Seminar 8

Aplicații

$\boxed{2.2.33}$ Fie A o mulțime oarecare și un inel R. Pe mulțimea

$$R^A = \{f : A \to R \mid f \text{ este o funcție}\}$$

se definesc operațiile:

$+, \cdot : R^A \times R^A \to R^A$ prin $f+g$, $fg : A \to R$,

$$(f+g)(x) = f(x) + g(x) \text{ și}$$
$$(fg)(x) = f(x)g(x) \text{ pt. orice}$$

$f, g \in R^A$, $\forall\ x \in A$.

Dem. că R^A este un inel, iar R^A este comutativ sau unitar, când R are aceeași proprietate.

<u>Soluție</u>: $(R, +, \cdot)$ inel

$(R^A, +, \cdot)$ inel dacă:

I. $(R^A, +)$ grup abelian

II. $(R^A, \cdot)$ monoid comutativ

III. $\forall\ f, g, h \in R^A$

$\Rightarrow \quad f \cdot (g+h) = fg + fh$

$\boxed{\text{I.}}$ • $\forall\ f, g \in R^A \Rightarrow f+g \in R^A$

$$(f+g)(x) = \underbrace{f(x)}_{\in R^A} + \underbrace{g(x)}_{\in R^A} \in R^A \quad (\text{p.s.})$$

• $\forall\ f, g, h \in R^A$ (asociativitatea)

$$(f+g)+h = f+(g+h)$$

$$((f+g)+h)(x) = (f+g)(x) + h(x) =$$

$$= f(x) + \underbrace{g(x) + h(x)} =$$

$$= f(x) + (g+h)(x) = (f+(g+h))(x)$$

• $\forall \; f, g \in \mathbb{R}^A, \; f+g = g+f$

$(f+g)(x) = f(x) + g(x) = g(x) + f(x)$

$= (g+f)(x)$ (comutativitatea)

• $\forall \; f, e \in \mathbb{R}^A$

$f + e = f$

$(f+e)(x) = f(x)$

$f(x) + e(x) = f(x)$

$e(x) = 0 \Rightarrow \underline{0(x) = 0}$

$\forall x \in A$

(e.n.)

• $f, f' \in \mathbb{R}^A$ a.î. $f + f' = 0$

$(f+f')(x) = 0(x)$

$\Rightarrow f(x) + f'(x) = 0(x)$

$f'(x) = -f(x)$

$f' = -f \in \mathbb{R}^A$

$\forall x \in A$

$\Rightarrow (\mathbb{R}^A, +)$ grup abelian

$\boxed{\text{I}}$ • $\forall\ f, g \in \mathbb{R}^A,\ f \cdot g \in \mathbb{R}^A$

$$(f \cdot g)(x) = \underbrace{f(x)}_{\in \mathbb{R}^A} \cdot \underbrace{g(x)}_{\in \mathbb{R}^A} \in \mathbb{R}^A \ (\text{p.s.})$$

• $\forall\ f, g, h \in \mathbb{R}^A,\ f \cdot (g \cdot h) = (f \cdot g) \cdot h$

$$(f \cdot (g \cdot h))(x) = f(x) \cdot (g \cdot h)(x) = f(x) \cdot g(x) \cdot h(x) = (f \cdot g)(x) \cdot h(x) = ((f \cdot g) \cdot h)(x) \ (\text{asociativitatea})$$

• $\forall\ f, g \in \mathbb{R}^A,\ f \cdot g = g \cdot f$

$$(f \cdot g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x) = (g \cdot f)(x) \ (\text{com.})$$

↳ "·" com. în $\mathbb{R}$

• $\forall\ f \in \mathbb{R}^A,\ \exists\ e \in \mathbb{R}^A$ a.î. $f \cdot e = f$

$$(f \cdot e)(x) = f(x)$$

$$f(x) \cdot e(x) = f(x)$$

$$e(x) = 1$$

$1 : A \to \mathbb{R}$, $1(x) = 1$, $\forall x \in A$
(e.n.)

