**Algebruh**

1. **MULȚIMI, FUNCȚII, RELAȚII**

**Mulțimi**. *Mulțimea este o colecție de obiecte distincte și bine determinate (numite elemente).* Mulțimile pot fi date în mod direct prin enumerarea explicită a elementelor lor (altfel spus sintetic) sau prin precizarea unei condiții (proprietăți) pe care trebuie să o îndeplinească (adică analitic). Vom scrie x ∈ A (și vom spune că ”x aparține mulțimii A”) pentru a exprima faptul că x este un element al mulțimii A. De notat că noțiunile ”mulțime” și ”apartenență” sunt primare, adică ele nu se definesc.

Următoarele afirmații sunt valabile pentru orice mulțimi A, B și C: (a) A ⊆ A (**reflexivitate**). (b) Dacă A ⊆ B și B ⊆ C atunci A ⊆ C (**tranzitivitate**). (c) A=B dacă A ⊆ B și B ⊆ A (**antisimetrie**). (d) ∅ ⊆ A. (e) Mulțimea vidă este unic determinată.

Fie A și B mulțimi. Se definește: (a) **Reuniunea** dintre A și B prin A ∪ B = {x | x ∈ A ∨ x ∈ B}. (b) **Interseția** dintre A și B prin A ∩ B = {x | x ∈ A ∧ x ∈ B}. (c) **Diferența** dintre A și B prin A \ B = {x | x ∈ A ∧ x ∉ B}.

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

P (A) = {X | X ⊆ A}.

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

A × B = {(a, b) | a ∈ A ¸si b ∈ B}.

Pentru o mulțime A avem A1 = A și An = An−1 × A, pentru orice n > 1.

**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 domeniulde definiție (sau simplu domeniul), respectiv domeniul de valori (sau codomeniul)funcției. Se scrie f: A → B sau A -f→ B. Pentru a ∈ A se notează f(a) uniculelement din B care îi corespunde lui a prin f (numit și imaginea lui a prin f). Senotează cu BA mulțimea tuturor funcțiilor de la A la B, adică:

BA = {f: A → B | f este o funcție}.

(a) Pentru orice mulțime A se definește **funcția identitate** prin 1A: A → A, 1A(x) = x pentru orice x ∈ A. Se notează uneori idA = 1A. (b) Dacă A și B sunt mulțimi, așa încât A ⊆ B, se definește **funcția incluziune** prin i=iA,B : A → B, i(x) = x, pentru orice x ∈ A. De notat că iA,B = 1A dacă A = B, altfel iA,B≠1A. (c) Dacă A,B,C sunt mulțimi, așa încât C ⊆A și f: A→B este o funcție se construiește **funcția restricție** a lui f la C, prin f|C: C → B, f|C(x) = f(x) pentru orice x ∈ C.

Fie f: A → B o funcție și fie X ⊆ A, Y ⊆ B două submulțimi (a lui A respectiv B). Se definește: (a) **Imaginea** lui X prin f, ca fiind f(X) = {f(x) | x ∈ X} = {y ∈ B | ∃x ∈ X astfel încât f(x) = y}. În cazul X = A vom vorbi despre imaginea funcției f, și anume f(A) = Imf. (b) **Contraimaginea** (imaginea inversă) lui Y prin f, ca fiind f−1(Y) = {x ∈ A | f(x) ∈ Y}.

Dacă f: A → B și g: B → C sunt funcții, atunci **compunerea** lor este definită astfel: g ◦ f: A → C, (g ◦ f)(x) = g(f(x)) pentru orice x ∈ A.

**Teoremă**. Atunci când este definită compunerea funcțiilor este asociativă, adică pentru A -f→ B -g→ C -h→ D avem (h ◦ g) ◦ f = h ◦ (g ◦ f). Funcția identitate acționează ca element neutru pentru compunerea funcțiilor, adică pentru A -f→ B avem f = f ◦ 1A = 1B ◦ f

O funcție f: A → B se numește **inversabilă** dacă există o altă funcție f’ : B → A astfel încât f’ ◦ f = 1A și f ◦ f’ = 1B

Dacă A -f→ B -g→ C sunt două funcții inversabile, atunci tot așa este și g ◦ f; mai mult avem (g ◦ f)−1 = f−1 ◦ g−1.

**Injectivitate, surjectivitate, bijectivitate**. O funcție f: A → B se numește: (a) **injectivă** dacă pentru x1, x2 ∈ A, x1 ≠ x2 implică f(x1) ≠ f(x2). (b) **surjectivă** dacă pentru orice y ∈ B există x ∈ A așa încât f(x) = y. (c) **bijectivă** dacă f este atât injectivă, cât și surjectivă.

În mod echivalent, o funcție f: A → B este: (a) injectivă dacă x1, x2 ∈ A, f(x1) = f(x2) implică x1 = x2. (b) surjectivă dacă f(A) = B.

O funcție f : A → B este injectivă, surjectivă sau bijectivă dacă pentru orice y ∈ B ecuația f(x) = y are cel mult, cel puțin, respectiv exact o soluție x ∈ A.

Următoarele propoziții sunt adevărate pentru două funcții A -f→B -g→ C:

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

Fie f: A → B o funcție cu A *≠* ∅. Următoarele afirmații sunt echivalente: (i) f este injectivă. (ii) f are o **inversă la stânga**, adică există g: B → A, astfel încât g ◦ f = 1A. (iii) f este **simplificabilă la stânga**, adică dacă h1, h2: A’ → A sunt functii atunci f ◦ h1 = f ◦ h2 implică h1 = h2.

Fie g: B → A o funcție. Următoarele afirmații sunt echivalente: (i) g este surjectivă. (ii) g are o **inversă la dreapta**, adică există f: A → B astfel încât g ◦ f = 1A. (iii) g este **simplificabilă la dreapta**, adică dacă k1, k2: A → A’ sunt funcții atunci k1 ◦ g = k2 ◦ g implică k1 = k2.

**Teoremă**. Fie f: A → 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 → B.* O mulțime A este finită dacă A = ∅ sau există n ∈ N\* așa încât A și {1, 2, . . . , n} au același cardinal. În ultimul caz, numărul natural n este unic determinat, deoarece nu există o bijecție {1, 2 , . . . , n} → {1, 2, . . . , m} pentru n ≠ 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 |∅| = 0.

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

Fie A o mulțime finită. Următoarele afirmații sunt echivalente pentru o funcție f: A → A: (i) f este injectivă. (ii) f este surjectivă. (iii) f este bijectivă.

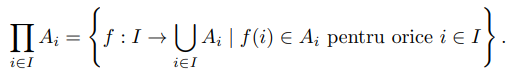
O mulțime infinită A poate fi caracterizată prin proprietatea că există o funcție injectivă (sau surjectivă) f : A → A care nu este bijectivă.

