CURS 11

27.03.2018

Inele de polinoame

Notăm R = inel comutativ cu unitate
F = corp comutativ

Def: Prin te-un polinom cu coeficienți în R scris cu nedeterminata X înțelegem o combinație liniară formală a unor puteri naturale ale lui X formată cu coeficienți din R: $f = f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$, unde $X^0 = 1$

Datorită acestui fel de reprezentare putem elimina termenii $a_i X^i$ pt. care $a_i = 0$

- Dacă $f = 0$, atunci spunem că gradul lui f este $-\infty$
- Dacă $\exists i = \overline{0,n}$ a.î. $a_i \neq 0$ și k este cel mai mare a.î. $a_k \neq 0$, atunci spunem că gradul lui f este k.

Exemple:

$R = (\mathbb{Z}_4, +, \cdot)$ inel comutativ cu divizori ai lui zero.

$f = \hat{0} \cdot X^3 + \hat{3} \cdot X^2 + \hat{2}$ polinom de gradul 2.

Notație: $\text{grad}(f)$ = gradul lui f

Def: Fie $f = a_n X^n + \dots + a_1 X + a_0$ un polinom de grad n
$g = b_m X^m + \dots + b_1 X + b_0$ un polinom de grad m.
Spunem că $f = g$ dacă
i) $\text{grad}(f) = \text{grad}(g)$
ii) $\forall i = \overline{0,n}$, $a_i = b_i$

Notație: Notăm cu $R[X]$ = mulțimea polinoamelor cu coeficienți în R

Def: Dacă $f = a_n X^n + \dots + a_1 X + a_0$ și $g = b_m X^m + \dots + b_1 X + b_0$ sunt polinoame din $R[X]$, atunci definim: (și $m \leq n$)

$$f + g = a_n X^n + \dots + a_{m+1} X^{m+1} + (a_m + b_m) X^m + \dots + (a_1 + b_1) X + (a_0 + b_0)$$

$$f \cdot g = c_{m+n} X^{m+n} + c_{m+n-1} X^{m+n-1} + \dots + c_1 X + c_0, \text{ unde:}$$

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$
$$\dots$$
$$c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_i b_{k-i} + \dots + a_k b_0$$
$$c_{m+n} = a_n b_m$$

Teorema
$(R[X], +, \cdot)$ e un inel comutativ cu unitate.

Propoziție
Dacă $f, g \in R[X]$, atunci:
a) $\text{grad}(f+g) \leq \max(\text{grad}(f), \text{grad}(g))$
b) $\text{grad}(f \cdot g) \leq \text{grad}(f) + \text{grad}(g)$
c) dacă R este domeniu de integritate, atunci $\text{grad}(f \cdot g) = \text{grad}(f) + \text{grad}(g)$

Exemple

$f, g \in [X]$, $f = \hat{2} \cdot X$, $g = \hat{2} X + 1$

$\text{grad}(f) = \text{grad}(g) = 1$

$f \cdot g = \hat{4} \cdot X^2 + \hat{2} \cdot X = \hat{2} \cdot X \Rightarrow \text{grad}(f \cdot g) = 1 < \text{grad}(f) + \text{grad}(g)$

Corolar
Dacă R este un domeniu de integritate, atunci și R[X] este domeniu de integritate

Teorema (împărțirii cu rest)
Fie F un corp comutativ și $f, g \in F[X]$ a.î $f \neq 0$. Atunci $\exists$ și sunt unice $q, r \in F[X]$ a.î i) $g = f \cdot q + r$

ii) $\text{grad}(r) < \text{grad}(f)$

Def: q - câtul împărțirii lui g la f
r - restul împărțirii lui g la f.

Dem:
• Existența
$f = a_m X^m + \dots + a_1 X + a_0$
$g = b_n X^n + \dots + b_1 X + b_0$ cu $\text{grad}(f) = m \in \mathbb{N}$ și $\text{grad}(g) = n$ sau $\text{grad}(g) = -\infty$

I Dacă $\text{grad}(g) = -\infty \Rightarrow g = 0 = f \cdot 0 + 0$, $q = 0$, $r = 0$
$\text{grad}(r) = -\infty < \text{grad}(f) \in \mathbb{N}$

II Dacă $\text{grad}(g) \geq 0$. Aplicăm inducția după grad(g)
Verificare
$\text{grad}(g) = 0 \Rightarrow g = b_0 \in F^*$
caz a) $\text{grad}(f) = 0 \Rightarrow f = a_0 \in F^* \Rightarrow g = f \cdot (a_0^{-1} \cdot g) + 0$
$q = a_0^{-1} \cdot g$, $r = 0$ $\Rightarrow \text{grad}(r) < \text{grad} f$

cazb) $\text{grad}(f) > 0 \Rightarrow g = f \cdot 0 + g$
$q = 0$, $r = g$, $\text{grad}(r) = 0 < \text{grad}(f)$
⇒ etapa de verificare este completă

