– Zadaci –

22. X 1986.

1. Dokazati da je $\cong$ relacija ekvivalencije na klasi alg. struktura jezika L.

Dokaz:

$\mathcal{K}(L)$ – klasa svih algebri jezika L [kolekcija / klasa / skup]

– klasa ne može biti element druge klase

(R) $\mathcal{A} \cong \mathcal{A}$; $i_A : \mathcal{A} \cong \mathcal{A}$

(S) $\mathcal{A} \cong \mathcal{B} \Rightarrow \exists \varphi : \mathcal{A} \cong \mathcal{B} \Rightarrow \exists \Psi : \mathcal{B} \cong \mathcal{A}$; $\Psi = \varphi^{-1} \Rightarrow \mathcal{B} \cong \mathcal{A}$

(T) $\mathcal{A} \cong \mathcal{B}$, $\mathcal{B} \cong \mathcal{C} \Rightarrow \exists \varphi : \mathcal{A} \cong \mathcal{B} \wedge \Psi : \mathcal{B} \cong \mathcal{C}$

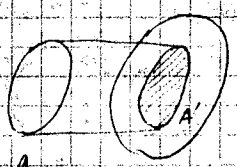
$\Rightarrow \exists \theta : \mathcal{A} \cong \mathcal{C}$; $\theta = \Psi \circ \varphi$

$\Rightarrow \mathcal{A} \cong \mathcal{C}$

QED

---

2. Neka je $\varphi : A \to B$ utapanje. Dokazati da postoji podalg. $\mathcal{A}' \subseteq \mathcal{B}$, tako da je $\mathcal{A}' \cong \mathcal{B}$.



Dokaz:

$A' = \{ \varphi(x) \mid x \in A \} = \varphi(A) = \mathrm{Im}\,\varphi$

$a_1', \dots, a_n' \in A' \Rightarrow F^{\mathcal{B}}(a_1', \dots, a_n') \in A'$ (?)

PP: $a_1', \dots, a_n' \in A' \Rightarrow (\exists a_1, \dots, a_n \in A)\ \varphi(a_i) = a_i'$ $(1 \le i \le n)$

$F^{\mathcal{B}}(a_1', \dots, a_n') = F^{\mathcal{B}}(\varphi(a_1), \dots, \varphi(a_n))$

$= \varphi(F^{\mathcal{A}}(a_1, \dots, a_n)) \in A' = \varphi(A)$

$F^{\mathcal{A}'}(a_1', \dots, a_n') \overset{def}{=} F^{\mathcal{B}}(a_1', \dots, a_n')$, $a_1', \dots, a_n' \in A'$

$F^{\mathcal{A}'}$ je restrikcija $F^{\mathcal{B}}$ na A'.

$c \in \mathrm{Const}_L \Rightarrow c^{\mathcal{B}} = \varphi(c^{\mathcal{A}}) \Rightarrow c^{\mathcal{B}} \in \varphi(A) = A'$

$c^{\mathcal{A}'} = c^{\mathcal{B}}$

$\mathcal{A}' = (A', F^{\mathcal{B}}|A', \dots, c^{\mathcal{B}}, \dots)$

QED

---

3. Proveriti da li je klasa svih polja varijetet.

Rešenje:

$\mathcal{F}$ = klasa svih polja

$(Q, +, \cdot, 0, 1)$

PP: Q je varijetet: $\mathbb{Z} \subseteq Q \wedge \mathbb{Z} \notin \mathcal{F}$ # $\Rightarrow \mathcal{F}$ nije varijetet

$(\forall x)\ x \neq 0 \Rightarrow (\exists y)\ xy = 1$ — ne može se zamijeniti skupom alg. identiteta

4. Neka je Z skup celih brojeva i F unarni oper. znak, $L = \{+, F\}$.

1° Dokazati da postoji formula predikatskog računa jezika L koja definiše operaciju množenja u alg. $(Z, +, F^2)$, ako je $F^2(x) = x^2$.

2° Dokazati da ne postoji term t jezika L tako da je $x \cdot y = t^Z(x,y)$ $(x,y \in Z)$, i $F^2(x) = x^2$.

3° Dokazati da ne postoji formula PR jez. L koja definiše operaciju množenja F^2, ako je $F^2(x) = x^3$.

Dokaz:

1° $z = x \cdot y \Leftrightarrow \varphi(x, y, z, +, F^2)$

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

$z = x \cdot y \Leftrightarrow (x+y)^2 = x^2 + z + z + y^2 \Leftrightarrow F^2(x+y) = F^2(x) + z + z + F^2(y)$

2° $t(x, y, +, F^2) = x \cdot y$ $(\neg\exists)$

SP: $\dfrac{\partial xy}{\partial x \partial y} = 1$, $t \in Term_L \Rightarrow 2 \mid \dfrac{\partial t}{\partial x \partial y}(0, \ldots, 0)$ (indukcijom po $sl(t)$)

$\dfrac{\partial x}{\partial x \partial y} = 0$, $\dfrac{\partial (x+y)}{\partial x \partial y} = \dfrac{\partial x}{\partial x \partial y} + \dfrac{\partial y}{\partial x \partial y}$

$\dfrac{\partial u^2}{\partial x \partial y} = 2\dfrac{\partial u \frac{\partial u}{\partial x}}{\partial y}$

3° $\varphi : x \mapsto -x$, $\varphi \in Aut(Z, +, \cdot)$ jer je $(-x)^3 = -x^3$

$\Phi(a_1, \ldots, a_n) \Leftrightarrow \Phi(\varphi(a_1), \ldots, \varphi(a_n))$

29 X 1986

- Zadaci -

1 Dokazati da asocijativni zakon nije posledica zakona.

$$(x(yz))t = (xy)z)t$$
$$= (xy)(zt)$$
$$= x(y(zt))$$
$$= x((yz)t)$$

Dokaz: minimalni nosioci $\cdot$: 0, c, $c*c$, $(c*c)*c$, $c*(c*c)$ (svi različiti)

$\cdot$	0	c	$(c*c)$	$(c*c)*c$	$c*(c*c)$
0	0	0	0	0	0
c	0	$c*c$	$c*(c*c)$	0	0
$(c*c)$	0	$(c*c)*c$	0	0	0
$(c*c)*c$	0	0	0	0	0
$c*(c*c)$	0	0	0	0	0

$L = \{*, 0\}$

$S = \{0, c, c*c, (c*c)*c, c*(c*c)\}$

$S = (S, \cdot, 0)$

$l(u)$ – broj pojavljivanja simbola c u izrazu u

$u^S[\lambda] = 0$ ako je $l(u) \geq 4$

1° $u \cdot 0 = 0, \quad 0 \cdot u = 0 \quad (u \in S)$

2° $u \cdot v = \begin{cases} 0, & l(u*v) \geq 4 \\ u*v, & l(u*v) < 4 \end{cases}$

U S važe zakoni $((x*y)*z)*t = (x*(y*z))*t = \ldots$ (po def. „$\cdot$")

Asocijativni zakon ne važi: $(x \cdot y) \cdot z \neq x \cdot (y \cdot z)$

$(c*c)*c = c*(c*c)$ ⊥ QED

– može: $0 = 0, \quad 1 = c, \quad 2 = (c*c), \quad 3 = (c*c)*c, \quad 4 = c*(c*c)$

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	2	4	0	0
2	0	3	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0

$(\{0,1,2,3,4\}, \cdot) \models (x \cdot y) \cdot z = x \cdot (y \cdot z)$

$(1 \cdot 1) \cdot 1 = 3$

$1 \cdot (1 \cdot 1) = 4$ $\Big\}$ $\neq$

2. Dokazati da grupoid G ima idempotentan elemenat akko za svaki grupoid H postoji $\varphi: H \to G$ (homomorfizam).

(a – idempotentan $\overset{def}{\iff}$ $a^2 = a$)

Dokaz:

($\Rightarrow$): $a \in G$ idempotentan; H-grupoid; $\varphi: H \to G$, $\varphi(x) = a$ $(x \in H)$

$\varphi(xy) = a, \quad \varphi(x)\varphi(y) = a \cdot a = a \Rightarrow \varphi(xy) = \varphi(x)\varphi(y) \quad (\forall x, y \in H)$

($\Leftarrow$) $(\{1\}, \cdot)$, $1 \cdot 1 = 1$, $\varphi: H \to G$, $a = \varphi(1)$

$a \cdot a = \varphi(1) \cdot \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) = a$ QED

3. Dokazati da svaki konačan grupoid zadovoljava neki netrivijalan zakon.

$L = \{\cdot\}$, Zakon $u = v$ je netrivijalan ako su u, v različite reči.

Dokaz:

$(A, *) = A$ konačan grupoid

$\varphi_0(x) = x * x \quad (x \in A)$

$\varphi_1(x) = (x * x) * x \quad (x \in A)$

$\varphi_2(x) = \varphi_1(x) * x \quad (x \in A)$

$\vdots$

$\varphi_n(x) = (\ldots(x * x) * \ldots * x) * x$

$S = \{\varphi_0, \varphi_1, \varphi_2, \ldots\}$, $\varphi \in S \Rightarrow \varphi : A \to A \Rightarrow \varphi \in A^A \Rightarrow S \subseteq A^A$

A - konačan $\Rightarrow A^A$ - konačan $\Rightarrow S$ - konačan

$\exists m, n,\ m \neq n : \varphi_m = \varphi_n$, npr. : $\varphi_2 = \varphi_3 \Leftrightarrow x * x = (x * x) * x \quad (\forall x \in A)$

QED

$\Rightarrow$ važi zakon: $xx = (x \cdot x) \cdot x$

4. Dokazati da postoji grupoid koji zadovoljava sve zakone jezika $L = \{\cdot\}$.

Dokaz: Trivijalan grupoid.

5. Ako je $u = v$ netrivijalan zakon jezika $\{\cdot\}$, onda postoji konačan grupoid koji ne zadovoljava taj zakon.

Dokaz: (ideja)

$S = \{0\} \cup \{t \in Term \mid t$ je podterm od u ili t je podterm od $v\}$

S je konačan skup

operacija $*$ na S: 1) $0 * t = 0, \quad t * 0 = 0 \quad (t \in S)$

$l(t)$ - broj simbola u t,

2) $t_1 * t_2 = \begin{cases} (t_1 \cdot t_2), & \text{ako je } l(t_1 \cdot t_2) \leq n \\ 0, & \text{ako je } l(t_1 \cdot t_2) > n \end{cases}$

$n = \max\{l(u), l(v)\}$

Važi: Ako je $l(t) \leq n$, onda je $t^A[\lambda] = t$, za $\lambda(x) = x \ (x \in Var)$

Otuda sledi $u^A[\lambda] = u$, $v^A[\lambda] = v$, ali u, v su različiti termi,

pa je $u^A[\lambda] \neq v^A[\lambda]$ tj. $(S, \cdot) \not\models u = v$

QED

Dopuna: $t = (x*y)*(z*u) = t_1 * t_2$

podtermi: $x, y, z, u, (x*y), (z*u), t$

$\{x, y, z, u, (x*y), (z*u), t\}$

$x \cdot y = x * y$

$t^S[\lambda] = t_1^S \cdot t_2^S = (t_1^S * t_2^S) = (x*y)*(z*u) = t$

$\lambda(x) = x$ ako $x \in S$ $\wedge$ $\lambda(x) = 0$ ako $x \notin S$ netrivijalan

6. Dokazati da postoji grupoid koji ne zadovoljava ni jedan V alg. zakon

Dokaz:

$R_0 = \emptyset$, $R_{n+1} = R_n \cup \mathcal{P}(R_n)$, $R_\omega = \bigcup_{n \in N} R_n$, $L = \{*\}$

$a, b \in R_\omega \Rightarrow (a,b) \in R_\omega$

$G = (R_\omega, \cdot)$, $a \cdot b \overset{def}{=} (a,b)$ (grupoid)

(1) $a_1 b_1 = a_2 b_2 \Rightarrow a_1 = a_2 \wedge b_1 = b_2$

A) Indukcijom po $\max\{sl(u), sl(v)\}$ dokazujemo (potpunom)

ako $G \models u = v$, onda su u i v isti termi

D: IH: tvrdnja važi za $\max\{sl(u), sl(v)\} < n$ $(\forall u, v \in Term_L)$

Neka su $u, v \in Term_L$, $\max\{sl(u), sl(v)\} = n$, i pretpostavimo

$G \models u = v$

$n = 0$: $u, v \in Var \Rightarrow u = v$ (zato je G trivijalan grupoid)

$n > 0$: $sl(u) = n$, $u \equiv u_1 * u_2$

$u^G[\lambda] \equiv (u_1^G[\lambda], u_2^G[\lambda])$,

$G \models u = v \Rightarrow v^G[\lambda] = u^G[\lambda]$, pa je v oblika $v = (v_1 * v_2)$

$u_1^G[\lambda] \cdot u_2^G[\lambda] = v_1^G[\lambda] \cdot v_2^G[\lambda]$

Prema (1): $u_1^G[\lambda] = v_1^G[\lambda] \wedge u_2^G[\lambda] = v_2^G[\lambda]$

(IH) $\Rightarrow$ u_1 i v_1 su isti termi i u_2 i v_2 su isti termi QED

7. Neka je A neprazan skup i $\mathcal{A} = (A^A, \circ, id_A)$. Dokazati:

(1) $f \in A^A$ je levo invertibilan akko je f 1-1 presl.

(2) $f \in A^A$ je desno " " " f NA "

(3) Ako je A konačan skup, tada: f je levo invertibilan

akko je f desno invertibilan.

Def: $G = (G, \cdot, 1)$

$a \in G$ je levo invertabilan $\overset{def}{\Leftrightarrow} (\exists b \in G)\ b \cdot a = 1$

$a \in G$ je desno " $\overset{def}{\Leftrightarrow} (\exists b \in G)\ a \cdot b = 1$

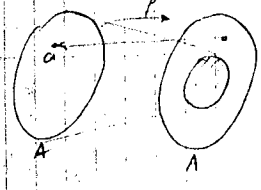
Dokaz:

(1) $f \in A^A$ je levo inv. $\Leftrightarrow (\exists g \in A^A)\ g \circ f = i_A$

($\Rightarrow$): PP f je levo inv. $\Rightarrow (\exists g \in A^A)\ g \circ f = i_A$

$f(x) = f(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow i_A(x) = i_A(y) \Rightarrow x = y$.

($\Leftarrow$) PP: $f \in A^A$ je 1-1



$g \in A^A$: $g = f^{-1} \cup \{(z, a) \mid z \in A \setminus f(A)\}$

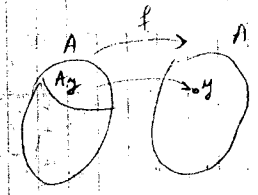
$$g(x) = \begin{cases} f^{-1}(x), & \text{ako } x \in f(A) \\ a, & \text{ako } x \notin f(A) \end{cases}$$

$(g \circ f)(x) = g(f(x)) = f^{-1}(f(x)) = x \Rightarrow g \circ f = i_A$ za $x \in A$.

(2) f je desno inv. $\Leftrightarrow (\exists g \in A^A)\ f \circ g = i_A$ 5. XI 1986.

($\Leftarrow$) $A \supseteq f(A) \supseteq f(g(A))$, $g: A \to A$, $f \circ g = i_A$

$\therefore \quad = i_A(A) = A \Rightarrow f(A) = A$



($\Rightarrow$) f je NA , $A_y = f^{-1}(\{y\})$

$(\forall y \in A)\ A_y \neq \emptyset$, $\{A_y \mid y \in A\}$ particija skupa A, jer:

1° $(\forall y \in A)\ A_y \neq \emptyset$

2° $y \neq y' \Rightarrow A_y \cap A_{y'} = \emptyset$

3° $\bigcup_{y \in A} A_y = A$

Aksioma izbora: Za svaku particiju $\{A_y \mid y \in A\}$ nekog skupa X postoji transverzala (izborni skup) T za odlikom:

$(\forall y \in A)\ |T \cap A_y| = 1$.

T - transverzala za familiju $\{A_y \mid y \in A\}$

$T = \{g(y) \mid y \in A\}$, $T \cap A_y = \{g(y)\} \Rightarrow g: A \to A$

$f(g(y)) = y$, jer $g(y) \in f^{-1}(\{y\}) \Rightarrow f \circ g = i_A$.

(3) Dirichleov princip: A je konačan $\Rightarrow f \in A^A$ 1-1 $\Leftrightarrow f$ je NA

($\Rightarrow$) $f: A \xrightarrow{1-1} A$, ST f nije NA, tj. neka je $a \in A \setminus f(A)$

↓

$S = \{a, f(a), f^2(a), f^3(a), \ldots\} \subseteq A$, $a \neq f(a)$ jer $a \notin f(A)$

$a \neq f^2(a)$, $a \neq f^n(a)$ $(n \geq 2)$

$f^i(a) = f^j(a)$, $i = j+k$ $(k>0)$ $\overset{1-1}{\Rightarrow}$ $f^k(a) = a$ #

$\Rightarrow$ S je beskonačan skup # $\Rightarrow$ f je NA

$(\Leftarrow)$ $f : A \xrightarrow{NA} A$

(2) $\Rightarrow$ $(\exists g \in A^A)\ f \circ g = 1_A$

(1) $\Rightarrow$ g je 1-1 $\Rightarrow$ g je NA, tj. bijekcija

$\Rightarrow$ $(f \circ g) \circ g^{-1} = 1_A \circ g^{-1} = g^{-1}$

$\Rightarrow$ $f \circ 1_A = g^{-1} \Rightarrow f = g^{-1} \Rightarrow f$ je 1-1 a.e.d.

((3) može i indukcijom po $\mathrm{card}\, A$)

-Zadaci-

1. (1) Opisati $Aut(Z,+,0)$

(2) Dokazati da je $(End(Z,+,0), \circ, 1_A) \cong (Z, \cdot, 1)$

Rešenje:

(1) $\varphi \in Aut(Z,+,0) \Rightarrow \varphi : Z \xrightarrow[NA]{1-1} Z$, $\varphi(0) = 0$, $\varphi(x+y) = \varphi(x) + \varphi(y)$ $(x,y \in Z)$

$\varphi(1+1) = \varphi(1) + \varphi(1)$, $\varphi(2) = 2\varphi(1)$

$n \in N$: $\varphi(n) = n \cdot \varphi(1)$

$0 = \varphi(0) = \varphi(n + (-n)) = \varphi(n) + \varphi(-n)$ $\Rightarrow$ $\varphi(-n) = -\varphi(n) = -n\varphi(1)$

$\Rightarrow$ $(\forall x \in Z)\ \varphi(x) = x \cdot \varphi(1)$, $a = \varphi(1)$

$\Rightarrow$ $(\forall x \in Z)\ \varphi(x) = ax$

X φ je NA : $\varphi(x) = 1$ ima rešenja po x

$\Rightarrow$ $ax = 1$ ima rešenja $\Rightarrow$ $a \in \{1, -1\}$

$\varphi(x) = x$, $\psi(x) = -x$

$\Rightarrow$ $Aut(Z,+,0) = \{\varphi, \psi\}$

(2) $A = End(Z,+,0) = \{\varphi : Z \to Z \mid \varphi(x) = ax$, za neko $a \in Z\}$

$f : A \to Z$, $f(\varphi) = a \overset{def}{\Leftrightarrow} \varphi(x) = ax$

(i) $\varphi, \psi \in A$; $\varphi(x) = ax$, $\psi(x) = bx$ $\Rightarrow$ $(\varphi \circ \psi)(x) = abx$

$\Rightarrow$ $f(\varphi \circ \psi) = ab = f(\varphi) \cdot f(\psi)$

(ii) $i_A : A \to A$; $i_A(x) = x = 1 \cdot x \Rightarrow f(i_A) = 1$

(iii) $f(\varphi) = f(\Psi) \Rightarrow a = b \Rightarrow \varphi = \Psi$: f je 1-1

(iv) $c \in Z$: $\chi(x) = cx$, $\chi : Z \to Z$, $\chi \in A$

$f(\chi) = c$: f je NA

(i) – (iv) $\Rightarrow$ $f : (End(Z,+,0), \circ, i_A) \cong (Z, \cdot, 1)$

$\Rightarrow$ $(End(Z,+,0), \circ, i_A) \cong (Z, \cdot, 1)$ QED

– Zadaci –

12. XI 1986.

1. Neka je $A = (A, +, 0)$ Abelova grupa i neka je $End\, A = (End A, +, \circ, \mathcal{O}, i_A)$, gde je $(\forall x \in A)\ \mathcal{O}(x) = 0$, i_A je identičko preslikavanje skupa A, i $(\forall x \in A)(\varphi + \Psi)(x) = \varphi(x) + \Psi(x)$; $\circ$ je slaganje f-ja.

Dokazati da je $End\, A$ prsten sa jedinicom.

(prsten endomorfizama sa jedinicom)

2. Dokazati: $End(Z,+,0) \cong (Z, +, \cdot, 0, 1)$

Dokaz: $\varphi \in End(Z,+,0) \Rightarrow \varphi(x) = ax$

$f : End(Z,+,0) \to Z$, $f(\varphi) = \varphi(1)$

$f(\varphi + \Psi) = (\varphi + \Psi)(1) = \varphi(1) + \Psi(1) = f(\varphi) + f(\Psi) \Rightarrow$ QED

3. Odrediti $Aut(Q, +, \cdot, 0, 1)$

Rešenje:

$\varphi \in Aut(Q, +, \cdot, 0, 1)$

$x \in Z_+ \Rightarrow \varphi(x) = x \cdot \varphi(1)$; $0 = \varphi(0) = \varphi(x + (-x)) = \varphi(x) + \varphi(-x)$

$\Rightarrow \varphi(-x) = -x \cdot \varphi(1)$

$\Rightarrow (\forall x \in Z)\ \varphi(x) = x \cdot \varphi(1)$

$p, q \in Z,\ q > 0$ $x = \frac{p}{q}$ $q\varphi(x) = \underbrace{\varphi(x) + \dots + \varphi(x)}_{q} = \varphi(qx) = \varphi(q\frac{p}{q}) = \varphi(p)$

$\Rightarrow \varphi(\frac{p}{q}) = \frac{p}{q}\varphi(1)$

$(\forall x \in Q)\ \varphi(x) = x \cdot \varphi(1)$

$\varphi \in Aut(Q, +, \cdot, 0, 1) \Rightarrow \varphi(x) = ax$, $a \neq 0$

$\varphi(1) = 1 \Rightarrow a = 1$

$Aut(Q, +, \cdot, 0, 1) = \{ i_Q \}$

2° $(End(Q,+,0), \circ, i_Q) \cong (Q, \cdot, 1)$, 2° $End(Q,+,0) \cong (Q, +, 0, 1)$

4. Opisati skup $Aut(R,+,\cdot,0,1)$.

Rešenje: $Aut(R,+,\cdot,0,1) = \{i_R\}$.

(1) $\varphi \in Aut(R,+,\cdot,0,1) \Rightarrow \varphi \uparrow$

PP: $\varphi \in Aut(R,+,\cdot,0,1)$

$(\forall x \in Q)\ \varphi(x) = x$ $\varphi(1) = x$, jer je $\varphi(1) = 1$

$\varphi|_Q = i_Q$

$x < y \Rightarrow y = x + a^2$ za neki $a \neq 0$ iz R

$\Rightarrow \varphi(y) = \varphi(x + a^2) = \varphi(x) + \varphi(a^2)$

$= \varphi(x) + \varphi(a)\cdot\varphi(a) = \varphi(x) + \varphi(a)^2 \Rightarrow \varphi(x) < \varphi(y)$, jer je $\varphi(a)^2 > 0$

$x \in R$; $(x_n) \in Q^N$, $x_n \uparrow$, $(y_n) \in Q^N$, $y_n \downarrow$; $\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n = x$

$x_n \le x \le y_n \Rightarrow \varphi(x_n) \le \varphi(x) \le \varphi(y_n)$ $(\forall n \in N)$

$\Rightarrow x_n \le \varphi(x) \le y_n$ $(\forall n \in N)$

$\Rightarrow x \le \varphi(x) \le x \Rightarrow \varphi(x) = x$ QED

(*) $\mathbb{C} = (C,+,\cdot,0,1)$; $|Aut\,\mathbb{C}| = 2^c$

$\varphi|_R = i_R \Rightarrow Aut_1\mathbb{C} = \{i_C, -\}$ (za domaći)

5. Cauchy-eva funkcionalna jednačina

$f(x+y) = f(x) + f(y)$ $(x,y \in R)$ (J)

1° $f|_Q = i_Q$

$f(qx) = qf(x)$, $q \in Q$, $x \in R$

$(R,+,0)$ je VP nad Q

(rešiti (J) je isto što i opisati sve LP VP $(R,+,0)$)

Hamelova baza je maksimalna baza prostora $(R,+,0)$.

$\{x_i \mid i \in I\}$; $(\forall x \in R)(\exists!\, q_i \in Q)\ x = \sum_{i=1}^{n} q_i x_i$

$Card\,R > \aleph_0 \Rightarrow Card\,I > \aleph_0$ $(Card\,R = 2^{\aleph_0} = c)$

1) (uslov neprekidnosti): $f(x) = ax$

1) $f \subset R$: $x \in Q \Rightarrow f(x) = xf(1)$, $f(x) = ax$, $f(1) = a$

$\overline{Q} = R \Rightarrow f(x) = ax$ $(\forall x \in R)$

2) (uslov monotonosti): $f(x) = ax$ $(a \ge 0$ za $f \uparrow\downarrow)$

3) (uslov ograničenosti na realnom intervalu)

$(\forall a<b\in R)(\exists L\in R)(\forall x\in[a,b])\ |f(x)|\le L$ (za domaći)

$\Rightarrow f(x)=ax$. (Darbu)

6. $|X|=n$; $(\mathcal{P}(X);\cup,\cap,^c,\emptyset,X)=\mathbb{P}(X)$

Dokazati: $(Aut\,\mathbb{P}(X),\circ,^{-1})\cong S_n$ (S_n – grupa permutacija skupa od n elem)

7. $\mathcal{B}$ – konačna Bulova algebra $\Rightarrow$ $\mathcal{B}\cong\mathbb{P}(X)$ za neki X.

---

6. Rešenje: $X=\{a_1,\dots,a_n\}$ $(i\neq j\Rightarrow a_i\neq a_j)$, $|X|=n$

$f\in Aut\,\mathbb{P}(X)$, $A\in\mathcal{P}(X)$, $A=\{a_{i_1},\dots,a_{i_k}\}$, $|A|=k\le n$

$f(A)=f(\{a_{i_1},\dots,a_{i_k}\})$

$=f(\{a_{i_1}\}\cup\dots\cup\{a_{i_k}\})$

$=f(\{a_{i_1}\})\cup\dots\cup f(\{a_{i_k}\})$

$\Rightarrow$ Svaki automorfizam $f\in Aut\,\mathbb{P}(X)$ jednoznačno je određen svojim preduostima na singltonima.

$F:X\to X$, F je 1-1 i NA ; $f:\mathcal{P}(X)\to\mathcal{P}(X)$

$f(\{x\})=\{F(x)\}$ i $f(\emptyset)=\emptyset$, tj. $f(A)=\bigcup_{a\in A}\{F(a)\}$

$f(A)=f(B)\Rightarrow f(\{a_{i_1},\dots,a_{i_k}\})=f(\{a_{i_{k+1}},\dots,a_{i_n}\})$

$\Rightarrow\{F(a_{i_1}),\dots,F(a_{i_k})\}=\{F(a_{i_{k+1}}),\dots,F(a_{i_n})\}$

$\Rightarrow A=B$ (1-1)

Skup $\mathcal{P}(X)$ je konačan $\Rightarrow$ f je NA

$f(A\cap B)=f(\{a_{i_1},\dots,a_{i_k}\}\cap\{a_{j_1},\dots,a_{j_\ell}\})$

$=f(\{a_{m_1},\dots,a_{m_\ell}\})$

$=\{F(a_{m_1}),\dots,F(a_{m_\ell})\}$

$f(A)\cap f(B)=\{F(a_{i_1}),\dots,F(a_{i_k})\}\cap\{F(a_{j_1}),\dots,F(a_{j_\ell})\}$

$=\{F(a_{m_1}),\dots,F(a_{m_\ell})\}$ $\Rightarrow$ $f(A\cap B)=f(A\cap B)$

$f(A\cup B)=f(A)\cup f(B)$, $f(A^c)=f(A)^c$ $\Rightarrow$ $f\in Aut\,\mathbb{P}(X)$

Svaki automorf. $f\in Aut\,\mathbb{P}(X)$ određen je jednom bijekcijom $F:X\to X$.

