CURS 9 — 08.05.2018

Inele și corpuri

Def Fie R o mulțime și $+,\cdot$ două operații pe R. Spunem că $(R,+,\cdot)$ este un inel dacă: i) $(R,+)$ grup abelian
ii) $(R,\cdot)$ semigrup
iii) „$\cdot$" este distributivă față de „$+$":
$\forall a,b,c\in R$, $a(b+c)=ab+ac$
$(b+c)\cdot a=ba+ca$

Dacă $(R,\cdot)$ este monoid, spunem că inelul este cu unitate
Dacă „$\cdot$" e comutativă, spunem că $(R,+,\cdot)$ e un inel comutativ

Notații:
0 = elementul neutru față de „$+$"
1 = elementul neutru față de „$\cdot$" (dacă $\exists$)

Def: Spunem că inelul $(R,+,\cdot)$ este un corp dacă:
$(R\setminus\{0\},\cdot)$ este un grup.

Exemple:
1) $(\mathbb{N},+,\cdot)$ nu formează un inel pt. că $(\mathbb{N},+)$ nu e grup abelian
2) $(\mathbb{Z},+,\cdot)$ inel comutativ cu unitate
3) $(2\mathbb{Z},+,\cdot)$ inel comutativ fără unitate
4) $(\mathcal{M}_n(R),+,\cdot)$ inel care e necomutativ dacă $n\geq 2$
Obs: Toate inelele de mai sus nu sunt corpuri (la 4) pt. $n\geq 2$)
5) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ – corpuri comutative
6) Fie $\mathbb{Q}=\{\pm 1,\pm i,\pm j,\pm k\}$ (grupul cuaternionilor)
$i^2=j^2=k^2=-1$
$i\cdot j=k$, $jk=i$, $ki=j$
$j\cdot i=-k$, $kj=-i$, $ik=-j$

Notăm cu $\underline{\mathbb{Q}}$ mulțimea combinațiilor liniare formale:
$$\underline{\mathbb{Q}}=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{R}\}$$ cu operațiile „$+$" și „$\cdot$" definite în mod natural a.î. „$\cdot$" este distributivă față de „$+$"

$$\left.\begin{aligned} q&=a+bi+cj+dk\\ q'&=a'+b'i+c'j+d'k\end{aligned}\right\}\Rightarrow \begin{aligned} q+q'&=a+a'+(b+b')i+(c+c')\cdot j+(d+d')\cdot k\\ q\cdot q'&=(aa'-bb'-cc'-dd')+(ab'+b\cdot a'+cd'-d\cdot c)\cdot i+\\ &+(ac'+ca'+db'-bd')\cdot j+(ad'+da'+bc'-cb')\cdot k\end{aligned}$$

$(\underline{\mathbb{Q}},+,\cdot)$ este un corp necomutativ, numit corpul cuaternionilor. (cel mai simplu corp necomutativ)

Reguli de calcul în inele:
Fie $(R,+,\cdot)$ inel, $a,b,c\in R$
a) $a\cdot 0=0\cdot a=0$
b) $a\cdot(-b)=(-a)\cdot b=-(ab)$
c) $(-a)(-b)=a\cdot b$
d) $a\cdot(b-c)=ab-ac$
$(b-c)\cdot a=ba-ca$
e) $m,n\in\mathbb{Z}$ $(ma)(nb)=(mn)(ab)$
$ma=\underbrace{a+\dots+a}_{m\text{ ori}}$
f) $m,n\in\mathbb{N}^*$, $a^m\cdot a^n=a^{m+n}$
g) Dacă $\exists\, 1\in R\to a^0=1$
h) Dacă $ab=ba$, $n\in\mathbb{N}^*\Rightarrow (a\cdot b)^n=a^n\cdot b^n$

Dem:

Exemple
$n \in \mathbb{N}$, $n \geq 2 \Rightarrow (\mathbb{Z}_n, +, \cdot)$ inel cu unitate comutativ
$\hat{x} + \hat{y} = \widehat{x+y}$
$\hat{x} \cdot \hat{y} = \widehat{x \cdot y}$
elementul neutru față de $+$ = $\hat{0}$
elementul neutru față de $\cdot$ = $\hat{1}$
$n=6$: $\hat{2} \cdot \hat{3} = \hat{0}$
$n=8$: $\hat{2}^3 = \hat{0}$

Def: Spunem că un inel $(R, +, \cdot)$ este fără divizori ai lui 0 dacă
dacă $x, y \in R$, $xy = 0 \Rightarrow x = 0$ sau $y = 0$

Def: Spunem că un inel $(R, +, \cdot)$ e un domeniu de integritate dacă R este comutativ, cu unitate și este fără divizori ai lui 0.

Ex: 1) $(\mathbb{Z}, +, \cdot)$ domeniu de integritate
2) $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ domeniu de integritate față de operațiile obișnuite de „+" și „·"
↓ domeniul întregilor lui Gauss.
3) Orice corp comutativ este un domeniu de integritate.

