⑥ Neka je $(R, +, \cdot)$ prsten i $a \in R$.
Posmatrajmo preslikavanje $f_a(x) = a \cdot x$.
$f_a : R \to R$
$\overline{R} = \{ f_a \mid a \in R \}$
Dokazati da je $(\overline{R}, +, \circ)$ ima strukturu prstena, ako je $+$ def. sa
$(f_a + f_b)(x) = f_a(x) + f_b(x)$, a $\circ$ sa:
$(f_a \circ f_b)(x) = f_a(f_b(x))$

I) $(\overline{R}, +)$ - Abelova grupa?

1) $a, b \in R$
$f_a, f_b \in \overline{R}$

Dokazaćemo da je $f_a + f_b = f_{a+b}$.

$$\left.\begin{array}{l}(f_a + f_b)(x) = f_a(x) + f_b(x) = a \cdot x + b \cdot x \\ f_{a+b}(x) = (a+b) \cdot x\end{array}\right\} \Rightarrow$$

$\boxed{R \text{ je prsten}} \Rightarrow (a+b) \cdot x = a \cdot x + b \cdot x$
$f_{a+b}(x) = f_a(x) + f_b(x)$

$\Rightarrow (\forall x \in R)\ (f_a + f_b)(x) = f_{a+b}(x) \Rightarrow$

$\Rightarrow f_a + f_b = f_{a+b} \in \overline{R}$

2) $f_a, f_b, f_c \in \overline{R}$

$$(f_a+f_b)+f_c \stackrel{?}{=} f_a+(f_b+f_c)$$

$$L = ((f_a+f_b)+f_c)(x) = (f_a+f_b)(x)+f_c(x) =$$
$$= (f_a(x)+f_b(x))+f_c(x) = (ax+bx)+cx$$

$$D = (f_a+(f_b+f_c))(x) = f_a(x)+(f_b+f_c)(x) =$$
$$= f_a(x)+(f_b(x)+f_c(x)) = ax+(bx+cx)$$

R je prsten $\Longrightarrow (ax+bx)+cx \overset{\text{asoc. u } (R,+)}{=} ax+(bx+cx)$

$L = D$

važi asoc. u $(\overline{R},+)$

3) $f_a+f_b = f_{a+b} = f_a$

Za $b=0$: $f_a+f_0 = f_{a+0} = f_a$

Neutralni el. je $f_0(x) = 0\cdot x = 0$.

4) $f_a \xrightarrow{\text{inverz}} f_{-a}$

$f_a+f_{-a} = f_{a-a} = f_0$

$f_{-a}+f_a = f_{-a+a} = f_0$

5) Komutativnost se prenosi:

$$\left.\begin{aligned}(f_a+f_b)(x) &= ax+bx\\ (f_b+f_a)(x) &= bx+ax\end{aligned}\right\} \xrightarrow{R \text{ je prsten}} f_a+f_b = f_b+f_a$$

$\underline{\text{II}})$ $(\overline{R},\circ)$

1) $f_a, f_b \in \overline{R}$

Tvrdimo da je $f_a \circ f_b = f_{ab}$.

$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(bx) = a(bx)$

$f_{ab}(x) = (ab)x$

R je prsten $\Rightarrow (\forall x \in R)\ (f_a \circ f_b)(x) = f_{ab}(x)$

$\Rightarrow f_a \circ f_b = f_{ab} \in \overline{R} \quad (ab \in R)$

2) Asoc. važi za sva preslikavanja

$(f \circ g) \circ h = f \circ (g \circ h)$

III) Distributivnost:

$f_a, f_b, f_c \in \overline{R}$

$f_a \circ (f_b + f_c) \overset{?}{=} f_a \circ f_b + f_a \circ f_c$

$L = (f_a \circ (f_b + f_c))(x) = f_a(f_b(x) + f_c(x)) =$
$= f_a(bx + cx) = a(bx + cx) = abx + acx$

$D = (f_a \circ f_b + f_a \circ f_c)(x) = (f_a \circ f_b)(x) + (f_a \circ f_c)(x) =$
$= abx + acx$

$\Rightarrow L = D \Rightarrow$ važi dist.