$\varphi: Aut\,\mathbb{P}(X)\to S_n$

$\varphi(f)=(k_1,\dots,k_n)\overset{def}{\Leftrightarrow}F(a_i)=a_{k_i}$ $(1\le i\le n)$

$\varphi(f) = \varphi(g) \Leftrightarrow F = G \Rightarrow f = g$, 1-1

$(k_1, \dots, k_n) \in S_n$; $F(a_i) = a_{k_i}$ $(1 \le i \le n)$, $F: X \to X$, $f(\{a_i\}) = \{F(a_i)\}$

$f \in \mathrm{Aut}\,\mathbb{P}(X) \wedge \varphi(f) = (k_1, \dots, k_n)$, NA

$f \in \mathrm{Aut}\,\mathbb{P}(X)$, $\varphi(f) = (k_1, \dots, k_n)$, $F(a_i) = a_{k_i}$ $(1 \le i \le n)$

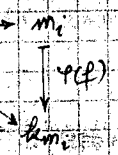
$g \in \mathrm{Aut}\,\mathbb{P}(X)$, $\varphi(g) = (m_1, \dots, m_n)$, $G(a_i) = a_{m_i}$; $(1 \le i \le n)$

$$(f \circ g)(\{a_i\}) = f(g(\{a_i\}))$$
$$= f(\{G(a_i)\}) = f(\{a_{m_i}\})$$
$$= \{F(a_{m_i})\}$$
$$= \{a_{k_{m_i}}\} \quad (1 \le i \le n) \quad ; \quad \varphi(i_{\mathrm{Aut}\,\mathbb{P}(X)}) = i_S$$

$\varphi(f \circ g) = (k_{m_1}, \dots, k_{m_n})$

$\varphi(f) \circ \varphi(g) = (k_1, \dots, k_n) \circ (m_1, \dots, m_n)$

$= (k_{m_1}, \dots, k_{m_n})$



$\Rightarrow \varphi(f \circ g) = \varphi(f) \circ \varphi(g)$

$\Rightarrow$ φ je izomorfizam $(\mathrm{Aut}\,\mathbb{P}(X), \circ, i)$ na $(S_n, \circ, i_S)$

$\Rightarrow (\mathrm{Aut}\,\mathbb{P}(X), \circ, i) \cong (S_n, \circ, i_S)$ QED

(*) Dokazati da je skup

$$\mathrm{Aut}_1\,\mathbb{C} = \{ f \in \mathrm{Aut}\,\mathbb{C} \mid f|R = i_R \} = \{ i_{\mathbb{C}}, \bar{} \},$$

gde je $\mathbb{C} = (C, +, \cdot, 0, 1)$, a $\bar{}$ operacija konjugovanja.

Dokaz:

$f \in \mathrm{Aut}_1\,\mathbb{C}$; $f|R = i_R \Rightarrow \mathrm{Re}\, f(x) = \mathrm{Re}\, x$

$f(i) \cdot f(i) = f(i^2) \Leftrightarrow f(i)^2 = f(-1)$

$\Leftrightarrow f(i)^2 = -1$, jer je $f(1) = 1$

$\Leftrightarrow f(i) \in \{i, -i\}$

1° $f(i) = i$

$a, b \in R \Rightarrow f(a + ib) = f(a) + f(i) f(b)$

$= a + ib \quad \Rightarrow \quad f = i_{\mathbb{C}}$

2° $f(i) = -i$

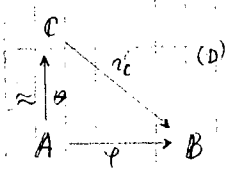
$a, b \in R \Rightarrow f(a + ib) = a - ib \quad \Rightarrow \quad f = \bar{}$

$\Rightarrow \mathrm{Aut}_1\,\mathbb{C} = \{ i_{\mathbb{C}}, \bar{} \}$ QED

19. XI 1986.

- Zadaci -

1. Neka su A, B alg. jezika L i $\varphi: A \xrightarrow{1-1} B$ (utapanje). Dokazati da postoji podalgebra $\mathbb{C} \subseteq \mathbb{B}$, tako da dijagram (D) komutira.

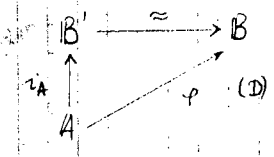


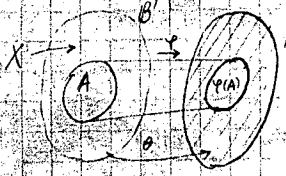
Rešenje:

$$\mathbb{C} = \varphi(\mathbb{A})$$

(Prva teorema o prenosu algebre)

2. Neka su $\mathbb{A}, \mathbb{B}$ alg. jezika L i $\varphi: A \xrightarrow{1-1} B$.
Dokazati da postoji alg. $\mathbb{B}'$ jezika L, tako da dijagram (D) komutira.





Rešenje:

Neka je X skup takav da je: $X \cap A = \emptyset$ i $|X| = |B \setminus \varphi(A)|$

$\Rightarrow (\exists \theta)\ \theta: X \xrightarrow[NA]{1-1} B \setminus \varphi(A)$

$A \subseteq B'$

Neka je $B' = A \cup X$.

Za $c \in Const_L$, $c^{B'} = c^A$

$\psi = \varphi \cup \theta$, $\psi: B' \longrightarrow B$ bijekcija ($\varphi \cap \theta = \emptyset$, $dom\,\varphi \cap dom\,\theta = \emptyset$)

$*$ - simbol binarne operacije jezika L,

$x \cdot y$ umesto $x *^{B'} y$

$x, y \in A \rightarrow x \cdot y \overset{def}{=} x *^A y$

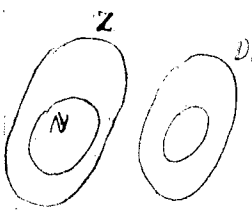
U opštem slučaju: $x \cdot y \overset{def}{=} \psi^{-1}(\psi(x) *^B \psi(y))$

$F \in Fc_n$, $ar(F) = n$

$F^{B'}(x_1, \ldots, x_n) \overset{def}{=} \psi^{-1}(F^B(\psi(x_1), \ldots, \psi(x_n)))$

Tada: 1° $\psi: \mathbb{B}' \cong \mathbb{B}$

2° $\psi | A = \varphi$, tj. (D) komutira.



dokaz: 2° važi, jer je $\psi = \varphi \cup \theta$

1° $c \in Const_L$: $\psi(c^{B'}) = \psi(c^A) = \varphi(c^A) = c^B$

Za $b_1, \ldots, b_n \in B'$, $F \in Fc_n$

$\psi(F^{B'}(b_1, \ldots, b_n)) = \psi(\psi^{-1}(F^B(\psi(b_1), \ldots, \psi(b_n)))) = F^B(\psi(b_1), \ldots, \psi(b_n))$ QED

$\uparrow$ = identifikacija, 2. je 2 teorema prenosa algebri

3. Neka je G semi-grupa sa jedinicom i $a, b \in G$ takvi da vazi:

$ab = 1$, $a^3 = a$, $b^3 = b$

Dokazati: $a = b$, $a^2 = 1$.

Dokaz:

$a = a \cdot 1 = a^3b^2$; $a^2 = a \cdot a^2 = a \cdot b$

$= a \cdot ab = ab^2 = a \cdot b$

$= a^2b = ab \cdot b = 1$ QED

$= a^2 \cdot 1 \cdot b = 1 \cdot b$

$= a^2 \cdot ab \cdot b = b$

---

4. Neka je G grupa i $a, b \in G$, takvi da: $a^7 = 1$ (1), $b^3 = 1$ (2), $ba = a^3b$ (3)

Dokazati da je: $a = 1$

Dokaz:

(Novikov — ne postoji univerzalna procedura za resavanje ovakvih zad.)

$b^3a = b^2ba$ (3) $a = b^2a^3b$ (5)

$= b^2a^3b$ (4)

(6) $b^2a^3b = bbaa^2b = \ldots = ba^3b^2$ visestrukom primenom (3)

(7) $a = ba^3b^2$ (5), (6)

(8) $a = ba^2b^2$ (1), (7)

(9) $ba^2b^2 = baab^2 = a^6b^3 = a^6$ (3), (2)

(10) $a = a^6$ (7), (9)

(11) $a^5 = 1$, $a^2 = 1$ (1), (10)

(12) $a = 1$ (11) QED

A* (za domaći): Neka je G grupa, $a, b \in G$, takvi da:

$bab = a$, $abb = b$. Dokazati $a^4 = 1$, $b^2 = a^2$.

---

5. Neka je $\langle A_i \mid i \in I \rangle$ familija alg jezika L i $A = \prod_{i \in I} A_i$,

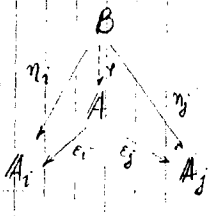
$\varepsilon_i : A \to A_i$ projekcije $(i \in I)$. Neka je B algebra jezika L

i $\eta_i : B \to A_i$ homomorfizam. Dokazati da postoji jedinstven

homomorfizam $\varphi : B \to A$, takav da je $\eta_i = \varepsilon_i \circ \varphi$ $(i \in I)$. ⊤

Dokaz:

$$\varphi(b) = \langle \eta_i(b) \mid i \in I \rangle \qquad (b \in B)$$



(1) $\varepsilon_i(\varphi(b)) = \eta_i(b)$

$\Rightarrow \quad \varepsilon_i \circ \varphi = \eta_i$

(2) $\varphi(c^B) = \langle \eta_i(c^B) \mid i \in I \rangle$

$= \langle c^{A_i} \mid i \in I \rangle = c^A$

(3) $\varphi(b_1 *^B b_2) = \langle \eta_i(b_1 *^B b_2) \mid i \in I \rangle$

$= \langle \eta_i(b_1) *^{A_i} \eta_i(b) \mid i \in I \rangle$

$= \langle \eta_i(b_1) \mid i \in I \rangle *^A \langle \eta_i(b_2) \mid i \in I \rangle$

$= \varphi(b_1) *^A \varphi(b_2)$

(jedinstvenost)

SP $(\exists \Psi)\ \varepsilon_i \circ \Psi = \eta_i$, $\Psi : B \to A$

$\Psi(b), \varphi(b) \in A$,

$\varepsilon_i(\Psi(b)) = \eta_i(b)$, $\varepsilon_i(\varphi(b)) = \eta_i(b)$ $(i \in I) \Rightarrow (\forall i \in I)\ \varepsilon_i(\Psi(b)) = \varepsilon_i(\varphi(b))$

$\Rightarrow \Psi(b) = \varphi(b) \Rightarrow \Psi = \varphi$ QED

6. Neka je m alg. varijetet jezika L i $\langle A_i \mid i \in I \rangle$ familija algebri varijeteta m, $\mathbb{C} \in m$, $\rho_i : \mathbb{C} \to A_i$ $(i \in I)$ homomorfizmi za osobinom:

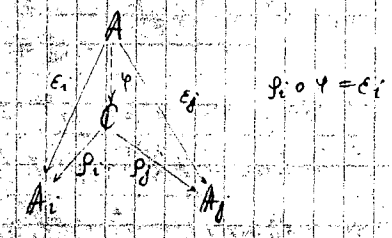
Ako je $B \in m$ i $\eta_i \in Hom(B, A_i)$, tada postoji jedinstven homomorfizam $\varphi : B \to \mathbb{C}$, takav da za sve $i \in I$ $\rho_i \circ \varphi = \eta_i$.

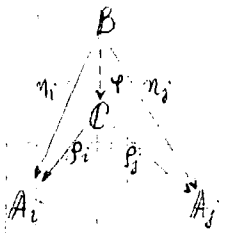
Dokazati da je $\mathbb{C} \cong \prod_{i \in I} A_i$.

(mogućnost druk̄ije def. proizvoda algebri – u teor. kategorija)

Dokaz:

$A = \prod_{i \in I} A_i$

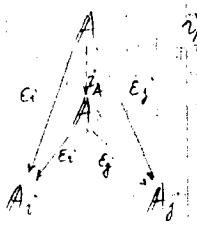




– postoji φ prema uslovu zadatka

– $\exists_1 \Psi : \mathbb{C} \to A$, $\varepsilon_i \circ \Psi = \rho_i$

$\varphi \circ \psi : A \to A$



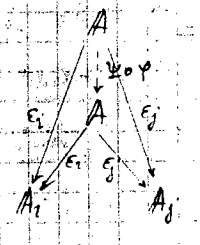
i_A – jedini homomorf. takav da ovaj dijagr. komutira

$\varepsilon_j \circ (\psi \circ \varphi) = (\varepsilon_i \circ \psi) \circ \varphi$

$= \rho_i \circ \varphi$

$= \varepsilon_i \Rightarrow$

$\Rightarrow \psi \circ \varphi = i_A$



Analogno se dokazuje: $\varphi \circ \psi = i_C$

$\Rightarrow \varphi, \psi$ su izomorfizmi.

A* Rešenje: $a, b \in G$: (1) $bab = a$; (2) $aba = b$

(3) $abab = a^2$ iz (1) množenjem slijeva sa a

(4) $abab = b^2$ iz (2) — " — zdesna sa b

(5) $a^2 = b^2$ iz (3) i (4) i tranzitivnost „=“

(6) $a^2 = bab\,bab$ iz (1)

(7) $= bab^2ab$

(8) $= ba^4b$ iz (5)

(9) $b^2 = aba \cdot aba$ iz (2)

(10) $= aba^2ba$

(11) $= ab^4a$ iz (3)

(12) $a^2 = ba^4aba$ iz (8) i (2)

(13) $= ba^5ba$

(14) $ba^5ba = ab^4a$ iz (5), (13) i (3), i tranzitivnost „=“

(15) $ba^5 = ab^3$ zakon desne kancelacije u grupi

(16) $ba^3 \cdot a^2 = ab \cdot b^2$

$= aba^2$ iz (5)

(17) $ba^3 = ab$ zakon desne kancelacije u grupi

(18) $ba^4 = aba$ množenje zdesna sa a

(19) $\quad = b$ iz (2)

(20) $a^4 = 1$ množenje slijeva sa b^{-1} QED

26. XI 1986.

- Zadaci -

1. Neka je $u = v$ zakon jezika L i neka je A algebra jez. L.
Dokazati: ako $u = v$ važi na svakoj konačno generisanoj podalgebri alg. A, onda $u = v$ važi i na alg. A.

Dokaz:

PP: $u \equiv u(x_1, \dots, x_n)$, $v \equiv v(x_1, \dots, x_n)$

Neka su $a_1, \dots, a_n \in A$ i neka je $B = \langle a_1, \dots, a_n \rangle_A$. Tada:

$$u^A[a_1, \dots, a_n] = u^B[a_1, \dots, a_n]$$
$$= v^B[a_1, \dots, a_n]$$
$$= v^A[a_1, \dots, a_n] \quad \text{QED}$$

(za domaći)

Svaki skup se može linearno urediti. (Stav kompaktnosti)

$B = (B, +, \cdot, ', 0, 1)$ je Bulova alg.

$(x+y)+z = x+(y+z)$ $\qquad$ $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

$x+y = y+x$ $\qquad$ $x \cdot y = y \cdot x$

$x+x = x$ $\qquad$ $x \cdot x = x$

$x(y+z) = (x \cdot y) + (x \cdot z)$ $\qquad$ $x + (y \cdot z) = (x+y) \cdot (x+z)$

$x+0 = x$, $x+1 = 1$ $\qquad$ $x \cdot 0 = 0$, $x \cdot 1 = x$

$x + x' = 1$ $\qquad$ $x \cdot x' = 0$

$0 \neq 1$ $\qquad$ (ne mora, jer nije identitet)

Primeri:

1.) Dokazati da je $P(X) = (P(X), \cup, \cap, ^c, \emptyset, X)$ BA.

2.) " " " $(P(X), \cap, \cup, ^c, X, \emptyset)$ BA.

3.) $\mathbb{2} = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$

4.) X – beskonačan skup $\qquad B = \{ Y \subseteq X \mid Y \text{ je konačan} \vee Y^c \text{ je konačan} \}$

$(B, \cup, \cap, ^c, \emptyset, X)$ je BA

Dokaz:

(zatvorenost)

$Y_1, Y_2 \in B \overset{?}{\Rightarrow} Y_1 \cup Y_2 \,,\; Y_1 \cap Y_2, Y_1^c, Y_2^c \in B$

1)

Y_1	Y_2	$Y_1 \cup Y_2$	
k	k	k	
k	b	b	$\Rightarrow Y_1 \cup Y_2 \in B$
b	k	b	
b	b	b	

2)

Y_1	Y_2	$Y_1 \cap Y_2$	
k	k	k	
k	b	k	
b	k	k	
b	b	b	$(Y_1 \cap Y_2)^c = Y_1^c \cup Y_2^c$ konačan

3) $Y \in B$:

Y	Y^c
k	b
b	k

QED

---

2. Neka je $B = (B, +, \cdot, ', 0, 1)$ BA. Dokazati da je:

(a) $(B, \cdot, +, ', 1, 0)$ je BA.

(b) $' : B \cong (B, \cdot, +, ', 1, 0)$.

Dokaz:

(a) $u(x_1, \ldots, x_n, +, \cdot, ', 0, 1) = v(x_1, \ldots, x_n, +, \cdot, ', 0, 1)$ važi u BA

$\Rightarrow u(x_1, \ldots, x_n, \cdot, +, ', 1, 0) = v(x_1, \ldots, x_n, \cdot, +, ', 1, 0)$

(indukcijom po $\max\{sl(u), sl(v)\}$)

(b) $(x+y)' = x' \cdot y'$; $(x \cdot y)' = x' + y'$; $0' = 1$, $1' = 0$; $x'' = x$ QED

– De Morgan

---

3. Neka je $B = (B, +, \cdot, ', 0, 1)$ BA i neka je:

$$x \leq y \overset{def}{\iff} x = x \cdot y .$$

Dokazati: (1) $(B, \leq)$ je parcijalno uređen skup.

(2) $x + y = \sup\{x, y\}$; (3) $x \cdot y = \inf\{x, y\}$

Dokaz: (1) $x \leq x$, zbog $x = x \cdot x$ (R)

(S) $x \leq y \wedge y \leq x \Rightarrow x = x \cdot y \wedge y = y \cdot x$; $xy = yx \Rightarrow x = y$

(T) $x \leq y \wedge y \leq z \Rightarrow x = xy \wedge y = yz \Rightarrow x = (xy)z = xz \Rightarrow x \leq z$

(2) $x \leq x + y$ $\quad x(x+y) = (x \cdot x) + (x \cdot y) = x + x \cdot y = x \cdot 1 + x \cdot y$

$= x \cdot (1+y) = x \cdot 1 = x$

$x, y \leq z \Rightarrow x = xz, \; y = yz \Rightarrow x + y = (xz) + (yz)$

$\Rightarrow x + y = (x+y) \cdot z \Rightarrow x + y \leq z \Rightarrow x + y = \sup\{x, y\}$.

(3) (dualno)

---

4. Neka je $B = (B, +, \cdot, ', 0, 1)$ BA. Dokazati:

(1) $x \leq y \Leftrightarrow y = x + y$

(2) $x + y = 1 \wedge xy = 0 \Rightarrow y = x'$

(3) $(x+y)' = x'y'$; $(x \cdot y)' = x' + y'$

(4) $x \leq y \Leftrightarrow y' \leq x'$

(5) $x'' = x$

Dokaz:

(1) $x \leq y \Rightarrow x = xy \Rightarrow x + y = xy + y \Rightarrow (x+1)y = x + y \Rightarrow y = x + y$

$y = x + y \Rightarrow xy = x(x+y) \Rightarrow xy = (x \cdot x) + (xy) \Rightarrow xy = x \cdot 1 + xy$

$\Rightarrow xy = x$

(2) $x + y = 1 \Rightarrow x' \cdot 1 = x'(x+y) \Rightarrow x' = (x' \cdot x) + (x'y)$

$\Rightarrow x' = 0 + x'y \Rightarrow x' \leq y$

$xy = 0 \Rightarrow x' = x' + (xy) \Rightarrow x' = (x' + x)(x' + y)$

$\Rightarrow x' = 1 \cdot (x' + y) \Rightarrow x' = x' + y \Rightarrow y \leq x'$

$\Rightarrow y = x'$

(3) $(x+y) + x'y' = (x + y + x')(x + y + y')$

$= (1+y)(1+x) = 1$

$(x+y) \cdot x'y' = x'(x'y') + y(x'y') = 0 + 0 = 0$

(2) $\Rightarrow (x+y)' = x'y'$

(4), (5) za domaći.

5. Neka je t Boole-ov term. Dokazati:

(1) U BA-ma važi:

$$t(x, x_1, \dots, x_n) = x\,t(0, x_1, \dots, x_n) + x\,t(1, x_1, \dots, x_n)$$

(2) U BA-ma važi:

$$t(x_1, \dots, x_n) = \sum_{\alpha \in 2^n} t(\alpha_1, \dots, \alpha_n)\, x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

$2 = \{0, 1\}$; $\alpha = (\alpha_1, \dots, \alpha_n)$; $x^0 = x'$, $x^1 = x$

Dokaz:

(1) Dokaz indukcijom po $sl(t)$.

$sl(t) = 0$:

(A) $t \equiv 0$, $BA \models 0 = x \cdot 0 + x \cdot 0$

(B) $t \equiv 1$, $BA \models 1 = x \cdot 1 + x' \cdot 1$

(C) $t \in Var$

$t \equiv x$ $\quad BA \models x = x \cdot 0 + x \cdot 1$

$t \equiv x_i \ (\neq x)$ $\quad BA \models x_i = x' x_i + x \cdot x_i$

Pretpostavka važi $\forall$ Term$_u$, $sl(u) < n$ $(n > 0)$

$sl(t) = n$:

(A) $t \equiv t_1 + t_2$

(B) $t \equiv t_1 \cdot t_2$ $\Big\}$ $sl(t_1), sl(t_2), sl(u) < n$

(C) $t \equiv u'$

$$t_1(x, x_1, \dots, x_n) = x' t_1(0, x_1, \dots, x_n) + x\, t_1(1, x_1, \dots, x_n)$$

$$t_2(x, x_1, \dots, x_n) = x' t_2(0, x_1, \dots, x_n) + x \cdot t_2(1, x_1, \dots, x_n)$$

(A) $t(x, x_1, \dots, x_n) = x\,t_1(0, x_1, \dots, x_n) + x\,t_1(1, x_1, \dots, x_n) +$

$x\,t_2(0, x_1, \dots, x_n) + x\,t_2(1, x_1, \dots, x_n)$

$= x'(t_1(0, x_1, \dots, x_n) + t_2(0, x_1, \dots, x_n)) + x(t_1(1, x_1, \dots, x_n) + t_2(1, x_1, \dots, x_n))$

$= x'\,t(0, x_1, \dots, x_n) + x\,t(1, x_1, \dots, x_n)$

(B) $t(x, x_1, \dots, x_n) = (x\,t_1(0, x_1, \dots, x_n) + x\,t_1(1, x_1, \dots, x_n))$

$(x'\,t_2(0, x_1, \dots, x_n) + x\,t_2(1, x_1, \dots, x_n))$

$= x' x'\,t_1(0, x_1, \dots, x_n)\, t_2(0, x_1, \dots, x_n) + x \cdot x\, t_1(1, x_1, \dots, x_n)\, t_2(1, x_1, \dots, x_n)$

$= x'\,t(0, x_1, \dots, x_n) + x\,t(1, x_1, \dots, x_n)$.

(C)

$u(x, x_1, \dots, x_n) = x'u(0, x_1, \dots, x_n) + x\,u(1, x_1, \dots, x_n)$

$(u(x, x_1, \dots, x_n))' = (x' + u(0, x_1, \dots, x_n))' \cdot (x' + u(1, x_1, \dots, x_n))'$

$= x'u'(0, x_1, \dots, x_n) + x\,u'(1, x_1, \dots, x_n) + u'(0, x_1, \dots, x_n)\,u'(1, x_1, \dots, x_n)$

$= x't(0, x_1, \dots, x_n) + xt(1, x_1, \dots, x_n)$

$BA \models x'a + xb + ab = x'a + xb$ (homework)

(2) (indukcijom po n)

$n = 1$: (1)

$n > 1$ $\quad t(x_1, \dots, x_n, x_{n+1}) = \sum_{\alpha \in 2^n} t(\alpha_1, \dots, \alpha_n, x_{n+1})\, x_1^{\alpha_1} \cdots x_n^{\alpha_n}$

(1) $\Rightarrow$ $\quad t(\alpha_1, \dots, \alpha_n, x_{n+1}) = x_{n+1}'\, t(\alpha_1, \dots, \alpha_n, 0) + x_{n+1}\, t(\alpha_1, \dots, \alpha_n, 1)$

$\Rightarrow$ $\quad t(x_1, \dots, x_n, x_{n+1}) = \sum_{\alpha \in 2^n} (x_{n+1}'\, t(\alpha_1, \dots, \alpha_n, 0) + x_{n+1}\, t(\alpha_1, \dots, \alpha_n, 1))\, x_1^{\alpha_1} \cdots x_n^{\alpha_n}$

$= \sum_{\alpha \in 2^n} t(\alpha_1, \dots, \alpha_n, 0)\, x_1^{\alpha_1} \cdots x_n^{\alpha_n} x_{n+1}' +$

$+ \sum_{\alpha \in 2^n} t(\alpha_1, \dots, \alpha_n, 1)\, x_1^{\alpha_1} \cdots x_n^{\alpha_n} x_{n+1}$

$= \sum_{\alpha \in 2^{n+1}} t(\alpha_1, \dots, \alpha_n, \alpha_{n+1})\, x_1^{\alpha_1} \cdots x_n^{\alpha_n} x_{n+1}^{\alpha_{n+1}}$ QED

Svaka konačno generisana BA je konačna. (homework)

Dokaz:

$B = (B, +, \cdot, ', 0, 1)$ BA $\quad X \subseteq B$; $|X| = n \in N$; $\langle X \rangle_B = B$

$X = \{a_1, \dots, a_n\}$; $B = \{ t^B(a_{i_1}, \dots, a_{i_k}) \mid t \in Term_L,\ k \le n,\ a_{i_1}, \dots, a_{i_k} \in X \}$

$t(x_{i_1}, \dots, x_{i_k}) = \sum_{\alpha \in 2^k} t(\alpha_1, \dots, \alpha_k)\, x_{i_1}^{\alpha_1} \cdots x_{i_k}^{\alpha_k}$, $\alpha = (\alpha_1, \dots, \alpha_k)$; $2 = \{0, 1\}$

$\Rightarrow t^B(a_{i_1}, \dots, a_{i_k}) = \sum_{\alpha \in 2^k} t^B(\alpha_1, \dots, \alpha_k)\, a_{i_1}^{\alpha_1} \cdots a_{i_k}^{\alpha_k}$, $\lambda = \begin{pmatrix} x_{i_1} \cdots x_{i_k} \\ a_{i_1} \cdots a_{i_k} \end{pmatrix}$

$t^B(\alpha_1, \dots, \alpha_k) \in \{0, 1\}$

Elemenata oblika $b_1^{\alpha_1} \cdots b_n^{\alpha_n}$ ima 2^n

" $t^B(\alpha_1, \dots, \alpha_n)$ ima $2^{2^n} = |\mathcal{P}(2^n)|$ $\Rightarrow |B| \le 2^{2^n}$ QED

3. XII 1986.

- Zadaci -

1. Neka je B BA , $a \in B \setminus \{0, 1\}$.

$B_a = (B_a, +, \cdot, {}', 0, a)$

$B_a = \{x \in B \mid x \le a\}$, $x \in B \Rightarrow x' \overset{def}{=} x'a$

(1) B_a je BA.

