq = \leq^{-1}$, adică $x \geq y$ ddacă $y \leq x$. Este uşor de a verifica că $\geq$ este de asemenea o relaţie de ordine (vezi Exerciţiu 1.4.48). Se poate observa că $a \in A$ este minimal sau cel

$x \leq y \iff y \geq x$

1.4.19. Dem (1) rezultă din 1.4.17.

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

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

$$\left.\begin{array}{l} a \equiv_\pi b \overset{(*)}{\Longrightarrow} \exists X \in \pi : a, b \in X \\ b \equiv_\pi c \overset{(*)}{\Longrightarrow} \exists X' \in \pi : b, c \in X' \end{array}\right\} \Rightarrow b \in X \cap X' \Rightarrow X \cap X' \neq \emptyset$$

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

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

Deci $(A, A, \equiv_\pi)$ este o rel. de echivalență.

(3)

$$\{(A, A, \equiv) \mid \text{rel. de echiv.}\} \xrightarrow{(1)} \{\pi \subseteq P(A) \mid \pi \text{ partiție}\} \xrightarrow{(2)} \{(A, A, \equiv) \mid \text{rel. de echiv}\}$$

$$(A, A, \equiv) \longmapsto A/_\equiv \xmapsto{(*)} (A, A, \equiv_{(A/_\equiv)})$$

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

$$\{\pi \subseteq P(A) \mid \pi \text{ partiție}\} \xrightarrow{(2)} \{(A, A, \equiv) \mid \text{rel. de echiv}\} \xrightarrow{(1)} \{\pi \subseteq P(A) \mid \text{partiție}\}$$

$$\pi \xmapsto{(*)} (A, A, \equiv_\pi) \longmapsto A/_{\equiv_\pi}$$

De arătat $\pi = A/_{\equiv_\pi}$ (4)

Pt. (3):

$(a, b) \in A \times A$ a.î. $a \equiv b \Rightarrow \underset{\underset{a}{\cup}}{[a]} = \underset{\underset{b}{\cup}}{[b]} \in A/_\equiv$.

Deci $\exists X = [a] = [b] \in A/_\equiv$ a.î. $a, b \in X \overset{*}{\Longrightarrow} a \equiv_{(A/_\equiv)} b$.

Reciproc dacă $a \equiv_{(A/_\equiv)} b \overset{(*)}{\Longrightarrow} \exists X \in \underset{\underset{\{[x] \mid x \in A\}}{\parallel}}{A/_\equiv}$ a.î. $a, b \in X \Rightarrow$

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

Deci $\left.\begin{array}{l} a \in [c] \Rightarrow c \equiv a \overset{S}{\Longrightarrow} a \equiv c \\ b \in [c] \Rightarrow c \equiv b \end{array}\right\} \overset{(T)}{\Longrightarrow} a \equiv b$, ceea ce arătă (3).

La (4) se procedează în același fel.

$(P(A), \subseteq)$ este o <u>mulțime ordonată</u> = poset

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

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

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

$\exists X, Y \in P(A)$ a.î. $X \not\subseteq Y$ și $Y \not\subseteq X$.

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

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

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

diagrama Hasse

$\left.\begin{array}{l}\{a\} \not\subseteq \{b\} \\ \{b\} \not\subseteq \{a\}\end{array}\right\}$ sunt incomparabile

$\{a\} \subseteq \{a\}$ ✓ $\qquad \{a,b\} \subseteq \{a,b\}$

$(\mathbb{N}, \leq)$

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

<u>Dem</u>. 1.4.24. $(A, \leq)$ m.o.

Știm că $\exists\, a \in A$ a = cel mai mic elem.

Fie $x \in A$ a.î. $x \leq a$
a este cel mai mic $\Rightarrow a \leq x$ $\Big\} \xRightarrow{(A)} x = a$. Deci a e minimal.

Fie $a' \in A$ un elem. minimal
Cum a e cel mai mic $\Rightarrow a \leq a'$ $\Big\} \xRightarrow{a' \text{ minimal}} a = a'$. ⊠

<u>Dem</u> 1.4.25 Fie $a, a' \in A$ ambele verifică prop. de a fi cel mai mic elem. $\overset{1.4.24}{\Rightarrow}$ a este unicul elem. minimal
a' — " —

$\Rightarrow a = a'$. ⊠.

mai mic element în $(A, \leq)$ ddacă a este maximal, respectiv cel mai mare element în $(A, \geq)$ şi invers. Această observaţie se poate extinde pentru toate noţiunile şi afirmaţiile referitoare la mulţimi ordonate şi este aşa numitul principiu al dualităţii.

Lemă 1.4.24. *Fie $(A, \leq)$ o mulţime 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 mulţimi ordonate, dacă există, este unic.*

Demonstraţie. □

nevidă

Cat punct.

$(A, \leq) = (\mathbb{N}, \leq)$

Teoremă 1.4.26. *Următoarele afirmaţii sunt echivalente pentru o mulţime ordonată $(A, \leq)$:*

(i) *Orice submulţime nevidă a lui A are un element minimal (condiţia minimalităţii).*

(ii) *Orice lanţ descrescător de elemente din A este finit, adică dacă $a_0 \geq a_1 \geq a_2 \geq \dots$ cu $a_0, a_1, a_2, \dots \in A$, atunci există $n \in \mathbb{N}$ aşa încât $a_n = a_{n+1} = \dots$ (condiţia lanţurilor descrescătoare).*

(iii) *Dacă $B \subseteq A$ are proprietăţile*
   (a) *B conţine toate elementele minimale ale lui A;*
   (b) *pentru $a \in A$ dacă $\{x \in A \mid x < a\} \subseteq B$ atunci $a \in B$;*
   atunci $B = A$ (condiţia inductivităţii).

$B = \{n \in \mathbb{N} \mid P(n)\}$

(a) $P(0)$

(b) $a \in \mathbb{N}$: $P(0), \dots, P(a-1)$

$\Downarrow$

$P(a)$

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

Definiţie 1.4.27. Fie $(A, \leq)$ o mulţime ordonată şi $X \subseteq A$. O margine inferioară (superioară) pentru X este un element $a \in A$ aşa încât, $a \leq x$ (respectiv $x \leq a$) pentru orice $x \in X$. Se numeşte *infimum (supremum)* a lui X în A cea mai mare (mică) margine inferioară (respectiv superioară) a lui X, adică

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

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

Observaţie 1.4.28. Fie $(A, \leq)$ o mulţime ordonată şi $X \subseteq A$.

(1) Dacă există $\inf X$ şi $\sup X$ 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 $\inf \mathbb{Z}$ şi nu exsită $\sup(0, \infty)$.

$\overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$

(2) În $(\mathbb{Q}, \leq)$ nu există $\sup\{x \in \mathbb{Q} \mid x^2 < 2\}$.
(3) Într-o mulţime ordonată $(A, \leq)$ există $\inf \emptyset$ ($\sup \emptyset$) exact atunci când A are cel mai mare (respectiv mic) element a, şi avem $\inf \emptyset = a = \sup A$ ($\sup \emptyset = a = \inf A$).

$X = A \subseteq A$

Definiţie 1.4.30. O *latice* este o mulţime ordonată $(L, \leq)$ cu proprietatea că ~~exsită~~ există $\inf\{x, y\}$ şi $\sup\{x, y\}$ pentru orice două elemente $x, y \in L$. Notăm $x \vee y = \sup\{x, y\}$ şi $x \wedge y = \inf\{x, y\}$. Laticea L se zice *completă* dacă există $\inf(X)$ şi $\sup(X)$ pentru orice submulţime $X \in L$.

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

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

Dem 1.h.26 (i) $\Rightarrow$ (iii). Presupunem concluzia falsă deci există $B \subseteq A$ care verifică (a) și (b) dar $B \neq A \Rightarrow A \setminus B \neq \emptyset$

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

Dacă a minimal în $A \overset{(a)}{\Longrightarrow} a \in B$ imposibil.

Deci a nu e minimal în $A \Rightarrow \{x \in A \mid x < a\} \neq \emptyset$.

Fie $x \in A$ $x < a$. Dacă presupunem $x \notin B$ atunci $x \in A \setminus B$ ceea ce contrazice minimalitatea lui a în $A \setminus B$. imposibil

Înseamnă că $x \in B$. Deci $\{x \in A \mid x < a\} \subseteq B$ și conform cu prop. (b) avem $a \in B$, ceea ce este imposibil.

Așadar (iii) este adevărată.

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

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

- Fie $a = a_0 \geq a_1 \geq a_2 \geq \dots \xRightarrow{a \text{ minimal}} a = a_0 = a_1 = a_2 = \dots$ deci $n = 0$.

  Deci $a \in B$ de unde rezultă că B satisface cond (a).

- Fie $a \in A$ cu prop. $\{x \in A \mid x < a\} \subseteq B$.

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

  Caz I. $a = a_0 = a_1 = a_2 = \dots \Rightarrow$ lanțul este staționar.

  Caz II $\exists\, k \geq 0$ a.i. $a_k > a_{k+1}$. Atunci $a = a_0 \geq a_k > a_{k+1}$

  $\Rightarrow a_{k+1} \in \{x \in A \mid x < a\} \subseteq B$

  $a_{k+1} \geq a_{k+2} \geq \dots$ lanț descresc.

  $\Rightarrow \exists\, n \in \mathbb{N}, n \geq k+1$ a.i. $a_n = a_{n+1} = \dots$ (este staționar).

  Atunci
  $$a = a_0 \geq a_1 \geq \dots \geq \underset{(>)}{a_k \geq a_{k+1}} \geq \dots \geq \underset{(=)}{a_n \geq a_{n+1}} \underset{(=)}{\geq} \dots \quad \text{este staționar.}$$

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

  Conform condiției (iii) care este ipotezată 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; am găsit ceea ce căutăm.

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.m.d. Condiția (ii) care este ipotezată ne spune algoritmul de mai sus trebuie să se oprească deci $\exists\, n \in \mathbb{N} : a_n \in B$ este minimal în B. $\boxtimes$.

Teoremă 1.4.31. *Într-o latice $(L, \leq)$ sunt valabile proprietăţile:*

(a) $x \vee (y \vee z) = (x \vee y) \vee z$ *şi* $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ *(asociativitate).*
(b) $x \vee y = y \vee x$ *şi* $x \wedge y = y \wedge x$ *(comutativitate).*
(c) $x \vee (x \wedge y) = x = x \wedge (x \vee y)$ *(absorbţie).*

Invers, dacă L este o mulţime împreună cu două operaţii $\vee, \wedge : L \times L \to L$ aşa încât sunt valabile proprietăţile (a), (b), (c) de mai sus, atunci L este o mulţime ordonată în raport cu relaţia $x \leq y$ ddacă $x \wedge y = x$; mai mult $(L, \leq)$ este chiar o latice în care $\inf\{x, y\} = x \wedge y$ *şi* $\sup\{x, y\} = x \vee y$*, pentru orice $x, y \in L$.*

Demonstraţie. □

Propoziţie 1.4.32. *O mulţime ordonată $(L, \leq)$ este o latice completă ddacă* ~~*exsită*~~ există $\inf X$ *pentru orice $X \subseteq L$.*

Demonstraţie. □

Exerciţii la Relaţii.

Exerciţiu 1.4.33. Fie $f : A \to B$ şi $g : B \to C$ două funcţii. Să se arate că funcţia compusă $g \circ f$ este acelaşi lucru ca şi relaţia compusă $g \circ f$.

Exerciţiu 1.4.34. Fie $r = (A, B, R)$ o relaţie si notăm cu δ_A şi δ_B relaţiile de egalitate pe A respectiv B.

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

Exerciţiu 1.4.35. Fie $r = (A, B, R)$ şi $s = (B, C, S)$ două relaţii, unde A, B şi C sunt mulţimi finite cu $|A| = m$, $|B| = n$ şi $|C| = p$. Se ordonează elementele din A, B şi C şi se consideră matricile $M(r) \in \mathbb{M}_{m \times n}(\{0, 1\})$ şi $M(s) \in \mathbb{M}_{n \times p}(\{0, 1\})$. Să se determine $M(r^{-1})$ şi $M(s \circ r)$ în funcţie de $M(r)$ şi $M(s)$. Să se scrie un algoritm care citeşte $M(r)$ şi $M(s)$ şi calculează $M(r^{-1})$, $M(s \circ r)$.

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

Exerciţiu 1.4.37. Să se determine toate relaţiile de echivalenţă care se pot defini pe $A = \{a, b, c\}$.

Exerciţiu 1.4.38. Să se arate că următoarele relaţii sunt echivalenţe şi să se calculeze respectivele mulţimi factor:

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

Exerciţiu 1.4.39. Să se arate că relaţia dată prin

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

este o echivalenţă pe $\mathbb{Z} \times \mathbb{Z}^*$ şi să se determine mulţimea factor

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

1.4.32. $(L, \leq)$ m.o.

$(L, \leq)$ latice completă $\Leftrightarrow$ $\forall X \subseteq L$ $\exists \inf(X) \in L$
$\exists \sup(X) \in L$.

Reciproc presupunem că pt. orice submulțime $X \subseteq L$ $\exists \inf(X) \in L$.

Considerăm $M = \{a \in L \mid \forall x \in X : x \leq a\} \subseteq L$ (mulțimea margini-lor superioare pt. X).

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

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

Așadar $m \in M$.

Dar $\forall a \in M$ avem $m \leq a$ (pt. că $m = \inf(M)$) $\Rightarrow m$ este cel mai mic elem. din $M \Rightarrow m = \sup X$. $\boxtimes$.

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

$\frac{-1}{-2} = \frac{1}{2} = \frac{2}{4}$ $\quad \underbrace{f\left(\frac{1}{2}\right) = \frac{1+1}{2^2} = \frac{2}{4} = \frac{1}{2}}$ $\neq f\left(\frac{2}{4}\right) = \frac{2+1}{4^2} = \frac{3}{16}$

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

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

Exerciţiu 1.4.40. Sunt bine definite următoarele funcţii

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

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

NU $h : \mathbb{Z} \to \mathbb{Z},\ h(x) = \frac{x}{2}$ pentru orice $x \in \mathbb{Z}$, $\quad h\left(\frac{1}{2}\right) \notin \mathbb{Z} \quad h\left(\frac{3}{2}\right) \notin \mathbb{Z}$

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

Exerciţiu 1.4.41. Considerăm mulţimea $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/_\sim$ ca în Exerciţiul 1.4.39. Să se arate că $+, \cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ sunt bine definite, unde:

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

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

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

(1) Congruenţa modulo n, şi anume $(\mathbb{Z}, \mathbb{Z}, \equiv_n)$ dată de $x \equiv_n y$ (sau $x \equiv y(\mod n)$) ddacă $n|(x-y)$ este o relaţie de echivalenţă.
(2) Mulţimea factor corespunzătoare este mulţimea tuturor claselor de resturi modulo n: $\mathbb{Z}_n = \mathbb{Z}/_{\equiv_n} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.
(3) Operaţiile următoare sunt bine definite:

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

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

Exerciţiu 1.4.43. Fie A o mulţime şi $r = (A, A, R)$ o preordine pe A. Să se arate că $r \cap r^{-1}$ unde $x(r \cap r^{-1})y$ ddacă xry şi yrx este o relaţie de echivalenţă pe A şi pe mulţimea factor $A/_{(r \cap r^{-1})}$ relaţia r induce o ordine: $[x] \leq_r [y]$ ddacă xry. Să se studieze cazul particular când $A = \mathbb{Z}$ şi preordinea este divizibilitatea (vezi Exerciţiu 1.4.36).

Exerciţiu 1.4.44. Fie $f : A \to B$ o funţie. *Nucleul* funţiei f este o relaţie omogenă pe A notată cu $\ker f$ şi definită prin $a(\ker f)b$ ddacă $f(a) = f(b)$. Să se arate că $\ker f$ este o relaţie de echivalenţă pe A. Invers, pentru orice relaţie de echivalenţă $(A, A, \equiv)$ să se găsescă o funcţie $f : A \to B$, astfel încât $\equiv$ este nucleul lui f.

Exerciţiu 1.4.45. Să se găsească numărul tuturor relaţiilor de echivalenţă care se pot defini pe o mulţime A cu n elemente.

Exerciţiu 1.4.46. Să se determine toate relaţiile de ordine care se pot defini pe $A = \{a, b, c\}$. În fiecare caz să se precizeze elemente;e minimale, maximale, cel mai mic şi/sau cel mai mare element.

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

Exerciţiu 1.4.48. Dacă $(A, \leq)$ este o mulţime ordonată, atunci tot aşa este şi $(A, \geq)$.

Exerciţiu 1.4.49. Orice latice finită este completă.

Exerciţiu 1.4.50. Orice lanţ este o latice. Este orice lanţ o latice completă?

Exerciţiu 1.4.51. Orice latice completă are cel mai mic şi un cel mai mare element.

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

Exerciţiu 1.4.53. Arătaţi că $(\mathbb{N}, \leq)$ este o latice care nu este completă. Explicaţi de ce acest exemplu nu contrazice Propoziţia 1.4.32.

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

Exerciţiu 1.4.55. Pe mulţimea $\mathcal{L}$ a tuturor propoziţiilor logice se defineşte relaţia $p \preceq q$ ddacă $p \to q$ este o tautologie. Să se arate că $\preceq$ este o preordine. Să se determine relaţia de echivalenţă asociată $\equiv = (\preceq \cap \preceq^{-1})$ (vezi Exerciţiul 1.4.35) şi mulţimea factor $\mathcal{L}/_{\equiv}$ (această mulţime este numită *algebra Lindenbaum-Tarski*). Să se arate că $\mathcal{L}/_{\equiv}$ este o latice completă.

2. Grupuri, inele, corpuri

2.1. **Grupuri.**

Definiţie 2.1.1. Un *grup* este o pereche $(G, \cdot)$ care constă dintr-o mulţime G împreună cu o operaţie $\cdot : G \times G \to G$, astfel încât $\cdot$ este asociativă, are un element neutru şi fiecare element din G este inversabil în raport cu $\cdot$. În cazul în care $\cdot$ este şi comutativă atunci G se numeşte *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 ceva!
$(M_{m\times n}(\mathbb{R}), \cdot)$ pt. $n \neq m$

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

Propoziţie 2.1.5. *Fie $(M, \cdot)$ un monoid şi 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 operaţia $\cdot$ induce pe $M^\times$, iar $M^\times$ împreună cu operaţia indusă formează un grup.

Demonstraţie. □

Corolar 2.1.6. *Următoarele construcţii conduc la grupuri neabeliene:*

(1) Dacă A este o mulţime, atunci $\mathrm{S}(A) = \{\sigma : A \to A \mid \sigma \text{ este bijectivă}\}$ este un grup împreună cu compunerea funcţiilor; acest grup nu este abelian pentru $|A| \geq 3$. Grupul $\mathrm{S}(A)$ se numeşte grupul simetric *al mulţimii A.*

2.1.5. Dem $(M,\cdot)$ monoid

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

- Arătăm că $M^\times$ este parte stabilă: ✓

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

$x\cdot y \in M$ $\quad (xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x\cdot 1\cdot x^{-1} = x\cdot x^{-1} = 1$

$\quad (y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}\cdot 1\cdot y = y^{-1}\cdot y = 1$ $\Big\} \Rightarrow$

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

- $1 \in M^\times$ pt. că $1^{-1} = 1 \in M$.
- asociativitatea înmulțirii din $M^\times$ nu mai trebuie verificată căci se „moștenește" din M.
- $x \in M^\times \Rightarrow \exists x^{-1} \in M$: --- $\Rightarrow (x^{-1})^{-1} = x \in M \Rightarrow x^{-1} \in M^\times$.

Deci $(M^\times,\cdot)$ este grup.

2.1.6. (a) $M = A^A = \{f : A \to A \mid f$ funcție$\}$

$(A^A, \circ)$ monoid. – compunerea este asociativă

– $1_A : A \to A$ este elem. neutru

$(A^A)^\times = \{\sigma \in A^A \mid \sigma$ inversabil$\} = \{\sigma : A \to A \mid \sigma$ bij$\} = S(A)$

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

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

$\sigma = \begin{pmatrix} a & b & c & \dots & x & \dots \\ b & a & c & \dots & x & \dots \end{pmatrix} \qquad \tau = \begin{pmatrix} a & b & c & \dots & x & \dots \\ a & c & b & \dots & x & \dots \end{pmatrix}$

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

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

– înmulțirea este asociativă I_n elem. neutru

$M_{n\times n}(K)^\times = \{A \in M_{n\times n}(K) \mid \exists A^{-1}$ a.î. $A^{-1}A = I_n = A\cdot A^{-1}\}$

$= \{\text{—} \mid \det A \neq 0\} = GL_n(K)$

grup.

