Aritmetica lui $\mathbb{Z}$ și $K[X]$, K corp comutativ

NU INTRĂ ÎN EXAMEN!

$\mathbb{Z}$	$K[X]$
domenii de integritate	
orice ideal este principal	
$U(\mathbb{Z})=\{1,-1\}$	$U(K[X])=K\setminus\{0\}$
funcția modul $\lvert\cdot\rvert$	funcția grad
teoremă de împărțire cu rest	
$U(\mathbb{Z})=\{1,-1\}$	$U(K[X])=K\setminus\{0\}$

$K[X]$

$f,g\in K[X]$, $g\neq 0 \Rightarrow$
$\Rightarrow (\exists!)\ c,r\in K[X]$ cu

$$\begin{cases} f=c\cdot g+r \\ \deg(r)<\deg(g) \end{cases}$$

$\mathbb{Z}$

Teoremă: Fie $a,b\in\mathbb{Z}$, $b\neq 0$. Atunci
$(\exists!)\ c,r\in\mathbb{Z}$ cu

$$\begin{cases} a=c\cdot b+r \\ 0\leq r<|b| \end{cases}$$

Dem.:

Existența:

$\{a - kb \mid k \in \mathbb{Z}\} \cap \mathbb{N} \neq \emptyset$

Caut $a - kb \geq 0 \Leftrightarrow kb \leq a \Leftrightarrow \begin{cases} k \leq \frac{a}{b}, & b > 0 \\ k \geq \frac{a}{b}, & b < 0 \end{cases}$

Fie r cel mai mic element $a, b \in \mathbb{Z}$

$$\begin{cases} r = a - cb \text{ pt. un } c \in \mathbb{Z} \\ \text{și } r \geq 0 \end{cases}$$

$$\Downarrow$$

$$a = bc + r$$

Vreau $r < |b|$.

Altfel, dacă $r \geq |b|$, avem

$|b| = \varepsilon b$ cu $\varepsilon \in \{1, -1\}$

$$0 \leq r - |b| = a - bc - \varepsilon b = a - \underbrace{(c + \varepsilon)}_{\in \mathbb{N}} b \in X$$

$r - |b| < r$, contradicție cu minimalitatea lui r

Așadar, $r < |b|$, gata!

Unicitatea.

$$a = \underbrace{c_1 b + r_1 = c_2 b + r_2}$$

$$\Downarrow$$

$$(c_1 - c_2) b = r_2 - r_1$$

$0 \leq r_1, r_2 < |b| \Rightarrow |r_1 - r_2| < |b| \Rightarrow$

$\Rightarrow |c_1 - c_2| \, |x_1| < |x_1|$

$\Rightarrow |c_1 - c_2| < 1$

$\Rightarrow c_1 - c_2 = 0 \Rightarrow c_1 = c_2 \Rightarrow x_1 = x_2$

Divizibilitate

R va fi $\mathbb{Z}$ sau $K[X]$

Def.: Fie $a, b \in R$. Spunem că $a | b$ (a îl divide pe b, b se divide cu a) dacă $(\exists) c \in R$ cu $b = ca$.

Observație! $a | 0$, $u \in U(R) \Rightarrow u | a$

$a = a \cdot 0$ $\qquad a = u \cdot u^{-1} a$

Proprietăți: Pentru $a, b, c \in R$

(1) $a | b \Leftrightarrow (b) \subset (a)$

(2) $a | a$

(3) $a | b$, $b | c \Rightarrow a | c$

(4) $a | b$ și $b | a \Leftrightarrow (\exists) u \in U(R)$ cu $b = ua$

"$\Leftarrow$": $b = ua \Rightarrow a | b$

$u^{-1} b = a \Rightarrow b | a$

"$\Rightarrow$": Dacă $a = 0$ sau $b = 0 \Rightarrow$

$a = b = 0$

$u = 1$

Presupunem $a, b \neq 0$.

$a \mid b \Rightarrow (\exists) u \in R \quad b = ua$

$b \mid a \Rightarrow (\exists) v \in R \quad a = vb$

$a = vb = v(ua) \xrightarrow{a \neq 0}$

$vu = 1 \Rightarrow$

$\Rightarrow u \in U(R)$

a și b sunt asociate în divizibilitate

Notăm $a \sim b \Leftrightarrow a \mid b$ și $b \mid a$

$\sim$ relație de echivalență $\Leftrightarrow (a) = (b)$

(5) $a \mid b, a \mid c \Rightarrow a \mid xb + yc$, $(\forall) x, y \in R$

(6) $\left.\begin{matrix} a \mid b \\ b \neq 0 \end{matrix}\right| \Rightarrow |a| \leq |b|$ dacă $R = \mathbb{Z}$

$\deg a \leq \deg b$, dacă $R = K[X]$, cu egalitate doar pentru $a \sim b$

Def.: Fie $a, b \in R$.

