Curs 13 — 12.01.2021

Aritmetică în $\mathbb{Z}$ și $K[X]$. Pol. ireductibile

Reamintim

$K[X]$

Teorema împărțirii cu rest

$f, g \in K[X]$, $g \neq 0$ $\exists!\, q, r \in K[X]$ a.î.

$f = g \cdot q + r$ $\quad \deg(r) < \deg(g)$

$f(x) \in K[X]$ $\deg(f) \geq 1$ ($= n$) în $K[X]/(f(x))$ un SCR este $\{a_0 + a_1 X + \dots + a_{n-1} X^{n-1} \mid a_0, \dots, a_{n-1} \in K\}$

în $K[X]$ definim la fel divizibilitatea

$f, g \in K[X]$ $\quad f \mid g \overset{\text{def}}{\iff} (\exists)\, q \in K[X]$ a.î. $g = f \cdot q$.

Exemple 1) $X - 1 \mid X^2 - 3X + 2$ $\quad (X^2 - 3X + 2 = (X-1)(X-2))$

2) E adevărat că $X^2 - 3X + 2 \mid X^3 - 3X + 2$?

cu thm. împ cu rest:

$X^3 - 3X + 2 = (X^2 - 3X + 2)(X + 3) + (4X - 4)$

$r = 4X - 4 \neq 0 \Rightarrow$

$\Rightarrow X^2 - 3X + 2 \nmid X^3 - 3X + 2$.

$f, g \in K[X]$ $\quad \operatorname{cmmdc}(f, g) =$ pol. $d(X)$ a.î. $d(X) \mid f(X)$, $d(X) \mid g(X)$, $d(X)$ are gradul cel mai mare cu ac. propr. și $d(X)$ e monic.

— " — pt $\operatorname{cmmmc}(f, g)$

Exemple Let $f = X^3 - 3X^2 + 3X - 1$, $g = X^3 - 3X + 2$

$f = g \cdot 1 + (-3X^2 + 6X - 3)$

$g = (-3X^2 + 6X - 3) \cdot \left(-\frac{1}{3}X - \frac{2}{3}\right) + 0$

$(f, g) = \operatorname{cmmdc}(f, g) = X^2 - 2X + 1 = (X-1)^2$

Aplicație (vezi seminar) $(X^n - 1, X^m - 1) = X^{(n,m)} - 1$

Aplicație info Scrieți un program în C++ care să calculeze $(2^{2100} - 1, 2^{950} - 1) = 2^{(2100, 950)} - 1 = 2^{50} - 1$.

$\mathbb{Z}$

Teorema împărțirii cu rest

$a, b \in \mathbb{Z}$, $b \neq 0$ $\quad \exists!\, q, r \in \mathbb{Z}$

$a = b \cdot q + r$, $\quad 0 \leq r < |b|$.

$n \geq 2$ în $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ un SCR este $\{0, 1, \dots, n-1\}$.

Divizibilitate $\quad a, b \in \mathbb{Z}$

$b \mid a \overset{\text{def}}{\iff} (\exists)\, c \in \mathbb{Z}$ a.î. $a = bc$

$(a \mid b \iff a\mathbb{Z} \supseteq b\mathbb{Z})$

$\operatorname{cmmdc}(a, b) =$ nr. natural d a.î. $d \mid a$ și $d \mid b$; mai mare cu ac. propr. $(-2, 4) = 2$

$\operatorname{cmmmc}(a, b) =$ nr. natural m a.î. $a \mid m$ și $b \mid m$; mai mic cu această propr. $[-2, 4] = 4$

Algoritmul lui Euclid

$a, b \in \mathbb{Z}$, $b \neq 0$

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ b &= r_1 \cdot q_2 + r_2 \\ &\vdots \\ r_{t-1} &= r_t \cdot q_{t+1} + r_{t+1} \\ r_t &= r_{t+1} \cdot q_{t+2} + 0 \end{aligned}$$

$r_{t+1} = \operatorname{cmmdc}(a, b) = (a, b)$ pt $k, l \in \mathbb{Z}$

$= a \cdot k + b \cdot l$

- $(a, b) = 1 \iff (\exists)\, a', b' \in \mathbb{Z}$ a.î. $a' \cdot a + b' \cdot b = 1$.

