1) Fie R un inel cu unitate finit, $a \in R$. Arătați că a este divizor al lui zero sau a este inversabil.

Sol: Dacă a este divizor al lui zero ✓

Dacă a nu este divizor al lui zero $\Rightarrow a \in U(R)$

Fie $f: R \to R$, $f(r) = ar$ $\forall r \in R$

$f(r_1) = f(r_2) \Leftrightarrow ar_1 = ar_2 \Leftrightarrow a(r_1 - r_2) = 0$ } $\Rightarrow$
a nu este divizor al lui zero

$\Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2$.

Deci f = inj
R = mulț. finită } $\Rightarrow f$ = surj } $\Rightarrow$
$f: R \to R \ni 1$

$\Rightarrow \exists r \in R$ a.î. $f(r) = 1 \Leftrightarrow ar = 1$. Deci $\exists a^{-1} = r$.

Consecință: În $\mathbb{Z}_n$ orice elem este fie divizor al lui zero, fie inversabil.

$U(\mathbb{Z}_n) = \{\hat{a} \mid (a,n) = 1\} \to \varphi(n)$ elem

$D(\mathbb{Z}_n) = \{\hat{a} \mid (a,n) \neq 1\} \to n - \varphi(n)$ elem

↳ mulț. div. lui zero din $\mathbb{Z}_n$

Def R-inel com. unitar
$x \in R$ - s.n. nilpotent dacă $\exists n \in \mathbb{N}^*$ a.î. $x^n = 0$

$N(R) = \{x \in R \mid x - \text{nilpotent}\} \subseteq D(R)$
↳ divizorii lui zero

2) i) Arătă R-inel com unitar, $N(R)$ este ideal al lui R.

ii) $N(\mathbb{Z}_n) = ?$

Sol: i) $\cdot \forall x, y \in N(R) \Rightarrow x - y \in N(R)$

$\cdot \forall a \in R$ și $x \in N(R) \Rightarrow ax \in N(R)$

$x, y \in N(R) \Rightarrow \exists m, n \in \mathbb{N}^*$ a.î. $x^m = 0 = y^n$.

$$(x-y)^{m+n} \underset{R = \text{com}}{=} \sum_{k=0}^{m+n} (-1)^k C_{m+n}^k x^{m+n-k} y^k$$

$$= \underbrace{x^{m+n}}_{=0} - C_{m+n}^1 \underbrace{x^{m+n-1}}_{=0} y + \ldots + (-1)^n C_{m+n}^n \underbrace{x^m}_{=0} \underbrace{y^n}_{=0}$$

$$+ (-1)^{n+1} C_{m+n}^{n+1} x^{m-1} \underbrace{y^{n+1}}_{=0} + \ldots + (-1)^{m+n} \underbrace{y^{n+m}}_{=0} = 0$$

$$(ax)^m \underset{ax = xa}{=} a^m x^m = a^m \cdot 0 = 0 \Rightarrow ax \in N(R).$$

ii) $N(\mathbb{Z}_n) = \widehat{p_1 \cdots p_t}\, \mathbb{Z}_n$ *, $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$
↑ descomp. în prime distincte

"$\subseteq$" $\hat{x} \in N(\mathbb{Z}_n) \Leftrightarrow \exists m \in \mathbb{N}^*$ a.î. $\hat{x}^m = \hat{0}$ în $\mathbb{Z}_n$

$\Leftrightarrow n = p_1^{\alpha_1} \cdots p_t^{\alpha_t} \mid x^m = \underbrace{x \cdots x}_{m\text{-ori}}$
$p_i \mid n$, p_i = prim
$\Big\} \Rightarrow p_i \mid x \ \forall 1 \le i \le t$
$(p_i, p_j) = 1 \ \forall i \ne j$
$\Big\} \Rightarrow$

$\Rightarrow p_1 \cdots p_t \mid x \Rightarrow \hat{x} \in \widehat{p_1 \cdots p_t}\, \mathbb{Z}_n$.

