Teorema de împărțire cu rest:

Fie A inel comutativ, $f, g \in A[X]$ a.î. $g \neq 0$ și coeficientul dominant al lui g este inversabil în A. Atunci există și sunt unice $C, R \in A[X]$ pentru care:

$$\begin{cases} (i) & f = C \cdot g + R \\ (ii) & \deg R < \deg g \end{cases}$$

C = câtul împărțirii cu rest a lui f la g
R = restul împărțirii cu rest a lui f la g

Dem.:

Existența:

Dacă $\deg(f) < \deg(g)$

$$f = \underset{C}{\underset{\parallel}{0}} \cdot g + \underset{R}{\underset{\parallel}{f}}$$

Fie $g = b_m X^m + \ldots + b_0$, $b_m \in U(A)$

Dem. prin inducție după $n \geq m$ că pentru orice f cu $\deg(f) \leq n$ există C, R cu (i) + (ii)

$\underline{n = m}$ $\quad f = a_m X^m + \ldots + a_0$

$f - a_m b_m^{-1} g$ are grad $< m$

Atunci $f = \underbrace{a_m b_m^{-1}}_{C} g + (\underbrace{f - a_m b_m^{-1} g}_{R})$

Presupunem adevărat pentru $n-1$ și demonstrăm pentru n: $n > m$

Fie f cu $\deg(f) \leq n$.

Dacă $\deg(f) < n$, există C și R din ipoteza de inducție.

Dacă $\deg(f) = n$, fie $f = a_n X^n + \ldots + a_0$

$f - a_n b_m^{-1} X^{n-m} g$ are grad $< n$ (deci $\leq n-1$)

Aplic ipoteza de inducție pentru

$\Rightarrow (\exists)\ C_0, R_0 \in A[X]$ cu

$$f - a_n b_m^{-1} X^{n-m} g = C_0 g + R_0$$

$$\deg R_0 < \deg g$$

$$\Rightarrow f = \underbrace{(a_n b_m^{-1} X^{n-m} + C_0)}_{C} g + \underbrace{R_0}_{R}$$

Unicitatea:

Presupunem $f = C_1 \cdot g + R_1 = C_2 \cdot g + R$ cu

$C_1, C_2, R_1, R_2 \in A[X] \Rightarrow$

$\deg(R_1), \deg(R_2) < \deg(g)$

$\Downarrow$

$\deg(R_2 - R_1) < \deg(g)$

$\Rightarrow (C_1-C_2)\cdot g = R_2-R_1$

Dacă $C_1 \neq C_2 \Rightarrow \deg((C_1-C_2)\cdot g) = \overbrace{\deg(C_1-C_2)}^{\geq 0}\cdot$
$\deg(g) \geq \deg(g)$

Contradicție! $\Rightarrow C_1 = C_2 \Rightarrow R_1 = R_2$

Teoremă: Fie K un corp comutativ. Atunci orice ideal din $K[X]$ este principal.

Dem.:

Fie I ideal din $K[X]$.
Dacă $I=0$, dar $I=(0)$.
Presupunem $I\neq 0$. Fie g un element $\neq 0$ din I de grad minim posibil. Arăt că $I=(g)$.

$$(g) = \{hg \mid h\in K[X]\}$$

„$\supseteq$": Fie $hg \in (g)$, unde $h\in K[X]$.

$$\left.\begin{array}{l} g\in I \\ h\in K[X]\end{array}\right| \xRightarrow[\text{ideal}]{I} hg\in I$$

„$\subseteq$": Fie $f\in I$. Împart f la g.

$(\exists)\ C, R \in K[X]$ cu $f = g\cdot C + R$
$\deg(R) < \deg(C)$

$$\Rightarrow R = \underbrace{\underset{\in I}{f} - \underset{\in I}{C\cdot g}}_{} \in I$$
$\in I$

Dacă $R \neq 0$, contrazic minimalitatea lui $\deg(g)$.

