INELE DE POLINOAME

1. Inele de polinoame într-o nedeterminată

Fie R un inel 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 unitar. Dacă, în plus, R este comutativ, atunci şi* $(R^{(\mathbb{N})}, +, \cdot)$ *este comutativ.*

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.

Remarca 1.3. (i) Să observăm că deşi R nu este neapărat inel comutativ avem totuşi o proprietate de comutare în $R[X]$, care rezultă din modul în care a fost construit acesta: $aX = Xa$ pentru orice $a \in R$.
(ii) $a_0 + a_1X + \dots + a_nX^n = 0$ dacă şi numai dacă $a_0 = a_1 = \dots = a_n = 0$.

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 1.4. *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 1.5. *Fie R un inel unitar 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 1.6. *Fie R un inel unitar integru. Atunci* $U(R[X]) = U(R)$.

Remarca 1.7. 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 1.8. 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 $1 \leq i \leq n$.
(iii) f este divizor al lui zero dacă şi numai dacă există $a \in R$, $a \neq 0$, cu $af = 0$.
(iv) f este idempotent dacă şi numai dacă $f = a_0$ şi $a_0^2 = a_0$.
*(v) Daţi exemple din care să reiasă că proprietăţile (i)–(iv) nu mai sunt adevărate în cazul în care R este inel necomutativ.

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 1.9. (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 $a \in R$. $\square$

Remarca 1.10. (i) Proprietatea de universalitate a inelelor de polinoame nu are loc în cazul în care inelul este necomutativ.
De exemplu, funcţia $\psi : \mathbb{H}[X] \to \mathbb{H}$ definită prin $\psi(f) = f(\mathbf{j})$ nu este morfism de inele: avem $(X + \mathbf{i})(X - \mathbf{i}) = X^2 + 1$, dar $\psi(X + \mathbf{i})\psi(X - \mathbf{i}) = 2\mathbf{k} \neq 0 = \psi(X^2 + 1)$.
(ii) Avem totuşi o proprietate de universalitate şi în cazul în care inelele sunt necomutative, dar cu condiţia ca $s \in C(S)$.

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 $\overline{i}_s(X) = s$.

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

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 1.11. *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 1.12. *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 1.13. 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 unitar, $f, g \in R[X]$, $g \neq 0$ 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 1.4(ii). $\square$

Remarca 2.2. Analog se arată că există $q', r' \in R[X]$ unice cu proprietatea că $f = q'g + r'$ şi $\deg r' < \deg g$.

Corolarul 2.3. *Fie R un inel unitar, $f \in R[X]$ şi $\alpha \in R$. Atunci există $q \in R[X]$ şi $r \in R$ unice cu proprietatea că $f = (X - \alpha)q + r$.*

Remarca 2.4. (i) În mod similar avem că există $q' \in R[X]$ şi $r' \in R$ unice cu proprietatea că $f = q'(X - \alpha) + r'$.
(ii) De fapt, dacă $f = a_0 + a_1X + \cdots + a_nX^n$, atunci $r = a_0 + \alpha a_1 + \cdots + \alpha^n a_n$ iar $r' = a_0 + a_1\alpha + \cdots + a_n\alpha^n$.

Exemplul 2.5. Nu este însă necesar ca $q' = q$ şi $r' = r$. Să considerăm de exemplu $R = \mathbb{H}$ şi $\alpha = \mathbf{j}$. Avem

$$\mathbf{i}X^2 + \mathbf{i}X = (\mathbf{i}X + \mathbf{k} + \mathbf{i})(X - \mathbf{j}) + \mathbf{k} - \mathbf{i} = (X - \mathbf{j})(\mathbf{i}X - \mathbf{k} + \mathbf{i}) - \mathbf{k} - \mathbf{i}$$

Corolarul 2.6. *Fie R un inel unitar, $f \in R[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$ şi $\alpha \in R$. Atunci următoarele condiţii sunt echivalente:*
(i) Există $q \in R[X]$ cu proprietatea că $f = (X - \alpha)q$;
(ii) $a_0 + \alpha a_1 + \cdots + \alpha^n a_n = 0$.