Temă verificați că $GL_n(K)$ este necomutativ pt. $n \geq 2$. ☒.

Obs. $(\mathbb{R},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{C},\cdot)$ monoizi comut.

$\mathbb{R}^\times = \mathbb{R}^* = \mathbb{R}\setminus\{0\}$, $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{C}^\times = \mathbb{C}^*$

(2) *Fie* $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ *şi* $n \in \mathbb{N}^*$. *Mulţimea* $\mathrm{G}L_n(K) = \{A \in \mathbb{M}_{n\times n}(K) \mid \det(A) \neq 0\}$ *împreună cu înmulţirea matricilor formează un grup, care nu este comutativ pentru* $n \geq 2$. *Grupul* $\mathrm{G}L_n(K)$ *se numeşte* grupul linear general *de rang* n *peste* K.

Demonstraţie. □

Subgrupuri.

operatie

Definiţie 2.1.7. Fie $(G, \cdot)$ un grup. Un *subgrup* a lui G este o submulţime $H \subseteq G$, astfel încât operaţia pe G induce o ~~oprtţie~~ 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), şi H împreună cu ~~oprtaţi~~ a indusă fo~~rmează~~ formeata un grup. Se scrie $H \leq G$.

operatia

$\cdot : H \times H \to H$

Exemplu 2.1.8. (1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ (cu adunarea).
(2) $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$ (cu înmulţirea).
(3) $\mathbb{R}^*_+ \leq \mathbb{R}^*$, unde $\mathbb{R}^*_+ = (0, \infty)$.
(4) Orice grup G are aşa numitele subgrupuri triviale i. e. $\{1\}$ şi G.

Propoziţie 2.1.9 (Teorema de caracterizare a subgrupurilor)**.** *Fie* $(G, \cdot)$ *un grup şi fie* $H \subseteq G$ *o submulţime. Următoarele afirmaţii 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) $x, y \in H \Rightarrow xy^{-1} \in H$.

Demonstraţie. □

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

Demonstraţie. □

Observaţie 2.1.11. Reuniunea a două sau mai multe subgrupuri nu este cu necesitate subgrup (~~Übung~~ Exercitiul 2.1.58).

Definiţie 2.1.12. Fie $(G, \cdot)$ un grup şi $X \subseteq G$ o submulţime 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 $X = \{x_1, x_2, \ldots, x_n\}$ este o mulţime finită atunci scriem ~~$\langle x_1, x_2, \langle, x_n \rangle$~~ în loc de ~~$\langle\{x_1, x_2, \langle, x_n\}\rangle$~~. $\langle \{x_1, x_2, \ldots, x_n\} \rangle$ $\langle x_1, x_2, \ldots, x_n \rangle$

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

(a) $\langle X \rangle \leq G$.
(b) $X \subseteq \langle X \rangle$ *şi* $X = \langle X \rangle$ *ddacă* $X \leq G$.
(c) $\langle X \rangle$ *este cel mai mic subgrup a lui* G *care conţine submulţimea* X, *adică*

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

$\Downarrow$
$H \subseteq K$

(d) ~~Gilt~~ Dacă $X \subseteq Y \subseteq G$ ~~so gilt auch~~ atunci $\langle X \rangle \leq \langle Y \rangle \leq G$.

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

Dem 2.1.9 (i) $\Rightarrow$ (ii) pt. că asociativitate este o prop. ereditară

mai precis dacă $x\cdot(y\cdot z) = (x\cdot y)\cdot z$, $\forall x,y,z \in G$, iar $H \subseteq G$ atunci

cu atât mai mult $x\cdot(y\cdot z) = (x\cdot y)\cdot z$, $\forall x,y,z \in H$.

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

Fie $x, y \in H \xrightarrow{(iii c)} x, y^{-1} \in H \xrightarrow{(iii b)} x\cdot y^{-1} \in H$ ✓

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

Fie $x \in H$; știm $1, x \in H \xrightarrow{(iii b)} 1\cdot x^{-1} \in H \Rightarrow x^{-1} \in H$.

Fie $x, y \in H$; știm $x, y^{-1} \in H \xrightarrow{(iii b)} x\cdot (y^{-1})^{-1} \in H \Rightarrow x\cdot y \in H$. ☒.

Obs. (1) $\boxed{(2\mathbb{Z}+1, +) \text{ NU Există asa ceva!!!}}$

Dacă $x, y, z \in 2\mathbb{Z}+1$: $(x+y)+z = x+(y+z)$ asoc în $(\mathbb{Z}, +)$.

(2) $(\mathbb{N}^*, +)$ dar $0 \notin \mathbb{N}^*$ $(\mathbb{N}, +)$ parte stab.

parte stabilă $\Rightarrow$ operație bine definită $0 \in \mathbb{N}$

$\mathbb{N} \nsubseteq \mathbb{Z}$.

2.1.10. Dem. Not $H = \bigcap_{i \in I} H_i = \{x \in G \mid x \in H_i, \forall i \in I\}$.

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

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

$x\cdot y^{-1} \in H$ (**).

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

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

$2 \in \mathbb{C}^*$ $\langle 2 \rangle = \{2, 2^2 = 4, 2^3, 16, \dots, 2^4, \dots, 1 = 2^0, 2^{-1} = \frac{1}{2}, 2^{-2}, \dots\}$

$= \{2^n \mid n \in \mathbb{Z}\} \leq \mathbb{C}^*$

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

Dem. 2.1.14. Notăm

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

Arătăm că $H \leq G$ (1) OK.

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

$y_1, \dots, y_m \in X \cup X^{-1}$

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

• 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

$$x^{-1} = (x_1 x_2 \dots x_n)^{-1} = x_n^{-1} \dots x_2^{-1} x_1^{-1} \in H$$

Arătăm $X \subseteq H$ (2) ✓

Fie $x \in X$; notăm $x_1 = x \in X$, pt $n=1$ obținem $x = x_1 \in H$. (produs cu un singur factor)

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

Fie $K \leq G$ cu prop. $X \subseteq K \overset{K \leq G}{\Longrightarrow} X^{-1} \subseteq K$

Fie $x \in H \Rightarrow x = x_1 x_2 \dots x_n$, $x_1, x_2, \dots, x_n \in X \cup X^{-1}$ $\Big\} \overset{K \leq G}{\underset{\text{p-stab.}}{\Longrightarrow}} x_1 x_2 \dots x_n \in K \Downarrow x \in K$.

Deci $H \subseteq K$.

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

Dem. (a) $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \;\Big|\cdot f(1)^{-1} \Rightarrow 1 = f(1)$.

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

(b) Fie $x \in G \Rightarrow \exists\, x^{-1} \in G$: $x \cdot x^{-1} = 1 = x^{-1} \cdot x \Rightarrow$

$$f(x \cdot x^{-1}) = f(1) = f(x^{-1} \cdot x) \overset{f}{\underset{\text{morf.}}{\Longrightarrow}}$$

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

Dem 2.1.20.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dr, "g \circ f"'] & H \arrow[d, "g"] \\ & K \end{tikzcd}$$

f, g morfisme de gr. $\overset{\mathcal{X}}{\Longrightarrow} g \circ f$ morf.

Fie $x, y \in G$

$$(g \circ f)(x \cdot y) = g(f(xy)) \overset{f}{\underset{\text{morf}}{=}} g(f(x) \cdot f(y)) \overset{g}{\underset{\text{morf}}{=}} g(f(x)) \cdot g(f(y)) = (g \circ f)(x) \cdot (g \circ f)(y).$$

De acum știm că f este izomorfism cu condiția (ri) bij.

$\Rightarrow \exists\, f^{-1}: H \to G$ a.î. $f \circ f^{-1} = 1_H$, $f^{-1} \circ f = 1_G$. Mai mult f^{-1} este bij.

Fie $x', y' \in H$; not $x = f^{-1}(x') \in G$, $y = f^{-1}(y') \in G$. Este clar

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

$$f^{-1}(x' \cdot y') = f^{-1}(f(x) \cdot f(y)) \overset{f}{\underset{\text{morf}}{=}} f^{-1}(f(xy)) = 1_G(xy) = x \cdot y = f^{-1}(x') f^{-1}(y').$$

Deci f^{-1} este morf. $\Rightarrow$ izomorfism. $\boxtimes$

Demonstraţie. □

Propoziţie 2.1.14. *Fie $(G, \cdot)$ un grup şi $X \subseteq G$ o submulţime 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 conţine toate elementele ~~orzedin~~ din G care se pot scrie ca un produs finit de elemente din $X \cup X^{-1}$.

Demonstraţie. □

Observaţie 2.1.15. Fie $(G, \cdot)$ un grup şi $x \in G$. Pentru orice $n \in \mathbb{Z}$ se defineşte:

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

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

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

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

(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 $\langle x, y \rangle = \{x^n y^m \mid n, m \in \mathbb{Z}\}$.* $X = \{x, y\}$

Homomorfisme de grupuri. = morfisme de grupuri

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

Exemplu 2.1.18. Pentru orice două grupuri G şi H funcţiile 1_G şi $e : G \to H$, $e(x) = 1$ sunt un izomorfism respectv un homomorfism de grupuri. Dacă $G \leq H$ atunci funcţia de incluziune $i : G \to H$ este un homomorfism. $1_G : G \to G$.

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

(a) $f(1) = 1$.

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

Demonstraţie. □

Lemă 2.1.20. *Compunerea a două homomorfisme este de asemenea un homomorfism. Funcţia inversă a unui izomorfism de grupuri este de asemenea un izomorfism.*

Demonstraţie. □

Definiţie 2.1.21. Fie $f : G \to H$ un homomorfism. Numim *nucleul* respectiv *imaginea* lui f mulţimile

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

Propoziţie 2.1.22. *Dacă $f : G \to H$ este un homomorfism, atunci:*

Dem. 2.1.22. $f: G \to H$ morf.

(a) • $G \ni 1$ $f(1) = 1 \in H \Rightarrow 1 \in \operatorname{Ker} f$.

• $x, y \in \operatorname{Ker} f \Rightarrow f(x) = 1 = f(y)$

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

• $x \in \operatorname{Ker} f \Rightarrow f(x) = 1$

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

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

(b) • $1 = f(1) \in \operatorname{Im} f$

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

$x' \cdot y' = f(x) \cdot f(y) \underset{\text{morf}}{\overset{f}{=}} f(\underset{\in G}{x \cdot y}) \in \operatorname{Im} f$.

• $x' \in \operatorname{Im} f \Rightarrow \exists\, x \in G : f(x) = x'$

$(x')^{-1} = f(x)^{-1} = f(\underset{\in G}{x^{-1}}) \in \operatorname{Im} f$.

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

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

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

„$\Leftarrow$" Fie $x, y \in G$ a.î. $f(x) = f(y) \mid \cdot f(y)^{-1} \Rightarrow f(x) f(y)^{-1} = 1$

$\exists\, f(y)^{-1} \in H$

$\Rightarrow f(x) f(y^{-1}) = 1 \Rightarrow f(xy^{-1}) = 1 \Rightarrow x \cdot y^{-1} \in \operatorname{Ker} f$

Din ipoteză $\operatorname{Ker} f = \{1\}$ $\Big\} \Rightarrow$

$xy^{-1} = 1 \mid \cdot y \Rightarrow x = y$. Deci f este inj.

(a) $\mathrm{Ker} f \leq G$.
(b) $\mathrm{Im} f \leq H$.
(c) *f este injectiv ddacă* $\mathrm{Ker} f = \{1\}$.
(d) *f este surjectiv ddacă* $\mathrm{Im} f = H$ (reformulare cunoscută pt. surjectivitate)

Demonstraţie. □

Grupuri ciclice şi ordinul unui element.

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

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

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

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

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

Demonstraţie. □

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

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

Acţiuni ale grupurilor pe mulţimi.

Definiţie 2.1.28. Fie A o mulţime şi $(G, \cdot)$ un grup. Se numeşte *acţiune (la stânga)* a lui G pe A o funcţie $\alpha : G \times A \to A$ cu proprietăţile:
(1) $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ pentru orice $g, h \in G$ şi orice $x \in A$.
(2) $\alpha(1, x) = x$ pentru orice $x \in A$.

Observaţie 2.1.29. Adesea funcţia $\alpha : G \times A \to A$ este văzută ca o operaţie (înmulţire) externă, în sensul că operanzii nu sunt luaţi din aceeasşi mulţime, şi este notată prin $gx = \alpha(g, x)$. În acest caz, egalităţile (1) şi (2) din definiţia 2.1.28 devin:

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

Teoremă 2.1.30. *Fie A o mulţime şi $(G, \cdot)$ un grup.*
(a) *Dacă $G \times A \to A$, $(g, x) \mapsto gx$ este o acţiune a lui G pe A, atunci $\phi : G \to \mathrm{S}(A)$, $\phi(g) : A \to A$, $\phi(g) : x \mapsto gx$ este un homomorfism de grupuri.*
(b) *Dacă $\phi : G \to \mathrm{S}(A)$ este un homomorfism de grupuri, atunci $G \times A \to A$, $(g, x) \mapsto \phi(g)(x)$ este o acţiune a lui G pe A.*

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

„$\Rightarrow$". Știm $\operatorname{ord}(x)=n$, Atunci $x^n=1$

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

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

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

Deci $m=n\cdot q \Rightarrow n\mid m$.

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

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

Pe de altă parte din def. ordinului m este cel mai mic în $\mathbb{N}^*$ cu prop. $x^m=1$ deci $m\le n$.

Prin urmare $n=m=\operatorname{ord}(x)$. $\boxtimes$.

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

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

Cat I. $\operatorname{ord}(x)=\infty$. Vom arăta că $\overbrace{x^k=x^t}^{k,t\in\mathbb{Z}} \overset{?}{\Rightarrow} k=t$.

$$\left.\begin{array}{l} x^k=x^t \mid\cdot x^{-t} \Rightarrow x^{k-t}=1 \Rightarrow x^{|k-t|}=1 \\ \exists\, x^{-t}\in G \qquad\qquad |k-t|\in\mathbb{N} \\ \qquad\qquad\qquad\qquad \operatorname{ord}(x)=\infty \end{array}\right\} \Rightarrow |k-t|=0$$

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

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

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

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

$\forall\, x^m\in\langle x\rangle$ $(m\in\mathbb{Z})$

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

$x^m = x^{n\cdot q+r} = (x^n)^q\cdot x^r = 1^q\cdot x^r = 1\cdot x^r = x^r\in\{1,x,x^2,\dots,x^{n-1}\}$

$$\left.\begin{array}{l} k,t\in\{0,\dots,n-1\} \quad x^k=x^t \xrightarrow{\mid\cdot x^{-t}} x^{k-t}=1 \Rightarrow n\mid(k-t) \\ \text{Dar } k-t\in\{-n+1,-n+2,\dots,-1,0,1,\dots,n-1\} \end{array}\right\} \Rightarrow$$

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

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

(a) G ciclic $\Rightarrow \exists\, x \in G$: $\left.\begin{array}{l} G = \langle x \rangle \\ |G| = \infty \end{array}\right\} \overset{(a)}{\Rightarrow} |\langle x \rangle| = \infty \Rightarrow$

$\Rightarrow ord(x) = \infty$ (sunteem în cazul I de demonstrație).

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

Am arătat în cazul aI că f este inj.

f este surj. pt. că $G = \langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$ $\Big\} \Rightarrow f$ bij.

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

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

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

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

Sunteem în cazul IIa.

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

Bine definită $\hat{k} = \hat{m} \Leftrightarrow n \mid (k-m) \Rightarrow x^{k-m} = 1 \Rightarrow$

$x^k \cdot x^{-m} = 1 \mid \cdot x^m \Rightarrow x^k = x^m$. ok.

f este inj. cum am arătat la (I.a).

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

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

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

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

ρ = rotația în sens trigonometric în jurul lui 0 cu $\frac{\pi}{2}$

$\left\{ \underset{\rho^4}{\overset{\rho^0 = 1}{\parallel}}, \underset{\rho}{\overset{\rho^1}{\parallel}}, \rho^2, \rho^3 \right\} \cong (\mathbb{Z}_4, +)$

(c) *Procedeele de la (a) şi (b) descriu func ctii mutual inverese între mulţimea tuturor acţiunilor lui G pe A şi mulţimea tuturor homomorfismeleor de grupuri $G \to \mathrm{S}(A)$.*

Demonstraţie. □

Definiţie 2.1.31. Fie $G \times A \to A$, $(g, x) \mapsto gx$ o acţiune a grupului $(G, \cdot)$ pe mulţimea A. Se numeşte *reprezentare prin permutări* a acestei acţiuni homomorfismul de grupuri $\phi : G \to \mathrm{S}(A)$ concstruit în Teorema 2.1.30. Acţiunea se zice *fidelă*, dacă reprezentarea ei prin permutări este un homomorfism injectiv.

Propoziţie 2.1.32. *Fie $G \times A \to A$, $(g, x) \mapsto gx$ o acţiune a grupului $(G, \cdot)$ pe mulţimea A. Relaţia $(A, A, \equiv)$ dată prin $x \equiv y$ ddacă există $g \in G$ astfel încât $gx = y$, pentru orice $x, y \in A$ este o relaţie de echivalenţă, a carei clase de echivalenţă (numite* orbite*) se determină ca fiind $Gx = \{gx \mid g \in G\}$, mit $x \in A$.*

Demonstraţie. □

Corolar 2.1.33. *Notăm cu $[A/_{\equiv}]$ un sistem de reprezentanţi pentru mulţimea tuturor orbitelor unei acţiuni $G \times A \to A$ a grupului $(G, \cdot)$ pe mulţimea A. Atunci este valabilă egalitatea:*

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

Demonstraţie. □

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* $\mathrm{ord}(x)$ *divide $|G|$.*

$\mathrm{ord}(x) = |\langle x \rangle|$

Demonstraţie. □

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

Grupul simetric.

Definiţie 2.1.36. Fie n un număr natural şi G un subgrup al grupului simetric $\mathrm{S}_n = \mathrm{S}(\{1, 2, \ldots, n\})$. Acţiunea lui G pe $\{1, 2, \ldots, n\}$ a cărei reprezentare prin permutări este funcţia de incluziune $i : G \to \mathrm{S}_n$ este numită acţiunea canonică. Pentru $\sigma \in \mathrm{S}_n$ se numesc *σ-orbite* orbitele acţinii canonica a grupului $G = \langle \sigma \rangle$. O σ-orbită se zice *trivială* dacă ea conţine un singur element. Un *ciclu* este o permutare care are o singură orbită netrivială. În acest caz, cardinalul acestei orbite (netriviale) este numită *lungimea* ciclului. Doă cicluri se zic *disjuncte* în cazul î n care orbitelel lor netriviale sunt disjuncte (ca mulţimi).

Observaţie 2.1.37. Fie $\sigma \in \mathrm{S}_n$.

(1) $\sigma = e$ (e este permutatarea 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 exsită o submulţime $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$, astfel încât $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \ldots, \sigma(i_n) = i_1$ şi $\sigma(i) = i$ pentru $i \notin \{i_1, i_2, \ldots, i_k\}$. În acest caz $\{i_1, i_2, \ldots, i_k\}$ este singura orbită netrivială a lui σ şi notăm $\sigma = (i_1 i_2, \ldots, i_k)$.

Teorema lui Lagrange

2.1. Th. (a). G grup, $H \leq G$

Definim relația ρ_H pe G prin $x \rho_H y \iff x^{-1} \cdot y \in H$, $\forall x, y \in G$.

(A) Arătăm că ρ_H este o rel. de echivalență

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

(T). $x, y, z \in G$ $\quad x \rho_H y,\ y \rho_H z \Rightarrow x^{-1} \cdot y \in H,\ y^{-1} z \in H \xrightarrow[\text{p. stab.}]{\text{op}}$

$x^{-1} y \cdot y^{-1} z \in H \Rightarrow x^{-1} z \in H \Rightarrow x \rho_H z.$

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

$y^{-1} x \in H \Rightarrow y \rho_H x.$

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

$xH = \{x \cdot h \mid h \in H\} \overset{?}{=} \{y \in G \mid x \rho_H y\}$

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

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

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

φ_x este surj pt. că $xH = \{xh \mid h \in H\}$.

