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

c) Dacă R și S au unitate și f e un izomorfism, atunci: $f(1)=1$ (adică f e unital)

Propoziție
Fie $f: R \to S$ un morfism de inele
a) Dacă H - subinel al lui $R \Rightarrow f(H)$ subinel în S
b) Dacă L - subinel al lui $S \Rightarrow f^{-1}(L)$ subinel în R
c) $\ker f = \{x \in R, f(x)=0\}$ - subinel al lui R
d) f e injectivă $\Leftrightarrow \ker f = \{0\}$
e) compusa a 2 morfisme este morfism.
f) Dacă f izomorfism $\Rightarrow f^{-1}: S \to R$ e un izomorfism

Def Fie $(R,+,\cdot)$ un inel și $I \subseteq R$.
Spunem că I e un ideal (bilateral) al lui R dacă:
i) I e subinel în R
ii) $\forall x \in I, \forall h \in R, x \cdot h \in I$ și $h \cdot x \in I$

Exemple
1) $(\mathbb{Z},+,\cdot)$, $I = k\mathbb{Z}$, $k \in \mathbb{N}$, fixat
$\Rightarrow I$ este ideal

2) $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R} \right\}$, $I = \left\{ \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{R} \right\}$
I subinel în R
Fie $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R$, $X = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \in I$

$A \cdot X = \begin{pmatrix} 0 & a \cdot x \\ 0 & 0 \end{pmatrix} \in I$

$X \cdot A = \begin{pmatrix} 0 & x \cdot c \\ 0 & 0 \end{pmatrix} \in I$

Deci, I e un ideal în R

$J = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x,y \in \mathbb{R} \right\}$, J subinel în R

$Y = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$

$A \cdot Y = \begin{pmatrix} ax & ay \\ 0 & 0 \end{pmatrix}$, $Y \cdot A = \begin{pmatrix} ax & bx+ay \\ 0 & 0 \end{pmatrix}$

Deci, J e ideal

$S = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{R} \right\}$ - nu este ideal

Prop: Dacă I e un ideal în R și $\exists u \in I$ inversabil, atunci $I = R$
Dem:
$u \in I$ inversabil $\Rightarrow \exists u^{-1} \in R$
$\left.\begin{matrix} u \in I \\ u^{-1} \in R \end{matrix}\right\} \overset{I \text{ ideal}}{\Rightarrow} u \cdot u^{-1} \in I \Rightarrow 1 \in I$
Fie $x \in R$, $1 \in I$ $\Rightarrow x = x \cdot 1 \in I \Rightarrow R \subseteq I$; $I \subseteq R$ $\Rightarrow I = R$

Teoremă
Fie $(R,+,\cdot)$ inel comutativ cu unitate. Următoarele afirmații sunt echivalente:
a) R - corp
b) Dacă I e un ideal în $R \Rightarrow I = \{0\}$ sau $I = R$
Dem:
a) $\Rightarrow$ b) R corp
Fie I un ideal în R cu $I \neq \{0\} \Rightarrow \exists u \in I, u \neq 0$ ($u \in R$ corp) $\Rightarrow u$ inversabil $\overset{\text{Prop.}}{\Rightarrow} I = R$

b) ⇒ a)

Fie $u \in R$ cu $u \neq 0$

Fie $I = u \cdot R = \{ u \cdot x \mid x \in R \}$

$0 = u \cdot 0 \in I$

$a_1, a_2 \in I \Rightarrow \exists\, x_1, x_2 \in R$ a.î. $\begin{cases} a_1 = u x_1 \\ a_2 = u x_2 \end{cases} \Rightarrow \begin{cases} a_1 - a_2 = u(x_1 - x_2) \in I \\ a_1 \cdot a_2 = u(x_1 \cdot u \cdot x_2) \in I \end{cases}$

$\Rightarrow I$ este subinel

Fie $a \in I$ și $r \in R$

$a \in I \Rightarrow \exists\, x \in R$ a.î. $a = u \cdot x \Rightarrow a \cdot r = u(x \cdot r) \in I$

$r \cdot a \overset{\text{com.}}{=} a \cdot r \in I$

$\Rightarrow I$ e un ideal

$\left.\begin{matrix} u = u \cdot 1 \in I \\ u \neq 0 \end{matrix}\right\} \Rightarrow I \neq 0 \overset{b)}{\Longrightarrow} I = R \Rightarrow 1 \in I \Rightarrow \exists\, x \in R$ a.î. $1 = u \cdot x = x \cdot u \Rightarrow \exists\, u^{-1} \in R$

$\Rightarrow \forall\, u \in R^*, \exists\, u^{-1} \in R \Rightarrow R$ corp

Obs În teorema anterioară, condiția „R e comutativ" este esențială.

$\exists$ inele necomutative R - care nu sunt corpuri și care au proprietatea de la b)

Exemplu: $M_n(K)$ cu $n \geq 2$, K - corp comutativ

Există o variantă a teoremei și pt. cazul general, dar aceasta folosește ideale unilaterale

Teoremă

Fie $(R, +, \cdot)$ inel și $I \subseteq R$ un ideal. Atunci:

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

b) Operația $\cdot : R/_I \times R/_I \longrightarrow R/_I$

$(r_1 + I)(r_2 + I) = r_1 r_2 + I$ este bine definită.

c) $(R/_I, +, \cdot)$ inel

d) $p_I : R \longrightarrow R/_I$, $p_I(r) = r + I$ morfism de inele surjectiv

Dem: similară cu cea de la grupuri factor.

