

INELE DE POLINOAME

Pe parcursul acestui capitol prin inel se va înțelege inel comutativ și unitar iar morfismele de inele vor fi unitare.

1. INELE DE POLINOAME ÎNTR-O NEDETERMINATĂ

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

$$(a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}} = (a_n + b_n)_{n \in \mathbb{N}},$$

$$(a_n)_{n \in \mathbb{N}} \cdot (b_n)_{n \in \mathbb{N}} = (c_n)_{n \in \mathbb{N}},$$

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

Propoziția 1.1. $(R^{(\mathbb{N})}, +, \cdot)$ este inel comutativ și unitar.

Definim un morfism injectiv de inele unitare $\varepsilon : R \rightarrow R^{(\mathbb{N})}$, $\varepsilon(a) = (a, 0, 0, \dots)$ care ne permite să-l identificăm pe R cu un subinel al lui $R^{(\mathbb{N})}$. Vom nota cu X șirul $(0, 1, 0, 0, \dots)$ și-l vom numi *nedeterminată*. Observăm că

$$X^n = (\underbrace{0, \dots, 0}_n, 1, 0, 0, \dots)$$

n termeni

pentru orice $n \in \mathbb{N}^*$. Ca de obicei, considerăm X^0 ca fiind egal cu elementul unitate. Se observă că $(a_0, a_1, \dots, a_n, 0, 0, \dots) = \varepsilon(a_0) + \varepsilon(a_1)X + \dots + \varepsilon(a_n)X^n$ iar prin identificarea lui R cu un subinel al lui $R^{(\mathbb{N})}$ dată de ε putem scrie

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

Definiția 1.2. Inelul $R^{(\mathbb{N})}$ se notează cu $R[X]$ și se numește inelul polinoamelor în nedeterminata X cu coeficienți în R .

Dacă $f \in R[X]$, atunci $f = a_0 + a_1 X + \dots + a_n X^n$, $a_i \in R$ și f se numește *polinom în nedeterminata X* . Polinoamele X^n , $n \in \mathbb{N}$ se numesc *monoame în nedeterminata X* . Așadar orice polinom este în mod unic o combinație liniară de monoame cu coeficienți în R . Polinoamele $a_i X^i$ cu $a_i \neq 0$ se numesc *termeni* ai lui f , iar $a_i \neq 0$ *coeficienți*. Definim $\deg f = \max\{i : a_i \neq 0\}$ și-l numim *gradul* lui f . Dacă $n = \deg f$, atunci a_n se numește *coeficientul dominant* al lui f . Polinoamele al căror coeficient dominant este 1 se numesc polinoame *monice*.

În cele ce urmează vom face următoarea convenție: $\deg 0 = -\infty$.

Propoziția 1.3. Fie $f, g \in R[X]$. Atunci:

(i) $\deg(f + g) \leq \max(\deg f, \deg g)$.

(ii) $\deg(fg) \leq \deg f + \deg g$, cu egalitate dacă și numai dacă produsul coeficienților dominanți ai lui f și g este nenul.

Corolarul 1.4. Fie R un inel integru. Atunci $\deg(fg) = \deg f + \deg g$ pentru orice $f, g \in R[X]$. Mai mult, $R[X]$ este, de asemenea, inel integru.

Corolarul 1.5. Fie R un inel integru. Atunci $U(R[X]) = U(R)$.

Remarca 1.6. Proprietatea de mai sus nu mai rămâne adevărată dacă R nu este inel integru. Fie $R = \mathbb{Z}/4\mathbb{Z}$ și $f = \hat{1} + \hat{2}X \in R[X]$. Avem $f^2 = \hat{1}$, deci $f \in U(R[X])$, dar $f \notin U(R)$.

Exercițiul 1.7. Fie R un inel comutativ unitar și $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Să se arate că:

- (i) f este nilpotent dacă și numai dacă a_i este nilpotent pentru orice $0 \leq i \leq n$.
- (ii) f este inversabil dacă și numai dacă a_0 este inversabil și a_i este nilpotent pentru orice $1 \leq i \leq n$.

Reamintim că există un morfism (canonic) de inele unitare $\varepsilon : R \rightarrow R[X]$ dat prin $\varepsilon(a) = a$ pentru orice $a \in R$.

