25.02.2016

SEMINAR 1

"⊆" ① $ZD(\mathbb{Z}/_n) = \{\hat{k} : (k, n) \neq 1\}$

$\hat{k} \in ZD(\mathbb{Z}/_n) \Rightarrow \exists\ \hat{k'} \in \mathbb{Z}/_n$ a.î. $\hat{k} \cdot \hat{k'} = \hat{0}$, $\hat{k'} \neq \hat{0}$

$\left.\begin{array}{l} k \cdot k' \vdots n \\ Pp\ (m, k) = 1 \end{array}\right\} \Rightarrow k' \vdots n \Rightarrow \hat{k'} = \hat{0}$ contradicție

"⊇" $d = (n, k) \neq 1$

$\left.\begin{array}{l} n = d \cdot n_1 \\ k = d \cdot k_1 \\ k' = n_1 \end{array}\right\} \Rightarrow kk' = d k_1 n_1 = n \cdot k_1 \Rightarrow \hat{k}\hat{k'} = \hat{0}$

Pp. $\hat{k'} = \hat{0} \Rightarrow n / k' \Leftrightarrow d\, n_1 / k' \Leftrightarrow d\, n_1 / n_1 \Leftrightarrow d / 1$ contradicție $\Rightarrow \hat{k'} \neq \hat{0}$

- Ex: $ZD(\mathbb{Z}/_8) = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}\}$

② R inel finit, comutativ $\Rightarrow R = ZD(R) \cup U(R)$

Fie $a \in R$, $a \notin ZD(R) \Rightarrow a$ inversabil

$f_a : R \to R$, $f_a(x) = ax$

f_a e injectivă $\Leftrightarrow \forall\ x, y \in R, x \neq y \Rightarrow f_a(x) \neq f_a(y)$

$\left.\begin{array}{l} f_a(x) = ax \\ f_a(y) = ay \end{array}\right. \Rightarrow ax = ay \Rightarrow ax - ay = 0 \Rightarrow$

$\left.\begin{array}{l} \Rightarrow a(x-y) = 0 \\ a \notin ZD\ \cancel{\Rightarrow a \neq 0} \end{array}\right\} \Rightarrow x - y = 0 \Rightarrow$
$\Rightarrow x = y$

$\left.\begin{array}{l} \text{deci } f_a \text{ e injectivă} \\ R \text{ inel finit} \Rightarrow f_a \text{ e surjectivă} \end{array}\right\} \Rightarrow f$ bijectivă

$\Rightarrow \exists\ b \in R$ a.î. $f_a(b) = 1_R \Rightarrow ab = 1_R \Rightarrow a$ inversabil la dreapta

$g_a : R \to R$, $g_a(x) = xa$

$\left.\begin{array}{l} g_a \text{ e injectivă} \\ g_a \text{ finit} \end{array}\right\}$ și surjectivă $\Rightarrow g_a$ e bijectivă

$\Rightarrow \exists\ b' \in R$ a.î. $g_a(b') = 1_R \Leftrightarrow b'a = 1_R \Rightarrow a$ inversabil la stânga

$b' / ab = 1$, $b'a = 1$ $\Rightarrow b'(ab) = b' \Rightarrow (b'a)b = b' \Rightarrow b = b' \Rightarrow a$ element inversabil

③ $A \in M_n(\mathbb{Q}) \Rightarrow A$ zerodiv sau A inversabilă

Fie $d = \det(A)$ $\begin{cases} d = 0 & \Rightarrow A \text{ zerodivizor} \\ d \neq 0 & \Rightarrow A \text{ inversabilă} \end{cases}$

Dem. că dacă $d = 0 \Rightarrow A$ zerodivizor

$\exists x \neq 0$ a.î. $Ax = 0$ $\quad \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = 0 \\ \dots \\ a_{n1}x_1 + \dots + a_{nn}x_n = 0 \end{cases}$

$\det A = 0 \Rightarrow c_1(A) = \alpha_2 c_2(A) + \dots + \alpha_n c_n(A)$

$$\begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} = \alpha_2 \begin{pmatrix} a_{12} \\ \vdots \\ a_{n2} \end{pmatrix} + \dots + \alpha_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix}$$

$$\begin{cases} a_{11} - \alpha_2 a_{12} - \dots - \alpha_n a_{1n} = 0 \\ \dots \\ a_{n1} - \alpha_2 a_{n2} - \dots - \alpha_n a_{nn} = 0 \end{cases}$$

deci, $(x_1, \dots, x_n) = (1, -\alpha_2, \dots, -\alpha_n)$

$B = (x \dots x)$

$$B = \begin{pmatrix} x_1 & x_1 & \dots & x_1 \\ \vdots & \vdots & & \vdots \\ x_n & x_n & \dots & x_n \end{pmatrix}$$

$\left.\begin{array}{l} AB = 0 \\ \text{cum } B \neq 0 \end{array}\right\} \Rightarrow A$ divizor al lui 0 la stânga

$\exists x \neq 0$ cu $x'A = 0$

$$\begin{cases} x_1' a_{11} + \dots + x_n' a_{n1} = 0 \\ \dots \\ x_1' a_{n1} + \dots + x_n' a_{nn} = 0 \end{cases}$$

$\det A = 0$

$$c = \begin{pmatrix} x' \\ x' \\ \vdots \\ x' \end{pmatrix}$$

$\left.\begin{array}{l} cA = 0 \\ \text{cum } c \neq 0 \end{array}\right\} \Rightarrow A$ este ~~zerodivizor~~ divizor al lui 0 la dreapta

④ Pr. 105 → de ruitres cu

$R = \{\frac{a}{b} \mid a, b \in \mathbb{Z}\}$. R inel comutativ. $U(R) = ?$
(b impar)

$\frac{a}{b} \cdot \frac{c}{d} = 1$, b, d impare

$\frac{ac}{bd} = 1 \Rightarrow ac = bd \Rightarrow ac$ impare $\Rightarrow$ ~~a, c sunt impare~~ a e impar

Dacă a impar $\Rightarrow \frac{a}{b}$ inv. ptr. că $\exists \frac{b}{a} \in R$

$U(R) = \{\frac{a}{b} ; a$ impar, b impar$\}$

⑤ $R = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a, b \in \mathbb{Q}\}$. R inel comutativ. $U(R) = ?$

Arătăm că e comutativ deoarece în general ~~matricele nu~~ inelul de matrice nu e comutativ.

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 \\ -(b_1+b_2) & a_1+a_2 \end{pmatrix} \in R$$

$$\left.\begin{aligned} &\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_2b_1 + a_1b_2) & -b_1b_2 + a_1a_2 \end{pmatrix} \in R \\ &\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & a_2b_1 + a_1b_2 \\ -(a_1b_2 + a_2b_1) & -b_1b_2 + a_1a_2 \end{pmatrix} \in R \end{aligned}\right\} \Rightarrow$$ inelul e comutativ

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in U(R) \Leftrightarrow \exists\, c, d \in \mathbb{Q} \text{ a.î. } \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow$$

$$\Rightarrow \begin{cases} ac - bd = 1 \\ -(bc + ad) = 0 \end{cases} \Rightarrow \begin{cases} ac - bd = 1 \\ ad + bc = 0 \end{cases}$$

$\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2 \neq 0 \Leftrightarrow a \neq 0$ sau $b \neq 0$

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in R$; $U(R) = R \setminus \{0\}$, R corp

⑥ $R = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a, b \in \mathbb{Z}_3\}$. R inel comutativ. $U(R) = ?$

$R = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a, b \in \mathbb{Z}_5\}$. R inel comutativ. $U(R) = ?$

10.03.2016

SEMINAR 2

1 a) $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, a, b \in \mathbb{Z}_3 \right\}$. R inel comutativ. $U(R) = ?$
(cu 9 elemente) corp

b) $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, a, b \in \mathbb{Z}_5 \right\}$. R inel comutativ. $U(R) = ?$
cu 25 elemente
(nu e corp)

(a) Fie $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

$A^{-1} = (a^2 + b^2)^{-1} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Care sunt matricile inversabile?

Trebuie $a^2 + b^2 \neq \hat{0}$.

$a^2 + b^2 = \hat{0}$

$b \backslash a$	$\hat{0}$	$\hat{1}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{2}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{2}$

O matrice $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ cu $a, b \in \mathbb{Z}_3$ este inversabilă pentru orice $a = b \neq \hat{0}$.

Pentru $a = b = \hat{0}$, matricea nu este inversabilă.
Ca să fie corp ar trebui ca orice matrice nenulă să fie inversabilă.

(b)

$b \backslash a$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{0}$	$\boxed{\hat{0}}$	$\hat{1}$	$\hat{4}$	$\hat{4}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\boxed{\hat{0}}$	$\boxed{\hat{0}}$	$\hat{2}$
$\hat{2}$	$\hat{4}$	$\boxed{\hat{0}}$	$\hat{3}$	$\hat{3}$	$\boxed{\hat{0}}$
$\hat{3}$	$\hat{4}$	$\boxed{\hat{0}}$	$\hat{3}$	$\hat{3}$	$\boxed{\hat{0}}$
$\hat{4}$	$\hat{1}$	$\hat{2}$	$\boxed{\hat{0}}$	$\boxed{\hat{0}}$	$\hat{2}$

Există matrici nenule, care au determinantul $= 0 \Rightarrow$ neinversabile.

$R \setminus U(R) = \left\{ \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{2} \\ -\hat{2} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{3} \\ -\hat{3} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{2} & \hat{1} \\ -\hat{1} & \hat{2} \end{pmatrix}, \begin{pmatrix} \hat{3} & \hat{1} \\ -\hat{1} & \hat{3} \end{pmatrix}, \begin{pmatrix} \hat{4} & \hat{2} \\ -\hat{2} & \hat{4} \end{pmatrix}, \begin{pmatrix} \hat{4} & \hat{3} \\ -\hat{3} & \hat{4} \end{pmatrix}, \begin{pmatrix} \hat{2} & \hat{4} \\ -\hat{4} & \hat{2} \end{pmatrix}, \begin{pmatrix} \hat{3} & \hat{4} \\ -\hat{4} & \hat{3} \end{pmatrix} \right\}$

Este R inel integru? Caut 2 matrici care înmulțite între ele să dea O_2.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} b & a \\ -a & b \end{pmatrix} = \begin{pmatrix} a & a^2 + b^2 \\ -(a^2 + b^2) & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

T. FERMAT Orice nr prim de forma $\widehat{4k+1}$ este suma de două pătrate.
↳ pentru numere prime

$\boxed{2}$ Demonstrați că idealul de $(3, x)$ din $\mathbb{Z}[X]$ nu este principal.

$I = (3, x)$ = idealul generat de 3 și x

$I = \{3f + xg \mid f, g \in \mathbb{Z}[X]\}$ nu e principal (~~adică~~ nu e generat de un singur element, adică 3 și x nu sunt multipli de același polinom)

mulțimea polinoamelor care au termenul liber multiplu de 3

$\boxed{\text{DE ÎNV!}}$ forma idealelor, suma a două ideale, intersecția

Pp. prin reducere la absurd că idealul $I = (3, x) \underset{"\subseteq"}{\overset{"\supseteq"}{=}} (h)$ e prin

Mai importantă este incluziunea „$\subseteq$".

$(h) = \{h\alpha, \alpha \in \mathbb{Z}[X]\}$.

