# Inele de polinoame

Fie $R$ un inel (nu neapărat comutativ). Fie $S=\{(a_0,a_1,\dots) \mid a_0,a_1,\dots\in R\}$, adică $S$ este mulțimea $\mathbb{N}$-uplurilor de elemente din $R$ (deci $S$ este produsul cartezian al unei familii de copii ale lui $R$, indexată de $\mathbb{N}$).

Vom nota $(a_0,a_1,\dots)$ și cu $(a_i)_{i\in\mathbb{N}}$.

Avem $(a_i)_{i\in\mathbb{N}}=(b_i)_{i\in\mathbb{N}} \Leftrightarrow a_i=b_i$ pt. orice $i\in\mathbb{N}$.

Pe $S$ avem o adunare indusă de cea a lui $R$, și anume:

$$(a_0,a_1,\dots)+(b_0,b_1,\dots)=(a_0+b_0,a_1+b_1,\dots),$$

cu care $S$ devine grup abelian. În fapt, acesta este produsul direct al unei familii de copii ale grupului abelian $(R,+)$, indexată după $\mathbb{N}$.

Elementul neutru este $(0,0,\dots)$, iar opusul lui $(a_0,a_1,\dots)$ este $(-a_0,-a_1,\dots)$.

Pe $S$ definim o înmulțire astfel:

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) \overset{df.}{=} (x_0, x_1, \dots),$$

unde $x_n = \sum\limits_{0 \le i \le n} a_i b_{n-i} = a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0$,

pentru orice $n \in \mathbb{N}^*$.

[Observație: Pe $S$ mai există o înmulțire, cea pe poziții. Cu acea înmulțire și cu adunarea precedentă, $S$ este chiar produsul direct al unei familii de copii ale inelului $R$, indexată după $\mathbb{N}$.

Înmulțirea definită mai sus pe $S$ este diferită de cea pe poziții.]

<u>Propoziție</u>. $S$ este inel cu adunarea și înmulțirea de mai sus. Dacă $R$ este comutativ, atunci și $S$ este comutativ.

În plus, aplicația $\varphi: R \to S$, $\varphi(a) = (a, 0, 0, \dots)$ pt. orice $a \in R$, este morfism injectiv de inele.

<u>Demonstrație</u>. Am văzut deja că $(S, +)$ este grup abelian.

(ip) (3)

Arătăm că înmulțirea este asociativă. Fie $f=(a_i)_{i\in\mathbb{N}}$, $g=(b_i)_{i\in\mathbb{N}}$ și $h=(c_i)_{i\in\mathbb{N}}$ elemente din $\mathcal{S}$. Fie $fg=(x_i)_{i\in\mathbb{N}}$, deci $x_j=\sum\limits_{0\le i\le j} a_i b_{j-i}$ pentru orice $j\in\mathbb{N}$.

Fie acum $(fg)h=(u_i)_{i\in\mathbb{N}}$, așadar pt. orice $n$ avem

$$u_n=\sum_{0\le j\le n} x_j c_{n-j}=\sum_{0\le j\le n}\Big(\sum_{0\le i\le j} a_i b_{j-i}\Big)c_{n-j}$$

$$=\sum_{\substack{0\le j\le n\\ 0\le i\le j}} a_i b_{j-i} c_{n-j}$$

Observăm că ~~{(i,j-i,n-j) | 0≤j≤n, 0≤i≤j}~~

$$\{(i,j-i,n-j) \mid 0\le j\le n,\ 0\le i\le j\}=\{(p,q,r)\mid p+q+r=n\}$$

(toate $i,j,p,q,r$ se presupun a fi în $\mathbb{N}$).

Într-adevăr:

"$\subseteq$" Dacă $0\le j\le n$ și $0\le i\le j$, fie $p=i$, $q=j-i$, $r=n-j$. Avem $(i,j-i,n-j)=(p,q,r)$, iar

$$p+q+r=i+j-i+n-j=n.$$

"$\supseteq$" Dacă $p+q+r=n$, fie $i=p$ și $j=p+q$, atunci $r=n-p-q=n-j$, deci $(p,q,r)=(i,j-i,n-j)$.

