Seminarul 4

Tuesday, March 9, 2021 4:48 PM

Corpuri (cont.)

2.2. $\mathbb{Z}[i]/(3)$ e corp cu 9 elemente.

am văzut data trecută

$\{ \widehat{0+0i}, \widehat{0+1i}, \widehat{0+2i}, \widehat{1+0i}, \ldots, \widehat{2+2i} \}$

Dacă $\widehat{a+bi} \neq \hat{0}$ $(\Leftrightarrow 3 \nmid a$ sau $3 \nmid b)$

$\Rightarrow (\widehat{a+bi}) \cdot (\widehat{a-bi}) = \widehat{a^2+b^2} \neq \hat{0}$ în $\mathbb{Z}_3$!

$\Downarrow$ inversabil!

! $3 \nmid a$ sau $3 \nmid b \Rightarrow 3 \nmid a^2+b^2$

(verificate toate cazurile: $\widehat{1^2+1^2} = \hat{2} \neq \hat{0}$, $\widehat{1^2+2^2} = \hat{5} \neq \hat{0}$, ...)

$$\Longrightarrow \boxed{(\widehat{a+bi})^{-1} = (\widehat{a^2+b^2})^{-1} \cdot (\widehat{a-bi})}$$

$\hat{5}^{-1}$ în $\mathbb{Z}_3$? $\quad \hat{5}^{-1} = \hat{2}$

$\widehat{1891}^{-1}$ în $\mathbb{Z}_{3797}$, dacă există?

<u>Idee</u> Dacă $(1891, 3797) = 1 \Leftrightarrow \exists\, \widehat{1891}^{-1}$

Th Euler $\Rightarrow$ $\widehat{1891}^{\varphi(3797)} = \hat{1}$

neplăcut

Algoritmul lui Euclid: $\underline{\underline{m}} \cdot 1891 + n \cdot 3797 = 1$

$\xRightarrow{\text{în } \mathbb{Z}_{3797}} \hat{m} = \widehat{1891}^{-1}$.

2.2. Ex: $\mathbb{Z}[i]/(5)$ inel cu 25 de elemente care <u>nu este corp</u>

$(\widehat{1+2i})(\widehat{1-2i}) = \hat{5} = \hat{0}$, dar $\widehat{1+2i}, \widehat{1-2i} \neq \hat{0}$.

! În $\mathbb{Z}_5$, se poate ca $\widehat{a^2+b^2} = \hat{0}$ fără ca $\hat{a} = \hat{b} = \hat{0}$.

<u>Exc la care vom reveni</u> $\mathbb{Z}[i]/(p)$ e corp $\Leftrightarrow p \equiv 3\ (4)$

2.1. Fie p prim și K corp (comutativ) cu char $K = p$.

2.1. Fie p prim și K corp comutativ cu (char $K = p$).

$\underbrace{1+1+1+\ldots+1}_{p \text{ ori}} = 0$

Fie $\varphi : K \to K$, $\varphi(x) = x^p$.

Obs Dacă $K = \mathbb{Z}_p$, $\varphi = id$ (Mica Teoremă a lui Fermat: Dacă p prim $\Rightarrow a^p \equiv a \pmod p$)

Atunci:

φ injectivă

i) φ morfism de corpuri

ii) Dacă K finit $\Rightarrow$ φ este izomorfism de corpuri

Dem i)

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ ✓ $\forall a, b \in K$
- $\varphi(1) = 1$ ✓ indiferent de char K

$(ab)^n \underset{\text{comutativ}}{=} a^n b^n$

$\boxed{C_p^i = \binom{p}{i}}$

- $\varphi(a+b) = (a+b)^p \overset{?}{=} a^p + b^p$

$$(a+b)^p = \sum_{i=0}^{p} C_p^i a^{p-i} b^i = a^p + b^p + \sum_{i=1}^{p-1} C_p^i a^{p-i} b^i$$

$\vdots p$ de $1 \le i \le p-1$

char $K = p$: $a^p + b^p$; $C_p^i = \dfrac{p!}{i!(p-i)!}$ p nu se poate simplifica!

Def φ s.n. morfismul Frobenius.

Def K corp. $\mathrm{char}\,K = \mathrm{ord}(1) =$ cel mai mic $n \in \mathbb{N}^*$

a.î. $\underbrace{1+1+\dots+1}_{n} = 0$, dacă $\exists$ astfel de n

$= 0$, dacă $\mathrm{ord}(1) = \infty$.

