8.01.2023

Curs 13.

Aritmetică în $\mathbb{Z}$ și în $K[Z]$

K corp comutativ ($\mathbb{Q}, \mathbb{R}, \mathbb{Z}_p, \mathbb{C}$)...

Atunci: $D = \mathbb{Z}$ sau $K[X]$.

Def: Fie $a, b \in D$. Spunem că a divide pe b (not $a \mid b$) dacă $\exists c \in D$ cu $a \cdot c = b$.

Prop: 1) $a \mid a \quad \forall a \in D$ (reflexivitate)

2) $a \mid b$ și $b \mid c \Rightarrow a \mid c$ (tranzitivitate)

Dem: $b = a \cdot \ell$ cu $\ell \in D$

$c = b \cdot \beta$ cu $\beta \in D \Rightarrow c = a \cdot \ell \cdot \beta$.

Întrebare: "Este relația $\mid$ antisimetrică?

pe $\mathbb{Z}$ nu: $2 \mid -2$ și $-2 \mid 2$ dar $2 \neq -2$.

Def: Spunem că $a, b \in D$ sunt asociate în divizibilitate ($a \sim b$) dacă $a \mid b$ și $b \mid a$.

Prop: $a, b \in D$ sunt asociate în divizibilitate $\Leftrightarrow \exists u \in D$ inversabil a.î. $a = u \cdot b$.

Dem: "$\Leftarrow$" $a = ub$ cu $u \in U(D) \Rightarrow b \mid a$

$\Downarrow$

$u^{-1} \cdot a = b \Rightarrow a \mid b$ $\Big| \Rightarrow a \sim b$

"$\Rightarrow$" $a \mid b \Rightarrow \exists c \in D$ cu $b = a \cdot c$

$b \mid a \Rightarrow \exists c_1 \in D$ cu $a = b \cdot c_1$ $\Rightarrow a = a \cdot (c \cdot c_1) \Rightarrow$

$\Rightarrow a(1 - cc_1) = 0$

D domeniu $\Rightarrow a = 0$ sau $\Rightarrow b = 0 \Rightarrow a = 1 \cdot b$

$1 - cc_1 = 0 \Rightarrow cc_1 = 1 \Rightarrow c, c_1 \in U(D)$ □

- $U(\mathbb{Z}) = \{\pm 1\}$
- $U(K[X]) = U(K) = K \setminus \{0\}$

K corp — polinoamele nenule constante

Prop: 1) $a \mid b \Leftrightarrow b \in (a)\Delta \Leftrightarrow (b)\Delta \subseteq (a)\Delta$

2) $a \sim b \Leftrightarrow (a)\Delta = (b)\Delta$

3) $a \mid b$ și $a \mid b_1 \Rightarrow \forall c, c_1 \in \Delta \quad a \mid c \cdot b + c_1 \cdot b_1$

Dem: $b = a \cdot \alpha$ cu $\alpha, \alpha_1 \in \Delta$

$b_1 = a \cdot \alpha_1$

$c \cdot b + c_1 \cdot b_1 = c \cdot a \cdot \alpha + c_1 \cdot a \cdot \beta = a(c \cdot \alpha + c_1 \beta)$

Teorema împărțirii cu rest

în $\mathbb{Z}$: Oricare ar fi $a, b \in \mathbb{Z}$ cu $b \neq 0$ există și sunt unice $q, r \in \mathbb{Z}$ a.î. $a = q \cdot b + r$ și $0 \leq r \leq |b|$

Dem: $\{a - xb \mid x \in \mathbb{Z}, a - xb \geq 0\} \subseteq \mathbb{N}$

notez $r =$ min

r va fi restul căutat

$r = a - xb$ pt un anume $x \in \mathbb{Z}$

acest x este câtul q căutat

Demă: $0 \leq r < |b|$;

r, q unici

Teorema împărțirii cu rest în $K[X]$

Oricare ar fi $f(X), g(X) \in K[X]$ și $g \neq 0$.
există și sunt unice $q(X), r(X) \in K[X]$ a.î.
$f(X) = g(X) \cdot q(X) + r(X)$ și $\text{grad } r < \text{grad } g$

