Seminar 1 : Sem II

INELE

Def: O mulțime R împreună cu două op. algebrice „+", „·" s.n. inel dacă sunt îndeplinite următoarele axiome:

1. $(R,+)$ grup abelian
2. $(R,\cdot)$ monoid
3. $(\forall)\, a,b,c \in R$, $(a+b)\cdot c = ac+bc$

$c(a+b) = ca+cb$

În plus dacă „·" admite element neutru inelul R s.n. inel unitar.

Not: $(R,+,\cdot)$

Dacă „·" este comutativă atunci inelul R este comutativ.

Def morfismului de inele.

Fie $(R_1,+,\cdot)$ și $(R_2,+,\cdot)$ o funcție $f: R_1 \to R_2$ s.n. morfism de inele dacă:

1) $f(a+b) = f(a)+f(b)$ $(\forall)$ $a,b \in R_1$

2) $f(a\cdot b) = f(a)\cdot f(b)$ — " —

$18 \times 16 = 256$

$x^2 = x$

$(x \cancel{+} 1) x = 0$

$2 \cdot 3^2$

$Idem(\mathbb{Z}_{36}) = \{0, 1, 9, 28\}$

$a^2 = a$

$a \cdot a = a \quad | \cdot a^{-1}$

$a^{-1} = 1 \quad | \cdot b$

$ab = b$

<u>Subinele</u>

Def $(R, +, \cdot)$ inel și $S \subseteq R$

s.n subinel dacă $(S, +, \cdot)$ inel.

$(R, +)$ grup comutativ

$(S, +, \cdot)$ inel $\Rightarrow (S, +)$ grup comutativ.

$\Rightarrow S \trianglelefteq R$

S este subinel $\Leftrightarrow$ $\begin{cases} (\forall) x, y \in S, \ x - y \in S \\ (\forall) x, y \in S \ \ x \cdot y \in S \end{cases}$

$J \trianglelefteq M_2(R)$

$I = \{ a \in R \mid (\exists) A \in J, A = (a_{ij})_{i,j}$ și

$a_{lt} = a \}$

$a, b \in I$

$\exists A \in J$ și $B \in J$

$a_{ij} = a \quad b_{lt} = b$

$a - b$ este un element din $A \setminus B \in J$

$\left.\begin{array}{l} r \in R \\ a \in I \end{array}\right\} \Rightarrow \exists A \in J$ a.î. $a_{ij} = a$

cum J ideal în $M_2(R) \Rightarrow$

$$\underbrace{r I_2 \cdot A}_{= B} = B \in J$$

$b_{ij} = r a_{ij} = r a \in I$

$f: R_1 \to R_2$ morfism unitar de inele.

i) f surj $I_1 \trianglelefteq R_1 \Rightarrow f(I_1) \trianglelefteq R_2$

ii) $I_2 \trianglelefteq R_2 \Rightarrow f^{-1}(I_2) \trianglelefteq R_1$

Sunt de forma $I_1 \times I_2$ cu

$I_1 \trianglelefteq R_1$

$I_2 \trianglelefteq R_2$

$(R, +, \cdot)$ inel.

$I \trianglelefteq R \Rightarrow (I, +) \trianglelefteq (R, +)$

$\left(\frac{R}{I}, +\right)$

$\hat{a} \cdot \hat{b} = \widehat{ab}$

Ex: Arătați că $\left(\frac{\mathbb{Q}}{\mathbb{Z}}, +\right)$ nu există structuri de inel unitar.

$\text{End}(\mathbb{Q},+) = \{ f : \mathbb{Q} \to \mathbb{Q} \mid f(x) = \rho x, \rho \in \mathbb{Q} \}$

$f(1) = 1 \Rightarrow \rho = 1.$

$\text{End}(\mathbb{Q}) = \{ id_{\mathbb{Q}} \}.$

$f : (\mathbb{R},+,\cdot) \to (\mathbb{R},+,\cdot)$ end. unitar de inele

$f(x) = \rho \cdot x$ cu $x \in \mathbb{Q}$ și $\rho \in \mathbb{Q}$

$f(x) = x.$

Pt $x \in \mathbb{R} \setminus \mathbb{Q}.$

Fie $x_1, x_2 \in \mathbb{R}$ cu $x_1 < x_2.$

$f(\underbrace{x_2 - x_1}_{>0}) = f(x_2) - f(x_1) = f\left((\sqrt{x_2 - x_1})^2\right) = f(\sqrt{x_2 - x_1})^2 \geq 0$