Așadar, $R = 0 \Rightarrow f = C \cdot g \in (g)$

Descrierea inelelor factor $\frac{A[X]}{(g)}$, unde g are coeficient dominant inversabil

$f \in A[X]$

$$f = C \cdot g + R \quad \text{cu } \deg(R) < \underbrace{\deg(g)}_{= m}$$

$$\hat{f} = \hat{C} \cdot \underbrace{\hat{g}}_{= 0} + \hat{R} = \hat{R}$$

$$\frac{A[X]}{(g)} = \{ \hat{R} \mid R \in A[X], \deg(R) \leq m-1 \}$$

R_1, R_2 grade $\leq m-1$

$$\hat{R_1} = \hat{R_2} \Leftrightarrow R_1 = R_2$$

În particular, dacă A este inel finit cu q elemente (și $\deg(g) = m$):

$$\frac{A[X]}{(g)} = \{ a_0 + a_1 X + \ldots + a_{m-1} X^{m-1} \mid a_0, \ldots, a_{m-1} \in R \}$$

$$\left| \frac{A[X]}{(g)} \right| = q^m$$

Teoremă: (Proprietatea de universalitate a inelelor de polinoame)

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[dr, "f"'] & A[X] \arrow[d, dashed, "\bar{f}"] \\ & B \ni x \end{tikzcd}$$

Fie A un inel comutativ, $\varphi : A \to A[X]$ morfismul canonic ($\varphi(a) = a$, $(\forall)\, a \in A$). Atunci pentru orice inel comutativ B, orice morfism de inele $f : A \to B$ și orice element $x \in B$, există un unic morfism de inele $\bar{f} : A[X] \to B$ pentru care $\bar{f}\varphi = f$ [adică $\bar{f}(a) = f(a)$, $(\forall)\, a \in A$] și $\bar{f}(X) = x$

Dem. (schiță):

Existența (schiță):

Fie $\bar{f} : A[X] \to B$ definit prin:

$$\bar{f}(a_0 + a_1X + \ldots + a_nX^n) = f(a_0) + f(a_1)x + \ldots + f(a_n)x^n$$

Atunci $\bar{f}$ morfism de inele (exercițiu: calcul).

$$\bar{f}(a) = f(a)$$
$$\bar{f}(X) = x$$

Unicitatea:

Dacă $\tilde{f}$ este un alt astfel de morfism, atunci

$$\tilde{f}(a_0 + a_1X + \ldots + a_nX^n) = \tilde{f}(a_0) + \tilde{f}(a_1)\tilde{f}(X) + \ldots + \tilde{f}(a_n)\tilde{f}(X)^n$$
$$= f(a_0) + f(a_1)x + \ldots + f(a_n)x^n$$
$$= \bar{f}(a_0 + a_1X + \ldots + a_nX^n),$$

deci $\tilde{f} = \bar{f}$

Caz particular:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[dr, "Id_A"'] & A[X] \arrow[d, dashed, "\varphi_a"] \\ & A \ni a \end{tikzcd}$$

Pentru $a \in A$:

$(\exists!)$ $\varphi_a : A[X] \to A$ morfism de inele cu $\varphi_a(c) = c$, $(\forall)\, c \in A$ și $\varphi_a(X) = a$

$$\varphi_a(\underbrace{a_0 + a_1X + \ldots + a_nX^n}_{= P}) = \underbrace{a_0 + a_1a + \ldots + a_n \cdot a^n}_{\text{not.}\ = P(a)}$$

$P(a)$ = valoarea lui P în a

φ_a = evaluarea lui P în a

φ_a morfism de inele $\Rightarrow$ $(P+Q)(a) = P(a) + Q(a)$

$(PQ)(a) = P(a)\,Q(a)$

$a \in A$ s.n. **rădăcină** a lui P dacă $P(a) = 0$

$P \in A[X]$: Definim $\tilde{P} : A \to A$, $\tilde{P}(a) = P(a)$
$\hat{A}$

$\tilde{P}$ = funcția polinomială asociată lui P

Exemplu:

Se poate ca $P \neq Q$ și $\tilde{P} = \tilde{Q}$.

