PROPOZICIJA 2.9. Sljedeće tvrdnje su ekvivalentne

(1) Y je normalna podgrupa od X

(2) $xY \subseteq Yx, \ \forall x \in X$

(3) $xYx^{-1} \subseteq Y, \ \forall x \in X$

(1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1)

trivijalno

(2) $\Rightarrow$ (3)

$xY \subseteq Yx \ / \cdot x^{-1}$

$xYx^{-1} \subseteq Y\underbrace{xx^{-1}}_{e}$

(3) $\Rightarrow$ (1)

$xYx^{-1} \subseteq Y \ / \cdot x$

$xY \subseteq Yx$

$xY = Yx \quad \forall x$

$x \cdot / \ x^{-1}Yx \subseteq Y$

$Yx \subseteq xY$

PRIMJER 2.13. $H = \left\{ \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} : b \in \mathbb{R} \right\}$

a) $H \leq GL(2, \mathbb{R})$ regularna matrica reda 2 nad $\mathbb{R}$

b) $H \ntrianglelefteq GL(2, \mathbb{R})$

$\hookrightarrow$ nije normalna podgrupa

a) $A, B \in H \qquad AB^{-1} \in H$

$A = \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} \qquad AB^{-1} = \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -b & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ a-b & 1 \end{bmatrix}$

$\in H$

$\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ b & 1 & 0 & 1 \end{array} \right) \overset{(-b)}{\underset{+}{\sim}} \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & -b & 1 \end{array} \right) \rightarrow b^{-1} = \begin{bmatrix} 1 & 0 \\ -b & 1 \end{bmatrix}$

b) $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in GL(2, \mathbb{R})$

$B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in H$

$ABA^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ ne pripada H

$H \ntrianglelefteq GL(2, \mathbb{R})$

Zadaća $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$

Dokažite da je

(1) $H \leq S_3$

(2) $H \ntrianglelefteq S_3$

Y normalna podgrupa od X

X/Y

$[x_1][x_2] = [x_1 x_2]$

$[x_1'] = [x_1]$

$[x_2'] = [x_2]$

$\Downarrow$

$[x_1' x_2'] = [x_1 x_2]$

$x_1' = x_1 y_1$

$x_2' = x_2 y_2$ $\quad y_1, y_2 \in Y$

$x_1' x_2' = x_1 y_1 \cdot x_2 y_2 = x_1 x_2 \cdot \underbrace{y_1' \cdot y_2}_{\in Y}$

$Yx_2 = x_2 Y$

jer ima normalnu podgrupu

$y_1 x_2 = x_2 y_1', \quad y_1' \in Y$

$[x_1 x_2] = [x_1' x_2']$

očito $([x_1][x_2])[x_3] = [x_1]\cdot([x_2][x_3])$

zbog asocijativnosti u G

neutralni $[e]$ $[e][x] = [ex] = [x] = [x][e]$

inverz $[x]^{-1} = [x^{-1}]$

$(X/Y, \cdot)$ kvocijentna grupa

$q : X \to X/Y$

$q(x) = [x]$

kvocijentni homomorfizam

NAPOMENA 2.5. Ako je X abelova onda je i X/Y abelova

PRIMJER 2.14. Neka je $n \in \mathbb{N}$

a) $n\cdot\mathbb{Z} = \{nz : z \in \mathbb{Z}\} \subseteq \mathbb{Z}$

$(n\mathbb{Z}, +) \triangleleft (\mathbb{Z}, +)$

↳ Abelova

$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$

b) S_n A_n - parna permutacija

$A_n \triangleleft S_n$, $n \geq 3$

(ne treba znat)

DEFINICIJA 2.11. $f : X \to Y$ homomorfizam grupa

jezgra homomorfizma f je

$$\mathrm{Ker}\, f = \{x \in X,\ f(x) = e_Y\}$$

$\to$ slika homomorfizma

$$\mathrm{Im}\, f = \{f(x),\ x \in X\}$$

LEMA 2.10. $\mathrm{Ker}\, f \leq X$, $\mathrm{Im}\, f \leq Y$

DOKAZ a) $a, b \in \mathrm{Ker}\, f$ $\qquad ab^{-1} \in \mathrm{Ker}\, f$

$$f(a) = e_Y \ , \ f(b) = e_Y$$

$$f(ab^{-1}) = f(a) \cdot f(b^{-1}) = e_Y \cdot (f(b))^{-1} = e_Y \cdot e_Y^{-1} = e_Y$$

b). $\mathrm{Im}\, f \leq Y$

$y_1, y_2 \in Y$

$y_1 y_2^{-1} \in Y$

$y_1 = f(x_1)$

$y_2 = f(x_2)$

$$y_1 y_2 = f(x_1) \cdot (f(x_2))^{-1} = f(x_1) \cdot f(x_2^{-1})$$
$$= f(x_1 x_2^{-1}) \in \mathrm{Im}\, f$$

