CURSUL 10: CONSTRUCŢII IMPORTANTE DE INELE

G. MINCU

1. Inel produs

Exemplul 1. Fie $R_1, R_2, \ldots, R_n$ inele. Pe produsul cartezian $R \overset{\text{not}}{=} R_1 \times R_2 \times \ldots \times R_n$ 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 2. Inelul din exemplul anterior se numeşte **produsul direct** al inelelor $R_1, R_2, \ldots, R_n$.

Observaţia 3. 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!)

2. Inele de matrice

În acest paragraf, R va desemna un inel, iar $m, n \in \mathbb{N}^*$.

Definiţia 4. 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 matricelor 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: $A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$.
- Vom folosi şi următoarele variante mai economicoase de notaţie: $A = (a_{ij})_{\substack{i=1,2,\ldots,m \\ j=1,2,\ldots,n}}$, 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 matricei $(a_{ij})_{i,j}$ este matricea $(-a_{ij})_{i,j}$.

Dacă $A = (a_{ij})_{\substack{i=1,2,\ldots,m\\ j=1,2,\ldots,n}} \in \mathcal{M}_{m,n}(R)$ şi $B = (b_{jk})_{\substack{j=1,2,\ldots,n\\ k=1,2,\ldots,p}} \in \mathcal{M}_{n,p}(R)$, definim produsul lor astfel: $AB = \left(\sum_{j=1}^{n} a_{ij}b_{jk}\right)_{\substack{i=1,2,\ldots,m\\ k=1,2,\ldots,p}}$. 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

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

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

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

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

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

Definiţia 7. Matricea I_n definită mai sus se numeşte **matricea unitate de ordin** n (sau **matricea identică de ordin** n).

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

Definiţia 8. 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 9. 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 10. Dacă $f, g \in R[[X]]$, atunci
a) $\mathrm{ord}(f + g) \geq \min\{\mathrm{ord}\ f, \mathrm{ord}\ g\}$
b) $\mathrm{ord}(fg) \geq \mathrm{ord}\ f + \mathrm{ord}\ g$.
Dacă, în plus, R este domeniu de integritate, atunci
b') $\mathrm{ord}(fg) = \mathrm{ord}\ f + \mathrm{ord}\ g$.

Observaţia 11. Dacă R este domeniu de integritate, atunci şi $R[[X]]$ este domeniu de integritate.

Propoziţia 12. $U(R[[X]]) = \{a_0 + a_1X + \cdots \in R[[X]] : a_0 \in U(R)\}$.

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 13. 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 14. 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 15. 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 16. 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 17. Dacă $f, g \in R[X]$, atunci
a) $\mathrm{grad}(f + g) \leq \max\{\mathrm{grad}\ f, \mathrm{grad}\ g\}$
b) $\mathrm{grad}(fg) \leq \mathrm{grad}\ f +$ grad g.
Dacă, în plus, R este domeniu de integritate, atunci
b') $\mathrm{grad}(fg) = \mathrm{grad}\ f +$ grad g.

Propoziţia 18. 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 19. 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 20. (**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 21. 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 22. Prin **funcţia polinomială asociată polinomului** $f \in R[X]$ înţelegem funcţia $\widetilde{f} : R \to R$, $\widetilde{f}(x) = f(x)$.

Observaţia 23. La polinoame egale corespund funcţii polinomiale egale. Reciproca nu este numaidecât adevărată.

Bibliografie

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