CURSUL 12: INELE

G. MINCU

1. Morfisme de inele

Definiția 1. Fie R și S două inele. Spunem că funcția $f: R \to S$ este **morfism de inele** dacă sunt îndeplinite condițiile:

- i) $\forall x, y \in R$ f(x+y) = f(x) + f(y) şi
- ii) $\forall x, y \in R$ f(xy) = f(x)f(y).

Definiția 2. Dacă R și S sunt inele unitare, atunci morfismul de inele $f: R \to S$ se numește **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 numește **morfismul identic** al lui R.

Exemplul 4. Dacă R și S sunt inele, atunci $f: R \to S$, f(x) = 0 este un morfism de inele. El se numește **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 $n \in \mathbb{N}$, $\pi : \mathbb{Z} \to \mathbb{Z}_n$, $\pi(a) = \hat{a}$ este morfism unitar de inele.

Exemplul 7. Fie R_1, R_2, \ldots, R_n inele (unitare) și $R = R_1 \times R_2 \times \ldots \times R_n$ produsul lor direct. Atunci:

- Funcţia $\sigma_i: R_i \to R$, $\sigma_i(a) = (0, 0, \dots, 0, a, 0, \dots, 0)$ este morfism de inele (Temă: demonstraţi această afirmaţie!). Acest morfism se numeşte **injecţia canonică** a lui R_i în R.
- Funcţia $\pi_i: R \to R_i, \ \pi_i(a_1, a_2 \dots, a_n) = a_i$ 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 $j : R \to \mathcal{M}_n(R)$,

$$j(a) = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a \end{pmatrix} \text{ este un morfism injectiv de inele.}$$

Propoziția 9. Dacă $f: R \to S$ și $g: S \to T$ sunt morfisme (unitare) de inele, atunci $g \circ f$ este morfism (unitar) de inele.

Definiția 10. Numim **endomorfism de inele** orice morfism de inele $f: R \to R$.

Definiția 11. Morfismul de inele $f:R\to S$ se numește **izomorfism** de inele dacă:

- i) f este funcție inversabilă și
- ii) f^{-1} este morfism de inele.

Propoziția 12. Fie R și S două inele și o funcție $f: R \to S$. Atunci, f este izomorfism de inele dacă și numai dacă f este morfism bijectiv de inele.

Definiția 13. Inelele R și 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.

Demonstrație: " \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 bijecție.

,, \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, de unde (m, n) = 1. \square

Definiția 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.

Notații:

Vom nota cu $\mathbf{Hom_{Rng}}(\mathbf{R},\mathbf{S})$ mulțimea morfismelor de inele de la R la S

Vom nota cu $\mathbf{End_{Rng}}(\mathbf{R})$ mulţimea endomorfismelor de inel ale lui R. Vom nota cu $\mathbf{Aut_{Rng}}(\mathbf{R})$ 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 operațiile

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$$

 $(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (a_0 b_0, a_0 b_1 + a_1 b_0, \ldots, \sum_{i+j=n} a_i b_j, \ldots).$

 $R^{\mathbb{N}}$ are în raport cu aceste operații o structură de inel comutativ și unitar (temă: demonstrați această afirmație!); notând $X=(0,1,0,0,\ldots)\in R^{\mathbb{N}},\ X^0=1,$ și 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 $(a_0,a_1,\ldots)=\sum_{i>0}a_iX^i.$ Această construcție justifică următoarele:

Definiția 17. Inclul definit mai sus se numește inclul seriilor formale în nedeterminata X cu coeficienți în R.

Notația standard pentru inelul seriilor formale în nedeterminata X cu coeficienți în inelul R este R[[X]]. Din acest moment, vom folosi și noi această notație.

Definiția 18. Prin **ordinul** seriei formale nenule $f = \sum_{i \geq 0} a_i X^i \in R[[X]]$ înțelegem 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.

Propoziția 19. Dacă $f, g \in R[[X]]$, atunci

- a) $\operatorname{ord}(f+g) \ge \min\{\operatorname{ord} f, \operatorname{ord} g\}$
- b) $\operatorname{ord}(fg) \ge \operatorname{ord} f + \operatorname{ord} g$.