$\left.\begin{array}{l} 3 = h\alpha \\ x = h\beta \end{array}\right| \Rightarrow$ grad $h = 0 \Rightarrow h \in \mathbb{Z}$

$h \mid x \Rightarrow h$ poate să fie 1 sau -1

$\Rightarrow I = (\pm 1)$.

Dacă un ideal conține $\pm 1 \Rightarrow$ conține tot inelul. $\} \Rightarrow I = \mathbb{Z}[X]$

Dar în $\mathbb{Z}[X]$ există polinoame care nu au termen liber multiplu de 3 $\Rightarrow$ Pp. falsă $\Rightarrow I$ nu este inel principal.

TEMĂ! a) Arătați că: $I = (3, x)$ este ~~inel~~ principal în inelul $\mathbb{Z}_6[X]$

$x = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\} \in \mathbb{Z}_6[X]$

$I = (3, x) = \mathbb{Z}_6 * x * \mathbb{Z}_6 + \mathbb{Z}_6 * 3 * \mathbb{Z}_6 =$

$= \{x^n + a \mid n = \hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5};\ a = \hat{0}, \hat{3}\} =$

$= \{\hat{1}, \hat{4}, x, x+\hat{3}, x^2, x^2+\hat{3}, \dots, x^5, x^5+\hat{3}\} \overset{?}{=} \mathbb{Z}_6[X]$

$x = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$

Evident $I \subseteq \mathbb{Z}_6[X]$

$\mathbb{Z}_6[X]$ e generată de polinoamele cu coeficienți în $\mathbb{Z}_6 \Rightarrow \mathbb{Z}_6[X] \overset{?}{\subseteq} I$

$\Rightarrow I = \mathbb{Z}_6[X]$

b) $R = R_1 \times R_2$

$I \leq R \iff \begin{cases} \exists\, I_1 \leq R_1 \\ \exists\, I_2 \leq R_2 \end{cases}$ a.î. $I = I_1 \times I_2$

Se dă inelul $\mathbb{Z}/_{12} \times \mathbb{Q}$. Aflați idealele.

Aflăm idealele lui $\mathbb{Z}/_{12}$, ale lui $\mathbb{Q}$ și facem produsul.

Un K corp poate să aibă 2 ideale (0) și (K) – el însuși

$\left.\begin{array}{l} K \text{ corp} \\ I \leq K \end{array}\right| \Rightarrow I = (0)$ sau $I = (K)$

$I = (0) \Rightarrow \exists\, a \in I, a \neq 0 \Rightarrow \exists\, a^{-1} \in K, \underbrace{a^{-1} \cdot a}_{=1} \in I$

$\Downarrow$

$I = K$

Idealele lui $\mathbb{Z}/_{12} = \{ \{\hat{0}\}, \mathbb{Z}/_{12}, \hat{2}\,\mathbb{Z}/_{12}, \hat{3}\,\mathbb{Z}/_{12}, \hat{4}\,\mathbb{Z}/_{12}, \hat{6}\,\mathbb{Z}/_{12} \}$ (elemente care nu sunt inversabile)

SEMINAR 2

① a) $R_1 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a, b \in \mathbb{Z}/_3 \right\}$. R inel comutativ, chiar corp. cu 9 elemente

b) $R_1 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a, b \in \mathbb{Z}/_5 \right\}$. R inel comutativ, dar nu este corp cu 25 elemente

a) $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = (a^2+b^2)^{-1} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$; $a^2+b^2 \neq \hat{0}$

Care sunt matricile inversabile?

b \ a	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\boxed{\hat{0}}$	$\hat{1}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{2}$
$\hat{2}$	$\hat{1}$	$\hat{2}$	$\hat{2}$

O matrice $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ cu $a, b \in \mathbb{Z}_3$ este inversabilă pt. orice $a, b \neq 0$
Pentru $a = b = 0$, matricea nu este inversabilă.
Ca să fie corp trebuie ca orice matrice nenulă să fie inversabilă.

b)

b \ a	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{0}$	$\boxed{\hat{0}}$	$\hat{1}$	$\hat{4}$	$\hat{4}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\boxed{\hat{0}}$	$\boxed{\hat{0}}$	$\hat{2}$
$\hat{2}$	$\hat{4}$	$\boxed{\hat{0}}$	$\hat{3}$	$\hat{3}$	$\boxed{\hat{0}}$
$\hat{3}$	$\hat{4}$	$\boxed{\hat{0}}$	$\hat{3}$	$\hat{3}$	$\boxed{\hat{0}}$
$\hat{4}$	$\hat{1}$	$\hat{2}$	$\boxed{\hat{0}}$	$\boxed{\hat{0}}$	$\hat{2}$

$R - U(R) = \left\{ \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{2} \\ -\hat{2} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{3} \\ -\hat{3} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{2} & \hat{1} \\ -\hat{1} & \hat{2} \end{pmatrix}, \begin{pmatrix} \hat{3} & \hat{1} \\ -\hat{1} & \hat{3} \end{pmatrix}, \begin{pmatrix} \hat{4} & \hat{2} \\ -\hat{2} & \hat{4} \end{pmatrix}, \begin{pmatrix} \hat{4} & \hat{3} \\ -\hat{3} & \hat{4} \end{pmatrix}, \begin{pmatrix} \hat{2} & \hat{4} \\ -\hat{4} & \hat{2} \end{pmatrix}, \begin{pmatrix} \hat{3} & \hat{4} \\ -\hat{4} & \hat{3} \end{pmatrix} \right\}$ matrici neinversabile (au det =

două matrici înmulțite $= O_2$

• R este inel integru? (caut divizorii lui $\hat{0}$)

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} b & a \\ -a & b \end{pmatrix} = \begin{pmatrix} ab-ba & a^2+b^2 \\ -b^2-a^2 & -ab+ab \end{pmatrix} = \begin{pmatrix} 0 & a^2+b^2 \\ -(a^2+b^2) & 0 \end{pmatrix} \Rightarrow$ R nu este inel integru

TEOREMA lui FERMAT: Orice nr. prim de forma $4k+1$ este sum de două pătrate.

(2) $I=(3,X)$ idealul generat de 3 și x, ideal în $\mathbb{Z}[X]$ care nu este principal (nu e generat de un singur element, adică 3 și x nu sunt multipli de același polinom)

$= \{3f + Xg : f,g \in \mathbb{Z}[X]\} =$

$=$ mulțimea polinoamelor care au termenul liber multiplu de 3 (*)

Arătați că nu se poate așa ceva!

Pp. prin reducere la absurd că idealul $I=(3,X)=(h)$, unde ~~$h=3f+Xg$, $f,g\in\mathbb{Z}[X]$~~. $h=\{h\alpha : \alpha\in\mathbb{Z}[X]\}$.

$h=3f+Xg$, $f,g\in\mathbb{Z}[X]$

$\left.\begin{cases} 3=h\alpha \\ X=h\beta \end{cases}\right\} \Rightarrow \begin{cases} \text{grad } h=0 \\ h/X, \text{ iar } h=1 \text{ sau } h=-1 \end{cases} =$

$\Rightarrow I=(\pm 1) \Rightarrow I=\mathbb{Z}[X]$ FALS! deoarece (*)

curs: Dacă un ideal conține $\pm 1 \Rightarrow$ coincide cu inelul.

Arătați că:

TEMĂ: $I=(3,X)$ este principal în inelul $\mathbb{Z}_6[X]$. 3p / 10p

(3) $R=R_1\times R_2$; R_1, R_2 inele comutative unitare

$I\trianglelefteq R \Leftrightarrow (\exists)\, I_1\trianglelefteq R_1, (\exists)\, I_2\trianglelefteq R_2$ a.î. $I=I_1\times I_2$

Dacă $\left.\begin{matrix} K \text{ corp} \\ I\trianglelefteq K \end{matrix}\right\} \Rightarrow I=(0)$ sau $I=K$ $\Rightarrow$ Există două ideale ale unui corp: 0 și el însuși

I ideal al lui K

$I\neq(0) \Rightarrow (\exists)\, a\in I, a\neq 0$

$(\exists)\, a^{-1} \in K$

$1=a^{-1}\cdot a\in I \Rightarrow I=K$

Idealele lui $\mathbb{Z}_{12} \times \mathbb{Q}$: $\{\{\hat{0}\}, \mathbb{Z}_{12}, \hat{2}\mathbb{Z}_{12}, \hat{3}\mathbb{Z}_{12}, \hat{4}\mathbb{Z}_{12}, \hat{6}\mathbb{Z}_{12}\}$

$\hat{5}\mathbb{Z}_{12} = \mathbb{Z}_{12} = \hat{7}\mathbb{Z}_{12} = \hat{8}\mathbb{Z}_{12} = \hat{9}\mathbb{Z}_{12} = \hat{10}\mathbb{Z}_{12} = \hat{11}\mathbb{Z}_{12}$ deoarece sunt inversabile

[$p^3 \cdot q^2$ p, q prime distincte ; exponentul dă nr. de divizori

nr. de div $= (3+1) \cdot (2+1)$]

(3) Consider $f : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_2$, $f(m+ni) = \widehat{m+n}$.

$\{m+ni : m, n \in \mathbb{Z}[i]\}$.

Arătați că a) f e morfism surjectiv de inele.

b) $\operatorname{Ker} f = (1+i)$

??? (a) ~~$f(m_1+n_1 i) \cdot f(m_2+n_2) = (\widehat{m_1+n_1})(\widehat{m_2+n_2})$~~

$f(m_1+n_1 i) \cdot f(m_2+n_2 i) = f((m_1+n_1 i)\cdot(m_2+n_2 i)) \Leftrightarrow$

$\Leftrightarrow \widehat{m_1+n_1} \cdot \widehat{m_2+n_2} = \widehat{m_1 m_2 + m_1 n_2 + m_2 n_1 - n_1 n_2}$

$\Leftrightarrow \widehat{m_1 m_2 + m_1 n_2 + n_1 m_2 + n_1 n_2} = m_1 m_2 +$

(b) $\operatorname{Ker} f = (1+i)$

$\operatorname{Ker} f = \{x \mid f(x) = \hat{0}, x \in \mathbb{Z}[i]\}$

$\operatorname{Ker} f = \{m+ni \mid \widehat{m+n} = \hat{0}\} = \{m+ni \mid m+n \text{ par}\}$

$(1+i) = \{\underbrace{(1+i)(a+bi)}_{a-b+(a+b)i} : a, b \in \mathbb{Z}\}$

$$\begin{cases} m = a-b \\ n = a+b \end{cases}$$

$a = \frac{m+n}{2} \in \mathbb{Z}$

$b = \frac{n-m}{2} \in \mathbb{Z}$

$b = \frac{n+m}{2} - m$

17.03.2016

SEMINAR 3

Temă a) Pp. că $I = (3, X)$ e ideal principal în $\mathbb{Z}_6[X]$, atunci $\exists h$ a.î. $I = (h)$

$h = 3f + Xg$, $f, g \in \mathbb{Z}_6[X] \Rightarrow h \in \{0, 3\}$

$3 = h\alpha$

$X = h\beta$

Pp. $gr(h) = 0$ $\Rightarrow h = 1$ sau $h = 5$

Pp. $gr(h) = 0 \Rightarrow$ absurd

Pp. $gr(h) = 1 \Rightarrow h = aX + b$, $a \neq 0$

$(aX + b)\alpha = 3 \Rightarrow b \in \{1, 3, 5\}$

singurele elemente care înmulțite cu un alt element pot da 3

$(aX + b)\beta = X \Rightarrow b \in \{3, 2, 4\}$

Alegem $b = 3$ să vedem dacă merge.

