Seminar 10

Morfisme de inele

Reamintim: $(R,+,\cdot)$, $(S,+,\cdot)$ inele, $f: R \to S$ funcție

f se numește morfism de inele dacă $\begin{cases} f(x+y)=f(x)+f(y) \\ f(x\cdot y)=f(x)\cdot f(y) \end{cases}$

Izomorfism = morfism bijectiv

Dacă $1 \in R$, $1 \in S$ atunci f se zice unital dacă $f(1)=1$.

Obs. Orice izomorfism de inele unitale este unital.

Într-adevăr dacă $f: R \to S$ este un izomorfism și $s \in S$ atunci $\exists!\, r \in R$ a.î. $f(r)=s$, deci

$$\left.\begin{aligned} f(1)\cdot s &= f(1)\cdot f(r) = f(1\cdot r) = f(r) = s \\ s\cdot f(1) &= f(r)\cdot f(1) = f(r\cdot 1) = f(r) = s \end{aligned}\right\} \Rightarrow f(1) \in S \text{ este unitate.}$$

Temă: Arătați că dacă $1 \in R$ și $f: R \to S$ este un morfism surjectiv de inele atunci S este unital și f este unital.

Obs. Un morf de inele este morf. de grupuri între $(R,+)$ și $(S,+)$.

Deci $f(0)=0$ și $f(-x)=-f(x)$, $\forall x \in R$ etc.

Obs Dacă $f: R \to S$ este morf. de inele și $1 \in R$ atunci

$f(1)^2 = f(1)\cdot f(1) = f(1\cdot 1) = f(1)$ deci $f(1) \in S$ este idempotent.

1. Demonstrați că $(2\mathbb{Z},+,\cdot)$ și $(3\mathbb{Z},+,\cdot)$ nu sunt izomorfe.

Soluție. Presupunem că ar exista un izomorfism $f: 2\mathbb{Z} \to 3\mathbb{Z}$

Notăm $f(2)=3k \in 3\mathbb{Z}$ $(k \in \mathbb{Z})$. Atunci

$$\left.\begin{aligned} f(4) &= f(2+2) = f(2)+f(2) = 3k+3k = 6k \\ f(4) &= f(2\cdot 2) = f(2)\cdot f(2) = 3k\cdot 3k = 9k^2 \end{aligned}\right\} \Rightarrow 9k^2 = 6k \Rightarrow$$

$\Rightarrow k(3k-2)=0 \Rightarrow k=\frac{2}{3} \notin \mathbb{Z}$ (nu convine) sau $k=0$.

Deci $f(2)=0=f(0) \Rightarrow f$ nu este injectiv contradicție.

Temă. Arătați că grupurile $(2\mathbb{Z},+)$ și $(3\mathbb{Z},+)$ sunt izomorfe dar nu există un alt morfism de inele $f: 2\mathbb{Z} \to 3\mathbb{Z}$ în afara celui nul.

2. Fie p un număr prim. Notăm

$$\mathbb{Z}[\sqrt{p}]=\{a+b\sqrt{p} \mid a,b\in\mathbb{Z}\}, \quad \mathbb{Q}[\sqrt{p}]=\{a+b\sqrt{p} \mid a,b\in\mathbb{Q}\}$$

$$\mathbb{Z}[i\sqrt{p}]=\{a+bi\sqrt{p} \mid a,b\in\mathbb{Z}\}, \quad \mathbb{Q}[i\sqrt{p}]=\{a+bi\sqrt{p} \mid a,b\in\mathbb{Q}\}.$$

Arătați că în raport cu adunarea și înmulțirea nr. reale/complexe

a) $\mathbb{Z}[\sqrt{p}]$ și $\mathbb{Z}[i\sqrt{p}]$ sunt domenii de integritate care nu sunt corpuri

b) $\mathbb{Q}[\sqrt{p}]$ și $\mathbb{Q}[i\sqrt{p}]$ sunt corpuri (comutative).

c) $\mathbb{Z}[\sqrt{2}]\neq\mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[\sqrt{2}]\neq\mathbb{Z}[\sqrt{3}]$.

d) $\mathbb{Q}[\sqrt{2}]\neq\mathbb{Q}[i\sqrt{2}]$, $\mathbb{Q}[\sqrt{2}]\neq\mathbb{Q}[\sqrt{3}]$.

