SKRIPTA

iz

ALGEBRE III

SLAVIČA PREŠIĆ, MGD. 1962.

S. PREŠIĆ

I. UVODNI ZADACI. RELACIJE I OPERACIJE

Zadatak 1. Dokazati da jednačina

/1/ $$ax^{n+m} + bx^n + c = 0$$

gde su a, b i c tri cela neparna broja i gde su m i n prirodni brojevi, nema rešenja u skupu Ra racionalnih brojeva.

Rešenje. Predpostavimo obrnuto, odnosno da jednačina /1/ ima rešenje $x = p/q$ u skupu Ra. Neka su p i q relativno prosti. Smenom $x = p/q$ u jednačini /1/ ona postaje

/2/ $$ap^{n+m} + bp^n q^m + cq^{n+m} = 0$$

Izvršićemo redukciju svih brojeva u /2/ po modulu 2. Ako je l bilo koji ceo broj, onda sa l' označimo redukciju po modulu 2, odnosno $l' = 1'$ ako je l neparan i $l = 0'$ ako je l paran. Simboli 1' i 0' su reprezenti klase neparnih odnosno parnih brojeva. Sa njima su definisane operacije: $1' + 1' = 0'$, $1' + 0' = 0' + 1' = 1'$, $1' + 0' = 0' + 1' = 1'$, $1'.0' = 0'.1'; 0'.0' = 0'$ koje su u vezi sa poznatim osobinama parnih i neparnih brojeva.

Pošto je $(s+t)' = s' + t'$, $(st)' = s'.t'$ za proizvoljna dva cela broja s i t, to jednakost /2/ prelazi u

/3/ $$p' + p'q' + q' = 0'$$

Budući da su p i q relativno prosti za njih mogu nastupiti sledeći slučajevi

1/ $p' = 1'$, $q' = 1'$ 2/ $p' = 1'$, $q' = 0'$ 3/ $p' = 0'$, $q' = 1'$

Medjutim, /3/ nije ispunjena ni za jedan od tih slučajeva, tj. /3/ nije uopšte moguća.

Dakle, /1/ zaista nema racionalnih rešenja.

Primedba. Izvršiti generalizaciju jednačine /1/. Takodje posmatrati, umesto redukcije po modumu 2, redukciju po modulu k gde je k proizvoljan prirodan broj.

Zadatak 2. Neka je $P(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ polinom stepena n sa celim koeficijentima $a_0 = 0, a_1, \ldots, a_n$. Neka je m dat prirodan broj. Potreban i dovoljan uslov da $P(i)$, bude deljiv sa m za $i = 1, 2 \ldots, n+1, \ldots$ jeste da brojevi $P(1), P(2), \ldots, P(n)$ i $P(n+1)$ budu deljivi sa m. Dokazati.

Uputstvo. Poći od identiteta

$$P(x+n+1) = \binom{n+1}{1} P(x+n) + \binom{n+1}{2} P(x+n-1) - \binom{n+1}{3} P(x+n-2) \ldots \ldots (-1)^{n+1} P(x) = 0.$$

Đ. Baćvanat

i primeniti metod matematičke indukcije.

Zadatak 3. Dokazati relaciju

$$(A \cup B) \cap (A \cup C) \cap (B \cup C) = (A \cap B) \cup (A \cap C) \cup (B \cap C),$$

gde su A, B i C podskupovi istog skupa S.

Rešenje. Često je zgodnije operatore $\cup$ i $\cap$ označiti respektivno sa + i $\cdot$, jer nam je podesnije u tom slučaju da koristimo zakone koji ih vezuju i koji su slični sa zakonima sabiranja i množenja brojeva. Treba još naročito obratiti pažnju na zakone $A \cup (A \cap B) = A$ i $A \cap (A \cup B) = A$, odnosno $A + (A \cdot B) = A$ i $A \cdot (A + B) = A$ koji su podesniji za korišćenje.

• Smenom $\cup$ i $\cap$ respektivno sa + i $\cdot$, na osnovu izloženog imamo

$(A \cup B) \cap (A \cup C) \cap (B \cup C) = (A+B) \cdot (A+C) \cdot (B+C) = (A+AB+AC+BC) \cdot (B+C) = (A+BC) \cdot (B+C) = (AB+AC+BC) = (A \cap B) \cup (A \cap C) \cup (B \cap C)$, pa je navedena relacija dokazana.

Zadatak 5. Ako su A, B i C podskupovi istog skupa S proveriti dali važe relacije

1/ $(A \cup B) - C = (A - C) \cup (B - C)$

2/ $(A \cup B') \cap (C \cup A') \cap (B \cup C') = A \cap B \cap C$.

3/ $(X \triangle A) \cap (X \triangle B) \cap (X \triangle C) = (X \cap A' \cap B' \cap C') \cup (X' \cap A \cap B \cap C)$

4/ $(X \cup A) \cap (X \cup B) \cap (X \cup C) = X \cup (A \cap B \cap C)$

/$X \subset S$, $\triangle$ je znak za simetričnu razliku /.

Zadatak 6. Ako su $A_1, A_2, \ldots, A_n$ podskupovi skupa S onda važi identitet

• $A_1 \cup (A_1' \cap A_2) \cup (A_1' \cap A_2' \cap A_3) \cup \ldots \cup (A_1' \cap A_2' \cap \ldots \cap A_{n-1}' \cap A_n) = \bigcup_{i=1}^{n} A_i$

Rešenje. Označimo levu stranu sa L, znake $\cup$ i $\cap$ sa + i $\cdot$ (videti zadatak 3) i nadjimo L'.

$L' = A_1' (A_1 + A_2') (A_1 + A_2 + A_3') \ldots (A_1 + A_2 + \ldots + A_{n-1} A_n') = A_1' A_2' \ldots A_n'$ jer je $A \cdot A' = \emptyset = \emptyset A$. Pošto je $L = (L')'$, to je $L = (A_1' A_2' \ldots A_n')' = (A_1 + A_2 + \ldots + A_n) = A_1 \cup A_2 \cup \ldots \cup A_n$,

pa je gornji identitet dokazan.

Zadatak 7.Dokazati relacije

1/ $A \cap (BUC \cup D) = (A \cap B) \cup (A \cap C) \cup (A \cap D)$

2/ $A \cup (B \cap C \cap D) = (A \cup B) \cap (A \cup C) \cap (A \cup D)$

3/ $A \cup (A' \cap B) \cup (A' \cap B' \cap C) \cup (A' \cap B' \cap C' \cap D) \cup (A' \cap B' \cap C' \cap D') = \emptyset$

u kojima su A, B, C i D podskupovi istog skupa a sa ' je označen komplement.

Zadatak 8.Proveriti da li iz $A \cap B = A \cap C$ i $A \cup B = A \cup C$ sledi $B = C$.

Zadatak 9.Neka je S neprazan skup i neka je P(S) partitivan skup ovog skupa.Neka znaci + i · respektivno označuju operacije U i $\cap$ skupa P/S/.Poznajući $X_1, Y_1 \in P(S)$,naći X_n i Y_n u funkciji X_1 i Y_1 ako je

$$/1/ \qquad X_{n+1} = AX_n + BY_n$$

$$Y_{n+1} = BX_n + AY_n \qquad /n = 1, 2.../,$$

gde su A i B dva data elementa skupa P(S).

Rešenje 1.Problem se svodi na rešavanje skupovnog sistema diferaijalnih jednačina(1). Sistem /1/ se može podesnije napisati sa matricama čiji su elementi skupovi,odnosno elementi iz P(S).Tako je

$$/2/ \qquad M_{n+1} = \begin{pmatrix} A & B \\ B & A \end{pmatrix} M_n \text{ gde je } M_n = \begin{pmatrix} X_n \\ Y_n \end{pmatrix} \qquad /n = 1, 2.../$$

iz/2/ dobijamo

$$M_2 = \begin{pmatrix} A & B \\ B & A \end{pmatrix} M_1, M_3 = \begin{pmatrix} A & B \\ B & A \end{pmatrix}^2 M_1, \quad M_4 = \begin{pmatrix} A & B \\ B & A \end{pmatrix}^2 M_1, \ldots$$

i u opšte

$$/3/ \qquad M_{n+1} = \begin{pmatrix} A & B \\ B & A \end{pmatrix}^n M_1 \qquad /n = 1, 2.../$$

što se lako indukcijom dokazuje.

Prema tome problem se svodi na traženje n - tog stepena matrice $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$.Označimo $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$ sa K i podjimo od jednakosti

$$/4/ \qquad K = \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} + \begin{pmatrix} \emptyset & B \\ B & \emptyset \end{pmatrix}, \text{ gde } \emptyset \text{ označuje prazan skup.}$$

$$\begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix}\begin{pmatrix} \emptyset & B \\ B & \emptyset \end{pmatrix} = \begin{pmatrix} \emptyset & AB \\ AB & \emptyset \end{pmatrix} = \begin{pmatrix} \emptyset & B \\ B & \emptyset \end{pmatrix}\begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix}$$

Zbog ovoga, prema binomnom obrascu, iz /4/ dobijamo

$$/5/\quad K^n = \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix}^n \binom{n}{1} + \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix}^{n-1} \begin{pmatrix} \emptyset & B \\ B & \emptyset \end{pmatrix} \cdots \binom{n}{i} \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix}^{n-i} \begin{pmatrix} \emptyset & B \\ B & \emptyset \end{pmatrix}^{i} +,.$$

$$\cdots + \begin{pmatrix} \emptyset & B \\ B & \emptyset \end{pmatrix}^n = \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix}\begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} \cdots L = \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} L + \cdots + L^n \quad \left[L = \begin{pmatrix} \emptyset & B \\ B & O \end{pmatrix} \right],$$

jer je $\begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix}^k = \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix}$ /k proizvoljan priridan broj/.

Potencije matrice L su

$$L^2 = \begin{pmatrix} \emptyset & B \\ B & \emptyset \end{pmatrix}\begin{pmatrix} \emptyset & B \\ B & \emptyset \end{pmatrix} = \begin{pmatrix} B & \emptyset \\ \emptyset & B \end{pmatrix},\ L^3 = L,\ L = L^2, \ldots,$$

odnosno

$$L^n = \begin{cases} L^2, & \text{sko je } n \text{ paran} \\ L, & \text{ako je } n \text{ neparan.} \end{cases}$$

Zadnje tvrdjenje se lako dokazuje indukcijom.

Prema ovome /5/ postoje

$$K^2 = \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} + \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} L = L^2$$

$$K^n = \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} + \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} L + \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} L^2 + L^2$$

^{2} ,ako je $n < 2$ paran i

$K^n = \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} + \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} L + \begin{pmatrix} A & \emptyset \\ \emptyset & A \end{pmatrix} L^2 + L^2$, ako je $n > 2$ neparan.

Uvršćenjem L zadnje jednakosti daju

$$/6/\quad K^n = \begin{cases} \begin{pmatrix} A & B \\ B & A \end{pmatrix} & \text{ako je } n = 1,\ 3,\ 5,\ 7, \ldots \\ \begin{pmatrix} A & B \\ AB & \end{pmatrix}\begin{pmatrix} AB & \\ A & B \end{pmatrix} & \text{ako je } n = 2,\ 4,\ 6,\ 8, \ldots \end{cases}$$

Prema ovome jednakost /3/ daje

$$/7/\quad X_n = AX_1 + BY_1 \qquad X_n = (A+B)X_1 + ABY_1$$

$$Y_n = BX_1 + AY_1 \quad /n = 2,4,\ldots/ \qquad Y_n = ABX_1 + (A+B)Y_1 \quad /n = 1,3,\ldots/$$

Rešenje 2. Prema /1/ je

$$X_2 = AX_1 + BY_1, \quad X_3 = A(AX_1 + BY_1) + B(BX_1 + AY_1) = (A+B)X_1 + ABY_1$$

$$Y_2 = BX_1 + AY_1, \quad Y_3 = B(AX_1 + BY_1) + A(BX_1 + AY_1) = ABX_1 + (A+B)Y_1$$

$$X_4 = A\left[(A+B)X_1 + ABY_1\right] + B\left[ABX_1 + (A+B)Y_1\right] = AX_1 + BY_1$$

$$Y_4 = B\left[(A+B)X_1 + ABY_1\right] + A\left[ABX_1 + (A+B)Y_1\right] = BX_1 + AY_1$$

jer je $X + XY = X$ ($X, Y \in P(S)$); zakon apsorpcije.

Odavde možemo predpostaviti da vredi /7/. Matematičkom indukcijom se može lako opravdati ta predpostavka, odnosno izvesti /7/.

Zadatak 10. Rešiti sličan problem za sledeće sisteme diferencijalnih jednačina:

a/ $X_{n+1} = AX_n + BY_n$, $Y_{n+1} = CY_n$

b/ $X_{n+1} = AX_n + BY_n$, $Y_{n+1} = CX_n + DY_n$

c/ $X_{n+1} = AX_n + BY_n + C$, $Y_{n+1} = DX_n + EY_n + F$

a takodje i za diferencne jednačine:

d/ $X_{n+1} = AX_n + B$

e/ $X_{n+2} = AX_{n+1} + BX_n + C$

Zadatak 22. U skupu svih realnih nizova je uvedena binarna relacija s na sledeći način

$$(a_n)\ s\ (b_n) \Leftrightarrow a_n - b_n \to 0, \text{ kad } n \to \infty .$$

Ispitati relaciju

Rešenje. Pošto $a_n - a_n \to 0$, kad $n \to \infty$, navedena relacija je refleksivna. Ako je $(a_n)\ s\ (b_n)$, onda $a_n - b_n \to 0$ / $n \to \infty$/ , pa i $b_n - a_n \to 0$ / $n \to \infty$/ , tj, $(b_n)\ s\ (a_n)$. Stoga je s simetrična. Najzad ako je $(a_n)\ s\ (b_n)$, $(b_n)\ s(c_n)$, tada $a_n - b_n \to 0$, $b_n - c_n \to 0$ /$n \to \infty$/ pa $a_n - c_n = (a_n - b_n) + (b_n - c_n) \to 0$ kad $n \to \infty$. Znači s je i tranzitivna. Pošto je s refleksivna, simetrična i tranzitivna,

zaključujemo da je s relacija ekvivalencije.

Zadatak 23. Neka je s relacija ekvivalencije skupa S i neka je p permutacija skupa S. Dokazati da je relacija R definisana na sledeći način

$$x\ R\ y \Leftrightarrow xp\ s\ yp \quad / x,y,\ xp,\ yp \in S /,$$

jedna relacija ekvivalencije.

Rešenje. Pošto je xp s xp / $\forall$ xp $\in$ S/, to je x R x / $\forall$ x $\in$ S/ . Ako je x R y, onda xp s yp pa zbog simetrije relacije s je yp s xp, odnosno y R x. Slično, x R y i y R z daju x R z. Stoga je R zaista relacija ekvivalencije.

Zadatak 24. Ispitati relacije s date u navedenim skupovima

1. $x\ s\ y \Leftrightarrow x^2 - xy + y^2 = 1$ /x,y $\in$ R /;

2. $x\ s\ y \Leftrightarrow xp \mid yp$ /x,y prirodni brojevi, p data permutacija skupa prirodnih brojeva/

3. $x\ s\ y = m \mid (x-y)$ /x,y, m celi brojevi/

4. f /x/ s g/x/ $\Leftrightarrow \exists$ p/x/, f p/x/ = p g/x/ f /x/, g /x/ i p/x/ su elementi skupa svih permutacija skupa realnih brojeva.

5. (a,b) s (c,d) $\Leftrightarrow$ ad = bc /a, b, c,d celi brojevi b i d $\neq$ $\neq$ 0 /.

6. $x\ s\ y \Leftrightarrow x \overset{*}{+} y = y \overset{*}{+} x$ /x,y elementi semigrupe $(S, \overset{*}{+})$/

7. $x\ s\ y \Leftrightarrow x^2 \leq y^2$ /x,y $\in$ R /

Zadatak 25. U skupu R realnih brojeva je definisana relacija s na sledeći način

$$x\ s\ y \Leftrightarrow x > 1 \text{ i } y > 1.$$

Ispitati relaciju.

Rešenje. Relacija s nije refleksivna, odnosno nije x s x za svako x $\in$ R, jer na primer 1 non 1. Relacija s je simetrična i tranzitivna što se vidi iz sledećeg:

1/ $x\ s\ y \Rightarrow (x > 1 \text{ i } y > 1) \Rightarrow y\ s\ x$;

2/ $x\ s\ y,\ y\ s\ z \Rightarrow (x > 1 \text{ i } y > 1,\ y > 1 \text{ i } z > 1) \Rightarrow (x > 1 \text{ i } z > 1) \Rightarrow x\ s\ z.$

Dakle, s je simetrična i tranzitivna, a nije refleksivna.

Ovaj primer dokazuje nezavisnost aksiome refleksivnosti od aksioma simetričnosti i tranzitivnosti.

Primedba. Sličnu osobinu imaju i sledeće relacije:

1/ $x\ s\ y \Leftrightarrow \sqrt{x} = \sqrt{y}$ / $x, y \in R$/ ; 2/ $x\ s\ y \Leftrightarrow x = a, y = a$,

gde su x i y elementi skupa $\{a, b\}$.

Zadatak (26). U skupu $S = \{a, b, c\}$ je definisana relacija s na sledeći način. Element x je u relaciji sa elementom y, ako i samo ako je par (x,y) u skupu

$$B = \{(a, a), (a, b), (b, a), (b, b), (b, c), (c, b), (c, c)\}.$$

Ispitati relaciju.

Rešenje. Relacija s je refleksivna i simetrična. Medjutim je a s b, b s c, dok a non s c, pa s nije tranzitivna.

Navedeni primer dokazuje nezavisnost aksiome tranzitivnosti od aksioma refleksivnosti i simetričnosti.

Zadatak (27). U skupu binarnih relacija skupa S uočimo dve operacije U i $\cap$ definisane na sledeći način

$$x\ (s_1\ U\ s_2)\ y \Leftrightarrow x\ s_1\ y \text{ ili } x\ s_2\ y$$

$$x\ (s_1 \cap s_2)\ y \Leftrightarrow x\ s_1\ y \text{ i } x\ s_2\ y \quad /x, y \in S/.$$

Dokazati da su navedene operacije komutativne, asocijativne, distributivne jedna prema drugoj i svaka prema sebi samoj.

Rešenje. Izmedju binarnih relacija skupa S i podskupa S x S, prema definicije binarne relacije, postoji veza 1 - 1, odnosno binarnoj relaciji s odgovara jedan i samo jedan $Bs \in S \times S$ tako da je

$$x\ s\ y \Leftrightarrow (x, y) \in Bs$$

i skupu Bs jednoznačno odgovara relacija s. Dokazaćemo da ako je $s = s_1 U s_2$, da je onda i $Bs = Bs_1\ U\ Bs_2$. Zaista $s = s_1\ U\ s_2$ daje

$$x\ s\ y \Leftrightarrow x\ s_1\ y \text{ ili } x\ s_2\ y, \text{ tj}$$

$$(x,y) \in Bs \Leftrightarrow (x,y) \in Bs_1 \text{ ili } (x,y) \in Bs_2,$$

što znači $Bs = Bs_1\ U\ Bs_2$. Na sličan način dokazujemo da je

$$B_{s_1 \cap s_2} = B_{s_1} \cap B_{s_2}$$

Pošto je $(Bs_1 \cup Bs_2) \cup Bs_3 = Bs_1 \cup (Bs_2 \cup Bs_3)$ imamo, zbog $(Bs_1 \cup Bs_2) \cup Bs_3 = Bs_1 \cup s_2 \cup Bs_3 = B_{(s_1 \cup s_2) \cup s_3}$ i $Bs_1 \cup (Bs_2 \cup Bs_3) = Bs_1 \cup Bs_2 \cup s_3 = Bs_1 \cup (s_2 \cup s_3)$, da je $B_{(s_1 \cup s_2) \cup s_3} = B_{s_1 \cup (s_2 \cup s_3)}$, tj $(s_1 \cup s_2) \cup s_3 = s_1 \cup (s_2 \cup s_3)$, za tri proizvoljne binarne relacije s_1, s_2 i s_3 skupa S. Na taj način je dokazana asocijativnost operacije U. Na sličan način se dokazuje i ostala tvrdjenja.

Uopšte, za navedene U i $\cap$ važe potpuno analogni zakoni kao za skupovne operacije U i $\cap$.

Zadatak 28. Neka je S dat skup i neka je f funkcija koja preslikava S u S. Dokazati da je relacija s definisana na sledeći način:

$$x \; s \; y \Leftrightarrow f(x) = f(y) \qquad (x, y \in S),$$

relacija ekvivalencije.

Obrnuto, ako je s bilo koja relacija ekvivalencije skupa S, onda postoji funkcija $f : S \to S$ takva da

$$x \; s \; y \Leftrightarrow f(x) = f(y) \qquad (x, y \in S).$$

Dokazati.

Rešenje. Kako je $f(x) = f(x)$, to je $x \; s \; x \; (\forall x \in S)$. Iz $f(x) = f(y)$ sleduje $f(y) = f(x)$, pa $x \; s \; y$ povlači $y \; s \; x$. Iz $f(x) = f(y)$ i $f(y) = f(z)$ sleduje da je $f(x) = f(z)$, pa $x \; s \; y$ i $y \; s \; z$ povlači $x \; s \; z$. Pošto je s refleksivna, simetrična i tranzitivna to je s relacija ekvivalencije.

Neka je sada s bilo kakva relacija ekvivalencije. Pomoću s se skup S razlaže u klase ekvivalencije. U svakoj klasi ekvivalencije izaberimo po jedan elemenat i preslikavanjem f definišimo tako da svakom elementu jedne klase ekvivalencije odgovara izabrani elemenat te klase ekvivalencije. Ovo preslikavanje prema aksiomi izbora Zermelo - a, postoji. Preslikavanje f je preslikavanje skupa S u skup S. Činjenica $x \; s \; y$ je ekvivalentna činjenica $f(x) = f(y)$, pa je tvrdjenje u potpunosti dokazano.

Zadatak 35. U skupu $S = \{1, 2, 3, 4\}$ je definisana binarna relacija s na sledeći način.

$x \; s \; y \Leftrightarrow (x,y) \in \{(1,1), (2.2), (1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\} = Bs$. Ispitati da li je s tranzitivna relacija.

Rešenje.

$Bs \overset{*}{+} Bs = \{u \overset{*}{+} v \; ; \; u,v \in Bs\} = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4)\}$.

Kako je $Bs \overset{*}{+} Bs \leq Bs$ tj. $s \overset{*}{+} s \leq s$, tj. s jeste tranzitivna relacija.

Primedba. Pri formiranju $Bs \overset{*}{+} Bs$, množenje uredjenih parova u i v $\in Bs$, smo vršili po pravilu množenja parova /Brandtov proizvod/, odnosno $(\alpha, \beta) \overset{*}{+} (\beta, \gamma) = (\alpha, \gamma)$.

Zadatak 36. Ako su s i ζ tranzitivne relacije onda nemora biti tranzitivna relacija. Dokazati.

Zadatak 37. Označimo sa R/n/ broj relacija ekvivalencija koje se mogu definisati u skupu sa n elemenata.

Dokazati jednakost $R/n+1/ = \sum_{\nu=0}^{n} \binom{n}{\nu} R(\nu)$, $R/0/=1$, /1/

Rešenje. Broj R /n/ relacija ekvivalencija koje se mogu definisati u skupu sa n elemenata je jednak broju različitih razlaganja skupa na neprazne disjunktne podskupove čija je unija taj skup.

Za $n = 1$ skup $S = \{a_1\}$ ima samo jedno navedeno razlaganje, pa je $R/1/ = 1$. Za $n = 2$ skup $S = \{a_1, a_2\}$ ima razlaganja $\{a_1\}, \{a_2\}$ i $\{a_1, a_2\}$ pa je $R/2/ = 2$. Isti rezultat daje i /1/ za $n = 1$, pa je tvrdjenje tačno za $n = 1$. Predpostavimo da /1/ važi za 1,2,... n /indukcijska hipoteza/.

Ako je $S = \{a, a_1, a_2, \ldots a_n\}$ bilo koji skup sa n+1 - im elementom, onda navedenih razlaganja skupa S u kojima se u istom podskupu nalaze a i još ν $(0 \leq \nu \leq n)$ elementa iz S, prema indukcijskoj hipotezi ima $\binom{n}{\nu} R(n-\nu) = \binom{n}{n-\nu} R(n-\nu)$. Uzimajući $\nu = 0, 1, 2, \ldots$ n dobijamo sva različita razlaganja skupa S na nepoznate disjunktne podskupove čija je unija skup S.

Zbog ovog $R(n+1)=\sum_{\nu=0}^{n}\binom{n}{\nu}R(\nu)$ gde je $R/0/=1$, pa je /1/ u potpunosti dokazano.

Zadatak 38. Binarna relacija $\equiv \pmod m$ je relacija ekvivalencije. Šta su klase ekvivalencije ?

Rešenje. Pre svega po definiciji $a \equiv b \pmod m$ ako i samo ako $m \mid (a-b)$. Uvek je $a \equiv a \pmod m$, znači relacija je refleksivna.

Ako je $a \equiv b \pmod m$, onda je $m \mid (a-b)$ pa i $m \mid (b-a)$ tj. $b \equiv a \pmod m$. Znači iz $a \equiv b \pmod m$ sledi $b \equiv a \pmod m$, pa je relacija simetrična. Neka je $a \equiv b \pmod m$ i $b \equiv c \pmod m$. Tada je $m \mid (a-b)$ i $m \mid (b-c)$ pa i $m \mid (a-b)+(b-c)$ tj. $m \mid (a-c)$, odnosno $a \equiv c \pmod m$. Relacija je takva tranzitivna. Pošto je refleksivna, simetrična i tranzitivna, ona je relacija ekvivalencije.

Elementi skupa $S = \{0, 1, 2, \ldots, m-1\}$ su medjusobno nekongruentni po modulu m. Ma koji celi broj van toga skupa se može prikazati na jedan i samo jedan način u obliku $mq + r$, gde je $r \in S$, a q ceo broj, pa je kongruentan po modulu m broju r iz tog skupa. Klase ekvivalencija ćemo označiti sa $0', 1', \ldots (m-1)'$ one su

$$0' = \{0, \pm m, \pm 2m, \pm \ldots\}, \quad 1' = \{1, \pm m+1, \pm 2m+1, \pm \ldots\}$$
$$(m-1)' = \{m-1, \pm m(m-1), \pm 2m(m-1), \pm \ldots\}$$

Skup klasa ekvivalencija $0', 1', \ldots (m-1)'$ dogovoreno zovemo sistem ostataka po modulu m.

Ako je a elemenat klase ν', nju ćemo takodje označavati i sa a'. Činjenica $a' = b'$ znači ujedno i $a \equiv b \pmod m$.

Zadatak 39. Jedina relacija kongruencije u prstenu Z celih brojeva je $\equiv \pmod m$.

Rešenje. Pre svega $\equiv \pmod m$ je relacija kongruencije. Neka je $\sim$ bilo koja relacija ekvivalencije koja je kongruencija u prstenu Z celih brojeva. Sada znači, predpostavljamo da iz $a \sim b$ i $c \sim d$ sledi

$$a + c \sim b + d$$

$$a.c \sim b.d$$

Označimo sa S skup elemenata ~ 0. Razlikovaćemo dva slučaja:

I slučaj. Skup S ima samo jedan elemenat 0. Onda je $\sim$ obična jednakost ($\equiv \pmod 0$) jer iz $a \sim b$ i $(-b) \sim (-b)$ sledi

$a - b \sim 0$, tj. $a - b = 0$; $a = b$.

II slučaj. Skup S ima više od jednog elementa. Ako $1 \in S$ onda i $-1 \in S$ (pripada) S pa se u S nalazi bar jedan prirodan broj. Označimo sa m najmanji prirodan broj koji se nalazi u S. Ako je $s \in S$ bilo koji element onda se on može jedinstveno prikazati u obliku

$$s = mq + r$$

/q,r su celi brojevi, $0 \leq r < m$ /. Iz $s \sim 0$, $m \sim 0$, $- q \sim -q$ zaključujemo

$$s - mq = r \sim 0,$$

tj. $r = 0$. Znači da je

$$S = \{mq\}$$

gde je q ceo broj.

Ako je $m = 1$ onda je relacija $\sim$ takva da je $a \sim b$ za sve a i b. Ovu $\sim$ zovemo $\equiv \pmod 1$.

Ako je m veće od 1 onda iz $a \sim b$ i $(-b) \sim (-b)$ dobijamo $a - b \sim 0$, tj. $a - b = mq$, $a \equiv b \pmod m$ pa je $\sim$ ustvari $\equiv \pmod m$.

Zadatak 40. U proveravanju ispravnosti obavljenih osnovnih računskih radnji često se koristi tzv. devetična proba koja se u osnovi oslanja na činjenici da $a = b \pmod 9$, $c = d \pmod 9$ povlači $a+c \equiv b+d \pmod 9$ i $ac \equiv bd \pmod 9$. Podesnost metode je u tome što za zadane prirodne brojeve a i c brojeve b i d dobijamo sabirajući cifre za a, odnosno za c po modulu 9.

U slučaju kada se prirodni brojevi pišu ne u dekadnom sistemu već u sistemu čija je osnova prirodan broj a ($a > 1$), ispitati dali slična pravila kao za devetičnu probu vrede za probu po modulu $a - 1$.

Primedba. Ovo je jedan od problema profesora D. Markovića. Videti bliže u njegovom članku: nekoliko problema (Ves. društva mat. i fiz. NRS, VII, 1-2, 1955 g.).

Zadatak 41. Ako je p prost broj tada $p \mid ab$ povlači $p \mid a$ ili $p \mid b$.

Rešenje. Oznaka $m \mid n$ /m, n celi brojevi/ znači da se m sadrži u n. Korističemo teoremu: Ma kakva dva cela broja $a \neq 0, b \neq 0$ imaju najveći pozitivan zajednički delilac a,b. On se može prikazati kao linearna kombinacija brojeva a i b, odnosno postoje celi brojevi s i t takvi da je $(a,b) = sa + tb$. Predjimo sada na dokaz stava.

Ili je p/a ili p non/a.Ako je p/a onda je stav dokazan.Neka je p non/a.Tada je (p, a) = 1.Postoje celi brojevi s i t takvi da je 1 = sa +tp.Odavde,množeći sa b, dobijamo: b = sab+ tpb.Pošto je p/ab odavde sleduje zaključak p/b.Znači ili je p/a ili je p/b pa je stav dokazan.Važi i širi stav

Iz $c \mid ab$, $(a,c)= 1$ sleduje $c \mid b$.

42. Zadatak.Ako je s relativno prosto sa m, tada iz $sa \equiv cb \pmod m$ sleduje $a \equiv b \pmod m$, gde su a, b i c, b i c kao i $m > 1$ celi brojevi.

Rešenje.Iz $ca \equiv cb \pmod m$ sleduje da $m \mid (ca - cb)$,odnosno $m \mid c/a-b/$.Kako je $(c , m) = 1$ to $m \mid (a-b)$ pa je $a \equiv b \pmod m$).

Zadatak 43. Ako je $(c, m) =1$,tada jednačina $cx \equiv b \pmod m$ ima celo rešenje x. Ma kakva dva rešenja x_1 i x_2 su kongruentna po modulu m.

Rešenje.Kako $(c, m) = 1$, to postoje celi brojevi s i i takvi da je $1 = sc+ tm$. Množeći sa b imamo $b = sbc + tbm$ a ovde $(sb)c \equiv b \pmod m$ pa je jedno rešenje jednačine $x = sb$.

Neka su x_1 i x_2 rešenja. Tada $cx_1 \equiv b \pmod m$, $cx_2 \equiv b \pmod m$. Odavde $cx_1 \equiv cx_2 \pmod m$.Pošto $(c, m) = 1$ to je $x_1 \equiv x_2 \pmod m$ prema zadatku 42.

Zadatak 44.Dokazati da jednačina $30x^n = 91$ /n veće od 1,prirodan broj/ nema racionalnih rešenja.

Zadatak 45. Dokazati da ako $x^2 \equiv n \pmod{65}$ ima rešenja da i $x^2 \equiv -n \pmod{65}$ takodje ima rešenje.

Zadatak 46.Ispitati da li skup S uredjenih trojki racionalnih brojeva različitih od trojke (0, 0, 0) čini grupoid u odnosu na operaciju $\overset{*}{+}$:

$$(a, b, c) \overset{*}{+} (A, B, C) = (aA+bC+cB,\ aC+bB+cA,\ aB+bA+cC).$$

Rešenje.Prema pravilu operacije $\overset{*}{+}$ proizvod dve uredjene trojke je uredjena trojka.Treba još ispitati da li proizvod dve trojke $\neq (0, 0, 0)$ može biti (0, 0, 0).Ako se ovo desi onda $(S, \overset{*}{+})$ nije grupoid.

Uslov da $(a, b, c) \overset{*}{+} (A, B, C)$ bude (0, 0, 0)daje sistem

$$\begin{aligned} aA + bC + cB &= 0 \\ aC + bB + cA &= 0 \\ aB + bA + cC &= 0. \end{aligned}$$

Determinanta ovog sistema, shvaćenog kao sistem jednačina po a, b i c, je $\Delta = ABC - A^3 - B^3 - C^3$. Ova determinanta može biti jednaka 0 za $(A, B, C) \neq (0, 0, 0)$. Tako na primer, za $A = 1$, $B = -1$ i $C = 0$ je $\Delta = 0$. U ovom slučaju gornji sistem postaje

$$\begin{aligned} a - c &= 0 \\ c - b &= 0 \\ b - a &= 0 \end{aligned}$$

i biće zadovoljen, na primer, za $a=b=c=1$. Prema tome je

$$(1, 1, 1) \overset{*}{+} (1, -1, 0) = (0, 0, 0).$$

Dakle, $(S, \overset{*}{+})$ nije grupoid.

Zadatak 47. Dat je skup $S = \{ a+b\sqrt{3} \; ; \; a, b \in Ra, \; a^2+b^2 \neq 0 \}$. Ispitati da li je S grupoid u odnosu na operaciju množenja.

Zadatak 48. Dokazati da skup realnih brojeva R čini kvazigrupu u odnosu na operaciju:

$$x \overset{*}{+} y = x^3 + x + 3y \qquad /x, y \in R/.$$

Rešenje. Ako su $x, y \in R$ onda je $x^3 + x + 3y \in R$ pa je $(R, \overset{*}{+})$ grupoid. Treba još ispitati jednačine $a \overset{*}{+} x = b$, $y \overset{*}{+} a = b$ gde su a i b dati realni brojevi.

Jednačina $a \overset{*}{+} x = b$, tj $a^3 + a + 3x = b$ ima u skupu R jedinstveno rešenje $x = \frac{1}{3}(b - a - a^3)$.

Jednačina $y \overset{*}{+} a = b$, tj. $y^3 + y + 3a = b$ ima u skupu R jedinstveno rešenje jer je funkcija $\varphi(y) = y^3 + 3y$ permutacija skupa R / preslikava biunivoko R na R/.

Znači (R, +) jeste kvazigrupa.

Zadatak 49. Ispitati da li skup R_+ pozitivnih realnih brojeva čini lupu u odnosu na operaciju :

$$x \overset{*}{+} y = 2xy$$

Uputstvo. Treba proveriti da li je $(R_+, \overset{*}{+})$ kvazigrupa i da li $\overset{*}{+}$ ima jediničan element.

Zadatak 50. Ispitati da li su navedenim Cayle-evim tablicama definisane semigrupe

1.

	a	b
b	a	a
a	a	a

2.

	a	b
a	a	a
b	b	a

3.

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

4.

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

5.

	a_1	a_2	a_3	. . .	a_n
a_1	a_1	a_1	a_1	. . .	a_1
a_2	a_1	a_2	a_2	. . .	a_2
a_3	a_1	a_2	a_3	. . .	a_3
:	:	:	:	:	:
a_n	a_1	a_2	a_3	. . .	a_n

Zadatak 51. U skupu $S = \{a_1, a_2, \ldots a_n\}$ su definisane operacije

1/ $a_i * a_j = a_{max(i,j)}$ 2/ $a_i * a_j = a_{|i-j|}$

3. $a_i * a_j = a_i$ 4/ $a_i * a_j = a_{i+j+ij}$/sabiranje i množenje su po modulu n/.