$b = 3 \Rightarrow (aX + 3)\alpha = 3$

$\Leftrightarrow a\alpha X + 3\alpha = 3 \Rightarrow \alpha$ poate lua valorile 1, 3 sau 5 (inversa)

(restul nu se potrivesc) $\Rightarrow \alpha = 3$, $a \cdot \alpha = 0$ $\Rightarrow a = 2$ sau $a = 4$

$h = 2X + 3 \Rightarrow (2X + 3)\beta = X \Leftrightarrow (2X + 3)(cX + d) = X \Leftrightarrow$

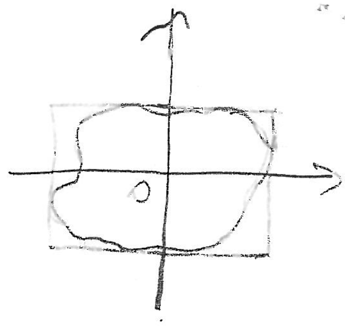
$\Leftrightarrow \underbrace{2cX^2}_{c=3} + (2d + 3c)X + \underbrace{3d}_{d=2} = X$

$4 + 1 = 1 \Rightarrow I = (2X + 3)$

Sunt doi generatori.

$\underbrace{(3X + 4)(4X + 3) = X}_{\mathbb{Z}_6[X]}$

b) $R = R_1 \times R_2$, R_1, R_2 inele comutative $\mathbb{R} \times \mathbb{R}$



$\underbrace{I \trianglelefteq R}_{\text{ideal al lui } R} \Longleftrightarrow \begin{cases} \exists\, I_1 \trianglelefteq R_1 \\ \exists\, I_2 \trianglelefteq R_2 \end{cases}$ a.î. $I = I_1 \times I_2$

" $\Rightarrow$ " $I_1 = p_1(I)$ $\qquad p_1 : R \to R_1$

proiecție $\qquad p_1(x_1, x_2) = x_1$

$I_2 = p_2(I)$ $\qquad p_2 : R \to R_2$

$\qquad p_2(x_1, x_2) = x_2$

Trebuie să arătăm că $I = I_1 \times I_2$

" $\supseteq$ "

Fie $(x_1, x_2) \in I_1 \times I_2 \Leftrightarrow x_1 \in I_1$ și $x_2 \in I_2$, adică $x_1 = p_1(x_1, *)$
$x_2 = p_2(*, x_2)$

$\cancel{I_1 \ni x_1 = p_1(x_1, *)}$

$\cancel{I_2 \ni x_2 = p_2(*, x_2)}$

Vrem să arătăm că

$\left.\begin{aligned} (x_1, *) &\in I \\ (*, x_2) &\in I \end{aligned}\right\} \overset{?}{\Longrightarrow} (x_1, x_2) \in I$

Mai clar $\quad I = I_1 \times I_2$, adică $I = \overset{I_1}{\overset{\parallel}{p_1(I)}} \times \overset{I_2}{\overset{\parallel}{p_2(I)}}$

" $\supseteq$ " $\quad (x_1, x_2) \in p_1(I) \times p_2(I) \Leftrightarrow x_1 \in p_1(I)$
$x_2 \in p_2(I)$

$\Leftrightarrow x_1 = p_1(?) \qquad ? \in I$

$x_2 = p_2(??) \qquad ?? \in I$

$I \ni ? = (x_1, *)$

$I \ni ?? = (*, x_2)$

$(x_1, *) \cdot (1, 0) = (x_1, 0) \in I$

$(*, x_2) \cdot (0, 1) = (0, x_2) \in I$ " + "

$\overline{\qquad (x_1, x_2) \in I \qquad}$

" $\subseteq$ " $\quad \underset{(a_1, a_2)}{\overset{}{a}} \in I \to a \in I_1 \times I_2$

! Orice mulțime e inclusă în produsul direct al proiecțiilor sale pe axele

$\left.\begin{aligned} p_1(a_1, a_2) &= a_1 \in I_1 \\ p_2(a_1, a_2) &= a_2 \in I_2 \end{aligned}\right\} \Rightarrow (a_1, a_2) \in I_1 \times I_2$

TEMĂ Arătați că în $\underbrace{\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\ldots\times\mathbb{R}}_{n\in\mathbb{N}}$ (șiruri de nr. reale) idealele nu sunt de forma $I_1\times I_2\times\ldots\times I_n$. (De găsit un astfel de ideal.

$n=1$ $\quad I=I_1\times I_2$

$(a_1,a_2)\in I$ și $(b_1,b_2)\in I \Rightarrow (a_1,a_2)-(b_1,b_2)\in I \Leftrightarrow (\underset{I_1}{\underset{\Uparrow}{a_1-b_1}}, \underset{I_2}{\underset{\Uparrow}{a_2-b_2}})\in I$

$(a_1,a_2)\in I$ și $(r_1,r_2)\in R \Rightarrow (a_1,a_2)(r_1,r_2)\in I \Leftrightarrow (\underset{I_1}{\underset{\Uparrow}{a_1r_1}}, \underset{I_2}{\underset{\Uparrow}{a_2r_2}})\in I$

1 $\quad {R_1\times R_2}/{I_1\times I_2} \simeq R_1/I_1 \times R_2/I_2$

$R \xrightarrow[\text{morf. surj.}]{f} R' \Rightarrow R/\mathrm{Ker}f \simeq R'$ (Conf. T.F.I. inele)

$R_1\times R_2 \xrightarrow[\text{morf. surj.}]{f} R_1/I_1 \times R_2/I_2$, $\mathrm{Ker}f = I_1\times I_2$

proiecții canonice

Definim $f(a_1,a_2)=(\underbrace{\bar{a}_1}_{\hat{r}_1 \bmod I_1}, \bar{\bar{a}}_2)$ $R_2 \bmod I_2$ e clar că e morf. surj

$\mathrm{Ker}f = \{(a_1,a_2) : f(a_1,a_2)=(\bar{0},\bar{\bar{0}})\} =$

$=\{(a_1,a_2) : \bar{a}_1=\bar{0}$ și $\bar{\bar{a}}_2=\bar{\bar{0}}\} =$

$a_1\in I_1$ și $a_2\in I_2$

$= I_1\times I_2$

sigur la examen

Aplicăm T.F.I.I.

$R=\mathbb{Z}_{12}\times\mathbb{Q}$

$I(R)=\{\{\hat{0}\}\times\mathbb{Q}, \{\hat{0}\}\times\{0\}, \hat{2}\mathbb{Z}_{12}\times\{0\}, \hat{2}\mathbb{Z}_{12}\times\mathbb{Q}, \hat{3}\mathbb{Z}_{12}\times\{0\}, \hat{3}\mathbb{Z}_{12}\times\mathbb{Q},$
$\hat{4}\mathbb{Z}_{12}\times\{0\}, \hat{4}\mathbb{Z}_{12}\times\mathbb{Q}, \hat{6}\mathbb{Z}_{12}\times\{0\}, \hat{6}\mathbb{Z}_{12}\times\mathbb{Q}, \mathbb{Z}_{12}\times\{0\}, \mathbb{Z}_{12}\times\mathbb{Q}\}$

$\dfrac{\mathbb{Z}_{12}\times\mathbb{Q}}{\{\hat{0}\}\times\mathbb{Q}} \simeq \mathbb{Z}_{12}/\{\hat{0}\} \times \mathbb{Q}/\mathbb{Q} \simeq \mathbb{Z}_{12}\times 0 \simeq \mathbb{Z}_{12}$

$\mathbb{Z}_{12}\times\mathbb{Q}/\{\hat{0}\}\times 0 \simeq \mathbb{Z}_{12}/\{\hat{0}\} \times \mathbb{Q}/0 \simeq \mathbb{Z}_{12}\times\mathbb{Q}$

$$\mathbb{Z}_{12}\times\mathbb{Q}\Big/\hat{2}\mathbb{Z}_{12}\times\{0\} \simeq \mathbb{Z}_{12}\Big/\hat{2}\mathbb{Z}_{12} \times \mathbb{Q}\Big/\{0\} \simeq \mathbb{Z}_2\times\mathbb{Q}$$

$$\mathbb{Z}_{12}\times\mathbb{Q}\Big/\hat{2}\mathbb{Z}_{12}\times\mathbb{Q} \simeq \mathbb{Z}_2\times 0 \simeq \mathbb{Z}_2$$

$$\mathbb{Z}_{12}\times\mathbb{Q}\Big/\hat{3}\mathbb{Z}_{12}\times\{0\} \simeq \mathbb{Z}_3\times\mathbb{Q}$$

$$\mathbb{Z}_{12}\times\mathbb{Q}\Big/\hat{3}\mathbb{Z}_{12}\times\mathbb{Q} \simeq \mathbb{Z}_3$$

$$\mathbb{Z}_{12}\times\mathbb{Q}\Big/\hat{4}\mathbb{Z}_{12}\times\{0\} \simeq \mathbb{Z}_4\times\mathbb{Q}\,;\quad \mathbb{Z}_{12}\times\mathbb{Q}\Big/\hat{4}\mathbb{Z}_{2}\times\mathbb{Q} \simeq \mathbb{Z}_4$$

$$\mathbb{Z}_{12}\times\mathbb{Q}\Big/\hat{6}\mathbb{Z}_{12}\times\{0\} \simeq \mathbb{Z}_6\times\mathbb{Q}\,;\quad \mathbb{Z}_{12}\times\mathbb{Q}\Big/\hat{6}\mathbb{Z}_{12}\times\mathbb{Q} \simeq \mathbb{Z}_6$$

$$\mathbb{Z}_{12}\times\mathbb{Q}\Big/\mathbb{Z}_{12}\times\{0\} \simeq \cancel{\mathbb{Z}_{12}}\,0\times\mathbb{Q} = \mathbb{Q}\,;\quad \mathbb{Z}_{12}\times\mathbb{Q}\Big/\mathbb{Z}_{12}\times\mathbb{Q} \simeq \cancel{\mathbb{Z}_{12}}\,0$$

Dumitrescu: pg. 83 $\Rightarrow$ 108, 111, 112, 121

105320 24.03.2016

SEMINAR 4

Ex. 111 pagina 83

$\rightarrow \mathbb{Z}_2[X]/(X^2+X+\hat{1})$ corp

$f(X) = (X^2+X+\hat{1})g(X) + r(X) = (X^2+X+\hat{1})g(X) + aX+b$

$gr(x) \leq 1$

$r(X) = aX+b$

$\overline{f(X)} = \overline{(X^2+X+\hat{1})g(X)+aX+b} = \overline{(X^2+X+1)}\ \overline{g(X)} + \overline{aX+b} = \overline{aX+b}$

$+$	$\hat{0}$	$\hat{1}$	$\overline{X}$	$\overline{X+1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\overline{X}$	$\overline{X+1}$
$\hat{1}$	$\hat{1}$	$\hat{0}$	$\overline{X+1}$	$\overline{X}$
$\overline{X}$	$\overline{X}$	$\overline{X+1}$	$\hat{0}$	$\hat{1}$
$\overline{X+1}$	$\overline{X+1}$	$\overline{X}$	$\hat{1}$	$\hat{0}$

