INELE DE POLINOAME

Pe parcursul acestui capitol inelele vor fi comutative şi unitare iar morfismele de inele vor fi unitare.

1. Inele de polinoame într-o nedeterminată

Fie R un inel comutativ şi unitar. Notăm cu $R^{(\mathbb{N})}$ mulţimea şirurilor $(a_n)_{n\in\mathbb{N}}$ cu elemente din R şi care au doar un număr finit de termeni nenuli. Pe $R^{(\mathbb{N})}$ definim două operaţii 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 $c_n = \sum_{i+j=n} a_i b_j$.

Propoziţia 1.1. $(R^{(\mathbb{N})}, +, \cdot)$ *este inel comutativ şi unitar.*

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

$$X^n = (\underbrace{0, \dots, 0}_{n \text{ termeni}}, 1, 0, 0, \dots)$$

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

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

Definiţia 1.2. *Inelul $R^{(\mathbb{N})}$ se notează cu $R[X]$ şi se numeşte* inelul polinoamelor în nedeterminata X cu coeficienţi în R.

Dacă $f \in R[X]$, atunci $f = a_0 + a_1X + \dots + a_nX^n$, $a_i \in R$ şi f se numeşte *polinom în nedeterminata X*. Polinoamele X^n, $n \in \mathbb{N}$ se numesc *monoame în nedeterminata X*. Aşadar orice polinom este în mod unic o combinaţie liniară de monoame cu coeficienţi în R. Polinoamele a_iX^i cu $a_i \neq 0$ se numesc *termeni* ai lui f, iar $a_i \neq 0$ *coeficienţi*. Definim $\deg f = \max\{i : a_i \neq 0\}$ şi-l numim *gradul* lui f. Dacă $n = \deg f$, atunci a_n se numeşte *coeficientul dominant* al lui f. Polinoamele al căror coeficient dominant este 1 se numesc polinoame *monice*.

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

Propoziţia 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 şi numai dacă produsul coeficienţilor dominanţi ai lui f şi 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 $R = \mathbb{Z}/4\mathbb{Z}$ şi $f = \widehat{1} + \widehat{2}X \in R[X]$. Avem $f^2 = \widehat{1}$, deci $f \in U(R[X])$, dar $f \notin U(R)$.

Exerciţiul 1.7. Fie R un inel comutativ unitar şi $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Să se arate că:
(i) f este nilpotent dacă şi numai dacă a_i este nilpotent pentru orice $0 \leq i \leq n$.
(ii) f este inversabil dacă şi numai dacă a_0 este inversabil şi a_i este nilpotent pentru orice $1 \leq i \leq n$.

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

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

Proof. Să vizualizăm această proprietate cu ajutorul următoarei diagrame:

$$\begin{tikzcd} R \arrow[r, "\varepsilon"] \arrow[dr, "\varphi"'] & R[X] \arrow[d, dotted, "\overline{\varphi}"] \\ & S \end{tikzcd}$$

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

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

$$\begin{tikzcd} R \arrow[r, "\varepsilon"] \arrow[dr, hook, "i"'] & R[X] \arrow[d, dotted, "\overline{i}_s"] \\ & S \end{tikzcd}$$

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

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

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

Definiţia 1.10. *Funcţia $\widetilde{f} : S \to S$ definită mai sus se numeşte* funcţia polinomială pe S asociată lui f. *Când $S = R$, funcţia $\widetilde{f} : R \to R$ se numeşte* funcţia polinomială asociată lui f.

Remarca 1.11. Polinoame diferite pot avea funcţii polinomiale egale. De exemplu, $f, g \in \mathbb{Z}_2[X]$, $f = X$ şi $g = X^2$. Avem că $\widetilde{f}, \widetilde{g} : \mathbb{Z}_2 \to \mathbb{Z}_2$, $\widetilde{f}(\widehat{0}) = \widetilde{g}(\widehat{0}) = \widehat{0}$ şi $\widetilde{f}(\widehat{1}) = \widetilde{g}(\widehat{1}) = \widehat{1}$.