Provjeriti distributivnost sa desne strane.

$(\overline{R}, +, \circ)$ je prsten

Def. $(R,+,\cdot)$ je prsten, $A \subseteq R$

Za A kažemo da je lijevi ideal ako:

1) $(A,+) \leq (R,+)$

2) $RA \subseteq A$

Desni ideal ako je:

1) $(A,+) \leq (R,+)$

2) $AR \subseteq A$

7. Neka je $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a,b,c \in \mathbb{Z} \right\}$.

a) Dokazati da je $(R,+,\cdot)$ prsten.

b) Dokazati da je skup $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,b \in \mathbb{Z} \right\}$ ideal u R.

a) Lako

b) $(I,+) \leq (R,+)$?

$$\underbrace{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}}_{A}, \underbrace{\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}}_{B} \in I, \quad a,b,c,d \in \mathbb{Z}$$

$$A - B \overset{?}{\in} I$$

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -c & -d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ 0 & 0 \end{pmatrix} \in I \Rightarrow$$

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

II) $M = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in R$, $x, y, z \in \mathbb{Z}$

$A = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in I$, $a, b \in \mathbb{Z}$

$M \cdot A = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xa & xb \\ 0 & 0 \end{pmatrix} \in I$

Analogno za $A \cdot M \in I$ $\Longrightarrow$ I je ideal u R

8.

Vježbe

Def. Neka je $(R,+,\cdot)$ prsten. Za element $a \in R$ kažemo da je nilpotentan ako $\exists n \in \mathbb{N}$ t.d. $a^n = a \cdot a \cdots a = 0$.

1. Ako su a i b nilpotentni elementi prstena $(R,+,\cdot)$ koji je komutativan, tada je i element $a+b$ nilpotentan.

$$\left.\begin{array}{l}(\exists n \in \mathbb{N})\ a^n = 0 \\ (\exists m \in \mathbb{N})\ b^m = 0\end{array}\right\} \quad ?\ \exists s\ \ (a+b)^s = 0\ ?$$

$s = m + n$

U komutativnom prstenu važi Njutnova binomna formula

$$(a+b)^s = \sum_{k=0}^{s} \binom{s}{k} a^k b^{s-k}$$

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}$$

1°) $k \geq n$, tada je $a^k = \underbrace{a^n}_{0} \cdot a^{k-n} = 0$

2°) $0 \leq k < n$, tada je $n+m-k \geq m$

$b^{n+m-k} = \underbrace{b^m}_{0} \cdot b^{n-k} = 0$

$\forall k \in \{0, \dots, n+m\} \quad \binom{n+m}{k} a^k b^{n+m-k} = 0$

$\Rightarrow \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k} = 0 \Rightarrow (a+b)^{n+m} = 0$

2. Dokazati da prsten R nema nilpotentnih elemenata (osim 0) akko iz $x^2 = 0 \Rightarrow x = 0$.

($\Rightarrow$) R nema nilpotentnih elemenata osim 0.
Neka je $x^2 = 0$. Jasno, tada je $x = 0$.

($\Leftarrow$) $x^2 = 0 \Rightarrow x = 0$

Pretpostavimo da $(\exists \underset{\neq 0}{a} \in R)(\exists \underset{\geq 2}{k} \in \mathbb{N})$ $\quad a^k = 0$ $\wedge$ $\underbrace{a^{k-1} \neq 0}$

$b = a^{k-1}$

$b^2 = (a^{k-1})^2 = a^{2k-2} = \underbrace{a^k}_{=0} \cdot a^{k-2} = 0 \Rightarrow b = 0$
$\Downarrow$
$\underbrace{a^{k-1} = 0}$ $\lightning$

$x \cdot 0 = 0$ u prstenu

$x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$, $x \cdot 0 = a$

$a = a + a$

$a + (-a) = a + a + (-a) \Rightarrow a = 0 \Rightarrow x \cdot 0 = 0$

3. Neka je R komutativan prsten. Dokazati da je $N(R)$ ideal u R.

$N(R)$ - skup svih nilpotentnih elemenata iz R

$$N(R) = \{ a \in R \mid (\exists n \in \mathbb{N}) \ a^n = 0 \}$$

1°| $(N(R), +) \leq (R, +)$

2°| $N(R) \cdot R \subseteq N(R)$
$R \cdot N(R) \subseteq N(R)$

$a, b \in N(R)$

? $a - b \in N(R)$?

