CURSUL 1: INELE

G. MINCU

1. Inele

Definiţia 1. Fie M o mulţime şi două legi de compoziţie, $\triangle$ şi $\star$, 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 şi la stânga şi la dreapta în raport cu $\triangle$.

Definiţia 2. Numim **inel** orice triplet $(R, \triangle, \star)$ format dintr-o mulţime R şi două legi de compoziţie, $\triangle$ şi $\star$, pe R cu proprietăţile:
(G) $(R, \triangle)$ este grup abelian,
(S) $(R, \star)$ este semigrup, şi
(D) $\star$ este distributivă în raport cu $\triangle$.

Definiţia 3. Spunem că inelul $(R, \triangle, \star)$ este **comutativ** dacă operaţia $\star$ este comutativă.
Spunem că inelul $(R, \triangle, \star)$ este **unitar** dacă operaţia $\star$ admite element neutru.

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

Observaţia 5. Ţinând cont de faptul că în exemplele ,,standard" prezentate mai sus rolul operaţiilor $\triangle$ şi $\star$ este jucat de adunare, respectiv de înmulţire, convenim ca din acest moment să utilizăm în toate inelele cu care vom lucra notaţia ,,+" şi denumirea de ,,adunare" pentru ,,prima lege" şi notaţia ,,·" şi denumirea de ,,înmulţire" 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 $+$, şi cu 1 elementul neutru al lui R în raport cu operaţia $\cdot$ (dacă acesta există!).

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

Propoziţia 6. (Reguli de calcul în inele):
Fie R un inel. Atunci:
i) $\forall a \in R \quad a \cdot 0 = 0 \cdot a = 0.$
ii) $\forall a, b \in R \quad a(-b) = (-a)b = -ab;\ (-a)(-b) = ab.$
iii) $\forall n \in \mathbb{Z}\ \forall a, b \in R \quad (na)b = a(nb) = n(ab).$
iv) $\forall m, n \in \mathbb{N}^*\ \forall a_i, b_j \in R \quad \left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j.$
v) $\forall a, b \in R \quad ab = ba \Rightarrow \forall n \in \mathbb{N}^* \quad (a+b)^n = a^n + \sum_{k=1}^{n-1}\binom{n}{k} a^{n-k}b^k + b^n.$
vi) $\forall a, b \in R \quad ab = ba \Rightarrow \forall n \in \mathbb{N}^* \setminus \{1\}$

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

Definiţia 7. Fie R un inel, iar S o submulţime nevidă a lui R. Spunem că S este **subinel** al lui R dacă sunt îndeplinite condiţiile:
i) $\forall x, y \in S \quad x - y \in S$ şi
ii) $\forall x, y \in S \quad xy \in S.$

Exemplul 8. Dacă R este un inel, atunci R şi $\{0\}$ sunt subinele ale lui R.

Exemplul 9. $\mathbb{Z}$ 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: demonstraţi aceste afirmaţii!)

Exemplul 10. Dacă R este un inel, atunci $C(R) \overset{\text{not}}{=} \{a \in R : \forall x \in R\ ax = xa\}$ este subinel al lui R (Temă: demonstraţi această afirmaţie!). $C(R)$ se numeşte **centrul** inelului R.

Observaţia 11. Dacă S este subinel al inelului R, atunci S are o structură de inel în raport cu legile induse.

Exemplul 12. Pentru orice $n \in \mathbb{N}^* \setminus \{1\}$, $(n\mathbb{Z}, +, \cdot)$ este inel comutativ, dar neunitar.

Exemplul 13. Pentru orice $n \in \mathbb{N}$, $(\mathbb{Z}_n, +, \cdot)$ este inel comutativ şi unitar (aici $+$ şi $\cdot$ desemnează adunarea, respectiv înmulţirea modulo n).

Exemplul 14. Dacă M este o mulţime nevidă, iar R este un inel (comutativ, unitar), mulţimea $\mathcal{F}(M, R)$ a funcţiilor definite pe M cu valori în R are o structură de inel (comutativ, unitar) în raport cu adunarea şi înmulţirea definite astfel: $(f+g)(x) = f(x)+g(x)$ pentru orice $x \in M$ şi $(fg)(x) = f(x)g(x)$ pentru orice $x \in M$. (Temă: demonstraţi această afirmaţie!)

Exemplul 15. Fie $(G,+)$ un grup abelian arbitrar. Atunci, mulţimea $\text{End}(G)$ 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 $x \in G$ şi cu compunerea. (Temă: demonstraţi această afirmaţie!)

Exemplul 16. Fie $(G,+)$ un grup abelian arbitrar. Dacă definim pe G o nouă operaţie 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: demonstraţi această afirmaţie!)

Exemplul 17. 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 numeşte **inelul opus al lui** $(R,+,\cdot)$.

2. Inel produs

Exemplul 18. Fie $R_1, R_2, \ldots, R_n$ inele. Pe produsul cartezian $R \stackrel{\text{not}}{=} R_1 \times R_2 \times \ldots \times R_n$ considerăm operaţiile de adunare şi înmulţire definite pe componente. În raport cu aceste operaţii, R capătă o structură de inel. (Temă: demonstraţi această afirmaţie!)

Definiţia 19. Inelul din exemplul anterior se numeşte **produsul direct** al inelelor $R_1, R_2, \ldots, R_n$.

Observaţia 20. Inelul $R_1 \times R_2 \times \ldots \times R_n$ este comutativ dacă şi numai dacă $R_1, R_2, \ldots, R_n$ sunt comutative.
Inelul $R_1 \times R_2 \times \ldots \times R_n$ este unitar dacă şi numai dacă $R_1, R_2, \ldots, R_n$ sunt unitare; în caz că există, elementul unitate al lui $R_1 \times R_2 \times \ldots \times R_n$ este $(1, 1, \ldots, 1)$.
(Temă: demonstraţi aceste afirmaţii!)