Ispitati u svim slučajevaima da li je $(S, *)$ semigrupa.

Zadatak 54. Neka su $*$ i $\circ$ dve binarne operacije u S tako da je za operaciju $*$, operacija $\circ$ suprotna, tj. ako je $x \circ y = y * x$, $\forall x, y \in S$, pokazati tvrdjenja:

1. Ako je operacija $*$ kvazigrupna, onda je i operacija $\circ$ kvazigrupna;

2. Ako je operacija $*$ asocijativna, onda je i operacija $\circ$ asocijativna;

3. Ako operacija $*$ ima levi (desni) neutralni element, onda operacija $\circ$ ima desni (levi) neutralni element.

Rešenje

1/ Iz egzistencije jednostavnog x, odnosno y, iz jednačina: $x * a = b$ i $a * y = b$, sleduje i jedinstvenost x, odnosno y, i u jednačinama: $a \circ x = b$ i $y \circ a = b$, čime je pokazana kvazigrupnost operacije $\circ$.

2/ Kako je $(x * y) * z = z \circ (x * y) = z \circ (y \circ x)$

i $x * (y * z) = (y * z) \circ x = z \circ (y \circ x)$ to zbog jednakosti $(x * y) * z = x * (y * z)$ sleduje da je i $z \circ (y \circ x) = (z \circ y) \circ x$.

3/ Iz $x = e * x = x \circ e$ i $x = x * e'$ $e' = e \circ x$ direktno sleduje tvrdjenje.

Zadatak 55. Neka je u $S = \{a_1, a_2, a_3, \ldots, a_n\}$ definisana operacija Δ na sledeći način $a_i \Delta a_j = a_{\max(i,j)}$.

Pokazati da je opšti oblik komutativne operacije dat obrascem

$$a_i * a_j = f(a_i, a_j) \Delta f(a_j, a_i)$$

gde je f proizvoljna funkcija koja S^2 preslikava u S.

Rešenje. Kako je operacija Δ komutativna, jer je $\max(i,j) = \max(j,i)$ to je $a_i * a_j = f(a_i, a_j) \Delta f(a_j, a_i) \Delta f(a_j, a_i) \Delta f(a_i, a_j) = a_j * a_i$, što znači da je operacija komutativna.

Neka nam je za bilo koju komutativnu operaciju $*$ data multiplikativna tablica za skup S. Izaberimo za funkciju f onu funkciju za koju je prema tablici, $f(a_i, a_j) = a_i * a_j$. Tada je zbog dokazane komutativnosti operacije

$$f(a_i, a_j) \Delta f(a_j, a_i) = (a_i * a_j) \Delta (a_j * a_i) = (a_i * a_j) \Delta (a_i * a_j),$$

ili $f(a_i, a_j) \Delta f(a_j, a_i) = a_\nu \Delta a_\nu = a_{\max(\nu, \nu)} = a_\nu = a_i * a_j$ čime je pokazana proizvoljnost funkcije f.

Zadatak 56. Definišimo na skupu R realnih brojeva binarne operacije $\oplus$, $\odot$, + pomoću jednakosti: $a \oplus b = a + b + 1$, $a \odot b = a + b + ab$, $a * b = (a \oplus b) \oplus (a \odot b)$.

1. Ispitati komutativnost i asocijativnost navedenih operacija.

2. Ispitati levu i desnu distributivnost operacije $\odot$ prema $\oplus$, operacije $\oplus$ prema $\odot$ i $*$ prema $*$.

3. Da li je $(R, +, \cdot)$ izomorfno sa $(R, \oplus, \odot)$?

4. Ako je $z^n = z \odot z \odot \ldots \odot z$, $z^{(n)} = z * z * \ldots * z$ / u oba slučaja $n \neq 1$ faktora/, $z^{(-1)} = z^{-1} = z$ izvesti "binarne fomule" $(a \oplus b)^{(n)}$, $(a * b)^{(n)}$.

5. Rešiti jednačine $n^{(n)} = 0$, $x^{(n)} = 0$

6. Izraziti $\sum_{n=1}^{\infty} \frac{(x)^{(n)}}{n!}$, $\sum_{n=1}^{\infty} \frac{x^{(n)}}{n!}$

pomoću elementarnih funkcija.

7. Uvedimo "determinante" slično običnim determinantama

smenjujući u definiciji običnih determinanata + sa $\oplus$, sa $\odot$ i - inverznom operacijom operacije $\oplus$. Razviti :

$$\begin{matrix} 0 & a & a^{(2)} \\ 0 & b & b^{(2)} \\ 0 & c & c^{(2)} \end{matrix}$$

Zadatak 71. Ispitati da li se u svakom skupu S može definisati operacija $*$ takva da :

1/ $*$ bude asocijativna,

2/ $*$ ne bude asocijativna.

Rešenje. 1/ Operacija $a * b = a$ /a, b $\in$ S/ je asocijativna pa je odgovor na 1/ potvrdan.

2/ Ako S ima jedan i samo jedan element, onda $*$ ne postoji jer mora biti $a * a = a$ / a $\in$ S).

Ako S ima bar dva elementa a i b, onda je operacija $*$ definisana pomoću $a * a = a * b = b$, $b * a = b * b = a$, a za ostale parove / ako postoje/ ma kako je neasocijativna, jer :

$(a * a) * a \neq a * (a * a)$, (pošto $a * a) * a = b * a = a$, $a * (a * a) = a * b = b$.

Zadatak 72. Neka je $(S, *)$ data semigrupa sa jediničnim elementom e. Naći obrazac za dobijanje svih operacija o takvih da je

/1/ $a \circ (b * c) = (a \circ b) * c$ $\forall$ a, b, c $\in$ S .

Rešenje. Jednakost /1/ za b = e daje sledeću jednakost

/2/ $a \circ c = (a * e) * c$ $\forall$ a, c, $\in$ S.

Prema /2/ problem nalaženja operacije o se svodi na traženje $a \circ e = f/a/$. Sa ovom zadnjom oznakom prema /2/ imamo $a \circ b = f/a/ * b$. Smenom u /1/ imamo

$f/a/ * (b * c) = (f/a/ * b) * c$ $\forall a, b, c \in S$, što pretstavlja identitet, jer je $*$ asocijativna operacija. Dakle, f/a/ može biti proizvoljna funkcija, pa je traženi obrazac

$$a \circ b = f/a/ \circ b \qquad (f: S \to S).$$

Zadatak 73. Neka je na skupu $S = \{a, a, c, \ldots\}$ definisana jedna interna asocijativna operacija $*$. Neka za elemente a i b važe jednakosti:

/1/ $ab = ba$, $aba = a$, $bab = b$, $/a * b = ab /$.

Ako je c bilo koji element skupa S koji je komutativan sa elementom a /ac = ca/, dokazati da važe relacije:

1^{o}. $acb = bac$; 2^{o} . $bc = cb$.

Rešenje. Polazeći od /1/, dobijamo :

$bac = bca = bcaba = bca^2 b = ba^2 cb = abacb = acb$;

$cb = cbab = cabb = acbb = bacb = bbac = babc = bc$.

Ovim je tvrdjenje dokazano.

Zadatak 74. Neka su S i T dva neprazna skupa, takva da je $k/S/ \leq k/T/$. Neka je f jednoznačna funkcija koja preslikava skup T na skup S i neka je f^{-1} jedna inverzna funkcija ove funkcije. Neka je, dalje, u skupu S svuda definisana binarna operacija *. U skupu T definišemo operaciju $\triangle$ na sledeći način

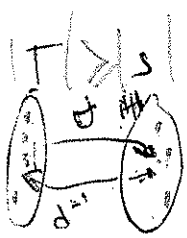
/1/ $x \triangle y = (f^{-1}(f/x/ * f/y/) \quad \forall /x, y \in T /$.

1^{o}. Ako je (S, *) semigrupa onda je i $(T, \triangle)$ semigrupa. Dokazati.

2^{o}. Ako (S, *) ispunjava zakon $(x * y) * (x * z) = y * z$ $/\forall x, y, z \in S)$ onda (T, $\triangle$) ispunjava zakon $(x \triangle y) \triangle (x \triangle z) = y \triangle z$ $/\forall x, y, z \in T /$. Dokazati.

3^{o}. Ako (S, *) poseduje jediničan element, onda $(T, \triangle)$ ne mora da ga poseduje.

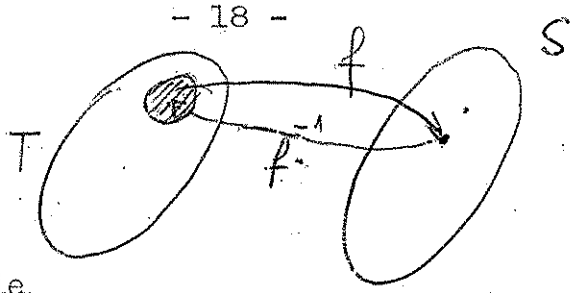
4^{o}. Neka je (S, *) sledeća semigrupa



*	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

i neka je T skup svih realnih brojeva. Izabrati jednu funkciju f, kao i njenu inverzmu f^{-1} koja ispunjava predpostavke zadatka, a zatim pomoću /1/ konstruisati operaciju.

Rešenje. U toku rešavanja od najbitnijeg značenja su činjenice da je $f\left[f^{-1}/x/\right] = x \quad /\forall x \in S /$ i $f^{-1}\left[f/x/\right]$ nije za svako $x \in T$ jednako sa x.



1°. Iz /1/ je

$(x \Delta y) \Delta z \quad f^{-1}(f/x/ * f/y/) \Delta z = f^{-1}\left(ff^{-1}(f/x/ * f/y/) * f/z/\right) =$

$f^{-1}(f/x/ * f/y/ * f/z/)$ i $x \Delta (y \Delta z) = x \Delta f^{-1}(f/y/ * f/z/)$

$f^{-1}\left[f/x/ * ff^{-1}(f/y/ * f/z/)\right] = f^{-1}(f/x/ * f/y/ * f/z/)$ pa

je $(x \Delta y) \Delta z = x \Delta (y \Delta z)$ / $\forall$ x, y, z $\in$ T /.

Na taj način je trvdjenje 1° dokazano.

2°. Slično kao za 1° imamo

$(x \Delta y) \Delta (x \Delta z) = f^{-1}(f/x/ * f/y/) \Delta f^{-1}(f/x/ * f/z/) =$

$f^{-1}\left[ff^{-1}(f/x/ * f/y/) * ff^{-1}(f/x/ * f/z/)\right] = f^{-1}\left[(f/x/ * f/y/) * (f/x/ * f/z/)\right] = f^{-1}(f/y/ * f/z/) = y \Delta z$ / $\forall$ x,y, z $\in$ T /, jer * ispunjava zakon

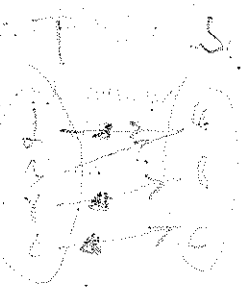
$$(x * y) * (x * z) = y * z \quad / \quad \forall\, x,y,z \in S/.$$

Tako je 2° dokazano.

3°. Za dokaz /3/ dovoljno je navesti primer. Tako, (S, *) i (T, Δ) dati tablicama

*	a	b	c
a	a	b	c
b	b	b	b
c	c	b	b

Δ	α	β	γ^2	δ
α	α	α	γ^2	δ
β	α	α	γ^2	δ^2
γ^2	γ^2	γ^2	γ^2	γ^2
δ	δ	δ	γ^2	γ^2



Ispunjavaju /1/, gde je $f(\alpha) = f(\beta) = a$, $f(\gamma) = b$, $f(\delta) = c$ i $f^{-1}/a/ = \alpha$, $f^{-1}/b/ = \gamma$, $f^{-1}/c/ = \gamma$

Dok (S, *) ima jedinični element a, grupoid (T, Δ) nema jedinični element.

4°. Funkcija f je odredjena izborom tri disjunktna neprazna

podskupa R_1, R_2, R_3 skupa R takvih da je $\bigcup_{i=1}^{3} R_i = R$ i definisanjem $f(R_1) = a$, $f(R_2) = b$ i $f(R_3) = c$. Inverzna funkcija je odredjena ako u R_1, R_2 i R_3 izaberemo respektivno elemente r_1, r_2 i r_3 i definišemo $f^{-1}(r_1) = a$, $f^{-1}(r_2) = b$ i $f^{-1}(r_3) = c$.

Prema ovome zaključujemo da problem ima više rešenja. Evo jednog od njih. Neka je $R_1 = \{x ; x \leq 1\}$, $r_1 \leq 1$; $R_2 = \{x ; 1 < x \leq 2\}$ $r_2 = 2$ i $R_3 = \{x ; x > 2\}$, $r_3 = 3$. Tada je obrascem /1/ odredjen-a operacija $\triangle$, čija se Cayleyeva tablica može ovako predočiti

$\triangle$	R_1	R_2	R_3
R_1	1	1	1
R_2	1	2	3
R_3	1	3	2

gde je, na primer, $4 \triangle 0 = 1$, $0 \triangle 0 = 1$, $2 \triangle 3 = 3$ itd.

Primedba. Načinom koji je izložen pod 4^0 se može u skupu realnih brojeva definisati po volji mnogo asocijativnih operacija.

Zadatak 75. Neka je $F(x,y,z)$ takva realna funkcija da jednakost $F(x,y,z)$ jednako 0 definiše z jednoznačno kao funkciju od x, i y.

Ako $F(x,y,z)$ ispunjava uslov /1/ $F(x,y,z) = F(y,z,x)$ $\forall x,y$, $z \in R$ pokazati da operacija $*$ /2/ $x * y = z \Leftrightarrow F(x,y,z) = 0$ ispunjava uslov /3/ $x = y * (x * y)$ $\forall x, y \in R$.

Navesti jedan primer takve funkcije F i operacije $*$.

Rešenje. Operacija $*$ definisana pomoću /2/ prema /1/ ispunjava zahtev $z = x * y \Rightarrow x = y * z$, $\forall x,y \in R$, tj. $x = y * (x * y)$, $\forall x, y \in R$, pa je /3/ dokazana.

Za $F(x,y,z) = x + y + z$ odgovarajuća operacija $*$ je $x * y = -x - y$ i ona ispunjava /3/.

Zadatak 76. Neka je $(S, \cdot)$ konačna semigrupa. Pokazati da u S mora postojati bar jedan idenpotentnat elemenat. Pokazati da ako

da ako (S, $\cdot$) nije konačna semigrupa takav element nemora da postoji.

Rešenje. Neka je S reda g i neka je a $\in$ S bilo koji element. Formirajmo skup

$$\sum = \left\{ a^{2^1}, a^{2^2}, a^{2^3}, a^{2^4}, \ldots, a^{2^g}, a^{2^{g+1}} \right\}$$

Skup $\sum$ je podskup skupa S. U $\sum$ moraju bar dva elementa biti jednaka inače S ima g + 1 elemenat. Neka $a^{2^\ell} = a^{2^s}$ /ℓ veće od s/

Ako je x bilo kakav prirodan broj onda množeći ovu jednakost sa a^x dobijamo :

$$a^{2^\ell + x} = a^{2^s + x} \qquad /x \geqslant 0 / \qquad /*/$$

Potražimo x iz uslova

$$2^\ell + x = 2\,(2^s + x)$$

Ovde je $x = 2^\ell - 2^{s+1}$. Za ovaj broj x jednakost /*/ postaje:

$$(a^{2^\ell - 2^s})^2 = (a^{2^\ell - 2^s})$$

Odavde sledi zaključak da je $a^{2^\ell - 2^s}$ idenpotentan.

Da bi smo dokazali drugi deo tvrdjenja navedimo jedan primer. Skup prirodnih brojeva u odnosu na sabiranje čini senigrupu bez idenpotentnog elementa,

Zadatak 77. Dokazati da je svaka senigrupa izomorfna nekoj senigrupi funkcija.

Rešenje. Razlikovaćemo dva slučaja, prema tome da li senigrupa (S,$*$) ima jedinicu ili ne. Akc (S,$*$) ima jedinicu e, svakom elementu a $\in$ S dodelimo funkciju f_a definisanu na sledeći način:

$xf_a = x * a$ / $\forall$ x $\in$ S/. Tada $f_a = f_b$ daje $x * a = x * b$ / $\forall$ x $\in$ S/, pa je $e * a = e * b$, tj. a = b. Znači, preslikavanje $a \to f_a$ je preslikavanje 1 - 1 skupa S na izvestan podskup $P = \{ f_a ; a \in S \}$ skupa svih funkcija koje S prevode u S.

Pošto je $xf_{a*b} = x * a * b = (xf_a) f_b \equiv xf_a \circ f_b / \forall x \in S /$, to je $f_{a*b} = f_a \circ f_b$, pa je (P, o) $\cong$ (S,$*$) gde smo sa o označili operaciju množenja funkcija. Na taj način je u ovom slučaju tvrdjenje dokazano.

Ako (S,$*$) nema jedinicu onda S proširujemo elementom $\exists \in$ S i u S $=$ S $\cup \{\}$ definišemo operaciju $\oplus$ na sledeći način

$$x \oplus y = x * y, \quad \text{ako } x \wedge y \in S$$
$$= x, \quad \text{ako } y = \xi$$
$$= y, \quad \text{ako } x = \xi$$

Sistem (S' , $\oplus$) je, takodje semigrupa što se može neposredno proveriti.U ovoj semigrupi je $\xi \in S'$ jediničan element.

Svakom elelemntu $a \in S$ dodelimo funkciju f_a definisanu na sledeći način $xf_a = x * a$ / $\forall x \in S'$/.Ovo preslikavanje /$a \to f_a$ / će opet realizovati traženi izomorfizam kao i u gornjem slučaju. Elelement ξ je dodat da bismo i u ovom slučaju imali preslikavanje 1 - 1, odnosno da $f_a = f_b$ povlači a = b.

Zadatak 80. Grupoid izotopan kvazigrupi je takodje kvazigrupa.Dokazati.

Rešenje.Neka su (G,$*$) i (K,o) grupoid i kvazigrupa koji su izotopni.Tada je

/$*$/ $\quad f(x * y) = \varphi(x) \circ \psi(y) \qquad /x,y \in G /,$

gde su f, φ i ψ tri funkcije koje biunivoko preslikavaju G na K. Ove funkcije imaju jedinstvene inverzne funkcije.Prema / $*$ / je

$$x * y = f^{-1}\left[\varphi(x) \circ \psi(y)\right]$$

Jednačina $x * a = b$ / $a,b \in G$ / tada glasi

$$f^{-1}\left[\varphi(x) \circ \psi(a)\right] = b$$

Odakle $\varphi(x) \circ \psi(a) = f(b)$. Pošto $\psi(a), f(b) \in K$ jednačina $\varphi(x) \circ \psi(a) = f(b)$ ima u K rešenje po $\varphi(x)$. Neka je to rešenje / koje je jedinstveno/ jednako c, tj. $\varphi(x) = c$.Iz $\varphi(x) = c$ imamo $x = \varphi^{-1}(c) \in G$. Dakle jednačina $x * a = b$ ima rešenje u G. Ovo je rešenje jedinstveno.

Slično ij jednačina $a * x = b$ / $a,b \in G$ / ima jedinstveno rešenje u G,pa je (G,$*$) zaista kvazigrupa.

Zadatak 81. Neka je (S,$*$) lupa.Neka u njoj važe uslovi

$(\exists a \in S)$ / $\forall x,y \in S$ / $\quad a * (x * y) = (a * x) * y,$

$(\exists b \in S)$ / $\forall x,y \in S$/ $\quad x * (b * y) = (x * b) * y,$

$(\exists c \in S)$ / $\forall x,y \in S$ / $\quad x * (y * c) = (x * y) * c.$

Tada kažemo da je a levi, b srednji i c desni asocijator lupe S. Sa A_ℓ, A_s i A_b označimo redom skup svih levih, skup svih srednjih, odnosno skup svih desnih asocijatora lupe. Dokazati da su $(A_\ell, *)$ $(A_s, *)$ i $(A_d, *)$ grupe.

Primedba A_ℓ, A_s i A_d postoje za bilo koju lupu, one uvek sadrže jedinični element $e \in S$.

Rešenje. Dokažimo prvo da je $(A_\ell, *)$ grupa. Neka $a, b \in A_\ell$. Tada

$a * (x * y) = (a * x) * y$ i $b * (x * y) = (b * x) * y$ / $\forall x,y \in S$/. Ako kod prve kod ovih jednakosti smenimo $x = b * X$ ona postaje

$$a * [(b * X) * y] = [a * (b * X)] * y$$

odakle, pošto su $a, b \in A_\ell$ imamo

$a * [b * (X * y)] = a * [(b * X) * y] \Rightarrow (a * b) * (X * y) = [a * (b * X)] * y \Rightarrow (a * b) * (X * y) = [(a * b) * X] * y$.

Zadnja jednakost daje $a * b \in A_\ell$ jer / $\forall x,y \in S$/ $\Rightarrow$ $\Rightarrow$ / $\forall x, y \in S$/. Znači $(A_\ell, *)$ je grupoid. Očigledno je $(A_\ell, *)$ i semigrupa. Dalje $e \in A_1$ jer je $(e * x) * y = e * (x * y)$ / $\forall x,y \in S$/. Neka je za $a \in A_\ell$ element a^{-1} desni inverzni. Ako stavimo $L = a^{-1} * * (x * y)$ / $x,y \in S$/, $D = (a^{-1} * x) * y$ / $x,y \in S$/, onda je $a * L = (a * a^{-1}) * (x * y) = (x * y)$, $a * D = [(a * a^{-1}) * x] * y = x * y$, tj. $a * L = a * D$, pa je $L = D$, odnosno $a^{-1} * (x * y) = (a^{-1} * x) * y$ / $x,y \in S$/. Dakle, $a \in A_\ell$ daje $a^{-1} \in A_\ell$ pa je $(A_\ell, *)$ zaista grupa.

Na sličan način se dokazuje da je $(A_d, *)$ grupa.

Kod dokaza da je $(A_s, *)$ grupa u delu dokazau kome se utvrdjuje da je $(A_s, *)$ semigrupa sa jediničnim elementom imamo slične momente koje smo izložili, pa taj deo i ne navodimo. Teškoća se javlja kada se dokazuje da $a \in A_s$ povlači $a^{-1} \in A_s$ gde je a^{-1} desni inverzan element za a.

Dokazaćemo prethodno da je a^{-1} i levi invezan element za a^{-}. Zaista, neka je $a * a^{-1} = e$, $a^{-1} * a = s$. Tada je

$a^{-1} = a^{-1} * e = a^{-1} * (a * a^{-1}) = (a^{-1} * a) * a^{-1} = \ell * a^{-1}$ jer je $a \in A_s$. Medjutim, iz $a^{-1} = \ell * a^{-1}$ zbog $a^{-1} = e * a^{-1}$ imamo $e * a^{-1} = \ell * a^{-1}$ odakle je $\ell = e$. Znači a^{-1} je levi inverzan element za a.

Ako podjemo od $L = x * (a^{-1} * y)$; $D = (x * a^{-1}) * y$ /x,y $\in$ S /

i smenimo $x = X * a, y = a * Y$ imamo zbog $a \in A_s$ da je $L = (X * a) * Y$, $D = [(X * a) * a^{-1}] * (a * Y) = X * (a * Y) = (X * a) * Y$, pa je $L = D$, tj. $x * (a^{-1} * y) = (x * a^{-1}) * y$ / $\forall$ x,y $\in$ S /. Znači, $a \in A_s$ daje $a^{-1} \in A_s$ pa je $(A_s, *)$ grupa.

Napomena. Videti članak G.N. Garrison-a Quasi-grups, /Ann. of Math., 41 /1940/, 474 - 487/.

Zadatak 82. Operacija * skupa S = {a.b.s} je asocijativna ako je ispunjen uslov $x * (y * z) = (x * y) * z$, / $\forall$ x,y,z $\in$ S /. Ovaj uslov se sastoji iz 27 jednakosti. Dokazati da se u skupu S ne može definisati operacija * tako da sve, sem jedne od tih jednakosti, budu ispunjene.

Primedba. Ako skup ima četiri ili više elemenata onda je operacija * moguće konstruisati tako da ispuni sve jednakosti asocijativnosti sem jedne. Drugim rečima, u ovom slučaju jednakosti asocijativnosti pretstavljaju nezavistan sistem aksioma.

Detaljnije o ovme videti u članku G. Szasz -a: Uber die Unabhangigket der Assoziativitatsbedingungen kommutativer multiplicativer Strukturen / Acta Sci. Math., Szeged, 15, 1954/.

Zadatak 83. Neka je * jedna binarna operacija definisana u skupu S sa n elemenata. Pokazati da je broj medjusobno različitih operacija u skupu S, izomorfnih operaciji * jednak $\frac{n!}{r(a)}$ gde je r/a/ broj elemenata grupe automorfizama grupoida (S, *).

Rešenje. Ako je o bilo koja izomorfna operacija operaciji * onda je:

1. $f(x \circ y) = f/x/ * f/y/$ / $\forall$ x,y $\in$ S/ gde je f izvesna permutacija skupa S. Iz /1/ imamo

/2/ $x \circ y = f^{-1}[f/x/ * f/y/]$, / $\forall$ x,y $\in$ S/

Jednakost /2/ služi kao obrazac za dobijanje svih izomorfnih operacija operaciji *. Za ovo je dovoljno u /2/ umesto f

uzimati redom elemente iz simetrične grupe S_n.

Medjutim, u opštem slučaju, obrazac /2/ ne mora dati n! različitih operacija, jer mogu dve funkcije f, g $\in S_n$ dati istu operaciju $o_f = o_g$.

Ispitajmo kada će ovo nastupiti. Ako ovo nastupi, onda:

3/ $f^{-1}\left[f/x/ \ast f/y/\right] = g^{-1}\left[g/x/ \ast g/y/\right]$ /$\forall$ x,y $\in$ S/ pa

$(gf^{-1})\left[f/x/ \ast f/y/\right] = g/x/ \ast g/y/$ /$\forall$ x,y $\in$ S/, odakle

4/ $(gf^{-1}).(x \ast y) = (gf^{-1})\ /x/ \ast (gf^{-1})\ /y/$ /$\forall$ x,y $\in$ S/.

Iz /4/ zaključujemo da $gf^{-1} \in A$, gde je A grupa automorfizama grupoida (S, $\ast$). Obrnuto, iz $gf^{-1} \in A$ sleduje /3/, tj. $o_f = o_g$. Ovo znači da ako S_n razložimo pomoću A : $S_n = A + Ab_2 + \ldots + Ab_k$, gde je $\frac{n!}{r(a)}$, da funkcije f i g će prema /2/ dati istu operaciju ako i samo ako i f i g budu u istom kosetu. Zbog ovoga je traženi broj jednak broju koseta, odnosno $\frac{n!}{r(a)}$ pa je tvrdjenje u potpunosti dokazano.

Primedba. Videti o ovome detaljnije u članku V. Devide -a /Glasnik mat.- fiz. i atron., Zagreb, Ser.II, T.7, 1952, st. 4-6/.

Zadatak 84. Neka je (G, o) grupa. Definišimo u njoj operaciju $\ast$ pomoću jednakosti : $a \ast b = a \circ b^{-1}$ /a, b $\in$ G /.

1/ Dokazati da je (G, $\ast$) kvazigrupa u kojoj je

$$(a \ast b) \ast (c \ast b) = a \ast c \quad /\forall\ a,b,c \in G\ /$$

2/ Neka je (G, $\ast$) bilo kakva kvazigrupa u kojoj je

$$(a \ast b) \ast (c \ast b) = a \ast c \quad /\forall\ a,b,c \in G\ /$$

Ispitati da li se pomoću $\ast$ i njenih inverznih operacija može u G definisati operacija o tako da je (G, o)grupa.

Rešenje. 1/ Neposredno koristeći definiciju grupe i osnovne osobine dokazuje se 1/.

2/ Pošto je (G, o) kvazigrupa, jednakošću $x \ast a = b$ /a,b $\in$ G/ je definisana svuda u G jedna binarna operacija o za koju je $a \circ b = x$. Ovo je jedna inverzna operacija operacije $\ast$. (G,o) je takodje kvazigrupa. Ova operacija je asocijativna što se zaključuje na sledeći način. Stavljajući $a \ast b = A$, $c \ast b = B$, $a \ast c = C$ jednakost $(a \ast b) \ast (c \ast b) = a \ast c$ daje $A \ast B = C$, $a \ast b = A$,

$c * b = B$, $a * c = C$ odakle prema definiciji operacije o dobijamo $A = B\ C$, $a = b \circ A$, $c\ b \circ B$, $a = c \circ C$. Eliminacijom, A, A, c dobijamo $C \circ (B \circ b) = (C \circ B) \circ b$ .Pošto $\forall\ a,b,c \in S \Rightarrow \forall\ b,\ B,\ C \in S$,asocijativnost operacije je dokazana.

Zadatak 85. Neka je S neprazan skup i neka su (S,i) / i 1, 2, 2, 3, 4/ četiri kvazigrupe,takve da je :

1/ $x1\ (y\ 2\ z) = (x\ 3\ y)4\ z$, $\forall x,y,z \in S$.

Dokazati da su kvazigrupe (S,i) izotopne sa istom grupom S, .

Rešenje. Neka je $a \in S$ jedan fiksiran element. Uvedimo sledeće funkcije:

2/ $L_i x = a_i x$, $D_i x = x\ i\ a$ /i = 1, 2,3,4/.

Pošto su (S,i) /i = 1,2,3,4/ kvazigrupe uvedene funkcije su permutacije /biunivoko preslikavanje S na S/.Prema /1/ za x = a, za y = a i za z = a imamo redom jednakosti

$L_1(y\ 2\ z) = (L_3 y)\ 4\ z$, $x\ 1 (L_2 z) = (L_3 x)4 x\ 1\ D_2 y = D_4(x\ 3\ y)$,

$\forall\ x,y,z \in S$. Iz ovih jednakosti imamo:

3/ $y\ 2\ z = L_1^{-1}\left[(L_3 y)4\ z\right]$, $x\ 1\ z = (D_3 x)4\ (L_2^{-1} z)$

$x\ 3\ y = D_4^{-1}\left[(D_3 x)4\ (L_2^{-1} D_2 y)\right]$ $\forall\ x,y,z \in S$ pa je dovoljno dokazati tvrdjenje jedino za S,4 . Koristeći /3/ jednakost /1/ daje

4/ $(D_3 x)4\left\{L_2^{-1} L_1^{-1}\left[(L_3 y)4\ z\right]\right\} = D_4^{-1}\left[(D_3 x)4 (L_2^{-1} D_2 y)\right]\ 4\ z$

$\forall x,y,z \in S$. Neka su dalje F, φ, ψ tri privremeno neodredjene permutacije skupa S. Uvedimo operaciju $*$ pomoću jednakosti

5/ $x\ 4\ y = F\left[(\varphi x) + (\psi y)\right]$

Uvodjenjem $*$ pomoću /5/ jednakost /4/ postaje

6/ $F\left\{D_3 x * \varphi L_2^{-1} L_1^{-1} F\left[(\varphi L_3 y) * (\psi z)\right]\right\} = F\left\{\psi D_4^{-1} F\left[(D_3 x) * (\psi L_2^{-1} D_2 y)\right] * (\psi z)\right\}$.

Permutacije F, φ i ψ ćemo potražiti iz uslova da /6/ bude jednačina asocijativnosti operacije $*$. Za ovo je dovoljno da F, φ, ψ ispune uslove

7/ $\varphi D_4^{-1} F = 1$, $\psi L_2^{-1} L_1^{-1} F = 1$, $\varphi L_3 = \psi L_2^{-1} D_2$,gde smo sa 1 označili identično preslikavanje.

Prema /1/ za $x = a$, $z = a$ dobijamo $L_1 D_2 = D_4 L_3$. Koristeći ovo za funkcije F, φ, ψ dovoljno je izabrati $\varphi = 1$, $F = D_4$, $\psi = L_3 D_2^{-1} L_2$.

Za ovako uzete permutacije F, φ i ψ je $(S, *)$ grupa. Jednakost /5/ dokazuje tvrdjenje za $(S, 4)$, pa je tvrdjenje u potpunosti dokazano.

II. G R U P A

Zadatak 1. Skup brojeva $S = \{1, i, -1, -i\}$ čini Abelovu grupu u odnosu na množenje.

Rešenje. Proizvod bilo koja dva elementa ovog skupa je opet element tog skupa. Asocijativni zakon je ispunjen jer važi za skup svih kompleksnih brojeva a ovo je podskup tog skupa pa važi i za njega. U ovom skupu postoji jedinični element. To je 1. Svaki element ima svoj inverzni : $1^{-1} = 1$, $(-1)^{-1} = -1$, $(-i)^{-1} = i$. Primećujemo još da je množenje komutativno. Stoga S čini Abelovu grupu.

Zadatak 3. Neka je $S = \{(a,b)\}$, /a, b su racionalni brojevi, $a \neq 0$/. U skupu S je definisana operacija $*$ pomoću

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

Dokazati da je $(S, *)$ grupa.

Rešenje. Ako su (a,b), (c,d) racionalni brojevi onda su takvi ac i $bc + c + d$; dalje je ac različito od 0 ako su a i c različiti od 0. Znači $*$ je unutrašnja operacija. Operacija $*$ je asocijativna jer je

$$[(a,b) * (c,d)] * (e,f) = (ac + c + d) * (e,f) =$$

$$= (ace,\ bce + ce + de + e + f)$$

$$(a,b) * [(c,d) * (e,f)] = (a,b) * (ce, de + e + f) =$$

$$= (ace,\ bce + ce + de + e + f).$$

Potražimo jednačini element. Ako je on (x,y) onda jednakost

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

daje jednostavno rešenje $x = 1, y = -1$. Znači $(1,-1) \in S$ je jedinični element.

Iz jednakosti

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

nalazimo da je inverzni element elemenata a,b sledeći

$$\left(\frac{1}{a} , - \frac{b+a+1}{a} \right)$$

Znači (S,) je zaista grupa.

Zadatak 4. Skup S funkcija $f_1/x/ = x$, $f_2/x/ = \frac{1}{1-x}$, $f_3/x/ = \frac{x-1}{x}$, $f_4/x/ = \frac{1}{x}$, $f_5/x/ = 1-x$ i $f_6 = \frac{x}{x-1}$ u odnosu na množenje " " funkcija definisano sa $f_\nu/x/ \circ f_\mu/x/ = f_\nu\left[f_\mu/x/\right]$ čini grupu.

Rešenje. Označimo $f_\nu/x/$ kratko sa f_ν. Multiplikativna tablica izgleda

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

Gde na primer

$$f_3 \circ f_4 = f_3\left[f_4/x/\right] = f_3\left[x^{-1}\right] = \frac{x^{-1} - 1}{x^{-1}} = 1 - x = f_5 ,$$

$$f_6 \circ f_6 = f_6\left[f_6/x/\right] = f_6\left[\frac{x}{x-1}\right] = x = f_1 .$$

Iz tablice vidimo da je S grupoid / tj. proizvod bilo koja dva elementa skupa S je element tog skupa /. Jedinični element je f_1. Svaki element skupa S ima inverzni element. Asocijativni zakon je ispunjen jer on važi kod navedenog proizvoda ma kakvih funkcija. Znači S zaista čini grupu.

Zadatak 5. Dokazati da skup realnih funkcija

$$S = \left\{ x,\ 2-x,\ \frac{2}{2-x},\ \frac{2x-2}{x-2},\ \frac{x-2}{x-1},\ \frac{x}{x-1},\ 2 - \frac{2}{x},\ \frac{2}{x} \right\}$$

čini grupu u odnosu na operaciju množenja funkcija.

Zadatak 6. Dokazati da skup racionalnih brojeva $S = \left\{ \frac{1 + 2m}{1 + 2n} \right\} / m, n = 0, \pm 1, \pm 2, \ldots$ čini grupu u odnosu na operaciju množenja.

