e^{ix}

(S1) Inele și corpuri

Def Un inel este un triplet de forma $(A, +, \cdot)$, unde A este o mulțime nevidă și $+, \cdot$ două op. pe A cu proprietățile:

1) $(A, +)$ grup abelian
2) $(A, \cdot)$ monoid
3) înmulțirea e distrib. față de adunare

$$\begin{cases} a(b+c) = ab + ac \\ (b+c)a = ba + ca \end{cases}, \forall a, b \in A$$

Def Un inel comutativ în care orice element nenul este inversabil se numește corp.

$(\mathbb{Z}, +, \cdot)$
$(\mathbb{Q}, +, \cdot)$
$(\mathbb{R}, +, \cdot)$
$(\mathbb{C}, +, \cdot)$
$(\mathbb{Z}_n, +, \cdot)$
} inele comutative

$U(\mathbb{Z}) = \{\pm 1\}$
$(\mathbb{Q}, +, \cdot)$ corp $U(\mathbb{Q}) = \mathbb{Q}^*$
$(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ corpuri

$\forall n \geq 2$, $(\mathbb{Z}_n, +, \cdot)$ este corp $\Leftrightarrow$ n este nr prim
$\mathbb{Z}_n$ este corp $\Leftrightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{\hat{0}\}$ $\Leftrightarrow$
$\Leftrightarrow$ $\hat{x}$ reprimă cu n se divid cu n $\Leftrightarrow$ n prim
$(\mathbb{Z}_2, +, \cdot)$, $(\mathbb{Z}_5, +, \cdot)$, ... corpuri
$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$
$(\mathbb{Z}[i], +, \cdot)$ inel
$U(\mathbb{Z}[i]) = ?$

Fie $z_1 = a + bi \in \mathbb{Z}[i]$: $a, b \in \mathbb{Z}$
$z_1 \in U(\mathbb{Z}[i]) \Leftrightarrow \exists\, z_2 \in \mathbb{Z}[i]$, $z_2 = c + di$ a.î. $z_1 z_2 = 1$

$a\hat{i}\ (a+bi)(c+di)=1$

$|(a+bi)(c+di)|=1^2$ $\quad a^2=0, b^2=1 \Rightarrow a=0, b=\pm 1 \Rightarrow 0\pm i$

$(a^2+b^2)(c^2+d^2)=1 \Rightarrow a^2+b^2=1 \leftarrow a^2=1, b=0 \Rightarrow a=\pm 1, b=0 \Rightarrow \pm 1$

$\in \mathbb{N} \quad \in \mathbb{N}$

$c^2+d^2=1$

$U(\mathbb{Z}[i])=\{\pm 1, \pm i\}$

Def: Spunem că inelul A are divizori ai lui zero, dacă $\exists\, x,y\in A, x,y\neq 0$ a.î. $x\cdot y=0$.

ex $\mathbb{Z}_6: \hat{2}\cdot\hat{3}=\hat{6}=\hat{0} \Rightarrow (\mathbb{Z}_6,+,\cdot)$ are divizori ai lui 0.

$(\mathbb{Z}\times\mathbb{Z},+,\cdot)\ (0,1)\cdot(1,0)=(0,0)$

Rinel; $\forall n\geq 2$, $(M_n(R),+,\cdot)$ = inelul matricelor de ordin n cu elem din R

$\forall n\geq 2, (M_n(R),+,\cdot)$ este un inel necomutativ cu divizori ai lui zero

$n=2$ $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$

$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ $\Rightarrow M_2(\mathbb{R})$ este necom

$\neq O_2 \quad \neq O_2$

$\Rightarrow M_2(\mathbb{R})$ are div. ai lui zero

$U(M_n(R))=GL_n(R)$ - grupul general liniar de ordin n cu elem din R

(mat. inversabile)

$GL_n(R)=\{A\in M_n(R) \mid \det A\neq 0\}$

$GL_n(\mathbb{Z}_6)=\{A\in M_n(\mathbb{Z}_6) \mid \text{cmmdc}(\det A, 6)=1\}$

① Fie $a,b\in\mathbb{R}^*, c\in\mathbb{R}$

Def pe $\mathbb{R}$ legea de comp

$x*y=ax+by+c, \forall x,y\in\mathbb{R}$

Def a,b,c a.î. $(\mathbb{R},*,\cdot)$ să fie inel. Ce obținem?

Verif assoc. lui $*$: $(x*y)*z = x*(y*z)$

$(ax+by+c)*z = x*(ay+bz+c)$

~~$a(ax+by+c)+bz+c$~~

$(cx+by+c)+bz+c =$

$= ax + b(ay+bz+c)+c$

$a^2x + aby + ac + bz = ax + aby + b^2z$

~~$ax(a-1) + c(a-b) + zb(1-b) = 0$~~ bc

$a^2 = a \Rightarrow a = 1$

$ac = bc$

$b^2 = b \Rightarrow b = 1$

$a, b \neq 0$

$x * y = x + y + c$

Com este evidente

Elem neutro, $x * e = x$.

$x + e + c = x$

$e + c = 0 \Rightarrow e = -c$.

Elem inv, $\forall x \in \mathbb{R}^*, \exists x^{-1} \in \mathbb{R}$ a $x * x^{-1} = -c$

$x + x^{-1} + c = -c$.

$x^{-1} = -x - 2c \in \mathbb{R}$.

$(\mathbb{R}, *)$ grup com

~~Verif~~ assoc, $\forall x \in \mathbb{R}$, 1 elem neutro

~~$(x*y)*z = x*(y*z)$~~

Distributividade:

$(x*y)\cdot z = xz * yz$

$(x+y+c)\cdot z = xz + yz + c$

$xz + yz + cz = xz + yz + c \Rightarrow c = cz \ \forall z \in \mathbb{R}$

$\Rightarrow c = 0$

Daí $x * y = x + y$

Em conclusão, $\exists$ um único anel $(\mathbb{R}, *, \cdot)$ em que a lei $*$ é definida por $x * y = ax + by + c$, $c, b \in \mathbb{R}^*$, $c \in \mathbb{R}$ e onde $(\mathbb{R}, +, \cdot)$

$x^2 = a$ elem. idempotente

② Să se rezolve sist de ec în inelul $\mathbb{Z}_{12}$

a) $\begin{cases} \hat{3}x + \hat{2}y = \hat{1} \\ \hat{5}x + \hat{3}y = \hat{2} \end{cases}$ b) $\begin{cases} \hat{2}x + \hat{3}y = \hat{2} \\ \hat{5}x + \hat{6}y = \hat{3} \end{cases}$

a) $(-)\ \begin{matrix} x + y = \hat{1} \\ \hat{5}x + \hat{2}y = \hat{1} \end{matrix} \quad \begin{matrix} |\cdot 2 \\ \end{matrix} \quad \begin{cases} \hat{2}x + \hat{2}y = \hat{2} \\ \hat{3}x + \hat{2}y = \hat{1} \end{cases} \Rightarrow \hat{x} = -\hat{1} \Rightarrow x = \hat{11} \Rightarrow y = \hat{2}$

b) ~~(d,d)~~ $12 : 7 = 1 \cdot 7 + 5$

$12 = 1 \cdot 7 + 5$

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

~~$1 + \frac{1}{1 + \frac{1}{2}}$~~ $= 1 + \frac{1}{\frac{3}{2}} = 1 + \frac{2}{3} = \frac{5}{3}$

	s_j	q_j	t_j
$j=0$	12	—	0
$j=1$	2	1	1
$j=2$	5	1	-1
$j=3$	2	2	2
$j=4$	1	2	-5

$t_j = t_{j-2} - t_{j-1} \cdot q_{j-1}, \forall j \geq 2.$

$t_0 = 0, t_1 = 1.$

$(t_j)_{j \geq 0}$ $t_2 = 0 - 1 \cdot 1 = -1$

$t_3 = 1 + 1 \cdot 1 = 2.$

$t_4 = -1 - 2 \cdot 2 = -5$

$7^{-1} \pmod{12} = -5 = 7.$

$7x + 3y = 2 \mid \cdot \hat{7}^{-1} = 7$

$x + 21y = 14$

$x + 9y = 2$

$x = 2 - 9y$

$4(2 - 9y) + 6y = 3$

$8 - 36y + 6y = 3$

$8 + 6y = 3$

$6y = -5 \rightarrow 6y = 7 \Rightarrow$ am are sol

$6y \neq 7 \Rightarrow$ sist e incompatibil

Fie A un inel

O submult $\emptyset \neq B \subseteq A$ se numește subinel dacă 1) $B \leq (A,+)$, adică $x-y \in B, \forall x,y \in B$

" 2) B este parte stabilă în raport cu " dacă $xy \in B, \forall x,y \in B$

" 3) $1 \in B$

$\mathbb{Z}[i] \subseteq \mathbb{C}$ $\quad (a+bi)-(c+di) = \underbrace{(a-c)}_{\in\mathbb{Z}} + \underbrace{(b-d)}_{\in\mathbb{Z}} i \in \mathbb{Z}[i]$

$\{a+bi \mid a,b \in \mathbb{Z}\}$

$(a+bi)(c+di) = \underbrace{(ac-bd)}_{\in\mathbb{Z}} + \underbrace{(ad+bc)}_{\in\mathbb{Z}} i \in \mathbb{Z}[i]$ $\quad \forall x,y \in B$

$1 = 1 + 0 \cdot i \in \mathbb{Z}[i]$

$\Rightarrow \mathbb{Z}[i]$ subinel al lui $\mathbb{C}$.

Alt exemplu:

$\{\frac{a}{b} \mid a,b \in \mathbb{Z}, b \text{ impar}\} \subseteq \mathbb{Q}$ subinel

Def Fie A un inel. Se numește ideal stg o mulțime $\emptyset \neq J \subseteq A$ cu

i) $x-y \in J, \forall x,y \in J$

ii) $ax \in J, \forall a \in A, x \in J$

A = comut $\Rightarrow ax = xa$ - not de ideal stg $\equiv$ id dreapt (ideal)

③ Să se studieze dacă următ. submulțimi sunt ideale ale unor inele respective:

a) $J_1 = \{f \in \mathbb{Z}[X] \mid \text{grad}(f) \geq 6\}$, $R = \mathbb{Z}[X]$.

fie $f = X^6 + X \in J_1$

$g = X^6 \in J_1$

$f - g = X^6 + X - X^6 = X \notin J_1 \Rightarrow J_1$ nu e ideal în $\mathbb{Z}[X]$

$0 \notin J_1 \Rightarrow J_1$ nu e subinel

b) $J_2 = \{f \in \mathbb{Z}[X] \mid \text{grad } f = 5\} \cup \{0\}$.

$f = X^5 + X^2 \in J_2$

$g = X^5 \in J_2$

dar $f - g = X^2 \notin J_2 \Rightarrow J_2$ nu e ideal în $\mathbb{Z}[X]$

c) $I_3 = \{ f \in \mathbb{Z}[x] \mid \text{grad } f \leq 3 \}$
$i = x^2 \cdot 3$
$\varepsilon = x^3 + x \in \mathbb{Z}[x]$ } $\Rightarrow a = x^5 + \dots \notin I_3$

d) $I_4 = \{ f \in \mathbb{Q}[x] \mid 2 \text{ este rad pt } f \}$
$\mathbb{Z} = \mathbb{Q}[x]$
Fie $f, g \in I_4 \Rightarrow f(2) = 0$
$g(2) = 0$
$(f \cdot g)(2) = f(2) \cdot g(2) = 0 \cdot 0 = 0 \Rightarrow fg \in I_4$
Fie $f \in I_4$, $p \in \mathbb{Q}[x]$
$(fp)(2) = f(2) p(2) = 0 \Rightarrow fp \in I_4$ } $\Rightarrow I_4$ ideal

e) $I_5 = \{ A = \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \in M_2(\mathbb{R}) \mid a, b \in \mathbb{R} \}$
Fie $A = \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \in I_5$
$A - B = \begin{pmatrix} 0 & 0 \\ a-c & b-d \end{pmatrix} \in I_5$

- ideal stg
Fie $\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \in I_5$, $\begin{pmatrix} m & n \\ p & q \end{pmatrix} \in M_2(\mathbb{R})$
$\begin{pmatrix} m & n \\ p & q \end{pmatrix} \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} = \begin{pmatrix} na & \dots \\ \dots & \dots \end{pmatrix} \notin I_5 \Rightarrow$ nu e ideal stg

- ideal drept
$\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \begin{pmatrix} m & n \\ p & q \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ am+bp & an+bq \end{pmatrix} \in I_5 \Rightarrow I_5$ e ideal drept

Algebră Seminar 2.

$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

$U(\mathbb{Z}) = \{\pm 1\}$

$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

$U(\mathbb{Z}[\sqrt{2}]) = \{\pm (1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$

Notez cu $u = 1+\sqrt{2}$ e un element inversabil $|1+\sqrt{2}| = 1$.

$R = \mathbb{Z}[\sqrt{2}]$

Fie $W = \{a + b\sqrt{2} \in U(R) \mid a, b \in \mathbb{N}\}$

Vă uit la $x \cdot u^{-n}$, $x \in W$ $\left(u^{-1} \in R \Rightarrow u^{-n} \in R\right)$

Notez $x \cdot u^{-n} = c + d\sqrt{2} > 0$ (o alegere)

1. $cd > 0 \Rightarrow c, d > 0 \Rightarrow x \cdot u^{-n} \in W$

$x \in W \Rightarrow \exists n \in \mathbb{N}$ a.î. $x \in [u^n, u^{n+1})$

$x \cdot u^{-n} \in W \Rightarrow x \cdot u^{-n} \geq 1+\sqrt{2} = u \overset{\cdot u^n}{\Rightarrow} x \geq u^{n+1}$ ✗

2. $cd < 0 \Rightarrow \underbrace{x \cdot u^{-n}}_{\in U(R) = c + d\sqrt{2}} = \frac{c^2 - 2d^2}{c - d\sqrt{2}}$

Obs $x \cdot u^{-n}$ este el. inversabil $\Rightarrow |x \cdot u^{-n}| = 1$

$\exists y \in R$ a.î. $(x \cdot u^{-n}) \cdot y = 1 \Rightarrow |(x \cdot u^{-n}) \cdot y| = \underbrace{|x \cdot u^{-n}|}_{\in \mathbb{N}} \cdot \underbrace{|y|}_{\in \mathbb{N}} = 1 \Rightarrow |u^{-n} \cdot x| = 1$

$|x \cdot u^{-n}| = 1 \Rightarrow |c + d\sqrt{2}| = 1 \Rightarrow |(c + d\sqrt{2})(c - d\sqrt{2})| = 1 \Rightarrow |c^2 - d^2 2| = 1 \Rightarrow c - d^2 2 = \pm 1$ (*)

$x \cdot u^{-n} = \frac{c^2 - 2d^2}{c - d\sqrt{2}} \overset{(*)}{=} \frac{1}{|c| + |d|\sqrt{2}} \leq \frac{1}{u} \Rightarrow x \cdot u^{-n} \leq \frac{1}{u} \Rightarrow x \leq u^{n-1}$ ✗

3. $c \cdot d = 0$. $c \neq 0$ $d = 0 \Rightarrow$

$\Rightarrow \underset{\in U(R)}{x} u^{-n} = c \Rightarrow x \cdot u^{-n} = 1 \Rightarrow x = u^n \Rightarrow$ orice element inversabil este o putere de $1+\sqrt{2}$

$U(\mathbb{Z}[\sqrt{2}]) = \{\pm (1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$

$U(\mathbb{Z}[\sqrt{3}]) = ?$

$\sqrt{3} = \boxed{1} + (\sqrt{3} - 1)$

$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} = 1 + \left(\frac{\sqrt{3}+1}{2} - 1\right) = \boxed{1} + \frac{\sqrt{3}-1}{2}$

$\frac{2}{\sqrt{3}-1} = 2\frac{(\sqrt{3}+1)}{2} = \sqrt{3} + 1 = 2 + (\sqrt{3} + 1 - 2) = \boxed{2} + \underline{(\sqrt{3} - 1)}$ STOP

mă opresc dacă o parte fracționară se repetă.

$\sqrt{3} = (1; 1; 2)$ - primul întreg se pun normal, iar a urmează divine perioadă ultimul din perioadă se taie

$1 + \frac{1}{1} = 2 \rightsquigarrow 2 + 1 \cdot \sqrt{3}$

$2 + \sqrt{3}$ unitate fundamentală.

$U(\mathbb{Z}[3]) = \{\pm (2+\sqrt{3})^n \mid n \in \mathbb{Z}\}$

$(1; \overline{1,2,3,4})$ → metoda fracțiilor continue.

$1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3}}}$

Ex2) $U(\mathbb{Z}[\sqrt{29}]) = ?$

$\sqrt{29} = 5 + (\sqrt{29} - 5)$

$\frac{1}{\sqrt{29}-5} = \frac{\sqrt{29}+5}{4} = 2 + \left(\frac{\sqrt{29}+5}{4} - 2\right) = 2 + \left(\frac{\sqrt{29}-3}{4}\right)$

$\frac{4}{\sqrt{29}-3} = \frac{4(\sqrt{29}+3)}{20} = \frac{\sqrt{29}+3}{5} = 1 + \left(\frac{\sqrt{29}+3}{5} - 1\right) = 1 + \left(\frac{\sqrt{29}-2}{5}\right)$

$\frac{5}{\sqrt{29}-2} = \frac{5(\sqrt{29}+2)}{25} = \frac{\sqrt{29}+2}{5} = 1 + \left(\frac{\sqrt{29}+2}{5} - 1\right) = 1 + \left(\frac{\sqrt{29}-3}{5}\right)$

$\frac{5}{\sqrt{29}-3} = \frac{5(\sqrt{29}+3)}{20} = \frac{\sqrt{29}+3}{4} = 2 + \left(\frac{\sqrt{29}+3}{4} - 2\right) = 2 + \left(\frac{\sqrt{29}-5}{4}\right)$

$\frac{4}{\sqrt{29}-5} = \frac{4(\sqrt{29}+5)}{4} = \sqrt{29}+5 = 10 + (\sqrt{29}-5)$ → STOP.

$\sqrt{29} = (5; \underbrace{2,1,1,2,10}_{\text{perioada}})$

$5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}} = 5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{2}{3}}} = 5 + \cfrac{1}{2 + \cfrac{3}{5}} = \frac{13}{5} + \frac{5}{13} =$

$= \frac{70}{13} \rightsquigarrow 70 + 13\cdot\sqrt{29}$

$U(\mathbb{Z}[\sqrt{29}]) = \{\pm (70 + 13\cdot\sqrt{29})^n \mid n \in \mathbb{Z}\}$ $\quad 70^2 + 29\cdot 13^2 = \pm 1$

169 | 29 | 5
145 | 5 | 1
24 | 1
1

A determina elementele inversabile din $\mathbb{Z}[\sqrt{29}]$ e tot una cu a găsi soluțiile ecuației $x^2 - 29y^2 = \pm 1$.

$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$

A determina elem. inversabile din $\mathbb{Z}[\sqrt{d}] \Leftrightarrow$ a găsi soluțiile ec. $x^2 - dy^2 = \pm 1$.

C. Idealele lui $\mathbb{C}$?

R = un corp comutativ

Fie I un ideal. $\{0\} \neq I \subseteq R$. *

Fie $0 \neq x \in I \Rightarrow x \in R \underset{\text{R corp}}{\Rightarrow} x^{-1} \in R \Rightarrow \underset{\in R}{x^{-1}} \cdot \underset{\in I}{x} \in I \Rightarrow 1 \in I \Rightarrow \forall r \in R \; r = r \cdot 1 \in I$

$\Rightarrow R \subseteq I \overset{*}{\Rightarrow} R = I$.

Morala: Singurele ideale într-un corp comutativ sunt $\{0\}, R$.

$\boxed{1 \in I \Rightarrow I = R}$

Idealele din $(\mathbb{Z}, +, \cdot)$

Orice subgrup al lui $(\mathbb{Z}, +, \cdot)$ e de forma $n\mathbb{Z}$, $n \in \mathbb{N}$ și acestea sunt chiar idealele lui $(\mathbb{Z}, +, \cdot)$

Fie $a, b \in n\mathbb{Z} \Rightarrow \begin{matrix} a = na_1 \\ b = nb_1 \end{matrix} \quad \begin{matrix} b_1, a_1 \in \mathbb{Z} \\ n \in \mathbb{N} \end{matrix} \Rightarrow$

$\Rightarrow a - b = na_1 - nb_1 = n(\underset{\in \mathbb{Z}}{a_1 - b_1}) \in n\mathbb{Z}$,

Fie $\begin{matrix} a \in n\mathbb{Z} \\ r \in \mathbb{Z} \end{matrix} \Rightarrow a = na_1$

$ra = a \cdot r = (na_1) \cdot r = n(a_1 \cdot r) \in n\mathbb{Z}$

$(\mathbb{Z}, +, \cdot)$ inel comutativ

$\Rightarrow n\mathbb{Z}$ sunt ideale ale lui $(\mathbb{Z}, +, \cdot)$

Idealele lui $(\mathbb{Z}_n, +, \cdot)$

Subgrupurile lui $(\mathbb{Z}_n, +, \cdot)$ sunt de forma $d\mathbb{Z}_n$ cu d/n și acestea sunt chiar idealele lui $(\mathbb{Z}_n, +, \cdot)$

Fie $\bar{a}, \bar{b} \in d\mathbb{Z}_n \quad \bar{a} = d \cdot \bar{a_1} \quad \bar{b} = d \cdot \bar{b_1}$

$\bar{a} - \bar{b} = d \cdot \bar{a_1} - d \cdot \bar{b_1} = d(\bar{a_1} - \bar{b_1}) = d(\underset{\in \mathbb{Z}_n}{\overline{a_1 - b_1}}) \in d\mathbb{Z}_n$ ①

Fie $\bar{r} \in \mathbb{Z}_n \Rightarrow a \cdot r = r \cdot a \in d\mathbb{Z}_n \quad \bar{a} = d \cdot \bar{a_1}$ $(\mathbb{Z}_n, +, \cdot)$ comutativ ③

$\bar{r} \cdot (d \cdot \bar{a_1}) = d \cdot \bar{r} \cdot \bar{a_1} = d(\underset{\in \mathbb{Z}_n}{\overline{r \cdot a_1}}) \in d\mathbb{Z}_n$ ②

Din ① și ② $\overset{③}{\Rightarrow}$ $d\mathbb{Z}_n$ este ideal al lui $(\mathbb{Z}_n, +, \cdot)$

Problema:

1) Fie $I=20\mathbb{Z}$ $J=36\mathbb{Z}$. Găsiți $I\cap J$, $I+J$, $I\cdot J$.

Propoziție: I, J, ideale în R, R=inel.

1) $I\cap J$ este ideal în R

2) $I+J=\{i+j \mid i\in I, j\in J\}$ ideal în R

3) $I\cdot J=\{\sum_{i=1}^{m} x_i y_i \mid x_i\in I, y_i\in J \quad m\in\mathbb{N}\}=(xy \mid x\in I, y\in J)$

$I=a\mathbb{Z}$ $J=b\mathbb{Z}$

$a\mathbb{Z}\cap b\mathbb{Z}=[a,b]\mathbb{Z}$ (cmmmc(a,b)$\mathbb{Z}$) $\qquad a\mathbb{Z}\cdot b\mathbb{Z}=ab\mathbb{Z}$

$a\mathbb{Z}+b\mathbb{Z}=(a,b)\mathbb{Z}$ (cmmdc(a,b)$\mathbb{Z}$)

$I\cap J=[20,36]\mathbb{Z}=180\mathbb{Z}$

$I+J=(20,36)\mathbb{Z}=4\mathbb{Z}$

$I\cdot J=20\cdot 36\mathbb{Z}=720\mathbb{Z}$

Elemente speciale în inel

1) inversabile ✓ $\qquad U(R)$

2) divizorii lui 0 ✓ $\qquad D(R)$

3 (x se numește divizor al lui 0 dacă $\exists y\neq 0, y\in R$ a.î. $x\cdot y=0$)

3) idempotenți $\qquad Idem(R)$

$x\in R$ s.n. idempotent dacă $x^2=x$

4) nilpotenți $\qquad N(R)$

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

a) Dacă $R=(\mathbb{Z},+,\cdot)$

$U(\mathbb{Z})=\{\pm 1\}$ $\qquad Idem(\mathbb{Z})=\{0,1\}$ $\qquad x^2=x$ în $\mathbb{Z}\Rightarrow x(x-1)=0\Rightarrow$ I $x=0$, II $x=1$

$D(\mathbb{Z})=\{0\}$ $\qquad N(\mathbb{Z})=\{0\}$

b) $R=(\mathbb{Z}_6,+,\cdot)$

$U(\mathbb{Z}_6)=\{\hat{1},\hat{5}\}$ $\qquad Idem(\mathbb{Z}_6)=\{\hat{0},\hat{1},\hat{3},\hat{4},\}$

$D(\mathbb{Z}_6)=\{\hat{0},\hat{2},\hat{3},\hat{4}\}$ $\qquad N(\mathbb{Z}_6)=\{\hat{0}\}$

$D(\mathbb{Z}_n)=\mathbb{Z}_n-U(\mathbb{Z}_n)$

$N(\mathbb{Z}_m)=?$ $\qquad n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ $\qquad p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}\mid \hat{x}^k\Rightarrow p_i\mid x^k, i\in\overline{1,t}\Rightarrow$

$\hat{x}\in N(\mathbb{Z}_m)\Leftrightarrow \exists k\in\mathbb{N}^*$ a.î. $\hat{x}^k=\hat{0}\Leftrightarrow m\mid \hat{x}^k\}_{=1}$

$\Rightarrow p_1p_2\cdots p_t\mid x\Rightarrow x\in \frac{p_1\cdots p_t}{d}\mathbb{Z}_m$

Alg S2
pags

$x \in d\mathbb{Z}_m \Rightarrow x = p_1 \cdots p_t \cdot m$, $m \in \mathbb{Z}_m$

$\Rightarrow ? \nexists N$ a.i. $(\overline{x^N} = \overline{0} \Rightarrow m / (\overline{x^N}) \Rightarrow m / (p_1 p_2 \cdots p_t m)^N =$

$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} \mid (p_1 p_2 \cdots p_t)^N$

$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} \mid p_1^N p_2^N \cdots p_t^N$

$N \geq \max(\alpha_1, \alpha_2, \ldots, \alpha_t)$

$\mathcal{N}(\mathbb{Z}_m) = d\mathbb{Z}_m$, $d = p_1 \cdots p_t$ $m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$.

3) Aflarea coef monoamelor
pt a det coef A și B dăm val notat.

$x_1=1 \quad s_1=2 \quad f(1,1,2)=2=4+A=1A=-2$
$x_2=1 \quad s_2=1$
$x_3=0 \quad s_3=0$

$x_1=1 \quad s_1=3$
$x_2=1 \quad s_2=3 \quad f(1,1,1)=6=27+(-21)\cdot 9+B\cdot 3=9+3B$
$x_3=1 \quad s_3=1 \Rightarrow 6=9+3B \Rightarrow 3B=-3 \Rightarrow B=-1$

Seminar 3

Rezultat: R_1, R_2 inele comutative
$U(R_1\times R_2)=U(R_1)\times U(R_2)$
$Idem(R_1\times R_2)=Idem(R_1)\times Idem(R_2)$
$W(R_1\times R_2)=W(R_1)\times W(R_2)$
$\mathcal{Q}(R_1\times R_2)=?$

Prop:
Fie R un inel comut. și $f=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$ un polinom. $grad(f)=n$, $a_n\neq 0$. Atunci:

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

ii) $f\in U(R[X]) \iff a_1, \dots, a_1\in \mathcal{N}(R), a_0\in U(R)$

iii) $f\in \mathcal{Q}(R[X]) \iff \exists d\in R$ a.i. $d\cdot f=0$
$d\neq 0$.

Ex: Câte polinoame inv sunt în $\mathbb{Z}_5[X]$?
$|U(\mathbb{Z}_5[X])|=?$
Fie $f=a_nx^n+\dots+a_1x+a_0$; $a_0,a_1,\dots,a_n\in\mathbb{Z}_5$
$f\in U(\mathbb{Z}_5[X]) \iff a_1,\dots,a_1\in\mathcal{N}(\mathbb{Z}_5)$ și $a_0\in U(\mathbb{Z}_5)$ (1)
$U(\mathbb{Z}_5)=\{\hat{1},\hat{2},\hat{3},\hat{4}\}$ (2)
$\mathcal{N}(\mathbb{Z}_5)=\{\hat{0}\}$ (3)
Din (1) (2) (3) $\Rightarrow$ 4 polinoame inversabile

$\mathcal{N}(\mathbb{Z}_{54}[X]) = ?$

Fie $f = a_n X^n + \dots + a_1 X + a_0$ cu $a_0, a_1, \dots, a_n \in \mathcal{N}(\mathbb{Z}_{54})$

$\mathcal{N}(\mathbb{Z}_{54}) = 2 \cdot 3 \mathbb{Z}_{54} = 6\mathbb{Z}_{54} = \{\hat{0}, \hat{6}, \hat{12}, \dots, \hat{48}\}$

$54 = 2 \cdot 3^2$

$d = 2 \cdot 3$

Polinoame nilpotente în $\mathbb{Z}_{54}[X]$. Exemplu:

$f = \hat{12} X^4 + \hat{6} X^3 + \hat{48}$

② Factorizați următoarele polinoame în $\mathbb{Z}[X], \mathbb{R}[X], \mathbb{C}[X]$

a) $f_1(X) = X^4 + X^3 - X - 1$

b) $f_2(X) = X^3 + 2X^2 - 5X - 6$

c) $f_3(X) = X^3 + 2X^2 - 4X + 1$

d) $f_4(X) = 4X^4 + 12X^3 + X^2 + 12X + 4$

Sg. polinoame ired din $\mathbb{C}[X]$ sunt cele de grad I. Sg. pol ired din $\mathbb{R}[X]$ sunt cele de grad I + cele de grad II cu $\Delta < 0$.

a) $f_1(X) = X^4 + X^3 - X - 1$

$f_1(X) = X^3(X+1) - (X+1) = (X+1)(X^3 - 1) = (X+1)(X-1)\underbrace{(X^2 + X + 1)}$

$\Delta < 0 \Rightarrow X^2 + X + 1$ ired în $\mathbb{R}[X]$

$X^2 + X + 1 \Rightarrow \Delta = -3 \Rightarrow x_1 = \frac{-1 - i\sqrt{3}}{2}$, $x_2 = \frac{-1 + i\sqrt{3}}{2}$ $\Rightarrow f = (X+1)(X-1)\left(X - \frac{-1-i\sqrt{3}}{2}\right)\left(X - \frac{-1+i\sqrt{3}}{2}\right)$ în $\mathbb{C}[X]$

Continuare Seminar 3

b) $f_2(X) = x^3+2x^2-5x-6$ Să se scrie o soluție?

$f_2(x) = 0 \Leftrightarrow x = 2$

$x^3+2x^2-5x-6 \mid x-2$

$-x^3+2x^2 \quad\quad x^2+4x+3$

$/\ 4x^2-5x-6$

$-4x^2+8x$

$3x-6$

$-3x+6$

$=$

$f_2(x) = (x-2)(x^2+4x+3)$

$\Delta = 16-12 = 4$

$x_{1,2} = \frac{-4 \pm 2}{2} \begin{cases} x_1 = -3 \\ x_2 = -1 \end{cases}$

$f_2(x) = (x-2)(x+3)(x+1)$

c) $f_3(X) = x^3+2x^2-4x+1$

$f_3(1) = 0$

$x^3+2x^2-4x+1 \mid x-1$

$-x^3+x^2 \quad\quad x^2+3x-1$

$3x^2-4x+1$

$-3x^2+3x$

$-x+1$

$f_3(x) = (x-1)(x^2+3x-1)$ - fără pește $\mathbb{Z}[X]$

$\Delta = 9+4 = 13$

$x_{1,2} = \frac{-3 \pm \sqrt{13}}{2} \begin{cases} x_1 = \frac{-3+\sqrt{13}}{2} \\ x_2 = \frac{-3-\sqrt{13}}{2} \end{cases}$

$f_3(x) = (x-1)\left(x - \frac{(-3+\sqrt{13})}{2}\right)\left(x - \frac{(-3-\sqrt{13})}{2}\right)$

d) $f_4(x) = 4x^4 - 12x^3+x^2+12x+4$

$f_4(2) = 0$

$4x^4-12x^3+x^2+12x+4 \mid x-2$

$-4x^3+x^2+12x+4 \quad\quad 4x^3-4x^2-7x-2$

$4x^3-8x^2$

$-7x^2+12x+4$

$7x^2-14x$

$-2x+4$

$2x+4$

//

$f_4(x) = (x-2)(4x^3-4x^2-7x-2)$

2 sol

$4x^3-4x^2-7x-2 \mid x-2$

$-4x^3+8x^2 \quad\quad 4x^2+4x+1$

$-4x^2-7x-2$

$-4x^2+8x$

$x-2$

$-x+2$

$f_4(x) = (x-2)(x-2)(4x^2+4x+1)$

$f_4(x) = (x-2)^2(2x+1)^2$

desc peste toate mult.

SEMINAR 4

Forma fundamentală de izomorfism pt inele

Fie R un inel, fie I un ideal al inelului
$\Rightarrow I$ este un subgrup (normal)
$\Rightarrow \left(\frac{R}{I}, +\right)$ grup factor $\quad \hat{r} = r + I$ un element $r \in R$

Definim $\widehat{x \cdot y} = \hat{x} \cdot \hat{y}$
$\left(\frac{R}{I}, +, \cdot\right)$ inel factor

Fie $(R_1, +, \cdot), (R_2, *, \circ)$ inele
$f: R_1 \to R_2$ un morfism de inele
dacă
$$\begin{cases} f(x+y) = f(x) * f(y) \\ f(x \cdot y) = f(x) \circ f(y) \\ f(1_{R_1}) = 1_{R_2} \end{cases} \quad \forall x, y \in R_1$$

TF1

Fie R_1, R_2 inele, $f: R_1 \to R_2$ morfism de inele
Atunci $\frac{R_1}{\ker f} \simeq \operatorname{Im} f$

(f surj : $\operatorname{Im} f = R_2$)
$\Leftrightarrow \frac{R_1}{\ker f} \simeq R_2$

② $\frac{\mathbb{Z}[x]}{n\mathbb{Z}[x]} \simeq \mathbb{Z}_n[x]$ isom. di anelli

Cost $f: \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ morfismo suriettivo di anelli con $\ker f = (n)$

$(n) = (n)\mathbb{Z}[x] = \{ n\,h(x) \mid h(x) \in \mathbb{Z}[x] \}$

$f(P) = \hat{P}$ $\quad \in \mathbb{Z}[x]$

scelgo coeff dei interi in resto della div per n

$P = a_m x^m + \dots + a_0 \in \mathbb{Z}[x] \to \hat{P} = \hat{a}_m x^m + \dots + \hat{a}_0$
$\quad a_i \in \mathbb{Z} \qquad\qquad \hat{a}_i \in \mathbb{Z}_n$

f morfismo di anelli

$f(P+Q) = \widehat{P+Q} = \hat{P} + \hat{Q} = f(P) + f(Q)$

$f(PQ) = \widehat{PQ} = \hat{P} \cdot \hat{Q} = f(\hat{P}) + f(\hat{Q})$

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

f surj $\forall \hat{P} \in \mathbb{Z}_n[x]$, $\exists$ ceva $\in \mathbb{Z}[x]$ tale che $f(\text{ceva}) = \hat{P}$
dov $f(P) = \hat{P} \Rightarrow f$ surj

$\ker f = (n)$

$\ker f = \{ P \in \mathbb{Z}[x] \mid f(P) = 0 \} = \{ P \in \mathbb{Z}[x] \mid \hat{P} = 0 \} = \{ P \in \mathbb{Z}[x] \mid$ coef tutti $P/n \}$

$\ker \subseteq (n)\mathbb{Z}[x]$ ①

$P = n(\dots)$

Se $P \in (n)\mathbb{Z}[x] \Rightarrow P = n\,h(x)$
$\quad h(x) \in \mathbb{Z}[x]$

$\to f(P) = \hat{P} = n \cdot h(x) = \hat{n} \cdot \widehat{h(x)} = 0$

$f(P) = 0 \Rightarrow P \in \ker f \Rightarrow (n) \subseteq \ker f$ ②

① + ② $\Rightarrow$
$\ker f = (n)$

TFI $\Rightarrow$ $\frac{\mathbb{Z}[x]}{n\mathbb{Z}[x]} \simeq \mathbb{Z}_n[x]$
"buf

Polinoamele Simetrica Fundamentale

$K[x_1, \ldots, x_n]$ inelul de pol în nedeterminate peste corpul K

$s_1 = x_1 + x_2 + \ldots + x_n$

$s_2 = x_1x_2 + x_1x_3 + \ldots = \sum_{i<j} x_ix_j$

$\vdots$

$s_k = \sum_{i_1 < \ldots < i_k} x_{i_1} x_{i_2} \ldots x_{i_k}$

$s_n = x_1x_2 \ldots x_n$

Teorema Fundamentale a ~~polinoamelor Simetrice~~

$\forall f \in K[x_1 \ldots x_n]$ polin. simetric se scrie în mod unic ca o expresie polinomială de pol simetrica fundamentale $f(x_1, \ldots x_n) = g(s_1 \ldots s_n)$ adică $\forall f \in K[x_1 \ldots x_n]$ $\exists! g$ a.î. $f(x_1, \ldots x_n)$

1) $f(x,y) = x^2+y^2 = (x+y)^2 - 2xy = s_1^2 - 2s_2$

$s_1 = x+y$

$s_2 = xy$

2) $f(x,y) = x^3 + 2xy^2 + 2x^2y + x + y + y^3 = f(y,x)$

$f(x,y) = x^3 + y^3 + 2xy(y+x) + x + y =$

$= (x+y)(x^2 - xy + y^2) + 2s_1s_2 + s_1$

$f(x,y) = s_1((x+y)^2 - 3xy) + 2s_1s_2 + s_2$

$= s_1(s_1^2 - 3s_2) + 2s_1s_2 + s_1$

$= s_1^3 - s_1s_2 + s_1$

3) $f(x,y,z) = x^3+y^3+z^3$

împart componentele omogene în funcție de grad

$T(f) = cx_1^{a_1}x_2^{a_2} \ldots x_n^{a_n} \rightsquigarrow c s_1^{a_1-a_2} s_2^{a_2-a_3} \ldots s_n^{a_n}$

$T(f) = x^3 \rightsquigarrow 1 \cdot s_1^{3-0} s_2^{0-0} s_3^{0} = s_1^3$

$x^3y^0z^0$

$\Rightarrow f(x,y,z) = s_1^3 - s_1^3 + x^3 + y^3 + z^3$

④ $\frac{\mathbb{R}[x]}{(x-a)} \simeq \mathbb{R}$
$a \in \mathbb{R}$

$(x-a)$ = ideal generat de polinomul $x-a$

$(x-a) = \{(x-a)h(x) \mid h(x) \in \mathbb{R}[x]\}$
$\| $
$(x-a)\mathbb{R}[x]$

Caut $f: \mathbb{R}[x] \to \mathbb{R}$ morfism surjectiv de inele cu $\ker f = (x-a)$

$f(P) = P(a) \in \mathbb{R}$
$P \in \mathbb{R}[x]$

Dem
f morfism de inele
$f(P+Q) = (P+Q)(a) = P(a)+Q(a) = f(P)+f(Q)$
$f(PQ) = (PQ)(a) = P(a)Q(a) = f(P)\cdot f(Q)$
$f(1) = 1(a) = 1$
f surj
$\forall b \in \mathbb{R}$ $\exists$ ceva $\in \mathbb{R}[x]$ a.î. $f(\text{ceva}) = b$
$f(b) = b(a) = b$
b polinom constant

$\ker f = (x-a)$
$\text{Im} f = \{P \in \mathbb{R}[x] \mid f(P) = 0\} = \{P \in \mathbb{R}[x] \mid P(a) = 0\}$
$\ker f = \{P \in \mathbb{R}[x] \mid x-a \mid P\} \subseteq (x-a)$ ①
se demonstrează
fie $P \in (x-a) \Rightarrow P = (x-a)h(x)$
$h(x) \in \mathbb{R}[x]$
$P(a) = (a-a)h(a) = 0 \Rightarrow f(P) = 0 \Rightarrow P \in \ker f$
$\Rightarrow (x-a) \in \ker f$ ②
① + ② $\Rightarrow \ker f = (x-a)$

TFI
$\Rightarrow \frac{\mathbb{R}[x]}{\ker f} \simeq$
$\frac{\mathbb{R}[x]}{(x-a)} \simeq \mathbb{R}$

③ $\frac{\mathbb{Z}[x]}{(x^2+1)} \simeq \mathbb{Z}[i]$ izo de inele

*

Caut $f: \mathbb{Z}[x] \to \mathbb{Z}[i]$ morfism surj de inele cu $\ker f = (x^2+1)$

$f(P) = \in \mathbb{Z}[x]$

$P = a_m x^m + \dots + a_0 \rightsquigarrow a_m i^m + \dots + a_1 i + a_0 \in \mathbb{Z}[i]$
$a_i \in \mathbb{Z}$

f morfism
f surj
$\forall\, a+bi \in \mathbb{Z}[i]$, f cunoscut in $\mathbb{Z}[x]$ al $A(\text{cunoscut}) = a+bi$.

$f(a+bx) = a+bi$
$\in \mathbb{Z}[x]$

$\ker f = (x^2+1)$

$\ker f = \{P \in \mathbb{Z}[x] \mid f(P) = 0\} = \{P \in \mathbb{Z}[x] \mid P(i) = 0\}$ ($P(-i) = 0$) $= \{P \in \mathbb{Z}[x]\}$

$= \{P \in \mathbb{Z}[x] \mid x^2+1 \mid P\} \subseteq (x^2+1)$ ①

Fie $P \in (x^2+1) \Rightarrow P = (x^2+1)h(x)$

$f(P) = P(i) = (i^2+1)h(i) = 0$
$\qquad\qquad\qquad\quad \| 0$

$\Rightarrow P \in \ker f \Rightarrow (x^2+1) \subseteq \ker f$ ②

① + ② $\Rightarrow \ker f = (x^2+1)$

TFI $\Rightarrow \frac{\mathbb{Z}[x]}{(x^2+1)} \simeq \operatorname{Im} f = \mathbb{Z}[i]$
(Im f)

Polinoame Simetrice

$f(x) = x^3 + 2x^2 + 5 \in \mathbb{Z}[x]$ pol simetric ($\forall$ pol cu 0 ca radacina e simetric)

$f(x,y) = x^2 - y^2 + x + y \in \mathbb{Z}[x,y]$

$f(y,x) = y^2 - x^2 + y + x$ Nu pol e simetric

$f(x,y) = x + y^2 + x + y = f(y,x)$ DA

$f(x,y,z) = x^3 + 2x^2 + 5 \in \mathbb{Z}[x,y,z]$ e simetric $\forall$

Seminar 5

$f(x,y,z) = (x-y)^2(x-z)^2(y-z)^2$

Scrieți f în fct. de pol. simetrice fundamentale S_1, S_2, S_3.

Atunci am găsit

$$\boxed{f = a S_1^2 S_2^2 + b S_1^3 S_3 + c S_2^3 + d S_1 S_2 S_3 + e S_3^2}$$

Pas I $T(f) = x^2 \cdot x^2 y^2 = x^4 y^2$ (în ordine lexicografică lui f)

$T(f) = x^4 y^2 z^0 \rightsquigarrow$

$x^{a_1} y^{a_2} z^{a_3} \rightsquigarrow \begin{matrix} a_1-a_2 & a_2-a_3 & a_3 \\ S_1 & S_2 & S_3 \end{matrix}$

$T(f) = S_1^{4-2} S_2^{2-0} S_3^0 = S_1^2 S_2^2$

Pas II Caut monoamele de același grad ca termenul dominant dar mai mici lexico-grafic.

$(4,2,0) \rightarrow S_1^2 \cdot S_2^2$

$(4,1,1) \rightarrow x^4 y z \rightsquigarrow S_1^{4-2} S_2^{1-1} S_3^1 = S_1^2 S_3$

$(4,0,2) \rightarrow S_1^4 y_2^{-2} S_3^2 \rightarrow$ NU

$(3,3,0) \rightarrow x^3 y^3 \rightarrow S_1^{3-3} S_2^{3-0} S_3^0 = S_2^3$

$(3,2,1) \rightarrow x^3 y^2 z^1 \Rightarrow S_1^{3-2} S_2^{2-1} S_3^1 = S_1^1 S_2 S_1$

$(2,2,2) \rightarrow x^2 y^2 z^2 \rightarrow S_1^{2-2} S_2^{2-2} S_3^2 = S_3^2$

$f(x,y,z) = a \cdot S_1^2 S_2^2 + b \cdot S_1^3 S_3 + c S_2^3 + d S_1 S_2 S_3 + e S_3^2$

$a, b, c, d = ?$

$a =$ coef. termenului dominant $=$ coef $T(f) = \boxed{1}$

x	y	z	S_1	S_2	S_3	$f(x,y,z)$
1	1	0	2	1	0	$f(1,1,0) = (1-1)^2 \cdot (1-0) \cdot (0-1)^2 = 0$

$S_2 = xy + yz + xz$

$S_3 = x \cdot y \cdot z$

$S_1 = x + y + z$

alegem convenabil

$z^2 \cdot 1 + c \cdot 1 = 0 \Rightarrow 4 + c = 0 \Rightarrow \boxed{c = -4}$

x	y	z	S_1	S_2	S_3	$f(x,y,z)$
-1	1	0	0	-1	0	$f(-1,1,0)$
-1	-1	2	0	-3	2	0

$x = 2$
$z = 2$
$z = 1$
$y = 0$

$(-4)(-3)^3 + e \cdot 2^2 = 0 \Rightarrow \boxed{e = -27}$

x	y	z	S_1	S_2	S_3	$f(x,y,z)$
1	1	1	3	3	1	0
1	1	-1	1	-1	-1	0

$8 + b \cdot 27 + 4 \cdot 27 + d \cdot 9 - 27 = 0$

$\boxed{27b + 9d = 54}$

$1 + b(c-1) + (-4)\cdot(-1) + d - 27 = 0$

$1 - b + 4 + d - 27 = 0$

$\boxed{-b + d = 22}$

$\begin{cases} -b + d = 22 \\ 27b + 9d = 54 \end{cases}$; $b = -4$, $d = 18$ $\Longrightarrow f(x,y,z) = S_1^2 S_2^2 - 4S_1^3 S_3 - 4S_2^3 + 18 S_1 S_2 S_3 - 27 S_3^2$

Pt. $n = 2$: $x_1 x_2$

$ax^2 + bx + c = 0$

$a = 0$, $a, b, c \in \mathbb{R}$

are rād distincte $\iff \Delta \neq 0$.

$\Delta = b^2 - 4ac$

$\boxed{S_1 = x_1 + x_2 = -\frac{b}{a} \quad / \text{ Viette}}$

$\boxed{S_2 = x_1 \cdot x_2 = \frac{c}{a}}$

$\Delta = b^2 - 4ac = a^2\left(\frac{b^2}{a^2} - \frac{4c}{a}\right) = a^2\left(S_1^2 - 4S_2\right)$

$S_1^2 - 4S_2 = (x_1 + x_2)^2 - 4(x_1 x_2) = (x_1 - x_2)^2$

$\Delta = a^2(x_1 - x_2)^2 \neq 0 \iff x_1 \neq x_2$

Pb:

Dat un polinom: $a_n x^n + \dots + a_1 x + a_0$, $a_n \neq 0$.

Det daca toate rād distincte

$\Delta = \prod (x_i - x_j)^2$, $i \neq j = g(S_1, \dots, S_n)$

$S_1 = \frac{-a_{n-1}}{a_n}$

$S_2 = \frac{a_{n-2}}{a_n}$

$S_3 = -\frac{a_{n-3}}{a_n}$

$\Delta \neq 0 \iff$ toate rād sunt distincte

② Fie $f(t) = \hat{2}t^3 - \hat{3}t^2 + \hat{4}t + \hat{1} \in \mathbb{Z}_{11}[t]$
Det. dacă f are rād distincte două câte două.

$S_1 = -(-\hat{5})(\hat{2})^{-1} = \hat{5}\cdot\hat{6} = \hat{30} = \hat{8}$

$S_2 = \hat{4}\cdot(\hat{2})^{-1} = \hat{4}\cdot\hat{6} = \hat{24} = \hat{2}$

$S_3 = (-\hat{1})\cdot(\hat{2})^{-1} = \hat{10}\cdot\hat{6} = \hat{60} = \hat{5}$

$\Delta = (x-y)^2(x-z)^2(y-z)^2 = a^2 S_2^2 - 4a^3 S_3 - 4a S_2^3 + 18 a^2 S_2 S_3 - 27 a^3$

$\Delta = 256 - \dots$

$\Delta \neq 0 \Rightarrow$ f(t) are toate rād dist

③ Fie x_1, x_2, x_3 rād pol $2x^3 + 5x + 6$.
constr. un pol. cu rād y_1, y_2, y_3 unde:

a) $y_i = x_i + 2$

b) $y_i = \frac{1}{x_i + 1}$

a) $S_1 y = y_1 + y_2 + y_3 = S_1 x + 6$

$S_1 x = 0$

$S_2 x = \frac{5}{2}$

$S_3 = -3$

$S_2 y = y_1y_2 + y_1y_3 + y_2y_3 = (x_1+2)(x_2+2) + (x_1+2) + (x_2+2)(x_3+2)$

$= x_1x_2 + 2x_2 + 4 + x_1x_3 + 2x_1 + 4 + x_2x_3 + 2x_3 + 2x_2 + 4$

$= S_2x + 12 + 4x_1 + 4x_2 + 4x_3 = 12 + S_2x + 4S_1 = 12 + \frac{5}{2} + 0 = \frac{19}{2}$

$S_{3y} = y_1 \cdot y_2 \cdot y_3 = (x_1+2)(x_2+2)(x_3+2)$

$= (x_1x_2 + 2x_1 + 2x_2 + 4)(x_3+2)$ ~~$x_1x_2x_3 + 2x_1x_3 + 2x_2x_3 + 8 = S_{3x}$~~

$= x_1x_2x_3 + 2x_1x_3 + 2x_2x_3 + 4x_3 + 2x_1x_2 + 4x_1 + 4x_2 + 8 =$

$= S_{3x} + 2S_{2x} + 4S_{1x} + 8$

$= -3 + 2 \cdot \frac{5}{2} + 4 \cdot 0 + 8 = 10$

$P(Y) = y^3 - S_{1y}y^2 + S_{2y}y - S_{3y} = y^3 - 6y^2 + \frac{29}{2}y - 10.$

b) $S_{1y} = y_1 + y_2 + y_3 = \frac{1}{x_1+1} + \frac{1}{x_2+1} + \frac{1}{x_3+1} =$

$= \frac{(x_2+1)(x_3+1) + (x_1+1)(x_3+1) + (x_1+1)(x_2+1)}{(x_1+1)(x_2+1)(x_3+1)}$

$= \frac{x_2x_3 + x_2 + x_3 + 1 + x_1x_3 + x_1 + x_3 + 1 + x_1x_2 + x_1 + x_2 + 1}{(x_1+1)(x_2+1)(x_3+1)}$

$= \frac{S_{2x} + 2S_{1x} + 3}{(x_1+1)(x_2+1)(x_3+1)}$

(4) Calculate $x^5y^5z^5$, unde x, y, z sunt rad ec. $t^3 + t + 1 = 0$.

x, y, z sunt rad ale ec.: $\begin{cases} x^3+x+1=0 \mid x^2 \\ y^3+y+1=0 \mid y^2 \\ z^3+z+1=0 \mid z^2 \end{cases}$ (+)

$\Delta_1 = 0$
$\Delta_2 = 1$
$\Delta_3 = -1$

$x^3+y^3+z^3 = -(x+y+z) - 3 \Rightarrow x^3+y^3+z^3 = -3$

(5) $\begin{cases} x^5 + x^3 + x^2 = 0 \\ y^5 + y^3 + y^2 = 0 \\ z^5 + y^3 + y^2 = 0 \end{cases}$

$x^5+y^5+z^5 = -(\underbrace{x^3+y^3+z^3}_{-3}) - (\underbrace{x^2+y^2+z^2}_{S_1^2 - 2S_2 = -2}) = +3+2 = 5.$

(7) Calc. $x_1^{2018} + x_2^{2018} + x_3^{2018} \pmod{11}$, unde x_1, x_2, x_3 sunt rad ec $x^3 + 2x + 3 = 0$.

$\begin{cases} x_1^3 + 2x_1 + 3 = 0 \\ x_2^3 + 2x_2 + 3 = 0 \\ x_3^3 + 2x_3 + 3 = 0 \end{cases}$ (+)

$x_1^3 + x_2^3 + x_3^3 = \underbrace{-2(x_1+x_2+x_3)}_{\Delta_1} - 9$

$$\begin{cases} x_1^3 + 2x_1 + 3 = 0 \mid \cdot x_1 \\ x_2^3 + 2x_2 + 3 = 0 \mid \cdot x_2 \\ x_3^3 + 2x_3 + 3 = 0 \mid \cdot x_3 \end{cases} \Rightarrow x_1^4 + x_2^4 + x_3^4 = -2\underbrace{(x_1^2 + x_2^2 + x_3^2)}_{0^2 - 2\cdot 0} \underbrace{-3 \cdot 0}_{=0}$$

$$= 8.$$

La puterea 5:

$$x_1^5 + x_2^5 + x_3^5 - 2(\underbrace{x_1^3 + x_2^3 + x_3^3}_{-9}) - 3(\underbrace{0^2 - 2\cdot 0}_{-4}) = 18 + 12 = 30$$

La puterea 6:

$$x_1^6 + x_2^6 + x_3^6 = -2(x_1^4 + x_2^4 + x_3^4) - 3(\underbrace{x_1^3 + x_2^3 + x_3^3}_{=9}) = -16 + 27 = 11 \equiv 0 \pmod{11}$$

$2018 : 6 = 336$ rest 2

$$x_1^{2018} + x_2^{2018} + x_3^{2018} = -2(x_1^{2016} + x_2^{2016} + x_3^{2016}) - 3(x_1^{2015} + x_2^{2015} + x_3^{2015})$$

$$x_1^7 + x_2^7 + x_3^7 = -2(x_1^5 + x_2^5 + x_3^5) - 3(x_1^4 + x_2^4 + x_3^4)$$

$$= -60 - 24 = -84 \equiv -4 \pmod{11}$$

=

Seminar 7

1) K corp finit $\Rightarrow |K| = p^n$, p-prim, $n \in \mathbb{N}^*$
2) $\forall$ p prim, $\forall$ $n \in \mathbb{N}^* \Rightarrow \exists$ K corp a.î. $|K| = p^n$
3) K corp finit $\Rightarrow$ comutativ
4) K, L corpuri finite, $|K| = |L| \Rightarrow K \simeq L$

Din curs 13:
a) Calcul inversului
1) $\frac{\mathbb{Z}[i]}{(5)}$ este corp cu 25 elemente

Găsiți inversul lui $\overline{7+2i}$

În general $\frac{\mathbb{Z}[i]}{a+bi} \simeq \mathbb{Z}_{|a^2+b^2|}$, $a, b \in \mathbb{Z}$

Ex: $\left|\frac{\mathbb{Z}[i]}{(2+5i)}\right| = 29$

Caut $a+bi \in \mathbb{Z}[i]$ a.î. $(7+2i)(a+bi) = \bar{1} \pmod 5$

$7a + 7bi + 2ai - 2b - 1 \equiv \bar{0} \pmod 5$

$\Rightarrow 7a - 2b - 1 + (7b + 2a)i \equiv \bar{5}(m+ni)$ — multiplu de 5 din $\mathbb{Z}[i]$

$= 5m + 5ni$

$$\begin{cases} 7a - 2b - 1 = 5m \\ 7b + 2a = 5n \end{cases} \overset{\mathbb{Z}[i]}{\Rightarrow} \begin{cases} \hat{2}a - \hat{2}b - 1 = \hat{0} \\ \hat{2}b + \hat{2}a = \hat{0} \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} 4a = \hat{1} \pmod 5 \\ b = -a \pmod 5 \end{cases} \Leftrightarrow \begin{cases} a = 4^{-1} \pmod 5 \Rightarrow a = \bar{4} \\ b = \bar{1} \end{cases}$$

Deci inversul lui $\overline{7+2i}$ este $\overline{4+i}$

2) Câte elemente $x \in \mathbb{Z}_{561}$ au prop că $x^2 = x$?
$\Leftrightarrow |\mathcal{I}dem(\mathbb{Z}_{561})| = ?$

$561 = 3 \cdot 17 \cdot 11$

$\mathbb{Z}_{561} \cong \mathbb{Z}_3 \times \mathbb{Z}_{17} \times \mathbb{Z}_{11}$ (Lema chineză a resturilor)

$\mathbb{Z}_n$, cu $n = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \Rightarrow \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_n^{\alpha_n}}$

$|\mathcal{I}dem(561)| \leftrightarrow |\mathcal{I}dem(\mathbb{Z}_3)| \cdot |\mathcal{I}dem(\mathbb{Z}_{17})| \; \mathcal{I}dem(\mathbb{Z}_{11})|$

$(\mathcal{I}dem\, \mathbb{Z}_p)$, p - prim $\Leftrightarrow$ a găsi idempotenții din $(\mathbb{Z}_p, +, \cdot)$ e totuna de a rezolva ecuația $x^2 = \bar{x}$ în $\mathbb{Z}_p$

$x^2 = x$ în $\mathbb{Z}_p \Leftrightarrow x^2 - x \equiv 0 \pmod p \Rightarrow$

$\Rightarrow p \mid x^2 - x \Rightarrow p \mid x(x-1) \Rightarrow p \mid x$ sau $p \mid x-1$
(p-prim)

$p \mid \bar{x} \Rightarrow \bar{x} = \bar{0}$

$p \mid \bar{x-1} \Rightarrow \bar{x} = \bar{1}$

Deci $\mathcal{I}dem(\mathbb{Z}_p) = \{\bar{0}, \bar{1}\}$, p = prim

$\mathcal{I}dem(\mathbb{Z}_{p^k}) = \{\bar{0}, \bar{1}\}$, p-prim, $k \geq 1$

$\Rightarrow |\mathcal{I}dem\, \mathbb{Z}_{p^k}| = 2$, p = # prim, $k \geq 1$

$|\mathcal{I}dem(\mathbb{Z}_{561})| = 2 \cdot 2 \cdot 2 = 2^3 = 8$

Mai general $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k} \Rightarrow |\mathcal{I}dem(\mathbb{Z}_n)| = 2^k$

③ TFI:

$$\frac{\mathbb{Z}[i]}{(2-i)} \simeq \mathbb{Z}_5$$

Caut $f: \mathbb{Z}[i] \to \mathbb{Z}_5$ un morfism surjectiv de inele cu nucleul

$f(a+bi) = ? \in \mathbb{Z}_5$

$f(a+bi) = f(a) + f(b) \cdot f(i)$

f morfism

$f(a) = f(\underbrace{1+\dots+1}_{a \text{ ori}}) = \underbrace{f(1)+\dots f(1)}_{a \text{ ori}} = a f(1) = \bar{a}$, $\bar{a} \in \mathbb{Z}_5$ ($f(1) = 1$)

$f(a+bi) = \hat{a} + \hat{b} \cdot f(i)$

$\ker f \supset (2-i) \Rightarrow (2-i) \Rightarrow f(2-i) = 0$

f-morfism $\Downarrow$

$f(2) - f(i) = 0 \Rightarrow \bar{2} = f(i)$

Deci $f(a+bi) = \hat{a} + \hat{b}\,\hat{2} = \overline{a+2b}$

~~$f(a+bi)(c+di) = f(ac + adi + bdi +$~~

$f(a+bi)(c+di) = f(ac - bd + (ad+bc)i) =$

$= \overline{ac - bd + 2(ad+bc)}$ (*)

$f(a+bi) \cdot f(c+di) = \overline{(a+2b)(c+2d)} =$

$= \overline{ac + 4bd + 2(ad+bc)} = *$

$4 = -1 \pmod 5$

Curs 13:

④ $f(x) = x^4 + 1 \in \mathbb{Z}_{89}[X]$

Descompunere în factori ireductibili

Idee: $(x^2)^2 + 1 \Rightarrow y^2 + 1$

Vreau să rezolv ec $y^2 + \hat{1} = \hat{0}$ în $\mathbb{Z}_{89}$

$y^2 + 1 = 0$

$\Delta = -4 \equiv 85 \pmod{89}$ Adun 89 până găsesc număr pătrat perfect

$\Delta = 85 + 89 \cdot m = 441$ p. perfect

$\sqrt{\Delta} = 21$

$245 = 90 = \hat{1} \pmod{89}$

$$y_1 = \frac{0 - 21}{2} = -\frac{21}{2} = -21 \cdot 2^{-1} = -21 \cdot 45 = -3060 = 34 \pmod{89}$$

$$y_2 = 21 \cdot 2^{-1} = 21 \cdot 45 \equiv 55 \pmod{89}$$

$\Rightarrow x^2 \in \{34, 55\}$

$x^2 \equiv 55 \pmod{89} \equiv 144 \pmod{89} \equiv (\pm 12)^2$

$55 + 89 = 144 = 12^2 \Rightarrow x = \pm 12$

$x^2 \equiv 34 \pmod{89} \equiv 1369 \equiv (\pm 37)^2$

$f(x) = (X - \hat{12})(X + \hat{12})(X - \hat{37})(X + \hat{37})$ - sunt descompunere ireductibilă în $\mathbb{Z}_{89}[X]$

⑤ $\frac{\mathbb{R}[X]}{(X^2-17X)} \simeq \mathbb{R}\times\mathbb{R}$

Vreau $f: \mathbb{R}[X] \to \mathbb{R}\times\mathbb{R}$ să fie un morfism surjectiv de inele cu nucleul ~~generat de~~ $\ker f = (X^2-17X)$

$X^2-17X = X(X-17)$

$f(P) = (P(0), P(17))$ - morfismul

↑ P polinom $\in \mathbb{R}[X]$

! Cramer, inverse de matrici

⑥ $(X^n-2)^n - X - 2 = [(X^n-2+X-X)^n] - [X] - 2$

$= [(X^n-X-2)+X]^n - X - 2$

$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$ ✗

$= \sum C_n^k (X^n-X-2)^{n-k} X^k - X - 2 =$

$= (X^n-X-2)^n + \sum_{k=1}^{n-1} C_n^k (X^2-X-2)^{n-k} X^k + (X^n-X-2)$

$= (X^n-X-2)\cdot Q[X]$ $\Rightarrow P$ este reductibil în $\mathbb{Z}[X]$
$\in \mathbb{Z}[X]$