Fundamentele Algebrice ale Informaticii

Adelina Manea

Structura cursului

Curs 1: Mulțimi. Funcții.
Curs 2: Relactii.
Curs 3: Structuri Agebrice. Monoid. Monoidul liber generat de o mulțime
Curs 4: Grupuri. Morfisme de grupuri. Subgrupuri
Curs 5. Teorema lui Lagrange. Grup factor. Grupuri ciclice. Ordinul unui element.
Curs 6: Inele și corpuri
Curs 7: Inele de polinoame. Inele de matrice

Curs 8: Spații vectoriale. Subspații
Curs 9: Bază și dimensiune
Curs 10: Produs scalar. Ortogonalitate. Subspațiu ortogonal
Curs 11: Transformări liniare
Curs 12: Introducere în teoria codurilor liniare
Curs 13: Corectarea erorilor

- I. D. Ion, N. Radu, *Algebra*, Ed. Didactică și Pedagogică, București, 1975.
- I. D. Ion, N. Radu, C. Niță, D. Popescu *Probleme de Algebră*, Ed. Didactică și Pedagogică, București, 1981.
- C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, vol.1, Ed. Academiei RSR, 1986.
- L. Panaitopol, I.C. Drăghicescu, *Polinoame și ecuații algebrice*, Ed. Albatros, București, 1980.
- I. Purdea, C. Pelea, *Probleme de Algebră*, Ed. Eikon, Cluj-Napoca, 2008.
- I.Tofan, A.C.Volf, *Algebră: Inele. Module. Teorie Galois*, Ed. MatrixRom, București, 2001.
- F. L. Țiplea, *Fundamentele algebrice ale informaticii*, Ed. Polirom, 2006.

O mulțime poate fi descrisă prin enumerarea elementelor sale sau prin precizarea unei proprietăți pe care o au toate elementele sale și doar ele. Numărul de elemente al unei mulțimi A îl numim *cardinalul* mulțimii A și îl notăm $|A|$.
Date fiind două elemente a, b, numim *pereche ordonată* notată (a, b) mulțimea $\{a, \{a, b\}\}$. Evident, egalitatea $(a, b) = (c, d)$ este posibilă dacă și numai dacă $a = c$ și $b = d$.

1. Intersectia($\cap$): $A \cap B = \{x | x \in A$ și $x \in B\}$,
În cazul în care $A \cap B = \Phi$ spunem că mulțimile A și B sunt *disjuncte*.
2. Reuniunea ($\cup$): $A \cup B = \{x | x \in A$ sau $x \in B\}$,
3. Diferența ($-$):$A - B = \{x | x \in A$ și $x \notin B\}$,
4. Diferența simetrică (Δ): $A \Delta B = (A - B) \cup (B - A)$,
5. Produs cartezian ($\times$): $A \times B = \{(a, b) | a \in A$ și $b \in B\}$.

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

Observație

Dacă A,B sunt două mulțimi finite cu $|A| = m$, $|B| = n$, se demonstrază prin inducție matematică după m (sau n) următoarele:

$$|A \times B| = mn, \quad |P(A)| = 2^m.$$

A doua egalitate se poate justifica și utilizând identitatea

$$C_m^0 + C_m^1 + ... + C_m^m = 2^m.$$

Dacă $A = \Phi$ sau $B = \Phi$, atunci $A \times B = \Phi$, $P(A) = \{\ \}$.

Egalitatea a două mulțimi se demonstrează prin dublă incluziune.

Propoziție

Fie A, B, C mulțimi. Atunci:
(1) $A \cap (B \cap C) = (A \cap B) \cap C$ *(asociativitate);*
(2) $A \cap B = B \cap A$ *(comutativitate);*
(3) $A \cap A = A$ *(idempotență);*
(4) $A \cap \Phi = \Phi$*;*
(5) $P(A) \cap P(B) = P(A \cap B)$*;*
(6) $A \cup (B \cup C) = (A \cup B) \cap C$ *(asociativitate);*
(7) $A \cup B = B \cup A$ *(comutativitate);*
(8) $A \cup A = A$ *(idempotență);*
(9) $A \cup \Phi = A$*;*
(10) $P(A) \cup P(B) \subseteq P(A \cup B)$*;*
(11) $A - A = \Phi$, $A - \Phi = A$, $\Phi - A = \Phi$*;*
(12) $A - (B - C) = (A - B) \cup (A \cap C)$*;*
(13) $(A - B) \cup C = (A \cup C) - (B - C)$*;*
(14) $(A - B) \cap C = (A \cap C) - B = A \cap (C - B)$*;*
(15) $A \times (B \cap C) = (A \times B) \cap (A \times C)$*;* $(B \cap C) \times A = (B \times A) \cap (C \times A)$*;*
(16) $A \times (B \cup C) = (A \times B) \cup (A \times C)$*;* $(B \cup C) \times A = (B \times A) \cup (C \times A)$*;*

Propoziție

Fie M o mulțime nevidă și A, B două submulțimi ale sale. Au loc următoarele egalități:
(1) $C_M(C_MA) = A$; $C_M\Phi = M$; $C_MM = \Phi$;
(2) $C_M(A \cap B) = C_MA \cup C_MB$; $C_M(A \cup B) = C_MA \cap C_MB$, *(legile lui De Morgan);*
(3) $A \cap C_MA = \Phi$; $A \cup C_MA = M$; $A - B = A \cap C_MB$.