LEMA 2.11. $\mathrm{Ker}\, f \trianglelefteq X$

$K = \mathrm{Ker}\, f$

$xKx^{-1} \subseteq K \quad \forall x \in X$

$u \in xKx^{-1} \qquad u = xk^{-1}x \qquad k \in \mathrm{Ker}\, f$

$$f(u) = f(xk^{-1}x) = f(x)\underbrace{f(k)}_{e_Y}f(x^{-1}) = f(x) \cdot f(x^{-1}) = f(xx^{-1}) = f(e_X) = f(e_Y)$$

$\Rightarrow u \in \mathrm{Ker}\, f$

NAPOMENA 2.6. Slika $\mathrm{Im} f$ općenito nije normalna podgrupa od Y

DEFINICIJA 2.12. $f: X \to Y$ homom. grupa

(1) f injekcija - monomorfizam

(2) f surjekcija - epimorfizam

(3) f bijekcija - izomorfizam

PRIMJER 2.15. $K_4 = \{1, -1, i, -i\}$ $(K_4, *)$

$$f: (\mathbb{Z}, +) \to (K_4, \cdot), \quad f(x) = i^x$$

dokazati da je preslikavanje homomorfizam i naći jezgru

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

$$f(x+y) = i^{x+y} = i^x \cdot i^y = f(x) \cdot f(y)$$

$$\mathrm{Ker}\, f = \{x \in \mathbb{Z}, f(x) = 1\} = \{x, i^x = 1\} = 4\mathbb{Z}$$

PRIMJER 2.16. a) dokažite da postoji izomorfizam $(\mathbb{R}, +)$ i $(\mathbb{R}^+, \cdot)$

b) dokažite da ne postoji izomorfizam $(\mathbb{Q}, +)$, $(\mathbb{Q}^+, \cdot)$

a) $f(x) = e^x$

$f: \mathbb{R} \to \mathbb{R}^+$

bijekcija

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

$$f(x+y) = e^{x+y} = e^x e^y = f(x) f(y)$$

b) $g: \mathbb{Q} \to \mathbb{Q}^+$

pretp. suprotno $\quad g$: izomorfizam

$\exists x \in \mathbb{Q}, \; g(x) = 2$

$$g(x) = g\left(\frac{x}{2} + \frac{x}{2}\right) = g\left(\frac{x}{2}\right) g\left(\frac{x}{2}\right) = \left[g\left(\frac{x}{2}\right)\right]^2 = 2 \Rightarrow g\left(\frac{x}{2}\right) = \sqrt{2}$$

kontradikcija

Zadaća Dokažite da grupe $(\mathbb{Q},+)$, $(\mathbb{Z},+)$ nisu izomorfne

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

$x \quad , \quad f(x) = 1$

$f\left(\frac{x}{2} + \frac{x}{2}\right) = 1$

$f\left(\frac{x}{2}\right) + f\left(\frac{x}{2}\right) = 2f\left(\frac{x}{2}\right) = 1$

$f\left(\frac{x}{2}\right) = \frac{1}{2}$

kontradikcija

LEMA 2.12. Homomorfizam $f: X \to Y$ je injekcija ako i samo ako je $\operatorname{Ker} f = \{e_X\}$

$\Rightarrow$ f injekcija $\to$ $\operatorname{Ker} f = \{e_X\}$

kaže Krnić: „očito je, zar ne?"

$\Leftarrow$ $\operatorname{Ker} f = \{e_X\}$

$f(a) = f(b) \quad / \cdot (f(b))^{-1}$

$f(a) \cdot (f(b))^{-1} = e_Y$

$f(ab^{-1}) = e_Y$

$ab^{-1} = e_Y$

$ab^{-1} = e_X \quad / \cdot b$

$a = b$

Zadaća: Dokažite da grupe $(\mathbb{R}^*, \cdot)$ i $(\mathbb{C}^*, \cdot)$ nisu izomorfne

