6. Neka su $A, B \leq G$ takve da je $AB = G$, $A \cap B = \{e\}$ i svaki element iz A komutira sa svakim elementom iz B. Dokazati da je $G \cong A \times B$.

$\forall a \in A, \forall b \in B \quad a \cdot b = b \cdot a$

$(\forall g \in G)(\exists a \in A)(\exists b \in B) \quad g = a \cdot b$

Dokazaćemo da su a i b jedinstveni. U suprotnom postojali bi a_1, b_1 i a_2, b_2 t.d. $g = a_1 b_1 = a_2 b_2$.

$a_1 \cdot b_1 = a_2 \cdot b_2$

$\underbrace{a_2^{-1} \cdot a_1}_{\in A} = \underbrace{b_2 \cdot b_1^{-1}}_{B} = e$ zbog $A \cap B = \{e\}$

$\Rightarrow a_1 = a_2, \; b_1 = b_2$

$G \overset{?}{\cong} A \times B$

$\phi : G \to A \times B$

$\phi(x) = (a, b) \qquad x \in G, \; x = a \cdot b$

ϕ je dobro definisano zbog jedinstvenosti predstavljanja $x = a \cdot b$, $a \in A$, $b \in B$

ϕ je homomorfizam:

$\phi(\underset{a_1 \cdot b_1}{\underset{\shortparallel}{x}} \cdot \underset{a_2 \cdot b_2}{\underset{\shortparallel}{y}}) = \phi(a_1 \cdot b_1 \cdot a_2 \cdot b_2) = \phi((\underbrace{a_1 \cdot a_2}_{\in A}) \cdot (\underbrace{b_1 \cdot b_2}_{\in B})) =$

$= (a_1 a_2, b_1 b_2)$

$\phi(x) = (a_1, b_1), \; \phi(y) = (a_2, b_2)$

$\phi(x)\phi(y) = (a_1, b_1) \odot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$

$\mathrm{Ker}\,\phi = \{x \in G \mid \phi(x) = (e, e)\} =$

$= \{x \in G \mid x = e \cdot e = e\} = \{e\}$

$\mathrm{Im}\,\phi = A \times B$ jer ako $x = a \cdot b \in G$ tada $x \xrightarrow{\phi} (a, b)$.

Osn. t.

$\Longrightarrow \quad G/_{\{e\}} \cong A \times B$

$G/_{\{e\}} \cong G \qquad f(x) = x$

(7.) Neka su $A, B \trianglelefteq G$ t.d. $AB = G$ i $A \cap B = \{e\}$. Dokazati da je $G \cong A \times B$.

$a \in A, b \in B$

$\underbrace{aba^{-1}}_{\in B}\underbrace{b^{-1}}_{\in B} \in B \qquad \underbrace{a}_{\in A}\underbrace{ba^{-1}b^{-1}}_{\in A} \in A$

$aba^{-1}b^{-1} \in A \cap B = \{e\}$

$aba^{-1}b^{-1} = e \ / b$

$aba^{-1} = b \ / a$

$ab = ba$

$\Rightarrow$ Svaki element iz A komutira sa svakim elementom iz B, (zad. 6) $\Rightarrow G \cong A \times B$

(8.) $A \cong C,\ B \cong D \overset{?}{\Rightarrow} A \times B \cong C \times D$

$A \cong C \Rightarrow \exists f_1 : A \xrightarrow{izom.} C$

$B \cong D \Rightarrow \exists f_2 : B \xrightarrow{izom.} D$

$f : A \times B \to C \times D$

$$f(\underset{\substack{\cap \\ A}}{a}, \underset{\substack{\cap \\ B}}{b}) = (\underbrace{f_1(a)}_{\in C}, \underbrace{f_2(b)}_{\in D})$$

$$f((a_1, b_1) \otimes (a_2, b_2)) = f(a_1 \cdot a_2, b_1 * b_2) =$$

$$= (f_1(a_1 \cdot a_2), f_2(b_1 * b_2)) = (f_1(a_1) \underset{u\ C}{\cdot} f_1(a_2), f_2(b_1) \underset{u\ D}{*} f_2(b_2)) =$$