$a^n = 0, \ b^m = 0$

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k (-b)^{n+m-k} = \dots = 0$$

$\Rightarrow a - b \in N(R)$

$a \in N(R), \ x \in R$
$a^n = 0$

$$(a \cdot x)^n = \underbrace{(ax) \cdots (ax)}_{n} = \underset{\overset{\parallel}{0}}{a^n} \cdot x^n = 0$$

Analogno za $x \cdot a$.

$\Rightarrow N(R)$ je ideal u R

Svaki prsten ima bar dva ideala:
- nula ideal
- sam taj prsten

$\Big\}$ trivijalni ideali

Ako je A ideal; $x \underset{\uparrow}{\sim} y \Leftrightarrow x - y \in A$
rel. ekv.

$$R/A = \{ x + A \mid x \in R \}$$

$$(x+A) \oplus (y+A) = (x+y) + A$$

$$(x+A) \odot (y+A) = (x \cdot y) + A \leftarrow \text{samo za ideal}$$

$(R/A, \oplus, \odot)$ – faktor prsten prstena R po idealu A

(4.) Ako je R komutativan prsten, tada je prsten $R/N(R)$ prsten bez nilpotentnih elemenata (osim nultog).

$$(x + N(R))^n = N(R)$$

$$\underbrace{(x + N(R)) \odot (x + N(R))}_{n} = N(R)$$

$$x^n + N(R) = N(R)$$

$$x^n + \underset{\substack{\cap \\ N(R)}}{a} = b \in N(R) \Rightarrow x^n \in N(R)$$

$$\exists m \quad (x^n)^m = 0$$

$x^{n \cdot m} = 0 \Rightarrow x$ je nilpotentan $\Rightarrow \underline{x \in N(R)}$

$x + N(R) = N(R)$

Jedini element iz $R/_{N(R)}$ koji je nilpotentan je $N(R)$.

(5.) Neka je R prsten sa jedinicom i $n \in \mathbb{N}$. Dokazati da je

$$I_n = \{ nx \mid x \in R \} \text{ ideal u } R.$$

$\underline{1^\circ}|$ $(I_n, +) \leq (R, +)$

$a, b \in I_n$

$a = n \cdot x,\ b = n \cdot y,\ x, y \in R$

$?\ a - b \in I_n\ ?$

$$\overset{a+(-b)}{\overset{\shortparallel}{a-b}} = n x - n y = \underbrace{x + \dots + x}_{n} - (\underbrace{y + \dots + y}_{n}) =$$

$$= \underbrace{(x-y) + \dots + (x-y)}_{n} =$$

$$= n(x-y) \Rightarrow a - b \in I_n \Rightarrow (I_n, +) \leq (R, +)$$

$\underline{2^\circ}|$ $x \in I_n$

$x = n \cdot x_1,\ x_1 \in R$

$r \in R$

Scanned by TapScanner

$$x \cdot r = (n \cdot x_1) \cdot r = (\underbrace{x_1 + \cdots + x_1}_{n}) \cdot r = \underbrace{x_1 r + \cdots + x_1 r}_{n} =$$

$$= n \underbrace{(x_1 \cdot r)}_{\in R} \in I_n$$

$r \cdot x = \cdots$ analogno

$\Rightarrow I_n$ je ideal u R

$(I_n, +, \cdot) \trianglelefteq (R, +, \cdot)$

6. Neka su I_1, I_2 ideali u R. Dokažati da su sljedeći skupovi također ideali:

a) $I_1 \cap I_2$

b) $I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$

c) $I_1 \cdot I_2 = \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in I_1, b_i \in I_2, n \in \mathbb{N}\}$

a) $$\left.\begin{array}{l} (I_1, +) \leq (R, +) \\ (I_2, +) \leq (R, +) \end{array}\right\} \Rightarrow (I_1 \cap I_2, +) \leq (R, +)$$

