Curs 11

22.12.2020

Reamintesc • $(A,+,\cdot)$ inel (unitar) ($(A,+)$ grup abelian, $(A,\cdot)$ monoid, $\cdot$ este distributivă față de adunare)

$\boxed{\text{NOTAȚIE}}$ De acum înainte inel = inel comutativ

• $A[X] = \{a_0 + a_1X + \dots + a_nX^n \mid a_0, \dots, a_n \in A, n \in \mathbb{N}\}$ $(A[X], +, \cdot)$

inelul de polin. în nedeterminata X cu coeficienți în inelul com. A

$(a_0 + \dots + a_nX^n) + (b_0 + b_1X + \dots + b_nX^n) = (a_0+b_0) + (a_1+b_1)X + \dots + (a_n+b_n)X^n$

$(a_0 + \dots + a_nX^n) \cdot (b_0 + b_1X + \dots + b_mX^m) = a_0 \cdot b_0 + (a_1 \cdot b_0 + a_0 \cdot b_1)X + \dots + \left(\sum_{i+j=k} a_i b_j\right) X^k + \dots + a_n b_m X^{n+m}$

• $(A,+,\cdot)$ corp dacă $(A,+,\cdot)$ inel și orice element nenul este inversabil.

• $(A,+,\cdot)$ inel, $\emptyset \neq I \subseteq A$. I s.n. ideal dc: 1) $(I,+) \leq (A,+)$

2) $(\forall) a \in A$, $(\forall) x \in I$ $\Rightarrow a \cdot x \in I$.

Obs 1) Idealele lui $\mathbb{Z}$ sunt $n\mathbb{Z}$, $n \in \mathbb{N}$.

2) Orice inel nenul A are 2 ideale: (0) și A.

3) Un inel nenul A este corp $\Leftrightarrow$ are exact 2 ideale (0) și A.

(Dem: "$\Rightarrow$" A e corp. Fie $I \neq (0)$ un ideal al lui A. $\Rightarrow (\exists) x \in I, x \neq 0$

$\xrightarrow{x \neq 0} x \in U(A)$, $x \in I$ $\xRightarrow{\text{Exc!}} I = A$

(Exc! $x \in U(A) \cap I$

Fie $a \in A$. Deoarece I e ideal și $x \in I$ $\xRightarrow{\text{def}} x \cdot \underbrace{(x^{-1}a)}_{=a} \in I$

"$\Leftarrow$" Fie $a\in A$, $a\neq 0$. Mulțimea $\{ax \mid x\in A\}$ este un ideal al lui A $\Longrightarrow$
$\overset{\Downarrow}{a} = a\cdot 1$ nenul ipoteza

$\{ax\mid x\in A\} = A \ni 1 \Rightarrow 1 = a\cdot y$ pt un $y\in A \Rightarrow a\in U(A) \Rightarrow A$ e corp. ∎

Operații cu ideale: ① Fie I, J 2 ideale ale lui A. Atunci $I\cap J$ și $I+J$ sunt ideale ale lui A. $I+J \overset{def}{=} \{a+b \mid a\in I, b\in J\}$

② Dc. I, J sunt ideale ale lui A, atunci $I\cup J$ este ideal $\Longleftrightarrow$ $I\subseteq J$ sau $J\subseteq I$.

---

① $I\cap J = \{a \mid a\in I \text{ și } a\in J\}$

Dem: 1) $(I\cap J,+)\le(A,+)$ deoarece intersecție de subgrupuri e subgrup

2) Fie $a\in A$, $x\in I\cap J$. Deoarece I este ideal $\Rightarrow ax\in I$
$\Updownarrow$
$x\in I$ și $x\in J$ $\qquad$ J este ideal $\Rightarrow ax\in J$ $\Rightarrow$

$\Rightarrow ax\in I\cap J$. $\Rightarrow I\cap J$ este ideal

② Pp abs. că $I\not\subseteq J$ și $J\not\subseteq I$ $\Rightarrow$ $(\exists)\ x_1\in I\setminus J$, $(\exists)\ x_2\in J\setminus I$.