(2) $B \cong B_a \times B_{a'}$

Dokaz:

(1) ax, za $+$, $\cdot$ vaše

$x \in B_a$: $x'_a + x = x'a + x = x'a + ax = a(x' + x) = a \cdot 1 = a$, jer je $x \le a$, pa je $x = xa$

$x'_a \cdot x = a' \cdot x = a(x'x) = a \cdot 0 = 0$

$x + a = x$, jer je $x \le a$; $xa = a$; $\neg(B_a \subseteq B)$

(2) $\varphi : B \to B_a \times B_{a'}$; $\varphi(x) = (ax, a'x)$

$ax \le a$, $a'x \le a'$; jer je $ax = \inf\{x, a\}$

1° φ je 1-1

$\varphi(x) = \varphi(y) \Rightarrow (ax, a'x) = (ay, a'y)$

$\Rightarrow ax = ay \wedge a'x = a'y$

$\Rightarrow ax + a'x = ay + a'y$

$\Rightarrow (a + a')x = (a + a')y$

$\Rightarrow 1 \cdot x = 1 \cdot y$

$\Rightarrow x = y$

2° φ je NA

$(u, v) \in B_a \times B_{a'} \Rightarrow u \le a \wedge v \le a'$

Neka je $x = u + v$.

$x \le y \Rightarrow ax \le ay \wedge a + x \le a + y$

$\Rightarrow ax = a(u + v) = au + av = u + 0 = u$

$a'x = a'(u + v) = a'u + a'v = 0 + v = v$

Dakle : $\varphi(x) = (ax, a'x) = (u, v)$

3° φ je homomorfizam

$\varphi(x + y) = (a(x + y), a'(x + y)) = (ax + ay, a'x + a'y)$

$= (ax, a'x) + (ay, a'y)$

$= \varphi(x) + \varphi(y)$

$\varphi(x \cdot y) = (a(xy), a'(xy)) = ((ax)(ay), (a'x)(a'y)) = (ax, a'x) \cdot (ay, a'y) = \varphi(x) \cdot \varphi(y)$

$\varphi(0) = (a\cdot 0, a'\cdot 0) = (0,0) = \mathbb{0}$

$\varphi(1) = (a\cdot 1, a'\cdot 1) = (a,a') = \mathbb{1}$

Pomožno tvrdenje:

$\psi: B_1 \to B_2$, $\psi(0)=0$, $\psi(1)=1$; $\psi(x+y)=\psi(x)+\psi(y)$, $\psi(xy)=\psi(x)\cdot\psi(y)$

$\Rightarrow$ ψ je homomorfizam, tj. $\psi(x') = \psi(x)'$

Dokaz:

$$\left.\begin{aligned} 1 &= \psi(1) = \psi(x+x') = \psi(x)+\psi(x') \\ 0 &= \psi(0) = \psi(x\cdot x') = \psi(x)\cdot\psi(x') \end{aligned}\right\} \Rightarrow \psi(x') = \psi(x)'$$

$\Rightarrow$ φ je izomorfizam

QED

QES

2. Ako je $\mathbb{B}$ konačna BA, onda postoji $n\in\mathbb{N}$, tako da vrijedi:

$$\boxed{\mathbb{B} \cong 2^n}$$

Dokaz: (indukcija po $\mathrm{Card}\, B$)

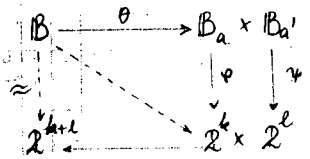
$|B| = 2 \Rightarrow \mathbb{B} \cong \mathbb{2}$

Neka je $|B| > 2$ i $a \in B \setminus \{0,1\}$. Tada je $\theta: \mathbb{B} \cong \mathbb{B}_a \times \mathbb{B}_{a'}$.

$|B_a| < |B|$ i $|B_{a'}| < |B|$ jer $1 \notin B_a, B_{a'}$

IH $\Rightarrow \varphi: \mathbb{B}_a \cong \mathbb{2}^k$, $\psi: \mathbb{B}_{a'} \cong \mathbb{2}^l$

$\Rightarrow$ $\mathbb{B} \cong \mathbb{2}^k \times \mathbb{2}^l \cong \mathbb{2}^{k+l}$



$\varphi \times \psi: B_a \times B_{a'} \to 2^k \times 2^l$

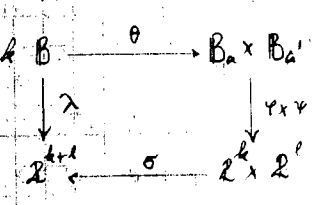
$(\varphi\times\psi)(x,y) = (\varphi(x), \psi(y))$ izomorfizam

$\sigma: 2^k \times 2^l \to 2^{k+l}$ izomorfizam

$\sigma((x_1,\dots,x_k),(y_1,\dots,y_l)) = (x_1,\dots,x_k,y_1,\dots,y_l)$

$\lambda = \sigma\circ(\varphi\times\psi)\circ\theta$ izomorfizam

homework



QED

3. Neka je $u = v$ zakon jezika $L = \{+,\cdot,',0,1\}$. Dokazati:

Ako $u = v$ vrijedi na $\mathbb{2}$, onda on vrijedi na svim BA.

Dokaz: $\mathbb{2} \models u = v$

(1) $u = v$ vrijedi na svim konačnim BA $\mathbb{B}$, jer je $\mathbb{B} \cong \mathbb{2}^n$

(2) $u = v$ " " " konačno generisanim BA, jer je svaka

. konačno generisana BA konačna.

(3) Ostalo poznatom zadatku $\Rightarrow$ QED.

Primer: $BA \models xy + xz + yz = (x+y)(x+z)(y+z)$

- diskusijom po $x \in \{0,1\}$

---

4. Dokazati: $(X \cap Y) \cup (X \cap Z) \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) \cap (Y \cup Z)$

Dokaz:

$X, Y, Z \in B$, $B = \mathbb{P}(S)$, $S = X \cup Y \cup Z$ QED

(homework) Ako neki identitet jezika $\{\wedge, \vee\}$ važi u 2 (dvočlanoj BA) važi i u svakoj distributivnoj mreži.

---

5. Ako je B konačna BA, tada postoji X, tako da važi $B \cong \mathbb{P}(X)$.

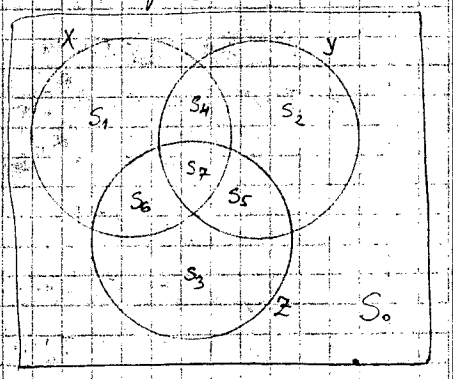
Dokaz:

$|B| < \aleph_0 \Rightarrow (\exists n \in N) \varphi\ B \cong 2^n$, X - proizvoljan skup, $|X| = n$

$\varphi : P(X) \longrightarrow 2^n$; $A \subseteq X \Rightarrow \varphi(A) = \chi_A$ izomorfizam

$\theta = \varphi^{-1} \circ \psi : B \cong \mathbb{P}(X)$ QED

(homework): Data su 3 kruga X, Y, Z ako neki skupovni identitet važi na ova tri kruga, onda on važi uopšte



Dokaz:

$S_1 = X \setminus (Y \cup Z)$; $S_2 = Y \setminus (X \cup Z)$; $S_3 = Z \setminus (X \cup Y)$

$S_4 = (X \cap Y) \setminus Z$; $S_5 = (Y \cap Z) \setminus X$; $S_6 = (X \cap Z) \setminus Y$

$S_7 = X \cap Y \cap Z$

$L = \{+, \cdot, ', 0, 1\}$

$u \equiv u(x,y,z)$; $v \equiv v(x,y,z)$ (nad L)

BA: $\mathbb{A} = (\mathbb{P}(U), \cup, \cap, ^c, \emptyset, U)$; $U = X \cup Y \cup Z$

$S_i \in \mathbb{P}(U)$ $(1 \le i \le 7)$;

$B = \langle S_1, S_2, S_3, S_4, S_5, S_6, S_7 \rangle_{\mathbb{A}}$, $\mathbb{B} = (B, \cup, \cap, ^c, \emptyset, S)$; $S = \bigcup_{i=1}^{7} S_i$

$u^{\mathbb{A}}[x,y,z] \in B$, $v^{\mathbb{A}}[x,y,z] \in B$

$u^{\mathbb{A}}[x,y,z] = v^{\mathbb{A}}[x,y,z] \Leftrightarrow u^{\mathbb{B}}[x,y,z] = v^{\mathbb{B}}[x,y,z]$

$\mathbb{A} \models u = v \Leftrightarrow \mathbb{B} \models u = v$

P, Q, R – proizvoljni skupovi ; $U' = P \cup Q \cup R$

$\mathbb{A}' = (\mathcal{P}(U'), \cup, \cap, ^c, \emptyset, U')$ BA

S_i' $(1 \le i \le 7)$ se definišu na analogan način kao i S_i $(1 \le i \le 7)$

$\mathbb{B}' = \langle S_1', \dots, S_7' \rangle_{\mathbb{A}'} \subseteq \mathbb{A}'$; $\bigcup_{i=1}^{7} S_i' = S'$

$\mathbb{B}' = (B', \cup, \cap, ^c, \emptyset, S')$ BA ,

$u^{\mathbb{A}'}[P,Q,R] \in B'$; $v^{\mathbb{A}'}[P,Q,R] \in B'$

$\mathbb{A}' \models u = v \Leftrightarrow \mathbb{B}' \models u = v$

$\varphi : B \to B'$,

$T \in B \Rightarrow (\exists t \in Term_4)\ T = t^{\mathbb{B}}[S_1, \dots, S_7]$; izpravka: $T = \bigcup_{i \in I} S_i$

$\varphi(T) \overset{def}{=} t^{\mathbb{B}'}[S_1', \dots, S_7']$ $(I \subseteq \{0,1,\dots,7\})$

$t_i(x_1, \dots, x_7) = x_i \quad (1 \le i \le 7)$

$\varphi(S_i) = \varphi(t_i^{\mathbb{B}}[S_1, \dots, S_7]) = t_i^{\mathbb{B}'}[S_1', \dots, S_7'] = S_i' \quad (1 \le i \le 7)$

1° *Preslikavanje φ je dobro definisano, jer svakom $T \in B$, dodeljuje tačno 1 element $\varphi(T) \in B'$.*

2° φ je NA : $T' \in B' \Rightarrow (\exists t \in Term_4)\ T' = t^{\mathbb{B}'}[S_1', \dots, S_7']$

$\Rightarrow T' = \varphi(t^{\mathbb{B}}[S_1, \dots, S_7]) = \varphi(T)$, $T = t^{\mathbb{B}}[S_1, \dots, S_7] \in B$

3° φ je *homomorfizam*

$\varphi(T_1 \cup T_2) = \varphi(t_1^{\mathbb{B}}[S_1, \dots, S_7] \cup t_2^{\mathbb{B}}[S_1, \dots, S_7])$, $T_j = t_j^{\mathbb{B}}[S_1, \dots, S_7]$ $(j = 1,2)$

$= \varphi(t^{\mathbb{B}}[S_1, \dots, S_7])$, $t = t_1 + t_2 \in Term_4$

$= t^{\mathbb{B}'}[S_1', \dots, S_7']$

$= t_1^{\mathbb{B}'}[S_1', \dots, S_7'] \cup t_2^{\mathbb{B}'}[S_1', \dots, S_7']$

$= \varphi(T_1) \cup \varphi(T_2)$

$\varphi(T_1 \cap T_2) = \varphi(T_1) \cap \varphi(T_2)$ (analogno)

$\varphi(T^c) = \varphi(t'^{\mathbb{B}}[S_1, \dots, S_7])$, $T = t^{\mathbb{B}}[S_1, \dots, S_7]$

$= t'^{\mathbb{B}'}[S_1', \dots, S_7'] = (t^{\mathbb{B}'}[S_1, \dots, S_7])^c = (\varphi(T))^c$

$1° \wedge 2° \wedge 3° \Rightarrow \varphi$ je epimorfizam $\Rightarrow \left(\mathcal{B} \models u = v \Rightarrow \mathcal{B}' \models u = v \right)$

$u^{\mathcal{B}}[x,y,z] \equiv v^{\mathcal{B}}[x,y,z] \Rightarrow u^{\mathcal{B}'}[P,Q,R] \equiv v^{\mathcal{B}'}[P,Q,R]$,

jer je:

$\varphi(X) = \varphi(S_1 \cup S_4 \cup S_6 \cup S_7) = S_1' \cup S_4' \cup S_6' \cup S_7' = P$

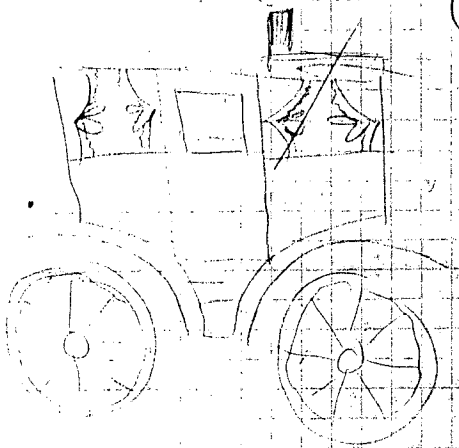
$\varphi(Y) = \quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad = Q$

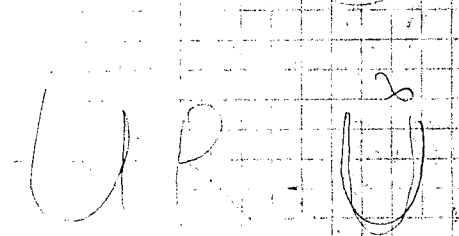
$\varphi(Z) = \quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad = R$

QED

NAJLEPŠE ŽELJE.

ISKRENE ČESTITKE





UP - UA

10. XII 1986.

Zadaci

1.) Neka je S konačna semigrupa. Dokazati da S sadrži idempotentan element, tj. $(\exists b \in S)\ b^2 = b$.

Dokaz: $(a^{2^n})_{n\in\mathbb{N}}$ $\quad X = \{a^{2^n} \mid n \in \mathbb{N}\} \subseteq S \quad (a \in S)$

$(\exists m, n \in \mathbb{N})\ m > n \wedge a^{2^m} = a^{2^n}$; $2^m > 2^n \Rightarrow 2^m \geq 2^{n+1}$

Neka je $b = a^{2^m - 2^n}$.

$$b^2 = (a^{2^m-2^n})^2 = a^{2^{m+1}-2^{n+1}}$$
$$= a^{2^m+2^m-2^n-2^n}$$
$$= a^{2^m+(2^m-2^{n+1})}$$
$$= a^{2^m} a^{2^m-2^{n+1}}$$
$$= a^{2^n} \cdot a^{2^m-2^{n+1}}$$
$$= a^{2^n+2^m-2^{n+1}}$$
$$= a^{2^m+2^m-2^\nu-2^\mu}$$
$$= a^{2^n+2^m}$$
$$= b \qquad \text{QED}$$

$2^m = 2^{m+1}$

$\Rightarrow (a^{2^n})^2 = a^{2^{n+1}} = 2^m = a^{2^n}$

$\Rightarrow b^2 = b$

2.) Ispitati da li je sledeći grupoid semi-grupa:

	a	b	c	d
a	b	c	d	b
b	c	d	b	c
c	d	b	c	d
d	b	c	d	b

Rešenje: $(xy)z = x(yz) \quad (x,y,z \in S)$.

$4 \cdot 4^3 = 256$ množenja

$s \mapsto \varphi_s$, $\varphi_s = \begin{pmatrix} 1 & a & b & c & d \\ s & sa & sb & sc & sd \end{pmatrix}$

	1	a	b	c	d
1	1	a	b	c	d
a	a				
b	b		S		
c	c				
d	d				

$\cong$

$\circ$	φ_1	φ_a	φ_b	φ_c	φ_d
φ_1					
φ_a		φ_b	φ_c	φ_d	φ_b
φ_b		φ_c	φ_d	φ_b	φ_c
φ_c		φ_d	φ_b	φ_c	φ_d
φ_d		φ_b	φ_c	φ_1	φ_b

$$\varphi_1 = \begin{pmatrix} 1 & a & b & c & d \\ 1 & a & b & c & d \end{pmatrix}, \quad \varphi_a = \begin{pmatrix} 1 & a & b & c & d \\ a & b & c & d & b \end{pmatrix}$$

$$\varphi_a \circ \varphi_b = \begin{pmatrix} 1 & a & b & c & d \\ a & b & c & d & b \end{pmatrix} \circ \begin{pmatrix} 1 & a & b & c & d \\ b & c & d & b & c \end{pmatrix} = \begin{pmatrix} 1 & a & b & c & d \\ c & d & b & c & d \end{pmatrix} = \varphi_c$$

$\varphi : S \cong S'$, $\varphi(x) = \varphi_x$ $\Rightarrow$ QED

3.) Neka su q, r kongruencije algebre A i neka je $q \circ r = r \circ q$. Dokazati da je $q \circ r$ kongruencija algebre A.

Dokaz:

(R) $\Delta_A \subseteq q \wedge \Delta_A \subseteq r \Rightarrow \Delta_A \circ \Delta_A = \Delta_A \subseteq q \circ r$

(S) $q^{-1} \subseteq q \wedge r^{-1} \subseteq r$

$(q \circ r)^{-1} = r^{-1} \circ q^{-1} \subseteq r \circ q = q \circ r$

(T) $(q \circ r) \circ (q \circ r) = (q \circ r) \circ (r \circ q) = q^2 \circ r^2 \subseteq q \circ r$

(saglasnost):

Neka je F n-arna operacija alg. A

$$(x_1, y_1), \ldots, (x_n, y_n) \in q \circ r \Rightarrow (\exists z_1, \ldots, z_n)\ \left\{ \begin{array}{l} (x_1, z_1), \ldots, (x_n, z_n) \in q \\ (z_1, y_1), \ldots, (z_n, y_n) \in r \end{array} \right\}$$

$\Rightarrow (F(x_1, \ldots, x_n), F(z_1, \ldots, z_n)) \in q \wedge (F(z_1, \ldots, z_n), F(y_1, \ldots, y_n)) \in r$

$\Rightarrow (F(x_1, \ldots, x_n), F(y_1, \ldots, y_n)) \in q \circ r$ QED

(homework)

1.) Neka je data familija $\langle A_i \mid i \in I \rangle$, $A = \prod_i A_i$, i relacija

$f, g \in A$: $f \sim g \overset{\text{def}}{\Leftrightarrow} \{ i \in I \mid f(i) \neq g(i) \}$ konačan.

Dokazati da je $\sim$ kongruencija algebre A.

2.) Ako je $p/q \in \mathbb{Q} \setminus \mathbb{Z}$, $p > 0$, onda $|[p/q] - p/q| \geq 1/q$.

3.) Neka je $e = \sum_{i=0}^{\infty} \frac{1}{i!}$ i $1 + \frac{1}{1!} + \ldots + \frac{1}{n!} = \frac{S_n}{n!}$. Dokazati:

1° $\frac{S_n}{n!} < e < \frac{S_n}{n!} + \frac{1}{n!}$;

2° $[ne] = \left[\frac{S_n}{(n-1)!}\right]$, 3° e je iracionalan

4.) $1+\frac{1}{2}+\ldots+\frac{1}{n}\in Q\setminus Z$

5.) Dokazati da u prstenu Z_p važi: $\sum_{i=1}^{p-1}\frac{1}{i}=0$, $p\geq 3$ je prost broj

6.) $\sum_{i=1}^{p-1}\frac{1}{i^2}=0$, $p\geq 4$ je prost broj (u Z_p).

14. XII 1986.

– Rešenja –

1.) 1° $\sim$ je relacija ekvivalencije

(R) $f\sim f$, jer je $\{i\in I \mid f(i)\neq f(i)\}=\emptyset$ konačan

(S) $f\sim g \Rightarrow \{i\in I \mid f(i)\neq g(i)\}$ konačan

$\Rightarrow \{i\in I \mid g(i)\neq f(i)\}$ konačan

$\Rightarrow g\sim f$

(T) $f\sim g \wedge g\sim h \Rightarrow P=\{i\in I \mid f(i)\neq g(i)\}$ konačan

$\wedge\ Q=\{i\in I \mid g(i)\neq h(i)\}$ konačan

$\Rightarrow P\cup Q=\{i\in I \mid f(i)\neq g(i) \vee g(i)\neq h(i)\}$

$=\{i\in I \mid \neg(f(i)=g(i)\wedge g(i)=h(i))\}$

$\supseteq \{i\in I \mid f(i)\neq h(i)\}$ konačan

$\Rightarrow f\sim h$

2° $\sim$ je saglasna sa operacijama algebre $A=\prod_{i\in I}A_i$

$f_1,\ldots,f_n,g_1,\ldots,g_n\in A$, $F\in F_m$ $(\text{ar } F=n)$

$f_1\sim g_1 \wedge \ldots \wedge f_n\sim g_n \Rightarrow P_k=\{i\in I \mid f_k(i)\neq g_k(i)\}$ konačni $(1\leq k\leq n)$

$\Rightarrow \bigcup_{k=1}^{n}P_k=\{i\in I \mid \neg(f_1(i)=g_1(i)\wedge\ldots\wedge f_n(i)=g_n(i))\}$

$\supseteq \{i\in I \mid F^A[f_1(i),\ldots,f_n(i)]\neq F^A[g_1(i),\ldots,g_n(i)]\}$

$=\{i\in I \mid (F^A[f_1,\ldots,f_n])(i)\neq (F^A[g_1,\ldots,g_n])(i)\}$ konačan

$\Rightarrow F^A[f_1,\ldots,f_n]\sim F^A[g_1,\ldots,g_n]$ QED

2.) $\frac{p}{q}\in Q\setminus Z$, $p>0 \Rightarrow p\in N$, $q\in N$, $\neg(q\mid p)$

(i) $0<\frac{p}{q}<1 \Rightarrow \left[\frac{p}{q}\right]=0$

$\Rightarrow \left|\left[\frac{p}{q}\right]-\frac{p}{q}\right|=\left|\frac{p}{q}\right|=\frac{p}{q}\geq\frac{1}{q}$ $(p\geq 1)$

(ii) $p>q$

$p = qk + r, \quad 0 < r < q \Leftrightarrow 1 \leq r < q$

$\left[\frac{p}{q}\right] \leq \frac{p}{q}$

$\Rightarrow \left| \left[\frac{p}{q}\right] - \frac{p}{q} \right| = \frac{p}{q} - \left[\frac{p}{q}\right] = k + \frac{r}{q} - k = \frac{r}{q} \geq \frac{1}{q}$ QED

3.) $e = \sum_{i=0}^{\infty} \frac{1}{i!}$; $\sum_{i=0}^{n} \frac{1}{i!} = \frac{s_n}{n!} = s_n$, $t_n = s_n + \frac{1}{n!}$ $(n \geq 0)$

1° $s_n < s_{n+1}$ $(n \in N) \Rightarrow$ $s_n \uparrow$

$t_n - t_{n+1} = \sum_{i=0}^{n} \frac{1}{i!} + \frac{1}{n!} - \left(\sum_{i=0}^{n+1} \frac{1}{i!} + \frac{1}{(n+1)!} \right) = \frac{n-1}{(n+1)!} > 0$, za $n \geq 2$

$\Rightarrow$ $t_n \downarrow$ (za $n \geq 2$) ; $s_n < t_n$

$\Rightarrow 2{,}5 = s_2 \leq s_n < t_n \leq t_2 = 3 \quad (n \geq 2)$

Monoton i ograničen niz je konvergentan.

$\lim_{n\to\infty} s_n = e$

$\lim_{n\to\infty} t_n = \lim_{n\to\infty} \left(s_n + \frac{1}{n!}\right) = e + 0 = e$ $\Rightarrow \underline{s_n < e < t_n}$

2° $s_n = \frac{s_n}{n!} \Rightarrow \frac{s_n}{(n-1)!} = n \cdot s_n$ $\quad [ne] \overset{(?)}{=} [n s_n]$

$\lim_{n\to\infty} \frac{[ne]}{n} = e \wedge \lim_{n\to\infty} \frac{[n s_n]}{n} = e$, $n s_n < ne \Rightarrow [n s_n] \leq [ne]$

$a_n = \frac{[ne] - [n s_n]}{n}$; $\lim_{n\to\infty} a_n = 0$, $a_n \geq 0$

$a_n - a_{n+1} = \frac{[ne] - [n s_n]}{n} - \frac{[(n+1)e] - [(n+1)s_{n+1}]}{n+1}$

$= \frac{(n+1)\left([ne] - [n s_n]\right) - n\left([(n+1)e] - [(n+1)s_{n+1}]\right)}{n(n+1)}$

$(n+1)[ne] - n[(n+1)e] \geq (n+1)[ne] - n\left([ne] + \underbrace{[e]}_{3} + 1\right)$

$= [ne] - 3n \geq [n][e] - 3n = 3n - 3n = 0$

$n[(n+1)s_{n+1}] - (n+1)[n s_n] \Rightarrow n \cdot [n s_{n+1} + s_{n+1}] - (n+1)[n s_n]$

$\geq n\left([n s_{n+1}] + [s_{n+1}]^{*}\right) - (n+1)[n s_n]$ $\quad$ *) $[a_{n+1}] \geq [s_n]$

$= n\left([n s_{n+1}] - [n s_n]\right) + (n-1)[n s_n] \geq 0$

$\Rightarrow$ $a_n \downarrow$

$\Rightarrow$ $0 \leq a_n \leq a_1 = [e] - [s_1] = 0 \Rightarrow a_n = 0 \quad (\forall n \in N)$

$\Rightarrow$ $[ne] = [n s_n] \quad (n \in N)$

3° SP: $e = \frac{p}{q} \in \mathbb{Q}$

$s_q < e < t_q \Leftrightarrow \sum_{i=0}^{q} \frac{1}{i!} < \frac{p}{q} < \sum_{i=0}^{q} \frac{1}{i!} + \frac{1}{q!} \quad | \cdot q!$

$\Rightarrow k < p \cdot q! < k+1 \quad (p \cdot q! \in \mathbb{N}) \quad \#$ $\Rightarrow e \notin \mathbb{Q}$ QED

---

4) $m = \max \{ i \in \mathbb{N} \mid 2^i \leq n \} \quad (n \geq 2)$

$1 + \frac{1}{2} + \dots + \frac{1}{n} = 1 + \frac{1}{2} + \dots + \frac{1}{2^m} + \dots + \frac{1}{n} = \frac{p_1 + p_2 + \dots + k + \dots + p_n}{2^m k} = \frac{p}{q}$

$p_1, p_2, \dots, p_n$ (bez k) su parni brojevi, jer se u njihovoj faktorizaciji pojavljuje faktor oblika 2^i $(1 \leq i \leq m)$.

k je neparan broj

$\Rightarrow p$ je neparan broj ; q je paran broj

$\Rightarrow \frac{p}{q} = 1 + \frac{1}{2} + \dots + \frac{1}{n} \in \mathbb{Q} \setminus \mathbb{Z}$. QED

5.) $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$, p je prost broj $\Rightarrow \mathbb{Z}_p$ je polje

$x \neq y \ (\in \mathbb{Z}_p) \Rightarrow x^{-1} \neq y^{-1}$

SP: $x^{-1} = y^{-1} \Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Rightarrow x = y$ #

$\Rightarrow \{1^{-1}, 2^{-1}, \dots, (p-1)^{-1}\} = \{1, 2, \dots, p-1\}$; $+_p$ je asoc. i komut.