"$\cdot$"	$\hat{0}$	$\hat{1}$	$\overline{X}$	$\overline{X+1}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{X}$	$\hat{0}$	$\overline{X}$	$\overline{X+1}$	$\hat{1}$
$\overline{X+1}$	$\hat{0}$	$\overline{X+1}$	$\hat{1}$	$\overline{X}$

$\rightarrow \mathbb{Z}_2[X]/(X^2+X)$ inel care nu e integru

"$\cdot$"	$\hat{0}$	$\hat{1}$	$\overline{X}$	$\overline{X+1}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{X}$	$\hat{0}$	$\overline{X}$	$\overline{X}$	$\hat{0}$
$\overline{X+1}$	$\hat{0}$	$\overline{X+1}$	$\hat{0}$	$\overline{X+1}$

$g(x+\hat{1}) \leftarrow g(x)$

$f(x) \mapsto f(X+\hat{1})$

$\boxed{\mathbb{Z}_2[X]/X^2} \simeq \mathbb{Z}_2[X]/(X^2+\hat{1}) = \boxed{\mathbb{Z}_2[X]/(X+\hat{1})^2}$

$X^2+\hat{1} = (X+\hat{1})^2$

$\rightarrow \mathbb{Z}_2[X]/(X^2)$

$\cdot$	$\hat{0}$	$\hat{1}$	$\overline{X}$	$\overline{X+1}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\boxed{\hat{1}}$	$\overline{X}$	$\overline{X+1}$
$\overline{X}$	$\hat{0}$	$\overline{X}$	$\hat{0}$	$\cancel{\overline{X}}$
$\overline{X+1}$	$\hat{0}$	$\overline{X+1}$	$\cancel{\overline{X}}$	$\boxed{\hat{1}}$

$\boxed{\text{Ex. 112 pag. 84}}$

$(a+bi)(a-bi)$

$a^2 - \cancel{abi} + \cancel{abi} + b^2$
a^2+b^2

$$\mathbb{Z}_4,\ \mathbb{Z}_2\times\mathbb{Z}_2,\ \mathbb{Z}_2[X]/_{X^2},\ \mathbb{Z}_2[X]/_{(X^2+X+\hat{1})}$$

← sigur la examen cu LCR cu izomorfism

$R = \mathbb{Z}_2 \times \mathbb{Z}_2$

$\cdot$	$(\hat0,\hat0)$	$(\hat1,\hat1)$	$(\hat1,\hat0)$	$(\hat0,\hat1)$
$(\hat0,\hat0)$	$(\hat0,\hat0)$	$(\hat0,\hat0)$	$(\hat0,\hat0)$	$(\hat0,\hat0)$
$(\hat1,\hat1)$	$(\hat0,\hat0)$	$\boxed{(\hat1,\hat1)}$	$(\hat1,\hat0)$	$(\hat0,\hat1)$
$(\hat1,\hat0)$	$(\hat0,\hat0)$	$(\hat0,\hat0)$	$(\hat1,\hat0)$	$(\hat1,\hat0)$
$(\hat0,\hat1)$	$(\hat0,\hat0)$	$(\hat0,\hat1)$	$(\hat0,\hat0)$	$(\hat0,\hat1)$

$x^2+x = x(x+1)$

$I_1 = X$
$I_2 = X+\hat1$
$\Big\}\ I_1 I_2 = (X(X+\hat1)) \Longleftrightarrow 1 \in I_1 + I_2$

$I_1 + I_2 = \mathbb{Z}_2[X]$

$1 = \underset{I_1}{X} + \underset{I_2}{(X+\hat1)}$

Din LCR $\Longrightarrow \mathbb{Z}_2[X]/_{(X^2+X)} \simeq \underbrace{\mathbb{Z}_2[X]/_{X}}_{=\mathbb{Z}_2} \times \underbrace{\mathbb{Z}_2[X]/_{X+\hat1}}_{=\mathbb{Z}_2}$

$\mathbb{Z}_4 \not\simeq \mathbb{Z}_2[X]/_{(X^2+X+1)}$ deoarece $\mathbb{Z}_2[X]/_{(X^2+X+1)}$ e corp

$\mathbb{Z}_4 \not\simeq \mathbb{Z}_2\times\mathbb{Z}_2$. Dacă ar fi izomorfe ca grupuri, ar fi izomorfe și ca inele.

$(\mathbb{Z}_4, \cdot)$

$\cdot$	$\hat0$	$\hat1$	$\hat2$	$\hat3$
$\hat0$	$\hat0$	$\hat0$	$\hat0$	$\hat0$
$\hat1$	$\hat0$	$\hat1$	$\hat2$	$\hat3$
$\hat2$	$\hat0$	$\hat2$	$\hat0$	$\hat2$
$\hat3$	$\hat0$	$\hat3$	$\hat2$	$\hat1$

$(\mathbb{Z}_4, +)$

$+$	$\hat0$	$\hat1$	$\hat2$	$\hat3$
$\hat0$	$\hat0$	$\hat1$	$\hat2$	$\hat3$
$\hat1$	$\hat1$	$\hat2$	$\hat3$	$\hat0$
$\hat2$	$\hat2$	$\hat3$	$\hat0$	$\hat1$
$\hat3$	$\hat3$	$\hat0$	$\hat1$	$\hat2$

$(\mathbb{Z}_2[X]/_{X^2}, +)$

$+$	$\hat0$	$\hat1$	$\overline{X}$	$\overline{X+1}$
$\hat0$	$\hat0$	$\hat1$	$\overline{X}$	$\overline{X}$
$\hat1$	$\hat1$	$\hat0$	$\overline{X+1}$	$\overline{X}$
$\overline{X}$	$\overline{X}$	$\overline{X+1}$	$\hat0$	[illegible]
$\overline{X+1}$	$\overline{X+1}$	$\overline{X}$	$\hat1$	

TEMA de la curs: 122, 123, 115

Ex. ~~120~~ pg. 85

$\mathbb{Z}[i]/_{1+i} \simeq \mathbb{Z}_2$

$\varphi : \mathbb{Z}[i] \to \mathbb{Z}_2$

$\varphi(a+bi) = \overline{a+b}$

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

Pentru a dem. că $R/_I \simeq R'$ construim un $\varphi : R \to R'$ morf. surj., $\operatorname{Ker}\varphi = I$, apoi aplicăm TFI.

$1+i \in \operatorname{Ker} f \Leftrightarrow \varphi(1+i) = 0$

$\varphi(x+y) = \varphi(x) + \varphi(y)$ (1)

$\varphi(x \cdot y) = \varphi(x)\, \varphi(y)$ (2)

$x = a+bi$

$y = c+di$

$$\left.\begin{array}{l} \varphi(a+bi+c+di) = \overline{a+b} + \overline{c+d} \\ \cancel{\varphi((a+bi)(c+di)) = a+b} \\ \varphi(a+bi) = \overline{a+b} \\ \varphi(c+di) = \overline{c+d} \end{array}\right\} \Rightarrow (1)$$

Din $\mathbb{Z}_2$ "$+$" = "$-$"

$$\left.\begin{array}{l} \varphi((a+bi)(c+di)) = \varphi(ac-bd) + i(bc+ad) = \overline{ac+bd+bc+ad} \\ \varphi(a+bi)\,\varphi(c+di) = (\overline{a+b})(\overline{c+d}) = \overline{ac+ad+bc+bd} \end{array}\right\} \Rightarrow (2)$$

Dem. că φ e surjectivă $\Leftrightarrow (\forall)\, y \in \mathbb{Z}_2 \Rightarrow \exists\, x \in \mathbb{Z}[i]$ a.î. $\varphi(x) = y$

$y = \hat{0} \Rightarrow \varphi(\bar{0}) = \hat{0} \Rightarrow x = \bar{0}$

$y = \hat{1} \Rightarrow \varphi(\bar{1}) = \hat{1} \Rightarrow x = \bar{1}$

$\varphi(x) = 0 \Rightarrow x \in (1+i) \Leftrightarrow x = (1+i)(a+bi)$

$x = m+ni$

$\varphi(x) = 0 \Leftrightarrow \overline{m+n} = \bar{0} \Leftrightarrow \bar{m} + \bar{n} = \bar{0} \Leftrightarrow \begin{array}{l}\bar{m} = \bar{0} \\ \bar{n} = \bar{0}\end{array}$ sau $\begin{array}{l}\bar{m} = \bar{1} \\ \bar{n} = \bar{1}\end{array}$

$\Downarrow$ m, n pare $\Rightarrow m = 2k$ și $n = 2p \Rightarrow$

$x = 2k + 2pi = 2(k+pi) = (1+i)(1-i)(k+pi)$

$\Downarrow$ m, n impare $\Rightarrow m = 2k+1$ și $n = 2p+1 \Rightarrow$

$x = 2k+1+(2p+1)i = 2k+1+2pi+i = 2(k+pi)+1+i = (1+i)(1-i)(k+pi)+(1+i)$
$= (1+i)[(1-i)(k+pi)+1]$

Din TFI $\Rightarrow \mathbb{Z}[i]/_{(1+i)} \simeq \mathbb{Z}_2$

SEMINAR 5

$\boxed{\text{EX } 115 \text{ pg. } 84 - \text{DUMITRESCU}}$ Aflați idealele lui $A = \mathbb{Z}_2[X]/(X^2)$

Idealele lui R/I sunt de forma J/I cu $J \trianglelefteq R$ și $I \subseteq J$.

Rezolvare:

Idealele lui A sunt de forma $J/(X^2)$ unde $J \trianglelefteq \mathbb{Z}_2[X]$

OBS: Dacă $\left.\begin{array}{l} K \text{ corp comutativ} \\ J \trianglelefteq K[X] \end{array}\right\} \Rightarrow J$ ideal principal (adică $(\exists)\ f \in K[X]$ a.î. $J = (f)$)

Orice subgrup al lui $\mathbb{Z}$ are și elemente pozitive și negative.

$J \neq \{0\}$ $f \in J$: grad $(f) =$ min, unde $f \neq 0$

Arătăm că $J = (f)$

Fie $g \in J$.