$$= (f_1(a_1), f_2(b_1)) \otimes (f_1(a_2), f_2(b_2)) =$$

$$= f(a_1, b_1) \otimes f(a_2, b_2) \Rightarrow f \text{ je homomorfizam}$$

"1 - 1":

$$f(x_1, y_1) = f(x_2, y_2)$$

$$(f_1(x_1), f_2(y_1)) = (f_1(x_2), f_2(y_2))$$

$$\left.\begin{array}{l} \Rightarrow f_1(x_1) = f_1(x_2) \xrightarrow{f_1 \text{ je izom.}} x_1 = x_2 \\ \Rightarrow f_2(y_1) = f_2(y_2) \xrightarrow{f_2 \text{ je izom.}} y_1 = y_2 \end{array}\right\} \Rightarrow (x_1, y_1) = (x_2, y_2)$$

"na":

$$f: A \times B \to C \times D$$

Neka je $(\underset{\substack{\cap \\ C}}{c}, \underset{\substack{\cap \\ D}}{d}) \in C \times D$

$$c \in C \Rightarrow \exists a \in A \quad f_1(a) = c$$

$$d \in D \Rightarrow \exists b \in B \quad f_2(b) = d$$

$$f(a, b) = (f_1(a), f_2(b)) = (c, d) \Rightarrow f \text{ je "na"}$$

$$\Rightarrow f \text{ je izomorfizam}$$

Prsten

Na skupu R su definisane dvije operacije $+$ i $\cdot$.
Važe svojstva:

1) $(R, +)$ je Abelova gr.

2) $(R, \cdot)$ je polugrupa

3) $a \cdot (b + c) = a \cdot b + a \cdot c$
$(a + b) \cdot c = a \cdot c + b \cdot c$

Prsten sa jedinicom ako $(R, \cdot)$ ima jedinični el.
Ako je $\cdot$ komutativna onda je to komutativni prsten.
Za prsten sa jedinicom kažemo da je tijelo ako
$\forall x \in R \setminus \{0\}$ važi da $\exists x^{-1}$ t.d. $x \cdot x^{-1} = x^{-1} x = 1$.
Komutativno tijelo je polje. (F)

1. Ispitati da li su sljedeće strukture prsteni:

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

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

c) $(\mathbb{R}, +, \cdot)$

d) $(\mathbb{C}, +, \cdot)$

e) $(\mathbb{Z}_m, +, \cdot)$

a) I) $(\mathbb{Z}, +)$ je Abelova grupa
II) $(\mathbb{Z}, \cdot) \rightarrow$ 1) Zatvorenost važi, 2) asoc ✓, 3) $1 \in \mathbb{Z}$, 4) <u>Ne važi</u>, 5) ✓

III) Važi distributivnost.

$\Rightarrow$ Komutativan prsten sa jedinicom.

b) I) $(2\mathbb{Z}, +)$ jeste Abelova gr.

II) $(2\mathbb{Z}, \cdot)$

1) Zatvorenost ✓ $2k \cdot 2l = 2 \cdot (2kl)$
2) Asoc. ✓
3) Nema neutralni element $1 \notin 2\mathbb{Z}$
4) Nema inverzni
5) Važi kom.

III) Važi distributivnost

$\Rightarrow$ Komutativan prsten

c) $(\mathbb{R}, +, \cdot)$

I) $(\mathbb{R}, +)$ Abelova

II) $(\mathbb{R}, \cdot)$

1), 2), 3) ✓
4) $\forall x \in \mathbb{R} \setminus \{0\} \quad \exists \frac{1}{x}$
5) ✓

$\Rightarrow$ $(\mathbb{R}, +, \cdot)$ je polje

d), e) slično

Scanned by TapScanner

Primjeri.

$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$

I) $(\mathbb{Z}_m, +_m)$ - Abelova gr.

