R • K corp (= inel în care orice element nenul este inversabil)

• $n \geq 2$ $\quad \mathbb{Z}_n$ e corp ($\Leftrightarrow \mathbb{Z}_n$ e domeniu de integritate) $\Leftrightarrow n$ e prim.

• Exemple de corpuri comutative ($\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ cu p - prim)

R R inel com. $\quad R[X] = \{ \underbrace{a_0 + a_1X + \dots + a_nX^n}_{\text{polinom}} \mid a_0, \dots, a_n \in R, n \in \mathbb{N} \}$

$f(X) = a_0 + \dots + a_nX^n$, $a_n \neq 0$ $\quad$ grad$(f) = n$ (gradul polinomului nul este $-\infty$)

• $f(X)$ s.n. monic dacă $a_n = 1$.

grad$(f+g) \leq \max\{$grad(f), grad$(g)\}$

grad$(f \cdot g) \leq$ grad(f) + grad(g)

$R[X]$ este inel comutativ împreună cu "+" și "·" definite astfel:

$f(X) = \sum_{i=0}^{n} a_iX^i$; $g(X) = \sum_{i=0}^{n} b_iX^i \rightsquigarrow f(X) + g(X) = \sum_{i=0}^{n} (a_i + b_i) \cdot X^i$

$f(X) = \sum_{i=0}^{n} a_iX^i$; $g(X) = \sum_{i=0}^{m} b_iX^i \rightsquigarrow f(X) \cdot g(X) = \sum_{i=0}^{n+m} \left(\sum_{j+l=i} a_jb_l \right) X^i$

Ex $\quad f(X) = 2X^2 + 3X + 1$, $g(X) = 3X^2 - 1 \in \mathbb{Q}[X]$

$f(X) \cdot g(X) = (2X^2 + 3X + 1) \cdot (3X^2 - 1) = 6X^4 - 2X^2 + 9X^3 - 3X + 3X^2 - 1 =$
$= 6X^4 + 9X^3 + X^2 - 3X - 1$.

$f(X) + g(X) = 5X^2 + 3X$.

Inelul de polinoame $K[X]$, K corp comutativ

Proprietăți $\quad$ • $K[X]$ e domeniu de integritate și $U(K[X]) = K \setminus \{0\}$.

Dem $\quad f(X) = a_0 + \dots + a_nX^n \neq 0$ ($n \geq 0$, $a_n \neq 0$)

$g(X) = b_0 + \dots + b_mX^m \neq 0$ ($m \geq 0$, $b_m \neq 0$)

$\boxed{a_n \neq 0, b_m \neq 0 \Rightarrow a_nb_m \neq 0 \text{ în } K}$

$f(X) \cdot g(X) = \sum_{i=0}^{n+m} \left(\sum_{j+l=i} a_jb_l \right) X^i =$

$= \underset{\neq 0}{a_nb_m} X^{n+m} + \dots \neq 0 \Rightarrow K[X]$ dom. de integritate

și în particular grad$(f(X) \cdot g(X))$ = grad$(f(X))$ + grad$(g(X))$. (*)

Din $(*) \Rightarrow U(K[X]) = K\setminus\{0\} = U(K)$ (Fie $f(x) \in U(K[X]) \Rightarrow$
$\Rightarrow (\exists)\ g(x) \in K[X]$ a.î. $f(x)\cdot g(x) = 1$. Din $(*) \Rightarrow$

$$\underset{\substack{\parallel \\ 0}}{\mathrm{grad}(1)} = \mathrm{grad}(f(x)) + \mathrm{grad}(g(x)) \Rightarrow \begin{cases} \mathrm{grad}(f(x)) = 0 \\ \mathrm{grad}(g(x)) = 0 \end{cases} \Rightarrow$$

$\Rightarrow f(x), g(x)$ sunt polinoame constante nenule. $\Rightarrow$ "$\subseteq$")

"$\supseteq$" evidentă din definiția corpului.