Def: Inelul $(R/_I, +, \cdot)$ s.n. INELUL FACTOR INDUS DE I.

Obs: Operația + pe $R/_I$ este operația grupului factor $(R/_I, +)$:

$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$

Exemplu:

$R = \mathbb{Z}$, $I = n\mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$

$R/_I = \mathbb{Z}/_{n\mathbb{Z}} = \{ k + n\mathbb{Z} \mid k \in \mathbb{Z} \}$, $k + n\mathbb{Z} = l + n\mathbb{Z} \Leftrightarrow l - k \in n\mathbb{Z} \Leftrightarrow$ k și l dau același rest prin împărțire la n

$\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n = \{ \hat{0}, \hat{1}, \ldots, \widehat{n-1} \}$, $\hat{i} = i + n\mathbb{Z}$

$\hat{i} + \hat{j} = (i + n\mathbb{Z}) + (j + n\mathbb{Z}) = (i + j) + n\mathbb{Z} = \widehat{i + j}$

$i \cdot j = (i + n\mathbb{Z}) \cdot (j + n\mathbb{Z}) = (i \cdot j) + n\mathbb{Z} = \widehat{i \cdot j}$

$\Rightarrow (\mathbb{Z}_n, +, \cdot)$ - inelul factor al lui $\mathbb{Z}$ indus de idealul $n\mathbb{Z}$

Teoremă (prima teoremă de izomorfism)

Fie $f : R \to S$ un morfism de inele. Atunci:

a) $\ker(f)$ e un ideal al lui R

b) funcția $\bar{f} : R/_{\ker(f)} \longrightarrow f(R)$, $\bar{f}(r + \ker(f)) = f(r)$ e bine definită și e un izomorfism de inele.

Dem: (temă)

Teorema (a II-a de izomorfism)
Fie R un inel, $S \leq R$ subinel și $I \leq R$ un ideal
a) $S+I = \{s+i \mid s \in S, i \in I\}$ formează un subinel al lui R
b) I este ideal în $S+I$ și $S \cap I$ este ideal în S
c) $\frac{S+I}{I} \simeq \frac{S}{S \cap I}$

Teorema (a III-a de izomorfism)
Fie $(R,+,\cdot)$ inel, I, J ideale în R a.î. $I \leq J$. Atunci:
J/I e ideal în R/I și $\frac{(R/I)}{(J/I)} \simeq \frac{R}{J}$

Exemple:
$R = \mathbb{Z}$, $I = n\mathbb{Z}$, $S = m\mathbb{Z}$
Teorema a I-a $\Rightarrow \frac{n\mathbb{Z}+m\mathbb{Z}}{n\mathbb{Z}} \simeq \frac{m\mathbb{Z}}{n\mathbb{Z} \cap m\mathbb{Z}}$
$\frac{(m,n)\mathbb{Z}}{n\mathbb{Z}} \simeq \frac{m\mathbb{Z}}{[m,n]\cdot\mathbb{Z}}$
Teorema a II-a: $n\mathbb{Z} \leq m\mathbb{Z} (\Leftrightarrow m \mid n) \Rightarrow$ teoremă

Aplicație (caracteristica unui inel cu unitate)
Fie $(R,+,\cdot)$ inel cu unitatea 1_R.
Definim $f: \mathbb{Z} \to R$, $f(k) = k \cdot 1_R \Rightarrow f$ morfism de inele
$\Rightarrow \ker(f)$ e un ideal în $\mathbb{Z} \Rightarrow \exists n \in \mathbb{N}$ a.î. $\ker(f) = n\mathbb{Z}$
$\Rightarrow \mathbb{Z}/n\mathbb{Z} \simeq \{k \cdot 1_R \mid k \in \mathbb{Z}\}$ (subinel al lui R)
Def: n s.n. caracteristica inelului R

Obs: Dacă $n > 0 \Rightarrow n$ este cel mai mic nr. natural (cel mai mic) cu proprietatea: $n \cdot 1_R = 0$
Dacă $n = 0 \Rightarrow \forall n \in \mathbb{N}^*$, $n \cdot 1_R \neq 0$

Propoziție
Fie R un domeniu de integritate de caracteristică > 0. Atunci caracteristica lui R este un număr prim.
Dem:
Fie p = caracteristica inelului $\Rightarrow p > 0$
Dacă $p = 1 \Rightarrow 1 \cdot 1_R = 0_R \Rightarrow 1_R = 0_R$ contradicție cu $0_R \neq 1_R$
$\Rightarrow p > 1$
Pp. că p nu e prim $\Rightarrow \exists a, b \in \{2, \dots, p-1\}$ a.î. $p = a \cdot b$
$\Rightarrow p \cdot 1_R = (a \cdot b) \cdot 1_R = (a \cdot 1_R) \cdot (b \cdot 1_R)$ și $p \cdot 1_R = 0_R \Rightarrow (a \cdot 1_R) \cdot (b \cdot 1_R) = 0$
$\Downarrow$ R domeniu de integritate
$a \cdot 1_R = 0_R$ sau $b \cdot 1_R = 0_R$
$\Downarrow$ contradicție cu faptul că p e cel mai mic nr. natural (cel mai mic) cu proprietatea că: $p \cdot 1_R = 0_R$
$\Downarrow$
p prim.