„⊇" $\hat{x} \in \widehat{p_1 \cdots p_t}\,\mathbb{Z}_n \Rightarrow \hat{x} = \widehat{p_1 \cdots p_t} \cdot \hat{y}, \ \hat{y} \in \mathbb{Z}_n$.

Iau $m = \max\{\alpha_1, \dots, \alpha_t\} \in \mathbb{N}^* \Rightarrow$

$$\Rightarrow \hat{x}^m = \underbrace{\widehat{p_1^{\alpha_1} \cdots p_t^{\alpha_t}}}_{\hat{n} = \hat{0}} \cdot \widehat{p_1^{m-\alpha_1}} \cdots \widehat{p_t^{m-\alpha_t}} \cdot \hat{y}^m = \hat{0}$$

$\Rightarrow \hat{x} \in N(\mathbb{Z}_n)$.

<u>Exemplu</u> $|N(\mathbb{Z}_{720})| = \dfrac{720}{2 \cdot 3 \cdot 5} = 24$ $\qquad 720 = 2^4 \cdot 3^2 \cdot 5$

$$N(\mathbb{Z}_{720}) = \widehat{2 \cdot 3 \cdot 5}\,\mathbb{Z}_{720} = \widehat{30}\,\mathbb{Z}_{720}$$

$$= \{\hat{0}, \widehat{30}, \widehat{60}, \dots, \widehat{690}\}.$$

3) R = inel com. unitar, $\mathrm{Idemp}(R) = \{x \in R \mid x^2 = x\}$.
$$\underset{0,1}{\Psi} \; ; \; \underset{x}{\Psi} \Rightarrow \underset{1-x}{\Psi}$$

Pt $n \in \mathbb{N} \setminus \{0,1\}$ și $R = \mathbb{Z}_n$, dacă $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$
descomp. în prime distincte

atunci $\mathrm{Idemp}(\mathbb{Z}_n) \simeq \mathcal{P}(\{p_1, \dots, p_t\})$. În particular, $|\mathrm{Idemp}(\mathbb{Z}_n)| = 2^t$.

Sol: Fie $\hat{x} \in \mathrm{Idemp}(\mathbb{Z}_n) \Rightarrow \hat{x}^2 = \hat{x} \iff n \mid x(x-1)$

$$\left.\begin{array}{l} \iff p_1^{\alpha_1} \cdots p_t^{\alpha_t} \mid x(x-1) \\ (x, x-1) = 1 \end{array}\right\} \iff \exists \{i_1, \dots, i_s\} \subseteq \{1, \dots, t\}$$

a.î. $\left\{ \begin{array}{l} p_i^{\alpha_i} \mid x \quad \forall i \in \{i_1, \dots, i_s\} \\ p_j^{\alpha_j} \mid x-1, \quad \forall j \in \{1, \dots, t\} \setminus \{i_1, \dots, i_s\} \end{array} \right.$

Arăt că
$$\left.\begin{array}{l} \mathrm{Idemp}(\mathbb{Z}_n) \xrightarrow{\varphi} \mathcal{P}(\{p_1, \dots, \alpha_t\}) \\ \qquad \hat{x} \longrightarrow \{p_{i_1}, \dots, p_{i_s}\} \text{ (ca mai sus)} \end{array}\right\} \begin{array}{l} \text{este bine def. și} \\ \text{bijectivă} \end{array}$$

φ bine def: $\hat{x} = \hat{y}$; $p_v^{\alpha_v} \mid x \iff p_v^{\alpha_v} \mid y$.
$\Updownarrow$
$p_1^{\alpha_1} \cdots p_t^{\alpha_t} = n \mid x - y \iff p_v^{\alpha_v} \mid x-y$, $\forall 1 \le v \le t$.