$\Rightarrow (\mathbb{R}^A, \cdot)$ monoid comutativ

$\boxed{\text{III.}}$ $\forall f, g, h \in \mathbb{R}^A$

$\Rightarrow f(g+h) = f \cdot g + f \cdot h$

$(f \cdot (g+h))(x) = f(x) \cdot (g+h)(x) =$
$= f(x) \cdot (g(x) + h(x)) =$
$= f(x) \cdot g(x) + f(x) \cdot h(x)$

$\Rightarrow$ distr. „$\cdot$" față de „$+$"

$\Rightarrow (\mathbb{R}^A, +, \cdot)$ inel comutativ
($(\mathbb{R}, +, \cdot)$ inel comutativ)

$\boxed{2.2.37.}$ Să se determine toate subinelele lui $(\mathbb{Z}, +, \cdot)$.

Soluție: Știm că:

$Sub(\mathbb{Z},+) = \{ n\mathbb{Z} \mid n \in \mathbb{N} \}$

Verificăm dacă $n\mathbb{Z}$ este p.s. a lui $\mathbb{Z}$ în rap. cu „$\cdot$":

$x, y \in n\mathbb{Z}$

$x = n \cdot p$
$y = n \cdot q$, $p, q \in \mathbb{Z}$, $n \in \mathbb{N}$

$\Rightarrow xy = npnq = n(\underbrace{pnq}_{\in \mathbb{Z}}) \in n\mathbb{Z}$

$\forall\ x, y, z \in n\mathbb{Z}$, $x\cdot(y+z) = xy + xz$

$$\left.\begin{array}{l} x = np \\ y = nq \\ z = n\cdot r \end{array}\right\} \Rightarrow np(nq + nr) = npnq + npnr = xy + xz$$

(distr.)

$\boxed{2.2.38}$ Fie $n \in \mathbb{N}$, $n \geq 2$.

Să se arate că:

$\mathbb{Z}_n^\times = \{ [k]_n \mid (n, k) = 1 \}$.

Să se folosească acest rezultat pt. a arăta că $\mathbb{Z}_n$ este corp dacă n este nr. prim.

<u>Soluție</u>: $k \in \mathbb{Z}_n^\times \iff \exists\ \underline{k' \in \mathbb{Z}}$:

$$\hat{k} \cdot \hat{k'} = \hat{1} \iff \widehat{kk'} = \hat{1}$$

$$\iff n \mid (1 - kk')$$

$$\implies 1 - kk' = n \cdot r, \quad \underline{r \in \mathbb{Z}}$$

$$\implies \underset{\in \mathbb{Z}}{nr} + \underset{\in \mathbb{Z}}{kk'} = 1, \quad r, k' \in \mathbb{Z}$$

$$\iff (n, k) = 1$$

Dacă <u>n este prim</u>:

$$\implies \forall\, k \in \{1, \ldots, n-1\}$$

$$(n, k) = 1 \implies \mathbb{Z}_n^\times = \mathbb{Z}_n^*$$

$$\implies (\mathbb{Z}_n, +, \cdot) \text{ corp}$$

$\boxed{2.2.39}$ Să se rezolve următoarele ecuații în $\mathbb{Z}_6$:

a) $\hat{4}x + \hat{5} = \hat{1}$

$\left([4]_6 x + [5]_6 = [1]_6 \right)$

b) $\hat{5}x + \hat{3} = \hat{1}$

<u>Soluție</u>: a) $\hat{4}x + \hat{5} = \hat{1}$

$\hat{4}x = \hat{1} - \hat{5}$

$\hat{4}x = \hat{1} + \hat{1} = \hat{2}$

x	$\hat{0}$	$\hat{1}$	$\boxed{\hat{2}}$	$\hat{3}$	$\hat{4}$	$\boxed{\hat{5}}$
$\hat{4}x$	$\hat{0}$	$\hat{4}$	$\boxed{\hat{2}}$	$\hat{0}$	$\hat{4}$	$\boxed{\hat{2}}$