Pentru o submulțime X a unei mulțimi A se definește **funcția caracteristică** ch : A → {0, 1} a lui X (în raport cu A) prin ch(x) = {1 dacă x ∈ X sau 0 dacă x ∉ X}

**Lemă**. Pentru orice mulțime A, funcția ch: P(A) → {0, 1}A, ch(X) = chX este bijectivă.

**Corolar**. Pentru orice mulțime A avem |P(A)| = |{0, 1}A| și mulțimile A și P(A) nu au același cardinal.

**Produs cartezian**. Se consideră **familia de mulțimi** Ai cu i ∈ I. Prin definiție, produsul cartezian al acestei familii este:



Existența produsului cartezian necesită o axiomă specială a teoriei mulțimilor, și anume Axioma Alegerii. Deși intuitiv este clar, din punct de vedere formal nu este posibil ca în lipsa acestei axiome să construim o funcție f : I → Ui∈I Ai așa încât f(i) ∈ Ai pentru orice i ∈ I (adică să alegem elementele f(i) ∈ Ai, i ∈ I).

**Operații**. *Fie A o mulțime. O operație (binară) pe A este o functie ∗ : A × A → A. Adesea se scrie a ∗ b în loc de ∗(a, b).*

O operație ∗ : A × A → A pe A se numește: (a) **operație** **asociativă** dacă a ∗ (b ∗ c) = (a ∗ b) ∗ c pentru orice a, b, c ∈ A. (b) **operație** **comutativă** dacă a ∗ b = b ∗ a pentru orice a, b ∈ A.

Un element e ∈ A cu proprietatea e ∗ a = a ∗ e = a pentru orice a ∈ A se numește **element neutru** pentru ∗. Dacă operația ∗ are un element neutru e, atunci un element x ∈ A se numește **inversabil** dacă exsită x’ ∈ A așa încât x ∗ x’ = e = x’ ∗ x.

Se consideră o operație asociativă ∗ : A × A → A care are un element neutru e. (a) Dacă x ∈ A este inversabil, atunci elementul x’ ∈ A cu proprietatea x∗x’ = e = x'∗x este unic. El se notează cu x−1 și se numește inversul (sau simetricul) lui x. Mai mult, avem (x−1)−1 = x. (b) Dacă x, y ∈ A sunt inversabile, atunci x∗y este de asemenea inversabil și avem (xy)−1 = y−1x−1

Un **monoid** este o pereche (structură) (M, ∗) care consistă dintr-o mulțime M împreună cu o operație asociativă ∗ : M ×M → M, care are un element neutru. Pentru doi monoizi (M, ∗) ¸si (N, ∗) se numește **homomorfism de monoizi** o funcție f : M → N cu proprietatea f(x ∗ y) = f(x) ∗ f(y) pentru orice x, y ∈ M.

**Relații**. *O relație este un triplet (A, B, R), unde A și B sunt două mulțimi oarecare, iar R ⊆ A × B.* Uneori notăm r = (A, B, R) și scriem arb în loc de (a, b) ∈ R, alteori scriem numai R ⊆ A × B pentru a desemna o relație. Ca și în cazul funcțiilor A și B se numesc domeniu respectiv codomeniu. Dacă A = B atunci relația R ⊆ A × A se numește **omogenă** (pe A).

Funțiile pot fi privite ca fiind cazuri speciale de relații, și anume o funcție f : A → B este o relație f = (A, B, F) cu proprietatea suplimentară că pentru orice x ∈ A există un singur element y ∈ B așa încât xfy. În acest caz F = {(a, f(a)) | a ∈ A} este graficul funcției f.

Pentru orice relație (A, B, R) se definește **relația inversă** ca fiind (B, A, R−1), unde (b, a) ∈ R−1 dacă (a, b) ∈ R pentru orice pereche (a, b) ∈ A×B.

Fie r = (A, B, R) o relație și X ⊆ A, Y ⊆ B submulțimi. Se definesc: r(X) = {y ∈ B | există x ∈ X așa încât xry} și r−1(Y ) = {x ∈ A | există y ∈ Y așa încât xry}

Pentru o relație r = (A, B, R) și o submulțime Y ⊆ B avem (r−1)(Y) = r−1(Y).

Fie (A, B, R) și (C, D, S) două relații. **Compunerea celor două relații** este definită prin: (A, D, S ◦ R) unde

S ◦ R = {(a, d) | există x ∈ B ∩ C așa încât (a, x) ∈ B și (x, d) ∈ D}.

O relație omogenă r = (A, A, R) se numește: (a) **relație reflexivă** dacă *ara* pentru orice a ∈ A. (b) **relație tranzitivă** dacă pentru orice a, b, c ∈ A din *arb* și *brc* rezultă *arc*. (c) **relație simetrică** dacă pentru orice a, b ∈ A din *arb* rezultă *bra*. (d) **relație antisimetrică** dacă pentru orice a, b ∈ A din *arb* și *bra* rezultă a = b.

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

**Relații de echivalență**. *Fie A o mulțime. O relație de echivalență (sau pe scurt echivalență) pe A este o preordine care este de asemene simetrică, adică o relație omogenă pe A care este reflexivă, tranztivă și simetrică*.

Fie ≡ o relație de echivalență pe o mulțime A. Pentru un element a ∈ A se notează:

[a] = [a]≡ = {x ∈ A | a ≡ x}

**clasa de echivalență** a lui a. Se numește **mulțimea factor** a lui A modulo ≡ multimea tuturor claselor de echivalență, adică

A/≡ = {[a] | a ∈ A}.

Funția p = p≡ : A → A/≡ dată prin p(x) = [x] se numește **proiecția canonică** atașată relației de echivalență ≡.

Fie (A, A, ≡) o relație de echivalență pe mulțime A și a, b ∈ A. Avem: (a) a ∈ [a], așadar [a] ≠ ∅. (b) [a] = [b] dacă a ≡ b. (c) [a] ∩ [b] ≠ ∅ dacă [a] = [b]. (d) Ux∈A[x] = A.

Fie A o mulțime. O **partiție** a mulțimii A este o submulțime π ⊆ P(A) a mulțimii putere a lui A (adică o mulțime a cărei elemente sunt submulțimi ale lui A), așa încât: (a) ∅ ∈/ π. (b) Pentru X, Y ∈ π dacă X ∩ Y ≠ ∅ atunci X = Y . (c) UX∈πX = A.

**Teoremă**. Fie A o mulțime. (1) Dacă (A, A, ≡) este o relație de echivalență pe A, atunci A/≡ este o partiție a mulțimii A. (2) Dacă π⊆P(A) este o partiție a lui A, atunci (A, A, ≡π) este o relație de echivalență, unde pentru orice a, b ∈ A avem a ≡π b dacă există X ∈ π așa încât a, b ∈ X. (3) Procedeele de la (1) și (2) descriu două funcții inverse una celeilalte între mulțimea tuturor echivalențelor pe A și mulțimea tuturor partițiilor pe A.

**Relații de ordine**. *Fie A o mulțime. O relație de ordine (sau pe scurt ordine) pe A este o preordine care este și antisimetrică, adică o relație omogenă pe A care este* ***reflexivă****,* ***tranzitivă*** *și* ***antisimetrică***. Adesea se notează o relație de ordine cu ≤ și se spune că (A, ≤) este o mulțime ordonată. În acest caz notăm x < y relația x ≤ y și x ≠ y.

