Inele de polinoame

Fie R inel comutativ. Notăm cu $R^{(\mathbb{N})}$ mulțimea șirurilor $(a_n)_{n\in\mathbb{N}}$ cu elemente din R și care au doar un nr. finit de termeni nenuli.
Pe $R^{(\mathbb{N})}$ definim două oper. alg.

$$(a_n)+(b_n)=(a_n+b_n)$$

$$(a_n)\cdot(b_n)=(c_n),$$

unde $c_n=\sum_{i+j=n} a_i b_j$

<u>Prop.</u> $(R^{(\mathbb{N})},+,\cdot)$ este inel comutativ.

Avem un morfism injectiv de inele

$$\varepsilon: R \longrightarrow R^{(\mathbb{N})},$$

$\varepsilon(a)=(a,0,0,\dots)$ care ne permite identificarea lui R cu un subinel al lui $R^{(\mathbb{N})}$.

Vom nota cu X șirul $(0,1,0,\dots)$ și îl vom numi <u>nedeterminată</u>.

Avem că $X^n=(\underbrace{0,0,\dots,0}_{n \text{ termeni}},1,0,\dots)$, $(\forall)\, n\geq 1$.

Astfel putem scrie

$$(a_0,a_1,\dots,a_n,0,\dots)=a_0+a_1X+\dots+a_nX^n.$$

<u>Def.</u> Inelul $R^{(\mathbb{N})}$ se notează $R[X]$ și s.n. <u>inelul polinoamelor</u> (în nedeterminata X) <u>cu coeficienți în R</u>.

<u>Def.</u> Dc. $f\in R[X]$, $f=a_0+a_1X+\dots+a_nX^n$, at.

f s.n. <u>polinom</u>, termenii a_iX^i s.n. <u>monoame</u>

iar $a_0, a_1, \dots a_n$ <u>coeficienți</u>.

$\max\{i \mid a_i \neq 0\} = \operatorname{grad} f$ s.n. <u>gradul polin.</u> f

iar dc. $n = \operatorname{grad} f$, a_n s.n. <u>coeficientul dominant</u> al lui f. Polinoamele cu coef. dom. 1 s.n. <u>monice</u>.

Vom face urm. convenție: $\operatorname{grad} 0 = -\infty$.

<u>Prop.</u> $f, g \in R[X]$.

i) $\operatorname{grad}(f+g) \leq \max(\operatorname{grad} f, \operatorname{grad} g)$.

ii) $\operatorname{grad}(fg) \leq \operatorname{grad} f + \operatorname{grad} g$

cu egalitate dc. și numai dc. produsul coef. dom. ai lui f și g este $\neq 0$.

<u>Cor. 1</u> R integru $\Rightarrow$ $\operatorname{grad}(fg) = \operatorname{grad} f + \operatorname{grad} g$, $(\forall) f, g \in R[X]$. Mai mult, $R[X]$ este de asemenea integru.

<u>Cor. 2</u> R integru $\Rightarrow$ $U(R[X]) = U(R)$.

<u>Obs.</u> $R = \mathbb{Z}_4$, $f = \hat{1} + \hat{2}X \in U(R[X])$; $f^2 = 1$.

<u>Teoremă</u> (propriet. de universalitate a inelelor de polinoame)

R inel comutativ

$f: R \to S$ morf. de inele comutative

și $\alpha \in S$.

$$\begin{tikzcd} R \arrow[r, "\varepsilon"] \arrow[d, "f"'] & R[X] \arrow[dl, dotted, "\bar{f}"] \\ \alpha \in S & \end{tikzcd}$$

At. există un morfism de inele $\bar{f}: R[X] \to S$ unic cu propriet. că $\bar{f} \circ \varepsilon = f$ și $\bar{f}(X) = \alpha$.