$\left.\begin{array}{l} g = q f + r, \text{ grad } r < \text{grad } f \text{ sau } r = 0 \\ g \in J \quad q \in J \end{array}\right\} \Rightarrow \left.\begin{array}{l} r \in J \text{ (deoarece } g - qf = r) \\ \text{grad } r < \text{grad } f \end{array}\right\} \Rightarrow r = 0$

$\left.\begin{array}{l} \left.\begin{array}{l} \mathbb{Z}_2[X] \text{ corp} \\ J \leq \mathbb{Z}_2[X] \end{array}\right\} \Rightarrow J \text{ e ideal principal} \Leftrightarrow J = (f) \\ I = X^2 \\ I \subseteq J \end{array}\right\} \Rightarrow X^2 \in (f) \Rightarrow$

$\Rightarrow f \mid X^2 \Rightarrow f = X^2$ sau $f = X$ sau $f = \hat{1}$

Idealele lui A sunt: $(X^2)/(X^2) = \{0\}$, $(X)/(X^2)$, $(1)/(X^2) = \mathbb{Z}_2[X]/(X^2)$

$A/\{0\} \simeq A$

$A/A \simeq \{0\}$

$\cancel{A/(X)/(X^2)}$ $\dfrac{A}{(X)/(X^2)} = \dfrac{\mathbb{Z}_2[X]/(X^2)}{(X)/(X^2)} \simeq \mathbb{Z}_2[X]/(X) \simeq \mathbb{Z}_2$

~~Ex.~~ ~~exercițiu~~ pg. Aflați x astfel încât:

$x \equiv 5 \pmod 7$

$x \equiv 9 \pmod{15}$

$(7,15) = 1 \Rightarrow$ există un astfel de x

METODA DIRECTĂ (NERECOMANDAT) M1

$x = 5 + 7k$

$x = 9 + 15l$ ☹ m-am blocat

$5 + 7k = 9 + 15l$

$7k = 4 + 15l$

$7k = 7 - 3 + 15l \Leftrightarrow 7k - 7 = -3 + 15l \Leftrightarrow 7(k-1) = -3 + 15l \Leftrightarrow 7(k-1) = 3(-1+5l)$

$\begin{cases} 7 / 5l-1 \\ 3 / k-1 \end{cases} \Rightarrow \begin{matrix} 5l - 1 = 7l_1 \\ k - 1 = 3k_1 \end{matrix}$ și avem că $7 \cdot 3k_1 = 3 \cdot 7 l_1 \Rightarrow k_1 = l_1 = a$

$5l = 7l_1 + 1 = 7a + 1 \Rightarrow x = 9 + 15\frac{(7a+1)}{5} = 9 + 21a + 3 = 21a + 12$

$k = 3k_1 + 1 = 3a + 1 \Rightarrow x = 5 + 7(3a+1) = 5 + 21a + 7 = 12 + 21a$

Deci $x = 12 + 21a$

METODA de la CURS M2

$(7, 15) = 1 \Rightarrow \hat{15} \in U(\mathbb{Z}_7) \Rightarrow (\exists)\ \hat{y_1} \in \mathbb{Z}_7$ a.î. $\hat{15} \cdot \hat{y_1} = \hat{1}$
m_2, m_1

$\Leftrightarrow \hat{y_1} = \hat{1}$

$(\Rightarrow)\ 5 \cdot 7 \cdot \hat{1} = 5 \pmod{7}$

$(15, 7) = 1 \rightarrow \hat{7} \in U(\mathbb{Z}_{15}) \Rightarrow (\exists)\ \hat{y_2} \in \mathbb{Z}_{15}$ a.î. $\hat{7} \cdot \hat{y_2} = \hat{1}$
m_1, m_2

$\Leftrightarrow \hat{y_2} = \hat{13}$

$a_1 = 5$

$a_2 = 9$

$(\Rightarrow)\ 9 \cdot 15 \cdot \hat{13} = 9 \pmod{15}$

CEVA DUBIOS !!!

~~$x = 5 \cdot 5 \cdot 13 + 9 \cdot 15 \cdot 13 = 1038$~~

$x = a_1 m_2 y_1 + a_2 m_1 y_2$

continuare M1

~~$x = 5 \cdot 7 \cdot 1 + 9 \cdot 15 \cdot 13$~~

~~$35 + 1755 = 1790$~~

$x = 9 \cdot 7 \cdot 13 + 15 \cdot 5 = 894 =$

$= 21 \cdot 42 + 12$

$15 / 21a + 12 - 9$

$3 \cdot 5 / 21a + 3$

$5 / 21a + 3 \Rightarrow 5 / a + 3$

$a + 3 = 5m \Rightarrow a = 5m - 3$

$x = 21a + 12 = 21(5m - 3) + 12 = 105m - 63 + 12 = 105m - 51$

Dacă $m = 1 \Rightarrow x = 105 - 51 = 54$ (x min)

TEMĂ – SEMINAR 5

$\boxed{\text{EX. 415 pag. 84 – DUMITRESCU}}$

Listați idealele lui $A = \mathbb{Z}_2[X]/_{X^2}$.

$A = \mathbb{Z}_2[X] = \{ax+b \mid a, b \in \mathbb{Z}_2\} = \{\hat{0}, \hat{1}, \hat{x}, \widehat{x+1}\}$

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{x}$	$\widehat{x+1}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{x}$	$\widehat{x+1}$
$\hat{x}$	$\hat{0}$	$\hat{x}$	$\hat{0}$	$\hat{x}$
$\widehat{x+1}$	$\hat{0}$	$\widehat{x+1}$	$\hat{x}$	$\hat{1}$

$\{\hat{0}, \hat{1}\} \subset A$: 1) $\hat{0} - \hat{1} = -\hat{1} = \hat{1} \in \{\hat{0}, \hat{1}\}$
2) $(\forall) a \in A, (\forall) x \in \{\hat{0}, \hat{1}\} \Rightarrow a \cdot \hat{0} \in \{\hat{0}, \hat{1}\}$, $a \cdot \hat{1} \notin \{\hat{0}, \hat{1}\}$
$\Rightarrow \{\hat{0}, \hat{1}\}$ nu e ideal al lui A

$\{\hat{0}, \hat{x}\} \subset A$: 1) $\hat{0} - \hat{x} = -\hat{x} = \hat{x} \in \{\hat{0}, \hat{x}\}$
2) $(\forall) a \in A, (\forall) y \in \{\hat{0}, \hat{x}\} \Rightarrow a \cdot \hat{0} \in \{\hat{0}, \hat{x}\}$, $a \cdot \hat{x} \in \{\hat{0}, \hat{x}\}$
$\Rightarrow \{\hat{0}, \hat{x}\}$ e ideal al lui A

$\{\hat{0}, \widehat{x+1}\} \subset A$: 1) $\hat{0} - \widehat{x+1} = -\widehat{x+1} = \widehat{x+1} \in \{\hat{0}, \widehat{x+1}\}$
2) $(\forall) a \in A, (\forall) y \in \{\hat{0}, \widehat{x+1}\} \Rightarrow a \cdot \hat{0} \in \{\hat{0}, \widehat{x+1}\}$, $a \cdot \widehat{x+1} \notin \{\hat{0}, \widehat{x+1}\}$
$\Rightarrow \{\hat{0}, \widehat{x+1}\}$ nu e ideal al lui A

$\{\hat{1}, \hat{x}\} \subset A$: 1) $\hat{1} - \hat{x} = \hat{1} + \hat{x} \notin \{\hat{1}, \hat{x}\}$
2) $(\forall) a \in A, (\forall) y \in \{\hat{1}, \hat{x}\} \Rightarrow a \cdot \hat{1} \notin \{\hat{1}, \hat{x}\}$, $a \cdot \hat{x} \notin \{\hat{1}, \hat{x}\}$
$\Rightarrow \{\hat{1}, \hat{x}\}$ nu e ideal al lui A

$\{\hat{1}, \widehat{x+1}\} \subset A$: 1) $\hat{1} - \widehat{x+1} = \hat{x} \notin \{\hat{1}, \widehat{x+1}\}$
2) $(\forall) a \in A, (\forall) y \in \{\hat{1}, \widehat{x+1}\} \Rightarrow a \cdot \hat{1} \notin \{\hat{1}, \widehat{x+1}\}$, $a \cdot \widehat{x+1} \notin \{\hat{1}, \widehat{x+1}\}$
$\Rightarrow \{\hat{1}, \widehat{x+1}\}$ nu e ideal al lui A

$\{\hat{x}, \widehat{x+1}\} \subset A$: 1) $\hat{x} - \widehat{x+1} = \hat{1} \notin \{\hat{x}, \widehat{x+1}\}$
2) $(\forall) a \in A, (\forall) y \in \{\hat{x}, \widehat{x+1}\} \Rightarrow a \cdot \hat{x} \notin \{\hat{x}, \widehat{x+1}\}$, $a \cdot \widehat{x+1} \notin \{\hat{x}, \widehat{x+1}\}$
$\Rightarrow \{\hat{x}, \widehat{x+1}\}$ nu e ideal al lui A

A e inel $\Rightarrow 0$ și A sunt ideale

Idealele lui A sunt $0, A$ și $\{\hat{0}, \hat{x}\}$

EX. 424 pg. 84 DUMITRESCU

Arătați că are loc ~~izo~~morfismul $\mathbb{Z}[i]/_{(2+i)} \simeq \mathbb{Z}_5$

Fie $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_5$, $\varphi(a+bi) = \widehat{a+3b}$, $a,b \in \mathbb{Z}$

$2+i \in \operatorname{Ker}\varphi \Rightarrow \varphi(2+i)=0$

Demonstrăm că φ e morfism.

$\varphi(a+bi+c+di) = \varphi(ac+i(b+d)) = \widehat{a+c+3(b+d)}$
$\varphi(a+bi)+\varphi(c+di) = \widehat{a+3b}+\widehat{c+3d} = \widehat{a+c+3(b+d)}$
$\Rightarrow \varphi(a+bi+c+di) = \varphi(a+bi)+\varphi(c+di)$ (1)

$\varphi((a+bi)(c+di)) = \varphi(ac-bd+i(ad+bc)) = \widehat{ac-bd+3(ad+bc)}$
$\varphi(a+bi)\varphi(c+di) = \widehat{a+3b}\ \widehat{c+3d} = \widehat{ac+3ad+3bc+9bd} = \widehat{ac+3(ad+bc)-bd}$ =

$\Rightarrow \varphi((a+bi)(c+di)) = \varphi(a+bi)\varphi(c+di)$ (2)

~~Din~~ (1) și (2) $\Rightarrow \varphi$ e morfism

Demonstrăm că φ e surjectiv $\Leftrightarrow (\forall) y \in \mathbb{Z}_5 \Rightarrow \exists x \in \mathbb{Z}[i]$ a.î. $\varphi(x)=y$

$y=\hat{0} \Rightarrow \varphi(0)=\hat{0} \Rightarrow x=0$ ~~sau~~
$y=\hat{1} \Rightarrow \varphi(1)=\hat{1} \Rightarrow x=1$
$y=\hat{2} \Rightarrow \varphi(2)=\hat{2} \Rightarrow x=2$
$y=\hat{3} \Rightarrow \varphi(3)=\hat{3} \Rightarrow x=3$
$y=\hat{4} \Rightarrow \varphi(4)=\hat{4} \Rightarrow x=4$

$\Rightarrow \varphi$ e surjectiv

Deci φ e morfism surjectiv

$\varphi(x)=0 \Rightarrow x \in (2+i) \Leftrightarrow x=(2+i)(a+bi)$
$x = m+ni$, $m,n \in \mathbb{Z}_5$

$\varphi(x)=0 \Leftrightarrow \widehat{m+3n} = \hat{0} \Leftrightarrow \hat{m}+\widehat{3n} = \hat{0} \Rightarrow$
$m=\hat{0}$ și $n=\hat{0}$
$m=\hat{1}$ și $n=\hat{3}$
$m=\hat{2}$ și $n=\hat{1}$
$m=\hat{3}$ și $n=\hat{4}$
$m=\hat{4}$ și $n=\hat{2}$

(c1) $m=5k$; $n=5p \Rightarrow x = 5k+5pi = 5(k+pi) = (2+i)(2-i)(k+pi)$

(c2) $m=5k+\hat{1}$; $n=5pi+\hat{3}i \Rightarrow x = 5(k+pi)+\hat{1}+\hat{3}i = (2+i)(2-i)(k+pi)+(2+i)(2-i) =$
$= (2+i)[(2-i)(k+pi)+2-i]$

(c3) $m=5k+\hat{2}$; $n=5pi+\hat{1}i \Rightarrow x=5(k+pi)+\hat{2}+\hat{1}i = (2+i)(2-i)(k+pi)+\hat{2}+i =$
$=(2+i)[(2-i)(k+pi)+\hat{1}]$

(c4) $m=5k+\hat{3}$; $n=5pi+\hat{4}i \Rightarrow x=5(k+pi)+\hat{3}+\hat{4}i = (2+i)(2-i)(k+pi)+(2+i)^2 =$
$=(2+i)[(2-i)(k+pi)+2+i]$

(c5) $m=5k+\hat{4}$; $n=5pi+\hat{2}i \Rightarrow x=5(k+pi)+\hat{4}+\hat{2}i = (2+i)(2-i)(k+pi)+2(2+i)$
$=(2+i)[(2-i)(k+pi)+2]$

Din TFI $\Rightarrow \mathbb{Z}[i]/_{(2+i)} \simeq \mathbb{Z}_5$

Arătați că are loc izomorfismul $\mathbb{Z}[i]/_5 \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$.

