PRSTENI I POLJA

DEF. Struktura $(R,+,\cdot)$ je PRSTEN ako
(i) $(R,+)$ Abelova grupa
(ii) $(R,\cdot)$ polugrupa
(iii) $(\forall x,y,z) \in R$ $(x(y+z) = xy + xz \wedge (x+y)z = x\cdot z + y\cdot z)$

1. Provjeriti da li je prsten:

a) $(\mathbb{Z},+)$
b) $(\{2k : k \in \mathbb{Z}\},+,\cdot)$
c) $(\mathbb{Q},+,\cdot)$
d) $(\mathbb{R},+,\cdot)$
e) $(\mathbb{Z}_m,+_m,\cdot_m)$

$(\mathbb{Z},+)$ Ab gr. ✓✓ $(\mathbb{Z},\cdot)$ distr. ✓✓
- asocijativnost se prenosi na podskup ✓
- 0-gubi broj
- kvo ta je sp. op
- kom. isto se prenosi

$(2\mathbb{Z},+)$ Ab gr. ✓✓
$(2\mathbb{Z},\cdot)$ polugrupa ✓✓
distr. ✓✓

$m=4$
$\bar{0},\bar{1},\bar{2},\bar{3}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(2\mathbb{Z},+,\cdot)$ distr. ✓✓

DEF. Podskup P prstena $(R,+,\cdot)$ je POTPRSTEN u $(R,+,\cdot)$ ako je i P prsten u odnosu na restrikcije operacija iz $(R,+,\cdot)$.

TEO. Neprazan podskup P prstena R je potprsten ako je ispunjeno za sve $x,y \in P$
1) $x-(-y) \in P$
2) $x\cdot y \in P$

DEF. Potprsten I je IDEAL prstena $(R,+,\cdot)$ ako za sve $x \in I$ i sve $r \in R$ je
1) $xr \in I \wedge rx \in I$

Neprazan podskup I prstena R je njegov ideal ako je ispunjeno
1)
2) za sve $x,y \in I$ $x-y \in I$.

2. Dokazati da $(2\mathbb{Z},+,\cdot_2)$ nema netrivijalnih potprstena.

Ako je $(R,+,\cdot)$ prsten i P njegov potprsten, onda je $(P,+)$ podgrupa od $(R,+)$

$(2\mathbb{Z},+_2)$ nema netrivijalnih podgrupa $\Rightarrow$ $(2\mathbb{Z},+_2,\cdot_2)$ nema netrivijalnih potprstena

3. Naći sve potprstena i ideale od $(\mathbb{Z}_4,+_4,\cdot_4)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Trivijalni potprsteni
$(\{\bar{0}\},+_4,\cdot_4)$
$(\mathbb{Z}_4,+_4,\cdot_4)$

$(\{\bar{0},\bar{2}\},+_4,\cdot_4)$ Netrivijalni potprsten

Provjerimo da li je ideal.

$\underbrace{\bar{0},\bar{1},\bar{2},\bar{3}}_{\text{bilo koji iz prstena}} \cdot \underbrace{\{\bar{0},\bar{2}\}}_{\text{iz ideala}} \overset{?}{=} \underbrace{\{\bar{0},\bar{2}\}}_{\text{iz ideala}}$ ✓✓ jest i ideal.

4. Neka je f homomorfizam prstena $(R,+,\cdot)$ u njega samog. Dokazati da je

$$S = \{x \in R : f(x) = x\}$$

domen potprstena od $(R,+,\cdot)$.

$*$ $f: R \to R$
$f(x+y) = f(x) + f(y)$
$f(x\cdot y) = f(x)\cdot f(y)$

0.) Da li smo sigurni da $S \neq \emptyset$.
Čini nam se da $0 \in S$. Probaćemo to i dokazati.
Želimo $f(0) = 0$

$\underline{0} = \underline{0+0} \Rightarrow \underline{f(0)} = \underline{f(0+0)} = \underline{f(0)} + \underline{f(0)} \Rightarrow \boxed{f(0) = 0}$

1) $x,y \in S \Rightarrow x+(-y) \in S$
želimo prvo utvrditi da $f(-y) = -f(y)$
$0 = y-y \Rightarrow \underbrace{f(0)}_{0} = f(y+(-y)) = f(y) + f(-y)$
$\Rightarrow f(-y) = -f(y)$ ✓✓

$f(x+(-y)) = f(x) + f(-y) = f(x) - f(y) = x - y$ ✓✓
$x\in S$ $y\in S$

2) $x,y \in S \Rightarrow x\cdot y \in S$
$f(x)=x,\ f(y)=y$ želimo $f(x\cdot y) \overset{?}{=} x\cdot y$
$f(x\cdot y) \overset{\text{kom}}{=} f(x)\cdot f(y) = x\cdot y$ ✓✓

5. Ako su I i J ideali prstena P, dokazati
a) $I \cap J \trianglelefteq P$
b) $I+J = \{i+j : i\in I, j\in J\}$ je domen najmanjeg ideala koji sadrži $I \cup J$.

a) 0.) $0\in I \wedge 0 \in J \Rightarrow 0 \in I\cap J$. $I\cap J \neq \emptyset$ ✓✓

$\underbrace{x,y \in I\cap J}_{\text{ideali}}$, $p\in P$ $\Rightarrow$ 1) $xp \in I \wedge px \in I \cap J$
2) $x-y \in I\cap J$