$\Rightarrow f \nearrow.$

Fie $\alpha \in \mathbb{R} \setminus \mathbb{Q}.$

$(\forall)\ x \in \mathbb{Q}$ cu $x \leq \alpha.$

$f(x) \leq f(\alpha).$

$x \leq f(\alpha).$

Similar pt $x_0 \geq \alpha$

$\Rightarrow f(\alpha) \geq x_0.$ $\Big| \Rightarrow$

Ex.

2). $M = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \middle| a, b \in \mathbb{C} \right\}$ este subinel în $\mathcal{M}_2(\mathbb{C})$.

Fie $A, B \in M \Rightarrow$

$$A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \quad B = \begin{pmatrix} c & d \\ -\bar{d}, & \bar{c} \end{pmatrix}.$$

$$A - B = \begin{pmatrix} a-c & b-d \\ -(\overline{b-d}) & \overline{a-c} \end{pmatrix} \in M.$$

$$A \cdot B = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}\begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix} = \begin{pmatrix} ac-b\bar{d} & ad+b\bar{c} \\ \overline{-ad+b\bar{c}} & \overline{ac-b\bar{d}} \end{pmatrix}$$

$\in M$.

3). $(R, +, \cdot)$ inel.

Def: O submulțime nevidă $\emptyset \neq I \subseteq R$ s.n. ideal la stânga (respectiv la dreapta) dacă:

i). $(\forall)\ x, y \in I$, $x - y \in I$

ii) $(\forall)\ x \in I, r \in R$, $rx \in I$. $(xr \in I)$

$(R, +, \cdot)$

$x \in R$ s.n idempotent daca $x^2 = x$.

R s.n inel Boolean daca $(\forall) x \in R$, $x^2 = x$.

Ex 1) Arătați că $|Idem(\mathbb{Z}_n)| = 2^k$ unde

$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

Surjectivitate

$A = p_{i_1}^{\alpha_1} \dots p_{i_k}^{\alpha_n}$

Luăm $x = Al$ și vreau ca $Al \equiv 1 \pmod{\frac{n}{A}}$,

dar $\left(A, \frac{n}{A}\right) = 1 \Rightarrow A$ inversabil cu $\mathbb{Z}_{\frac{n}{A}} \Rightarrow \exists\, l$ gata.

$B = p_{j_1} \dots p_{j_{n-k}}$

$(A, B) = 1 \Rightarrow (\exists) \alpha, \beta \in \mathbb{Z}$ a.î.

$\alpha A + \beta B = 1$

$\hat{x} = \alpha \hat{A}$.

$x^{\#} = (-1)x \in M$

Din cele de mai sus $(M,+)$ grup abelian

Parte stabilă:

Fie $x, y \in M$.

$$x \cdot y = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix} \in M$$

Asoc.

Fie $x, y, z \in M$.

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$, din

prop. produsului.

Distributivitate

Fie $x, y, z \in M$.

$$x \cdot (y+z) = xy + xz.$$

$$(y+z)x = yx + zx$$

din prop. înm.

$(\mathbb{Z}_p, +, *_a)$.

$\hat{1} * \hat{1}_a = \hat{a}$. cu $a \in \overline{1, p-1}$.

$f : (\mathbb{Z}_p, +, \cdot) \to (\mathbb{Z}_p, +, \underset{a}{*})$

$a \neq 0$.

