

CURS 10: INELE

SAI

1. INELE

Definiția 1. Fie M o mulțime și două legi de compoziție, \triangle și \star , pe M .

Spunem că \star **este distributivă la stânga în raport cu \triangle** dacă pentru orice $a, b, c \in M$ avem $a \star (b \triangle c) = (a \star b) \triangle (a \star c)$.

Spunem că \star **este distributivă la dreapta în raport cu \triangle** dacă pentru orice $a, b, c \in M$ avem $(b \triangle c) \star a = (b \star a) \triangle (c \star a)$.

Spunem că \star **este distributivă în raport cu \triangle** dacă \star este distributivă și la stânga și la dreapta în raport cu \triangle .

Definiția 2. Numim **inel** orice triplet (R, \triangle, \star) format dintr-o mulțime R și două legi de compoziție, \triangle și \star , pe R cu proprietățile:

- (G) (R, \triangle) este grup abelian,
- (S) (R, \star) este semigrup, și
- (D) \star este distributivă în raport cu \triangle .

Definiția 3. Spunem că inelul (R, \triangle, \star) este **comutativ** dacă operația \star este comutativă.

Spunem că inelul (R, \triangle, \star) este **unitar** dacă operația \star admite element neutru.

Exemplul 4. Conform proprietăților cunoscute de la școala generală sau de la liceu, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt inele comutative și unitare. $(\mathbb{N}, +, \cdot)$ nu este inel, deoarece $(\mathbb{N}, +)$ nu este grup!

Observația 5. Ținând cont de faptul că în exemplele „standard” prezentate mai sus rolul operațiilor \triangle și \star este jucat de adunare, respectiv de înmulțire, convenim ca din acest moment să utilizăm în toate inelele cu care vom lucra notația „+” și denumirea de „adunare” pentru „prima lege” și notația „ \cdot ” și denumirea de „înmulțire” pentru „cea de-a doua lege”. Continuând paralela cu legile din exemplul anterior, dat fiind inelul $(R, +, \cdot)$, vom nota cu 0 elementul neutru al lui R în raport cu +, cu $-a$ simetricul elementului $a \in R$ în raport cu +, și cu 1 elementul neutru al lui R în raport cu operația \cdot (dacă acesta există!).

Dacă operațiile de inel sunt subînțelese în context, vom spune uneori „inelul R ” în loc de „inelul $(R, +, \cdot)$ ”.

Exemplul 6. Pentru orice $n \in \mathbb{N}^* \setminus \{1\}$, $(n\mathbb{Z}, +, \cdot)$ este inel comutativ, dar neunitar.

Exemplul 7. Pentru orice $n \in \mathbb{N}$, $(\mathbb{Z}_n, +, \cdot)$ este inel comutativ și unitar (aici $+$ și \cdot desemnează adunarea, respectiv înmulțirea modulo n).

Exemplul 8. Dacă M este o mulțime nevidă, iar R este un inel (comutativ, unitar), mulțimea $\mathcal{F}(M, R)$ a funcțiilor definite pe M cu valori în R are o structură de inel (comutativ, unitar) în raport cu adunarea și înmulțirea definite astfel: $(f + g)(x) = f(x) + g(x)$ pentru orice $x \in M$ și $(fg)(x) = f(x)g(x)$ pentru orice $x \in M$. (Temă: demonstrați această afirmație!)

Exemplul 9. Fie $(G, +)$ un grup abelian arbitrar. Atunci, mulțimea $\text{End}(G)$ a endomorfismelor lui G capătă o structură de inel unitar în raport cu adunarea definită prin $(f + g)(x) = f(x) + g(x)$ pentru orice $x \in G$ și cu compunerea. (Temă: demonstrați această afirmație!)

Exemplul 10. Fie $(G, +)$ un grup abelian arbitrar. Dacă definim pe G o nouă operație prin $xy = 0$ pentru orice $x, y \in G$, atunci $(G, +, \cdot)$ este un inel comutativ. Dacă G are mai mult de un element, acest inel nu admite element unitate. (Temă: demonstrați această afirmație!)

Exemplul 11. Fie $(R, +, \cdot)$ un inel (unitar). Atunci $(R, +, \star)$, unde $x \star y = yx$ pentru orice $x, y \in R$, este un inel (unitar). $(R, +, \star)$ se numește **inelul opus al lui** $(R, +, \cdot)$.

