

Elemente de algebră

Relații de echivalență. Partiții

Fie $M \neq \emptyset$. Numim *relație binară pe M* orice submulțime nevidă ρ a produsului cartezian $M \times M$. Dacă $(x; y) \in \rho$, notăm $x \rho y$.

Fie ρ o relație binară pe mulțimea M . Spunem că ρ este:

- *reflexivă*, dacă $\forall x \in M, x \rho x$;
- *simetrică*, dacă $\forall x, y \in M, x \rho y \Rightarrow y \rho x$;
- *tranzitivă*, dacă $\forall x, y, z \in M, x \rho y$ și $y \rho z \Rightarrow x \rho z$.

O relație binară reflexivă, simetrică și tranzitivă se numește *relație de echivalență*. De multe ori, o relație de echivalență pe o mulțime M se va nota \sim ; scriem $x \sim y$ (citim *x echivalent cu y*), sau scriem $x \not\sim y$ (citim *x nu este echivalent cu y*).

Fie $n \in \mathbb{N}^*$ și $x, y \in \mathbb{Z}$. Spunem că x este *congruent cu y modulo n* și scriem $x \equiv y \pmod{n}$ dacă n divide $x - y$.

Fie M o mulțime nevidă înzestrată cu relația de echivalență „ \sim ”. Pentru $a \in M$, *clasa de echivalență a lui a* este mulțimea $\hat{a} \stackrel{\text{def}}{=} \{x \in M \mid x \sim a\}$.

Mulțimea claselor de echivalență se notează \widehat{M} (sau (M / \sim)) și se numește *mulțimea factor a lui M prin relația „ \sim ”*. $\widehat{M} \stackrel{\text{def}}{=} \{\hat{a} \mid a \in M\}$.

Fie \sim o relație de echivalență pe M . Clasele de echivalență definite de \sim pe M , sunt disjuncte două câte două.

Fie M o mulțime nevidă. O familie $\{C_i\}_{i \in I}$ de părți nevide ale lui M se numește *partiție a mulțimii M* dacă:

- 1) $\forall i, j \in I, i \neq j \Rightarrow C_i \cap C_j = \emptyset$;
- 2) $\forall x \in M, \exists i \in I$ astfel încât $x \in C_i$.

Fie $\{C_i\}_{i \in I}$ partiție a mulțimii M . $M = \bigcup_{i \in I} C_i$.

Pentru o relație de echivalență pe M , clasele de echivalență definite de această relație formează o partiție a mulțimii M .

Legi de compoziție

Fie M o mulțime nevidă. O aplicație

$$\varphi : M \times M \rightarrow M, (x, y) \mapsto \varphi(x, y),$$

se numește *lege de compoziție (internă)* sau *operație (algebrică, binară) pe mulțimea M* . Elementul $\varphi(x; y) \in M$ se numește *compusul lui x cu y prin φ* (în această ordine).

De obicei, în loc de $\varphi(x; y)$ notăm $x * y$ sau $x \circ y$ sau $x \top y$ sau $x \Delta y$ etc.

Tabla lui Cayley asociată legii de compoziție φ pe mulțimea M este un tabel cu linii și coloane corespunzătoare elementelor mulțimii M obținut astfel: la intersecția liniei a_i cu coloana a_j se află compusul lui a_i cu a_j prin operația φ .

φ	a_1	a_2	...	a_j	...	a_n
a_1						\vdots
a_2						\vdots
\vdots						\vdots
a_i	\dots	\dots	\dots	$\varphi(a_i, a_j)$	\dots	\dots
\vdots						\vdots
a_n						\vdots

Ori de câte ori notăm $(M, *)$ subînțelegem că $*$ este o lege de compoziție internă pe mulțimea nevidă M .