Cel mai mare divizor comun și cmmmc

Def: Fie $a, b \in \Delta$. Spunem că $d \in \Delta$ este cmmdc (a, b)
dacă: 1) $d | a$ și $d | b$ și
2) $\forall e \in \Delta$ cu $e | a$ și $e | b \Rightarrow e | d$

Spunem că $m \in \Delta$ este cmmmc (a, b) dacă:
1) $a | m$ și $b | m$ și
2) $\forall e \in \Delta$ cu $a | e$ și $b | e \Rightarrow m | e$.

Întrebări: 1) Există $\gcd(a, b)$ $\forall a, b \in \Delta$?
$\text{lcm}(a, b)$ . . . .
2) Dacă există $\gcd(a, b)$ și $\text{lcm}(a, b)$, sunt ele unice?

Prop: Dacă d_1, d_2 sunt gcd-uri pt a și b atunci $d_1 \sim d_2$
Dem: d, d_1 sunt divizori și pt a și pt b
$\Rightarrow d_1 | d$ și $d | d_1 \Rightarrow d \sim d_1$

Obs: Dacă $a | b \Rightarrow a = \gcd(a, b)$
$b = \text{lcm}(a, b)$

Temă: aflați $\gcd(X^{54} - 1, X^{17} - 1)$ în $\mathbb{Q}[X]$

Algoritmul lui Euclid

Input: $a, b \in \Delta$

Output: $\gcd(a,b) \in \Delta$

Dacă $b=0$, atunci $\gcd(a,b)=a$

Dacă $b \neq 0$: împărțim cu rest pe a la b

$$a = q_1 \cdot b + r_1$$

- Dacă $r_1 = 0 \Rightarrow b \mid a \Rightarrow \gcd(a,b) = b$
- Dacă $r_1 \neq 0 \Rightarrow b = q_2 \cdot r_1 + r_2$

Continuăm împărțirile cât timp restul este $\neq 0$.

$$r_1 = q_3 \cdot r_2 + r_3$$

$$\vdots$$

$$r_n = q_{n+2} \cdot r_{n+1} + r_{n+2}, \quad r_{n+2} \neq 0$$

$$r_{n+1} = q_{n+3} \cdot r_{n+3} + 0$$

Atunci ultimul rest nenul este $\gcd(a,b)$.

Alg lui Euclid extins Date $a, b \in \Delta$

există $u, v \in \Delta$ cu $\gcd(a,b) = u \cdot a + v \cdot b$

Obs: acești u și v nu sunt unici.

Exemplu:

Dt $a=54$, $b=17$ aflăm $\gcd(a,b) = u \cdot a + v \cdot b$

$54 = 3 \cdot 17 + 3$

$17 = 5 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$ STOP

Deci $\gcd(54,17) = 1$

$1 = 3 - 2 = 3 - (17 - 5 \cdot 3) = 6 \cdot 3 - 17 =$

$= 6(54 - 3 \cdot 17) - 17 =$

$= 6 \cdot 54 - 19 \cdot 17$

Verificare $1 = 6 \cdot 54 - 19 \cdot 17$

$u = 6$, $v = -19$

Def: Dacă $\gcd(a,b)=1$, spunem a și b prime între ele

Aplicații: Aflați dacă există $\hat{17}^{-1}$ în $\mathbb{Z}_{54}$.