Fie $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_5 \times \mathbb{Z}_5$, $\varphi(a+bi) = (\widehat{a+3b}, \widehat{a+2b})$.
$a, b \in \mathbb{Z}$

$5 \in \operatorname{Ker} f \Rightarrow \varphi(5) = (\hat{0}, \hat{0})$

Demonstrăm că φ e morfism.

$$\left.\begin{aligned}
&\varphi(a+bi+c+di) = \varphi(a+c+i(b+d)) = (\widehat{a+c+3(b+d)}, \widehat{a+c+2(b+d)}) \\
&\varphi(a+bi) + \varphi(c+di) = (\widehat{a+3b}, \widehat{a+2b}) + (\widehat{c+3d}, \widehat{c+2d}) = \\
&= (\widehat{a+c+3(b+d)}, \widehat{a+c+2(b+d)})
\end{aligned}\right\} \Rightarrow$$

$\Rightarrow \underline{\varphi(a+bi+c+di) = \varphi(a+bi) + \varphi(c+di)}$ (1)

$$\left.\begin{aligned}
&\varphi((a+bi)(c+di)) = \varphi(ac-bd+i(ad+bc)) = (\widehat{ac-bd+3(ad+bc)}, \widehat{ac-bd+2(ad+bc)}) \\
&\varphi(a+bi) \cdot \varphi(c+di) = (\widehat{a+3b}, \widehat{a+2b}) \cdot (\widehat{c+3d}, \widehat{c+2d}) = \\
&= (\widehat{ac+3(ad+bc)+9bd}, \widehat{ac+2(ad+bc)+4bd}) = \\
&= (\widehat{ac+4bd+3(ad+bc)}, \widehat{ac+4bd+2(ad+bc)}) = \\
&= (\widehat{ac-bd+3(ad+bc)}, \widehat{ac-bd+2(ad+bc)})
\end{aligned}\right\} \Rightarrow$$

$\Rightarrow \underline{\varphi((a+bi)(c+di)) = \varphi(a+bi)\,\varphi(c+di)}$ (2)

Din (1) și (2) $\Rightarrow$ $\underline{\varphi \text{ e morfism}}$ (3)

Demonstrăm că φ e surjectiv $\Leftrightarrow (\forall) y \in \mathbb{Z}_5 \times \mathbb{Z}_5 \Rightarrow \exists x \in \mathbb{Z}[i]$ a.î. $\varphi(x) = y$

$y = (\hat{0}, \hat{0}) \Leftrightarrow \varphi(0) = (\hat{0}, \hat{0}) \Rightarrow x = 0$
$y = (\hat{0}, \hat{1}) \Leftrightarrow \varphi(3+4i) = (\hat{0}, \hat{1}) \Rightarrow x = 3+4i$
$y = (\hat{0}, \hat{2}) \Leftrightarrow \varphi(1+3i) = (\hat{0}, \hat{2}) \Rightarrow x = 1+3i$
$y = (\hat{0}, \hat{3}) \Leftrightarrow \varphi(4+2i) = (\hat{0}, \hat{3}) \Rightarrow x = 4+2i$
$y = (\hat{0}, \hat{4}) \Leftrightarrow \varphi(2+i) = (\hat{0}, \hat{4}) \Rightarrow x = 2+i$

$y = (\hat{1}, \hat{0}) \Leftrightarrow \varphi(3+i) = (\hat{1}, \hat{0}) \Rightarrow x = 3+i$
$y = (\hat{1}, \hat{1}) \Leftrightarrow \varphi(1) = (\hat{1}, \hat{1}) \Rightarrow x = 1$
$y = (\hat{1}, \hat{2}) \Leftrightarrow \varphi(4+4i) = (\hat{1}, \hat{2}) \Rightarrow x = 4+4i$
$y = (\hat{1}, \hat{3}) \Leftrightarrow \varphi(2+3i) = (\hat{1}, \hat{3}) \Rightarrow x = 2+3i$
$y = (\hat{1}, \hat{4}) \Leftrightarrow \varphi(2i) = (\hat{0}, \hat{4}) \Rightarrow x = 2i$

$y = (\hat{2}, \hat{0}) \Leftrightarrow \varphi(1+2i) = (\hat{2}, \hat{0}) \Rightarrow x = 1+2i$
$y = (\hat{2}, \hat{1}) \Leftrightarrow \varphi(4+i) = (\hat{2}, \hat{1}) \Rightarrow x = 4+i$
$y = (\hat{2}, \hat{2}) \Leftrightarrow \varphi(2) = (\hat{2}, \hat{2}) \Rightarrow x = 2$
$y = (\hat{2}, \hat{3}) \Leftrightarrow \varphi(4i) = (\hat{2}, \hat{3}) \Rightarrow x = 4i$
$y = (\hat{2}, \hat{4}) \Leftrightarrow \varphi(3+3i) = (\hat{2}, \hat{4}) \Rightarrow x = 3+3i$

$y = (\hat{3}, \hat{0}) \Leftrightarrow \varphi(4+3i) = (\hat{3}, \hat{0}) \Rightarrow x = 4+3i$
$y = (\hat{3}, \hat{1}) \Leftrightarrow \varphi(2+2i) = (\hat{3}, \hat{1}) \Rightarrow x = 2+2i$
$y = (\hat{3}, \hat{2}) \Leftrightarrow \varphi(i) = (\hat{3}, \hat{2}) \Rightarrow x = i$
$y = (\hat{3}, \hat{3}) \Leftrightarrow \varphi(3) = (\hat{3}, \hat{3}) \Rightarrow x = 3$
$y = (\hat{3}, \hat{4}) \Leftrightarrow \varphi(1+4i) = (\hat{3}, \hat{4}) \Rightarrow x = 1+4i$

$y = (\hat{4}, \hat{0}) \Leftrightarrow \varphi(2+4i) = (\hat{4}, \hat{0}) \Rightarrow x = 2+4i$
$y = (\hat{4}, \hat{1}) \Leftrightarrow \varphi(3i) = (\hat{4}, \hat{1}) \Rightarrow x = 3i$
$y = (\hat{4}, \hat{2}) \Leftrightarrow \varphi(3+2i) = (\hat{4}, \hat{2}) \Rightarrow x = 3+2i$

$y = (\hat{4}, \hat{3}) \Leftrightarrow \varphi(1+i) = (\hat{4}, \hat{3}) \Rightarrow x = 1+i$
$y = (\hat{4}, \hat{4}) \Leftrightarrow \varphi(4) = (\hat{4}, \hat{4}) \Rightarrow x = 4$

$\Rightarrow \varphi$ e $\underline{\text{surjectivă}}$ (4)

Din (3) și (4) $\Rightarrow \varphi$ e morfism surjectiv

$\varphi(x) = (\hat{0}, \hat{0}) \Rightarrow x \in \langle 5 \rangle \Leftrightarrow x = 5(a+bi)$

$x = n + mi,\ m, n \in \mathbb{Z}/5$

$\varphi(x) = (\hat{0}, \hat{0}) \Rightarrow (\widehat{n+3m}, \widehat{n+2m}) = (\hat{0}, \hat{0}) \Leftrightarrow n+3m = \hat{0}$ și $n+2m = \hat{0}$

$\Rightarrow \begin{cases} n = 5k \\ m = 5p \end{cases} \Rightarrow x = 5k + 5pi = 5(k+pi)$

Din TFII $\Rightarrow \mathbb{Z}[i]/_5 \simeq \mathbb{Z}/_5 \times \mathbb{Z}/_5$

SEMINAR 6

Pr. 1 Să se afle $x \in \mathbb{N}$ minim cu proprietatea că $\begin{cases} x \equiv 5 \pmod{18} \\ x \equiv 27 \pmod{35} \end{cases}$

I.
$(18, 35) = 1 \Rightarrow 18 \in U(\mathbb{Z}_{35}) \Rightarrow \exists \hat{y_2} \in \mathbb{Z}_{35}$ a.î. $18 \hat{y_2} = 1 \Rightarrow \hat{y_2} = \hat{2}$

$35 \in U(\mathbb{Z}_{18}) \Rightarrow \exists \hat{y_1} \in \mathbb{Z}_{18}$ a.î. $35 \hat{y_1} = 1 \Rightarrow \hat{y_1} = \hat{17}$

$$x = \underset{5}{a_1} \cdot \underset{35}{n_2} \cdot \underset{17}{y_1} + \underset{27}{a_2} \cdot \underset{18}{n_1} \cdot \underset{2}{y_2} = 2975 + 972 = 3947$$

$r_0' < r_0 < 18 \cdot 35$

$(35 \cdot 18) = 630$

$3947 : 630 = 6$ rest 467 ← minim

122 Arătați că inelul factor $\mathbb{Z}[X]/(X^2-X) \simeq \mathbb{Z} \times \mathbb{Z}$.

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

$X^2 - X = X(X-1)$

$\left.\begin{matrix} I_1 = (X) \\ I_2 = (X-1) \end{matrix}\right\} \Rightarrow I_1 + I_2 = \mathbb{Z}[X]$

$\underset{I_1}{X} + \underset{I_2}{(-X+1)} = 1$

$\mathbb{Z}[X]/(X-1) \simeq \mathbb{Z}$

$\varphi : \mathbb{Z}[X] \to \mathbb{Z}$ morfism surjectiv. $\operatorname{Ker}\varphi \overset{\supseteq}{=} (X-1)$

$X-1 \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(X-1) = 0$

$f \in \operatorname{Ker}\varphi \Rightarrow f \in (X-1)$

$\Updownarrow$

$\varphi(f) = 0$

$f = a_0 + a_1 X + \ldots + a_m X^n,\ a_i \in \mathbb{Z}$

$\varphi(f) = \varphi(a_0) + \varphi(a_1 X^1) + \varphi(a_2 X^2) + \ldots + \varphi(a_m X^n)$

$= a_0 + \varphi(a_1) \cdot \varphi(X)^1 + \ldots + \varphi(a_m) \cdot \varphi(X)^n$

$= a_0 + a_1 + \ldots + a_n = f(1)$

$\varphi(X) = 1$

$\varphi(f) = 0 \Leftrightarrow f(1) = 0 \Leftrightarrow X-1 / f \Leftrightarrow f \in (X-1)$

TEMĂ: ex. 131, 133

① Arătați că inelul de polinoame $\mathbb{R}[X]/_{(X^2-19X+34)} \simeq \mathbb{R}\times\mathbb{R}$.

② Arătați că $X^6 + aX + \hat{5} \in \mathbb{Z}_7[X]$ are o rădăcină în $\mathbb{Z}_7$ pentru orice a.

③ Scrieți ca polinom de polinoame simetrice fundamentale următoarele polinoame simetrice $X_1^4X_2 + X_1^4X_3 + X_2^4X_1 + X_2^4X_3 + X_3^4X_1 + X_3^4X_2$.