$f(\hat{x}) = \widehat{a^{-1}x}$

$f(\hat{x}+\hat{y}) = \cancel{\widehat{ax} + \widehat{ay}}$ $\widehat{a^{-1}(x+y)} = \widehat{a^{-1}x} + \widehat{a^{-1}y} =$

$= f(\hat{x}) + f(\hat{y})$

$f(\widehat{x \cdot y}) = \cancel{\widehat{ax \cdot ay}}$ $\cancel{\widehat{axy} =}$

~~$= x *_a y =$~~

$= \widehat{a^{-1}xy} = \widehat{a \, a^{-1}x \, a^{-1}y} = \widehat{a(a^{-1}x \cdot a^{-1}y)}$

$= \widehat{a^{-1}x} * \widehat{a^{-1}y} = f(\hat{x}) \cdot f(\hat{y})$

f inj. $\Leftrightarrow$ $(\forall)$ $x, y \in \mathbb{Z}_p$ cu $f(x) = f(y)$

avem $x = y$

$f(x) = f(y) \Rightarrow \widehat{a^{-1}x} = \widehat{a^{-1}y} \Rightarrow \hat{x} = \hat{y} \Rightarrow$

f inj.

$$x(y+z) = \begin{pmatrix} a_1 & b_1 \\ \hat{0} & c_1 \end{pmatrix}\left(\begin{pmatrix} a_2 & b_2 \\ \hat{0} & c_2 \end{pmatrix}+\begin{pmatrix} a_3 & b_3 \\ \hat{0} & c_3 \end{pmatrix}\right)$$

...

2) Să se determine numărul structurilor neizomorfe de inel care pot fi definite pe o mulțime cu p elemente, unde p e nr. prim.

Orice grup cu exact p elemente este izomorf cu $(\mathbb{Z}_p, +)$

Prin urmare căutăm structurile de inel def. pe $\mathbb{Z}_p$.

Fie „$*$" $: \mathbb{Z}_p^2 \to \mathbb{Z}_p$

„$*$" asoc și distributivă față de adunare

$\mathbb{Z}_p = \langle \hat{1} \rangle$ e suficient să definim operația algebrică „$*$" pt $\hat{1} * \hat{1} = \hat{a} \in \mathbb{Z}_p$

$\hat{x}, \hat{y} \in \mathbb{Z}_p$. $\hat{x} * \hat{y} = \widehat{xya}$

$\hat{x} = \underbrace{\hat{1} + \hat{1} + \dots + \hat{1}}_{x \text{ ori}}$

$\hat{y} = \underbrace{\hat{1} + \dots + \hat{1}}_{y \text{ ori}}$

În plus dacă R_1 și R_2 sunt inele unitare

$f(1_{R_1}) = 1_{R_2}$

Ex 1: Să se arate că mulțimea

$$M = \left\{ \begin{pmatrix} a & b \\ \hat{0} & c \end{pmatrix} \middle| a, b, c \in \mathbb{Z}_p \right\}$$ este

inel în rap. cu adunarea și înmulțirea matricilor

Fie $X, Y \in M$.

$$X+Y = \begin{pmatrix} a & b \\ \hat{0} & c \end{pmatrix} + \begin{pmatrix} d & e \\ \hat{0} & f \end{pmatrix} = \begin{pmatrix} a+d & b+e \\ \hat{0} & c+f \end{pmatrix} \in M$$

$\Rightarrow M$ parte stabilă în rap cu $+$.

Asociativitatea și comutativitatea se obțin din proprietățile matricilor. $(M_2(\mathbb{Z}_p), +)$

<u>El. neutru</u>

$(\exists) E \in M$ $(\forall)$ $X \in M$ a.î.

$X + E = E + X = X$.

$$E = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix} = O_2 \in M.$$

<u>El. simetrizabile</u>

$(\forall) X \in M$ $\exists X' \in M$ a.î. $X + X' = X' + X = E$

Fie $\hat{y} \in \mathbb{Z}_p$.

$\Rightarrow f(\hat{x}) = \hat{y} \Leftrightarrow \hat{a}^{-1} x = \hat{y}$

$\hat{x} = \widehat{ay}$,

$\Rightarrow f$ bij. $\Rightarrow$ cl

3) Câte structuri de inel unitar pe $(\mathbb{Z}_p, +)$ există.

$\hat{x} + \hat{y} = \widehat{axy}$

$(\mathbb{Z}_n, +, *)$ unitar $\Leftrightarrow \hat{a}$ inversabil

4) Să se determine endomorfismele unitare ale lui $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$.

