Reamintire din și completare la capitolul "Inele și corpuri"

<u>Inel</u>: $(R,+,\cdot)$, unde R este o mulțime înzestrată cu operațiile $+$ și $\cdot$ astfel încât

- $(R,+)$ grup abelian
- $(R,\cdot)$ monoid
- $a(b+c)=ab+ac$, $(b+c)a=ba+ca$ pt. orice $a,b,c\in R$.

Vom presupune că în R avem $0\neq 1$ ($\Leftrightarrow R\neq 0$).

Inelul R s.n. <u>comutativ</u> dacă $ab=ba$ pt. orice $a,b\in R$.

Un element $a\in R$ s.n. <u>inversabil</u> dacă există $b\in R$ cu $ab=ba=1$. În acest caz b este unic determinat și se numește inversul lui a; notație $b=a^{-1}$.

<u>Observație</u>. Dacă $a\in R$ și există $b\in R$ pentru care $ab=1$, atunci a nu este neapărat inversabil (a este doar inversabil la dreapta, iar b este un invers la dreapta al lui a).

<u>Exerciții</u> (1) Să se dea exemplu de un inel R și $a\in R$ care este inversabil la dreapta, dar nu este inversabil.

(2) Dacă $a\in R$ este inversabil la dreapta, dar nu este inversabil, atunci a are o infinitate de inversi la dreapta.

3. Fie R inel și $a,b \in R$. Atunci $1-ab$ este inversabil la dreapta (stânga) $\Leftrightarrow$ $1-ba$ este inversabil la dreapta (stânga).

Un inel R s.n. <u>corp</u> dacă orice $a \in R \setminus \{0\}$ este inversabil.

Dacă R este inel, o submulțime A a lui R se numește <u>subinel</u> dacă: $\begin{cases} A \leq (R,+) \\ a,b \in A \Rightarrow ab \in A \\ 1 \in A \end{cases}$

Dacă R este corp, o submulțime A a lui R se numește <u>subcorp</u> dacă A este subinel și $a^{-1} \in A$, pt. orice $a \in A \setminus \{0\}$.

Dacă R și S sunt inele, atunci $f: R \to S$ este morfism de inele dacă: $\begin{cases} \left.\begin{array}{l} f(a+b) = f(a) + f(b) \\ f(ab) = f(a)f(b) \end{array}\right\} \text{pt. orice } a,b \in R \\ f(1_R) = 1_S \end{cases}$

Dacă R și S sunt corpuri, o funcție $f: R \to S$ se numește morfism de corpuri dacă f este morfism de inele.

Orice morfism de corpuri este injectiv.

Câteva exemple de inele:

1. Inele de numere: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

$\mathbb{Q}$ = corpul de fracții al domeniului de integritate $\mathbb{Z}$ (construcție făcută în sem. I).

$\mathbb{R}$ se construiește din $\mathbb{Q}$ ca mulțimea factor a mulțimii șirurilor Cauchy de numere raționale în raport cu o anumită relație de echivalență (se face cândva la cursul de Analiză)

$\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$; dar cine este i? Și ce sens are bi? Și $a+bi$?

Iată o construcție a lui $\mathbb{C}$, presupunându-l cunoscut pe $\mathbb{R}$.

Pe mulțimea $K = \mathbb{R} \times \mathbb{R}$ definim operațiile $\cdot$ și $+$ prin:

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

$$(a,b)\cdot(c,d)=(ac-bd,ad+bc)$$

pt. orice $a,b,c,d \in \mathbb{R}$.

Atunci $(K,+,\cdot)$ este corp comutativ (Exercițiu!).

În plus, $\mathbb{R}$ se scufundă în K (adică $\mathbb{R}$ este izomorf cu un subcorp al lui K, sau echivalent, există un morfism de corpuri $\varphi: \mathbb{R} \to K$) prin morfismul de corpuri $\varphi: \mathbb{R} \to K$, $\varphi(a)=(a,0)$ pt. orice $a \in \mathbb{R}$.