Fie (A, ≤) o mulțime ordonată. Un element a ∈ A se numește: (a) **minimal** dacă pentru orice x ∈ A din x ≤ a rezultă x = a. (b) **maximal** dacă pentru orice x ∈ A din a ≤ x rezultă x = a. (c) **cel mai mic element** a lui A dacă ≤ x pentru orice x ∈ A. (d) **cel mai mare element** a lui A dacă x ≤ a pentru orice x ∈ A.

Fie (A, ≤) o mulțime ordonată. Se notează ≥=≤−1, adica x ≥ y dacă y ≤ x. Este ușor de a verifica că ≥ este de asemenea o relație de ordine. Se poate observa că a ∈ A este minimal sau cel mai mic element în (A, ≤) dacă a este maximal, respectiv cel mai mare element în (A, ≥) și invers. Această observație se poate extinde pentru toate noțiunile și afirmațiile referitoare la mulțimi ordonate și este așa numitul principiu al dualității.

**Lemă**. Fie (A, ≤) o mulțime ordonată. Dacă A are un cel mai mic (mare) element, atunci acest element este unicul element minimal (respectiv maximal). Cel mai mic (mare) element al unei mulțimi ordonate, dacă există, este unic.

**Teoremă**. Următoarele afirmații sunt echivalente pentru o mulțime ordonată (A, ≤): (i) Orice submulțime nevidă a lui A are un element minimal(**condiția minimalității**). (ii) Orice lanț descrescător de elemente din A este staționar, adică dacă a0 ≥ a1 ≥ a2 ≥ . . . cu a0, a1, a2, . . . ∈ A, atunci există n ∈ N așa încât an = an+1 = . . . (**condiția lanțurilor descrescătoare**).

(iii) Dacă B ⊆ A are proprietățile: (a) B conține toate elementele minimale ale lui A; (b) pentru a ∈ A dacă {x ∈ A | x < a} ⊆ B atunci a ∈ B; atunci B = A (**condiția inductivitații**).

Fie (A, ≤) o mulțime ordonată și X ⊆ A. O margine inferioară (superioară) pentru X este un element a ∈ A așa încât, a ≤ x (respectiv x ≤ a) pentru orice x ∈ X. Se numește **infimum** (**supremum**) a lui X în A cea mai mare (mică) margine inferioară (respectiv superioară) a lui X, adică: **infX** = a ∈ A dacă {a ≤ x pentru orice x ∈ X și dacă a’ ∈ A așa încât a’ ≤ x pentru orice x ∈ X atunci a’ ≤ a}. **supX** = a ∈ A dacă {x ≤ a pentru orice x ∈ X și dacă a’ ∈ A așa încât x ≤ a’ pentru orice x ∈ X atunci a ≤ a’}

Fie (A, ≤) o mulțime ordonată și X ⊆ A. (1) Dacă există inf X și sup X sunt unice. (2) Dacă există cel mai mic (mare) element a a lui X atunci a = inf X (a = sup X)

O **latice** este o mulțime ordonată (L, ≤) cu proprietatea că există inf{x, y} și sup{x, y} pentru orice două elemente x, y ∈ L. Notăm x∨y = sup{x, y} și x∧y = inf{x, y}. Laticea L este o **latice completă** dacă există inf(X) și sup(X) pentru orice submulțime X ∈ L.

**Teoremă**. Într-o latice (L, ≤) sunt valabile proprietățile: (a) x ∨ (y ∨ z) = (x ∨ y) ∨ z și x ∧ (y ∧ z) = (x ∧ y) ∧ z (**asociativitate**). (b) x ∨ y = y ∨ x și x ∧ y = y ∧ x (**comutativitate**). (c) x ∨ (x ∧ y) = x = x ∧ (x ∨ y) (**absorbție**).

Invers, dacă L este o mulțime împreună cu două operații ∨, ∧ : L × L → L așa încât sunt valabile proprietățile (a), (b), (c) de mai sus, atunci L este o multime ordonată în raport cu relația x ≤ y dacă x ∧ y = x; mai mult (L, ≤) este chiar o latice în care inf{x, y} = x ∧ y și sup{x, y} = x ∨ y, pentru orice x, y ∈ L.

O mulțime ordonată (L, ≤) este o latice completă dacă exsită inf X pentru orice X ⊆ L.

**\* de făcut exerciții la relații**

**2. GRUPURI, INELE, CORPURI**

**Grupuri**. *Un grup este o pereche (G, ·) care constă dintr-o mulțime G împreună cu o operație · : G×G → G, astfel încât · este* ***asociativă****, are un* ***element neutru*** *și* ***fiecare element din G este inversabil*** *în raport cu ·.* În cazul în care · este și comutativă atunci G se numește **abelian** sau **comutativ**.

Cel mai adesea operația unui grup oarecare este notată multiplicativ, adică (G, ·). În acest caz elementul neutru este notat 1 și pentru x ∈ G notăm cu x−1 elementul invers. Pentru un grup abelian însă operația este adesea notată aditiv, adică (G, +). În acest caz, elementul neutru se notează 0, iar pentru x ∈ G notăm −x elementul opus.

Următoarele construcții conduc la grupuri neabeliene: (1) Dacă A este o mulțime, atunci S(A) = {σ : A → A | σ este bijectivă} este un grup împreună cu compunerea funcților; acest grup nu este abelian pentru |A| ≥ 3. Grupul S(A) se numește **grupul simetric** al mulțimii A. (2) Fie K ∈ {Q, R, C} și n ∈ N\*. Mulțimea G Ln(K) = {A ∈ Mn×n(K) | det(A) ≠ 0} împreună cu înmulțirea matricilor formează un grup, care nu este comutativ pentru n ≥ 2. Grupul G Ln(K) se numește **grupul linear general de rang n** peste K.

**Subgrupuri**. *Fie (G, ·) un grup. Un subgrup a lui G este o submulțime H ⊆ G, astfel încât operația pe G induce o operație bine definită pe H (i. e. x,y ∈ H ⇒ xy∈ H; se spune de asemenea că H este o parte stabilă a lui G), și H împreună cu oprtația indusă fofrmează un grup.* Se scrie H ≤ G.

**Teorema de caracterizare a subgrupurilor**. Fie (G, ·) un grup și fie H ⊆ G o submulțime. Următoarele afirmații sunt echivalente: (i) H ≤ G. (ii) (a) 1 ∈ H. . (b) x, y ∈ H ⇒ xy ∈ H. . (c) x ∈ H ⇒ x−1 ∈ H. (iii) (a) 1 ∈ H. . (b) x, y ∈ H ⇒ xy−1 ∈ H.

Fie (G, ·) un grup. Dacă Hi ≤ G, cu i ∈ I, atunci **∩**i∈I Hi ≤G. Reuniunea a două sau mai multe subgrupuri nu este cu necesitate subgrup (Ubung 2.1.58).

Fie (G, ·) un grup și X ⊆ G o submulțime a lui G. **Subgrupul generat** de X este definit prin:



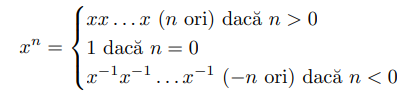
Dacă X = {x1, x2, . . . , xn} este o mulțime finită atunci scriem **〈**x1, x2,. . ., xn**〉**în loc de **〈**{x1, x2,. . ., xn}**〉**

**Lemă**. Fie (G, ·) un grup și X ⊆ G o submulțime a lui G. Atunci: (a)**〈**X**〉**≤ G. (b) X ⊆ **〈**X**〉**și X = **〈**X**〉** dacă X ≤ G. (c) **〈**X**〉** este cel mai mic subgrup a lui G care conține submulțimea X (d) Dacă X ⊆ Y ⊆ G atunci **〈**X**〉**≤**〈**Y**〉**≤ G.