Pt inj. $\varphi_x(h) = \varphi_x(k)$, $h, k \in H \Rightarrow \underset{x^{-1}|}{} xh = xk \Rightarrow h = k$ OK.

Obs $1H = H$

Avem $G = \bigcup_{x \in G} (xH)$ (propr. de la partiție)

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

Dacă $|G| < \infty \Rightarrow |H| \mid |G|$. $\boxtimes$.

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

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

Demonstraţie. □

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

Demonstraţie. □

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

Demonstraţie. □

Observaţie 2.1.41. Se numeşte decompunerea lui σ ca produs de cicluri duoă câte două disjuncte dată în Teorema 2.1.40. Uneori această descompunere conţine de asemenea şi cicluri triviale $(i) = e$, unde $i \in \{1, 2, \ldots, n\}$ cu proprietatea $\sigma(i) = i$, incluzând cazul $\sigma = e$ din Teorema precedentă.

Definiţie 2.1.42. O *inversiune* pentru $\sigma \in \mathrm{S}_n$ este o pereche $(i, j) \in \{1, 2, \ldots, n\}^2$, astfel încât $i < j$ şi $\sigma(i) > \sigma(j)$. e notează cu $m(\sigma)$ numărul de inversiuni şi se defineşte *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.*

Demonstraţie. □

Exerciţii la grupuri.

Exerciţiu 2.1.44. Se consideră mulţimea

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

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

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

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

Exerciţiu 2.1.47. Fie $(G_i, \cdot)$ o familie de grupuri. Să se arate că $\left(\prod_{i\in I} G, \cdot\right)$ 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 $p_j : \prod_{i\in I} \to G_j$, $p_j(x_i)_{i\in I} = x_j$ este un homomorfism surjectiv pentru orice $j \in I$.

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

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

Exerciţiu 2.1.50. Se consideră un grup $(G, \cdot)$, şi se notează $\mathrm{Sub}(G) = \{H \subseteq G \mid H \leq G\}$ mulţimea tuturor subgrupurilor. Să se arată că $(\mathrm{Sub}(G), \leq)$ este o latice.

Exerciţiu 2.1.51. Fie $A_1A_2 \dots A_n$ un poligon regulat (cu n vârfuri şi n laturi) cu centrul O într-un plan α. (considerat ca o mulţime de puncte). O izometrie este o funcţie $f : \alpha \to \alpha$ cu proprietatea că $|f(X)f(Y)| = |XY|$ pentru orice $X, Y \in \alpha$, unde prin $|XY|$ notăm distanţa dintre X şi Y. Se consideră mulţimea tuturor izometriilor care invariază poligonul $A_1A_2 \dots A_n$ mai precis

$$D_n = \{f : \alpha \to \alpha \mid f \text{ este o izometrie şi } f(A_1A_2 \dots A_n) = A_1A_2 \dots A_n\}.$$

Notăm cu s rotaţia în jurul centrului O cu $\frac{2\pi}{n}$ radiani, (de la A_1 către A_2) şi cu t simetria axială faţa de axa A_1O. Să observăm că $s, t : \alpha \to \alpha$ sunt izometrii. Să se arate că

(1) $s^n = 1 = t^2$ (aici $1 = 1_\alpha$ este funcţia 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 funcţiilor (care este numit *grupul diedral*)
(5) Să se determine $\langle s \rangle$, $\langle t \rangle$, $\langle s, t \rangle$

Să se construiască tablele operaţiilor D_3 şi D_4.

Exerciţiu 2.1.52. Pe mulţimea $H = \{1, -1, i, -i, j, -j, k, -k\}$ se defineşte în felul următor o înmulţire:

- 1 este elementul neutru.
- Înmulţirea respectă regula semnelor: $(-x)y = x(-y) = -xy$ (altfel semnele $+$ şi $-$ 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*).

Exerciţiu 2.1.53. Să se arete că grupurile $(\mathbb{R}, +)$ şi $(\mathbb{R}_+^*, \cdot)$ sunt izomorfe.

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

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

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

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

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

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

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

Exerciţiu 2.1.60. Fie $(G, \cdot)$ un grup şi $H, K \leq G$. Să se arate că $H \cup K \leq G$ ddacă $H \subseteq K$ sau $K \subseteq H$.

Exerciţiu 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 $k = \mathrm{lcm}(n, m)$.
(c) $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, unde $d = \gcd(n, m)$.

$n\mathbb{Z} + m\mathbb{Z} = \{an + bm \mid a, b \in \mathbb{Z}\}$

$1 = (-2)3 + 1 \cdot 7 = 5 \cdot 3 + (-2) \cdot 7$

Exerciţiu 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 $d = sn + tm$. Folosiţi acest rezultat ca să arătaţi că $1 = \gcd(n, m)$ ddacă există $s, t \in \mathbb{Z}$ astfel încât $1 = sn + tm$.

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

Exerciţiu 2.1.64. Să se găsească toate grupurile (pâna la un izomorfism) care se pot defini pe o mulţime cu 4 elemente.

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

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

Exerciţiu 2.1.66. Fie $f : G \to H$ un homomorfism de grupuri. Dacă $x \in G$ este de ordin finit, atunci tot aşa este şi $f(x)$, şi avem $\mathrm{ord}(f(x)) | \mathrm{ord}(x)$.

Exerciţiu 2.1.67. Două grupuri ciclice infinite sunt izomorfe. Două grupuri ciclice finite sunt izomorfe ddacă au acelaşi număr de elemente.

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

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

Exerciţiu 2.1.70. Fie $G \times A \to A$, $(g, x) \mapsto gx$ o acţiune a grupului $(G, \cdot)$ pe mulţimea A. Să se arate că:

(a) Pentru orice $x \in A$ submulţimea $\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}$ formează un subgrup a lui G.
(b) Mulţimea $K = \{g \in G \mid gx = x \text{ für alle } x \in A\}$ este un subgrup a lui G (acest subgrup este numit *nucleul* acţiunii. Mai mult avem: $K = \bigcap_{x \in A} \mathrm{Stab}_G(x)$.
(c) Acţiunea este fidelă ddacă nucleul este trivial, adică $K = \{1\}$.

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

(a) Să se definească o acţiune netrivială a lui H pe N, (adică $\cdot : H \times N \to N$) aşa încât $h \cdot 1 = h$ pentru orice $h \in H$.
(b) Care este nucleul acestei acţiuni?
(c) Pentru $h \in H$ se consideră $\phi_h : N \to N$, $\phi_h(n) = h \cdot n$. Să se arate că ϕ_h este un izomorfism.
(d) Considerăm $G = N \times H$ ca mulţimi. Se defineşte o operaţie 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 operaţie este un grup neabelian cu 12 elemente.

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

Exerciţiu 2.1.73. Dacă mulţimile A şi B au acelaşi cardinal, atunci grupurile $\mathrm{S}(A)$ şi $\mathrm{S}(B)$ sunt izomorfe.

Exerciţiu 2.1.74. Să se descompună $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 5 & 6 & 4 & 8 & 7 \end{pmatrix} \in \mathrm{S}_8$ ca produs de cicluri două câte două disjuncte.

Exerciţiu 2.1.75. Fie $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}, \tau == \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \in \mathrm{S}_5$.
(a) Să se descompună σ şi 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 $\mathrm{ord}(\sigma)$ şi $\langle\sigma\rangle$.
(d) Să se calculeze $\epsilon(\sigma)$ şi $\epsilon(\tau)$.

Exerciţiu 2.1.76. Să se arate că
(a) $\epsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$ pentru orice $\sigma \in \mathrm{S}_n$.
(b) $\epsilon : \mathrm{S}_n \to \{1, -1\} = U_2$ (vezi Exerţiul 2.1.56) este un homomorfism.
(c) $\mathrm{Ker}\epsilon = \mathrm{A}_n$, unde $\mathrm{A}_n = \{\sigma \in \mathrm{S}_n \mid \sigma \text{ este pară}\}$.

Exerciţiu 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 transpoziţii, dar această descompunere nu mai este unică. Reamintiim că o transpoziţie este un ciclu de lungime 2.

Exerciţiu 2.1.78. Fie $\sigma \in \mathrm{S}_n$ 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) $\mathrm{ord}(\sigma) = l$.

Exerciţiu 2.1.79. Să se arate că $(12)(3456) \in \mathrm{S}_6$ este o permutare para care nu este patratul nici unei alte permutări din S_6.

2.2. **Inele şi corpuri.**

Definiţie 2.2.1. Un *inel* este un triplet $(R, +, \cdot)$, care constaă dintr-o mulţime R împreună cu două operaţii $+, \cdot : R \times R \to R$, astfel încât
(a) $(R, +)$ este un grup abelian.
(b) $\cdot$ este asociativă.

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

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

Inelul R se zice *comutativ* sau *unitar*, după cum operaţia $\cdot$ este şi comutativă, respectiv are unitate.

Observaţie 2.2.2. Într-un inel R se notează cu 0 elementul neutru pentru $+$ şi cu 1 elementul neutru pentru $\cdot$ (dacă acesta din urmă există). Ordinea operaţiilor este cea obişnuită, mai precis mai întâi acţionează înmulţirea şi pe urmă adunarea.

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

(b) Dacă R este un inel comutativ, atunci $(\mathbb{M}_{n\times n}(R), +, \cdot)$ este de asemenea inel; totuşi $(\mathbb{M}_{n\times n}(R), +, \cdot)$ nu este în mod necesar comutativ. Dacă R este unitar aunci to aşa este şi $(\mathbb{M}_{n\times n}(R), +, \cdot)$, iar elementul neutru pentru înmulţirea matricilor este aşa 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 numeşte *de pătrat nul*. In particular $R = \{0\}$ este un inel (unitar!), unde $0 + 0 = 0 \cdot 0 = 0$ (acest inel se numeşte *inelul nul* şi este notat $R = 0$).

(d) Dacă $(R, +, \cdot)$ este un inel, atunci tot aşa este şi $R^o, +.*$, unde $R^o = R$ şi $x * y = yx$ pentru orice $x, y \in R$; R^o se numeşte *inelul opus* lui R.

Propoziţie 2.2.4. *(Reguli de calcul in inele) Fie R un inel şi $x, y, x \in R$. Avem:*

(a) $x0 = 0x = 0$.

(b) $x(-y) = (-x)y = -xy$.

(c) $x(y - z) = xy - xz$ *şi* $(y - z)x = yx - zx$.

(d) *Dacă $R \neq 0$ este un inel unitar, atunci $1 \neq 0$.*

Demonstraţie. □

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

Observaţie 2.2.6. În conformitate cu Propoziţia 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 şi subcorpuri.

Definiţie 2.2.8. Fie $(R, +, \cdot)$ un inel. Un *subinel* a lui R este o submulţime $S \subseteq R$, cu proprietatea că operaţiile $+$ şi $\cdot$ din R induc operaţii 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 $+$ şi $\cdot$), iar cu operaţiile 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 $\{0\}$ şi R.

Propoziţie 2.2.10 (Teorema de caractcterizare a subinelelor)**.** *Fie $(R, +, \cdot)$ un inel şi fie $S \subseteq R$ o submulţime. Următoarele afirmaţii 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) $x, y \in S \Rightarrow xy \in S$.

Demonstraţie. □

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

Observaţie 2.2.12. Reuniunea a două sau mai multe subinele, nu este cu necesitate subinel (a se vedea şi Observaţia 2.1.11). 2.1.11).

Definiţie 2.2.13. Fie $(K, +, \cdot)$ un corp. Un *subcorp* a lui K este o submuţime $L \subseteq K$ cu proprietatea că operaţiile $+$ şi $\cdot$ din R induc operaţii bine definite pe S, iar cu operaţiile induse L formează un corp. Se scrie $L \leq K$.

Observaţie 2.2.14. Un subcorp este un subinel unitar

Propoziţie 2.2.15 (Teorema de caractcterizare a subcorpurilor)**.** *Fie $(K, +, \cdot)$ un corp şi fie $L \subseteq K$ o submulţime. Următoarele afirmaţii 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) $x, y \in L^* \Rightarrow xy^{-1} \in S$.

Demonstraţie. □

Observaţie 2.2.16. Ca şi în cazul grupurilor putem defini subinelul sau subcorpul generat.

Homomorfisme.

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

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

Lemă 2.2.19. *Un homomorfim de corpuri este sau unitar sau nul.*

Demonstraţie. □

Lemă 2.2.20. *Compunerea a două homomorfisme de inele (corpuri) este de asemenea un homomorfism. Funţia inversă a unui izomorfism de inele (corpuri) este de asemenea un izomorfism.*

Demonstraţie. □

Elemente speciale într-un inel

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

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

Definiţie 2.2.21. Fie R un inel. Un element $x \in R$ se numeşte:

(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 şi la dreapta.
(2) *idempotent* dacă este adevărată egalitatea $x^2 = x$.
(3) *nilpotent* dacă există $n \in \mathbb{N}$, astfel încât $x^n = 0$.

Observaţie 2.2.22. Fie $R \neq 0$ un inel şi 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 conţine divizori netriviali ai lui zero.
(b) 0 şi 1 (dacă există $1 \in R$, ceea ce înseamnă R este unitar) sunt elemente idempotente; aceşti idempotenţi sunt numiţi triviali.
(c) Dacă x este idempotent, atunci este valabilă egalitatea $x^n = x$, pentru orice $n \in \mathbb{N}^*$.
(d) Dacă x este nilpotent şi $x^n = 0$ 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 $[6]_{12}^2 = [0]_{12}$.

Propoziţie 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) ddacă 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.

Demonstraţie. □

Definiţie 2.2.25. Un *domeniu de integritate* este un inel comutativ, unitar şi fără divizori ai lui zero.

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

Demonstraţie. □

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 şi domenii deintegritate. $\mathbb{Z}$ este un domeniu de integritate care nu este corp.

Propoziţie 2.2.29. *Un doemeniu de interitate finit este un corp (comutativ).*

Demonstraţie. □

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

Exerciţii la inele şi corpuri.

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

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

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

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

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

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

Exerciţiu 2.2.33. Se consideră o mulţime oarecare A şi un inel R. Pe mulţimea $R^A = \{f : A \to R \mid f \text{ este o funţie}\}$ se definesc operaţiile $+, \cdot : R^A \times R^A \to R^A$ prin $f + g, fg : A \to R$, $(f + g)(x) = f(x) + g(x)$ şi $(fg)(x) = f(x)g(x)$ pentru orice $f, g \in R^A$ şi 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 aceeşi proprietate.

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

Exerciţiu 2.2.35. Se consideră grupul quaternionilor $H = \{\}$ (vezi Exerciţiul 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

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

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

(adică înmulţirea în $\mathbb{H}$ este indusă de în mulţirea în H).

Exerciţiu 2.2.36. Fie R un inel comutativ şi unitar. Să se verifice că mulţimea tuturor polinoamelor

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

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

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

Exerciţiu 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 ddacă n este un număr prim.

Exerciţiu 2.2.39. Să se rezolve următoarele ecuaţii în $\mathbb{Z}_6$: $[4]_6 x + [5]_6 = [1]_6$ şi $[5]_6 x + [3]_6 = [1]_6$

Exerciţiu 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 $(\mathbb{M}_{2\times 2}(\mathbb{Z}), +, \cdot)$, şi $R \cong \mathbb{Z} + i\mathbb{Z}$. Sunt $\mathbb{Z} + i\mathbb{Z}$ şi/sau R domenii de integritate? Dar corpuri?

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

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

Exerciţiu 2.2.43. Fie R un inel comutativ şi unitar. Să se arate că inelele $\mathbb{M}_{n\times n}(R)$ şi $\mathbb{M}_{n\times n}(R)^o$ sunt izomorfe. De aici să se deducă echivalenţa următoarelor afirmaţii, 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.

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

Exerciţiu 2.2.45. Să se arate că următoarele corpuri nu sunt izomorfe: $\mathbb{R}$ şi $\mathbb{C}$.

Exerciţiu 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 $\mathbb{C}$.

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

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

Exerciţiu 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 corpuri comutative sunt în special $K = \mathbb{R}$ sau $K = \mathbb{C}$ dar cazurile $K = \mathbb{Q}$ sau $K = \mathbb{Z}_p$, şie $p \in \mathbb{N}$ este un număr prim sunt de asemenea posibile.

$K \in \{\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}_p\}$

$(K, +, \cdot)$

3.1. Spaţii vectoriale si aplicaţii liniare.

Definiţie 3.1.1. Un *spaţiu vectorial* peste K sau mai scurt *K-spaţiu vectorial* este format dintr-un grup abelian $(V, +)$ împreună cu o operaţie externă $\cdot : K \times V \to V$ care satisface 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 $x, y \in V$ şi orice şi orice $\alpha, \beta \in K$. Se scrie ${}_KV$. Elementele din V şi K sunt numite *vectori* respectiv *scalari*. Adunarea în V şi operaţia externă se numesc *adunarea vectorilor* respectiv *înmulţirea cu scalari*. Spaţiile vectoriale sunt numite uneori *spaţii liniare*.

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

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

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

şi cu înmulţirea cu scalari: $(x_1+y_1, x_2+y_2, \ldots, x_n+y_n)$

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

$M_{m\times 1}(K)$

$\parallel$

$\left\{ \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} \middle| x_i \in K \right\}$

(3) $\mathbb{M}_{m\times n}(K)$ este un K-spaţiu vectorial cu adunarea matricilor şi cu înmulţirea unei matrici cu un scalar, adică pentru $A = [a_{i,j}]$ şi $B = [b_{i,j}]$ şi $\alpha \in K$, avem $A + B = [a_{i,j} + b_{i,j}]$ şi $\alpha A = [\alpha a_{i,j}]$. ce obţinem când punem $m = 1$? Dar pentru $n = 1$?

(4) Dacă K este un corp ~~şi~~ subc L ~~este un subcorp~~ i-L, atunci L este un K-spaţiu vectorial, unde adunarea vectorilor este adunarea în L, iar înmulţirea cu scalari este:

$\mathbb{Q} \times \mathbb{R} \to \mathbb{R}$

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

(5) Mulţimea tuturor polinoamelor

$$K[X] = \{a_0 + a_1X + \ldots + a_nX^n \mid n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in K\}$$

este un K-spaţiu vectorial în raport cu adunarea polinoamelor (vectori) şi înmulţirea polimoamelor cu scalari din K.

(6) Mulţimea tuturor vectorilor liberi din plan (sau din spaţiu) în raport cu adunarea vectorilor liberi şi die obişnuita înmulţire cu scalari este un $\mathbb{R}$-spaţiu vectorial.

Propoziţie 3.1.3. *(Reguli de calcul în spaţii vectoriale) Fie V un K-spaţiu vectorial, $x, y \in V$ şi $\alpha, \beta \in K$. Avem:*

(a) $\alpha 0 = 0 = 0x$. $\alpha \cdot \vec{0} = \vec{0} = 0x$
(b) $\alpha(-x) = (-\alpha)x = -\alpha x$.
(c) $\alpha(x - y) = \alpha x - \alpha y$ *şi* $(\alpha - \beta)x = \alpha x - \beta x$.
(d) $\alpha x = 0$ *ddacă* $\alpha = 0$ *sau* $x = 0$. $\alpha \cdot x = \vec{0} \Leftrightarrow \alpha = 0$ sau $x = \vec{0}$

Demonstraţie. □

$\mathbb{R}^2$ = planul real

Vector fixat în $\mathbb{R}^2$: o pereche (A,B) de puncte $A, B \in \mathbb{R}^2$

Se definește o relație numită echipolență prin

$(A,B) \sim (A',B') \iff$ segmentele $[AB']$ și $[A'B]$ au același mijloc.

Această rel. este una de echivalență pe mulțimea vectorilor fixați

Un vector liber este o clasă de echivalență.

$$\overrightarrow{AB} = \{(X,Y) \mid (A,B) \sim (X,Y)\}$$

Notăm cu $V = \{\overrightarrow{AB} \mid A, B \in \mathbb{R}^2\}$ mulțimea factor

V este un $\mathbb{R}$-sp. vectorial în rap. cu adunarea vectorilor și înmulțirea cu scalari (din $\mathbb{R}$) definite după una din metodă

$\overrightarrow{AE} = \overrightarrow{CD}$

(cu regula paralelogramului)

$\alpha \in \mathbb{R}$

$\alpha > 0$ $\quad \alpha\overrightarrow{AB}$ = aceeași direcție același sens $|\alpha\overrightarrow{AB}| = |\alpha| \cdot |AB|$

$\alpha = 0$ $\quad \alpha\overrightarrow{AB} = \vec{0} = \overrightarrow{AA} = \overrightarrow{BB} = \overrightarrow{XX}$, $\forall X \in \mathbb{R}^2$

$\alpha < 0$ $\quad \alpha\overrightarrow{AB}$ = aceeași direcție sens contrar $|\alpha\overrightarrow{AB}| = |\alpha|\,|AB|$

Se arată că $(V,+)$ este un $\mathbb{R}$-sp. vectorial.