$\Rightarrow \sum_{i=1}^{p-1} \frac{1}{i} = \frac{(p-1)p}{2} = k \cdot p = 0$, jer je $p-1 \in 2\mathbb{N}$ QED

6.) $x, y \in \mathbb{Z}_p$ (p - prost broj), $0 < x < y < p$; $y = x + z$; $x^2 = y^2$

$y^2 = x^2 + 2xz + z^2 \Rightarrow 2xz + z^2 = k \cdot p = 0$

$z(2x + z) = 0 \Rightarrow z = 0 \ \vee \ 2x + z = 0$ ($\mathbb{Z}_p$ je polje)

$z \neq 0 \quad (x < y)$

$\Rightarrow 2x + z = 0 \Rightarrow x + y = 0$; $x < p \wedge y < p \Rightarrow x + y < 2p \ (u \ \mathbb{Z})$

$\Rightarrow x + y = p \ (u \ \mathbb{Z})$

$(\forall i \in \mathbb{Z}_p) \ (i^2)^{-1} = (i^{-1})^2$ $\quad \hat{\{1^{-1}, \dots, (p-1)^{-1}\}} = \{1, \dots, p-1\}$

$\Rightarrow \sum_{i=1}^{p-1} (i^2)^{-1} = \sum_{i=1}^{p-1} (i^{-1})^2 = \sum_{i=1}^{p-1} i^2$

$= 2 \sum_{i=1}^{\frac{p-1}{2}} i^2 = 2 \cdot \frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)\left(2 \cdot \frac{p-1}{2} + 1\right)}{6} = \frac{p^2-1}{12} \cdot p = m$;

(kako $\frac{p^2-1}{12} p \in \mathbb{Z}$ i p je prost $\Rightarrow m = \frac{p^2-1}{12} \in \mathbb{Z}$)

17. XII 1986.

- Zadaci -

1.) *Primer algebarskog varijeteta m za osobinom da su sve njegove konačne algebre trivijalne, dok je m netrivijalan.*

Rešenje:

R - polje realnih brojeva

$(\forall r \in R)\ \underline{r} \in Const_L$, $L = \{+, \cdot, -, ^{-1}\} \cup \{\underline{r} \mid r \in R\}$

Aksiome:

$\underline{a} \cdot \underline{b} = \underline{c}$, gde je $c = a \cdot_R b$ $(u\ R)$ $\quad \forall a, b, c \in R$

$\underline{a} + \underline{b} = \underline{c}$, — ||— $c = a +_R b$ $\quad \lceil 0^{-1} \overset{def}{=} 0 \rfloor$

T: $-\underline{a} = \underline{b}$, — ||— $b = -a$

$\underline{a}^{-1} = \underline{b}$, gde je $b = a^{-1}$

(neprebrojiv skup aksioma)

$R^* = (R, a)_{a \in R} \in m$

m - alg. varijetet teorije T

$A \in m \Rightarrow A^* = (A, a_r)_{r \in R}$, $a_r = \underline{r}^{A^*}$ $(r \in R)$

$A = (A, +, \cdot, -, ^{-1}, 0, 1)$

$S = \{a_r \mid r \in R\}$ S je polje $\vee$ S je trivijalna algebra

$a_r + a_s = \underline{r}^{A^*} + \underline{s}^{A^*} = \underline{(r+s)}^{A^*} = a_{r+_R s}$

$a_r \cdot a_s = \ldots = a_{r \cdot_R s}$

$\mathcal{S} = (S, +, \cdot, 0, 1)$ homomorfna slika polja R

$\varphi : R \to \mathcal{S}$, $\varphi(r) = a_r = \underline{r}^{A^*}$

$\varphi(R) = \mathcal{S}$

Važi: ako je $\mathbb{F}$ polje i $h : \mathbb{F} \to K$ homomorf. $(K$ = polje$)$, onda je h utapanje.

$\lceil h$ nije konstantno, jer je $1 \neq 0$, $h(1) = 1$, $h(0) = 0 \rfloor$

Dokaz:

$h(x+y) = h(x) + h(y)$

$h(xy) = h(x)\,h(y)$, $h(0) = 0$; $h(1) = 1$

SP: $a \neq b \wedge h(a) = h(b)$ 16

$h(a) - h(b) = 0 \Rightarrow h(a-b) = 0 \to h(x) = 0$, za $x = a - b \neq 0$

$c \cdot c^{-1} = 1 \quad (c \neq 0)$

$\Rightarrow h(c c^{-1}) = h(1) \Rightarrow h(c) \cdot h(c^{-1}) = 1$

$\Rightarrow h(c) \cdot h(c^{-1}) = 1 \Rightarrow 0 \cdot h(c^{-1}) = 1 \Rightarrow 0 = 1$ # $\Rightarrow$ QED

$\Rightarrow \varphi$ je utapanje

$\Rightarrow |R| \leq |S| \Rightarrow A$ je beskonačan skup $(S \subseteq A)$ QED

2.) Ako je $H < G$, onda je broj levih razreda podgr. H jednak broju desnih razreda podgrupe H u G.

Dokaz: $L = \{xH \mid x \in G\}$, $D = \{Hx \mid x \in G\}$

$\varphi : D \to L$, $\varphi(Hx) = x^{-1}H$

1° φ je dobro def. i 1-1

$Hx = Hy \overset{?}{\Leftrightarrow} x^{-1}H = y^{-1}H$

$Hx = Hy \Leftrightarrow Hxy^{-1} = H$

$\Leftrightarrow xy^{-1} \in H$

$\Leftrightarrow (xy^{-1})^{-1} \in H$

$\Leftrightarrow yx^{-1} \in H$

$\Leftrightarrow yx^{-1}H = H \Leftrightarrow x^{-1}H = y^{-1}H$

$\Leftrightarrow \varphi(Hx) = \varphi(Hy)$ QED

Tm.: $\tau : G \to G$, $\tau(x) = x^{-1}$

$\varphi(Hx) = \tau(Hx) = (Hx)^{-1} = x^{-1}H^{-1} = x^{-1}H$

(Homework) 1) Dokazati da se svaki prebrojiv uređen skup može utopiti u uređeno racionalnih brojeva.

2.) Neka je $(A, \leq)$ prebrojiv linearno uređen skup u kojem je

1° $(\forall x)(\exists y)\ x \leq y$ (Kuratowski - Mostowski : Teorija skupova)

2° $(\forall x)(\exists y)\ y < x$ (D. Kurepa : T. skupova, 1952)

3° $(\forall x,y)(x < y \Rightarrow (\exists z)\ x < z < y)$

4° $|A| \geq 2$

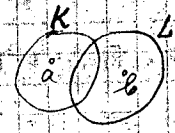
Dokazati da je $(A, \leq) \cong (Q, \leq)$ (Cantor)

3.) Da li se svaki linearno uređen skup može kontinuuma može utopiti u linearno uređen skup realnih brojeva ?
(Ne može ! vidi C)

4.) Dokazati da skupovna unija 2 podgrupe, podgrupa akko je jedna sadržana u onoj drugoj.

Dokaz:

$(\Rightarrow)$ $K < G$, $L < G$; $S = K \cup L$) $S < G$



sp.: $\neg(K \subseteq L) \wedge \neg(L \subseteq K)$

$\Rightarrow (\exists a)\, a \in K \setminus L$, $(\exists b)\, b \in L \setminus K$, $a, b \in S$

$\Rightarrow ab \in S \Rightarrow ab \in K \vee ab \in L$

(i) $ab \in K \Rightarrow a^{-1}ab = b \in K$ } $\neq$

(ii) $ab \in L \Rightarrow abb^{-1} = a \in L$ }

$A, B, C < G$, $A \subseteq B \cup C \Rightarrow A \subseteq B \vee A \subseteq C$

Dokaz:

$A \subseteq B \cup C \Rightarrow A = (A \cap B) \cup (A \cap C)$ $\quad A \cap B < G$, $A \cap C < G$

$\Rightarrow A = A \cap B \vee A = A \cap C$

$\Rightarrow A \subseteq B \vee A \subseteq C$, QED

24. XII 1986

– Zadaci –

1.) Neka su $F, H < G$, G je konačna grupa. Dokazati:

(1) $G = FH$ ili $|G| \geq |F| + |H|$, $FH = \{xy \mid x \in F \wedge y \in H\}$

(2) $|F \cdot H| = |F|\,|H| \,/\, |F \cap H|$

(3) $|F \cdot H| \leq |F \cap H|\,|F \vee H|$, $F \vee H = \langle F \cup H \rangle_G$

Dokaz:

(1) $G \neq FH$, $FH \subsetneq G$

$|F|\,|G|$ (Lagrange) $\quad |H|\,|G| \Rightarrow |G| \geq 2|F|$ $\quad (|G:F| \geq 2)$

$|G| \geq 2|H|$

$\Rightarrow |G| \geq |F| + |H|$

$(G = F \vee G = H \vee |G| \geq |F| + |H|)$

(2) $\varphi : F \times H \to FH$

$\varphi(x,y) = xy \quad (x \in F, y \in H)$, φ je NA

Neka je $\sim$ relacija na $F \times H$ def. sa:

$(x_1,y_1) \sim (x_2,y_2) \overset{def}{\Leftrightarrow} x_1y_1 = x_2y_2 \qquad (x_1,x_2 \in F,\ y_1,y_2 \in G)$

$x_1y_1 = x_2y_2 \Leftrightarrow x_2^{-1}x_1 = y_2y_1^{-1}$, $x_2^{-1}x_1 \in F$, $y_2y_1^{-1} \in H$

$\Leftrightarrow x_2^{-1}x_1,\ y_2y_1^{-1} \in F \cap H$

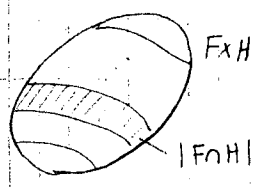
$(\exists h \in F \cap H)\ x_2^{-1}x_1 = h$, $y_2y_1^{-1} = h$

$\Leftrightarrow x_2 = x_1h^{-1}$, $y_2 = hy_1$

Dakle, $(x_2,y_2) \sim (x_1,y_1) \Leftrightarrow (\exists h \in F \cap G)\ (x_2,y_2) = (x_1h^{-1}, hy_1)$

tj. $(x,y)/\sim = \{(xh^{-1}, hy) \mid h \in F \cap H\}$

$\Rightarrow |(x,y)/\sim| = |F \cap H|$



$F \times H \xrightarrow[NA]{\varphi} FH$

$h \downarrow \qquad \nearrow \psi$ (1-1, NA)

$F \times H/\sim$ $\Rightarrow |FH| = |F \times H/\sim|$

$F \times H = \bigcup_{i \in I} (x_i,y_i)/\sim \Rightarrow |F \times H| = \sum_{i \in I} |(x_i,y_i)/\sim| = |F \times H/\sim| \cdot |F \cap H|$

$\Rightarrow |FH| = \dfrac{|F \times H|}{|F \cap H|} = \dfrac{|F| \cdot |H|}{|F \cap H|}$

(3) $|F| \cdot |H| = |FH| \cdot |F \cap H|$, $FH \subseteq F \vee H \Rightarrow |FH| \leq |F \vee H|$

$\Rightarrow |F| \cdot |H| \leq |F \vee H| \cdot |F \cap H|$ QED

2.) Svaka beskonačna grupa ima beskonačno mnogo podgrupa.

Dokaz: G - grupa , $|G| = \infty$

1° Svi elementi su konačnog reda.

$a_0 \in G$, $H_0 = \langle a_0 \rangle_G = \{1, a_0, \ldots, a_0^{n-1}\}$

$\exists a_1 \in G \setminus H_0$, $H_1 = \langle a_1 \rangle$, $H_1 \neq H_0$, H_1 je konačna

$\exists a_2 \in G \setminus (H_0 \cup H_1)$, $H_2 = \langle a_2 \rangle$, $H_2 \neq H_0, H_1$

$\vdots$

2° *Postoji element u G ∞ reda.*

$a \in G$, a je ∞ reda, $H = \langle a \rangle$

$\Rightarrow H = \{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$ (*ciklična grupa ∞ reda*)

$H_n = \{\ldots, a^{-2n}, a^{-n}, 1, a^n, a^{2n}, \ldots\}$ za $n = 0, 1, 2, 3, \ldots$

$H_0 = \{1\}$

$H_1 = H$

$H_2 = \{\ldots, a^{-4}, a^{-2}, 1, a^2, a^4, \ldots\}$

$H_3 = \{\ldots, a^{-6}, a^{-3}, 1, a^3, a^6, \ldots\}$

$m \neq n \Rightarrow H_m \neq H_n$

$m < n \Rightarrow a^m \in H_m$, $a^m \notin H_n$

$H_m = \{\ldots, a^{-2m}, a^{-m}, 1, a^m, a^{2m}, \ldots\}$; $H_n = \{\ldots, a^{-2n}, a^n, 1, a^n, a^{2n}, \ldots\}$

$a^m = a^{kn}$ → jer je a beskonačnog reda

$\Rightarrow a^{m-kn} = 1 \Rightarrow m - kn = 0 \Rightarrow m = kn \Rightarrow n \mid m$

$\rightarrow n \leq m$ # QED

3.) *Opisati grupe koje imaju tačno jednu pravu podgrupu.*

Rešenje:

G *mora biti konačna grupa*, $|G| = n$

1° n *je prost broj* $\Rightarrow$ G *nema pravih podgrupa (Lagrange)*

2° $a \in G$, $C = \langle a \rangle = \{1, a, \ldots, a^{k-1}\}$ *ciklična grupa*

$\Rightarrow k$ *je prost*

sp: $k = k_1 k_2$, $k_1, k_2 > 1$

$C_1 = \{1, a^{k_1}, a^{2k_1}, \ldots, a^{(k_2-1)k_1}\}$ *grupa*

$C_2 = \{1, a^{k_2}, a^{2k_2}, \ldots, a^{(k_1-1)k_2}\}$ *grupa*

$C_1 \neq C_2$, *osim kad je* $k_1 = k_2$

$a, b \in G \setminus \{1\}$: $\langle a \rangle = \langle b \rangle$ v $\langle a \rangle = G$ v $\langle b \rangle = G$

$|G| = n \Rightarrow$ *n nije proizvod 2 razl. prosta broja, niti proizvod više od 2 prosta broja*

$\Rightarrow n = p^2$, *p je prost broj*

G jeste ciklična ↳

Nije $G = C_1 \times C_2$, $|C_1| = |C_2| = p$ (ciklične grupe)

SP: $\Rightarrow$ $C_1 < G$, $C_2 < G$

$a \in G$, $G \neq \langle a \rangle$ (nije ciklična) $\Rightarrow (\exists b \in G \setminus \langle a \rangle)$ $\langle b \rangle < G$, $\langle b \rangle \neq$

$\Rightarrow$ G mora biti ciklična

$a \neq 1$, $b \neq 1$ $\Rightarrow$ $\langle a \rangle, \langle b \rangle$ su različite i nisu trivijalne ni G

„Ravno" rešenje:

(1) G je ciklična:

SP: $a \in G \setminus \{1\}$, $G \setminus \langle a \rangle \neq \emptyset \Rightarrow \exists b \in G \setminus \langle a \rangle$

$\Rightarrow$ $b \neq 1 \wedge \langle b \rangle \neq G$ (jer G nije ciklična)

$\langle a \rangle \neq \langle b \rangle$, jer $b \notin \langle a \rangle$ #

Neka je $G = \langle a \rangle$.

(2) $n \notin Prost$

(3) n nije proizvod 2 različita faktora.

SP: $n = k_1 k_2$, $k_1 \neq k_2$

$\Rightarrow$ $C_1 = \{1, a^{k_1}, a^{2k_1}, \ldots, a^{(k_2-1)k_1}\}$

$C_2 = \{1, a^{k_2}, a^{2k_2}, \ldots, a^{(k_1-1)k_2}\}$

$C_1 \neq C_2$, $C_1 < G$, $C_2 < G$, $C_1, C_2 \subsetneq G$ #

(4) $n = p^2$, $p \in Prost$

$\Rightarrow$ G je ciklična grupa p^2

(homework) 1) G - ciklična g. Ako je G konačna, onda je $G \cong (\mathbb{Z}_n, +_n, 0)$

2) G je beskonačna $\Rightarrow G \cong (\mathbb{Z}, +, 0)$

3) Homomorfna slika ciklične grupe je ciklična g.

4) Podgrupa " " " " "

5) Svaka ciklična grupa je homomorfna slika aditivne grupe celih brojeva.

6) G - konačna c.g. i $n \mid |G| \Rightarrow (\exists H < G)$ $|H| = n$

18. 02. 1987.

- Zadaci -

1.) Neka je $p \in Prost$, $p \geq 3$.

1° Ako je $a \in Z_p$, tada jednačina $x^2 = a$ ima rešenja u Z_p akko

$$a^{\frac{p+1}{2}} = a.$$

2° Dokazati da jednačina $x^2 + x + 1 = 0$ ima rešenja u Z_p, akko

$$(-3)^{\frac{p-1}{2}} = 1 \pmod p$$

Koristiti činjenicu: Ako je F polje i G konačna podgrupa multiplikativne grupe polja F, onda je G ciklična.

Dokaz:

1° ($\Rightarrow$): pp: $x^2 = a$ ima rešenje u Z_p

$\Rightarrow$ $(\exists b \in Z_p)$ $b^2 \equiv a$ $\Rightarrow$ $a^{(p+1)/2} = (b^2)^{\frac{p+1}{2}} = b^{2\frac{p+1}{2}} = b^{p+1} = b^2 b^{p-1}$

$(Z_p \setminus \{0\}, \cdot, 1)$ $\qquad = a \cdot b^{p-1} = a \cdot 1 = a$

($\Leftarrow$): $Z_p \setminus \{0\} = \langle c \rangle$, $a = c^i$ za neko i

(i) $i = 2k$ $\Rightarrow a = c^{2k} = (c^k)^2$

(ii) $i = 2k+1$ $\Rightarrow a = c^{2k+1}$

$$a^{\frac{p+1}{2}} = a \Rightarrow a^{\frac{p-1}{2}} = 1 \Rightarrow (c^{2k+1})^{\frac{p-1}{2}} = 1$$

$$\Rightarrow c^{(2k+1)\frac{p-1}{2}} = 1 \Rightarrow c^{k(p-1) + \frac{p-1}{2}} = 1$$

$$\Rightarrow \frac{c^{k(p-1)}}{1} \cdot c^{\frac{p-1}{2}} = 1 \Rightarrow c^{\frac{p-1}{2}} = 1 \quad \# \text{ jer je } c \text{ reda } p-1$$

2° $x^2 + x + 1 = 0$, $x^2 + x + 1 \equiv (x + \frac{1}{2})^2 + \frac{3}{4}$

$$x^2 + x + 1 = 0 \iff (x + \tfrac{1}{2})^2 = -\frac{3}{4}$$

Jednačina $x^2 + x + 1 = 0$ ima rešenje akko $(x + \frac{1}{2})^2 = -\frac{3}{4}$ ima rešenje.

$$y^2 = -\frac{3}{4} \text{ ima reš.} \iff \left(-\frac{3}{4}\right)^{\frac{p+1}{2}} = -\frac{3}{4} \quad (u\ Z_p)$$

$$\iff (-3)^{\frac{p-1}{2}} = 4^{\frac{p-1}{2}} \iff (-3)^{\frac{p-1}{2}} = 2^{p-1} \quad (u\ Z_p)$$

$$\iff (-3)^{\frac{p-1}{2}} = 1 \ (u\ Z_p) \text{ (mala Fermaova teorema)}$$

$$\iff (-3)^{\frac{p-1}{2}} = 1 \pmod p \qquad \text{QED}$$

2.) (LAGRANGE-ova teorema)

Svaki prirodan broj je zbir kvadrata 4 cela broja.

Dokaz:

1° $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z} \Rightarrow$

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 +$$
$$+ (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 + (x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2 +$$
$$+ (x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2 \quad (*)$$

$z_1 = x_1 + ix_2$, $z_2 = x_3 + ix_4$, $v_1 = y_1 + iy_2$, $v_2 = y_3 + iy_4$

$$(|z_1|^2+|z_2|^2)(|v_1|^2+|v_2|^2) = |z_1v_1|^2 + |z_1v_2|^2 + |z_2v_1|^2 + |z_2v_2|^2$$

2° Ako je $p \in Prost$, $p>3$, onda postoji $n \in N$:

$n<p$, np je zbir kvadrata 4 cela broja.

dokaz: $A = \{x \mid 0 \le x \le \frac{p-1}{2}\}$, $|A| = \frac{p+1}{2}$

$x, y \in A$, $x^2 = y^2 \pmod p \Rightarrow p \mid (x-y)(x+y) \Rightarrow p \mid (x-y) \vee p \mid (x+y)$

$p \mid (x-y) \Rightarrow x-y = 0 \Rightarrow x = y$

$p \mid (x+y) \Rightarrow x = y = 0$ (jer je $x+y \le p-1$)

$\{x^2 \mid 0 \le x \le \frac{p-1}{2}\} = A'$ su različiti

$B' = \{-1-y^2 \mid 0 \le y^2 \le \frac{p-1}{2}\}$, $|B'| = \frac{p+1}{2}$

$\Rightarrow (\exists z)\ z \in A' \cap B'$, $z = x^2 \in A'$, $z = -1-y^2 \in B'$

$x^2 = -1-y^2 \pmod p$ $\quad (A' \cap B' \neq \emptyset)$

$\Rightarrow np = x^2+y^2+1^2+0^2 \le \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 + 1 = \frac{(p-1)^2}{2} + 1 < p^2$

$\Rightarrow n < p$

Dovoljno je dokazati tvrdenje za proste brojeve, zbog:

ako je $c \in N$, onda po osnovnoj teoremi a. $n = p_1 \dots p_k$ i prema 1°, tvrdenje važi.

(skup svih zbirova kvadrata 4 cela broja je semi-grupa)

3° U 2°. se može uzeti da je $n = 1$.

dokaz: Neka je n najmanji prirodan broj takav da je za neke $x_1, \dots, x_4$: $np = x_1^2+x_2^2+x_3^2+x_4^2$, i $n>0$

↓

(i) $n \in 2N \Rightarrow$ svi brojevi x_i su parni, ili su 2 parna a 2 neparna, ili su svi neparni

Neka su x_1, x_2 parni (ako među $x_1, \dots, x_4$ ima parnih)

$$2np = (x_1+x_2)^2 + (x_1-x_2)^2 + (x_3+x_4)^2 + (x_3-x_4)^2 \quad | : 4$$

$$\frac{n}{2}p = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2 \quad \# \quad \left(\frac{n}{2} < n\right)$$

(prema izboru broja n)

$\Rightarrow n \notin 2N$

(ii) $n \in 2N+1$: $\quad S = \left\{ y \mid -\frac{n-1}{2} \leq y \leq \frac{n-1}{2} \right\}$, $|S| = n$ (otpodna 2 elem. sk. S nisu $\equiv n$)

$y, y' \in S \Rightarrow y \not\equiv y' \pmod n$

(translacija intervala $[0, n-1] \cap \mathbb{Z}$ ulevo za $(n-1)/2$)

Svaki $x \in \mathbb{Z}$ kongruentan je nekom $y \in S$.

$y_i \equiv x_i \pmod n \quad y_i \in S \quad (1 \leq i \leq 4)$

$\Rightarrow y_i^2 \equiv x_i^2 \pmod n \quad (1 \leq i \leq 4)$

$\Rightarrow y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod p \equiv 0 \pmod n$

$\Rightarrow y_1^2 + y_2^2 + y_3^2 + y_4^2 = rn$

$r \neq 0$; SP: $r = 0 \Rightarrow y_1 = y_2 = y_3 = y_4 = 0 \Rightarrow p \mid x_i \Rightarrow p^2 \mid (x_1^2 + \dots + x_4^2) \Rightarrow p \mid n$ #

$r = 1$ (?)

$$(np)(rn) = (x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) \equiv I_1^2 + I_2^2 + I_3^2 + I_4^2 \quad (*)$$

$I_1 \equiv 0 \pmod n \Leftrightarrow I_1^2 \equiv 0 \pmod{n^2}$

$I_2 \equiv 0 \pmod n \Leftrightarrow I_2^2 \equiv 0 \pmod{n^2}$

$$x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 = x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod n$$

$I_k^2 \equiv 0 \pmod{n^2} \quad k = 1,2,3,4$

$\Rightarrow n^2$ desna strana $\Rightarrow n^2 \mid (np \cdot rn)$

$r < n < p$; $rp = \left(\frac{I_1}{n}\right)^2 + \dots + \left(\frac{I_4}{n}\right)^2$ #

$\Rightarrow n = 1$ QED

- Zadaci -

1.) Dokazati: $\mathbb{Z}_p \models (x+y)^p = x^p + y^p$, $(x-y)^p = x^p - y^p$ ($p \in Prost$)

Dokaz: Za $p \in Prost$ i $1 \leq x < p$, na osnovu male Fermaove teoreme važi $x^{p-1} = 1 \pmod p$, tj. $x^{p-1} = 1$ u $\mathbb{Z}_p$.

Dakle, $\mathbb{Z}_p \models x^p - x$. Odatle sledi:

$(x+y)^p - x + y = x^p + y^p$ i $(x-y)^p = x - y = x^p - y^p$. QED

2.) Ako je $p \in Prost$ i $1 + \frac{1}{2} + \dots + \frac{1}{p-1} = \frac{A}{B}$ $(A, B \in N)$, onda $p \mid A$ i $p \nmid B$.

Dokaz:

(1) $\mathbb{Z}_p \models \sum_{i=1}^{p-1} \frac{1}{i} = 0$, $\varphi(x) = x^{-1}$, $\varphi \in Sym(\mathbb{Z}_p \setminus \{0\})$

$\Rightarrow \mathbb{Z}_p \models \frac{A}{B} = 0 \Rightarrow \mathbb{Z}_p \models A = 0 \Rightarrow p \mid A$

(2) $(\forall i \in \{1, 2, \dots, p-1\})\ i^{p-1} \equiv 1$ (u $\mathbb{Z}_p$) (Mala Fermaova teorema)

$\Rightarrow i^{p-1} - 1 = 0$

$\Rightarrow$ Koreni polinoma $x^{p-1} - 1$ u $\mathbb{Z}_p$ su $1, 2, \dots, p-1$.

$x^{p-1} - 1 = (x-1)(x-2) \cdots (x-(p-1))$

$\Rightarrow 1 + 2 + \dots + (p-1) = 0$

$1 \cdot 2 + 1 \cdot 3 + \dots + (p-1)p = 0$

$S \equiv 1 \cdot 2 \cdots (p-2) + 1 \cdot 2 \cdots (p-3)(p-1) + \dots + 2 \cdot 3 \cdots (p-1) = 0$

$1 \cdot 2 \cdots (p-1) \equiv (-1)^{p-1}(-1)$

$\frac{A}{B} = 1 + \frac{1}{2} + \dots + \frac{1}{p-1} = \frac{S}{(p-1)!}$

$\mathbb{Z}_p \models S = 0 \Rightarrow S = 0 \pmod p \Rightarrow p \mid S \Rightarrow p \mid A \cdot p \nmid B$ QED

$[\ p^2 \mid S\ ]$

3.) Odrediti komutativan monoid A od 5 elemenata, koji sadrži elemente $a, b \neq 1$ takve da je:

$a \neq b$, $a^3 = a$, $b^3 = b$, $ab = 1$.

