CURSUL 9: 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) $\forall m,n\in\mathbb{N}^*\ \forall a_i,b_j\in R \quad \left(\sum_{i=1}^m a_i\right)\left(\sum_{j=1}^n b_j\right)=\sum_{i=1}^m\sum_{j=1}^n a_ib_j.$
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 $\mathrm{End}(G)$ 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. Caracteristica unui inel

Definiţia 18. 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 19. Inelele $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sunt de caracteristică zero.
car $\mathbb{Z}_n = n$.
car $\mathbb{Z}_6 \times \mathbb{Z}_8 = 24$.

3. Elemente interesante din inele

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

Definiţia 20. 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 21. În orice inel nenul, 0 este divizor al lui zero.

Definiţia 22. Inelul $(R,+,\cdot)$ se numeşte **integru** dacă nu admite divizori ai lui zero nenuli.

Definiţia 23. Numim **domeniu de integritate** orice inel comutativ, unitar şi integru.

Definiţia 24. Spunem că $a \in R$ este **nilpotent** dacă există $n \in \mathbb{N}^*$ astfel încât $a^n = 0$.

Observaţia 25. 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 26. Inelul $(R, +, \cdot)$ se numeşte **redus** dacă nu are elemente nilpotente nenule.

Definiţia 27. Spunem că $a \in R$ este **idempotent** dacă $a^2 = a$.

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

Definiţia 28. 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 29. 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 30. 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 31. Pentru orice inel unitar R avem $1 \in U(R)$, deci $U(R) \neq \emptyset$.

Observaţia 32. Pentru orice inel unitar R, $(U(R), \cdot)$ este grup. El se numeşte **grupul unităţilor** lui R.

Observaţia 33. 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 34. 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 $u + a$. $\square$

4. MORFISME DE INELE

Definiţia 35. Fie R şi S două inele. Spunem că funcţia $f : R \to S$ este **morfism de inele** dacă sunt îndeplinite condiţiile:
i) $\forall x, y \in R \quad f(x + y) = f(x) + f(y)$ şi
ii) $\forall x, y \in R \quad f(xy) = f(x)f(y)$.

Definiţia 36. Dacă R şi S sunt inele unitare, atunci morfismul de inele $f : R \to S$ se numeşte **unitar** dacă $f(1) = 1$.

Exemplul 37. Dacă R este un inel (unitar), atunci $\mathbf{1}_R : R \to R$, $\mathbf{1}_R(x) = x$ este un morfism (unitar) de inele. El se numeşte **morfismul identic** al lui R.

Exemplul 38. Dacă R şi S sunt inele, atunci $f : R \to S$, $f(x) = 0$ este un morfism de inele. El se numeşte **morfismul nul** de la R la S.

Exemplul 39. Dacă S este subinel al inelului R, atunci $i : S \to R$, $i(x) = x$ este morfism (injectiv) de inele.

Exemplul 40. Pentru orice $n \in \mathbb{N}$, $\pi : \mathbb{Z} \to \mathbb{Z}_n$, $\pi(a) = \widehat{a}$ este morfism unitar de inele.

Exemplul 41. Fie $R_1, R_2, \ldots, R_n$ inele (unitare) şi $R = R_1 \times R_2 \times \ldots \times R_n$ produsul lor direct. Atunci:
- Funcţia $\sigma_i : R_i \to R$, $\sigma_i(a) = (0, 0, \ldots, 0, a, 0, \ldots, 0)$ este morfism de inele (Temă: demonstraţi această afirmaţie!). Acest morfism se numeşte **injecţia canonică** a lui R_i în R.
- Funcţia $\pi_i : R \to R_i$, $\pi_i(a_1, a_2 \ldots, a_n) = a_i$ este morfism (unitar) de inele (Temă: demonstraţi această afirmaţie!). Acest morfism se numeşte **proiecţia canonică** a lui R pe R_i.

Exemplul 42. Dacă R este un inel, iar $n \in \mathbb{N}^*$, atunci $j : R \to \mathcal{M}_n(R)$, $j(a) = \begin{pmatrix} a & 0 & \ldots & 0 \\ 0 & a & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a \end{pmatrix}$ este un morfism injectiv de inele.

Propoziţia 43. Dacă $f : R \to S$ şi $g : S \to T$ sunt morfisme (unitare) de inele, atunci $g \circ f$ este morfism (unitar) de inele.

Definiţia 44. Numim **endomorfism de inele** orice morfism de inele $f : R \to R$.

Definiţia 45. Morfismul de inele $f : R \to S$ se numeşte **izomorfism de inele** dacă:
i) f este funcţie inversabilă şi
ii) f^{-1} este morfism de inele.

Propoziţia 46. Fie R şi S două inele şi o funcţie $f : R \to S$. Atunci, f este izomorfism de inele dacă şi numai dacă f este morfism bijectiv de inele.

Definiţia 47. Inelele R şi S se numesc **izomorfe** dacă există un izomorfism de inele între ele.

Exemplul 48. Fie $m, n \in \mathbb{N}^*$. Atunci, inelele $\mathbb{Z}_m \times \mathbb{Z}_n$ şi $\mathbb{Z}_{mn}$ sunt izomorfe dacă şi numai dacă $(m, n) = 1$.

Demonstraţie: ,,$\Leftarrow$": Definim $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $f(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z})$. Este imediat (temă!) că f este corect definită şi morfism injectiv de inele. Cum însă domeniul şi codomeniul lui f au ambele de cardinal mn, rezultă că f este bijecţie.
,,$\Rightarrow$": Cum caracteristica lui $\mathbb{Z}_{mn}$ este mn, iar cea a lui $\mathbb{Z}_m \times \mathbb{Z}_n$ este $[m, n]$, presupunerea de izomorfism ne conduce la egalitatea $[m, n] = mn = [m, n](m, n)$, de unde $(m, n) = 1$. $\square$

Definiţia 49. Numim **automorfism de inele** orice izomorfism de inele $f : R \to R$.

Exemplul 50. Dacă R este un inel, atunci $\mathbf{1}_R$ este un automorfism de inele.

Notaţii:
Vom nota cu $\mathbf{Hom_{Rng}(R, S)}$ mulţimea morfismelor de inele de la R la S.
Vom nota cu $\mathbf{End_{Rng}(R)}$ mulţimea endomorfismelor de inel ale lui R.
Vom nota cu $\mathbf{Aut_{Rng}(R)}$ mulţimea automorfismelor de inel ale lui R.
Dacă din context se subînţelege că este vorba de morfisme de inele, putem să omitem indicele Rng din notaţiile anterioare.

References

[1] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.
[2] I. D. Ion, N. Radu, *Algebra*, Ed. Universităţii din Bucureşti, 1981.
[3] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.