Rešenje. Proizvod ma koja dva elementa ovog skupa

$$\frac{1 + 2m_1}{1 + 2n_1} \cdot \frac{1 + 2m_2}{1 + 2n_2} = \frac{1 + 2(m_1 + m_2 + 2m_1 m_2)}{1 + 2(n_1 + n_2 + 2n_1 n_2)}$$ je element ovog skupa. Asocijativni zakon je ispunjen. Element $\frac{1}{1} \pm \frac{2.0}{2.0} \in S$ je jedinični. Svaki element ima svoj inverzni. Tako je

$$\left(\frac{1 + 2m}{1 + 2n}\right)^{-1} = \frac{1 + 2n}{1 + 2m}$$. Znači, S je grupa.

Zadatak 7. U skupu S svih uredjenih parova (m,n) celih brojeva je definisana binarna relacija ρ na sledeći način

$$(m_1, n_1) \rho (m_2, n_2) \Leftrightarrow m_1 - n_1 + 2m_1 n_2 = m_2 - n_2 + 2n_1 m_2$$

1^0. Dokazati da je ρ relacija ekvivalencije.

2^0. Ispitati da li skup S/ρ čini grupu u odnosu na operaciju

$$(m_1, n_1) * (m_2, n_2) = (m_1 + m_2 + 2m_1 m_2,\ n_1 + n_2 + 2n_1 n_2)$$

Uputstvo. Videti prethodni zadatak.

Zadatak 23. Skup C svih elemenata grupe G koji su permutativni sa svim elementima grupe G čini normalnu podgrupu te grupe.

Primedba. Skup C se zove centar grupe G.

Rešenje. Ako su $a, b \in C$, onda je $ax = xa, bx = xb \ / \forall x \in G /$, pa je $abx = axb = xab \ / \forall x \in G /$. Znači, $a, b \in C \Rightarrow a, b \in C$. Pošto je $ex = xe \ / \forall x \in G /$, to je $e \in C$. Dalje, ako je $a \in C$, onda je $ax = xa \ / \forall x \in G /$, pa je odavde $xa^{-1} = a^{-1}x \ / \forall x \in G /$, tj. $a^{-1} \in C$.

Pošto je $x^{-1}Cx = Cx = Cx^{-1}x = C \ / \forall x \in G /$, to je C normalna grupa G.

Zadatak 24. Neka je $(G, \cdot)$ zadana grupa. Definišimo binarnu operaciju $*$ preko $a * b = b \cdot a \ / a, b \in G /$. Pokazati da je $(G, *)$ grupa.

Rešenje. Iz $a, b \in G$ sleduje $b.a = a*b \in G$ pa je $(G, *)$ grupoid. Kako je

$$(a * b) * c = (b \cdot a) * c = c \cdot (b \cdot a)$$
$$a * (b * c) = a * (c \cdot b) = (c \cdot b) \cdot a$$

to je $(G, *)$ semigrupa. Element e je jedinični jer je

$$a * e = e * a = a$$

Inverzan element elementu a je a^{-1} jer je

$$a^{-1} * a = a * a^{-1} = e,$$
$$a * a^{-1} = a^{-1} * a = e$$

Znači $(G, *)$ je zaista grupa.

Primedba. Grupe $(G, \cdot)$ i $(G, *)$ su izomorfne. Dokazati.

Zadatak 25. Ako su a, b i c elementi neke grupe, tada jednačina

$$x\ b\ x\ c\ a = x\ a\ b$$

ima jedinstveno rešenje. Dokazati.

Zadatak 26. Dokazati da se Abelova grupa S može definisati sledećim postulatima:

1/ Ako $a, b \in S$, onda $a.b \in S$

2/ $(a.b).c = (b.c).a$ za sve $a, b, c \in S$

3/ Postoji $e \in S$ takav da je za svaki $a \in S$ $ae = a$

4/ Svakom $a \in S$ odgovara $a^{-1} \in S$ takav da je $aa^{-1} = e$.

Ispitati nezavisnost postulata 4/ od postulata 1/, 2/ i 3/.

Zadatak 27. Konačna semigrupa u kojoj važi zakon kancelacije je grupa. Dokazati.

Zadatak 28. Semigrupa $S = \{a, b, \ldots\}$ u kojoj svaka od jednačina $ax = b, ya = b$ / $a, b \in S$ / ima bar jedno rešenje je grupa. Dokazati.

Zadatak 29. Neka je $(S, *)$ semigrupa sa kancelacijom. Neka svakom $x \in S$ odgovara najmanje jedan $x' \in S$ tako da je $x * x' * x = x$. Dokazati da je onda $(S, *)$ grupa.

Rešenje. Dokazaćemo, što je dovoljno, da u ovakvoj semigrupi jednačine oblika $a * x = b$ i $y * a = b$ imaju rešenja.

Zaista, jednačina $a * x = b$ ima rešenje $x = a' * b$ jer

$$x = a' * b \Rightarrow a * x = a * a' * b \Rightarrow a * x = b .$$

Koristili smo $a = a * a' * a$. Na sličan način zaključujemo da jednačina $y * a = b$ ima rešenje $y = b * a'$.

Primedba. Detaljnije o ovome videti u članku Sur une condition necessaire et suffisante pour qu'un semi - groupe soit

in grupe / C. R. Acad. Sc., t 232, 1951, strana 376/ od G.Thierrin-a.

Zadatak 30. Elementi a i $(s^{-1}as)$ grupe G imaju isti red.

Rešenje. Primetimo da važi jednakost $(s^{-1}as)^{\nu} = s^{-1}a^{\nu}s$ za ma koji par elemenata (a, s) iz grupe G i za svaki ceo broj ν. Koristeći nju imamo $(s^{-1}as)^{\omega(a)} = s^{-1}a^{\omega(a)}s = s^{-1}es = e$. Odavde $\omega(s^{-1}as) \leq \omega(a)$. Slično $a^{\omega(s^{-1}as)} = \left[s(s^{-1}as)s^{-1}\right]^{\omega(s^{-1}as)} = s(s^{-1}as)^{\omega(s^{-1}as)}s^{-1} = ses^{-1} = e$. Odavde $\omega(a) \leq \omega(s^{-1}as)$. Znači, $\omega(a) = \omega(s^{-1}as)$.

Zadatak 31. Neka su A i B elementi grupe G. Pokazati da je $(AB)^{-1} = B^{-1}A^{-1}$.

Rešenje. Da bismo pokazali da je $B^{-1}A^{-1}$ inverzni element za AB treba pokazati $(AB)(B^{-1}A^{-1}) = e$. Zaista, koristeći asocijativni zakon imamo : $(AB).(B^{-1}A^{-1}) = A\left[B(B^{-1}A^{-1})\right] = A\left[(BB^{-1})A^{-1}\right] = A\left[eA^{-1}\right] = AA^{-1} = e$. Specijalna posledica ovog stava je $(A^n)^{-1} = (A^{-1})^n$, gde je n proizvoljan prirodan broj.

Zadatak 32. Elementi a i a^{-1} grupe G imaju isti red.

Rešenje. $(a^{-1})^{\omega(a)} = \left[a^{\omega(a)}\right]^{-1} = e^{-1} = e$ prema zadatku 31. Odavde $\omega(a^{-1}) \leq \omega(a)$. Slično $a^{\omega(a^{-1})} = \left[(a^{-1})^{\omega(a^{-1})}\right]^{-1} = e^{-1} = e$. Znači $\omega(a) \leq \omega(a^{-1})$. Iz obe nejednakosti sledi $\omega(a) = \omega(a^{-1})$.

Zadatak 33. Elementi ab i ba grupe G imaju isti red.

Rešenje. Ovo je neposredna posledica zadatka 30 jer je $ab = b^{-1}(ba)b$.

Zadatak 34. Neka su A i B elementi grupe G. Ako je $B^{-1}AB = A^k$ onda je $B^{-r}A^sB^r = A^{s.k^r}$. Dokazati.

Rešenje. Za r = 1 tvrdjenje glasi $B^{-1}A^sB = A^{s.k}$ što je tačno jer je

$$A^{s.k} = (A^k)^s = (B^{-1}AB)^s = B^{-1}A^sB$$

Neka je

1/ $$B^{-r}A^sB^r = A^{s.k^r}$$

Pokažimo da je $$B^{-(r+1)}A^sB^{r+1} = A^{s.k^{r+1}}$$

Iz /1/ dobijamo:

$$B^{-(r+1)}{}_A s_B{}^{r+1} = B^{-1}{}_A s.k^r{}_B = (B^{-1}{}_{AB}) s.k^r = A s.k^{r+1}.$$

Prema principu totalne indukcije tvrdjenje je dokazano.

Zadatak 35. U grupi S_4 svih permutacija od četiri elementa 1, 2, 3, 4 naći sledeće podgupe:

a/ skup svih takvih ϕ da skup $\{1, 2\}$ primenom ϕ prelazi u $\{1, 2\}$.

b/ skup svih ϕ takvih da iz $a \equiv b \pmod 2$ sleduje $a\phi \equiv b\phi \pmod 2$ za sve a, b iz $\{1, 2, 3, 4\}$.

/Permutacija (13) (24) ima to svojstvo/.

Zadatak 36. Ako su H_1 i H_2 dve podgrupe grupe G tada je i $H_1 \cap H_2$ podgrupa grupe G.

Zadatak 37. Ako je konačan podskup S grupe G grupoid, onda je S grupa.

Rešenje. Neka $S = \{a_1, a_2, \ldots, a_k\}$ bude grupoid čiji elementi $a_1, a_2, \ldots, a_k$ pripadaju grupi $G = \{a_1, a_2, \ldots a_k, a_{k+1}, \ldots\}$ Obrazujemo šemu:

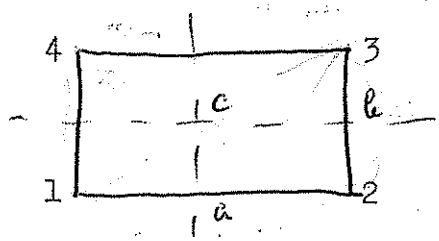
a_1	a_2	$\ldots$	a_k	:	S
a_1^2	a_1a_2	$\ldots$	a_1a_k	:	a_1S
a_2a_1	a_2^2	$\ldots$	a_2a_k	:	a_2S
$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$					
a_ia_1	a_ia_2	$\ldots$	a_ia_k	:	a_iS
$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$					
a_ka_1	a_ka_2	$\ldots$	a_k^2	:	a_kS

Pokazaćemo da u skupu S mora biti jedinični element i da svaki element ima inverzni u skupu S. To će biti dovoljno za dokaz da je S grupa. Skup $a_\mu S$ / $1 \leq \mu \leq k$/ ima k različitih elemenata, jer iz $a_\mu a_\alpha = a_\mu a_\beta$ sleduje $a_\alpha = a_\beta$ što nije tačno izuzev kada je $\alpha = \beta$. Pošto je S grupoid to $a_\mu S = S$. Uočimo u S element a_1. On mora biti jednak sa nekim elementom iz a_1S.

Neka je $a_1 = a_1 a_\alpha$. Odavde je $a_\alpha = e$; znači u S se nalazi jedinični element grupe G. Pokažimo još da svaki element iz S ima inverzni u S. Neka $a_\mu \in S$ ma koji element. Element e iz S mora biti jednak nekom elementu iz a_μ S. Neka je to $a_\mu a_\nu$. Znači $e = a_\mu a_\nu$ pa je $a_\mu = a_\nu^{-1}$ pa je gornji stav u potpunosti dokazan.

Zadatak 38. Naći grupu simetrija za a/pravougaonik; b/ kvadrat.

Rešenje. a/ definiciji simetrija geometriske figure je biunivoko preslikavanje tačaka te fugure na tačke te figure koje " čuva" udaljenje tačaka.



Neka su 1, 2, 3, 4 temena pravougaonika, C centar i neka su a i b prave kroz C koje su paralelne stranama 14 odnosno 12 pravougaonika. Pravougaonik ima sledeće simetrije:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1) \text{ ; identično preslikavanje,}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34) \text{; rotacija oko a za } \pi \text{ ,}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23) \text{; rotacija oko b za } \pi.$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24) \text{; rotacija oko C za } \pi.$$

Znači grupa simetrija pravougaonika je

$$G = \{(1), (12)(34), (13)(24), (14)(23)\}$$

b/ Na sličan način zaključujemo da je grupa simetrija kvadrata

$$G_1 = \{(1), (1234), (13)(24), (1432), (12)(34), (14)(23), (13)(24)\}$$

Zadatak 39. Naći grupe simetrija za a / romb, b/ ravnokraki trougao c/ ravnostrani trougao d/ pravilni petougao.

Zadatak 40. Grupa prostog reda je ciklična.

Rešenje. Grpa prostog reda ne može imati pravu podgrupu. Neka je $a \in G$ i $a \neq e$. Obrazujmo skup $S = \{a, a^2, a^3, \ldots, a^g\}$ gde je g red grupe. Elementi ovog skupa su različiti, jer ako je $a^\nu = a^\mu$ / $g \geq \nu > \mu$ / onda je $a^{\nu-\mu} = e$ pa je skup $\{a, a^2, \ldots, a^{\nu-\mu} = e\}$ prava podgrupa grupe G što je nemoguće. Pošto S ima g različitih elemenata grupe G to je $S = G$ pa je G ciklična grupa i a njen generator.

Zadatak 41. Ciklične grupe istog reda su izomorfne.

Rešenje. Neka su to grupe $G_1 = \{a, a^2, a^3, \ldots, a^g = e_1\}$ i $G_2 = \{b, b^2, b^3, \ldots, b^g = e_2\}$. Biunivoko preslikavanje ϕ, dato sa $a^\nu\phi = b^\nu$ je izomorfizam, jer $(a^\nu . a^\mu)\phi = a^{\nu+\mu}\phi = a^s\phi = b^s = b^{\nu+\mu} = b^\nu . b^\mu = (a^\nu\phi) . (a^\mu\phi)$, gde smo sa s označili element skupa $\{1, 2, \ldots, g\}$ koji je kongruentan sa $(\nu+\mu)$ po modulu g.

Dokaz je sličan i za ciklične grupe sa beskonačno elemenata.

Zadatak 42. Neka je $G = \{a, a^2, a^3, \ldots, a^g = e\}$ ciklična grupa reda g. Element a^p je generator te grupe tada i samo tada ako su p i g relativno prosti.

Rešenje. Neka su p i g relativno prosti. Pokažimo da je a^p generator. Svi elementi skupa $S = \{a^p, a^{2p}, \ldots, a^{gp} = e\}$ su medjusobno različiti jer ako je $a^{\nu p} \neq a^{\mu p}$ / $\nu < \mu$ / tada je $a^{(\nu-\mu)p} = e$, a odavde $g = (\nu-\mu)p$, što je nemoguće jer je $/g,p/ = 1$ a $\nu - \mu < g$. Dakle, $S = G$ pa je a^p zaista generator. Koristili smo činjenicu da ako je $a^\ell = e$ onda je $\omega(a) / \ell$. U gornjem slučaju $\omega(a)^\ell = g$, a $\ell = (\nu-\mu)p$.

Neka je sada a^p generator. Pokažimo da je $/p,g/ = 1$. U protivnom, ako je $/p,g/ = s \neq 1$ skup $\{a^p, a^{2p}, \ldots, a^{p\cdot\frac{g}{s}} = e\}$ je prava podgrupa grupe G pa a^p nije generator.

Zadatak 43. Dokazati da su podgrupe ciklične grupe takodje ciklične.

Zadatak 44. Dokazati da grupa reda p^m / p je prost broj/ mora imati podgrupu reda p.

Zadatak 45. Permutaciju $\begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}$ elemenata 1, 2, 3, i 4 označimo kratko sa abcd. U permutaciji abcd kažemo da su a i b, b i c, odnosno c i d dva susedna elementa. Neka je K skup svih permutacija elemenata 1, 2, 3 i 4 kod kojih su 1 i 2 susedni. Dokazati da K ne čini permutacionu grupu. Neka je H ⊂ K permutaciona grupa. Pokazati da se K može razložiti pomoću H na sličan način kao što se grupa razlaže po podgrupi.

Primedba. Navedeni problem je jedan deo problema koji je dao prof. D. Marković u članku : Napomene uz jedan elementarni problem iz permutacija / Ves. druš.mat. i fiz. NRS, IX, 1-2, 1957g./.

Zadatak 46. Ako $a \not\equiv 0 \pmod p$ i p prost broj onda je $a^{p-1} = 1 \pmod p$ ./Fermat/.

Rešenje. Drukčije rešeno, treba dokazati $(a^{p-1})' = 1'$. Zaista $(a^{p-1})' = (a')^{p-1}$, a element $a' \neq 0'$ pripada multiplikativnoj grupi $\{1', 2', 3', \ldots, (p-1)'\}$ pa mora $(a')^{p-1}$ biti $1'$. Znači $(a^{p-1})' = 1'$. Slično se dokazuje uopštenje ove teoreme koje glasi : ako /a,m/ = 1 onda je $a^{\varphi(m)} \equiv 1 \pmod m$ gde je $\varphi(m)$ Euler-ova funkcija koja je broj relativno prostih brojeva sa m skupa 0, 1, 2, ..., m -1. Tako je na primer, $\varphi(5) = 4$, $\varphi(6) = 2$, ...

Zadatak 47. U grupi G reda g svaki element ima red /periodu/ i on je činilac broja g.

Rešenje. Pod periodom elementa $a \in G$ smatramo najmanji pozitivan broj $\omega(a)$, takav da je $a^{\omega(a)} = e$. Ako je a = e, onda je $\omega(a) = 1$. Pošto je $1 \mid g$ to je u ovom slučaju tvrdjenje dokazano. Neka je $a \neq e$. Formirajmo skup $H = \{a, a^2, a^3, \ldots, a^g, a^{g+1}\}$. Svi elementi ovog skupa su elementi grupe G. Bar dva moraju biti ista jer inače bi G imala (g+1) član. Neka je $a^\nu = a^\mu$ / $\nu < \mu$ /. Tada je $a^{\nu-\mu} = e$. Pošto je $0 < \nu - \mu \leq g$ to u skupu $\{1, 2, 3, \ldots g\}$ postoji znači bar jedan element $\nu - \mu$ tako da je $a^{\nu-\mu} = e$. Ako je on jedini takav onda je $\omega(a) = \nu - \mu$, a ako ih ima više takvih u tom skupu onda je $\omega(a)$ po definiciji, najmanji od njih a takav sigurno postoji. Znači u svakom slučaju postoji $\omega(a)$.

Pokažimo da je $\omega(a) / g$. Skup $\{a, a^2, \ldots, a^{\omega(a)} = e\}$ je ciklična podgrupa grupe G pa prema Lagrange-ovoj teoremi $\omega(a) / g$ /tj. red podgrupe je činilac reda grupe/. Time dokaz završen.

Specijalno iz $\omega(a) / g$ sledi $a^g = e$ jer je $a^g = a^{\omega(a) \cdot \frac{g}{\omega(a)}} = \left[a^{\omega(a)}\right]^{\frac{g}{\omega(a)}} = e$.

Zadatak 48. U grupi G reda 7 rešiti jednačinu $x^3 = y^2$.

Uputstvo. Neka je a generatorni element grupe G. Ako stavimo $x = a^i$, $y = a^j$ /$0 \leq i, j \leq 6$/, onda se problem rešavanja gornje jednačine svodi na traženje i i j iz uslova $a^{3i} = a^{2j}$, odakle je $a^{3i-2j} = e$, odnosno $3i - 2j = 7k$ /k ceo broj/. Iz dobijene Diofantove jednačine treba tražiti i i j.

Zadatak 49. Neka su A i B dve podgrupe grupe G. Skup $A.B = \{a.b;\ a \in A,\ b \in B\}$ je grupa tada i sama ako je $AB = BA$.

Rešenje. Neka je prvo $AB = BA$. Tada se svaki element oblika b.a /$b \in B$, $a \in A$/ može napisati u obliku $a_1 b_1$ /$a_1 \in A, b_1 \in B$/ Koristeći ovu činjenicu i činjenicu da su A i B podgrupe grupe G lako proveravamo da skup elemenata $A \cdot B$ u odnosu na operaciju grupe G čini grupu. Neka drugo, skup $A \cdot B$ čini grupu u odnosu na operaciju grupe G. Tada $ae \in A \cdot B$, $eb \in A \cdot B \Rightarrow ebae = a_1 b_1 \in A.B$ tj. $ba \in AB$ za sve $b \in B$, $a \in A$, pa je $BA \subset AB$. Jednakost $(ab)^{-1} = a_1 b_1$ /$a, a_1 \in A$, $b, b_1 \in B$/ daje $ab = b_1^{-1} a_1^{-1}$ pa $ab \in BA$, tj. $AB \subset BA$. Iz $BA \subset AB$, $AB \subset BA$ zaključujemo $AB = BA$.

Zadatak 50. Dokazati da simetrična grupa S_n može biti generirana $n - 1$ - om transpozicijom

$$(12),\ (13),\ (14),\ \ldots,\ (1\ n\text{-}1)$$

Rešenje. Svaki element grupe S_n se može prikazati kao proizvod izvesnog broja transpozicija. Tako na primer /$1234\ldots n$/ $= (12).(13).(14)\ldots(1n)$. Tvrdjenje će dakle, biti dokazano ako pokažemo da se bilo koja transpozicija (ab) može izraziti preko navedenih transpozicija. To sledi iz

$$(ab) = (1b)^{-1}(1a)(1b), \quad (1b)^{-1} = (1b).$$

Zadatak 51. Pokazati da se simetrična grupa S_n / skup svih permutacija elemenata 1, 2,..., n/ može generisati pomoću permutacija: $P_1 = (1, 2, 3, \ldots, n\text{-}1)$, $P_2 = (n\text{-}1, n)$.

Rešenje. Svaka permutacija iz skupa S može se razložiti u proizvod dvočlanih ciklusa (a,b) / $1 \leq a \leq n$; $1 \leq n \leq n$ /, pa je dovoljno dokazati da se (a,b) može dobiti pomoću P_1 i P_2.

Primetimo da je $P_1^{-1} P_2 P_1 = (1,n)$, $P_1^{-2} P_2 P_1^2 = (2,n), \ldots,$

$P_1^{-k} P_2 P_1^k = (k,n)$; $/1 \leq k \leq n-1/$. Stoga je

$(a,b) = (n,a)^{-1}(n,b)(n,a) = (n,a)(n,b)(n,a) = P_1^{-a} P_2 P_1^a P_1^{-b} P_2 P_1^b P_1^{-a} P_2 P_1^a$.

Ovim je tvrdjenje dokazano.

Zadatak 52. U grupi parnog reda ima neparan broj elemenata čiji je red dva. Dokazati.

Zadatak 53. Data je Abelova grupa G. Ako je S skup svih elemenata grupe G konačnog reda onda je S podgrupa grupe G. Dokazati.

Rešenje. Pošto je grupa G Abelova to vredi jednakost $(ab)^n = a^n b^n$ / n proizvoljan ceo broj; $a,b \in G$ /. Koristeći ovu jednakost, zaključujemo da ako a i b imaju redove $\omega(a)$ i $\omega(b)$ respektivno da je onda

$$(ab)^{\omega(a)\omega(b)} = a^{\omega(a)\omega(b)} \cdot b^{\omega(a)\omega(b)} = e,$$

pa i ab ima sigurno konačan red, koji je izvestan delilac broja $\omega(a)\omega(b)$. Znači $a,b \in S \Rightarrow ab \in S$. Dalje, pošto $\omega(a) = \omega(a^{-1})$ zaključejemo da $a \in S \Rightarrow a^{-1} \in S$. Najzad je $e \in S$, pa je S zaista grupa.

Zadatak 54. Dokazati da se može desiti da grupa ima dva sistema nezavisnih generatora elemenata, tako da oba sistema imaju različit broj elemenata.

Rešenje. Dovoljno je navesti primer. Tako, ciklična grupa $C_6 = \{a, a^2, \ldots, a^6 = e\}$ može imati sledeće sisteme nezavisnih generatornih elemenata. Prvi sistem čini element a. Drugi sistem čine elementi $A = a^2$ i $B = a^3$. Zaista, ovo su nezavisni elementi i svaki element grupe se može dobiti pomoću njih :

$$a = A^2 B,\ a^2 = A,\ a^3 = B,\ a^4 = A^2,\ a^5 = AB,\ a^6 = A^3$$

Tvrdnjenje je dokazano jer jedan sistem ima 1 element, a drugi ima 2 elementa.

Primedba. Naći nekoliko sistema nezavisnih generatornih elemenata za grupu $(Z,+)$.

Zadatak 55 Binarna relacija ρ je u grupi G ovako definisana. Neka je H podgrupa grupe G onda je $a \rho b$ ako je i samo, ako je $ab^{-1} \in H$. Pokazati da je to relacija ekvivalencije i naći klase ekvivalencija.

Rešenje. Binarna relacija je relacija ekvivalencije ako je refleksivna, simetrična i tranzitivna. Primetimo prvo da je $aa^{-1} = e \in H$ tj. $a \rho a$, odnosno relacija je refleksivna. Neka je $a \rho b$ tj. $ab^{-1} \in H$, tada je $(ab^{-1})^{-1} = ba^{-1} \in H$ pa je $b \rho a$. Znači relacija je simetrična. Neka je $a \rho b$ i $b \rho c$; tada je $ab^{-1} \in H$, $bc^{-1} \in H$, a odavde $(ab^{-1}) \cdot (bc^{-1}) = ac^{-1} \in H$, pa je $a \rho c$ tj. relacija je tranzitivna. Dakle, relacija ρ je relacija ekvivalencije.

Ako je a bilo koji element iz G, onda je njegova klasa ekvivalencije C_a sledeći skup

$$C_a = \{x \mid a \rho x\} = \{x \mid xa^{-1} \in H\} = \{x \mid x \in Ha\} = Ha$$

tj. takozvani desni koset elementa a.

Zadatak 56 Naći centar grupe $G = \{e, A, A^2, A^3, B, AB, A^2B, A^3B\}$ $A^4 = e$, $A^2 = B^2$, $BA = A^3B$. $C = \{g \in G \mid (\forall a \in G)(ag = ga)\}$

Rešenje. Multiplikativna tablica ove grupe je

	e	A	A^2	A^3	B	AB	A^2B	A^3B
e	e	A	A^2	A^3	B	AB	A^2B	A^3B
A	A	A^2	A^3	e	AB	A^2B	A^3B	B
A^2	A^2	A^3	e	A	A^2B	A^3B	B	AB
A^3	A^3	e	A	A^2	A^3B	B	AB	A^2B
B	B	A^3B	A^2B	AB	A^2	A	e	A^3
AB	AB	B	A^3B	A^2B	A^3	A^2	A	e
A^2B	A^2B	AB	B	A^3B	e	A^3	A^2	A
A^3B	A^3B	A^2B	AB	B	A	e	A^3	A^2

jer je, na primer $(A^2B) \cdot (A^2B) = A^2(BA)(AB) = A^2A^3BAB = A(BA)B =$
$= AA^3BB = eB^2 = A^2$.

U centar C pre svega ulazi e. Ispitajmo da li je $A \in C$. Pošto $AB \neq BA$ to A ne pripada C jer nije komutativan sa B, takodje ni B ne pripada centru. $A^3 \notin C$ jer ako bi $A^3 \in C$ onda

bi i $A = (A^3)^3 \in C$ što nije. Element AB ne pripada centru jer na primer $(AB)\,A = B \neq A(AB)$. Slično A^3B ne prripada C jer $(A^3B)B = A \neq A^3 = B\,(A^3B)$ i $A^2B \in C$ jer $A\,(A^2B) = A^3B$ dok $(A^2B)A = AB$. Ispitajmo još da li $A^2 \in C$. Pošto je A^2 komutativan sa A i B to je komutativan sa svima elementima grupe G. Znači $C = \{e, A^2\}$.

Zadatak 57. Ako je element c grupe G reda m.n gde su m i n relativno prosti, tada se C može napisati na jedan i samo jedan način kao proizvod dva komutativna elementa reda m i n respektivno.

Rešenje. Pošto su m i n relativno prosti to postoje celi brojevi x i y takvi da je $mx + ny = 1$. Dalje, $C = C^{mx + ny}$ C^{ny}. $C^{mx} = M.N$, gde smo sa M označili element C^{ny} i sa N element C^{mx}. Ovi elementi su komutativni. Pokažimo da su reda m i n. Kako je $M^m = (C^{ny})^m = (C^{mn})^y = e^y = e$ to je $\omega(M) \leq m$. Pretpostavimo $\omega(M) < m$. Tada $e = M^{\omega(M)} = (C^{ny})^{\omega(M)} = (C^{yn})^{\omega(M)}$. Odavde pošto C ima periodu mn je $mn \mid yn\omega(M)$ tj. $m \mid y\omega(M)$ što je nemoguće, jer prema jednakosti $mx + ny = 1$ su y i n relativno prosti, a još i $\omega(M) < m$, po pretpostavci. Dakle, $\omega(M) = m$. Na sličan način možemo zaključiti $\omega(N) = n$. Dokazati smo da se pod navedenim uslovima mogu naći M i N koji su komutativni, reda m i n i takvi da je $C = MN$. Pokažimo da je ovakvo rastavljanje jedinstveno. Neka je $C = M_1N_1$ gde su M_1 i N_1 komutativni i reda m i n. Tada $M \cdot N = M_1 \cdot N_1$. Stepenujemo obe strane sa ny. Zbog komutativnosti i $N^n = N_1^n = e$ dobijamo $M^{ny} = M_1^{ny}$. Kako se prema jednačini $mx + ny = 1$ dobija $ny = 1 - mx$, to je $M^{1-mx} = M_1^{1-mx}$ odakle je $M(M^m)^{-x} = M_1 \cdot (M_1^m)^{-x}$, tj. $M = M_1$. Iz jednakosti $MN = M_1N_1$ dobijamo najzad i $N_1 = N$ pa je tvrdjenje u potpunosti dokazano.

Zadatak 58. Neka je G Abelova grupa konačnog reda čiji elementi $a_1, a_2, \ldots, a_g$ imaju redom periode $\alpha_1, \alpha_2, \ldots, \alpha_g$. Tada:

1. Svaki element grupe G se može na isti broj načina pretstaviti u obliku: (+) $a_1^{\beta_1} a_2^{\beta_2} \ldots a_g^{\beta_g}$ $\beta_i = 0, 1, \ldots, \alpha_i - 1$/

2. Ako je k broj pretstavljanja jediničnog elementa $e \in G$, tada je $\alpha_1\alpha_2 \ldots \alpha_g = kg$

3/ Ako je p prost broj koji se sadrži u g, tada postoji u G bar jedan element periode p.

Rešenje. 1/ Svaki element a_i pripada G se može bar na jedan način prikazati u obliku (*), jer je $a_i = a_1^0 a_2^0 \dots a_{i-1}^0 a_i^0 a_{i+1}^0 \dots a_g^0$. Označimo sa k broj načina pretstavljanja jediničnog elementa $e \in G$ u obliku (*). Neka je $a_{-i} \neq e$ bilo koji izabrani element iz G. Neka je ℓ_i broj načina pretstavljanja ovog elementa u obliku (*).

Množeći svako pretstavljanje (*) elementa e sa a_i dobijamo k različitih pretstavljanja za a_i. Stoga $\ell_i \geq k$. S druge strane, množeći svako pretstavljanje (*) elementa a_i sa $a_i^{\alpha_{i-1}}$ dobijamo ℓ_i različitih pretstavljanja elementa e. Zbog ovog $k \geq \ell_i$. Znači $\ell_i = k$ pa je tvrdjenje pod jedan dokazano.

2/ Svih formi (*) ima $\alpha_1, \alpha_2, \dots, \alpha_g$, a sa druge strane ih ima kg, pa sledi $\alpha_1 \alpha_2 \dots \alpha_g = kg$.

3/ $p \mid g \Rightarrow p \mid \alpha_1 \alpha_2 \dots \alpha_g \Rightarrow p \mid \alpha_i$ za neko i, pa $\alpha_i = ph$ gde je h izvestan prirodan broj. Element a_i^h je element reda p pa je tvrdjenje pod tri dokazano.

Zadatak 59. Neka je G grupa i neka je ρ binarna relacija u njoj definisana na sledeći način:

$$x \rho y \iff \exists\, s \in G, \quad y = s^{-1} x s$$

1/ Dokazati da je ρ relacija ekvivalencije.

2/ Ako je G grupa konačnog reda, onda je broj elemenata svake klase ekvivalencije delilac reda grupe. Dokazati.

3/ Ako je $x \rho y$, onda je $\omega(x) = \omega(y)$

4/ Naći G/ρ ako je G simetrična grupa S_4

Rešenje. 1/ Za $s = e$ je $x = e^{-1} x e$ /$x \in G$/, pa je $x \rho x$ za svako $x \in G$.

Ako je $y = s^{-1} x s$ /$s \in G$/, onda je $x = s y s^{-1}$, tj. $x \rho y$ jer je $s y s^{-1} = (s^{-1})^{-1} y (s^{-1})$ / $s^{-1} \in G$ /.

Najzad $x \rho y$ i $y \rho z$ daju $y = s^{-1} x s$, $z = t^{-1} y t$ /$s, t \in G$/, pa je $z = (st)^{-1} x (st)$ /$st \in G$/. Dakle, $x \rho z$.

Pošto je ρ refleksivna, simetrična i tranzitivna zaključujemo da je ρ relacija ekvivalencije.

2/ Neka je $a \in G$ proizvoljan element grupe G. Njegova

klasa ekvivalencije C_a je $C_a = \bigcup_{s \in S} \{s^{-1}as\}$. U zadnjoj uniji ne mogu biti svi članovi unije različiti. Ovo je od bitnog značaja za broj elemenata u C_a. Ispitajmo zato, kada je $s^{-1}as = t^{-1}at$.

Neka je $s^{-1}as = t^{-1}at$. Tada je $ts^{-1}a = ats^{-1}$, pa elementi a i ts^{-1} moraju biti permutativni. Označimo sa Na skup svih elemenata grupe G koji su permutativni sa elementom a. Ovaj skup Na je podgrupa grupe G / videti zad.21/. Znači $ts^{-1} \in$ Na. Ova činjenica znači da u razlaganju

$$(*) \qquad G = Na + (Na)b_2 + \ldots + (Na)b_\ell$$

grupe G pomoću podgrupe Na elementi ts i s padaju u isti koset. Lako se zaključuje da $ts^{-1} \in Na \Rightarrow s^{-1}as = t^{-1}at$, pa je pripadanje elemenata s i t istom kosetu u razlaganju (*) i potreban i dovoljan uslov da je $s^{-1}as = t^{-1}at$. Odavde zaključujemo da u $\bigcup_{s \in G} \{s^{-1}as\}$ ima onoliko različitih elemenata koliko u (*) ima koseta. Znači u Ca ima ℓ elemenata. Kako se ℓ, prema Lagrange-ovoj teoremi, sadrži u redu grupe G, to je tvrdjenje u potpunosti dokazano.

3/ Ovo sleduje prema zadatku 30.

4/ Koristeći zadatak 91 zaključujemo da $S_4/\mathfrak{P}$ ima elemente C_1, C_2, C_3, C_4, i C_5 gde je $C_1 = \{(1)(2)(3)(4)\}$,

$C_2 = \{(12),(13),(14),(23),(24),(34)\}$, $C_3 = \{(12)(34),(13)(24),(14)(23)\}$

$C_4 = \{(123),(124),(134),(234),(132),(142),(143),(243)\}$ i

$C_5 = \{(1234),(1243),(1324),(1342),(1423),(1432)\}$.

Zadatak 60. Ako je svaki element konačne grupe G, izuzev jediničnog elementa e, reda dva, tada je G reda 2^k.

Rešenje. Pre svega, grupa je Abelova. Neka su $a_1, a_2, \ldots, a_k$ generatorni elementi grupe G. Uočimo skup

$$S = \left\{ \alpha_1 \; \alpha_2 \; \alpha_3, \ldots, \alpha_k \right\}$$
$$\quad a_1 \quad a_2 \quad a_3 \quad a_k$$

gde je $\alpha_i = \begin{cases} 0 \\ 1 \end{cases}$. Ma koji element grupe G ima takvu jednu i samo jednu faktorizaciju preko

generatornih elemenata. Znači S = G.Broj svih elemenata u S je 2^k; otuda sleduje gornje tvrdjenje.

