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 $(a_0, a_1, \dots, a_n, 0, 0, \dots) = \varepsilon(a_0) + \varepsilon(a_1)X + \cdots + \varepsilon(a_n)X^n$ iar prin identificarea lui R cu un subinel al lui $R^{(\mathbb{N})}$ dată de ε putem scrie

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

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 $f = a_0 + a_1X + \cdots + a_nX^n$, $a_i \in R$ 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 $a \in R$. $\square$

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 $h = 0$. $\square$

Propoziţia 2.12. (Relaţiile lui Viète) *Fie R un inel integru, $f \in R[X]$, $f = a_0 + a_1 X + \cdots + a_n X^n$, $a_n \neq 0$. 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. $\square$