(izomorf cu $\mathbb{R}^2$)

3.1.3. Dem $\alpha, \beta \in K$, $x, y \in V$

(a) $\alpha \cdot \mid \vec{0} = \vec{0} + \vec{0}$ $\quad \alpha \cdot \vec{0} = \alpha(\vec{0} + \vec{0}) \overset{SV1}{=} \alpha\vec{0} + \alpha\vec{0}$

$$\alpha\vec{0} = \alpha \cdot \vec{0} + \alpha \cdot \vec{0} \quad \Big| + (-\alpha\vec{0})$$

$$\vec{0} = \alpha \cdot \vec{0}$$

$0 = 0 + 0 \quad \Big| \cdot x \quad \Rightarrow \quad 0 \cdot x = (0+0)x \overset{SV2}{=} 0 \cdot x + 0x$

$$0x = 0 \cdot x + 0 \cdot x \quad \Big| + (-0 \cdot x)$$

$$\vec{0} = 0 \cdot x + \vec{0} = 0 \cdot x$$

(b) $\alpha \mid x + (-x) = \vec{0}$

$$\alpha(x + (-x)) = \alpha \cdot \vec{0}$$

$$\alpha x + \alpha(-x) = \vec{0}$$

$$\alpha \cdot (-x) = -\alpha x$$

$\alpha + (-\alpha) = 0 \quad \Big| \cdot x$

$$(\alpha + (-\alpha))x = 0 \cdot x$$

$$\alpha x + (-\alpha) \cdot x = \vec{0}$$

$$(-\alpha)x = -\alpha x$$

(c) $\alpha(x - y) = \alpha(x + (-y)) = \alpha x + \alpha(-y) = \alpha x - \alpha y$

$(\alpha - \beta)x = (\alpha + (-\beta))x = \alpha x + (-\beta) \cdot x = \alpha x - \beta x.$

(d) „$\Leftarrow$" este deja arătată în (a).

„$\Rightarrow$". $\alpha x = \vec{0}$

Dacă $\alpha \neq 0 \Rightarrow \exists \alpha^{-1} \in K$

$$\alpha^{-1}(\alpha x) = \alpha^{-1}\vec{0} \overset{(SV3)}{\Longrightarrow}$$

$$(\alpha^{-1}\alpha)x = \vec{0}$$

$$1 \cdot x = \vec{0} \overset{(SV11)}{\Longrightarrow}$$

$$x = \vec{0}.$$

Subspaţii vectoriale.

Definiţie 3.1.4. Fie V un K-spaţiu vectorial. Un *subspaţiu (vectorial)* a lui V este o submulţime $U \subseteq V$, cu proprietatea că adunarea vactorilor şi înmulţirea cu scalari induc operaţii bine definite pe U (adică $x, y \in U, \alpha \in K \Rightarrow x + y, \alpha x \in U$), şi U împreună cu operaţiile restricţionate fromează un spaţiu vectorial. Se scrie $U \leq_K V$ sau simplu $U \leq V$.

Exemplu 3.1.5. Orice spaţiu vectorial ${}_K V$ are două subspaţii aş a zise *triviale*, anume $\{0\} \leq_K V$ şi $V \leq_K V$. $0 = \{0\}$

Propoziţie 3.1.6 (de caracterizare a subspaţiilor)**.** *Fie V un K-spaţiu vectorial şi fie $U \subseteq V$ o submulţime. Următoarele afirmaţii 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) $0 \in U$.
(b) $x, y \in U$, $\alpha, \beta \in K \Rightarrow \alpha x + \beta y \in U$.

Demonstraţie. □

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

Demonstraţie. □

Observaţie 3.1.8. Reuniunea a două sau mai multe subspaţii nu este cu necesitate subspaţiu (vezi de asemenea Observaţia 2.1.11).

Definiţie 3.1.9. Fie V un K-spaţiu vectorial şi $X \subseteq V$ o submulţime a lui V. *Subspaţiul generat* de X este definit prin

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

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

Lemă 3.1.10. *Fie V un K-spaţiu vectorial şi $X \subseteq V$ o submulţime a lui V. Avem:*

(a) $\langle X \rangle_K \leq_K V$.
(b) $X \subseteq \langle X \rangle_K$ *şi* $X = \langle X \rangle_K$ *ddacă* $X \leq_K V$.
(c) $\langle X \rangle_K$ *este cel mai mic subspaţiu a lui V care conţine X i. e.*

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

(d) *Dacă $X \subseteq Y \subseteq G$ atunci $\langle X \rangle_K \leq \langle Y \rangle_K \leq V$.* $(U \subseteq W)$

Demonstraţie. □

Propoziţie 3.1.11. *Fie V un K-spaţiu vectorial şi $X \subseteq V$ o submulţime a lui V. Avem:*

$$\langle X \rangle_K = \{\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n \mid n \in \mathbb{N}, x_1, x_2, \ldots, x_n \in X \text{ şi } \alpha_1, \alpha_2, \ldots, \alpha_n \in K\}.$$

Prop. 3.1.6 Dem. $\boxed{(i) \Rightarrow (ii)}$ evident.

$\boxed{(iii) \Rightarrow (i)}$ $0 \in U$ (din (iic)

U este parte stabil. faţă de $+$ din (iib) $\Big\}$ din ipoteză

$x \in U$ $\quad -x = -1 \cdot x = \underset{\in K}{(-1)} \cdot x \overset{(iic)}{\in} U$

Deci U subgrup în $(V, +)$

$\cdot : K \times U \to U$ este bine def. din (iic)

Prop. (SV1) – (SV4) sunt adev. pt. orice $x, y \in V$, $\forall \alpha, \beta \in K$

deci şi pt. $\forall x, y \in U \subseteq V$, $\forall \alpha, \beta \in K$.

$\boxed{(ii) \Rightarrow (iii)}$ (iii a) este (iia) şi pt. (iii b)

$x, y \in U$, $\alpha, \beta \in K \overset{(iib)}{\Longrightarrow} \alpha x, \beta y \in U \overset{(iib)}{\Longrightarrow} \alpha x + \beta y \in U$.

$\boxed{(iii) \Rightarrow (ii)}$ (iia) este (iiia).

Pt. (iib): Fie $x, y \in U \Rightarrow x + y = 1 \cdot x + 1 y \overset{(iiib)}{\in} U$.

Pt. (iic) Fie $x \in U, \alpha \in K \Rightarrow \alpha x = \alpha \cdot x + \alpha \cdot 0 \in U$. $\boxtimes$

$0 \in U$

Dem. 3.1.7 V este un K-sp. vect $U_i \leq_K V$, $i \in I$

Not $U = \bigcap_{i \in I} U_i = \{x \in V \mid x \in U_i, \forall i \in I\}$

- $0 \in U_i, \forall i \in I$ pt. că $U_i \leq V \Rightarrow 0 \in U$
- Fie $x, y \in U$, $\alpha, \beta \in K$ $\Rightarrow x, y \in U_i, \forall i \in I \Big\} \overset{U_i \leq_K V}{\Longrightarrow} \alpha x + \beta y \in U_i, \forall i \in I$

$\Rightarrow \alpha x + \beta y \in \bigcap_{i \in I} U_i \Rightarrow \alpha x + \beta y \in U$.

Conform prop. de caracterizare $U \leq_K V$. $\boxtimes$.

Dem. 1.3.11. $U := \{\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n \mid n \in \mathbb{N}, x_i \in X, \alpha_i \in K, i = \overline{1,n}\} \subseteq V$

De arătat: $U \leq_K V$ (1) ✓

$X \subseteq U$ (2) ✓

$W \leq_K V,\ X \subseteq W \Rightarrow U \subseteq W$ (3) ✓

Pt (1): • Pt $n=0$ suma finită formeni este 0 deci $0 \in U$.

• $\alpha, \beta \in K$, $x, y \in U \Rightarrow x = \alpha_1 x_1 + \dots + \alpha_n x_n$, $\alpha_i \in K$, $x_i \in X$, $i = \overline{1,n}$

$y = \beta_1 y_1 + \dots + \beta_m x_m$, $\beta_j \in K$, $y_j \in X$, $j = \overline{1,m}$

$$\alpha x + \beta y = \alpha(\alpha_1 x_1 + \dots + \alpha_n x_n) + \beta(\beta_1 y_1 + \dots + \beta_m y_m)$$

$$= \underset{\in K}{(\alpha\alpha_1)} x_1 + \dots + \underset{\in K}{(\alpha\alpha_n)} x_n + \underset{\in K}{(\beta\beta_1)} y_1 + \dots + \underset{\in K}{(\beta\beta_m)} y_m \in U$$

Pt(2): Fie $x \in X \Rightarrow x = \underset{\in K}{1} \cdot \underset{\in X}{x} \in U$

Pt(3): Fie $W \leq_K V$, $X \subseteq W$

Fie $x \in U \Rightarrow x = \alpha_1 x_1 + \dots + \alpha_n x_n$, $\alpha_i \in K$, $x_i \in X$, $i = \overline{1,n}$, $n \in \mathbb{N}$

$x_i \in X \subseteq W$, $i = \overline{1,n}$

$W \leq_K V$ $\Big\} \Rightarrow$

$\Rightarrow x \in W$. Deci $U \subseteq W$ ⊠.

Dem. 3.1.16. $S, T \leq_K V$

$S + T = \{x + y \mid x \in S, y \in T\}$

De arătat: $S + T \leq_K V$ (1) ✓

$S \cup T \subseteq S + T$ (2) ✓

$W \leq_K V$, $S \cup T \subseteq W \Rightarrow S + T \subseteq W$ (3).

Pt (1): • $0 = \underset{\in S}{0} + \underset{\in T}{0} \in S + T$.

• $\alpha, \beta \in K$, $u, v \in S + T \Rightarrow u = x + y$, $v = x' + y'$, $x, x' \in S$, $y, y' \in T$

$$\alpha u + \beta v = \alpha(x+y) + \beta(x'+y') = \underbrace{(\alpha x + \beta x')}_{\in S} + \underbrace{(\alpha y + \beta y')}_{\in T} \in S + T.$$

Pt (2):

$x \in S \Rightarrow x = \underset{\in S}{x} + \underset{\in T}{0} \in S + T \Rightarrow S \subseteq S + T$

$y \in T \Rightarrow y = \underset{\in S}{0} + \underset{\in T}{y} \in S + T \Rightarrow T \subseteq S + T$ $\Big\} \Rightarrow S \cup T \subseteq S + T$.

Pt (3): Fie $W \leq_K V$, $S \cup T \subseteq W$

Fie $u \in S + T \Rightarrow$ $u = x + y$, $x \in S \subseteq W$, $y \in T \subseteq W$, $W \leq_K V$ $\Big\} \Rightarrow x + y \in W \Rightarrow u \in W \Rightarrow S + T \subseteq W$.

⊠

$\langle X \rangle_K = \{\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m \mid m \in \mathbb{N}, \alpha_i \in K, x_i \in X, i = \overline{1,m}\}$

$\alpha_1 x_1 = \alpha_1 x_1 + 0 \cdot x_2 + \ldots + 0 \cdot x_n$

$0 = 0 x_1 + 0 x_2 + \ldots + 0 x_n$

În particular, pentru $X = \{x_1, x_2, \ldots, x_n\}$ avem:

$$\langle x_1, x_2, \ldots, x_n \rangle_K = \{\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n \mid \alpha_1, \alpha_2, \ldots, \alpha_n \in K\}.$$

Demonstraţie. □

Definiţie 3.1.12. Fie V un K-spaţiu vectorial şi $X \subseteq V$. Se numeşte *combinaţie liniară* a vectorilor din X o expresie de forma $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$ cu $n \in \mathbb{N}$, $x_1, x_2, \ldots, x_n \in X$ şi $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. În particular o combinaţie liniară a vectorilor $x_1.x_2, \ldots, x_n \in V$ este o expresie de forma $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$, $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, şi o combinaţie liniară a vectorilor $x, y \in V$ este $\alpha x + \beta y$, cu $\alpha, \beta \in K$.

Observaţie 3.1.13. Propoziţia 3.1.11 spune că subspaţiul generat de X conţine toţi vectorii care se pot scrie ca V care se pot scrie în formă de combinaţii liniare de elemente ale lui X.

Corolar 3.1.14. *Fie V un K-spaţiu 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 şi suma directă a subspaţiilor.

Definiţie 3.1.15. Fie V un K-spaţiu vectorial şi fie $S, T \leq_K V$ două subspaţii. Suma acestor subspaţii este definită ca fiind $S + T = \{x + y \mid x \in S, y \in T\}$.

Propoziţie 3.1.16. *Fie V un K-spaţiu vectorial şi fie $S, T \leq_K V$ două subspaţii. Atunci avem $\langle S \cup T \rangle_K = S + T$. In particular suma a două subspaţii este un subspaţiu.*

Demonstraţie. $S + T = \{v \in V \mid \exists x \in S, \exists y \in T : v = x + y\}$ □

Corolar 3.1.17. *Într-un K-spaţiu vectorial V notăm cu $\mathrm{Sub}_K(V) = \{S \mid S \leq_K V\}$ mulţimea tuturor subspaţiilor. Atunci $(\mathrm{Sub}_K(V), \leq_K)$ este o latice în care $\inf\{S, T\} = S \cap T$ şi $\sup\{S, T\} = S + T$.*

Demonstraţie. □

Elementele unei sume $S + T$ a două subspaţii $S, T \leq_K V$ sunt vectorii care se pot scrie ca o sumă între un vector din S şi un vector din T. Suntem interesaţi îndeosebi de cazul în care această scriere este unică.

Propoziţie 3.1.18. *Fie V un K-spaţiu vectorial şi fie $S, T \leq_K V$ două subspaţii. Următoarele afirmaţii sunt echivalente:*

(i) *$S \cap T = 0$;*
(ii) *Scrierea oricăriu vector din $S + T$ ca o sumă dintre un vector din S şi unul din T este unică, i. e. pentru $v \in S + T$ avem $v = x + y = s + t$ cu $x, s \in S$ şi $y, t \in T$ implică $x = s$ şi $y = t$.*

Demonstraţie. □

Definiţie 3.1.19. Se numeşte *directă* o sumă $S + T$ a două subspaţii S şi T care satisface condiţiile echivalente din Propoziţia 3.1.18. În acest caz se scrie $S \oplus T = S + T$.

Observaţie 3.1.20. Fie V K-spaţiu vectorial şi fie $S, T \leq_K V$ două subspaţii. Atunci $V = S \oplus T$ ddacă $S \cap T = 0$ şi $S + T = V$.

Dem. 3.1.18 . $\boxed{(i) \Rightarrow (ii)}$ Fie $v \in S+T$ cu prop. că

$v = x+y = s+t$, $x, s \in S$, $y, t \in T$

$$\underbrace{x-s}_{\in S} = \underbrace{t-y}_{\in T} \Rightarrow \left.\begin{array}{l} x-s = t-y \in S\cap T \\ S\cap T = \{0\} \end{array}\right\} \Rightarrow x-s = 0 = t-y$$

$$\Downarrow$$

$$x = s, \ t = y.$$

$\boxed{(ii) \Rightarrow (i)}$. $S, T \leq_K V \Rightarrow 0 \in S, 0 \in S \Rightarrow 0 \in S\cap T$

$\{0\} \subseteq S\cap T.$

Fie $v \in S\cap T \Rightarrow v = \underset{S}{v} + \underset{T}{0} = \underset{S}{0} + \underset{T}{v} \xrightarrow[\text{unicit. scrierii}]{(ii)} v = 0.$ $\Rightarrow$

$S\cap T = \{0\}$. $\boxtimes$

Dem. 3.1.25 $f: V \to W$, V și W sunt K-sp vect.

$\boxed{\text{„}\Rightarrow\text{"}}$ Fie $\alpha, \beta \in K$, $x, y \in V$

$$f(\alpha x + \beta y) = f(\alpha x) + f(\beta y) = \alpha f(x) + \beta f(y).$$

$\boxed{\text{„}\Leftarrow\text{"}}$. Fie $x, y \in V$

$$f(x+y) = f(1x + 1\cdot y) \overset{(ip)}{=} 1\cdot f(x) + 1\cdot f(y) = f(x) + f(y).$$

Fie $\alpha \in K$, $x \in V$

$$f(\alpha x) = f(\alpha x + 0\cdot x) \overset{ip}{=} \alpha \cdot f(x) + 0\cdot f(x) = \alpha f(x). \ \boxtimes.$$

Dem. 3.1.27

$$\begin{tikzcd} V \arrow[r, shift left, "f"] \arrow[r, shift right, "f'"'] \arrow[dr, "g\circ f"'] & W \arrow[d, "g"] \\ & U \end{tikzcd}$$

f, f', g trate liniare.

Fie $x, y \in V$

$\alpha, \beta \in K$

$$(g\circ f)(\alpha x + \beta y) = g(f(\alpha x + \beta y)) \underset{lin}{\overset{f}{=}} g(\alpha f(x) + \beta f(y)) \underset{lin}{\overset{g}{=}} \alpha g(f(x)) + \beta g(f(y))$$

$$= \alpha (g\circ f)(x) + \beta (g\circ f)(y) \quad \text{deci } g\circ f \in Hom_K(V, U).$$

$$(f+f')(\alpha x + \beta y) = f(\alpha x + \beta y) + f'(\alpha x + \beta y) \underset{lin}{\overset{f, f'}{=}} \alpha f(x) + \beta f(y) + \alpha f'(x) + \beta f'(y)$$

$$\underset{comut.}{=} \alpha (f(x) + f'(x)) + \beta (f(y) + f'(y)) = \alpha (f+f')(x) + \beta (f+f')(y)$$

deci $f + f' \in Hom_K(V, W)$

$\lambda \in K$ $\lambda f : V \to W$

$$(\lambda f)(\alpha x + \beta y) = \lambda \cdot f(\alpha x + \beta y) \underset{lin}{\overset{f}{=}} \lambda (\alpha f(x) + \beta f(y)) =$$

$$= (\lambda \alpha) f(x) + (\lambda \beta) f(y) \underset{comut.}{\overset{K}{=}} (\alpha \lambda) f(x) + (\beta \lambda) f(y) =$$

$$= \alpha (\lambda f)(x) + \beta (\lambda f)(y) \Rightarrow \lambda f \in Hom_K(V, W).$$

Acum luăm $f: V \to W$ aplic. liniară bijectivă (izomorfism).

$\Rightarrow \exists f^{-1}: W \to V$ a.î. $f \circ f^{-1} = 1_W$, $f^{-1} \circ f = 1_V$. Clar f^{-1} bij.

Fie $\alpha, \beta \in K$, $u, v \in W$. Notăm $x = f^{-1}(u) \in V$, $y = f^{-1}(v) \in V$

Este clar $f(x) = u$, $f(y) = v$

$$f^{-1}(\alpha u + \beta v) = f^{-1}(\alpha f(x) + \beta f(y)) \overset{f}{\underset{\text{lin}}{=}} f^{-1}(f(\alpha x + \beta y)) = (f^{-1} \circ f)(\alpha x + \beta y)$$

$$= 1_V(\alpha x + \beta y) = \alpha x + \beta y = \alpha f^{-1}(u) + \beta f^{-1}(v)$$ Deci $f^{-1} \in \mathrm{Hom}_K(W, V)$.

<u>Dem.</u> 3.1.28. $(\mathrm{Hom}_K(V, W), +)$ este grup abelian

- $0: V \to W$, $0(x) = 0$, $\forall x \in V$ este elem. neutru

  $0 + f = f + 0 = f$, $\forall f \in \mathrm{Hom}_K(V, W)$.

- comutativ. $f, g \in \mathrm{Hom}_K(V, W)$

  $f + g: V \to W$, $g + f: V \to W$

  $(f+g)(x) = f(x) + g(x) \underset{\text{comut. in } W}{=} g(x) + f(x) = (g+f)(x)$ $\Rightarrow f + g = g + f$.

- $-f: V \to W$, $(-f)(x) = -f(x)$, $\forall x \in V$

  $(-f) + f = 0$.