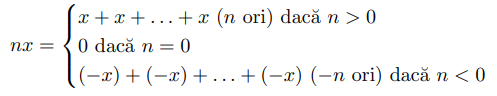
**** Fie (G, ·) un grup ¸si X ⊆ G o submulțime a lui G. Atunci:

unde X−1 = {x−1 | x ∈ X}. Aceasta înseamnă că grupul generat de X conține toate elementele din G care se pot scrie ca un produs finit de elemente din X ∪ X−1.

Fie (G, ·) un grup și x ∈ G. Pentru orice n ∈ Z se definește:



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



**Corolar**. Fie (G, ·) un grup. (a) Pentru x ∈ G avem **〈**x**〉** = {xn | n ∈ Z}. (b) Pentru x, y ∈ G cu xy = yx avem **〈**x, y**〉** = {xnym | n, m ∈ Z}.

**Homomorfisme de grupuri**. *Fie (G, ·) ¸si (H, ·) două grupuri. Se numește homomorfism (de grupuri) între G și H o funcție f : G → H cu proprietatea f(xy) = f(x)f(y) pentru orice x,y ∈ G*. Se numește **izomorfism** (de grupuri) un homomorfism care este *bijectiv*. În acest caz grupurile se numesc izomorfe și notăm G ≅ H.

**Lemă**. Dacă f : G → H este un homomorfism de grupuri atunci: (a) f(1) = 1. (b) f(x−1) = f(x)−1.

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

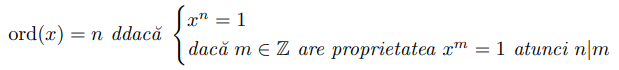
Fie f:G→H un homomorfism. Numim **nucleul**, respectiv **imaginea** lui f mulțimile:



Dacă f : G → H este un homomorfism, atunci: (a) Kerf ≤ G. (b) Imf ≤ H. (c) f este injectiv dacă Ker*f* = {1}. (d) f este surjectiv dacă Im*f* = H.

**Grupuri ciclice și ordinul unui element**. *Un* ***grup ciclic*** *este un grup care este generat de un singur element al său*. Fie (G, ·) un grup și x ∈ G. *Se spune că x este de ordin finit dacă există n ∈ N\* astfel încât xn = 1. În acest caz se numește* ***ordinul lui x*** *cel mai mic număr natural n ∈ N\* cu această proprietate; scriem n = ord(x)*. Elementul x este de ordin infinit dacă el nu este de ordin finit, caz în care scriem ord(x) = ∞.

Fie (G, ·) un grup, x ∈ G ¸si n ∈ N\*. Avem:



Fie (G, ·) un grup. Pentru orice x ∈ G avem ord(x) = |**〈**x**〉**|.

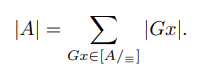
**Acțiuni ale grupurilor pe mulțimi**. Fie A o mulțime și (G, ·) un grup. Se numește acțiune (la stânga) a lui G pe A o funcție α : G × A → A cu proprietățile: (1) α(g, α(h, x)) = α(gh, x) pentru orice g, h ∈ G și orice x ∈ A. (2) α(1, x) = x pentru orice x ∈ A.

Adesea funcția α : G × A → A este văzută ca o operație (înmulțire) externă, în sensul că operanzii nu sunt luați din aceeași mulțime, și este notată prin gx = α(g, x). În acest caz, egalitățile devin: g(hx) = (gh)x, respectiv 1x = x, pentru orice g, h ∈ G ¸si orice x ∈ A.

**Teoremă**. Fie A o mulțime și (G, ·) un grup. (a) Dacă G×A → A, (g, x) → gx este o acțiune a lui G pe A, atunci φ : G → S(A), φ(g) : A → A, φ(g) : x → gx este un homomorfism de grupuri. (b) Dacă φ : G → S(A) este un homomorfism de grupuri, atunci G × A → A, (g, x) → φ(g)(x) este o acțiune a lui G pe A. (c) Procedeele de la (a) și (b) descriu funcții mutual inverese între mulțimea tuturor acțiunilor lui G pe A și mulțimea tuturor homomorfismeleor de grupuri G → S(A).

Fie G × A → A, (g, x) → gx o acțiune a grupului (G, ·) pe mulțimea A. Se numește reprezentare prin permutări a acestei acțiuni homomorfismul de grupuri φ : G → S(A) construit în teorema anterioară. **Acțiunea** se zice **fidelă**, dacă reprezentarea ei prin permutări este un homomorfism injectiv.

Fie G × A→A, (g, x) → gx o acțiune a grupului (G, ·) pe mulțimea A. Relația (A,A, ≡) dată prin x ≡ y dacă există g ∈ G astfel încât gx = y, pentru orice x, y ∈ A este o relație de echivalență, a cărei clase de echivalență (numite **orbite**) se determină ca fiind Gx = {gx | g ∈ G}, oricare ar fi x ∈ A.

 **Corolar**. Not˘am cu [A/≡] un sistem de reprezentanți pentru mulțimea tuturor orbitelor unei acțiuni G × A → A a grupului (G, ·) pe mulțimea A. Atunci este valabilă egalitatea:

**Teorema lui Lagrange**. Fie G un grup finit.

(a) Dacă H este un subgrup al lui G atunci |H| divide |G|.

(b) Dacă x ∈ G atunci ord(x) divide |G|.

Ordinul unui grup (G, ·) este cardinalul |G|.

**Grupul simetric**. Fie n un număr natural și G un subgrup al **grupului simetric** Sn = S({1, 2, . . . , n}). Acțiunea lui G pe {1, 2, . . . , n} a cărei reprezentare prin permutări este funcția de incluziune i : G → Sn este numită **acțiunea canonică**. Pentru σ ∈ Sn se numesc **σ-orbite** orbitele acțiunii canonice ale grupului G = **〈σ〉**. O σ-orbită se numește **trivială** dacă ea conține 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**. Două cicluri se numesc disjuncte în cazul în care orbitele lor netriviale sunt disjuncte (ca mulțimi).

Fie σ ∈ Sn: (1) σ = e (e este permutatarea identică) dacă toate σ-orbitele sunt triviale; Altfel spus e este un ciclu de lungime 1.

(2) σ este un ciclu de lungime 1 < k ≤ n dacă exsită o submulțime {i1, i2, . . . , ik} ⊆ {1, 2, . . . , n}, astfel încât σ(i1) = i2, σ(i2) = i3, . . . , σ(in) = i1 și σ(i) = i pentru i /∈ {i1, i2, . . . , ik}. În acest caz {i1, i2, . . . , ik} este singura orbită netrivială a lui σ și notăm σ = (i1, i2, . . . , ik).