$P = X^2 + X + \hat{1} \in \mathbb{Z}_2[X]$

$Q = \hat{1} \in \mathbb{Z}_2[X]$

$\tilde{P} : \mathbb{Z}_2 \to \mathbb{Z}_2$, $\tilde{P}(\hat{0}) = \hat{1}$, $\tilde{P}(\hat{1}) = \hat{1}$

$\tilde{Q} : \mathbb{Z}_2 \to \mathbb{Z}_2$, $\tilde{Q}(\hat{0}) = \tilde{Q}(\hat{1}) = \hat{1}$

Def.: Fie $P, Q \in A[X]$.
Spunem că P îl divide pe Q, scriem $P \mid Q$ dacă $(\exists)$ $F \in A[X]$ cu $Q = P \cdot F$.

Teorema lui Bézout:

Fie $f \in A[X]$ şi $a \in A$. Atunci $f(a) = 0 \iff X - a \mid f$

a rădăcină a lui f

Dem.:

„<=": $X - a \mid f \Rightarrow (\exists)\, g \in A[X]$ cu $f = (X-a)g \overset{\varphi_a}{\Rightarrow}$

$\Rightarrow f(a) = \underbrace{(a-a)}_{0} \cdot g(a) = 0$

„=>": Presupunem $f(a) = 0$.
Împart f la $X - a$.

$f = (X-a)C + R$ $\qquad \deg(R) < 1$

$\Downarrow$

$f = (X-a)C + \alpha$ $\qquad R = \alpha \in A$

$\Downarrow \varphi_a$

$f(a) = 0 + \alpha \Rightarrow \alpha = 0 \Rightarrow f = (X-a)C$

$\Downarrow$

$X - a \mid f$

Aplicație

$$\left.\begin{array}{l} A \text{ inel comutativ} \\ a \in A \end{array}\right| \Rightarrow \frac{A[X]}{(X-a)} \simeq A$$

$\varphi_a : A[X] \to A$ morf. de inele

$\varphi_a(f) = f(a)$, $(\forall)\ f \in A[X]$

φ_a surjectiv $\quad \lambda \in A$, iau $f = \lambda \in A[X]$

$\Downarrow \qquad\qquad\qquad\qquad \varphi_a(f) = \lambda$

$\operatorname{Im} \varphi_a = A$

$f \in \operatorname{Ker} \varphi_a \Leftrightarrow \varphi_a(f) = 0 \Leftrightarrow f(a) = 0 \overset{\text{Bézout}}{\Longleftrightarrow} X-a \mid f$

$\Leftrightarrow f \in (X-a)$

Deci $\operatorname{Ker} \varphi_a = (X-a)$

Teorema fundamentală de izomorfism pentru inele pentru φ_a

$$\left(\begin{array}{c} R \to S \text{ morf. de inele} \\ \Downarrow \\ \dfrac{R}{\operatorname{Ker} \varphi} \simeq \operatorname{Im} \varphi \end{array} \right)$$

$$\frac{A[X]}{(X-a)} \simeq A$$

Exemple:

1) $\frac{\mathbb{Q}[X]}{(X^2-X)} \simeq \mathbb{Q}\times\mathbb{Q}$ şi $\frac{\mathbb{Z}[X]}{(X^2-X)} \simeq \mathbb{Z}\times\mathbb{Z}$

În $\mathbb{Q}[X]$:

Fie $I=(X)$ şi $J=(X-1)$ în $\mathbb{Q}[X]$.