Fie M o mulțime nevidă și „ $*$ “ o lege de compoziție pe M . O submulțime nevidă H a lui M se numește *parte stabilă* în raport cu legea de compoziție „ $*$ “ dacă:

$$\forall x, y \in H \Rightarrow x * y \in H.$$

O lege de compoziție „ $*$ “ se numește *asociativă* dacă:

$$(x * y) * z = x * (y * z), \forall x, y, z \in M.$$

O lege de compoziție $M \times M \rightarrow M$, $(x; y) \mapsto x * y$ se numește *comutativă* dacă $x * y = y * x, \forall x, y \in M$.

Un element $e \in M$ se numește *element neutru* pentru legea de compoziție „ $*$ “, dacă $\forall x \in M \quad e * x = x * e = x$.

Fie M o mulțime nevidă înzestrată cu o lege de compoziție „ $*$ “ cu element neutru e . Spunem că un element $x \in M$ este *simetrizabil* în raport cu legea de compoziție „ $*$ “, dacă există $x' \in M$ astfel încât $x' * x = x * x' = e$. Elementul x' cu această proprietate se numește *simetricul lui x*.

În cazul în care legea de compoziție este o *lege de adunare* (de numere, de matrice, de polinoame, de funcții, de vectori, ...) folosim denumirea de *opus* în loc de simetric al unui element. Dacă legea de compoziție este o *lege de înmulțire* (de numere, de matrice, de polinoame, de funcții, ...) folosim denumirea de *invers* în loc de simetric al unui element. Aceeași denumire se folosește în cazul în care legea de compoziție este o lege de compunere de funcții.

Fie $n \in \mathbb{N}, n \geq 2$. Notăm \mathbb{Z}_n mulțimea claselor de echivalență pentru congruența modulo n . Avem $\mathbb{Z}_n = \{\hat{0}; \hat{1}; \hat{2}; \dots; \widehat{n-1}\}$. Pe \mathbb{Z}_n definim operațiile numite *adunarea* și *înmulțirea claselor de resturi modulo n* astfel: $\hat{\alpha} + \hat{\beta} = \widehat{\alpha + \beta}, \quad \hat{\alpha}\hat{\beta} = \widehat{\alpha\beta}, \quad \forall \hat{\alpha}, \hat{\beta} \in \mathbb{Z}_n$.

Grupuri

Un cuplu $(G; *)$, format cu o mulțime nevidă G și cu o lege de compoziție „ $*$ “ pe G , se numește *grup* dacă legea de compoziție $*$ este asociativă, are element neutru și orice element din M este simetrizabil.

Dacă, în plus, legea $*$ este comutativă, atunci G se numește *grup comutativ* sau *abelian*.

Un cuplu $(M, *)$ format cu o mulțime nevidă M și o lege de compoziție „ $*$ “ pe M , se numește *monoid* dacă legea $*$ este asociativă și are elementul neutru.

Regulile de simplificare într-un grup. Fie $(G, *)$ un grup. Pentru orice $a, b, c \in G$ avem: $a*b = a*c \Rightarrow b = c$ și $b*a = c*a \Rightarrow b = c$

Grupuri de matrice

$GL_2(\mathbb{R}) = \{A \in \mathcal{M}_2(\mathbb{R}) \mid \det A \neq 0\}$ înzestrat cu înmulțirea formează un grup numit *grupul general liniar de grad 2*.

Submulțimile $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid |A| = 1\}$, $O(2) = \{A \in GL_2(\mathbb{R}) \mid A = A^{-1}\}$, $SO(2) = \{A \in O(2) \mid \det A = 1\}$, înzestrate cu înmulțirea matricelor formează grupuri de matrice, numite respectiv *grupul special liniar de grad 2 peste \mathbb{R}* , *grupul ortogonal de grad 2* și *grupul ortogonal special de grad 2*.