Soluție a,b). • $0=0+0\sqrt{p}\in\mathbb{Z}[\sqrt{p}]$, $1=1+0\sqrt{p}\in\mathbb{Z}[\sqrt{p}]$

• $x,y\in\mathbb{Z}[\sqrt{p}] \Rightarrow x=a+b\sqrt{p}$, $y=c+d\sqrt{p}$, $a,b,c,d\in\mathbb{Z}\longrightarrow$

$$x-y=(a-c)+(b-d)\sqrt{p}\in\mathbb{Z}[\sqrt{p}]$$

$$x\cdot y=(ac+pbd)+(ad+bc)\sqrt{p}\in\mathbb{Z}[\sqrt{p}]$$

Deci $\mathbb{Z}[\sqrt{p}]$ este subinel cu unitate în corpul comutativ $(\mathbb{R},+,\cdot)$

$\Rightarrow \mathbb{Z}[\sqrt{p}]$ domeniu de integritate

(de fapt dacă $x,y\in\mathbb{Z}[\sqrt{p}]$ cu $x\cdot y=0$ atunci este clar că $x,y\in\mathbb{R}$ și $x\cdot y=0\longrightarrow x=0$ sau $y=0$, atât în $\mathbb{R}$ cât și în $\mathbb{Z}[\sqrt{p}]$)

Temă: $\mathbb{Q}[\sqrt{p}]$ subinel cu unitate în $\mathbb{R}$ și $\mathbb{Z}[i\sqrt{p}]$, $\mathbb{Q}[i\sqrt{p}]$ subinele cu unitate în $(\mathbb{C},+,\cdot)$.

Mai departe: $\mathbb{Z}[\sqrt{2}]$ nu este corp pt. că $2=2+0\sqrt{p}\in\mathbb{Z}[\sqrt{p}]$ dar din $2\cdot x=1$ rezultă $x=\frac{1}{2}$ în $\mathbb{R}$ și $\frac{1}{2}\notin\mathbb{Z}[\sqrt{2}]$. Analog $\mathbb{Z}[i\sqrt{p}]$ nu este corp.

Arătăm că $\mathbb{Q}[i\sqrt{p}]$ este corp (și rămâne temă $\mathbb{Q}[\sqrt{p}]$).

Fie $x=a+bi\sqrt{p}\in\mathbb{Q}[i\sqrt{p}]$. Atunci $x\cdot\bar{x}=(a+bi\sqrt{p})(a-bi\sqrt{p})=a^2+pb^2$

Dar $x\neq 0\Leftrightarrow$ cel puțin unul dintre a și b nu este zero $\Rightarrow$

$$a^2+pb^2\neq 0$$

Așadar $\frac{\bar{x}}{a^2+pb^2}=\frac{a}{a^2+pb^2}-\frac{b}{a^2+pb^2}i\sqrt{p}\in\mathbb{Q}[i\sqrt{p}]$ și $x\cdot\frac{\bar{x}}{a^2+pb^2}=1$

deci $\exists\, x^{-1}=\frac{\bar{x}}{a^2+pb^2}\in\mathbb{Q}[i\sqrt{p}]$.

Obs. Calculul lui x^{-1} de mai sus este calculul obișnuit al inversului elementului $x\in\mathbb{C}^*$. -2-

b) În cazul lui $\mathbb{Q}[\sqrt{p}]$ intervine o dificultate suplimentară, anume de a arăta că dacă cel puțin unul dintre a și b nu sunt zero atunci $a^2 - pb^2 \neq 0$ ($\Leftrightarrow a^2 + pb^2$ este clar $\Leftrightarrow$ că $a^2 + pb^2 > 0$). Rezolvarea dificultății se bazează pe faptul că $\sqrt{p} \notin \mathbb{Q}$.

c) Dacă $f: \mathbb{Z}[i\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ este un izomorfism de inele el este unital, deci $\forall n \in \mathbb{Z}$ ($n = n + 0 \cdot i\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$) avem $f(n) = n$. (Într-adevăr dacă $n > 0$ atunci

$$f(n) = f(\underbrace{1+1+\dots+1}_{n\text{-ori}}) = \underbrace{f(1)+f(1)+\dots+f(1)}_{n\text{ ori}} = \underbrace{1+1+\dots+1}_{n\text{-ori}} = n$$

dacă $n = 0$ atunci $f(0) = 0$, iar dacă $n < 0$ atunci

$$f(n) = f(-(-n)) = -f(-n) \underset{-n>0}{=} -(-n) = n.$$

Considerăm $i\sqrt{2} = 0 + 1 \cdot i\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ și calculăm

$$f(i\sqrt{2})^2 = f(i\sqrt{2}) \cdot f(i\sqrt{2}) = f(i\sqrt{2} \cdot i\sqrt{2}) = f(-2) = -2$$