Teorema 1.8. (Proprietatea de universalitate a inelelor de polinoame într-o nedeterminată) Fie $\varphi : R \rightarrow S$ un morfism de inele comutative unitare și $s \in S$. Atunci există un morfism unitar $\bar{\varphi} : R[X] \rightarrow S$ unic cu proprietatea că $\bar{\varphi} \circ \varepsilon = \varphi$ și $\bar{\varphi}(X) = s$.

Proof. Să vizualizăm această proprietate cu ajutorul următoarei diagrame:

$$\begin{array}{ccc} R & \xrightarrow{\varepsilon} & R[X] \\ & \searrow \varphi & \downarrow \bar{\varphi} \\ & & S \end{array}$$

Definim $\bar{\varphi}(a_0 + a_1X + \cdots + a_nX^n) = \varphi(a_0) + \varphi(a_1)s + \cdots + \varphi(a_n)s^n$. Se arată ușor că $\bar{\varphi}$ este morfism unitar de inele care satisface cele două proprietăți. Mai mult, acesta este unic, deoarece $\bar{\varphi}(X) = s$ conduce la $\bar{\varphi}(X^i) = s^i$ pentru orice $i \geq 1$ iar $\bar{\varphi} \circ \varepsilon = \varphi$ este echivalent cu $\bar{\varphi}(a) = \varphi(a)$ pentru orice $a \in R$. \square

1.1. Funcții polinomiale. Rădăcini. Fie S un inel comutativ și unitar, $R \subseteq S$ un subinel și $i : R \rightarrow S$ morfismul incluziune. Fie $s \in S$. Din proprietatea de universalitate a inelelor de polinoame într-o nedeterminată există un morfism unitar $\bar{i}_s : R[X] \rightarrow S$ unic cu proprietatea că $\bar{i}_s \circ \varepsilon = i$ și $\bar{i}_s(X) = s$.

$$\begin{array}{ccc} R & \xrightarrow{\varepsilon} & R[X] \\ & \searrow i & \downarrow \bar{i}_s \\ & & S \end{array}$$

Dacă $f \in R[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$, atunci $\bar{i}_s(f) = a_0 + a_1s + \cdots + a_ns^n$. Notăm $a_0 + a_1s + \cdots + a_ns^n$ cu $f(s)$ și avem $\bar{i}_s(f) = f(s)$.

Definiția 1.9. Un element $s \in S$ cu proprietatea că $f(s) = 0$ se numește rădăcină a lui f .

Pentru orice polinom $f \in R[X]$ putem defini o funcție $\tilde{f} : S \rightarrow S$ prin $\tilde{f}(s) = f(s)$ pentru orice $s \in S$.

Definiția 1.10. Funcția $\tilde{f} : S \rightarrow S$ definită mai sus se numește funcția polinomială pe S asociată lui f . Când $S = R$, funcția $\tilde{f} : R \rightarrow R$ se numește funcția polinomială asociată lui f .

Remarca 1.11. Polinoame diferite pot avea funcții polinomiale egale. De exemplu, $f, g \in \mathbb{Z}_2[X]$, $f = X$ și $g = X^2$. Avem că $\tilde{f}, \tilde{g} : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, $\tilde{f}(\hat{0}) = \tilde{g}(\hat{0}) = \hat{0}$ și $\tilde{f}(\hat{1}) = \tilde{g}(\hat{1}) = \hat{1}$.

Vom vedea însă că acest lucru nu mai este posibil dacă $f, g \in R[X]$, unde R este un domeniu de integritate *infinit*.

2. TEOREMA DE ÎMPĂRȚIRE CU REST PENTRU POLINOAME ÎNTR-O NEDETERMINATĂ

Teorema 2.1. (Teorema de împărțire cu rest) Fie R un inel, $f, g \in R[X]$, $g \neq 0$ iar coeficientul dominant al lui g este inversabil. Atunci există $q, r \in R[X]$ unice cu proprietatea că $f = gq + r$ și $\deg r < \deg g$.

Proof. Dacă $\deg f < \deg g$, atunci scriem $f = g \cdot 0 + f$. În cazul în care $\deg f \geq \deg g$ facem inducție după $\deg f$.

Unicitatea rezultă imediat folosind Propoziția 1.3(ii). \square

Corolarul 2.2. Fie R un inel, $f \in R[X]$ și $\alpha \in R$. Atunci există $q \in R[X]$ și $r \in R$ unice cu proprietatea că $f = (X - \alpha)q + r$.

