recapitulare

Wednesday, December 22, 2021 12:31 PM

1. Mulțimi. Funcții. Relații

$p \to q = \neg p \vee q$

$p \leftrightarrow q = \neg p \oplus q$

$\oplus$ = xor

$\neg$ = negare

$\wedge$ = și logic $\quad \vee$ = sau logic $\quad \to$ = implicație logică $\quad \leftrightarrow$ = echivalență logică

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \to q$	$p \leftrightarrow q$
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

Mulțimea este o colecție de obiecte distincte

Mulțimile pot fi date în mod direct prin enumerarea explicită a elementelor lor sau prin precizarea unei condiții pe care trebuie s-o îndeplinească

Exemple: a). $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, $C = \{?, 7, *, \vee\}$, $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$

b). $\mathbb{Z} = \{x \mid x \in \mathbb{N}$ și $0 \le x < 10\}$, $[-3, 8) = \{x \mid x \in \mathbb{R}$ și $-3 \le x < 8\}$

Două mulțimi sunt egale când conțin aceleași elemente.

Exemplu: $\{1, 2, 3\} = \{x \in \mathbb{N} \mid 1 \le x \le 3\} = \{x \in \mathbb{Z} \mid 0 < x < 4\}$

Elementele unei mulțimi nu sunt ordonate în nici un fel: $\{1, 2\} = \{2, 1\}$ sau

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

Într-o mulțime un element apare numai odată: $\{1, 2\}$ și NU $\{1, 2, 2, 1\}$

Mulțimi de numere:
- Nr. naturale: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, $\mathbb{N}^* = \{1, 2, 3, \dots\}$
- Nr. întregi: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- Nr. raționale: $\mathbb{Q} = \{\frac{m}{n} \mid n, m \in \mathbb{Z}, n \neq 0\}$
- Nr. reale: $\mathbb{R}$
- Nr. complexe: $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ și $i^2 = -1$

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

$\emptyset$ - mulțimea vidă

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

(a) reflexivitate: $A \subseteq A$

(b) tranzitivitate: Dacă $A \subseteq B$ și $B \subseteq C$ atunci $A \subseteq C$

(c) antisimetrie: $A = B$ dacă $A \subseteq B$ și $B \subseteq A$

(d) $\emptyset \subseteq A$

(e) Mulțimea vidă este unic determinată

Operații cu mulțimi:

(a) Reuniunea dintre A și B prin $A \cup B = \{x \mid x \in A \vee x \in B\}$

(b) Intersecția dintre A și B prin $A \cap B = \{x \mid x \in A \wedge x \in B\}$

(c) Diferența dintre A și B prin $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$

În cazul în care $A \subseteq U$ se numește complementara lui A în U mulțimea $C_U A = U \setminus A$

Fie A o mulțime. Mulțimea putere a mulțimii A este mulțimea tuturor submulțimilor lui A.

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

Pentru două mulțimi A și B se definește produsul cartezian ca fiind:

$A\times B=\{(a,b)\mid a\in A$ și $b\in B\}$, aici (a,b) este o pereche (ceea ce înseamnă o mulțime ordonată), care din perspectiva teoriei mulțimilor poate fi definită prin $(a,b)=\{a,\{a,b\}\}$

Funcții

O funcție (sau aplicație) este un triplet (A,B,f) care este format din două mulțimi A și B și o lege de corespondență f, așa încât fiecărui element din A îi corespunde un singur element din B. Mulțimile A și B se numesc domeniul de definiție (sau simplu domeniul), respectiv domeniul de valori (sau codomeniul) funcției. Se scrie $f:A\to B$ 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 și imaginea lui a prin f). Se notează cu B^A mulțimea tuturor funcțiilor de la A la B, adică: $B^A=\{f:A\to B \mid f \text{ este o funcție}\}$

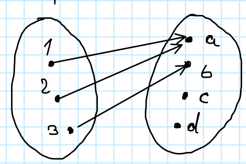
Funcțiile pot fi definite în mai multe moduri:

(a) Prin indicarea directă a imaginii fiecărui element din domeniu de exemplu: $f:\{1,2,3\}\to\{a,b,c,d\}$, $f(1)=f(2)=f(3)$. Variante (pentru aceeași funcție).