Pentru $n \in \mathbb{N}^*$ pot fi definite grupurile $SL_n(\mathbb{Q})$, $SL_n(\mathbb{R})$ și $SL_n(\mathbb{C})$, numite *grupul special liniar de grad n peste \mathbb{Q} , \mathbb{R} , respectiv \mathbb{C}* . De asemenea, pot fi introduse grupurile $O(n)$ și $SO(n)$, numite respectiv *grupul ortogonal de grad n* și *grupul ortogonal special de grad n* .

Morfisme de grupuri

Fie grupurile (G, \circ) și $(G', *)$. Funcția $f: G \rightarrow G'$ se numește *morfism de grupuri* dacă: $f(x \circ y) = f(x) * f(y)$, $\forall x, y \in G$.

Fie (G, \circ) și $(G', *)$ două grupuri. O funcție $f: G \rightarrow G'$ se numește *izomorfism de grupuri* dacă: (1) $f(x \circ y) = f(x) * f(y)$, $\forall x, y \in G$; (2) f este bijectivă.

Spunem că grupul G este *izomorf* cu grupul G' și scriem $G \simeq G'$, dacă există un izomorfism $f: G \rightarrow G'$. În caz contrar, spunem că grupul G *nu este izomorf* cu grupul G' și scriem $G \not\simeq G'$.

Dacă G este grup, atunci un morfism (izomorfism) $f: G \rightarrow G$ se numește *endomorfism* (respectiv *automorfism*) al grupului G .

Grupuri de permutări

Fie A o mulțime finită cu n elemente, $n \in \mathbb{N}^*$. O funcție bijectivă $\sigma: A \rightarrow A$ se numește *permutare* a mulțimii A . Vom nota cu S_A mulțimea tuturor permutărilor mulțimii A .

Pentru $\sigma, \pi \in S_A$, *compunerea permutărilor* σ și π este funcția $\sigma \circ \pi: A \rightarrow A$, cu $(\sigma \circ \pi)(x) = \sigma(\pi(x))$, $x \in A$. Funcția $\sigma \circ \pi$ este de asemenea bijectivă, deci $\sigma \circ \pi \in S_A$. (S_A, \circ) este grup. *Grupul permutărilor* mulțimii $\{1, 2, \dots, n\}$ se notează (S_n, \circ) .

Subgrupuri

Fie $(G, *)$ un grup și H o parte stabilă a lui G . $(H, *)$ se numește *subgrup* al lui G dacă $(H, *)$ este grup.

Fie (G, \cdot) un grup de element neutru e și $a \in G$. Spunem că a este element de *ordin finit* al grupului G dacă există $m > 0$ astfel încât $a^m = e$.

Dacă a este element de ordin finit, atunci cel mai mic număr $m > 0$ cu proprietatea $a^m = e$ se numește *ordinul* lui a și notăm $\text{ord } a = m$.

Grupuri de transformări geometrice

O aplicație $T: \mathcal{P} \rightarrow \mathcal{P}$ se numește *transformare geometrică* a planului \mathcal{P} . Vom spune că T este *izometrie* dacă T conservă distanțele dintre puncte: $d(T(A), T(B)) = d(A, B), \forall A, B \in \mathcal{P}$.

Notăm cu $\text{Izom}(\mathcal{P})$ mulțimea tuturor izometriilor planului \mathcal{P} . Dacă T_1 și T_2 sunt izometrii, atunci și $T_1 \circ T_2$ este o izometrie. $(\text{Izom}(\mathcal{P}), \circ)$ este un grup, numit *grupul izometriilor planului \mathcal{P}* .

Fie F o figură plană, $F \subset \mathcal{P}$ și $T: \mathcal{P} \rightarrow \mathcal{P}$ o izometrie; notăm cu $T(F) = \{T(P) \mid P \in F\}$. Spunem că T *invariază* (global) *pe F* dacă $T(F) = F$.

Notăm cu $\text{Sim}(F)$ mulțimea tuturor izometriilor care invariază pe F .