Dacă, în plus, R este domeniu de integritate, atunci

b') $\operatorname{ord}(fg) = \operatorname{ord} f + \operatorname{ord} g$.

Observația 20. Dacă R este domeniu de integritate, atunci și R[[X]] este domeniu de integritate.

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

Demonstrație: 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 $b_0=a_0^{-1}$ și, 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 submulțimea lui R[[X]] alcătuită din acele serii formale care au un număr finit de coeficienți nenuli este subinel al lui R[[X]]. Conform observației 2 din primul curs, această submulțime are o structură de inel în raport cu legile induse de adunarea și înmulțirea din R[[X]].

4

Definiția 22. Inelul definit mai sus se numește **inelul de polinoame** în nedeterminata X cu coeficienți în R. Elementele acestui inel se numesc **polinoame** în nedeterminata X cu coeficienți în R.

Notația standard pentru inelul polinoamelor în nedeterminata X cu coeficienți în inelul R este R[X].

Observația 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 $a_0, a_1, \ldots, a_n \in R$ și $a_n \neq 0$. Două polinoame $f = \sum_{i=0}^m a_iX^i, g = \sum_{j=0}^n b_jX^j \in R[X]$ sunt egale dacă și numai dacă $a_0 = b_0, \ a_1 = b_1, \ldots, a_{\max\{m,n\}} = b_{\max\{m,n\}}$.

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

Definiția 25. Prin **gradul** polinomului nenul $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ înțelegem 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.

Propoziția 26. Dacă $f, g \in R[X]$, atunci

- a) $grad(f + g) \le max\{grad f, grad g\}$
- b) $\operatorname{grad}(fg) \leq \operatorname{grad} f + \operatorname{grad} g$.

Dacă, în plus, R este domeniu de integritate, atunci

b') $\operatorname{grad}(fg) = \operatorname{grad} f + \operatorname{grad} g$.

Propoziția 27. Fie R un inel comutativ și unitar și $f \in R[X]$. Atunci: i) f este nilpotent dacă și numai dacă toți coeficienții săi sunt nilpotenți. ii) f este inversabil dacă și numai dacă termenul său liber este inversabil, iar toți ceilalți coeficienți ai săi sunt nilpotenți.

- iii) f este idempotent dacă și numai dacă este element idempotent al lui R.
- iv) f este divizor al lui zero dacă și numai dacă există $a \in R \setminus \{0\}$ astfel încât af = 0.

Observația 28. Funcția $j: R \to R[X]$, j(a) = a este morfism unitar de inele. Acest morfism se numește **injecția canonică** a lui R în R[X].

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

Propoziția 29. (Proprietatea de universalitate a inelului de polinoame într-o nedetereminată) Pentru orice inel comutativ unitar S, orice morfism unitar de inele $u: R \to S$ și orice $s \in S$ există un

unic morfism de inele unitare $v:R[X]\to S$ cu proprietățile v(X)=s și $v\circ j=u$.

Demonstrație: Presupunând mai întâi că există un morfism v ca în concluzia propoziției, constatăm că, dat fiind $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, condițiile din enunț 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 uşurință că el este morfism de inele, ceea ce justifică și afirmația de existență din enunț. \square

Definiția 30. Prin valoarea polinomului $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ în elementul $r \in R$ înțelegem elementul $\sum_{i=0}^{n} a_i r^i \in R$. Vom nota acest element cu f(r).

Definiția 31. Prin funcția polinomială asociată polinomului $f \in R[X]$ înțelegem funcția $\widetilde{f} : R \to R$, $\widetilde{f}(x) = f(x)$.

Observația 32. La polinoame egale corespund funcții polinomiale egale. Reciproca nu este numaidecât adevărată.

3. Corpuri

Definiția 33. Inelul unitar R se numește **corp** dacă sunt îndeplinite condițiile:

- i) $1 \neq 0$.
- ii) orice element nenul al lui R este inversabil.

Observația 34. Orice corp este inel integru.

Exemplul 35. Conform proprietăților cunoscute de la școala 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 și 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 și numai dacă n este număr prim.

Definiția 37. Fie R un inel. O submulțime nevidă K a lui R se numește **subcorp** al lui R dacă K este corp în raport cu operațiile induse de cele de pe R.

