CURS 3

Inelul polinoamelor cu coeficienţi într-un corp comutativ

Fie $(K, +, \cdot)$ un corp comutativ. Fie $K^{\mathbb{N}}$ mulţimea şirurilor cu termenii din K, adică

$$K^{\mathbb{N}} = \{f \mid f : \mathbb{N} \to K\}.$$

Dacă $f : \mathbb{N} \to K$ atunci notând $f(n) = a_n$ scriem

$$f = (a_0, a_1, a_2, \dots).$$

Pentru $f = (a_0, a_1, a_2, \dots),\ g = (b_0, b_1, b_2, \dots) \in K^{\mathbb{N}}$ se definesc:

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) \tag{1}$$

$$f \cdot g = (c_0, c_1, c_2, \dots) \tag{2}$$

unde

$$\begin{aligned}
&c_0 = a_0 b_0,\\
&c_1 = a_0 b_1 + a_1 b_0,\\
&\vdots\\
&c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = \sum_{i+j=n} a_i b_j,\\
&\vdots
\end{aligned}$$

Teorema 1. $K^{\mathbb{N}}$ formează în raport cu operaţiile definite în (1) şi (2) un inel comutativ şi cu unitate numit **inelul seriilor formale** cu coeficienţi din K.

Demonstraţie. TEMĂ

□

Fie $f = (a_0, a_1, a_2, \dots) \in K^{\mathbb{N}}$. Se numeşte **suportul lui** f submulţimea lui $\mathbb{N}$

$$supp\, f = \{k \in \mathbb{N} \mid a_k \neq 0\}.$$

Notăm cu $K^{(\mathbb{N})}$ submulţimea lui $K^{\mathbb{N}}$ formată din şirurile de **suport finit**. Deci

$$f \in K^{(\mathbb{N})} \Leftrightarrow \exists\ n \in \mathbb{N} \text{ astfel încât } a_i = 0 \text{ pentru } i \geq n \Leftrightarrow f = (a_0, a_1, a_2, \dots, a_{n-1}, 0, 0, \dots).$$

Teorema 2. i) $K^{(\mathbb{N})}$ este un subinel al lui $K^{\mathbb{N}}$ ce conţine unitatea.
ii) Funcţia $\varphi : K \to K^{(\mathbb{N})},\ \varphi(a) = (a, 0, 0, \dots)$ este un omomorfism unital injectiv de inele.

Demonstraţie.

□

Inelul $(K^{(\mathbb{N})}, +, \cdot)$ se numeşte **inelul polinoamelor** cu coeficienţi din K. Cum ajunge el să ,,arate" aşa cum îl ştim din liceu?

Omomorfismul injectiv φ ne permite să identificăm elementul $a \in K$ cu polinomul $(a, 0, 0, \dots)$. După această identificare K devine subinel al inelului $K^{(\mathbb{N})}$. Polinomul

$$X = (0, 1, 0, 0, \dots)$$

se numeşte **nedeterminată** peste K. Din (2) rezultă:

$$\begin{aligned} X^2 &= (0, 0, 1, 0, 0, \dots) \\ X^3 &= (0, 0, 0, 1, 0, 0, \dots) \\ &\vdots \\ X^m &= (\underbrace{0, 0, \dots, 0}_{m\ ori}, 1, 0, 0, \dots) \\ &\vdots \end{aligned}$$

Identificând pe $a \in K$ cu $(a, 0, 0, \dots)$, din (2) urmează

$$aX^m = (\underbrace{0, 0, \dots, 0}_{m\ ori}, a, 0, 0, \dots) \tag{3}$$

şi astfel,

Teorema 3. Orice $f \in K^{(\mathbb{N})}$ nenul se scrie în mod unic sub forma

$$f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \tag{4}$$

numită **forma algebrică** a lui f, unde $a_i \in K$, $i \in \{0, 1, \dots, n\}$ cu $a_n \neq 0$.

Acum putem rescrie

$$K^{(\mathbb{N})} = \{f = a_0 + a_1X + \cdots + a_nX^n \mid a_0, a_1, \dots, a_n \in K,\ n \in \mathbb{N}\} \overset{not}{=} K[X].$$

Pentru un element al acestei mulţimi folosim şi numele **polinom cu coeficienţi din K în nedeterminata X**, iar pentru $K[X]$ mulţimea sau inelul polinoamelor cu coeficienţi în corpul K în nedeterminata X. De asemenea, putem rescrie operaţiile din inelul $(K[X], +, \cdot)$ aşa cum le ştim din liceu (la seminar).

Dacă $f \in K[X]$, $f \neq 0$ şi f are reprezentarea (4), atunci n se numeşte **gradul lui f**, iar dacă $f = 0$ atunci se spune că f are gradul $-\infty$. Gradul lui f îl vom nota cu $grad\, f$. Rezultă că

$$grad\, f = 0 \Leftrightarrow f \in R^*.$$

Luăm prin definiţie

$$-\infty + m = m + (-\infty) = -\infty,\ -\infty + (-\infty) = -\infty,\ -\infty < m,\ \forall\, m \in \mathbb{N}.$$

Au loc următoarele:
i) $grad\,(f + g) \leq \max\{grad\, f, grad\, g\}, \forall f, g \in K[X]$;

ii) $grad\,(fg) = grad\,f + grad\,g, \forall f, g \in K[X]$;
iii) $K[X]$ este domeniu de integritate (la seminar);
iv) un polinom $f \in K[X]$ este inversabil în $K[X]$ dacă şi numai dacă $f \in K^*$ (la seminar).