Etapa de demonstrație:
Pp. că proprietatea este valabilă pt. toate polinoamele g' cu $\text{grad}(g') < m$ și luăm g a.î $\text{grad}(g) = m$

Împărțim pe $g = X^2 + 2X + 3$ la $f = X^5 + 1$
cazul a) $\text{grad}(g) < \text{grad}(f) \Rightarrow g = f \cdot 0 + g$ și $q = 0$, $r = g$

cazul b) $\text{grad}(g) \geq \text{grad}(f)$ $g = 3X^7 + 2X + 3$, $f = X^5 + X^4$

$3X^7 + 2X + 3 \mid X^5 + X^4$
$3X^7 + 3X^6 \quad\quad 3X^2$
$-3X^6$ (-)
...

Fie $g' = g - f \cdot (a_n^{-1} \cdot b_m) X^{m-n} \Rightarrow \text{grad}(g') < \text{grad}(g)$
⇒ pt. g' putem aplica ipoteza inducției ⇒ $\exists q', r' \in F[X]$ a.î $g' = f \cdot q' + r'$, $\text{grad}(r) < \text{grad}(f)$

$\Rightarrow g = g' + (a_n^{-1} \cdot b_m) f \cdot X^{m-n} = f\left(q' + a_n^{-1} b_m X^{m-n}\right) + r'$

⇒ Punem $q = q' + a_n^{-1} \cdot b_m \cdot X^{m-n}$
$r = r'$, q.e.d.

Def: Dacă R este un inel comutativ și $r \in R$, atunci idealul $(r) = r \cdot R$ s.n. idealul principal generat de r

Spunem că R este cu ideale principale dacă toate idealele lui R sunt princip.

Exemplu:
$(\mathbb{Z}, +, \cdot)$ este un domeniu cu ideale principale.

Teorema
$(F[X], +, \cdot)$ este un domeniu cu ideale principale.

Dem:
$F[X]$ domeniu de integritate (s-a demonstrat anterior)
Fie I un ideal în $F[X]$.
Caz a) $I = \{0\} \Rightarrow I = 0 \cdot F[X] = (0)$
Caz b) $I \neq \{0\} \Rightarrow \exists\, f \in I$ cu $\text{grad}(f) \geq 0$
$\Rightarrow \exists\, f \in I$ a.î. $\text{grad}(f) \geq 0$ și $\forall\, h \in I^*$ $\text{grad}(f) \leq \text{grad}(h)$

$\forall\, I = f \cdot F[X]$
$f \cdot F[X] \subseteq I$ evidentă (din definiția idealelor)
Fie $h \in I$, $f \neq 0$ $\Rightarrow \exists\, g, r \in F[X]$ a.î. $h = f \cdot g + r$ și $\text{grad}(r) < \text{grad}(f)$

$\Rightarrow r = \underbrace{h}_{\in I} - \underbrace{f \cdot g}_{\in I} \in I \Rightarrow r \in I$ și $\text{grad}(r) < \text{grad}(f) \Rightarrow r \notin I^* = I \setminus \{0\} \Rightarrow r = 0$

$\Rightarrow \exists\, g \in F[X]$ a.î. $h = f \cdot g \in f \cdot F[X] = (f)$
$\Rightarrow I = f \cdot F[X]$
$\Rightarrow F[X]$ este un ideale principale.

Obs. Teorema împărțirii cu rest poate fi demonstrată pt. polinoame cu coeficienți într-un domeniu de integritate dacă adăugăm condiția a_n este inversabil. ($f = a_n X^n + \dots$)
Deci, în general $R[X]$, unde R - domeniu de integritate NU e cu ideale principale.

Exemplu:
$\mathbb{Z}[X]$, $I = \{ f = a_n X^n + \dots + a_1 X + a_0 \mid a_0 \text{ par} \}$ - ideal care nu e principal.