**Lemă**. Pentru σ ∈ Sn și i ∈ {1, 2, . . . , n} există un cel mai mic număr natural k ≤ 1, astfel încât σk(i) = i. Acest număr k este lungimea orbitelor **〈σ〉**i și avem: **〈σ〉**i = {i, σ(i), . . . , σk−1(i)}.

**Lemă**. Dacă σ1 și σ2 sunt cicluri disjuncte, atunci σ1σ2 = σ2σ1.

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

Se numește decompunerea lui σ ca produs de cicluri două câte două disjuncte dată în teorema anterioară. Uneori această descompunere conține de asemenea și cicluri triviale (i) = e, unde i ∈ {1, 2, . . . , n} cu proprietatea σ(i) = i, incluzînd cazul σ = e din teorema precedentă.

O inversiune pentru σ ∈ Sn este o pereche (i, j) ∈ {1, 2, . . . , n}2, astfel încât i < j și σ(i) > σ(j). Se notează cu m(σ) numărul de inversiuni și se definește semnul lui σ prin ε(σ) = (−1)m(σ). Permutarea σ se numește (im)pară în cazul în care m(σ) este (im)par.

**Teorema lui Cayley**. Orice grup este izomorf cu un subgrup al unui grup de permutări.

**\* de făcut exerciții grupuri.**

**Inele**. *Un inel este un triplet (R, +, ·), care constă dintr-o mulțime R împreună cu două operații +, · : R × R → R, astfel încât*: (a) (R, +) este un **grup abelian**. (b) · este **asociativă**. (c) · este **distributivă bilateral** în raport cu +, adică pentru orice x, y, x ∈ R avem: x(y + z) = xy + xz și (y + z)x = yx + zx.

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

**Exemple**. (a) (Z, +, ·), (Q, +, ·), (R, +, ·), (C, +, ·) sunt inele comutative și unitare. (b) Dacă R este un inel comutativ, atunci (Mn×n(R),+, ·) este de asemenea inel. totuși (Mn×n(R), +, ·) nu este în mod necesar comutativ. Dacă R este unitar atunci tot așa este și (Mn×n(R), +, ·), iar elementul neutru pentru înmulțirea matricilor este matricea unitate de rank n. (c) Dacă (R, +) este un grup abelian, atunci (R, +, ·) este un inel unde xy = 0 pentru orice x, y ∈ R (un astfel de inel se numește de pătrat nul. În particular R = {0} este un inel(unitar), unde0+0=0·0=0(acest inel se numește inelul nul și este notat R = 0) (d) Dacă (R, +, ·) este un inel, atunci tot așa este și (Ro, +, ∗), unde Ro = R șix ∗ y = yx pentru orice x, y ∈ R; Ro se numește inelul opus lui R.

**Reguli de calcul în inele**. Fie R un inel și x, y, x ∈ R. Avem: (a) x0 = 0x = 0. (b) x(−y) = (−x)y = −xy. (c) x(y − z) = xy − xz și (y − z)x = yx − zx. (d) Dacă R ≠ 0 este un inel unitar, atunci 1 ≠ 0.

**Corpuri**. *Un corp este un inel unitar (K, +, ·) cu proprietatea că oricare x ∈ K\* este* ***inversabil*** *(în raport cu ·)*. (Aici și în continuare notăm K\* = K \ {0}). Un inel unitar K este exact atunci un corp cînd (K, ·) este un grup.

**Exemple**. (a) (Q, +, ·), (R, +, ·), (C, +, ·) sunt corpuri comutative. (b) (Z, +, ·) nu este un corp.

**Subinele**. *Fie (R, +, ·) un inel. Un subinel a lui R este o submulțime S ⊆ R, cu proprietatea că operațiile + și · din R induc operații bine definite pe S* (adică x, y ∈ S ⇒ x + y, xy ∈ S; se mai spune că S este o parte stabilă în raport cu + și ·), iar cu operațiile induse S formează un inel. Se scrie S ≤ R. Dacă 1 ∈ R atunci se numește un subinel unitar S ≤ R cu proprietatea 1 ∈ S.

**Teorema de caractcterizare a subinelelor**. Fie (R, +, ·) un inel și fie S ⊆ R o submulțime. Următoarele afirmații sunt echivalente: (i) S ≤ R. (ii) (a) 0 ∈ S. . (b) x, y ∈ S ⇒ x + y ∈ S. . (c) x ∈ S ⇒ −x ∈ S. . (d) x, y ∈ S ⇒ xy ∈ S. (iii) (a) 0 ∈ S. . (b) x, y ∈ H ⇒ x − y ∈ H. . (c) x, y ∈ S ⇒ xy ∈ S.

Fie (R, +, ·) un inel. Dacă Si ≤ R, cu i ∈ I, atunci avem **∩**i∈I Si ≤ R. Reuniunea a două sau mai multe subinele nu este cu necesitate subinel.

**Subcorpuri**. *Fie (K, +, ·) un corp. Un subcorp a lui K este o submuțime L ⊆ K cu proprietatea că operațiile + și · din R induc operații bine definite pe S, iar cu operațiile induse L formează un corp*. Se scrie L ≤ K. Un subcorp este un subinel unitar.

**Teorema de caractcterizare a subcorpurilor**. Fie (K, +, ·) un corp și fie L ⊆ K o submulțime. Următoarele afirmații sunt echivalente: (i) L ≤ K. (ii) (a) 0, 1 ∈ L. . (b) x, y ∈ L ⇒ x + y ∈ L. . (c) x ∈ L ⇒ −x ∈ L. . (d) x, y ∈ L ⇒ xy ∈ L. . (e) x ∈ L\* ⇒ x−1 ∈ L (iii) (a) 0, 1 ∈ L. . (b) x, y ∈ L ⇒ x − y ∈ L. . (c) x, y ∈ L\* ⇒ xy−1 ∈ S.

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

**Homomorfisme de inele și de corpuri**. *Un homomorfism de inele (respectiv corpuri) este o funcție f : R → S (f : K → L), unde R și S (K și L) sunt două inele (corpuri), astfel încât f(x + y) = f(x) + f(y) și f(xy) = f(x)f(y) pentru orice x, y ∈ R (x, y ∈ K)*. Dacă inelele R și S sunt unitare, atunci un homomorfism f : R → S se numește **unitar** dacă f(1) = 1. Un homomorfism de inele (corpuri) se numește **izomorfism** dacă este și bijectiv; în acest caz, inelele (corpurile) se numesc izomorfe și scriem R ≅ S (sau K ≅ L).

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

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

**Elemente speciale într-un inel**. Ca și în cazul monoizilor, pentru un inel unitar R notăm:



Fie R un inel. Un element x ∈ R se numește: (1) **divizor al lui zero la stânga sau dreapta** dacă există y ∈ R, y ≠ 0 astfel încât xy = 0 respectiv yx = 0. Elementul x este numit **simplu divizor al lui zero** dacă este un divizor al lui zero atât la stânga cât și la dreapta. (2) **idempotent** dacă este adevărată egalitatea x2 = x. (3) **nilpotent** dacă există n ∈ N, astfel încât xn = 0.