Dar $f(i\sqrt{2}) \in \mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ ceea ce este imposibil, deci

$$\mathbb{Z}[i\sqrt{2}] \not\cong \mathbb{Z}[\sqrt{2}].$$

Analog dacă am presupune că $f: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{3}]$ este un izomorfism atunci $f(n) = n$, $\forall n \in \mathbb{Z}$. Dar

$$(f(\sqrt{2}))^2 = f(\sqrt{2}) \cdot f(\sqrt{2}) = f(\sqrt{2} \cdot \sqrt{2}) = f(2) = 2 \text{ deci}$$

$f(\sqrt{2}) = a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ astfel încât $(f(\sqrt{2}))^2 = 2$

$$\Rightarrow (a + b\sqrt{3})^2 = 2 \Rightarrow a^2 + 2ab\sqrt{3} + 3b^2 = 2 \to$$

$$2ab\sqrt{3} = 2 - a^2 - 3b^2$$

Dacă $ab \neq 0$ atunci $\sqrt{3} = \frac{2 - a^2 - 3b^2}{2ab} \in \mathbb{Q}$ contradicție. Deci $a \cdot b = 0$ de unde $a = 0$ sau $b = 0$.

Dacă $a = 0$ atunci $3b^2 = 2 \Rightarrow b^2 = \frac{2}{3} \Rightarrow \sqrt{\frac{2}{3}} = b \in \mathbb{Q}$ fals.

Dacă $b = 0$ atunci $a^2 = 2 \Rightarrow \sqrt{2} = a \in \mathbb{Q}$ fals.

Toate cazurile au sfârșit în contradicție, deci $\mathbb{Z}[\sqrt{2}] \not\cong \mathbb{Z}[\sqrt{3}]$.

Temă. Completați restul soluției!

3. Determinați morfismele de inele (corpuri) între

a) $(\mathbb{Z},+,\cdot)$ și $(2\mathbb{Z},+,\cdot)$

b) $(\mathbb{Z},+,\cdot)$ și $(\mathbb{Z},+,\cdot)$

c) $(\mathbb{Z},+,\cdot)$ și $(\mathbb{Q},+,\cdot)$

d) $(\mathbb{Q},+,\cdot)$ și $(\mathbb{Q},+,\cdot)$

e) $(\mathbb{R},+,\cdot)$ și $(\mathbb{R},+,\cdot)$

f) $(\mathbb{C},+,\cdot)$ și $(\mathbb{C},+,\cdot)$

Soluție. a), b), c). Dacă $(R,+,\cdot)$ este un inel și $f:\mathbb{Z}\to R$ un morfism de inele atunci notăm $e=f(1)\in R$. Este clar că pt. orice $n\in\mathbb{Z}$ avem $f(n)=n\cdot e$ (se arată pe rând pt. $n>0$, $n\geq 0$ și $n<0$ - v. ex. anterior; de fapt este vorba de faptul că orice morfism de grupuri $(\mathbb{Z},+)\to(R,+)$ este de forma $f(x)=x\cdot e$, unde $e=f(1)\in R$). Mai departe $e^2=f(1)\cdot f(1)=f(1\cdot 1)=f(1)=e$ deci e trebuie să fie un idempotent în $(R,+,\cdot)$.

Reciproc dacă $e\in R$ este un idempotent atunci $f_e:\mathbb{Z}\to R$, $f_e(x)=xe$ este un morfism de inele. Într-adevăr

$$f(x+y)=e(x+y)=ex+ey=f(x)+f(y)$$

$$f(x)\cdot f(y)=(xe)\cdot(ye)=(e+\dots+e)(e+\dots+e)=\underbrace{e^2+e^2+\dots+e^2}_{xy\text{ ori}}=xye^2=xye=f(xy)$$

Deci mulțimea morf. de inele $(\mathbb{Z},+,\cdot)\to(R,+,\cdot)$ este exact

$$\{f_e \mid e=e^2\in R \text{ (idempotent)}\}, \text{ unde } f_e:\mathbb{Z}\to R,\ f_e(x)=xe$$

a) - $2\mathbb{Z}$ are un singur idempotent 0 deci singurul morf. de inele este cel nul

b) $\mathbb{Z}$ are doi idempotenți 0 și 1 $\Rightarrow$ două morfisme

$$0:\mathbb{Z}\to\mathbb{Z},\ 0(x)=0 \text{ și } 1_{\mathbb{Z}}:\mathbb{Z}\to\mathbb{Z},\ 1_{\mathbb{Z}}(x)=x$$