TEOREM 2.13. TM o izomorfizmu grupa

$f: X \to Y$ homomorfizam grupa

Tada $\exists$ jedinstveni monomorfizam

$\bar{f}: X/\ker f \to Y$ takav da je

$\bar{f} \circ g = f$, $g: X \to X/\ker f$ kvocijentni homomorfizam

ako je f epimorfizam $\Rightarrow$ $\bar{f}$ izomorfizam

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "g"'] & Y \\ X/\ker f \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

PRIMJER 2.17. $(\mathbb{R}, +)/(\mathbb{Z}, +) \overset{\text{izomorfno}}{\simeq} (S^1, \cdot)$

S^1 – jedinična kružnica

$f: \mathbb{R} \to S^1$

$f(x) = \cos(2\pi x) + i\sin(2\pi x) = e^{2\pi i x}$

f očito surjekcija :)

f – homomorfizam

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

$$f(x+y) = e^{2\pi i (x+y)} = e^{2\pi i x} e^{2\pi i y} = f(x) \cdot f(y)$$

$$\cos 2\pi x + i \sin 2\pi x = 1$$

$$x \in \mathbb{Z} \quad \ker f = \mathbb{Z}$$

$$\operatorname{Im} f \quad (\mathbb{R}, +)/\underbrace{\ker f}_{= (\mathbb{Z}, +)} \simeq (S^1, \cdot)$$

TEOREM 2.14. (Cayley)

Svaka grupa X je izomorfna nekoj podgrupi grupe $B(X)$ svih bijekcija skupa X na samog sebe

$a \in X \qquad f_a : X \to X \qquad f_a(x) = ax$

$f_a \in B(X)$

$a \to f_a$

monomorfizam

DEFINICIJA 2.13. $(G, *)$, $(H, \cdot)$ grupe

$G \times H = \{(g, h), g \in G, h \in H\}$

$G \times H$ je grupa uz binarnu operaciju

$(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2)$

neutralni element od $G \times H$ (e_G, e_H)

Zadatak Na skup $S = \{(a,b) \in \mathbb{R}^2, a \neq 0\}$

$(a,b) * (c,d) = (ac, ad+b)$

dokažite $(S,*)$ grupa, da li je abelova?

$(a,b) \in S, \quad (c,d) \in S$

$(a,b) * (c,d) \in S$

$= (ac, ad+b)$ zatvorenost ✓

ASOCIJATIVNOST $((a,b) * (c,d)) * (e,f) = (ac, ad+b) * (e,f)$

$= (ace, acf + b + ad)$

$(a,b) * ((c,d) * (e,f)) = (a,b) * (ce, cf+d) = (ace, acf + b + ad)$

neutralni element

$(a,b) * (x,y) = (a,b)$

$(ax, ay+b) = (a,b)$

$ax = a \Rightarrow x = 1$

$ay+b = b \Rightarrow ay = 0 \rightarrow y = 0$

neutralni element $(1,0)$

$(a,b) * (x,y) = (1,0)$

$(ax, ay+b) = (1,0)$

$ax = 1 \rightarrow x = \frac{1}{a}$

$ay+b = 0 \rightarrow y = \frac{-b}{a}$

inverz $(a,b)^{-1} = \left(\frac{1}{a}, \frac{-b}{a}\right)$

nije abelova! $(c,d) * (a,b) = (ca, bc+d)$

PRIMJER 2.18. Da li su grupe

a) $\mathbb{Z}_2 \times \mathbb{Z}_2$ i $\mathbb{Z}_4$ izomorfne?

b) $\mathbb{Z}_2 \times \mathbb{Z}_3$ i $\mathbb{Z}_6$ izomorfne?

a) $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$

$f(1) = (a,b)$

$$f(2) = f(1 +_4 1) = f(1) \oplus f(1) = (a,b) \oplus (a,b)$$
$$= (a +_2 a, b +_2 b)$$
$$= (0,0)$$

$f(2) = (0,0)$ ali $f(0) = (0,0)$ f nije injekcija $\rightarrow$ NIJE izom.