- SV 1. $f, g \in \mathrm{Hom}_K(V, W)$, $\alpha \in K$

  $\alpha(f+g) \overset{?}{=} \alpha f + \alpha g$

  $\alpha(f+g): V \to W$, $\alpha f + \alpha g: V \to W$

  $\alpha(f+g)(x) = \alpha f(x) + (\alpha g)(x)$ din SV1 în W.

  celelalte detalii temă.

  $\alpha(f+g)(x) = \alpha(f(x) + g(x)) = \alpha f(x) + \alpha \cdot g(x)$

  $= (\alpha f)(x) + (\alpha g)(x)$.

Aplicaţii liniare.

Definiţie 3.1.21. Fie V şi W două K-spaţii vectoriale. Se numeşte *aplicaţie liniară* sau homomorfism de spaţii vectoriale între V şi W o funcţie $f : V \to W$ cu proprietăţile $f(x+y) = f(x)+f(y)$ şi $f(\alpha x) = \alpha f(x)$ pentru orice $x, y \in V$ şi orice $\alpha \in K$. Se numeşte *isomorfism* o aplicaţie liniară care este şi bijectivă. În acest caz spaţiile vectoriale V şi W ise zic izomorfe şi scriem $V \cong W$.

$1_V : V \to V$

Exemplu 3.1.22. Pentru orice două K-spaţii vectoriale V şi W aplicaţiile 1_V şi $0 : V \to W$, $0(x) = 0$ sunt liniare; mai mult 1_V este chiar un isomorfism. Daca $V \leq_K W$ atunci aplicaţia de incluziune $i : V \to W$ este liniară.

$i(x) = x, \forall x \in V$

$1_V(x) = x, \forall x \in V$

Notaţie 3.1.23. Fie V şi W două K-spaţii vectoriale. Vom nota

$$\mathrm{Hom}_K(V, W) = \{f : V \to W \mid f \text{ este liniară}\} \text{ şi } \mathrm{End}_K(V) = \mathrm{Hom}_K(V, V)$$

(o aplicaţie liniară $f : V \to V$ mai este numită şi *endomorfism* a lui V).

Observaţie 3.1.24. Orice aplicaţie liniară $f : V \to W$ este şi un morfism de grupuri, aşadar avem:

(a) $f(0) = 0$.
(b) $f(-x) = -f(x)$.

Propoziţie 3.1.25. *Fie V şi W două K-spaţii vectoriale. O aplicaţie $f : V \to W$ este liniară ddacă $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$, pentru orice $x, y \in V$ şi orice $\alpha, \beta \in K$.*

Demonstraţie. □

Observaţie 3.1.26. Prin inducţie se poate arăta că o aplicaţie liniară păstrează combinaţiileliniare, i. e. dacă $f : V \to W$ este liniară, $\alpha_1, \ldots, \alpha_n \in K$ şi $x_1, \ldots, x_n \in V$ atunci avem:

$$f(\alpha_1 x_1 + \ldots + \alpha_n x_n) = \alpha_1 f(x_1) + \ldots + \alpha_2 f(x_n).$$

Lemă 3.1.27. *Compunerea şi adunarea a două aplicaţii liniare (dacă există) sunt de asemenea aplicaţii liniare. Înmulţirea unei aplicaţii liniare cu un scalar este o aplicaţie liniară. Funcţia inversă a unui izomorfism este de asemenea un izomorfism.*

Demonstraţie. □

Teoremă 3.1.28. *Fie V şi W două K-spaţii vectoriale. Atunci $\mathrm{Hom}_K(V, W)$ este de asemenea un K-spaţiu vectorial în raport cu adunarea vectorilor (a funcţiilor):*

$$+ : \mathrm{Hom}_K(V, W) \times \mathrm{Hom}_K(V, W) \to \mathrm{Hom}_K(V, W),$$

$f+g : V \to W$

$V \underset{g}{\overset{f}{\rightrightarrows}} W$

$$(f + g)(x) = f(x) + g(x) \text{ pentru orice } x \in V,$$

şi cu înmulţirea cu scalari

$$\cdot : K \times \mathrm{Hom}_K(V, W) \to \mathrm{Hom}_K(V, W), (\alpha f)(x) = \alpha f(x), \text{ pentru orice } x \in V.$$

$\alpha f : V \to W$

În particular $(\mathrm{End}_K(V), +, \circ)$ este un inel unitar.

Demonstraţie. □

Definiţie 3.1.29. Fie $f : V \to W$ o aplicaţie liniară. Numim *nucleul* respectiv *imaginea* lui f mulţimile

$$\mathrm{Ker} f = \{x \in V \mid f(x) = 0\} \text{ şi } \mathrm{Im} f = \{f(x) \mid x \in V\}.$$

3.1.30 <u>Dem</u> $f \in \mathrm{Hom}_K(V, W)$

(a) $\mathrm{Ker}\, f = \{x \in V \mid f(x) = 0\}$

- $f(0) = 0 \Rightarrow 0 \in \mathrm{Ker} f$
- $\alpha, \beta \in K$, $x, y \in \mathrm{Ker}\, f \Rightarrow f(x) = 0 = f(y)$

$$f(\alpha x + \beta y) \underset{\text{lin}}{\overset{f}{=}} \alpha f(x) + \beta f(y) = \alpha \cdot 0 + \beta \cdot 0 = 0 \Rightarrow \alpha x + \beta y \in \mathrm{Ker} f.$$

(b) $\mathrm{Im}\, f = \{w \in W \mid \exists x \in V : f(x) = w\}$

- $0 = f(0) \in \mathrm{Im}\, f$
- $\alpha, \beta \in K$, $w, u \in \mathrm{Im}\, f \Rightarrow \exists x \in V : f(x) = w$, $\exists y \in V : f(y) = u$

$$\alpha w + \beta u = \alpha f(x) + \beta f(y) \underset{\text{lin}}{\overset{f}{=}} f(\underbrace{\alpha x + \beta y}_{\in V}) \in \mathrm{Im}\, f.$$

(c) $\boxed{\Rightarrow}$ $x \in \mathrm{Ker}\, f \Rightarrow f(x) = 0 = f(0) \underset{\substack{f \text{ inj} \\ \text{(ipoteza)}}}{\Longrightarrow} x = 0$. Deci $\mathrm{Ker}\, f = \{0\}$.

$\boxed{\Leftarrow}$ $x, y \in V$: $f(x) = f(y) \Rightarrow f(x) - f(y) = 0 \underset{\text{lin}}{\overset{f}{\Longrightarrow}} f(x - y) = 0 \Rightarrow$

$$\left.\begin{array}{l} x - y \in \mathrm{Ker}\, f \\ \text{Din ipoteza } \mathrm{Ker}\, f = \{0\} \end{array}\right\} \Rightarrow x - y = 0 \Rightarrow x = y.$$ Deci f este inj.

(d) evident.

Propoziţie 3.1.30. *Dacă $f : V \to W$ este o aplicaţie liniarăatunci avem:*

(a) $\mathrm{Ker} f \leq_K V$.
(b) $\mathrm{Im} f \leq_K W$.
(c) *f este injectivă ddacă* $\mathrm{Ker} f = \{0\}$. Ker $f = \{0\} = 0$
(d) *f este surjectivă ddacă* $\mathrm{Im} f = W$.

Demonstraţie. □

Exerciţii la spaţii vectoriale.

Exerciţiu 3.1.31. Să se arate că $\mathbb{R}_+^* = (0, \infty)$ este un $\mathbb{R}$-spaţiu vectorial în raport cu adunarea vectorilor:

$$\boxplus : \mathbb{R}_+^* \times \mathbb{R}_+^* \to \mathbb{R}_+^*,\ x \boxplus y = xy,\ \text{pentru orice } x, y \in \mathbb{R}_+^*,$$

şi cu înmulţirea cu scalari

$$\boxdot : \mathbb{R} \times \mathbb{R}_+^* \to \mathbb{R}_+^*,\ \alpha \boxdot x = x^\alpha \text{ pentru orice } x \in \mathbb{R}_+^*, \alpha \in \mathbb{R}.$$

Exerciţiu 3.1.32. Să se verifice că operaţiile:

$$\boxplus : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ x \boxplus y = \sqrt[5]{x^5 + y^5},\ \text{pentru orice } x, y \in \mathbb{R},$$

$$\boxdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ \alpha \boxdot x = \alpha \sqrt[5]{\alpha} x \text{ pentru orice } \alpha, x \in \mathbb{R}$$

definesc o structură de $\mathbb{R}$-spaţiu vectorial pe $\mathbb{R}$.

Exerciţiu 3.1.33. Care dintre următoarele submulţimi ale mulţimii $\mathbb{R}^3$ sunt $\mathbb{R}$-subspaţii:

- $A = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid 2x_1 + x_2 - x_3 = 0\}$.
- $B = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid 2x_1 + x_2 - x_3 = 1\}$.
- $C = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 = x_2 = x_3\}$.
- $D = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1^2 + x_2 = 0\}$.
- $E = \mathbb{R}^3 \setminus A$.
- $F = (\mathbb{R}^3 \setminus A) \cup \{0\}$.

Exerciţiu 3.1.34. Fie $n \in \mathbb{N}$ fixat. Să se arate că $K_n[X] = \{f \in K[X] \mid \mathrm{grad}(f) \leq n\}$ este un K-subspaţiu a lui $K[X]$.

Exerciţiu 3.1.35. Să se găsească ecuaţiile care determină vectorii din următoarele subspaţii: $S = \langle [1, 2, -1] \rangle$ şi $T = \langle [1, 2, 1], [-2, 1, -3] \rangle$ ale lui $\mathbb{R}^3$ (ecuaţiile acestor subspaţii).

Exerciţiu 3.1.36. Să se scrie subspaţiile $S = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 - x_2 - x_3 = 0\}$ şi $T = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 - x - 2 = x_2 - x_3 = x_3 - x_1\}$ ale lui $\mathbb{R}^3$ ca subspaţii generate (cu număr minimal de generatori).

Exerciţiu 3.1.37. Se consideră submulţimile $S, T \subseteq \mathbb{R}^3$ date prin $S = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\}$ şi $T = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 = x_2 = x_3\}$. Să se arate că $S, T \leq \mathbb{R}^3$ şi $S \oplus T = \mathbb{R}^3$.

Exerciţiu 3.1.38. Se consideră $S = \{\alpha I_2 \in \mathbb{M}_{2\times 2}(\mathbb{R}) \mid \alpha \in \mathbb{R}\}$ şi $T = \{A \in \mathbb{M}_{2\times 2}(\mathbb{R}) \mid \mathrm{Tr}(A) = 0\}$, unde $\mathrm{Tr}(A)$ este suma intrărilor de pe diagonala principală a matricii A. Să se arate că $S, T \leq_{\mathbb{R}} \mathbb{M}_{2\times 2}(\mathbb{R})$ şi $S \oplus T = \mathbb{M}_{2\times 2}(\mathbb{R})$.

Exerciţiu 3.1.39. Se consideră o mulţime oarecare A şi $\mathbb{R}^A = \{f : A \to \mathbb{R} \mid f$ este o funcţie$\}$. Să se arate că $\mathbb{R}^A$ este un $\mathbb{R}$-spaţiu vectorial în raport cu adunarea vectorilor (a funcţiilor):

$$+ : \mathbb{R}^A \times \mathbb{R}^A \to \mathbb{R}^A, (f+g)(x) = f(x) + g(x), \text{ pentru orice } x \in A,$$

şi cu înmulţirea cu scalari

$$\cdot : \mathbb{R} \times \mathbb{R}^A \to \mathbb{R}^A, (\alpha f)(x) = \alpha f(x), \text{ pentru orice } x \in A.$$

Exerciţiu 3.1.40. Se consideră submulţimile $S = \{f \in \mathbb{R}^{\mathbb{R}} \mid f$ este pară$\}$ şi $T = \{f \in \mathbb{R}^{\mathbb{R}} \mid f$ este impară$\}$ în $\mathbb{R}^{\mathbb{R}}$. Să se arate că $S, T \leq \mathbb{R}^{\mathbb{R}}$ şi $S \oplus T = \mathbb{R}^R$.

Exerciţiu 3.1.41. Se consideră un mumăr prim $p \in N$. Să se arate că în orice $\mathbb{Z}_p$-spaţiu vectorial este valabilă efgalitatea $0 = x + x + \ldots + x(p \text{ mal})$, pentru orice $x \in V$. Există o structură de $\mathbb{Z}_p$-spaţiu vectorial pe grupul abelian $(\mathbb{Z}, +)$?

Exerciţiu 3.1.42. Care dintre următoarele aplicaţii sunt liniare:

(1) $f : \mathbb{R}^3 \to \mathbb{R}^3$, $f[x_1, x_2, x_3] = [x_1 - x_2, x_2 - x_3, x_3 - x_1]$.
(2) $f : \mathbb{R}^3 \to \mathbb{R}^3$, $f[x_1, x_2, x_3] = [x_1 - 1, x_2 + 2, x_3 + 1]$.
(3) $f : \mathbb{R}^3 \to \mathbb{R}^2$, $f[x_1, x_2, x_3] = [2x_1 - 3x_2 + x_3, -x_1 + x_2 + 3x_3, x_1 + x_2 + x_3]$.
(4) $f : \mathbb{R}^2 \to \mathbb{R}^3$, $f[x_1, x_2] = [x_1 + x_2, x_1 - x_2, 2x_1 + x_2]$.
(5) $f : \mathbb{R}^2 \to \mathbb{R}$, $f[x_1, x_2] = x_1^2 - x_2^2$.
(6) $f : \mathbb{R}^2 \to \mathbb{R}^2$, $f[x_1, x_2] = [a_{1,1}x_1 + a_{2,1}x_2, a_{1,2}x_1 + a_{2,2}x_2]$, unde $a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2} \in \mathbb{R}$ sunt fixate.

Pentru aplicaţiile care sunt liniare să se determine ecuaţiile subspaţiilor Ker$f$ şi Imf.

3.2. **Baza unui spaţiu vectorial.**

Independenţă liniară. (sistem de vectori)

$$\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

Definiţie 3.2.1. Fie V un K-spaţiu vectorial. Se numeţe *listă de vectori* un element $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t$ din $V^{n \times 1}$, unde $n \in \mathbb{N}$ este arbitrar. O listă de vectori $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t$ se zice *liniar independentă* dacă pentru $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ scalari avem $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0 \Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$. O listă se zice *liniar dependentă* dacă nu este liniar independentă. În acest caz o relaţie de dependenţă liniară este o egalitate de forma $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$ cu scalarii $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ nu toţi nuli.

Observaţie 3.2.2. (1) Definiţia liniar independenţei unei liste $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t$ se poate scrie astfel:

$$[\alpha_1, \alpha_2, \ldots, \alpha_n][v_1, v_2, \ldots, v_n]^t = 0 \Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_n = 0.$$

Acesta este motivul pentru care luăm $[v_1, v_2, \ldots, v_n]^t \in V^{n \times 1}$ în loc de $[v_1, v_2, \ldots, v_n] \in V^n$.

(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 $[v_1, v_2, \ldots, v_n]^t \in V^{n \times 1}$ conţine vectorul nul $v_i = 0$, atunci ea este liniar dependentă, deoarece

$$0v_1 + \ldots + 1v_i + \ldots + 0v_n = 0.$$

$\alpha \in K$, $\underset{v_1}{\underset{\shortparallel}{x}} \in V$ $\qquad \alpha x = 0 \underset{\Leftarrow}{\Rightarrow} \alpha = 0$ sau $x = 0$

$$(\alpha_1 \ \alpha_2 \dots \alpha_n)\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n$$

$1\times \boxed{n \ = \ n} \times 1$ $\qquad$ 1×1

In K^m $\quad v_1 \in K^n$ $\quad v_1 = (v_{11}\ v_{12} \dots v_{1m})$, $v_{ij} \in K$

$v_2 = (v_{21}\ v_{22} \dots v_{2m})$ $\qquad$ Atunci

$\dots$

$v_n = (v_{n1}\ v_{n2} \dots v_{nm})$

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1m} \\ v_{21} & v_{22} & \dots & v_{2m} \\ & \dots & & \\ v_{n1} & v_{n2} & \dots & v_{nm} \end{bmatrix}$$

$\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$

$\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 = 0$

$\alpha_1(1,0,0) + \alpha_2(0,1,0) + \alpha_3(0,0,1) = (0,0,0)$

$(\alpha_1, \alpha_2, \alpha_3) = (0,0,0) \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0.$

Temă K^n $\quad e_1 = (1,0,\dots,0)$

$e_2 = (0,1,\dots,0)$ $\quad$ sunt liniar indep.

$\dots$

$e_n = (0,0,\dots,1)$

<u>Dem</u> 3.2.4 $\quad w = \begin{bmatrix} v_{i_1} \\ \vdots \\ v_{i_m} \end{bmatrix}$ lin. dep. și w este subliste în $v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$ $(m \le n)$

$\Rightarrow \exists\, \alpha_{i_1}, \dots, \alpha_{i_m} \in K$ nu toți nuli a.î. $\alpha_{i_1} v_{i_1} + \dots + \alpha_{i_m} v_{i_m} = 0$

Completăm astfel:

$$\alpha_i = \begin{cases} \alpha_{i_k} & \text{dacă } i = i_k,\ k = \overline{1,m} \\ 0 & \text{altfel} \end{cases} \qquad i = \overline{1,n}$$

Atunci

$\alpha_1 v_1 + \dots + \alpha_n v_n = 0$ și nu toți $\alpha_1, \alpha_2, \dots, \alpha_n$ sunt nuli

$\Rightarrow v$ este lin. dep. $\boxtimes$.

<u>Dem</u>. 3.2.6. $\quad v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \in V^{n\times 1}$

$\boxed{\Rightarrow}$ v lin dep. $\Rightarrow \exists\, \alpha_1, \dots, \alpha_n$ nu toți nuli a.î. $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$

Alegem $i \in \{1, \dots, n\}$ a.î. $\alpha_i \neq 0$. $\Rightarrow \exists\, \alpha_i^{-1} \in \mathbb{R}$

$\alpha_i^{-1} \mid \alpha_1 v_1 + \dots + \alpha_i v_i + \dots + \alpha_n v_n = 0$

$\alpha_i^{-1}\alpha_1 v_1 + \dots + v_i + \dots + \alpha_i^{-1}\alpha_n v_n = 0$

$$v_i = (-\alpha_i^{-1}\alpha_1) v_1 + \dots + (-\alpha_i^{-1}\alpha_n) v_n = \sum_{\substack{j=1 \\ j\neq i}}^{n} (-\alpha_i^{-1}\alpha_j) v_j \in \langle v^{\setminus i} \rangle$$

$\boxed{\Leftarrow}$ Din ipoteză $\exists\, i \in \{1,\dots,n\}$ a.î. $v_i = \underbrace{\beta_1 v_1 + \dots + \beta_n v_n}_{\text{fără } i} = \sum_{\substack{j=1 \\ j\neq i}}^{n} \beta_j v_j$

$$\underbrace{(-\beta_1)v_1 + \dots + 1\cdot v_i + \dots + (-\beta_n)v_n}_{\neq 0} = 0$$

$\beta_j \in \mathbb{R},\ j \neq i$ $\Big|\Rightarrow$ v lin. dep. $\boxtimes$.

Dem. 3.2.7 $\boxed{\Rightarrow}$ $v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$ este lin. dep. $\overset{3.2.6}{\Rightarrow} \exists\, i \in \{1,\dots,n\}$ a.î.

$$\left.\begin{array}{l} \left.\begin{array}{l} v_i \in \langle v^{\setminus i}\rangle \\ j \neq i \quad v_j \in \langle v^{\setminus i}\rangle \end{array}\right\} \Rightarrow \langle v\rangle \subseteq \langle v^{\setminus i}\rangle \\ \qquad\qquad \text{Este evident că } \langle v^{\setminus i}\rangle \subseteq \langle v\rangle \end{array}\right\} \Rightarrow \langle v\rangle = \langle v^{\setminus i}\rangle.$$

$\boxed{\Leftarrow}$. Dacă $\exists\, i \in \{1,\dots,n\}$ a.î. $\langle v^{\setminus i}\rangle = \langle v\rangle$ atunci $v_i \in \langle v^{\setminus i}\rangle \Rightarrow v_i$ este o comb. liniară a celorlalți $\overset{3.2.6}{\Rightarrow}$ v lin. dep.

