Planul cursului:

I. Aritmetică în inele

II. Introducere în teoria modulelor

· Contextul părții I: inele comutative, unitare, <u>fără</u> divizori ai lui 0
(domenii de integritate)
(proful le va spune doar „domenii")

$\boxed{a \neq 0, b \neq 0 \Rightarrow a \cdot b \neq 0}$

Exemple: $(\mathbb{Z}, +, \cdot)$, $\underbrace{\mathbb{Q}, \mathbb{R}, \mathbb{C}}_{= \text{corpuri}}$

Th: $\left.\begin{array}{l} A = \text{domeniu} \\ B \subseteq A \\ \downarrow \\ \text{subinel} \end{array}\right| \Rightarrow B = \text{domeniu}$

Fie $\theta \in \mathbb{C}$

$$\mathbb{Z}[\theta] = \{a + b \cdot \theta \,/\, a, b \in \mathbb{Z}\}$$

$\boxed{Q}$: Când este $\mathbb{Z}[\theta]$ subinel în $\mathbb{C}$?

$$a + b \cdot \theta = a' + b' \cdot \theta \;\; \not\Rightarrow \;\; a = a' \text{ și } b = b'$$
$$\Leftarrow$$

exemplu: $1 + \underset{b}{1} \cdot 0 = 1 + \underset{b'}{2} \cdot 0$, $b \neq b'$

„$\Rightarrow$" este adevărată $\overset{\text{d.ș.n.}}{\underset{\text{d.}}{\Longleftrightarrow}}$ $\theta \notin \mathbb{Q}$.

Dem:

Pp. $\theta \notin \mathbb{Q}$.

Pp. că $a + b\cdot\theta = a' + b'\cdot\theta \Rightarrow (b-b')\theta = a - a'$

Dacă $b \neq b' \Rightarrow \theta = \dfrac{a-a'}{b-b'} \in \mathbb{Q}$

$\lightning$

! Dacă $\theta \notin \mathbb{Q}$ și $z \in \mathbb{C}$ a.î. $\exists\, a, b \in \mathbb{Z}$ cu $z = a + b\cdot\theta$, atunci $a$ și $b$ sunt <u>unice</u>!

$\boxed{Q}$: $\mathbb{Z}[\theta]$ e subinel?

Pp. $\theta \notin \mathbb{Q}$.

$\mathbb{Z}[\theta]$ subinel:

- $(a+b\cdot\theta) + (a' + b'\cdot\theta) = (a+a') + (b+b')\cdot\theta \in \mathbb{Z}[\theta]$
- $1 = 1 + 0\cdot\theta \in \mathbb{Z}[\theta]$

(*) $\cdot\ (a+b\cdot\theta)(a'+b'\cdot\theta) = aa' + (ab' + a'b)\theta + \underline{b\cdot b'\cdot\theta^2}$

$\Rightarrow \theta^2 \in \mathbb{Z}[\theta]$

$\theta^2 = a + b\cdot\theta \Rightarrow \theta^2 - b\theta - a = 0$
$a, b \in \mathbb{Z}$

$\Downarrow$

$\theta$ este rădăcina unui polinom monic de gr. II, cu coef. întregi

Reciproc: Pp. $\theta$ este rădăcină a lui $f \in \mathbb{Z}[X]$, grad $f = 2$, $f$ monic

$\Rightarrow \mathbb{Z}[\theta]$ este subinel

$f(\theta) = 0$

$f = X^2 + \alpha \cdot X + \beta, \ \alpha, \beta \in \mathbb{Z}$

$$\theta^2 = -\alpha \cdot \theta - \beta \overset{(*)}{=} (a + b \cdot \theta)(a' + b'\theta)$$
$$= aa' + (a'b + a \cdot b')\theta + bb'(-\alpha\theta - \beta)$$
$$= \delta + \gamma \cdot \theta \in \mathbb{Z}[\theta]$$

$\in \mathbb{Z}$

---

Alte exemple de domenii, subinele în $\mathbb{C}$

- $\theta = \sqrt{-1} = i \notin \mathbb{Q}$

  $\theta^2 + 1 = 0 \Rightarrow \theta$ este rădăcină pentru $f = X^2 + 1$

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

  $\hookrightarrow$ INELUL ÎNTREGILOR LUI GAUSS

- $\theta = \frac{-1 + i\sqrt{3}}{2} \notin \mathbb{Q} \rightarrow$ rădăcina de ordin 3 a unității