b) $f: \mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_6$ $\quad f(a,b) = 3a +_6 2b$

f: bijekcija

$f(0,0) = 0 +_6 0 = 0$

$f(0,1) = 0 +_6 2 = 2$

$f(0,2) = 0 +_6 4 = 4$

f je bijekcija – preslikali su se svi u različite

$f(1,0) = 3 +_6 0 = 3$

$f(1,1) = 3 +_6 2 = 5$

$f(1,2) = 3 +_6 4 = 1$

$f(a,b) * (c,d) = f(a +_2 c, b +_3 d) = 3(a +_2 c) +_6 2(b +_3 d)$

$x \equiv x' \pmod 2$

$3x \equiv 3x' \pmod 6 \to 3a +_6 3c$

$= (3a +_6 3c) +_6 (2b +_6 2d)$

$\hookrightarrow x \equiv x' \pmod 3$

$2x \equiv 2x' \pmod 6$

$(3a +_6 2b) +_6 (3c +_6 2d)$

$f(a,b) +_6 f(c,d)$

Pr. 2.19. pogledati

2.2. PRSTENI I POLJA

DEFINICIJA 2.14. Prsten je skup $\mathbb{R}$ zajedno sa dvije binarne operacije $+$ i $\cdot$ tako da je:

(1) $(\mathbb{R},+)$ abelova grupa

(2) $(\mathbb{R},\cdot)$ polugrupa

(3) $x(y+z)=xy+xz$ i $(x+y)z=xz+yz$, $\forall x,y,z\in\mathbb{R}$

distributivnost množenja prema zbrajanju

NAPOMENA 2.7. $0\cdot a=a\cdot 0=0$

$$a\cdot 0=a(0+0)=a\cdot 0+a\cdot 0 \quad /-a\cdot 0$$

$$0=a\cdot 0$$

neutralni element za množenje (ako postoji) $\rightarrow 1$

PRIMJER 2.20. (1) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ prsteni

komutativni prsteni

(2) M_n - prsten uz $\cdot$, $+$

(3) $\mathbb{Z}_m$ prsten uz $+_m$, $\cdot_m$

komutativni prsteni

prsteni sa jedinicom

(4) Prsten polinoma

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

$$p(t)=a_nt^n+a_{n-1}t^{n-1}+\dots+a_1+a_0$$

$$a_0,a_1,\dots,a_n\in\mathbb{R},\ n\in\mathbb{N}_0$$

zbrajanje i množenje polinoma

$(R[t], +, \cdot)$ - prsten polinoma

Pr. 2.21. Dokažimo da u prstenu s jedinicom komutativnost zbrajanja slijedi iz ostalih aksioma

$(a+1)(b+1) = (a+1)b + (a+1)1 = ab + b + a + 1$

$(a+1)(b+1) = a(b+1) + 1(b+1) = ab + a + b + 1$

$a + b = b + a$

Pr. 2.22. Ako svi elementi komutativnog prstena P imaju zajednički djelitelj d onda P ima jedinicu

$\forall x \quad x = dy$

specijalno za $x = d \quad d = d \cdot e$

$\underline{e \cdot x} = e \cdot (dy) = e \cdot d \cdot y = \underbrace{d \cdot e}_{d} \cdot y = dy = x$

$\downarrow$

komutativnost

$e = 1$

DEFINICIJA 2.15. Homomorfizam prstena

$(R, +, \cdot) \quad (P, +, \cdot)$ prsteni

$f : R \to P$ je homomorfizam prstena ako je

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

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

Predavanje 9

DEFINICIJA 2.16. $(R, +, \cdot)$ prsten

$P \subseteq R$ potprsten ako je on prsten s obzirom na $+, \cdot$

KRITERIJ ZA POTPRSTEN

$x, y \in P \qquad x - y \in P$
$\qquad\qquad\quad x \cdot y \in P$

Zadatak Dokažite da je skup $P = \{a + b\sqrt[3]{3} + c\sqrt[3]{9},\ a, b, c \in \mathbb{Z}\}$ prsten uz uobičajeno zbrajanje i množenje realnih brojeva.

$(P, +, \cdot)$ potprsten $(R, +, \cdot)$

$x, y \in P \qquad x - y \in P$
$x \cdot y \in P \qquad x \cdot y \in P$

$x = a_1 + b_1\sqrt[3]{3} + c_1\sqrt[3]{9}$
$y = a_2 + b_2\sqrt[3]{3} + c_2\sqrt[3]{9}$

$$x - y = \underbrace{(a_1 - a_2)}_{\in \mathbb{Z}} + \underbrace{(b_1 - b_2)}_{\in \mathbb{Z}}\sqrt[3]{3} + \underbrace{(c_1 - c_2)}_{\in \mathbb{Z}}\sqrt[3]{9} \quad \in P \ ✓$$

$$x \cdot y = (a_1 + b_1\sqrt[3]{3} + c_1\sqrt[3]{9})(a_2 + b_2\sqrt[3]{3} + c_2\sqrt[3]{9})$$