"$\Rightarrow$" $I\cup J$ este ideal $\xrightarrow[x_1, x_2\in I\cup J]{1)}$ $x_1+x_2\in I\cup J \Rightarrow x_1+x_2\in I$ sau $x_1+x_2\in J$

$(I,+)\le(A,+)$, $x_1\in I$ $\Rightarrow x_2 = (x_1+x_2)-x_1\in I$ ✗

$x_2\in J$ $\Rightarrow x_1\in J$ ✗, $x_1 = (x_1+x_2)-x_2$

Def Fie $\{a_1, \dots, a_n\} \subseteq A$, $(A,+,\cdot)$ inel. Idealul generat de mulțimea $\{a_1,\dots,a_n\}$ se notează cu $(a_1,\dots,a_n)$ sau $(a_1,\dots,a_n)A$ (dacă inelul în care lucrăm se schimbă) și reprezintă mulțimea

$$(a_1,\dots,a_n)A = \{a_1b_1 + \dots + a_nb_n \mid b_1,\dots,b_n \in A\}.$$

În particular, (a) (sau aA sau $(a)A$) $= \{ax \mid x \in A\}$. s.n. idealul principal generat de a.

Aplicație ①
$$\underbrace{\left(22\mathbb{Z} + (3\mathbb{Z} \cap 17\mathbb{Z})\right)}_{\text{ideal al lui } \mathbb{Z}} + 6\mathbb{Z} = n\mathbb{Z}$$
Cine e n? $\boxed{n=1}$

$\Rightarrow (22\mathbb{Z} + 51\mathbb{Z}) + 6\mathbb{Z} = \mathbb{Z} + 6\mathbb{Z} = \mathbb{Z} = 1\mathbb{Z}$

Exc
$$\begin{cases} a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z} \\ a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z} \end{cases}$$
, unde (a,b) e cmmdc al lui a și b
$[a,b]$ e cmmmc al lui a și b

Def Dacă A și B sunt 2 inele, atunci produsul direct al celor 2 inele este inelul $A \times B$ definit pe produsul cartezian $A \times B$ astfel:

$$(a,b)+(c,d) = (a+c, b+d)$$
$$(a,b)\cdot(c,d) = (ac, bd)$$

(Exc! Să se verifice că $(A\times B,+,\cdot)$ e inel)

Exc Să se arate că idealele lui $(A\times B,+,\cdot)$, unde A,B sunt inele, sunt de forma $I \times J$ cu I ideal al lui A și J ideal al lui B

Def Fie A și B 2 inele. O funcție $f : A \to B$ s.n. morfism de inele (unitar) dacă:

1) $f(x+y) = f(x)+f(y)$ $(\forall)$ $x,y \in A$
2) $f(x\cdot y) = f(x)\cdot f(y)$ $(\forall)$ $x,y \in A$
3) $f(1_A) = 1_B$.

Exemple

① $1_A : A \to A$, $1_A(x) = x$ este morfismul identic; izomorfism de inele (A inel oarecare)

② $f : \mathbb{Z} \to A$, $f(k) = k\cdot 1_A$ este morfism de inele

③ Nu există morfisme de inele de la $\mathbb{Q}$ în $\mathbb{Z}$.

④ Exc! Să se arate că $f : \mathbb{Z}[i] \to \mathbb{Z}_2$, $f(a+bi) = \widehat{a+b}$ este morfism de inele.

⑤ Fie A, B inele. Atunci $p_A : A\times B \to A$, $p_A((a,b)) = a$ și $p_B : A\times B \to B$, $p_B((a,b)) = b$ $(\forall)$ $(a,b)\in A\times B$ sunt morfisme surjective de inele.

⑥ Fie $n \in \mathbb{N}$, $n \geq 2$. Atunci $p : \mathbb{Z} \to \mathbb{Z}_n$, $p(k) = \hat{k}$ $(\forall)$ $k \in \mathbb{Z}$ este un morfism surjectiv de inele.

Def Un morfism de inele bijectiv se numește izomorfism de inele.

