Seminar 12

22.12.2020

Exc 1 $a\mathbb{Z}+b\mathbb{Z}=(a,b)\mathbb{Z}$, $a\mathbb{Z}\cap b\mathbb{Z}=[a,b]\mathbb{Z}$

$d=(a,b) \Rightarrow \begin{matrix} a=da_1 \\ b=db_1 \end{matrix}$ $(a_1,b_1)=1$

Fie $d=(a,b)$, $m=[a,b]$. Vreau $a\mathbb{Z}+b\mathbb{Z} \overset{\supseteq}{\underset{\subseteq}{=}} d\mathbb{Z}$

"$\subseteq$" Fie $x\in a\mathbb{Z}+b\mathbb{Z} \Rightarrow x=a\cdot k+b\cdot l$ cu $k,l\in\mathbb{Z}$

$x=da_1k+db_1\cdot l=d(a_1k+b_1l)\in d\mathbb{Z}$.

Alg. Euclid $\underset{d=(a,b)}{\Rightarrow}$ (*) $d=a\cdot m+b\cdot n$ pt $m,n\in\mathbb{Z}$

"$\supseteq$" Fie $x\in d\mathbb{Z} \Rightarrow x=dk$, $k\in\mathbb{Z} \overset{(*)}{\Rightarrow}$

$x=(am+bn)k=a\cdot(mk)+b\cdot(nk)\in a\mathbb{Z}+b\mathbb{Z}$. ☒

$a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}$

Dem: "$\supseteq$" $m=[a,b] \Rightarrow \begin{matrix} a|m \\ b|m \end{matrix}$ Fie $x\in m\mathbb{Z} \Rightarrow m|x \Rightarrow \left.\begin{matrix} a|x \Rightarrow x\in a\mathbb{Z} \\ b|x \Rightarrow x\in b\mathbb{Z} \end{matrix}\right| \Rightarrow$

$\Rightarrow x\in a\mathbb{Z}\cap b\mathbb{Z}$ ☒.

"$\subseteq$" Fie $y\in a\mathbb{Z}\cap b\mathbb{Z} \Rightarrow \left.\begin{matrix} y\in a\mathbb{Z} \Rightarrow a|y \\ \text{și } y\in b\mathbb{Z} \Rightarrow b|y \end{matrix}\right| \Rightarrow \underset{m}{\underset{\parallel}{[a,b]}}|y \Rightarrow y\in m\mathbb{Z}$

Exc 2 Să se calculeze idealele: 1) $18\mathbb{Z}+(2\mathbb{Z}\cap 3\mathbb{Z})=18\mathbb{Z}+6\mathbb{Z}=6\mathbb{Z}$

2) $15\mathbb{Z}\cap(12\mathbb{Z}+16\mathbb{Z})=15\mathbb{Z}\cap 4\mathbb{Z}=60\mathbb{Z}$.

Exc 3 Dacă $f: A \to B$ este un morfism surjectiv de inele și I este un ideal al lui A atunci $f(I)$ este un ideal al lui B.

Dem Tb. să arătam că: $\left[\begin{array}{l} 1)\ (f(I),+) \leq (B,+) \\ 2)\ (\forall) b \in B\ (\forall) x \in f(I) \Rightarrow bx \in f(I). \end{array}\right.$

$f: A \to B$ morf. de inele înseamnă $\left.\begin{array}{l} f(x+y) = f(x)+f(y) \\ f(xy) = f(x)f(y) \end{array}\right\} (\forall)\ x,y \in A$

$f(1_A) = 1_B$

1) Fie $x,y \in f(I)$. Vreau să arăt că $x-y \in f(I)$

$x,y \in f(I) \Rightarrow (\exists)\ a,c \in I$ a.î. $x = f(a)$, $y = f(c)$

$x - y = f(a) - f(c) \overset{f}{\underset{\text{morfism}}{=\!=}} f(a-c) \in f(I)$.

$(I,+) \leq (A,+)$ deoarece I e ideal $\underset{a,c \in I}{\Longrightarrow} a-c \in I$

Deci $x-y \in f(I)$.

2) Fie $b \in B$, $x \in f(I)$. $x \in f(I) \Rightarrow (\exists)\ a \in I$ a.î. $x = f(a)$

f surjectiv $\Rightarrow f(A) = B \underset{b \in B}{\Longrightarrow} (\exists)\ d \in A$ a.î. $b = f(d)$

Atunci $b \cdot x = f(d) \cdot f(a) \overset{f}{\underset{\text{morfism}}{=\!=}} f(d \cdot a)$

I este ideal $\overset{\text{def}}{\underset{d \in A,\, a \in I}{\Longrightarrow}} d \cdot a \in I$ $\Bigg| \Rightarrow \underset{b \cdot x}{\overset{\|}{f(d \cdot a)}} \in f(I)$ ☒