Printr-un tabel:

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

Printr-o diagramă:

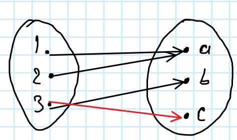


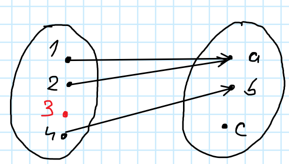
(b) Printr-o formulă de calcul a imaginii fiecărui element, de exemplu $f: \mathbb{N}\to\mathbb{N}$, $f(x)=x+1$ pentru orice $x\in\mathbb{N}$

- Pentru orice mulțime A se definește funcția identitate prin $1_A: A\to A$, $1_A(x)=x$ pt $\forall x\in A$
- Dacă A și B sunt mulțimi așa încât $A\subseteq B$, se definește funcția de incluziune prin $i=i_{A,B}:A\to B$, $i(x)=x$ pentru orice $x\in A$.

Dacă A, B, C sunt mulțimi, așa încât $C\subseteq A$ și $f:A\to B$ este o funcție se construiește funcția restricție a lui $f|_C: C\to B$, $f|_C(x)=f(x)$ pt. $\forall x\in C$

- Următoarele corespondențe nu sunt funcții:





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

(a) Imaginea lui X prin f, ca fiind

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

(a) Imaginea lui X prin f, ca fiind

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

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

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

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

- Dacă $f: A \to B$ și $g: B \to C$ sunt funcții, atunci compunerea lor este definită astfel $g \circ f: A \to C$, $(g \circ f)(x) = g(f(x))$ pt $\forall\, x \in A$
  - Compunerea funcțiilor este asociativă, de exemplu:

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \text{ , avem } (g \circ f) \circ h = g \circ (f \circ h)$$

- O funcție $f: A \to B$ se numește inversabilă dacă există o altă funcție $f': B \to A$ a.î. $f' \circ f = 1_A$ și $f \circ f' = 1_B$
  - Dacă $f: A \to B$ este inversabilă, atunci există o singură funcție $f': B \to A$ cu proprietatea $f' \circ f = 1_A$ și $f \circ f' = 1_B$. Notăm cu f^{-1} această funcție și o numim inversa funcției f. De asemenea avem $(f^{-1})^{-1} = f$.

- $\exp: \mathbb{R} \to (0, \infty)$, $\exp(x) = e^x$ este inversabilă și are inversa $\ln: (0, \infty) \to \mathbb{R}$. A se observa legătura dintre inversabilitatea funcțiilor și soluția (eventual unică) a ecuațiilor!
  - Dacă $A \xrightarrow{f} B \xrightarrow{g} C$ sunt două funcții inversabile, atunci tot așa este și $g \circ f$; mai mult avem $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Injectivitate. Surjectivitate. Bijectivitate

- O funcție $f: A \to B$ se numește:

  (a) injectivă dacă pentru $x_1, x_2 \in A$, $x_1 \neq x_2$ implică $f(x_1) \neq f(x_2)$

  (b) surjectivă dacă pentru orice $y \in B$ există $x \in A$ așa încât $f(x) = y$.

  (c) bijectivă dacă f atât injectivă cât și surjectivă

- În mod echivalent o funcție $f: A \to B$ este

  (a) injectivă dacă $x_1, x_2 \in A$, $f(x_1) = f(x_2)$ implică $x_1 = x_2$

  (b) surjectivă dacă $f(A) = B$

- O funcție $f: A \to B$ este:
  - injectivă dacă pt. $\forall\, y \in B$ ecuația $f(x) = y$ are cel mult o soluție;
  - surjectivă — // — — // — — // — — // — cel puțin o soluție,
  - bijectivă — // — — // — — // — — // — exact o soluție.