$(\text{Sim}(F), \circ)$ este un subgrup al grupului $(\text{Izom}(\mathcal{P}), \circ)$, numit *grupul de simetrie al lui F* .

Fie $n \in \mathbb{N}$, $n \geq 3$ și P_n un poligon regulat cu n laturi din planul \mathcal{P} . Grupul de simetrie al lui P_n se notează $D_n = \text{Sym}(P_n)$ și se numește *grupul diedral*.

Inele

În cele ce urmează, se lucrează numai cu inele unitare.

Un triplet $(R, +, \cdot)$, unde R este o mulțime nevidă iar „+” și „ \cdot ” sunt două legi de compoziție pe R (numite *adunare* și *înmulțire*), se numește *inel* dacă:

(G) $(R, +)$ este grup abelian

(M) (R, \cdot) este monoid

(D) înmulțirea este distributivă față de adunare:

$$\forall x, y, z \in R, \quad x(y + z) = xy + xz, \quad (y + z)x = yx + zx.$$

În inelul R , elementul neutru al legii de compoziție „ \cdot ” se numește *element unitate*.

Spunem că *inelul R nu are divizori ai lui zero*, dacă $x \neq 0, y \neq 0 \Rightarrow xy \neq 0$; în caz contrar spunem că R este *inel cu divizori ai lui zero*.

Un *inel R* se numește *comutativ* dacă satisface și axioma: $(M_3) \quad xy = yx, \forall x, y \in R$.

Un inel comutativ, cu cel puțin două elemente și fără divizori ai lui zero, se numește *domeniu de integritate* (sau inel integru).

Morfisme de inele

Fie inelele $(R, +, \cdot)$ și (R', \oplus, \odot) . O funcție $f: R \rightarrow R'$ se numește *morfism de inele* dacă, $\forall x, y \in R$:

(1) $f(x + y) = f(x) \oplus f(y)$;

(2) $f(x \cdot y) = f(x) \odot f(y)$;

(3) $f(1) = 1'$, unde 1 este unitatea inelului R și $1'$ unitatea lui R' .

Un morfism de inele bijectiv se numește *izomorfism*. Vom spune că inelul R este izomorf cu inelul R' , și scriem $R \simeq R'$, dacă există cel puțin un izomorfism $f: R \rightarrow R'$.

Grupul unităților. Subinele

Elementele inversabile ale unui inel R se numesc *unități* ale lui R . Notăm cu $U(R)$ mulțimea unităților inelului R .

Fie R un inel; $U(R)$ este grup în raport cu operația indusă de înmulțirea lui R , numit *grupul unităților* inelului R .

Fie $(R, +, \cdot)$ un inel cu elementul unitate notat 1 și $S \subset R$; S se numește *subinel* al lui R dacă $(S, +, \cdot)$ este inel și $1 \in S$.

Exemple de inele

Numerele complexe $a + bi$, cu $a, b \in \mathbb{Z}$ se numesc *întregi ai lui Gauss* (de exemplu: $2 + 3i, -1 + 2i, 4 = 4 + 0i, i = 0 + 1 \cdot i$ sunt întregi ai lui Gauss). Notăm $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ mulțimea întregilor lui Gauss. $(\mathbb{Z}[i], +, \cdot)$ este un inel integru.

Fie I o mulțime nevidă și R un inel. Notăm $R^I = \{f \mid f: I \rightarrow R\}$ mulțimea tuturor funcțiilor $f: I \rightarrow R$.

Pentru $f, g \in R^I$ și $x \in I$, $f(x)$ și $g(x)$ sunt elemente ale inelului R . Putem defini astfel funcțiile: $f + g: I \rightarrow R$, $(f + g)(x) = f(x) + g(x)$, $x \in I$ și $fg: I \rightarrow R$, $(fg)(x) = f(x) \cdot g(x)$ numite *suma*, respectiv *produsul funcției f cu funcția g* .