Principiul includerii și excluderii:

Propoziție

Cardinalul reuniunii a m mulțimi este dat de formula de mai jos

$$|A_1 \cup A_2 \cup ... \cup A_m| = \sum_{i=1}^{m} |A_i| - \sum_{1 \leq i < j \leq m} |A_i \cap A_j| + ... +$$

$$+(-1)^k \sum_{1 \leq i_1 < i_2 < ... < i_k \leq m} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}| + ... + (-1)^{n+1} | \cap_{i=1}^{m} |A_i|.$$

Noțiunea de funcție se introduce în gimnaziu ca fiind o lege f care asociază fiecărui element dintr-o mulțime A numită *domeniu de defin iție* un element și numai unul din altă mulțime B, numită *codomeniu*. Scriem $f: A \to B$, unde mulțimile A, B sunt domeniul, respectiv codomeniul funcției f. Pentru a da o funcție trebuie precizate domeniul, codomeniul și legea de definiție. Două funcții sunt egale dacă au același domeniu, codomeniu și acceași lege de definiție.
Mulțimea funcțiilor definite pe A cu valori în B se notează B^A.

Exemplu

Fie $A = \{1, 2, 3\}$, $B = \mathbf{N}$.

a) $f : A \to B$, $\begin{array}{c|ccc} x & 1 & 2 & 3 \\ \hline f(x) & 1 & 4 & 9 \end{array}$ și $g : A \to B$, $g(x) = x^2$ sunt egale.

b) $f : A \to B$, $f(x) = x - 2$ nu este funcție deoarece $f(1) \notin B$.

c) Dată fiind o mulțime nevidă A, funcția $\mathbf{1}_A : A \to A$ definită prin $\mathbf{1}_A(x) = x, (\forall) x \in A$, se numește funcția identitate a mulțimii A. Pentru $a \in A$ fixat, funcția $f : A \to A$ definită prin $f(x) = a, (\forall) x \in A$, se numește funcția constantă a.

Pentru o mulțime nevidă A se definește funcția :

$$\chi : P(A) \to \{0, 1\}^A, \quad \chi(A') = \chi_{A'} : A \to \{0, 1\},$$

$$\chi_{A'}(x) = 1, pt.x \in A', \quad \chi_{A'}(x) = 0, pt.x \notin A'.$$

Funcția $\chi_{A'}$ se numește funcția caracteristică a submulțimii $A' \subset A$.

Exemplu

Fie $A = \{1, 2, 3\}$ și $B = \{a, b\}$. Atunci $B^A = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$, unde:

$$\begin{array}{c|ccc} x & 1 & 2 & 3 \\ \hline f_1(x) & a & a & a \\ f_2(x) & a & a & b \\ f_3(x) & a & b & a \\ f_4(x) & a & b & b \\ f_5(x) & b & a & a \\ f_6(x) & b & a & b \\ f_7(x) & b & b & a \\ f_8(x) & b & b & b \end{array}.$$

Scrieți toate elementele mulțimii A^B.

Propoziție

Dacă mulțimile A, B sunt finite, de cardinal m, respectiv n, atunci $|B^A| = n^m$.

Fie funcția $f: A \to B$,și submulțimile $A' \subseteq A$, $B' \subseteq B$. Prin *imaginea mulțimii A' prin f* înțelegem

$$f(A') = \{b \in B / (\exists) a \in A', f(a) = b\} \subseteq B,$$

sau, echivalent,

$$f(A') = \{f(a) / a \in A'\} \subseteq B.$$

Submulțimea $Im(f) = f(A)$ a lui B se numește *imaginea funției f*.
Prin *imaginea inversă* sau *preimaginea mulțimii B' prin f* înțelegem

$$f^{-1}(B') = \{a \in A / f(a) \in B'\} \subseteq A.$$

Exemplu

a) Pentru funcția $f\colon \{1,2,3,4\} \to \{a,b,c\}$ definită prin

x	1	2	3	4
$f(x)$	a	a	b	a

,

$Imf = \{a, b\}$, $f(\{1,2\}) = \{a\}$, $f^{-1}(\{c\}) = \Phi$, $f^{-1}(\{a,c\}) = \{1,2,4\}$.