Obs char K e număr prim (sau 0)

Dacă $\mathrm{char}\,K = m \cdot n$ cu $m, n > 1$, atunci

$0 = \underbrace{1+1+\dots+1}_{mn} = \underbrace{(1+1+\dots+1)}_{m}\underbrace{(1+\dots+1)}_{n} \Rightarrow \underbrace{1+1+\dots+1}_{m} = 0$

sau

$\underbrace{1+1+\dots+1}_{n} = 0$

ko cu minimalitatea lui mn.

2.3. Fie $\mathbb{H}$ corpul cuaternionilor

$\mathbb{H} = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \}$

$i^2 = j^2 = k^2 = -1$ și $k \curvearrowright i \curvearrowright j$ adică $ij = k$

$ji = -k$

$x = a + bi + cj + dk$ $\qquad kj = -i$

$\bar{x} = a - bi - cj - dk$ - - -

și aplicațiile $T: \mathbb{H} \to \mathbb{H}$, $T(x) = x + \bar{x}$

$N: \mathbb{H} \to \mathbb{H}$, $N(x) = x \cdot \bar{x}$.

a) $(1+2i-j+k)(2-i+3j+2k) = 2 + 4i - 2j + 2k$ ←

$-i - 2i^2 + ji - ki$ ←

$+3j + 6ij - 3j^2 + 3\underbrace{kj}_{-i}$ ←

$+2k + 4ik - 2\underbrace{jk}_{i} + 2k^2$ ←

$= (2+2+3-2) + (4-1-3-2)i + (-2-1+3-4)j + (2-1+6+2)k$

$= 5 - 2i - 4j + 9k$

b) Arătați că $T(x)$, $N(x) \in \mathbb{R}$, $\forall x \in \mathbb{H}$

și $\boxed{x^2 - T(x)x + N(x) = 0.}$ ← seamănă cu Hamilton-Cayley

<u>Obs</u> $T(x) = T(a+bi+cj+dk) = 2a \in \mathbb{R}$

$N(x) = (a+bi+cj+dk)(a-bi-cj-dk)$

$= - - — -$

<u>Th (Hamilton-Cayley)</u> $A^2 - tr(A) \cdot A + \det A \cdot I_2 = O_2$,

$\forall A \in \mathcal{M}_2(\mathbb{C})$

Remarcare / Prop

$$\left(\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}, +, \cdot\right) \overset{(*)}{\simeq}$$

$$\left(\left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \;\middle|\; z, w \in \mathbb{C} \right\}, +, \cdot\right)$$

Pt $\mathbb{C}$: $a + bi \longleftrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in \mathbb{R}$

Pt $\mathbb{H}$: $a + bi + cj + dk = \underbrace{(a+bi)}_{z} + \underbrace{(c+di)}_{w} j$

Dem că (*) izomorfism:

$$(z_1 + w_1 j)(z_2 + w_2 j) = z_1 z_2 + z_1 w_2 j + w_1 j z_2 + w_1 j w_2 j$$

$w_1 \overline{w_2} j j = -w_1 \overline{w_2}$

$$= z_1 z_2 + z_1 w_2 j + w_1 \overline{z_2} j - w_1 \overline{w_2} = (**)$$

$\varphi \in \mathbb{C}$, $\varphi = a + bi$, $\varphi j = j \overline{\varphi}$, $\forall \varphi \in \mathbb{C}$

$$(a + bi) j = aj + bk = j(a - bi)$$

$$(**) = (z_1 z_2 - w_1 \overline{w_2}) + (z_1 w_2 + w_1 \overline{z_2}) j$$

$$\begin{pmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{pmatrix} \cdot \begin{pmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{pmatrix} = \begin{pmatrix} z_1 z_2 - w_1 \overline{w_2} & z_1 w_2 + w_1 \overline{z_2} \\ -\left(z_2 \overline{w_1} + \overline{z_1} \overline{w_2}\right) & -\overline{w_1} w_2 + \overline{z_1}\,\overline{z_2} \end{pmatrix}$$

$$= \begin{pmatrix} \underline{z_1 z_2 - w_1 \overline{w_2}} & \underline{z_1 w_2 + w_1 \overline{z_2}} \\ -\overline{\left(z_1 w_2 + w_1 \overline{z_2}\right)} & \overline{\left(z_1 z_2 - w_1 \overline{w_2}\right)} \end{pmatrix}$$

$\Rightarrow$ $(*)$ este izomorfism de corpuri (la fel ca $\mathbb{C}$ din seminarul 1 despre $\mathbb{C}$)

Hamilton–Cayley $\Rightarrow$ $\mathbb{H} \ni x \equiv \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \Rightarrow x^2 - \operatorname{tr}(x) \cdot x + \det x = 0$

