Propoziție: Fie $m \in \mathbb{N}$, $m \geq 2$ și $\hat{a} \in \mathbb{Z}_m$.
Atunci $\hat{a} \in U(\mathbb{Z}_m) \Leftrightarrow (a,m)=1$

Dem.:

"$\Rightarrow$": $\hat{a} \in U(\mathbb{Z}_m) \Rightarrow (\exists)\, \hat{\alpha} \in \mathbb{Z}_m$ cu $\hat{a}\hat{\alpha} = \hat{1} \Leftrightarrow \widehat{a\alpha} = \hat{1}$

$$\Updownarrow$$
$$m \mid (a\alpha - 1)$$

Fie $d=(a,m)$

$$\left.\begin{array}{l} d \mid m \Rightarrow d \mid a\alpha - 1 \\ d \mid a \Rightarrow d \mid a\alpha \end{array}\right\} \Rightarrow d \mid a\alpha - (a\alpha - 1) = 1$$
$$\Rightarrow d = 1$$

"$\Leftarrow$": Dacă $(a,m)=1$, atunci $(\exists)$ $x,y \in \mathbb{Z}$ cu $xa + ym = 1$

$$\Rightarrow \hat{x}\hat{a} + \hat{y}\underbrace{\hat{m}}_{=\hat{0}} = \hat{1}$$

$$\Rightarrow \hat{x} \cdot \hat{a} = \hat{1} \Rightarrow \hat{a} \in U(\mathbb{Z}_m)$$

$$|U(\mathbb{Z}_m)| = |\underbrace{\{a \in \mathbb{N} \mid 1 \leq a \leq m-1,\ (a,m)=1\}}_{\varphi(m)}|$$

$\varphi(m)$ [indicatorul lui Euler]

Exemple:

1) $U(\mathbb{Z}_{12}) = \{\hat{1}, \hat{5}, \hat{7}, \widehat{11}\}$
[deci $\varphi(12)=4$]

2) p prim $\Rightarrow U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{\hat{0}\}$
(adică $\mathbb{Z}_p$ este corp)

Teoremă: (Proprietatea de universalitate a inelului factor)

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[dr, "f"'] & R/_I \arrow[d, dashed, "\bar{f}"] \\ & A \end{tikzcd}$$

Fie R inel comutativ, I ideal în R, $I \neq R$, $\pi : R \to R/_I$ proiecție canonică. Atunci pentru orice inel comutativ A și orice morfism de inele $f : R \to A$ cu proprietatea că $I \subset \operatorname{Ker} f$, există un unic morfism de inele $\bar{f} : R/_I \to A$ a.î. $\bar{f}\pi = f$. În plus, $\bar{f}$ injectiv $\Leftrightarrow I = \operatorname{Ker} f$ și $\bar{f}$ surjectiv $\Leftrightarrow f$ surjectiv.

Dem.:

$(R,+)$, I subgrup normal

$(A,+)$

Proprietatea de universalitate a grupului factor $R/_I$

$\Rightarrow (\exists!)$ morfismul de grupuri $\bar{f} : R/_I \to A$ cu

$\bar{f}\pi = f$ (adică $\bar{f}(\hat{x}) = f(x)$)

Arăt că $\bar{f}$ este chiar morfism de inele.

$$\bar{f}(\hat{x}\cdot\hat{y}) = \bar{f}(\widehat{xy}) = f(xy) \overset{f \text{ morf.}}{\underset{\text{de inele}}{=\!=\!=}} f(x)f(y) =$$

$$= \bar{f}(\hat{x})\,\bar{f}(\hat{y})$$

$$\bar{f}(\hat{1}) = f(1) = 1$$

Corolar:

Teorema fundamentală de izomorfism pentru inele:

Fie $f: R \to S$ un morfism de inele. Atunci există un izomorfism de inele $R/_{\mathrm{Ker}\, f} \simeq \mathrm{Im}\, f$.