Rešenje:

Opšti oblik elemenata iz A: $a^{\alpha_1}b^{\beta_1}\,a^{\alpha_2}b^{\beta_2} = a^{\alpha}b^{\beta}$

$A = \{1, a, b, a^2, b^2\}$

	1	a	a^2	b	b^2
1	1	a	a^2	b	b^2
a	a	a^2	a	1	b
a^2	a^2	a	a^2	a	1
b	b	1	a	b^2	b
b^2	b^2	b	1	b	b^2

$\alpha > \beta$: $a^{\alpha}b^{\beta} = a^{\alpha-1}ab\,b^{\beta-1}$

$= a^{\alpha-1}b^{\beta-1}$

$= a^{\alpha-\beta}$

$a^{\alpha}b^{\alpha} = 1$

$f_1 = \begin{pmatrix} 1 & a & a^2 & b & b^2 \\ 1 & a & a^2 & b & b^2 \end{pmatrix}$

$f_a = \begin{pmatrix} 1 & a & a^2 & b & b^2 \\ a & a^2 & a & 1 & b \end{pmatrix}$, $f_a^2 = \begin{pmatrix} 1 & a & a^2 & b & b^2 \\ a^2 & a & a^2 & a & 1 \end{pmatrix}$

$f_b = \begin{pmatrix} 1 & a & a^2 & b & b^2 \\ b & 1 & a & b^2 & b \end{pmatrix}$, $f_b^2 = \begin{pmatrix} 1 & a & a^2 & b & b^2 \\ b^2 & b & 1 & b & b^2 \end{pmatrix}$

$\circ$	f_1	f_a	f_a^2	f_b	f_b^2
f_1	f_1	f_a	f_a^2	f_b	f_b^2
f_a	f_a	f_a^2			
f_a^2	f_a^2				
f_b	f_b				
f_b^2	f_b^2				

$\varphi : A \to S$, $\varphi(x) = f_x$

φ je izomorfizam

---

4) Neka su q i r kongruencije grupe G kojim redom odgovaraju normalne podgrupe K i H. Tada važi

(a) $q \cap r$ je kongruencija grupe G kojoj odgovara normalna podgrupa $K \cap H$

(b) $q \circ r$ je kongruencija grupe G kojoj odgovara normalna podgrupa KH

Dokaz:

(a) $K = \{x \in G \mid x \sim_q 1\}$, $H = \{x \in G \mid x \sim_r 1\}$

$K \lhd G$, $H \lhd G$.

$q \cap r$ je relacija ekvivalencije

$G = (G, \cdot, 1)$

$(x,y) \in q \cap r \wedge (a,b) \in q \cap r \Rightarrow (x,y) \in q \wedge (x,y) \in r \wedge (a,b) \in q \wedge (a,b) \in r$

$\Rightarrow (xa, yb) \in q \wedge (xa, yb) \in r \Rightarrow (xa, yb) \in q \cap r$

$P = \{ x \in G \mid x \sim_{q \cap r} 1 \} \qquad P \lhd G$

$x \in P \Leftrightarrow x \sim_{q \cap r} 1 \Leftrightarrow x \sim_q 1 \wedge x \sim_r 1 \Leftrightarrow x \in K \wedge x \in H \Leftrightarrow x \in K \cap H$

$\Rightarrow P = K \cap H$

(b) $q \circ r$ je relacija ekvivalencije ako je $q \circ r = r \circ q$

(R) $(\forall x \in G)\ (x,x) \in q \wedge (x,x) \in r \Rightarrow (x,x) \in q \circ r$

(S) $q^{-1} \subseteq q \wedge r^{-1} \subseteq r \Rightarrow (q \circ r)^{-1} = r^{-1} \circ q^{-1} \subseteq r \circ q = q \circ r$

(T) $q \circ q \subset q \wedge r \circ r \subseteq r \Rightarrow (q \circ r) \circ (q \circ r) = (q \circ q) \circ (r \circ r) \subseteq q \circ r$

$(x,y) \in q \circ r \wedge (a,b) \in q \circ r$

$\Rightarrow (\exists z, c \in G)\ (x,z) \in q \wedge (z,y) \in r \wedge (a,c) \in q \wedge (c,b) \in r$

$\Rightarrow (\exists z, c)\ (xa, zc) \in q \wedge (zc, yb) \in r$

$\Rightarrow (xa, yb) \in q \circ r$

$\Rightarrow q \circ r$ je kongruencija

$S = \{ x \in G \mid (x,1) \in q \circ r \} \quad , \quad S \lhd G$

$x \in S \Leftrightarrow (\exists y \in G)\big((x,y) \in q \wedge (y,1) \in r\big)$

$\Leftrightarrow (\exists y)(x \sim_q y \wedge y \sim_r 1)$

$\Leftrightarrow (\exists y)(xy^{-1} \sim_q 1 \wedge y \in H)$

$\Leftrightarrow (\exists y)(xy^{-1} \in K \wedge y \in H)$

$\Leftrightarrow (\exists y)(y \in H \wedge x \in Ky)$

$\Leftrightarrow x \in KH$

$\Rightarrow S = KH$

5.) Neka je G grupa. Tada vrijedi:

(1) $K \lhd G \wedge H < G \Rightarrow KH = HK \wedge KH < G$

(2) $K \lhd G \wedge H \lhd G \Rightarrow KH \lhd G$

Dokaz:

(1) $x \in KH \Rightarrow (\exists k \in K)(\exists h \in H)\ x = kh$

$\Rightarrow (\exists k' \in K)(\exists h \in H)\ x = hk'$, jer je $hK = Kh$

$\Rightarrow x \in HK$

Dakle, $KH \subseteq HK$. Analogno $HK \subseteq KH$, pa je $KH = HK$

(i) $1 \in KH$, $\emptyset \neq KH \subseteq G$

(ii) $x, y \in KH \Rightarrow (\exists k_1, k_2 \in K)(\exists h_1, h_2 \in H)(x = k_1 h_1 \wedge y = k_2 h_2)$

$\Rightarrow xy = k_1 h_1 \cdot k_2 h_2$

$\Rightarrow xy = k_1 h_1 \cdot h_2 k_2'$, za neko $k_2' \in K$ (zbog $K \triangleleft G$)

$\Rightarrow xy = k_1 h_3 \cdot k_2'$, gde je $h_3 = h_1 h_2 \in H$

$\Rightarrow xy = k_1 k_2'' h_3$, za neko $k_2'' \in K$

$\Rightarrow xy = k_3 \cdot h_3$, gde je $k_3 = k_1 k_2''$

$\Rightarrow xy \in KH$

(iii) $x \in KH \Rightarrow (\exists k \in H)(\exists h \in H)\ x = kh$

$\Rightarrow x^{-1} = h^{-1} k^{-1}$

$\Rightarrow x^{-1} \in HK$, jer $h^{-1} \in H$, $k^{-1} \in K$

$\Rightarrow x^{-1} \in KH$, jer je $HK = KH$

Dakle, $KH < G$.

(2) $\sigma_x : G \to G$, $\sigma_x(g) = x^{-1} g x$, $\sigma_x \in Inn(G)$

$\sigma_x(K) = K$, $\sigma_x(H) = H$ za sve $x \in G$

$\sigma_x(KH) = \sigma_x(K) \cdot \sigma_x(H)$, jer je σ_x automorfizam

$= KH$

Dakle, $KH \triangleleft G$. QED

13. 05. 1987.

Prsteni

A - prsten

$x \in A$ je nilpotentan akko $(\exists n)\ x^n = 0$

$x \in A$ je idempotentan akko je $x^2 = 1$

- Zadaci -

1.) Neka je A prsten takav da $(\forall x \in A)(\exists n = n(x) \in N)\ x^n = x$

(a) Dokazati: $(\forall a, b \in A)(\exists n \in N)\ a^n = a \wedge b^n = b$.

(b) Da li se (a) generalise na konacan broj elemenata ?

(c) a nilpotentan $\Rightarrow a = 0$.

(d) Ako A nma nedelitelj nule $\Rightarrow A \ni 1$.

Dokaz:

(a) $a^n = a$, $b^m = b$ („$a^{n-1} = 1$", „$b^{m-1} = 1$")

$n = (n-1)(m-1) + 1$

$\Rightarrow a^n = a^{(n-1)(m-1)+1} \overset{?}{=} a$

$a^{(n-1)k+1} = a$, $\forall k$

dokaz indukcijom po k

$k = 1$: $a^{n-1+1} = a$

$a^{(n-1)(k+1)+1} = a^{(n-1)k+n-1+1} = a$ $\Rightarrow$ qed

$b^n = b$ ($b^{k(m-1)+1} = b$ - analogno)

(b) (homework)

(c) $a^m = 0$ za neko m , $a^n = a$ za neko n

$a = a^n = (a^n)^n = a^{n^2} = \dots = a^{n^k}$, $\forall k$

$(\exists k)\ n^k > m$

$a = a^{(n^k - m) + m} = a^{n^k - m}\, a^m = a^{n^k - m}\, 0 = 0$

(d) pp: $a \in A$ nije delitelj 0

$ax = 0 \Rightarrow x = 0$

$xa = 0 \Rightarrow x = 0$

$e = a^{n-1}$, n takvo da je $a^n = a$

$xe = x$, $ex = x$ $(\forall x \in A)$

$(xe - x)a = (xa^{n-1} - x)a = xa^n - xa = xa - xa = 0 \Rightarrow xe - x = 0$

$a(ex - x) = 0 \Rightarrow ex - x = 0$ QED

- *Ideali prstena* -

A - prsten, $\sim$ relacija ekv. koja je **kongruencija** u odn. $+$, $\cdot$

$I = \{a \in A \mid a \sim 0\}$

- kongr. u odn. na $+ \Rightarrow$ I je aditivna podgrupa (1)

- " " " na $\cdot$ $\Rightarrow$ $\left.\begin{matrix} a \sim b \\ c \sim d \end{matrix}\right\} ac \sim bd$

$\left.\begin{matrix} x \in I \Rightarrow x \sim 0 \\ a \sim b \Rightarrow ax \sim b0 = 0 \end{matrix}\right\} x \sim 0 \Rightarrow ax \sim 0 \wedge xa \sim 0$

$x \in I, a \in A \Rightarrow ax, xa \in I$ (2)

$I \subseteq A \wedge (1) \wedge (2) \Rightarrow I$ je ideal

def. $I \subseteq A$ je (levi, desni) **obostrani ideal** akko:

1° I je aditivna podgrupa

2° $AI \subseteq I$, $IA \subseteq I$

$I \subset A$ ideal $\longrightarrow$ $\sim$ kongruencija

$a \sim b \Leftrightarrow a - b \in I$ $(a - b \sim 0)$

$A/\sim = A/I$ količnički (faktor) prsten po idealu I

$= \{a + I \mid a \in A\}$

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

$\Leftrightarrow$ $a \sim 0 \wedge b \sim 0 \Rightarrow ab \sim 0$

- *Homomorfizam prstena* -

$h : A \to B$, $\left.\begin{matrix} h(a + a') = h(a) + h(a') \\ h(a \cdot a') = h(a) \cdot h(a') \end{matrix}\right\}$ $\ker h = \{a \in A \mid h(a) = 0\}$

- Zadaci -

1) Nadi sve ideale prstena $\mathbb{Z}$.

Rešenje:

$I \subseteq \mathbb{Z}$, I je podgrupa $\Rightarrow I = n\mathbb{Z}$

$n\mathbb{Z}\cdot\mathbb{Z} \subset n\mathbb{Z}$: $I = n\mathbb{Z} = (n)$ je ideal

Svaka podgrupa od $\mathbb{Z}$ je ideal.

[A - komutativan prsten : $(a) = aA$ - najmanji ideal koji sadrži a]

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$

$m + n\mathbb{Z} = (kn + r) + n\mathbb{Z} = r + n\mathbb{Z}$, $r = \text{rest}(m, n)$

$m + n\mathbb{Z} \longmapsto r$ izomorfizam

2.) (a) $\text{Ker}\, h \subseteq A$ je ideal (obostrani)

(b) Da li je $\text{Im}\, h \subseteq B$ ideal ?

Rešenje:

(a) $x \in \text{Ker}\, h$, $a \in A \Rightarrow h(ax) = h(a)\cdot h(x) = 0 \Rightarrow ax \in \text{Ker}\, h$

$xa \in \text{Ker}\, h$

(b) $\text{Im}\, h = \{ h(a) \mid a \in A \}$ je podprsten

$b \in B$: $b\, h(a) = h(a')$? ne mora biti

h je NA $\Rightarrow \text{Im}\, h \subseteq B$ jeste ideal

Primer: $\mathbb{Z} \subset \mathbb{R}$

[$I \subset A$ je ideal $\Rightarrow I$ je podprsten]

Teorema o homomorfizmu

$h : A \to B$

$$\begin{array}{ccc} A & \xrightarrow{h} & B \\ {\scriptstyle k}\downarrow & & \uparrow \\ A/\text{Ker}\, h & \cong & \text{Im}\, h \end{array}$$

A, B prsteni $\Rightarrow A \times B$ prsten (koordinatno def. operacije)

$A \times \{0\} \subset A \times B$, $A \times \{0\} \cong A$

1) $A \times \{0\}$ je ideal

$(a, b) \in A \times B$, $(c, 0) \in A \times \{0\}$

$(a, b)\cdot(c, 0) = (ac, b0) = (ac, 0) \in A \times \{0\}$

$A \times B / A \times \{0\} \cong B$

$A \times B / A \times \{0\} \cong \mathrm{Im}\,\varphi$, $\varphi : A \times B \to B$, $\varphi(a,b) = b$ epimorf.

$\mathrm{Ker}\,\varphi = \{(a,b) \mid b = 0\} = A \times \{0\}$

$\Rightarrow A \times B / \mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi = B$

$A \times B / \{0\} \times B \cong A$

$\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$

2.) Neka je A prsten karakteristike p i $I_m = \{x \in A \mid mx = 0\}$

(a) I_m je ideal u A $(m \in N)$

(b) $n \mid m \Rightarrow I_n \subset I_m$.

(c) $I_m = I_d$, gde je $d = M(m,p)$

(d) $p = ab$, $M(a,b) = 1 \Rightarrow A \cong I_a \times I_b$.

Dokaz:

(a) (i) $I_m < (A, +, 0)$

$\varphi : A \to A$, $\varphi(x) = mx$, $\mathrm{Ker}\,\varphi = I_m$

φ je homomorfizam Ab. grupa

(ii) $A I_m \subset I_m$, $I_m A \subset I_m$

$m(ax) = ax + \dots + ax = a(mx) = 0$

$m(xa) = 0$

(b) $n \mid m$: $x \in I_n \Rightarrow nx = 0 \Rightarrow mx = k \cdot nx = 0 \Rightarrow x \in I_m$

(c) (b) $\Rightarrow I_d \subset I_m$, jer $d \mid m$

$d = NZD(m,p) \Rightarrow d = km + lp$ $(k, l \in Z)$

$mx = 0 \Rightarrow dx = (km + lp)x$

$= kmx + lpx$

$= lpx = 0$, jer je $\mathrm{char}\,A = p$

$I_m \subset I_d$

Ideala ima koliko i delitelja karakteristike p.

$p = 6$: I_1, I_2, I_3, I_6 $(I_1 = \{0\},\ I_6 = A)$

$I_6 \supset I_2 \supset I_1 \subset I_3$

(d) $p = ab$, $M(a,b) = 1$

$\Rightarrow (\exists k, l \in \mathbb{Z})\ ka + lb = 1$

$I_a, I_b \subset A$ ideali

$I_a \cap I_b = ?$

$x \in I_a \cap I_b \Rightarrow ax = 0 \wedge bx = 0$

$\Rightarrow x = 1 \cdot x = (ka + lb)x = kax + lbx = 0$

$\Rightarrow I_a \cap I_b = \{0\}$ jedinstvenost reprezentacije

$x \in A \overset{?}{\Rightarrow} x = yz$, $ay = 0$, $bz = 0$

$\varphi : I_a \times I_b \to A$, $(x,y) \overset{\varphi}{\mapsto} xy$ (*)

$\varphi((x,y) + (x',y')) = \varphi(x+x', y+y')$

$= (x+x')(y+y')$

$= xy + xy' + x'y + x'y'$

$\varphi(x,y) + \varphi(x',y') = xy + x'y'$

(*) $xy \in I_a \cap I_b = \{0\}$

$\varphi : I_a \times I_b \to A$, $\varphi(x,y) = x+y$

φ je izomorfizam (homework)

3.) Neka $A \neq 0$ prsten. Dokazati da su sledeći uslovi ekv.:

(a) A je telo ($A^* = A \setminus \{0\}$)

(b) Jedini ideali prstena A su trivijalni (0 i A).

(c) $B \neq 0$, $h : A \to B$ homomorfizam $h \neq 0 \Rightarrow h$ je 1-1

Dokaz:

(a) $\Rightarrow$ (b) $I \subset A$ ideal, $I \neq 0$

$\Rightarrow (\exists a \in I)\ a \neq 0$

$\Rightarrow \exists a^{-1} \in A$

$b \in A : b = aa^{-1}b = \underset{\downarrow I}{a}(\underset{\downarrow A}{a^{-1}b}) \in I \Rightarrow I = A$

$I \neq 0 \Rightarrow I = A$

(b) $\Rightarrow$ (c) $h : A \to B$

$\operatorname{Ker} h = I$ ideal u $A \Rightarrow \operatorname{Ker} h = 0 \vee \operatorname{Ker} h = A$

$\ker h = A \Rightarrow h = 0$ #

$\Rightarrow \ker h = \{0\} \Rightarrow h$ je 1-1

(c) $\Rightarrow$ (a) sp. $a \neq 0$, $I = (a) \Rightarrow I \neq 0, A$ *) inače je a invertibilan.

$h : A \to A/I$, $h(x) = x + I$, $h \neq 0$, $A/I \neq 0$

(c) $\Rightarrow$ h je 1-1 ; $h(a) = a + I = I$, $h(0) = 0 + I = I$

$\Rightarrow$ $a = 0$ # $\Rightarrow$ a je invertibilan

*) (a) $= A \Leftrightarrow a$ je invertibilan

($\Leftarrow$) : $ab = 1 \Rightarrow x = abx = a(bx)$; $A = (a)$

($\Rightarrow$) : $(\exists b)\, ab = 1 \Rightarrow a$ je invertibilan ged

Def. Ako je A komutativan prsten, tada je ideal $I \subsetneq A$ maksimalan akko za svaki ideal J, $I \subsetneq J$, važi $J = A$.

4.) Ako je A komutativan prsten sa 1, onda A ima maksimalni ideal.

Dokaz: Koristi se Axiom of choice (tj. Zornova lema). 16. 05. 1987.

1.) (AC : $X_\alpha \neq \emptyset \Rightarrow \prod X_\alpha \neq \emptyset$ $(\alpha \in A)$

$f \in \prod X_\alpha \Rightarrow f : A \to \bigcup_\alpha X_\alpha$, $f(\alpha) \in X_\alpha$,

Zornova lema $\Leftrightarrow$ AC

$(X, \leq)$, svaki lanac ima majorantu $\Rightarrow$ X ima maksimalan element)

$\mathcal{P} = \{$ svi pravi ideali u $A\}$, $(\mathcal{P}, \subseteq)$ uređen skup

I_α - lanac pravih ideala $\Rightarrow$ $\bigcup I_\alpha$ je pravi ideal ?

$\bigcup I_\alpha \subseteq \mathcal{P}$

1° Unija ideala je ideal

$x \in \bigcup I_\alpha$, $a \in A \Rightarrow x \in I_\alpha$ za neko $\alpha \Rightarrow ax \in I_\alpha$ za neko α
$xa \in I_\alpha$

$\Rightarrow ax, xa \in \bigcup I_\alpha$

2° $\bigcup I_\alpha \neq A$

sp: $\bigcup I_\alpha = A \Rightarrow 1 \in \bigcup I_\alpha \Rightarrow 1 \in I_\alpha$ za neko α

$\Rightarrow a\,1 = a \in I_\alpha \Rightarrow I_\alpha = A$ $(1 \in I \Leftrightarrow I = A)$

$\Rightarrow \bigcup I_\alpha \in \mathcal{P}$

Familija $\mathcal{P}$ zadovoljava uslov Zornove leme *)

*) $\mathcal{P} \ni (0) \Rightarrow \mathcal{P} \neq \emptyset$

$\Rightarrow \exists\, m \in \mathcal{P}\,,\ I \in \mathcal{P} \wedge m \subseteq I \Rightarrow m = I$

(ili: $m \subseteq I \subseteq A \Rightarrow I = A \vee I = m$) QED

Prosti ideali komutativnog prstena:

A - komut. prsten sa 1

$I \subseteq A$ je prost ideal $\Leftrightarrow$

$ab \in I \Rightarrow a \in I \vee b \in I$

2.) Ako je I maksimalan, onda je I prost.

Dokaz:

m - max. ideal, $ab \in m$

$a \notin m$: $J = m + (b)$

$m \subsetneq m + (b) \subseteq A$

Zbir ideala:

$I + J = \{a + b \mid a \in I,\ b \in J\}$

$\Rightarrow$ 1° $m + (b) = m \Leftrightarrow b \in m$, ili

2° $m + (b) = A$

$\Rightarrow 1 = m + xb \quad / \cdot a \Rightarrow a = \overbrace{ma}^{\in m} + \overbrace{xab}^{\in m} \in m$ #

$\Rightarrow b \in m$ QED

3.) Naći sve proste i maksimalne ideale prstena $\mathbb{Z}$.

Rešenje:

$I \subseteq \mathbb{Z}$ ideal $\Rightarrow I = (a)$ glavni ideal

$\mathbb{Z}$ je glavnoidealski prsten

$(a) = a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\}$

Neka je (a) prost.

$xy \in (a) \Rightarrow x \in (a)$ ili $y \in (a)$

($z \in (a) \Leftrightarrow z = ab \Leftrightarrow a \mid z$)

$a \mid xy \Rightarrow a \mid x \vee a \mid y \quad \Leftrightarrow a \in Prost$

(a) je prost $\Leftrightarrow a$ je prost broj

$(0), (2), (3), (5), (7), \ldots$ su prosti ideali

[Skup svih prostih ideala zove se **spektar**

$\operatorname{Spec} A = \{$ skup svih prostih ideala prstena $A\}$]

$(0) \in \operatorname{Spec} A \Leftrightarrow \left(xy \in (0) \Rightarrow x \in (0) \vee y \in (0) \right)$

$\Leftrightarrow \left(xy = 0 \Rightarrow x = 0 \vee y = 0 \right)$

$\Leftrightarrow$ A je oblast celih

$(0) \in \operatorname{Spec} A \Leftrightarrow A$ je oblast celih

Svaki ideal (p) $(p \in \text{Prost})$ je max

$(p) \subseteq I \subseteq \mathbb{Z} \quad \wedge \quad I \neq \mathbb{Z} \Rightarrow I = (p)$ (?)

$(p) \subseteq (a) \Leftrightarrow p \in (a) \Rightarrow a \mid p$ [$I \subseteq J \Leftrightarrow J$ „deli" I]

$\Rightarrow a = 1 \vee a = p$

$a = 1 \Leftrightarrow I = \mathbb{Z}$

$a \neq 1 \Rightarrow a = p \Rightarrow (p) = I$ QED

Svaki prost ideal u $\mathbb{Z}$ je i max, osim (0), jer je $(0) \subseteq (a)$

$\operatorname{Specm} A = \{$ skup svih max ideala $\}$

$\operatorname{Specm} A \subseteq \operatorname{Spec} A$ i ne mora da važi $=$

4.) $K[x]$ je glavnoidealski.

$I \subseteq K[x]$ prost $\Rightarrow I = (f)$, f je nerastavljiv polinom

$\mathbb{C}[x]$: $(x-a)$ je prost ideal

$\mathbb{R}[x]$: $(x-a)$, (x^2+px+q) $(p^2-4q<0)$

5.) Ako je $I \subseteq A$ ideal, dokazati:

(a) I je prost akko A/I je oblast celih.

(b) I je max akko A/I je polje

Dokaz:

$\mathbb{Z}/(0) \cong \mathbb{Z}$ $\quad (a \sim b \Leftrightarrow a - b \in (0) \Leftrightarrow a - b = 0)$

$\mathbb{Z}/(p) \cong \mathbb{Z}_p$

(a) ($\Rightarrow$): $(a+I)(b+I) = I \quad (= 0+I)$

$\Rightarrow ab + I = I$

$\Rightarrow ab \in I \Rightarrow a \in I \vee b \in I \Rightarrow a + I = I \vee b + I = I$

($\Leftarrow$): analogno

(6) ($\Rightarrow$): I je max, $a \notin I$

$a + I \neq I$ $(a) + I$ je ideal u A

$(a) + I \supsetneq I \Rightarrow (a) + I = A$

$\Rightarrow 1 = a \cdot b + x \quad (x \in I)$

$\Rightarrow 1 + I = (a + I)(b + I)$

$\Rightarrow a + I$ ima inverz QED

---

def. Presek svih prostih ideala je <u>nilradikal</u>.

$$\bigcap_{P \in \operatorname{Spec} A} P = \operatorname{nil} A$$

$$\bigcap_{m \in \operatorname{Spec m} A} m = \mathcal{J}(A) \quad - \text{<u>Džekobsonov radikal</u>}$$

$\operatorname{nil} \mathbb{Z} = (0)$, $\mathcal{J}(\mathbb{Z}) = (0)$

$(a \in (p) \Leftrightarrow p \mid a \ \forall p \in \text{Prost} \Leftrightarrow a = 0)$

1) <u>$\operatorname{nil} A = \{$ skup svih nilpotentnih elemenata $\}$</u>

Dokaz:

$I = \{$ skup svih nilpotenata $\}$

<u>I je ideal</u>

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

$i \geq n \ \vee \ (i < n \wedge k - i \geq m)$

$k = m + n \Rightarrow a + b \in I$

$x \in A, \ a \in I \Rightarrow (xa)^n = x^n a^n = 0$ (A je komutativan)

<u>$I \subseteq \operatorname{nil} A$</u>

$a \in I \Rightarrow a^n = 0 \Rightarrow (\forall P \in \operatorname{Spec} A) \ a^n \in P$

$\Rightarrow a \in P$ (indukcijom po n)

($a_1, \dots a_k \in P \Rightarrow (\exists j) \ a_j \in P$, za P - prost ideal)

$\Rightarrow I \subseteq P, \ \forall P \in \operatorname{Spec} A \Rightarrow I \subseteq \operatorname{nil} A$

$\operatorname{nil} A \subseteq I$

SP: $a \in \operatorname{nil} A$, $a \notin I$

$S = \{a, a^2, a^3, \dots\} \not\ni 0$

Konstruisaćemo $P \in \operatorname{Spec} A$, $P \cap S = \emptyset$

$\mathcal{F} = \{ I \mid I \text{ je ideal}, I \cap S = \emptyset \}$, $(\mathcal{F}, \subseteq)$ je uređen skup

$\mathcal{F} \neq \emptyset$, jer $(0) \in \mathcal{F}$ $((0) \cap S = \emptyset)$

$I_\alpha \in \mathcal{F} \overset{?}{\Rightarrow} \bigcup I_\alpha \in \mathcal{F}$

$\bigcup I_\alpha$ je ideal

SP: $\bigcup I_\alpha \cap S \ni a^k \Rightarrow a^k \in I_\alpha$ za neko α #

$\Rightarrow \bigcup I_\alpha \in \mathcal{F}$

Zornova lema $\Rightarrow$ Postoji max element u familiji $\mathcal{F}$.

$P \in \mathcal{F}$, $P \cap S = \emptyset$

P je prost

$xy \in P \Rightarrow x \in P \vee y \in P$

$x, y \notin P$: $I = P + (x)$, $J = P + (y)$; $P \subsetneq I$, $P \subsetneq J$

$\Rightarrow I, J \notin \mathcal{F}$ jer je P max u $\mathcal{F}$

$\Rightarrow I \cap S \neq \emptyset$, $J \cap S \neq \emptyset$

$\Rightarrow a^n \in I \wedge a^m \in J$

$a^{n+m} = a^n a^m \in I \cdot J = (P + (x))(P + (y)) = P + (xy)$

$\Rightarrow (P + (xy)) \cap S \neq \emptyset$

$\Rightarrow xy \notin P$

Postoji prost ideal P za koji važi $(\forall k \in \mathbb{N})\ a^k \notin P$

$a \in \bigcap_{I \in \operatorname{Spec} A} I \subseteq P \Rightarrow a \in P$ #

$\Rightarrow 0 \in I$

$\Rightarrow \operatorname{nil} A \neq I$ QED

2.) (pismeni, april 97.)