Dem: Fie $(K, +, \cdot)$ corp comutativ $\Rightarrow (K \setminus \{0\}, \cdot)$ grup $\Rightarrow$
$\Rightarrow$ i) $\exists\, 1 \in K \setminus \{0\}$ elem. neutru față de „·"
ii) $\forall\, a \in K \setminus \{0\}$, $\exists\, a^{-1} \in K \setminus \{0\}$ a.î. $a \cdot a^{-1} = 1$
$1 \cdot 0 = 0$
i) $\Rightarrow 1$ e element neutru în $(K, \cdot)$
$\Rightarrow K$ are unitate
Fie $a, b \in K$ a.î. $a \cdot b = 0$
Pp. că $b \neq 0 \Rightarrow \exists\, b^{-1} \in K \Rightarrow a = a \cdot 1 = a \cdot b \cdot b^{-1} = 0 \cdot b^{-1} = 0$
$\Rightarrow K$ nu are divizori ai lui 0
$\Rightarrow (K, +, \cdot)$ domeniu de integritate.

Teoremă
Dacă $(R, +, \cdot)$ este un inel cu unitate finit și fără divizori ai lui 0, atunci el este un corp.
Dem:
Fie $a \in R \setminus \{0\}$. Notăm cu $t_a : R \to R$, $t_a(x) = ax$
Pp. că $x, y \in R$ a.î. $t_a(x) = t_a(y) \Rightarrow ax = ay \Rightarrow ax - ay = 0 \Rightarrow a(x-y) = 0$
$a \neq 0$, R nu are divizori ai lui 0 $\Rightarrow x - y = 0 \Rightarrow x = y$
$\Rightarrow t_a$ injectivă, R finită $\Rightarrow t_a$ surjectivă $\Rightarrow \exists\, a' \in R$ a.î. $a \cdot a' = 1$
Analog, folosind funcția $t'_a : R \to R$, $t'_a(x) = x \cdot a \Rightarrow \exists\, a'' \in R$ a.î. $a'' \cdot a = 1$
$\Rightarrow a' = 1 \cdot a' = (a'' \cdot a) a' = a'' \cdot (a \cdot a') = a'' \cdot 1 = a''$
$\Rightarrow \exists\, a^{-1} = a' = a''$ a.î. $a \cdot a^{-1} = a^{-1} \cdot a = 1$
$\Rightarrow (R, +, \cdot)$ corp.

Convenție: Atunci când vorbim despre inele cu unitate presupunem automat că $1 \neq 0$ (inele cu cel puțin 2 elemente)

Corolar:
Orice domeniu de integritate finit este un corp.

Corolar
Fie $n \in \mathbb{N}$, $n \geq 2$. Următoarele afirmații sunt echivalente:
a) n - prim
b) $\mathbb{Z}_n$ - domeniu de integritate

Dem:

b(⇒ c) din rezultatele anterioare

a) ⇒ b)

Fie $\hat{x},\hat{y}\in\mathbb{Z}_n$ a.î. $\hat{x}\cdot\hat{y}=\hat{0} \Rightarrow x\hat{y}=\hat{0} \Rightarrow n \mid xy$, n prim $\Rightarrow n\mid x$ sau $n\mid y$

$\hat{x}=\hat{0}$ sau $\hat{y}=\hat{0}$

$\Rightarrow \mathbb{Z}_n$ domeniu de integritate

b) ⇒ a)

Pp. că n-nu e prim $\Rightarrow \exists\, x,y\in\{1,2,\dots,n-1\}$ a.î. $n=xy \Rightarrow$

$\Rightarrow \exists\, \hat{x},\hat{y}\in\mathbb{Z}_n\setminus\{\hat{0}\}$ a.î. $\hat{0}=\hat{n}=x\hat{y}=\hat{x}\cdot\hat{y}$

$\Rightarrow \mathbb{Z}_n$ are divizori ai lui 0 $\Rightarrow \mathbb{Z}_n$ nu este domeniu de integritate

$\Rightarrow$ contradicție !

$\Rightarrow$ p - nr prim

Def: Fie $(R,+,\cdot)$ și $(A,+,\cdot)$ 2 inele. Spunem că o funcție $f: R\to A$ este un morfism de inele dacă:

a) $\forall\, x_1,x_2\in R : f(x_1+x_2)=f(x_1)+f(x_2)$

b) $\forall\, x_1,x_2\in R : f(x_1\cdot x_2)=f(x_1)\cdot f(x_2)$

Dacă f este și bijectivă, spunem că f e un izomorfism de inele

Dacă R și A sunt inele cu unitate și f e un morfism a.î. $f(1_R)=1_A$, atunci f s.n. morfism de inele unital.