3.2.11
$e_1 = (1,0,\dots,0)$
$e_2 = (0,1,\dots,0)$
$\dots$
$e_n = (0,0,\dots,1)$

form. o bază în K^n peste K

- lin. indep. ca mai sus.

Pt. generare este clar că $\langle e_1, e_2, \dots, e_n\rangle \subseteq K^n$. $(\leq_K)$

Pt. incluziunea inversă dacă $x \in K^n \Rightarrow x = (x_1, x_2, \dots, x_n)$, $x_i \in K$

Atunci
$$\begin{aligned} x &= (x_1,0,\dots,0) + (0,x_2,\dots,0) + \dots + (0,0,\dots,x_n) \\ &= x_1\cdot(1,0,\dots,0) + x_2(0,1,\dots,0) + \dots + x_n(0,0,\dots,1) \\ &= x_1 e_1 + x_2 e_2 + \dots + x_n e_n \in \langle e_1, e_2, \dots, e_n\rangle \end{aligned}$$

Deci $K^n = \langle e_1, e_2, \dots, e_n\rangle$.

Dem. 3.2.12 $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \in V^{n\times 1}$

$\boxed{(i) \Rightarrow (iii)}$

b lin. ind. și maximală și este clar $\langle b\rangle \subseteq V$ $(\leq_K)$

Fie $x \in V \Rightarrow \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \\ x \end{pmatrix}$ este lin. dep. $\Rightarrow \exists\, \alpha_1, \dots, \alpha_n, \alpha \in K$ nu toți nuli

a.î. $\alpha_1 b_1 + \dots + \alpha_n b_n + \alpha x = 0$

Dacă $\alpha = 0$ atunci am obține o rel. de dep. lin. pt. b imposibil.

Deci $\alpha \neq 0$ și cu dem. de la 3.2.6 rezultă $x \in \langle b\rangle$.

Atunci $V = \langle b\rangle$. Liniar ind. + generare înseamnă bază.

$\boxed{(iii) \Rightarrow (i)}$. b bază pt. $V \Rightarrow b$ lin. ind $\langle b\rangle = V$.

Fie $x \in V = \langle b\rangle \Rightarrow x$ se scrie ca o comb lin. de $b \underset{3.2.6}{\Rightarrow} \begin{pmatrix} b_1 \\ \vdots \\ b_n \\ x \end{pmatrix}$ lin. dep.

$\boxed{(ii) \Rightarrow (iii)}$ $\langle b \rangle = V$ și $\forall i \in \{1, \dots, n\}$ $\langle b^{\setminus i} \rangle \neq V$

Dacă presup. b lin. dep. $\overset{3.2.7.}{\Longrightarrow} \exists i \in \{1, \dots, n\} : \langle b^{\setminus i} \rangle = \langle b \rangle = V$ } absurd

Deci b este lin. indep. } $\Rightarrow b$ este bază

$\langle b \rangle = V$

$\boxed{(iii) \Rightarrow (ii)}$ b bază $\Rightarrow b$ lin. ind $\langle b \rangle = V$.

Dacă $\exists i \in \{1, \dots, n\}$ a.î. $\langle b^{\setminus i} \rangle = V \Rightarrow b_i \in \langle b^{\setminus i} \rangle \Rightarrow$

b_i este o comb. liniară a ceilalți $\Rightarrow b$ lin. dep. (imposibil).

Deci $\forall i \in \{1, \dots, n\}$ $\langle b^{\setminus i} \rangle \neq V$. $\boxtimes$.

<u>Dem</u> 3.2.14. Fie $V = \langle b_1, b_2, \dots, b_n \rangle$ sp. vectorial finit generat

Dacă $b_1, b_2, \dots, b_n$ lin. ind. $\Rightarrow$ form. o bază STOP.

Dacă $b_1, b_2, \dots, b_n$ nu sunt lin. ind $\Rightarrow$ sunt liniar dep.

$\Rightarrow \exists i \in \{1, \dots, n\}$ a.î. $\langle b^{\setminus i} \rangle = \langle b \rangle = V$.

Reluăm raționamentul cu $V = \langle \{b_1, \dots, b_n\} \setminus \{b_i\} \rangle$.

După cel mult n pași găsim o bază pt. V. $\boxtimes$.

<u>Obs</u> (a) $V = \{0\}$ are baza $\emptyset$.

(b) $V \neq \{0\} \Rightarrow \exists x \in V, x \neq 0$, x lin. ind. deci baza lui V nu este $\emptyset$.

(5) Dacă lista $[v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ conţine doi vectori egali $v_i = v_j$ cu $i \neq j$ atunci ea este liniar dependentă, deoarece

$$0v_1 + \ldots + 1v_i + \ldots + (-1)v_j + \ldots 0v_n = 0.$$

(6) Uneori nu suntem interesaţi de ordinea vectorilor dintr-o lista $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t$ şi spunem că vectorii $v_1, v_2, \ldots, v_n$ sunt liniar (in)dependenţi 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 $v_1 = [1, 0, 1]$, $v_2 = [1, 2, 3]$ şi $v_3 = v_1 + v_2 = [2, 2, 4]$ 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 $[w_1, w_2, \ldots, w_m]^t \in V^{m\times 1}$ este o sublistă a listei $[v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ dacă $\{w_1, w_2, \ldots, w_m\} \subseteq \{v_1, v_2, \ldots, v_n\}$. Cu alte cuvinte $[w_1, w_2, \ldots, w_m]^t = [v_{i_1}, v_{i_2}, \ldots, v_{i_m}]^t$, pentru anumiţi indici $i_1, i_2, \ldots, i_n \in \{1, \ldots, n\}$. $(m \leq n)$

Propoziţie 3.2.4. *Se consideră* $\mathbf{w} = [v_{i_1}, v_{i_2}, \ldots, v_{i_m}]^t \in V^{m\times 1}$ *o sublistă a listei* $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$. *Dacă* $\mathbf{w}$ *este liniar dependentă, atunci tot aşa este şi* $\mathbf{v}$. *Echivalent, dacă* $\mathbf{v}$ *este liniar independentă, atunci tot aşa este şi* $\mathbf{w}$.

Demonstraţie. □

Notaţie 3.2.5. Fie $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ o listă de vectori. Pentru $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ notăm $\mathbf{v}^{\setminus i_1, i_2, \ldots, i_k}$ sublista care este obţinută din $\mathbf{v}$ prin eliminarea vectorilor $v_{i_1}, v_{i_2}, \ldots, v_{i_n}$.

Pentru o listă de vectori $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$ scriem simplu $\langle \mathbf{b} \rangle = \langle b_1, b_2, \ldots, b_n \rangle$ şi vom vorbi despre supspaţiul generat de respectiva listă.

Propoziţie 3.2.6. *Fie* $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ *o listă de vectori. Lista* $\mathbf{v}$ *este exact atunci liniar dependentă când există* $i \in \{1, 2, \ldots, n\}$, *astfel încât* v_i *este o combinaţie liniară a vectorilor din lista* $\mathbf{v}^{\setminus i}$.

Demonstraţie. □

Corolar 3.2.7. *Fie* $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ *o listă de vectori, astfel încât există* $i \in \{1, 2, \ldots, n\}$, *cu proprietatea că* v_i *este o combinaţie liniară a vectorilor din lista* $\mathbf{v}^{\setminus i}$ ~~*iar*~~ *Atunci* $\langle \mathbf{v} \rangle = \langle \mathbf{v}^{\setminus i} \rangle$.

Demonstraţie. □

Definiţie 3.2.8. O submulţime finită $\{v_1, v_2, \ldots, v_n\} \subseteq V$ se numeşte *liberă* dacă lista $[v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ este liniar independentă. O submulţime oarecare (posibil infinită) $B \subseteq V$ se numeşte *liberă* dacă fiecare submulţime finită a lui B este liberă.

Baze şi coordonate.

Definiţie 3.2.9. O *bază (ordonată)* a unui K-spaţiu vectorial V este o listă de vectori $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$ astfel încât $\mathbf{b}$ este liniar independentă şi $\langle \mathbf{b} \rangle = V$ gilt (i. e. vectorii din această listă generează V).

Observaţie 3.2.10. (a) Adesea suntem interesaţi de baze care nu sunt ordonate, ceea ce înseamnă submulţimi

$$\{b_1, b_2, \ldots, b_n\} \subseteq V$$

astfel încât $[b_1, b_2, \ldots, b_n]^t$ este o bază (ordonată) în sensul Definiţiei 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 spaţiu vectorial V este o sumbulţime $B \subseteq V$ astfel încât B este liberă şi $\langle B \rangle = V$.

Exemplu 3.2.11. Lista $\mathbf{e} = [e_1, e_2, \ldots, e_n]^t$ unde $e_1 = [1, 0, \ldots, 0] \in K^n$, $e_2 = [0, 1, \ldots, 0] \in K^n$, ..., $e_n = [0, 0, \ldots, 1] \in K^n$ este o bază pentru K^n. Această bază se numeşte *baza canonică* a lui K^n. Baza canonică se poate scrie cu ajutorul aşa numitelor simboluri lui Kronecker:

$$e_i = [\delta_{i,j}]_{1 \leq j \leq n} \in K^n, \text{ unde } \delta_{i,j} = \begin{cases} 1 \text{ dacă } i = j \\ 0 \text{ dacă } i \neq j \end{cases} \quad \text{pentru orice } i \in \{1, \ldots, n\}.$$

Propoziţie 3.2.12. *Fie V un K-spaţiu vectorial şi $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n \times 1}$. Următoarele afirmaţii sunt echivalente:*

(i) $\mathbf{b}$ *este o listă de vectori maximal liniar independentă, i. e.* $\mathbf{b}$ *este liniar independentă şi pentru orice $x \in V$ lista $\mathbf{b}' = [b_1, b_2, \ldots, b_n, x]$ nu mai are aceeaşi proprietate.*

(ii) $\mathbf{b}$ *este o listă minimală cu proprietatea că generează V, i. e. $\langle \mathbf{b} \rangle = V$ şi pentru oricare $i \in \{1, \ldots, n\}$, avem $\langle \mathbf{b}^{\setminus i} \rangle \neq V$.*

(iii) $\mathbf{b}$ *este o bază a lui V.*

Demonstraţie. □

Definiţie 3.2.13. Un K-spaţiu vectorial V se numeşte *finit generat* dacă exsită o submulţime finită $\{b_1, b_2, \ldots, b_n\} \subseteq V$ astfel încât $\langle b_1, b_2, \ldots, b_n \rangle = V$.

Corolar 3.2.14. *Orice spaţiu vectorial finit generat are o bază.*

Demonstraţie. □

Observaţie 3.2.15. Aici şi în ce urmează, vom considera numai spaţii vectoriale finit generate. Totuşi multe rezultate (de ex. Corolarul 3.2.14, Teorema 3.2.24, Corolarul 3.2.19 etc.) sunt valabile sau au un analog şi în cazul spaţiilor vectoriale care nu sunt finit generate.

Propoziţie 3.2.16. *Fie V un K-spaţiu vectorial şi $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n \times 1}$. Următoarele afirmaţii sunt echivalente:*

(i) $\mathbf{b}$ *este o bază a lui V.*

(ii) *Pentru orice vector $x \in V$ există un unic sistem de scalari*

$$\alpha = [\alpha_1, \ldots, \alpha_n] \in K^n \text{ astfel încât } x = \alpha\mathbf{b} = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_n b_n.$$

Demonstraţie. □

Definiţie 3.2.17. Fie V un K-spaţiu vectorial şi $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n \times 1}$. Numim *coordonatele* unui vector $x \in V$ în raport cu $\mathbf{b}$ scalari unic determinaţi $[\alpha_1, \ldots, \alpha_n]$ cu proprietatea $x = \alpha_1 b_1 + \ldots + \alpha_n b_n$.

3.2.16. Dem. $\boxed{(i) \Leftrightarrow (ii)}$. $b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \in V^{n\times 1}$

$\langle b \rangle = V \Leftrightarrow \forall x \in V,\ x \in \langle b \rangle \Leftrightarrow \forall x \in V\ \exists\, \alpha_1, \alpha_2, \dots \alpha_n \in \mathbb{K}$:

$x = \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_n b_n$

b lin. i-d. și $x = \alpha_1 b_1 + \dots + \alpha_n b_n$

$x = \alpha_1' b_1 + \dots + \alpha_n' b_n$ $-$

$0 = (\alpha_1 - \alpha_1') b_1 + \dots + (\alpha_n - \alpha_n') b_n \xRightarrow[\text{i-d.}]{\text{lin}} \alpha_1 - \alpha_1' = \dots = \alpha_n - \alpha_n' = 0$

$\alpha_1 = \alpha_1' \ \dots \ \alpha_n = \alpha_n'$

(unicit.

Reciproc dacă există unicitatea scrierii și

$\alpha_1, \dots, \alpha_n \in \mathbb{K}$ cu $\alpha_1 b_1 + \dots + \alpha_n b_n = 0 = 0 \cdot b_1 + \dots + 0 b_n \xrightarrow{\text{unicit.}}$

$\alpha_1 = \dots \alpha_n = 0$. Deci b este lin. i-d. $\boxtimes$.

Dimensiune unui spaţiu vectorial.

Lemă 3.2.18. *(Lema lui Steinitz) Se consideră două liste de vectori* $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ *şi* $\mathbf{w} = [w_1, w_2, \ldots, w_m]^t \in V^{m\times 1}$ *într-un* K*-spaţiu vectorial* V*, unde* $n, m \in \mathbb{N}$*. Dacă* $\mathbf{v}$ *este liniar independentă şi* $\langle \mathbf{w} \rangle = V$*, atunci avem* $n \leq m$ *şi, după o eventuală renumerotare,* $\langle v_1, \ldots, v_n, w_{n+1}, \ldots, w_m \rangle = V$*.*

Demonstraţie. □

Corolar 3.2.19. *Oricare două baze ale unui* K*-spaţiu vectorial (finit generat) au acelaşi număr de elemente.*

Demonstraţie. □

Definiţie 3.2.20. Prin definiţie *dimensiunea* unui K-spaţiu 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 spaţii finit generate, şi vom folosi noţiunea echivlentă (dar mai elegantă) de spaţii finit dimensionale.

Exemplu 3.2.21. (1) $\dim 0 = 0$.
(2) $\dim_K K^n = n$; în particular $\dim_{\mathbb{R}} \mathbb{R} = 1$, $\dim_{\mathbb{R}} \mathbb{R}^2 = 2$, $\dim_{\mathbb{R}} \mathbb{R}^3 = 3$

Observaţie 3.2.22. Următoarele afirmaţii sunt adevu arate într-un spaţiu finit dimensional:

(a) Orice listă liniar independentă se poate completa până la o bază.
(b) Din orice listă care generează pe V se poate extrage o bază.
(c) $\dim V$ ieste cel mai mare număre de vectori liniar independenţi care există în V.
(d) $\dim V$ este cel mai mic număr de lemente a unel liste care generează V.

Propoziţie 3.2.23. *Fie* V *un* K*-spaţiu vectorial cu* $\dim_K V = n$ *şi* $\mathbf{b} = [b_1, b_2, \ldots, b_n] \in V^{n\times 1}$ *o listă de vectori. Următoarele afirmaţii sunt echivalente:*

(i) $\mathbf{b}$ *este liniar independentă.*
(ii) $\langle \mathbf{b} \rangle = V$.
(iii) $\mathbf{b}$ *este o bază.*

Demonstraţie. □

Proprietatea de universalitate a bazei unui spaţiu vectorial.

Teoremă 3.2.24. *[Proprietatea de universalitate a bazei] Fie* V *şi* W *două* K*-spaţii vectoriale şi* $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ *o bază a lui* V*. Pentru orice funcţie* $f : \{v_1, v_2, \ldots, v_n\} \to W$ *există o aplicaţie liniară unică* $\bar{f} : V \to W$ *astfel încât* $\bar{f}(v_i) = f(v_i)$ *pentru orice* $1 \leq i \leq n$ *(i. e.* $\bar{f}$ *prelungeşte pe* f *sau* f *este o restricţie a lui* $\bar{f}$*).*

Demonstraţie. □

Corolar 3.2.25. *Fie* V *şi* W *două* K*-spaţii vectoriale şi* $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ *o bază a lui* V*.*

(a) *Dacă* $f, g : V \to W$ *sunt aplicaţii 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* $V \cong W$*.* (două sp. vectoriale cu aceeaşi dimensiune sunt izomorfe).
(c) $V \cong K^n$*.*

obs $\dim_K K^n = n$ deci (c) este cat parte pt. (b).

3.2.18. Dem. Inducție după $n \in \mathbb{N}$.

Dacă $n=0$ atunci concluzia este evident adevărată.

Presupunem concluzia adevărată pt. $n=k$ vectori $\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}$

Deci $k \leq m$ & după o eventuală renumerotare

$$\langle v_1, \dots, v_k, w_{k+1}, \dots, w_m \rangle = V. \quad (1)$$

Fie atunci o listă $v = \begin{bmatrix} v_1 \\ \vdots \\ v_k \\ v_{k+1} \end{bmatrix}$ despre care știm că este liniar ind.

Atunci $\begin{bmatrix} v_1 \\ \vdots \\ v_k \end{bmatrix}$ este liniar ind. deci se poate aplica ipoteza de ind și obținem $k \leq m$ & (1).

Presupunem că $k = m$ atunci în (1) am înlocuit toți vectorii din w, așadar $\langle v_1, \dots, v_k \rangle = V$. Dar $v_{k+1} \in V = \langle v_1, \dots, v_k \rangle$ este o comb. liniară a vect. $v_1, \dots, v_k \overset{3.2.6}{\Longrightarrow}$ v este lin. dep. ↯.

Așadar $k \leq m$ & $k \neq m \Rightarrow k < m \Rightarrow k+1 \leq m$.

Avem $v_{k+1} \in V \overset{(1)}{=} \langle v_1, \dots, v_k, w_{k+1}, \dots, w_m \rangle \Rightarrow \exists\, \alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_m \in K$

$$v_{k+1} = \alpha_1 v_1 + \dots + \alpha_k v_k + \alpha_{k+1} w_{k+1} + \dots + \alpha_m w_m \quad (2)$$

Dacă presupunem că $\alpha_{k+1} = \dots = \alpha_m = 0$ atunci v_{k+1} s-ar scrie ca o combinație liniară de $v_1, \dots, v_k$ deci ar fi lin. dep. ceea ce este imposibil. Deci $\exists\, j \in \{k+1, \dots, m\}$ a.î. $\alpha_j \neq 0$. După o eventuală renumerotare putem presupune că $j = k+1$.

Avem $\alpha_{k+1} \neq 0 \Rightarrow \exists\, \alpha_{k+1}^{-1} \in K$. Din (2) rezultă

$$\alpha_{k+1}^{-1} v_{k+1} = \alpha_{k+1}^{-1} \alpha_1 v_1 + \dots + \alpha_{k+1}^{-1} \alpha_k v_k + \underbrace{\alpha_{k+1}^{-1} \alpha_{k+1}}_{1} w_{k+1} + \dots + \alpha_{k+1}^{-1} \alpha_m w_m$$

$$w_{k+1} = (-\alpha_{k+1}^{-1} \alpha_1) v_1 + \dots + (-\alpha_{k+1}^{-1} \alpha_k) v_k + \alpha_{k+1}^{-1} v_{k+1} + \dots + (-\alpha_{k+1}^{-1} \alpha_m) w_m$$

$$\left.\begin{array}{l} \text{Deci } w_{k+1} \in \langle v_1, \dots, v_k, v_{k+1}, \dots, w_m \rangle \\ \text{Este clar că } v_1, \dots, v_k, w_{k+2}, \dots, w_m \in \langle v_1, \dots, v_k, v_{k+1}, \dots, w_m \rangle \end{array}\right\} \Rightarrow$$

$$V \overset{(1)}{=} \langle v_1, \dots, v_k, w_{k+1}, \dots, w_m \rangle \subseteq \langle v_1, \dots, v_k, v_{k+1}, \dots, w_m \rangle \subseteq V$$

Deci $\langle v_1, \dots, v_k, v_{k+1}, \dots, w_m \rangle = V$. ☒.