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

Fie $a+bi, c+di \in \mathbb{Z}[i]$ $f(a+bi+c+di) = f((a+c)+(b+d)i) = \widehat{(a+c)+(b+d)} = \widehat{a+b+c+d}$

$$f(a+bi)+f(c+di) = \widehat{a+b} + \widehat{c+d} \underset{\mathbb{Z}_2}{=} \widehat{(a+b)+(c+d)}$$

$\Rightarrow f(a+bi)+f(c+di) = f(a+bi+c+di)$ ①

$$f((a+bi)\cdot(c+di)) = f((ac-bd)+i(ad+bc)) = \widehat{ac-bd+ad+bc}$$

$$f(a+bi)\cdot f(c+di) = \widehat{a+b}\cdot\widehat{c+d} = \widehat{(a+b)\cdot(c+d)} = \widehat{ac+bd+ad+bc}$$

$\Rightarrow$

în $\mathbb{Z}_2$ $\hat{k} = -\hat{k} = \widehat{-k}$

$\Rightarrow f((a+bi)\cdot(c+di)) = f(a+bi)\cdot f(c+di)$ ②

$f(1) = f(1+0\cdot i) = \hat{1}$ ③ Din ①, ② și ③ $\Rightarrow$ f e morfism de inele.

Obs ① f e morf. surjectiv $(f(0) = \hat{0}, f(1) = \hat{1})$

② $\ker f = \{a+bi \in \mathbb{Z}[i] \mid f(a+bi) = \hat{0}\} = \{a+bi \mid a,b \in \mathbb{Z}$ și $a+b$ par$\}$

$f(a+bi) = \widehat{a+b}$; $\widehat{a+b} = \hat{0} \Leftrightarrow 2 \mid a+b \Leftrightarrow a \equiv b \pmod 2$

$\mathrm{Ker} f$ este idealul lui $\mathbb{Z}[i]$ generat de $1+i$, i.e. $\mathrm{Ker} f \underset{\supseteq}{=} (1+i)$.
evid.

"$\subseteq$" Fie $a+bi \in \mathrm{Ker} f$, adică $a, b \in \mathbb{Z}$ și $a+b$ e par. $\Rightarrow \underline{a+b=2c}$, $c \in \mathbb{Z}$

$$a+bi = a(1+i) + (b-a)i$$
$$= 2c - b + bi = 2c - b(1-i) =$$
$$= 2c + bi(1+i) =$$
$$= (1+i)(1-i) \cdot c + bi(1+i) =$$
$$= (1+i)\left[c - ci + bi\right] = (1+i)\left[c + \underbrace{(b-c)}_{\in \mathbb{Z}[i]} i\right] \Rightarrow a+bi \in (1+i).$$

$\boxed{-(1-i) = i(1+i)}$

$\boxed{2 = (1+i)(1-i)}$

Deci $\mathrm{Ker} f = (1+i)\mathbb{Z}[i] \left(= (1+i)\right)$

③ Aplicând T.F.I la inele obținem că $\mathbb{Z}[i]/\mathrm{Ker} f \underset{\text{izom. de inele}}{\simeq} \mathrm{Im} f = \mathbb{Z}_2$,

adică $\mathbb{Z}[i]/(1+i) \underset{\text{izom. de inele}}{\simeq} \mathbb{Z}_2$.

Exc 5 Dacă A și B inele atunci idealele lui $A\times B$ sunt de forma $I\times J$ unde I este un ideal al lui A și J este un ideal al lui B.

Aplicație: Determinați idealele inelului produs direct $\mathbb{Z}\times\mathbb{Z}$

(merge pentru $\underbrace{\mathbb{Z}\times\mathbb{Z}\times\ldots\times\mathbb{Z}}_{k \text{ ori}}$)

$\mathbb{Z}\times\mathbb{Z}=\{(a,b) \mid a,b\in\mathbb{Z}\}$

$(a,b)+(c,d)=(a+c,b+d)$

$(a,b)\cdot(c,d)=(a\cdot c,b\cdot d)$

Idealele lui $\mathbb{Z}\times\mathbb{Z}$ (via Exc 5) sunt: $n\mathbb{Z}\times m\mathbb{Z}$ $\quad n,m\in\mathbb{N}$.

$n=1, m=1 \Rightarrow n\mathbb{Z}\times m\mathbb{Z}=\mathbb{Z}\times\mathbb{Z}$

LCR Date $m_1, m_2, \ldots, m_k\in\mathbb{N}$, mai mari sau egale cu 2, a.î. $(m_i, m_j)=1$ $(\forall)\, i\neq j$; și $a_1, a_2, \ldots, a_k\in\mathbb{Z}$ atunci sistemul de congruențe

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ \vdots \\ x\equiv a_k \pmod{m_k} \end{cases}$$

are soluție unică modulo $m_1\cdot m_2\cdot\ldots\cdot m_k$.