Corolarul 2.3. (Bézout) Fie R un inel, $f \in R[X]$ și $\alpha \in R$. Atunci $X - \alpha \mid f$ dacă și numai dacă $f(\alpha) = 0$.

Exercițiul 2.4. Fie R inel comutativ unitar și $\alpha \in R$. Atunci $R[X]/(X - \alpha) \simeq R$.

Exercițiul 2.5. Arătați că:

- (i) $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.
- (ii) $\mathbb{Z}[X]/(X^2 - 2) \simeq \mathbb{Z}[\sqrt{2}]$.

Exercițiul 2.6. Să se arate că $R = \mathbb{Z}[X]/(2, X^2 + 1)$ este un inel cu 4 elemente, dar R nu este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exercițiul 2.7. Considerăm idealul $I = (3, X^3 - X^2 + 2X + 1)$ în $\mathbb{Z}[X]$. Să se arate că I nu este ideal principal și că $\mathbb{Z}[X]/I$ nu este inel integru.

Exercițiul 2.8. Aflați inversul lui $\widehat{4X + 3}$ în inelul factor $\mathbb{Z}_{11}[X]/(X^2 + 1)$.

Propoziția 2.9. Fie R un inel integru și $f \in R[X]$, $\deg f = n$. Atunci f are cel mult n rădăcini distincte în R .

Proof. Fie $\alpha_1, \dots, \alpha_m \in R$ distincte cu proprietatea că $f(\alpha_i) = 0$ pentru orice $i = 1, \dots, m$. Vom demonstra prin inducție după m că $(X - \alpha_1) \cdots (X - \alpha_m) \mid f$. Cazul $m = 1$ rezultă din corolarul 2.3. Dacă $m > 1$, atunci, din ipoteza de inducție $(X - \alpha_1) \cdots (X - \alpha_{m-1}) \mid f$ și putem scrie $f = (X - \alpha_1) \cdots (X - \alpha_{m-1})g$ cu $g \in R[X]$. Din $f(\alpha_m) = 0$ obținem $(\alpha_m - \alpha_1) \cdots (\alpha_m - \alpha_{m-1})g(\alpha_m) = 0$. Dar cum R este integru și $\alpha_i \neq \alpha_m$ pentru orice $i \neq m$ rezultă $g(\alpha_m) = 0$ și din corolarul 2.3 deducem că $X - \alpha_m \mid g$.

În concluzie, $n = \deg f \geq m$. \square

Remarca 2.10. Dacă R nu este integru, atunci proprietatea de mai sus este falsă. De exemplu, polinomul $f \in \mathbb{Z}_6[X]$, $f = X^3 - X$ are șase rădăcini distincte în \mathbb{Z}_6 .

Corolarul 2.11. Fie R un inel integru infinit și $f, g \in R[X]$. Dacă $\tilde{f} = \tilde{g}$, atunci $f = g$.

Proof. Fie $h = f - g$. Deoarece $\tilde{f} = \tilde{g}$ avem $\tilde{h} = 0$, adică $h(\alpha) = 0$ pentru orice $\alpha \in R$. Din propoziția 2.9 rezultă $h = 0$. \square

Propoziția 2.12. (Relațiile lui Viète) Fie R un inel integru, $f \in R[X]$, $f = a_0 + a_1X + \dots + a_nX^n$, $a_n \neq 0$. Presupunem că f are n rădăcini $\alpha_1, \dots, \alpha_n \in R$. Atunci au loc relațiile:

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

Proof. Arătăm prin inducție după n că $f = a_n(X - \alpha_1) \cdots (X - \alpha_n)$ și apoi identificăm coeficienții. \square

3. INELE DE POLINOAME ÎNTR-UN NUMĂR FINIT DE NEDETERMINATE

Definiția 3.1. Fie R un inel. Atunci 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 notează $R[X_1, \dots, X_n]$. Elementele inelului $R[X_1, \dots, X_n]$ se numesc polinoame în nedeterminatele X_1, \dots, X_n .

Remarca 3.2. Orice polinom $f \in R[X_1, \dots, X_n]$ se scrie (în mod unic) sub forma

$$f = f_0 + f_1X_n + \dots + f_rX_n^r$$

cu $f_i \in R[X_1, \dots, X_{n-1}]$ pentru orice $i = 0, 1, \dots, r$.