Rezultă că $u_n=\sum\limits_{p+q+r=n} a_p b_q c_r$.

Apoi dacă $f(gh) = (v_i)_{i\in\mathbb{N}}$, avem după un calcul similar:

$$gh = (y_i)_{i\in\mathbb{N}}, \quad y_j = \sum_{0\le i\le j} b_i c_{j-i}$$

$$v_n = \sum_{0\le j\le n} a_j y_{n-j} = \sum_{\substack{0\le j\le n\\ 0\le i\le n-j}} a_j b_i c_{n-j-i},$$

și se verifică la fel ca mai sus că

$$\{(j, i, n-j-i) \mid 0\le j\le n, 0\le i\le n-j\} = \{(p,q,r) \mid p+q+r=n\}.$$

Obținem că

$$v_n = \sum_{p+q+r=n} a_p b_q c_r = u_n \text{ pt. orice } n\in\mathbb{N},$$

de unde $(fg)h = f(gh)$.

Mai departe, dacă $e = (1, 0, 0, \ldots)$, definiția înmulțirii arată că $ef = fe = f$ pt. orice $f \in S$, deci $e$ este element neutru la înmulțire.

În sfârșit, arătăm că înmulțirea este distributivă față de adunare, adică

$f(g+h) = fg + fh$ și $(g+h)f = gf + hf$ pt. orice $f, g, h \in S$.

Fie $f = (a_i)_{i\in\mathbb{N}}$, $g = (b_i)_{i\in\mathbb{N}}$, $h = (c_i)_{i\in\mathbb{N}}$.

(ip) (5)

Cum $g+h=(b_i+c_i)_{i\in\mathbb{N}}$, rezultă că

$f(g+h)=(\alpha_i)_{i\in\mathbb{N}}$, unde

$$\alpha_n=\sum_{0\le i\le n} a_i(b_{n-i}+c_{n-i}).$$

Apoi $fg=(\beta_i)_{i\in\mathbb{N}}$ și $fh=(\gamma_i)_{i\in\mathbb{N}}$, unde

$\beta_n=\sum_{0\le i\le n} a_i b_{n-i}$, $\gamma_n=\sum_{0\le i\le n} a_i c_{n-i}$, deci

$fg+fh=(\beta_i+\gamma_i)_{i\in\mathbb{N}}$, iar

$$\beta_n+\gamma_n=\sum_{0\le i\le n}(a_i b_{n-i}+a_i c_{n-i})$$

$$=\sum_{0\le i\le n} a_i(b_{n-i}+c_{n-i})=\alpha_n.$$

Așadar $fg+fh=f(g+h)$. La fel se verifică distributivitatea la dreapta.

În concluzie $\mathcal{S}$ este inel.

Dacă $\varphi: R\to \mathcal{S}$, $\varphi(a)=(a,0,0,\dots)$, atunci

$\varphi(a)+\varphi(b)=(a,0,\dots)+(b,0,\dots)=(a+b,0,\dots)=\varphi(a+b)$ și

$\varphi(a)\varphi(b)=(a,0,\dots)\cdot(b,0,\dots)=(ab,0,\dots)=\varphi(ab)$.

Cum $\varphi(1)=(1,0,\dots)=e$ (el. neutru la înmulțire în $\mathcal{S}$), rezultă că $\varphi$ e morfism de inele.

Clar $\varphi$ e injectiv.

Dacă $R$ e comutativ, atunci pentru $f=(a_i)_{i\in\mathbb{N}}$ și $g=(b_i)_{i\in\mathbb{N}}$, fie $fg=(x_i)_{i\in\mathbb{N}}$ și $gf=(y_i)_{i\in\mathbb{N}}$.