Câteva noţiuni şi proprietăţi utile referitor la polinoame:
Dacă $f, g \in K[X]$ atunci

$$f \mid g \Leftrightarrow \exists\ h \in R,\ g = fh.$$

Relaţia de divizibilitate $\mid$ este o relaţie reflexivă şi tranzitivă în $K[X]$. Polinomul nul se comportă faţă de aceste relaţii astfel:

$$f \mid 0,\ \forall f \in K[X] \text{ şi } \nexists f \in K[X] \setminus \{0\} :\ 0 \mid f.$$

Două polinoame $f, g \in K[X]$ sunt **asociate în divizibilitate** (scriem $f \sim g$) dacă avem

$$\exists\ a \in K^* :\ f = ag.$$

Relaţia de asociere în divizibilitate $\sim$ este o relaţie de echivalenţă pe $K[X]$.

Un **polinom** $f \in K[X]^*$ se numeşte **ireductibil** dacă $grad\,f \geq 1$ şi

$$f = gh\ (g, h \in K[X]) \Rightarrow g \in K^* \text{ sau } h \in K^*.$$

Noţiunile de c.m.m.d.c. şi c.m.m.m.c. se definesc ca în cazul numerelor întregi, produsul c.m.m.d.c. cu c.m.m.m.c. a două polinoame este asociat în divizibilitate cu produsul polinoamelor, iar comportamentul relaţiei de divizibilitate faţa de sumă şi produs este similar cu cel pe care îl cunoaştem de la numere întregi.

Dacă $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$ şi $c \in K$, atunci

$$f(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n \in K$$

se numeşte **imaginea polinomului f în (punctul) c.** Elementul $c \in K$ se numeşte **rădăcină a lui f** dacă $f(c) = 0$.

Teorema 4. (Teorema împărţirii cu rest în $K[X]$) Pentru orice polinoame $f, g \in K[X]$, $g \neq 0$, există două polinoame unice $q, r \in K[X]$ astfel încât

$$f = gq + r \text{ şi } grad\,r < grad\,g. \tag{5}$$

Demonstraţie. (facultativ) Fie $a_0, \ldots, a_n, b_0, \ldots, b_m \in K$, $b_m \neq 0$ şi

$$f = a_0 + a_1X + \cdots + a_nX^n \text{ şi } g = b_0 + b_1X + \cdots + b_mX^m.$$

Existenţa polinoamelor q şi r: Dacă $f = 0$ atunci $q = r = 0$ verifică (5).

Pentru $f \neq 0$ procedăm prin inducţie după $n =$ grad f. Dacă $n < m$ (întrucât $m \geq 0$ există polinoame f care verifică această condiţie), atunci $q = 0$ şi $r = f$ verifică pe (5).

Presupunem afirmaţia adevărată pentru polinoamele de grad mai mic decât $n \geq m$. Cum a_nX^n este termenul de grad maxim al polinomului $a_nb_m^{-1}X^{n-m}g$, pentru polinomul $h = f - a_nb_m^{-1}X^{n-m}g$, avem grad $h < n$ şi conform ipotezei există $q', r \in R[X]$ astfel încât

$$h = gq' + r \text{ şi } \text{grad}\,r < \text{grad}\,g.$$

Rezultă că $f = h + a_n b_m^{-1} X^{n-m} g = (a_n b_m^{-1} X^{n-m} + q')g + r = gq + r$ unde $q = a_n b_m^{-1} X^{n-m} + q'$. Deci existenţa polinoamelor q şi r care verifică pe (5) este demonstrată.

Unicitatea polinoamelor q şi r: Dacă mai avem

$$f = gq_1 + r_1 \text{ şi } \operatorname{grad} r_1 < \operatorname{grad} g,$$

atunci $gq + r = gq_1 + r_1$ de unde rezultă $r - r_1 = g(q_1 - q)$ şi $\operatorname{grad}(r - r_1) < \operatorname{grad} g$. Întrucât $g \neq 0$ urmează $q_1 - q = 0$ ceea ce implică $r - r_1 = 0$, adică $q_1 = q$ şi $r_1 = r$. □

Polinoamele q şi r din (5) se numesc **câtul**, respectiv **restul** împărţirii lui f la g.

Corolarul 5. Fie K este un corp comutativ şi $c \in K$. Atunci restul împărţirii unui polinom $f \in K[X]$ la polinomul $X - c$ este $f(c)$.

Într-adevăr, din (5) rezultă că restul r al împărţirii lui f la $X - c$ este un element din K, iar cum $f = (X - c)q + r$, se deduce că $r = f(c)$. Cazul $r = 0$ ne conduce imediat la:

Corolarul 6. Fie K este un corp comutativ. Un element $c \in K$ este rădăcină a lui f dacă şi numai dacă $(X - c) \mid f$.

Corolarul 7. Dacă K este un corp comutativ, atunci un polinom nenul $f \in K[X]$ de grad k are cel mult k rădăcini în K.

Într-adevăr pentru polinoamele de gradul zero afirmaţia este adevărată deoarece polinoamele de gradul zero nu au rădăcini. Presupunem $k > 0$ şi afirmaţia adevărată pentru polinoamele de grad mai mic decât k. Dacă $c_1 \in K$ este rădăcină a lui f, atunci $f = (X - c_1)q$ şi $\operatorname{grad} q = k - 1$. Conform ipotezei, polinomul q are cel mult $k-1$ rădăcini în K. Cum K este corp comutativ, $K[X]$ este domeniu de integritate şi din $f = (X - c_1)q$ rezultă că $c \in K$ este rădăcină a lui f dacă şi numai dacă $c = c_1$ sau c este rădăcină lui q. Deci f are cel mult k rădăcini în K.