3.2.19. Dem. Fie $e = \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix}$ și $b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$ două baze pt. V

$$\left.\begin{array}{l} e \text{ lin. ind. } \langle b \rangle = V \overset{3.2.18}{\Longrightarrow} n \leq m \\ \langle e \rangle = V \text{ și } b \text{ lin. ind.} \overset{3.2.18}{\Longrightarrow} m \leq n \end{array}\right\} \Rightarrow n = m.$$

Obs $\dim_{\mathbb{R}} \mathbb{R} = 1$

$v \in \mathbb{R}$, $v \neq 0$ form. o bază pt. $\mathbb{R}$-sp. vect. $\mathbb{R}$

Dem. 3.2.24. $\{v_1,\dots,v_n\}$ bază în V (deci $\dim_K V = n$).

$f:\{v_1,\dots,v_n\}\to W$ funcție oarecare

$$\begin{tikzcd} \{v_1,\dots,v_n\} \arrow[r, "f"] \arrow[d, "g"'] & W \\ V \arrow[ur, dashed, "\exists!\,\bar f \text{ liniară}"'] & \end{tikzcd}$$

$g(v_i)=v_i\in V \quad 1\le i\le n$

$\bar f\circ g = f \iff \bar f(v_i)=f(v_i),\ 1\le i\le n$

<u>Unicit</u>: Fie $\bar f,\tilde f\in \mathrm{Hom}_K(V,W)$ a.î. $\bar f(v_i)=f(v_i)=\tilde f(v_i)$, $1\le i\le n$.

Fie $x\in V$.
Dar $V=\langle v_1,\dots,v_n\rangle$ $\Big\}\Rightarrow \exists\,\alpha_1,\dots,\alpha_n:\ x=\alpha_1v_1+\dots+\alpha_nv_n$

$\bar f(x)=\bar f(\alpha_1v_1+\dots+\alpha_nv_n)\overset{\bar f}{\underset{\text{lin}}{=}}\alpha_1\bar f(v_1)+\dots+\alpha_n\bar f(v_n)=\alpha_1f(v_1)+\dots+\alpha_nf(v_n)$

$\tilde f(x)=\tilde f(\text{——}\,''\,\text{——})=\alpha_1\tilde f(v_1)+\dots+\alpha_n\tilde f(v_n)=\alpha_1f(v_1)+\dots+\alpha_nf(v_n)$

Deci $\bar f(x)=\tilde f(x)\Rightarrow \bar f=\tilde f$.

<u>Existența</u>. Definim $\bar f$ în felul următor: $\bar f: V\to W$

Dacă $x\in V$ cum $\{v_1,\dots,v_n\}$ este bază $\exists!\,\alpha_1,\dots,\alpha_n\in K$ a.î.

$x=\alpha_1v_1+\dots+\alpha_nv_n$ not. (*)

Def. $\bar f(x)=\alpha_1f(v_1)+\dots+\alpha_nf(v_n)$ (este bine definită această funcție din unicitate).

Fie $i\in\{1,\dots,n\}$ $\quad v_i=0\cdot v_1+\dots+1\cdot v_i+\dots+0\cdot v_n$. Atunci din (*):

$\bar f(v_i)=0\cdot f(v_1)+\dots+1\cdot f(v_i)+\dots+0\cdot f(v_n)=f(v_i)$. Cum i este arbitrar

$\bar f(v_i)=f(v_i)$, $\forall i\in\{1,\dots,n\}$.

Fie $x,y\in V$ și $\alpha,\beta\in K$

$x,y\in V\Longrightarrow \exists!\,\alpha_1,\dots,\alpha_n\in K:\ x=\alpha_1v_1+\dots+\alpha_nv_n$

$\exists!\,\beta_1,\dots,\beta_n\in K:\ y=\beta_1v_1+\dots+\beta_nv_n$

$$\bar f(\alpha x+\beta y)=\bar f(\alpha\alpha_1v_1+\dots+\alpha\alpha_nv_n+\beta\beta_1v_1+\dots+\beta\beta_nv_n)=$$
$$=\bar f((\alpha\alpha_1+\beta\beta_1)v_1+\dots+(\alpha\alpha_n+\beta\beta_n)v_n)$$
$$\overset{(*)}{=}(\alpha\alpha_1+\beta\beta_1)f(v_1)+\dots+(\alpha\alpha_n+\beta\beta_n)f(v_n)$$

$$\alpha\bar f(x)+\beta\bar f(y)\overset{(*)}{=}\alpha(\alpha_1f(v_1)+\dots+\alpha_nf(v_n))+\beta(\beta_1f(v_1)+\dots+\beta_nf(v_n))$$
$$=(\alpha\alpha_1+\beta\beta_1)f(v_1)+\dots+(\alpha\alpha_n+\beta\beta_n)f(v_n).$$

Deci $\bar f(\alpha x+\beta y)=\alpha\bar f(x)+\beta\bar f(y)\Rightarrow \bar f\in\mathrm{Hom}_K(V,W)$. $\boxtimes$.

3.2.25. Dem. (a). $f,g\in\mathrm{Hom}_K(V,W)$ și $\{v_1,\dots,v_n\}$ bază în V a.î.

$f(v_i)=g(v_i)$, $i=\overline{1,n}$.

Considerăm funcția $h:\{v_1,\dots,v_n\}\to W$, $h(v_i)=f(v_i)=g(v_i)$, $i=\overline{1,n}$

(h este restricția comună a funcțiilor f și g).

Din prop. de universalitate (3.2.24) $\Rightarrow$ $f=\bar h=g$ unde $\bar h$ este unica extindere liniară a lui h.

(b) $\dim_K V = \dim_K W = n$, $\{v_1, \dots, v_n\}$ bază în V și fie $\{w_1, \dots, w_n\}$ bază în W

Definim funcțiile

$f : \{v_1, \dots, v_n\} \to W$, $f(v_i) = w_i$, $1 \le i \le n$ $\overset{3.224 \text{ (p.u.)}}{\Longrightarrow}$ $\exists!\, \bar{f} \in \mathrm{Hom}_K(V, W)$: $\bar{f}(v_i) = w_i$, $1 \le i \le n$

$g : \{w_1, \dots, w_n\} \to V$, $g(w_i) = v_i$, $1 \le i \le n$ $\Longrightarrow$ $\exists!\, \bar{g} : \mathrm{Hom}_K(W, V)$, $\bar{g}(w_i) = v_i$, $1 \le i \le n$.

$$\begin{tikzcd} V \arrow[r, "\bar{f}"] \arrow[dr, shift left, "\bar{g}\circ\bar{f}"] \arrow[dr, shift right, "1_V"'] & W \arrow[d, "\bar{g}"] \\ & V \end{tikzcd}$$

$(\bar{g}\circ\bar{f})(v_i) = \bar{g}(\bar{f}(v_i)) = \bar{g}(w_i) = v_i = 1_V(v_i)$ $\quad 1 \le i \le n$ $\Big\}$ (a) $\Longrightarrow$

$\bar{g}\circ\bar{f}, 1_V \in \mathrm{Hom}_K(V, V)$

$\bar{g}\circ\bar{f} = 1_V$.

Analog

$$\begin{tikzcd} W \arrow[r, "\bar{g}"] \arrow[dr, shift left, "\bar{f}\circ\bar{g}"] \arrow[dr, shift right, "1_W"'] & V \arrow[d, "\bar{f}"] \\ & W \end{tikzcd}$$

și avem $\bar{f}\circ\bar{g} = 1_W$.

Deci $\bar{f}, \bar{g}$ sunt izomorfisme și $\bar{g} = \bar{f}^{-1}$.

(c) cat. part. pt. b cînd $W = K^n$. $\boxtimes$.

Formule legate de dimensiune.

Propoziţie 3.2.26. *Se consideră un K-spaţiu vectorial V şi $S, T \leq_K$ două subspaţii. Avem:*

$$\dim S + \dim T = \dim(S + T) + \dim(S \cap T).$$

Demonstraţie. $\dim(S+T) = \dim S + \dim T - \dim(S \cap T)$ □

Corolar 3.2.27. *Dacă V este un K-spaţiu vectorial finit dimensional şi $S \leq_K V$, atunci $\dim S \leq \dim V$. Mai mult, $\dim S = \dim V$ ddacă $S = V$.*

Demonstraţie. □

Propoziţie 3.2.28. *Fie $f : V \to W$ o aplicaţie liniară între două K-spaţii vectoriale V şi W. Atunci:*

$$\dim V = \dim \mathrm{Ker} f + \dim \mathrm{Im} f.$$

Demonstraţie. □

Corolar 3.2.29. *Fie V şi W două K-spaţii vectoriale cu $\dim V = \dim W$* $= n$ finit dim. *şi $f : V \to W$ o aplicaţie liniară.* *eine lineare Abbildung.* *Următoarele afirmaţii sunt echivalente:*

(i) *f ist injectivă.*
(ii) *f ist surjectivă.*
(iii) *f ist bijectivă.*

Demonstraţie. □

Lema substituţiei.

Teoremă 3.2.30. *(Lema substituţiei) Fie $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t$ o bază a K-spaţiului vectorial V şi $v \in V$ cu coordonatele $[\alpha_1, \alpha_2 \ldots, \alpha_n]$ în raport cu baza $\mathbf{b}$ (i. e. $v = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_n b_n$). Considerăm lista de vectori $\mathbf{v}' = [b_1, \ldots, v, \ldots, b_n]$ care rezultă din $\mathbf{v}$ prin înlocuirea (substituţia) vectorului b_i cu v. Atunci:*

(a) *$\mathbf{b}'$ este o bazăddacă $\alpha_i \neq 0$.*
(b) *Dacă $\mathbf{b}'$ este o bazăşi $x \in V$ are coordonatele $[x_1, x_2 \ldots, x_n]$ în raport cu $\mathbf{v}$ şi $[x'_1, x'_2 \ldots, x'_n]$ în raport cu $\mathbf{v}'$ atunci:*

$$\begin{cases} x'_i = \alpha_i^{-1} x_i \\ x'_j = \alpha_i^{-1}(\alpha_i x_j - \alpha_j x_i) \text{ pentru } j \neq i \end{cases}.$$

Demonstraţie. □

Definiţie 3.2.31. Se numeşte rangul unei liste de vectori n $\mathbf{v} = [v_1, \ldots, v_n]^t$ dimensiunea spaţiului generat de $\mathbf{v}$, i. e. $\mathrm{rank}\, \mathbf{v} = \dim\langle \mathbf{v} \rangle$.

Observaţie 3.2.32. Deoarece orice listă liniar independentă se poate completa până la o bază, se poate folosi lema substituţiei pentru a calcula rangul unei liste de vectori.

3.2.26. <u>Dem</u>. Fie $\{x_1,\dots,x_k\}$ o bază în $S\cap T$; $\dim(S\cap T)=k$

$S\cap T \leq_k S \Rightarrow x_1,\dots,x_k$ lin. ind în $S \overset{3.2.22}{\Longrightarrow}$ se poate completa la o bază

$\{x_1,\dots,x_k,y_{k+1},\dots,y_n\}$ în S ; implicit $\dim S=n$

$S\cap T\leq_k T \Rightarrow x_1,\dots,x_k$ lin. ind. în $T \Rightarrow$ se poate completa la o bază

$\{x_1,\dots,x_k,z_{k+1},\dots,z_m\}$ în T ; implicit $\dim T=m$.

Vom arăta că $\{x_1,\dots,x_k,y_{k+1},\dots,y_n,z_{k+1},\dots,z_m\}$ este o bază în $S+T$. ?

Deci $\dim(S+T)=k+(n-k)+(m-k)=n+m-k=\dim S+\dim T-\dim(S\cap T)$.

<u>Liniar ind.</u> Fie scalari $\alpha_1,\dots,\alpha_k,\beta_{k+1},\dots,\beta_n,\gamma_{k+1},\dots,\gamma_m\in K$ a.î.

$$\alpha_1x_1+\dots+\alpha_kx_k+\beta_{k+1}y_{k+1}+\dots+\beta_ny_n+\gamma_{k+1}z_{k+1}+\dots+\gamma_mz_m=0$$

$$\underbrace{\gamma_{k+1}z_{k+1}+\dots+\gamma_mz_m}_{\in T}=\underbrace{-(\alpha_1x_1+\dots+\alpha_kx_k+\beta_{k+1}y_{k+1}+\dots+\beta_ny_n)}_{\in S}$$

Deci $\left.\begin{array}{l}\gamma_{k+1}z_{k+1}+\dots+\gamma_mz_m\in S\cap T\\ \{x_1,\dots,x_k\}\text{ bază în }S\cap T\end{array}\right\}\Longrightarrow \exists!\ \alpha_1',\dots,\alpha_k'\in K$

$$\gamma_{k+1}z_{k+1}+\dots+\gamma_mz_m=\alpha_1'x_1+\dots+\alpha_k'x_k$$

$$\left.\begin{array}{l}(-\alpha_1')x_1+\dots+(-\alpha_k')x_k+\gamma_{k+1}z_{k+1}+\dots+\gamma_mz_m=0\\ \{x_1,\dots,x_k,z_{k+1},\dots,z_m\}\text{ bază în }T\Rightarrow\text{lin. ind.}\end{array}\right\}\Rightarrow \begin{array}{l}-\alpha_1'=\dots=-\alpha_k'=0\\ \gamma_{k+1}=\dots=\gamma_m=0.\end{array}$$

Atunci $\left.\begin{array}{l}\alpha_1x_1+\dots+\alpha_kx_k+\beta_{k+1}y_{k+1}+\dots+\beta_ny_n=0\\ \{x_1,\dots,x_k,y_{k+1},\dots,y_n\}\text{ bază în }S\Rightarrow\text{lin. ind.}\end{array}\right\}\Rightarrow \begin{array}{l}\alpha_1=\dots=\alpha_k=0\\ \beta_{k+1}=\dots=\beta_n=0.\end{array}$

Generarea: Fie $v\in S+T\Rightarrow v=s+t$, $s\in S$, $t\in T$.

$s\in S=\langle x_1,\dots,x_k,y_{k+1},\dots,y_n\rangle\Rightarrow\exists\ \alpha_1,\dots,\alpha_k,\beta_{k+1},\dots,\beta_n\in K: s=\alpha_1x_1+\dots+\alpha_kx_k+\beta_{k+1}y_{k+1}+\dots+\beta_ny_n$

$t\in T=\langle x_1,\dots,x_k,z_{k+1},\dots,z_m\rangle\Rightarrow\exists\ \alpha_1',\dots,\alpha_k',\gamma_{k+1},\dots,\gamma_m\in K: t=\alpha_1'x_1+\dots+\alpha_k'x_k+\gamma_{k+1}z_{k+1}+\dots+\gamma_mz_m$

$$v=s+t=(\alpha_1+\alpha_1')x_1+\dots+(\alpha_k+\alpha_k')x_k+\beta_{k+1}y_{k+1}+\dots+\beta_ny_n+\gamma_{k+1}z_{k+1}+\dots+\gamma_mz_m.$$

Deci $S+T=\langle x_1,\dots,x_k,y_{k+1},\dots,y_n,z_{k+1},\dots,z_m\rangle$. $\boxtimes$.

3.2.28. <u>Dem</u>. $f\in\mathrm{Hom}_K(V,W)$ $\quad \mathrm{Ker}f\leq_k V$, $\mathrm{Im}f\leq_k W$

Fie $\{x_1,\dots,x_k\}$ bază în $\mathrm{Ker}f$; implicit $\dim\mathrm{Ker}f=k$

$x_1,\dots,x_k$ sunt lin. ind. în $\mathrm{Ker}f$ dar și în $V\Rightarrow$ se pot completa

până la o bază $\{x_1,\dots,x_k,x_{k+1},\dots,x_n\}$ în V ; implicit $\dim V=n$.

Vom arăta că $\{f(x_{k+1}),\dots,f(x_n)\}$ bază în $\mathrm{Im}f$. Rezultă

$$\dim\mathrm{Im}f=n-k=\dim V-\dim\mathrm{Ker}f.$$

Lin. ind. Fie $\alpha_{k+1},\dots,\alpha_n\in K$: $\alpha_{k+1}f(x_{k+1})+\dots+\alpha_nf(x_n)=0$

$$f(\alpha_{k+1}x_{k+1}+\dots+\alpha_nx_n)=0$$

$$\alpha_{k+1}x_{k+1}+\dots+\alpha_nx_n\in\mathrm{Ker}f\Rightarrow\exists\ \alpha_1,\dots,\alpha_k\in K$$

$$\alpha_{k+1}x_{k+1}+\dots+\alpha_n x_n=\alpha_1 x_1+\dots+\alpha_k x_k$$

$$\left.\begin{array}{l}(-\alpha_1)x_1+\dots+(-\alpha_k)x_k+\alpha_{k+1}x_{k+1}+\dots+\alpha_n x_n=0\\ x_1,\dots,x_k,x_{k+1},\dots,x_n \text{ baze în } V \Rightarrow \text{lin. ind.}\end{array}\right\}\Rightarrow$$

$$-\alpha_1=\dots=-\alpha_k=0 \ \& \ \alpha_{k+1}=\dots=\alpha_n=0.$$

<u>Generarea</u>. Fie $y\in \operatorname{Im} f \Rightarrow \exists x\in V: f(x)=y$

$x\in V \Rightarrow \exists \alpha_1,\dots,\alpha_k,\alpha_{k+1},\dots,\alpha_n\in K$ a.î.

$$x=\alpha_1x_1+\dots+\alpha_kx_k+\alpha_{k+1}x_{k+1}+\dots+\alpha_nx_n.$$

$$y=f(x)\overset{f}{\underset{\text{lin}}{=}}\alpha_1\underset{0}{\underset{\parallel}{f(x_1)}}+\dots+\alpha_k\underset{0}{\underset{\parallel}{f(x_k)}}+\alpha_{k+1}f(x_{k+1})+\dots+\alpha_nf(x_n)$$

Deci $y\in\langle f(x_{k+1}),\dots,f(x_n)\rangle$. Deci

$$\operatorname{Im} f=\langle f(x_{k+1}),\dots,f(x_n)\rangle \ \boxtimes.$$

Exerciţii la Baze.

Exerciţiu 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 $K = \mathbb{R}$, şi $V = \mathbb{R}^3$. Când este o listă de vectori $[x, y, z]^t \in (\mathbb{R}^3)^{3\times 1}$ liniar dependentă?

Exerciţiu 3.2.34. Fie V un K-spaţiu vectorial cu $\dim V = n$. Să se arate că pentru orice număr natural $m \leq n$ există un subspaţiu $S \leq_K V$ astfel încât $\dim S = m$.

Exerciţiu 3.2.35. Fie $f : V \to W$ o aplicaţie liniară şi $X \subseteq V$. Să se arate că $f(\langle X\rangle) = \langle f(X)\rangle$.

Exerciţiu 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 $\mathbb{Q}$-spaţiu vectorial şi să se determine o bază şi demensiunea.

Exerciţiu 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 $\mathbb{Q}$-spaţiu vectorial şi să se determine o bază şi demensiunea.

Exerciţiu 3.2.38. Fie $f : V \to W$ o aplicaţie liniară şi $\mathbf{v} = [v_1, \ldots, v_n]^t \in V^{n\times 1}$ o listă de vectori. Notăm $f(\mathbf{v}) = [f(v_1), \ldots, f(v_n)]^t \in W^{n\times 1}$. Atunci:

(a) dacă f este injectiv şi $\mathbf{v}$ este liniar independentăatunci $f(\mathbf{v})$ are aceeaşi proprietate.
(b) Dacă f este surjectiv şi $\langle \mathbf{v}\rangle = V$, atunci $\langle f(\mathbf{v})\rangle = W$.
(c) Dacă f este bijectiv şi $\mathbf{v}$ este o bază a lui V atunci $f(\mathbf{v})$ este de asemenea o bază (a lui W).

Exerciţiu 3.2.39. Pentru un K-spaţiu vectorial V cu $\dim V = n$ şi $S \leq_K V$, să se arate că există $T \leq_K V$ astfel încât $S \oplus T = V$.

Exerciţiu 3.2.40. Se consideră în $\mathbb{R}^3$ lista de vectori $\mathbf{v} = [v_1, v_2, v_3]^t$. Folosind două metode (definiţia bazei respectiv lema substituţiei) 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) $v_1 = [2, 1, -1]$, $v_2 = [0, 3, -1]$, $v_3 = [1, a, 1]$.

Exerciţiu 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 $\mathbb{R}^4$ şi să se determine coordonatele lui $x = [2, 3, 2, 10]$ în raport cu acea bază.

Exerciţiu 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:

$$v_1 = (a, 1, 1), v_2 = (1, a, 1), v_3 = (1, 1, a).$$

Exerciţiu 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) $[[1, 2, -1, 2], [2, 3, 0, -1], [2, 4, 0, 6], [1, 2, 1, 4], [3, 6, -1, -1], [1, 3, -1, 0]]^t$.