<u>Dem.</u> Def. $\bar{f}(a_0 + a_1X + \dots + a_nX^n) = f(a_0) + f(a_1)\alpha + \dots + f(a_n)\alpha^n$. //

Inele de polinoame într-un număr finit de nedeterminate

Def. R inel comutativ unitar. At. inelul de polinoame în nedeterminatele $X_1, \dots, X_n$ cu coeficienți în R se definește inductiv ca fiind $R[X_1, \dots, X_{n-1}][X_n]$ și se not. $R[X_1, \dots, X_n]$.

Obs. $f \in R[X_1, \dots, X_n]$ se scrie $f = f_0 + f_1 X_n + \dots + f_r X_n^r$, unde $f_i \in R[X_1, \dots, X_{n-1}]$, $\forall i$.

Prop. $(\forall) f \in R[X_1, \dots, X_n]$ $(\exists!)$ $a_{i_1 \dots i_n} \in R$, $k_1, \dots, k_n \in \mathbb{N}$, $0 \le i_1 \le k_1, \dots, 0 \le i_n \le k_n$ a.î.

$$f = \sum_{i_1, \dots, i_n = 0}^{k_1, \dots, k_n} a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}$$

Dem. Inducție după $n \ge 1$. Scriem

$f = f_0 + f_1 X_n + \dots + f_{k_n} X_n^{k_n}$, $f_i \in R[X_1, \dots, X_{n-1}]$, $\forall i$

și aplicăm ipot. de ind.

Pt. unicitate să pp. $f = 0$. Scriem

$$f = f_0 + f_1 X_n + \dots + f_{k_n} X_n^{k_n},$$

unde $f_j = \sum_{i_1, \dots, i_{n-1} = 0}^{k_1, \dots, k_{n-1}} a_{i_1 \dots i_{n-1} j} X_1^{i_1} \dots X_{n-1}^{i_{n-1}} \in R[X_1, \dots, X_{n-1}]$

$f = 0 \Rightarrow f_j = 0$, $\forall j$ $\Rightarrow a_{i_1 \dots i_n} = 0$, $(\forall) i_1, \dots, i_n$. //

Def. Un polinom de forma $a X_1^{i_1} \dots X_n^{i_n}$, $a \ne 0$, s.n. monom, iar gradul său se consideră a fi $i_1 + \dots + i_n$. Dc. $f \in R[X_1, \dots, X_n]$, at. gradul său este maximul gradelor monoamelor ce apar în scrierea sa. Dc. toate monoamele au același grad, at. f s.n. polinom omogen.

Obs. Orice polinom se scrie ca sumă de polinoame omogene.

Prop. $f, g \in R[X_1, \dots, X_n]$.

a) $\text{grad}(f+g) \leq \max(\text{grad} f, \text{grad} g)$

b) $\text{grad}(fg) \leq \text{grad} f + \text{grad} g$

c) R integru $\Rightarrow R[X_1, \dots, X_n]$ integru şi avem egalitate la b)

Dem. c) Inducţie după $n \geq 1$.

Corolar R integru $\Rightarrow U(R[X_1, \dots, X_n]) = U(R)$.

Teoremă (proprietatea de universalitate a inelelor de polinoame într-un nr. finit de nedeterminate)

R inel comutativ

$f : R \to S$ morf. de inele unitare şi $\alpha_1, \dots, \alpha_n \in S$.

$$\begin{tikzcd} R \arrow[r, "\varepsilon"] \arrow[dr, "f"'] & R[X_1, \dots, X_n] \arrow[d, dashed, "\bar{f}"] \\ & S \ni \alpha_1, \dots, \alpha_n \end{tikzcd}$$

At. există un morf. de inele $\bar{f} : R[X_1, \dots, X_n] \to S$ unic cu propriet. că $\bar{f} \circ \varepsilon = f$ şi $\bar{f}(X_i) = \alpha_i, \forall i$.

Dem. Inducţie după $n \geq 1$.