Zadatak 61. Dokazati da je izomorfizam kod grupa jedna relacija ekvivalencije.

Zadatak 62. Pokazati da su izomorfne sledeće grupe:

$$G_1 = \{1, i, -1, -i\} \text{ / operacija množenja brojeva /,}$$

$$G_2 = \left\{ \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}, \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix}, \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} \right\}$$

/operacija matrično množenje /.

Rešenje. Elemente grupe G_1 označimo respektivno sa a_1, a_2, a_3, a_4, a druge grupe G_2 sa b_1, b_2, b_3, b_4. Odgovarajuće tablice množenja onda izgledaju:

	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_3	a_4	a_1
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_1	a_2	a_3

	b_1	b_2	b_3	b_4
b_1	b_1	b_2	b_3	b_4
b_2	b_2	b_3	b_4	b_1
b_3	b_3	b_4	b_1	b_2
b_4	b_4	b_1	b_2	b_3

Uvedimo biunivoku preslikavanja ϕ definisano sa $a_\nu\phi = b_\nu$. Iz navedenih tablica zaključujemo da je $(a_\nu \cdot a_\mu)\phi = (a_\nu\phi).(a_\mu\phi)$ pa je ϕ izomorfizam.

Primedba. Naći sve izomorfizme izmedju G_1 i G_2.

Zadatak 63. Da li je multiplikativna grupa svih pozitivnih realnih brojeva izomorfna sa aditivnom grupom svih realnih brojeva?

Zadatak 64. Neka je $(G, *)$ zadana grupa i neka je $a \in G$ jedan odredjen element. Dokazati da je $(G, *) \cong (G, \circ)$, gde je operacija definisana jednakošću $x \circ y = x * a * y$,

, $\forall\, x,y \in G$.

Zadatak 65. Postoje samo dve grupe reda 4, obe su Abelove.

Rešenje. Navedeni iskaz znači da u mnoštvu grupa reda 4 postoje samo dve neizomorfne. Neka je $G = \{e, a, b, c\}$ ma kakva grupa reda 4. Elementi a, b, c mogu biti reda 4 ili 2. Razlikovaćemo dva slučaja:

I slučaj : Bar jedan od elemenata a, b, c je reda 4. Neka je to element a . Skup $S = \{e, a, a^2, a^3\}$ ima 4 različita elementa grupa G pa je S = G ; znači G je ciklična grupa.

II slučaj: Nijedan od elemenata a, b, c nije reda 4. Tada su svi reda dva. Tada iz $a^2 = e$, $b^2 = e$, $c^2 = e$ sle-duje $a=a^{-1}$, $b = b^{-1}$, $c = c^{-1}$ pa je $aba^{-1}b^{-1}=(ab)^2= e$ tj. ab = ba, slično ac = ca, bc = cb pa je grupa Abelova. U skupu $S = \{e, a, b, ab\}$ se nalaze 4 različita elementa grupa. Znači S = G. Multiplikativna tablica grupe izgleda.

s	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Ovakva grupa zove se Klein- ova vierer grupa.

Zadatak 66. Postoje samo dve grupe reda 6, jedna je ciklična i jedna nekomutativna.

Rešenje. Neka je $G = \{e, A, B, C, D, E\}$ grupa reda 6. Njeni elementi mogu biti reda 1 / takav je samo e /, reda 2, reda 3, ili 6. Razlikovaćemo dva slučaja.

I slučaj: U G postoji bar jedan element reda 6. Neka je to A . Tada skup $S = \{e, A, A^2, A^3, A^4, A^5\}$ ima 6 različitih elemenata grupa pa je G = S tj. G je ciklična grupa.

II slučaj: U G ne postoji ni jedan element reda 6. Tada su elementi različiti od e, reda 2 i 3. Svi ne mogu biti reda 2 jer grupa nije reda 2^k. Znači u G postoji bar jedan element reda 3. Neka je to A. Skup $S_1=\{A, A^2, A^3= e\}$ je podgrupa grupe G. Neka $B \in G$ i $B \notin S_1$. Formirajmo skup $S =\{ A, A^2, A^3, AB, A^2B, A^3B\}$, $(A^3 = e)$. Svi elementi ovoga skupa su različiti. Ako postoji grupa G u II slučaju, mora biti G = S. Radi formiranja multiplikativnog tabloa potražimo prethodno B^2. Moguće su ove pretpostavke:

1/ $B^2 = A$ 4/ $B^2 = AB$,

2/ $B^2 = A^2$, 5/ $B^2 = A^2B$,

3/ $B^2 = e$, 6/ $B^2 = B$.

Pretpostavke 4, 5, 6 dovode odmah do kontradikcije zbog pretpostavke o B . Neka je $B^2 = A$, odavde zaključujemo da je B reda 3, inače bi bilo A = e što nije. Iz $B^2= A$ bi sledilo $B^3 = AB$, tj. AB = e pa je $B = A^2$ što nije moguće, jer $B \notin S_1$. Dakle je $B^2 \neq A^2$. Odavde opet zaključak da je B reda 3 pa je $B^3 = A^2B$ tj. $A^2B = e$ što daje B = A , što nije moguće. Dakle je $B^2 \neq A^2$. Znači,ako u II slučaju postoji grupa G mora biti $B^2 = e$. Nadjimo sada BA. Moguće su ove pretpostavke:

1/ BA = A, 4/ BA = B,

2/ $BA = A^2$ 5/ BA = AB,

3/ BA = e , 6/ $BA = A^2B$.

Pretpostavke 1, 2 , 3, 4 neposredno dovode do kontradikcije. Neka je BA = AB . Tada je $(AB)^3= B^3 = B \neq e$, $(AB)^2 = A^2 \neq e$, pa je AB reda 6 što je nemoguće.Dakle mora biti $BA = A^2B$.

Na osnovu nadjenih podataka lako je formirati

multiplikativnu tablicu. Ona izgleda:

	e	A	A^2	B	AB	A^2B
e	e	A	A^2	B	AB	A^2B
A	A	A^2	e	AB	A^2B	B
A^2	A^2	e	A	A^2B	B	AB
B	B	A^2B	AB	e	A^2	A
AB	AB	B	A^2B	A	e	A^2
A^2B	A^2B	AB	B	A^2	A	e

gde je, na primer, $B.A^2 = (BA)\,A = A^2\,BA = A^2.A^2B = AB$,

$B.AB = (BA)\,B = A^2BB = A^2$,

$AB.AB = A\,.\,(B.AB) = A.A^2 = e$.

Iz ove tablice, možemo saznati da je S zaista grupa, pa u II slučaju postoji zaista samo jedna grupa.

Zadatak 67. Ako su dve grupe izotopne, onda su one i izomorfne. Dokazati.

Rešenje. Ne smanjujući opštost rasudjivanja pretpostavimo da su obe grupe $(G,*)$ i $(G,\circ)$ o kojima je reč definisane na istom skupu G. Pošto su $(G,*)$ i $(G,\circ)$ izotopne, to postoje tri permutacije f, g i h skupa G, takve da

$$1/ \qquad f(x * y) = g(x) \circ h(y) \,, \quad \forall\, x, y \in G \,.$$

Za $y = e$ /e je jedinični element grupe G / jednakost/1/ daje: $f(x) = g(x) \circ h(e)$ a za $x = e$: $f(y) = g(e) \circ h(y)$, pa je

$$g(x) = f(x) \circ \left[h(e) \right]^{-1} , \quad h(x) = \left[g(e) \right]^{-1} \circ f(x) .$$

Smenom u/1/ dobijamo:

$$f(x * y) = f(x) \circ \left[h(e) \right]^{-1} \circ \left[g(e) \right]^{-1} \circ f(y), \text{tj.}$$

2/ $F(x * y) = F/x/ \circ F/y/$, $\forall x,y \in G$ gde je

$$F/x/ = \left[h/e/\right]^{-1} \circ \left[g/e/\right]^{-1} \circ f/x/ .$$

Jednakost /2/ dokazuje tvrdjenje jer je F /x/ permutacija skupa G.

Generalizacija. Navedeno tvrdjenje je specijalan slučaj sledeće teoreme : Ako su (G,*) i (G,o) dva grupoida od kojih prvi ima jedinični element,a drugi je semigrupa i ako su izotopni,onda su oni i izomorfni.

Ovu teoremu je dokazao A Sade / Videti o tome Pacif. Jour of Math.Vol. 9. No. 2, 1959, p 583 - 584 /.

Zadatak 68. Cikličnoj grupi reda 3 naći i izomorfnu grupu matrica.

Zadatak 69. Ako su dve grupe antiizomorfne onda su one i izomorfne. Dokazati.

Rešenje. Neka su G_1 i G_2 antiizomorfne i neka preslikavanje $f : x \to xf$ / $x \in G_1$, $xf \in G_2$ / ostvaruje antiizomorfizam.Tada

$$(xy)f = yf.xf , \quad \forall x, y \in G_1 .$$

Uvedimo preslikavanje g jednakošću $xg = xf^{-1}$, gde je $(xf)^{-1}$ inverzan element elemenata $xf \in G_2$. Ovo preslikavanje je preslikavanje 1-1 grupe G_1 n G_2. Kako je

$$(xy)\,g = \left[(xy)f\right]^{-1} = \left[(yf)(xf)\right]^{-1} = (xf)^{-1}(yf)^{-1} = xg.yg, \quad \forall x,y \in G_2$$

preslikavanje g je izomorfizam pa je tvrdjenje dokazano.

Zadatak 70. Dokazati Cayley - evu teoremu : Ma kom elementu a grupe $G = \{a_1 , a_2, \dots , a, \dots, a_g\}$ koordinirajmo permutaciju a'_μ

$$a'_\mu = \begin{pmatrix} a_1 & a_2 & \dots & a_g \\ a_1 a_\mu & a_2 a_\mu & \dots & a_g a_\mu \end{pmatrix} .$$

Tada skup svih ovih permutacija formira G' /podgrupu od S_g / izomorfnu datoj grupi G pri biunivokom preslikavanju $a_\mu \leftrightarrow a'_\mu$.

Dokaz. Skup $G' = \{a'_1, a'_2 , \dots , a'_g\}$ formirajmo prema navedenoj konvenciji. Navedeno preslikavanje je 1-1. Neka je $a_\mu . a_\nu = a_\sigma$. Pokažimo da je $a'_\mu . a'_\nu = a'_\sigma$ Zaista:

$$a'_\mu \cdot a'_\nu = \begin{pmatrix} a_1 & a_2 & \cdots & a_g \\ a_1 a_\mu & a_2 a_\mu & & a_g a_\mu \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & \cdots & a_g \\ a_1 a & a_2 a & \cdots & a_g a \end{pmatrix} =$$

$$= \begin{pmatrix} a_1 & a_2 & \cdots & a_g \\ a_1 a_\mu & a_2 a_\mu & \cdots & a_g a_\mu \end{pmatrix} \cdot \begin{pmatrix} a_1 a & a_2 a & \cdots & a_g a \\ (a_1 a_\mu) a_\nu & (a_2 a_\mu) a_\nu & \cdots & (a_g a_\mu) a_\nu \end{pmatrix} =$$

$$= \begin{pmatrix} a_1 & a_2 & \cdots & a_g \\ a_1 a_\mu a_\nu & a_2 a_\mu a_\nu & \cdots & a_g a_\mu a_\nu \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \cdots & a_g \\ a_1 a_\tau & a_2 a_\tau & \cdots & a_g a_\tau \end{pmatrix} = a'_\tau$$

Iz dokazane izomorfije sleduje, pošto je G grupa, da je G' grupa, podrgupa simetrične grupe S_g.

Zadatak 71. Grupi iz zadatka 4 naći izomorfnu regularnu grupu permutacija.

Rešenje. Koristeći Cayley - evu teoremu izomorfnu regularnu grupu permutacija dobijamo iz njene multiplikativne tablice. Nadjimo odgovarajuću permutaciju za f_4 :

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6\},$$

$$G.f_4 = \{f_4, f_6, f_5, f_1, f_3, f_2\}$$

To znači da je

$$f'_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix} = (14)(26)(35).$$

Slično nalazimo i ostale permutacije. Cela grupa G', $f'_1 = (1)$, $f'_2 = (123)(456)$, $f'_3 = (132)(465)$, $f'_4 = (14)(26)(35)$, $f'_5 = (15)(24)(36)$, $f'_6 = (16)(25)(34)$.

Zadatak 72. Grupi $\{i, -i, 1, -1\}$ /operacija množenja kompleksnih brojeva/. Naći izomorfnu grupu regularnih permutacija.

Rešenje. Stavimo $a_1 = i$, $a_2 = -i$, $a_3 = 1$, $a_4 = -1$. Načinimo šemu :

$$\{a_1, a_2, a_3, a_4\} = G$$
$$\{a_4, a_3, a_1, a_2\} = Ga_1$$
$$\{a_3, a_4, a_2, a_1\} = Ga_2$$
$$\{a_1, a_2, a_3, a_4,\} \quad Ga_3$$
$$\{a_2, a_1, a_4, a_3,\} \quad Ga_4$$

ODAVDE je $a_1' = (1423)$, $a_2' = (1324)$, $a_3' = (1)$, $a_4' = (12)(34)$ pa je tražena izomorfna grupa

$$(1), (1423), (1324), (12)(34) .$$

Zadatak 73. Na polju j_3 su dati polinomi x, 2x, 1+2x, 2+ 2x, 1+x, 2+x.

1/ Dokazati da je skup tih polinoma grupa u odnosu na množenje supstitucijom.

2/ Ispitati da li je preslikavnje

$$\begin{pmatrix} x & 2x & 1+2x & 2+2x & 1+x & 2+x \\ (1) & (12) & (13) & (23) & (123) & (132) \end{pmatrix}$$

izomorfizam ili antiizomorfizam ?

3/ Dokazati da je $\{a + bx ; a, b, \in J_3\}$ semigrupa u odnosu na množenje supstitucijom.

4/ Ispitati da li je $\{a + bx ; b \neq 0 ; a, b \in J_p\}$ grupa u odnosu na množenje supstitucijom.

Zadatak 74. U skupu N svih prirodnih brojeva definisati bar jednu operaciju $*$,tako da (N,$*$) bude grupa.

Rešenje. Izmedju skupova Z / skup svih celih brojeva/ i N uspostavimo korespodenciju 1 - 1 na sledeći način

$$f \begin{pmatrix} 0, & 1, & -1, & 2, & -2, & 3, & -3, & 4, & -4, & 5, & -5, \ldots \\ 1, & 2, & 3, & 4, & 5, & 6, & 7. & 8, & 9, & 10, & 11, \ldots \end{pmatrix}$$

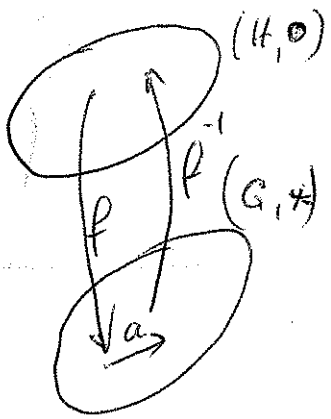
Analitički izraz ove korespodencije je $f(n) = (-1)^n \left[\frac{n}{2}\right]$ / n prirodan broj/, a inverzna funkcija je $f^{-1}(c) = 2c + \theta(c)$ / c ceo broj/, gde je

$$\theta(c) = \begin{cases} 0, & c = 0 \\ 1 & c \neq 0 \end{cases}$$

Operaciju $*$ ćemo definisati iz uslova da je $(Z,+) \cong (N,*)$ i da se izomorfizam ostvaruje preslikavanjem f, odnosno $f(n * m) = f(n) + f(m)$ / $\forall$ n, m $\in$ N /. Odavde $n * m = f^{-1}(f(n) + f(m))$, pa je $*$ potpuno odredjena u $(N,*)$ jeste grupa.

Zadatak 75. Neka su H i G dve izomorfne grupe. Kardinalni broj skupa svih izomorfizama izmedju H i G je jednak kardinalnom broju skupa svih automorfizama grupe G.

Rešenje. Neka su $J = \{f, \varphi, \ldots\}$ i $A = \{a, b, \ldots\}$ redom skupovi svih izomorfizama grupe $(H,\circ)$ na grupu $(G,*)$ i automorfizama grupe $(G,*)$.



Neka je f jedan fiksirani elemenat skupa J. Tada je

1/ $(x \circ y) f = xf * yf \quad \forall x,y \in H$.

Ako je φ bilo koji element iz J onda je.

2/ $(x \circ y)\varphi = x\varphi * y\varphi \quad \forall x,y \in H$.

Iz /1/ imamo $x * y = (xf^{-1} \circ yf^{-1}) f$, pa je $(x * y) f^{-1} = xf^{-1} \circ yf^{-1}$. Odavde prema /2/ je $(x * y) f^{-1}\varphi = xf^{-1}\varphi \circ yf^{-1}\varphi$ tj. $f^{-1}\varphi \in A$. Pošto $f^{-1}\varphi_1 = f^{-1}\varphi_2$ povlači $\varphi_1 = \varphi_2$, zaključujemo da je preslikavanje $\phi : \varphi \to f^{-1}\varphi$ biunivoko preslikavanje skupa J u skup A.

Dalje, ako je a proizvoljan elemenat skupa A, onda je $fa \in J$ / ovo se dobija na sličan način/.

Medjutim, za $\varphi = fa$ gornje preslikavanje / $\varphi \to f^{-1}\varphi$ /

da je $\varphi \to a$ pa je ϕ preslikavanje skupa J na skup A, odnosno $k(J) = k(A)$, pa je tvrdjenje dokazano.

Zadatak 76. Dokazati da je grupa Abelova tada i samo tada ako je preslikavanje $A \leftrightarrow A^{-1}$, $B \leftrightarrow B^{-1}$,... automorfizam.

Rešenje. Predpostavimo prvo da je preslikavanje $A \leftrightarrow A^{-1}$, $B \leftrightarrow B^{-1}$, ... automorfizam. Tada elementu AB sa jedne strane odgovara $A^{-1} B^{-1}$, a sa druge strane $(AB)^{-1}$. Znači, $(AB)^{-1} = A^{-1} B^{-1}$. Uzmimo inverzne elemente sobe strane pa imamo $AB = (A^{-1}B^{-1})^{-1} = BA$ tj. grupa je Abelova.

Neka, sada, grupa bude Abelova. Preslikavanje $A \leftrightarrow A^{-1}$, $B \leftrightarrow B^{-1}$, ... je biunivoko jer ako je $\alpha \to \beta$ i $\alpha \to \gamma$ onda je $\beta = \alpha^{-1}$, $\gamma = \alpha^{-1}$ pa $\beta = \gamma$. Ovo preslikavanje je automorfizam jer ako je $A \leftrightarrow A^{-1}$, $B \leftrightarrow B^{-1}$ onda je $AB \leftrightarrow (AB)^{-1} = A^{-1}B^{-1}$.

Zadatak 77. Potreban je dovoljan uslov da grupa G bude Abelova jeste da preslikavanje $A \leftrightarrow A^2$, $B \leftrightarrow B^2$,...bude endomorfizam. Dokazati.

Zadatak 78. Neka je preslikavanje $A \to A^k$, $B \to B^k$,... /$k > 1$, prirodan broj / biunivoko preslikavanje grupe G. Dokazati da G ne može biti reda k^n gde je n prirodan broj.

Rešenje. Neka je $A \neq e$ bilo koji element grupe G. Predpostavimo da je red grupe jednak k^n, gde je n izvestan prirodan broj. Tada / videti zadatak 47 / je $A^{k^n} = e$ pa iz $(A^{k^{n-1}})^k = e$ i $e^k = e$, prema pretpostavci biunivokosti navedenog preslikavanja, dobijamo $A^{k^{n-1}} = e$. Nastavljajući ovaj postupak dolazimo do $A^k = e$, odakle $A = e$ jer je i $e^k = e$. Time je dokaz završen jer nas je pretpostavka da je red grupe k^n dovela do kontradikcije.

Zadatak 79. Potreban i dovoljan uslov za preslikavanje $x \to axb$ grupe G, gde su a i b dva fiksirana elementa

grupe G, bude automorfizam je ab = e. Dokazati.

Zadatak 80. Neka je G grupa reda 8 sa definisionim jednakostima :

$$A^2 = e, \quad B^2 = e, \quad AB^4 = e$$

Pokazati da je G izomorfna sa grupom svih svojih automorfizama.

Ako se grupa G može proizvesti pomoću elemenata a i b, koji zadovoljavaju relaciju: /1/ $a^3 = b^2 = (ab)^2 = e$ / e je jedinični elemenat grupe G / pokazati da se grupa G sastoji iz šest elemenata: $a^m b^k$ /m=0,1 , 2;k=0,1/.

Zadatak 81. Ako su G i H grupa onda i skup G x H svih uredjenih parova (g_i, h_j) /$g_i \in G$, $h_j \in H$ / čini grupu odnosno operaciju

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

Rešenje. Navedena operacija je unutrašnja u skupu G x H, asocijativna. Jedinični element je e_1, e_2, /e_1 je jedinični element grupe G, e_2 je jedinični element grupe H/. Ako je (g,h) bilo koji element iz G x H onda (g^{-1}, h^{-1}) je njegov inverzni. Znači (G x H.) je zaista grupa.

Primedba. Dobijena grupa G x H se zove direktan proizvod grupa G i H.

Zadatak 82. Dokazati da je direktan proizvod dve ciklične grupe relativno prostog reda, ciklična grupa.

Rešenje. Neka su $C_r = \{a, a^2, \ldots, a^r = e_1\}$ i $C_s = \{b, b^2, \ldots, b^s = e_2\}$ ciklične grupe reda r, odnosno s. Tada je $C_r \times C_s = \{(a^i, b^j)\ i = 1, 2, \ldots, r\ ;\ j = 1, 2, \ldots s\}$. Element (a, b) ima osobinu: $(a, b)^{r.s} = (a^{r.s}, b^{r.s}) = (e_1, e_2)$. S druge strane, ako $(a,b)^k = (e_1, e_2)$ imamo $a^k = e_1$, $b^k = e_2$

pa $r \mid k$ i $s \mid k$. Kako je / r, s / = 1, to je / r, s/$\mid$k.

Znači perioda elemenata (a, b) je r.s pa je tvrdjenje u potpunosti dokazano.

Zadatak 83. Ako su G_1 i G_2 grupe,onda su grupe $G_1 \times G_2$ i $G_2 \times G_1$ izomorfne. Dokazati.

Generalizacija. Ako su G_1, G_2 i G_3 grupe onda su grupe $G_1 \times G_2 \times G_3$, $G_2 \times G_3 \times G_1$, $G_3 \times G_1 \times G_2$, ... Izomorfne.

Zadtak 84. Skup svih racionalnih brojeva oblika $2^m 3^n 5^p$ /m, n, p celi brojevi / u odnosu na množenje čini grupu izomorfnu grupi (Z,+) x (Z,+) x (Z,+). Dokazati.

Zadatak 85. Skup unutrašnjih automorfizama grupe G čini grupu homomorfnu datoj grupi.

Rešenje. Ako je $a \in G$ onda njemu odgovara unutrašnji automorfizam f_a: $xf_a = a^{-1}xa$ / $x \in G$/. Skup unutrašnjih automorfizama čini kao što je poznato grupa. Pošto je

$$xf_{ab} = (ab)^{-1} x (ab) = b^{-1}a^{-1} xab = (xf_a)f_b = x f_a . f_b,$$

zaključujemo $f_{ab} = f_a . f_b$, pa je preslikavanje $a \to f_a, b \to f_b$, homomorfizam grupe G na grupu unutrašnjih automorfizama grupe G.

Zadatak 86. Potreban i dovoljan uslov da element a grupe G inducira indentičan unutrašnji automorfizam je da je a u centru grupe G .

Zadatak 89. tranzitivne grupe G od n promenljivih je deljiv sa n .

Rešenje. Grupa G permutacija od n promenljivih $x_1, x_2, \ldots, x_n$ se zove tranzitivna ako ona sadrži permutacije s_i koje x_1 prevode u x_i za i = 1, 2, ... , n

Specijalno ako je G. reda n, onda se zove regularna .

Skup svih permutacija iz grupe G koje x_1 prevode u x_1 čine grupu H, podgrupu grupe G / jer proizvod takve dve

permutacije prevodi x_1 u x_1 / . Obrazulmo skup $S = \{H, H_{s_2}, H_{s_3}, \ldots, H_{s_n}\}$ gde smo sa $s_2, s_3, \ldots, s_n$ označili / n - 1/ - vu permutaciju iz G koje prevode x_1 respektivno u $x_2, x_3, \ldots, x_n$. Takve u G sigurno postoje, jer je G tranzitivna. Hoćemo da dokažemo da je S = G. Neka je $a = \begin{pmatrix} x_1 & x_2 \ldots x_n \\ x_i & x_j \ldots x \end{pmatrix} \in G$ ma koja permutacija iz G. Primetimo da a. S_i^{-1} prevodi x_1 u x_1. Otuda $aS_i^{-1} = h \in H$. Znači $a = hS_i \in Hs_i$ pa je $a \in S$. Znači, zaista je S = G. Tvrdjenje je dokazano jer svi elementi u S su različiti a njihov broj je deljiv sa n .

Zadatak 90. Podgrupa indeksa 2 je uvek invarijantna podgrupa.

Rešenje. Neka $H \in G$ i neka g/h = 2 gde su g i h redovi grupe G i H. Pokažimo da je $H \prec G$. Razložimo grupu G preko njene podgrupe H. Neka je $\sum \in (G - H)$ bilo kakav element. Tada $G = H + H\sum$ i takodje $G = H + \sum H$. Odavde je $H\sum = \sum H$ tj. $\sum^{-1} H \sum = H$.
Pošto ovakva jednakost važi i za $\sum \in H$, to znači za makakav $\sum \in G$ je $\sum^{-1} H \sum = H$, što znači da je $H \subset G$.

Zadatak 91. Pokazati da je $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ normalna podgrupa simetrične grupe S_4.

Rešenje. Simetrična grupa S_4 se sastoji od ovih permutacija: (1),(12),(13),(14),(23),(24),(34), (12)(34), (13)(24),(14)(23), (123), (124), (134), (132),(142),(143), (243), (1234),(1243),(1324),(1342),(1423),(1432).Primetimo odmah da u $(S_4 - V_4)$ nema permutacija oblika (ab) (cd) gde $a \neq b \neq c \neq d$, kakve se sve nalaze u V_4. Da bismo dokazali da je $V_4 \prec S_4$, treba da dokažemo da ako je $x \in S_4$ bilo kakva

permutacija, da je onda $x^{-1} V_4 x = V_4$.

Napišimo x u obliku

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \alpha & \beta & \gamma & \delta \end{pmatrix}$$

Tada $x^{-1}V_4x = x^{-1}\{(1), (12)(34), (13)(24), (14)(23)\} x =$

$= \{x^{-1}(1)x, x^{-1}(12)(34)x, x^{-1}(13)(24)x, x^{-1}(14)(23)x\} =$

$= \{(1), (\alpha\beta)(\gamma\delta), (\alpha\gamma)(\beta\delta), (\alpha\delta)(\beta\gamma)\} = V_4$. Koristili smo važnu jednakost

$$\begin{pmatrix} 1 & 2 & \dots & m & \dots & p & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_m & \dots & \alpha_p & \dots & \alpha_n \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 2 & \dots & n \\ m & p & \dots & e \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & \dots & m & \dots & p & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_m & \dots & \alpha_p & \dots & \alpha_n \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_m & \alpha_p & \dots & \alpha_e \end{pmatrix}$$

Zadatak 92. Naći S_4 / C_4 gde je S_4 simetrična grupa od 4 elementa a C_4 Klein - ova vierer podgrupa.

Zadatak 93. Neka su A i B podgrupe grupe G i neka je A normalna podgrupa grupe G. Dokazati da je $A \cap B$ normalna podgrupa grupe B.

Zadatak 94. Ako su A i B dve normalne podgrupe grupe G i ako je $A \cap B = e$, tada svaki element iz A je komutativan sa svakim elementom iz B.

Rešenje. Neka $a \in A$, $b \in B$. Obrazujmo $aba^{-1}b^{-1}$. Pošto su A i B dve normalne podgrupe to je $aba^{-1} \in B$, $ba^{-1}b^{-1} \in A$, pa znači $aba^{-1} \cdot b^{-1} \in B$ i $a \cdot ba^{-1}b^{-1} \in A$, tj. $aba^{-1}b^{-1} \in A \cap B$. Pošto je $A \cap B = e$ to je $aba^{-1}b^{-1} = e$, odakle je $ab = ba$, pa je tvrdjenje dokazano.

Zadatak 95. Dokazati da je skup $\{a_1^k, a_2^k, a_3^k, \dots a_g^k\}$ invarijantan podskup grupe $G = \{a_1, a_2, a_3, \dots a_g\}$ za svaki prirodan broj k.

Rešenje. Označimo dati skup sa S_k. Treba dokazati

da je $a^{-1}S_k a = S_k$ za bilo koji $a \in G$. Koristićemo jednakost $s^{-1}a^k s = (s^{-1}as)^k$ koja važi za makoji par elemenata a i s iz grupe za svaki prirodan broj k. Pomoću nje imamo:

$$a_\nu^{-1} S_k a_\nu = a_\nu^{-1} \{ a_1^k, \ldots, a_g^k \} a_\nu$$

$$= \{ a_\nu^{-1} a_1^k a_\nu, \; a_\nu^{-1} a_2^k a_\nu, \; \ldots \; a_\nu^{-1} a_g^k a_\nu \} =$$

$$= \{ (a_\nu^{-1} a_1 a_\nu)^k, \; (a_\nu^{-1} a_2 a_\nu)^k, \; \ldots (a_\nu^{-1} a_g a_\nu)^k \} = S_k$$

Jer skup $S_1 = \{ a_\nu^{-1} a_1 a_\nu, \; a_\nu^{-1} a_2 a_\nu, \ldots, a_\nu^{-1} a_g a_\nu \}$ Ima g različitih elemenata pa je isti kao sama grupa.

Primedba . Naći i druge skupove slične osobine.

Zadatak 96. Ako je ρ kongruencija u grupi G, onda postoji normalna podgrupa H grupe G, takva da za sve $a, b \in G$ je $a \rho b$ ako i samo ako $ab^{-1} \in H$. Dokazati.

Rešenje. Pošto je ρ kongruencija to je

1/ ρ relacija ekvivalencije

2/ iz $a \rho b$ i $c \rho d$ sledi $ac \rho bd$.

Označimo sa H klasu ekvivalencije za jedinični element e. Pokažimo da je H normalna podgrupa za G. Neka $a, b \in H$. Tada $a \rho e$, $b \rho e$, pa je $ab \rho ee$, $ab \rho e$ tj. $a.b \in H$. Iz $a \rho e$ i $a^{-1} \rho a^{-1}$ imamo $a.a^{-1} \rho e.a^{-1}$, tj. $a^{-1} \rho e$. Znači $a^{-1} \in H$. Otuda je H podgrupa za G . Neka $s \in G$, $a \in H$ tada iz relacija $a \rho e$, $s^{-1} \rho s^{-1}$, $s \rho s$ sledi $s^{-1}as \rho s^{-1}es$, $s^{-1}as \rho e$, pa je $s^{-1}as \in H$. Znači H je normalna podgrupa grupe G pa je stav dokazan.

Zadatak 97. H i K su podgrupe grupe G . Dokazati da je relacija ρ u grupi G: $x \rho y \Leftrightarrow (\exists h \in H), (\exists k \in K), x = hyk$, jedna relacija ekvivalencije.

Rešenje. Navedena relacija je refleksivna jer

$x = xex$ ($e \in H$, $e \in K$) . Ona je simetrična jer $x \rho y$ daje $x = hyk$ / $h \in H$, $k \in K$) , odakle : $y = h^{-1}xk^{-1}$ /$h^{-1} \in H$, $k^{-1} \in K$ / pa je $y \rho x$. Najzad, ρ je tranzitivna jer: $x \rho y$, $y \rho z \Rightarrow x = h_1 y k_1$, $y = h_2 z k_2$ /$h_1, h_2 \in H$, $k_1, k_2 \in K$ pa je : $x = h_1 h_2 z k_1 k_2$ / $h_1, h_2 \in H$, $k_1 k_2 \in K$) $\Rightarrow x \rho z$.

Zadtak 98. Neka je H podgrupa grupe G. Dokazati da je $K = \bigcap_{S \in G} s^{-1} Hs$ normalna grupa G.

Rešenje. Neposredno se dokazuje da je K podgrupa grupe G. Ako je,dalje x (G bilo koji element,imamo

$$x^{-1} Kx = x^{-1} \left(\bigcap_{S \in G} s^{-1} Hs \right) x \subset \bigcap_{S \in G} x^{-1} s^{-1} Hsx = \bigcap_{S \in G} (sx)^{-1} H(sx) =$$

$$= \bigcap_{r \in G} r^{-1} Hr = K, \text{ tj. } x^{-1} Kx \subset K, \text{ pa je K zaista normalna}$$

podgrupa,jer $x^{-1} Kx \subset K$ / $\forall x \in G$ / $\Rightarrow x^{-1} Kx = K$ / $\forall x \in G$/.

Zadatak 99. Neka su M i N invarijantne podgrupe grupe G. Šta predstavlja skup $Q = \{x.y \, ; \, x \in M, \, y \in N\}$ u odnosu na operaciju u grupi G ?

Rešenje. Neka su x . y i X.Y bilo koja dva elementa Q / $x, X \in M$, $y, Y \in N$ / . Zbog invarijantnosti podgrupa M i N važi $X^{-1} y X = \alpha \in N$. Prema ovome je

$$(x.y)(X.Y) = xXX^{-1} yXY = x.Y\alpha . Y \in Q$$

jer $x.X \in M$, $\alpha . Y \in N$. Znači$(Q, \cdot)$ je grupoid, a svakako i semigrupa zbog asocijativnosti operacije grupe G.

Za $x = e \in M$, $y = e \in N$ dobijamo $e.e = e \in Q$. Ako $x.y \in Q$ / $x \in M$, $y \in N$/ onda i

$$y^{-1} x^{-1} = y^{-1} x^{-1} yy^{-1} = x_1 . y^{-1} \in Q$$

jer $y^{-1} x^{-1} y \in M$. Kako je $x.y^{-1} x^{-1} = e$ to svaki element u Q ima inverzni element. Znači $(Q, \cdot)$ je grupa,podgrupa grupe G.

Proverimo da li je invarijantna podgrupa. Za $s \in G$ važi

$$s^{-1}xys = (s^{-1}xs).(s^{-1}ys) \in Q$$

jer $s^{-1}xs \in M$, $s^{-1}ys \in N$. Znači Q je invarijantna podgrupa grupe G.

Zadatak 100. Dokazati da je centar Z bilo koje grupe G normalna podgrupa za G i da je G/Z izomorfna sa grupom unutrašnjih automorfizama grupe G.

Zadatak 101. Neka su a = (12) i b = (13)(24) dva elementa grupe S_4. Formirati podgrupu grupe S_4 čiji su generatorni elementi a i b, a zatim naći grupu unutrašnjih automorfizama te podgrupe.

Zadatak 102. Neka je C centar nekomutativne grupe G. Dokazati da faktor grupa G/C nije ciklična.

Rešenje. Pretpostavimo obrnuto da je G/C ciklična i da je Cb njen generatorni element. Tada je $G/C = \{(CB)^{\nu}; -\infty < \nu < +\infty\}$ bez obzira na moć skupova G i C. Kako je $(Cb)^{\nu} = Cb^{\nu}$ $/-\infty < \nu < +\infty/$, svaki element grupe G ima oblik cb^{ν} / $c \in C$, $-\infty < \nu < +\infty$ / . Ako su c_1b^{ν} i c_2b^{ν} i c_2b^{μ} dva elementa grupe G tada :

$$c_1b^{\nu} \cdot c_2b^{\nu} = c_1c_2b^{\nu+\mu}$$

$$c_2b^{\mu} \cdot c_1b^{\nu} = c_1c_2b^{\nu+\mu}, \ /c_1, c_2 \in C/,$$ pa je grupa komutativna. Dobijena kontradikcija dokazuje tvrdjenje.