c) $\mathbb{Q}$ are doi idempotenți 0 și 1 $\Rightarrow$ două morfisme

$$0:\mathbb{Z}\to\mathbb{Q},\ 0(x)=0 \text{ și } i:\mathbb{Z}\to\mathbb{Q},\ i(x)=x,\ \forall x\in\mathbb{Z}.$$
(inclusiunea)

d) Cu același argument ca și mai sus se arată că dacă $f:\mathbb{Q}\to\mathbb{Q}$ este un morfism de inele atunci $e=f(1)\in\mathbb{Q}$ este idempotent și $f(n)=ne$, $\forall n\in\mathbb{Z}$. Mai departe pt. $n\in\mathbb{N}^*$ avem

$\underbrace{\frac{1}{n}+\frac{1}{n}+\dots+\frac{1}{n}}_{n\text{-ori}}=1$ deci $f\left(\frac{1}{n}\right)+f\left(\frac{1}{n}\right)+\dots+f\left(\frac{1}{n}\right)=f(1)=e$

$\Rightarrow f\left(\frac{1}{n}\right)=\frac{e}{n}$.

In general pt. $x\in\mathbb{Q}$ scriem $x=\frac{m}{n}$, $m\in\mathbb{Z}$, $n\in\mathbb{N}^*$ deci

$$f(x)=f\left(m\cdot\frac{1}{n}\right)=f(m)\cdot f\left(\frac{1}{n}\right)=m e\cdot\frac{e}{n}=\frac{m}{n}\cdot e^2=x\cdot e^2=x\cdot e$$

Cum $\mathbb{Q}$ are doi idempotenti $\Rightarrow$ două morfisme de inele

$0:\mathbb{Q}\to\mathbb{Q}$, $0(x)=0$ și $1_{\mathbb{Q}}:\mathbb{Q}\to\mathbb{Q}$, $1_{\mathbb{Q}}(x)=x$.

e) Cu același argument ca și la d) arătăm că dacă

$f:\mathbb{R}\to\mathbb{R}$ este un morfism atunci $e=f(1)\in\mathbb{R}$ este idempotent

și $f(x)=x\cdot e$, $\forall x\in\mathbb{Q}$.

Vom arăta acum că f este o funcție crescătoare. Știm adevărat dacă $x\geq 0$ atunci $\exists\, y\in\mathbb{R}$ a.i. $y^2=x$ (clar $y=\pm\sqrt{x}$), deci

$$f(x)=f(y^2)=f(y\cdot y)=f(y)f(y)=f(y)^2\geq 0$$

Mai departe dacă $x\leq y$ atunci $y-x\geq 0$ deci $f(y-x)\geq 0$ $\Rightarrow$

$f(y)-f(x)\geq 0$ $\Rightarrow$ $f(x)\leq f(y)$ ceea ce arată că f este crescătoare.

Fie acum $x\in\mathbb{R}$ oarecare. Considerăm două șiruri de numere raționale cu proprietatea că $x_n\leq x_{n+1}\leq x\leq y_{n+1}\leq y_n$ astfel încât $\lim\limits_{n\to\infty}x_n=x=\lim\limits_{n\to\infty}y_n$ (îl cuprindem pe x într-un „clește" a cărui ajutorul a două șiruri de numere raționale, unul crescător către x iar celălalt descrescător). Deoarece f crescătoare obținem

$$f(x_n)\leq f(x)\leq f(y_n)\Rightarrow x_n e\leq f(x)\leq y_n e.$$

Dar $\lim\limits_{n\to\infty}(x_n e)=xe=\lim\limits_{n\to\infty}(y_n e)$ deci $f(x)=xe$. Cum x a fost arbitrar obținem morf. de forma $f:\mathbb{R}\to\mathbb{R}$, $f(x)=xe$, $e=e^2\in\mathbb{R}$.

Dar $\mathbb{R}$ are numai idempotenți triviali $\Rightarrow$ două morfisme

$$0:\mathbb{R}\to\mathbb{R},\ 0(x)=0 \text{ și } 1_{\mathbb{R}}:\mathbb{R}\to\mathbb{R},\ 1_{\mathbb{R}}(x)=x.$$

f). Adaptăm argumentul de mai sus pt. a arăta că dacă $f:\mathbb{C}\to\mathbb{C}$ morf. de inele atunci $e=f(1)\in\mathbb{C}$ este idempotent (deci $e\in\{0,1\}$) și $f(x)=xe$, $\forall x\in\mathbb{R}$. Pt. a determina $f(z)$ unde $z=x+iy$, $x,y\in\mathbb{R}$

mai trebuie să vedem cât poate f $f(i)$. Din $i^2=-1$ rezultă $f(i)\in\{i,-i\}$ deci obținem trei morfisme:

$0:\mathbb{C}\to\mathbb{C}$, $0(x)=0$, $1_{\mathbb{C}}:\mathbb{C}\to\mathbb{C}$, $1_{\mathbb{C}}(z)=z$, $f:\mathbb{C}\to\mathbb{C}$, $f(z)=\bar{z}$.