Neka je $A = \{ f : \mathbb{R} \to \mathbb{R} \}$ (prsten). Naći $\bigcap \{ P \mid P \text{ je prost u } A \}$.

Rešenje:

1° $\mathrm{nil}\, A = \bigcap \{P \mid P \text{ je prost u } A\} = \{\text{skup svih nilpotentnih ...}$

$f \in A$ je nilpotentan $\Leftrightarrow (\exists n)\ f^n = 0$

$\Leftrightarrow (\exists n)(\forall x)\ (f(x))^n = 0(x) = 0$

$\Rightarrow f(x) = 0$ za sve x

$\Rightarrow f = 0$

$\mathrm{nil}\, A = \{0\}$

2° $x \in \mathbb{R}$ fix., $m_x = \{f \in A \mid f(x) = 0\}$ je ideal

$f \in m_x$, $g \in A \Rightarrow (fg)(x) = f(x)g(x) = 0 \Rightarrow fg \in m_x$

m_x je prost

$fg \in m_x \Rightarrow (fg)(x) = 0 \Rightarrow f(x)g(x) = 0 \Rightarrow f(x) = 0 \vee g(x) =$

$\Rightarrow f \in m_x \vee g \in m_x$

$\bigcap \{P \mid P \text{ je prost}\} \subseteq \bigcap_{x \in \mathbb{R}} m_x = \{0\}$

m_x je maksimalan

$f \sim g \Leftrightarrow f - g \in m_x$

$\Leftrightarrow (f-g)(x) = 0 \Leftrightarrow f(x) = g(x)$

$f/\sim \longmapsto f(x)$, $A/m_x \xrightarrow{\varphi} \mathbb{R}$

Ovo preslikavanje je izomorfizam.

$\varphi(f/\sim) = \varphi(g/\sim) \Rightarrow f(x) = g(x) \Rightarrow f \sim g \Rightarrow f/\sim = g/\sim$

$a \in \mathbb{R}$, $f = a$ (const.) $\Rightarrow \varphi(f/\sim) = a$ (NA)

$A/m_x \cong \mathbb{R}$ polje $\Rightarrow m_x$ je max.

Prsten polinoma

A - komut. prsten sa 1 ; $A[x]$ je komut. sa 1

$A[x] \supseteq A$;

$A[x_1, \dots, x_n] \supseteq A$, za $n > 1$ nema delenja !

$A[x_1, \dots, x_n]$ nije glavnoidealski

1.) Dokazati da je $I = (2, x)$ u $\mathbb{Z}[x]$ maksimalan, a (x) prost i nije max. Naći $\mathbb{Z}[x]/I$.

Dokaz:

$(2,x) = (2)+(x)$

$I \ni 2f + xg = 2n + xg$

$f \sim g \pmod I \Leftrightarrow f-g \in I \Leftrightarrow (f-g)(0) \in 2\mathbb{Z} \Leftrightarrow f(0) \equiv g(0) \pmod 2$

$(f \in I \Leftrightarrow f(0) \in 2\mathbb{Z})$

$\varphi: \mathbb{Z}[x] \longrightarrow Z_2, \quad \varphi(f) = \text{rest}(f(0), 2)$

φ je kompozicija homomorf. $\mathbb{Z}[x] \to \mathbb{Z} \to Z_2$

$f \longmapsto f(0) \longmapsto \text{rest}(f(0),2)$

$\text{Ker}\,\varphi \ni f \Leftrightarrow f(0) = 0 \pmod 2 \Leftrightarrow f(0) \in 2\mathbb{Z} \Leftrightarrow f \in I$

$\text{Ker}\,\varphi = I$

$\text{Im}\,\varphi = Z_2 \quad (\varphi \text{ je NA})$

$\mathbb{Z}[x] \longrightarrow Z_2$

$\mathbb{Z}[x]/I \xrightarrow{\sim}$

$\Rightarrow \mathbb{Z}[x]/I$ je polje

$\Rightarrow I$ je maksimalan

$(x) \subsetneq (2,x) \Rightarrow (x)$ nije max, ali je prost

$fg \in (x) \Rightarrow x \mid fg \Rightarrow (fg)(0) = 0 \Rightarrow f(0)\,g(0) = 0$

$\Rightarrow x \mid f \vee x \mid g$

$\Rightarrow f \in (x) \vee g \in (x)$

$(0) \subsetneq (x) \subsetneq (2,x)$ dužina lanca prostih idеala je 3

u $\mathbb{Z}$: $(0) \subsetneq (p)$ dužina lanca 2

2.) (homework) Ako je $h: A \to B$ homomorfizam prstena i:

(a) $P \subseteq B$ prost, onda je $h^{-1}(P)$ takođe prost u A

(b) Ako je $m \subseteq B$ max, da li je $h^{-1}(m)$ max?

Rešenje:

(a) $ab \in h^{-1}(P) \Rightarrow h(ab) = h(a)\,h(b) \in P$

$\Rightarrow h(a) \in P \vee h(b) \in P$

$\Rightarrow a \in h^{-1}(P) \vee b \in h^{-1}(P)$

20. 05. 1987.

- Zadaci -

1.) (april 85.)

$S \subseteq A$, gde je A komut. prsten sa 1, je multiplikativan skup akko: 1° $1 \in S$

2° $a, b \in S \Rightarrow ab \in S$.

Neka je $\mathcal{F} = \{ I \mid I$ je ideal u A, $I \cap S = \emptyset \}$ familija uredjena sa $\subseteq$

(a) Dokazati da $\mathcal{F}$ ima max element P.

(b) Dokazati da je P prost ideal.

- Teorija polja -

Polje razlomaka oblasti celih:

A - komut. prsten sa 1 bez delitelja 0

$A \subset K = \{ \frac{a}{b} \mid a, b \in A, b \neq 0 \}$ $(Z \subset Q)$

$K[x] \subset K(x)$ - polje racionalnih f-ja

$K[x_1, \dots, x_n] \subset K(x_1, \dots, x_n)$ (U daljem: Sva polja su karakteristike 0.)

2.) Neka je K polje, i $F, G \in K[x,y]$, dva relativno prosta polinoma. Dokazati da sistem jedn.:

$$\begin{cases} F(x,y) = 0 \\ G(x,y) = 0 \end{cases}$$

ima najviše konačno mnogo rešenja u K^2.

Dokaz: $K[x,y] \subset \underbrace{K(x)[y]}_{L} = L[y]$ - euklidski prsten

$F(x,y) = f_0(x) + f_1(x)y + \dots + f_n(x)y^n$

$G(x,y) = g_0(x) + g_1(x)y + \dots + g_n(x)y^n$

F, G su relativno prosti $\Rightarrow$ F, G su rel. prosti u $L[y]$

Sp: $H(y) = a_0(x) + a_1(x)y + \dots + a_k(x)y^k \in L[y]$, $a_i \in K(x) = L$

$H \mid F$ i $H \mid G$ u $L[y] \Rightarrow H = \frac{\tilde{H}(x,y)}{a(x)}$ (svodjenjem na zajedn.

$\tilde{H}(x,y) \in K[x,y]$, $a(x) \in K[x]$

$F = H \cdot \tilde{F}$ u $L[y] \Rightarrow F \cdot a = \tilde{H} \cdot \tilde{F}$ u $K[x,y]$

$\Rightarrow F = \tilde{H} \cdot F'$ u $K[x,y]$ (jer $a \nmid \tilde{H}$ pa $a \mid \tilde{F}$)

$\tilde{H} \mid F \wedge \tilde{H} \mid G$ #

$\Rightarrow (\exists A, B \in L[y])\ F \cdot A + G \cdot B = 1$

$\Rightarrow F\tilde{A} + G\tilde{B} = C(x)$, gde su $\tilde{A}, \tilde{B} \in K[x,y]$

(svodjenjem na zajednički imenilac)

$(x_0, y_0) \in K^2$ - rešenje $\Rightarrow$ $\left.\begin{matrix} F(x_0,y_0)=0 \\ G(x_0,y_0)=0 \end{matrix}\right\} \Rightarrow C(x_0)=0$

(x_0, y_0) rešenje $\Rightarrow$ x_0 je koren pol. C, y_0 " " " D $\Rightarrow$ QED

(Analogno: $\mathbb{Z}[x] \subset \mathbb{Q}[x]$, jer u $\mathbb{Z}[x]$ ne važi Euklidov algoritam)

$K \subset L$ (K, L - polja)

3.) Ako je $h : K \to L$ homomorfizam polja, $h \neq 0$, onda je h 1-1.

Dokaz:

$\operatorname{Ker} h \subset K$ ideal u K ($\{0\}, K$)

$\operatorname{Ker} h = K \Rightarrow h = 0$ #

$\Rightarrow \operatorname{Ker} h = 0 \Rightarrow h$ je 1-1 QED

Svaki homomorf. polja može se shvatiti kao inkluzija $K \hookrightarrow L$

$\Rightarrow L$ je proširenje od K , L/K

$\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ (kula proširenja)

L/K je konačno proširenje akko je $\dim_K L < \infty$

$\dim_K L = [L : K]$ stepen proširenja

$[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$ ($2^{\aleph_0}$)

L/K je konačno generisano akko je $L = K(a_1, \ldots, a_n)$, $a_i \in L \setminus K$

$a_1, \ldots, a_n$ su generatori

$\sqrt{2} \notin \mathbb{Q}$: $L = \mathbb{Q}(\sqrt{2})/\mathbb{Q}$

$n=1$: prosto proširenje (primitivno)

Ako je $K \subset L \subset M$ tada konačnih proširenja, onda je i M/K konačno i

$$[M:K] = [M:L]\cdot[L:K]$$

4.) (Teorema) Ako je $f(x) \in K[x]$ nerastavljiv polinom $\deg f = n$, L/K proširenje takvo da $a \in L$, $f(a) = 0$, onda je $K(a) = K[a]$ konačno proširenje i $[K(a):K] = n$.

f se naziva minimalni polinom za a.

$\sqrt{2} = \alpha \in \mathbb{C}$, koren polinoma $x^2 - 2 \in \mathbb{Q}[x]$

$x^2 - 2$ je nerastavljiv nad $\mathbb{Q}$

($p = 2$ - Eisenstein-ov kriterijum,

analogno: $x^n - 2$ je nerastavljiv nad $\mathbb{Q}$ za svako $n \in \mathbb{N}$)

$\Rightarrow [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$

$(\forall n)\ [\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}] = n$

K - polje $\Rightarrow$ $\mathrm{Aut}\, K$ je grupa automorfizama

L/K proširenje,

$G = \{g \in \mathrm{Aut}\, L \mid (\forall a \in K)\, g(a) = a\} < \mathrm{Aut}\, K$

G je grupa Galoa : $G = \mathrm{Gal}(L/K)$;

5.) Naći $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

Rešenje

$g : \mathbb{C} \to \mathbb{C}$, $g \in \mathrm{Aut}\, \mathbb{C}$, $g(a) = a$ za sve $a \in \mathbb{R}$.

$g(a+bi) = a + b\,g(i)$ $\quad (a, b \in \mathbb{R})$

$i^2 + 1 = 0$ $\quad /g$

$g(i^2) + 1 = 0 \iff (g(i))^2 + 1 = 0 \Rightarrow g(i)$ je koren jedn. $x^2 + 1 = 0$

$\Rightarrow g(i) \in \{i, -i\}$

$g(i) = i \Rightarrow g = id$

$g(i) = -i \Rightarrow g(z) = \bar{z}$

$\Big\}$ $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{id, conj\} \cong \mathbb{C}_2$

Zadaci

1) Ako je proširenje konačno, onda je konačno generisano.
Obrat ne vrazi

Dokaz:

$\dim_K L = n$; $[e_1, \dots, e_n]$ baza L nad K

$L = Ke_1 + \dots + Ke_n \subseteq K(e_1, \dots, e_n)$ $\Big\}(=)$

$e_i \in L$, $K \subseteq L \Rightarrow K(e_1, \dots, e_n) \subseteq L$

($[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2}$ (racionalizacija imenioca)

$\frac{f(\sqrt{2})}{g(\sqrt{2})} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = a' + b'\sqrt{2}$

$\mathbb{C} = \mathbb{R}(i)$; $i : x^2+1 = 0$ (nerastavljiv nad $\mathbb{R}$)

$\mathbb{C} = \mathbb{R} + \mathbb{R}i$; $[1, i]$ baza

$\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ $\frac{f_1(\sqrt[n]{2})}{g(\sqrt[n]{2})} =$)

$\mathbb{R}(x)/\mathbb{R}$ je konačno gen., ali nije konačno; x je transcedentan

$1, x, x^2, \dots$ je $\subset \mathbb{N}$

$a \in L$ je algebarski nad K akko postoji polinom $f \in K[x]$, t.d. je $f(a) = 0$.

U suprotnom, a je transcedentan.

$\pi, e \in \mathbb{R}/\mathbb{Q}$ transc.

Proširenje L/K je algebarsko akko je svaki $a \in L$ algebarski nad K.

2.) Konačno generisano <u>algebarsko</u> proširenje je konačno i to prosto (teorema o primitivnom elementu)

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\xi)$, ξ postoji, ξ je primitivni element

$\xi = c_1a_1 + \dots + c_na_n$, $c_i \in K$, $L = K(a_1, \dots, a_n)$

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, ξ nije jedinstveno

---

$a \in L$, a algebarski nad K

$\Rightarrow$ Polinom najmanjeg stepena $\mu_a \in K[x]$, $\mu_a(a) = 0$, je minimalni polinom μ_a je nerast. $[K(a) : K] = \deg \mu_a(x)$

$$\underbrace{\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})}_{\text{stepen } 2,\ x^2-2} \subset \underbrace{\mathbb{Q}(\sqrt{2})(\sqrt{3})}_{2,\ x^2-3} = \mathbb{Q}(\sqrt{2},\sqrt{3})$$

Da li je $x^2-3 \in \mathbb{Q}(\sqrt{2})[x]$ nerastavljiv? Jeste.

SP x^2-3 je rastavljiv nad $\mathbb{Q}(\sqrt{2})[x]$

$\Rightarrow \sqrt{3} \in \mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2}$

$\sqrt{3} = a + b\sqrt{2}$ $(a,b \in \mathbb{Q}) \Rightarrow 3 = a^2 + 2b^2 + 2ab\sqrt{2}$

$\Rightarrow \sqrt{2} \in \mathbb{Q}$ #

$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$; $\deg_{\mathbb{Q}} \xi = 4$

---

3) Dokazati:

(a) Ako dva elementa cikličke grupe nisu kvadrati, njihov proizvod jeste

(b) Za svako $p \in$ Prost jedan od elemenata skupa $\{2,3,6\}$ je potpun kvadrat u $\mathbb{Z}_p$.

(c) Polinom $x^4 - 10x^2 + 1$ je nerastavljiv nad $\mathbb{Q}$, a rastavljiv nad $\mathbb{Z}_p$ za svako $p \in$ Prost.

Dokaz:

(a) $G = \langle a \rangle$, a^k je kvadrat $\Leftrightarrow$ k je paran

a^k, a^l nisu kvadrati $\Rightarrow k, l$ su neparni

$\Rightarrow a^k a^l = a^{k+l}$ je kvadrat

(b) $6 = 2 \cdot 3$; $\mathbb{Z}_p^*$ je ciklična reda $p-1$

(i) 2 je kvadrat : OK

(ii) 3 " " OK

(iii) 2 i 3 nisu kvadrati $\overset{(a)}{\Rightarrow}$ 6 je kvadrat

(c)
$$x^4 - 10x^2 + 1 = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}) \quad \text{nad } \mathbb{R}$$

$$= (x^2 + 2\sqrt{2}x - 1)(x^2 - 2\sqrt{2}x - 1)$$

$$= (x^2 + 2\sqrt{3}x + 1)(x^2 - 2\sqrt{3}x + 1)$$

$$= (x^2 + 5 + 2\sqrt{6})(x^2 + 5 - 2\sqrt{6})$$

jedine 3 moguće faktorizacije na kvadratne faktore

i naći stepen tog proširenja

b) Odrediti bar jedan polinom sa koef. iz $\mathbb{Q}$ čije je F korensko polje.

Dokaz:

(a) $F \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

$$\frac{x_1\sqrt{2} + y_1\sqrt{3} + z_1\sqrt{5}}{x_2\sqrt{2} + y_2\sqrt{3} + z_2\sqrt{5}} = \frac{x_1 + y_1\sqrt{\frac{3}{2}} + z_1\sqrt{\frac{5}{2}}}{x_2 + y_2\sqrt{\frac{3}{2}} + z_2\sqrt{\frac{5}{2}}}$$

$F \subset \mathbb{Q}(\sqrt{\frac{3}{2}}, \sqrt{\frac{5}{2}})$

$F = \operatorname{Im} h$, $h : \mathbb{Q}(x,y) \longrightarrow \mathbb{C}$, $h(x) = \sqrt{\frac{3}{2}}$, $h(y) = \sqrt{\frac{5}{2}}$

h je monomorfizam, jer je $\mathbb{Q}(x,y)$ polje

$h : \mathbb{Q}(x,y) \cong \operatorname{Im} h$ (?) = neposredno proveravanje *)

(b) $F = \mathbb{Q}(\alpha, \beta)$, $\alpha = \sqrt{\frac{3}{2}}$, $\beta = \sqrt{\frac{5}{2}}$

($\subseteq$): true

($\supseteq$): $\alpha, \beta \in F$, F polje $\Rightarrow \mathbb{Q}(\alpha,\beta) \subset F$

*) $x, y \in F \Rightarrow x+y \in F, x \cdot y \in F$

$x \neq 0 \Rightarrow x^{-1} \in F$

Primitivni element: $\gamma = \sqrt{\frac{3}{2}} + \sqrt{\frac{5}{2}}$: $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha,\beta)$

$\gamma^2 = \frac{3}{2} + 2\alpha\beta + \frac{5}{2}$

$\Rightarrow \gamma^2 - 4 = \sqrt{15} \Rightarrow (\gamma^2-4)^2 = 15$

$p(x) = x^4 - 8x^2 + 1$ zadovoljava γ

p nema racionalnih korena

$x^4 - 8x + 1 = (x^2 + px + q)(x^2 + p'x + q')$

Korени: $\pm\sqrt{4 \pm \sqrt{15}}$ ($= x_{1,2,3,4}$)

$(x - x_1)(x - x_2) \notin \mathbb{Q}[x]$

$\Rightarrow p$ je nerastavljiv, p je minimalni za γ

$\Rightarrow [\mathbb{Q}(\gamma) : \mathbb{Q}] = \text{st } p = 4$

α i β se izražavaju preko γ: 34

$\gamma = \alpha + \beta$; $(\alpha+\beta)(\alpha-\beta) = \frac{3}{2} - \frac{5}{2} = -1 \Rightarrow \alpha - \beta = -\frac{1}{\gamma} \Rightarrow \begin{cases} \alpha = \frac{1}{2}(\gamma - \frac{1}{\gamma}) \\ \beta = \frac{1}{2}(\gamma + \frac{1}{\gamma}) \end{cases}$

- ZADACI -

1. Ako je $N \lhd G$, $H < G$, dokazati:

a) $N \cap H \lhd G$; b) $NH < G$.

Dokaz:

b) $1 \in NH$; $\emptyset \neq NH \subset G$

$x = n_1 h_1$, $y = n_2 h_2 \in NH$ ($n_i \in N$, $h_i \in H$, $i = 1,2$)

$\Rightarrow \quad xy = n_1 h_1 n_2 h_2$

$N \lhd G \Rightarrow (\exists n_2' \in N)\ h_1 n_2 = n_2' h_1$

$\Rightarrow xy = n_1 n_2' h_1 h_2 \in NH$

$x = nh \in NH \Rightarrow x^{-1} = h^{-1} n^{-1} = n' h^{-1} = n' h' \in NH$, za neko $n' \in N$

---

2. Dokazati: (a) $(R,+) \cong (C,+)/(R,+)$;

(b) $(Q^+, \cdot) \cong (Q^*, \cdot)/C_2$

(c) $(C^*, \cdot) \cong (C,+)/(Z,+)$.

Dokaz:

(a) $f : C \to R$, $f(z) = \mathrm{Im}\, z$, $f(C) = R$, $\mathrm{Ker} f = R$

$f(z_1 + z_2) = \mathrm{Im}(z_1 + z_2) = \mathrm{Im}\, z_1 + \mathrm{Im}\, z_2 \Rightarrow f(z_1) + f(z_2)$

$\Rightarrow (C,+)/(R,+) \cong (R,+)$

$$\begin{array}{ccc} (C,+) & \xrightarrow{f} & (R,+) \\ {\scriptstyle k}\downarrow & \nearrow_{\sim} & \\ (C,+)/(R,+) & & \end{array}$$

(b) $\varphi : Q^* \to Q^+$, $\varphi(x) = |x|$

$\varphi(xy) = |xy| = |x|\,|y| = \varphi(x)\,\varphi(y)$,

$\mathrm{Ker}\,\varphi = \{x \in Q^* \mid \varphi(x) = 1\} = \{-1, 1\} = C_2$

$\varphi(Q^*) = Q^+ \Rightarrow (Q^*, \cdot)/C_2 \cong (Q^+, \cdot)$

$$\begin{array}{ccc} (Q^*, \cdot) & \xrightarrow{\varphi} & (Q^+, \cdot) \\ {\scriptstyle k}\downarrow & \nearrow_{\sim} & \\ (Q^*, \cdot)/C_2 & & \end{array}$$

---

3. Ako je $C = \langle a ; a^n = 1 \rangle$ *abelova grupa reda* n, *onda je*

$$\mathrm{Aut}\, C \cong (\Phi_n, \cdot, 1)$$

gde je $\Phi_n = \{k \in N \mid 1 \leq k < n,\ (k,n) = 1\}$, $\cdot$ *množenje po mo*

Dokaz:

Neka je $f \in \mathrm{Aut}\, C$. Tada za svako $x \in C$, postoji $i \in N$, $0 \leq i < n$, tako da je $x = a^i$, pa je $f(x) = f(a^i) = f(a)^i$. Dakle, f je jednoznačno određeno pomoću slike generatorsk

elementa $f(a)$. Kako je f automorfizam, sledi $\text{red}(a) = \text{red}(f(a))$, a kako $f(a) \in C$, sledi $f(a) = a^k$ za neko $k \in N$, $1 \leq k < n$. Dakle, $\text{red}(a) = \text{red}(a^k)$, a to je moguće samo ako je $(k,n) = 1$. Zaista, ako je $n = kl$, za neko $l \in N$, $1 < l < n$, onda je $f(a)^l = (a^k)^l = a^{kl} = a^n = 1$, pa je $\text{red}(f(a)) = \text{red}(a^k) \leq l < n$, što je u suprotnosti sa pretpostavkom.

Prema tome, svako $k \in N$, $1 < k < n$, $(k,n) = 1$ određuje točno jedan automorfizam $f_k \in \text{Aut}\, C$, $f_k(a) = a^k$, pa je preslikavanje $k \mapsto f_k$ skupa Φ_n u $\text{Aut}\, C$ bijekcija. Kako je za sve $k_1, k_2 \in \Phi_n$:

$$(f_{k_1} \circ f_{k_2})(a) = f_{k_1}(a^{k_2}) = a^{k_1 k_2} = a^{k_1 \cdot_n k_2} = f_{k_1 \cdot_n k_2}(a)$$

to preslikavanje je i homomorfizam, dakle izomorfizam. QED

Posljedica: $|\text{Aut}\, C_n| = \varphi(n)$, gdje je φ Eulerova funkcija

$p \in \text{Prost} \Rightarrow |\text{Aut}\, C_p| = p - 1$

---

4. Dokazati: (a) $(\forall i \in I)\, H_i \in \text{Inv}(G) \Rightarrow \bigcap_{i \in I} H_i \in \text{Inv}(G)$.

(b) $(\forall i \in I)\, H_i \in \text{Inv}(G) \Rightarrow \langle \bigcup_{i \in I} H_i \rangle \in \text{Inv}(G)$

(c) $(\exists_1 H)(H < G \wedge |H| = n) \Rightarrow H \in \text{Char}(G)$

(d) Sve podgrupe ciklične grupe su potpuno inv.

(e) $Z(G)$ nije uvijek potpuno inv. podgrupa u G.

Dokaz:

(a) $f \in \text{End}\, G$: $f(\bigcap_{i \in I} H_i) \subseteq \bigcap_{i \in I} f(H_i) \subseteq \bigcap_{i \in I} H_i$

(b) $\langle \bigcup_{i \in I} H_i \rangle = \{ h_1^{s_1} \cdots h_n^{s_n} \mid n \in N,\ s_1, \ldots, s_n \in Z,\ h_k \in H_{i_k},\ k = \overline{1,n} \}$

$f \in \text{End}\, G$, $x = h_1^{s_1} \cdots h_n^{s_n}$

$\Rightarrow f(x) = f(h_1^{s_1} \cdots h_n^{s_n}) = f(h_1)^{s_1} \cdots f(h_n)^{s_n}$, $f(h_k) \in f(H_{i_k}) \subseteq H_{i_k}$

$\Rightarrow f(x) \in \langle \bigcup_{i \in I} H_i \rangle \Rightarrow f(\langle \bigcup_i H_i \rangle) \subseteq \langle \bigcup_i H_i \rangle$

(c) $|H| = n$, $f \in \text{Aut}\, G \Rightarrow f(H) < G$, $|f(H)| = n \Rightarrow f(H) = H$

(d) $C = \langle a \rangle$; $H = \langle a^k \rangle < C$, $f \in \mathrm{End}\, C$

$\Rightarrow f(a) \in C \Rightarrow (\exists m \in \mathbb{Z})\ f(a) = a^m$

$f(a^k) = f(a)^k = (a^m)^k = a^{mk} = (a^k)^m \in H \Rightarrow f(H) \subseteq H$

(e) Neka je $G = \{A \in M_2(K) \mid \det A \neq 0\}$ (K je polje). Neka preslikavanje $f : G \to K \setminus \{0\}$ zadovoljava uslov

$$f(AB) = f(A) + f(B) \qquad (A, B \in G).$$

Preslikavanje $\Psi : G \to G$, $\Psi(A) = \begin{bmatrix} 1 & f(A) \\ 0 & 1 \end{bmatrix}$ je jedan endomorfizam grupe G. Centar grupe G je oblika

$$Z(G) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in K, a \neq 0 \right\}$$

Neka je $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in Z(G)$. Tada je $\Psi(A) = \begin{bmatrix} 1 & f(A) \\ 0 & 1 \end{bmatrix}$, pa $\Psi(A) \notin Z(G)$, jer $f(A) \neq 0$. Dakle, $Z(G) \notin \mathrm{Inv}(G)$. QED

---

5. Dokazati: $\mathrm{Aut}\, S_3 \cong S_3$.

Dokaz: $S_3 \cong D_3 = \langle a, b ;\ a^3 = 1,\ b^2 = 1,\ ab = ba^2 \rangle = \{1, a, a^2, b, ba, ba^2\}$

$f \in \mathrm{Aut}\, S_3$: $\mathrm{red}\, f(a) = \mathrm{red}(a) = 3 \Rightarrow f(a) \in \{a, a^2\}$

$\mathrm{red}\, f(b) = \mathrm{red}(b) = 2 \Rightarrow f(b) \in \{b, ba, ba^2\}$

$(ba)^2 = baba = bba^2a = b^2a^3 = 1 \Rightarrow \mathrm{red}(ba)^2 = 2$

$(ba^2)^2 = aba^2 = a^3 = 1 \Rightarrow \mathrm{red}(ba^2) = 2$

$\Rightarrow |\mathrm{Aut}\, S_3| = |\{a, a^2\}| \times \{b, ba, ba^2\}| = 6$

Kako je $\mathrm{Aut}\, S_3$ nekomutativna*), sledi $\mathrm{Aut}\, S_3 \cong S_3$, jer je do jedina nekomutativna (do na izomorfizam) grupa reda 6

*) $f_1 = \begin{pmatrix} 1 & a & a^2 & b & ba & ba^2 \\ 1 & a & a^2 & ba^2 & b & ba \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & a & a^2 & b & ba & ba^2 \\ 1 & a^2 & a & ba^2 & ba & b \end{pmatrix}$

$(f_1 \circ f_2)(b) = ba \neq b = (f_2 \circ f_1)(b) \Rightarrow f_1 \circ f_2 \neq f_2 \circ f_1$

---

6. Ako su f i g disjunktne permutacije skupa X, onda je $fg = gf$.

Dokaz: $x \in X$

1° $f(x) = x \Rightarrow (gf)(x) = g(x) \wedge (fg)(x) = g(x)$

SP: $(fg)(x) \neq g(x) \Leftrightarrow f(g(x)) \neq g(x) \Rightarrow g(g(x)) = g(x) \Rightarrow g(x) = x$

$\Rightarrow (fg)(x) = f(x) = x \quad \wedge \quad (gf)(x) = g(x) = x$

$\Rightarrow (fg)(x) = (gf)(x)$

$2^\circ \; f(x) \neq x \Rightarrow g(x) = x \quad ; \quad (fg)(x) = f(x)$

SP: $(gf)(x) \neq f(x) \Leftrightarrow g(f(x)) \neq f(x) \Rightarrow f(f(x)) = f(x) \Rightarrow f(x) = x$ #

$\Rightarrow (gf)(x) = f(x)$

$\Rightarrow (fg)(x) = (gf)(x)$ QED

---

7. Sledeće permutacije predstaviti kao proizvod disjunktnih ciklusa:

(a) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$, (b) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 8 & 7 & 9 & 2 & 1 & 3 & 6 \end{pmatrix}$

Rešenje:

(a) $C_1 = \{1, f(1), f^2(1), \dots\} = \{1, 2, 4\} = C_2 = C_4$

$C_3 = \{3, f(3), f^2(3), \dots\} = \{3, 5\} = C_5$

$\Rightarrow f = (1\,2\,4)(3\,5)$

(b) $C_1 = \{1, g(1), g^2(1), \dots\} = \{1, 4, 7\} = C_4 = C_7$

$C_2 = \{2, 5, 9, 6\} = C_5 = C_6 = C_9$

$C_3 = \{3, 8\} = C_8$

$g = (1\,4\,7)(2\,5\,9\,6)(3\,8) \quad \left(= (2\,5\,9\,6)(1\,4\,7)(3\,8) = \dots \right)$

---

8. Neka je G konačna grupa reda n i neka je $k \in \mathbb{N}$ takav da je $NZD(k, n) = 1$. Dokazati da je preslikavanje $f: G \to G$ definisano sa $f(x) = x^k$ $(x \in G)$, bijektivno.