Funcţii polinomiale. Rădăcini ale polinoamelor

Fie S inel comutativ, $R \subset S$ subinel şi $i : R \to S$ morf. incluziune. Avem diagrama ($\alpha \in S$)

$$\begin{tikzcd} R \arrow[r, "\varepsilon"] \arrow[dr, "i"'] & R[X] \arrow[d, "\bar{i}_\alpha"] \\ & \alpha \in S \end{tikzcd}$$

Din prop. de univ. există $\bar{i}_\alpha : R[X] \to S$ un morf. cu propr. $\bar{i}_\alpha \circ \varepsilon = i$ şi $\bar{i}_\alpha(X) = \alpha$. Deci

$$\bar{i}_\alpha(f) = \underbrace{\sum_{i=0}^{n} a_i \alpha^i}_{\overset{\text{not}}{=}\, f(\alpha) \in S}, \quad f = \sum_{i=0}^{n} a_i X^i.$$

Def. $\alpha \in S$ este rădăcină a polinomului f dc. $f(\alpha)=0$.

Obs. $f \in R[X]$; putem def. o funcție

$$\tilde{f}: S \to S,\ \tilde{f}(\alpha)=f(\alpha).$$

Def. Funcția $\tilde{f}: S \to S$ def. mai sus s.n. funcția polinomială pe S asociată polinomului f. Când $R=S$, at. $\tilde{f}$ s.n. funcția polinomială asoc. lui f.

Obs. Polinoame diferite pot avea funcții polinomiale egale!

$f, g \in \mathbb{Z}_2[X]$, $f=X$, $g=X^2 \Rightarrow \tilde{f}=\tilde{g}$.

Vom vedea că acest lucru nu este posibil at. când $f, g \in R[X]$, R integru infinit.

Prop (teorema de împărțire cu rest pt. polinoame)

$f, g \in R[X]$, $g \neq 0$ și coef. dom. al lui g inversabil. At. există $q, r \in R[X]$ unice cu propriet. că $f = gq + r$, $\operatorname{grad} r < \operatorname{grad} g$.

Dem. $\operatorname{grad} f < \operatorname{grad} g$; $f = 0 \cdot g + f$.

$\operatorname{grad} f \geq \operatorname{grad} g$. Inducție după $\operatorname{grad} f$.

Corolar 1

$f \in R[X]$, $\alpha \in R \Rightarrow (\exists!)\, q \in R[X]$ a.î. $f = (X-\alpha)q + f(\alpha)$.

Corolar 2 (Bézout)

$f \in R[X]$, $\alpha \in R$; $X-\alpha \mid f \Leftrightarrow f(\alpha)=0$.

Prop. $f \in R[X]$, $f \neq 0$, $\operatorname{grad} f = n$, R integru $\Rightarrow f$ are cel mult n rădăcini distincte în R.

Dem. Fie $\alpha_1, \dots, \alpha_m \in R$ distincte, $f(\alpha_i) = 0$.
Vom dem. prin inducție după m că f se divide cu $\prod_{i=1}^{m}(X-\alpha_i)$. De aici rezultă grad $f \geq m$.

$m=1$: Teorema lui Bézout.

$m>1$: $f = \prod_{i=1}^{m-1}(X-\alpha_i) g$, $g \in R[X]$.

$f(\alpha_m) = 0 \Rightarrow \prod_{i=1}^{m-1}(\alpha_m - \alpha_i) g(\alpha_m) = 0 \Rightarrow g(\alpha_m) = 0$

$\Rightarrow X - \alpha_m \mid g$. //

Obs. Dc. R nu este integru, at. prop. este falsă!
$f \in \mathbb{Z}_6[X]$, $f = X^3 - X$ are 6 răd. dist. în $\mathbb{Z}_6$.