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 împărţire cu rest pentru polinoame într-o nedeterminată

Teorema 2.1. (Teorema de împărţire 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 $f = gq + r$ şi $\deg r < \deg g$.*

Proof. Dacă $\deg f < \deg g$, atunci scriem $f = g \cdot 0 + f$. În cazul în care $\deg f \geq \deg g$ facem inducţie după $\deg f$.
Unicitatea rezultă imediat folosind Propoziţia 1.3(ii). □

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

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

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

Exerciţiul 2.5. Arătaţi că:
(i) $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.
(ii) $\mathbb{Z}[X]/(X^2 - 2) \simeq \mathbb{Z}[\sqrt{2}]$.

Exerciţiul 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 $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exerciţiul 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 şi că $\mathbb{Z}[X]/I$ nu este inel integru.

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

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

Proof. Fie $\alpha_1, \ldots, \alpha_m \in R$ distincte cu proprietatea că $f(\alpha_i) = 0$ pentru orice $i = 1, \ldots, m$. Vom demonstra prin inducţie 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 inducţie $(X - \alpha_1) \cdots (X - \alpha_{m-1}) \mid f$ şi putem scrie $f = (X - \alpha_1) \cdots (X - \alpha_{m-1}) g$ cu $g \in R[X]$. Din $f(\alpha_m) = 0$ obţinem $(\alpha_m - \alpha_1) \cdots (\alpha_m - \alpha_{m-1}) g(\alpha_m) = 0$. Dar cum R este integru şi $\alpha_i \neq \alpha_m$ pentru orice $i \neq m$ rezultă $g(\alpha_m) = 0$ şi din corolarul 2.3 deducem că $X - \alpha_m \mid g$.
În concluzie, $n = \deg f \geq m$. □

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 şase rădăcini distincte în $\mathbb{Z}_6$.

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

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

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

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

Proof. Arătăm prin inducţie după n că $f = a_n(X - \alpha_1)\cdots(X - \alpha_n)$ şi apoi identificăm coeficienţii. □

3. Inele de polinoame într-un număr finit de nedeterminate

Definiţia 3.1. *Fie R un inel. Atunci* inelul de polinoame în nedeterminatele $X_1, \dots, X_n$ cu coeficienţi în R *se defineşte inductiv ca fiind* $R[X_1, \dots, X_{n-1}][X_n]$ *şi 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

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

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

Propoziţia 3.3. *Pentru orice polinom $f \in R[X_1, \dots, X_n]$ există şi sunt unice $k_1, \dots, k_n \in \mathbb{N}$ şi $a_{i_1,\dots,i_n} \in R$, unde $0 \le i_1 \le k_1, \dots, 0 \le i_n \le k_n$ 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. Inducţie după n. Scriem $f = f_0 + f_1X_n + \cdots + f_{k_n}X_n^{k_n}$ cu $f_i \in R[X_1, \dots, X_{n-1}]$ şi aplicăm ipoteza de inducţie.
Pentru unicitate fie

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

şi să presupunem că $f = 0$. Scriem

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

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

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

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

Propoziţia 3.5. *Fie* $f, g \in R[X_1, \ldots, X_n]$. *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* $R[X_1, \ldots, X_n]$ *este, de asemenea, integru şi* $\deg(fg) = \deg f + \deg g$ *pentru orice* $f, g \in R[X_1, \ldots, X_n]$.

Proof. Prima afirmaţie rezultă imediat prin inducţie 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 $f_p \neq 0$ şi $g_q \neq 0$. De aici rezultă că $\deg f = p$ şi $\deg g = q$. Cum însă $R[X_1, \ldots, X_n]$ este inel integru vom avea $f_p g_q \neq 0$, deci $\deg(fg) = p + q$. □

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

Reamintim că există un morfism canonic $\varepsilon : R \to R[X_1, \ldots, X_n]$ 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* $\varphi : R \to S$ *un morfism de inele comutative unitare şi* $s_1, \ldots, s_n \in S$. *Atunci există un morfism unitar de inele* $\overline{\varphi} : R[X_1, \ldots, X_n] \to S$ *unic cu proprietatea că* $\overline{\varphi} \circ \varepsilon = \varphi$ *şi* $\overline{\varphi}(X_i) = s_i$ *pentru orice* $i = 1, \ldots, n$.