Notăm $I=(0,1)$. Observăm că

$$I^2=(-1,0)=\varphi(-1)=-\varphi(1), \text{ și}$$

$$(0,b)=(b,0)(0,1)=\varphi(b)\,I \text{ pt. orice } b\in\mathbb{R}.$$

Atunci $(a,b)=(a,0)+(0,b)=\varphi(a)+\varphi(b)I$, de unde

$K=\{\varphi(a)+\varphi(b)I \mid a,b\in\mathbb{R}\}$, cu

$$\varphi(a)+\varphi(b)I=\varphi(c)+\varphi(d)I \iff a=c \text{ și } b=d$$

$$(\varphi(a)+\varphi(b)I)+(\varphi(c)+\varphi(d)I)=\varphi(a+c)+\varphi(b+d)I$$

$$(\varphi(a)+\varphi(b)I)\cdot(\varphi(c)+\varphi(d)I)=\varphi(ac-bd)+\varphi(ad+bc)I$$

pt. orice $a,b,c,d\in\mathbb{R}$.

Dacă notăm $\varphi(a)=\bar{a}$, aceste relații se rescriu:

$$(*)\begin{cases} K=\{\bar{a}+\bar{b}I \mid a,b\in\mathbb{R}\} \\ \bar{a}+\bar{b}I=\bar{c}+\bar{d}I \iff a=c \text{ și } b=d \iff \bar{a}=\bar{c} \text{ și } \bar{b}=\bar{d} \\ (\bar{a}+\bar{b}I)+(\bar{c}+\bar{d}I)=\overline{a+c}+\overline{b+d}\,I=(\bar{a}+\bar{c})+(\bar{b}+\bar{d})I \\ (\bar{a}+\bar{b}I)(\bar{c}+\bar{d}I)=\overline{ac-bd}+\overline{ad+bc}\,I \\ \qquad =(\bar{a}\,\bar{c}-\bar{b}\,\bar{d})+(\bar{a}\,\bar{d}+\bar{b}\,\bar{c})I \end{cases}$$

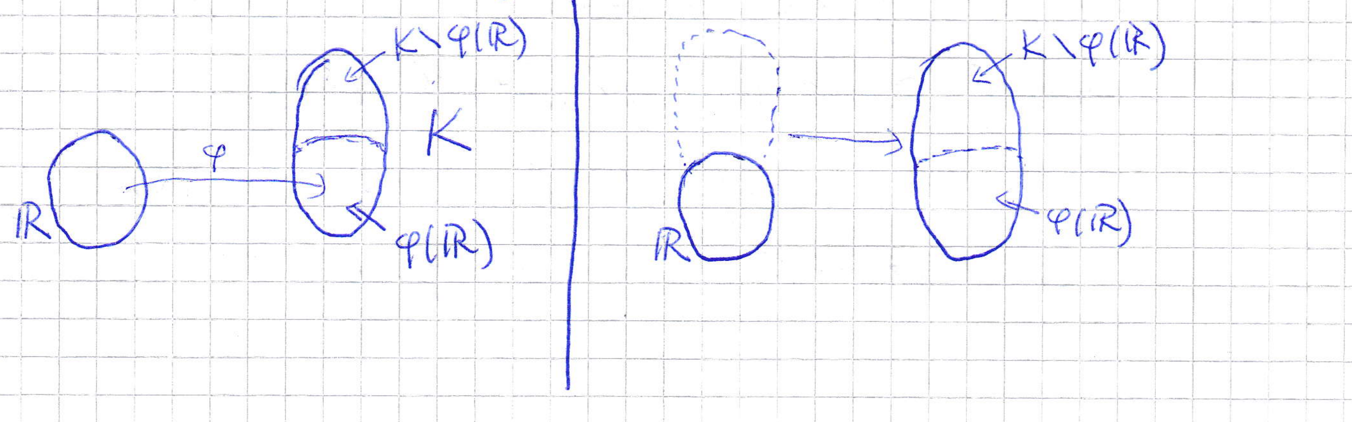
(am folosit $\bar{x}+\bar{y}=\varphi(x)+\varphi(y)=\varphi(x+y)=\overline{x+y}$ și

$\bar{x}\,\bar{y}=\varphi(x)\varphi(y)=\varphi(xy)=\overline{xy}$, deoarece φ este morfism de corpuri).

În plus, avem $I^2=\overline{-1}=-\bar{1}$.