Dacă $p_v^{\alpha_v} \mid x \Rightarrow p_v^{\alpha_v} \mid x - (x-y) = y$ ✓

$p_v^{\alpha_v} \mid y \Rightarrow p_v^{\alpha_v} \mid (x-y) + y = x$ ✓

φ = inj: $\varphi(\hat{x}) = \varphi(\hat{y}) \Rightarrow \hat{x} = \hat{y}$
$\quad \| $
$\{p_{i_1}, \dots, p_{i_s}\}$

$$\left.\begin{array}{l} \forall v \in \{i_1, \dots, i_s\}: \; p_v^{\alpha_v} \mid x, \; p_v^{\alpha_v} \mid y \Rightarrow p_v^{\alpha_v} \mid x-y \\ \forall j \in \{1, \dots, t\} \setminus \{i_1, \dots, i_s\}: \; p_j^{\alpha_j} \mid x-1, \; p_j^{\alpha_j} \mid y-1 \Rightarrow p_j^{\alpha_j} \mid x-y \end{array}\right\} \Rightarrow$$

$\Rightarrow p_k^{\alpha_k} \mid x-y \quad \forall 1 \le k \le t \Rightarrow n = p_1^{\alpha_1} \cdots p_t^{\alpha_t} \mid x-y \Rightarrow \hat{x} = \hat{y}$

φ = surj: $\quad \forall \{p_{i_1}, \dots, p_{i_s}\} \subseteq \{p_1, \dots, p_t\}, \ \exists\, \hat{x} \in \mathrm{Idemp}(\mathbb{Z}_n)$

a.î. $\varphi(\hat{x}) = \{p_{i_1}, \dots, p_{i_s}\}$. $\iff \begin{cases} \hat{x} \in \mathrm{Idemp}(\mathbb{Z}_n) & (1) \\ p_i^{\alpha_i} \mid x \ \ \forall i \in \{i_1, \dots, i_s\} & (2) \\ p_j^{\alpha_j} \mid x - 1, \ \forall j \in \{1, \dots, t\} \setminus \{i_1, \dots, i_s\}. & (3) \end{cases}$

$$\left(\prod_{i \in \{i_1, \dots, i_s\}} p_i^{\alpha_i}, \prod_{j \in \{1, \dots, t\} \setminus \{i_1, \dots, i_s\}} p_j^{\alpha_j} \right) = 1 \Rightarrow \exists\, \alpha, \beta \in \mathbb{Z} \text{ a.î.}$$

$$\underbrace{\alpha \prod_{i \in \{i_1, \dots, i_s\}} p_i^{\alpha_i}}_{\overset{not}{=} x} + \underbrace{\beta \prod_{j \in \{1, \dots, t\} \setminus \{i_1, \dots, i_s\}} p_j^{\alpha_j}}_{= 1 - x} = 1.$$

x verifică (2)

$1 - x$ verifică (3)

Rămas (1): $\quad x(1-x) = \alpha\beta\, p_1^{\alpha_1} \cdots p_t^{\alpha_t} = \alpha\beta n$

$$\Rightarrow \hat{x} \cdot \widehat{1-x} = \hat{0} \iff \hat{x} = \hat{x}^2 \ \checkmark.$$

Exemplu: $\mathrm{Idemp}(\mathbb{Z}_{60})$

$$60 = 2^2 \cdot 3 \cdot 5 \Rightarrow |\mathrm{Idemp}(\mathbb{Z}_{60})| = 2^3 = 8.$$

$$\mathrm{Idemp}(\mathbb{Z}_{60}) = \{ \hat{0}, \hat{1}, \widehat{16}, \hat{1} - \widehat{16} = \widehat{45}, \widehat{36}, \hat{1} - \widehat{36} = \widehat{25}, \widehat{40}, \hat{1} - \widehat{40} = \widehat{21} \}.$$