Similar

- orice ideal al lui $K[X]$ e principal, i.e.
$(\forall) I$ ideal al lui $K[X] \Rightarrow (\exists) f(x) \in K[X]$ a.î. $I = (f(x))$
(Obs. Dem. e "copy-paste" cu cea de)
- $K[X]$ e domeniu de integritate
$U(K[X]) = K^* (= K \setminus \{0\})$

- Exemplu $(x^3-1)\mathbb{Q}[x] + (x^2-1)\mathbb{Q}[x] = (x-1)\mathbb{Q}[x]$
unde $x-1 = (x^3-1, x^2-1)$.
$(x^3-1)\mathbb{Q}[x] \cap (x^2-1)\mathbb{Q}[x] = (x^4+x^3-x-1)\mathbb{Q}[x]$
unde $x^4+x^3-x-1 = [x^3-1, x^2-1] = (x^3-1)(x+1)$.

Inelul $(\mathbb{Z}, +, \cdot)$

- orice ideal al lui $\mathbb{Z}$ e principal ($n\mathbb{Z}$, $n \in \mathbb{N}$)
- domeniu de integritate
- $U(\mathbb{Z}) = \{\pm 1\}$

- $a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z}$
$a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}$
$a \cdot b \sim (a,b) \cdot [a,b]$
[asociat în divizibilitate]

LCR (versiunea din $K[X]$)

$f, g \in K[X]$ $(f,g) = 1$.

$$K[X]/(f \cdot g) \simeq K[X]/(f) \times K[X]/(g)$$

Exemplu Arătați că $\mathbb{Q}[x]/(x^2-1)$ este izomorf cu produsul direct de inele $\mathbb{Q}[x]/(x-1) \times \mathbb{Q}[x]/(x+1)$
(mai mult, este izomorf cu produsul direct de inele $\mathbb{Q} \times \mathbb{Q}$)

Aplicăm LCR pt $f(x) = x-1$, $g(x) = x+1$ $(f,g) = 1$ și $\mathbb{Q}[x]/(x^2-1) \simeq \mathbb{Q}[x]/(x-1) \times \mathbb{Q}[x]/(x+1)$
(pt ultima parte apl. T.F.I $\mathbb{Q}[x]/(x-1) \simeq \mathbb{Q}$
$\mathbb{Q}[x]/(x+1) \simeq \mathbb{Q}$)

Lema chineză a resturilor

$m, n \in \mathbb{Z}$ $(m,n) = 1$ $\mathbb{Z}_{mn}$ este izomorf cu produsul direct de inele $\mathbb{Z}_m \times \mathbb{Z}_n$

Def Un polinom neconstant $f(x) \in K[x]$ (i.e. $\text{grad}(f) \geq 1$) s.n. **polinom ireductibil** dacă f nu se poate scrie ca produs de 2 polinoame neconstante. Echivalent, f nu are decât divizorii a și af cu $a \in K^*$.

Propr în $K[x]$,
- polinoamele de grad 1 sunt ireductibile
- un polinom ireductibil de grad ≥ 2 nu are rădăcini în K (**dem**: dc. $f(x)$ are o rădăcină în $K \overset{\text{Bézout}}{\Rightarrow} f(x) = (x-a)g(x)$, $\text{grad} = n$, $\text{grad} = \text{grad} - 1 \geq 1$ ⚠)
- (seminar) un polinom de grad 2 sau 3 este ireductibil în $K[x] \Leftrightarrow$ nu are rădăcini în K.

Atenție!!! $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$ și f este reductibil în $\mathbb{Q}[x]$ dar f nu are rădăcini în $\mathbb{Q}$

Exemplu x^2-2 ireductibil în $\mathbb{Q}[x]$, reductibil în $\mathbb{R}[x]$ ($x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$ în $\mathbb{R}[x]$)

Teoremă (Euclid) (cu dem. "copy-paste")
- orice polinom neconstant $f \in K[x]$ se poate scrie ca produs de polinoame ireductibile
- mulțimea polinoamelor ireductibile monice este infinită

Număr prim $p \neq 0, \pm 1$ în $\mathbb{Z}$, p s.n. prim dacă $p \mid ab \Rightarrow p \mid a$ sau $p \mid b$

Număr ireductibil $p \neq 0, \pm 1$ în $\mathbb{Z}$, p s.n. ireductibil dacă p nu se poate scrie ca produsul a 2 nr. întregi diferite de ± 1. Echivalent, p are ca divizori doar pe $\pm 1, \pm p$.