Fie R inel comutativ. Notăm $R[X]$ mulțimea polinoamelor cu coeficienții în R . $(R[X], +, \cdot)$ este inel.

Fie $f \in R[X]$. Funcția $f^*: R \rightarrow R$ definită prin $f^*(x) = f(x) \in R$, $\forall x \in R$, este numită *funcția polinomială* asociată polinomului f . Vom nota funcția f tot cu f .

Zerourile funcției polinomiale f , se numesc *rădăcini* (din R) ale polinomului f . Așadar, un element $\alpha \in R$ este *rădăcină* (din R) a polinomului $f \in R[X]$ dacă $f(\alpha) = 0$.

Corpuri. Morfisme de corpuri

Un inel K se numește *corp* dacă $0 \neq 1$ și orice element nenul din K este simetrizabil în raport cu înmulțirea. Dacă înmulțirea este comutativă, K se numește *corp comutativ*.

O funcție $f: K \rightarrow K'$ de la un corp K la un corp K' se numește *morfism (izomorfism)* de corpuri dacă este morfism (izomorfism) de la K la K' considerate ca inele.

Un izomorfism (morfism) $f: R \rightarrow R$ de la inelul $(R, +, \cdot)$ în el însăși se numește *automorfism* (respectiv *endomorfism*) al inelului R . Aceeași terminologie se folosește și pentru corpuri.

Inelul $(\mathbb{Z}_n, +, \cdot)$ este corp dacă și numai dacă n este număr prim.

Aritmetica polinoamelor cu coeficienți într-un corp comutativ

Teorema împărțirii cu rest. Fie K un corp comutativ și $f, g \in K[X]$, $g \neq 0$. Există unic determinate polinoamele $q, r \in K[X]$ astfel încât $f = gq + r$, unde $\text{grad } r < \text{grad } g$ dacă $r \neq 0$.

Polinoamele q și r din teorema împărțirii ($f = gq + r$) se numesc *câtul*, respectiv *restul* împărțirii polinomului f prin polinomul g .

Fie K corp comutativ și $f, g \in K[X]$. Spunem că f este *divizibil cu* g și notăm $g \mid f$ sau $f : g$, dacă există $h \in K[X]$ cu $f = g \cdot h$.

Fie K corp comutativ și $f, g \in K[X]$. Spunem că f este *asociat în divizibilitate* cu g și scriem $f \sim g$, dacă $f \mid g$ și $g \mid f$.

Teorema restului. Restul împărțirii polinomului $f \in K[X]$ prin $X - \alpha \in K[X]$ este egal cu valoarea în α a polinomului f .

Teorema lui Bézout. Polinomul $f \in K[X]$ se divide prin polinomul $X - \alpha \in K[X]$ dacă și numai dacă $f(\alpha) = 0$.

Fie K corp comutativ, $f \in K[X]$, $a \in K$ și $n \in \mathbb{N}$, $n \geq 2$. Spunem că a este *rădăcină multiplă de ordin n* dacă $(X - a)^n \mid f$ și $(X - a)^{n+1} \nmid f$.

Fie K corp comutativ și $f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$, din $K[X]$. Polinomul $f' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \dots + a_1$ se numește *derivata formală de ordinul I a polinomului f* .

Derivata formală de ordinul II a polinomului f este derivata formală de ordinul I a polinomului f' și este notată f'' .

Derivata formală de ordinul k a polinomului f este derivata formală de ordinul I a polinomului $f^{(k-1)}$.

Fie K un corp comutativ și $f \in K[X]$ un polinom de grad $f = n > 0$. Spunem că *polinomul f este reductibil peste K* dacă există polinoamele $g, h \in K[X]$, de grade strict mai mici ca n , cu $f = gh$. În caz contrar, spunem că f este *ireductibil peste K* .

Orice polinom f din $K[X]$, grad $f \geq 1$, se descompune în mod unic în produs de polinoame ireductibile peste K .