1) $x\in I \wedge p\in P \Rightarrow xp \in I \wedge px \in I$
$x\in J \wedge p\in P \Rightarrow xp \in J \wedge px \in J$ } $px, xp \in I\cap J$ ✓✓
ideali ideali

2) $x,y\in I \Rightarrow x-y \in I$
$x,y \in J \Rightarrow x-y \in J$ } $x-y \in I\cap J$. ✓✓

b) Dokažimo prvo da je ideal.
0) $I+J \neq \emptyset$ $\quad \underbrace{0}_{\in I} = \underbrace{0+0}_{\in I\ \in J} \in I+J$ ✓✓

1) $x\in I+J$, $p\in P$ $\Rightarrow$ $x\cdot p,\ p\cdot x \overset{?}{\in} I+J$

$x = i+j$ $\quad p\in P$
$x\cdot p = (i+j)\cdot p = \underbrace{i\cdot p}_{\in I} + \underbrace{j\cdot p}_{\in J} \in I+J$ ✓✓
$p\cdot x = p\cdot(i+j) = \underbrace{p\cdot i}_{\in I} + \underbrace{p\cdot j}_{\in J} \in I+J$.

2) $x,y \in I+J \overset{?}{\Rightarrow} x-y \in I+J$

$x\in I+J \Rightarrow x = i_1+j_1$
$y\in I+J \Rightarrow y = i_2+j_2$
$x-y = (i_1+j_1)-(i_2+j_2)$
$= \underbrace{i_1-i_2}_{\in I} + \underbrace{j_1-j_2}_{\in J} \in I+J$ ✓✓

Dokazujemo sada $I\cup J \subseteq I+J$
$I \subseteq I+J$ $\overset{\text{pomoću } i=0}{\Rightarrow} i = i+0 \in I+J$
$J \subseteq I+J$ $\quad j = 0+j \in I+J$

$\hookrightarrow$ $I\cup J \subseteq I+J$.

Dokazujemo da je $I+J$ najmanji takav ideal.
Ako imamo $K \trianglelefteq P$ t.d. $I\cup J \subseteq K$ onda $I+J \subseteq K$.

$I\cup J \subseteq K \Rightarrow$ $I\subseteq K$, $J\subseteq K$
za sve $i\in I$ i $j\in J$ vrši $i\in K$ i $j\in K$ tj. $i+j \in K$.

$I+J \subseteq K$

Karakteristika prstena R je najmanji prirodan broj n takav da za sve $x\in R$ vrši $n\cdot x = x+x+\dots+x = 0$. Ako takav broj ne postoji, onda je karakteristika 0 (oznaka: $\mathrm{Char}(R)$).

$*$ U komutativnom prstenu R za sve $x,y\in R$ vrši
$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$ (binomna formula)

6. Ako $\mathrm{Char}(R)$ prost broj p i R je komutativan prsten, dokazati da za $x,y\in R$ vrši $(x+y)^p = x^p + y^p$

$(x+y)^p \overset{p}{=} \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = \underbrace{x^p}_{} + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k}_{=0} + \underbrace{y^p}_{} = x^p + y^p$

$\binom{p}{k} = \frac{p\cdot(p-1)\cdot\ldots\cdot(p-k+1)}{1\cdot 2\cdot\ldots\cdot k}$ $\leftarrow$ ako broj dođe sa p $= p\cdot q$

$\underbrace{\underbrace{\sqcup+\sqcup+\dots+\sqcup}_{p} + \underbrace{\sqcup+\dots+\sqcup}_{p} + \dots + \underbrace{\sqcup+\sqcup+\dots+\sqcup}_{p}}_{q} = 0$

7. Karakteristika konačnog polja je uvek prost broj.
Dokazati.

$\mathbb{F}$ - polje $\quad |\mathbb{F}| = n$ Pro ćemo ustvari da $\mathrm{Char}(\mathbb{F}) \neq 0$

Posmotrajmo: $\{1, 1+1, 1+1+1, 1+1+1+1, \dots, \underbrace{1+1+\dots+1}_{n+1}\}$

Sigurno u ovom skupu imamo bar dva iste elementa.
Neka su k_1, k_2 u.o.
$\underbrace{1+1+\dots+1}_{i} = \underbrace{1+1+\dots+1}_{j}$ $\quad 1 \leq i < j \leq n+1$
$\Rightarrow \underbrace{1+1+\dots+1}_{j-i} = 0$

Ak sada za bilo koje x
$\underbrace{x+x+\dots+x}_{j-i} = x\cdot\underbrace{(1+1+\dots+1)}_{j-i} = x\cdot 0 = \underline{0}$

Sada znamo da $\mathrm{Char}(\mathbb{F}) \leq i-j \leq n$
Neka je $\mathrm{Char}(\mathbb{F}) = m \leq n$. Pp.s. da m nije prost broj.
tj. $m = p\cdot q$, $1 < p, q < m$
$0 = m\cdot 1 = p\cdot q\cdot 1 = p\cdot 1\cdot q\cdot 1 = \underbrace{(1+1+\dots+1)}_{p}\underbrace{(1+1+\dots+1)}_{q}$

Pošto polje nema dekitelje nule, slidi $p\cdot 1 = 0$ ili $q\cdot 1 = 0$
t.u.o. $p\cdot 1 = 0$.

Ak sada za bilo koje $x\in\mathbb{F}$
$\underbrace{x+x+\dots+x}_{p} = x\cdot\underbrace{(1+1+\dots+1)}_{p} = x\cdot 0 = \underline{0}$ ↯

$\Rightarrow$ Dakle m jesti prost broj.