b) Pentru funcția $f\colon \mathbf{R} \to \mathbf{R}$, $f(x) = x^2, (\forall)x \in \mathbf{R}$, avem:
$Imf = [0,\infty)$, $f((-2,4]) = [0,16]$, $f^{-1}([4,9)) = (-3,-2] \cup [2,3)$,
$f^{-1}(-\infty,0]) = 0$

Propoziție

Fie $f : A \to B$, $A' \subseteq A$ *și* $B' \subseteq B$. *Au loc incluziunile:*

$$A' \subseteq f^{-1}(f(A')); \quad f(f^{-1}(B')) \subseteq B'.$$

Definition

Funcția $f : A \to B$ spunem că este
a)**injectivă** dacă $f(x_1) = f(x_2)$ implică $x_1 = x_2$, sau, echivalent, pentru $x_1 \neq x_2$, $f(x_1) \neq f(x_2)$;

b)**surjectivă** dacă $Im(f) = B$;

c)**bijjectivă** dacă este injectivă și surjectivă.

Exemplu

a) Funcția indentică $\mathbf{1}_A : A \to A, \mathbf{1}_A(x) = x$, $(\forall) x \in A$, este bijectivă.
b) Pentru $A' \subseteq A$, funcția incluziune $i : A' \to A, \quad i(x) = x, (\forall) x \in A'$ este injectivă dar nu mereu surjectivă,
c) Funcția caracteristică a submulțimii A', $\chi_{A'} : A \to \{0, 1\}$, $\chi_{A'}(x) = 1$, pentru $x \in A'$, respectiv $\chi_{A'}(x) = 0$, dacă $x \notin A'$, nu este nici injectivă nici surjectivă. Funcția $\chi : P(A) \to \{0, 1\}^A$, $\chi(A') = \chi_{A'}$ este bijectivă.

Două mulțimi intre care există o bijecție se numesc *echipotente*, sau *cardinal echivalente* deoarece au același număr de elemente.

Exemplu

a) Mulțimile *P(A) și* $\{0,1\}^A$ *sunt echipotente, deoarece funcția* χ *din exemplul anterior este bijectivă. În consecințăa,* $|P(A)| = 2^{|A|}$.
b) Funcția $f : \boldsymbol{R} \to (0,1)$, *definită prin* $f(x) = \frac{e^x}{1+e^x}$ *este bijectivă, deci mulțimea numerelor reale este echipotentă cu intervalul* $(0,1)$.

Propoziție

Fie $f : A \to B$, $A' \subseteq A$ *și* $B' \subseteq B$.
a) Dacă f este injectivă, atunci $A' = f^{-1}(f(A'))$.
b) Dacă f este surjectivă, atunci $f(f^{-1}(B')) = B'$.

Fie funcțiile $f: A \to B$, $g: B \to C$. Prin *compusa funcțiilor* f și g înțelegem funcția notată $g \circ f: A \to C$ definită prin $(g \circ f)(x) = g(f(x))$, $(\forall) x \in A$. Se verifică cu ușurință faptul că:

Propoziție

Compunerea funcțiilor este asociativă.

Definition

O funcție $f : A \to B$ se numește **inversabilă** dacă există $g : B \to A$ astfel încât $g \circ f = \mathbf{1_A}$ și $f \circ g = \mathbf{1_B}$. Funcția g se numește inversa funcției f și se notează f^{-1}.

Propoziție

O funcție este inversabilă dacă și numai dacă este bijectivă.

1. Fie A, B două mulțimi nevide și $\{M_i\}_{i\in I} \subset P(A)$, $\{N_j\}_{j\in J} \subset P(B)$, câte o familie de submulțimi ale lor. Dacă $f\colon A \to B$ este o funcție, atunci arătați că:
a) $f(\cup_{i\in I} Mi) = \cup_{i\in I} f(M_i)$;
b) $f^{-1}(\cup_{j\in J} N_j) = \cup_{j\in J} f^{-1}(N_j)$;
c) $f(\cap_{i\in I} Mi) \subseteq \cap_{i\in I} f(M_i)$;
d) $f^{-1}(\cap_{j\in J} N_j) = \cap_{j\in J} f^{-1}(N_j)$;

2. Fie A, B mulțimi finite cu n, respectiv m elemente. Dacă $n \leq m$, câte funcții injective putem defini de la A la B? Dacă $m = n$, câte funcții bijective putem defini de la A la B? Justificați răspunsul.

3. Fie A, B două mulțimi nevide și $f\colon A \to B$. Demonstrați că f este injectivă dacă și numai dacă

$$|f^{-1}(f(x))| = 1, \quad (\forall) x \in A.$$

4. Fie funcțiile $f: A \to B$ și $g: B \to C$. Demonstrați că:
a) Dacă $g \circ f$ este injectivă, atunci f este injectivă.
b) Dacă $g \circ f$ este surjectivă, atunci g este surjectivă.
c) Dacă $g \circ f$ este bijectivă, atunci f este injectivă și g este surjectivă.