  $\theta^2 + \theta + 1 = 0$

  $f(\theta) = 0, \ f = X^2 + X + 1$

  $\mathbb{Z}\left[\frac{-1 + i\sqrt{3}}{2}\right] \subseteq \mathbb{C}$ subinel

  $\hookrightarrow$ INELUL ÎNTREGILOR EISENSTEIN

- $d \in \mathbb{Z}$ fixat a.î. $\sqrt{d} \in \mathbb{Q}$

  $(\sqrt{d})^2 - d = 0 \Rightarrow f(\sqrt{d}) = 0, \ f = X^2 - d$

  $\Rightarrow \mathbb{Z}[\sqrt{d}]$ subinel

  $\hookrightarrow$ INELUL ÎNTREGILOR PĂTRATICI

$\cdot \sqrt{d} \notin \mathbb{Q}$

$\theta = \dfrac{1+\sqrt{d}}{2}$

$\mathbb{Z}[\theta] =$ subinel? $\underline{\underline{\text{nu}}}$ mereu

$$\theta^2 = \frac{1+2\sqrt{d}+d}{2} = \frac{2(1+\sqrt{d})}{4} + \frac{d-1}{4} = \theta + \frac{d-1}{4}$$

Dacă $\dfrac{d-1}{4} \in \mathbb{Z} \Rightarrow f(\theta) = 0$, unde $f = x^2 - x - \underbrace{\dfrac{d-1}{4}}_{\in \mathbb{Z}}$

$\Rightarrow \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] \underset{\text{subinel}}{\subseteq} \mathbb{C}$

$\dfrac{d-1}{4} \in \mathbb{Z} \Leftrightarrow 4 \mid d-1 \Leftrightarrow d = 4k+1$

$\Leftrightarrow d \equiv_4 1$ (modulo 4)

(atunci $\mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$ subinel)

Dacă $\mathbb{Z}[\underbrace{\dfrac{1+\sqrt{d}}{2}}_{\theta}]$ este subinel, atunci $d \equiv_4 1$.

$$\theta^2 = \theta + \frac{d-1}{4}$$

$\exists f, f(\theta) = 0 \Rightarrow f = x^2 + \alpha x + \beta = 0, \quad \alpha, \beta \in \mathbb{Z}$

$\theta^2 = -\alpha\theta - \beta \Rightarrow \theta + \dfrac{d-1}{4} = -\alpha\theta - \beta$

$\xRightarrow[\text{(scrierea e unică)}]{\theta \notin \mathbb{Q}} \quad \alpha = -1$ și $\dfrac{d-1}{4} = -\beta \in \mathbb{Z} \Rightarrow d \equiv_4 1$

Concluzie: $\mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] =$ subinel în $\mathbb{C}$

$\sqrt{d} \notin \mathbb{Q}, \ d \equiv_4 1$

## Alte exemple de domenii

- $A[X_1,\dots,X_n]$ = inelul de polinoame cu coef. în $A$ = dom.
- $K$ = corp $\Rightarrow$ $K$ = domeniu
- $A$ = domeniu, $S$ = sistem multiplicativ în $A$ $\Rightarrow$ $S^{-1}\cdot A$ domeniu

$$\boxed{\begin{array}{l} 1\in S \\ 0\notin S \\ s\cdot s'\in S \ (s,s'\in S) \end{array}}$$

$$S^{-1}\cdot A = \left\{ \frac{a}{s} \;/\; \begin{array}{l} a\in A \\ s\in S \end{array} \right\}$$

$$\frac{a}{s}+\frac{a'}{s'}=\frac{a\cdot s'+a'\cdot s}{s\cdot s'}$$

$$\frac{a}{s}\cdot\frac{a'}{s'}=\frac{a\cdot a'}{s\cdot s'}$$

### Divizibilitate în domeniu

$A$ = domeniu

Def: Spunem că $a|b$ în $A$ („$a$ divide $b$")
$\Leftrightarrow$ $\exists\, c\in A$ a.î. $b=a\cdot c$

$a|a$, $1|a$, $a|0$

$a|1$ $\Leftrightarrow$ $a$ este INVERSABIL ($U(A)$ = mult. elem. inversabile)

$0|a$ $\Leftrightarrow$ $a=0$

Proprietăți (Dem: Exc!)

- $a|b$ și $b|c$ $\Rightarrow$ $a|c$ (tranzitivitate)
- $a|a$ (reflexivă)
- $a|b$ și $b|a$ $\not\Rightarrow$ $a=b$ (nu este antisimetrică

Def: $a \sim b \iff a \mid b$ și $b \mid a$

↳ asociate în divizibilitate

Exc: „$\sim$" rel. de echivalență

$a \sim b \iff \exists\, u \in U(A)$ a.î. ~~$b = a \cdot u$~~ $a = b \cdot u$