Dem.:

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[dr, "f'"'] & R/_{\mathrm{Ker}\, f} \arrow[d, dashed, "(\exists!)\ \overline{f'}"] \\ & \mathrm{Im}\, f \end{tikzcd}$$

$f': R \to \mathrm{Im}\, f$

$f'(x) = f(x)$, $(\forall)\ x \in R$

f' morfism surjectiv de inele

$\mathrm{Ker}\, f' = \mathrm{Ker}\, f$

Proprietatea de universalitate $\Rightarrow$

$\overline{f'}$ izomorfism de inele

$$\begin{tikzcd} R \arrow[r] \arrow[dr, "\substack{\text{morfism} \\ \text{surj. de inele} \\ \text{cu } \mathrm{Ker} = I}"'] & R/I \arrow[d, dashed] \\ & A \end{tikzcd}$$

Exemplu:

$R = \mathbb{Z}$, $I = n\mathbb{Z}$, $J = m\mathbb{Z}$

$\phantom{R = \mathbb{Z}, I =}\ (n) \qquad (m)$

$IJ = (nm) = nm\mathbb{Z}$

$I \cap J = n\mathbb{Z} \cap m\mathbb{Z} = [n,m]\mathbb{Z}$

R inel comutativ

I, J ideale

$I \cap J$ ideal, $I + J = \{x + y \mid x \in I, y \in J\}$ ideal

$\in J$

$IJ \overset{\text{def.}}{=\!=} \{\underbrace{\underbrace{x_1 y_1}_{\in I} + \ldots + \underbrace{x_n y_n}_{\in I}}_{\in I} \mid n \in \mathbb{N}^*, x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J\}$

(ideal) $\to$ exercițiu

$IJ \subset I\cap J \subset I \subset I+J$

$I\cap J \subset J \subset I+J$

Exercițiu: Dacă $I=(a)=\{xa \mid x\in R\}$ și $J=(b)=\{xb \mid x\in R\}$, atunci $IJ=(ab)$

Lema chineză a resturilor:

Fie R inel comutativ, I, J ideale în R.
$I\neq R$, $J\neq R$ a.î. $I+J=R$ (I, J sunt comaximale)
Atunci există un izomorfism de inele

$$\frac{R}{I\cap J} \simeq \frac{R}{I}\times\frac{R}{J}$$

În plus, $I\cap J = IJ$.

Dem.: Vreau $f: R\to \frac{R}{I}\times\frac{R}{J}$ morfism surjectiv de inele.

$\ker f = I\cap J$

$\frac{R}{I} \to \hat{x}$

$\frac{R}{J} \to \bar{x}$

Definim

$f(x)=(\hat{x},\hat{y})$

f morfism de inele

$f(x+y)=(\widehat{x+y}, \overline{x+y}) = (\hat{x}+\hat{y}, \bar{x}+\bar{y})$

$=(\hat{x},\bar{x})+(\hat{y},\bar{y}) = f(x)+f(y)$

$f(xy)=(\widehat{xy},\overline{xy}) = (\hat{x}\hat{y}, \bar{x}\bar{y}) = (\hat{x},\bar{x})\cdot(\hat{y},\bar{y}) =$
$= f(x)f(y)$

$f(1)=(\hat{1},\bar{1})$

$\ker f = \{x \in R \mid f(x) = (\hat{0}, \bar{0})\}$
$= \{x \in R \mid (\hat{x}, \bar{x}) = (\hat{0}, \bar{0})\}$
$= \{x \mid x \in I \text{ și } x \in J\}$
$= I \cap J$

- f surj. $\quad I + J = R \Rightarrow (\exists)\ a \in I, b \in J$ cu $a + b = 1$

Fie $(\hat{x}, \bar{y}) \in \frac{R}{I} \times \frac{R}{J}$.

Atunci $f(bx + ay) = (\widehat{bx + ay}, \overline{bx + ay})$
$= (\hat{b}\hat{x} + \cancel{\hat{a}\hat{y}}, \cancel{\bar{b}\bar{x}} + \bar{a}\bar{y})$
$= (\hat{x}, \bar{y})$

$\hat{a} = \hat{0}$, $\bar{b} = \bar{0}$, $\bar{a} = \bar{1}$

$a \in I$, $b \in J$
$a + b = 1$

$\hat{a} = \hat{0}$, $\bar{b} = \bar{0}$
$\hat{b} = \hat{1}$, $\bar{a} = \bar{1}$

Consecință: Fie $m, n \in \mathbb{N}$, $m, n \geq 2$ cu $(m, n) = 1$. Atunci $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ (izomorfism de inele).

$R = \mathbb{Z}$, $I = m\mathbb{Z}$, $J = n\mathbb{Z}$

$I + J = \underbrace{(m, n)}_{=1}\mathbb{Z} = \mathbb{Z}$

$I \cap J = [m, n]\mathbb{Z} = mn\mathbb{Z}$

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

Demonstrăm $I \cap J = IJ$ din Lema Chineză.

„⊇": Mereu.