Teoremă (Euclid)
- orice număr întreg N diferit de $0, \pm 1$ se poate scrie în mod unic ca produs de numere prime. ($N = \pm p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, $p_1, \ldots, p_s$ prime pozitive distincte, și $\alpha_1, \ldots, \alpha_s \geq 1$, $s \geq 1$)
- mulțimea numerelor prime este infinită

Consecință Orice polinom neconstant $F(x) \in K[x]$ se scrie în mod unic sub forma $F(x) = a\,\pi_1(x)^{\alpha_1} \cdots \pi_s(x)^{\alpha_s}$ cu $\pi_1, \ldots, \pi_s$ pol. monice ireductibile distincte 2 câte 2, $a \in K^*$, $\alpha_1, \ldots, \alpha_s \geq 1$

Reamintesc

Teorema fundamentală a algebrei Orice polinom neconstant $f(x) \in \mathbb{C}[X]$ are exact grad(f) rădăcini în $\mathbb{C}$.

⇓

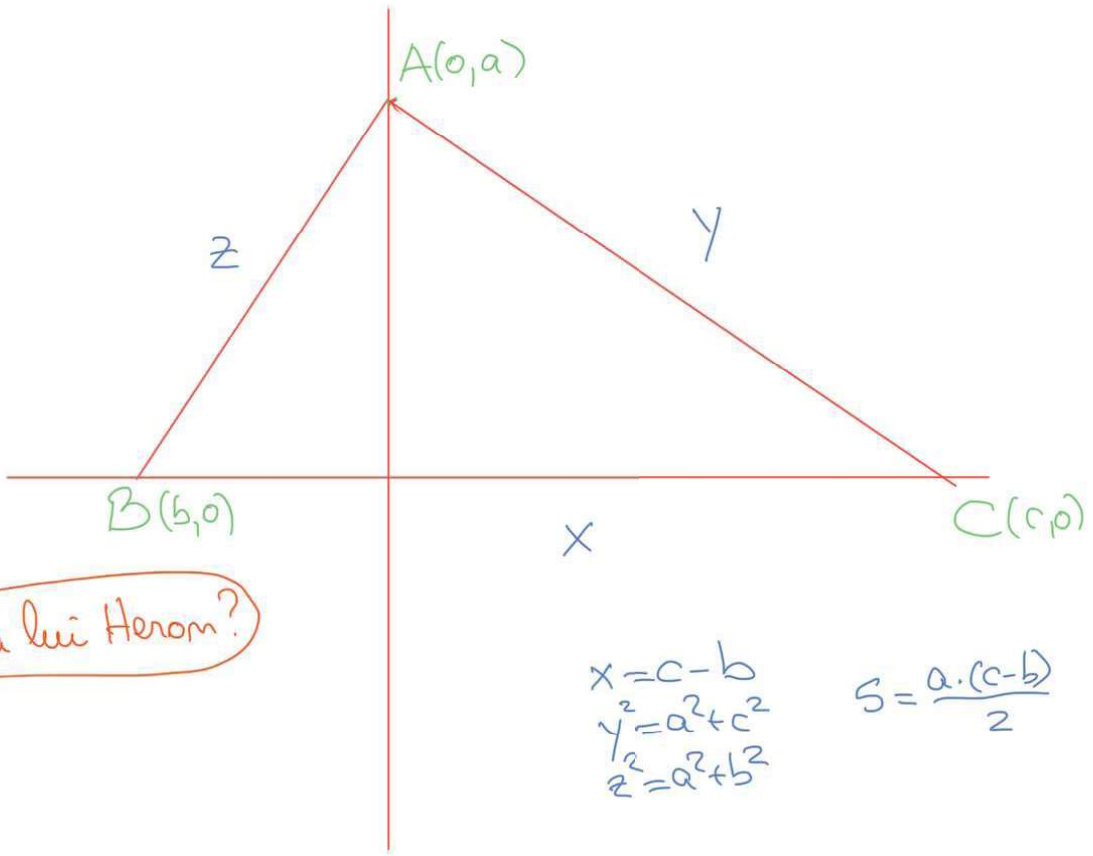
❗ 1) Polinoamele ireductibile din $\mathbb{C}[X]$ sunt polinoamele de grad 1.