Propoziția 3.3. Pentru orice polinom $f \in R[X_1, \dots, X_n]$ există și sunt unice $k_1, \dots, k_n \in \mathbb{N}$ și $a_{i_1, \dots, i_n} \in R$, unde $0 \leq i_1 \leq k_1, \dots, 0 \leq i_n \leq k_n$ astfel încât

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

Proof. Inducție după n . Scriem $f = f_0 + f_1X_n + \dots + f_{k_n}X_n^{k_n}$ cu $f_i \in R[X_1, \dots, X_{n-1}]$ și aplicăm ipoteza de inducție.

Pentru unicitate fie

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

și să presupunem că $f = 0$. Scriem

$$f = f_0 + f_1X_n + \dots + f_{k_n}X_n^{k_n},$$

unde $f_j = \sum_{i_1=0}^{k_1} \cdots \sum_{i_{n-1}=0}^{k_{n-1}} a_{i_1, \dots, i_{n-1}, j} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}} \in R[X_1, \dots, X_{n-1}]$. Deoarece $f = 0$ rezultă $f_j = 0$ pentru orice $j = 0, 1, \dots, k_n$ și din ipoteza de inducție $a_{i_1, \dots, i_{n-1}, j} = 0$ pentru orice $j = 0, 1, \dots, k_n$. \square

Un polinom de forma $X_1^{i_1} \cdots X_n^{i_n}$ se va numi *monom în nedeterminatele* X_1, \dots, X_n iar *gradul* său se consideră a fi $i_1 + \cdots + i_n$. Așadar orice polinom $f \in R[X_1, \dots, X_n]$ este (în mod unic) o combinație liniară de monoame cu coeficienți în R . Polinoamele $a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}$ cu $a_{i_1, \dots, i_n} \neq 0$ se numesc *termeni* ai lui f , iar $a_{i_1, \dots, i_n} \neq 0$ *coeficienți*. Definim *gradul* lui f ca fiind maximul gradelor monoamelor care apar în scrierea sa. Dacă toate monoamele au același grad, atunci f se numește *polinom omogen*.

Remarca 3.4. Orice polinom se scrie în mod unic ca o sumă de polinoame omogene. Mai precis, dacă $f \in R[X_1, \dots, X_n]$, atunci $f = f_0 + f_1 + \cdots + f_t$ cu $f_i \in R[X_1, \dots, X_n]$ polinom omogen de grad i . În plus, $f = 0$ dacă și numai dacă $f_i = 0$ pentru orice $i = 0, 1, \dots, t$.

Propoziția 3.5. Fie $f, g \in R[X_1, \dots, X_n]$. Atunci:

- (i) $\deg(f + g) \leq \max(\deg f, \deg g)$.
- (ii) $\deg(fg) \leq \deg f + \deg g$.

Corolarul 3.6. Fie R un inel integru. Atunci $R[X_1, \dots, X_n]$ este, de asemenea, integru și $\deg(fg) = \deg f + \deg g$ pentru orice $f, g \in R[X_1, \dots, X_n]$.

Proof. Prima afirmație rezultă imediat prin inducție după $n \geq 1$. Pentru cea de-a doua vom scrie $f = f_0 + f_1 + \cdots + f_p$, respectiv $g = g_0 + g_1 + \cdots + g_q$ cu f_i, g_j polinoame omogene de grad i (respectiv, j). Presupunem că $f_p \neq 0$ și $g_q \neq 0$. De aici rezultă că $\deg f = p$ și $\deg g = q$. Cum însă $R[X_1, \dots, X_n]$ este inel integru vom avea $f_p g_q \neq 0$, deci $\deg(fg) = p + q$. \square

Corolarul 3.7. Fie R un inel integru. Atunci $U(R[X_1, \dots, X_n]) = U(R)$.

Reamintim că există un morfism canonic $\varepsilon : R \rightarrow R[X_1, \dots, X_n]$ dat prin $\varepsilon(a) = a$ pentru orice $a \in R$.