Dokaz:

Kako je $NZD(k, n) = 1$, prema Bezuovoj stavi postoje $m, l \in \mathbb{Z}$, takvi da je $km + nl = 1$. Za $x \in G$ imamo:

$x = x^{km+nl} = x^{km} = (x^m)^k = f(x^m)$, pa je preslikavanje f NA, jer $x^m \in G$.

Neka su $x, y \in G$. Tada važi:

$f(x) = f(y) \Rightarrow x^k = y^k \Rightarrow x^{km} = y^{km}$

$\Rightarrow x^{km+nl} = y^{km+nl}$

$\Rightarrow x = y$, pa je f 1-1. QED

9. Ako je G konačna grupa i $G/Z(G)$ ciklična, onda je G Abelova.

Dokaz:

Neka je $G/Z(G) = \langle aZ(G) \rangle$, za neko $a \in G$ i neka je $red(aZ(G)) = n$ (tj. $G/Z(G) \cong \mathbb{C}_n$). Tada je

$$G/Z(G) = \{ Z(G), aZ(G), \dots, a^{n-1}Z(G) \},$$

pa je $G = Z(G) \cup aZ(G) \cup \dots \cup a^{n-1}Z(G)$, pri čemu je unija disjunktna. Neka su $x, y \in G$. Tada postoje $k_1, k_2 \in \mathbb{N}$, $0 \leq k_1, k_2 < n$, $z_1, z_2 \in Z(G)$, takvi da je

$$x = a^{k_1} z_1 \quad \text{i} \quad y = a^{k_2} z_2.$$

Sledi: $xy = a^{k_1} z_1 \cdot a^{k_2} z_2 = a^{k_1} a^{k_2} z_1 z_2 = a^{k_1 + k_2} z_2 z_1$

$= a^{k_2} a^{k_1} z_2 z_1 = a^{k_2} z_2 a^{k_1} z_1 = yx$,

pa je grupa G komutativna. QED

---

10. Da li postoji nekomutativna grupa reda 81 koja ima centar reda 27?

Rešenje: Ako bi G postojala, onda bi bilo $|G : Z(G)| = 3$, i zato $G/Z(G) \cong \mathbb{C}_3$, pa bi na osnovu zadatka 9. grupa G bila Abelova što je suprotno pretpostavci. Dakle, G ne postoji.

---

11. Neka je $n \geq 3$.

a) Odrediti centar $Z(D_{2n})$ dijedarske grupe D_{2n}.

b) Dokazati da je $D_{2n}/Z(D_{2n}) \cong D_n$.

Rešenje:

a) Kako je $D_{2n} = \langle \rho, \sigma ; \rho^{2n} = 1, \sigma^2 = 1, \rho\sigma = \sigma\rho^{2n-1} \rangle$

$= \{ 1, \sigma, \rho, \rho^2, \dots, \rho^{2n-1}, \sigma\rho, \sigma\rho^2, \dots, \sigma\rho^{2n-1} \}$, sledi da ako $x \in Z(D_{2n})$, onda je $x = \sigma^i \rho^j$ za neko $i \in \{0,1\}$, $j \in \{0, \dots, 2n-1\}$

1° slučaj: $x = \sigma\rho^j$ $(0 \leq j \leq 2n-1)$

Neka je $a = \rho^m \in D_{2n}$ $(0 \leq m \leq 2n-1)$. Tada je $ax = xa$.

tj. $\rho^m\sigma\rho^j = \sigma\rho^j\rho^m$, odn. $\rho^m\sigma = \sigma\rho^m$.

Kako je $\rho^m\sigma = \rho^{m-1}\rho\sigma = \rho^{m-1}\sigma\rho^{2n-1} = \dots = \sigma\rho^{m(2n-1)} = \sigma\rho^{-m}$

sledi $\sigma\rho^m = \sigma\rho^{-m}$, pa je $\rho^{2m} = 1$, tj. $m = 0$, pa

$x \in Z(D_{2n})$ ne može biti oblika $\sigma\rho^j$

2° slučaj: $x = \rho^k$ $(0 \le k < 2n)$.

Neka je $a = \sigma^i\rho^j$ $(i \in \{0,1\},\ j \in \{0,1,\dots,2n-1\})$. Tada imamo

$ax = xa \Leftrightarrow \sigma^i\rho^j\rho^k = \rho^k\sigma^i\rho^j \Leftrightarrow \sigma^i\rho^k = \rho^k\sigma^i$ (*)

Za $i = 0$, (*) je tačno, a za $i = 1$, treba da je $\sigma\rho^k = \rho^k\sigma$.

Kako je $\rho^k\sigma = \sigma\rho^{-k}$, sledi $\sigma\rho^k = \sigma\rho^{-k}$, tj. $\rho^{2k} = 1$,

pa je $2n = 0 \pmod{2n}$, i zato $k \in \{0, n\}$

Dakle, $Z(D_{2n}) = \{1, \rho^n\} \cong C_2$.

b) Primetimo da je $|D_{2n}/Z(D_{2n})| = |D_{2n} : Z(D_{2n})| = \frac{4n}{2} = 2n$

$= |D_n|$. Kako je $D_{2n}/Z(D_{2n}) = \{xZ(D_{2n}) \mid x \in D_{2n}\}$ =

zbog $\rho^k Z(D_{2n}) = \{\rho^k, \rho^{n+k}\} = \rho^{n+k}Z(D_{2n})$ (za $0 \le k \le n-1$)

i $\sigma\rho^k Z(D_{2n}) = \{\sigma\rho^k, \sigma\rho^{k+n}\} = \sigma\rho^{n+k}Z(D_{2n})$ $(k = \overline{0, n-1})$,

sledi: $D_{2n}/Z(D_{2n}) = \{Z, \sigma Z, \rho Z, \rho^2 Z, \dots, \rho^{n-1}Z, \sigma\rho Z, \sigma\rho^2 Z, \dots, \sigma\rho^{n-1}Z\}$,

gde je $Z = Z(D_{2n})$.

Preslikavanje $f : D_{2n}/Z(D_{2n}) \to D_n$ $(D_n = \langle a, b; a^n = 1, b^2 = 1, ab = ba^{n-1}\rangle)$

definisano sa $f(\sigma^i\rho^j Z) = b^i a^j$ $(i \in \{0,1\},\ j \in \{0,1,\dots,n-1\})$

je izomorfizam što se lako proverava. Q.E.D.

---

12. Dokazati da je jedina grupa reda 15 ciklična grupa C_{15}.

Dokaz: $(G, \cdot, 1)$ grupa, $|G| = 15 = 3 \cdot 5$.

I Sylow. - teorema: $(\exists P, Q)$ $P < G$, $Q < G$, $|P| = 3$, $|Q| = 5$

$|G : Q| = 15/5 = 3$, 3 je najmanji prost broj koji deli 15

$\Rightarrow Q \lhd G$; $P = \{1, a, a^2\} = \langle a\rangle$, $Q = \{1, b, b^2, b^3, b^4\} = \langle b\rangle$

$b^a = a^{-1}ba \in Q \Rightarrow (\exists i \in \{1,2,3,4\})\ b^a = b^i$

$b^a = b^i \to (b^a)^a = (b^i)^a \Rightarrow b^{a^2} = (b^a)^i \Rightarrow b^{a^2} = b^{i^2}$

$\Rightarrow b^{a^3} = b^{i^3}$; $b^{a^3} = b^1 = b \Rightarrow b^{i^3} = b^1$ 3Y

$\Rightarrow i^3 = 1 \pmod 5 \Rightarrow i \in \{1,6,11,\dots\} \cap \{1,2,3,4\} = \{1\}$

$\Rightarrow b^a = b, \Rightarrow a^{-1}ba = b \Rightarrow ba = ab \Rightarrow G$ je Abelova

$\Rightarrow G = C_{15} \cong C_3 \times C_5$ QED

---

13. Dokazati da svaka grupa reda 30 sadrži bar jednu pravu normalnu podgrupu, tj. da nije prosta.

Dokaz:

Neka je G grupa reda 30. Ako je G Abelova, svaka njena prava podgrupa (na primer, S_2 - podgrupa reda 2) je normalna. Neka je zato G neabelova.

Prema I Sylow-ljevoj teoremi postoje S_3- i S_5- podgrupe P, Q grupe G, respektivno, pri čemu je $|P| = 3$, $|Q| = 5$, i zato $P = \langle a; a^3 = 1\rangle \cong C_3$, $Q = \langle b; b^5 = 1\rangle \cong C_5$. Neka je $H = \langle P \cup Q\rangle$. Kako je $P < H$, $Q < H$, $H < G$, sledi $3 \mid |H|$, $5 \mid |H|$, $|H| \mid 30$, pa je $|H| \in \{15, 30\}$. Međutim, u H nema elemenata reda 2 (jer ga nema ni u P i Q), a kako $2 \mid |G|$, prema Cauchy-jevoj lemi u G postoji element reda 2. Dakle, $H \neq G$, pa je $|H| = 15$. Na osnovu toga je $|G:H| = 2$, pa kako je 2 najmanji prost broj koji deli $|G| = 30$, sledi da je $H \lhd G$. Dakle, G nije prosta. QED

---

14. Neka je G grupa i $H \lhd G$, takva da je $H \cong C_2$. Dokazati: ako je G/H ciklična grupa, onda je G Abelova grupa.

Dokaz:

Neka je $H = \langle a; a^2 = 1\rangle$. Dokazaćemo da je $H < Z(G)$. Zaista, za $x \in G$ imamo: $x \cdot 1 = 1 \cdot x$ i $x \cdot a = a \cdot x$, jer ako bi bilo $x \cdot a = 1 \cdot x$, sledilo bi $a = 1$, što nije tačno (kako je $H \lhd G$ važi: $(\forall x \in G)(\forall h \in H)(\exists h' \in H)\ xh = h'x$).

Dakle, svi elementi iz H komutiraju sa svim elementima iz G, pa je $H \subseteq Z(G)$ i zato $H < Z(G)$. Analogno, kao

u zadatku 9., iz pretpostavke da je G/H ciklična grupa, dokazuje se da je G Abelova grupa. QED

Uopštenje rezultata u zad. 9.:

Ako je G grupa, $H < Z(G)$ i G/H ciklična, onda je G Abelova

---

15. Dokazati da je prvi izvod grupe normalna podgrupa u G

Dokazati, zatim, da je G Abelova akko je $G' = \{1\}$.

Dokaz: $[a,b] = aba^{-1}b^{-1} \quad (a,b \in G)$

$G' = \langle \{[a,b] \mid a,b \in G\} \rangle = \{[a_1,b_1] \cdots [a_n,b_n] \mid n \in N,\ a_i, b_i \in G\}$

$\sigma_x([a,b]) = \sigma_x(aba^{-1}b^{-1}) = \sigma_x(a)\sigma_x(b)\sigma_x(a)^{-1}\sigma_x(b)^{-1} = [\sigma_x(a), \sigma_x(b)] \quad (x \in G)$

$g \in G' \Rightarrow g = [a_1,b_1] \cdots [a_n,b_n] \Rightarrow \sigma_x(g) = [\sigma_x(a_1), \sigma_x(b_1)] \cdots [\sigma_x(a_n), \sigma_x(b_n)] \ (x \in G)$

$\Rightarrow \sigma_x(g) \in G' \Rightarrow \sigma_x(G') \subseteq G' \Rightarrow G' \lhd G$

$(\forall a,b \in G)\ ab = ba \Leftrightarrow (\forall a,b \in G)\ aba^{-1}b^{-1} = 1 \Leftrightarrow (\forall a,b \in G)\ [a,b] = 1$

$\Leftrightarrow G' = \{1\}$ QED

---

16. Neka je G grupa i $H < G$, $|G : H| = n$. Dokazati da postoji homomorfizam $\varphi : G \to \mathrm{Sym}\, X$, takav da je $\mathrm{Ker}\,\varphi$ maksimalna normalna podgrupa u G među onima koje su sadržane u H.

Dokaz: Kako je $|G/H| = n$, postoje različiti elementi $g_1, \ldots, g_n \in G$, takvi da je $G/H = \{Hg_1, \ldots, Hg_n\}$, pri čemu $i \neq j$ povlači $Hg_i \cap Hg_j = \emptyset$. Posmatrajmo preslikavanje $\varphi : G \to \mathrm{Sym}\, G/H$, definisano sa

$$\varphi(x) = \begin{pmatrix} Hg_1 & \cdots & Hg_n \\ Hg_1x & & Hg_nx \end{pmatrix}$$

Kako je $\varphi(x) \cdot \varphi(y)(Hg_i) = \varphi(y)(\varphi(x)(Hg_i)) = Hg_ixy = \varphi(xy)(Hg_i)$ (leva notacija), pres. φ je homomorfizam. Dokazujemo da je $\mathrm{Ker}\,\varphi \subseteq H$.

$x \in \mathrm{Ker}\,\varphi \Rightarrow \varphi(x) = \iota_{G/H} \Rightarrow (\forall i)\ \varphi(x)(Hg_i) = Hg_i$

$\Rightarrow (\forall i)\ Hg_ix = Hg_i \Rightarrow (\forall i)\ x \in Hg_i \Rightarrow x \in H \cdot 1 = H$

Dokazujemo $\operatorname{core}(H) \subseteq \operatorname{Ker}\varphi$ ($\operatorname{core}(H)$ je maksimalna normalna podgrupa u G, sadržana u H).

$$x \in \operatorname{core}(H) \Rightarrow x \in \bigcap_{g\in G} \sigma_g(H) \Rightarrow (\forall g \in G)\ x \in g^{-1}Hg$$
$$\Rightarrow (\forall g \in G)\ gx \in Hg$$
$$\Rightarrow (\forall i)\ \varphi(x)(Hg_i) = Hg_i x = Hg_i \text{ , jer } g_i x \in H, \text{ a } HHg_i = Hg_i$$
$$\Rightarrow \varphi(x) = 1_{G|H} \Rightarrow x \in \operatorname{Ker}\varphi$$

Primetimo da je $\operatorname{Sym} X \cong S_n$, zbog $|X| = |G/H| = n$, pa je, dakle, grupa G homomorfna sa S_n. QED

---

17. Dokazati da su permutacije $p, q \in S_n$ konjugovane u grupi S_n akko se mogu rastaviti na jednak broj disjunktnih ciklusa i među tim ciklusima se može uspostaviti bijektivno preslikavanje tako da su odgovarajući ciklusi iste dužine.

Dokaz:

Dokazujemo, prvo, da za proizvoljnu permutaciju $f \in S_n$ i ciklus $(a_1 \dots a_k)$ važi:

$$f^{-1}(a_1 \dots a_k) f = (f^{-1}(a_1) \dots f^{-1}(a_k)), \tag{1}$$

što je ekvivalentno sa: $(a_1 \dots a_k) f = f(f^{-1}(a_1) \dots f^{-1}(a_k))$. (1')

Obeležimo levu stranu u (1') sa L, a desnu sa D.

Ako je $x = f^{-1}(a_i)$ za neko i, $1 \le i \le k$, onda je

$L(x) = a_{i+1}$ i $D(x) = a_{i+1}$ (ako je $i = k$, onda $a_{k+1} = a_1$)

pa je $L(x) = D(x)$. Ako $x \notin \{f^{-1}(a_1), \dots, f^{-1}(a_k)\}$, onda je opet $L(x) = f(x) = D(x)$, jer $f(x) \notin \{a_1, \dots, a_k\}$. Dakle, važi (1'), a time i (1).

($\Rightarrow$): Pretpostavimo da su p i q konjugovane permutacije. Tada postoji $f \in S_n$, takvo da je $f^{-1} p f = q$. Neka je

$$p = (i_1^{(1)} \dots i_{k_1}^{(1)}) \dots (i_1^{(s)} \dots i_{k_s}^{(s)}) \tag{2}$$

proizvod disjunktnih ciklusa. Neposredno iz (1) sledi da je

$$f^{-1} p f = (f^{-1}(i_1^{(1)}) \dots f^{-1}(i_{k_1}^{(1)})) \dots (f^{-1}(i_1^{(s)}) \dots f^{-1}(i_{k_s}^{(s)})) = q.$$

Kako je rastav permutacije q na produkt disjunktnih ciklusa jedinstven do na raspored ciklusa, sledi da upravo bijekcija f uspostavlja traženu korespondenciju između ciklusa permutacije p i permutacije q.

($\Leftarrow$): Neka važi (2) i neka je

$$q = (j_1^{(1)} \dots j_{k_1}^{(1)}) \dots (j_1^{(s)} \dots j_{k_s}^{(s)})$$

produkt disjunktnih ciklusa. Ako postoji bijekcija između ciklusne dekompozicije permutacija p i q, onda je to preslikavanje $f: \{1, \dots, n\} \to \{1, \dots, n\}$, definisano sa

$$f(x) = \begin{cases} j_m^{(r)}, & \text{ako je } x = i_m^{(r)} \\ x, & \text{ako } x \notin \{ i_m^{(r)} \mid 1 \le r \le s, 1 \le m \le k_r \} \end{cases}$$

Neposredno se dokazuje da f zaista jeste bijekcija, tj. $f \in S_n$.

Da važi: $p = (f^{-1}(j_1^{(1)}) \dots f^{-1}(j_{k_1}^{(1)})) \dots (f^{-1}(j_1^{(s)}) \dots f^{-1}(j_{k_s}^{(s)}))$,

a je prema (1) $p = f^{-1} q f$, tj. p i q su konjugovane. QED

Primer: $n = 10$

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 1 & 10 & 6 & 2 & 3 & 9 & 8 & 4 \end{pmatrix}, \quad q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 8 & 1 & 9 & 7 & 2 & 10 & 6 & 4 & 5 \end{pmatrix}$$

$$p = (1\ 7\ 3)(2\ 5\ 6)(4\ 10)(8\ 9),$$

$$q = (1\ 3)(2\ 8\ 6)(4\ 9)(5\ 7\ 10) = (2\ 8\ 6)(5\ 7\ 10)(1\ 3)(4\ 9)$$

$$f^{-1} q f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 5 & 6 & 1 & 7 & 10 & 8 & 4 & 9 & 3 \end{pmatrix}$$

Provera:

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 1 & 10 & 8 & 2 & 3 & 5 & 7 & 9 & 6 \end{pmatrix}$$

$$qf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 1 & 10 & 6 & 2 & 3 & 9 & 8 & 4 \end{pmatrix} = p$$

Dakle, p i q su konjugovane.

Dokazati: $\boxed{G / Z(G) \cong \operatorname{Inn} G}$

Dokaz:

$$\varphi: G \to \operatorname{Aut} G, \quad \varphi(x) = \sigma_x, \quad \sigma_x(g) = x^{-1} g x \quad (g \in G)$$

$$(\varphi(x) \cdot \varphi(y))(g) = \varphi(y)(\varphi(x)(g)) = y^{-1} x^{-1} g x y = (xy)^{-1} g xy = \sigma_{xy}(g) = \varphi(xy)(g)$$

$$\Rightarrow \quad \varphi(xy) = \varphi(x) \cdot \varphi(y)$$

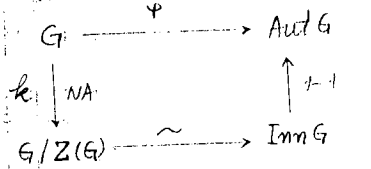
$\operatorname{Im}\varphi = \varphi(G) = \operatorname{Inn} G$

$x \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(x) = i_G \Leftrightarrow (\forall g \in G)\ \sigma_x(g) = g$ } $\operatorname{Ker}\varphi = Z(G)$

$\Leftrightarrow (\forall g \in G)\ x^{-1}gx = g \Leftrightarrow x \in Z(G)$ }

$G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$

$\Leftrightarrow G/Z(G) \cong \operatorname{Inn} G$ QED



---

19. Neka je G grupa u kojoj je preslikavanje $f(x) = x^{-1}$ unutrašnji automorfizam, tj. $f \in \operatorname{Inn} G$.

(1) Dokazati da su u grupi G svi elementi reda 2.

(2) Dokazati da ako je G konačna, onda je $|G| = 2^n$ za neko $n \in \mathbb{N}$.

Dokaz:

(1) Ako $f \in \operatorname{Inn} G$, onda postoji $y \in G$, takvo da za sve $x \in G$ važi $f(x) = y^{-1}xy$. Stavljajući $x = y$ dobijamo $f(y) = y$, pa kako je $f(y) = y^{-1}$, sledi $y = y^{-1}$, tj. $y^2 = 1$. Dalje, za $a, b \in G$ važi $aba^{-1}b^{-1} = ab\,f(a)\,f(b) = ab\,f(ab) = ab(ab)^{-1} = 1$, pa je G Abelova. Iz $y^{-1}xy = x^{-1}$ dobijamo $x = x^{-1}$, pa je $x^2 = 1$ za svako $x \in G$.

(2) Ako je $p \in \mathbb{P}rost$, $p > 2$ i $p \mid |G|$, onda, na osnovu Cauchy-jeve leme, postoji element $g \in G$ reda p, što je suprotno izvedenom iz (1). Dakle, red grupe G deljiv je samo dvojkama, pa postoji $n \in \mathbb{N}$, takav da je $|G| = 2^n$ QED

---

20. Neka je $G = \left\{ \begin{bmatrix} \pm 1 & a \\ 0 & 1 \end{bmatrix} \mid a \in \mathbb{Z}_n \right\}$ $(n \in \mathbb{N})$.

(a) Dokazati da je $(G, \cdot)$ grupa i naći njen red.

(b) Ako je $n = 3$, opisati G.

Rešenje:

(a) $\begin{bmatrix} \pm 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \pm 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \pm b + a \\ 0 & 1 \end{bmatrix} \in G$, $E \in G$ $\quad (a, b \in \mathbb{Z}_n)$

$\begin{bmatrix} \pm 1 & a \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} \pm 1 & \mp a \\ 0 & 1 \end{bmatrix} \in G \Rightarrow$ $(G, \cdot)$ je grupa

Neka je $A = \begin{bmatrix} \pm 1 & a \\ 0 & 1 \end{bmatrix} \in G$ $(a \in \mathbb{Z}_n)$, onda je $A^2 = E$, pa je $\text{red}(A) = 2$.
Neka je $A = \begin{bmatrix} +1 & a \\ 0 & 1 \end{bmatrix} \in G$, onda je $A^k = \begin{bmatrix} 1 & ka \\ 0 & 1 \end{bmatrix}$. Kako je
$\text{char}\,\mathbb{Z}_n = n$, sledi $A^n = 1$ i $\text{red}(A) = n$. Dakle, $2 \mid |G|$ i $n \mid |G|$,
pa je $G \supseteq \{E, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, \ldots, \begin{bmatrix} -1 & n-1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & n-1 \\ 0 & 1 \end{bmatrix}\} = S$.
No ako $A = \begin{bmatrix} \pm 1 & a \\ 0 & 1 \end{bmatrix} \in G$, onda $a \in \{0, 1, \ldots, n-1\}$, pa $A \in S$, te
je $G = S$. Prema tome, $|G| = 1 + n + n - 1 = 2n$.

(b) Za $n = 3$ je $|G| = 2 \cdot 3 = 6$, pa kako je G nekomutativna
$\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right)$ sledi $G \cong D_3$ $(\cong S_3)$, jer su
jedine dve grupe reda 6 grupa C_6 (komutativna) i D_3 $(\cong S_3)$.
Dakle, $G = \langle A, B ; A^3 = 1, B^2 = 1, AB = BA^2 \rangle$,
gde je $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$.

---

21. Neka je G konačna komutativna grupa neparnog reda. Dokazati da je sa $f(x) = x^2$ $(x \in G)$ definisan jedan automorfizam grupe G.

Dokaz:
$$f(xy) = (xy)^2 = xyxy = x^2y^2 = f(x)f(y) \quad (x, y \in G)$$
$$f(x) = f(y) \Rightarrow x^2 = y^2 \Rightarrow x^2y^{-2} = 1 \Rightarrow (xy^{-1})^2 = 1$$
G je neparnog reda pa nijedan element nije reda 2.
Otuda je $xy^{-1} = 1$, pa je $x = y$. Dakle, f je 1–1, a zbog
komutativnosti skupa G, f je i NA. Sledi $f \in \text{Aut}\, G$ QED

---

22. Dokazati: (a) $Z(A \times B) = Z(A) \times Z(B)$
(b) $(A \times B)' = A' \times B'$
(c) Ako su A i B konačne Abelove grupe uzajamno prostih redova, onda je: $\text{Aut}(A \times B) \cong \text{Aut}\, A \times \text{Aut}\, B$.

Dokaz:

(a) $(a, b) \in Z(A \times B) \Leftrightarrow (\forall (x, y) \in A \times B)\ (a, b)(x, y) = (x, y)(a, b)$
$\Leftrightarrow (\forall x \in A)(\forall y \in B)\ (ax, by) = (xa, yb)$
$\Leftrightarrow (\forall x \in A)(\forall y \in B)\ (ax = xa \wedge by = yb)$
$\Leftrightarrow a \in Z(A) \wedge b \in Z(B) \Leftrightarrow (a, b) \in Z(A) \times Z(B)$ 40

(b) $[(a_1,b_1);(a_2,b_2)] = (a_1,b_1)(a_2,b_2)(a_1,b_1)^{-1}(a_2,b_2)^{-1}$

$= (a_1 a_2 a_1^{-1} a_2^{-1}, b_1 b_2 b_1^{-1} b_2^{-1})$

$= ([a_1,a_2],[b_1,b_2])$.