Avem
$$x_n=\sum_{0\le i\le n}a_i b_{n-i}=\sum_{i+j=n}a_i b_j \overset{R\text{ comutativ}}{=\!=\!=}\sum_{i+j=n}b_j a_i$$
$$=\sum_{j+i=n}b_j a_i=\sum_{0\le j\le n}b_j a_{n-j}=y_n,$$

deci $fg=gf$, adică $S$ este inel comutativ, ceea ce încheie demonstrația.

---

Considerăm acum o submulțime a lui $S$, și anume

$$P=\{(a_i)_{i\in\mathbb{N}}\in S \mid \text{există } n\in\mathbb{N} \text{ pt. care } a_i=0 \text{ pt. orice } i>n\}.$$

(adică elementele lui $P$ sunt $\mathbb{N}$-upluri de forma $(a_0,\dots,a_n,0,0,\dots)$ pt. un $n\in\mathbb{N}$ și niște $a_0,\dots,a_n\in R$).

<u>Propoziție</u>. $P$ este subinel al lui $S$.

<u>Demonstrație</u>. Fie $f=(a_i)_{i\in\mathbb{N}}$, $g=(b_i)_{i\in\mathbb{N}}\in P$, deci există $n,m\in\mathbb{N}$ pentru care $a_i=0$ pt. orice $i>n$ și $b_i=0$ pt. orice $i>m$.

Dacă $i>\max(m,n)$, atunci $a_i=0$ și $b_i=0$, deci și $a_i-b_i=0$. Rezultă că $f-g\in P$.

Notăm $fg=(x_i)_{i\in\mathbb{N}}$. Dacă $p>m+n$, atunci $x_p=\sum\limits_{i+j=p} a_ib_j$. Dar pt. orice $i,j$ cu $i+j=p$ avem $i>m$ sau $j>n$ [într-adevăr, dacă $i\le m$ și $j\le n$, atunci $i+j\le m+n$, adică $p\le m+n$, contradicție]. Rezultă că pt. orice astfel de $i,j$ avem $a_i=0$ sau $b_j=0$, deci termenul $a_ib_j$ al sumei de mai sus este nul. Așadar $x_p=0$ pt. orice $p>m+n$, de unde $fg\in\mathcal{P}$. Cum $e=(1,0,0,\dots)\in\mathcal{P}$, rezultă că $\mathcal{P}$ este subinel al lui $\mathcal{S}$.

---

Vom da acum o nouă descriere a inelului $\mathcal{P}$.

Notăm $X=(0,1,0,0,\dots)$. Clar $X\in\mathcal{P}$. Atunci

$$X^2=(0,1,0,\dots)(0,1,0,\dots)=(0,0,1,0,0,\dots)$$

$$X^3=X\cdot X^2=(0,1,0,0,\dots)\cdot(0,0,1,0,\dots)=(0,0,0,1,0,\dots)$$

și se arată imediat prin inducție că

$$X^n=(0,0,\dots,0,\underset{\substack{\downarrow\\ \text{a }(n+1)\text{-a poziție}}}{1},0,\dots) \text{ pt. orice } n\in\mathbb{N}.$$

(ip) (8)

De asemenea, pt. orice $a \in R$ și orice $n \in \mathbb{N}^*$

$$\varphi(a)X^n = (a,0,0,\dots)\cdot(0,\dots,0,\underset{\substack{\downarrow\\ \text{poziția } (n+1)}}{1},0,\dots)$$

$$= (0,\dots,0,\underset{\substack{\downarrow\\ \text{poziția } (n+1)}}{a},0,\dots) = X^n\varphi(a).$$

Atunci dacă $f = (a_0, a_1, \dots, a_n, 0, 0, \dots) \in P$, avem

$$f = (a_0,0,0,\dots) + (0,a_1,0,\dots) + \dots + (0,\dots,0,\underset{\substack{\downarrow\\ \text{poziția}(i+1)}}{a_i},0,\dots) + \dots + (0,\dots,0,\underset{\substack{\downarrow\\ \text{poz.}(n+1)}}{a_n},0,\dots)$$

$$= \varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_i)X^i + \dots + \varphi(a_n)X^n.$$