Propoziția 12. (Reguli de calcul în inele):

Fie R un inel. Atunci:

$$i) \quad \forall a \in R \quad a \cdot 0 = 0 \cdot a = 0.$$

$$ii) \quad \forall a, b \in R \quad a(-b) = (-a)b = -ab; \quad (-a)(-b) = ab.$$

$$iii) \quad \forall n \in \mathbb{Z} \quad \forall a, b \in R \quad (na)b = a(nb) = n(ab).$$

$$iv) \quad \forall m, n \in \mathbb{N}^* \quad \forall a_i, b_j \in R \quad \left(\sum_{i=1}^m a_i \right) \left(\sum_{j=1}^n b_j \right) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j.$$

$$v) \quad \forall a, b \in R \quad ab = ba \Rightarrow \forall n \in \mathbb{N}^* \quad (a+b)^n = a^n + \sum_{k=1}^{n-1} \binom{n}{k} a^{n-k} b^k + b^n.$$

$$vi) \quad \forall a, b \in R \quad ab = ba \Rightarrow \forall n \in \mathbb{N}^* \setminus \{1\}$$

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}).$$

2. INEL PRODUS

Exemplul 13. Fie R_1, R_2, \dots, R_n inele. Pe produsul cartezian $R \stackrel{\text{not}}{=} R_1 \times R_2 \times \dots \times R_n$ considerăm operațiile de adunare și înmulțire definite pe componente. În raport cu aceste operații, R capătă o structură de inel. (Temă: demonstrați această afirmație!)

Definiția 14. Inelul din exemplul anterior se numește **produsul direct** al inelelor R_1, R_2, \dots, R_n .

Observația 15. Inelul $R_1 \times R_2 \times \dots \times R_n$ este comutativ dacă și numai dacă R_1, R_2, \dots, R_n sunt comutative.

Inelul $R_1 \times R_2 \times \dots \times R_n$ este unitar dacă și numai dacă R_1, R_2, \dots, R_n sunt unitare; în caz că există, elementul unitate al lui $R_1 \times R_2 \times \dots \times R_n$ este $(1, 1, \dots, 1)$.

(Temă: demonstrați aceste afirmații!)

3. INELE DE MATRICE

Fie R un inel și $m, n \in \mathbb{N}^*$.

Definiția 16. Numim **matrice de tip m, n cu elemente din inelul R** orice funcție definită pe $\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}$ cu valori în R .

Notății:

- Vom nota cu $\mathcal{M}_{m,n}(R)$ mulțimea matricilor de tip m, n cu elemente din R .

- Prin $\mathcal{M}_n(R)$ vom desemna mulțimea $\mathcal{M}_{n,n}(R)$.

- Dacă $A \in \mathcal{M}_{m,n}(R)$, $A(i, j) = a_{ij}$, A este frecvent prezentată sugestiv

$$\text{sub formă de tablou astfel: } A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

- Vom folosi și următoarele variante mai economice de notație: $A = (a_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}}$, sau, dacă nu este pericol de confuzie, $A = (a_{ij})_{i,j}$.

Pe $\mathcal{M}_{m,n}(R)$ definim operația $(a_{ij})_{i,j} + (b_{ij})_{i,j} \stackrel{\text{def}}{=} (a_{ij} + b_{ij})_{i,j}$. Se vede ușor că $\mathcal{M}_{m,n}(R)$ este grup abelian în raport cu această operație. Elementul neutru al acestui grup este matricea nulă de tip m, n , iar simetrica în acest grup a matricii $(a_{ij})_{i,j}$ este matricea $(-a_{ij})_{i,j}$.

Dacă $A = (a_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}} \in \mathcal{M}_{m,n}(R)$ și $B = (b_{jk})_{\substack{j=1,2,\dots,n \\ k=1,2,\dots,p}} \in \mathcal{M}_{n,p}(R)$, definim produsul lor astfel: $AB = \left(\sum_{j=1}^n a_{ij} b_{jk} \right)_{\substack{i=1,2,\dots,m \\ k=1,2,\dots,p}}$. Se constată

că, dacă $m, n, p, q \in \mathbb{N}^*$, $A = (a_{ij})_{i,j} \in \mathcal{M}_{m,n}(R)$, $B = (b_{jk})_{j,k} \in \mathcal{M}_{n,p}(R)$, iar $C = (c_{kl})_{k,l} \in \mathcal{M}_{p,q}(R)$, atunci

$$\begin{aligned} (AB)C &= \left(\left(\sum_{j=1}^n a_{ij} b_{jk} \right)_{\substack{i=1,2,\dots,m \\ k=1,2,\dots,p}} \right) \cdot C = \\ &= \left(\sum_{k=1}^p \left(\sum_{j=1}^n a_{ij} b_{jk} \right) c_{kl} \right)_{\substack{i=1,2,\dots,m \\ l=1,2,\dots,q}} = \left(\sum_{j,k=1}^{n,p} a_{ij} b_{jk} c_{kl} \right)_{\substack{i=1,2,\dots,m \\ l=1,2,\dots,q}} \\ &= \left(\sum_{j=1}^n a_{ij} \left(\sum_{k=1}^p b_{jk} c_{kl} \right) \right)_{\substack{i=1,2,\dots,m \\ l=1,2,\dots,q}} = A \cdot \left(\sum_{k=1}^p b_{jk} c_{kl} \right)_{\substack{j=1,2,\dots,n \\ l=1,2,\dots,q}} = A(BC). \end{aligned}$$

În consecință, $(\mathcal{M}_n(R), \cdot)$ este semigrup.