Fie $x \in I \cap J$. Atunci $x = x \cdot 1 = x(a+b) = \underset{\in J}{xa} + \underset{\in I}{xb} \in IJ$

$(n,m)=1$

$(\forall)\ i,j \in \mathbb{Z}$

$(\exists)\ a \in \mathbb{Z},\ a \equiv i \pmod{n}$ $\quad \hat{a} = \hat{i}$

$a \equiv j \pmod{m}$ $\quad \bar{a} = \bar{j}$

$|U(\mathbb{Z}_m)|$

$\varphi(m)$

$\varphi(p^k) = p^k - p^{k-1}$

$1, \dots, p^k - 1, p^k$

$1 \cdot p, 2 \cdot p, \dots, p^{k-1} \cdot p$

$p^k - p^{k-1}$

$m_1, \dots, m_r \in \mathbb{N},\ \geq 2$

$(m_i, m_j) = 1,\ (\forall)\ i \neq j$

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_r} \simeq \mathbb{Z}_{m_1 m_2 \dots m_r}$$

$$U(\_\_\_\_\_\_\_\_\_\_\_\_) \simeq U(\_\_)$$

$$\varphi(m_1)\varphi(m_2)\dots\varphi(m_r) = \varphi(m_1 m_2 \dots m_r)$$

$$m = p_1^{k_1} \dots p_r^{k_r} \Rightarrow \varphi(m) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r}) =$$

$$\left(\begin{array}{l} p_1, \dots, p_r \text{ prime distincte} \\ k_1, \dots, k_r \in \mathbb{N}^* \end{array} \right)$$

$$= (p_1^{k_1} - p_1^{k-1}) \dots (p_r^{k_r} - p_r^{k_r - 1}) = m\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

$$\varphi(12) = \varphi(2^2 \cdot 3) = (2^2 - 2^1)(3^1 - 3^0) = 2 \cdot 2 = 4$$

Teorema lui Euler

Fie $m \in \mathbb{N}$, $m \geq 2$ și $a \in \mathbb{Z}$ cu $(a, m) = 1$. Atunci $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Dem.: $\mathbb{Z}_m$, $(U(\mathbb{Z}_m), \cdot)$ grup

$|U(\mathbb{Z}_m)| = \varphi(m)$

$\hat{a} \in U(\mathbb{Z}_m)$ $\Rightarrow \hat{a}^{\varphi(m)} = \hat{1}$

$\hat{a}^{\varphi(m)} = \widehat{a^{\varphi(m)}}$

G grup cu $|G| = k$

$g \in G$

$\Downarrow$

$g^k = 1$

Caz particular:

Mica Teoremă a lui Fermat:

p prim, $a \in \mathbb{Z}$, $p \nmid a$

$\Downarrow$

$a^{p-1} \equiv 1 \pmod{m}$

$m = p$, $\varphi(p) = p - 1$

R inel comutativ

$a \in R$ s.n. divizor al lui zero dacă $(\exists)\, b \in R \setminus \{0\}$ cu $ab = 0$

0 divizor al lui zero $\quad 0 \cdot 1 = 0$

$\mathbb{Z}$: 0 este singurul divizor al lui zero

K corp comutativ

$$ab = 0 \quad / \cdot a^{-1} \Rightarrow b = 0$$

$$a \neq 0$$

$\mathbb{Z}_6$: $\hat{2} \cdot \hat{3} = \hat{0}$

($\hat{2}$, $\hat{3}$ divizori ai lui zero)

R inel comutativ s.n. domeniu de integritate dacă 0 este singurul divizor al lui zero

$[ab = 0 \Rightarrow a = 0$ sau $b = 0]$

Exercițiu: $\mathbb{Z}_n$ domeniu de integritate $\Leftrightarrow$ n prim

Inele de polinoame

$$a_0 + a_1 X + \ldots + a_n X^n$$

A inel comutativ

$$\mathcal{P} = \{(a_0, a_1, a_2, \ldots) \mid a_0, a_1, \ldots \in A \text{ și } (\exists)\, n \text{ a.î. } a_{n+1} = a_{n+2} = \ldots = 0\}$$

$$(a_0, a_1, \ldots) = (b_0, b_1, \ldots)$$
$$\Updownarrow$$
$$a_0 = b_0,\ a_1 = b_1, \ldots$$

Pe $\mathcal{P}$ definim $+$ și $\cdot$ astfel:

$(a_0, a_1, \dots) + (b_0, b_1, \dots) \overset{\text{def.}}{=} (a_0 + b_0, a_1 + b_1, \dots)$

$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) \overset{\text{def.}}{=} (c_0, c_1, \dots)$, unde $\in \mathcal{P}$

$$c_m = \sum_{\substack{i,j \geq 0 \\ i+j=m}} a_i b_j$$

$$= a_0 b_m + a_1 b_{m-1} + \dots + a_m b_0$$

$c_0 = a_0 b_0$

$c_1 = a_0 b_1 + a_1 b_0$

$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

$\vdots$

Propoziție: $(\mathcal{P}, +, \cdot)$ inel comutativ

El. neutru la $\cdot$ este $(1, 0, 0, \dots)$

Fie $X = (0, 1, 0, 0, \dots) \in \mathcal{P}$

Atunci $X^2 = (0, 1, 0, 0, \dots) \cdot (0, 1, 0, 0, \dots)$

$= (0, 0, 1, 0, 0, \dots)$

$X^3 = (0, 0, 0, 1, 0, \dots)$

$X^m = (0, 0, \dots, 0, 1, 0, \dots)$

poziția $m+1$

Apoi

$(a, 0, 0, \dots) \cdot X^m = (0, \dots, 0, a, 0, \dots)$

poziția $m+1$

$\mathcal{P} \ni (a_0, a_1, a_2, \dots) = (a_0, 0, 0, 0, \dots) + (0, a_1, 0, \dots) +$

$+ (0, 0, a_2, 0, \dots) + \dots$

$= (a_0, 0, 0, 0, \dots) + (a_1, 0, 0, \dots) \cdot X + (a_2, 0, 0, \dots) \cdot X^2 + \dots =$

Fie $\varphi : A \to \mathcal{P}$, $\varphi(a) = (a, 0, 0, 0, \dots)$

φ morfism injectiv de inele

$= \varphi(a_0) + \varphi(a_1) X + \varphi(a_2) X^2 + \dots =$

„Identific" a cu $\varphi(a)$

A cu $\varphi(A)$

$\varphi(a) X^i \longrightarrow a X^i$

$= a_0 + a_1 X + a_2 X^2 + \dots$

Orice $f \in \mathcal{P}$, $f \neq 0$ se scrie $f = a_0 + a_1 X + \dots + a_m X^m$ cu $m \in \mathbb{N}$, $a_0, \dots, a_m \in A$, $a_m \neq 0$

m s.n. gradul lui f

$\parallel$

$\deg(f)$

$a_0, \dots, a_m$ s.n. coeficienții lui f

a_m s.n. coeficientul dominant

X s.n. nedeterminată

$\mathcal{P} \overset{\text{not.}}{=\!=} A[X]$ inelul polinoamelor cu coeficienți în A în nedeterminata X

Operații:

$$aX^i + bX^i = (a+b)X^i$$
$$(aX^i)(bX^j) = ab\,X^{i+j}$$

$$(a_0 + a_1X + \ldots + a_nX^n) + (b_0 + b_1X + \ldots + b_mX^m) =$$
$$= (a_0+b_0) + (a_1+b_1)X + \ldots + (a_n+b_n)X^n$$

$$f = \sum_{i=\overline{0,n}} a_i X^i \quad , \quad g = \sum_{j=\overline{0,m}} b_j X^j$$

$$fg = \sum_{p=\overline{0,n+m}} \left(\sum_{i+j=p} a_i b_j \right) X^p$$
$$= a_0b_0 + (a_1b_0 + a_0b_1)X + \ldots + a_nb_mX^{n+m}$$

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$$
$$\deg(f\cdot g) \leq \deg(f) + \deg(g) \quad (*)$$

$=$ dacă:

$ab=0 \Rightarrow a=0$ sau $b=0$

- A este domeniu de integritate

sau

- $a_n \in U(A)$ sau $b_m \in U(A)$

Consecință: A domeniu de integritate $\Rightarrow A[X]$ domeniu de integritate, $U(A[X]) = U(A)$

K corp comutativ $\Rightarrow K[X]$ domeniu de integritate

exercițiu: $U(K[X]) = K \setminus \{0\}$

$\downarrow$

corp comutativ

$fg = 1$

În general, putem avea < în (*).

exemplu: $\mathbb{Z}_4[X]$

$f = \hat{1} + \hat{2}X$, $g = \hat{2}X$

$\deg(f) = \deg(g) = 1$

$fg = \hat{2}X \Rightarrow \deg(fg) = 1$