I şi J sunt comaximale, adică $\underset{\substack{\cup\\ X}}{I} + \underset{\substack{\cup\\ (1-X)}}{J} = \mathbb{Q}[X]$, $X+(1-X)=1$

Lema Chineză $\Rightarrow I\cap J = IJ = (X^2-X)$ şi

$$\frac{\mathbb{Q}[X]}{I\cap J} \simeq \frac{\mathbb{Q}[X]}{I}\times\frac{\mathbb{Q}[X]}{J}$$

$$\Rightarrow \frac{\mathbb{Q}[X]}{(X^2-X)} \simeq \underset{\substack{\wr\shortparallel\\ \mathbb{Q}}}{\frac{\mathbb{Q}[X]}{(X)}} \times \underset{\substack{\wr\shortparallel\\ \mathbb{Q}}}{\frac{\mathbb{Q}[X]}{(X-1)}} \simeq \mathbb{Q}\times\mathbb{Q} \quad \text{ideale}$$

2) $\frac{\mathbb{Q}[X]}{(X^2-1)} \simeq \mathbb{Q}\times\mathbb{Q}$, dar $\frac{\mathbb{Z}[X]}{(X^2-1)} \not\simeq \mathbb{Z}\times\mathbb{Z}$

În $\mathbb{Q}[X]$: $I=(X+1)$, $J=(X-1)$

I, J comaximale

$I+J=\mathbb{Q}[X]$

$\frac{1}{2}(X+1)+\frac{1}{2}(1-X)=1$

$\Downarrow$

$I\cap J = IJ = (X^2-1)$

$$\frac{\mathbb{Q}[X]}{(X^2-1)} \simeq \frac{\mathbb{Q}[X]}{(X+1)} \times \frac{\mathbb{Q}[X]}{(X-1)} \simeq \mathbb{Q} \times \mathbb{Q}$$

$$\frac{\mathbb{Z}[X]}{(X^2-1)} = \{ \widehat{a+bX} \mid a,b \in \mathbb{Z} \}, \text{ unde}$$

$$\widehat{a+bX} = \widehat{c+dX} \iff \begin{cases} a=c \\ b=d \end{cases}$$

R inel, $e \in R$

e s.m. idempotent dacă $e^2=e$

$f : R \to S$ izomorfism de inele

$e \in R$ idempotent $\iff$ $f(e)$ idempotent în S

$\Downarrow$

$(\exists)$ o bijecție între idempotenții lui R și idempotenții lui S

Care sunt idempotenții din $\mathbb{Z}$? $0, 1$

Dar din $\mathbb{Z} \times \mathbb{Z}$?

$$(a,b)^2 = (a,b) \iff \begin{cases} a^2=a \\ b^2=b \end{cases}$$

$$\| $$

$$(a^2,b^2) \qquad a \in \{0,1\},\ b \in \{0,1\}$$

$\mathbb{Z} \times \mathbb{Z}$ are 4 elemente idempotente

$(0,0), (0,1), (1,0), (1,1)$

$\widehat{a+bX}$ idempotent în $\dfrac{\mathbb{Z}[X]}{(X^2-1)}$

$$\Updownarrow$$

$$\widehat{a+bX}^{\,2} = \widehat{a+bX}$$

$$\widehat{a+bX}^{\,2} = \widehat{(a+bX)^2} = \widehat{a+2abX+b^2X^2}$$

$$= \widehat{b^2(X^2-1)+a^2+b^2+2abX}$$

$$= \underbrace{\widehat{b^2(X^2-1)}}_{\substack{\parallel \\ 0}} + \widehat{a^2+b^2+2abX}$$

$$\widehat{a+bX}^{\,2} = \widehat{a+bX} \iff \widehat{a^2+b^2+2abX} = \widehat{a+bX}$$

$$\underset{a,b\in\mathbb{Z}}{\iff} \begin{cases} a^2+b^2=a \\ 2ab=b \end{cases}$$

Dacă $b\neq 0 \Rightarrow 2a=1$, imposibil

Deci $b=0$

$$\Rightarrow a^2=a \Rightarrow a\in\{0,1\}$$

Idempotenții din $\dfrac{\mathbb{Z}[X]}{(X^2-1)}$ sunt $\hat{0}$ și $\hat{1}$.