Def: Spunem că $f \in F[X]$ e un polinom ireductibil dacă:
i) $f \notin F$ ($\text{grad}\, f \geq 1$)
ii) Din $f = g \cdot h \Rightarrow g \in F$ sau $h \in F$

Exemplu
Orice polinom de gradul 1 e ireductibil.
$f = aX + b$, $a \neq 0$
$f = g \cdot h \Rightarrow \text{grad}(g) + \text{grad}(h) = 1 \Rightarrow \text{grad}(g) = 0$ sau $\text{grad}(h) = 0$

Teoremă
Dacă $f \in F[X]$ și $\text{grad}(f) >$, atunci $\exists\, r_1, r_2, \dots, r_k$ polinoame ireductibile cu coeficientul dominant 1 și $\exists\, a \in F$ a.î. $f = a \cdot r_1 \cdot r_2 \cdots r_k$
(coeficient dominant → coeficientul lui X la cea mai mare putere)
În plus, această scriere este unică dacă facem abstracție de ordinea factorilor

Teoremă
Dacă $f \in F[X]$ este un polinom ireductibil, atunci $(F[X]/(f), +, \cdot)$ este un corp comutativ.

Dem:
$K = F[X]/(f)$ inel comutativ
$\Rightarrow$ este suficient să demonstrăm că inelul K nu are ideale netriviale (vezi curs anterior)
Fie U un ideal în K și p.p. că $U \neq \{0_K\}$
Fie $V = \{ h \in F[X] \mid h + (f) \in U \}$
$\Rightarrow V$ este ideal în $F[X]$ (temă)
$\Rightarrow \exists\, g \in F[X]$ a.î. $V = (g) = g \cdot F[X]$
$\Rightarrow$

Dacă $g \in F^* \Rightarrow g$ inversabil $\Rightarrow V = F[X] \Rightarrow U = K$
$g \in V$

Dacă $h \in F^* \Rightarrow V = (f) \Rightarrow U = \{0_K\}$ contradicție

$\Rightarrow K$ este corp comutativ.

Propoziție
Fie $f \in F[X]$ un polinom ireductibil. Atunci $\varphi : F \longrightarrow F[X]/(f)$, $\varphi(a) = a + (f)$ este un morfism injectiv de corpuri.
Deci, φ induce o structură de F - spațiu vectorial pe $F[X]/(f)$
În plus, $\dim_F F[X]/(f) = \text{grad}(f)$

Obs În general, se identifică F cu un subcorp al lui $F[X]/(f)$

Def: Fie $f = a_n X^n + \dots + a_1 X + a_0 \in F[X]$
Spunem că $h \in F$ este rădăcină pt. f dacă $f(h) = a_n h^n + a_{n-1} h^{n-1} + \dots + a_1 h + a_0 = 0$

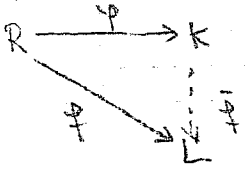
Teoremă
h este rădăcină pt. dacă $\exists\, f \in F[X]$ a.î. $f = (X-h) \cdot h$

CURS 12

29.05.2018

Elemente de teoria corpurilor XEROX → CURS

Teoremă (corpul fracțiilor unui domeniu de integritate)
Fie $(R, +, \cdot)$ un domeniu de integritate. Atunci, $\exists$ un corp K și un morfism unitar de inele $\varphi : R \to K$ a.î.:
a) φ este injectiv (adică putem identifica pe R cu un subinel a lui K)
b) Dacă L este corp și $f : R \to L$ este un morfism de inele unitar, atunci
$\exists!\, \bar{f} : K \to L$ morfism de corpuri a.î. $f = \bar{f} \circ \varphi$



Dem (schiță)
Fie $A = R \times R^* = \{(a,b) \mid a \in R, b \in R^*\}$
Pe A definim relația $\sim$ dată de
$(a,b) \sim (c,d) \iff a \cdot d = b \cdot c$
Se demonstrează că $\sim$ e o relație de echivalență pe A
(R) $(a,b) \sim (a,b) \iff a \cdot b = b \cdot a$ adevărat (pt. că înmulțirea e comutativă)
(T) $(a,b) \sim (c,d) \Rightarrow ad = bc \mid \cdot f \Rightarrow afd = bcf$
$(c,d) \sim (e,f) \Rightarrow cf = de \mid \cdot b \Rightarrow bcf = bed$
$\Rightarrow afd = bed$ ($d \neq 0$, R dom. de integritate) $\Rightarrow af = be \Rightarrow (a,b) \sim (e,f)$
(S) - temă
$K := A/\sim$ și notăm cu $\overline{(a,b)}$ clasa lui (a,b) în K
Definim operațiile $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc,\ bd)}$
$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac,bd)}$
Se demonstrează că tripletul $(K,+,\cdot)$ este corp comutativ ($+$ și $\cdot$ sunt independente de alegerea reprezentanților)
$\varphi : R \to K$, $\varphi(a) = \overline{(a,1)}$

Def: K s.n. corpul fracțiilor asociat lui R