Cu calcule similare celor de mai sus, se arată că pentru orice $A, B, C \in \mathcal{M}_n(R)$ au loc relațiile $A(B+C) = AB+AC$ și $(B+C)A = BA+CA$.

În urma acestor considerații obținem:

Propoziția 17. Dacă R este un inel, iar $n \in \mathbb{N}^*$, atunci $\mathcal{M}_n(R)$ are o structură de inel în raport cu adunarea și înmulțirea introduse mai sus.

Observația 18. Dacă inelul R este unitar, inelul $\mathcal{M}_n(R)$ este de asemenea unitar, având drept element unitate matricea

$$I_n \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Definiția 19. Matricea I_n definită mai sus se numește **matricea unitate de ordin n** (sau **matricea identică de ordin n**).

4. CARACTERISTICA UNUI INEL

Definiția 20. Prin **caracteristica** inelului unitar R înțelegem numărul natural

$$\text{car } R = \begin{cases} \text{ord}_{(R,+)}(1), & \text{dacă acesta este finit} \\ 0, & \text{altfel} \end{cases}$$

Exemplul 21. Inelele $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt de caracteristică zero.

$\text{car } \mathbb{Z}_n = n$.

$\text{car } \mathbb{Z}_6 \times \mathbb{Z}_8 = 24$.

5. ELEMENTE INTERESANTE DIN INELE

Fie $(R, +, \cdot)$ un inel.

Definiția 22. Spunem că $a \in R$ este **divizor al lui zero la stânga** dacă există $b \in R \setminus \{0\}$ astfel încât $ab = 0$.

Spunem că $a \in R$ este **divizor al lui zero la dreapta** dacă există $b \in R \setminus \{0\}$ astfel încât $ba = 0$.

Spunem că $a \in R$ este **divizor al lui zero** dacă el este divizor al lui zero la stânga și la dreapta.

Observația 23. În orice inel nenul, 0 este divizor al lui zero.

Definiția 24. Inelul $(R, +, \cdot)$ se numește **integr** dacă nu admite divizori ai lui zero nenuli.

Definiția 25. Numim **domeniu de integritate** orice inel comutativ, unitar și integr.

Definiția 26. Spunem că $a \in R$ este **nilpotent** dacă există $n \in \mathbb{N}^*$ astfel încât $a^n = 0$.

Observația 27. În orice inel, 0 este element nilpotent

Notăm de obicei $\mathcal{N}(R) = \{a \in R : a \text{ este nilpotent}\}$. Conform observației anterioare, $0 \in \mathcal{N}(R)$, deci $\mathcal{N}(R) \neq \emptyset$.

Definiția 28. Inelul $(R, +, \cdot)$ se numește **redus** dacă nu are elemente nilpotente nenule.

Definiția 29. Spunem că $a \in R$ este **idempotent** dacă $a^2 = a$.

Fie $(R, +, \cdot)$ un inel unitar.

Definiția 30. Spunem că $a \in R$ este **inversabil la stânga** dacă există $b \in R$ astfel încât $ba = 1$. Orice element b care verifică relația anterioară se numește **invers la stânga** pentru a .

Spunem că $a \in R$ este **inversabil la dreapta** dacă există $b \in R$ astfel încât $ab = 1$. Orice element b care verifică relația anterioară se numește **invers la dreapta** pentru a .

Spunem că $a \in R$ este **inversabil** dacă el este inversabil la stânga și la dreapta.

Observația 31. Dacă elementul a al inelului R este inversabil, atunci el admite un unic invers la stânga și un unic invers la dreapta și, în plus, acestea coincid.

Definiția 32. Dacă elementul a al inelului R este inversabil, unicul element $b \in R$ cu proprietățile $ab = ba = 1$ se numește **inversul lui** a și se notează a^{-1} .

Notăm $U(R) = \{a \in R : a \text{ este inversabil}\}$.

Observația 33. Pentru orice inel unitar R avem $1 \in U(R)$, deci $U(R) \neq \emptyset$.

Observația 34. Pentru orice inel unitar R , $(U(R), \cdot)$ este grup. El se numește **grupul unităților** lui R .