Teorema 3.8. (Proprietatea de universalitate a inelelor de polinoame într-un număr finit de nedeterminate) Fie $\varphi : R \rightarrow S$ un morfism de inele comutative unitare și $s_1, \dots, s_n \in S$. Atunci există un morfism unitar de inele $\bar{\varphi} : R[X_1, \dots, X_n] \rightarrow S$ unic cu proprietatea că $\bar{\varphi} \circ \varepsilon = \varphi$ și $\bar{\varphi}(X_i) = s_i$ pentru orice $i = 1, \dots, n$.

Proof. Să vizualizăm această proprietate cu ajutorul următoarei diagrame:

$$\begin{array}{ccc} R & \xrightarrow{\varepsilon} & R[X_1, \dots, X_n] \\ & \searrow \varphi & \downarrow \bar{\varphi} \\ & & S \end{array}$$

Procedăm prin inducție după n aplicând în mod repetat teorema 1.8. \square

Exercițiul 3.9. Fie R inel comutativ unitar și $\alpha_1, \dots, \alpha_n \in R$. Atunci avem următorul izomorfism: $R[X_1, \dots, X_n]/(X - \alpha_1, \dots, X - \alpha_n) \simeq R$.

4. POLINOAME SIMETRICE

Fie R un inel comutativ și unitar, $n \geq 2$ și $\sigma \in S_n$. Din teorema 3.8 rezultă că există un morfism unitar de inele $\bar{\sigma} : R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$ cu proprietatea că $\bar{\sigma} \circ \varepsilon = \varepsilon$ și $\bar{\sigma}(X_i) = X_{\sigma(i)}$ pentru orice $i = 1, \dots, n$.

Exemplul 4.1. Fie $f \in R[X_1, X_2, X_3]$, $f = X_1^2 X_3 + X_1 X_2 X_3^2$ și $\sigma = (1 \ 2 \ 3)$. Atunci $\bar{\sigma}(f) = X_1 X_2^2 + X_1^2 X_2 X_3$.

În general vom avea că $\bar{\sigma}(f(X_1, \dots, X_n)) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ pentru orice $f \in R[X_1, \dots, X_n]$.

Remarca 4.2. (i) Dacă $\sigma, \tau \in S_n$, atunci $\overline{\sigma \circ \tau} = \bar{\sigma} \circ \bar{\tau}$.

(ii) $\bar{e}(f) = f$ pentru orice $f \in R[X_1, \dots, X_n]$, unde $e \in S_n$ este permutarea identică.

(iii) $\bar{\sigma}$ este un izomorfism, iar $\bar{\sigma}^{-1} = \overline{\sigma^{-1}}$.

Definiția 4.3. Fie $f \in R[X_1, \dots, X_n]$. Dacă $\bar{\sigma}(f) = f$ pentru orice $\sigma \in S_n$, atunci f se numește polinom simetric.

Remarca 4.4. $f \in R[X_1, \dots, X_n]$ este polinom simetric dacă și numai dacă $\bar{\tau}(f) = f$ pentru orice transpoziție $\tau \in S_n$.

Exemplul 4.5. Polinomul $f \in R[X_1, X_2]$, $f = X_1^2 + X_2^2$ este simetric. Să observăm că dacă îl considerăm pe f ca polinom în $R[X_1, X_2, X_3]$, atunci acesta nu mai este simetric.

Propoziția 4.6. Mulțimea $\Sigma = \{f \in R[X_1, \dots, X_n] : f \text{ polinom simetric}\}$ este un subinel unitar al lui $R[X_1, \dots, X_n]$.

Proof. Rezultă din faptul că $\bar{\sigma}$ este morfism de inele pentru orice $\sigma \in S_n$. □

Propoziția 4.7. Polinoamele $s_k \in R[X_1, \dots, X_n]$ definite prin

$$s_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \cdots X_{i_k},$$

pentru orice $k = 1, \dots, n$, sunt polinoame simetrice.