$$= a_1a_2 + a_1b_2\sqrt[3]{3} + a_1c_2\sqrt[3]{9} + b_1\sqrt[3]{3}a_2 + b_1\sqrt[3]{3}b_2\sqrt[3]{3} + b_1\sqrt[3]{3}\cdot c_2\sqrt[3]{9} + c_1\sqrt[3]{9}a_2 + c_1\sqrt[3]{9}b_2\sqrt[3]{3} + c_1\sqrt[3]{9}\cdot c_2\sqrt[3]{9}$$

$$= \underbrace{(a_1a_2 + 3b_1c_2 + 3c_1b_2)}_{\in \mathbb{Z}} + \underbrace{(a_1b_2 + b_1a_2 + 3c_1c_2)}_{\in \mathbb{Z}}\sqrt[3]{3} + \underbrace{(a_1c_2 + b_1b_2 + c_1a_2)}_{\in \mathbb{Z}}\sqrt[3]{9}$$

$\in P$ ✓

IDEAL I u prstenu R je potprsten sa svojstvom da $\forall x \in R$ vrijedi

$$xI \subseteq I \quad i \quad Ix \subseteq I$$

$I \subseteq R$ ideal

$\hookrightarrow$ $(I,+)$ abelova grupa

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

$R/I = \{x+I, x \in R\}$

$(x+I)+(x'+I) = x+x'+I$

Definiramo množenje

$(x+I)(x'+I) = xx'+I = x_1x_1'+I$

treba dokazati da je množenje dobro definirano

$x_1 \sim x \quad x_1' \sim x'$ tj. $x_1 = x+y \quad x_1' = x'+y' \quad y, y' \in I$

$$x_1x_1' = (x+y)(x'+y') = xx' + \underbrace{\underbrace{xy'}_{\in I} + \underbrace{yx'}_{\in I} + \underbrace{yy'}_{\in I}}_{\in I}$$

$x_1x_1' \sim xx'$

$(R/I, \oplus, \odot)$ – kvocijentni prsten po idealu I

PRIMJER 2.23. $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$

$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, \ldots\}$

$n\mathbb{Z} = \{\ldots -3n, -2n, -n, 0, n, 2n, \ldots\}$

$\rightarrow R$ komutativni prsten s jedinicom

$(a) = Ra = \{ra : r \in R\}$ – ideal

$\hookrightarrow$ najmanji ideal generiran s a

$\hookrightarrow$ glavni ideal u R

DEFINICIJA 2.18.

R komutativni prsten s jedinicom tada je $(a_1, a_2, \dots, a_n)$ najmanji ideal generiran elementima $a_1, a_2, \dots, a_n$

PROPOZICIJA 2.16. $(a_1, a_2, \dots, a_n) = \{ \sum_{i=1}^{n} x_i a_i , x_i \in R \}$

dokaz neće biti u ispitu jer je trivijalan

DEFINICIJA 2.17.

Prsten glavnih ideala $\rightarrow$ svi ideali glavni

trivijalni ideali su $\{0\}$ i R

PRIMJER 2.24.

$I \subseteq \mathbb{Z}$ ideal

$I \neq \{0\}$

$I \neq \mathbb{Z}$

$d = \min \{a \in I, a > 0\}$

$n \in I$ podijeliti sa d

$n = qd + r \quad , \quad 0 \leq r < d$

$\underbrace{n - qd}_{\in I} = \underbrace{r}_{\in I} \Rightarrow r = 0$

$n = qd$ tj. $I = (d)$

PROPOZICIJA 2.17. U prstenu $\mathbb{Z}$ vrijedi $(m, n) = (d)$ $d = nzd(m, n)$

ne treba dokaz

DEFINICIJA 2.19. R prsten $x \in R \setminus \{0\}$ $\exists y \in R \setminus \{0\}$

t.d. je $xy = 0 \Rightarrow$ x djelitelj nule)

INTEGRALNA DOMENA - domena je prsten s 1 u kojem nema djelitelja nule

$(\mathbb{Z}_6, +, \cdot)$ nije integralna domena $\rightarrow 2 \cdot 3 = 0$

TEOREM 2.18. $\mathbb{Z}_m$ je integralna domena $\Leftrightarrow$ m prost

DOKAZ: m složen $\quad m = a \cdot b \quad 1 < a, b < m$

$[a], [b] \neq 0 \quad [a][b] = [ab] = [m] = [0] \Rightarrow \mathbb{Z}_m$ nije integralna domena

m prost $\quad a, b \quad [a] \neq 0 \quad [b] \neq 0$

$\Rightarrow [a][b] = 0 \Rightarrow [ab] = 0 \Rightarrow m | ab \Rightarrow m | a$ ili $m | b$ tj. $[a] = 0$ ili $[b] = 0$