$a \in I_1 \cap I_2, r \in R$

? $a \cdot r, r \cdot a \in I_1 \cap I_2$?

$$\left.\begin{array}{l} \left.\begin{array}{l} a \in I_1 \\ r \in R \end{array}\right\} \Rightarrow a \cdot r \in I_1 \\ \left.\begin{array}{l} a \in I_2 \\ r \in R \end{array}\right\} \Rightarrow a \cdot r \in I_2 \end{array}\right\} \Rightarrow a \cdot r \in I_1 \cap I_2$$

Analogno za $r \cdot a$.

b) $I_1 + I_2 = \{a+b \mid a \in I_1, b \in I_2\}$

1°| $x, y \in I_1 + I_2$

$$\left.\begin{array}{l} x = a_1 + b_1 \\ y = a_2 + b_2 \end{array}\right\} \quad a_1, a_2 \in I_1, \quad b_1, b_2 \in I_2$$

? $x - y \in I_1 + I_2$?

$$x - y = a_1 + b_1 - (a_2 + b_2) = \underbrace{(a_1 - a_2)}_{\in I_1} + \underbrace{(b_1 - b_2)}_{\in I_2} \in I_1 + I_2$$

2°| $x \in I_1 + I_2$

$x = a_1 + b_1$

$r \in R$

$$r \cdot x = r \cdot (a_1 + b_1) = \underbrace{r a_1}_{\in I_1} + \underbrace{r b_1}_{\in I_2} \in I_1 + I_2$$

Analogno $x \cdot r \in I_1 + I_2$.

$I_1 + I_2 \trianglelefteq R$

c) $x, y \in I_1 \cdot I_2$

$x = a_1 b_1 + \dots + a_n b_n$

$y = c_1 d_1 + \dots + c_m d_m$

1°| $x - y = a_1b_1 + \cdots + a_nb_n - c_1d_1 - \cdots - c_md_m =$

$$= \underbrace{a_1}_{\in I_1}\underbrace{b_1}_{\in I_2} + \cdots + \underbrace{a_n}_{\in I_1}\underbrace{b_n}_{\in I_2} + \underbrace{(-c_1)}_{\in I_1}\underbrace{d_1}_{\in I_2} + \cdots + \underbrace{(-c_m)}_{\in I_1}\underbrace{d_m}_{\in I_2} \in I_1 \cdot I_2$$

2°| $x = a_1b_1 + \cdots + a_nb_n \in I_1 \cdot I_2$

$r \in R$

$$x \cdot r = (a_1b_1 + \cdots + a_nb_n)r = (a_1b_1)r + \cdots + (a_nb_n)r =$$

$$= \underbrace{a_1}_{\in I_1}\underbrace{(b_1r)}_{\in I_2} + \cdots + \underbrace{a_n}_{\in I_1}\underbrace{(b_nr)}_{\in I_2} \in I_1 \cdot I_2$$

Analogno $r \cdot x \in I_1 \cdot I_2$.

$I_1 \cdot I_2 \trianglelefteq R$

Def.| $(R_1, +, \cdot), (R_2, +, \cdot)$ – prsteni

$f: R_1 \to R_2$ je homomorfizam prstena ako

$(\forall a, b \in R_1)$:

$f(a + b) = f(a) + f(b)$

$f(a \cdot b) = f(a) \cdot f(b)$

$\mathrm{Ker} f = \{x \in R_1 \mid f(x) = 0\}$

(7.) Ako su R_1, R_2 prsteni, $f: R_1 \xrightarrow{hom.} R_2$