$x \equiv z + wj$

$= (a+bi) + (c+di)j$

$\operatorname{tr}(x) = z + \overline{z} = 2a = T(x)$

$\det x = z\overline{z} + w\overline{w} = a^2 + b^2 + c^2 + d^2$

? $N(x) = x\overline{x} = z\overline{z} + w\overline{w}$?

$$N(x) = x\overline{x} = (z + wj) \cdot \overline{(z + wj)} \overset{!}{=} (z + wj) \cdot (\overline{z} - wj)$$

$$= z\overline{z} \cancel{- zwj} + \underbrace{wj\overline{z}}_{\cancel{wzj}} \underbrace{- wjwj}_{+ w\overline{w}} = z\overline{z} + w\overline{w} \quad \checkmark$$

! $\overline{(z + wj)} = \overline{\left((a+bi) + (c+di)j\right)} = \overline{a + bi + cj + dk}$

$= a - bi - cj - dk = (a - bi) + (-c - di)j = \bar{z} + (-w)j$

Cayley $\Rightarrow$ $x^2 - T(x)x + N(x) = 0$ și $T(x), N(x) \in \mathbb{R}$

c) $(1+2i-j+k)^{-1} = ?$

$$\boxed{x\bar{x} = N(x) = a^2+b^2+c^2+d^2} \Rightarrow$$

$\Rightarrow$ x e inversabil $\Leftrightarrow$ $N(x) \neq 0$ $(\Leftrightarrow x \neq 0)$ și $x^{-1} = \frac{1}{N(x)}\bar{x}$

$$\Rightarrow (1+2i-j+k)^{-1} = \frac{1}{N(1+2i-j+k)}\overline{(1+2i-j+k)}$$

$$= \frac{1}{7}(1-2i+j-k).$$

d) $Z(\mathbb{H}) = ?$ $\quad a, b, c, d \in \mathbb{R}$; $\quad Z(\mathbb{H}) = \{x \in \mathbb{H} \mid xy = yx, \forall y \in \mathbb{H}\}$

i k j

Fie $x = a + bi + cj + dk$

$$\left.\begin{aligned} ix &= ai - b + ck - dj \\ xi &= ai - b - ck + dj \end{aligned}\right\} \xRightarrow{ix = xi} c = d = 0 \quad (1)$$

$$jx = aj - bk - c + di \quad \xRightarrow{jx = xj} \quad b = d = 0 \quad (2)$$

$$\left.\begin{aligned} jx &= aj - bk - c + di \\ xj &= aj + bk - c - di \end{aligned}\right\} \overset{jx=xj}{\Longrightarrow} b = d = 0 \quad (2)$$

$\Rightarrow x = a \in \mathbb{R}$. Pe de altă parte, evident $\mathbb{R} \subset Z(\mathbb{H})$

$$\Rightarrow Z(\mathbb{H}) = \mathbb{R} = \{a + 0i + 0j + 0k \mid a \in \mathbb{R}\}$$

e) Comentariu (corolar la Bezout)

Dacă R domeniu (comutativ & integru), atunci un polinom $f \in R[X]$ are cel mult n rădăcini.
$\deg f = n$

"Dem" a răd a lui $f \overset{\text{Bezout}}{\Longleftrightarrow} (X-a) \mid f \Leftrightarrow f = g(X-a)$, $g \in R[X]$.

R domeniu $\Rightarrow \deg g = n-1$ + inducție

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

Dacă renunțăm la comutativitate:

e) Rezolvați ecuația $\boxed{x^2 = -1}$ în $\mathbb{H}$.

Obs: i, j, k sunt rădăcini!

$$x^2 = -1 \quad \Big| \cdot N(\ )$$

$$N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$$

(pt că $N(z + wj) = \det\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$)

$$\Rightarrow \underbrace{N(x^2)}_{= (N(x))^2} = 1$$

$$\Rightarrow (a^2 + b^2 + c^2 + d^2)^2 = 1 \quad \ldots ?$$

$$x^2 = -1 \quad \Big| \cdot \bar{x}$$

$$N(x) \cdot x = -\bar{x}$$

$$N(x)(a + bi + cj + dk) = -a + bi + cj + dk$$

$$\Rightarrow \overset{\geq 0}{N(x)} \cdot a = -a \Longrightarrow a = 0$$

$$\left.\begin{array}{l} N(x) \cdot b = b \\ N(x) \cdot c = c \\ N(x) \cdot d = d \end{array}\right\} \Longrightarrow N(x) = 1$$

b, c, d nu pot fi toate 0

Deci, dacă $x^2 = -1 \Rightarrow a = 0$ și $N(x) = 1$

Reciproc, dacă $a = 0$ și $N(x) = 1 \Rightarrow x = -\bar{x} \quad \Big| \cdot x$

$$\Rightarrow x^2 = -x\bar{x} = -N(x) = -1.$$

$\Rightarrow$ rădăcinile lui $x^2=-1$ sunt $\left\{ x \in \mathbb{H} \mid T(x)=0 \text{ și } N(x)=1 \right\}$