Proof. Se consideră polinomul

$$g(T) = (T - X_1) \cdots (T - X_n),$$

$g \in R[X_1, \dots, X_n][T]$. Avem că

$$g(T) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n.$$

Fie $\sigma \in S_n$. Definim

$$\bar{\sigma} : R[X_1, \dots, X_n, T] \rightarrow R[X_1, \dots, X_n, T]$$

astfel: $\bar{\sigma}(X_i) = X_{\sigma(i)}$ pentru orice $i = 1, \dots, n$ și $\bar{\sigma}(T) = T$. Atunci

$$\bar{\sigma}(g) = (T - X_{\sigma(1)}) \cdots (T - X_{\sigma(n)}) = g.$$

Pe de altă parte,

$$\begin{aligned} \bar{\sigma}(g) &= \bar{\sigma}(T^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n) = \\ &= T^n - \bar{\sigma}(s_1) T^{n-1} + \bar{\sigma}(s_2) T^{n-2} - \cdots + (-1)^n \bar{\sigma}(s_n). \end{aligned}$$

De aici rezultă că $s_k = \bar{\sigma}(s_k)$ pentru orice $k = 1, \dots, n$, deci polinoamele s_k sunt simetrice. \square

Definiția 4.8. Polinoamele s_k , $k = 1, \dots, n$, definite mai sus se numesc polinoamele simetrice fundamentale în nedeterminatele X_1, \dots, X_n .

Definiția 4.9. Vom defini pe mulțimea monoamelor în n nedeterminate o relație de ordine astfel:

$$X_1^{i_1} \cdots X_n^{i_n} > X_1^{j_1} \cdots X_n^{j_n}$$

dacă există $s \in \{1, \dots, n\}$ cu proprietatea că $i_1 = j_1, \dots, i_{s-1} = j_{s-1}$ și $i_s > j_s$. Aceasta se va numi ordinea lexicografică.

Propoziția 4.10. Ordinea lexicografică este o relație de ordine totală pe mulțimea monoamelor.

Definiția 4.11. Fie $f \in R[X_1, \dots, X_n]$, $f \neq 0$ și fie $X_1^{i_1} \cdots X_n^{i_n}$ cel mai mare monom în ordinea lexicografică dintre cele care apar în scrierea lui f ca o combinație liniară de monoame. Acesta se numește monomul principal al lui f și se notează $\text{LM}(f)$. Dacă $a \in R$, $a \neq 0$ este coeficientul monomului principal al lui f , atunci a se numește coeficientul principal al lui f și se notează $\text{LC}(f)$ iar $aX_1^{i_1} \cdots X_n^{i_n}$ se numește termenul principal al lui f și se notează $\text{LT}(f)$.

În mod evident avem $\text{LT}(f) = \text{LC}(f) \text{LM}(f)$.

Exemplul 4.12. Fie $f \in \mathbb{Q}[X_1, X_2, X_3]$, $f = 2X_1^2X_2^2 + 3X_1X_2^3X_3 - X_1^2X_2X_3^5$. Atunci $\text{LM}(f) = X_1^2X_2^2$, $\text{LC}(f) = 2$ și $\text{LT}(f) = 2X_1^2X_2^2$.

Lema 4.13. Fie $m_1, m_2 \in R[X_1, \dots, X_n]$ monoame cu $m_1 > m_2$. Atunci:

- (i) $m_1m > m_2m$, oricare ar fi $m \in R[X_1, \dots, X_n]$ monom.
- (ii) Dacă $m'_1, m'_2 \in R[X_1, \dots, X_n]$ sunt monoame și $m'_1 > m'_2$, atunci $m_1m'_1 > m_2m'_2$.

Proof. (i) Fie $m_1 = X_1^{i_1} \cdots X_n^{i_n}$, $m_2 = X_1^{j_1} \cdots X_n^{j_n}$ și $m = X_1^{k_1} \cdots X_n^{k_n}$. Deoarece $m_1 > m_2$ există $s \in \{1, \dots, n\}$ cu proprietatea că $i_1 = j_1, \dots, i_{s-1} = j_{s-1}$ și $i_s > j_s$. Atunci $i_1 + k_1 = j_1 + k_1, \dots, i_{s-1} + k_{s-1} = j_{s-1} + k_{s-1}$ și $i_s + k_s > j_s + k_s$, deci $m_1m > m_2m$.

(ii) Rezultă din (i): $m_1 > m_2 \implies m_1m'_1 > m_2m'_1$ iar $m'_1 > m'_2 \implies m_2m'_1 > m_2m'_2$. \square

Propoziția 4.14. Fie $f_1, f_2 \in R[X_1, \dots, X_n]$ polinoame nenule. Dacă $\text{LT}(f_1) = a_1m_1$, $\text{LT}(f_2) = a_2m_2$ și $a_1a_2 \neq 0$, atunci $\text{LT}(f_1f_2) = (a_1a_2)m_1m_2 = \text{LT}(f_1)\text{LT}(f_2)$.