•• <u>Propoziție</u> Fie $\varphi: K \to S$ un morfism de inele (K poate fi chiar inel) și $b \in S$. Funcția $\tilde{\varphi}: K[X] \to S$ definită prin $\tilde{\varphi}(a_0 + a_1X + \dots + a_nX^n) = \varphi(a_0) + \varphi(a_1)\cdot b + \dots + \varphi(a_n)\cdot b^n$ este un morfism de inele.

<u>Exemplu</u> Fie $K = \mathbb{Q}$, $S = \mathbb{R}$ și $\varphi: \mathbb{Q} \to \mathbb{R}$ $\varphi(a) = a\ (\forall)\ a \in \mathbb{Q}$. $b = \sqrt{2}$.

$\tilde{\varphi}: \mathbb{Q}[X] \to \mathbb{R}$ $\tilde{\varphi}(a_0 + a_1X + \dots + a_nX^n) = a_0 + a_1\sqrt{2} + \dots + a_n(\sqrt{2})^n$

$(\forall)\ a_0 + a_1X + \dots + a_nX^n \in \mathbb{Q}[X]$; $\tilde{\varphi}$ este morfism de inele.

<u>Teorema împărțirii cu rest</u> Fie $f(x), g(x) \in K[X]$ cu $g(x) \neq 0$. Atunci există și sunt unice polinoamele $q(x), r(x) \in K[X]$ a.î.

$$f(x) = g(x)\cdot q(x) + r(x), \quad \mathrm{grad}(r(x)) < \mathrm{grad}(g(x)).$$

<u>Exemplu</u> Aplicați teorema împărțirii cu rest pentru polinoamele
$f(x) = x^3 - 3x + 2$, $g(x) = 2x + 1$; $f(x), g(x) \in \mathbb{Q}[X]$.

$$\begin{array}{l|l} x^3 - 3x + 2 & 2x+1 \\ \cline{2-2} -x^3 - \frac{1}{2}x^2 & \frac{1}{2}x^2 - \frac{1}{4}x - \frac{11}{8} \\ \cline{1-1} \ /\ -\frac{1}{2}x^2 - 3x + 2 & \\ \quad +\frac{1}{2}x^2 + \frac{1}{4}x & \\ \cline{1-1} \quad /\ -\frac{11}{4}x + 2 & \\ \qquad +\frac{11}{4}x + \frac{11}{8} & \\ \cline{1-1} \qquad /\quad \frac{27}{8} & \end{array}$$

$$f(x) = g(x)\cdot \underbrace{\left(\frac{1}{2}x^2 - \frac{1}{4}x - \frac{11}{8}\right)}_{q(x)} + \underbrace{\frac{27}{8}}_{r(x)}$$

$$0 = \mathrm{grad}\, r(x) < \mathrm{grad}\, g(x) = 1.$$

Teorema lui Bézout Fie $f(x)\in K[X]$ și $a\in K$. Atunci restul împărțirii lui $f(x)$ la $(x-a)$ este $f(a)$. În particular, a este rădăcină a lui $f(x)$ $\iff$ $f(x)=(x-a)\cdot g(x)$ pentru un $g(x)\in K[X]$.

Dem a e rădăcina lui $f(x)$ (vezi def. mai jos) $\iff f(a)=0$.

T. împ. cu rest $\Rightarrow$ $f(x)=(x-a)\cdot q(x)+\underset{b}{\underset{\shortparallel}{r(x)}}$, cu $\operatorname{grad}(r(x))<\underset{1}{\underset{\shortparallel}{\operatorname{grad}(x-a)}}$

$\Rightarrow \operatorname{grad}(r(x))\leq 0 \Rightarrow r(x)=b\in K$.

$f(a)=(a-a)\cdot q(a)+\underset{b}{\underset{\shortparallel}{r(a)}}=b$. $\Rightarrow$ echivalența ■

Obs În exemplul anterior puteam calcula restul împărțirii lui $f(x)=x^3-3x+2$ la $g(x)=2x+1$ astfel: $f\left(-\frac{1}{2}\right)=-\frac{1}{8}+\frac{3}{2}+2=\frac{27}{8}$.

$$f(x)=g(x)\cdot q(x)+f\left(-\tfrac{1}{2}\right)$$

Def 1) Dacă $f(x)\in K[X]$, $f(x)=a_0+a_1X+\dots+a_nX^n$ (de exemplu $f(x)=3+2x+x^2\in\mathbb{Q}[x]$), $b\in S$ (de ex $\sqrt{2}\in\mathbb{R}$) și K e subinel al lui S (de ex $\mathbb{Q}\subseteq\mathbb{R}$), atunci $f(b)=a_0+a_1b+\dots+a_nb^n$ s.n. valoarea polinomului $f(x)$ în b.
(de ex $f(\sqrt{2})=3+2\sqrt{2}+2=5+2\sqrt{2}$). b s.n. rădăcină a lui $f(x)$ dacă $f(b)=0$.