3.2.44. a) $S = \langle (2,0,1,-1), (0,1,3,2), (-1,0,1,1), (1,1,5,2) \rangle$

$T = \langle (1,0,2,0), (2,1,-1,2), (-1,-1,3,-2) \rangle$

Exerciţiu 3.2.44. Se consideră subspaţiile

(b) $$S = \langle [2,0,1,-1], [0,1,2,3], [-1,0,1,1], [1,1,5,2] \rangle$$
$$T = \langle [1,0,2,0], [2,1,-1,2], [-1,-1,3,-2] \rangle$$

Să se determine

ale spaţiului vectorial real $\mathbb{R}^4$. ~~Şă se folosească lema substituţiei pentru a determina~~ dimensiunea şi câte o bază în subspaţiile S, T, $S+T$ şi $S \cap T$.

Exerciţiu 3.2.45. ~~Folosind lema substituţiei~~ Folosind lema substituţiei, să se calculeze dimensiunea şi câte o bază a subspaţiilor $\mathrm{Ker} f$ şi $\mathrm{Im} f$, în cazurile:

(1) $f : \mathbb{R}^3 \to \mathbb{R}^3$ $f[x_1, x_2, x_3] = [x_1 + 2x_2, x_2 + x_3, x_1 - 2x_3]$.
(2) $f : \mathbb{R}^4 \to \mathbb{R}^3$ $f[x_1, x_2, x_3, x_4] = [x_1 - x_2 - x_3, 3x_2 + x_4, 3x_1 - 3x_3 + x_4]$
(3) $f : \mathbb{R}^3 \to \mathbb{R}^2$ $f[x_1, x_2, x_3] = [-x_1 + 2x_2, x_1 - x_2 + x_3, x_2 + 2x_3]$.
(4) $f : \mathbb{R}^2 \to \mathbb{R}^3$ $f[x_1, x_2] = [x_1 - 3x_2, 2x_1, -x_1 + x_2]$.
(5) $f : \mathbb{R}^4 \to \mathbb{R}^4$
$f[x_1, x_2, x_3, x_4] = [x_1 + 2x_2 + x_3 - x_4, x_1 + 2x_2 - x_3 + x_4, x_1 + 2x_2, x_3 - x_4]$.

3.3. **Aplicaţii liniare şi matrici.**

Matricea unei liste de vectori. În cele ce urmează se consideră un K-spaţiu vectorial V cu $\dim_K V = n$. Reamintim că dacă $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t$ o bază a lui V şi $x \in V$, atunci coordonatele lui x în baza $\mathbf{b}$ sunt scalarii unic determinaţi $[x_1, x_2, \ldots, x_n] \in K^n$ cu proprietatea

$$x = x_1 b_1 + x_2 b_2 + \ldots + x_n b_n = [x_1, x_2, \ldots, x_n][b_1, b_2, \ldots, b_n]^t.$$

Notăm $[x]_{\mathbf{b}} = [x_1, x_2, \ldots, x_n]$ si egalitatea de mai sus se scrie $x = [x]_{\mathbf{b}}\mathbf{b}$.

Definiţie 3.3.1. Fie V un K-spaţiu vectorial cu $\dim_K V = n$. Fie $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t$ o bază a lui V şi $x \in V$. Coordonatele lui x în baza $\mathbf{b}$ sunt scalarii $\mathbf{v} = [v_1, v_2, \ldots, v_m]^t$ un sistem de vectori. Prin matricea listei $\mathbf{v}$ în baza $\mathbf{b}$ se înţelege:

$$[\mathbf{v}]_{\mathbf{b}} = [[v_1]_{\mathbf{b}}, [v_2]_{\mathbf{b}}, \ldots, [v_m]_{\mathbf{b}}]^t \in \mathbb{M}_{m \times n}(K).$$

Cu alte cuvinte

$$[\mathbf{v}]_{\mathbf{b}} = \begin{bmatrix} [v_1]_{\mathbf{b}} \\ [v_2]_{\mathbf{b}} \\ \vdots \\ [v_m]_{\mathbf{b}} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}$$

unde $v_i = a_{i1} b_1 + a_{i2} b_2 + \ldots + a_{in} b_n$ pentru $1 \le i \le m$.

Propoziţie 3.3.2. *Fie V un K-spaţiu vectorial cu $\dim_K V = n$. Fie $\mathbf{e} = [e_1, e_2, \ldots, e_n]^t$ o bază şi fie $\mathbf{b} = [b_1, b_2, \ldots, b_n]$ un sistem de vectori în V. Atunci $\mathbf{b}$ este bază ddacă $[\mathbf{b}]_{\mathbf{e}} \in \mathrm{G}L_n(K)$ (adică $[\mathbf{b}]_{\mathbf{e}}$ este inversabilă), şi în acest caz pentru $x \in V$ avem*

$$[x]_{\mathbf{b}} = [x]_{\mathbf{e}} [\mathbf{b}]_{\mathbf{e}}^{-1}.$$

În particular avem $[\mathbf{e}]_{\mathbf{b}} = [\mathbf{b}]_{\mathbf{e}}^{-1}$.

Demonstraţie. □

Observaţie 3.3.3. Dacă $\mathbf{e} = [e_1, e_2, \ldots, e_n]^t$ şi $\mathbf{b} = [b_1, b_2, \ldots, b_n]$ sunt baze, iar $\mathbf{v} = [v_1, v_2, \ldots, v_m]$ este un sistem de vectori în V atunci

$$[\mathbf{v}]_{\mathbf{b}} = [\mathbf{v}]_{\mathbf{e}} [\mathbf{b}]_{\mathbf{e}}^{-1}.$$

Observaţie 3.3.4. Dacă $\mathbf{v} = [v_1, v_2, \ldots, v_m]^t$ este un sistem de vectori iar $\mathbf{b} = [b_1, b_2, \ldots, b_m]^t$ este o baza a K-spaţiului vectorial V atunci:

$$\operatorname{rank} \mathbf{v} = \operatorname{rank}[\mathbf{v}]_{\mathbf{b}}.$$

Matricea unei aplicaţii liniare.

Definiţie 3.3.5. Se consideră K-spaţiile vectoriale V şi W cu $\dim_K V = m$ şi $\dim_K W = n$. Prin *matricea unei aplicaţii liniare* $f \in \operatorname{Hom}_K(V, M)$ în raport cu perechea de baze $\mathbf{v} = [v_1, v_2, \ldots, v_m]$ a lui V şi $\mathbf{w} = [w_1, w_2, \ldots, w_n]$ a lui W înţelegem

$$[f]_{\mathbf{v},\mathbf{w}} = [f(\mathbf{v})]_{\mathbf{w}} \in \mathbb{M}_{m\times n}(K),$$

unde prin $f(\mathbf{v})$ am notat sistemul de vectori $[f(v_1), f(v_2), \ldots, f(v_m)]^t$ în W. Cu alte cuvinte

$$[f]_{\mathbf{v},\mathbf{w}} = \begin{bmatrix} [f(v_1)]_{\mathbf{w}} \\ [f(v_2)]_{\mathbf{w}} \\ \vdots \\ [f(v_m)]_{\mathbf{w}} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}$$

unde $f(v_i) = a_{i1}w_1 + a_{i2}w_2 + \ldots + a_{in}w_n$ pentru $1 \le i \le m$.

Propoziţie 3.3.6. *Se consideră K-spaţiile vectoriale V, W şi U cu $\dim_K V = m$, $\dim_K W = n$ şi $\dim_K U = p$, împreună cu bazele $\mathbf{v} = [v_1, v_2, \ldots, v_m]$, $\mathbf{w} = [w_1, w_2, \ldots, w_n]$ şi $\mathbf{u} = [u_1, u_2, \ldots, u_p]$ în V, W, respectiv U. Dacă $\alpha \in K$, $f, f \in \operatorname{Hom}_K(V, W)$ şi $g \in \operatorname{Hom}_K(W, U)$ 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) $[g \circ f]_{\mathbf{v},\mathbf{u}} = [f]_{\mathbf{v},\mathbf{w}} \cdot [g]_{\mathbf{w},\mathbf{u}}$.

Demonstraţie. □

Teoremă 3.3.7. *Se consideră K-spaţiile vectoriale V şi W cu $\dim_K V = m$, $\dim_K W = n$, împreună cu bazele $\mathbf{v} = [v_1, v_2, \ldots, v_m]$ şi $\mathbf{w} = [w_1, w_2, \ldots, w_n]$. Atunci*

(a) *Aplicaţia $\varphi : \operatorname{Hom}_K(V, W) \to \mathbb{M}_{m\times n}(K)$, $\varphi(f) = [f]_{\mathbf{v},\mathbf{w}}$ este un izomorfism de spaţii vectoriale.*
(b) *Aplicaţia $\varphi : \operatorname{End}_K(V) \to \mathbb{M}_{m\times n}(K)^o$, $\varphi(f) = [f]_{\mathbf{v},\mathbf{v}}$ este un izomorfism de inele.*

Demonstraţie. □

Observaţie 3.3.8. Pentru $f \in \operatorname{End}_K(V)$ vom nota uneori $[f]_{\mathbf{v}} = [f]_{\mathbf{v},\mathbf{v}}$ (ca si $\mathbb{M}_n(K)$ în loc de $\mathbb{M}_{n\times n}(K)$).

Teoremă 3.3.9 (Formula schimbării de bază)**.** *Se consideră K-spaţiile vectoriale V şi W cu $\dim_K V = m$, $\dim_K W = n$, împreună cu bazele $\mathbf{v} = [v_1, v_2, \ldots, v_m]$, $\mathbf{v}' = [v'_1, v'_2, \ldots, v'_m]$ în V şi $\mathbf{w} = [w_1, w_2, \ldots, w_n]$, $\mathbf{w}' = [w'_1, w'_2, \ldots, w'_n]$ în W. Dacă $f \in \operatorname{Hom}_K(V, W)$ atunci avem*

$$[f]_{\mathbf{v}'\mathbf{w}'} = [\mathbf{v}']_{\mathbf{v}} \cdot [f]_{\mathbf{v},\mathbf{w}} \cdot [\mathbf{w}']_{\mathbf{w}}^{-1}.$$

Demonstraţie. □

Exerciţii la Aplicatii liniare si matrici.

Exerciţiu 3.3.10. Fie $f : \mathbb{R}^3 \to \mathbb{R}^2$, $f[x_1, x_2, x_3] = [x_2, -x_1]$ şi $\mathbf{v} = [[1, 1, 0], [0, 1, 1], [1, 0, 1]]^t$ şi $\mathbf{w} = [[1, 1], [1, -2]]^t$.

(a) Să se arate că $f \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^3, \mathbb{R}^2)$.
(b) Să se arate că $\mathbf{v}$ şi $\mathbf{w}$ sunt baze în $\mathbb{R}^3$, respectiv $\mathbb{R}^2$ şi să se determine matricile $[f]_{\mathbf{v},\mathbf{e}}$ şi $[f]_{\mathbf{v},\mathbf{w}}$, unde $\mathbf{e}$ este baza canonică din $\mathbb{R}^2$.
(c) Să se determine dimensiunea şi câte o bază în $\mathrm{Ker}(f)$ şi $\mathrm{Im}(f)$.

Exerciţiu 3.3.11. Fie $f : \mathbb{R}^4 \to \mathbb{R}^4$, $f[x_1, x_2, x_3, x_4] = [x_1 + 2x_2 + x_3 + x_4, 3x_1 + 7x_2 + 5x_3 + 2x_4, x_1 + 3x_2 + 3x_3, 4x_1 + 9x_2 + x_3 + 8x_4]$ şi $\mathbf{e} = [e_1, e_2, e_3, e_4]^t$ baza canonică în $\mathbb{R}^4$.

(a) Să se arate că $f \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^4)$.
(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 $\mathbb{R}^4$, şi să se determine $[f]_{\mathbf{b}}$ şi $[v]_{\mathbf{b}}$ unde $v = [1, 2, -1, 0]$.
(d) Să se determine dimensiunea şi câte o bază în $\mathrm{Ker}(f)$ şi $\mathrm{Im}(f)$.

3.4. **Diagonalizarea unui endomorfism de spaţii vectoriale.** În cele ce urmează fixăm un K-spaţiu vectorial V, cu $\dim_K V = n \geq 1$, şi un endomorfism $f \in \mathrm{End}_K(V)$.

Propoziţie 3.4.1. *Pentru orice $\lambda \in K$, mulţimea $V(\lambda) = \{x \in V \mid f(x) = \lambda x\}$ este un subspaţiu vectorial al lui V.*

Demonstraţie. □

Observaţie 3.4.2. Avem $V(\lambda) = \mathrm{Ker}(\lambda 1_V - f)$.

Spunem că $\lambda \in K$ este o *valoare proprie* pentru f daca ecuaţia $f(x) = \lambda x$ are soluţii nenule in V, cu alte cuvinte dacă $V(\lambda) \neq 0$. În acest caz, o soluţie nenulă a acestei ecuaţii, adică un vector $0 \neq x \in V(\lambda)$ se numeşte *vector propriu* asociat valorii proprii λ. O matrice se zice *diagonală* dacă este de forma

$$\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & \lambda_n \end{bmatrix}$$

Spunem că f este *diagonalizabil* dacă există o bază b a lui V astfel încât $[f]_b$ este diagonală.

Teoremă 3.4.3. *Fie $b = [b_1, b_2, \ldots, b_n]^t$ o bază a lui V. Atunci*

$$[f]_b = \mathrm{diag}(\lambda_1, \lambda_2, \ldots .\lambda_n)$$

ddacă $\lambda_1, \lambda_2, \ldots .\lambda_n$ sunt valori proprii ale lui f (nu neapărat distincte) iar b_i, $1 \leq i \leq n$ sunt vectori proprii corespunzători acestor valori proprii. Aşadar $f \in \mathrm{End}_K(V)$ este diagonalizabil ddacă există o bază a lui V constituită din vectori proprii, caz ın care matricea lui f in acestă bază are pe diagonală valorile proprii respective.

Demonstraţie. □

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.

Propoziţie 3.4.4. *Polinomul caracteristic al lui f nu depinde de baza în care calculăm matricea lui f, mai precis dacă e şi e' sunt baze pentryu V şi $A = [f]_e$, $A' = [f]_{e'}$, atunci* $\det(tI_n - A) = \det(tI_n - A')$.

Demonstraţie. □

Exemplu 3.4.5. Pentru $n = 2$ şi $[f]_e = A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ avem

$$p_f(t) = \begin{vmatrix} t-a & -b \\ -c & t-d \end{vmatrix} = t^2 - (a+d)t + (ad - bc) = t^2 - \mathrm{trace}(A)t + \det(A).$$

Printr-un uşor abuz de limbaj vorbim uneori de polinomul caracteristic al matricii $A = [f]_e$ în loc de polinomul catacteristic al endomorfismului f şi scriem $p_A(t)$ în loc de $p_f(t)$. Acelaşi lucru este valabil şi pentru vectori şi valori proprii.

Observaţie 3.4.6. Avem:

(a) $\deg p_f = n$.
(b) Dacă $p_f(t) = p_0 + p_1 t + \cdots + p_{n-1}t^{n-1} + p_n t^n$ atunci $p_n = 1$, $p_{n-1} = -\mathrm{trace}(A)$, $p_0 = (-1)^n \det(A)$.

Propoziţie 3.4.7. *$\lambda \in K$ este valoare proprie a lui f ddacă λ este rădăcină a polinomului caracteristic al lui f adică $p_f(\lambda) = 0$.*

Demonstraţie. □

Corolar 3.4.8. *Endomorfismul f are cel mult n valori proprii distincte.*

Numim *multiplicitate algebrică* a valorii proprii $\lambda \in K$ a lui f, multiplicitatea lui λ ca rădăcină a polinomului $p_f(t)$ şi o notăm cu $m(\lambda)$. Numim *multiplicitate geometrică* a valorii proprii $\lambda \in K$ a lui f dimensiunea $d(\lambda) = \dim V(\lambda)$.

Observaţie 3.4.9. Pentru orice valoare proprie $\lambda \in K$ a lui f avem $1 \leq m(\lambda)$ şi $m(\lambda)$ 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 $(t-\lambda)^{m(\lambda)+1} \nmid p_f(t)$.

Propoziţie 3.4.10. *Pentru orice valoare proprie $\lambda \in K$ a lui f avem*

$$1 \leq d(\lambda) \leq m(\lambda).$$

Demonstraţie. □

Lemă 3.4.11. *Dacă $\lambda_1, \lambda_2, \ldots, \lambda_r$ sunt valori proprii distincte pentru f şi $0 \neq b_i \in V(\lambda_i)$, cu $1 \leq i \leq r$, sunt vectori proprii corespunzători, atunci $b_1, b_2, \ldots, b_n$ sunt liniar independenţi.*

Demonstraţie. □

Teoremă 3.4.12. *Următoarele afirmaţii sunt echivalente:*

(i) f este diagonalizabil.
(ii) f are toate valorile proprii în K şi 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.

Demonstraţie. □

Corolar 3.4.13. *Dacă f are n valori proprii distincte în K atunci f este diagonalizabil.*

Ideea algoritmului Page Ranking. (Larry Page - cofondator Google).

Î: Cum se măsoară importanţa unei pagini de internet? R: Importanţa unei pagini de internet depinde de numărul de linkuri care trimit la aceea pagină, dar şi de importanţa paginilor care trimit linkuri către acea pagină. Într-un anume fel o pagină "moşteneşte" din importanţa paginilor care trimit la ea.

Considerăm o reţea fromată din paginile $p_1, p_2 \ldots, p_n$. Căutăm o măsură a importanţei de forma $I : \{p_1, p_2 \ldots, p_n\} \to \mathbb{R}$, care creşte direct proporţional cu importanţa respectivei pagini. Dacă de la o pagină p_i pleacă l_i linkuri către paginile $p_{j_1}, p_{j_2}, \ldots, p_{j_{l_i}}$ atunci fiecăreia dintre aceste pagini i se transferă a l_i-a parte din importanţa paginii p_i. Avem aşadar

$$I(p_j) = \sum \frac{I(p_i)}{l_i}$$

unde suma se face după toate paginile care trimit către p_j. Cu ajutorul numărului de linkuri (care se poate determina) se construieţe 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 trimite 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

$$[I(p_1), I(p_2), \ldots, I(p_n)] = [I(p_1), I(p_2), \ldots, I(p_n)]L,$$

adică $[I(p_1), I(p_2), \ldots, I(p_n)]$ este un vector propriu al lui L corespunzător valorii proprii 1.

Este aşdar util sa avem metode care să determine vectorii si valorile proprii ale unei matrici!

Exerciţii la Diagonalizare.

Exerciţiu 3.4.14. Să se diagonalizeze endomorfismul f (adică să se spună dacă f este diagonalizabil şi în caz afirmativ să se găşească matricea diagonală care îl reprezintă pe f precum şi baza în care f are această matrice) în următoarele cazuri:

(a) $f \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^3)$, $f(x_1, x_2, x_3) = (3x_1 + x_2, -4x_1 - x_2, -4x_1 - 8x_2 - 2x_3)$.

(b) $f \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^4)$ 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) $f \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^3)$, $f(x_1, x_2, x_3) = (x_1 + 3x_3, x_2, 3x_1 - x_3)$. În acest caz să se calculeze f^n cu $n \in \mathbb{N}$.

(d) $f \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^4)$ cu matricea (în baza canonică) $[f]_e = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

Exerciţiu 3.4.15. Să se arate că o matrice cu proprietatea că suma elementelor de pe fiecare linie este 1 admite valoarea proprie 1.

Exerciţiu 3.4.16. Fie $A \in \mathbb{M}_{n\times n}(\mathbb{C})$, cu valorile proprii $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{C}$.

(a) Să se arate că $\det(A) = 0$ ddacă A are valoarea proprie $\lambda = 0$.

(b) Să se determine valorile proprii ale matricilor A^m, unde $m \in \mathbb{N}$ şi A^{-1} (dacă această matrice există).

Exerciţiu 3.4.17. Pentru o matrice $A \in \mathbb{M}_{n\times n}(\mathbb{C})$, să se arate că următoarele afirmaţii 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 şi Informatică, Str. Mihail Kogălniceanu 1, 400084 Cluj-Napoca, România
E-mail address: cmodoi@math.ubbcluj.ro