II) $(\mathbb{Z}_m, \cdot_m)$ → zatvorenost ✓
→ asocijativnost ✓
→ neutralni je $\overline{1}$

III) Distributivnost ✓

$(\mathbb{Z}_m, +_m, \cdot_m)$ - prsten (komutativan, sa jedinicom)

$\mathbb{Z}_6 \setminus \{\overline{0}\}$

$\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$

Tvrđenje: $(\mathbb{Z}_p, +_p, \cdot_p)$ je polje $\Longleftrightarrow$ p je prost

1. Neka je $(R, +, \cdot)$ prsten sa jedinicom, u kojem važi da je $(x+y)^2 = x^2 + y^2$ $\forall x, y \in R$. Dokazati da je R komutativan i da $(\forall x \in R)$ $2x = 0$ tj. $x + x = 0$.

$(x+y)^2 = x^2 + y^2$

$(x+y)^2 = (x+y)(x+y) = x^2 + xy + yx + y^2 =$

$= x^2 + y^2$

$$-x^2 \ \cancel{x^2} + xy + yx + \cancel{y^2} = \cancel{x^2} + \cancel{y^2} \ / -y^2$$

$(\forall x, y \in R) \quad xy + yx = 0$

$y = 1, \ \forall x \quad x \cdot 1 + 1 \cdot x = 0$

$$x + x = 0 \Rightarrow x = -x$$

$$2x = 0$$

$$xy + yx = 0$$

$$xy = -yx = yx$$

$xy = yx \Rightarrow R$ je komutativan

2. Ispitati da li je sljedeći skup, sa standardnim operacijama $+$ i $\cdot$ prsten.

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

I) $(\mathbb{Q}(\sqrt{2}), +)$ je Abelova grupa

1) $(a + b\sqrt{2}) + (c + d\sqrt{2}) = \underbrace{(a+c)}_{\in \mathbb{Q}} + \underbrace{(b+d)}_{\in \mathbb{Q}}\sqrt{2}$

2) Asoc. se prenosi iz $(\mathbb{R}, +)$

3) Neutralni je $0 = 0 + 0 \cdot \sqrt{2} \in \mathbb{Q}(\sqrt{2})$

4) $a + b\sqrt{2} \to -a - b\sqrt{2}$ je inv.

5) Komutativnost se prenosi iz $(\mathbb{R}, +)$

II) $(\mathbb{Q}(\sqrt{2}), \cdot)$

1) Zatvorenost: $(a + b\sqrt{2})(c + d\sqrt{2}) =$

Scanned by TapScanner

$= (ac + 2bd) + \sqrt{2}(bc + ad)$

2) Asoc. iz $(\mathbb{R}, \cdot)$

3) Neutralni $1 = 1 + 0 \cdot \sqrt{2} \in \mathbb{Q}(\sqrt{2})$

4) $(a + b\sqrt{2})(x + y\sqrt{2}) = 1$

$$x + y\sqrt{2} = \frac{1}{a + b\sqrt{2}}, \quad a \neq 0 \vee b \neq 0$$

$$x + y\sqrt{2} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

5) Kom. iz $(\mathbb{R}, \cdot)$

$(\mathbb{Q}(\sqrt{2}) \setminus \{0\}, \cdot)$ je takođe zatvoren $\Rightarrow$

$\Rightarrow (\mathbb{Q}(\sqrt{2}) \setminus \{0\}, \cdot)$ je Abelova grupa

III) Dist. iz $(\mathbb{R}, +, \cdot)$

$\Rightarrow (\mathbb{Q}(\sqrt{2}), +, \cdot)$ je polje

3. $S = \left\{ \frac{a}{p^n} \mid a \in \mathbb{Z}, n \in \mathbb{N} \cup \{0\}, p - \text{fix prost br.} \right\}$

Dokazati da je S podprsten prstena racionalnih brojeva.

Jasno je da je $S \subseteq \mathbb{Q}$.