$a \qquad 1-a$

$$\varphi : \mathrm{Idemp}(\mathbb{Z}_{60}) \to \mathcal{P}(\{2,3,5\}).$$

- $\emptyset \rightsquigarrow 2^2, 3, 5 \mid a-1 \Leftrightarrow 60 \mid a-1 \Leftrightarrow \hat{a} = \hat{1}.$
- $\{2\} \rightsquigarrow \begin{cases} 2^2 \mid a \\ 3, 5 \mid a-1 \end{cases}$; caut $\alpha, \beta \in \mathbb{Z}$ a.î. $\alpha \cdot 2^2 + \beta \cdot 3 \cdot 5 = 1$

Iau $\alpha = 4$, $\beta = -1 \Rightarrow a = \alpha \cdot 2^2 = 16$; $\hat{a} = \widehat{16}$

- $\{2,3\} \rightsquigarrow \begin{cases} 2^2, 3 \mid a \\ 5 \mid a-1 \end{cases}$; caut $\alpha, \beta \in \mathbb{Z}$ a.î. $\alpha \cdot 2^2 \cdot 3 + \beta \cdot 5 = 1$

Iau $\alpha = -2$, $\beta = 5 \Rightarrow a = -2 \cdot 2^2 \cdot 3 \Rightarrow \hat{a} = \widehat{36}$

- $\{2,5\} \rightsquigarrow \begin{cases} 2^2, 5 \mid a \\ 3 \mid a-1 \end{cases}$; caut $\alpha, \beta \in \mathbb{Z}$ a.î. $\alpha \cdot 2^2 \cdot 5 + \beta \cdot 3 = 1$

Iau $\alpha = -1$, $\beta = 7 \Rightarrow a = -1 \cdot 2^2 \cdot 5 \Rightarrow \hat{a} = \widehat{40}$

4) Fie $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ de grad n ($a_n \neq 0$). Atunci:

(i) $f \in N(R[X]) \iff a_0, a_1, \dots, a_n \in N(R)$.

(ii) $f \in U(R[X]) \iff a_0 \in U(R)$ și $a_1, \dots, a_n \in N(R)$

(iii) $f \in D(R[X]) \iff \exists\, 0 \neq a \in R$ a.î. $af = 0$

($\iff \exists\, 0 \neq a \in R$ a.î. $a a_i = 0, \forall i = \overline{0,n}$)

(iv) $f \in Idemp(R[X]) \iff f = a_0 \in Idemp(R)$,

adică $Idemp(R[X]) = Idemp(R)$.

<u>Sol</u>: (i) "$\Rightarrow$" $f \in N(R[X])$

Ind. după $grad(f) = n \geq 0$.

$n = 0 \Rightarrow f = a_0 \in N(R[X]) \cap R = N(R)$ ✓.

$n-1 \mapsto n$: $f \in N(R[X]) \Rightarrow \exists\, t \in \mathbb{N}^*$ a.î. $\underbrace{f^t}_{\text{"are coef dominant"} = a_n^t} = 0$ $\Rightarrow$

(coef lui X^{nt})

$\Rightarrow a_n^t = 0 \Rightarrow a_n \in N(R) \Rightarrow a_n X^n \in N(R[X])$

$f = a_n X^n + \dots \in N(R[X])$ $\Big\} \Rightarrow$

$N(R[X]) \trianglelefteq R[X]$ (ideal) $\Longrightarrow f - a_n X^n = a_{n-1} X^{n-1} + \dots + a_0 \in N(R[X])$

$\uparrow$ de grad cel mult $n-1$

ip. de ind. $\Longrightarrow a_0, \dots, a_{n-1} \in N(R)$ ✓.

"$\Leftarrow$" $a_i \in N(R), \forall i = \overline{0,n} \Rightarrow f \in N(R[X])$ #.

$a_i \in N(R) \Rightarrow a_i X^i \in N(R[X])$ - ideal $\Longrightarrow$ $\forall\, 0 \leq i \leq n$

$\Rightarrow \sum_{i=0}^{n} a_i X^i \in N(R[X]) \Rightarrow f \in N(R[X])$.