$\Rightarrow \quad x \in \{\hat{2}, \hat{5}\}$

b) $\hat{5}x + \hat{3} = \hat{1}$

$\hat{5}x = \hat{1} - \hat{3}$

$\hat{5}x = \hat{1} + \hat{3} = \hat{4}$

I.

x	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{5}x$	$\hat{0}$	$\hat{5}$	$\underline{\hat{4}}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

II. $\hat{5}x = \hat{4}$, $(5,6) = 1 \Rightarrow \exists\ \hat{5}^{-1} = \hat{5}$

$$x = \hat{4} \cdot \hat{5}$$
$$x = \hat{2}$$

$\boxed{2.2.34.}$ Să se verifice că $(\mathbb{Q}, +, \cdot)$ este un corp, unde $+$ și $\cdot$ sunt definite ca în 1.4.41, adică:

$$+, \cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ și}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad a, b, c, d \in \mathbb{Z}, \; b \neq 0, \; d \neq 0$$

<u>Soluție:</u>

$(\mathbb{Q}, +, \cdot)$ <u>corp</u>

$\Longleftarrow$ $(\mathbb{Q}, +, \cdot)$ inel $\begin{cases} e_1 = 0 \text{ e.n pt. } (\mathbb{Q}, +) \\ e_2 = 1 \text{ e.n. pt. } (\mathbb{Q}, \cdot) \end{cases}$

$\ell_1 \neq \ell_2$

$\forall \ x \in \mathbb{Q}^*, \quad \exists \ x' \in \mathbb{Q}$ a.î.

$$x \cdot x' = x' \cdot x = 1$$

I. $(\mathbb{Q}, +)$ grup abelian

- $\forall \ x, y \in \mathbb{Q}, \quad x = \frac{a}{b}, \ y = \frac{c}{d}$

$a, b, c, d \in \mathbb{Z}, \quad b, d \neq 0$

$$\Longrightarrow x + y \in \mathbb{Q}$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in \mathbb{Q}, \quad bd \neq 0$$

- $\forall \ x, y, z \in \mathbb{Q}, \quad x = \frac{a}{b}, \ y = \frac{c}{d},$

$z = \frac{e}{f}, \quad a, b, \ldots, f \in \mathbb{Z}, \quad b, d, f \neq 0$

$$\Longrightarrow \quad x + (y + z) = (x + y) + z$$

$$x + (y + z) = \frac{a}{b} + \frac{cf + ed}{fd} =$$

$$= \frac{afd + cfb + ebd}{bfd} = (x + y) + z$$

- $\frac{a}{b} + \frac{c}{d} = \frac{da+cb}{db} = \frac{c}{d} + \frac{a}{b}$ (com.)

$\forall\ x \in \mathbb{Q},\ \exists\ e \in \mathbb{Q}$ a.î. $x + e = x$

$\frac{a}{b} + x = \frac{a}{b} \implies \boxed{x = 0} \in \mathbb{Q}$

- $\forall\ x \in \mathbb{Q}\ \ \exists\ x' \in \mathbb{Q}$ a.î. $x + x' = 0$

$\frac{a}{b} + x' = 0 \implies x' = -\frac{a}{b} \in \mathbb{Q}$

$b \neq 0$

II. $(\mathbb{Q}, \cdot)$ monoid

- $\forall\ x, y \in \mathbb{Q} \implies x \cdot y \in \mathbb{Q}$

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}$, $bd \neq 0$

- $\forall\ x, y, z \in \mathbb{Q} \implies x \cdot (y \cdot z) = (x \cdot y) \cdot z$

- $\forall\ x \in \mathbb{Q},\ \exists\ e \in \mathbb{Q}$ a.î.