Obținem că

$$P = \{\varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_n)X^n \mid n \in \mathbb{N}, a_0, \dots, a_n \in R\}.$$

Dacă $f = \varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_n)X^n$ și
$g = \varphi(b_0) + \varphi(b_1)X + \dots + \varphi(b_m)X^m$, atunci

$$f = g \iff \begin{cases} a_0 = b_0, \dots, a_n = b_n, & \text{în cazul } n = m \\ a_0 = b_0, \dots, a_n = b_n, b_{n+1} = \dots = b_m = 0 & \text{în cazul } n < m \\ a_0 = b_0, \dots, a_m = b_m, a_{m+1} = \dots = a_n = 0 & \text{în cazul } n > m. \end{cases}$$

Astfel, pt. orice $f, g \in P$ există $p \in \mathbb{N}$ a.î. $f$ și $g$ se reprezintă ca mai sus cu aceeași lungime, adică
$f = \varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_p)X^p$ și $g = \varphi(b_0) + \varphi(b_1)X + \dots + \varphi(b_p)X^p$
(se ia $p = \max\{n, m\}$ în reprezentarea de mai sus, apoi

dacă $n \neq m$, se completează acela dintre $f$ și $g$ care are reprezentarea mai scurtă cu zerouri, până la lungimea respectivă).

Cu această prezentare a elementelor lui $P$, operațiile se efectuează astfel:

- adunarea: dacă $f = \varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_p)X^p$ și $g = \varphi(b_0) + \varphi(b_1)X + \dots + \varphi(b_p)X^p$ sunt în $P$ (am observat mai sus că putem alege prezentări de aceeași lungime pt. $f$ și $g$), atunci

$$f + g = \varphi(a_0 + b_0) + \varphi(a_1 + b_1)X + \dots + \varphi(a_p + b_p)X^p.$$

- înmulțirea este indusă de relațiile

$$(\varphi(a)X^i)(\varphi(b)X^j) = \varphi(ab)X^{i+j} \text{ pt. orice } a, b \in R, i, j \in \mathbb{N}$$

(unde facem următoarea convenție:

$$X^0 = e = \text{el. neutru la înmulțire} = \varphi(1)),$$

deci dacă $f = \sum_{i=\overline{0,n}} \varphi(a_i)X^i$ și $g = \sum_{j=\overline{0,m}} \varphi(b_j)X^j$, atunci

$$fg = \sum_{k=\overline{0,m+n}} \varphi\Big(\sum_{i+j=k} a_i b_j\Big) X^k.$$

Cum $\varphi : R \to S$ este morfism injectiv de inele, deci $\varphi(R) \simeq R$ (izomorfism de inele), putem identifica $\varphi(R)$ cu $R$ (aceste inele fiind izomorfe, ele au aceleași proprietăți care țin de structura de inel). Aceasta înseamnă că în fapt îl înlocuim pe $\varphi(a)$ cu $a$ pt. orice $a \in R$ ~~și atunci~~ (faptul că $\varphi$ este morfism de inele arată că $\varphi(a)+\varphi(b)=\varphi(a+b)$, adică $\varphi(a)$ și $\varphi(b)$ se adună "la fel" cum se adună $a$ și $b$, și similar și la înmulțire). Atunci

$$P = \{ a_0 + a_1 X + \dots + a_n X^n \mid n \in \mathbb{N},\ a_0, \dots, a_n \in R \}.$$

Vom renota $P$ cu $R[X]$; acesta se numește inelul polinoamelor în nedeterminata $X$ cu coeficienți în inelul $R$. Elementele lui $P$ se numesc polinoame.

Dacă $f \in P$, $f \neq 0$, atunci $f$ se reprezintă unic sub forma $f = a_0 + a_1 X + \dots + a_n X^n$, cu $n \in \mathbb{N}$, $a_0, \dots, a_n \in R$ și $a_n \neq 0$. Pt. această reprezentare: