Seminarul 3

Wednesday, March 3, 2021 8:53 AM

Ideale maximale. Inele locale (inelele sunt comutative)

Def $I \trianglelefteq R$, $I \neq R$ e maximal dacă $\forall J \trianglelefteq R$, $I \subset J \subset R$ $\Rightarrow J = I$ sau $J = R$

Curs $I \trianglelefteq R$ maximal $\iff R/I$ este corp

2.1. Fie R inel, $I \trianglelefteq R$.

I e maximal $\iff \forall a \notin I$, $I + (a) = R$.

Dem „$\Rightarrow$” $J = I + (a)$ în definiția maximalității:

$$I \subset I+(a) \subset R \xRightarrow{def} I+(a) = I \leftarrow \text{dar } a \notin I \text{ (contradicție)}$$

sau

$$\underline{I+(a) = R}$$

„$\Leftarrow$” Presupunem că I nu e maximal $\Rightarrow \exists J \trianglelefteq R$, $I \subsetneq J \subsetneq R$

$I \subsetneq J \Rightarrow \exists a \in J \setminus I$

$$\underbrace{I \subsetneq I+(a)}_{\xRightarrow{ip} I+(a) = R} \subset J \not\Rightarrow J = R \text{ (contradicție)}$$

2.2. a) Demonstrați că Teorema de corespondență a idealelor este compatibilă cu idealele maximale:

Th: $f: R \to S$ morfism surjectiv de inele

Atunci $\{I \trianglelefteq R \mid I \supset \operatorname{Ker} f\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \{J \trianglelefteq S\}$,

$$\varphi(I) = f(I), \quad \psi(J) = f^{-1}(J)$$

se restrânge la ideale maximale:

se restrânge la ideale maximale :

$$\{I \trianglelefteq R \mid I \supset \mathrm{Ker} f, I \text{ maximal}\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \{J \trianglelefteq S \mid J \text{ maximal}\}$$

Dem Corespondența păstrează relația de ordine!

(sau: $f(I)$ maximal dacă $I \trianglelefteq R$ maximal ← Exc!
$f^{-1}(J)$ ———— $J \trianglelefteq S$ ——)

b) Redemonstrați că I maximal $\Leftrightarrow$ R/I e corp.

Fie $p : R \to R/I$, $p(x) = \hat{x}$ (mod I)
proiecția canonică pe inelul factor.

TR de corespondență (pt ideale maximale):

$$A = \{I' \trianglelefteq R \mid I' \supset I, I' \text{ maximal}\} \overset{1:1}{\longleftrightarrow} \underbrace{\{J \trianglelefteq R/I \mid J \text{ maximal}\}}_{B}$$

"$\Rightarrow$" Dc I maximal $\xRightarrow{\text{def idealului maximal}}$ $A = \{I\} \overset{1:1}{\longleftrightarrow} B = \{\underset{p(I)}{(0)} \trianglelefteq R/I\}$

$\Updownarrow$!

R/I e corp

"$\Leftarrow$" La fel : R/I e corp $\Rightarrow$ $B = \{(0) \trianglelefteq R/I\} \overset{1:1}{\longleftrightarrow} A = \{I\} \Rightarrow$ I e maximal

---

2.3. Idealele maximale ale lui $\mathbb{Z}$ și $\mathbb{Z}_n$?

Dem • $\mathbb{Z}$:

Var 1 Fie $I \trianglelefteq \mathbb{Z} \Rightarrow I = n\mathbb{Z}$ pt un $n \in \mathbb{N}$.

I maximal $\Leftrightarrow$ $\mathbb{Z}/I$ e corp $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ e corp $\Leftrightarrow$

I maximal $\iff \mathbb{Z}/I$ e corp $\iff \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ e corp $\iff$ n e prim.

$\Rightarrow \mathcal{M} = \{p\mathbb{Z} \mid p \text{ prim}\}$ mulțimea idealelor maximale ale lui $\mathbb{Z}$.

<u>Var 2.</u> Fie $I = n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

$$n\mathbb{Z} \text{ maximal} \overset{def}{\iff} \left(\forall\, J \trianglelefteq \mathbb{Z},\ n\mathbb{Z} \subset J \subset \mathbb{Z} \Rightarrow J = n\mathbb{Z} \text{ sau } J = \mathbb{Z}\right)$$

$$\iff \left(\forall\, m\mathbb{Z} \trianglelefteq \mathbb{Z},\ \underline{n\mathbb{Z} \subset m\mathbb{Z}} \subset \mathbb{Z} \Rightarrow m\mathbb{Z} = n\mathbb{Z} \text{ sau } m\mathbb{Z} = \mathbb{Z}\right)$$

$$\iff \left(\forall\, m \in \mathbb{Z},\ m \mid n \Rightarrow m = \pm n \text{ sau } m = \pm 1\right)$$

$\iff n$ e prim.

- $\mathbb{Z}_n$:

<u>Var 1</u> Th de corespondență a idealelor:

$$\{I \trianglelefteq \mathbb{Z} \mid I \supset n\mathbb{Z},\ I \text{ maximal}\} \xleftrightarrow{1:1} \{J \trianglelefteq \mathbb{Z}/n\mathbb{Z} \mid J \text{ maximal}\}$$

Mai clar:

din principala a TCI:

$$\{p\mathbb{Z} \trianglelefteq \mathbb{Z} \mid p \mid n,\ p \text{ prim}\} \xleftrightarrow{1:1} \underbrace{\left\{ \overset{p\mathbb{Z}_n}{\overset{\parallel}{p\mathbb{Z}/n\mathbb{Z}}} \;\middle|\; p \mid n,\ p \text{ prim}\right\}}_{\text{mulțimea idealelor maximale ale lui } \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.}$$

<u>Var 2</u> Fie $I \trianglelefteq \mathbb{Z}_n \Rightarrow I = m\mathbb{Z}_n$ pt un $m \mid n$

$$= {}^{m\mathbb{Z}}/_{n\mathbb{Z}}, \quad m \mid n.$$

$I = m\mathbb{Z}_n$ e maximal $\iff \mathbb{Z}_n / m\mathbb{Z}_n$ e corp

$$\iff \frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \text{ e corp} \iff \mathbb{Z}/m\mathbb{Z} \text{ e corp} \iff m \text{ prim.}$$

Th I izo $\simeq \mathbb{Z}/m\mathbb{Z}$ (o demonstrăm azi sau data viitoare)

2.4. Când este $\mathbb{Z}_n$ <u>inel local</u>?

inel cu un singur ideal maximal

<u>Obs</u> Orice corp e inel local ((0) e unicul ideal maximal).

Idealele maximale ale lui $\mathbb{Z}_n = \{p\mathbb{Z}_n \mid p \text{ prim}, p \mid n\}$

$\Rightarrow |\ \ | = 1 \iff n = p^k$ pt un p prim și un $k \geq 1$.

Deci $\mathbb{Z}_{p^k}$ sunt inele locale. Dintre ele, corpuri sunt $\mathbb{Z}_p$.

2.5. a) Fie $R_1, R_2, \dots R_n$ inele. Care sunt idealele maximale ale lui $R = R_1 \times R_2 \times \dots \times R_n$?

<u>Dem</u> Reamintire: idealele lui R sunt de forma
$$\boxed{I = I_1 \times I_2 \times \dots \times I_n, \quad I_j \trianglelefteq R_j.}$$

Var 1

<u>Obs</u> Dacă $\underline{m}_j \trianglelefteq I_j$ maximal

$\Rightarrow \underline{m} = R_1 \times R_2 \times \dots \times R_{j-1} \times \underline{m}_j \times R_{j+1} \times \dots \times R_n$ este

$\Rightarrow \underline{m} = R_1 \times R_2 \times \dots \times R_{j-1} \times m_j \times R_{j+1} \times \dots \times R_n$ este ideal maximal.

<u>Explicație</u> Dacă $\mathcal{J} \supset R_1 \times R_2 \times \dots \times R_{j-1} \times m_j \times R_{j+1} \times \dots \times R_n$

$\boxed{\mathcal{J} \trianglelefteq R}$

$\Rightarrow \mathcal{J} = \mathcal{J}_1 \times \mathcal{J}_2 \times \dots \times \mathcal{J}_n$ cu $\mathcal{J}_\ell \trianglelefteq R_\ell$.

$\Rightarrow \mathcal{J}_1 \supset R_1,\ \mathcal{J}_2 \supset R_2, \dots \mathcal{J}_{j-1} \supset R_{j-1},\ \mathcal{J}_j \supset m_j,\ \mathcal{J}_{j+1} \supset R_{j+1} \dots \mathcal{J}_n \supset R_n$

$\Rightarrow \mathcal{J}_\ell = R_\ell,\ \forall \ell \neq j$

$\mathcal{J}_j \supset m_j \xRightarrow{m_j \text{ maximal}}$ $\mathcal{J}_j = R_j \Rightarrow \mathcal{J} = R$ sau $\mathcal{J}_j = m_j \Rightarrow \mathcal{J} = \underline{m}$

<u>Exc</u> Acestea sunt <u>singurele</u> ideale maximale.

<u>Var 2</u> Fie $I = I_1 \times I_2 \times \dots \times I_n \trianglelefteq R = R_1 \times \dots \times R_n$.

I maximal $\Leftrightarrow R/I$ e corp

$\Leftrightarrow \dfrac{R_1 \times R_2 \times \dots \times R_n}{I_1 \times I_2 \times \dots \times I_n}$ e corp

$\wr\wr$! Exc

$R_1/I_1 \times R_2/I_2 \times \dots \times R_n/I_n$ e corp

$\Leftrightarrow$ Toate inelele, în afară de <u>unul</u>, sunt (0) și acela e corp

$\Rightarrow I_1 = I_n$ ai

și acesta e corp

$\exists\, j = \overline{1,n}$ aî

$\Leftrightarrow$ Toate $I_\ell = R_\ell$ pt $\ell \neq j$ și R_j / I_j e corp

$\Leftrightarrow \exists\, j = \overline{1,n}$ aî $I_\ell = R_\ell$ pt $\ell \neq j$ și $I_j \trianglelefteq R_j$ e maximal.

b) Idealele maximale ale lui $\mathbb{Z} \times \mathbb{R} \times \mathbb{Z}_8$?

$\mathbb{Z}$	$\mathbb{R}$	$\mathbb{Z}_8$
$\{p\mathbb{Z}, p \text{ prim}\}$	$\{(0)\}$ (e corp)	$\{2\mathbb{Z}_8\}$ $8 = 2^3$

$$\Rightarrow \mathcal{M} = \{\mathbb{Z} \times (0) \times \mathbb{Z}_8\} \cup \{p\mathbb{Z} \times \mathbb{R} \times \mathbb{Z}_8 \mid p \text{ prim}\} \cup \{\mathbb{Z} \times \mathbb{R} \times 2\mathbb{Z}_8\}$$

idealele maximale ale lui $\mathbb{Z} \times \mathbb{R} \times \mathbb{Z}_8$.

<u>Exc 2.6.</u> R inel comutativ. U.A.S.E.:

(i) R inel local

(ii) $\forall a, b \in R$, $a + b \in U(R) \Rightarrow a \in U(R)$ sau $b \in U(R)$

(iii) $R \setminus U(R)$ e ideal.

<u>Dem</u> (iii) $\Rightarrow$ (i) $\forall I \trianglelefteq R$, $I \neq R \Longrightarrow I \subset R \setminus U(R)$

Dem (ii) $\Rightarrow$ (i) $\forall I \trianglelefteq R,\ I \neq R \Longrightarrow \left(I \subset R \setminus U(R)\right)$

Dacă un ideal conține elemente inversabile, este întreg inelul

$R \setminus U(R)$ ideal $\Longrightarrow$ e singurul ideal maximal.

($a \notin U(R)$)

(ii) $\Rightarrow$ (iii) Obs (ii) $\Leftrightarrow$ $\left(\forall a, b \in R,\ a \in R\setminus U(R) \text{ și } b \in R \setminus U(R) \Rightarrow a+b \in R\setminus U(R)\right)$

$\Leftrightarrow$ $R\setminus U(R)$ e închis la adunare.

Vrem $R \setminus U(R)$ ideal:

- parte stabilă la adunare ✓ (ii)
- $\forall r \in R,\ \forall x \in R\setminus U(R) \Rightarrow rx \in R \setminus U(R)$

Altfel, $\exists\ a \in R$ a.î. $a(rx) = 1$

$\Updownarrow$

$(ar)x = 1$ ↯

$I \trianglelefteq R$ dacă

1) $(I,+)$ subgrup $\Longrightarrow$	1') $\forall a,b \in I,\ a+b \in I$
2) $\forall r \in R,\ \forall x \in I,\ rx \in I$	2) $\forall r \in R,\ \forall x \in I,\ rx \in I$

2): $b \in I \Rightarrow (-1)\cdot b = -b \in I$

1) $\Rightarrow$ 1') și $\left(1') \,\&\, 2)\right) \Longrightarrow \left(1) \,\&\, 2)\right)$

(i) $\Rightarrow$ (ii) Lema lui Krull Orice ideal $\neq R$ e conținut într-un

---

(i) ⇒ (ii) Lema lui Krull: Orice ideal $\neq R$ e conținut într-un ideal maximal.

Pp. că R e inel local, fie $\underline{m}$ idealul maximal.

Fie $a, b \in R$ a.î. $a+b \in U(R)$. Pp. că $a \notin U(R)$ și $b \notin U(R)$.

$(a) \neq R \overset{\text{Krull}}{\Longrightarrow} \exists$ un ideal maximal $\supset (a)$

De fapt, $\boxed{(a) \subset \underline{m}}$

La fel, $\boxed{(b) \subset \underline{m}}$ $\Rightarrow a, b \in \underline{m} \Rightarrow a+b \in \underline{m}$

$\Rightarrow a+b \notin U(R)$

&

$a+b \in U(R)$

De reținut: Dacă R e inel local, idealul său maximal este $R \setminus U(R)$.

Invers, dacă $R \setminus U(R)$ e ideal, R e inel local și $R \setminus U(R)$ e idealul său maximal.

2.7. Dem. că singurele elemente idempotente într-un inel local sunt 0 și 1.

Def. $a \in R$ e idempotent dacă $a^2 = a$

Dem. Pp. că $a \in R$ cu $a^2 = a$.

$$\boxed{a(a-1) = 0}$$

Obs 2.6 $\Rightarrow R\setminus U(R)$ ideal $\quad (*)$

Pp că $a \neq 0$ și $a \neq 1 \Rightarrow a,\ a-1$ sunt divizori ai lui zero

$\Rightarrow$ neinversabile $\Rightarrow \underbrace{a,\ a-1 \in R\setminus U(R)}_{\overset{(*)}{\Rightarrow}\ 1 \in R\setminus U(R)}$ ↯

2.8. Fie p un număr prim și

$$A = A_p = \left\{ \frac{a}{b} \;\middle|\; p \nmid b \right\}. \qquad \frac{19}{2} = \frac{57}{6} \in A_3$$

Demonstrați că A e inel local.

Dem • A e inel, pt că e subinel al lui $\mathbb{Q}$

- de exemplu, $\frac{a}{b}, \frac{c}{d} \in A_p$ cu $p \nmid b,\ p \nmid d$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in A_p \text{ pt că } p \nmid bd.$$

• Care este $A \setminus U(A)$?

Fie $\frac{a}{b} \in A$, $p \nmid b$, $a \neq 0$.

nu poate fi simplificată fracția prin p

$$\frac{a}{b} \in U(A) \Leftrightarrow \frac{b}{a} \in A \Leftrightarrow p \nmid a$$

pt că $\frac{b}{a}$ este inversul în $\mathbb{Q}$

De ex, $\frac{57}{6} \in A_3$ e inversabil, $\left(\frac{19}{2}\right)^{-1} = \frac{2}{19}$, $3 \nmid 19$!

$\frac{57}{6} = \frac{19}{2}$

$= p \cdot A = (p)$

Deci $A \setminus U(A) = \left\{ \frac{a}{b} \;\middle|\; p \nmid b,\ p \mid a \right\}$ ideal ...

• Vrem $A \setminus U(A) = \{ \frac{a}{b} \mid p \nmid b, p \mid a \}$ ideal, caz în care A este local și $A \setminus U(A)$ este idealul maximal.

Din exc 2.6. : e suficient <u>să fie parte stabilă la adunare</u>:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \in A \setminus U(A)$$

$p \nmid b_1$, $p \nmid b_2$ a.î. că $p \mid a_1 b_2 + a_2 b_1$

$p \mid a_1$, $p \mid a_2$

<u>Denumire</u> A_p s.n. <u>localizatul</u> lui $\mathbb{Z}$ în (p).

<u>Corpul de fracții al unui domeniu</u>

3.1. Fie F corp comutativ. Atunci $Q(F) \simeq F$ canonic.

<u>Recap</u> D domeniu.

$\forall a, b \in D$, $b \neq 0$, $(a, b) \sim (c, d) \Leftrightarrow ad - bc = 0$
$c, d \in D$, $d \neq 0$

Clasa de echivalență a lui (a, b) se notează $\frac{a}{b}$.

$$\frac{a}{b} = \frac{-a}{-b} = \frac{2a}{2b} = \dots$$

$Q(D) = \{ \frac{a}{b} \mid a, b \in D, b \neq 0 \}$ este corp. În plus,

$Q(D) = \left\{ \frac{a}{b} \;\middle|\; a, b \in D,\ b \neq 0 \right\}$ este corp. În plus,

$\exists\, \varphi : D \hookrightarrow Q(D)$ incluziune canonică

$\varphi(a) = \frac{a}{1}$.

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ $\neq 0$ de $b, d \neq 0$

Def $Q(D)$ s.n. corpul de fracții al domeniului D.

Prop (Proprietatea de universalitate a corpului de fracții)

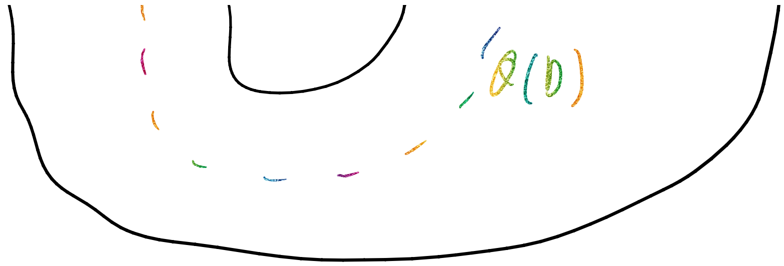
Fie D domeniu, și $f : D \to K$ morfism injectiv de inele.
K corp

$$\begin{tikzcd} D \arrow[rr, "f"] \arrow[dr, hook, "\varphi"'] & \arrow[d, phantom, "\circlearrowleft"] & K \\ & Q(D) \arrow[ur, dotted, "\bar f"'] & \end{tikzcd}$$

Atunci $\exists!\, \bar f : Q(D) \to K$ morfism de corpuri (deci injectiv) a.î. diagrama e comutativă, adică

$$f = \bar f \circ \varphi,$$

adică $f(a) = \bar f\left(\frac{a}{1}\right), \forall a \in D$.



<u>Idem</u> Cum definim $\bar{f}$?

$$\bar{f}\left(\frac{a}{b}\right) = f(a)\big(\underbrace{f(b)}_{\neq 0}\big)^{-1}, \quad \forall a,b \in D,\ b \neq 0.$$

<u>Exc</u> Faceți verificările!

Proprietatea de mai jos poate fi privită ca o <u>definiție</u> a corpului de fracții:

<u>Def</u> (Proprietatea de universalitate a corpului de fracții)

Fie D domeniu. Un corp Q împreună cu o aplicație injectivă $\varphi: D \to Q$ care respectă:

$\forall K$ corp, $\forall f: D \to K$ injectivă, $\exists\, \bar{f}: Q \to K$

a.î. $\bar{f} \circ \varphi = f$

$$\begin{tikzcd} D \arrow[r, "f"] \arrow[d, hook, "\varphi"'] & K \\ Q \arrow[ur, dashed, "\exists ?\ \bar{f}"'] & \end{tikzcd}$$

Sn <u>corpul de fracții</u> al lui D.

3.1. F corp $\Rightarrow Q(F) \simeq F$ canonic.

Prop de universalitate. Alegem, pe post de $D \xrightarrow{f} K$, $F \xrightarrow{id} F$

$$\begin{tikzcd}
F \arrow[r, "id"] \arrow[dr, hook, "\varphi"'] & F \\
& Q(F) \arrow[u, dashed, "\overline{id}"']
\end{tikzcd}$$

$\exists!\ \overline{id} : Q(F) \to F$ morfism de corpuri a.î. $\overline{id} \circ \varphi = id$

i.e. $\overline{id}\left(\frac{a}{1}\right) = id(a) = a$.

Vrem $\overline{id}$ surjectivă : $\overline{id} \circ \varphi = id \Leftarrow$ surjectivă

$\Rightarrow \overline{id}$ surjectivă.

3.2. $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$

$\mathbb{Q}[i] = \{a+bi \mid a, b \in \mathbb{Q}\}$

a) Arătați că sunt inele și că $\mathbb{Q}[i]$ e corp.

b) $Q(\mathbb{Z}[i]) \simeq \mathbb{Q}[i]$ (canonic).

Idee a) $\mathbb{Z}[i]$, $\mathbb{Q}[i]$ sunt subinele în $\mathbb{C}$! (Verificați!)

În plus, dacă $a+bi \in \mathbb{Q}[i]$ cu $a^2+b^2 \neq 0$.

În $\mathbb{C}$, $\overset{a-bi}{\frac{1}{a+bi}} = \frac{a}{a^2+b^2} + \left(-\frac{b}{a^2+b^2}\right) i$, $\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \in \mathbb{Q}$

În $\mathbb{C}$, $\frac{1}{a+bi} = \underbrace{\frac{a}{a^2+b^2} + \left(-\frac{b}{a^2+b^2}\right)i}_{\in \mathbb{Q}[i]}$, $\underbrace{\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}}\in \mathbb{Q}$

$a-bi$

Obs. Elem. inversabile din $\mathbb{Z}[i]$ sunt cele pt care $a^2+b^2 = \pm 1$

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

b) Idee: folosim din nou proprietatea de universalitate:

$$\begin{tikzcd} \mathbb{Z}[i] \arrow[r, "incl"] \arrow[d, bend right, "\varphi"'] & \mathbb{Q}[i] \\ \mathbb{Q}(\mathbb{Z}[i]) \arrow[ur, dashed, "\overline{incl}"'] & \end{tikzcd}$$

$incl(a+bi) = a+bi \in \mathbb{Q}[i]$

$\exists!\ \overline{incl} : \mathbb{Q}(\mathbb{Z}[i]) \longrightarrow \mathbb{Q}[i]$ a.î. $\overline{incl}\left(\frac{a+bi}{1}\right) = a+bi$.

Mai mult, $\overline{incl}\left(\underbrace{\frac{a+bi}{c+di}}_{\text{clasa de echivalență de perechi}}\right) = \underbrace{(a+bi)\cdot(c+di)^{-1}}_{\text{în } \mathbb{Q}[i]!} = \underbrace{\frac{a+bi}{c+di}}_{\text{fracție propriu-zisă în } \mathbb{C}}$.

Pt. ... $\overline{incl}$ surjectivă: Fie $\frac{m}{\ } + \frac{m'}{\ } i \in \mathbb{Q}[i]$

Rămâne ca $\overline{\text{incl}}$ surjectivă: Fie $\frac{m}{n} + \frac{m'}{n'} i \in \mathbb{Q}[i]$.

$$\frac{m}{n} + \frac{m'}{n'} i = \frac{n'm}{nn'} + \frac{nm'}{nn'} i = \frac{n'm + nm'i}{nn'} =$$

$$= \overline{\text{incl}}\left(\frac{\overbrace{n'm + nm'i}^{\in \mathbb{Z}[i]}}{\underbrace{nn'}_{\in \mathbb{Z}[i]}}\right)$$

3.4. $K = \mathbb{Z}[i]/(3)$ este corp cu 9 elemente (și char $K = 3$).

<u>Tentative</u> $K = \mathbb{Z}_3[i] = \{\hat{a} + \hat{b}\, i \mid \hat{a}, \hat{b} \in \mathbb{Z}_3\}$

ce sens are?

<u>Idee</u> La $\mathbb{Z}_3$, "adăugam" un element care este soluție a ecuației $X^2 = -\hat{1}$.

$$\mathbb{Z}[i]/(3) = \{ \widehat{0+0i}, \widehat{1+0i}, \widehat{2+0i}, \widehat{0+1i}, \widehat{1+1i}, \widehat{2+1i}, \widehat{0+2i}, \widehat{1+2i}, \widehat{2+2i} \}$$

$\leftarrow$ 9 elemente

$$\widehat{26+59i} = \widehat{2+2i}$$

• Corp $\Leftrightarrow$ (3) ideal maximal.

Folosim Exc 2.1: fie $a+bi \in \mathbb{Z}[i]$, $a+bi \notin (3)$.

Vrem $(3)+(a+bi) = \mathbb{Z}[i]$.

$3 \nmid a$ sau $3 \nmid b$.

Temă Încheiați argumentul + exc 3.3.