CURS 11: MORFISME DE INELE

SAI

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:
$\mathbf{Hom_{Rng}(R, S)}$ este mulţimea morfismelor de inele de la R la S.
$\mathbf{End_{Rng}(R)}$ este mulţimea endomorfismelor de inel ale lui R.
$\mathbf{Aut_{Rng}(R)}$ este 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.

Theorem 17. *(Teorema de corespondenţă pentru subinele şi ideale.) Fie $f : R \to S$ un morfism de inele. Atunci:*

(i) Dacă A este un subinel al lui R atunci $f(A)$ este subinel al lui S. În particular, $\mathrm{Im}(f) := f(R)$ *este subinel al lui S;*

(ii) Dacă B este subinel al lui S atunci $f^{-1}(B)$ este subinel al lui R;

(iii) Dacă J este ideal stâng (respectiv drept, bilateral) al lui S atunci $f^{-1}(J)$ este ideal stâng (respectiv drept, bilateral) al lui R. În particular $\mathrm{Ker}(f) := f^{-1}(\{0\})$ *este ideal bilateral al lui R;*

(iv) Dacă f este surjectiv atunci $\forall I$ ideal stâng (respectiv drept, bilateral) al lui R avem că $f(I)$ este ideal stâng (respectiv drept, bilateral) al lui S. Mai mult, dacă f este surjectiv atunci există o corespondnţă bijectivă între mulţimea idealelor stângi (respectiv drepte, bilaterale) ale lui R ce conţin pe $\mathrm{Ker}(f)$ *şi mulţimea idealelor stângi (respectiv drepte, bilaterale) ale lui S.*

Demonstraţie: Similară cu cea de la grupuri.

2. Inel factor, teorema fundamentală de izomorfism pentru inele

Fie R un inel şi I un ideal bilateral al său. În particular, I este subgrup al grupului abelian $(R, +)$ şi, deci, are sens să considerăm grupul factor $(\frac{R}{I}, +)$. Operaţia $\cdot$ de pe R induce operaţia pe $\frac{R}{I}$: $\hat{a} \cdot \hat{b} = \widehat{ab}$, $\forall\ a, b \in R$. Aceasta este bine definită deoarece: $\hat{a} = \hat{a'}$ şi $\hat{b} = \hat{b'}$ implică $a = a' + x$ şi $b = b' + y$, pentru anumite elemente $x, y \in I$. Rezultă că

$$ab - a'b' = \underbrace{a'y}_{\in I} + \underbrace{xb'}_{\in I} + \underbrace{xy}_{\in I} \in I \ \Leftrightarrow\ \widehat{ab} = \widehat{a'b'}.$$

Theorem 18. *Fie R inel şi I un ideal bilateral al său. Atunci grupul factor $(\frac{R}{I}, +)$ împreună cu $\cdot$ definită mai sus admite o structură de inel, numit inel factor al lui R prin I. În plus,*

(i) $p : R \to \frac{R}{I}$ definit de $p(a) = \hat{a}$ $\forall a \in R$ este morfism surjectiv de inele (numit surjecţia canonică);

(ii) $\frac{R}{I}$ este unitar (respectiv comutativ) dacă R este unitar (respectiv comutativ);

(iii) Proprietatea de universalitate a inelului factor: pentru orice morfism $f : R \to S$ de inele există un unic morfism de inele $\overline{f} : \frac{R}{I} \to S$ astfel încât $\overline{f} \circ p = f$ dacă şi numai dacă $I \subset \mathrm{Ker}(f)$. Dacă există $\overline{f}$ ca mai sus atunci:

- *$\overline{f}$ este injectiv $\Leftrightarrow I = \mathrm{Ker}(f)$;*
- *$\overline{f}$ este surjectiv $\Leftrightarrow f$ este surjectiv;*
- *$\overline{f}$ este bijectiv $\Leftrightarrow f$ este surjectiv şi $I = \mathrm{Ker}(f)$.*

Demonstraţie: Este imediată. De notat că (iii) rezultă în mare parte din proprietatea de universalitate a grupului factor; pentru (iii): $\overline{f}(\hat{a}) = f(a)$, $\forall \hat{a} \in \frac{R}{I}$.

Theorem 19. *(Teorema fundamentală de izomorfism pentru inele.) Fie $f : R \to S$ un morfism de inele. Atunci*

(i) $\mathrm{Ker}(f)$ *este ideal bilateral al lui R iar* $\mathrm{Im}(f)$ *este subinel al lui S.*

(ii) $F : \frac{R}{\mathrm{Ker}(f)} \to \mathrm{Im}(f)$ dat de $F(\hat{a}) = f(a)$ $\forall\ \hat{a} \in \frac{R}{\mathrm{Ker}(f)}$ este bine definit şi un izomorfism de inele.

Demonstraţie: Partea (i) a fost demonstrată mai sus.

(ii) Ştim de la grupuri că F este bine definit şi un izomorfism de grupuri. Este un izomorfism de inele fiindcă $F(\hat{a}\cdot\hat{b}) = F(\widehat{ab}) = f(ab) = f(a)f(b) = F(\widehat{a})F(\hat{b})$ $\forall\ \hat{a}, \hat{b}$. Dacă f este morfism unitar (de inele unitare), $F(\hat{1}) = f(1) = 1$ şi, deci, F este un izomorfism de inele unitare.