Proof. Să vizualizăm această proprietate cu ajutorul următoarei diagrame:

$$\begin{tikzcd} R \arrow[r, "\varepsilon"] \arrow[dr, "\varphi"'] & R[X_1, \ldots, X_n] \arrow[d, dotted, "\overline{\varphi}"] \\ & S \end{tikzcd}$$

Procedăm prin inducţie după n aplicând în mod repetat teorema 1.8. □

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

4. Polinoame simetrice

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

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

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

Remarca 4.2. (i) Dacă $\sigma, \tau \in S_n$, atunci $\overline{\sigma \circ \tau} = \overline{\sigma} \circ \overline{\tau}$.
(ii) $\overline{e}(f) = f$ pentru orice $f \in R[X_1, \dots, X_n]$, unde $e \in S_n$ este permutarea identică.
(iii) $\overline{\sigma}$ este un izomorfism, iar $\overline{\sigma}^{-1} = \overline{\sigma^{-1}}$.

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

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

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.

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

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

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

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

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

$$\overline{\sigma} : R[X_1, \dots, X_n, T] \to R[X_1, \dots, X_n, T]$$

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

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

Pe de altă parte,

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

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

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

Definiţia 4.9. *Vom defini pe mulţimea monoamelor în n nedeterminate o relaţie de ordine astfel:*

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

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

Propoziţia 4.10. *Ordinea lexicografică este o relaţie de ordine totală pe mulţimea monoamelor.*

Definiţia 4.11. *Fie $f \in R[X_1, \ldots, X_n]$, $f \neq 0$ şi 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 combinaţie liniară de monoame. Acesta se numeşte* monomul principal al lui f *şi se notează* $\mathrm{LM}(f)$. *Dacă $a \in R$, $a \neq 0$ este coeficientul monomului principal al lui f, atunci a se numeşte* coeficientul principal al lui f *şi se notează* $\mathrm{LC}(f)$ *iar* $aX_1^{i_1} \cdots X_n^{i_n}$ *se numeşte* termenul principal al lui f *şi se notează* $\mathrm{LT}(f)$.

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

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 $\mathrm{LM}(f) = X_1^2X_2^2$, $\mathrm{LC}(f) = 2$ şi $\mathrm{LT}(f) = 2X_1^2X_2^2$.

Lema 4.13. *Fie $m_1, m_2 \in R[X_1, \ldots, X_n]$ monoame cu $m_1 > m_2$. Atunci:*
(i) $m_1m > m_2m$, oricare ar fi $m \in R[X_1, \ldots, X_n]$ monom.
(ii) Dacă $m_1', m_2' \in R[X_1, \ldots, X_n]$ sunt monoame şi $m_1' > m_2'$, atunci $m_1m_1' > m_2m_2'$.

Proof. (i) Fie $m_1 = X_1^{i_1} \cdots X_n^{i_n}$, $m_2 = X_1^{j_1} \cdots X_n^{j_n}$ şi $m = X_1^{k_1} \cdots X_n^{k_n}$. Deoarece $m_1 > m_2$ există $s \in \{1, \ldots, n\}$ cu proprietatea că $i_1 = j_1, \ldots, i_{s-1} = j_{s-1}$ şi $i_s > j_s$. Atunci $i_1 + k_1 = j_1 + k_1, \ldots, i_{s-1} + k_{s-1} = j_{s-1} + k_{s-1}$ şi $i_s + k_s > j_s + k_s$, deci $m_1m > m_2m$.
(ii) Rezultă din (i): $m_1 > m_2 \implies m_1m_1' > m_2m_1'$ iar $m_1' > m_2' \implies m_2m_1' > m_2m_2'$. $\square$

Propoziţia 4.14. *Fie $f_1, f_2 \in R[X_1, \ldots, X_n]$ polinoame nenule. Dacă* $\mathrm{LT}(f_1) = a_1m_1$, $\mathrm{LT}(f_2) = a_2m_2$ *şi* $a_1a_2 \neq 0$, *atunci* $\mathrm{LT}(f_1f_2) = (a_1a_2)m_1m_2 = \mathrm{LT}(f_1)\,\mathrm{LT}(f_2)$.