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

  (a) Dacă f și g sunt injective, atunci așa este și $g \circ f$;

  (b) — // — — // — surjective, — // — — // — — // —;

  (c) — // — — // — bijective, — // — — // — — // —;

(d) Dacă $g \circ f$ este injectivă, atunci așa este și f;

(e) – // – – // – surjectivă, – // – – // – g;

(f) – // – – // – bijectivă, atunci f este injectivă și g este surjectivă.

- Fie g $B \to A$ o funcție cu $A \neq \emptyset$. Următoarele afirmații sunt echivalente:

  (i) f este injectivă

  (ii) f are o inversă la stânga, adică $g: B \to A$, a.î. $g \circ f = 1_A$

  (iii) f este simplificabilă la stânga adică dacă $h_1, h_2 : A' \to A$ sunt funcții atunci $f \circ h_1 = f \circ h_2$ implică $h_1 = h_2$

- Fie $g: B \to A$ o funcție. Următoarele afirmații sunt echivalente:

  (i) g este surjectivă

  (ii) g are o inversă la dreapta adică există $f: A \to B$ a.î. $g \circ f = 1_A$

  (iii) g este simplificabilă la dreapta, adică dacă $k_1, k_2 : A \to A'$ sunt funcții atunci $k_1 \circ g = k_2 \circ g$ implică $k_1 = k_2$

- Fie $f: A \to B$ o funcție. Următoarele afirmații sunt echivalente:

  (i) f este bijectivă

  (ii) f este inversabilă

  (iii) f este simplificabilă bilateral

Cardinalul unei mulțimi

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

- Fie A o mulțime finită. Următoarele afirmații sunt echivalente pentru o funcție $f: A \to A$:

  (i) f este injectivă

  (ii) f este surjectivă

  (iii) f este bijectivă

Operații

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

- O operație $*: A \times A \to A$ pe A se numește:

  (a) asociativă dacă $a * (b * c) = (a * b) * c$ pt $\forall a, b, c \in A$

  (b) comutativă dacă $a * b = b * a$ pt $\forall a, b \in A$

Un element $e \in A$ cu proprietatea $e * a = a * e = a$ pentru $\forall a \in A$ se numește el. neutru pt $*$

(b) comutativă dacă $a * b = b * a$ pt $\forall a, b \in A$

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

- Considerăm o operație asociativă $* : A \times A \to A$ care are un el. neutru e.

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

(b) Dacă $x, y \in A$ sunt inversabile, atunci $x * y$ este de asemenea inversabil și avem $(x * y)^{-1} = y^{-1} * x^{-1}$

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

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

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

Exemplu: $A = B = \mathbb{R}$

$$\mathcal{R} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

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

(a) reflexivă dacă ara pt. orice $a \in A$

(b) tranzitivă dacă pt. orice $a, b, c \in A$ arb și brc rezultă arc.

(c) simetrică dacă pt orice $a, b \in A$ din arb și bra rezultă $a = b$

(d) antisimetrică dacă pentru orice $a, b \in A$ din arb și bra rezultă $a = b$

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

Exemple: (1) Relația de egalitate pe o mulțime arbitrară

(2) Congruența triunghiurilor (pe mulțimea tuturor triunghiurilor din plan)

(3) Asemănarea triunghiurilor (pe mulțimea tuturor triunghiurilor din plan)

Fie A o mulțime. O relație de ordine (pe scurt ordine) pe A este o preordine care este și asimetrică, adică o relație omogenă pe A care este reflexivă, tranzitivă și asimetrică asimetrica, adică o relație omogenă pe A care este reflexivă, tranzitivă și asimetrică

Exemple. (1) Relația de egalitate pe o mulțime arbitrară.