$f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ morfism de grupuri

$f(x) = f(\underbrace{1 + 1 + \ldots + 1}_{x \text{ ori}}) = \underbrace{f(1) + \ldots + f(1)}_{x \text{ ori}}$

$= x f(1)$.

$\Rightarrow$ Endomorfismele f sunt de forma $k \cdot x$

Pp ca avem $\left(\frac{\mathbb{Q}}{\mathbb{Z}}, +, *\right)$ inel integr.

$\Rightarrow \exists \frac{n}{m} \in \mathbb{Q}$ a.î. $\widehat{\frac{n}{m}}$ el. neutru în

$\frac{\mathbb{Q}}{\mathbb{Z}}$ față de $*$.

$$\widehat{\frac{n}{m}} = \widehat{n \cdot \frac{1}{m}} = \hat{n} \cdot \widehat{\frac{1}{m}} = \hat{0} \Rightarrow$$

$\Rightarrow \frac{n}{m}$

$\in \mathbb{R}\}$ $\Rightarrow$ ~~$f(\alpha)=x$~~

$$\left.\begin{array}{l} \left.\begin{array}{l} x \leq \alpha \\ x \leq f(\alpha) \\ f \nearrow \end{array}\right| \Rightarrow \alpha \leq f(\alpha) \\ \\ \left.\begin{array}{l} x_0 \geq \alpha \\ f(\alpha) \geq x_0 \\ f \nearrow \end{array}\right| \Rightarrow \alpha \geq f(\alpha) \end{array}\right\} \Rightarrow f(\alpha)=\alpha$$

Fie $(R,+,\cdot)$ inel.

$U(R)=\{a\in R \mid a^{-1}\in R\}$

mulțimea el. inversabile din R.

$D(R)=\{a\in R \mid \exists\, b\in R$ a.î. $a\cdot b=0$ sau $b\cdot a=0\}$

$\mathcal{N}(R)=\{a\in R \mid \exists\, k\in \mathbb{N}^*$ a.î. $a^k=0\}$

Ex 5) Calculați $U(\mathbb{Z}_n)$, $D(\mathbb{Z}_n)$, $\mathcal{N}(\mathbb{Z}_n)$.

$U(\mathbb{Z}_n)=\{\hat{a} \mid (a,n)=1\}$

$D(\mathbb{Z}_n)=\{\hat{a} \mid \exists\, \hat{b}\in\mathbb{Z}_n$ a.î. $\hat{a}\hat{b}=\hat{0}\}$

$\mathcal{N}(\mathbb{Z}_n)$.

Idealul I s.n. bilateral dacă I este ideal și la stânga și la dreapta.

Not $\trianglelefteq$

$2\mathbb{Z} \subset \mathbb{Z}$.

$\mathbb{Q} \subseteq \mathbb{R}$ subinel, dar nu e ideal.

Ex. Fie $(R,+,\cdot)$ inel comutativ. Arătați că orice ideal bilateral al lui $M_2(R)$ e de forma

$$M_2(I), \ I \trianglelefteq R.$$

$$J = \left\{\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \middle| a, b \in R\right\} \leq I \text{ la stânga}$$

nu la dreapta.

Fie $A, B \in J$

$$A - B = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} - \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & a-c \\ 0 & b-d \end{pmatrix} \in J$$

ii) Fie $A = J$.

$R \in M_2(R)$.

$$A R = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} 0 & al \\ bk & bl \end{pmatrix}$$

$$RA = \begin{pmatrix} i & j \\ k & l \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & j\cdot b \\ 0 & ka+bl \end{pmatrix}$$

$M_2(I) \trianglelefteq M_2(R)$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(I)$

$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \in M_2(R)$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} ax+bz & \\ & \dots \end{pmatrix} \in M_2(R)$

Fie $A \ntrianglelefteq R$

$\Rightarrow \exists\, a \in A,\ r \in R$ ai. $aR \notin A$

$X = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in M_2(A)$

$Y = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \in M_2(R)$

$XY = \begin{pmatrix} \overset{\notin A}{ar} & 0 \\ 0 & ar \end{pmatrix} \in M_2(A)$. (dupto)