3. Inele de matrice

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

Definiţia 21. Numim **matrice de tip** m, n **cu elemente din inelul** R orice funcţie definită pe $\{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\}$ cu valori în R.

Notaţii:
- Vom nota cu $\mathcal{M}_{m,n}(R)$ mulţimea matricilor de tip m, n cu elemente din R.
- Prin $\mathcal{M}_n(R)$ vom desemna mulţimea $\mathcal{M}_{n,n}(R)$.
- Dacă $A \in \mathcal{M}_{m,n}(R)$, $A(i,j) = a_{ij}$, A este frecvent prezentată sugestiv

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 şi următoarele variante mai economicoase de notaţie: $A = (a_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}}$, sau, dacă nu este pericol de confuzie, $A = (a_{ij})_{i,j}$.

Pe $\mathcal{M}_{m,n}(R)$ definim operaţia $(a_{ij})_{i,j} + (b_{ij})_{i,j} \stackrel{\text{def}}{=} (a_{ij} + b_{ij})_{i,j}$. Se vede uşor că $\mathcal{M}_{m,n}(R)$ este grup abelian în raport cu această operaţie. 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 $A = (a_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}} \in \mathcal{M}_{m,n}(R)$ şi $B = (b_{jk})_{\substack{j=1,2,\dots,n \\ k=1,2,\dots,p}} \in \mathcal{M}_{n,p}(R)$, 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

$$(AB)C = \left(\left(\sum_{j=1}^{n} a_{ij}b_{jk}\right)_{\substack{i=1,2,\dots,m \\ k=1,2,\dots,p}}\right) \cdot C =$$

$$= \left(\sum_{k=1}^{p}\left(\sum_{j=1}^{n} a_{ij}b_{jk}\right) c_{kl}\right)_{\substack{i=1,2,\dots,m \\ l=1,2,\dots,q}} = \left(\sum_{j,k=1}^{n,p} a_{ij}b_{jk}c_{kl}\right)_{\substack{i=1,2,\dots,m \\ l=1,2,\dots,q}}$$

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

În consecinţă, $(\mathcal{M}_n(R), \cdot)$ este semigrup.
Cu calcule similare celor de mai sus, se arată că pentru orice $A, B, C \in \mathcal{M}_n(R)$ au loc relaţiile $A(B+C) = AB+AC$ şi $(B+C)A = BA+CA$. În urma acestor consideraţii obţinem:

Propoziţia 22. Dacă R este un inel, iar $n \in \mathbb{N}^*$, atunci $\mathcal{M}_n(R)$ are o structură de inel în raport cu adunarea şi înmulţirea introduse mai sus.

Observaţia 23. Dacă inelul R este unitar, inelul $\mathcal{M}_n(R)$ este de asemenea unitar, având drept element unitate matricea

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

Definiţia 24. Matricea I_n definită mai sus se numeşte **matricea unitate de ordin** n (sau **matricea identică de ordin** n).

4. Caracteristica unui inel

Definiţia 25. Prin **caracteristica** inelului unitar R înţelegem numărul natural

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

Exemplul 26. Inelele $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt de caracteristică zero.
car $\mathbb{Z}_n = n$.
car $\mathbb{Z}_6 \times \mathbb{Z}_8 = 24$.

5. Elemente interesante din inele

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

Definiţia 27. 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 şi la dreapta.

Observaţia 28. În orice inel nenul, 0 este divizor al lui zero.

Definiţia 29. Inelul $(R, +, \cdot)$ se numeşte **integru** dacă nu admite divizori ai lui zero nenuli.

Definiţia 30. Numim **domeniu de integritate** orice inel comutativ, unitar şi integru.

Definiţia 31. Spunem că $a \in R$ este **nilpotent** dacă există $n \in \mathbb{N}^*$ astfel încât $a^n = 0$.

Observaţia 32. În orice inel, 0 este element nilpotent

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

Definiţia 33. Inelul $(R, +, \cdot)$ se numeşte **redus** dacă nu are elemente nilpotente nenule.

Definiţia 34. Spunem că $a \in R$ este **idempotent** dacă $a^2 = a$.

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

Definiţia 35. Spunem că $a \in R$ este **inversabil la stânga** dacă există $b \in R$ astfel încât $ba = 1$. Orice element b care verifică relaţia anterioară se numeşte **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 relaţia anterioară se numeşte **invers la dreapta** pentru a
Spunem că $a \in R$ este **inversabil** dacă el este inversabil la stânga şi la dreapta.

Observaţia 36. Dacă elementul a al inelului R este inversabil, atunci el admite un unic invers la stânga şi un unic invers la dreapta şi, în plus, acestea coincid.

Definiţia 37. Dacă elementul a al inelului R este inversabil, unicul element $b \in R$ cu proprietatăţile $ab = ba = 1$ se numeşte **inversul lui** a şi se notează a^{-1}.

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

Observaţia 38. Pentru orice inel unitar R avem $1 \in U(R)$, deci $U(R) \neq \emptyset$.

Observaţia 39. Pentru orice inel unitar R, $(U(R), \cdot)$ este grup. El se numeşte **grupul unităţilor** lui R.

Observaţia 40. 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.

Propoziţia 41. Fie R un inel comutativ şi unitar, $u \in R$ un element inversabil, iar $a \in R$ un element nilpotent. Atunci, $u \pm a$ este element inversabil al lui R.

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

Bibliografie

[1] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.

[2] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.