123 pg. 84 Dumitrescu

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

$$\mathbb{Q}[X]/_{(X^2-1)} = \mathbb{Q}[X]/_{(X-1)(X+1)} \simeq \underbrace{\mathbb{Q}[X]/_{(X-1)}}_{\simeq\mathbb{Q}} \times \underbrace{\mathbb{Q}[X]/_{(X+1)}}_{\simeq\mathbb{Q}}$$

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

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

$$\mathbb{Z}[X]/_{(X^2-1)} \not\simeq \mathbb{Z}\times\mathbb{Z}$$

$(X-1) + (X+1) \overset{?}{=} \mathbb{Z}[X]$

$\boxed{(X-1)f(X) + (X+1)g(X) = 1}$ $\quad f, g \in \mathbb{Z}[X]$

$X = 1 \Rightarrow 2g(1) = 1$ abs

NU SE POATE APLICA LCR!

Pp. $\mathbb{Z}[X]/_{(X^2-1)} \simeq \mathbb{Z}\times\mathbb{Z} \Rightarrow \exists$ izomorfism $\varphi : \mathbb{Z}[X]/_{(X^2-1)} \to \mathbb{Z}\times\mathbb{Z}$

$\mathbb{Z}[X]/_{(X^2-1)} = \{\widehat{a+bX} \,;\, a, b \in \mathbb{Z}\}$

$\varphi(\hat{0}) = (0,0)$ $\qquad \varphi(\hat{X}) = (\alpha, \beta)$

$\varphi(\hat{1}) = (1,1)$

$\vdots$

$\varphi(\hat{n}) = (n,n)$

$\varphi(\widehat{a+bX}) = \cancel{\widehat{a+bX}}\ \varphi(\hat{a} + \hat{b}\cdot\hat{X}) = \varphi(\hat{a}) + \varphi(\hat{b})\cdot\varphi(\hat{X}) = (a,a) + (b,b)\cdot(\alpha,\beta)$

$= (a + b\alpha, a + b\beta)$

$(\hat{X})^2 = \hat{1}$

$\left.\begin{array}{l}\varphi(\hat{X}^2) = \varphi(\hat{X})^2 = (\alpha,\beta)^2 = (\alpha^2, \beta^2) \\ \varphi(\hat{X}^2) = \varphi(\hat{1}) = (1,1)\end{array}\right\} \Rightarrow \alpha^2 = 1,\ \beta^2 = 1$

$\varphi(\hat{x}) = (-1, 1)$ sau $\varphi(\hat{x}^{\prime}) = (1, -1)$

$\varphi(\widehat{a+bx}) = (a-b, a+b)$ $\Rightarrow$ doar numere pare, deci nu verifică.

~~Ex~~ $(1,0) \notin \operatorname{Im} f \Rightarrow \varphi$ nu e surjectiv

$\varphi(\hat{x}^{\prime}) = (-1, -1)$

$\varphi(\widehat{a+bx}) = (a-b, a+b)$ $\Rightarrow \varphi$ nu e surjectiv

SEMINAR 7

I) LEMA CHINEZĂ A RESTURILOR

$(S)\begin{cases} 6x \equiv 2 \bmod 8 \\ 5x \equiv 5 \bmod 6 \end{cases} \Rightarrow 3x \equiv 1 \bmod 4 \Rightarrow \begin{cases} x \equiv 3 \bmod 4 \\ x \equiv 1 \bmod 6 \end{cases} \Rightarrow x \equiv 3$ nu

$8 / 6x-2 \Rightarrow 4/3x-1$

$(S) \Leftrightarrow \begin{cases} x \equiv 3 \bmod 4 \\ x \equiv 1 \bmod 3 \end{cases}$

$(4,3)=1 \Rightarrow 4 \in U(\mathbb{Z}_3) \Rightarrow \exists y_1 \in \mathbb{Z}_3$ astfel încât $\hat{4}\cdot y_1 = \hat{1} \Rightarrow y_1 = \hat{1}$

$\Rightarrow 3 \in U(\mathbb{Z}_4) \Rightarrow \exists y_2 \in \mathbb{Z}_4$ astfel încât $\hat{3}\cdot y_2 = \hat{1} \Rightarrow y_2 = \hat{3}$

$\left.\begin{array}{l} x = 3\cdot 3\cdot 3 + 4\cdot 1\cdot 1 = 27+4 = 31 \\ x = 4\cdot 3\cdot q + r = 12q + r \end{array}\right\} \Rightarrow 12q + r = 31 \Rightarrow q=2$ și $r=7$

$S = \{7 + 12k\}$

431 pg. 85 - Dumitrescu

$\mathbb{Z}[X,Y] / (X-1,\ Y-2)$

$(X-1)k(X)$ $\qquad$ $(Y-2)q(y)$

433 pg. 85 - Dumitrescu

Nu există morfism surjectiv de inele $f: \mathbb{Z}[X,Y] \to \mathbb{Q}$.
Presupunem că există f morfism surjectiv.

$f(n) = n,\ \forall n \in \mathbb{Z}$

$p(x,y) = \sum n_{ij}\, x^i x^j,\quad n_{ij} \in \mathbb{Z}$

$f(x) = \frac{a}{b},\ (a,b)=1$

$f(y) = \frac{c}{d},\ (c,d)=1$

$f(p(x,y)) = \sum f(n_{ij})\, f(x^i)\, f(x^j)$

$= \sum n_{ij}\, f(x^i) f(x^j)$

$= \sum n_{ij} \left(\frac{a}{b}\right)^i \left(\frac{c}{d}\right)^j$

$= \sum n_{ij} \frac{a^i c^j}{b^i d^j}$

$= \frac{\dots}{b^k d^k}$

Fie p prim cu proprietatea că $p \nmid b, p \nmid d \Rightarrow \frac{1}{p} \neq f(p)$

altfel $\frac{1}{p} = \frac{\dots}{b^k d^k} \Leftrightarrow b^k d^k = (\dots) \cdot p \Rightarrow p / \cancel{b}^k d^k$ ~~ab~~

<u>470 pg. 408 – Dumitrescu</u>

Exprimați polinomul $f = (X_1 - X_2)^2 (X_2 - X_3)^2 (X_1 - X_3)^2$ în funcție de polinoamele simetrice fundamentale folosind metoda coeficienților nedeterminați.

$$f = (X_1 - X_2)^2 (X_2 - X_3)^2 (X_1 - X_3)^2$$

$$lt(f) = X_1^4 X_2^2 \to (4, 2, 0) = lt(s_1^2 s_2^2)$$

$s_1 = X_1 + X_2 + X_3$

$s_2 = X_1 X_2 + X_1 X_3 + X_2 X_3$

$s_3 = X_1 X_2 X_3$

$$f = s_1^2 s_2^2 + a \cdot s_1^3 s_3 + b \cdot s_2^3 + c \cdot s_1 s_2 s_3 + d \cdot s_3^2$$

$X_1 \to T X_1$

$X_2 \to T X_2$

$X_3 \to T X_3$

$$X_1^{i_1} \cdot X_2^{i_2} \cdot X_3^{i_3} = T^{i_1} X_1^{i_1} \cdot T^{i_2} X_2^{i_2} \cdot T^{i_3} X_3^{i_3}$$
$$= T^6 X_1^{i_1} X_2^{i_2} X_3^{i_3}$$

$$f(TX_1, TX_2, TX_3) = [(TX_1 - TX_2)^2 (TX_2 - TX_3)^2 (TX_1 - TX_3)^2] =$$
$$= T^6 (X_1 - X_2)^2 (X_2 - X_3)^2 (X_1 - X_3)^2$$
$$= T^6 f(X_1, X_2, X_3)$$

$(4,1,1) \to X_1^4 X_2 X_3$

$(3,3,0) \to X_1^3 X_2^3$

$(3,2,1) \to X_1^3 X_2^2 X_3$

$(2,2,2) \to X_1^2 X_2^2 X_3^2$

$$\left.\begin{array}{l} X_1 = 1 \\ X_2 = 1 \\ X_3 = 0 \end{array}\right\} \Rightarrow \begin{array}{l} s_1 = 2 \\ s_2 = 1 \\ s_3 = 0 \end{array}$$

$$\left.\begin{array}{l} f(1,1,0) = 0 \\ f(1,1,0) = 4 + b \end{array}\right\} \Rightarrow \boxed{b = -4}$$

$$\left.\begin{array}{l} x_1 = 2 \\ x_2 = -1 \\ x_3 = -1 \end{array}\right\} \Rightarrow \begin{array}{l} s_1 = 0 \\ s_2 = -3 \\ s_3 = 2 \end{array}$$

$$\left.\begin{array}{l} f(2,-1,-1) = 0 \\ f(2,-1,-1) = (-4)\cdot(-3)^2 + 4d = 108 + 4d \end{array}\right\} \Rightarrow 4d = -108 \Rightarrow \boxed{d = -27}$$

$$\left.\begin{array}{l} x_1 = 2 \\ x_2 = -1 \\ x_3 = 2 \end{array}\right\} \Rightarrow \begin{array}{l} s_1 = 3 \\ s_2 = 0 \\ s_3 = -4 \end{array}$$

$$\left.\begin{array}{l} f(2,-1,2) = 0 \\ f(2,-1,2) = a\cdot 3^3\cdot(-4) + (-27)\cdot(-4)^2 = -108a - 432 \end{array}\right\} \Rightarrow -108a = 432 \Rightarrow$$

$$\Rightarrow \boxed{a = -4}$$

$$\left.\begin{array}{l} x_1 = 1 \\ x_2 = 1 \\ x_3 = 1 \end{array}\right\} \Rightarrow \begin{array}{l} s_1 = 3 \\ s_2 = 3 \\ s_3 = 1 \end{array}$$

$$\left.\begin{array}{l} f(1,1,1) = 0 \\ f(1,1,1) = 3^2 3^2 + (-4)\cdot 3^3\cdot 1 + (-4)\cdot 3^3 + c\cdot 3\cdot 3\cdot 1 + (-27)\cdot 1^2 = 9c - 162 \end{array}\right\} \Rightarrow 9c = 162 \Rightarrow \boxed{c = 18}$$

$$f(x_1, x_2, x_3) = s_1^2 s_2^2 - 4 s_1^3 s_3 - 4 s_2^3 + 18 s_1 s_2 s_3 - 27 s_3^2$$

$x^3 + px + q = 0$

$s_2 = p$

$s_3 = -q$

$f(x_1, x_2, x_3) = -4p^3 + 27q^2 = S$

Temă

1) $\begin{cases} x^5 + y^5 = 33 \\ x + y = 3 \end{cases}$

$\sqrt{97 - x} + \sqrt[4]{x} = 5$

2) $x^4 + x^3 + 2x^2 + x + 1 = 0$

$x_1^3 + x_2^3 + x_3^3 + x_4^3 = ?$

3) $x^3 + 3x - 5 = 0$

$x_1^5 + x_2^5 + x_3^5 = ?$

24.04.2016

SEMINAR 8

$\boxed{1}$ $\begin{cases} x^5 + y^5 = 33 \\ x + y = 3 \end{cases}$

$t^2 + bt + c = 0$

$b = -3$

$c = xy = ?$

$P_5 = x^5 + y^5 = P_4 S_1 - P_3 S_2$

$P_4 = P_3 S_1 - P_2 S_2$

$P_3 = P_2 S_1 - P_1 S_2$

$\left.\begin{array}{l} P_2 = P_1 S_1 - 2S_2 \\ P_1 = S_1 = 3 \end{array}\right\} \Rightarrow P_2 = 3 \cdot 3 - 2S_2 = 9 - 2S_2$

