CURSUL 2: INELE

G. MINCU

1. MORFISME DE INELE

Definiţia 1. 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 2. Dacă R şi S sunt inele unitare, atunci morfismul de inele $f : R \to S$ se numeşte **unitar** dacă $f(1) = 1$.

Exemplul 3. 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 4. 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 5. Dacă S este subinel al inelului R, atunci $i : S \to R$, $i(x) = x$ este morfism (injectiv) de inele.

Exemplul 6. Pentru orice $n \in \mathbb{N}$, $\pi : \mathbb{Z} \to \mathbb{Z}_n$, $\pi(a) = \widehat{a}$ este morfism unitar de inele.

Exemplul 7. 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 8. 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 9. 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 10. Numim **endomorfism de inele** orice morfism de inele $f : R \to R$.

Definiţia 11. 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 12. 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 13. Inelele R şi S se numesc **izomorfe** dacă există un izomorfism de inele între ele.

Exemplul 14. 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 15. Numim **automorfism de inele** orice izomorfism de inele $f : R \to R$.

Exemplul 16. 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.

2. INELE DE POLINOAME

În acest paragraf, R va desemna un inel comutativ şi unitar.
Pe mulţimea $R^{\mathbb{N}}$ a şirurilor $(a_0, a_1, \ldots)$ de elemente din R introducem

operaţiile

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$$
$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (a_0b_0, a_0b_1 + a_1b_0, \ldots, \sum_{i+j=n} a_ib_j, \ldots).$$

$R^{\mathbb{N}}$ are în raport cu aceste operaţii o structură de inel comutativ şi unitar (temă: demonstraţi această afirmaţie!); notând $X = (0, 1, 0, 0, \ldots) \in R^{\mathbb{N}}$, $X^0 = 1$, şi identificând R cu $\phi(R)$, unde ϕ este morfismul injectiv de inele de la R la $R^{\mathbb{N}}$ dat prin $a \mapsto (a, 0, 0, \ldots)$, constatăm că $(a_0, a_1, \ldots) = \sum_{i\geq 0} a_iX^i$. Această construcţie justifică următoarele:

Definiţia 17. Inelul definit mai sus se numeşte **inelul seriilor formale** în nedeterminata X cu coeficienţi în R.

Notaţia standard pentru inelul seriilor formale în nedeterminata X cu coeficienţi în inelul R este $R[[X]]$. Din acest moment, vom folosi şi noi această notaţie.

Definiţia 18. Prin **ordinul** seriei formale nenule $f = \sum_{i\geq 0} a_iX^i \in R[[X]]$ înţelegem cel mai mic număr natural j pentru care $a_j \neq 0$. Convenim că ordinul seriei formale nule este $+\infty$.

Vom nota ordinul seriei formale $f \in R[[X]]$ cu **ord f**.

Propoziţia 19. Dacă $f, g \in R[[X]]$, atunci
a) $\text{ord}(f + g) \geq \min\{\text{ord } f, \text{ ord } g\}$
b) $\text{ord}(fg) \geq \text{ord } f + \text{ ord } g$.
Dacă, în plus, R este domeniu de integritate, atunci
b') $\text{ord}(fg) = \text{ord } f + \text{ ord } g$.

Observaţia 20. Dacă R este domeniu de integritate, atunci şi $R[[X]]$ este domeniu de integritate.

Propoziţia 21. $U(R[[X]]) = \{a_0 + a_1X + \cdots \in R[[X]] : a_0 \in U(R)\}$.

Demonstraţie: Fie $f = a_0+a_1X+\cdots \in R[[X]]$. Dacă f este inversabilă, atunci există $g = b_0 + b_1X + \cdots \in R[[X]]$ astfel încât $fg = 1$. Rezultă $a_0b_0 = 1$, deci $a_0 \in U(R)$. Reciproc, dacă $a_0 \in U(R)$, punem $b_0 = a_0^{-1}$ şi, presupunând construite $b_0, b_1, \ldots, b_n$, definim $b_{n+1} = -a_0^{-1}(a_1b_n + a_2b_{n-1} + \cdots + a_{n+1}b_0)$. Este clar că $b_0 + b_1X + \ldots$ este inversa lui f. $\square$

Este imediat faptul că submulţimea lui $R[[X]]$ alcătuită din acele serii formale care au un număr finit de coeficienţi nenuli este subinel al lui $R[[X]]$. Conform observaţiei 2 din primul curs, această submulţime are o structură de inel în raport cu legile induse de adunarea şi înmulţirea din $R[[X]]$.