$1 = 6 \cdot 54 - 19 \cdot 17$

$\hat{1} = \widehat{6 \cdot 54 - 19 \cdot 17}$

$\hat{1} = \hat{6} \cdot \hat{54} + \widehat{-19} \cdot \hat{17}$

$\hat{1} = \widehat{-19} \cdot \hat{17}$ (deoarece $\hat{54} = \hat{0}$)

$\widehat{-19} = \hat{35}$

Deci $\hat{17} \in U(\mathbb{Z}_{54})$ și $\hat{17}^{-1} = \hat{35}$

Dem Alg Euclid:

- Terminarea: în $\mathbb{Z}$: $b > r_1 > \dots > r_n \geq 0$

  în $K[X]$: $\gcd b > \gcd r_1 > \dots > \gcd r_n$
- Corectitudinea: $\gcd(a,b) = \gcd(b, a-bq) \quad \forall q \in \Delta$

  Perechile $\{a,b\}$ și $\{b, a-bq\}$ au aceeași divizori comuni
- Obs: $r_{i+2} < \frac{1}{2} r_i \quad \forall i$ cu $r_i \neq 0$.

Teoremă: În inelele $\mathbb{Z}$ și $K[X]$ orice ideal este principal

$\forall I \leq \mathbb{Z} \quad \exists n \in \mathbb{Z}$ cu $I = (n)$

$\leq K[X] \quad \exists f \in K[X]$ cu $I = (f)$

Dem: în $\mathbb{Z}$: ✓

Fie $I \neq \emptyset$ ideal în $K[X]$, aleg $f \in I$ pt care $\deg f$ este minim. $\emptyset \neq T$ ... □

Prop: Fie $a, b \in \Delta$. Atunci:

$a\Delta + b\Delta = \gcd(a,b)\,\Delta$

$a\Delta \cap b\Delta = \operatorname{lcmm}(a,b)\,\Delta$

~~$\gcd(a,b)\cdot\operatorname{lcmm}(a,b) =$~~

$\gcd(a,b)\cdot\operatorname{lcmm}(a,b) \sim a\cdot b$

Prop: 1) Fie $a, b \in \Delta$. Atunci $\gcd(a,b)=1 \Leftrightarrow \exists u, v \in \Delta$ cu $u\cdot a + v\cdot b = 1$.

Dem: „$\Rightarrow$" $\checkmark$ alg Euclid extins

„$\Leftarrow$" Știm $u\cdot a + v\cdot b = 1$

Dacă $d \mid a$ și $d \mid b$ $\Rightarrow d \mid ua+vb = 1$

$\Rightarrow d \mid a$, $1 \mid d$ $\Rightarrow d \sim 1$.

$\gcd(a,b) = 1$.

2) Dacă $d = \gcd(a,b)$, atunci $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Dem: $\exists u, v \in \Delta$ cu $d = u\cdot a + v\cdot b$.

$1 = u\cdot\frac{a}{d} + v\cdot\frac{b}{d}$ $\Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

3) $\gcd(a\cdot b, a\cdot c) = a\cdot\gcd(b,c)$ $\forall a, b \in \Delta$

Dem: $ab\Delta + ac\Delta = \{a\cdot bu + a\cdot cv \mid u, v \in \Delta\} =$

$= a\cdot\{bu + cv \mid u, v \in \Delta\} = a(b\Delta + c\Delta)$

4) Dacă $\gcd(a,b) = \gcd(a,c) = 1 \Rightarrow \gcd(a, bc) = 1$.

Dem: avem $1 = ua + vb$

$1 = u_1 a + v_1 b$ $\Big| \overset{(\times)}{\Rightarrow} 1 = uu_1 a^2 + uv_1 ac + u_1 vab + vv_1 bc$

$1 = a(\text{ceva}) + vv_1 bc \Rightarrow$

$\gcd(a, bc) = 1$

5) Dacă $a \mid bc$ și $\gcd(a,b) = 1$ atunci $a \mid c$.

Dem: Scriem $1 = ua + vb$ cu $u, v \in \Delta$

$\Rightarrow c = uac + vbc$

$a \mid bc$

$a \mid uac$ $\Big| \Rightarrow a \mid c$