2) Polinoamele ireductibile din $\mathbb{R}[X]$ sunt polinoamele de grad 1 și cele de grad 2 fără rădăcini reale.

❓ Dar pol. ired. din $\mathbb{Q}[X]$?

❗ Avem în $\mathbb{Q}[X]$ pol. ireductibile de orice grad. De ex $X^n - 2$ este ireductibil în $\mathbb{Q}[X]$ $(\forall) n \geq 1$. (se folosește criteriul lui Eisenstein, vezi seminar)

FOR FUN



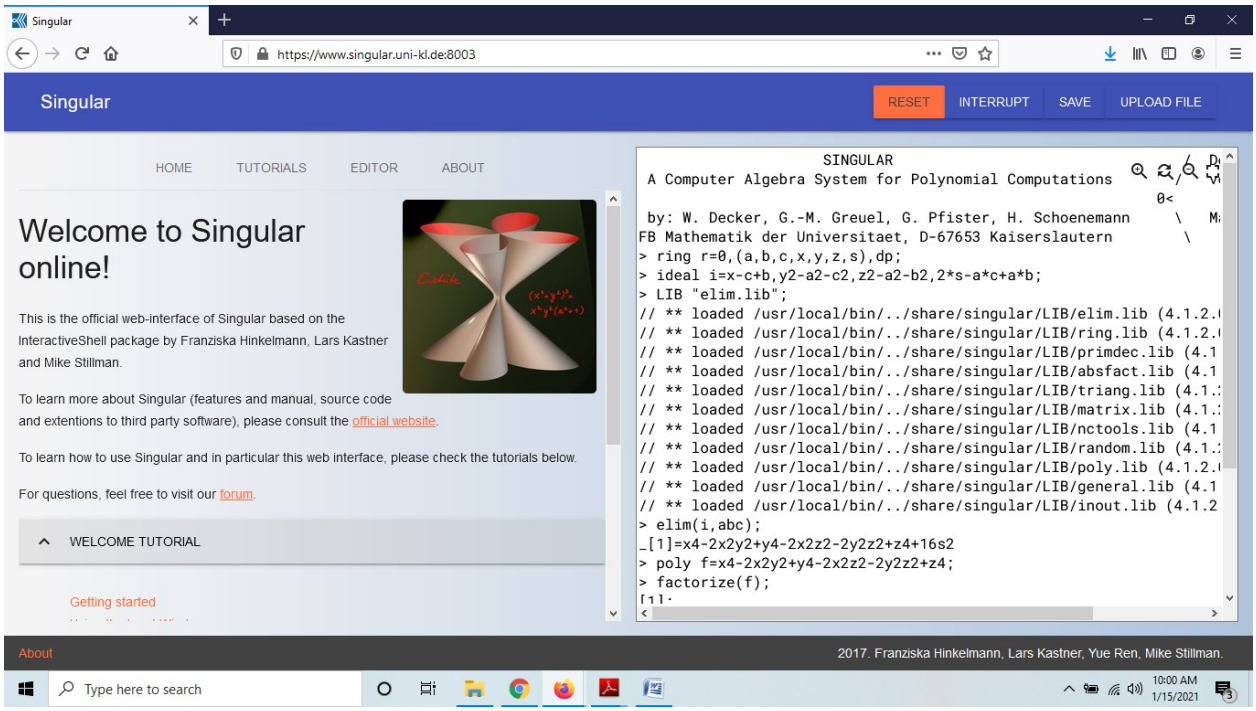
Formula lui Heron?

$x = c - b$

$y^2 = a^2 + c^2$

$z^2 = a^2 + b^2$

$S = \frac{a \cdot (c-b)}{2}$




```
> ring r=0,(a,b,c,x,y,z,s),dp;

> ideal i=x-c+b,y2-a2-c2,z2-a2-b2,2*s-a*c+a*b;

> LIB "elim.lib";

> elim(i,abc);

_[1]=x4-2x2y2+y4-2x2z2-2y2z2+z4+16s2

> poly f=x4-2x2y2+y4-2x2z2-2y2z2+z4;

> factorize(f);

[1]:

  _[1]=1

  _[2]=-x+y-z

  _[3]=x+y-z

  _[4]=-x+y+z

  _[5]=x+y+z

[2]:

  1,1,1,1,1
```