Definiţia 22. Inelul definit mai sus se numeşte **inelul de polinoame** în nedeterminata X cu coeficienţi în R. Elementele acestui inel se numesc **polinoame** în nedeterminata X cu coeficienţi în R.

Notaţia standard pentru inelul polinoamelor în nedeterminata X cu coeficienţi în inelul R este $R[X]$.

Observaţia 23. Orice polinom $f \in R[X] \setminus \{0\}$ se reprezintă în mod unic sub forma $a_0 + a_1X + \cdots + a_nX^n$ cu $a_0, a_1, \ldots, a_n \in R$ şi $a_n \neq 0$. Două polinoame $f = \sum_{i=0}^{m} a_iX^i, g = \sum_{j=0}^{n} b_jX^j \in R[X]$ sunt egale dacă şi numai dacă $a_0 = b_0$, $a_1 = b_1, \ldots, a_{\max\{m,n\}} = b_{\max\{m,n\}}$.

Definiţia 24. Dat fiind polinomul $f = \sum_{i=0}^{n} a_iX^i \in R[X]$ cu $a_n \neq 0$, a_0 se numeşte **termenul liber** al lui f, iar a_n se numeşte **coeficientul dominant** al lui f. Dacă $a_n = 1$, polinomul f se numeşte **monic**. Dacă f nu are alţi coeficienţi nenuli decât (eventual) pe a_0, el se numeşte **constant**.

Definiţia 25. Prin **gradul** polinomului nenul $f = \sum_{i=0}^{n} a_iX^i \in R[X]$ înţelegem numărul natural $\max\{j \in \mathbb{N} | a_j \neq 0\}$. Convenim că gradul polinomului nul este $-\infty$.

Vom nota gradul polinomului $f \in R[X]$ cu grad f.

Propoziţia 26. Dacă $f, g \in R[X]$, atunci
a) $\text{grad}(f + g) \leq \max\{\text{grad } f, \text{grad } g\}$
b) $\text{grad}(fg) \leq \text{grad } f + \text{grad } g$.
Dacă, în plus, R este domeniu de integritate, atunci
b') $\text{grad}(fg) = \text{grad } f + \text{grad } g$.

Propoziţia 27. Fie R un inel comutativ şi unitar şi $f \in R[X]$. Atunci:
i) f este nilpotent dacă şi numai dacă toţi coeficienţii săi sunt nilpotenţi.
ii) f este inversabil dacă şi numai dacă termenul său liber este inversabil, iar toţi ceilalţi coeficienţi ai săi sunt nilpotenţi.
iii) f este idempotent dacă şi numai dacă este element idempotent al lui R.
iv) f este divizor al lui zero dacă şi numai dacă există $a \in R \setminus \{0\}$ astfel încât $af = 0$.

Observaţia 28. Funcţia $j : R \to R[X]$, $j(a) = a$ este morfism unitar de inele. Acest morfism se numeşte **injecţia canonică** a lui R în $R[X]$.

Dacă R este un inel comutativ şi unitar, iar j este injecţia canonică a lui R în $R[X]$, are loc:

Propoziţia 29. (**Proprietatea de universalitate a inelului de polinoame într-o nedetereminată**) Pentru orice inel comutativ unitar S, orice morfism unitar de inele $u : R \to S$ şi orice $s \in S$ există un unic morfism de inele unitare $v : R[X] \to S$ cu proprietăţile $v(X) = s$ şi $v \circ j = u$.

Demonstraţie: Presupunând mai întâi că există un morfism v ca în concluzia propoziţiei, constatăm că, dat fiind $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, condiţiile din enunţ implică $v(f) = u(a_0) + u(a_1)s + \cdots + u(a_n)s^n$, de unde unicitatea lui v. Definind acum v prin formula anterioară, constatăm cu uşurinţă că el este morfism de inele, ceea ce justifică şi afirmaţia de existenţă din enunţ. $\square$

Definiţia 30. Prin **valoarea polinomului** $f = \sum_{i=0}^{n} a_iX^i \in R[X]$ **în elementul** $r \in R$ înţelegem elementul $\sum_{i=0}^{n} a_ir^i \in R$. Vom nota acest element cu $f(r)$.

Definiţia 31. Prin **funcţia polinomială asociată polinomului** $f \in R[X]$ înţelegem funcţia $\widetilde{f} : R \to R$, $\widetilde{f}(x) = f(x)$.

Observaţia 32. La polinoame egale corespund funcţii polinomiale egale. Reciproca nu este numaidecât adevărată.

3. CORPURI

Definiţia 33. Inelul unitar R se numeşte **corp** dacă sunt îndeplinite condiţiile:
i) $1 \neq 0$.
ii) orice element nenul al lui R este inversabil.