Fie R ≠ 0 un inel și fie x ∈ 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 numește fără divizori ai lui zero, dacă R nu conține divizori netriviali ai lui zero. (b) 0 și 1 (dacă există 1 ∈ R, ceea ce înseamnă R este unitar) sunt elemente idempotente; acești idempotenți sunt numiți triviali. (c) Dacă x este idempotent, atunci este valabilă egalitatea xn = x, pentru orice n∈N\*. (d) Dacă x este nilpotent și xn = 0 pentru un n ∈ N, atunci avem xn+k = 0 pentru orice k ∈ N.

Fie R un inel unitar. (1) Dacă x ∈ R× atunci x nu este un divizor al lui zero. (2) x ∈ R nu este un divizor al lui zero la stânga (dreapta) dacă cu x se poate simplifica la stânga (dreapta). (3) Dacă e ∈ R este un idempotent netrivial, atunci e este un divizor al lui zero. (4) Dacă x ∈ R este nilpotent, atunci x este un divizor al lui zero.

Un **domeniu de integritate** este un inel comutativ, unitar și fără divizori ai lui zero. Un subinel unitar al unui corp comutativ este un domeniu de integritate.

**Corolar**. Un corp comutativ este un domeniu de integritate. Un domeniu de integritate finit este un corp (comutativ).

**Corolar**. Dacă p este un număr prim, atunci (Zp, +, ·) este un corp comutativ.

**\*de făcut exerciții la inele și corpuri**

**3. ALGEBRĂ LINIARĂ**

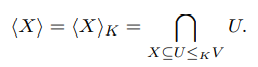
**Spații vectoriale si aplicații liniare**. *Un spațiu vectorial peste K sau mai scurt K-spațiu vectorial este format dintr-un grup abelian (V, +) împreună cu o operație externă · : K × V → V care satisface următoarele axiome*: (SV1) α(x + y) = αx + αy; (SV2) (α + β)x = αx + βx; (SV3) α(βx) = (αβ)x; (SV4) 1x = x pentru orice x, y ∈ V și orice α, β ∈ K. Se scrie KV . Elementele din V și K sunt numite **vectori** respectiv **scalari**. Adunarea în V și operația externă se numesc **adunarea vectorilor** respectiv **înmulțirea cu scalari**. Spațiile vectoriale sunt numite uneori spații liniare.

**Reguli de calcul în spații vectoriale**. Fie V un K-spațiu vectorial, x, y ∈ V și α, β ∈ K. Avem: (a) α0 = 0 = 0x. (b) α(−x) = (−α)x = −αx. (c) α(x − y) = αx − αy ¸si (α − β)x = αx − βx. (d) αx = 0 ddacă α = 0 sau x = 0.

**Subspații vectoriale**. Fie V un K-spațiu vectorial. *Un subspațiu (vectorial) a lui V este o submulțime U ⊆ V , cu proprietatea că adunarea vectorilor și înmulțirea cu scalari induc operații bine definite pe U (adică x, y ∈ U, α ∈ K ⇒ x + y, αx ∈ U), și U împreună cu operațiile restricționate formează un spațiu vectorial*. Se scrie U ≤K V sau simplu U ≤ V. Orice spațiu vectorial KV are două subspații așa zise triviale, anume 0 ≤K V și V ≤K V.

**Teorema de caracterizare a subspațiilor**. Fie V un K-spațiu vectorial și fie U ⊆ V o submulțime. Următoarele afirmații sunt echivalente: (i) U ≤K V . (ii) (a) 0 ∈ U. (b) x, y ∈ U ⇒ x + y ∈ U. (c) x ∈ U, α ∈ K ⇒ αx ∈ U. (iii) (a) 0 ∈ S. (b) x, y ∈ U ⇒ αx + βy ∈ U.

Fie V un K-spațiu vectorial. Dacă Ui ≤KV sunt subspații, cu i ∈ I, atunci avem **∩**i∈IUi ≤K V. Reuniunea a două sau mai multe subspații nu este cu necesitate subspațiu.

 Fie V un K-spațiu vectorial și X ⊆ V o submulțime a lui V. Subspațiul generat de X este definit prin:

Dacă X = {x1, x2, . . . , xn} este o mulțime finită, scriem **〈**x1, x2,. . ., xn**〉**K în loc de **〈**{x1, x2,. . ., xn}**〉**k.

**Lemă**. Fie V un K-spațiu vectorial și X ⊆ V o submulțime a lui V. Avem: (a) **〈**X**〉**K ≤K V . (b) X ⊆ **〈**X**〉**K și X = **〈**X**〉**K dacă X ≤K V . (c) **〈**X**〉**K este cel mai mic subspațiu a lui V care conține X (d) Dacă X ⊆ Y ⊆ G atunci **〈**X**〉**K ≤ **〈**Y**〉**K ≤ V.

 Fie V un K-spațiu vectorial și X ⊆ V o submulțime a lui V. Avem:

 În particular, pentru X = {x1, x2, . . . , xn} avem:

Fie V un K-spațiu vectorial și X ⊆ V . Se numește **combinație liniară** a vectorilor din X o expresie de forma α1x1 + α2x2 + . . . + αnxn cu n ∈ N, x1, x2, . . . , xn ∈ X și α1, α2, . . . , αn ∈ K. În particular o combinație liniară a vectorilor x1.x2, . . . , xn ∈ V este o expresie de forma α1x1 + α2x2 + . . . + αnxn; α1, α2, . . . , αn ∈ K, și o combinație liniară a vectorilor x, y ∈ V este αx + βy, cu α, β ∈ K.

Putem spune că subspațiul generat de X conține toți vectorii care se pot scrie ca V care se pot scrie în formă de combinații liniare de elemente ale lui X.

**Corolar**. Fie V un K-spațiu vectorial. (a) Pentru x ∈ V avem **〈**X**〉**K = {αx | α ∈ K}. (b) Pentru x, y ∈ V avem **〈**x, y**〉**K = {αx + βy | α, β ∈ K}.

**Suma și suma directă a subspațiilor**. Fie V un K-spațiu vectorial și fie S, T ≤K V două subspații. *Suma acestor subspații este definită ca fiind S + T = {x + y | x ∈ S, y ∈ T}*.

Fie V un K-spațiu vectorial și fie S, T ≤K V două subspații. Atunci avem **〈**S ∪ T**〉**K = S + T. In particular suma a două subspații este un subspațiu.

**Corolar**. Într-un K-spațiu vectorial V notăm cu SubK(V ) = {S | S ≤K V } mulțimea tuturor subspațiilor. Atunci (SubK(V ), ≤K) este o latice în care inf{S, T} = S ∩ T și sup{S, T} = S + T.

Fie V un K-spațiu vectorial și fie S, T ≤K V două subspații. Următoarele afirmații sunt echivalente: (i) S ∩ T = 0; (ii) Scrierea oricărui vector din S + T ca o suma dintre un vector din S și unul din T este unică, i. e. pentru v ∈ S + T avem v = x + y = s + t cu x, s ∈ S și y, t ∈ T implică x = s și y = t.

Se numește **sumă directă** o sumă S + T a două subspații S și T care satisfac condițiile echivalente din propoziția anterioară. În acest caz se scrie S ⊕ T = S + T.

Fie V un K-spațiu vectorial și fie S, T ≤K V două subspații. Atunci V = S ⊕ T dacă S ∩ T = 0 și S + T = V.