Corolar
R inel integru infinit și $f, g \in R[X]$.

$$\tilde{f} = \tilde{g} \Rightarrow f = g$$

Dem. $h = f - g \Rightarrow \tilde{h} = 0 \Rightarrow h(\alpha) = 0, (\forall)\alpha \in R \Rightarrow h = 0$. //

Prop. (Relațiile lui Viète)
R comutativ integru, $f \in R[X]$, $f = a_0 + a_1 X + \dots + a_n X^n$, grad $f = n$. Pp. că f are n rădăcini $\alpha_1, \dots, \alpha_n \in R$.
At. $f = a_n (X-\alpha_1) \dots (X-\alpha_n)$ și în plus au loc relațiile:

$$\begin{cases} \sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n} \in Q(R) \\ \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j = \frac{a_{n-2}}{a_n} \in Q(R) \\ \dots \\ \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n} \in Q(R) \end{cases}$$

Dem. Se identifică coef. //

Polinoame simetrice

R inel comutativ unitar, $n \geq 2$, $\sigma \in S_n$.
Din propr. de univ. a inelelor de polinoame într-un nr. finit de nedeterm. obț. că există $\overline{\sigma} : R[X_1, \ldots, X_n] \longrightarrow R[X_1, \ldots, X_n]$ morf. de inele cu propr. că $\overline{\sigma} \circ \varepsilon = \varepsilon$ și $\overline{\sigma}(X_i) = X_{\sigma(i)}$, $(\forall)\ i = 1, \ldots, n$.

Ex. $f = X_1^2 X_3 + X_1 X_2 X_3^2 \in R[X_1, X_2, X_3]$ și $\sigma = (1\,2\,3)$; at. $\overline{\sigma}(f) = X_1 X_2^2 + X_1^2 X_2 X_3$.

Obs. În general, $\overline{\sigma}(f(X_1, \ldots, X_n)) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$, $(\forall)\ f \in R[X_1, \ldots, X_n]$.

Obs. 1) $\sigma, \tau \in S_n \Rightarrow \overline{\sigma \circ \tau} = \overline{\sigma} \circ \overline{\tau}$

2) $\overline{e}(f) = f$

3) $\overline{\sigma}$ izomorfism cu $\overline{\sigma}^{-1} = \overline{\sigma^{-1}}$.

Def. $f \in R[X_1, \ldots, X_n]$ s.n. polinom <u>simetric</u> dc. $\overline{\sigma}(f) = f$, $(\forall)\ \sigma \in S_n$.

Obs. f simetric $\Leftrightarrow \overline{\tau}(f) = f$, $(\forall)\ \tau \in S_n$ transpoziție.

Ex. $f \in R[X_1, X_2]$, $f = X_1^2 + X_2^2$ este polinom simetric.

Obs. $\Sigma := \{ f \in R[X_1, \ldots, X_n] \mid f \text{ simetric} \}$

$\Sigma \subset R[X_1, \ldots, X_n]$ subinel.

Prop. Polinoamele $s_1, \ldots, s_n \in R[X_1, \ldots, X_n]$ def. prin $s_k = \sum\limits_{1 \leq i_1 < \ldots < i_k \leq n} X_{i_1} \cdots X_{i_k}$, $1 \leq k \leq n$, sunt polinoame simetrice.

Dem. Se consideră polinomul $g(T)=(T-X_1)\dots$
$\dots(T-X_n)$, $g\in R[X_1,\dots,X_n][T]$.

Avem $g(T)=T^n-s_1T^{n-1}+s_2T^{n-2}-\dots+(-1)^n s_n$.

Fie $\sigma\in S_n$. Def. $\bar\sigma : R[X_1,\dots,X_n,T]\to R[X_1,\dots,X_n,T]$ ai $\bar\sigma(X_i)=X_{\sigma(i)}$, $1\le i\le n$, $\bar\sigma(T)=T$.

At. $\bar\sigma(g)=(T-X_{\sigma(1)})\dots(T-X_{\sigma(n)})=g$. Pe de altă parte, $\bar\sigma(g)=\bar\sigma(T^n-s_1T^{n-1}+\dots+(-1)^n s_n)$
$=T^n-\bar\sigma(s_1)T^{n-1}+\dots+(-1)^n\bar\sigma(s_n)\Rightarrow s_k=\bar\sigma(s_k)$, $1\le k\le n$, deci polin. s_k sunt simetrice.//

<u>Def</u>. Polin. $s_1,\dots,s_n\in R[X_1,\dots,X_n]$ def. mai sus s.n. <u>polinoamele simetrice fundamentale</u> în nedeterminatele $X_1,\dots,X_n$.