Observaţia 34. Orice corp este inel integru.

Exemplul 35. Conform proprietăţilor cunoscute de la şcoala generală sau de la liceu, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt corpuri comutative. $(\mathbb{Z}, +, \cdot)$ nu este corp, deoarece $2 \in \mathbb{Z}$ este nenul şi neinversabil.

Exemplul 36. Întrucât $U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n : (a, n) = 1\}$, deducem că inelul $\mathbb{Z}_n$ este corp dacă şi numai dacă n este număr prim.

Definiţia 37. Fie R un inel. O submulţime nevidă K a lui R se numeşte **subcorp** al lui R dacă K este corp în raport cu operaţiile induse de cele de pe R.

Propoziţia 38. Fie K un corp. O submulţime L a lui K cu cel puţin două elemente este subcorp al lui K dacă şi numai dacă sunt îndeplinite condiţiile:
i) $\forall x, y \in L \quad x - y \in L$ şi
ii) $\forall x, y \in L \setminus \{0\} \quad xy^{-1} \in L$.

Propoziţia 39. Fie K un corp şi L_α, $\alpha \in A$ subcorpuri ale acestuia. Atunci, $P_K = \bigcap\limits_{\alpha \in A} L_\alpha$ este subcorp al lui K.

Definiţia 40. Un corp care nu admite subcorpuri proprii se numeşte **corp prim**.

Observaţia 41. Dat fiind un corp K, subcorpul său P_K este corp prim. El se numeşte **subcorpul prim** al lui K.

Fie K un corp de caracterisită $n \in \mathbb{N}^*$ şi P_K subcorpul său prim. Atunci, $1 \in P_K$, deci $\mathcal{M} = \{1, 1+1, \dots, \underbrace{1+1+\cdots+1}_{n}\} \subset P_K$. Este uşor de văzut că

$$(\underbrace{1+1+\cdots+1}_{u}) - (\underbrace{1+1+\cdots+1}_{v}) = \underbrace{1+1+\cdots+1}_{u-v \pmod n} \quad \text{şi}$$

$$(\underbrace{1+1+\cdots+1}_{u})(\underbrace{1+1+\cdots+1}_{v}) = \underbrace{1+1+\cdots+1}_{uv \pmod n}.$$

De aici deducem că $\varphi : \mathbb{Z}_n \to P_K$, $\varphi(\widehat{a}) = \underbrace{1+1+\cdots+1}_{a}$ este morfism de inele. Surjectivitatea acestuia fiind evidentă, din $|\mathbb{Z}_n| = |P_K|$ obţinem şi injectivitatea. Aşadar, inelele $\mathbb{Z}_n$ şi P_K sunt izomorfe. Rezultă că $\mathbb{Z}_n$ este inel integru, de unde deducem că n este număr prim. Am obţinut prin urmare:

Propoziţia 42. Caracteristica unui corp este fie zero, fie număr prim.

Propoziţia 43. Dacă K este un corp de caracteristică $p > 0$, atunci subcorpul său prim este izomorf cu $\mathbb{Z}_p$.

Procedând în mod similar, obţinem:

Propoziţia 44. Dacă K este un corp de caracteristică zero, atunci subcorpul său prim este izomorf cu $\mathbb{Q}$.

Din cele de mai sus rezultă şi:

Propoziţia 45. Singurul tip de corp prim de caracteristică p este $\mathbb{Z}_p$. Singurul tip de corp prim de caracteristică zero este $\mathbb{Q}$.

Exemplul 46. Considerăm submulţimea $\mathcal{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$ a lui $\mathcal{M}_2(\mathbb{C})$. Se constată că $\mathcal{H}$ este o parte stabilă a lui $\mathcal{M}_2(\mathbb{C})$ în raport cu adunarea şi cu înmulţirea matricilor. În raport cu legile induse, $\mathcal{H}$ are o structură de corp.

Definiţia 47. Corpul (necomutativ!) din exemplul anterior se numeşte **corpul cuaternionilor**. El se notează de obicei cu $\mathbb{H}$.

Exemplul 48. Fie R un domeniu de integritate. Pe $R \times (R \setminus \{0\})$ introducem relaţia $\sim$ astfel: $(a,s) \sim (b,t)$ dacă şi numai dacă $at = bs$. Se constată că această relaţie este de echivalenţă.
Notăm cu $\dfrac{a}{s}$ clasa elementului $(a,s) \in R \times (R \setminus \{0\})$ în raport cu relaţia $\sim$ şi cu M mulţimea factor $R \times (R \setminus \{0\})/\sim$.
Pe M introducem operaţiile $\dfrac{a}{s} + \dfrac{b}{t} = \dfrac{at+bs}{st}$ şi $\dfrac{a}{s} \cdot \dfrac{b}{t} = \dfrac{ab}{st}$.
Este uşor de văzut că aceste operaţii sunt corect definite şi că $(M, +, \cdot)$ este un corp comutativ.