$\Rightarrow \Leftarrow$

DEFINICIJA 2.20. $(R, +, \cdot)$ prsten s 1

$a \in R$ je invertibilan ako $\exists\, b \in R \quad ab = ba = 1 \quad (b = a^{-1})$

R^* - skup svih invertibilnih elem. u $R \quad (R^*, \cdot)$

$\downarrow$

grupa jedinica prstena R

DEFINICIJA 2.21. Prsten s jedinicom u kojem je svaki element $x \neq 0$ invertibilan tj. $(R \setminus \{0\}, \cdot)$ grupa se naziva TIJELO

Komutativno tijelo $\rightarrow$ POLJE

Primjer: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

POLJA

$(\mathbb{Z}, +, \cdot)$ - polje? NIJE POLJE

invers od $3 \rightarrow 3 \cdot \frac{1}{3}$

$\hookrightarrow \frac{1}{3}$ ne leži u $\mathbb{Z}$

$\hookrightarrow$ ne postoji invers

PROPOZICIJA 2.19. Sljedeća svojstva su invarijantna s obzirom na izomorfizam prstena

a) komutativnost

b) posjedovanje jedinice

c) biti integralna domena

d) biti tijelo

e) biti polje

$f : (P_1, +, \cdot) \to (P_2, +, \cdot)$ f-izomorfizam

DOKAZ: a) $(P_1, +, \cdot)$ kom. prsten

T. $(P_2, +, \cdot)$ kom. prsten

$a, b \in P_2$ $\quad ab = ba$

f izomorfizam

$f : P_1 \to P_2$

$\exists x, y \in P_1$

$f(x) = a$

$f(x) = b$

$$ab = f(x)\, f(y) \overset{izom}{=} f(xy) \overset{P_1 \text{ komut}}{=} f(yx) = f(y) \cdot f(x) = ba$$

c) $ab \in P_2$ $\quad ab = 0$

$$0 = ab = f(x) f(y) \overset{izom.}{=} f(xy)$$

$xy \in Ker f \Rightarrow xy = 0 \overset{P_1 \text{ int. dom.}}{\Longrightarrow} x = 0$ ili $y = 0 \Rightarrow$

$f(x) = 0$ ili $f(y) = 0$

$a = 0$ $\quad b = 0$

u ispit može doći bilo koji od dokaza a-e

(ostale dokaze pogledati u skripti str. 65, 66)

PRIMJER 2.26. $M_2[\mathbb{R}]$ $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ ima polje izom. $(\mathbb{C}, +, \cdot)$

$(M_n, +, \cdot)$ - prsten

$(X, +, \cdot)$ - potprsten od $(M_2[\mathbb{R}], +, \cdot)$

$A, B \in X$ $\quad A - B \in X$ $\quad A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ $\quad B = \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$

$AB \in X$

$$A - B = \begin{bmatrix} a-c & -(b-d) \\ b-d & a-c \end{bmatrix} \in X$$

$$AB = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} c & -d \\ d & a \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{bmatrix} \in X$$

skup X potprsten

$$\underbrace{f}_{\text{izomorfizam}} : (\mathbb{C}, +, \cdot) \to \overbrace{(X, +, \cdot)}^{\text{prsten}} \qquad f(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

$$f((a+ib) + (c+id)) = f(a+c+i(b+d)) = \begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix}$$

$$= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = f(a+bi) + f(c+id)$$

$$f((a+bi)(c+di)) = f(ac-bd+(ad+bc)i) =$$

$$= \begin{bmatrix} ac-bd & -bc-ad \\ bc+ad & ac-bd \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} c & -d \\ d & c \end{bmatrix}$$

$$= f(a+bi) \cdot f(c+di)$$

<u>KRITERIJ ZA (POT)POLJE</u>

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

$X \subseteq \mathbb{R}$ je potpolje ako $\to$ $\forall a, b \in X$

$a - b \in X$

$ab' \in X$

PRIMJER 2.27. $P = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$ polje

$(P, +, \cdot)$ potpolje od $(\mathbb{R}, +, \cdot)$

$(x, y) \in P$ $\qquad x = a + b\sqrt{2}$ $\quad a, b$ / c, d $\in \mathbb{Q}$

$x - y \in P$ $\qquad y = c + d\sqrt{2}$

$xy^{-1} \in P$

$y \neq 0$

$$x - y = \underbrace{(a - c)}_{\in \mathbb{Q}} + \underbrace{(b - d)}_{\in \mathbb{Q}}\sqrt{2} \in P$$