$x \cdot e = e \cdot x = x$

$e = 1 \in \mathbb{Q}$

III. $x(y+z) = xy + xz$

şi $(y+z)x = yx + zx$

I, II, III $\Longrightarrow$ $(\mathbb{Q}, +, \cdot)$ inel

IV. $\forall\, x \in \mathbb{Q}^*$, $\exists\, x' \in \mathbb{Q}$ a.î.

$$x \cdot x' = x' \cdot x = 1$$

$x = \frac{a}{b}$ $\Longrightarrow$

$$\frac{a}{b} \cdot \frac{c}{d} = 1 \quad , b, d \neq 0$$

$$\frac{c}{d} = \frac{b}{a} \in \mathbb{Q}^*, \quad a \neq 0, \ b \neq 0$$

$\Longrightarrow$ $(\mathbb{Q}, +, \cdot)$ corp

$\boxed{2.2.40}$ a.) Să se arate că

$\mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z}\}$ este un subinel al lui $\mathbb{C}$.

b.) Să se arate că

$$R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

este un subinel al lui $(\mathcal{M}_{2\times 2}(\mathbb{Z}), +, \cdot)$

c.) $R \simeq \mathbb{Z} + i\mathbb{Z}$

d.) $\mathbb{Z} + i\mathbb{Z}$, R domenii de integritate? Dar corpuri?

Soluție: a) $(\mathbb{Z}+i\mathbb{Z})$ inel comutativ cu unitate în raport cu „+" și „·" din $\mathbb{C}$

Fie $x = a+ib$, $y = c+id \in \mathbb{Z}+i\mathbb{Z}$, $a, b, c, d \in \mathbb{Z}$

$$x+y = (a+c)+i(b+d) \in \mathbb{Z}+i\mathbb{Z}$$

$$xy = ac-bd+i(ad+bc) \in \mathbb{Z}+i\mathbb{Z}$$

$$0 = 0+0i \in \mathbb{Z}+i\mathbb{Z}$$

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

$$-x = (-a)+i(-b) \in \mathbb{Z}+i\mathbb{Z}$$

$$\Rightarrow (\mathbb{Z}+i\mathbb{Z}, +, \cdot) \leq (\mathbb{C}, +, \cdot)$$

b) R subinel (temă)

c) Fie $f: \mathbb{Z}+i\mathbb{Z} \to R$

$$f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

$$x = a+ib, \quad y = c+id \in \mathbb{Z}+i\mathbb{Z}$$

$$f(x+y) = f((a+c)+i(b+d)) =$$

$$= \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} =$$

$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \underline{f(x)+f(y)}$$

$$\underline{f(x)f(y)} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} =$$

$$= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

$$\underline{f(xy)} = f(ac-bd+i(ad+bc)) =$$

$$= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

$\Rightarrow$ f morfism de inele (1)

- $f(x) = f(y) \Rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

$$\Rightarrow \begin{cases} a = c \\ b = d \end{cases} \Rightarrow x = y$$

$\forall \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $\exists\ a+ib \in \mathbb{Z}+i\mathbb{Z}$

a. î. $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

$\Rightarrow$ f bijectivă (2)

$$\xRightarrow{(1),(2)} R \simeq \mathbb{Z}+i\mathbb{Z}$$

- $\mathbb{Z} + i\mathbb{Z}$ inel com. cu unitate

$xy = 0 \Rightarrow x = 0$ sau $y = 0$ („A" datorită numerelor complexe)

Dar $2 \in \mathbb{Z} + i\mathbb{Z}$, însă $\frac{1}{2} \in \mathbb{Z} + i\mathbb{Z}$

$\Rightarrow$ <u>nu</u> e corp

- $R \simeq \mathbb{Z} + i\mathbb{Z}$ (au aceleași proprietăți)

$\Rightarrow$ R domeniu de integritate, dar <u>nu</u> este corp