Proof. Rezultă din lema 4.13. $\square$

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

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 şi $\overline{\tau}(f) = f$, unde $\tau = (1\ 2)$. $\square$

Propoziţia 4.16. *Orice şir 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 $i_1 = j_1, \dots, i_{s-1} = j_{s-1}$ şi $i_s > j_s$. 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 $k = 1,\dots,n$. Aşadar 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. □

Exerciţiul 4.17. Arătaţi că orice şir 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 şi este unic un polinom $g \in R[X_1,\dots,X_n]$ astfel încât

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

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

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

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 şi, în plus, $\mathrm{LM}(f_1) < \mathrm{LM}(f)$.
Unicitatea: Vom demonstra că dacă $h \in R[X_1,\dots,X_n]$ şi $h(s_1,\dots,s_n) = 0$, atunci $h = 0$. Scriem

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

şi din $h(s_1,\dots,s_n) = 0$ obţinem

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

Se remarcăm acum că

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

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 $\mathrm{LM}(s_1^{i_1}\cdots s_n^{i_n}) \neq \mathrm{LT}(s_1^{j_1}\cdots s_n^{j_n})$ dacă $(i_1,\dots,i_n) \neq (j_1,\dots,j_n)$, deci $a_{i_1,\dots,i_n} = 0$ pentru orice $i_1,\dots,i_n$. □

Exerciţiul 4.19. Să se arate că următoarele polinoame sunt simetrice şi să se scrie fiecare dintre ele ca polinom de polinoamele simetrice fundamentale:
(i) $X_1^3X_2 + X_1^3X_3 + X_1X_2^3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3$.
(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 $f \in R[X_1, \ldots, X_n]$ polinom simetric omogen de grad $k < n$. Dacă $f \neq 0$, atunci $f(X_1, \ldots, X_k, 0, \ldots, 0) \neq 0$.*

Proof. Fie $\mathrm{LM}(f) = X_1^{i_1} \cdots X_n^{i_n}$. Avem $i_1 \geq \cdots \geq i_n$ şi $i_1 + \cdots + i_n = k$. Deoarece $k < n$ rezultă $i_{k+1} = \cdots = i_n = 0$. Deci $\mathrm{LM}(f) = X_1^{i_1} \cdots X_k^{i_k}$ şi îl regăsim în $f(X_1, \ldots, X_k, 0, \ldots, 0)$. În concluzie, $f(X_1, \ldots, X_k, 0, \ldots, 0) \neq 0$. □

Teorema 4.21. (Formulele lui Newton)
(i) $p_k - p_{k-1}s_1 + \cdots + (-1)^n p_{k-n}s_n = 0$ pentru orice $k \geq n$.
(ii) $p_k - p_{k-1}s_1 + \cdots + (-1)^{k-1}p_1 s_{k-1} + (-1)^k k s_k = 0$ pentru orice $k = 1, \ldots, n-1$.

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

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

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

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

pentru orice $i = 1, \ldots, n$. Prin înmulţire cu X_i^{k-n} obţinem

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

pentru orice $i = 1, \ldots, n$. Adunăm aceste relaţii şi obţinem

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

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

$$f(X_1, \ldots, X_k, 0, \ldots, 0) = p_k' - p_{k-1}' s_1' + \cdots + (-1)^{k-1} p_1' s_{k-1}' + (-1)^k k s_k',$$

unde p_i', s_j' sunt polinoamele definite anterior, dar de data aceasta în nedeterminatele $X_1, \ldots, X_k$. Din (i), cazul $k = n$, se obţine $f(X_1, \ldots, X_k, 0, \ldots, 0) = 0$ şi conform lemei 4.20, $f = 0$. □

Exerciţiul 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 $X^4 + X^3 + 2X^2 + X + 1$.

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

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

Exerciţiul 4.25. Să se rezolve în numere reale sistemul de ecuaţii

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