$\Rightarrow P_3 = 3(9 - 2S_2) - 3S_2 = 27 - 6S_2 - 3S_2 = 27 - 9S_2 = 9(3 - S_2)$

$\Rightarrow P_4 = 27(3 - S_2) - (9 - 2S_2) = 81 - 27S_2 - 9S_2 + 2S_2^2 = 2S_2^2 - 36S_2 + 81$

$\Rightarrow P_5 = 3(2S_2^2 - 36S_2 + 81) - S_2(27 - 9S_2) = 33$

$6S_2^2 - 108S_2 + 243 - 27S_2 + 9S_2^2 = 33$

$15S_2^2 - 135S_2 + 243 = 33 \quad |:3$

$5S_2^2 - 45S_2 + 81 = 11 \Leftrightarrow 5S_2^2 - 45S_2 + 70 = 0 \Leftrightarrow$

$\Leftrightarrow S_2^2 - 9S_2 + 14 = 0$

$\Delta = 81 - 56 = 25 \Rightarrow S_{2_1} = \frac{9+5}{2} = \frac{14}{2} = 7$, $\quad S_{2_2} = \frac{9-5}{2} = \frac{4}{2} = 2$

$t^2 + bt + c = 0 \Leftrightarrow t^2 - 3t + 2 = 0$

$\Delta = 9 - 8 = 1$

$t_1 = \frac{3+1}{2} = 2 = x$

$t_2 = \frac{3-1}{2} = 1 = y$

$\boxed{2}$ $\sqrt[4]{97 - x} + \sqrt[4]{x} = 5 \Leftrightarrow \sqrt[4]{97 - x} = 5 - \sqrt[4]{x} \quad |^4 \Leftrightarrow 97 - x = (5 - \sqrt[4]{x})^4$

$\left.\begin{cases} 97 - x \geq 0 \Rightarrow 97 \geq x \\ x \geq 0 \end{cases}\right\} \Rightarrow 0 \leq x \leq 97 \Rightarrow x \in [0, 97]$

$a = \sqrt[4]{97 - x}$

$b = \sqrt[4]{x}$

$\Rightarrow \begin{cases} a + b = 5 \\ a^4 + b^4 = 97 \end{cases}$

$t^2 - S_1 t + S_2 = 0$

$S_1 = 5$

$P_4 = P_3 S_1 - P_2 S_2$

$P_3 = P_2 S_1 - P_1 S_2$

$P_2 = S_1^2 - 2S_2 = 25 - 2S_2$

$P_1 = S_1 = 5$

$\Rightarrow P_3 = 5(25 - 2S_2) - 5S_2 = 125 - 15S_2$

$\Rightarrow P_4 = 5(125 - 15S_2) - S_2(25$

$= 625 - 75S_2 - 25S_2 + 2$

$= 2S_2^2 - 100S_2 + 625$

$P_4 = 25S_2^2 - 100S_2 + 625 = 97 \Rightarrow 25S_2^2 - 100S_2 + 528 = 0$

$S_2^2 - 50S_2 + 264 = 0$

$\Delta = 2500 - 1056 = 1444$

$S_{2_1} = \frac{50-38}{2} = \frac{12}{2}$

$S_{2_2} = \frac{50+38}{2} = \frac{88}{2} = 4$

$S_1 = 5;\ S_2 = 6$

$t^2 - 5t + 6 = 0$

$a = 2$
$b = 3$ $\Rightarrow$ $x_1 = 16$
$x_2 = 81$

$S_1 = 5;\ S_2 = 44$

$t^2 - 5t + 44 = 0$

$\Delta = 25 - 44 \cdot 4 < 0$

$\boxed{3}$ $X^6 + aX + 5 \in \mathbb{Z}_7[X]$

$a = \hat{0} \Rightarrow X^6 + \hat{5}$

$\mathbb{Z}_7$ corp cu 7 elemente

$(\mathbb{Z}_7, +)$ - grup ciclic cu 7 elemente

$(\mathbb{Z}_7, \cdot)$ - nu este grup, pentru că $\hat{0}$ nu este inversabil

$\mathbb{Z}_7 \setminus \hat{0}$ - grup cu "·" cu 6 elemente

$\Rightarrow$ (orice element)$^{\text{ord } gr}$ = element neutru

$\Rightarrow \forall a \in \mathbb{Z}_7 \setminus \hat{0},\ a^6 = \hat{1}$

$\Rightarrow a, x+6$

$\boxed{4}$ Descrieți în factori ireductibili:

$x^n - 1$ în $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$.

Dacă $n = 2 \Rightarrow x^2 - 1 = (X-1)(X+1)$ ireductibil în $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$

$n = 3 \Rightarrow x^3 - 1 = (X-1)(X^2+X+1)$ descriere de factori ireductibili pe $\mathbb{Q}[X]$, $\mathbb{R}[X]$

ireductibil peste $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$

$x^2 + x + 1 = 0$

$\Delta = (1)^2 - 4 = -3$

$x_1 = \frac{-1+i\sqrt{3}}{2}$

$x_2 = \frac{-1-i\sqrt{3}}{2}$

$\Rightarrow x^3 - 1 = (X-1)\left(X - \frac{i\sqrt{3}-1}{2}\right)\left(X - \frac{-i\sqrt{3}-1}{2}\right)$ descriere de factori ireductibili peste $\mathbb{C}[X]$

$n=4 \Rightarrow X^4-1=(X^2-1)(X^2+1)=(X-1)(X+1)(X^2+1)$ descriere de factori ireductibili peste $\mathbb{Q}[X]$ și $\mathbb{R}[X]$

$X^4-1=(X-1)(X+1)(X-i)(X+i)$ descriere de factori ireductibili peste $\mathbb{C}[X]$

$n=6 \Rightarrow X^6-1=(X^3-1)(X^3+1)=(X-1)(X^2+X+1)(X+1)(X^2-X+1)$ descriere de factori ireductibili peste $\mathbb{Q}[X]$ și $\mathbb{R}[X]$

$n=5 \Rightarrow X^5-1=(X-1)\underbrace{(X^4+X^3+X^2+X+1)}_{\text{ireductibil peste } \mathbb{Q} \leftarrow \boxed{\text{TEMĂ}}}\ (*)$

Presupunem că e reductibil. Arătăm că nu e posibil să fie produs de două polinoame ireductibile.

$X^5-1=0$

$x_k=\cos\frac{2k\pi}{5}+i\sin\frac{2k\pi}{5},\ k=\overline{0,4}$

$x_0=\cos 0+i\sin 0=1$

$x_1=\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}$

$x_2=\cos\frac{4\pi}{5}+i\sin\frac{4\pi}{5}$

$x_3=\cos\frac{6\pi}{5}+i\sin\frac{6\pi}{5}$

$x_4=\cos\frac{8\pi}{5}+i\sin\frac{8\pi}{5}$

$$X^5-1=(X-1)\left(X-\cos\frac{2\pi}{5}-i\sin\frac{2\pi}{5}\right)\left(X-\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}\right)\left(X-\cos\frac{4\pi}{5}-i\sin\frac{4\pi}{5}\right)$$

$\left(X-\cos\frac{4\pi}{5}+i\sin\frac{4\pi}{5}\right)$. $\leftarrow$ descompunere de factori ireductibili peste $\mathbb{C}$

$X^5-1=(X-1)\left(X^2-2\cos\frac{2\pi}{5}X+1\right)\left(X^2-2\cos\frac{4\pi}{5}X+1\right) \leftarrow$ descompunere de factori ireductibili peste $\mathbb{R}[X]$

(*) $X^4+X^3+X^2+X+1$ ireductibil peste $\mathbb{Q}[X]$

a) Verific că nu are rădăcini în $\mathbb{Q}$ $\left(\pm 1=\frac{\text{div. termen liber}}{\text{div. termen dominant}}\right)$

b) Posibil produs de două polinoame de grad 2 din $\mathbb{Q}[X]$.

Arăt că $\cos\frac{2\pi}{5}$ nu e rațional

$\uparrow 72^\circ$ satisface o ecuație de gradul 3

$\cos 36^\circ$

$3\cdot 72=\frac{6\pi}{5}$

$3x=\pi-2x$

TEMĂ: 440, 441, 442, 443, 446, 449, 450, 452, 453 — pg. 99

EXAMEN !

0[illegible].04.2016

TEMĂ – SEMINAR 8

3 $X^4 + X^3 + 2X^2 + X + 1 = 0$

$x_1^3 + x_2^3 + x_3^3 + x_4^3 = ?$

$s_1 = -1$; $s_2 = 2$; $s_3 = -1$; $s_4 = 1$

$k=3$ și $n=4 \Rightarrow p_3 - p_2 s_1 + p_1 s_2 - 3 s_3 = 0 \Rightarrow p_3 + p_2 + 2p_1 + 3 = 0 \Rightarrow$

$\Rightarrow p_3 = -p_2 - 2p_1 - 3$

$k=2$ și $n=4 \Rightarrow p_2 - p_1 s_1 + 2 s_2 = 0 \Rightarrow p_2 + p_1 + 4 = 0 \Rightarrow p_2 = -4 - p_1$

$k=1$ și $n=4 \Rightarrow p_1 - s_1 = 0 \Rightarrow p_1 = s_1$

$\Rightarrow p_2 = -4 + 1 = -$

$\Rightarrow p_3 = 3 + 2 - 3 = 2 \Rightarrow x_1^3 + x_2^3 + x_3^3 + x_4^3 = 2$

4 $X^3 + 3X - 5 = 0$

$x_1^5 + x_2^5 + x_3^5 = ?$

$s_1 = 0$; $s_2 = 3$; $s_3 = 5$

$k=5$ și $n=3 \Rightarrow p_5 - p_4 s_1 + p_3 s_2 - p_2 s_3 = 0 \Rightarrow p_5 = p_4 s_1 - p_3 s_2 + p_2 s_3 \Rightarrow$

$\Rightarrow p_5 = -3p_3 + 5p_2$

$k=3$ și $n=3 \Rightarrow p_3 - p_2 s_1 + p_1 s_2 - 3 s_3 = 0 \Rightarrow p_3 = p_2 s_1 - p_1 s_2 + 3 s_3 \Rightarrow$

$\Rightarrow p_3 = 3 \cdot 5 - p_1 \cdot 3 = 15 - 3p_1$

$k=2$ și $n=3 \Rightarrow p_2 - p_1 s_1 + 2 s_2 = 0 \Rightarrow p_2 = p_1 s_1 + 2 s_2 \Rightarrow$

$\Rightarrow p_2 = 6$

$k=1$ și $n=3 \Rightarrow p_1 - s_1 = 0 \Rightarrow p_1 = s_1 \Rightarrow p_1 = 0$

$\Rightarrow p_3 = 15$

$p_5 = -3 \cdot 15 + 5 \cdot 6 = 30 - 45 = -15$

Aplicații la lema chineză (TEMA)

aflați ultimele două cifre ale numărului 49^{49}

Să se afle $x \in \mathbb{N}$ min cu proprietatea că $\begin{cases} x \equiv 5 \pmod{48} \\ x \equiv 24 \pmod{35} \end{cases}$

+ 122, 123

~~Ex 121 pg. 84~~