2) Fie $f(x)\in K[X]$ și $b\in K$. b s.n. rădăcină a lui f. b s.n. rădăcină multiplă de ordin $l\geq 1$ (sau rădăcină cu ordinul de multiplicitate $l\geq 1$) a lui f dacă $f(x)=(x-b)^l g(x)$, $g(x)\in K[x]$ și $g(b)\neq 0$.

3) Fie $f(x)\in K[X]$ și $b\in K$ a

Exemple 2) $f(x)=x^2+1\in\mathbb{R}[X]$ nu are rădăcini reale, dar $f(x)=x^2-2$ are.
3) $f(x)=(x-1)^3(x+2)(x-3)$ are 5 rădăcini; 1 e rădăcină cu ordin de multiplicitate 3; $-2, 3$ sunt rădăcini cu ordin de multiplicitate 1.

Obs 1) Dacă $f(x)\in K[x]$, $\operatorname{grad}(f(x))=n\geq 1$, are rădăcinile $\alpha_1,\dots,\alpha_r\in K$ fiecare având ordinul de multiplicitate $n_1,\dots,n_r$, atunci
$$f(x)=(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdot\ldots\cdot(x-\alpha_r)^{n_r}\cdot g(x),$$

cu $g(X) \in K[X]$ și $g(\alpha_j) \neq 0$ $(\forall)$ $j = \overline{1,r}$. În particular $f(X)$ are $m_1 + \dots + m_r$ rădăcini.

2) Deoarece $K[X]$ e domeniu de integritate $\Rightarrow$

$$\underbrace{\operatorname{grad}(f(X))}_{n} = \operatorname{grad}\left((X-\alpha_1)^{m_1} \cdot \ldots \cdot (X-\alpha_r)^{m_r}\right) + \operatorname{grad}(g(X)) \geq m_1 + \dots + m_r.$$

3) Un polinom nenul $f(X) \in K[X]$ are cel mult $\operatorname{grad}(f(X))$ rădăcini.

$\boxed{Q1}$ Ce legătură există între rădăcinile unui polinom și coeficienții polinomului?

Teoremă (Relațiile lui Viète) Fie $f(X) = a_0 + a_1 X + \dots + a_n X^n \in K[X]$ cu $a_n \neq 0$, $n \geq 1$. Presupunem că $f(X)$ are n rădăcini $\alpha_1, \dots, \alpha_n \in K$. Atunci

$$f(X) = a_n (X-\alpha_1) \cdot \ldots \cdot (X-\alpha_n)$$

și au loc următoarele egalități

$$\begin{cases} \sum_{i=1}^{n} \alpha_i = \alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{a_{n-1}}{a_n} \\ \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_1\alpha_n + \dots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n} \\ \dots \\ \sum_{1 \leq i_1 < \dots < i_j \leq n} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_j} = (-1)^j \frac{a_{n-j}}{a_n} \\ \dots \\ \alpha_1 \alpha_2 \cdots \alpha_n = (-1)^n \frac{a_0}{a_n}. \end{cases}$$

Exemplu Polinomul $P(X) = 1 \cdot X^3 + 3X + 1 \in \mathbb{C}[X]$ are 3 rădăcini $\alpha_1, \alpha_2, \alpha_3$. Calculați $\alpha_1^2 + \alpha_2^2 + \alpha_3^2$.