Algoritm de rezolvare

- Consider $N=m_1\cdot\ldots\cdot m_k$, $N_i=\dfrac{N}{m_i}$ $(\forall)\, i=\overline{1,k} \Longrightarrow (N_i, m_i)=1$ $(\forall)\, i=\overline{1,k}$
- Determinăm $x_1, \ldots, x_k$ a.î. $N_i x_i\equiv 1 \pmod{m_i}$ $(\forall)\, i=\overline{1,k}$
- Soluția unică modulo $m_1\cdot m_2\cdot\ldots\cdot m_k$ este $x \pmod N = a_1N_1x_1+\ldots+a_kN_kx_k \pmod N$

Exc $d=(a,b) \Rightarrow (\exists)\, m,t \in \mathbb{Z}$ a.î. $d = a\cdot m + b\cdot t$. Cum determin m și t?

Cu Algoritmul lui Euclid.

$a = b\cdot c_1 + r_1 \quad 0 \le r_1 < b$

$b = r_1 \cdot c_2 + r_2 \quad 0 \le r_2 \le r_1$

$\vdots$

$r_{n-2} = r_{n-1}\cdot c_n + \boxed{r_n} \quad 0 \le r_n < r_{n-1}$

$r_{n-1} = r_n \cdot c_{n+1} + 0$

Ultimul rest nenul, r_n în cazul nostru este $d=(a,b)$.

$r_1 = a - b\cdot c_1$

$b = (a - b\cdot c_1)\cdot c_2 + r_2 \Rightarrow$

$r_2 = b - a\cdot c_2 + b\cdot c_1 c_2 = b(1 + c_1 c_2) - a\cdot c_2$

ș.a.m.d. obținem $r_n = a\cdot m + b\cdot t$

Exemplu $a = 35,\ b = 24,\ d = (35,24) = 1$

$35 = 24\cdot 1 + \boxed{11}$

$24 = 11\cdot 2 + \boxed{2}$

$11 = 2\cdot 5 + \boxed{1} \quad \Rightarrow 1 = (35,24)$

$2 = 1\cdot 2 + 0$

$\boxed{11} = 35 - 24$

$\boxed{2} = 24 - (35-24)\cdot 2 = 24\cdot 3 - 35\cdot 2$

$1 = (35-24) - (24\cdot 3 - 35\cdot 2)\cdot 5$

$1 = 35\cdot 11 - 24\cdot 16$, deci

$m = 11$ și $t = -16$.

Exc2 Determinați cel mai mic nr. natural nenul n a.î. n să fie divizibil cu 8, $n+1$ să fie divizibil cu 7, $n+2$ să fie divizibil cu 6 și $n+3$ să fie divizibil cu 5

Exc 1 Determinați cel mai mic număr natural n care împărțit la 5 dă restul 3, împărțit la 7 dă restul 2 și împărțit la 9 dă restul 8.

$$(*)\begin{cases} n \equiv 3 \pmod 5 \\ n \equiv 2 \pmod 7 \\ n \equiv 8 \pmod 9 \end{cases}$$

($\Leftrightarrow 5 \mid n-3 \Leftrightarrow n$ dă restul 3 la împ cu 5)

Pt. "rapiditate" voi scrie $n \equiv 3(5)$ în loc de $n \equiv 3 \pmod 5$.

Obs. că $(m_1, m_2) = (m_1, m_3) = (m_2, m_3) = 1$

$$(*)\begin{cases} n \equiv 3(5) \\ n \equiv 2(7) \\ n \equiv 8(9) \end{cases}$$

$a_1 = 3 \quad a_2 = 2 \quad a_3 = 8$

$m_1 = 5 \quad m_2 = 7 \quad m_3 = 9$

$N = 5 \cdot 7 \cdot 9 \quad N_1 = \frac{N}{m_1} = 7 \cdot 9 \quad N_2 = 5 \cdot 9 \quad N_3 = 5 \cdot 7$

$N_1 x_1 \equiv 1(m_1) \rightsquigarrow 63 x_1 \equiv 1(5) \Leftrightarrow 3x_1 \equiv 1(5) \Leftrightarrow x_1 \equiv \boxed{2}(5) \Leftrightarrow x_1 \equiv -3(5)$

$N_2 x_2 \equiv 1(m_2) \rightsquigarrow 45 x_2 \equiv 1(7) \Leftrightarrow 3x_2 \equiv 1(7) \Leftrightarrow x_2 \equiv \boxed{5}(7)$

$N_3 x_3 \equiv 1(m_3) \rightsquigarrow 35 x_3 \equiv 1(9) \Leftrightarrow -x_3 \equiv 1(9) \Leftrightarrow x_3 \equiv -1(9) \Leftrightarrow x_3 \equiv \boxed{8}(9)$.

Soluția unică modulo $N = 5 \cdot 7 \cdot 9 = 315$ este

$x = 3 \cdot 63 \cdot 2 + 2 \cdot 45 \cdot 5 + 8 \cdot 35 \cdot 8 \pmod{315}$

$x = 3068(315)$; $x \equiv 233(315)$

Deci, cel mai mic nr. natural este 233.

(Verificare $233 \equiv 3(5)$, $233 \equiv 2(7)$, $233 \equiv 8(9)$)