(2) Relația obișnuită de mai mic sau egal pe $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ sau $\mathbb{R}$

(3) Incluziunea pe o mulțime a căror elemente sunt mulțimi de exemplu $(\mathcal{P}(M), \subseteq)$ este o mulțime ordonată, unde M este o mulțime oarecare

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

(a) minimal dacă pt orice $x \in A$ din $x \leq a \Rightarrow x = a$

(b) maximal dacă pt $\forall x \in A$ din $a \leq x \Rightarrow x = a$

(c) cel mai mic element a lui A dacă $a \leq x$ pt $\forall x \in A$

(d) cel mai mare element a lui A dacă $x \leq a$ pt $\forall x \in A$

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

Proprietăți valabile într-o latice:

(a) $x \vee (y \vee z) = (x \vee y) \vee z$ și $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (asociativitate)

(b) $x \vee y = y \vee x$ și $x \wedge y = y \wedge x$ (comutativitate)

(c) $x \vee (x \wedge y) = x = x \wedge (x \vee y)$ (absorbție)

GRUPURI

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

Exemple: (1) Grupuri abeliene:

(a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$

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

(c) $(\mathcal{M}_{m \times n}(\mathbb{Z}), +), (\mathcal{M}_{m \times n}(\mathbb{Q}), +), (\mathcal{M}_{m \times n}(\mathbb{R}), +), (\mathcal{M}_{m \times n}(\mathbb{C}), +)$

(2) Monoizi, dar nu grupuri:

(a) $(\mathbb{N}, +), (\mathbb{N}, \cdot)$

(b) $(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$

(c) $(\mathcal{M}_{m \times n}(\mathbb{Z}), \cdot), (\mathcal{M}_{m \times n}(\mathbb{Q}), \cdot), (\mathcal{M}_{m \times n}(\mathbb{R}), \cdot), (\mathcal{M}_{m \times n}(\mathbb{C}), \cdot)$

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

împreună cu operația indusă formează un grup. Se scrie $H \leq G$

Exemple: (1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ (cu adunarea)

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

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

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

Teorema de caracterizare a subgrupurilor

Fie un grup $(G, \cdot)$ și fie $H \subseteq G$ o submulțime. Următoarele afirmații sunt echivalente

(i) $H \leq G$

(ii) (a) $1 \in H$

(b) $x, y \in H \Rightarrow xy \in H$

(c) $x \in H \Rightarrow x^{-1} \in H$

(iii) (a) $1 \in H$

(b) $x, y \in H \Rightarrow xy^{-1} \in H$

Fie $(G, \cdot)$ și $(H, \cdot)$ două grupuri. Se numește homomorfism (de grupuri) între G și H o funcție $f: G \to H$ cu proprietatea $f(xy) = f(x)f(y)$ pt. $\forall\, x, y \in G$. Se numește izomorfism (de grupuri) un homomorfism care este bijectiv. În acest caz grupurile sunt numite izomorfe și notăm $G \cong H$

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

Fie $f: G \to H$ un homomorfism. Numim nucleul respectiv imaginea lui f mulțimile

$$\ker f = \{ x \in G \mid f(x) = 1 \} \quad \text{și} \quad \operatorname{Im} f = \{ f(x) \mid x \in G \}$$

Dacă $f: G \to H$ este un homomorfism atunci:

(a) $\ker f \leq G$

(b) $\operatorname{Im} f \leq H$

(c) f este injectiv dacă $\ker f = \{1\}$

(d) f este surjectiv dacă $\operatorname{Im} f = H$

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

Exemple: (a) În $\forall$ grup $(G, \cdot)$ există un singur element de ordin 1, anume el. neutru $\operatorname{ord}(1) = 1$

(b) În $(\mathbb{Z}, +)$ avem $\operatorname{ord}(2) = \operatorname{ord}(3) = \infty$ și chiar $\operatorname{ord}(x) = \infty$ pt $\forall\, x \neq 0$

(c) În $(\mathbb{R}^*, \cdot)$ avem $\operatorname{ord}(-1) = 2$ și $\operatorname{ord}(2) = \operatorname{ord}(-2) = \operatorname{ord}(3) = \infty$; mai mult, $\operatorname{ord}(x) = \infty$ pt $\forall\, x \in \mathbb{R} \setminus \{1, -1\}$