Zadatak 103. Neka je C centar grupe G i neka je G/C prostog reda. Dokazati da je G komutativna grupa.

Uputstvo. Videti prethodan zadatak.

Zadatak 104. Neka je S skup od n elemenata i neka $T \subset S$ ima m /m<n/ elemenata. Neka je, dalje, u skupu T svuda definisana binarna operacija f (x,y), tako da je (T,f) grupa.

Ispitati da li se f (xy) može proširiti u operaciju F (x,y) svuda definisanu na skupu S tako da (S,F) bude grupa.

Primedba. F (x,y) je proširenje za f (x,y) ako $F(x,y) = f(x,y)$ za $x,y \in T$.

Rešenje. Prema Lagrange - ocoj teoremi problem je moguć jedino ako je m/n . Ovo je, znači, nužan uslov. Pokazaćemo da je i dovoljan za egsistenc ju $F(x,y)$.

Neka m/n, tj. neka je $n = m.k$ gde je k izvestan ceo broj. Sa $C_k = \{ c, c^2, \ldots , c^k = e_1 \}$ označimo cikličnu grupu reda k. Neka su $t_1 = e, t_2, \ldots n_m$ svi elementi grupe (T,f). Neka je $(T \times C_k, o)$ direktan proizvod grupa T i C_k. Skup $(T \times C_k)$ ima tačno n elemenata. Neka je p funkcija koja preslikava S na $T \times C_k$ takva da je $p(t_i, e_1) / i = 1,2,\ldots m/$. Tada je operacija $F(x,y) = p^{-1}$ (p/x/o p/y/) definisana na čitavom skupu S i $F(x,y) = f(x,y)$ za $x,y \in T$. Pošto je (S,F) grupa dokazali smo da je problem moguć ako je m/n i našli smo jednu funkciju F (x,y).

Generalizacija . Proučiti sličan problem za kvazigrupe semigrupe, prstene i slično.

Zadatak 105. Dokazati da je kvaternionska grupa hamiltonijan.

Primedba. Nekomutativna grupa se zove hamiltonijan ako je svaka njena podgrupa normalna podgrupa.

Rešenje. Kvaternionsku grupu G čine kvaternioni $+1, +i, +j$, i k u odnosu na operaciju množenja kvaterniona. Ova grupa je nekomutativna.

Pošto je red grupe S , njene podgrupe mogu biti jedino reda 1, 2, 4, i 8. Podgrupe reda 1 i 8 su normalne podgrupe. Podgrupe reda 4 su takodje normalne jer je indeks ovih podgrupa 2. Ostaje još da se dokaže da su podgrupe reda 2 normalne. Pošto 2 prost broj ove podgrupe moraju biti sikliče Kako je jedino element - 1 reda 2, reda 2 je jedino podgrupa $H = \{ -1, 1 \}$. Pošto je $G = H + Hi + Hk$ i $G = H + iH + jH + kH$, zaključujemo da je H normalna podgrupa grupe G / kvaternionske grupe /.

pa.

Na taj način sve podgrupe nekomutativne grupe G su normalne pa je G hamiltonijan.

Zadatak 106. Naći grupu automorfizama za

a/ cikličnu grupu reda 12, b / Klein - ovu vierer- grupu c/ S_3, d/ kvaternionsku grupu, e / semigrupu čiji su elementi 1, 2, 3,..., n a operacija max f/ $C_4 \times C_2$, gde su C_2 i C_4 ciklične grupe reda 2 odnosno reda 4.

Zadatak 107. Naći sve automorfizme aditivne grupe racionalnih brojeva.

Rezultat . $xf = cx$, gde je c racionalan broj različit od nule.

Zadatak 108. Dokazati da grupa automorfizama nekomutativne grupe G ne može biti ciklična.

Rešenje. Grupa unutrašnjih automorfizama U grupe G je izomrfna sa G/C / C centar grupe G /.Pošto G/C nije ciklična /videti zad. 102 /,ne može ni U biti ciklična. Grupa A svih automorfizama grupe G nije cikličaa jer njena podgrupa U nije ciklična.

Zadatak 109. Neka je $G = \{ e, A, A^2, B, AB, A^2B \}$, ($A^3 = B^2 = e$, $BA = A^2B$) data grupa. Naći sve njene podgrupe normalne podgrupe,odgovarajuće faktor - grupe, kompozicione nizove i nizove indeksa.

Rešenje. Prave podgrupe mogu biti reda 2 i reda 3. Pošto su 2 i 3 prosti brojevi, to su one ciklične. Da bi smo ih odredili obrazujemo potencije svakog elementa date grupe dok ne dobijemo e . Skupovi potencija su:

$$H_1 = \{ A, A^2, A^3 = e \}$$

$$H_2 = \{ A^2, (A^2)^2, (A^2)^3 \} = \{ A^2, A, e \} = H_1$$

$$H_3 = \{ B, B^2 = e \}$$

$$H_4 = \{ AB, (AB)^2 \} = \{ AB, e \} \text{ jer } (AB)^2 = ABAB = A(BA)B =$$
$$= AA^2BB = A^3B^2 = e$$

$$H_5 = \{A^2B,\ (A^2B)^2\} = \{A^2B,\ e\}$$ jer $(A^2B)^2 = A^2B.A^2B =$

$$= A^2(BA)AB = A^2A^2BAB = ABAB = e$$

$$H_6 = \{e\}\ .$$

Dakle, prave podgrupe grupe G su : H_1, H_3, H_4 i H_5. Indeks podgrupe H_1 je 2 pa je ona normalna podgrupa/zad.90/. Za ostale cemo pokazati da nisu. Obrazujmo $A^{-1}H_3A$. Kako je $A^{-1} = A^2$ to :

$$A^{-1}H_3A = A^2H_3A = A^2\{B,\ e\}\ A = \{A^2BA,\ A^2eA\} = \{A^2A^2B, e\} =$$

$$= \{AB,\ e\} = H_4 \neq H_3\ .$$

Znači H_3 i H_4 su konjugovane podgrupe, otuda ni H_4 nije normalna podgrupa G. Obrazujmo $A^{-1}H_5A$. Slično kao gore imamo

$$A^{-1}H_5A = A^2H_5A = A^2\{A^2B,\ e\}A = \{A^2BA,\ e\} = \{B,\ e\} = H_3 \neq H_5.$$

Znači H_3, H_4, H_5 su konjugovane podgrupe pa pošto su različite to nijedna nije normalna.

Neprave podgrupe grupe G su H_6 i G . Postoji samo ovaj niz kompozicija $G > H_1 > H_6$. Redovi ovih grupa su respektivno 6, 3, 1 pa je niz indeksa $\frac{6}{3}$, $\frac{3}{1}$ odnosno 2,3. Nadjimo sada faktor grupu koja odgovara podgrupi H_1. Razložimo G preko H_1: $G = H_1 + H_1B$. Tražena faktor grupa G/H_1 je skup elemenata H_1 i H_1B snabdeven sa poznatom operacijom množenja dva podskupa bilo koje grupe. Nadjimo na primer $H_1B.H_1B$.

$$H_1B.H_1B = \{A,\ A^2,\ e\}B.\{A,\ A^2,\ e\}B = \{AB,\ A^2B,B\}\{AB,\ A^2B, B\} =$$

$$= \{ABAB,\ ABA^2B,\ ABB,\ A^2BAB,\ A^2BAB,\ A^2BB, BAB, BA^2B, BB\} =$$

$$= \{e,\ A^2,\ A,\ A,\ e\ A^2,\ A^2,\ A,\ e\} = \{A,\ A^2,\ e\} = H_1.$$

Slično dobijamo $H_1.H_1 = H_1$, $H_1.H_1B = H_1B.H_1 = H_1B$ take da tablica množenja faktor grupa izgleda :

	H_1	H_1B
H_1	H_1	N_1B
H_1B	H_1B	N_1

Najzad, faktor grupa H_1/H_6 ima elemente A, A^2, e . Ona je izomorfna sa H_1.

Zadatak 110. Neka su H i K dve podgrupe grupe G takve da je

1/ $H \cap K = e$, e jednačini element grupe G

2/ $hk = kh$, $\forall k \in K$, $\forall h \in H$.

3/ $G = H.K$, tada

1. $G \cong H \times K$

2. H i K su invarijantne podgrupe grupe G i $G/H \cong K$, $G/K \cong H$.

Rešenje. 1. Prema uslovu 3/ svaki element grupe G se može napisati u obliku h.k, $h \in H$, $k \in K$. Ova reprezentacija svakog elementa je jedinstvena jer $hk = h_1k_1 \Rightarrow h_1^{-1}h = k_1k^{-1} = e$ /zbog 1/ , pa $h = h_1$; $k_1 = k$. Preslikavnje $hk \Leftrightarrow h,k$ označuje izomorfizam $G \cong H \times K$, pa je tvrdjenje 1 dokazano.

2. Ako je h.k bilo koji element grupe G tada je $(h.k)^{-1}H(h.k) = k^{-1}.h^{-1}.H.h.k = k^{-1}Hk = k^{-1}kH = H$, pa je H invarijantna podgrupa grupe G.

Ostali deo tvrdjenja se dokazuje bez teškoća.

Zadatak 111. Svaka Abelova grupa G konačnog reda se može potopiti u grupu u kojoj jednačina $x^2 = a$, za svako $a \in G$, ima rešenja. Proveriti navedeno tvrdjenje.

Primedba. Rešiti analogan problem za opštiju jednačinu, kao na primer $x^n = a$/ $n>1$ prirodan broj /.

Zadatak 112. Ako G/H ima podgrupu K, gde je H reda h, K reda k, onda G ima podgrupu Z reda k.h i $H \subset Z$. Ako je $K \lhd \frac{G}{H}$ tada je $Z \lhd G$. Dokazati.

Zadatak 113. Ako su a i b dva elementa grupe G onda se $a^{-1}b^{-1}ab = [a,b]$ zove komutator elemenata a i b. Ako je $[a,b]$ za sve $a,b \in G$ u centru grupe G, onda se G zove nilpotentna grupa klase 2. Dokazati sledeće tvrdjenje:

Operacija $a * b = [a,b]$ grupe G je asocijativna operacija tada i samo tada ako je G nilpontna grupa klase 2.

Zadatak 114. Naći sve podgrupe za cikličnu grupu reda 12, kompozicione nizove i nizove indeksa.

Rešenje. Kod ciklične grupe sve njene podgrupe su takodje ciklične i normalne su. Neka je generator element a. Tada grupa izgleda:

$$G = \{a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7,\ a^8, a^9,\ a^{10},\ a^{11}, a^{12} = e\}$$

Obrazovanjem skupova potencijala svih članova grupe slično kao u zadatku 109 dobijamo da su sve podgrupe date grupe :

$$H_1 = \{a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7,\ a^8,\ a^9,\ a^{10},\ a^{11},\ a^{12} = e\},$$

$$H_2 = \{a^2,\ a^4,\ a^6,\ a^8,\ a^{10},\ a^{12} = e\},$$

$$H_3 = \{a^3,\ a^6,\ a^9,\ a^{12} = e\}$$

$$H_4 = \{a^4,\ a^8,\ a^{12} = e\}$$

$$H_5 = \{a^6,\ a^{12} = e\}$$

$$H_6 = \{a^{12} = e\}$$

Primetimo da su H_2 i H_3 maksimalne normalne podgrupe za H_1. Podgrupa H_4 je maksimalna normalna podgrupa za H_2. Podgrupa H_5 je maksimalna normalna podgrupa za H_3 i za H_2, a H_6 je maksimalna normalna podgrupa za H_5. Zbog svega ovoga su kompozicioni nizovi:

1/ $H_1 \gg H_2 \gg H_4 \gg H_6$

2/ $H_1 \gg H_2 \gg H_5 \gg H_6$

3/ $H_1 \gg H_3 \gg H_5 \gg H_6$

a nizovi indeksa su respektivno

1/ 2, 2, 3 ; 2/ 2, 3, 2; 3/ 3, 2, 2.

Zadatak 115. Ako je G ciklična grupa reda pq tada ona ima jednu i samo jednu podgrupu reda p. Dokazati.

Rešenje. Neka je $a \in G$ generatorni element grupe G. Tada je $(a^q)^p = a^{pq} = e$, a skup elemenata $\{a^q, a^{2q}, .., a^{pq}\}$ čini podgrupu reda p grupe G. Pokažimo da je to jedina podgrupa reda p. Neka je P izvesna podgrupa reda p grupa G. Kao podgrupa ciklične grupe i P je ciklična grupa. Neka je $a^i \in G$ njen generatorni element. Budući da je $(a^i)^p = e$, imamo $ip \equiv 0 \pmod{pq}$ odakle $i \equiv 0 \pmod{q}$, tj. $i = kq$ / k prirodan broj/.

Dakle, generatorni element pretpostavljene grupe P mora biti oblika $a^{kq} = (a^q)^k$. Medjutim, ovo znači da je generatorni element a^q, pa je tvrdjenje u potpunosti dokazano.

Zadatak 116. Naći sve podgrupe ciklične grupe G reda 30.

Uputstvo. Prema prethodnom zadatku postoji jedna i samo jedna podgrupa ove grupe reda p, gde je p delilac broja 30. Ako je a (G generatorni element grupe G, tada podgrupe grupe G imaju sledeće generatorne elemente:

$a, a^2, a^3, a^5, a^6, a^{10}, a^{15}, a^{30}$.

Zadatak 117. Grupa reda p^2, gde je p prost broj je uvek Abelova. Dokazati.

Rešenje. Za $p = 1$ je tvrdjenje tačno. Neka je $p > 1$. Sa C označimo centar date grupe G, a sa c označimo red centra / broj elemenata centra.

Centar, kao /normalna / podgrupa grupe G, mora imati red koji se sadrži u redu grupe G, tj. u p^2. Tvrdjenje će biti dokazano ako dokažemo da je $c = p^2$, jer onda $G = C$ pa je grupa Abelova.

Ako pretpostavimo $c = p$, onda faktor - grupa G/C je reda p, pa / videti zadatak 103 / G mora biti Abelova.

Medjutim, onda je $G = C$ pa je $c = p^2 \neq p$.

Pretpostavimo $c = 1$. U ovom slučaju $C = \{e\}$. Ako je $a \neq e$ bilo koji element iz G onda njegove klase ekvivalencije za relaciju ρ: $x \rho y \Leftrightarrow \exists s \in G,\ y = s^{-1} xs$ /videti zadatak 59 / ne može imati samo jedan element jer bi onda važilo $a \in C$. Njegova klasa ekvivalencije ne može imati ni p^2 elemenata, jer na primer $e \not\rho a$. Dakle, njegova klasa ekvivalencije, prema zadatku 59, sadrži tačno p elemenata. Ovo važi za $\forall a \in G \ / \ a \neq e \ /$.

Relaciji ρ odgovara razdvajanje grupe G na klase ekvivalencija, a tom razlaganju odgovara izvesna jednakost oblika $p^2 = 1 + \lambda p$ gde je λ broj klasa ekvivalencija koje sadrže po p elemenata. Medjutim, iz $p^2 = 1 + \lambda p$ dobijamo $\frac{1}{p} = p - \lambda$, što je nemoguće jer je $p > 1$. Znači $c \neq 1$.

Uslovi $c \neq 1$, $c \neq p$, c/p^2 daju $c = p^2$ tj. $G = C$, pa je G zaista Abelova grupa.

Zadatak 118. Dokazati da je grupa G reda p^2, gde je p prost broj, rešiva grupa.

Rešenje. Prema zadatku 117, G je Abelova grupa. Zato su joj sve podgrupe normalne podgrupe. Ako je G ciklična grupa sa generatornim elementom a, onda joj se jedan kompozicioni niz

$$G \gg H \gg I$$

gde je $H = \{b, b^2, \ldots, b^p = e;\ b = a^{p-1} \in G\}$ i $I = \{e\}$.

Odgovarajući niz indeksa je p, p, pa je G rešiva grupa jer je ovo niz prostih brojeva.

Ako G nije ciklična grupa, onda u G mora svaki element $a \neq e$ biti reda p. U ovom slučaju G poseduje kompozicioni niz

$$G \gg H \gg I, \quad G = \{a, a^2 \ldots, a^p = e\}, \quad I = \{e\},$$

kome odgovara niz indeksa p, p, pa je G rešiva

Dakle, u svakom slučaju je G rešiva grupa. Na taj način je tvrdjenje dokazano.

Zadatak 119. Ciklična grupa je uvek rešiva grupa. Dokazati.

Zadatak 120. Abelova grupa reda p.q ,gde su p i q prosti brojevi je rešiva grupa.Dokazati.

Zadatak 121. Opisati sve grupe sa 9 elemenata.

Zadtak 122. U grupi G pod komutatorom elemenata a i b nazivamo element $c = a^{-1} b^{-1} ab$. G' / prvi izvod grupe G / je grupa generirana od svih komutatora grupe G. Dokazati da je G' normalna podgrupa grupe G i da je G/G' Abelova grupa.

Rešenje. G' je normalna podgrupa, jer bilo koji unutrašnji automorfizam f : $xf = s^{-1}xs$ prevodi komutator $a^{-1}b^{-1}ab$ u komutator $(af)^{-1} (bf)^{-1} (af) (bf)$, pa zbog toga je $G'f = G'$.

Grupa G / G' je komutativna, jer ako su aG' i bG' bilo koja dva koseta onda je $aG' . bG' = abG' = ab . b^{-1}a^{-1}baG' =$ $= baG' = bG' . aG'$.

Koristili smo činjenicu da je $b^{-1}a^{-1}ba \in G'$.

Zadatak 123. Neka je G' prvi izvod grupe G / videti prethodni zadatak/ . Neka je H normalna podgrupa grupe G, tako da je G/H Abelova grupa. Tada je G' podgrupa za H.

Zadatak 124. Neka je x elelement grupe G. Neka je Nx normalizator za x, tj. skup svih elemenata grupe G koji su permutativni sa x. Neka je Cx ciklična podgrupa grupe G čiji je generatorni element x. Dokazati da je Cx normalna podgrupa za Nx.

Zadatak 125. Neka je G grupa reda p^2, gde je p prost broj. Kog je reda centar ove grupe ?

Zadatak 126. Pokazati da su rešive grupe S_3 i S_4 / simetrične grupe/.

Zadatak 127. Grupa G reda p^2, gde je p prost broj je ciklična ili izomorfna sa direktnim proizvodom dve ciklične grupe. Dokazati.

Rešenje. Prema zadatku 117 grupa G mora biti Abelova grupa. Ako je G ciklična onda je tvrdjenje dokazamo. Neka G nije ciklična. Neka je $a \neq e$ izvestan element grupe G. Skup svih njegovih potencija $H = \{ a, a^2, \ldots, a^p = e \}$ je normalna podgrupa reda d grupe G. Faktor - grupa G/H je reda p, pa mora biti cikličan. Neka je Hb /b $\in$ G / generatorni element ove grupe / $b \neq e$ i $b^p =$ Tada ma koji element . grupe G ima jednoznačnu reprezentaciju u obliku $a^{\ell} b^m$ / $0 \leq \ell$, $m < p$ /, pa je G izomorfna grupa $C_p \times_p C_p$, gde C_p označuje cikličnu grupu reda p.

Zadatak128. Neka je G Abelova grupa i neka je H podgrupa grupe G. Pokazati da grupa G ima bar jednu podgrupu izomorfnu sa G/H.

Zadatak 129. Neka su H i K maksimalne invarijantne podgrupe za G, neka $H \neq K$ i $D = H \cap K$. Tada je $G/H \cong K/D$, $G/K \cong H/D$.

Zadatak 130. Neka je G konačna grupa, N njena normalna podgrupa. Neka su N i G/N rešive grupe. Pokazati da je G grupa rešiva.

Zadatak 131. Formirati bar jednu grupu čiji svi elementi csim e imaju red p, gde je p zadan prost broj.

Rešenje. Ovu osobinu ima grupa $C_p \times C_p$, gde je C_p ciklična grupa reda p.

Zadatak 132. Neka su A i B dve date grupe. Grupa G se zove ekstenzija grupe A pomoću grupe B, ako G ima normalnu podgrupu A' izomorfnu sa A i ako je $G/A' \cong B$. Dokazati da A i B ne odredjuju jednoznačno grupu G.

Rešenje. Ako su A i B ciklične grupe reda 2 onda i ciklična grupa reda 4 i Klein - ova vierer - grupa su ekscenzije grupe A pomoću grupe B.

Zadatak 133. Neka su H_1 i H_2 normalne podgrupe grupe G i neka je H_2, H_1 tako da je H_1/H_2 normalna podgrupa za G/H_2. Dokazati da je kvocijent grupa grupe G/H_2 prema podrgupi H_1/H_2 izomorfna sa G/H_1.

Zadatak 134. Ako je red grupe paran broj tada jednačina $x^2 = e$ u ovoj grupi ima bar dva rešenja. Dokazati.

Zadatak 135. Dokazati da je aditivna grupa R racionalnih brojeva jedina grupa sa svojstvima: 1/ R je Abelova, 2/ R je beskonačna, 3/ svaki endomorfizam je ili automorfizam ili preslikavanje na nul - element.

Zadatak 136. Dokazati da svaka grupa sa više od dva elementa ima bar jedan automorfizam različit od identičnog preslikavanja.

Zadataka 137. Ako je G grupa bez centra / tj. centar sadrži samo e / onda je i grupa automorfizama ove grupe takodje bez centra. Dokazati.

Zadatak 138. Dokazati da aditivna grupa racionalnih brojeva nema ni jednu pravu podgrupu konačnog indeksa.

Zadatak 139. Neka je G grupa reda $m \cdot n$, takva da G ima normalnu podgrupu H koja je ciklična i reda m. Neka je G/H ciklična grupa.

Tada G može biti generirana sa dva elementa a i b takva da je $a^m = e$, $b^n = a^r$, $ba = a^s b$, gde su r i s celi brojevi takvi da su brojevi $r/s - 1$ i $s^n - 1$ multipli broja m. Dokazati.

Rešenje. Za a uzmimo jedan od generatornih elemenata podgrupe H. Pošto je G/H ciklična grupa, to bar jedan koset Hb ($b \notin H$) je generatorni element te grupe. Neka Hb označuje jedan odredjen generatorni element grupe G/H.

Na taj način smo izabrali a i b. Ma koji element grupe G je u izvesnom kosetu $(Hb)^k = Hb^k$, pa svaki element grupe G je oblika $a^\ell b^k$ / $0 \leq \ell < m$, $0 \leq k < n$ / jer su elementi iz H oblika a^ℓ / $0 \leq \ell < m$ / . Na taj način je dokazano da su a i b generatorni elementi grupe G. Dokazaćemo da a i b ispunjavaju i ostali deo tvrdjenja.

Pošto je $(Hb)^n = H$, to je $b^n \in H$, odnosno postoji takav broj r / $0 \leq r < m$ / da je $b^n = a^r$. Budući da je

H normalna podgrupa grupe G to $bHb^{-1} = H$, pa odavde $bab^{-1} \in H$, tj. $bab^{-1} = a^s$, gde je s odredjen broj /$0 \leq s < m$/. Kako je jasno da je $a^m = e$, ostaje još da se dokažu jednakosti $r(s-1) \equiv 0 \pmod m$ i $s^N - 1 \equiv 0 \pmod m$.

Iz jednakosti $bab^{-1} = a^s$ uzimanjem r - tih potencija obe strane imamo $ba^r b^{-1} = a^{sr}$, što prema $a^r = b^n$ daje $b^n = a^{sr}$, odnosno $a^r = a^{sr}$. Iz $a^r = a^{sr}$ dobijamo $a^{s(r-1)} = e$, odakle $s(r-1) \equiv 0 \pmod m$.

Na Sličan način ulimanjem s - tih potencija jednakost $bab^{-1} = a^s$ daje $ba^s b^{-1} = a^{s^2}$, a obe zajedno daju $b^2 ab^{-2} a^{s^2}$. Indukcijom se može lako dokazati da je uopšte $b^x ab^{-x} = a^{s^x}$ za svaki prirodan broj x.

Uzimajući $x = n$, prema $b^n = a^r$ dobijamo a^{s^n} da je jedanko a, odakle je $a^{s^n - 1} = e$. Najzad $a^{s^n - 1} =$ daje $s^n - 1 \equiv 0 \pmod m$, pa je tvrdjenje u potpunosti dokazano.

Zadatak 140. Neka je $(R, *)$ grupa, gde je R skup realnih brojeva. Ako je funkcija $F(x,y) = x * y$ neprekidna po x i y onda postoji neprekidna permutacija f skupa R, takva da je $f(x+y) = f(x) * f(y)$, $\forall\, x, y \in R$.

Rešenje. Pokažimo prethodno da je F/x,y/ strogo monotona po x i strogo monotona po y. Neka $a < b$, tada je $e * a < e * b$, gde je e jedinični element grupe $(R, *)$. Ako bi za neko c bilo $c * a \geq c * b$, tada iz $e * a < e * b$, $c * a \geq c * b$, zaključujemo, prema pretpostavci neprekidnosti, egzistenciju broja d takvog da je $d * a = d * b$. Medjutim, odavde $a = b$, što je nemoguće, Znači : $a < b \Rightarrow c * a < c * b$, $\forall\, c \in R$, pa je funkcija F/x,y/ rastuća po y. Slično dokazujemo da je rstuća i po x.

U daljem rasudjivanju, polazeći od funkcionalne jednačine

1/ $\quad f(x+y) = f(x) * f(y)$

konstruisaćemo jedno njeno rešenje f /x/ koje će zadovoljiti uslove tvrdjenja koje dokazujemo.

Za $y = x$, /1/ daje : $f/2x/ = f^2/x/$ i slično

2/ $f/nx/ = u^n$

/ $u = f/x/$, n prirodan broj / . Definišimo $f/1/ = d$ gde je d izvestan broj veći od e. Tada /2/ daje $f/n/ = d^n$.

Funkcija $g/u/ = u^n$ je neprekidna i strogo monotona po u, za svako u. Zbog ovoga, jednačina $u^n = d$ ima jednistveno rešenje u_n.

Uvedimo $u_n = f(\frac{1}{n})$. Ako je dalje, $\frac{m}{n}$ bilo kakav pozitivan broj onda uvodimo $f(\frac{m}{n}) = f^m(\frac{1}{n})$.

Funkcija f /x/ je na taj način definisana na skupu Ra(+) , pozitivnih racionalnih brojeva. Ako su $\frac{m}{n}$, $\frac{p}{n} \in$ Ra(+), onda

$$f(\frac{m}{n} + \frac{p}{n}) = f(\frac{m+p}{n}) = f^{m+p}(\frac{1}{n}) = f^m(\frac{1}{n}) \cdot f^p(\frac{1}{n}) = f(\frac{m}{n}) \cdot f(\frac{p}{n}),$$

pa f/x/ zadovoljava /I/ na skupu Ra .

Funkcija f/x/ je strogo monotona na skupu Ra (+) . Zaista, prvo $f(\frac{1}{n}) > e$, jer $f(\frac{1}{n}) \leq e$ daje $f/1/ \leq e^n = e$, što suprotno definiciji da je $f/1/ > e$. Zbog ovoga

$f(\frac{m+1}{n}) = f(\frac{m}{n}) \cdot f(\frac{1}{n}) > f(\frac{m}{n})$, /m,n $\in$ N / , pa ako je $\frac{p}{q} > \frac{r}{s}$ sigurno je $f(\frac{p}{q}) > f(\frac{r}{s})$ / $\frac{p}{q}$, $\frac{r}{s} \in$ Ra (+) /. Na taj način f/x/ je rastuća na Ra (+) . Za x = 0 uvodimo f/0/ = e što je u skladu sa jednačinom /1/.

Neka sada x bude bilo koji pozitivan realan broj. Prema Dedekindu x je odredjeno kao presek dve klase $\{r_n\}$ i $\{R_n\}$, $r_n < x < R_n$ racionalnih brojeva. Uvedimo definiciju: $f/x/ = \lim_{n\to\infty} f(r_n) = \lim_{n\to\infty} f(R_n)$. Ova definicija je, kao što se lako zaključuje jednoznačna jer uvedene granične vrednosti postoje i jednake su. Na ovaj način

$f/x/$ je definisana za $x \geq 0$. Za $x < 0$ uvedimo definiciju: $f/x/ = f^{-1}/-x/$. Funkcija $f/x/$ je na taj način definisana za svako x. Čitalac će lako proveriti da je $f/x/$ neprekidna rastuća funkcija / dakle, sigurno neprekidna permutacija/ i da $f/x/$ zadovoljava jednačinu /1/ Na taj način, $f/x/$ postoji pa je tvrdjenje u potpunosti dokazano.

Primedba : Detaljnije o ovome videzi u knjizi : Vorlessungen uber Funtionalgleichungen und ihre Auwendungen J. Aczel-a /Basel - Stuttgard 1961 godine/. 72, 73, 75 82, 91(A)

III PRSTENI, DOMENI I POLJA. TEORIJA GALOIS-A

Zadatak 1. Neka je S skup svih realnih neprekidnih funkcija $f/x,y/$. U S definisane su operacije + i . na sledeći način:

$(f+g)(x,y) = f/x,y/ + g/x,y/$, $(f \cdot g)(x,y) = \int_0^1 f/x,t/ . g/t,y/ dt$ $/f,g \in S/$. Ispitati da li je $(S, +, .)$ prsten.

Rešenje. Operacije + i . su unutrašnje operacije skupa S. Sistem $(S,+)$ je grupa jer

1/ + je asocijativna operacija,

2/ funkcija $0: /x,y/ \to 0$ je neutralni element,

3/ za $f/x,y/$ suprotan element je $-f/x,y/$.

Grupa $(S,+)$ je Abelova jer je $f/x,y/ + g/x,y/ = g/x,y/ + f/x,y/$ $/ \forall f, g \in S /$.

Sistem $(S,\cdot)$ je semigrupa jer je . asocijativna operacija kao što se vidi iz sledećeg:

$$\left[(fg)h\right](x,y) = \int_0^1 (fg)(x,t)h(t,y)dt = \int_0^1 \left(\int_0^1 f(x,\zeta)g(\zeta,t)h(t,y) d\zeta\right) dt = \iint_{0\le t,\, 1>\zeta} f(x,\zeta)g(\zeta,t)h(t,y)\, d\zeta\, dt = \int_0^1 f(x,\zeta)\left(\int_0^1 g(\zeta,t)h(t,y)\, dt\right) d\zeta = \int_0^1 f(x,\zeta)(gh)(\zeta,y)\, d\zeta = \left[f(gh)\right](x,y)$$

$/ \forall f,g,h \in S /$.

Budući da je

$$\left[f/g+h/\right](x,y) = \int_0^1 f(x,t)\left[g(t,y) + h(t,y)\right] dt = \int_0^1 f(x,t)g(t,y)dt +$$

$$+ \int_0^1 f(x,t)\, h(t,x)\, dt = \left[f.g+f.h\right](x,y),$$

$$\left[(g+h)\, f\right](x,y) = \int_0^1 \left[g(x,t) + h(x,t)\right] f(t,y)\, dt = \int_0^1 g(x,t)f(t,y)dt +$$

$$+ \int_0^1 h(x,t)\, f(t,y)\, dt = \left[g.f + h.f\right](x,y)$$

za svako $f,g\ h \in S$, zaključujemo da je množenje distribudivno prema sabiranju.

Znači $(S,+,\cdot)$, jeste prsten.

Zadatak 2. Ispitati da li je $(S,+,\cdot)$ prsten u sledećim slučajevima:

1/ S je skup svih parnih brojeva, + i · su obično sabiranje odnosno množenje.

2/ S je skup svih brojeva oblika $a + b\sqrt{2}$ /a,b celi brojevi , + i . su obično sabiranje i množenje.

3/ S je skup svih matrica oblika $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ /a, b, c celi brojevi /, + i · su sabiranje i množenje matrica.

4/ S je skup svih uredjenih parova realnih brojeva, + i · su operacije definisane na sledeći način:

$$(a,b + (A,B) = (a+ A, b+ B)$$

$$(a,b) \cdot (A,B) = (aA+ bB, aB+bA).$$

5/ S je skup svih realnih neprekidnih funkcija f /x/, a + i· su definisane na sledeći način

$$(f+g)(x) = f/x/ + g/x/$$

$$(f\cdot g)(x) = f\left[g/x/\right] .$$

6/ S je skup svih realnih funkcija f/x,y / a + i · su definisane pomoću jednakosti.

$$(f+g)(x,y) = f/x,y/ + g/x,y/$$

$$(f\cdot g)(x,y) = f\left[g/x,y,\ g/x,y/\right] .$$

Zadatak 3. Neka je S jedan skup i neka su $\emptyset$, X, Y, Z,. . .,S njegovi podskupovi. Sa X' označimo komplement skupa X. U skupu P(S) = $\emptyset$, X, Y, Z,..., S svih podskupova skupa S sabiranje i množenje pomoću:

$$X\cdot Y = X \cap Y$$

$$X+Y = (X \cap Y') \cup (Y \cap X')$$

1/ Pokazati da je (P (S), + , .) prsten.

2/ Pokazati da je $X^2 = X$ / tj.prsten je Boole-ov/ .

Rešenje. Operacija + je ustvari simetrična razlika skupova. Ova je operacija unutrašnja operacija skupa P(S). Asocijativnost ove operacije smo dokazali u zadatku 4 I glave.

Ona je komutativna. Element $\emptyset \in P(S)$ je jedinični element operacije + jer je $X + \emptyset = \emptyset + X = (X \cap \emptyset') \cup \emptyset \cap X') =$ $X \cap S = X$ / $\forall X \in P(S)$ /. Elelement X' je inverzan element elelmenata X jer je $X + X' = X' + X' = (X \cap X') \cup (X \cap X') =$ $\emptyset \cup \emptyset = \emptyset$.

Znači (S,+) je Abelova grupa.

Operacija · je unutrašnja operacija skupa P (S) . Ona je komutativna i asocijativna operacija.Pošto je

$$X.Y + X.Z = X \cap Y + X \cap Z = \left[(X \cap Y) \cap (X \cap Z)\right] \cup \left[(X \cap Y) \cap (X \cap Z)'\right] =$$

$$= \left[(X' \cup Y') \cap (X \cap Z)\right] \cup \left[(X \cap Y) \cap (X' \cup Z')\right] = \left[(X' \cap X \cap Z) \cup (Y' \cap X \cap Z)\right] \cup$$

$$\cup \left[(X \cap Y \cap X') \cup (X \cap Y \cap Z')\right] = \left[X \cap Y' \cap Z\right] \cup \left[X \cap Y \cap Z'\right] = X \cap \left[(Y \cap Z) \cup (Y \cap Z')\right] =$$

$$= X \cdot (Y + Z) \quad / \forall X, Y, Z \in S /$$

Zaključujemo da je operacija . levo distributivna prema operaciji + . Pošto je · komutativna to je ispunjen i desni distributivan zakon operacije · prema operaciji + .

Na taj način je (P S) , + , ·) zaista prsten.

2/ Pošto je $X \cap X = X$ / $\forall X \in P(S)$ / to je $X^2 = X$ / $\forall X \in P(S)$ /, pa je tvrdjenje u potpunosti dokazano.

Primedba. Navedena teorema je jedan od dveju teorema Stone-a koje dokazuju ekvivalenciju Boole-ove algebre i Boole-ovog prstena sa jediničnim elementom.

Zadatak 4. Neka je (P,+,) prsten sa jediničnim elementom e . Dokazati da je (P,⊕ ,⊙) takodje prsten gde su ⊕ i ⊙ definisane sa

$x \oplus y = x + y + e$, $x \odot y = xy + x + y$ / $x,y \in P$ / .

Dokazati relaciju $(P,+,\cdot) \cong (P, \oplus, \odot)$.