~~$f(1)=0$~~

Fie $f:(\mathbb{Z},+,\cdot)\to(\mathbb{Z},+,\cdot)$ morf de inele

$f(x)=k\cdot x$, $k\in\mathbb{Z}$

$f(1)=1$

$f(1)=k$ $\Rightarrow k=1$

$\Rightarrow f(x)=x$

$f(x\cdot y)=xy=f(x)\cdot f(y)$

$f(x+y)=f(x)+f(y)$ $\Rightarrow$ morfism

$End(\mathbb{Z})=\{id_{\mathbb{Z}}\}$

$f\left(\frac{p}{q}\right)=f\left(\frac{1}{q}+\frac{1}{q}+\dots+\frac{1}{q}\right)=f\left(\frac{1}{q}\right)+\dots+f\left(\frac{1}{q}\right)$

$=$ ~~$\frac{p}{q}f($~~ $p\,f\left(\frac{1}{q}\right)$

$f(p)=f(p\cdot$ $=p f(1)$

$f(p)=f\left(\frac{p}{q}\cdot q\right)=q\left(f\left(\frac{p}{q}\right)\right)$

$pf(1)=qf\left(\frac{p}{q}\right)\Rightarrow f\left(\frac{p}{q}\right)=\frac{p}{q}f(1)$

$p = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ (euclid).

$\mathcal{N}(\mathbb{Z}_n) = \{ \hat{a} \in \mathbb{Z}_n \mid a = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} \in \mathbb{Z}_n \}$

cu $\beta_1 \beta_2 \ldots \beta_k \in \mathbb{Z}_{\ldots}$

$= p_1 p_2 \ldots p_k \mathbb{Z}$.

Dem prin dublă incluziune...

$(\mathbb{Z}_n + \cdot)$

$U(\mathbb{Z}_n) = \{ \hat{a} \mid (a, n) = 1 \}$.

$|U(\mathbb{Z}_n)| = \varphi(n)$.

$D(\mathbb{Z}_n) = \mathbb{Z}_n \setminus U(\mathbb{Z}_n)$. $|D(\mathbb{Z}_n)| = n - \varphi(n)$

$\mathcal{N}(\mathbb{Z}_n) = \widehat{p_1 \ldots p_k} \mathbb{Z}_n$

unde $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$

$|\mathcal{N}(\mathbb{Z}_n)| = p_1^{\alpha_1 - 1} \ldots p_k^{\alpha_k - 1}$.

$Idem(\mathbb{Z}_n) = \{ \hat{a} \in \mathbb{Z}_n \mid \hat{a}^2 = \hat{a} \}$

$\hat{x}$ idempotent dacă $\hat{x}^2 = \hat{x}$.

$$\hat{x}^2 = \hat{x}. = \hat{0}$$

$$= \hat{x}(\hat{x}-\hat{1}) = \alpha\hat{A}(\hat{1}-\beta\hat{B}) = \cancel{\alpha\hat{A}} - \alpha\beta\widehat{AB}$$

$$\underbrace{\cancel{\alpha\hat{A}}}\ -\cancel{\alpha\hat{A}}-\beta\hat{B}$$

$= \cancel{\alpha\hat{A}} = \hat{0}$.

$\alpha\beta\hat{n}$

$\equiv$

n.

$A = p_{i_1}^{\alpha_{i_1}} \cdots p_{i_k}^{\alpha_{in}}$ and $p_i \mid \alpha A \Rightarrow$

$\Rightarrow \{i_1 \ldots i_k\} \subseteq f(\alpha\hat{A})$.

Dacă $p_i \mid \alpha A$ și $p_i \nmid A \Rightarrow p_i \mid \alpha$

$p_i \mid \alpha$

Din $\alpha A + \beta B = 1$ $\Rightarrow$

$p_1 \mid 1$ $\times 0$

36	2
18	2
9	3
3	3
1	

0, 1.

$36 = 2^2 \cdot 3^2$.

$7 \cdot 7 = 49 - 36$.

$12 \cdot 12 = 144$.