**Aplicații liniare**. Fie V și W două K-spații vectoriale. *Se numește aplicație liniară sau homomorfism de spații vectoriale între V și W o funcție f : V → W cu proprietățile f(x+y) = f(x) +f(y) și f(αx) = αf(x) pentru orice x, y ∈ V și orice α ∈ K*. Se numește izomorfism o aplicație liniară care este și bijectivă. În acest caz spațiile vectoriale V și W se numesc izomorfe și scriem V ≅ W.

Fie V și W două K-spații vectoriale. Vom nota HomK(V, W) = {f : V → W | f este liniară} și EndK(V ) = HomK(V, V ) (o aplicație liniară f : V → V mai este numită și endomorfism a lui V).

Orice aplicație liniară f : V → W este și un morfism de grupuri, așadar avem: (a) f(0) = 0. (b) f(−x) = −f(x).

Fie V și W două K-spații vectoriale. O aplicație f : V → W este liniară dacă f(αx + βy) = αf(x) + βf(y), pentru orice x, y ∈ V și orice α, β ∈ K.

**Lemă**. Compunerea și adunarea a două aplicații liniare (dacă există) sunt de asemenea aplicații liniare. Înmulțirea unei aplicații liniare cu un scalar este o ˆ aplicație liniară. Funcția inversă a unui izomorfism este de asemenea un izomorifism.

**Teoremă**. Fie V și W două K-spații vectoriale. Atunci HomK(V, W) este de asemenea un K-spațiu vectorial în raport cu adunarea vectorilor (a funcțiilor): + : HomK(V, W) × HomK(V, W) → HomK(V, W), (f+g)(x) = f(x) + g(x) pentru orice x ∈ V, · : K × HomK(V, W) → HomK(V, W), (αf)(x) = αf(x), pentru orice x ∈ V. În particular ˆ (EndK(V ), +, ◦) este un inel unitar.

Fie f : V → W o aplicație liniară. Numim **nucleul** respectiv **imaginea** lui f mulțimile Ker*f* = {x ∈ V | f(x) = 0} și Im*f* = {f(x) | x ∈ V}.

Dacă f : V → W este o aplicație liniară. atunci avem: (a) Ker*f* ≤K V. (b) Im*f* ≤K W. (c) f este injectivă dacă Ker*f* = {0}. (d) f este surjectivă dacă Im*f* = W.

**\*de făcut exerciții la spații vectoriale**

**Independența liniară**. Fie V un K-spațiu vectorial. Se numește listă de vectori un element v = [v1, v2, . . . , vn]t din Vn×1, unde n ∈ N este arbitrar. O listă de vectori v = [v1, v2, . . . , vn]t se numește **liniar independentă** dacă pentru α1, α2, . . . , αn ∈ K scalari avem α1v1 + α2v2 + . . . + αnvn = 0 ⇒ α1 = α2 = . . . = αn = 0. O listă se numește **liniar dependentă** dacă nu este liniar independentă. În acest caz o relație de dependență liniară este o egalitate de forma α1v1 +α2v2 +. . .+αnvn = 0 cu scalarii α1, α2, . . . , αn ∈ K nu toți nuli.

**Observații**. (1) Definiția liniar independenței unei liste v = [v1, v2, . . . , vn]t se poate scrie astfel: [α1, α2, . . . , αn][v1, v2, . . . , vn]t = 0 ⇒ α1 = α2 = . . . = αn = 0. Acesta este motivul pentru care luăm [v1, v2, . . . , vn]t ∈ Vn×1 în loc de [v1, v2, . . . , vn] ∈ Vn.

(2) Lista vidă de vectori este admisă (pentru n = 0). În particular lista vidă este liniar independentă.

(3) O listă cu un singur element [v1]t este exact atunci liniar independentă când v1 ≠ 0. (4) Dacă lista [v1, v2, . . . , vn]t ∈ Vn×1 conține vectorul nul vi = 0, atunci ea este liniar dependentă, deoarece 0v1 + . . . + 1vi + . . . + 0vn = 0. (5) Dacă lista [v1, v2, . . . , vn]t ∈ Vn×1 conține doi vectori egali vi = vj cu i ≠ j atunci ea este liniar dependentă, deoarece 0v1 + . . . + 1vi + . . . + (−1)vj + . . . 0vn = 0. (6) Uneori nu suntem interesați de ordinea vectorilor dintr-o listă v = [v1, v2, . . . , vn]t și spunem că vectorii v1, v2, . . . , vn sunt liniar (in)dependenți în loc să spunem că lista de vectori are respectiva proprietate.

**Exemple**. (1) Lista [v1, v2, v3]t cu vectorii v1 = [1, 0, 1], v2 = [1, 2, 3] și v3 = v1 + v2 = [2, 2, 4] este liniar dependentă în R3 deoarece 1v1 + 1v2 + (−1)v3 = v1 + v2 − v3 = 0. (2) Lista [e1, e2, e3]t cu vectorii e1 = [1, 0, 0], e2 = [0, 1, 0], e3 = [0, 0, 1] este liniar independentă în R3.

Se spune că lista de vectori [w1, w2, . . . , wm]t ∈ Vm×1 este o **sublistă** a listei [v1, v2, . . . , vn]t ∈ Vn×1 dacă {w1, w2, . . . , wm} ⊆ {v1, v2, . . . , vn}. Cu alte cuvinte [w1, w2, . . . , wm]t = [vi1 , vi2 , . . . , vim]t, pentru anumiți indici i1, i2, . . . , in ∈ {1, . . . , n}.

Se consideră w = [vi1 , vi2 , . . . , vim]t ∈ Vm×1 o sublistă a listei v = [v1, v2, . . . , vn]t ∈ Vn×1. Dacă w este liniar dependentă, atunci tot așa este și v. Echivalent, dacă v este liniar independentă, atunci tot așa este și w.

Fie v = [v1, v2, . . . , vn]t ∈ Vn×1 o listă de vectori. Pentru i1,i2, . . . , ik ∈ {1,2,. . .,n} notăm v\i1,i2,...,ik sublista care este obținută din v prin eliminarea vectorilor vi1 ,vi2 , . . ., vik

Pentru o listă de vectori v = [v1, v2, . . . , vn]t ∈ Vn×1 scriem simplu **〈**v**〉** =

**〈**v1, v2, . . . , vn**〉** și vom vorbi despre subspațiul generat de respectiva listă.

Fie v = [v1, v2, . . . , vn]t ∈ Vn×1 o listă de vectori. Lista v este exact atunci liniar dependentă când există i ∈ {1, 2, . . . , n}, astfel încât vi este o combinație liniară a vectorilor din lista v\i.

**Corolar**. Fie v = [v1, v2, . . . , vn]t ∈ Vn×1 o listă de vectori, astfel încât există i ∈ {1, 2, . . . , n}, cu proprietatea că vi este o combinație liniară a vectorilor din lista v\i. Atunci**〈**v**〉**=**〈**v\i**〉**.

O submulțime finită {v1,v2, . . . , vn} ⊆ V se numește **liberă** dacă lista [v1, v2, . . . , vn]t ∈ Vn×1 este liniar independentă. O submulțime oarecare (posibil infinită) B ⊆ V se numește liberă dacă fiecare submulțime finită a lui B este liberă.