Vom defini pe mulțimea monoamelor în n nedeterminate o relație de ordine ~~totală~~:
$\mu_1=aX_1^{i_1}\dots X_n^{i_n}>\mu_2=bX_1^{j_1}\dots X_n^{j_n}$ $(a,b\neq 0)$ dc. există $s\in\{1,\dots,n\}$ ai $i_1=j_1,\dots,i_{s-1}=j_{s-1}$ și $i_s>j_s$.
Rel. def. mai sus s.n. <u>ordinea lexicografică</u>.

<u>Obs</u>. Ordinea lexicografică este o rel. de ord. totală.

<u>Def</u>. $f\in R[X_1,\dots,X_n]$, $f\neq 0$. Cel mai mare monom (din scrierea lui f ca sumă de monoame) în ordinea lexicografică s.n. <u>termenul principal</u> al lui f și se not. $lt(f)$.

<u>Ex</u>. $f\in\mathbb{Q}[X_1,X_2,X_3]$, $f=\underline{X_1^2X_2^2}+X_1X_2^3X_3+X_1^2X_2$

$lt(f) = X_1^i X_2^i$.

Lemă Fie $m_1, m_2 \in R[X_1, ..., X_n]$ monoame $\neq 0$, $m_1 > m_2$.

a) $m_1 u > m_2 u$, $(\forall) u$ monom, $u \neq 0$.

b) $u_1 > u_2 \Rightarrow m_1 u_1 > m_2 u_2$.

Prop. $f, g \in R[X_1, ..., X_n]$, $f, g \neq 0$. Dc. $lt(f) = am$, $a \in R - \{0\}$, $lt(g) = bu$, $b \in R - \{0\}$ și $ab \neq 0$, at. $lt(fg) = (ab)mu = lt(f)\,lt(g)$.

Lemă $f \in R[X_1, ..., X_n]$ polinom simetric și $lt(f) = aX_1^{i_1} \cdots X_n^{i_n}$, $a \neq 0$, at. $i_1 \geq \cdots \geq i_n$.

Obs. Dc. $m = aX_1^{i_1} \cdots X_n^{i_n}$, $a \neq 0$, și $i_1 \geq \cdots \geq i_n$, at. există un nr. finit de monoame $u = bX_1^{j_1} \cdots X_n^{j_n}$, $b \neq 0$, $j_1 \geq \cdots \geq j_n$, ai $m > u$.

De fapt, orice șir descrescător de monoame este finit! (Se dem. prin inducție după $n \geq 1$.)

Teoremă (teorema fundam. a polin. simetrice)

Orice polinom simetric din $R[X_1, ..., X_n]$ se exprimă în mod unic ca polinom de polinoamele simetrice fundamentale.

Dem. Fie $f \in R[X_1, ..., X_n]$, f polinom simetric și $lt(f) = aX_1^{i_1} \cdots X_n^{i_n}$, $a \neq 0$ și $i_1 \geq \cdots \geq i_n$.

Deoarece $lt(\Delta_k) = X_1 \cdots X_k$, $1 \leq k \leq n$, avem că $lt(a\,\Delta_1^{i_1 - i_2} \cdots \Delta_{n-1}^{i_{n-1} - i_n} \Delta_n^{i_1}) = lt(f)$

Fie $f_1 = f - a\,\Delta_1^{i_1 - i_2} \cdots \Delta_{n-1}^{i_{n-1} - i_n} \Delta_n^{i_n}$; $f_1 \in R[X_1, ..., X_n]$, f_1 simetric.

Avem că $lt(f_1) < lt(f)$. (17)

Unicitatea Vom dem. că dacă $h \in R[X_1, \ldots, X_n]$ și $h(s_1, \ldots, s_n) = 0$, at. $h = 0$.