Dacă renunțăm la integritate:

$R=\mathbb{Z}\times\mathbb{Z}$, polinomul $(1,0)\cdot X=(0,0)$ are rădăcinile $\{(0,n) \mid n\in\mathbb{Z}\}$.

Inele de polinoame

3.1. Fie R inel integru, comutativ și $x\in R$ nilpotent.

a) rx e nilpotent, $\forall r\in R$

x nilpotent $\Rightarrow \exists\, n\in\mathbb{N}^*$ a.î. $x^n=0$.

$\Rightarrow (rx)^n = r^n\cdot x^n=0$.

b) $1+x$ e inversabil;

$\exists n$ a.î. $x^n=0 \Rightarrow x^{2n+1}=0$

$\Rightarrow 1=1+x^{2n+1}=(1+x)(1-x+x^2-\dots-x^{2n-1}+x^{2n})$

$(1-x)(1+x+x^2+\dots+\dots+x^{n-1})=1-x^n=1$

$\Rightarrow 1-x$ inversabil

Dt $y=-x$ tot nilpotent $\Rightarrow$ $\underset{\substack{\| \\ 1+x}}{1-y}$ inversabil.

c) $u+x$ inversabil, dacă u inversabil

$u^{-1}(u+x) = 1+\underbrace{u^{-1}x}_{\text{nilpotent din a)}}$ $\leftarrow$ inversabil din b)

3.2. Fie R comutativ și $f = a_0+a_1X+\dots+a_nX^n \in R[X]$.

a) Dem că f e inversabil în $R[X] \Leftrightarrow a_0 \in U(R)$ și $a_1, a_2, \dots a_n$ nilpotente.

Dem „$\Leftarrow$" a_iX^i nilpotent, $\forall i=\overline{1,n}$

a_0 inversabil

$\overset{3.1.c)}{\Longrightarrow}$ $\underbrace{a_0}_{u}+\underbrace{\sum_{i=1}^{n} a_iX^i}_{x}$ este inversabil

„$\Rightarrow$" $\exists g = b_0+b_1X+\dots+b_mX^m \in R[X]$ și $fg=1$.

$\Rightarrow a_0\cdot b_0 = 1$ $\leftarrow$ în grad 0 $\Rightarrow$ a_0 (și b_0) sunt inversabile

$a_n \cdot b_m = 0 \leftarrow$ în grad $n+m$

$a_n b_{m-1} + a_{n-1} b_m = 0 \;\Big|\cdot a_n \Rightarrow a_n^2 b_{m-1} + a_{n-1} \underbrace{b_m a_n}_{0} = 0$

(în grad $n+m-1$) $\Rightarrow a_n^2 b_{m-1} = 0$

$$(a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + a_n X^n) \cdot (b_0 + b_1 X + \ldots + b_{m-1} X^{m-1} + b_m X^m) = 1$$

În grad 1, $a_1 b_0 + a_0 b_1 = 0$

$$(5 + 2X - 3X^2)(6 + X + X^2 - 3X^3 + 2X^4) = (-3) \cdot 2X^6$$

În grad $n+m-2$: $a_{n-2} b_m + a_{n-1} b_{m-1} + a_n b_{m-2} = 0 \;\Big|\cdot a_n^2$

$$\Rightarrow a_{n-2} \cancel{b_m a_n^2} + a_{n-1} \cancel{b_{m-1} a_n^2} + a_n^3 b_{m-2} = 0$$

La fel, $a_n^{k+1} b_{m-k} = 0$, $\forall\ 0 \le k \le m$.