(d) În $(\mathbb{C}^*, \cdot)$ avem $\operatorname{ord}(i) = \operatorname{ord}(-i) = 4$, $\operatorname{ord}\left(\cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}\right) = 3$ $\operatorname{ord}(2) = \operatorname{ord}(-2) = \infty$; mai mult $\operatorname{ord}(x) = \infty$ pt $\forall\, x \in \mathbb{C}^*$ cu $|x| \neq 1$

Fie A o mulțime și $(G, \cdot)$ un grup. Se numește acțiune (la stânga) a lui G pe A o funcție $\alpha : G \times A \to A$ cu propr.: (1) $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ pt. $\forall g, h \in G$ și $\forall x \in A$

(2) $\alpha(1, x) = x$ pt $\forall x \in A$

Definiţie 2.1.36. Fie n un număr natural şi G un subgrup al grupului simetric $S_n = S(\{1, 2, \ldots, n\})$. Acţiunea lui G pe $\{1, 2, \ldots, n\}$ a cărei reprezentare prin permutări este funcţia de incluziune $i : G \to S_n$ este numită acţiunea canonică. Pentru $\sigma \in S_n$ 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).

INELE ȘI CORPURI

Un inel este un triplet $(R, +, \cdot)$ care constă dintr-o mulțime R împreună cu două operații $+, \cdot : R \times R \to R$, a.î.

(a) $(R, +)$ grup abelian

(b) $\cdot$ este asociativă

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

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

Inelul R se zice comutativ sau unitar, dacă operația $\cdot$ este și comutativă, respectiv are o unitate.

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 $(M_{n\times n}(R), +, \cdot)$ este de asemenea inel; totuşi $(M_{n\times n}(R), +, \cdot)$ nu este în mod necesar comutativ. Dacă R este unitar aunci to aşa este şi $(M_{n\times n}(R), +, \cdot)$, iar elementul neutru pentru înmulţirea matricilor este aşa numita matrice unitate de rank n:

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

(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.

Un corp este un inel unitar $(K, +, \cdot)$ cu proprietatea că $\forall x \in K^*$ este inversabil (în raport cu $\cdot$).

Exemple: (a) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt corpuri comutative.

(b) $(\mathbb{Z}, +, \cdot)$ nu este un corp.

Fie $(R, +, \cdot)$ un inel. Un subinel al lui R este o submulțime $S \subseteq R$, cu proprietatea că operațiile $+$ și $\cdot$ din R induc operații bine definite pe S (adică $x, y \in S \Rightarrow x+y, xy \in S$; se mai opune 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 $1 \in S$.

Exemple: (1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$

(2) $2\mathbb{Z} \leq \mathbb{Z}$ dar $1 \notin 2\mathbb{Z}$

(3) $\forall$ inel R are aşa numetele subinele triviale, adică $\{0\}$ şi R

Teorema de caracterizare 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) $x, y \in S \Rightarrow xy \in S$

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

Obs.: Un subcorp este un subinel unitar.

Teorema de caracterizare a subcorpurilor:

Fie $(K,+,\cdot)$ un corp şi fie $L \subseteq K$ o submulţime. Următoarele sunt echivalente.

(i) $L \leq K$

(ii) (a) $0, 1 \in L$

(b) $x, y \in L \Rightarrow x+y \in L$

(c) $x \in L \Rightarrow x\, y \in L$

(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) $x, y \in L^* \Rightarrow xy^{-1} \in S$

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.*

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

(1) divizor al lui zero la stânga sau dreapta dacă există $y \in R$, $y \neq 0$ a.î. $xy = 0$ respectiv $yx = 0$. Elementul x este numit simplu divizor al lui zero dacă este un divizor atât la st. cât şi la dr.