Temă: 1) Completați detaliile de la f).

2) Care dintre morfismele determinate anterior sunt izomorfisme?

3) Care dintre morfismele determinate anterior sunt morfisme de corpuri?

4. Determinați morfismele de inele $\mathbb{Z}_{12}\to\mathbb{Z}_{20}$.

Soluție. Fie $f:\mathbb{Z}_{12}\to\mathbb{Z}_{20}$ un morf. de inele. Notăm $\bar{e}=f(\hat{1})\in\mathbb{Z}_{20}$. Clar $\bar{e}^2=\bar{e}$ este un idempotent în $\mathbb{Z}_{12}$. Mai mult pt. orice $k\in\mathbb{Z}$ avem $f(\hat{k})=f(k\hat{1})=k\cdot\bar{e}$. Singura problemă rămasă este bine definirea funcției f. Mai precis dacă $\hat{k}=\hat{t}$ în $\mathbb{Z}_{12}$ trebuie să avem $k\bar{e}=t\bar{e}$ în $\mathbb{Z}_{20}$. Acest lucru se obține exact atunci când $12\bar{e}=\bar{0}$ în $\mathbb{Z}_{20}$. Într-adevăr $12\bar{e}=f(\hat{12})=f(\hat{0})=\bar{0}$ și dacă $12\bar{e}=\bar{0}$ și $\hat{k}=\hat{t}$ în $\mathbb{Z}_{12}$ atunci $k-t=12\cdot q$, $q\in\mathbb{Z}$ deci

$k\bar{e}-t\bar{e}=(k-t)\bar{e}=12\cdot q\cdot\bar{e}=\bar{0}\Rightarrow k\bar{e}=t\bar{e}$.

Verificarea faptului că f este morfism este imediată:

$f(\hat{k}+\hat{t})=f(\widehat{k+t})=(k+t)\bar{e}=\overline{(k+t)e}=\overline{ke}+\overline{te}=k\bar{e}+t\bar{e}=f(\hat{k})+f(\hat{t})$

$f(\hat{k}\cdot\hat{t})=f(\widehat{kt})=kt\bar{e}=\overline{kte}=\overline{kte^2}=\overline{ke}\cdot\overline{te}=f(\hat{k})\cdot f(\hat{t})$.

Deci mulțimea morfismelor de inele $\mathbb{Z}_{12}\to\mathbb{Z}_{20}$ este

$\{f_{\bar{e}}\mid \bar{e}=\bar{e}^2\in\mathbb{Z}_{20}$ și $12\bar{e}=\bar{0}$ în $\mathbb{Z}_{20}\}$ unde $f_{\bar{e}}:\mathbb{Z}_{12}\to\mathbb{Z}_{20}$, $f_{\bar{e}}(\hat{k})=k\bar{e}$

Idempotenții din $\mathbb{Z}_{20}$ sunt: $\bar{0}$, $\bar{1}$, $\bar{5}$ (verificare directă). Mai mult

$12\cdot\bar{0}=\bar{0}$, $12\cdot\bar{1}=\bar{12}\neq\bar{0}$ și $12\cdot\bar{5}=\bar{60}=\bar{0}\Rightarrow$

două morfisme $0:\mathbb{Z}_{12}\to\mathbb{Z}_{20}$, $0(\hat{k})=\bar{0}$, $f_{\bar{5}}:\mathbb{Z}_{12}\to\mathbb{Z}_{20}$, $f_{\bar{5}}(\hat{k})=k\cdot\bar{5}$, $k\in\mathbb{Z}$.

Temă: Determinați toți idempotenții din $\mathbb{Z}_m$ ($m\geq 2$). Determinați toate morfismele de inele $\mathbb{Z}_n\to\mathbb{Z}_m$ ($n,m\geq 2$).

5* (Temă). Arătați că dacă $*$ este o operație pe $\mathbb{Z}_n$ ($n\geq 2$) astfel încât $(\mathbb{Z}_n,+,*)$ este un inel cu unitate, atunci $(\mathbb{Z}_n,+,*)\cong(\mathbb{Z}_n,+,\cdot)$.