(1) Un element $d \in R$ s.n. un **cel mai mare divizor comun** (cmmdc) al lui a și b dacă

- $d \mid a$, $d \mid b$
- Dacă $d' \in R$, $d' \mid a$ și $d' \mid b$, atunci

$d' \mid d$

(2) Un element $m \in R$ s.n. un **cel mai mic multiplu comun** (cmmmc) al lui a si b daca:

- $a \mid m$, $b \mid m$
- daca $m \in R$, $a \mid m'$, $b \mid m'$, atunci $m \mid m'$

Observatie! Daca $a \mid b$, atunci a este un cmmdc al lui a si b si b este un cmmmc al lui a si b.

Teorema: Fie $R = \mathbb{Z}$ sau $K[X]$ si $a, b \in R$.
Fie $d, m \in R$ a.i. $(a)+(b)=(d)$ si $(a) \cap (b) = (m)$.
[d, m există deoarece orice ideal in R este principal]
Atunci d este un cmmdc al lui a si b, iar m este un cmmmc al lui a si b.

Dem.: $(a)+(b) = (d) \Rightarrow (a) \subset (d)$ si $(b) \subset (d)$

$\Rightarrow d \mid a$ si $d \mid b$

Observăm si că $d \in (d) = (a)+(b) \Rightarrow$

$\Rightarrow (\exists)\, x, y \in R$ cu $d = xa + yb$

Daca $d' \mid a$ si $d' \mid b \Rightarrow$

$(a) = \{xa \mid x \in R\}$

$\Rightarrow d' \mid xa + yb = d$

m - cmmmc - exercițiu

Observație! Fie $a, b \in R$ și $d \in R$ cu $(a)+(b)=(d)$, deci d este un cmmdc al lui a și b.

Dacă $d' \in R$, $d' \sim d$, atunci și d' este un cmmdc al lui a și b.

$d \sim d' \Rightarrow (d) = (d') \Rightarrow (a)+(b)=(d')$

$\Downarrow$ Teoremă

d' este un cmmdc

Dacă d'' este un alt cmmdc al lui a și b, atât că $d'' \sim d$.

$$\left.\begin{array}{l} d \text{ cmmdc al lui } a \text{ și } b \\ d'' \mid a,\ d'' \mid b \end{array}\right| \Rightarrow$$

$\Rightarrow d'' \mid d$

$$\left.\begin{array}{l} d'' \text{ cmmdc al lui } a \text{ și } b \\ d \mid a,\ d \mid b \end{array}\right| \Rightarrow$$

$\Rightarrow d \mid d''$

Def.: Mulțimea tuturor cmmdc ai lui a și b este $\{d' \mid d' \sim d\} = \{ud \mid u \in U(R)\}$

$\mathbb{Z}$ $\{d, -d\}$

$K[X]$ $\{\alpha d \mid \alpha \in K \setminus \{0\}\}$

$a, b \neq 0$

(a,b) = unicul cmmdc al lui a și b care este
- > 0, pentru $R = \mathbb{Z}$
- monic, pentru $R = K[X]$

Lemă: Fie $a, b, c, r \in R$ cu $a = c \cdot b + r$.
Atunci $(a,b) = (b,r)$.

Dem.:

$$\left.\begin{array}{l} (a,b) \mid b \\ (a,b) \mid a - cb = r \end{array}\right| \Rightarrow (a,b) \mid (b,r) \Bigg| \Rightarrow$$

$$\left.\begin{array}{l} (b,r) \mid b \\ (b,r) \mid cb + r = a \end{array}\right| \Rightarrow (b,r) \mid (a,b) \Bigg|$$

$\Rightarrow (a,b) = (b,r)$

Algoritmul lui Euclid:

Fie $a, b \in R \setminus \{0\}$. Dacă $b \mid a$, atunci b este un cmmdc al lui a și b. Dacă $b \nmid a$,
- împart a la b: $a = c_1 \cdot b + r_1$ (știm că $r_1^{-1} \neq 0$)
- împart b la r_1: $b = c_2 \cdot r_1 + r_2$ (dacă $r_2 = 0$, mă opresc)
- dacă $r_2 \neq 0$, împart r_1 la r_2: $r_1 = c_3 \cdot r_2 + r_3$ (dacă $r_3 = 0$, mă opresc)

• Dacă $r_2 \neq 0$, împart r_2 la r_3

• Dacă $r_m \neq 0$, împart r_{m-1} la r_m

$r_{m-1} = c_{m+1} \cdot r_m + r_{m+1} = 0$

(Dacă $r_{m+1} = 0$, mă opresc)

Atunci obținem un rest 0 (adică procedura se încheie) și dacă r_{m+1} este primul rest 0, atunci r_m este un cmmdc al lui a și b.