Scriem $h = \sum_{i_1, \ldots, i_n} a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$

$h(s_1, \ldots, s_n) = 0 \Rightarrow \sum a_{i_1 \ldots i_n} s_1^{i_1} \ldots s_n^{i_n} = 0$;

dc. $a_{i_1 \ldots i_n} \neq 0$, at. $lt(a_{i_1 \ldots i_n} s_1^{i_1} \ldots s_n^{i_n}) = a_{i_1 \ldots i_n} X_1^{k_1} \ldots X_n^{k_n}$, unde $k_1 = i_1 + \ldots + i_n$, $k_2 = i_2 + \ldots + i_n$, $\ldots$, $k_n = i_n$.

Mai mult, dc. $(i_1, \ldots, i_n) \neq (j_1, \ldots, j_n)$, at. $(k_1, \ldots, k_n) \neq (l_1, \ldots, l_n)$, unde $k_r = i_r + \ldots + i_n$
$l_r = j_r + \ldots + j_n$
$(1 \leq r \leq n)$.

Asta înseamnă că $lt(a_{i_1 \ldots i_n} s_1^{i_1} \ldots s_n^{i_n}) \neq lt(a_{j_1 \ldots j_n} s_1^{j_1} \ldots s_n^{j_n})$ pt. $(i_1, \ldots, i_n) \neq (j_1, \ldots, j_n)$, ceea ce reprezintă o contradicție. //

Fie $p_i = X_1^i + \ldots + X_n^i$, $i \geq 1$; p_i polinom simetric

Formulele lui Newton

1) $p_k - p_{k-1} s_1 + \ldots + (-1)^n p_{k-n} s_n = 0$, $k \geq n$

2) $p_k - p_{k-1} s_1 + \ldots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k = 0$, $1 \leq k \leq n$.

Dem. 1) $g(T) = (T - X_1) \ldots (T - X_n)$

$g(T) = T^n - s_1 T^{n-1} + \ldots + (-1)^n s_n$

$g(X_i) = 0$, $1 \leq i \leq n$, deci

$X_i^n - s_1 X_i^{n-1} + \ldots + (-1)^n s_n = 0$, $1 \leq i \leq n$.

Prin înmulțire cu X_i^{n-k} obț.

$$X_i^k - s_1 X_i^{k-1} + \dots + (-1)^n s_n X_i^{n-k} = 0, \quad 1 \le i \le n$$

Adunăm aceste relații și obț.

$$p_k - s_1 p_{k-1} + \dots + (-1)^n p_{k-n} s_n = 0.$$

2) Lemă $f \in R[X_1, \dots, X_n]$ polinom omogen simetric de grad $k < n$. At. $f \neq 0 \Rightarrow f(X_1, \dots, X_k, 0, \dots, 0) \neq 0$.

Dem. $u = a X_1^{i_1} \dots X_n^{i_n}$, $a \neq 0$, termenul principal al lui f; avem $i_1 \geq \dots \geq i_n$ și $i_1 + \dots + i_n = k$. Deoarece $k < n$, rezultă $i_{k+1} = \dots = i_n = 0$. Deci $u = a X_1^{i_1} \dots X_k^{i_k}$, asta însemnând că nu se anulează at. când $X_{k+1} = \dots = X_n = 0$. //

Fie acum $f = p_k - p_{k-1} s_1 + \dots + (-1)^k k s_k$, $k < n$. f este polinom simetric omogen de grad k și $f(X_1, \dots, X_k, 0, \dots, 0) = p_k' - p_{k-1}' s_1' + \dots + (-1)^k k s_k'$, unde p_i', s_j' sunt polinoamele def. anterior dar de data aceasta în k nedeterminate.

Din 1), cazul $k = n$, obț. $f(X_1, \dots, X_k, 0, \dots, 0) = 0$, deci, cf. Lemei, $f = 0$. //