Proof. Rezultă din lema 4.13. \square

Lema 4.15. Fie $f \in R[X_1, \dots, X_n]$, $f \neq 0$ polinom simetric și $\text{LM}(f) = X_1^{i_1} \cdots X_n^{i_n}$. Atunci $i_1 \geq \dots \geq i_n$.

Proof. Să presupunem, de exemplu, că $i_1 < i_2$. Atunci

$$X_1^{i_2}X_2^{i_1} \cdots X_n^{i_n} > X_1^{i_1}X_2^{i_2} \cdots X_n^{i_n}.$$

Dar monomul $X_1^{i_2}X_2^{i_1} \cdots X_n^{i_n}$ apare cu certitudine în f , deoarece f este simetric și $\bar{\tau}(f) = f$, unde $\tau = (1\ 2)$. \square

Propoziția 4.16. *Orice șir strict descrescător de monoame $X_1^{i_1} \cdots X_n^{i_n}$ cu $i_1 \geq \cdots \geq i_n$ este finit.*

Proof. Reamintim că $X_1^{i_1} \cdots X_n^{i_n} > X_1^{j_1} \cdots X_n^{j_n}$ dacă există $s \in \{1, \dots, n\}$ cu proprietatea că $i_1 = j_1, \dots, i_{s-1} = j_{s-1}$ și $i_s > j_s$. Deoarece avem $j_1 \geq \cdots \geq j_n$ rezultă că $i_s > j_s \geq j_{s+1} \geq \cdots \geq j_n$, deci $i_1 \geq j_k$ pentru orice $k = 1, \dots, n$. Așadar numărul monoamelor $X_1^{j_1} \cdots X_n^{j_n}$ cu $j_1 \geq \cdots \geq j_n$ care sunt mai mici decât $X_1^{i_1} \cdots X_n^{i_n}$ este finit. \square

Exercițiul 4.17. Arătați că orice șir strict descrescător de monoame este finit.

Teorema 4.18. (Teorema fundamentală a polinoamelor simetrice) *Orice polinom simetric se scrie în mod unic ca polinom de polinoamele simetrice fundamentale.*

Proof. Mai precis, avem de demonstrat că oricare ar fi $f \in R[X_1, \dots, X_n]$ polinom simetric există și este unic un polinom $g \in R[X_1, \dots, X_n]$ astfel încât

$$f(X_1, \dots, X_n) = g(s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)).$$

Existența: Fie $\text{LT}(f) = aX_1^{i_1} \cdots X_n^{i_n}$. Deoarece f este simetric avem $i_1 \geq \cdots \geq i_n$. Mai mult, $\text{LT}(s_k) = X_1 \cdots X_k$ pentru orice $k = 1, \dots, n$. De aici se obține că

$$\text{LT}(as_1^{i_1-i_2} \cdots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n}) = \text{LT}(f).$$

Fie $f_1 = f - as_1^{i_1-i_2} \cdots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n}$. În mod evident f_1 este polinom simetric și, în plus, $\text{LM}(f_1) < \text{LM}(f)$.

Unicitatea: Vom demonstra că dacă $h \in R[X_1, \dots, X_n]$ și $h(s_1, \dots, s_n) = 0$, atunci $h = 0$. Scriem

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

și din $h(s_1, \dots, s_n) = 0$ obținem

$$\sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1, \dots, i_n} s_1^{i_1} \cdots s_n^{i_n} = 0.$$

Se remarcăm acum că

$$\text{LM}(s_1^{i_1} \cdots s_n^{i_n}) = X_1^{k_1} \cdots X_n^{k_n},$$

unde $k_1 = i_1 + \cdots + i_n, k_2 = i_2 + \cdots + i_n, \dots, k_n = i_n$.