Definiţia 49. Corpul construit în exemplul anterior se numeşte **corpul de fracţii al domeniului** R. O notaţie frecvent folosită pentru acest corp este $Q(R)$.

Exemplul 50. Corpul de fracţii al lui $\mathbb{Z}$ este $\mathbb{Q}$.

Definiţia 51. Dacă K este corp comutativ, corpul de fracţii al lui $K[X]$ se numeşte **corpul de fracţii raţionale în nedeterminata** X **cu coeficienţi în** K şi se notează $\mathbf{K}(\mathbf{X})$.

Observaţia 52. $K(X) = \left\{ \dfrac{f}{g} : f, g \in K[X],\ g \neq 0 \right\}$.

Observaţia 53. Dat fiind un domeniu de integritate R, funcţia $j_R : R \to Q(R)$, $j_R(a) = \dfrac{a}{1}$ este un morfism injectiv şi unitar de inele.

Propoziţia 54. (**Proprietatea de universalitate a corpului de fracţii al unui domeniu de integritate**) Fie R un domeniu de integritate. Pentru orice inel unitar S şi orice morfism unitar de inele $u : R \to S$ cu proprietatea că $\operatorname{Im} u \setminus \{0\} \subset U(S)$ există un unic morfism de inele unitare $v : Q(R) \to S$ cu proprietatea $v \circ j_R = u$.

Demonstraţie: Presupunând mai întâi că există un morfism v ca în concluzia propoziţiei, constatăm că, dat fiind $x = \dfrac{a}{s} \in Q(R)$, condiţiile din enunţ implică $v(f) = u(a)u(s)^{-1}$, de unde unicitatea lui v. Definind acum v prin formula anterioară, constatăm cu uşurinţă că el este corect definit şi morfism unitar de inele, ceea ce justifică şi afirmaţia de existenţă din enunţ. $\square$

Definiţia 55. Fie K şi L două corpuri. Funcţia $f : K \to L$ se numeşte **morfism de corpuri** dacă este morfism unitar de inele.

Exemplul 56. $i_1 : \mathbb{Q} \to \mathbb{R}$, $i_1(x) = x$, $i_2 : \mathbb{Q} \to \mathbb{C}$, $i_2(x) = x$, $i_3 : \mathbb{R} \to \mathbb{C}$, $i_3(x) = x$ şi $i_4 : \mathbb{Q} \to \mathbb{Q}(\sqrt{2})$, $i_4(x) = x$ sunt câteva exemple imediate de morfisme de corpuri.

Exemplul 57. Pentru orice corp K, $\mathbf{1}_K$ este automorfism de corpuri.

Exemplul 58. $\alpha : \mathbb{R} \to \mathbb{H}$, $\alpha(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ este un morfism de corpuri.

Observaţia 59. Fie K un corp comutativ de caracteristică $p > 0$. Pentru orice $x \in K$ are loc relaţia

$$px = \underbrace{x + x + \cdots + x}_{p} = x(\underbrace{1 + 1 + \cdots + 1}_{p}) = 0.$$

Mulţumită comutativităţii, pentru orice $x, y \in K$ are loc

$$(xy)^p = x^p y^p.$$

Numărul p fiind prim, avem $p \mid \binom{p}{k}$ pentru orice $k \in \{1, 2, \ldots, p-1\}$. Prin urmare, pentru orice $x, y \in K$ are loc relaţia

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = x^p + y^p.$$

Drept consecinţă a acestei observaţii, obţinem

Exemplul 60. Fie K un corp comutativ de caracteristică $p > 0$. Atunci, $\varphi : K \to K$, $\varphi(x) = x^p$ este un endomorfism de corpuri.

Definiţia 61. Endomorfismul din exemplul anterior se numeşte **endomorfismul lui Frobenius**.

Se constată cu uşurinţă că toate morfismele din exemplele prezentate sunt injective (temă!). Aceasta este consecinţa unui fapt mai general, şi anume:

Propoziţia 62. Orice morfism de corpuri este injectiv.

(Temă: demonstraţi această propoziţie!)

Încheiem cu enunţul unui rezultat foarte interesant, pentru a cărui demonstraţie cititorul interesat este invitat să consulte, de pildă, [2]:

Teorema lui Wedderburn. Orice corp finit este comutativ.

Bibliografie

[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.