Remarca 2.7. În mod similar avem că există $q' \in R[X]$ cu proprietatea că $f = q'(X - \alpha)$ dacă şi numai dacă $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$.

Corolarul 2.8. (Bézout) *Fie R un inel comutativ unitar, $f \in R[X]$ şi $\alpha \in R$. Atunci $X - \alpha \mid f$ dacă şi numai dacă $f(\alpha) = 0$.*

Remarca 2.9. Dacă R nu este comutativ, atunci este posibil ca $X - \alpha$ să dividă pe f la dreapta, dar nu şi la stânga:

$$X^2 + (\mathbf{i} - \mathbf{j})X - \mathbf{k} = (X + \mathbf{i})(X - \mathbf{j}) + 0 = (X - \mathbf{j})(X + \mathbf{i}) + (-2\mathbf{k}).$$

Exerciţiul 2.10. Fie R inel comutativ unitar şi $\alpha \in R$. Atunci $R[X]/(X - \alpha) \simeq R$.

Exerciţiul 2.11. 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 2.12. 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 2.13. 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.

Propoziţia 2.14. *Fie R un inel comutativ unitar 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 2.8. 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 2.8 deducem că $X - \alpha_m \mid g$.
În concluzie, $n = \deg f \geq m$. □

Remarca 2.15. (i) 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 $\mathbb{Z}_6$.
(ii) Dacă inelul nu este comutativ, atunci proprietatea de mai sus este falsă. De exemplu, polinomul $f \in \mathbb{H}[X]$, $f = X^2 + 1$ admite pe $\pm\mathbf{i}$, $\pm\mathbf{j}$, $\pm\mathbf{k}$ ca "rădăcini".

Corolarul 2.16. *Fie R un inel comutativ unitar 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 2.14 rezultă $h = 0$. □

Propoziţia 2.17. (Relaţiile lui Viète) *Fie R un inel comutativ unitar integru, $f \in R[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$, $a_n \neq 0$. Presupunem că f are n rădăcini $\alpha_1, \ldots, \alpha_n \in R$. Atunci au loc relaţiile:*

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}$$

$$\sum_{1\leq i<j\leq n}^{n} \alpha_i\alpha_j = \frac{a_{n-2}}{a_n}$$

$$\cdots\cdots\cdots$$

$$\prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$$

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 unitar. Atunci* inelul de polinoame în nedeterminatele $X_1, \ldots, X_n$ cu coeficienţi în R *se defineşte inductiv ca fiind $R[X_1, \ldots, X_{n-1}][X_n]$ şi se notează $R[X_1, \ldots, X_n]$. Elementele inelului $R[X_1, \ldots, X_n]$ se numesc* polinoame în nedeterminatele $X_1, \ldots, X_n$..

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

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

cu $f_i \in R[X_1, \ldots, X_{n-1}]$ pentru orice $i = 0, 1, \ldots, r$.
(ii) Din modul în care a fost construit inelul de polinoame $R[X_1, \ldots, X_n]$ avem că $aX_i = X_ia$ şi $X_iX_j = X_jX_i$ pentru orice $a \in R$ şi pentru orice $i, j = 1, \ldots, n$.

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

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

Proof. Inducţie după n. Scriem $f = f_0 + f_1X_n + \cdots + f_{k_n}X_n^{k_n}$ cu $f_i \in R[X_1, \ldots, X_{n-1}]$ şi aplicăm ipoteza de inducţie.
Pentru unicitate fie

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

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 unitar 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 unitar 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 1.9. □

Remarca 3.9. Putem defini inele de polinoame şi într-o infinitate de nedeterminate. Deoarece $R \subset R[X_1] \subset R[X_1, X_2] \subset \cdots \subset R[X_1, \ldots, X_n] \subset \cdots$ este un şir crescător de inele, reuniunea lor $\bigcup_{n \geq 1} R[X_1, \ldots, X_n]$ este un inel notat $R[X_1, \ldots, X_n, \ldots]$ şi care se numeşte *inelul de polinoame în nedeterminatele* $X_1, \ldots, X_n, \ldots$ *cu coeficienţi în* R.