Zadatak 5. U integralnom domenu važe jednakosti:

1/ $a \cdot 0 = 0$ 4/ $/-a/\ b = -ab$

2/ $-/a+b/ = /-a/ + /-b/$ 5/ $/-a/\ /-b/ = ab$

3/ $-a = /-1/a$ 6/ ako je $c \neq 0$ i $ca = cb$ onda je $a = b$

Rešenje. 1/ Primetimo da je $a \cdot (a + 0) = a \cdot a + a \cdot 0$ i da je $a.(a + 0) = a \cdot a + 0$, pa je $a \cdot a + a \cdot 0 = a \cdot a + 0$, a odavde $a \cdot 0 = 0$.

2/ Sa $-\alpha$ se po konvenciji označuje element inverzan elementu u odnosu na sabiranje tj. $\alpha + (-\alpha) = 0$ .Kako je sa jedne strane $(a + b) + [-(a + b)] = 0$, a sa druge strane $(a + b) + [(-a) + (-b)] = a + (-a) + b + (-b) = 0 + 0 = 0$ to je $(a + b) + [-(a+b)] = (a + b) + [(-a) + (-b)]$. Dodajući na obe strane $-(a + b)$ dobijemo jednakost 2 / :

$$-(a + b) = (-a) + (-b)$$

3/ Iz $a + (-1)a = 1 \cdot a + (-1)a = [1 + (-1)]a = 0 \cdot a = a \cdot 0 = 0$ sledi $(-1)a = -a$.

4/ Slično $ab + (-a)b = [(a + (-a)]b = 0 \cdot b = b \cdot 0 = 0$, pa je $(-a)b = -ab$.

5/ Koristeći predjašnju jednakost dobijamo:

$(-a)(-b) = -\left[a(-b)\right] = -\left[(-b)a\right] = -\left[-ba\right] = -\left[-ab\right] = ab$

jer je uvek $-(-\alpha) = \alpha$ pošto $(-\alpha) + \alpha = 0$, tj. α je inverzni za $-\alpha$ u odnosu na sabiranje.

6/ Neka je $ca = cb$ i $c \neq 0$. Odavde $ca + (-c)b = 0$, tj. $0 = ca + c(-b) = c\left[a + (-b)\right]$. Pošto je $c \neq 0$, ne može biti i $a + (-b) \neq 0$ jer bi $c\left[a + (-b)\right]$ bilo različito od 0 što ovde nije. Znači $a + (-b) = 0$ pa je $a = b$.

Primedba. Jednakosti 1/, 2/, 4/ i 5/ važe i u svakom prstenu.

Zadatak 6. Prsten P se zove Boole-ov ako su mu svi elementi idempotentni. Dokazati da je Boole-ov prsten karakteristike ili 1 ili 2 i da je komutativan.

Rešenje. Ako P ima samo jedan element onda je karakteristika 1 i ispunjava sve navedene uslove.

Neka P ima bar dva elementa. Tada

$a,b \in P \Rightarrow (a + b)^2 = a^2 + b^2 + ab + ba \Rightarrow a + b + a + b + ab + ba \Rightarrow$

$ab + ba = 0$.

Odavde za $b = a$ dobijamo $a + a = 0$ / $\forall a \in P$/, pa je P karakteristike 2. Medjutim onda je i $ab + ab = 0$ pa

$ab + ba = 0 \Rightarrow ab + ba + ab = ab \Rightarrow ba = ab$ / $\forall a,b \in P$/, što znači da je P komutativan.

Na taj način je tvrdjenje u potpunosti dokazano.

Zadatak 7. Ispitati da li je navedenim Cayley-evim tablicama definisana prsten.

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

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

Zadatak 8. Ispitati da li skup svih realnih linearnih funkcija $ax + b$ čini prsten u odnosu na operaciju X i $\cdot$ definisane sa :

$$(ax + b) + (cx + d) = (a+c) x + (b + d),$$

$$(ax + b) \cdot (cx + d) = acx + (ad + b) .$$

Zadatak 9 . U skupu N prirodnih brojeva definisati operaciju $\oplus$ i $\odot$, tako da $(N, \oplus , \odot)$ bude a / prsten b / polje.

Zadatak 10. Neka su a i b dva permutativna elementa prstena karakterisike 2. Dokazati da je

$$(a + b)^2 = (a - b)^2 = a^2 + b^2 = a^2 - b^2.$$

Zadatak 11. Ako u aditivnoj Abelovoj grupi $(G,+)$ uvedemo operaciju množenja pomoću $a \cdot b = 0$ za sve $a,b \in G$ onda je $(G, +,\cdot)$ prsten. Dokazati.

Zadatak 12. Ispitati skup Z celih brojeva u odnosu na operacije $\oplus$ i $\odot$ definisane pomoću

$$a \oplus b = a + b + 2, \quad a \odot b = 2a + 2b + ab + 2$$

Da li je $(Z, + , \cdot) \cong (Z, \oplus , \odot)$?

Zadatak 13. Ako u prstenu P karakteristike 2 važi $(a + b)^2 = a^2 + b^2$ za sve $a \; b \in P$ onda je psten komutativan. Dokazati.

Zadatak 14. U nekomutativnom prstenu P definišimo operaciju + pomoću $x * y = xy - yx$.

a/ Pokazati da je $*$ distributivna prema sabiranju.

b/ Pokazai

$$x * (y * z) + y * (z * x) + z * (x * y) = 0$$

/Jacobi-ev identitet/.

Zadatak 15. Neka je $(P,+,\cdot)$ prsten u kome postoji jedan element c osobine:

1/ $\quad ca = cb \Rightarrow a = b$

Dokazati da je u ovakvom prstenu aksioma

2/ $\quad a + b = b + a \qquad \forall a, b \in P$

posledica ostalih aksioma iz (P,+,·)

Rešenje. Bez aksioma /2/ se u prstenu (P,+,·) izvode tvrdjenja: a(-b) =(-a) b = -(ab), $\forall a, b \in P$, pa ih u daljem izvodjenju koristimo.

Kako je : $c\left[-(a+b)\right] = (-c)(a+b) = (-c)a + (-c)b = c(-a) + c(-b) = c\left[(-a)+(-b)\right]$, prema /1/ imamo $-(a+b) = (-a)+(-b)$, $\forall a, b \in P$.

Odavde $-\left[-(a+b)\right] = -\left[(-a)+(-b)\right]$, pa prema osobinama grupe (P,+) /$-(p+q) = (-p)+(-q)$, $-(-p) = p$, $\forall p,q \in P$ /, imamo

$$a + b = b + a , \quad \forall a,b \in P .$$

Zadatak 16. Neka je S skup svih uredjenih p arova celih brojeva. U ovom definišimo operacije +,·, $\ast$ pomoću:

$$(a,b) + (a',b') = (a + a', b + b')$$

$$(a,b).(a',b') = aa' + 2bb', ab' + ba')$$

$$(a,b) \ast (a',b') = (aa' + 3bb', ab' + ba').$$

1/ Pokazati da su (S,+,·) i (S,+,$\ast$) prsteni.

2/ Pokazati da ti prsteni nisu izomorfni.

Zadatak 17. Skup brojeva $S = \{a + b\sqrt{3}\}$, gde su a i b celi brojevi čini integralni domen.

Rešenje. Integralni domen je skup S elemenata snabdeven dvema operacijama sabiranjem i množenjem koji:

1/ U odnosu na sabiranje čini Abelovu grupu.

2/ U odnosu na množenje ispunjava zahteve:

a/ ako $a \in S$, $b \in S$ onda $a \cdot b \in S$

b/ako je $a \neq 0$, $b \neq 0$ onda je $ab \neq 0$. Element 0 je jedinični element za sabiranje.

c/ ab = ba

d/ (ab) c = a(bc)

e/ Postoji $1 \neq 0$ takav da je $a.1 = a$ za $a \in S$.

3/ Važi distributivni zakon

$$a.(b + c) = a.b + a.c.$$

Neka $a + b\sqrt{3}, c + d\sqrt{3} \in S$, tada je

$(a+ b\sqrt{3}) +(c + d\sqrt{3}) = (a+ c)+(b + d)\sqrt{3} \in S$ i

$(a+ b\sqrt{3}).(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3} \in S$ jer zbir i proizvod celih brojeva je ceo broj. Asocijativni i komutativni zakon za sabiranje i množenje su ispunjeni. Distributivni zakon je ispunjen. Jedinični element za sabiranje je $0 = 0 + 0\sqrt{3}$ (S a za množenje je $1 = 1 + 0\sqrt{3} \in S$. Inverzni element elementu $a + b\sqrt{3}$ za sabiranje je $(-a) + (-b)\sqrt{3} \in S$. Neka $a + b\sqrt{3} \neq 0$, $c + b\sqrt{3} \neq 0$ tada je $(a+ b\sqrt{3}).(c + d\sqrt{3}) \neq 0$. Znači zaista S je integralni domen.

Zadatak 18. Neka je S skup svih brojeva oblika $\frac{a}{2} + \frac{b}{2}\sqrt{-3}$ gde su a, b celi brojevi. Da li je $(S,+,\cdot)$ integralni domen?

Zadatak 19. Sistem ostataka J_p po modulu p, gde je p prost broj u odnosu na operacije sabiranje i množenje čini polje.

Rešenje. U sistemu ostataka se sabiranje i množenje definišu sa $a'+ b' = (a+b)'$, $a'.b' = (ab)'$ .Da bi smo dokazali da je J_p polje treba da dokažemo

1/ Da je J_p Abelova grupa u odnosu na sabiranje.

2/ Da je skup J_p bez jediničnog elementa za sabiranje Abelova grupa u odnosu na množenje.

3/ Da važi distributivni zakon množenja prema sabiranju.

Akc $a',b' \in J_p$ onda $a'+ b' \in J_p$. Za sabiranje važi asocijativni zakon jer $(a'+b') + c' = (a+b)' + c' = [(a+b)+c]' =$
$= [a +(b + c)]' = a'+ (b+c)' = a'+(b'+ c')$.

Element $0'$ je jedinični za sabiranje,jer $a'+ 0' =$
$= (a+ 0)' = a'$.

Ma koji element a' ima inverzni, to je (-a)' . Znači J_p je aditivna Abelova grupa jer važi i komutativni zakon. Neka je J_p skup 1', 2',... , (p-1)'. Ako $a' \in J_p$, $b' \in J_p$ onda je a'.b' = (ab)' $\neq$ 0' jer ako bi bilo (ab)' = 0' imali bismo p/ab, odakle pošto je p prost broj je p/a ili p/b tj. a'= 0' ili b'= 0' što po pretpostavci nije. Znači a'.b' = (ab)' (J_p. Za množenje je ispunjen asocijativni zakon jer je

(a'.b').c' =(ab)'.c'= $\left[(ab)c\right]'$= $\left[a(bc)\right]'$= a'.(bc)'=a'(b'c').

Element 1' je jedinični element za množenje jer je a'.1' = (a.1)' = a'. Neka je $a' \in J_p$ ma koji.Pošto/a,p/=1 to jednačina ax = 1(mod p) ima jedno rešenje x = q . Za element a' je q' inverzan u odnosu na množenje,jer je a'.q' = (aq)' = 1', a naravno $q' \in J_p$. Pošto je a'b' = =(ab)'= (ba)'= b'a' to je zaista J_p Abelova multiplikativna grupa. Najzad, ispunjen je i distributivni zakon jer je a'.(b'+ c') = a'.(b+ c)' = $\left[a.\ (b+\ c)\right]'$ =(ab+ ac)'=(ab)+(ac)'= a'b'+ a'c' , pa je dokaz završen.

Primetimo da ako p nije prost broj onda J_p nije polje,već samo prsten. Dovoljno je primetiti samo to što ako je p = ℓ . k gde je $|\ell| \neq 1$, $|k| \neq 1$ onda je 1'.k' = =(ℓk)' = p' = 0' iako i $\ell' \neq 0'$ i $k' \neq 0'$ pa J_p nije polje. U odnosu na množenje podskup $\{1',\ a',\ b',\ \ldots,(p-1)'\}$ skupa J_p čini grupu ako su brojevi 1, a, b, ...,(p-1)relativno prosti sa p i ako ovaj podskup sadrži sve takve elemente.

Na primer za $J_6 = \{0',\ 1',\ 2',\ 3',4'\ ,\ 5',\}$ ta grupa ima elemente 1' i 5'.

Zadatak 20. Neka je C skup svih realnih neprekidnih funkcija definisanih na $[0.1]$. U C дефинисати на следећи начин :

$$+ :\ (f + g)(x) = f/x/ + g/x/$$
$$.:\ (f\cdot g)(x) = f/x/\ .\ g/x/.$$

Dokazati da (C,+,·) nije integralni domen,ali da jeste prsten.

Uputstvo. Da (C,+,·) nije integralni domen zaključujemo na sledeći način. Ako je

$$f(x)=\begin{cases}0 & 0\le x\le \frac{1}{2}\\ x-\frac{1}{2} & \frac{1}{2}<x\le 1\end{cases} \quad \text{i} \quad g(x)=\begin{cases}\frac{1}{2}-x & 0\le x\le \frac{1}{2}\\ 0 & \frac{1}{2}<x\le 1\end{cases}$$

onda je $f(x)\cdot g(x)=0 \quad /0\le x\le 1/.$

Zadatak 21. Neka je S skup svih uredjenih trojki realnih brojeva. Neka su u S definisane operacije + i · na sledeći način :

$$(a,b,c)+(A,B,C)=(a+A,\ b+B,\ c+C)$$

$$(a,b,c)\cdot(A,B,C)=(bC-Bc,\ cA-Ca,\ aB-bA).$$

Dokazati da (S,+, ·) ispunjava sve aksiome prstena izuzev asocijativnosti za množenje.

Primedba. Navedeni primer dokazuje nezavisnost aksiome asocijativnosti množenja kod prstena od ostalih aksioma prstena.

Zadatak 22. U prstenu Z celih brojeva definišimo operacije $\oplus$ i $\odot$ pomoću

$$a\oplus b=a+b+1$$

$$a\odot b=ab+a+b$$

Dokazati da su (Z,+,·) i (Z,$\oplus$, $\odot$) izomorfni prsteni.

Rešenje. Uvedimo preslikavanje φ pomoću jednakosti

$$a\varphi=a+1$$

/a je ceo broj/. Ovo preslikavanje je izomorfizam navedenih struktura jer je :

$$(a\odot b)\varphi=a\oplus b+1=a+b+2=a\varphi+b\varphi$$

$$(a\odot b)\varphi=a\odot b+1=ab+a+b+1=(a+1)(b+1)=a\varphi\cdot b\varphi$$

/a, b su celi brojevi/.

Na taj način je tvrdjenje dokazano jer je (Z,+,·) prsten.

Zadatak 23. Neka je S skup svih uredjenih trojki racionalnih brojeva. Neka je u s definisano sabiranje:

$$(a_1,b_1,c_1) + (a_2,b_2,c_2) = (a_1+a_2,\ b_1+b_2,\ c_1+c_2)$$

i množenje:

$$(a_1,b_1,c_1)\cdot(a_2,b_2,c_2) = (a_1c_2+b_1b_2+c_1c_2,\ 2a_1a_2+b_1c_2+$$

$$+b_2c_1,\ 2b_1a_2+2a_1b_2+c_1c_2)\ .$$

Da li je (S,+ ,·) polje ?

Zadatak 24. Da li se u datom skupu S mogu definisati operacije + i · tako da oba sistema (S, + , ·) i (S, · , +) budu prsteni ?

Rešenje. Ako S ima samo jedan element a, onda se + i · moraju definisati jednakostima a + a = a.a = a . Neposredno se može proveriti da je (S,+, ·) kao i (S, ·, +) prsten . Znači u ovom slučaju je odgovor potvrdan.

Neka S ima više od jednog elementa. Ako su (S,+, ·) i (S, ·, +) prsteni onda (S, +) i (S,·) moraju biti Abelove grupe. Ako je 0 jedinični element prve grupe, onda prema osobinama prstena, mora biti $x.0_+ = 0_+$ za $\forall\ x \in S$, pa (S,·) ne može biti grupa, jer bi inače $x.0_+ = 0_+.0_+ \ /\forall x \in S\ /$ povuklo $x = 0_+\ /\ \forall x \in S/$, što se kosi sa pretpostavkom da S ima više od jednog elementa.

Zadatak 25. Ako su $(P_1, +,\cdot)$ i $(P_2,+,\cdot)$ prsteni tada je sistem $(P_1 \times P_2, +,\cdot)$ prsten u kome su operacije + i · definisane na sledeći način

$$(a_1,a_2) + (b_1,b_2) = (a_1+b_1,\ a_2+b_2)$$

$$(a_1,a_2).(b_1b_2) = (a_1.b_1,\ a_2.b_2)\ /a_1,b_1, \in P_1 : a_2,b_2 \in P_2\ .$$

Ako su $(P_1,+,\cdot)$ i $P_2, +, \cdot)$ tela onda $P_1 \times P_2, +, \cdot)$ nije telo. Dokazati navedena tvrdjenja.

Primedba . Prsten $(P_1 \times P_2.+,\cdot)$ se zove direktan proizvod prstena $(P_1, +,\cdot)$ i $(P_2,+ \cdot)$.

Zadatak 26. formirati direktan proizvod prstena $(J_3,+ ,\cdot)$ i prstena $(J_4, + ,\cdot)$. Da li važi relacija

$$(J_{12}, + ,\cdot) \cong (J_3 \times J_4,+ ,\cdot) ? .$$

Zadatak 27. Ako su H_1 i H_2 redom podprsteni prstena P_1 i P_2 da li je podprsten $H_1 \times H_2$ podprsten $P_1 \times P_2$? .

Zadatak 28. Dokazati ako su P_1 i P_2 prsteni, da su onda prsteni $P_1 \times P_2$ i $P_2 \times P_1$ izomorfni.

Zadatak 29. Neka je P prsten sa jediničnim elementom. Ako je (P, +) ciklična grupa onda je prsten (P,+, ·) izomorfan ili sa (Jm,+ ,·) ili sa (Z, +,·). Dokazati.

Rešenje. Razlikujemo dva slučaja prema tome da li P ima konačno elemenata ili ima beskonačno- elemenata. Ako P ima m elemenata 0, e, a_3, a_4,... , a_m onda jednakost $\ell e = ke$ / $0<k\leq \ell\leq m$/ provlači $\ell = k$. Neka obrnuto $\ell > k$. iz $\ell e = ke$ sleduje / $\ell -k/e = 0$, odakle /$\ell -k/a = 0$ gde smo sa a označili generatorni element grupe (P,+) . Pošto je $0 <\ell -k< m$, a $\omega(a) = m$ zaključujemo da je jdnakost $(\ell -k)a=0$ nemoguća.

Prema dokazanom elementi prstena P su sledeći:

e, 2e, 3e, ...,me = 0 . Zakon x.(y + z) = x.y + x.z / $\forall x , y, z \in P$ / nam daje (ie) . (je) = (ij) e , pa za P sabiranje i množenje su definisane na sledeći način: ie + je = (i + j)e, (ie)(je) =(ij)e. Otuda je $(P,+,\cdot) \cong (Jm, + ,\cdot)$. Tako da je u ovom slučaju tvrdjenje dokazano.

Ako P ima beskonačno elemenata,onda pošto je(P, +) ciklična grupa,tih elemenata ima prebrojivo mnogo.Ako je e $\in$ P jedinični element onda jednakost $\lambda e = \mu e / \lambda, \mu \in Z$ /

povlači $\lambda = \mu$ jer u obrnutom slučaju postoji broj $k \neq 0$, takav da je $ka = 0$ /a generatorni element grupe $(P,+)$ • /, pa je broj elemenata grupe $(P,+)$ konačan.

Ako stavimo $e = \mu a$, $a^2 = \delta a$ / μ i δ izvesni celi brojevi/ onda jednakost $ae = a$ daje $\mu\delta = 1$ pa je $\mu = \pm 1$. Znači e može biti generatorni element prstena P. Elementi prstena P su oblika ie / $i \in Z$ /. Zakon $x.(y + z) = x.y + x.z$ / $\forall\ x,y,z \in P$ / nam govori da je $(ie).(je) = (ij)e$ / $i,j \in Z$ /, pa su sabiranje i množenje u prstenu P definisane na sledeći način :

$ie + je = (i + j)e$, $(ie).(je) = (ij)e$, $0e = 0$ /$i,j \in Z$ /.

Prema dobijemom rezultatu zaključujemo da važi relacija $(P,+,\cdot) \cong (Z,+,\cdot)$. Na taj način je tvrdjenje u potpunosti dokazano.

Zadatak 30. Naći sve detaljnije nule prstena Jm.

Zadatak 31. Prsten Jm se može potopiti u polje tada i samo tada ako je m prost broj. Dokazati.

Zadatak 32. Opisati sve prstene sa p elemenata, gde je p prost broj.

Rešenje. Za $p = 1$ jedini prsten je $(S, +, \cdot)$ gde je $S = \{a\}$ i $a + a = a.a = a$. Neka je $p > 1$. Postoji bar jedan prsten sa p elemenata. Takav je, na primer, Jp.

Neka je $(P, +, \cdot)$ bilo koji prsten sa p elemenata i neka su njegovi elementi $0, a_2, \ldots, a_p$ gde je 0 - nula tog prstena, odnosno jedinični element aditivne grupe $(P,+)$. Kako je red grupe $(P,+)$ prost broj ona mora biti ciklična i svaki element a_i / $2 \leq i \leq p$ / joj je generatorni element. Označimo a_2 sa a. Tada su svi elementi prstena P sledeći : $a, 2a, 3a, \ldots, (p-1)a, pa = 0$.

Pošto mora da važi zakon $x(y + z) = x.y + x.z$ / $\forall x, y, z \in P$ / zaključujemo da je $(ia)(ja) = (ij)a.a$ / $1 \leq i, j \leq p$ /. Odavde zaključujemo da je operacija množenje potpuno odredjena ako znamo a.a. Razlikujemo slučajeve:

I slučaj $a^2 = 0$. Tada je $x.y = 0$ / $\forall x, y \in P$ / .Sistem (P, +,·) kod koga je (ia) + ja = (i + j)a , ia.ja = 0 u ovom slučaju,čini prsten. Ovo je tzv. nula - prsten.

II slučaj $a^2 = ka$ gde je $0 < k < p$. Pošto je /k,p/= 1, to postoje celi brojevi s i t takvi da je sk + tp = 1 . Uvodjenjem elementa A = sa , prema $a^2 = ka$, zaključujemo da je $A^2 = s^2a^2 = s(sk)a = (sk)(sa) = A$ jer je $sk \equiv 1 (\mathrm{mod}\ p)$.

Elementi prstena (P,+ ,·) se mogu i pomoću A izraziti. Elementi prstena su A, 2A, ... , (p-1)A, pA , 0.Pošto je $A^2 = A$ zaključujemo da je iA + jA = (i+ j) A, iA.jA = =(ij)A / $0 < i, j \leq p$ / . Sistem (P, +,·) sa ovako definisanim operacijama čini prsten izomorfan prstenu $(J_p,+,\cdot)$.

Prema tome,reda p gde je p prost broj postoje dva neizomorfna prstena. To su J_p i nula - prsten reda p.

Zadatak 33. Neka je P prsten sa jediničnim elementom e. Ako $a \in P$ ima jedan i samo jedan desni inverzan element a^{-1}, onda je a^{-1} i levi inverzan element. Dokazati.

Rešenje. Pošto je $a (a^{-1} + a^{-1}a - e) = aa^{-1} + (aa^{-1})a - a = e$, zaključujemo da je $a^{-1} + a^{-1}a - e$ desni inverzan element elementa a. Pošto je a^{-1} jedinstven desni inverzni element,mora biti $a^{-1} + a^{-1}a - e = a^{-1}$. Odavde je $a^{-1}a = e$, pa je a^{-1} i levi inverzan element.

Na taj način je tvrdjenje dokazano.

Zadatak 34. Neka je prsten B_1 podprsten prstena B i neka je prsten A_1 izomorfan prstenu B_1 . Dokazati da se A_1 može proširiti u prsten A tako da je prsten A izomorfan prstenu B.

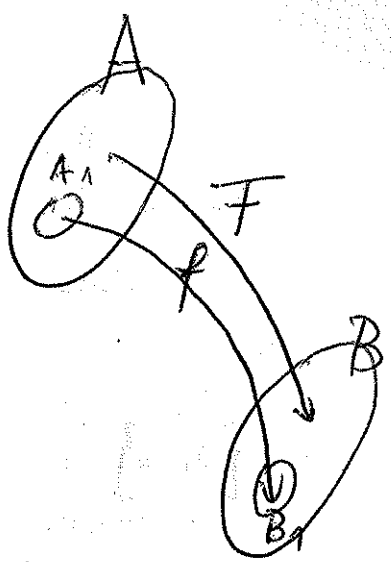
Rešenje. Neka preslikavanje f skupa A_1 na skup B_1 realizuje izomorfizam. Tada je:

$$x + y = (xf \oplus yf)\, f^{-1}$$

1/

$$x.y = (xf \odot yf) f^{-1} \quad /\forall x, y \in A_1/,$$

gde smo sa + i · označili operacije prstena A_1, a sa $\oplus$ i $\odot$ operacije prstena B_1. Skup A formirajmo na sledeći način: $A = A_1 \cup (B - B_1)$. Uvedimo preslikavanje F pomoću obrasca:



$$2/ \quad xF = \begin{cases} xf & \text{ako je } x \in A_1 \\ x & \text{ako je } x \in B - B_1. \end{cases}$$

Ovo preslikavanje uspostavlja korespodenciju 1 - 1 izmedju skupova A i B.

U skupu A definišimo operacije + i · pomoću

$$(x + y) = (xF \oplus yF)\, F^{-1}$$

$$(x.y) = (xF \odot yF)\, F^{-1}$$

Sistem (A, + , ·) je prsten izomorfan prstenu (B, $\oplus$, $\odot$) . Prema /1/ i /2/ zaključujemo da se ovako definisane operacije za $x, y \in A_1$ poklapaju sa operacijama prstena (A_1,+ ,·) . Znači A_1 je podprsten za prsten A , tj. A je proširenje za A_1 .

Na taj način je tvrdjenje u potpunosti dokazano.

Zadatak 35. Svaki integralni domen se može potopiti u polje.

Uputstvo. Dokaz je sličan uvodjenju polja racionalnih brojeva pomoću prstena celih brojeva.

Zadatak 36. Neka je A ma kakav prsten, Z prsten celih brojeva. U skupu $B = \{(m, a)\}$, / $m \in Z$, $a \in A$ / su definisane binarne operacije + i · pomoću

$$(m, a) + (n, b) = (m + n, a + b)$$

$$(m,a) .(n,b) = (mn,\ na + mb + ab)$$

$$\left[(m,a) = (p,b) \Leftrightarrow m = p,\quad a = b\right]$$

1/ Ispitati šta je $(B, +, \cdot)$.

2/ Pokazati da u B postoji jedinični element za operaciju ;

3/ Pokazati da je $(A', +, \cdot) = (A, +, \cdot)$ gde je $A' = \{0, a\}$, $0 \in Z$, $a \in A$.

Rešenje. 1/ $(B,+)$ je Abelova grupa . $(B,\cdot)$ je semi8 grupa, jer je operacija $\cdot$ unutrašnja i :

$$\left[(m,a) .(n,b)\right] . (p,c) = (mn,\ na + mb + ab) . (p,c) =$$

$$=(mnp, pna + pab + pmnc + nac + mbc + abc)$$

$$(m,a).\left[(n,b). (p,c)\right] = (m,a) .(np,\ pb + nc + bc) =$$

$$=(mnp,\ pna + pmb + pab + pmnc + nac + mbc + abc).$$

Pošto važe i oba distributivna zakona operacije + prema . jer je :

$$\left[(m,a) + (n,b)\right] (p,c) = (m + n,\ a + b).(p,c) =$$

$$=(mp + np,\ pa + pb + mc + nc + ac + bc) =$$

$$=(m,a) . (p,c) + (n,b). (p,c)$$

$$(p,c).\left[(m,a) + (n,b)\right] = (p,c).(m,a) + (p,c). (n,b)$$

to je $(B, +, \cdot)$ prsten.

2/ Iz definicije

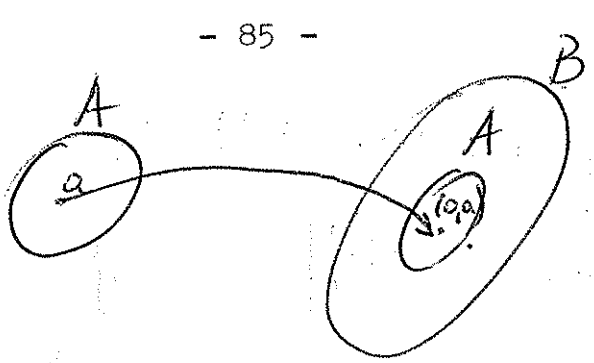
$$(m,a). (n,b) = (mn,\ na + mb + ab)$$

zaključujemo da je $(1,0)$, / gde je $1 \in Z$, $0 \in A$ / jedinični element.

3/ Uspostavimo biunikoko preslikavanje izmedju $A' = \{0, a\}$ i $A = \{a\}$ pomoću $(0,a) \leftrightarrow a$. Ovo preslikavanje označuje izomorfizam izmedju $(A', +, \cdot)$ i $(A,+, \cdot)$ jer je

$$(0,a) + (0,b) =(0,\ a + b) \Leftrightarrow a + b$$

$$(0,a) .(0,b) = (0,\ ab) \Leftrightarrow a.b$$



Primedba. Iz navedenog rasudjivanja se zaključuje poznata činjenica da se svaki prsten A može potopiti u prsten B koji ima jedinični element.

Zadatak 37. Neka je J_5 sistem ostataka po modulu 5. Formirati bar jedan polinom čiji svi koeficijenti nisu 0' koji za svako $x \in J_5$ ima vrednost 0'.

Rešenje. Takav je polinom

$$P/x/ = x(x-1')\,(x-2')\,(x-3')(x-4') = x^5-1'.x = x^5+4'x\ .$$

Zadatak 38. Ako konačno polje ima n elemenata onda n mora biti oblika p^m gde je p prost broj. Dokazati.

Zadatak 39. Svaki konačan integralni domen je polje. Dokazati.

Zadatak 40. Neka je $(P,+,\cdot)$ komutativan prsten sa jediničnim elementom e. Dokazati da skup S svih elemenata prstena P koji poseduju inverzan element čini multiplikativnu grupu.

Zadatak 41. Da li skup svih regularnih matrica reda n čini telo u odnosu na sabiranje i množenje matrica?

Zadatak 42. Neka je D konačan integralni domen sa n elemenata $a_1, a_2, \ldots, a_n$, Neka $m(x) = (x-a_1)\,..(x-a_n)$. Dokazati da ako dva polinoma $f/x/$ i $g/x/$ na D definišu istu funkciju da je onda $m/x/$ faktor polinoma $f/x/ - g/x/$.

Zadatak 43. Ako integralni domen D ima beskonačno elemenata onda dve polinomne funkcije P i Q su jednake tada samo tada ako su polinomi $P/x/$ i $Q/x/$ sa jednakim odgovarajućim koeficijentima.

Zadatak 44. Neka je F_4 polje sa četiri elementa.

a/ Dokazati da F_4 ima karakteristiku 2.

b/ Dokazati da svaki element ovog polja zadovoljava jednačinu $x^4 + x = 0$.

Zadatak 45. Dokazati da je polje Co kompleksnih brojeva izomorfno polju matrica $\left\{\begin{vmatrix} a & b \\ -b & a \end{vmatrix}\right\}$, /a, b su realni/.

Zadatak 46. Dokazati da je polje $Ra(\sqrt{m})$, /$\sqrt{m}$ nije racionalan/ , izomorfno polju matrica

$$\left\{\begin{vmatrix} a & b \\ mb & a \end{vmatrix}\right\}$$

Zadatak 47. Dokazati da polja $Ra(\sqrt{2})$ i $Ra(\sqrt{3})$ nisu izomorfna.

Zadatak 48. Dokazati da je polje $Ra(\sqrt{7})$ izomorfno polju $Ra(x)$.

Zadatak 49. Polju $Ra(\sqrt{2}, \sqrt{3})$ naći izomorfno polje matrica.

Zadatak 50. Uočimo skup

$$S = \left\{ \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \right\}$$

gde su a, b, c, d ma kakvi realni brojevi a i imaginarna jedinica.

1/ Dokazati da je $(S, +, \cdot)$ telo /nekomutativno polje/.

2/ Dokazati da je $(S, +, \cdot)$ ekstenzija polja kompleksnih brojeva Co.

Rešenje. 1/ Ma koji element skupa S možemo i ovako pisati

$$\begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix}$$

gde su z_1, z_2 kompleksni brojevi.

Lako je proveriti da je (S, +) Abelova grupa. Uočimo:

$$S' = S\left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}.$$

Neka $\begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix}, \begin{pmatrix} u_1 & u_2 \\ -\bar{u}_2 & \bar{u}_1 \end{pmatrix} \in S'$

Tada njihov proizvod

$$\begin{pmatrix} z_1u_1 - z_2\bar{u}_2 & z_1u_2 + z_2\bar{u}_1 \\ -\bar{z}_1\bar{u}_2 - \bar{z}_2u_1 & \bar{z}_1\bar{u}_1 - \bar{z}_2u_2 \end{pmatrix} \in S'$$

jer je u suprotnom slučaju

$$z_1u_1 - z_2\bar{u}_2 = 0$$

$$z_1u_2 + z_2\bar{u}_1 = 0$$

odakle je $\begin{vmatrix} u_1 & -\bar{u}_2 \\ u_2 & \bar{u}_1 \end{vmatrix} = |u_1|^2 + |u_2|^2 = 0$

što je nemoguće jer

$$\begin{pmatrix} u_1 & u_2 \\ -\bar{u}_2 & \bar{u}_1 \end{pmatrix} \in S' .$$

Sličnim zaključivanjem kao u zadatku 57 možemo pokazati da je $(S', \cdot)$ grupa, ali ne Abelova jer proizvod u ovom slučaju nije komutativan. Pošto još važe i levi i desni distributivni zakon množenja prema sabiranju to je $(S, +, \cdot)$ telo.

2/ Uočimo postupak $\sum = \left\{\begin{pmatrix} a & c \\ -c & a \end{pmatrix}\right\}$ /a,c realni / skupa S . Uspostavimo biunivoko preslikavanje izmedju $\sum$ i Co - - skupa kompleksnih brojeva na sledeći način:

$$\begin{pmatrix} a & c \\ -c & a \end{pmatrix} = a + i\,c$$

Tada je

$$\begin{pmatrix} a_1 & c_1 \\ -c_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & c_2 \\ -c_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & c_1 + c_2 \\ -c_1 - c_2 & a_1 + a_2 \end{pmatrix} \leftrightarrow$$

$$\leftrightarrow (a_1 + a_2) + i\,(c_1 + c_2) = (a_1 + i\,c_1) + (a_2 + i\,c_2)$$

$$\begin{pmatrix} a_1 & c_1 \\ -c_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & c_2 \\ -c_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - c_1c_2 & a_1c_2 + c_1a_2 \\ -a_1c_2 - c_1a_2 & a_1a_2 - c_1c_2 \end{pmatrix} \leftrightarrow$$

$$\leftrightarrow (a_1a_2 - c_1c_2) + i\,(a_1c_2 + c_1a_2) = (a_1 + i\,c_1)\cdot(a_2 + i\,c_2)$$

Znači $(\sum, +, \cdot)$ je polje izomorfno polju C. Otuda $(S,+,\cdot)$ je ekstenzija polja C.

Zadatak 51. Svako polje karakteristike "∞" je ekstenzija polja Ra racionalnih brojeva. Dokazati.

Rešenje. Označimo sa F posmatrano polje i sa $e \in F$ jedinični element tog polja. Pošto je karakteristika polja "∞" to jednakost $c_1 e = c_2 e$ gde su c_1 i c_2 celi brojevi povlači $c_1 = c_2$. Zbog ovoga su u skupu $S = \{\ldots, -3e, -2e, -e, e, 2e, 3e, \ldots\}$ svi elementi medju sobom različiti. Ako je $ce \in S \;/\; c \neq 0$ / sa $\frac{1}{e}$ e označimo njegov inverzan element. Dalje, neka $\frac{p}{q}\, e \;/\; q \neq 0$, p i q celi brojevi / označava $p \cdot (\frac{1}{q} e)$. Tada, što se može neposredno proveriti, skup T svih elemenata polja F oblika $\frac{p}{q}\, e \;/ q \neq 0$, p i q celi brojevi / čini polje u odnosu na operacije polja, preslikavanje $\frac{p}{q} e \to \frac{p}{q}$ e realizuje izomorfizam $(Ra,+,\cdot) \cong (T,+,\cdot)$.