"Identificând" $\mathbb{R}$ cu $\varphi(\mathbb{R})$ (adică a cu $\bar{a}$ pt. fiecare $a \in \mathbb{R}$), obținem descrierea cunoscută a lui $\mathbb{C}$, unde în loc de i am folosit I.
Dar ce înseamnă această identificare?

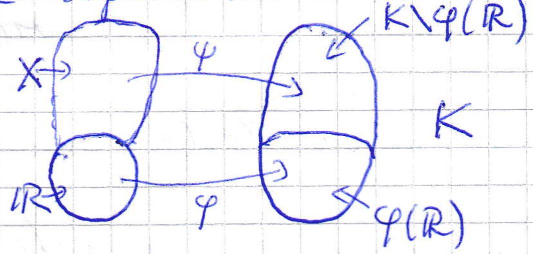
Un prim răspuns este că în loc de corpul $\mathbb{R}$ al numerelor reale folosim corpul $\varphi(\mathbb{R})$, izomorf cu $\mathbb{R}$, deci având aceleași proprietăți (de corp) ca $\mathbb{R}$. Atunci relațiile $(*)$ reprezintă definiția obișnuită a numerelor complexe, cu diferența că în loc de $\mathbb{R}$ se lucrează cu $\varphi(\mathbb{R})$.
A doua posibilitate de a explica identificarea este să schimbăm mulțimea K cu o alta care este în bijecție cu K, astfel încât $\varphi(\mathbb{R})$ să se corespundă cu $\mathbb{R}$ prin bijecția respectivă, apoi să transportăm structura de corp a lui K prin această schimbare.



~~Mai precis~~ Acest lucru se poate face "adăugând" la $\mathbb{R}$ o mulțime în bijecție cu $K \setminus \varphi(\mathbb{R})$. Mai precis, fie X o mulțime în bijecție cu $K \setminus \varphi(\mathbb{R})$, astfel încât $X \cap \mathbb{R} = \emptyset$. Fie $\psi : X \to K \setminus \varphi(\mathbb{R})$ o funcție bijectivă. Atunci funcția

$$f : \mathbb{R} \cup X \longrightarrow K, \quad f(t) = \begin{cases} \varphi(t), & \text{dacă } t \in \mathbb{R} \\ \psi(t), & \text{dacă } t \in X \end{cases},$$

este bijectivă



$$\mathbb{R} \cup X \xrightarrow{f} K$$

Atunci structura de corp a lui K induce via f o structură de corp pe $\mathbb{R} \cup X$ cu

- adunarea $\oplus$ dată de $u \oplus t = f^{-1}(f(u) + f(t))$
- înmulțirea $\odot$ dată de $u \odot t = f^{-1}(f(u) f(t))$,

pt. orice $u, t \in \mathbb{R} \cup X$.

În plus f este un izomorfism de corpuri între corpul $\mathbb{R} \cup X$ definit astfel și K.

(Exercițiu: verificați că $\mathbb{R} \cup X$ este corp și f este izomorfism de corpuri).

Dacă $a, b \in \mathbb{R}$, atunci

$$a \oplus b = f^{-1}(f(a)+f(b)) = f^{-1}(\varphi(a)+\varphi(b))$$

$$= f^{-1}(\varphi(a+b)) = f^{-1}(f(a+b)) = a+b$$

şi la fel se arată că $a \odot b = ab$.

Rezultă că $\mathbb{R}$ (cu structura uzuală de corp) este subcorp în $(\mathbb{R} \cup X, \oplus, \odot)$, deci nu este niciun pericol de confuzie dacă notăm $\oplus$ şi $\odot$ cu $+$ şi $\cdot$.

Dacă notăm $\mathbb{C} = \mathbb{R} \cup X$ şi $i = f^{-1}(I)$, atunci

$$\mathbb{C} = \{ f^{-1}(\varphi(a)+\varphi(b)I) \mid a, b \in \mathbb{R} \} = \{ a+bi \mid a, b \in \mathbb{R} \},$$

$$a+bi = c+di \iff \varphi(a+bi) = \varphi(c+di) \iff \varphi(a)+\varphi(b)I = \varphi(c)+\varphi(d)I$$

$$\iff a=c \text{ şi } b=d.$$

Operaţiile din corpul $\mathbb{C}$ sunt

$$\begin{aligned}(a+bi)+(c+di) &= f^{-1}(f(a+bi)+f(c+di)) \\ &= f^{-1}((\varphi(a)+\varphi(b)I)+(\varphi(c)+\varphi(d)I)) \\ &= f^{-1}((\varphi(a)+\varphi(c))+(\varphi(b)+\varphi(d))I) \\ &= f^{-1}(\varphi(a+c)+\varphi(b+d)I) \\ &= (a+c)+(b+d)i\end{aligned}$$

şi similar $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$.