(2) idempotent dacă este adevărată egalitatea $x^2 = x$

(3) nilpotent dacă există $n \in \mathbb{N}$, a.î. $x^n = 0$

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

(1) $[3]_{12}$ este un divizor al lui zero, pt. că $[3]_{12}[4]_{12} = [4]_{12}[3]_{12} = [0]_{12}$

(2) $[4]_{12}$ este idempotent pt. că $[4]_{12}^2 = [4]_{12}$

(3) $[6]_{12}$ este nilpotent pt. că $[6]_{12}^2 = [0]_{12}$

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

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

Exemplu: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sunt corpuri comutative, deci sunt şi domenii de integritate. $\mathbb{Z}$ este un domeniu de integritate care nu este corp.

SPAŢII VECTORIALE ŞI APLICAŢII LINIARE

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 $\forall x, y \in V$ şi $\forall \alpha, \beta \in K$. Se scrie K^V. 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:

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

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:

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

(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 $n = 1$?

K subcorp în L

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

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

(5) Mulţimea tuturor polinoamelor

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

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.

Reguli de calcul în spaţii vectoriale:

Fie V un K-spaţiu vectorial, $x, y \in V$ şi $\alpha, \beta \in K$. Avem:

(a) $\alpha 0 = 0 = 0x$

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

(c) $\alpha(x - y) = \alpha x - \alpha y$ şi $(\alpha - \beta)x = \alpha x - \beta x$

(d) $\alpha x = 0$ dacă $\alpha = 0$ sau $x = 0$

Fie V un K-spaţiu vectorial. Un subspaţiu (vectorial) a lui V este o submulţime $U \subseteq V$ cu proprietatea că adunarea vectorilor 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 formează un spaţiu vectorial. Se scrie $U \leq_K V$ sau simplu $U \leq V$

Exemplu: Orice spaţiu vectorial ${}_K V$ are două subspaţii aşa zise triviale anume $0 \leq {}_K V$ şi $V \leq {}_K V$

Teorema de caracterizare a subspaţiilor

Fie V un K-spaţiu vectorial şi fie $U \subseteq V$ o submulţime. Următoarele afirmaţii sunt echiv.

(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) $x, y \in U \Rightarrow \alpha x + \beta y \in U$

Fie V un K-spaţiu vectorial şi fie $S, T \leq_K V$ două subspaţii. Suma acestor subspaţii este definită ca fiind $S+T=\{x+y \mid x\in S, y\in T\}$

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 $V \cong W$.

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.

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).

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):*

$$+ : \mathrm{Hom}_K(V, W) \times \mathrm{Hom}_K(V, W) \to \mathrm{Hom}_K(V, W),$$
$$(f + g)(x) = f(x) + g(x) \text{ pentru orice } x \in V,$$

şi cu înmulţirea cu scalari

$$\cdot : K \times \mathrm{Hom}_K(V, W) \to \mathrm{Hom}_K(V, W), (\alpha f)(x) = \alpha f(x), \text{ pentru orice } x \in V.$$

În particular $(\mathrm{End}_K(V), +, \circ)$ *este un inel unitar.*

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* $\mathrm{Ker} f = 0$.
(d) f *este surjectivă ddacă* $\mathrm{Im} f = W$.

$\mathrm{Ker} f = \{0\} \overset{\text{not}}{=} 0$

Independenţă liniară.

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.

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 $i_1, i_2, \ldots, i_n \in \{1, \ldots, n\}$.

Propoziţie 3.2.4. *Se consideră* $\mathrm{w} = [v_{i_1}, v_{i_2}, \ldots, v_{i_m}]^t \in V^{m\times 1}$ *o sublistă a listei* $\mathrm{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$. *Dacă* w *este liniar dependentă, atunci tot aşa este şi* v. *Echivalent, dacă* v *este liniar independentă, atunci tot aşa este şi* w.

Definiţie 3.2.8. O submulţime finită $\{v_1, v_2, \ldots, v_n\} \subseteq V$ se numeşte *liberăi* 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 $\mathrm{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$ astfel încât b este liniar independentă şi $\langle \mathrm{b} \rangle = V$ (i. e. vectorii din această listă generează V).