Exemple:

1) $f:\mathbb{Z}\to\mathbb{Z}_n$, $f(x)=\hat{x}$ morfism de inele unital

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

$f:\mathbb{Z}[i]\to A$, $f(a+bi)=\begin{pmatrix} a & b\\ -b & a\end{pmatrix}$ izomorfism de inele

Proprietate

Dacă $(R,+,\cdot)$ și $(A,+,\cdot)$ sunt inele cu unitate și $f:R\to A$ este un izomorfism de inele, atunci f este unital

Dem: temă

Exemplu

Inelele $(\mathbb{Z},+,\cdot)$ și $(\mathbb{Z}[i],+,\cdot)$ nu sunt izomorfe

Pp că $\exists\, f:\mathbb{Z}\to\mathbb{Z}[i]$ izomorfism

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

f bijectivă $\Rightarrow \exists\, a\in\mathbb{Z}$ a.î. $f(a)=i \Rightarrow f(a^2)=i^2=-1$

} $\overset{f\text{ inj}}{\Longrightarrow} -1=a^2$ contradicție

$\Rightarrow (\mathbb{Z},+,\cdot)\not\cong(\mathbb{Z}[i],+,\cdot)$

Def: Fie $(R,+,\cdot)$ inel și $S\subseteq R$. Dacă S este stabilă față de „+" și „·", $(S,+,\cdot)$ formează un inel, spunem că S este un subinel al lui R.

- Dacă R are unitate ($\mu\neq 1$) și $1\in S$, spunem că S este un subinel unital (cu unitate)
- Dacă R corp și S este un subinel, a.î. $(S,+,\cdot)$ este corp, atunci spunem că S este subcorp al lui R.

Obs. Subcorpurile sunt automat unitale.

Teoremă

Fie $(R,+,\cdot)$ inel și $S\subseteq R$. Următoarele afirmații sunt echivalente:

a) S subinel în R

b) i) $0\in S$

ii) $\forall\, x,y\in S$, $x-y\in S$

iii) $\forall\, x,y\in S$, $x\cdot y\in S$

Teoremă
Fie $(K,+,\cdot)$ corp și $S \subseteq K$. Următoarele afirmații sunt echivalente:
a) S subcorp în K
b) i) $0,1 \in S$
ii) $\forall x,y \in S$, $x-y \in S$
iii) $\forall x,y \in S$ cu $y \neq 0$: $x \cdot y^{-1} \in S$

Exemple:
Fie $R = \mathcal{M}_2(\mathbb{R})$, $(R,+,\cdot)$ inel
a) $T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R} \right\}$ - subinel cu unitate

b) $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$ - subinel care nu este unitar ($pt.$ că $I_2 \notin S$)
Dar $(S,+,\cdot)$ este inel cu unitate
el are unitatea $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

c) $U = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{R} \right\}$ - subinel
$\forall X, Y \in U$: $X \cdot Y = 0$ (inel de pătrat nul)

d) $V = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a,b \in \mathbb{R} \right\}$ - subinel cu unitate în R
$(V,+,\cdot)$ inel comutativ

15.05.2018

CURS 10

Morfisme de inele. Ideale. Inele factor

Def: Fie $(R,+,\cdot)$ și $(S,+,\cdot)$ 2 inele. Spunem că o funcție $f: R \to S$ este un morfism de inele dacă: $\forall x,y \in R$: $f(x+y) = f(x) + f(y)$
$f(x \cdot y) = f(x) \cdot f(y)$

Dacă f e un morfism bijectiv, atunci spunem că f e un izomorfism și că inelele R și S sunt izomorfe. (notăm $R \simeq S$)

Dacă R și S sunt unitare și $f(1_R) = 1_S$ spunem că f e un morfism de inele unitar

Dacă R și S sunt corpuri și f e un morfism unitar spunem că f e un morfism de corpuri.

Dacă $f: R \to R$ este un morfism, spunem că f e un endomorfism.
Dacă $f: R \to R$ este un izomorfism, spunem că f e un automorfism.

Exemple:
1) $f: R \to \{0\}$ $f(x) = 0$, $\forall x \in R$ morfism de inele care nu e unitar

2) $1_R: R \to R$ $1_R(x) = x$, $\forall x \in R$ e un automorfism

3) S subinel al lui $R \Rightarrow$ aplicația de incluziune $i_S: S \to R$, $i_S(x) = x$, $\forall x \in S$ este un morfism de inele. El poate să nu fie unitar, chiar dacă R și S sunt inele cu unitate (dacă $1_S \neq 1_R$)

4) $f: \mathbb{C} \to M_2(\mathbb{R})$, $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ morfism de inele unitar

5) $C = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,b \in \mathbb{R} \right\} \Rightarrow (C,+,\cdot)$ corp și $f: \mathbb{C} \to C$, $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ este un izomorfism de corpuri.

6) $f: \mathbb{C} \to \mathbb{C}$, $f(z) = \bar{z}$ automorfism al lui $(\mathbb{C},+,\cdot)$

Th.: Fie $f: R \to S$ morfism de inele:
a) $\Rightarrow$ $f: (R,+) \to (S,+)$ morfism de grupuri, deci