Din Viète $\Rightarrow$
$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = -\frac{0}{1} = 0 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \frac{3}{1} = 3 \\ \alpha_1\alpha_2\alpha_3 = -\frac{1}{1} = -1 \end{cases}$$

$$\boxed{\alpha_1^2 + \alpha_2^2 + \alpha_3^2} = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = 0 - 6 = \boxed{-6}$$

$\Rightarrow$ P are o rădăcină reală și 2 complexe nereale.

$\boxed{Q2}$ Dat un polinom neconstant $f(x) \in \mathbb{C}[X]$ îi pot determina rădăcinile în "funcție de" coeficienții săi?

- da pentru orice polinoame de grad 2 (vine din antichitate)
- da —"— 3 (Cardano $\rightsquigarrow$ 1545)
- da —"— 4 (Ferrari $\rightsquigarrow$ sec 16)
- $\boxed{\text{NU}}$ pentru polinoame generale de grad ≥ 5 (Abel 1829 pe baza teoriei lui Galois)

Teorema fundamentală a algebrei (TFA) Orice polinom neconstant $f(x) \in \mathbb{C}[X]$ are exact grad$(f(x))$ rădăcini. (început de secol 19)

Obs TFA nu mai e valabilă dacă punem în loc de $\mathbb{C}$ $\mathbb{Q}$ sau $\mathbb{R}$.

Observație Folosind formulele lui Cardano se pot afla $\alpha_1, \alpha_2, \alpha_3$ din exemplul anterior.

Ele sunt:

$$\alpha_1 = \sqrt[3]{\tfrac{1}{2}(-1+\sqrt{5})} + \sqrt[3]{\tfrac{1}{2}(-1-\sqrt{5})} \in \mathbb{R}$$

$$\alpha_2 = \omega\sqrt[3]{\tfrac{1}{2}(-1+\sqrt{5})} + \omega^2\sqrt[3]{\tfrac{1}{2}(-1-\sqrt{5})} \in \mathbb{C}\setminus\mathbb{R}$$

$$\alpha_3 = \omega^2\sqrt[3]{\tfrac{1}{2}(-1+\sqrt{5})} + \omega\sqrt[3]{\tfrac{1}{2}(-1-\sqrt{5})} \in \mathbb{C}\setminus\mathbb{R},$$

unde $\omega\left(=\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Teoremă Fie K un corp, $f \in K[X]$ un polinom neconstant de grad $n \geq 1$. Atunci elementele inelului factor $K[X]/(f)$ se reprezintă unic sub forma $a_0 + a_1X + \dots + a_{n-1}X^{n-1}$ (modulo (f)). În particular, dacă $K = \mathbb{Z}_p$ (p-prim, $p \geq 2$), atunci $K[X]/(f)$ are p^n elemente.

Dem $K[X]/(f) = \left\{ \overline{a_0 + a_1X + \dots + a_{n-1}X^{n-1}} \mid a_0, \dots, a_{n-1} \in K, n \in \mathbb{N}^* \right\}$

unde $\overline{a_0 + a_1X + \dots + a_{n-1}X^{n-1}}$ reprezintă clasa de echivalență a lui $a_0 + a_1X + \dots + a_{n-1}X^{n-1}$ modulo idealul generat de f.

Ideal:

Teorema împărțirii cu rest:

Fie $g(x) \in K[x]$ $\quad g(x) = f(x) \cdot q(x) + r(x)$, grad $(r(x)) <$ grad $(f(x))$

$\Rightarrow g(x) - r(x) = f(x) \cdot q(x) \in (f(x)) \Rightarrow \widehat{g(x)} = \widehat{r(x)}$

(i.e. $g(x) - r(x) \in (f(x))$) $\boxed{\checkmark}$

Aplicație la T.F.I

Arătați că mulțimea $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ este un corp în raport cu ad. și înm. nr. reale. Demonstrați că

$$\mathbb{Q}[x]/(x^2-2) \simeq \mathbb{Q}[\sqrt{2}]$$ izomorfism de inele

Idee (vezi detalii la seminar) $\mathbb{Q}[x] \xrightarrow{\varphi} \mathbb{Q}[\sqrt{2}]$ $\quad \varphi(P(x)) = P(\sqrt{2})$ morfism de inele surj

Calculez $\operatorname{Ker} \varphi = (x^2-2)$

T.F.I