Exemplu 3.2.11. Lista $\mathrm{e} = [e_1, e_2, \ldots, e_n]^t$ 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:

$$e_i = [\delta_{i,j}]_{1\le j\le n} \in K^n, \text{ unde } \delta_{i,j} = \begin{cases} 1 \text{ dacă } i = j \\ 0 \text{ dacă } i \neq j \end{cases} \quad \text{pentru orice } i \in \{1, \ldots, n\}.$$

Propoziţie 3.2.12. *Fie* V *un* K*-spaţiu vectorial şi* $\mathrm{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$. *Următoarele afirmaţii sunt echivalente:*

(i) b *este o listă de vectori maximal liniar independentă, i. e.* b *este liniar independentă şi pentru orice* $x \in V$ *lista* $\mathrm{b}' = [b_1, b_2, \ldots, b_n, x]$ *nu mai are aceeaşi proprietate.*
(ii) b *este o listă minimală cu proprietatea că generează* V*, i. e.* $\langle \mathrm{b} \rangle = V$ *şi pentru oricare* $i \in \{1, \ldots, n\}$*, avem* $\langle \mathrm{b}^{\setminus i} \rangle \neq V$.
(iii) b *este o bază a lui* V.

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 $\langle b_1, b_2, \ldots, b_n \rangle = V$.

Propoziţie 3.2.16. *Fie* V *un* K*-spaţiu vectorial şi* $\mathrm{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$. *Următoarele afirmaţii sunt echivalente:*

(i) b *este o bază a lui* V.
(ii) *Pentru orice vector* $x \in V$ *există un unic sistem de scalari*

$$\alpha = [\alpha_1, \ldots, \alpha_n] \in K^n \text{ astfel încât } x = \alpha\mathrm{b} = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_n b_n.$$

Definiţie 3.2.17. Fie V un K-spaţiu vectorial şi $\mathrm{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$. Numim *coordonatele* unui vector $x \in V$ în raport cu b scalari unic determinaţi $[\alpha_1, \ldots, \alpha_n]$ cu proprietatea $x = \alpha_1 b_1 + \ldots + \alpha_n b_n$.

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 generază 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 genereazǎ V.

Propoziţie 3.2.23. *Fie V un K-spaţiu vectorial cu $\dim_K V = n$ şi $\mathrm{b} = [b_1, b_2, \ldots, b_n] \in V^{n\times 1}$ o listă de vectori. Următoarele afirmaţii sunt echivalente:*
(i) b *este liniear independentă.*
(ii) $\langle \mathrm{b} \rangle = V$.
(iii) b *este o bază.*

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 $\mathrm{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ 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 $\bar{f}$).*

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. □

Lema
~~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 $\dim V = \dim W$ $<\infty$ 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.*

Teoremă 3.2.30. *(Lema substituţiei) Fie $\mathrm{b} = [b_1, b_2, \ldots, b_n]^t$ o bază a K-spaţiului vectorial V şi $v \in V$ cu coordonatele $[\alpha_1, \alpha_2 \ldots, \alpha_n]$ în raport cu baza b (i. e. $v = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_n b_n$). Considerăm lista de vectori $\mathrm{b}' = [b_1, \ldots, v, \ldots, b_n]^t$ care rezultă din b prin înlocuirea (substituţia) vectorului b_i cu v. Atunci:*
(a) b' *este o bază* ($\Leftrightarrow$) $\alpha_i \neq 0$.
(b) *Dacă b' este o bazăşi $x \in V$ are coordonatele $[x_1, x_2 \ldots, x_n]$ în raport cu b şi $[x'_1, x'_2 \ldots, x'_n]$ în raport cu b' 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 $\mathrm{v} = [v_1, \ldots, v_n]^t$ dimensiunea spaţiului generat de v, i. e. $\mathrm{rank}\,\mathrm{v} = \dim\langle \mathrm{v} \rangle$.

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.