[Ultimul rest nenul din procedură este cmmdc pentru a și b]

Dem.: Presupunem că $r_m \neq 0, \forall m$. Atunci

- pentru $R = \mathbb{Z}$ $\quad |b| > r_1 > r_2 > r_3 > \dots$
- pentru $R = K[X]$ $\quad \deg b > \deg r_1 > \deg r_2 > \deg r_3 > \dots$

Șiruri infinite strict descrescătoare de nr. naturale

Rezultă că există un rest $= 0$.

Lema $\Longrightarrow (a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{m-1}, r_m) = (r_m, r_{m+1})$

$r_m \quad 0$

Algoritmul $\Rightarrow r_m = \text{cmmdc}(a, b)$

$r_1 = a - c_1 b$

$r_2 = b - c_2 r_1 = \alpha a + \beta b$

$\vdots$

Def: Un element $r \in R$ se numeste:

- **prim**, daca $r \neq 0$, $r \notin U(R)$, si pentru orice $a, b \in R$ cu $r \mid ab$ avem $r \mid a$ sau $r \mid b$
- **ireductibil**, daca $r \neq 0$, $r \notin U(R)$, si pentru orice $a, b \in R$ cu $r = ab$ avem $a \in U(R)$ sau $b \in U(R)$

$\Downarrow$ $a \sim r$

$\Downarrow$ $b \sim r$

Propozitie: Fie $r \in R \setminus \{0\}$, $r \notin U(R)$. Atunci r este prim $\iff$ r este ireductibil.

Dem.:

„$\Rightarrow$": Presupunem ca r este prim.

Fie $r = ab \Rightarrow r \mid ab \Rightarrow r \mid a$ sau $r \mid b$

$\Downarrow$

$a = rx$

$\Downarrow$

$r = rxb$

$\Downarrow$

$1 = xb$

$\Downarrow$

$b \in U(R)$

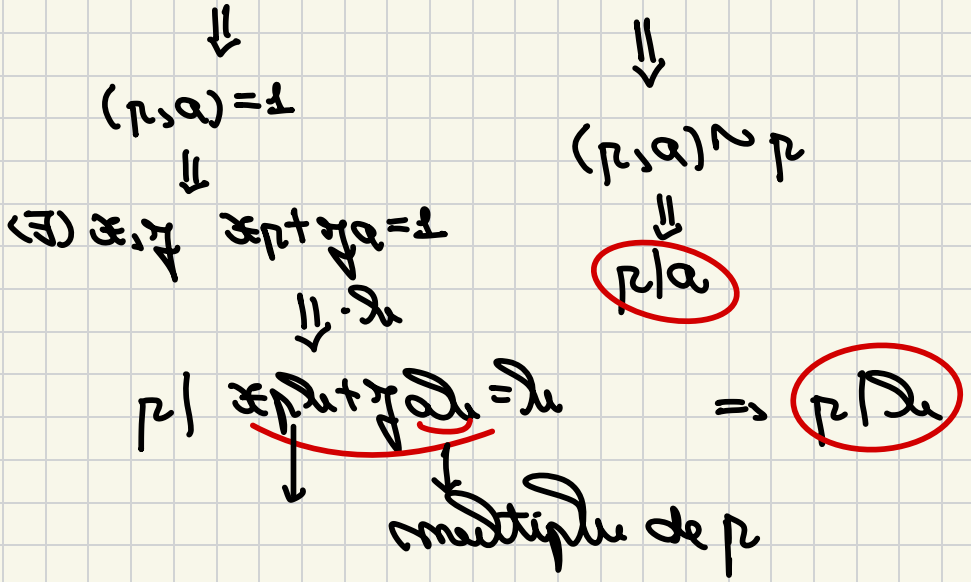
$r \mid a \Rightarrow a \in U(R)$

„$\Leftarrow$": Presupunem r ireductibil.

Fie $a, b \in R$ cu $r \mid ab$.

$(r, a) \mid r \Rightarrow r = (r, a) \cdot x \xrightarrow{r \text{ ired.}}$

$\Rightarrow (r, a) \in U(R)$ sau $x \in U(R)$



$\mathbb{Z}$: număr prim

$K[X]$: polinom ireductibil

Teoremă: Fie $R = \mathbb{Z}$ sau $K[X]$. Atunci orice $a \in R \setminus \{0\}$, $a \notin U(R)$, se scrie ca produs de elemente ireductibile. Mai mult, o astfel de scriere este unică până la o permutare a factorilor și asociere în divizibilitate.

$$a = r_1 \dots r_m = q_1 \cdot \dots \cdot q_n \qquad r_i, q_j \text{ ired.}$$

$$\Downarrow$$

$$m = n, (\exists)\, \sigma \in S_m \text{ a.î. } r_i \sim q_{\sigma(i)} \ (\forall) i$$

Dem.:

Existență:

Presupun că există a care nu se scrie ca în teoremă.