(c) $|A| = m$, $|B| = n$, $(m,n) = 1$

1° A i B su ciklične : $A = C_m$, $B = C_n$

$Aut(A \times B) = Aut(C_m \times C_n) \cong Aut\, C_{mn} \overset{①}{\cong} (\Phi(mn), \cdot_{mn})$

$\cong (\Phi(m), \cdot_m) \times (\Phi(n), \cdot_n)$ ① Zad. 3

$\cong Aut\, C_m \times Aut\, C_n = Aut\, A \times Aut\, B$ (dalje ?)

---

23. Neka je A prsten karakteristike p, $p = mn$, $(m,n) = 1$, $I_m = \{x \in A \mid mx = 0\}$, $I_n = \{x \in A \mid nx = 0\}$. Dokazati:

$$\boxed{A \cong I_m \times I_n}$$

Dokaz: I_m i I_n su ideali, $I_m \cap I_n = \{0\}$

$x \in I_m \cap I_n \Rightarrow mx = 0 \wedge nx = 0$

$(\exists k, l \in \mathbb{Z})\ km + ln = 1$

$x = 1\,x = (km + ln)x = kmx + lnx = k \cdot 0 + l \cdot 0 = 0$

$\varphi : I_m \times I_n \longrightarrow A$, $\varphi(x,y) = x + y$ $(x \in I_m, y \in I_n)$ je izomorfizam

$\varphi((x,y) + (a,b)) = \varphi(x+a, y+b) = x + a + y + b = x + y + a + b$

$= \varphi(x,y) + \varphi(a,b)$ $(x, a \in I_m;\ y, b \in I_n)$

$\varphi(x,y) \cdot \varphi(a,b) = (x+y)(a+b) = xa + xb + ya + yb = xa + yb$

$= \varphi(xa, yb) = \varphi((x,y)(a,b))$

jer je: $xb \in I_m$, $xb \in I_n \Rightarrow xb = 0$ (I_m je ideal)

Analogno: $ya = 0$

$\varphi(x,y) = \varphi(a,b) \Rightarrow x + y = a + b$

$\Rightarrow n(x+y) = n(a+b)$

$\Rightarrow nx + ny = na + nb$

$\Rightarrow n(x-a) = 0$; $x - a \in I_m$, $x - a \in I_n$

$\Rightarrow x - a \in I_m \cap I_n = \{0\} \Rightarrow x = a$; Analogno: $y = b$

$(1-1)$

$a \in A$; $(\exists k,l \in Z)\ km + ln = 1$

$a = 1\cdot a = (km + ln)a = kma + lna$; $y = kma$, $x = lna$

$mx = mlna = lpa = 0 \Rightarrow x \in I_m$; $ny = 0 \Rightarrow y \in I_n$

$\Rightarrow a = x + y = \varphi(x,y)$, $(x,y) \in I_m \times I_n$ (NA)

$\Rightarrow$ φ je izomorfizam QED

---

24. Neka je A komutativan prsten sa jedinicom 1. Skup $S \subseteq A$ je multiplikativan skup ako važi:

$1^\circ\ 1 \in S$, $2^\circ\ a \in S \wedge b \in S \Rightarrow ab \in S$.

Neka je $\mathcal{F} = \{ I \subseteq A \mid I$ je ideal u A, $I \cap S = \emptyset \}$ familija uređena inkluzijom.

(a) Dokazati da familija $\mathcal{F}$ ima maksimalan element P.

(b) " da je P prost ideal

Dokaz:

(a) 1° $(0) \in \mathcal{F} \Rightarrow \mathcal{F} \neq \emptyset$

2° $\mathcal{L} \subseteq \mathcal{F}$ lanac (u odnosu na $\subseteq$) $\Rightarrow \bigcup \mathcal{L} \in \mathcal{F}$.

$\bigcup \mathcal{L}$ je ideal; $(\forall I \in \mathcal{L})\ I \cap S = \emptyset \Rightarrow \bigcup_{I \in \mathcal{L}} I \cap S = \emptyset$

$(\forall I \in \mathcal{L})\ I \subseteq \bigcup \mathcal{L}$

Svaki lanac neprazne uređene familije ima majorantu, pa prema Zorn-ovoj lemi postoji maksimalan element P fam. $\mathcal{F}$.

(b) $a \notin P \wedge b \notin P$; $I = (a) + P$, $J = (b) + P$

$P \subsetneq I$, $P \subsetneq J \Rightarrow I, J \notin \mathcal{F} \Rightarrow I \cap S \neq \emptyset$, $J \cap S \neq \emptyset$

$(\exists x, y \in S)\ x \in I, y \in J$; $xy \in S$ (1°)

$I \cdot J = ((0) + P)((b) + P) = (a)(b) + P = (ab) + P \ni xy$

$\Rightarrow I \cdot J = (ab) + P \notin \mathcal{F} \Rightarrow (ab) + P \neq P \Rightarrow ab \notin P$

$[(a \notin P \wedge b \notin P) \Rightarrow ab \notin P] \Leftrightarrow [ab \in P \Rightarrow (a \in P \vee b \in P)] \Leftrightarrow P$ je prost. QED

---

25. Neka je A prsten i $Z(A) = \{ a \in A \mid (\forall x \in A)\ ax = xa \}$ njegov centar. Dokazati: ako za sve $x \in A$, $x^2 - x \in Z(A)$, onda je A komutativan prsten.

Dokaz: $a, b \in A \setminus Z(A)$, $-a \in A \setminus Z(A)$

$a^2 - a \in Z(A)$, $(-a)^2 - (-a) = a^2 + a \in Z(A)$

$(a^2-a)b = b(a^2-a) \Leftrightarrow a^2b - ab = ba^2 - ba \Leftrightarrow ab - ba = a^2b - ba^2$

$(a^2+a)b = b(a^2+a) \Leftrightarrow a^2b + ab = ba^2 + ba \Leftrightarrow ab - ba = -(a^2b - ba^2)$

$\Rightarrow 2(ab - ba) = 0 \Rightarrow ab - ba = 0 \quad \vee \quad \operatorname{char} A \in \{1, 2\}$

$\Rightarrow ab = ba \quad \vee \quad A$ je polje (?) $\Rightarrow A$ je komutativan QED

---

26. Ako je G nekomutativna grupa, onda:

(a) $\operatorname{Aut} G$ nije ciklična; (b) $|\operatorname{Inn} G| \geq 4$.

Dokaz:

G je nekomutativna $\Rightarrow G/Z(G)$ nije ciklična

$G/Z(G) \cong \operatorname{Inn} G \Rightarrow \operatorname{Inn} G$ nije ciklična $\Rightarrow \operatorname{Aut} G$ nije ciklična (a)

(Sve podgrupe ciklične grupe su ciklične.)

SP: $|\operatorname{Inn} G| < 4 \Rightarrow |\operatorname{Inn} G| \in \{1, 2, 3\} \Rightarrow \operatorname{Inn} G$ je ciklična# $\Rightarrow$ QED

---

27. Dokazati da je u prstenu $R[x]$ svaki prost ideal istovremeno i maksimalan, tj. $\operatorname{Spec} R[x] = \operatorname{Specm} R[x]$.

Dokaz: Prsten $R[x]$ je glavnoidealski, pa ako je I prost ideal, onda je $I = (p)$, gde je $p \in R[x]$ nerastavljiv nad R. Neka je $a \notin (p)$. Tada $a + (p) \neq (p) = 0$, gde je 0 - nula oblasti celih $R[x]/(p)$ ($R[x]/(p)$ je oblast celih, jer je (p) prost ideal). Kako $p \nmid a$, sledi $(a, p) = 1$, pa prema Bezuovoj stavi postoje polinomi $m, n \in R[x]$, takvi da je $a(x)m(x) + p(x)n(x) = 1$.

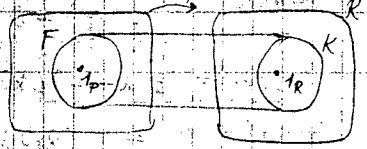
Tada je: $(a + (p))(m + (p)) = am + (p) = am + pn + (p)$

$= 1 + (p)$ (jer $pn \in (p)$), pa je $m + (p) = (a + (p))^{-1}$

Dakle, $R[x]/(p)$ je polje, pa je (p) maksimalan ideal, tj. $\operatorname{Spec} R[x] \subseteq \operatorname{Specm} R[x]$, pa kako važi i obrnuta inkluzija sledi $\operatorname{Spec} R[x] = \operatorname{Specm} R[x]$ QED

28. Neka su P i R prsteni sa 1, F podpolje prstena P koje ima istu jedinicu kao i prsten P i $f: P \to R$ homomorfizam takav da $f(1) = 1$. Dokazati da R sadrži podpolje izomorfno sa F.

Dokaz:



Neka je $K = f(F)$. Kako je F polje, ono je i komutativan prsten sa jedinicom, pa je to i K, jer komutativni prsteni sa 1 čine algebarski varijetet, pa su zatvoreni za homomorfizme. Neka je $y \in K^* = K \setminus \{0\}$. Tada postoji $x \in F^* = F \setminus \{0\}$ ($f(0) = 0$), takav da je $f(x) = y$. Kako je F polje, postoji $a \in F$, takav da je $ax = 1$. Tada je, za $b = f(a)$: $by = yb = 1$, pa je $b = y^{-1}$. Dakle, svi elementi iz K imaju inverz, pa je K polje. Svaki homomorfizam polja je istovremeno i monomorfizam, pa kako je f preslikavanje F na K, sledi: $K \cong F$. — QED

---

29. Dokazati da je $x^4 - 3$ nerastavljiv nad $\mathbb{Q}(i)$ i opisati grupu Galoa G tog polinoma nad $\mathbb{Q}(i)$.

Rešenje:

$$\begin{aligned}
x^4 - 3 &= (x^2 - \sqrt{3})(x^2 + \sqrt{3}) && (1)\\
&= (x - \sqrt[4]{3})(x + \sqrt[4]{3})(x - i\sqrt[4]{3})(x + i\sqrt[4]{3}) && (2)\\
&= x^4 + 2\sqrt{3}x^2 + 3 - 2\sqrt{3}x^2\\
&= (x^2 + \sqrt{3})^2 - (\sqrt{2}\sqrt[4]{3}\,x)^2\\
&= (x^2 - \sqrt{2}\sqrt[4]{3}\,x + \sqrt{3})(x^2 + \sqrt{2}\sqrt[4]{3}\,x + \sqrt{3}) && (3)\\
&= (x^2 - \sqrt{3})^2 + (\sqrt{2}\sqrt[4]{3}\,x)^2\\
&= (x^2 - i\sqrt{2}\sqrt[4]{3}\,x - \sqrt{3})(x^2 + i\sqrt{2}\sqrt[4]{3}\,x - \sqrt{3}) && (4)
\end{aligned}$$

Nijedna od mogućih faktorizacija (1) – (4) polinoma $f(x) = x^4 - 3$ nije nad $\mathbb{Q}(i)$, pa je on nerastavljiv nad $\mathbb{Q}(i)$.

Korensko polje polinoma f je $K_f = \mathbb{Q}(i)(\sqrt[4]{3}) = \mathbb{Q}(i, \sqrt[4]{3})$. Kako je f nerastavljiv nad $\mathbb{Q}(i)$ ($f(\sqrt[4]{3}) = 0$), sledi da je f minimalni polinom za $\sqrt[4]{3}$, pa je $|K_f : \mathbb{Q}(i)| = \operatorname{st} f = 4$.

Dakle, $|Gal(f)| = 4$, pa je $Gal(f) = \mathbb{C}_4$ ili $Gal(f) = \mathbb{C}_2^2 = V$.

---

30. Naći koreusko polje K_f polinoma $f(x) = 3x^3 - 4x^2 + 4x - 1 \in \mathbb{Q}[x]$.

Rešenje:

$$f(\tfrac{1}{3}) = 0$$

$$f(x) = 3(x - \tfrac{1}{3})(x^2 - x + 1) = 3(x - \tfrac{1}{3})\Big(x - \overbrace{\tfrac{1 + i\sqrt{3}}{2}}^{\alpha}\Big)\Big(x - \overbrace{\tfrac{1 - i\sqrt{3}}{2}}^{\beta}\Big)$$

$$K_f = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(i\sqrt{3})$$

$(\subseteq)$ $\alpha, \beta \in \mathbb{Q}(i\sqrt{3})$; $(\supseteq)$ $i\sqrt{3} = \alpha - \beta \in \mathbb{Q}(\alpha, \beta)$

$\Rightarrow K_f = \mathbb{Q}(i\sqrt{3})$

$g(x) = x^2 + 3$ je nerastavljiv nad $\mathbb{Q}$, $g(i\sqrt{3}) = 0$

$\Rightarrow g$ je minimalni polinom za $i\sqrt{3}$; $\operatorname{st} g = 2$

$\Rightarrow |K_f : \mathbb{Q}| = 2 \Rightarrow |Gal(K_f/\mathbb{Q})| = 2 \Rightarrow Gal(K_f/\mathbb{Q}) = \mathbb{C}_2$.

---

31. Ako u grupi G postoji element $x \in G$ koji ima tačno još jednog konjugata, onda G ima pravu normalnu podgrupu.

Dokaz: $conj(x) = \{x, y\}$ $(x \neq y)$, $H = \{1, x, y\}$, $conj(x) = conj(y)$

$(\forall g \in G)$ $g^{-1}xg \in conj(x)$, $g^{-1}yg \in conj(y) \Rightarrow H \lhd G$

$G = H \Rightarrow G = \mathbb{C}_3 = \{1, a, a^2\}$, $conj(a) \cap conj(a^2) = \emptyset$ #

$\Rightarrow H \neq G \Rightarrow H$ je prava normalna podgrupa QED

---

32. Opisati sve grupe reda $2p$ $(p \in Prost)$.

Rešenje:

$$\left.\begin{array}{l} P < G,\ |P| = 2,\ P = \langle a;\ a^2 = 1\rangle = \mathbb{C}_2 \\ Q < G,\ |Q| = p,\ Q = \langle b;\ b^p = 1\rangle = \mathbb{C}_p \end{array}\right\} \text{ I Sylow. t.}$$

$|G : Q| = 2p/p = 2 \Rightarrow Q \lhd G$

1° G je komutativna $\Rightarrow G = \mathbb{C}_{2p} \cong \mathbb{C}_2 \times \mathbb{C}_p$ $(za\ p > 2)$

$|G| = 2 \cdot 2 = 4 \Rightarrow G = \mathbb{C}_2^2$ v $G = \mathbb{C}_4$

2° G je nekomutativna

$b^a = a^{-1}ba \in Q = \{1, b, \ldots, b^{p-1}\}$, $b^a = b^i$ $(1 \leq i \leq p-1)$

$b^{a^2} = b^{i^2} \Rightarrow b^1 = b^{i^2} \Rightarrow i^2 = 1 \pmod p$

$\Rightarrow i \in \{1, p-1\}$

(i) $i=1 \Rightarrow a^{-1}ba = b \Rightarrow ab=ba \Rightarrow G$ je komutativna (v. 1°)

(ii) $i=p-1 \Rightarrow b^a = b^{p-1}$: $G = \langle a,b ; a^2=1, b^p=1, ba = ab^{p-1} \rangle$

$\Rightarrow G = D_p$

Za $p>2$ postoje tačno 2 neizomorfne grupe reda $2p$.

---

33. Neka je $A = \langle a_1, \dots, a_n \rangle$ Abelova grupa. Dokazati da je A homomorfna slika grupe $\mathbb{Z}^n$.

Dokaz:

$$A = \{ m_1a_1 + \dots + m_na_n \mid m_i \in \mathbb{Z},\ i=\overline{1,n} \}$$

$f : \mathbb{Z}^n \to A$, $f(m_1,\dots,m_n) = m_1a_1 + \dots + m_na_n$ $(m_i \in \mathbb{Z},\ i=\overline{1,n})$

$f(m_1+k_1,\dots,m_n+k_n) = (m_1+k_1)a_1 + \dots + (m_n+k_n)a_n$

$= (m_1a_1 + \dots + m_na_n) + (k_1a_1 + \dots + k_na_n)$

$= f(m_1,\dots,m_n) + f(k_1,\dots,k_n)$; f je NA QED

---

34. Neka je K Boole-ov prsten, tj. neka važi $x^2=x$ $(x \in K)$. Dokazati da je K komutativan prsten karakteristike 2.

Dokaz:

$$(x+x)^2 = x+x \Leftrightarrow x^2+2x^2+x^2 = x+x \Leftrightarrow 2x=0 \Rightarrow Char\,K = 2$$

$$\left.\begin{array}{l} (x+y)^2 = x+y \Leftrightarrow x^2+xy+yx+y^2 = x+y \Leftrightarrow xy = -yx \\ 2yx = 0 \Rightarrow yx = -yx \end{array}\right\} \Rightarrow xy = yx \quad \text{QED}$$

---

35. Jednačina $x^p - 1 = 0$ ima koren $\neq 1$ u $\mathbb{Z}_q$ akko $p \mid (q-1)$ $(p,q \in Prost)$

Dokaz:

$(\Rightarrow)$: $a^p = 1 \Rightarrow red(a) = p$ u grupi $(\mathbb{Z}_q \setminus \{0\}, \cdot, 1)$

$\Rightarrow p \mid (q-1)$ (Lagrange)

$(\Leftarrow)$ $p \mid (q-1) \overset{(Cauchy)}{\Rightarrow} (\exists a \in \mathbb{Z}_q \setminus \{0\})\ red(a) = p,\ a^p = 1$ QED

---

36. Neka je K oblast celih u kojoj su svi ideali glavni. Dokazati da je u K svaki prost nenula ideal maksimalan.

Dokaz:

Neka je $(x) \neq 0$ prost ideal u K i (y) ideal takav da $(x) \subset (y) \subseteq K$ $((y) \neq (x))$. Kako $x \in (y)$, postoji $u \in K$, tako da je $x = uy$. Ideal (x) je prost, pa $u \in (x)$ ili $y \in (x)$.

Kako je $(y) \neq (x)$, sledi $y \notin (x)$, pa $u \in (x)$. Zato postoji $v \in K$, takvo da je $u = xv$. Dakle, $x = xvy$, tj. $x(1-vy) = 0$. Kako je K oblast celih i $x \neq 0$, sledi $1 - vy = 0$, pa je $1 = vy \in (y)$ i otuda $(y) = K$. Dakle, (x) je max. QED

---

37. Neka je K polje i $p \in K[x]$. Dokazati da je ideal (p) maksimalan u $K[x]$ akko je p nesvodljiv nad K.

Dokaz:

($\Rightarrow$): Ako je (p) maksimalan ideal, onda je on i prost, pa je p nerastavljiv nad K.

($\Leftarrow$): $K[x]$ je oblast celih u kojoj su svi ideali glavni, pa ako je p nerastavljiv polinom nad K, onda je ideal (p) prost, te je na osnovu zad. 36 on i maksimalan. QED

Primer: Ideal (x^2+1) je maksimalan u $\mathbb{R}[x]$, a (x^2-2) u $\mathbb{Q}[x]$.

---

38. Opisati sve grupe reda 385 i dokazati da u svakoj od njih postoji element reda 77.

Dokaz:

Neka je G grupa, $|G| = 385$. Kako je $385 = 5 \cdot 7 \cdot 11$, postoje $P, Q, R < G$, redom S_5, S_7 i S_{11} – podgrupe grupe G. Kako je $s_7 = 1 \pmod 7$ i $s_7 \mid 385$, neposredno sledi $s_5 = 1$, pa je $Q \lhd G$. Na isti način: $s_{11} = 1 \pmod{11}$ i $s_{11} \mid 385$, povlači $s_{11} = 1$, pa je i $R \lhd G$.

Neka je $P = \langle a; a^5 = 1 \rangle \cong \mathbb{C}_5$, $Q = \langle b; b^7 = 1 \rangle \cong \mathbb{C}_7$ i $R = \langle c; c^{11} = 1 \rangle \cong \mathbb{C}_{11}$ (sve grupe prostog reda su ciklične). Posmatrajmo konjugovanje kao dejstvo podgrupe R na skup Q. Imamo $b^c = b^i$ za neko i, $1 \leq i \leq 6$ (jer je $Q \lhd G$), pa je $b^{c^{11}} = b^{i^{11}}$, tj. $i^{11} = 1 \pmod 7$. Neposredno se proverava da je jedino rešenje ove jednačine (tj. jednačine $x^{11} - 1 = 0$ u polju $\mathbb{Z}_7$) jednako 1. Dakle, $b^c = b$, pa je $bc = cb$.

Kako je, na osnovu prethodnog, $(bc)^k = b^k c^k$, sledi:

$red(bc) = NZS(red(b), red(c)) = NZS(7,11) = 77$

Dalje razlikujemo slučajeve:

A. $P \lhd G$: Kako je još $Q \lhd G$, $R \lhd G$, $P \cap Q = Q \cap R = R \cap P = \{1\}$,

$$|PQR| = \frac{|P|\,|QR|}{|P \cap QR|} = |P|\,|QR| = |P|\,\frac{|Q|\,|R|}{|Q \cap R|} = |P|\,|Q|\,|R| = 385 = |G|,$$

sledi $PQR = G$, pa je G unutrašnji, a time i spoljašnji direktni proizvod svojih podgrupa $P \cong C_5$, $Q \cong C_7$, $R \cong C_{11}$, tj.

$G \cong C_5 \times C_7 \times C_{11} \cong C_{385}$

B. $P \not\lhd G$: Kako je $Q \lhd G$, biće $b^a = b^i$, za neko $i \in \{1, \ldots, 6\}$.

Dalje je $b = b^1 = b^{a^5} = b^{i^5}$, pa je $i^5 = 1 \pmod 7$. Proverom sledi $i = 1$, pa je $b^a = b$, tj. $ba = ab$.

Analogno je $c^a = c^j$, za neko $j \in \{1, 2, \ldots, 10\}$, gde je $j^5 = 1 \pmod{11}$. Neposrednom proverom sledi $j \in \{1, 3, 4, 5, 9\}$ (za $j = 1$ dobija se da je G komutativna, što je obrnuto u A.)

Kako su $2, 3, 4, 5, 9$ rešenja iste jednačine $x^5 = 1$ u Z_{11}, sledi da su grupe $G_j = \langle a, b, c;\ a^5 = b^7 = c^{11} = 1,\ ab = ba,\ bc = cb,\ c^a = c^j \rangle$ za $j \in \{2, 3, 4, 5, 9\}$ međusobno izomorfne.

Kosime: Postoje 2 neizomorfne grupe reda 385: C_{385} i

$G = \langle a, b, c;\ a^5 = b^7 = c^{11} = 1,\ ab = ba,\ bc = cb,\ c^a = c^2 \rangle$.

---

33. Dokazati da grupa reda p^2q^2 $(p, q \in Prost)$ nije prosta.

Dokaz:

Neka je G grupa reda p^2q^2. Ako je $p = q$, sledi $|G| = p^4$. Kako za svaku grupu reda p^n, postoji podgrupa reda p^{n-1}, sledi da postoji $H < G$, $|H| = p^3$. Tada je $|G : H| = p$, pa je $H \lhd G$.

Neka je $p < q$ i neka je P S_p-, a Q S_q-podgrupa grupe G. Tada je $|P| = p^2$, $|Q| = q^2$. Kako je $s_q = 1 \pmod q$ i $s_q \mid p^2q^2$, sledi $s_q \mid p^2$, tj. $s_q \in \{1, p, p^2\}$.

Ako je $s_q = 1$, a kako su sve S_q-podgrupe grupe G konjugovane, sledi $Q \lhd G$. Ako je $s_q = p$, zbog $s_q = |G : N(Q)|$ $\frac{44}{}$

$N(Q) < G$, $p < q$, sledi $N(Q) \triangleleft G$. Ako $s_q = p^2$ (... kao u knjizi.)

40. Dokazati Prvu teoremu o izomorfizmu grupa: Ako je G grupa, $H \triangleleft G$, $F < G$, onda je $H \cap F \triangleleft F$ i

$$HF/H \cong F/(H \cap F) \qquad (*)$$

Dokaz:

$\sigma_x(H \cap F) = \sigma_x(H) \cap \sigma_x(F) = H \cap F$ za $x \in F \Rightarrow H \cap F \triangleleft F$

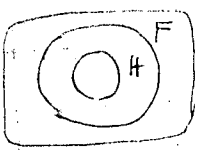
Neka je $k : G \to G/H$ kanonski homomorfizam i $k_1 = k|F$ (tj. $k_1 : F \to G/H$, $k_1(x) = k(x)$ za $x \in F$). Tada je:

$\operatorname{Ker} k_1 = \{x \in F \mid f(x) = H\} = \{x \in F \mid Hx = H\} = H \cap F$.

Dokazujemo da je $\operatorname{Im} k_1 = HF/H$. (1)

Zaista, ako je $y \in \operatorname{Im} k_1$, onda je $y = k_1(x) = Hx$ za neko $x \in F$, pa je $y \in HF/H$, jer je $Hx = Hhx$ ($h \in H$). Ako je $y \in HF/H$, onda je $y = Hhx$, za neko $h \in H$, $x \in F$, pa je $y = Hhx = Hx = k_1(x) \in \operatorname{Im} k_1$. Dakle, važi (1), pa je na osnovu Teoreme o razlaganju homomorfizma $F/\operatorname{Ker} k_1 \cong \operatorname{Im} k_1$, tj. važi (*).

QED



Druga teorema o izomorfizmu grupa:

Ako je G grupa, $H \triangleleft G$, $F \triangleleft G$, $H < F$, onda je $F/H \triangleleft G/H$ i

$$(G/H)/(F/H) \cong G/F$$

I Teorema o izomorfizmu prstena

Ako je $f : K \to A$ homomorfizam prstena K i A, onda je

$$K/\operatorname{Ker} f \cong \operatorname{Im} f.$$

II Teorema o izomorfizmu prstena

Ako je A prsten, $I, J \subseteq A$ ideali, onda je

$$(I+J)/J \cong I/(I \cap J)$$

III T o I P: Ako je A prsten, $J \subseteq I$ ideali u A, onda je I/J ideal u A/J i

$$(A/J)/(I/J) \cong A/I$$

41. Odrediti grupu Galoa G polinoma $f(x) = x^4 - 10x + 1$ nad $\mathbb{Q}$.

Rešenje:

$$f(x) = x^4 - 10x + 1 = x^4 - 10x + 25 - 24 = (x^2-5)^2 - (2\sqrt{6})^2$$
$$= (x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6})$$

Kako je $5 \pm 2\sqrt{6} = (\sqrt{2} \pm \sqrt{3})^2$, sledi

$$f(x) = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3}),$$

pa je korensko polje K_f polinoma f: $K_f = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dalje, $|G| = |K_f : \mathbb{Q}| = |K_f : \mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 4$. Neka je $\varphi \in G$, tj. $\varphi \in \mathrm{Aut}\, K_f$ i $\varphi \restriction \mathbb{Q} = 1_{\mathbb{Q}}$. Tada je

$$k = \varphi(k) = \varphi(\sqrt{k} \cdot \sqrt{k}) = \varphi(\sqrt{k})^2, \text{ za } k \in \{2, 3\},$$

pa je $\varphi(\sqrt{2}) = \pm\sqrt{2}$ i $\varphi(\sqrt{3}) = \pm\sqrt{3}$. Tako imamo $G = \{I, \varphi_1, \varphi_2, \varphi_1\varphi_2\}$, gde je I identičko preslikavanje polja K_f,

$$\varphi_1 = \begin{pmatrix} \sqrt{2} & \sqrt{3} \\ -\sqrt{2} & \sqrt{3} \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} \sqrt{2} & \sqrt{3} \\ \sqrt{2} & -\sqrt{3} \end{pmatrix}, \quad \varphi_1\varphi_2 = \varphi_2\varphi_1.$$

Dakle, $G \cong \mathbb{C}_2 \times \mathbb{C}_2 \cong V$