**Baze și coordonate**. *O bază (ordonată) a unui K-spațiu vectorial V este o listă de vectori b = [b1, b2, . . . , bn]t ∈ Vn×1 astfel încât b este liniar independentă și* ***〈****b****〉****= V* (i. e. vectorii din această listă generează V). (a) Adesea suntem interesați de baze care nu sunt ordonate, ceea ce înseamnă submulțimi {b1, b2, . . . , bn} ⊆ V astfel încât [b1, b2, . . . , bn]t este o bază (ordonată) (b) Cazul unei baze cu (posibil) o infinitate de elemente este de asemenea admis, chiar dacă noi nu îl vom studia. O bază a unui spațiu vectorial V este o sumbulțime B ⊆ V astfel încât B este liberă și**〈**B**〉** = V.

**Exemplu**. Lista e = [e1, e2, . . . , en]t unde e1 = [1, 0, . . . , 0] ∈ Kn, e2 = [0, 1, . . . , 0] ∈ Kn, . . ., en = [0, 0, . . . , 1] ∈ Kn este o bază pentru Kn. Această bază se numește baza canonică a lui Kn. Baza canonică se poate scrie cu ajutorul așa numitelor simboluri lui Kronecker: ei = [δi,j]1≤j≤n ∈ Kn, unde δi,j ={1 dacă i = j sau 0 dacă i ≠ j} pentru orice i ∈ {1, . . . , n}.

Fie V un K-spațiu vectorial și b = [b1, b2, . . . , bn]t ∈ Vn×1. Următoarele afirmații sunt echivalente: (i) b este o listă de vectori maximal liniar independentă, i. e. b este liniar independentă și pentru orice x ∈ V lista b’ = [b1, b2, . . . , bn, x]t nu mai are aceeași proprietate. (ii) b este o listă minimală cu proprietatea că generează V , i. e. **〈**b**〉** = V și pentru oricare i ∈ {1, . . . , n}, avem **〈**b\i**〉**≠ V. (iii) b este o bază a lui V.

Un K-spațiu vectorial V se numește **finit generat** dacă există o submulțime finită {b1, b2, . . . , bn} ⊆ V astfel încât **〈**b1, b2, . . . , bn**〉**= V.

**Corolar**. Orice spațiu vectorial finit generat are o bază.

Aici și în ce urmează, vom considera numai spații vectoriale finit generate. Totuși multe rezultate sunt valabile sau au un analog și în cazul spațiilor vectoriale care nu sunt finit generate.

Fie V un K-spațiu vectorial și b = [b1, b2, . . . , bn]t ∈ Vn×1. Următoarele afirmații sunt echivalente: (i) b este o bază a lui V . (ii) Pentru orice vector x ∈ V există un unic sistem de scalari α = [α1, . . . , αn] ∈ Kn astfel încât x = αb = α1b1 + α2b2 + . . . + αnbn.

Fie V un K-spațiu vectorial și b = [b1, b2, . . . , bn]t ∈ Vn×1. Numim **coordonatele unui vector x ∈ V în raport cu b** scalari unic determinați [α1, . . . , αn] cu proprietatea x = α1b1 + . . . + αnbn.

**Dimensiune unui spațiu vectorial**.

**Lema lui Steintz**. Se consideră două liste de vectori v = [v1, v2, . . . , vn]t∈ Vn×1 și w = [w1, w2, . . . , wm]t ∈ Vm×1 într-un K-spațiu vectorial V, unde n, m ∈ N. Dacă v este liniar independentă și **〈**w**〉** = V , atunci avem n ≤ m și după o eventuală renumerotare, **〈**v1, . . . , vn, wn+1, . . . , wm**〉** = V.

**Corolar**. Oricare două baze ale unui K-spațiu vectorial (finit generat) au același număr de elemente.

Prin definiție **dimensiunea unui K-spațiu vectorial** (finit generat) V este numărul elementelor unei baze a (prin urmare a tuturor bazelor) lui V. Se scrie dimKV sau simplu dimV. De acum nu vom mai vorbi despre spații finit generate, și vom folosi noțiunea echivlentă (dar mai elegantă) de spații finit dimensionale.

**Exemple**. (1) dim 0 = 0. (2) dimK Kn = n; în particular dimR R = 1, dimR R2 = 2, dimR R3 = 3

Următoarele afirmații sunt adevărate într-un spațiu finit dimensional: (a) Orice listă liniar independentă se poate completa până la o bază. (b) Din orice listă care generază pe V se poate extrage o bază. (c) dim V este cel mai mare număr de vectori liniar independenți care există în V. (d) dim V este cel mai mic număr de elemente a unel liste care generează V.

Fie V un K-spațiu vectorial cu dimK V = n și b = [b1, b2, . . . , bn] ∈ Vn×1 o listă de vectori. Următoarele afirmații sunt echivalente: (i) b este liniear independentă. (ii) **〈**b**〉** = V . (iii) b este o bază.

**Proprietatea de universalitate a bazei unui spațiu vectorial**.

Fie V și W două K-spații vectoriale și v = [v1, v2, . . . , vn]t ∈ Vn×1 o bază a lui V . Pentru orice funcție f : {v1, v2, . . . , vn} → W există o aplicație liniară unică ¯f : V → W astfel încât f’(vi) = f(vi) pentru orice 1 ≤ i ≤ n (i. e. f’ prelungește pe f sau f este o restricție a lui f’).

**Coloral**. Fie V și W două K-spații vectoriale și v = [v1,v2,. . .,vn]t∈Vn×1 o bază a lui V. (a) Dacă f,g : V → W sunt aplicații liniare astfel încât f(vi) = g(vi) pentru orice 1 ≤ i ≤ n, atunci f = g. (b) Dacă dimK W = n atunci V ≅ W. (c) V ≅ Kn.

**Formule legate de dimensiune**.

 Se consideră un K-spațiu vectorial V și S, T ≤K V două subspații. Avem:

**Lemă**. Dacă V este un K-spațiu vectorial finit dimensional și S ≤K V, atunci dim S ≤ dim V. Mai mult, dim S = dim V dacă S = V.

 Fie f : V → W o aplicație liniară între două K-spații vectoriale V și W. Atunci:

Fie V și W două K-spații vectoriale cu dimV = dimW și f : V → W o aplicație liniară. Următoarele afirmații sunt echivalente: (i) f este injectivă. (ii) f este surjectivă. (iii) f este bijectivă.

**Lema substituției**. (**Teoremă**) Fie b = [b1, b2, . . . , bn]t o bază a K-spațiului vectorial V și v ∈ V cu coordonatele [α1, α2 . . . , αn] în raport cu baza b (i. e. v = α1b1 + α2b2 + . . . + αnbn). Considerăm lista de vectori v’ = [b1, . . . , v, . . . , bn] care rezultă din v prin înlocuirea (substituția) vectorului bi cu v. Atunci: (a) b’ este o bază dacă αi ≠ 0. (b) Dacă b’ este o bază și x ∈ V are coordonatele [x1, x2 . . . , xn] în raport cu b și

[x’1, x’2 . . . , x’n] în raport cu b’ atunci: x’i = αi−1xi și x’j = αi−1 (αixj − αjxi) pentru j ≠ i