Zbog ovoga je polje F ekstenzija polja Ra.

Zadatak 52. Dokazati da aditivna grupa (F,+) polja F ne može biti izomorfna sa multiplikativnom grupom tog polja / Videti : Amer. Math.Monthly,Oct. 1956,problem 4644/.

Zadatak 53. Dokazati da je za polje Ra jedino podpolje Ra. Slično dokazati za J_p / p prost broj/ .

Zadatak 54. Konstruisati sva tela sa 2, 3, 4 i 5 elemenata.

Zadatak 55. Neka je C centar prstena P i neka je a jedan odredjen element centra. U prstenu P definisana je relacija ρ na sledeći način:

$$x \rho y \iff z \in P, \quad x - y = za.$$

Dokazati da je relacija ρ jedna relacija kongruencije.

Zadatak 56. Naći sve kongruencije prstena Jm.

Zadatak 57. Neka su p i q dva racionalna broja takva da $q^2 + 4p$ nije kvadrat ni jednog racionalnog broja.Uočimo

$$S = \left\{ \begin{pmatrix} a & bp \\ b & a + qb \end{pmatrix} \right\}$$

gde a, b $\in$ Ra .

1/ Dokazati da je (S, + ,·) polje .

2/ Preslikavanje $\begin{pmatrix} a & bp \\ b & a+qb \end{pmatrix} \leftrightarrow (a,b)$ je biunivoko preslikavanje izmedju S i $\sum = \{ (a,b) \}$ a,b $\in$ Ra . Kako u $\sum$ treba definisati binarne operacije + i · tako da bude

$$(\sum , +, \cdot) \cong (S,+ ,\cdot)$$

Rešenje. 1/ (S,+) je Abelova grupa,što se može neposredno proveriti. Neutralni element je $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ / a = 0, b = 0 / . Uočimo sada skup S bez 0. Označimo ovaj sa S'. Pokazaćemo da je (S', ·) Abelova grupa.

$$\begin{pmatrix} a_1 & b_1p \\ b_1 & a_1+qb_1 \end{pmatrix} \quad i \quad \begin{pmatrix} a_2 & b_2p \\ b_2 & a_2+qb_2 \end{pmatrix}$$

bilo koja dva elementa iz S' , njihov proizvod je:

$$\begin{pmatrix} a_1a_2 + b_1b_2p & p\left[a_1b_2 + b_1a_2 + b_1b_2q\right] \\ a_1b_2 + b_1a_2 + b_1b_2q & a_1a_2 + pb_1b_2 + q\left[a_1b_2+b_1a_2+b_1b_2q\right] \end{pmatrix}$$

Odavde saznajemo komutativnost. Takodje vidimo da ovaj proizvod pripada S . Pokažimo da pripada S'. Neka je obrnuto:

$$a_1a_2 + b_1b_2p = 0 \qquad a_1b_2 + b_1a_2 + b_1b_2q = 0$$

Pošto a_1 i b_1 nisu jednovremeno 0, to je

$$\begin{vmatrix} a_2 & b_2p \\ b_2 & a_2 + qb_2 \end{vmatrix} = 0$$

Odavde je $a_2^2 + a_2b_2q - b_2^2p = 0$. Ovu jednakost možemo i ovako pisati:

$$\left(a_2 + \frac{1}{2} b_2q\right)^2 - \frac{1}{4} b_2^2 \left(q^2 + 4p \right) = 0$$

što je nemoguće jer $q^2 + 4p$ nije potun kvadrat racionalnog broja i a_2 i b_2 nisu obe jednaka nuli . Znači (S', ·) je komutativan grupoid. Element

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S'$$

je jedinični i dobija se za $a = 1$, $b = 0$.

Ako

$$A = \begin{pmatrix} a & bp \\ b & a+bq \end{pmatrix} \in S' \text{ onda i}$$

$$A^{-1} = \begin{pmatrix} \frac{a + bq}{\Delta} & \frac{-bp}{\Delta} \\ \frac{-b}{\Delta} & \frac{a}{\Delta} \end{pmatrix} \in S' \ / \ \Delta = a^2 + ab - b^2p \neq 0.$$

Pošto je još operacija množenja matrica asocijativna to je (S', ·) zaista Abelova grupa.

Distributivni zakon sabiranja prema množenju je

ispunjen. Na osnovu svega $(S,+ ,\cdot)$ je polje.

2/ Dovoljno je u Σ definisati + i $\cdot$ na sledeći način:

$$(a_1,b_1) +(a_2,b_2) = (a_1+ a_2,\ b_1+ b_2) ,$$

$$(a_1,b_1).\ (a_2,b_2) = (a_1a_2 + pb_1b_2,\ \ a_1b_2+ b_1a_2+ b_1b_2q)$$

pa će $(\Sigma, + , \cdot)$ biti izomorfna struktura sa $(S,+ ,\cdot)$.

Zadatak 58. Dokazati da polje Ra racionalnih brojeva nema drugih automorfizama izuzev intentičkog preslikavanja.

Dokaz. Neka je ϕ automorfizam polja Ra. Iz $a + 0 = a$ sleduje $a\phi + 0\phi = a\phi$, tj. $0\phi = 0$. Iz $a.1 = a$ /$a \neq 0$/ sleduje $a\phi . 1\phi = a\phi$, tj. $1\phi = 1$. Iz $2 = 1+ 1$ sleduje $2\phi = 1\phi + 1\phi = 2$. Indukcijom lako dokazujemo da ako je n proizvoljan prirodan broj da je onda $n\phi = n$. Iz jednakosti $a + (-a) = 0$ sleduje $a\phi + (-a)\phi = 0\phi$ tj. $(-a\phi) = (- a\phi)$ jer $0\phi = 0$. Iz $a . \frac{1}{a} = 1$ /$a \neq 0$/ sleduje $a . \frac{1}{a} = 1$ a odavde je $\frac{1}{a}\phi = \frac{1}{a\phi}$.

Neka je sada $\frac{p}{q}$ / $q \neq 0$ / bilo koji racionalni broj. Njemu odgovarajući element $(\frac{p}{q})\phi$ mora biti $\frac{p}{q}$ jer

$$(\tfrac{p}{q})\phi = (p.\ \tfrac{1}{q})\phi = p\phi \cdot \tfrac{1}{q}\phi = p\phi . \tfrac{1}{q\phi} = p.\ \tfrac{1}{q} = \tfrac{p}{q} .$$

Znači pretpostavljeni automorfizam mora biti identičko preslikavanje. Time je stav u potpunosti dokazan.

Zadatak 59. Dokazati da polja Ra $(\sqrt{7})$ i Ra $(\sqrt{11})$ nisu izomorfna / Ra je polje racionalnih brojeva/.

Rešenje. Svaki element polja Ra $(\sqrt{7})$ se može jedinstveno napisati u obliku $a_o+ a_1\sqrt{7}$, a polja R_a $(\sqrt{11})$ u obliku $b_o+ b_1\sqrt{11}$ gde a_o, a_1, b_o, $b_1 \in$ Ra . Pretpostavimo obrnuto da su izomorfna, izomorfizam označimo sa $\mathcal{F}$. Neka $\sqrt{7}\mathcal{F} = b_o + b_1\sqrt{11}$. Element $\sqrt{7}$ je koren nesvodljive jednačine $x^2 - 7 = 0$, na polju Ra ; to je njegova definiciona jednačina. Znači $\sqrt{7} . \sqrt{7} = 7$ pa obadve

$(\sqrt{7}\cdot\sqrt{7})\mathcal{F} = 7\mathcal{F}$. Kako je $7\mathcal{F} = 7$ / videti zad. 58 / to je $7 = (\sqrt{7}\cdot\sqrt{7})\mathcal{F} = (\sqrt{7})\cdot(\sqrt{7})\mathcal{F} \ni (b_0 + b_1\sqrt{11})\cdot(b_0 + b_1\sqrt{11})$. Znači $b_0 + b_1\sqrt{11}$ je koren jednačine $x^2 - 7 = 0$, što je nemoguće jer su b_0, b_1 po pretpostavci racionalni. Znači polja nisu izomorfna.

Zadatak 60. Označimo sa Ra skup svih racionalnih brojeva a njegove elemente sa a, b, c, d, ... Neka je S_1 skup $\{a + b\sqrt{3}\}$, S_2 skup matrica $\begin{Vmatrix} a & 3b \\ b & a \end{Vmatrix}$ a skup S_3 neka je skup parova (a,b) snabdeven sa relacijom ekvivalencije $=$, tako da je $(a,b) = (c,d)$ ako i samo ako je $a = c$, $b = d$ i sa operacijama sabiranja i množenja definisanim sa:

$$(a,b) + (c,d) = (a + c, b + d)$$
$$(a,b)\cdot(c,d) = (ac + 3bd,\ ad + bc).$$

Pokazati da su S_1, S_2, S_3 medjusobno izomorfna polja.

Rešenje, Pokažimo da je S_1 polje. Dovoljno je dokazati da je S_1 integralni domen i da svaki element različit od 0 ima svoj inverzni u odnosu na množenje. U zadatku 17 dokazasmo pod manjim pretpostavkama da je S_1 integralni domen. Pokažimo još da $a + b\sqrt{3} = 0$ ima inverzni u odnosu na množenje. Rešavanjem jednačine $(a + b\sqrt{3})(x + y\sqrt{3}) = 1$ nalazimo

$$x = \frac{a}{a^2 - 3b^2}, \qquad y = -\frac{b}{a^2 - 3b^2}$$

Pošto $a + b\sqrt{3} = 0$, to $a^2 - 3b^2 \neq 0$ i za element $a + b\sqrt{3}$ je inverzan element

$$\frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3} \in S_1.$$

Znači S_1 je polje.

Uspostavimo sada preslikavanje F skupa S_1 na skup S_2 preko jednakosti :

$$(a + b\sqrt{3})\,F = \begin{Vmatrix} a & 3b \\ b & a \end{Vmatrix} .$$

Ovo preslikavanje je biunivoko . Pokažimo da je izomorfizam. Zaista:

$$\left[(a + b\sqrt{3})(c + d\sqrt{3})\right]F = \left[(ac + 3bd) + (ad + bc)\sqrt{3}\right]F =$$

$$= \begin{Vmatrix} ac + 3bd & 3(ad + bc) \\ ad + bc & ac + 3bd \end{Vmatrix} = \begin{Vmatrix} a & 3b \\ b & a \end{Vmatrix} \cdot \begin{Vmatrix} c & 3d \\ d & c \end{Vmatrix} =$$

$$(a + b\sqrt{3})\,F \;.\; (c + d\sqrt{3})\,F$$

$$\left[(a + b\sqrt{3}) + (c + d\sqrt{3})\right]F = \left[(a + c) + (b + d)\sqrt{3}\right]F =$$

$$\begin{Vmatrix} a + c & 3(b + d) \\ b + d & a + c \end{Vmatrix} = \begin{Vmatrix} a & 3b \\ b & a \end{Vmatrix} + \begin{Vmatrix} c & 3d \\ d & c \end{Vmatrix} =$$

$= (a + b\sqrt{3})\,F + (c + d\sqrt{3})\,F$ pa je F zaista izoforfižam. Pošto je S_1 polje, to je i S_2 polje izomorfno sa njim. Ako uspostavimo preslikavanje φ skupa S_1 na S_3 preko $(a + b\sqrt{3}) = (a, b)$ na sličan način zaključujemo da je S_3 izomorfno polje polju S_1 , pa je stav u potpunosti dokazan.

Zadatak 61. Neka je $R[x]$ skup svih polinoma sa realnim koeficijentima. Neka je J ideal $(x^2 + 1)$ .Dokazati da je polje Co (kompleksnih brojeva) izomorfno sa kvocijent prstenom $R[x]/J$.

Rešenje. Ideal J je glavni ideal za $x^2 + 1 \in R(x)$, odnosno $J = \{(x^2 + 1)\,p/x/ \;;\; p/x/ \in R[x]\}$. Neka je $P/x/ \in R[x]$ polinom stepena 2 ili većeg od 2. Deobom

$P/x/$ sa $x^2 + 1$ imamo

$$1/ \qquad P/x/ = (x^2 + 1)\ S/x/ + ax + b$$

gde je $S/x/ \in R[x]$ i a i b izvesni realni brojevi. Na osnovu /1/ je

$$P/x/ = ax + b \ (\mathrm{mod}\ J) .$$

Polinomi $ax + b$ i $cx + d$ / $a,b,c,d \in R$ / su $\equiv$ mod J ako i samo ako je $a = c$, $b = d$.

Na osnovu napred izloženog u svakoj klasi ekvivalencije po mod J postoji jedan i samo jedan polinom oblika $ax + b$ / $a, b \in R$ /. Sa C_{ax+b} označimo klasu ekvivalencije u kojoj je polinom $ax + b$. Tada je $R[x]/J = \{C_{ax+b}$; $a, b \in R$ sa operacijama:

$$2/ \qquad C_{ax+b} + C_{cx+d} = C_{(a+c)x+(b+d)}$$

$$C_{ax+b} \cdot C_{cx+d} = C_{x(ad+bc)+(bd-ac)}$$

/ $(ax + b)(cx + d) = x(ad + bc) + (bd - ac) \ (\mathrm{mod}\ J)$ /.

Preslikavanje $C_{ax+b} \rightarrow ai + b$ je biunivoko preslikavanje skupa $R[x]/J$ na skup Co, svih kompleksnih brojeva.

Na osnovu /2/ sleduje dokaz tvrdjenja.

Zadatak 62. Naći sve ideale sledećih prstena :

a/ J_8 b J_{17} c/ $J_8 \times J_{12}$ d/ $Ra[x]$ e/ Ra f/ R.

Zadatak 63. Ispitati da li navedeni skupovi čine ideale navedene prstene:

a/ 0', 2', 4', 6', 8', 10' za J_{12} b/ 1',3',5',7',9',11' za c/ 0', 5',10' za J_{15} d/ skup svih realnih polinoma p/x/ osobine p/8/ = 0 za prsten $R[x]$.

Zadatak 64. Za element a prstena P kažemo da je nul-potentan ako je $a^h = 0$ za izvestan prirodan broj h. Dokazati.

da u komutativnom prstenu skup svih nul- potentnih elemenata čini ideal tog prstena.

Zadatak 65. Neka je P komutativan prsten i J njegov ideal. Neka je $S \subset P$ skup svih elemenata prstena koji ina-ju osobinu

$$\forall a \in S, \exists n \in N, \quad a^n \in J .$$

Dokazati da je S ideal prstena P / tzv. radikal ideala J/.

Zadatak 66. Poljima $Ra(\sqrt{2})$, $Ra(\sqrt{2}, \sqrt{3})$, $Ra(\rho)$ gde je ρ jedan koren jednačine $\rho^3 + \rho^2 + 1 = 0$ naći izomor-fne kvocijent prstene.

Zadatak 67. Naći prsten endomorfizama za beskonačnu cikličnu grupu.

Rešenje. Ako je $a \in C$ generatorni element te grupe onda je grupa $C = \{\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots\}$. Neka je $f: x \to xf$ / $x \in C$ / endomorfizam grupe C. Tada je

$$1/ \quad (x + y)f = xf + yf \quad / \forall x, y \in C /$$

Odavde je $0f = 0$. Za $y = -x$ dobijamo $(-x)f = -(xf)$ / $\forall x \in C$ /. Takodje iz /1/ sleduje $(cx)f = c(xf)$ / $\forall c \in Z$, $\forall x \in C$ /. Na taj način je f potpuno odredjeno poznavanjem af jer je onda $(ca)f = c(af)$ / $\forall c \in Z$ /.

Neka je $af = ca$ gde je c izvestan ceo broj. Tada je $xf = cx$ za svako $x \in C$. Kako je

$$(x + y)f = c(x + y) = cx + cy = xf + yf \quad /\forall x, y \in C/,$$

zaključujemo da je f endomorfizam za svako $c \in Z$. Na taj način su svi endomorfizmi dati formulom $xf = cx$. Ako je $xf = cx$ endomorfizam f označujemo sa f_c. Kako $c_1 x = c_2 x$ / $\forall x \in C$; $c_1, c_2 \in Z$ / daje $c_1 = c_2$ zaključujemo da je preslikavanje $c \to f_c$ / $c \in Z$ / biunikovo preskikavanje

skupa Z celih brojeva na skup E svih endomorfizama grupe C. Kako je

$$xf_{c_1} + xf_{c_2} = (c_1 + c_2)x = xf_{c_1} + c_2$$

$$x(f_{c_1} \cdot f_{c_2}) \quad (xf_{c_1}) f_{c_2} = c_1c_2x = xf_{c_1c_2}$$

$$/ \forall x \in C \; ; \; c_1, c_2 \in Z /,$$

zaključujemo da je

$$f_{c_1} + f_{c_2} = f_{c_1 + c_2} \; , \; f_{c_1} \cdot f_{c_2} = f_{c_1} \cdot c_2$$

Ovo nam daje relaciju:

$$(E, +, \cdot) \cong (Z, +, \cdot)$$

pa je traženi prsten endomorfizama E izomorfan prstenu celih brojeva Z .

Zadatak 68. Neka je C = A x B direktan proizvod beskonačnih cikličnih grupa (A,+) i (B,+) . Dokazati da je prsten endomorfizama grupe C izomorfan prstenu matrica reda 2 čiji su elementi celi brojevi.

Rešenje. Neka su $A = \{ca \; ; \; c \in Z\}$ i $B = \{cb : \; c \in Z\}$ grupe A i B i neka su a odnosno b njihovi generatorni elementi. Elementi grupe C su oblika $(ca, sb) \; / c, s \in Z /$ a operacija ove grupe je

$$(ca, sb) + (c'a, s'b) = \{(c + c')a, (s + s') b\}$$

$/ c, c', s, s' \in Z /$.

Traženje endomorfizama grupe C se svodi na traženje funkcija f / x, $xf \in C$ / koje zadovoljavaju uslov

$$1/\ldots \; [(ca,sb) + (c'a,s'b)] f = (ca,sb)f + (c'a,s'b)f$$

$$/ \forall c,s,c',s' \in Z / .$$

Iz /1/ neposredno dobijamo jednakosti

$$(0,0)f = (0,0), \; (ca,sb)f = c(a,0)f + s(0,b)f \; /c,s \in Z /.$$

Prema tome f je potpuno odredjena poznavanjem (a,0)f i (0,b) f. Ako stavimo (a,0)f =(ja,kb) (0,b)f=(la,mb) gde su j, k, i m izvesni celi brojevi,onda je

2/... (ca,sb)f = c(ja,kb)+ s (a,mb) = (cja+sla, ,skb + smb) / ∀c,s ∈ Z /.

Ovako odredjena funkcija f zadovoljava uslov /1/ što se može lako proveriti.

Na taj način pri proizvoljnom izboru celih brojeva j, k, l, m funkcija f odredjena pomoću /2/ je endomorfizam grupe C. Funkciju f definisanu pomoću /2/ označavamo sa $f\begin{pmatrix} j & k \\ l & m \end{pmatrix}$. Neposredno se dokazuje da $f\begin{pmatrix} j & k \\ l & m \end{pmatrix} = f\begin{pmatrix} j' & k' \\ l & m \end{pmatrix}$ ako i samo ako je j = j', k = k', l = l' m = m'.

Zbog ovoga preslikavanje $\begin{pmatrix} j & k \\ l & m \end{pmatrix} \to f\begin{pmatrix} j & k \\ l & m \end{pmatrix}$ je biunivoko.Preslikavanje skupa $\longrightarrow$ M svih matrica reda 2 čiji su elementi celi brojevi na skup E svih endomorfizama grupe C. Kako je

$$f\begin{pmatrix} j & k \\ l & m \end{pmatrix} + f\begin{pmatrix} j' & k' \\ l & m' \end{pmatrix} = f\begin{pmatrix} j+j' & k+k' \\ l+l' & m+m' \end{pmatrix}$$

$$f\begin{pmatrix} j & k \\ l & m \end{pmatrix} \cdot f\begin{pmatrix} j' & k' \\ l' & m' \end{pmatrix} = f\begin{pmatrix} j & k \\ l & m \end{pmatrix} \cdot \begin{pmatrix} j' & k' \\ l' & m' \end{pmatrix}$$

/ ∀ j,j', k,k', l ,l', m,m' ∈ Z /,

što se može neposredno proveriti, zaključujemo da važi relacija

$$(M, +, \cdot) \cong (E, +, \cdot).$$

Na taj način je tvrdjenje u potpunosti dokazano.

Primedba. Važi slična teorema za direktan proizvod n beskonačnih cikličnih grupa i za odgovarajući prsten matrica.

Zadatak 69. Naći prsten endemorfizama za sledeće

grupe : a / Klein-ovu vierer - grupu, b / cikličnu grupu reda m, c/ grupu $C_p \times C_q$ / C_p i C_q su cikličke grupe reda p odnosno q/

d/ aditivnu grupu racionalnih brojeva.

Zadatak 70. Bilo koji prsten je izomorfan sa nekim podprstenom prstena endomorfizama neke grupe. Dokazati.

Zadatak 71. Neka je P dat komutativan prsten i neka je P [x] polinomni prsten ovog prstena. U P [x] definisano je preslikavanje na sledeći način. Ako je $f/x/ = a_0 + a_1 x + \ldots + a_n x^n \in P[x]$, onda je slika $f'/x/ = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$. Proveriti da li važe sledeće relacije

$$(f + g)' = f' + g', \quad (cf)' = cf' \ / \ c \in P /, \quad (fg)' = f'g + fg',$$

$$(fg)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} f^{(i)} g^{(k-i)} \quad \text{gde je}$$

$$f^{(i)} = (f^{(i-1)})', \quad f^{(0)} = f.$$

Zadatak 72. Naći sve nule polinoma $x^2 + 1$ u prstenu realnih kvaterniona.

Zadatak 73. U polju $J_5 = \{0', 1', 2', 3', 4'\}$ je data jednačina $x^2 = 2'$. Pokazati da se J_5 može potopiti u polje F u kome ta jednačina ima rešenja. Naći minimalno polje F navedene osobine.

Rešenje. Direktnom proverom zaključujemo da nijedan koren jednačine $x^2 = 2'$ nije u polju J_5. Radi formiranja polja F, postupimo na sledeći način.

U skupu $E = J_5 \times J_5$ definišimo sledeće operacije:

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (ac + 2bd, ad + bc)$$

Sistem (E,+ ,·) je polje. U ovom polju skup E' svih elemenata (a,0) / a $\in J_5$ / je podpolje polja E. Jednakosti :

$$(a, 0) + (b,0) = (a+ b, 0)$$

$$(a,0).(b,0) = (ab, 0)$$

nam dokazuju da je (E' ,+ ,·) $\cong$ (J_5,+ ,·) , pa je polje E proširenje polja J_5 .

Jednačina $x^2 = 2'$ u polju E glasi :$x^2 = (2', 0')$. Koreni ove jednačine su (0',1') i (0', - 1'), pa je E proširenje polja J_5 u kome jednačina $x^2 = 2'$ ima rešenja. Polje E je minimalno polje te osobine,što se vidi na sledeći način : Neka je F bilo kakvo polje koje je proširenje polja J_5 u kome jednačina $x^2 = 2'$ ima rešenja . Ako je r jedan koren,onda je -r drugi njen koren. Elemente ovog polja označimo sa 0,1,2,3,4,r, -r,a,b, ...,gde su 0, 1, 2, 3, 4 korespondentni elementi elementima 0', 1', 2', 3', 4' iz polja J_5 . Skup S elemenata oblika a + br, gde a, b $\in \{0, 1, 2, 3, 4\}$ u odnosu na operacije + i · čini polje. Uovom polju su r i -r. Kako je (a + br) + + (c + dr) = (a + c) +(b + d) r i (a + br) (c + dr) = = (ac + 2bd) + (ad + bc) r jer $r^2 = 2$, zaključujemo da je preslikavanje a + br$\longleftrightarrow$ (a', b') izomorfizam polja S i polja E . Zbog ovog je E zaista minimalno polje u kome jednačina $x^2 = 2'$ ima rešenja, pa je tvrdjenje dokazano.

Zadatak 74. Neka je (K,+, ·) polje sa sedam elemenata.

1/ Dokazujući da postoji samo jedno neizomorfno polje sa sedam elemenata formirati aditivnu i multiplikativnu tablicu tog polja.

2/ Polje K_7 potpuno pripada polju u kome jednačina $x^2 = 3e$ / e - jedinični element polja / ima rešenja.

3/ Objasniti način formiranja jednog polja u kome sve jednačine oblika: $ax^2 + bx + c = 0$ / $a \neq 0, b, c \in K_7$, 0- nula polja K_7 / imaju rešenja.

Rešenje. 1/ Neka su elementi polja e , 2e, 3e, 43, 5e, 6e, 7e = 0 gde je e jedinica polja, a 0 nula polja. Distributivnost množenja prema sabiranju daje (ie)(je) = = (ij) e / i,j = 1, 2, ... , 7 /. Kako je 7e = 0 biće 7x = 0 za svako x iz polja,pa polje K_7 mora biti izomorfno polju (J_7,+ ,·) gde J_7 označuje sistem ostataka po modulu 7.

2/ Jednačina $x^2 = 3e$ tj . $x^2 = 3'$ nema rešenja u polju K_7 jer $1'^2 = 6'^2 = 1'$, $2'^2 = 5^2 = 4'$, $3'^2 = 4'^2 = 2'$. Sistem ($J_7 \times J_7$, + , ·) gde : (a,b) +(c,d) = = (a +c), b + d), (a,b) . (c,d) = (ac + 2bd, ab +bc) / a,b, c,d $\in J_7$ / pretstavlja ekstenziju polja J_7 jer podskup $\{(a,0) ; a \in J_7\}$ ovog skupa u odnosu na operacije tog skupa čini polje izomorfno polju J_7. U ovom polju su rešenja navedene jednačine: $x_1 = (0', 1')$ i $x_2 = (0',6')$

Dobijeno polje nazovimo $J_7(\sqrt{3'})$.

3/ Svaka jednačina

/*/ $$ax^2 + bx + c = 0 , \quad / a \neq 0 /$$

na polju J_7 se može dovesti na oblik $(2ax + b)^2 = b^2 - 4ac$ pa sve jednačine / * / se mogu rešiti ako se mogu rešiti jednačine oblika $x^2 = \ell$, / $\ell \in J_7$ / . Iz izloženog pod 2/ vidimo da su od interesa slučajevi $\ell = 3', 5', 6'$. Traženo polje je, dakle, polje $J_7(\sqrt{3'}, \sqrt{5'}, \sqrt{6'})$ čiji je način formiranja sličan formiranju polja $J_7(\sqrt{3'})$. Dovoljno je vršiti postepeno proširenje polja J_7

na primer $J_7 \subset J_7(\sqrt{3}) \subset J_7(\sqrt{3}, \sqrt{5}) \subset J_7(\sqrt{3}, \sqrt{5}, \sqrt{6})$.

Zadatak 75. Izraziti diskriminantu jednačine

$$x^3 + px + q = 0$$

preko koeficijenta-ta p i q.

Rešenje. Pod diskriminantom kubne jednačine smatramo ~~al~~ kvadrat alternativne funkcije

$$\varphi = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

Ovu funkciju φ ne menjaju permutacije (1), (123), (132) iz S_3 tj. njena grupa je alternativna A_3. Primenom svih permutacija iz S_3 na φ ona će preći ili u φ ili u $-\varphi$. Pošto je $\mathcal{D} = \varphi^2$ to primenom ma koje permutacije iz S_3 diskriminanta se neće menjati, drukčije rečeno $\mathcal{D}$ je simetrična funkcija korena x_1, x_2, x_3 jednačine pa se može izraziti preko koeficijenata p i q. Predjimo na to izražavanje:

$$\mathcal{D} = -(x_1-x_2)(x_1-x_3) \cdot (x_2-x_1)(x_2-x_3) \cdot (x_3-x_1)(x_3-x_2) =$$

$$= -\left[x_1^2 - x_1(x_2+x_3) + x_2x_3\right] \cdot \left[x_2^2 - x_2(x_1+x_3) + x_1x_3\right]$$

$$\cdot \left[x_3^2 - x_3(x_1+x_2) + x_1x_2\right]$$

Koristeći jednakosti $x_1 + x_2 + x_3 = 0$ i $x_1x_2 + x_1x_3 + x_2x_3 = p$ možemo pisati:

$$\mathcal{D} = -\left[3x_1^2 + p\right] \cdot \left[3x_2^2 + p\right]\left[3x_2^2 + p\right]$$ jer na primer

$x_2x_3 = p - x_1(x_2 + x_3) = p - x_1(-x_1) = p + x_1^2$ i slično.

Dalje je

$$\mathcal{D} = -\left[p^3 + 3p^2(x_1^2 + x_2^2 + x_3^2) + 9p(x_1^2x_2^2 + x_2^2x_3^2 + x_1^2x_3^2) + 27x_1^2x_2^2x_3^2\right].$$

Iz jednakosti $x_1 + x_2 + x_3 = 0$ kvadriranjem

dobijamo

$$x_1^2 + x_2^2 + x_3^2 = -2(x_1x_2 + x_1x_3 + x_2x_3) = -2p \quad \text{a iz}$$

$$x_1x_2 + x_1x_3 + x_2x_3 = p \quad \text{kvadriranjem dobijamo}$$

$$x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = p^2 - 2x_1x_2x_3(x_1 + x_2 + x_3) = p^2$$

pa je $\mathcal{D} = -\left[p^3 + 3p^2(-2p) + 9p \cdot p^2 + 27q^2\right] = -4p^3 - 27q^2$

što je traženi izraz. Koristili smo i $x_1x_2x_3 = -q$.

Zadatak 76. Dokazati da je diskriminanta D jednačine n- tog stepena $a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$, date na polju F,

$$D = \begin{vmatrix} n & s_1 & s_2 & \cdots & s_{n-1} \\ s_1 & s_2 & s_3 & \cdots & s_n \\ s_2 & s_3 & s_4 & \cdots & s_{n\,1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{n-1} & s_n & s_{n\,1} & \cdots & s_{2n-2} \end{vmatrix}$$

gde je $s_i = \sum_{i=1}^{n} x^i$, /x_1, x_2, ... , x_n - koreni jednačine/

Uputstvo. Diskriminantu D izraziti kao kvadrat kao kvadrat Wronski- eve determinante, a zatim primeniti pravilo o množenju determinanata.

Zadatak 77. Diskriminanta jednačine n-tog stepena na polju karakteristike 2 je potpun kvadrat. Dokazati.

Zadatak 78. Eelement $\frac{2\Theta+1}{\Theta^2+1}$ polja Ra (Θ), gde je Θ koren jednačine $x^3 + 3x^2 + 2x - 1 = 0$ dovesti na normalan oblik.

Rešenjel . Potražimo takve racionalne brojeve a,b,c da je $\frac{2\theta + 1}{\theta^2 + 1} = a\theta^2 + b\theta + c$. Ovo je ekvivalentno traženju a, b i c iz uslova: $2\theta + 1 = (a\theta^2 + b\theta + c)(\theta^2+1)$. Kako je $\theta^3 = -3\theta^2 + 2\theta + 1$; $\theta^4 = -3\theta^3 + 2\theta^2 + \theta = -3(-3\theta^2 + 2\theta + 1) + 2\theta^2 + \theta = 11\theta^2 - 5\theta - 3$, dolazimo do uslova: $2\theta + 1 = 12a - 3b + c + \theta(-5a + 3b) + (-3a + b + c)$. Odavde: $12a - 3b + c = 0$, $-5a + 3b = 2$, $-3a + b + c = 1$.

Iz ovog sistema nalazimo $a = \frac{1}{5}$, $b = 1$, $c = \frac{3}{5}$ pa je $\frac{2\theta + 1}{\theta^2 + 1} = \frac{1}{5}\theta^2 + \theta + \frac{3}{5}$, čime je dobijen traženi normalni oblik.

Rešenje 2. Potražimo Euklidovim algoritnom najveci zajednički delilac polinoma $x^2 + 1$ i $x^3 + 3x^2 - 2x - 1$. Iz jednakosti: $x^3 + 3x^2 - 2x - 1 = (x^2 + 1)(x + 3) + (-3x - 4)$; $x^2 + 1 = (-3x - 4)(-\frac{x}{3} + \frac{4}{9}) + \frac{25}{9}$

eliminacijom $(-3x - 4)$ dobijamo:

1/ $(x^3 + 3x^2 - 2x - 1)(3x-4) + (x^2 + 1)(-3x^2 - 5x + 21) = 25$,

pa su navedeni polinomi relativno prosti. Iz /1/ za $x = \theta$ dobijamo:

$$\frac{1}{(\theta^2 + 1)} = \frac{1}{25(-3\theta^2 - 5\theta + 21)}$$, pa je $\frac{2\theta + 1}{\theta^2 + 1} =$

$= \frac{1}{25}(2\theta + 1)(-3\theta^2 - 5\theta + 21) = \frac{1}{25}(-6\theta^3 - 13\theta^2 + 37\theta + 21)$.

Kako je $\theta^3 = -3\theta^2 + 2\theta + 1$, imamo $\frac{2\theta + 1}{\theta^2 + 1} = \frac{1}{5}\theta^2 + \theta + \frac{3}{5}$, što smo i prvim načinom našli.

Zadatak 79. Neka je $\theta^3 - 3\theta + 3 = 0$. Dokazati da $\mu = \theta^2 - 1$ zadovoljava jednačinu

$$\mu^3 - 3\mu^2 - 5 = 0.$$

Dokazati da je: $\theta = \frac{2}{3} + \sqrt[3]{\frac{u}{3}} - \frac{v}{3}$.

Zadatak 80. Dokazati da $z = x_1x_2 + x_3x_4$, gde su x_1, x_2, x_3, x_4 koreni jednačine $x^4 + a_1x^3 + a_2x^2 + a_4 = 0$ / a_1, a_2, a_3, $a_4 \in Ra$, ima grupu reda 8 i dokazati da je

$$z^3 - a_2z^2 + (a_1a_3 - 4a_4)\, z - a_4(a_1^2 - 4a_2) - a_3^2 = 0$$

Zadatak 81. Polje Ra (θ) nastalo je iz polja Ra adjunkcijom θ , definisanim sa $\theta^3 - 5\theta^2 + 2\theta + 1 = 0$. Naći recipročan element elementu $1 + \theta + \theta^2$.

Rešenje. Polinom $x^3 - 5x^2 + 2x + 1$ je nesvodljiv u polju Ra / jer nema ni jedan racionalan koren / pa su polinomi $x^3 - 5x^2 + 2x + 1$ i $x^2 + x + 1$ relativno prosti. Znači postoje polinomi P /x/ i Q/x/ takvi da je $1 = P\,/x/\,(x^2+x+1) + Q\,/x/\,(x^3 - 5x^2 + 2x + 1)$. Polinome P /x/ i Q /x/ ćemo odrediti Euklidovim algoritmom.

$$x^3 - 5x^2 + 2x + 1 = (x^2 + x + 1)(x - 6) + (7x + 7)$$

$$x^2 + x + 1 = (7x + 7) \cdot \tfrac{1}{7}x + 1$$

Smenom polinoma $7x + 7$ iz prve u drugu jednačinu dobijamo:

$$x^2 + x + 1 = \left[(x^3 - 5x^2 + 2x + 1) - (x^2 + x + 1)(x - 6)\right] \cdot \tfrac{1}{7}x + 1$$

odakle $1 = (x^2 + x + 1)(\frac{x^2}{7} - \frac{6}{7}x + 1) - \frac{1}{7}x(x^3 - 5x^2 + 2x + 1)$ (*)

Znači $P\,/x/ = \frac{x^2}{7} - \frac{6}{7}x + 1$; $Q\,/x/ = -\frac{1}{7}x$.