3.1. **Funcţii polinomiale. Zerouri.** Fie S un inel comutativ şi unitar, $R \subseteq S$ un subinel şi $i : R \to S$ morfismul incluziune. Fie $\mathbf{s} = (s_1, \dots, s_n) \in S^n$. Din proprietatea de universalitate a inelelor de polinoame într-un număr finit de nedeterminate există un morfism unitar $\bar{i}_\mathbf{s} : R[X_1, \dots, X_n] \to S$ unic cu proprietatea că $\bar{i}_\mathbf{s} \circ \varepsilon = i$ şi $\bar{i}_\mathbf{s}(X_i) = s_i$ pentru orice $i = 1, \dots, n$. Aşadar

$$\bar{i}_\mathbf{s}(\sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}) = \sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1,\dots,i_n} s_1^{i_1} \cdots s_n^{i_n}.$$

Dacă $f \in R[X_1, \dots, X_n]$, $f = \sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}$, atunci notăm $\sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1,\dots,i_n} s_1^{i_1} \cdots s_n^{i_n}$ cu $f(s_1, \dots, s_n)$ şi avem $\bar{i}_\mathbf{s}(f) = f(s_1, \dots, s_n)$.

Definiţia 3.10. *Un element $(s_1, \dots, s_n) \in S^n$ cu proprietatea că $f(s_1, \dots, s_n) = 0$ se numeşte* zero al lui f.

Pentru orice polinom $f \in R[X_1, \dots, X_n]$ putem defini o funcţie $\widetilde{f} : S^n \to S$ prin $\widetilde{f}(s_1, \dots, s_n) = f(s_1, \dots, s_n)$ pentru orice $(s_1, \dots, s_n) \in S^n$.

Definiţia 3.11. *Funcţia $\widetilde{f} : S^n \to S$ definită mai sus se numeşte* funcţia polinomială pe S^n asociată lui f. *Când $S = R$, funcţia $\widetilde{f} : R^n \to R$ se numeşte* funcţia polinomială asociată lui f.

Stim deja că polinoame diferite pot avea funcţii polinomiale egale. De asemenea, nu este adevărat că un polinom de mai multe nedeterminate cu coeficienţi într-un un inel comutativ unitar integru are un număr finit de zerouri distincte. De exemplu, polinomul $f = XY \in \mathbb{Q}[X, Y]$ are o infinitate de zerouri, orice pereche de forma $(0, q)$ (respectiv, $(q, 0)$) cu $q \in \mathbb{Q}$ fiind un zero al lui f.

Rămâne totuşi adevărat următorul rezultat, analog celui obţinut în corolarul 2.16.

Propoziţia 3.12. *Fie R un inel comutativ unitar integru infinit, $n \geq 1$ şi $f, g \in R[X_1, \dots, X_n]$. 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 $\alpha \in R^n$. Vom arăta că $h = 0$.

Procedăm prin inducţie după n. Dacă $n = 1$, atunci $h = 0$ din corolarul 2.16. Presupunem adevărat pentru $n - 1$ şi demonstrăm pentru n. Scriem

$$h(X_1, \dots, X_n) = \sum_{i=0}^{m} h_i(X_1, \dots, X_{n-1}) X_n^i,$$

unde $h_i(X_1, \dots, X_{n-1}) \in R[X_1, \dots, X_{n-1}]$ pentru orice $0 \leq i \leq m$. Rezultă că pentru orice $(\alpha_1, \dots, \alpha_{n-1}) \in R^{n-1}$, funcţia polinomială asociată polinomului

$$h(\alpha_1, \dots, \alpha_{n-1}, X_n) = \sum_{i=0}^{m} \widetilde{h}_i(\alpha_1, \dots, \alpha_{n-1}) X_n^i \in R[X_n]$$

se anulează pentru orice $\alpha_n \in R$. Cum R este infinit, din corolarul 2.16 rezultă că polinomul $h(a_1, \dots, a_{n-1}, X_n)$ este nul, deci $\widetilde{h}_i(\alpha_1, \dots, \alpha_{n-1}) = 0$ pentru orice $0 \leq i \leq m$. Din ipoteza de inducţie rezultă că $h_i(X_1, \dots, X_{n-1}) = 0$ pentru orice $0 \leq i \leq m$, deci $h = 0$. $\square$