Alg un astfel de a cu → |a| minim, pt. $R = \mathbb{Z}$

→ $\deg(a)$ minim, pt. $R = K[X]$

a nu este ireductibil

$\Rightarrow a = b \cdot c$, $b, c \notin U(R)$

$|b|, |c| < |a|$ ✓

$\deg b, \deg c < \deg K[X]$

minimalitatea lui a ⟹ b și c se scriu ca produs de ired.

$\Downarrow$

bc = produs de ired.

$\|$

a contradicție!

Unicitatea: (Schițăm)

Inducție după m.

$m = m$ $\quad p_1 = q_1 \cdots q_m$

Dacă $m \geq 2$ $\quad p_1 = q_1 (q_2 \cdots q_m)$

$\Downarrow$ p_1 ired.

$m = 1$ $\quad p_1 = q_1$ $\quad a_1 \in U(R)$ sau $q_2, \dots, q_m \in U(R)$

$\Downarrow$

$q_2 \in U(R)$

contradicție!

$\Downarrow$

$a \in U(R)$

$m - 1 \longrightarrow m$ $\quad p_1 \cdots p_m = q_1 \cdots q_m$

$p_1 \mid q_1 \cdots q_m \xrightarrow{p_1 \text{ prim}} p_1 \mid q_i$ pt. un i

$q_i = p_1 \cdot *$

$\Downarrow$

$* \in U(R)$

$\Downarrow$

$p_1 \sim q_i$

$p_1 p_2 \cdots p_m = q_1 \cdots (p_1 *) \cdots q_m$ (i)

Rezultă din ipoteza de ind.

$m-1 = m-1 \Rightarrow m = m$

orice prim în $\mathbb{Z}$ este p sau $-p$, cu p prim $\in \mathbb{N}$

$\Downarrow$

ireed.

orice polinom ireductibil în $K[X]$ este αP cu P polinom ireductibil monic.

Consecință: $R = \mathbb{Z}$ orice $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ se scrie $a = \underbrace{\varepsilon}_{\in \{1,-1\}} \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ cu

$p_1, \dots, p_r$ prime naturale distincte

$\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$

$R = K[X]$ orice $a \in K[X]$, $\deg a \geq 1$ se scrie unic

$a = \underbrace{\varepsilon}_{K \setminus \{0\}} \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ cu $p_1, \dots, p_r$

polinoame ireductibile monice distincte

$\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$

Teoremă: (1) Mulțimea numerelor naturale prime este infinită.

(2) Mulțimea polinoamelor ireductibile monice din $K[X]$ este infinită.

Dem.:

(1) Presupunem prin absurd că e finită.

Fie $p_1 < p_2 < \dots < p_m$ toate nr. naturale prime

Fie $N = p_1 p_2 \dots p_m + 1 \in \mathbb{N}$, ≥ 2

N = produs de prime $\Rightarrow (\exists) i$ $p_i \mid N = p_1 \cdot p_i \dots p_m + 1$

$p_i \mid p_1 \dots p_m$ $\Rightarrow$

$p_1 \mid 1$ contradicție!

Propoziție: Fie P un polinom ireductibil în $K[X]$. Atunci $\frac{K[X]}{(P)}$ corp.

Dem.: Fie $\hat{f} \in \frac{K[X]}{(P)}$, $\hat{f} \neq 0$, adică $f \notin (P)$, adică

$P \nmid f$.

Atunci $\underbrace{(P, f)}_{\neq P} \mid P \xrightarrow{P \text{ ired.}} (P, f) = 1$

$\Rightarrow (\exists)$ $A, B \in K[X]$ $A \cdot P + B \cdot f = 1$

$\Rightarrow$ $\hat{A} \cdot \hat{P} + \hat{B} \cdot \hat{f} = \hat{1}$

$\hat{P} = 0$

$\hat{f}$ inversabil

Dacă K este corp finit

$|K| = q$

$\deg p = n$

$$\frac{K[X]}{(p)} = \{a_0 + a_1 X + \dots + a_{n-1} X^{n-1} \mid a_0, \dots, a_{n-1} \in K\}$$

↙ are q^n elemente

$(K = \mathbb{Z}_p)$ și p polinom ireductibil monic

↑ prim

Exemplu:

$\frac{\mathbb{Z}_2[X]}{(X^2 + X + \hat{1})}$ corp cu 4 elemente

↙ ired.

$\frac{\mathbb{Z}_2[X]}{(X^3 + X + \hat{1})}$ corp cu 8 elemente