$\Rightarrow a_n^{m+1} b_0 = 0$ inversabil $\Big|\cdot a_0 \Rightarrow \boxed{a_n^{m+1} = 0}$

$\Rightarrow a_n$ nilpotent

$\Rightarrow (f - a_n X^n)$ inversabil

$//$ + inducție

// (nilpotent)

$a_0+a_1X+\dots+a_{n-1}X^{n-1}$ $\xRightarrow{\text{la fel}}$ a_{n-1} nilpotent

$\Rightarrow \dots$

b) f nilpotent $\overset{\text{în } R[X]}{\iff}$ $a_0, a_1, \dots a_n$ nilpotenți în R

<u>Dem</u> „$\Leftarrow$" <u>Obs</u> x, y nilpotenți $\Rightarrow x+y$ nilpotent

$$\left.\begin{array}{l} x^n=0 \\ y^m=0 \end{array}\right\} \Rightarrow (x+y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^{n+m-i}$$

$$= \sum_{\substack{i=0 \\ i\le n}}^{n+m} \binom{n+m}{i} x^i \underbrace{y^{n+m-i}}_{0} + \sum_{\substack{i=0 \\ i>n}}^{n+m} \binom{n+m}{i} \underbrace{x^i}_{0} y^{n+m-i}$$

$i \le n \Rightarrow n+m-i > m$

$= 0$

În plus, $a_0, a_1X, a_2X^2, \dots a_nX^n$ nilpotente

$\xRightarrow{\text{obs}}$ $a_0+a_1X+\dots+a_nX^n = f$ nilpotent

„$\Rightarrow$" f nilpotent $\Rightarrow$ $1+f$ este inversabil $\xRightarrow{a)}$ $a_1, a_2, \dots a_n$ nilpotenți

$1+f = (a_0+1)+a_1X+\dots+a_nX^n$ (a_0+1 inversabil)

" " " "

$(a_0+1)+a_1X+\dots+a_nX^n$ (și $1+a_0$ inversabil)

nilpotent

Din $f^n=0$ pt un $n \Rightarrow a_0^n=0 \Rightarrow a_0$ nilpotent.

c) f este divizor al lui zero $\Leftrightarrow \exists a\in R$, $a\neq 0$ a.î. $af=0$.

<u>Dem</u> „$\Leftarrow$" din definiție:

$\exists a\in R$, $a\neq 0$ a.î. $af=0$

$\Rightarrow \exists g\in R[X]$, $g\neq 0$, $g=a$, a.î. $gf=0 \leftarrow$ definiția divizorului lui zero

„$\Rightarrow$" $(\exists a\in R,\ a\neq 0$ a.î. $af=0) \Leftrightarrow$ ($a_0, a_1, \dots a_n$ sunt divizori ai lui zero)

Temă!

d) f idempotent în $R[X] \Leftrightarrow a_0$ e idempotent și $a_1=a_2=\dots=a_n=0$.

Temă!

3.3. Determinați numărul de polinoame de grad 2

a) ireductibile

b) nilpotente

din $\mathbb{Z}_{36}[X]$.

Dem a) $f = \underset{\text{inv}}{a_0} + \underset{\text{nilpotenți}}{a_1 X + a_2 X^2}$ & $a_2 \neq 0$.

b) $f = \underbrace{a_0 + a_1 X + a_2 X^2}_{\text{nilpotenți}}$ & $a_2 \neq 0$.

$36 = 2^2 \cdot 3^2$

$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$

Se reduce la $|U(\mathbb{Z}_{36})| = \varphi(36) = 36\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = \cancel{36}^{12} \cdot \frac{1}{\cancel{2}} \cdot \frac{\cancel{2}}{\cancel{3}} = 12$

$|N(\mathbb{Z}_{36})| = 2^{2-1} \cdot 3^{2-1} = 6$

(Ex 1 (sau 2) din seminarul 1)

$\Rightarrow$ a) $\underset{a_0}{12} \cdot \underset{a_1}{6} \cdot \underset{a_2}{5} = \ldots$

b) $\underset{a_0}{6} \cdot \underset{a_1}{6} \cdot \underset{a_2}{5} = 180$

Temă "La fel pentru inelul de serii formale" $\left(\mathbb{Z}[i] / (1+2i) \right)$

Ex R comutativ $f = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n + \ldots \in R[[X]]$

Exc R comutativ $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n + \dots \in R[[X]]$ inelul de serii formale.

a) f e inversabil $\Leftrightarrow$ a_0 e inversabil

$$\left((1-X)(1+X+X^2+\dots) = 1 \right)$$

b) f nilpotent $\Rightarrow$ a_i nilpotenți, $\forall i \geq 0$.

Dați un contraexemplu pentru reciproca

c) f idempotent $\Leftrightarrow$ $a_0^2 = a_0$ și $a_i = 0$, $\forall i \geq 1$.

Exc K corp $\Rightarrow$ singurele ideale proprii ale lui $K[[X]]$ sunt cele de tipul (X^n), $n \geq 1$.

În particular, $K[[X]]$ inel local.