Exemplul 20. *Fie $f : \mathbb{Z}[i] \to \mathbb{Z}_2$ dat de $f(a + bi) = \overline{a + b}$ pentru orice $a, b \in \mathbb{Z}$. Atunci f este morfism surjectiv de inele unitare cu* $\mathrm{Ker}(f) = (1 + i)\mathbb{Z}[i] = \{a + bi \mid a \equiv b \pmod 2\}$. *Prin urmare, $F : \frac{\mathbb{Z}[i]}{(1+i)\mathbb{Z}[i]} \to \mathbb{Z}_2$ dat de $F(\widehat{a + bi}) = \overline{a + b}$, pentru orice $a, b \in \mathbb{Z}$, este bine definit şi un izomorfism de inele.*

3. 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 $(a_0, a_1, \ldots) = \sum\limits_{i\geq 0} a_iX^i$. Această construcţie justifică următoarele:

Definiţia 21. 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 22. 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 23. 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 24. Dacă R este domeniu de integritate, atunci şi $R[[X]]$ este domeniu de integritate.

Propoziţia 25. $U(R[[X]]) = \{a_0 + a_1X + \cdots \in R[[X]] : a_0 \in U(R)\}$.

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.
□

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 $R[[X]]$. Această submulţime are o structură de inel în raport cu legile induse de adunarea şi înmulţirea din $R[[X]]$.

Definiţia 26. 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 27. 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 28. 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 29. 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 30. Dacă $f, g \in R[X]$, atunci
a) $\text{grad}(f+g) \leq \max\{\text{grad } f, \text{ grad } g\}$
b) $\text{grad}(fg) \leq \text{grad } f +$ grad g.
Dacă, în plus, R este domeniu de integritate, atunci
b') $\text{grad}(fg) = \text{grad } f +$ grad g.

Propoziţia 31. 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 32. 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 33. (**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 34. 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 35. Prin **funcţia polinomială asociată polinomului** $f \in R[X]$ înţelegem funcţia $\widetilde{f} : R \to R$, $\widetilde{f}(x) = f(x)$.

Observaţia 36. La polinoame egale corespund funcţii polinomiale egale. Reciproca nu este numaidecât adevărată.

Theorem 37. *(Teorema împărţirii cu rest pentru polinoame.) Fie R inel comutativ unitar şi $f, g \in R[X]$ astfel încât g are coeficientul* *dominant inversabil (deci g este nenul). Atunci există şi sunt unice polinoamele $q, r \in R[X]$ cu proprietăţile:*

$$f = qg + r \text{ şi } \mathrm{grad(r)} < \mathrm{grad(g)}.$$

Demonstraţie: Pentru a arăta existenţa polinoamelor q şi r, considerăm $X := \{\mathrm{grad}(f - hg) \mid h \in R[X]\} \subseteq \mathbb{N} \cup \{-\infty\}$. Dacă $-\infty \in X$ atunci există $q \in R[X]$ a.î. $f = qg$, caz în care iau $r = 0$.

Dacă $-\infty \notin X$ sunt două posibilităţi. Prima, dacă $f = 0$ iau $q = r = 0$. A doua, dacă $f \neq 0$ atunci $X \subseteq \mathbb{N}$ şi îi iau primul element: cum $\mathbb{N}$ este bine ordonată, există $q \in R[X]$ a.î. $\mathrm{grad}(f - qg)$ este prim element al lui X. Notez $0 \neq r = f - qg \in R[X]$.

Dacă $\mathrm{grad}(r) \geq \mathrm{grad}(g)$, iau αX^n monomul ce defineşte gradul lui r şi βX^m monomul ce defineşte gradul lui g. Reamintim că $\alpha \neq 0$, $\beta \in U(R)$ şi $n \geq m$. Atunci $r - \alpha\beta^{-1}X^{n-m}g = f - (q + \alpha\beta^{-1}X^{n-m})g \in R[X]$ este polinom de grad mai mic strict decât $\mathrm{grad}(r)$, prim element în X; contradicţie! Deci $\mathrm{grad}(r) < \mathrm{grad}(g)$.

Unicitatea: fie $f = qg + r = q'g + r'$ cu $\mathrm{grad}(r), \mathrm{grad}(r') < \mathrm{grad}(g)$. Avem $r - r' = (q' - q)g$ şi $\mathrm{grad}(r - r') \leq \mathrm{grad}(r) < \mathrm{grad}(g)$. Cum g are coeficientul dominant inversabil, dacă $q - q' \neq 0$ atunci $\mathrm{grad}((q' - q)g) \geq \mathrm{grad}(g)$, o contradicţie. Rezultă că $q' - q = 0$ şi $r - r' = 0$.

Terminologie: q se numeşte câtul împărţirii lui f la g iar r restul.

Corolar 38. *(Teorema lui Bézout.) Fie R inel comutativ unitar şi $f \in R[X]$. Dacă $a \in A$, atunci restul împărţirii lui f la $X - a$ este $\widetilde{f}(a) \in R$, unde $\widetilde{f}$ este funcţia polinomială ataşată lui f.*

Demonstraţie: $f = (X - a)q + r$ cu $\mathrm{grad}(r) < 1$. Clar, $r = \widetilde{f}(a) \in R$.

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.