Se observă că dacă $(i_1, \dots, i_n) \neq (j_1, \dots, j_n)$, atunci $(k_1, \dots, k_n) \neq (l_1, \dots, l_n)$, unde $k_r = i_r + \cdots + i_n$, respectiv $l_r = j_r + \cdots + j_n$ pentru orice $r = 1, \dots, n$. Aceasta înseamnă că $\text{LM}(s_1^{i_1} \cdots s_n^{i_n}) \neq \text{LT}(s_1^{j_1} \cdots s_n^{j_n})$ dacă $(i_1, \dots, i_n) \neq (j_1, \dots, j_n)$, deci $a_{i_1, \dots, i_n} = 0$ pentru orice i_1, \dots, i_n . \square

Exercițiul 4.19. Să se arate că următoarele polinoame sunt simetrice și să se scrie fiecare dintre ele ca polinom de polinoamele simetrice fundamentale:

- (i) $X_1^3 X_2 + X_1^3 X_3 + X_1 X_2^3 + X_1 X_3^3 + X_2^3 X_3 + X_2 X_3^3$.
- (ii) $(X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2)$.

În cele ce urmează vom nota $p_i = X_1^i + \cdots + X_n^i$, pentru orice $i \geq 1$. Evident, acestea sunt polinoame simetrice. În mod uzual definim $p_0 = n$.

Lema 4.20. Fie $f \in R[X_1, \dots, X_n]$ polinom simetric omogen de grad $k < n$. Dacă $f \neq 0$, atunci $f(X_1, \dots, X_k, 0, \dots, 0) \neq 0$.

Proof. Fie $\text{LM}(f) = X_1^{i_1} \cdots X_n^{i_n}$. 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 $\text{LM}(f) = X_1^{i_1} \cdots X_k^{i_k}$ și îl regăsim în $f(X_1, \dots, X_k, 0, \dots, 0)$. În concluzie, $f(X_1, \dots, X_k, 0, \dots, 0) \neq 0$. \square

Teorema 4.21. (Formulele lui Newton)

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

(ii) $p_k - p_{k-1}s_1 + \dots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k = 0$ pentru orice $k = 1, \dots, n-1$.

Proof. (i) Considerăm din nou polinomul $g \in R[X_1, \dots, X_n, T]$,

$$g(T) = (T - X_1) \cdots (T - X_n).$$

Avem că $g(T) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \dots + (-1)^n s_n$. Cum $g(X_i) = 0$ pentru orice $i = 1, \dots, n$ obținem

$$X_i^n - s_1 X_i^{n-1} + s_2 X_i^{n-2} - \dots + (-1)^n s_n = 0$$

pentru orice $i = 1, \dots, n$. Prin înmulțire cu X_i^{k-n} obținem

$$X_i^k - s_1 X_i^{k-1} + s_2 X_i^{k-2} - \dots + (-1)^n s_n X_i^{k-n} = 0$$

pentru orice $i = 1, \dots, n$. Adunăm aceste relații și obținem

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

(ii) Fie $f = p_k - p_{k-1}s_1 + \dots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k$, unde $k < n$. Acesta este polinom simetric omogen de grad k și

$$f(X_1, \dots, X_k, 0, \dots, 0) = p'_k - p'_{k-1}s'_1 + \dots + (-1)^{k-1} p'_1 s'_{k-1} + (-1)^k k s'_k,$$

unde p'_i, s'_j sunt polinoamele definite anterior, dar de data aceasta în nedeterminatele X_1, \dots, X_k . Din (i), cazul $k = n$, se obține $f(X_1, \dots, X_k, 0, \dots, 0) = 0$ și conform lemei 4.20, $f = 0$. \square

Exercițiul 4.22. (i) Să se calculeze $x_1^5 + x_2^5 + x_3^5$, unde x_1, x_2, x_3 sunt rădăcinile polinomului $X^3 - 3X + 1$.

(ii) Să se calculeze $x_1^3 + x_2^3 + x_3^3 + x_4^3$, unde x_1, x_2, x_3, x_4 sunt rădăcinile polinomului $X^4 + X^3 + 2X^2 + X + 1$.

Exercițiul 4.23. Considerăm elementele $x_1, \dots, x_n \in \mathbb{C}$ cu proprietatea că $x_1^k + \dots + x_n^k = 0$ pentru orice $1 \leq k \leq n$. Să se arate că $x_1 = \dots = x_n = 0$.

Exercițiul 4.24. Să se rezolve în numere reale ecuația $\sqrt[4]{97-x} + \sqrt[4]{x} = 5$.

Exercițiul 4.25. Să se rezolve în numere reale sistemul de ecuații

$$\begin{cases} x^5 + y^5 = 33 \\ x + y = 3 \end{cases}$$