Propoziția 38. Fie K un corp. O submulțime L a lui K cu cel puțin două elemente este subcorp al lui K dacă și numai dacă sunt îndeplinite condițiile:

- i) $\forall x, y \in L \quad x y \in L$ şi
- ii) $\forall x, y \in L \setminus \{0\}$ $xy^{-1} \in L$.

Propoziția 39. Fie K un corp și L_{α} , $\alpha \in A$ subcorpuri ale acestuia. Atunci, $P_K = \bigcap_{\alpha \in A} L_{\alpha}$ este subcorp al lui K.

Definiția 40. Un corp care nu admite subcorpuri proprii se numește corp prim.

Observația 41. Dat fiind un corp K, subcorpul său P_K este corp prim. El se numește **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 $\mathcal{M} = \{1, 1+1, \ldots, \underbrace{1+1+\cdots+1}_n\} \subset P_K$. Este

ușor 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 mor-

fism de inele. Surjectivitatea acestuia fiind evidentă, din $|\mathbb{Z}_n| = |P_K|$ obținem și injectivitatea. Așadar, inelele \mathbb{Z}_n și P_K sunt izomorfe. Rezultă că \mathbb{Z}_n este inel integru, de unde deducem că n este număr prim. Am obținut prin urmare:

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

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

Procedând în mod similar, obținem:

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

Din cele de mai sus rezultă și:

Propoziția 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 submulțimea $\mathcal{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$ 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 și cu înmulțirea matricilor. În raport cu legile induse, \mathcal{H} are o structură de corp.

Definiția 47. Corpul (necomutativ!) din exemplul anterior se numește **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 relația \sim astfel: $(a,s)\sim(b,t)$ dacă și numai dacă at=bs. Se constată că această relație este de echivalență.

Notăm cu $\stackrel{a}{-}$ clasa elementului $(a,s)\in R\times (R\setminus\{0\})$ în raport cu relația

 \sim și cu M mulțimea factor $R\times (R\setminus\{0\})/\sim$. Pe M introducem operațiile $\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}$ și $\frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}.$ Este ușor de văzut că aceste operații sunt corect definite și că $(M,+,\cdot)$

este un corp comutativ.

Definiția 49. Corpul construit în exemplul anterior se numește corpul de fracții al domeniului R. O notație frecvent folosită pentru acest corp este Q(R).

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

Definiția 51. Dacă K este corp comutativ, corpul de fracții al lui K[X] se numește corpul de fracții raționale în nedeterminata X cu coeficienți în K și se notează K(X).

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

Observația 53. Dat fiind un domeniu de integritate R, funcția $j_R: R \to Q(R), j_R(a) = \frac{a}{1}$ este un morfism injectiv și unitar de inele.

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

Demonstrație: Presupunând mai întâi că există un morfism v ca în concluzia propoziției, constatăm că, dat fiind $x = \frac{a}{s} \in Q(R)$, condițiile din enunt implică $v(f) = u(a)u(s)^{-1}$, de unde unicitatea lui v. Definind acum v prin formula anterioară, constatăm cu uşurință că el este corect definit și morfism unitar de inele, ceea ce justifică și afirmația de existență din enunț.

Definiția 55. Fie K și L două corpuri. Funcția $f: K \to L$ se numește morfism de corpuri dacă este morfism unitar de inele.

Exemplul 56. $i_1: \mathbb{Q} \to \mathbb{R}, i_1(x) = x, i_2: \mathbb{Q} \to \mathbb{C}, i_2(x) = x,$ $i_3: \mathbb{R} \to \mathbb{C}, \ i_3(x) = x$ și $i_4: \mathbb{Q} \to \mathbb{Q}(\sqrt{2}), \ i_4(x) = x$ 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.

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

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

Multumită comutativității, 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 relația

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

Drept consecință a acestei observații, obținem

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.

Definiția 61. Endomorfismul din exemplul anterior se numește endomorfismul lui Frobenius.

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

Propoziția 62. Orice morfism de corpuri este injectiv.

(Temă: demonstrați această propoziție!)

Încheiem cu enunțul unui rezultat foarte interesant, pentru a cărui demonstrație cititorul interesat este invitat să consulte, de pildă, [?]:

Teorema lui Wedderburn. Orice corp finit este comutativ.

Bibliografie

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