$$xy^{-1} = \left(\frac{a + b\sqrt{2}}{c + d\sqrt{2}}\right) \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}}$$

$$= \frac{ac - ad\sqrt{2} + bc\sqrt{2} - 2db}{c^2 - 2d^2}$$

$$= \underbrace{\frac{ac - 2bd}{c^2 - 2d^2}}_{\in \mathbb{Q}} + \underbrace{\frac{bc - ad}{c^2 - 2d^2}}_{\in \mathbb{Q}}\sqrt{2}$$

$c^2 - 2d^2 = 0 \Rightarrow c^2 = 2d^2$

$\frac{c^2}{d^2} = 2 \Rightarrow \frac{c}{d} = \pm\sqrt{2}$

$\hookrightarrow$ nije moguće jer su c i $d \in \mathbb{Q}$

PRIMJER 2.28. Čine li brojevi oblika $a + b\sqrt[3]{2}$ $a, b \in \mathbb{Q}$ polje?

npr. $a = 0$ $\quad b = 1$

$\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$

da li postoje $a, b \in \mathbb{Q}$ t.d. je $a + b\sqrt[3]{2} = \sqrt[3]{4}$?

ne postoji

(pogledati u skripti) – str. 67

ZADATAK a) $P = \{a + b\sqrt[3]{3} + c\sqrt[3]{9},\ a,b,c \in \mathbb{Z}\}$ prsten

b) da li je P polje?

nije – inverz od $3 \to \frac{1}{3}$

↳ nije unutar $\mathbb{Z}$

$3 = 3 + 0\sqrt[3]{3} + 0\sqrt[3]{9}$

c) za zadaću $P = \{a + b\sqrt[3]{3} + c\sqrt[3]{9},\ a,b,c \in \mathbb{Q}\}$

da li je P polje, ako je dokažite

NAPOMENA 2.8.

a) u svakom tijelu i polju jednadžbe $ax = b$ i $ya = b$, $a \neq 0$ imaju uvijek jedinstveno rješenje

$a \neq 0 \quad \exists a^{-1} \quad ax = b \Rightarrow x = a^{-1}b$

b) svako tijelo je integralna domena

$ab = 0$ i $a \neq 0 \quad \exists a^{-1} \Rightarrow a^{-1}ab = a^{-1} \cdot 0 = 0$

$b = 0$

c) u tijelu nema pravih ideala

$I \subseteq \mathbb{R}$ ideal $I \neq \{0\}$

$\exists a \neq 0 \in I \qquad \underbrace{a^{-1}a}_{\in I} \in I \Rightarrow 1 \in I$

$x \in \mathbb{R} \qquad x \cdot 1 \in I$

$x \in I$

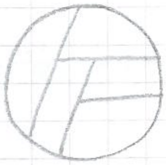
$\mathbb{R} \subseteq I \qquad I = \mathbb{R}$

PREDAVANJE 8

$Y \leq X$ podgrupa

$x \sim x \iff \exists y \in Y$ t.d. je $x = x'y$

relacija ekvivalencije



$[x]$ - klase ekvivalencije

Propozicija 2.5. $[x] = xY = \{xy : y \in Y\}$

DOKAZ: $[x] \leq xY$

$x' \in [x] \Rightarrow x' = xy$, $y \in Y \rightarrow x' = xy \in xY$

$xy \in [x]$

$x' \in xY$, $x' = xy$, $y \in Y \Rightarrow x' = [x]$

Napomena $[e] = eY = \{ey, y \in Y\} = \{y, y \in Y\} = Y$

$[x]$ - lijeva klasa po podgrupi Y

$$X = \bigcup_{x \in X} [x] = \bigcup_{x \in X} xY$$

Propozicija 2.6. Svaka lijeva klasa xY ima isti kardinalni broj

DOKAZ: $\phi : Y \rightarrow xY$

$\phi(y) = xy$ $\quad$ x fiksan

surjektivnost $\quad y \in xY \quad y = xy'$, $y' = y$

$\phi(y') = xy' = y$

bijektivnost $\quad \phi(y_1) = \phi(y_2)$

$xy_1 = xy_2 \rightarrow y_1 = y_2$ $\quad$ ϕ je bijekcija

DEFINICIJA 2.9. Kvocijentni skup $X/\sim$

lijevi kvocijentni skup grupe X po podgrupi $Y \rightarrow X/Y$

Kardinalni broj od X/Y zove se indeks podgrupe Y u grupi X i označava se $[X:Y]$

PROPOZICIJA 2.7. $k(X) = [X:Y] \cdot k[Y]$

↳ kad je grupa X konačan skup

KOROLAR 2.8. (Lagrange)