I) $(S, +)$ – Abelova?

1) $\dfrac{a}{p^{n_1}} + \dfrac{b}{p^{n_2}} = \dfrac{ap^{n_2}+bp^{n_1}}{p^{n_1+n_2}} \in S$ $\left[\begin{array}{l} n_1+n_2 \in \mathbb{N}\cup\{0\} \\ ap^{n_2}+bp^{n_1} \in \mathbb{Z} \end{array}\right]$

2) Asoc. se prenosi iz $(\mathbb{Q},+)$

3) $0 = \dfrac{0}{p^1} \in S$

4) $\dfrac{a}{p^n} \in S \rightarrow$ inverz je $-\dfrac{a}{p^n} \in S$ jer $(-a) \in \mathbb{Z}$

5) Kom. iz $(\mathbb{Q},+)$

II) $(S,\cdot)$

1) $\dfrac{a}{p^{n_1}}, \dfrac{b}{p^{n_2}} \in S$

$$\frac{a}{p^{n_1}} \cdot \frac{b}{p^{n_2}} = \frac{ab}{p^{n_1+n_2}} \in S \quad \left[\begin{array}{l} ab \in \mathbb{Z} \\ n_1+n_2 \in \mathbb{N}\cup\{0\} \end{array}\right]$$

2) Asoc. iz $(\mathbb{Q},\cdot)$

3) $a=1, n=0 \Rightarrow \dfrac{a}{p^n} = \dfrac{1}{1} = 1 \in S$ jedinični

4) $q \in S$, q je prost br. i $q \neq p$

$\downarrow$ inverz

$\dfrac{1}{q} \in S$?

$$\frac{a}{p^n} = \frac{1}{q} \Rightarrow \underbrace{qa}_{\text{djeljivo sa } q} = \underbrace{p^n}_{\text{nije djeljivo sa } q} \lightning$$

$\Rightarrow \frac{1}{2} \notin S$

III) Dist. iz $(\mathbb{Q}, +, \cdot)$

$\Rightarrow (S, +, \cdot)$ je komutativan prsten sa jedinicom

4. Neka je R prsten sa jedinicom u kojem $(\forall x \in R)\ x^3 = x$. Dokazati da je $(\forall x \in R)\ 6x = 0$.

$x \in R$

$x + x \in R$

$(x+x)^3 = x + x$

$(x+x)^3 = (x+x)(x+x)(x+x) =$

$= (x^2 + x^2 + x^2 + x^2)(x+x) = \underbrace{x^3 + x^3 + x^3 + \dots + x^3}_{8} =$

$= \underbrace{x + x + \dots + x}_{8}$

Imamo da je:

$\underbrace{x + \dots + x}_{8} = x + x \ / -x / -x$

$\underbrace{x + \dots + x}_{6} = 0$

$6x = 0$

5. Odrediti sve homomorfizme prstena $(\mathbb{Z}, +, \cdot)$.

Def. $f : R_1 \to R_2$

$(R_1, +, \cdot)$, $(R_2, \oplus, \odot)$ – prsteni

$(\forall x, y \in R_1)$ $f(x+y) = f(x) \oplus f(y)$

$f(x \cdot y) = f(x) \odot f(y)$

$\Rightarrow f$ je homomorfizam

$$f(x+y) = f(x) + f(y)$$

$$f : \mathbb{Z} \to \mathbb{Z}$$

$$f(n) = n \cdot f(\underset{a}{1}) \quad \text{(od ranije)}$$

$$f(x \cdot y) = f(x) \cdot f(y)$$

$$x = y = 1$$

$$f(1) = f(1) \cdot f(1)$$

$$f(1) = (f(1))^2$$

$$a = a^2$$

$$a^2 - a = 0$$

$$a(a-1) = 0$$

$$a = 0 \lor a = 1$$

$$\downarrow \qquad \qquad \downarrow$$

$$\underline{\underline{f(x) = 0}} \qquad \underline{\underline{f(x) = x}}$$