În plus, $i^2 = -1$ şi $\mathbb{R}$ este subcorp în $\mathbb{C}$. Aceasta este prezentarea obişnuită a corpului $\mathbb{C}$ al numerelor complexe.

Exercițiu (o prezentare matricială a lui $\mathbb{C}$)

Fie $L=\left\{\begin{pmatrix} a & b \\ -b & a\end{pmatrix} \middle| a,b\in\mathbb{R}\right\}$. Atunci L este închisă în raport cu adunarea și înmulțirea matricelor și este corp comutativ în raport cu aceste operații. În plus, aplicația $g:L\to\mathbb{C}$, $g\begin{pmatrix} a & b \\ -b & a\end{pmatrix}=a+bi$, este izomorfism de corpuri.

Indicație. Se poate rezolva cu calcul direct sau, pt. a evita calculele, se consideră

$h:\mathbb{C}\to M_2(\mathbb{R})$, $h(a+bi)=\begin{pmatrix} a & b \\ -b & a\end{pmatrix}$.

Se verifică că h este morfism injectiv de inele. Rezultă că $\mathbb{C}\simeq \mathrm{Im}\, h$ ca inele, deci $\mathrm{Im}\, h$ e și el corp, izomorf cu $\mathbb{C}$. Dar e clar că $\mathrm{Im}\, h=L$, gata!

În plus, g e chiar inversa corestricției lui h la L, deci e izo.

Observație Construcția lui $\mathbb{C}$ prezentată mai devreme conține două metode, care pot fi enunțate mult mai general.

(I) Dacă A este o mulțime înzestrată cu o anumită structură algebrică (de ex. grup, inel, corp), iar B este o mulțime în bijecție cu A, fie $f:B\to A$ o bijecție, atunci pe B se poate defini o structură algebrică de acelaşi tip, indusă de cea a lui A via f. Mai precis, pentru orice operaţie $*$ din structura lui A, se poate defini o operaţie $\circledast$ pe B prin

$$x \circledast y = f^{-1}(f(x) * f(y)) \text{ pt. orice } x, y \in B.$$

Mai mult, f devine un izomorfism (de structura respectivă) între B şi A.

II Dacă A este un obiect cu o anumită structură algebrică (de exemplu grup, inel, corp) care se scufundă într-un obiect K înzestrat cu acelaşi tip de structură (adică există un morfism injectiv $\varphi: A \to K$ de tipul structurii respective), atunci există un obiect B având acelaşi tip de structură, care este izomorf cu K şi astfel încât $A \subset B$, mai precis A este subobiect al lui B în structura respectivă (adică subgrup, subinel, subcorp). Altfel spus: orice scufundare poate fi privită (din punct de vedere al structurii) ca o incluziune.

(2) Inele de endomorfisme ale grupurilor abeliene:
dacă $(G,+)$ este grup abelian, atunci
$End(G) = \{f \mid f: G \to G$ morfism de grupuri$\}$
este inel cu
adunarea = adunarea uzuală a morfismelor
înmulțirea = compunerea funcțiilor
$End(G)$ s.n. inelul endomorfismelor lui G
(Verificați că axiomele inelului sunt satisfăcute!).

<u>Exercițiu</u>. Orice inel R se scufundă într-un inel de forma $End(G)$, cu G grup abelian, adică există un morfism injectiv de inele $\varphi: R \to End(G)$ pt. un astfel de G.
(Consecință: orice inel este subinel al unui $End(G)$).

(3) Inele de endomorfisme de spații vectoriale.
Fie K un corp comutativ și V un K-spațiu vectorial.
Atunci $End_K(V) = \{f \mid f: V \to V$ aplicație liniară$\}$
este inel cu adunarea uzuală a aplicațiilor liniare și compunerea funcțiilor.