Ako je X konačna grupa, a Y podgrupa od X

(1) red podgrupe dijeli red grupe X

(2) red svakog elementa $x \in X$ dijeli red od X

$|a| = n \qquad a^n = e \qquad \{e, a, a^2, \ldots, a^{n-1}\}$

NAPOMENA!

Eulerov teorem - specijalni slučaj Lagrangeovog teorema

$(\mathbb{Z}_m^*, \cdot_m)$

↳ svi brojevi manji od m koji su relativno prosti sa m

- red te grupe je $\varphi(m)$

$\forall a \in \mathbb{Z}_m^* \rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

Analogno definiramo desne klase Yx

$$k(Yx) = k(xY) = k(Y), \quad \forall x \in X$$

ali ne mora vrijediti $\rightarrow \quad Yx = xY$

DEFINICIJA 2.10. Podgrupa $Y \leq X$ je normalna ako je:

$$xY = Yx \quad \forall x \in X$$

↳ oznaka $Y \trianglelefteq X$

b) Odredi cikličku podgrupu generiranu sa 12 $(\mathbb{Z}_{15}, +_{15})$

$|\mathbb{Z}_{15}| = 15$

$12 +_{15} 12 = 9$

$9 +_{15} 12 = 6$

$6 +_{15} 12 = 3$

$3 +_{15} 12 = 0$

$\{0, 3, 6, 9, 12\}$

Koliki je red elementa 12?

$12x \equiv 0 \pmod{15} \; / :3$

$4x \equiv 0 \pmod{5}$

$x = 5$

najmanji $x \in \mathbb{N}$

c) 12 $(\mathbb{Z}_{17}, +_{17})$ $|\mathbb{Z}_{17}| = 17$ → prost broj

ciklička podgrupa je cijela grupa!
(ili trivijalna)

↳ NIJE TRIVIJALNA jer u podgrupi mora biti i neutralni element 0

d) 12 $(\mathbb{Z}_{13}^*, \cdot_{13})$ $|\mathbb{Z}_{13}^*| = 12$

$12 \cdot_{13} 12 = 1$

$\{1, 12\}$

Zadaća Odredi red elementa 12 u $(\mathbb{Z}_{17}^*, \cdot_{17})$

red elementa: 2, 4, 8, 16

NAPOMENA 2.4. X abelova $\Rightarrow$ svaka podgrupa je normalna

u bilo kojoj grupi G postoji barem dvije normalne podgrupe

podgrupe $\left.\begin{array}{l}\{e\} - \text{TRIVIJALNA} \\ G\end{array}\right\}$ trivijalne, normalne podgrupe

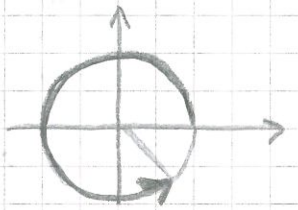
X - prosta ako nema netrivijalnih normalnih podgrupa

ZADATAK Odredi cikličku podgrupu generiranu zadanim elementom

a) $\dfrac{1-i}{\sqrt{2}}$ $(\mathbb{C}^*, \cdot)$

$$\frac{1-i}{\sqrt{2}} = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i$$

$$= \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}$$



$\cdot 3$ $\cdot 2$

$$a^2 = \cos\frac{7\pi}{2} + i\sin\frac{7\pi}{2} = -i$$

$$a^3 = \cos\frac{21\pi}{4} + i\sin\frac{21\pi}{4} = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i$$

$$a^4 = \cos 7\pi + i\sin 7\pi = -1$$

$$a^5 = \cos\frac{35\pi}{4} + i\sin\frac{35\pi}{4} = \frac{-\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

$$a^6 = \cos\frac{21\pi}{2} + i\sin\frac{21\pi}{2} = i$$

$$a^7 = \cos\frac{49\pi}{4} + i\sin\frac{49\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

$$a^8 = \cos 14\pi + i\sin 14\pi = 1$$

$$\{1, a, a^2, a^3, a^4, a^5, a^6, a^7\}$$

red elementa je 8

$|\mathbb{C}^*| = \infty$