Observația 35. Niciun element inversabil (la stânga, la dreapta) dintr-un inel nenul nu poate fi divizor al lui zero (la stânga, la dreapta) în acel inel.

Propoziția 36. Fie R un inel comutativ și unitar, $u \in R$ un element inversabil, iar $a \in R$ un element nilpotent. Atunci, $u \pm a$ este element inversabil al lui R .

Demonstrație: Fie $n \in \mathbb{N}^*$ cu proprietatea că $a^n = 0$. Atunci, $(u - a) \cdot [u^{-n}(u^{n-1} + u^{n-2}a + \dots + ua^{n-2} + a^{n-1})] = u^{-n}(u^n - a^n) = 1$, deci $u - a \in U(R)$. Cum $-a$ este și el nilpotent, obținem în mod similar și afirmația privitoare la inversabilitatea lui $u + a$. \square

6. SUBINEL. IDEAL

Definiția 37. Fie R un inel. O submulțime nevidă S a lui R se numește **subinel** dacă:

- (i) S este subgrup al lui $(R, +)$;
- (ii) S este parte stabilă a lui R în raport cu înmulțirea: pentru orice $x, y \in S$ avem $xy \in S$.

Dacă R este inel unitar cu unitatea 1_R , spunem că S este **subinel unitar** al lui R dacă, în plus, $1_R \in S$.

Exemplul 38. Dacă R este un inel, atunci R și $\{0\}$ sunt subinele ale lui R .

Exemplul 39. \mathbb{Z} este subinel al lui $(\mathbb{Q}, +, \cdot)$, \mathbb{Q} este subinel al lui $(\mathbb{R}, +, \cdot)$, \mathbb{R} este subinel al lui $(\mathbb{C}, +, \cdot)$. (Temă: demonstrați aceste afirmații!)

Exemplul 40. Dacă R este un inel, atunci

$$C(R) = \{a \in R \mid \forall x \in R, ax = xa\}$$

este subinel al lui R (Temă: demonstrați această afirmație!). $C(R)$ se numește **centrul** inelului R .

Observația 41. Dacă S este subinel al inelului R , atunci S are o structură de inel în raport cu legile induse.

Exemplul 42. (i) $n\mathbb{Z}$ este subinel (neunitar) al inelului \mathbb{Z} .

(ii) Mulțimea matricelor superior triunghiulare este un subinel unitar al unui inel de matrice.

(iii) Mulțimea fracțiilor $\frac{a}{b}$ cu $a, b \in \mathbb{Z}$ și b impar este un subinel unitar al lui \mathbb{Q} .

(iv) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ este subinel unitar al lui \mathbb{C} ; se numește inelul întregilor lui Gauss.

Definiția 43. Fie R un inel. O submulțime nevidă I a lui R se numește ideal stâng (respectiv drept) dacă:

(i) I este subgrup al lui $(R, +)$, adică $\forall x, y \in I$ avem $x - y \in I$;

(ii) $\forall x \in I$ și $r \in R$ avem $rx \in I$ (respectiv $xr \in I$).

Un ideal stâng și drept se numește ideal bilateral.

Exemplul 44. (i) $\{0\}$ și R sunt ideale bilaterale ale lui R ;

(ii) Idealele lui \mathbb{Z} sunt de forma $n\mathbb{Z}$, $n \in \mathbb{N}$, deci coincid cu subgrupurile lui \mathbb{Z} ;

(iii) Pentru orice $x \in R$ avem

• $Rx := \{rx \mid r \in R\}$ ideal stâng al lui R (se numește idealul principal stâng generat de x);

• $xR := \{xr \mid r \in R\}$ ideal drept al lui R (se numește idealul principal drept generat de x);

• $RxR = \left\{ \sum_{i=1}^n r_i x s_i \mid n \in \mathbb{N}^*, r_i, s_i \in R \forall i \right\}$ ideal bilateral al lui R (se numește idealul principal bilateral generat de x).

Dacă R este comutativ, $Rx = xR = RxR$ și se notează și cu (x) ; în acest caz se numește simplu idealul generat de x în R .

Observația 45. (i) Fie R inel unitar, Un ideal stâng (drept sau bilateral) I al lui R coincide cu R dacă și numai dacă I conține un element inversabil.

(ii) Orice ideal este subinel (neunitar dacă idealul este propriu) însă reciproc nu este adevărat: \mathbb{Z} este subinel al lui \mathbb{Q} dar nu este ideal pentru că $\frac{3}{5} \cdot 2 \notin \mathbb{Z}$, deși $\frac{3}{5} \in \mathbb{Q}$ și $2 \in \mathbb{Z}$.

BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] I. D. Ion, N. Radu, *Algebra*, Ed. Universității din București, 1981.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.