Propr. de bază ale morfismelor de inele

- compunerea a 2 morfisme de inele este un morfism de inele
- inversul unui izomorfism de inele este tot un izomorfism de inele

∵ Exc! Dacă $f: A \to B$ e morfism de inele și $a \in U(A) \Rightarrow f(a) \in U(B)$.

Propoziție Fie $f: A \to B$ un morfism de inele.

a) Dacă C e subinel al lui $A \Rightarrow f(C)$ e subinel al lui B (în particular $Im(f)$ e subinel al lui B).

b) Dacă $\mathcal{Y}$ este subinel al lui B (resp. ideal) atunci $f^{-1}(\mathcal{Y})$ este un subinel al lui A (resp ideal). (în particular $f^{-1}(\{0_B\}) = Ker f$ este subinel (resp ideal) al lui A)

preimaginea lui $\mathcal{Y}$

c) $Ker f$ este ideal al lui A și f injectiv $\Leftrightarrow Ker f = \{0_A\}$.

Exc! Dacă $f: A \to B$ e morfism de inele și A e corp $\Rightarrow f$ e injectiv.

Obs (Atenție!) ① Dacă $f: A \to B$ e morfism de inele și I este un ideal al lui A atunci, în general, $f(I)$ nu e ideal al lui B. De exemplu, fie $f: \mathbb{Z} \to \mathbb{Q}$ $f(a) = a$; f este morfism de inele (morfismul incluziune) și $f(2\mathbb{Z}) = 2\mathbb{Z}$. $2\mathbb{Z}$ este ideal al lui $\mathbb{Z}$, dar nu e ideal al lui $\mathbb{Q}$ ($\mathbb{Q}$ e corp și are doar 2 ideale (0) și $\mathbb{Q}$)

② Dacă $f: A \to B$ e morfism surjectiv de inele și I este un ideal al lui A atunci $f(I)$ este un ideal al lui B. (Exc!)

Inel factor (Reamintesc A inel com)

Fie $(A,+,\cdot)$ un inel și I un ideal al său. Cum $(I,+) \trianglelefteq (A,+)$ atunci putem considera grupul factor $(A/I,+)$.

($\hat{a}+\hat{b}=\widehat{a+b}$; $\hat{a}=\hat{b}$ în $A/I \Longleftrightarrow a-b\in I$)

Definim pe A/I operația de înmulțire astfel: $\hat{a}\cdot\hat{b}=\widehat{ab}$.

Operația e bine definită (Exc!) și în raport cu operațiile "+" și "$\cdot$" $(A/I,+,\cdot)$ este inel, numit inelul factor al lui A modulo I.

Teorema fundamentală de izomorfism la inele Fie $f: A\to B$ un morfism de inele. Atunci

$$A/\mathrm{Ker}f \underset{\text{izom. de inele}}{\simeq} \mathrm{Im}f$$

și $F: A/\mathrm{Ker}f \longrightarrow \mathrm{Im}(f)$ $F(\hat{x})=f(x)$ este un izomorfism de inele.

Corolar (Lema chineză a resturilor; LCR) Fie $m,n\in\mathbb{Z}$ nr. întregi a.î. $(m,n)=1$. Atunci $\mathbb{Z}_{mn}\simeq \underbrace{\mathbb{Z}_m\times\mathbb{Z}_n}_{\text{produsul direct al inelelor}}$.

Obs Se poate generaliza la: $n_1, n_2, \dots, n_r \geq 2$ întregi a.î. $(n_i, n_j) = 1$ $(\forall)\ i \neq j$. Atunci

$$\mathbb{Z}_{n_1 \cdot n_2 \cdot \ldots \cdot n_r} \underset{\substack{\uparrow \\ \text{izom. de inele}}}{\simeq} \underbrace{\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_r}}_{\text{prod. direct al inelelor}}$$

Aplicație practică (Vezi Exc. Seminar)

Sistemul de congruențe
$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$
$n_1, \dots, n_r \geq 2$ cu $(n_i, n_j) = 1$ $(\forall)\ i \neq j$

are soluție unică modulo $n_1 \cdot n_2 \cdot \ldots \cdot n_r$.