Smenom u / * / $x = \theta$ imamo

$1 = (\theta^2 + \theta + 1) \cdot (1 - \frac{6}{7}\theta + \frac{1}{7}\theta^2)$ pa je traženi recipročan element : $1 - \frac{6}{7}\theta + \frac{1}{7}\theta^2$.

Zadatak 82 . Polju Ra je adjungovan element θ definisan preko $\theta^2 - \theta + 1 = 0$. Dokazati da skup Ra (θ) čini polje. Naći grupu automorfizama ovog polja.

Rešenje. Skup Ra(θ) je skup svih izraza $a_1+a_2\theta$ gde a_1, $a_2 \in$ Ra . Pošto je jednačina $\theta^2 - \theta + 1 = 0$ nesvodljiva na polju Ra to je $a_1 + a_2\theta = b_1 + b_2\theta$ ako i samo ako je $a_1 = b_1$, $a_2 = b_2$.

I. Skup $\{a_1 + a_2\theta\}$ u odnosu na sabiranje čini Abelovu grupu jer :

1/ $(a_1+ a_2\theta)+(b_1+ b_2\theta) =(a_1+ b_1) + (a_2 + b_2)\theta$

2/ $(a_1+ a_2\theta) +(b_1+b_2\theta) = (b_1+ b_2\theta)+(a_1+a_2)$

3/ $\left[(a_1+ a_2\theta)+(b_1+ b_2\theta)\right] +(c_1+ c_2\theta)=(a_1+ a_2\theta) +\left[(b_1+ + b_2\theta)+(c_1 + c_2\theta)\right]$

4/ $0 = 0 + 0.\theta \in$ Ra .

5/ $-(a_1 + a_2\theta) =+(-a_2) \theta + (-a_1)$ tj. svaki element ima inverzni element u odnosu na sabiranje.

II. Skup $S' = \{a_1 + a_2\theta\}$ gde $a_1 + a_2\theta \neq 0 + 0.\theta$ čini Abelovu multiplikativnu grupu jer:

1/ Ako je $a_1+a_2\theta \in S'$, $b_1 + b_2\theta \in S'$, onda

$(a_1+ a_2\theta) .(b_1+ b_2\theta) = a_1b_1 + a_1b_2\theta + a_2b_2\theta^2 = a_1b_1 + a_1b_b\theta +$

$+ a_2b_1\theta + a_2b_2\theta - 1)=(a_1b_1 - a_2b_2)+(a_1b_2 + a_2b_1 + a_2b_2)\theta (S'$

jer ako je $a_1 + a_2\theta$ $b_1 + b_2\theta \neq 0 + 0.\theta$ onda je i

$(a_1+ a_2\theta) . (b_1+ b_2\theta) \neq 0 + 0.\theta$.

2/ $(a_1+ a_2\theta) . (b_1+ b_2\theta) = (b_1+ b_2\theta).(a_1+ a_2\theta)$

3/ $\left[(a_1+a_2\theta).(b_1+ b_2\theta)\right]. (c_1+ c_2\theta) = (a_1+ a_2\theta).$ [

$[(b_1 + b_2\theta) \cdot (c_1 + c_2\theta)]$

4/ $1 = 1 + 0\,\theta \in S'$

5/ Neka $a_1 + a_2\theta \in S'$, polinomi $a_1 + a_2x$ i x^2-x+1 su relativno prosti pa postoje polinomi $P(x)$ i $Q(x)$ takvi da je

$$1 = P(x) \cdot (a_1 + s_2x) + Q(x) \cdot (x^2-x+1).$$

Odavde za $x = \theta$, zbog $\theta^2 - \theta + 1 = 0$ imamo $1 = P(\theta) \cdot (a_1 + a_2\theta)$, pa je $P(\theta)$ inverzan element elemenata $a_1 + a_2\theta$. Naravno $P(\theta) \in S'$, jer se može dovesti na oblik $b_1 + b_2\theta$ i $P(\theta) \neq 0$. Znači ma koji element $a_1 + a_2\theta \neq 0$ ima ima inverzan element za množenje.

III. Ispunjen je distributivni zakon množenja prema sabiranju.

Stoga je $Ra(\theta)$ polje.

Neka je ϕ ma kakav automorfizam polja $Ra(\theta)$. Tada je

$$(a_1 + a_2\theta)\phi = a_1\phi + a_2\phi \cdot \theta\phi = a_1 + a_2\theta\phi$$

pa će biti definisan ako odredimo $\theta\phi$, jer $a_n\phi = a_n$ prema zadatku 58. Kako je $\theta^2 - \theta + 1 = 0$ to $0\phi = (\theta^2 - \theta + 1)\phi = \theta^2\phi - \theta\phi + 1\phi = (\theta\phi)^2 - (\theta\phi) + 1$, tj. $(\theta\phi)^2 - (\theta\phi) + 1 = 0$, pa je ili θ ili $1 - \theta = \theta_2$, gde je θ_2 drugi koren jednačine $\theta^2 - \theta + 1 = 0$. Prvo rešenje $\theta\phi = \theta$ daje identičko preslikavanje I.

Proverimo da li je preslikavanje ϕ, za koje je $\theta\phi = \theta_2$ automorfizam. Preslikavanje ϕ je biunivoko. Dalje

$$[(a_1 + a_2\theta) + (b_1 + b_2\theta)]\phi = [(a_1 + b_1) + (a_2 + b_2)\theta]\phi =$$

$=(a_1+ b_1) + (a_2+ b_2)\,\theta_2 = (a_1+ a_2\theta_2)+(b_1+ b_2\theta^2) =$

$=(a_1+ a_2\theta)\phi + (b_1+ b_2\theta)\phi .$

$[(a_1+ a_2\theta) . (b_1+ b_2\theta)]\phi = [a_1b_1+ a_1b_2 + a_2b_1\theta + a_2b_2\theta^2]\phi =$

$=[(a_1b_1 - a_2a_2) +(a_1b_2 + a_2b_1 + a_2b_2)\theta]\phi =$

$= a_1b_1 - a_2b_2 +(a_1b_2 + a_2b_1 + a_2b_2)\theta_2 =$

$=(a_1+ a_2\theta_2 . (b_1 + b_2\theta_2) = (a_1+ a_2\theta)\phi(b_1+b_2\theta)\phi$, tj. ϕ

je zaista automorfizam.

Grupa automorfizama je G = I, .

Zadatak 83. Data je jednačina

$$x^4 + 1 = 0$$

1/ Dokazati da je jednačina nesvodljiva na polju Ra

2/ Dokazati da je jednačina normalna

3/ Adjunkcijom radikala formirati polje korena jednačine.

4/ Naći grupu automorfizama ko renskog polja i permutacionu grupu jednačine.

Rešenje. 1/ Jednačina $x^4 + 1 = 0$ nema racionalnih korena pa polinom $x^4 + 1$ nema linearnih racionalnih faktora. Pokažimo da nema ni kvadratnih racionalnih faktora. Pretpostavimo obrnuto da je

$$x^4 + 1 = (x^2 + px + q) (x^2 + sx + t)$$

gde $p, q, s, t \in Ra$. Odavde dobijamo sistem

$p + s = 0$ $\qquad$ $pt + qs = 0$

$ps + q + t = 0$ $\qquad$ $qt = 1$

Smenom $s = - p$ iz prve u ostale jednačine dobijamo sistem:

$$q + t - p^2 = 0 \qquad /1/$$

$$p/t - q/ = 0 \qquad /2/$$

$$qt = 1 \qquad /3/$$

Iz /2/ je $p = 0$ ili $t = q$. Ako bi bilo $p = 0$ onda bi /1/ T /3/ daje $q + t = 0$, $qt = 1$, što je nemoguće, a ako bi bilo $t = q$ onda prema /1/ i /3/ je $2q - p^2 = 0$, $q^2 = 1$ što je takodje nemoguće ako $p, q \in Ra$.

Znači $x^4 + 1$ je nesvodljiv na polju Ra.

2/ Označimo jedan koren jednačine sa ρ. Onda su ostali koreni $-\rho, \frac{1}{\rho}, -\frac{1}{\rho}$ jer je jednačina simetrična bikvadratna jednačina.

3/ Koreni jednačine su:

$$x_{k+1} = e^{\frac{2k+1}{4}\pi i}$$

gde je $k = 0, 1, 2, 3,$ tj.

$$x_1 = \frac{1}{2}(\sqrt{2} + \sqrt{-2}) ; \quad x_2 = \frac{1}{2}(-\sqrt{2} + \sqrt{-2}) ;$$

$$x_3 = \frac{1}{2}(-\sqrt{2} - \sqrt{-2}) ; \quad x_4 = \frac{1}{2}(\sqrt{2} - \sqrt{-2}) .$$

Polje korena jednačine $Ra(\sqrt{2}, \sqrt{-2})$. Ma koji element ovog polja je oblika

$$a + b\sqrt{2} + c\sqrt{-2} + d\sqrt{2}.\sqrt{-2}$$

gde $a, b, c, d \in Ra$. Polje korena je takodje i

$Ra(\rho) = Ra(\sqrt{2} + \sqrt{-2})$, jer je jednačina normalna.

4/ Automorfizmi polja $Ra(\sqrt{2}, \sqrt{-2})$ su dati tablicom:

	I	A	B	C
2	2	- 2	2	- 2
-2	-2	-2	- -2	- -2

Lako zaključujemo jednakosti

$$A^2 = B^2 = I , \qquad AB = BA = C$$

pa je grupa automorfizama

$$G = \{ I, \ A, \ B, \ AB \}$$

tj. Klein-ova vierer grupa . Primenom automorfizama I, A, B, AB na niz (x_1, x_2, x_3, x_4) dobijamo:

$$(x_1, x_2, x_3, x_4) I = (x_1, x_2, x_3, x_4)$$

$$(x_1, x_2, x_3, x_4)A = (x_2, x_1, x_4, x_3)$$

$$(x_1, x_2, x_3, x_4)B = (x_4, x_3, x_2, x_1)$$

$$(x_1, x_2, x_3, x_4)AB = (x_3, x_4, x_1, x_2)$$

Znači permutaciona grupa jednačine je:

$$G = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \right\} =$$

$$= \{ (1) , \ (12)(34), \ (13)(24), \ (14)(23) \} .$$

Zadatak 84. Naći permutaciönu grupu jednačine

$$x^3 - 1 = 0$$

na polju Ra.

Rešenje. Po definiciji permutaciona grupa jednačine $p_n/x/ = 0$ na polju F je skup S svih permutacija iz S_n koje imaju svojstvo:

A/ Ako je $\varphi(x_1, x_2, \dots , x_n) = 0$ ma koja racionalna relacija izmedju korena jednačine $p_n/x/ = 0$ sa koeficijentima u polju F onda primenom ma koje permutacije iz S ta jednakost opet postaje jednakost.

B/ Ako je $\varphi(x_1 , x_2 , \dots , x_n)$ racionalna

funkcija korena sa koeficijentima iz F i ako $\varphi S = \varphi$ onda je $\varphi(x_1, x_2, \dots x_n)$ jednako nekom broju iz polja F .

Data jednačina ima jedan koren 1. Označimo ga sa x_1. Ostali koreni su $x_2 = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ i $x_3 = -\frac{1}{2} - \frac{\sqrt{-3}}{2}$.

Napišimo sada nekoliko relacija izmedju korena x_1 , x_2, x_3 u polja Ra. Takve su:

1/ $x_1 = 1$ 5/ $x_3^3 - 1 = 0$

2/ $x_2 + x_3 = -1$ 6/ $x_1 + x_2 + x_3 = 0$

3/ $x_1^3 - 1 = 0$ 7/ $x_1x_2 + x_1x_3 + x_2x_3 = 0$

4/ $x_2^3 - 1 = 0$ 8/ $x_1x_2x_3 = 1$

Označimo grupu jednačine sa S. Simetrična grupa S_3 ima permutacije (1), (12), (13), (123), (132), (23) . Odredimo medju njima one koje ove jednakosti prevode u jednakosti, mi ćemo kratko reći one koje ne menjaju ove relacije. Permutacija (12) relaciju 3/ prevodi u $x_2^3 - 1 = 0$ što je tačno, tj. ona ne menja relaciju 3/, ali (12) menja relaciju 1/ jer je prevodi u $x_2 = 1$ što nije tačno. Znači (12) $\notin$ S . Permutacija (13) prevodi relaciju 1/ u $x_3 = 1$, što nije. Znači (13) $\notin$ S . Zbog istog razloga i (132) $\notin$ S. Permutacija (123) prevodi 1/ u $x_2 - 1$, što nije (123) $\notin$ S .

Kao "kandidati " za grupu jednačine su ostale permutacije (1), (23). Pošto je grupa jednačine grupa, to će grupa jednačine biti ili (1) ili (1), (23). Pokazaćemo da grupa jednačine nije (1). Pretpostavimo obrnuto da je grupa (1). Funkcija $x_1 + 8x_2 + 7x_3$ ima grupu (1), jer iz S_3 nju ne menja samo (1). Prema svojstvu B ova funkcija je jednaka nekom broju iz Ra, što ova očigledno nije jer je

$$x_1 + 8x_2 + 7x_3 = 1 + 8\left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right) + 7\left(-\frac{1}{2} - \frac{\sqrt{-3}}{2}\right) \notin \text{Ra} .$$

Znači grupa jednačine nije (1) već je (1), (23) .

Zadatak 85. Naći permutacionu grupu jednačine

$$x^3 - 9x + 9 = 0$$

u polju Ra.

Rešenje. Primetimo odmah da jednačina nema ni jedan racionalan koren, pa je nesvodljiva. Permutaciona grupa nesvodljive jednačine, prema poznatoj teoremi je trantitivna. Grupa S_3 ima ove tranzitivne podgrupe:

$$A_3 = \{(1),\ (123),\ (132)\} \text{ i } S_3 .$$

Da bismo odlučili da li je grupa A_3 ili S_3 potražimo dikriminantu Δ. Ona je

$$\Delta = -4p^3 - 27q^2 = -4(-9)^3 - 27.9^2 = 27^2$$

Pošto je

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{\Delta}$$

to ova relacija je

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{27}$$

u polju Ra. Nju menjaju permutacije iz $S_3 - A_3$ pa grupa ne može biti S_3 . Znači grupa jednačine je A_3.

Zadatak 86. Izvesti diskusiju permutacione grupe kubne jednačine

$$x^3 + ax^2 + bx + c = 0$$

u polju Ra, gde su njeni koeficijenti a, b, c .

Rešenje. Razlikovaćemo dva slučaja :

I slučaj : Jednačina je nesvodljiva u polju Ra. Tada joj grupa mora biti tranzitivna, tj. ili je A_3 ili S_3 . Ako $\sqrt{\Delta} \notin$ Ra onda je grupa S_3 a ako $\sqrt{\Delta} \in$ Ra onda je A_3 .

II slučaj: jednačina je svodljiva u polju Ra. Ovde ćemo razlikovati dva slučaja prema tome da li jednačina ima samo jedan racionalan koren ili sva tri.

Ako ima samo jedan racionalan koren i ako njega označimo sa x_1 onda je grupa jednačine (1) , (23)

Ako jednačina ima sva tri racionalna korena onda joj je grupa (1) jer (1) prvo ne menja bilo koju relaciju medju korenima i drugo bilo koja racionalna funkcija korena sa koeficijentima iz Ra je jednaka racionalnom broju. Ispunjeni su znači zahtevi A i B definicije grupe pa je (1) zaista grupa.

Zadatak 87. Obrazovati jednačinu $p/x/ = 0$ najnižeg stepena u polju Ra koju zadovoljava $u = \sqrt{2} + \sqrt{3}$

1/ Dokazati da je polje korena jednačine Ra /u/

2/ Dokazati da je Ra u = Ra ($\sqrt{2}, \sqrt{3}$)

3/ Naći sva podpolja polja Ra ($\sqrt{2}, \sqrt{3}$)

4/ Naći grupu automorfizama polja Ra ($\sqrt{2}$, $\sqrt{3}$), sve njene podgrupe kao i odgovarajuća podpolja polja Ra ($\sqrt{2}, \sqrt{3}$) u kojima su te podgrupe grupe date jednačine.

5/ Ispitati svodljivost polinoma $p/x/$ u svim podpoljima njegovog korenskog polja.

Rešenje. 1/ Pošto $\sqrt{2} + \sqrt{3}$ treba da bude koren jednačine sa racionalnim koeficijentima to njeni koreni moraju biti i $-\sqrt{2} + \sqrt{3}$, $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} - \sqrt{3}$. Prema tome jednačina najnižeg stepena zadovoljena brojem $\sqrt{2} + \sqrt{3}$ je četvrtog stepena. Nju ćemo ovako obrazovati:
$x = \sqrt{2} + \sqrt{3}$, $x - \sqrt{2} = \sqrt{3}$. Kvadriranjem dobijamo:
$x^2 - 2\sqrt{2}\, x + 2 = 3$, $x^2 - 1 = 2\sqrt{2}\, x$, odavde je :
$x^4 - 2x^2 + 1 = 8x^2$ tj. $x^4 - 10x^2 + 1 = 0$.

Kao $p/x/$ možemo uzeti $p/x/ = x^4 - 10x^2 + 1$. Ma koji element polja Ra u se jedinstveno može napisati u obliku $a_0 + a_1 u + a_2 u^2 + a_3 u^3$. Pošto su koreni polinoma $p/x/$ $x_1 = u$, $x_2 = -u$, $x_3 = \frac{1}{u} = 10u - u^3$, $x_4 = -\frac{1}{u} = u^3 - 10u$, to zaključujemo da je polje korena jednačine $p/x/ = 0$ zaista

Ra u jer svi koreni su u njemu.

2/ Ma koji element polja Ra $(\sqrt{2}, \sqrt{3})$ se može prikazati u obliku $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\cdot\sqrt{3}$ / $a,b,c,d \in Ra$/. Pošto je $u = \sqrt{2} + \sqrt{3}$ to $u \in Ra(\sqrt{2}, \sqrt{3})$ pa je $Ra(\sqrt{2}, \sqrt{3}) \supset Ra(u)$ Pokažimo i obrnuto. Dovoljno je pokazati da je $\sqrt{2}$ i $\sqrt{3} \in Ra(u)$.

Iz $u = \sqrt{2} + \sqrt{3}$ imamo $u - \sqrt{2} = \sqrt{3}$, a kvadriranjem $u^2 - 2u\sqrt{2} + 2 = 3$ tj. $\sqrt{2} = \frac{u^2 - 1}{2u} \in Ra(u)$. Iz $\sqrt{3} = u - \sqrt{2}$ sleduje $\sqrt{3} \in Ra(u)$, pa je dokazano da je $Ra(\sqrt{2}, \sqrt{3}) \in Ra(u)$

Znači $Ra(u) = Ra(\sqrt{2}, \sqrt{3})$.

3/ Ma koje podpolje polja $Ra(\sqrt{2}, \sqrt{3})$ sadrži 1 i 0. Otuda sadrži Ra. Pošto je ma koji element polja $Ra(\sqrt{2}, \sqrt{3})$ oblika $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\cdot\sqrt{3}$, $a,b,c,d \in Ra$, mogu se napisati ovi slučajevi:

I slučaj : Podpolje polja $Ra(\sqrt{2}, \sqrt{3})$ sadrži $\sqrt{2}$ a ne sadrži $\sqrt{3}$ i $\sqrt{2}\cdot\sqrt{3}$. To je podpolje $Ra(\sqrt{2})$.

II slučaj : Podpolje polja $Ra(\sqrt{2}, \sqrt{3})$ sadrži $\sqrt{3}$ a ne sadrži $\sqrt{2}$ i $\sqrt{3}\cdot\sqrt{2}$. To je podpolje $Ra(\sqrt{3})$.

III slučaj: Podpolje $Ra(\sqrt{2}\sqrt{3})$ sadrži $\sqrt{2}\cdot\sqrt{3}$, a ne sadrži $\sqrt{2}$ i $\sqrt{3}$. To je podpolje $Ra(\sqrt{2}\cdot\sqrt{3}) = \{a + d\sqrt{2}, \sqrt{3}\}$ gde $a, d \in Ra$.

IV slučaj : Podpolje polja $Ra(\sqrt{2}, \sqrt{3})$ sadrži dva od iracionaliteta $\sqrt{2}$, $\sqrt{3}$ i $\sqrt{2}\cdot\sqrt{3}$. Lako zaključujemo da je onda to podpolje samo polje $Ra(\sqrt{2}, \sqrt{3})$.

V. slučaj : Podpolje polja $Ra(\sqrt{2}, \sqrt{3})$ ne sadrži ni jedan od elemenata $\sqrt{2}$, $\sqrt{3}$, $\sqrt{2}\cdot\sqrt{3}$. To je Ra.

Znači sva podpolja su : $Ra(\sqrt{2})$, $Ra(\sqrt{3})$, $Ra(\sqrt{2}\cdot\sqrt{3})$ i $Ra(\sqrt{2}, \sqrt{3})$.

4/ da bismo definisali automorfizam dovoljno je navesti elemente u koje se preslikavaju $\sqrt{2}$ i $\sqrt{3}$ jer racionalni brojevi moraju biti invarijantni. Neka je ma

koji automorfizam tada iz $(\sqrt{2})^2 - 2 = 0$ i $(\sqrt{3})^2 - 3 = 0$ sleduje $(\sqrt{2}\phi)^2 - 2 = 0$ i $(\sqrt{3}\phi)^2 - 3 = 0$ / slično kao u zadatku 82/ . Odavde je $\sqrt{2}\phi$ ili $\sqrt{2}$ ili $-\sqrt{2}$ i $\sqrt{3}\phi$ ili $\sqrt{3}$ ili $-\sqrt{3}$. Uzimajući razne mogućnosti zaključujemo da automorfizmi mogu biti samo preslikavanja I,A,B,C data tablicom

	I	A	B	C
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$

Može se dokazati da su ova preslikavanja zaista automorfizmi. Mi ćemo to dokazati za C. Zaista

$$\left[(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\cdot\sqrt{3}) + (\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{2}\cdot\sqrt{3})\right] C =$$

$$= \left[(a+\alpha) + (b+\beta)\sqrt{2} + (c+\gamma)\sqrt{3} + (d+\delta)\sqrt{2}\cdot\sqrt{3}\right] C =$$

$$= (a+\alpha) + (b+\beta)(-\sqrt{2}) + (c+\gamma)(-\sqrt{3}) + (d+\delta)(-\sqrt{2})(-\sqrt{3}) =$$

$$= \left[(a + b\sqrt{-2}) + c(-\sqrt{3}) + d(-\sqrt{2})(-\sqrt{3})\right] + \left[\alpha + \beta(-\sqrt{2}) + \right.$$

$$\left. + \gamma(-\sqrt{3}) + \right.$$

$$+ \delta(-\sqrt{2})(-\sqrt{3}) = (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3})\, C +$$

$$+ (\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{2}\sqrt{3})\, C \quad \text{i}$$

$$\left[(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3})\cdot(\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{2}\sqrt{3})\right] C =$$

$$= \left[a\alpha + a\beta\sqrt{2} + a\gamma\sqrt{3} + ad\sqrt{2}\sqrt{3} + b\alpha\sqrt{2} + b\beta 2 + \right.$$

$$\left. + b\gamma\sqrt{2}\sqrt{3} + \right.$$

$$+ b\delta 2\sqrt{3} + c\alpha\sqrt{3} + c\beta\sqrt{2}\sqrt{3} + c\gamma 3 + c\delta\sqrt{2}\sqrt{3}\, d\alpha\sqrt{2}\sqrt{3} +$$

$$+ d\,2\,3 + d\,3 + 6d \quad C = a + (-2) + a(-3) +$$

$$+ a(-2)(-3) + b(-2) + b\,2 + b(-3) + b\,2.(-3) +$$

$$+ c(-3) + c(-2)(-3) + c\,3 + c(-2).3 + d(-2).$$

$$.(-3) +$$

$$+ d\,2(-3) - d\,.3(-2) + d = a + b(-2) + c(-3) +$$

$$+ d(-2)(-3) \qquad (-2) + (-3) + (-2)(-3) =$$

$$= (a + b\,2 + c\,3 + d\,2\,3)\, C \quad (\quad 2 + \quad 3 + \quad 2\,.\,3)C.$$

U skupu automorfizama nadjimo generatorne. Nadjimo A.B. Radi toga nadjimo $\sqrt{2}$ AB i $\sqrt{3}$ AB.

$$\sqrt{2}\ AB = (\sqrt{2}\ A)B = (-\sqrt{2})B = -(\sqrt{2}\ B) = -\sqrt{2}$$

$$\sqrt{3}\ AB = (\sqrt{3}\ A)B = \sqrt{3}\ B = -\sqrt{3}$$

Odavde zaključujemo $AB = C$. Na sličan način dobijamo $A^2 = B^2 = I$. $AB = BA$. Znači kao generatorni se mogu uzeti A i B pa je tražena grupa automorfizam.

$$G = I, A, B, AB$$

a njena multiplikativna tablica:

	I	A	B	AB
I	I	A	B	AB
A	A	I	AB	B
B	B	AB	I	A
AB	AB	B	A	I

Nadjimo sada podgrupe ove grupe. One mogu biti reda 1, 2, i 4 / činitelji reda grupe/. Reda 1 i 4 su podgrupe $H_1 = \{I\}$ i $G = \{I, A, B, AB\}$. Podgrupe reda 2, pošto je 2 prost broj, moraju biti ciklične. To su $H_2 = \{I, A\}$, $H_3 = \{I, B\}$, $H_4 = \{I, AB\}$.

Nadjimo podpolje čiji se elementi ne menjaju primenom automorfizama podgrupe H_2. Ma koji element polja $Ra(\sqrt{2}, \sqrt{3})$ je $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$. Potrebno i dovoljno da se ne menja primenom automorfizama iz H_2 je da:

$$(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3})\ A = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$$

tj. $a - b\sqrt{2} + c\sqrt{3} - d\sqrt{2}\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$.

Odavde $b = d = 0$ pa skup $a + c\sqrt{3} \in Ra(\sqrt{3})$ je traženo podpolje. Analogo elementi podpolja $Ra(\sqrt{2})$ se ne menjaju primenom automorfizama $H_3 = \{I, B\}$ a elemente

podpolja Ra ($\sqrt{2}, \sqrt{3}$) ne menjaju automorfizmi $H_4 = \{I, AB\}$.

Prema definiciji grupa jednačine u nekom podpolju korenskog polja jednačine je skup svih automorfizama korenskog polja koji ne menjaju elemente tog podpolja. Tako je u polju Ra grupa jednačine G, u polju Ra ($\sqrt{2}$) je H_3, u polju Ra($\sqrt{3}$) je H_2, u polju Ra($\sqrt{2} \cdot \sqrt{3}$) je H_4 a u polju Ra ($\sqrt{2}, \sqrt{3}$) je H_1.

5/ Radi ispitivanja svodljivosti polinoma p/x nadjimo permutacionu grupu jednačine.

Korene jednačine označimo sa $x_1 = \sqrt{2} + \sqrt{3}$,

$x_2 = -\sqrt{2} - \sqrt{3}$, $x_3 = -\sqrt{2} + \sqrt{3}$, $x_4 = \sqrt{2} - \sqrt{3}$.

Primenom automorfizama na korene neposredno dobijamo odgovarajuće permutacije iz permutacione grupe.

$(x_1, x_2, x_3, x_4)\ I = (x_1, x_2, x_3, x_4)$ $I\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=(1)$

$(x_1, x_2, x_3, x_4)\ A = (x_3, x_4, x_1, x_2)$ $A-\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(13)(24)$

$(x_1, x_2, x_3, x_4)\ B = (x_4, x_3, x_2, x_1)$ $B-\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(14)(23)$

$(x_1, x_2, x_3, x_4)\ AB = (x_2, x_1, x_4, x_3)$ $AB-\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(12)(34)$

Grupe jednačine i svodljivost u raznim podpoljima korenskog polja ćemo ovako tablicom izraziti:

Podpolje	Grupa jednačine	Tranzitivnost grupe	Svodljivost p/x/
Ra	1 , 12 34 , 13 24, 14 23	Tranzitivna	Nesvodljiv
Ra 2	1 , 14 23	Netranzitivna	Svodljiv
Ra 3	1 , 13 24	Netranzitivna	Svodljiv

./.

Ra 2. 3	1, 12 34	Netranzitivna svodljiv
Ra 2, 3	1,	Netranzitivna Svodljiv

Na primeru ćemo pokazati kako se faktorizacija u nekom području polja Ra $(\sqrt{2},\sqrt{3})$ može izvršiti. Izvršićemo faktorizaciju polinoma Ra $(\sqrt{2})$.

Pre svega je

$$p/x/ = (x - x_1)(x - x_2)(x - x_3)(x - x_4)$$

Ovo je faktorizacija u Ra $(\sqrt{2},\sqrt{3})$. Pošto $(x - x_4)$ i $(x - x_2)(x - x_3)$ se ne menjaju primenom permutacija (1), (14) (32) tj. grupe jednačina u Ra $(\sqrt{2})$ to $(x - x_4)$ i $(x - x_2)(x - x_3)$ su polinomi na polju Ra $(\sqrt{2})$. Zaista:

$$(x-x_1)(x-x_4) = (x-\sqrt{2} \quad -\sqrt{3})(x+\sqrt{3}-\sqrt{2}) = (x-2)^2 - 3 = x^2 - 2x\sqrt{2} - 1 \quad \text{i}$$

$$(x-x_2)(x-x_3) = (x+\sqrt{2}+\sqrt{3})(x-\sqrt{3}+\sqrt{2}) = (x+\sqrt{2})^2 - 3 = x^2 + 2x\sqrt{2} - 1$$

pa je faktorizacija polinoma p/x/ u Ra$(\sqrt{2})$.

$$P/x/ = (x^2 - 2x\sqrt{2} - 2)(x^2 + 2x\sqrt{2} - 1).$$

Zadatak 88. Data je jednačina

$$p/x/ \quad x^3 - 3x + 1 = 0$$

a/ Dokazati da je nesvodljiva u polju Ra

b/ Dokazati da je jednačina normalna u odnosu na polje Ra i naći x_2 i x_3 preko x_1.

c/ Naći permutacionu grupu jednačine u Ra.

Rešenje. a/ jednačina $x^3 - 3x + 1 = 0$ nema racionalnih korena pa je otuda p/x/ nesvodljiv polinom na polju Ra.

b/ Treba dokazati da ako je jedan koren jednačine $x_1 = \rho$ da su x_2 i x_3 polinomi po ρ na polju Ra, tj. da su u Ra (ρ) čiji su elementi oblika:

$$a + b\rho + c\rho^2 \; ; \quad a, b, c \in Ra.$$

Predpostavljajući da je jedan koren $x_1 = \rho$ potražićemo x_2 i x_3. Kako je:

$$x^3 - 3x + 1 = (x - \rho)(x^2 + \rho x + \rho^2 - 3) + \rho^3 - 3\rho + 1 =$$

$$= (x - \rho)\, x^2 + \rho x + \rho^2 - 3).$$

to ostala dva korena dobijamo iz jednačine

$$x^2 + \rho x + \rho^2 - 3 = 0$$

Iz nje $x_2 = \frac{1}{2}(-\rho + \sqrt{12 - 3\rho^2})$; $x_3 = \frac{1}{2}(-\rho - \sqrt{12 - 3\rho^2})$.

Da bi x_2 i $x_3 \in Ra(\rho)$ potrebno je i dovoljno da postoje racionalni brojevi a, b, c takvi da je

$$12 - 3\rho^2 = (a + b\rho + c\rho^2)^2 \qquad /*/$$

Potražimo ih iz ove jednakosti koja posle uprošćenja i uzimanja u obzir $\rho^3 = 3\rho - 1$ postaje:

$$12 - 3\rho^2 = (a^2 - 2bc) + \rho(2ab + 6bc - c^2) + \rho^2(b^2 + 3c^2 + 2ac)$$

odavde dobijamo sistem jednačina:

$$1/\; a^2 - 2bc = 12$$

$$2/\; 2ab + 6bc - c^2 = 0$$

$$3/\; b^2 + 3c^2 + 2ac = -3$$

Množenjem treće jednačine sa 4 i sabiranjem sa prvom dobijamo

$$a^2 + 4b^2 + 12c^2 + 8ac - 2bc = 0$$

Uočimo sada sistem:

$$4/\; 2ab + 6bc - c^2 = 0$$

$$5/\; a^2 + 4b^2 + 12c^2 + 8ac - 2bc = 0$$

Iz jednačina 1/, 2/, 3/ zaključujemo da $c \neq 0$. Deleći 4/ i 5/ sa c^2 i stavljajući $\frac{a}{c} = X$, $\frac{b}{c} = Y$ dobijamo

$$2XY + 6Y - 1 = 0$$

$$X^2 + 4Y^2 + 8X - 2Y + 12 = 0$$

Eliminacijom X iz ovih jednačina dolazimo do jednačine:

$$16Y^4 - 8Y^3 - 12Y^2 + 4Y + 1 = 0 \text{ ili}$$

$$2Y^4 - 2Y^3 - 3\ 2Y^2 + 2\ 2Y + 1 = 0.$$

Ovde zaključujemo da je jedino racionalno rešenje za Y, $Y = \frac{1}{2}$. Kako je $X = \frac{1 - 6Y}{2Y}$ to je $X = -2$. Iz jednakosti $\frac{a}{c} = X$, $\frac{b}{c} = Y$ nalazimo $\frac{a}{c} = -2$, $\frac{b}{c} = \frac{1}{2}$. Brojeve a, b i c sada tražimo iz sistema:

$$a = -2c$$
$$b = \frac{1}{2}c$$
$$a^2 - 2bc = 12$$

Iz njega dobijamo dva rešenja za a,b, c . Uzimamo jedno od njih $a = 4$, $b = -1$, $c = -2$ jer drugo rešenje $a = -4$, $b = 1$, $c = 2$ daje isto rešenje za x_2 i x_3. Jednakost/ + / postaje:

$$-(12 - 3\rho)^2 = (4 - \rho - 2\rho^2)^2$$

a koreni su:

$$x_2 = \frac{1}{2}(-\rho + 4 - \rho - 2\rho^2) = 2 - \rho - \rho^2$$

$$x_3 = \frac{1}{2}(-\rho - 4 + \rho + 2\rho^2) = -2 + \rho^2.$$

I tako je dokazano da je jednačina

$$x^3 - 3x + 1 = 0$$

normalna na polju Ra.

c/ Korensko polje jednačine je $Ra(\rho)$. Automorfizmi ovog polja I, A, B su dati tablicom:

	I	A	B
ρ		$2 - \rho - \rho^2$	$-2 + \rho^2$

Označimo korene sa $x_1 = \rho$, $x_2 = 2 - \rho - \rho^2$, $x_3 = -2 + \rho^2$ Tada je

$(x_1, x_2, x_3)\, I = (x_1, x_2, x_3)$ znači $I \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)$

$(x_1, x_2, x_3)A = (x_2, x_3, x_1)$ znači $A \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$

$(x_1, x_2, x_3)\, B = (x_3, x_1, x_2)$ znači $B \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$

jer na primer $x_2 A = (\rho - \rho - \rho^2)A = \rho - (\rho A) - (\rho A)^2 =$

$= \rho - (\rho - \rho^2) - (\rho - \rho - \rho^2)^2 = \rho + \rho^2 - \rho^2 - \rho^4 +$

$+ \rho + \rho^2 - \rho^3 = -\rho + \rho + \rho^2 - \rho^3 - \rho^4 =$

$= -\rho + \rho + \rho^2 - (\rho - 1) - (\rho^2 - \rho) = -\rho + \rho^2 =$

$= x_3$

i slično.

Znači permutaciona grupa jednačine je

$$G = (1), (123), (132) .$$

Napomena. Ovaj zadatak se mogao rešiti i na ovaj način. Kod jednačine $x^3 - 3x + 1 = 0$ je

$$\sqrt{D} = \sqrt{-4p^3 - 27q^2} = \sqrt{-4(-3)^3 - 27} = 9 \in Ra.$$

Pošto je jednačina nesvodljiva to je njena grupa

$$A_3 = (1), (123), (132) .$$

Ovo je regularna grupa pa je jednačina normalna.

Zadatak 89. Naći definicionu jednačinu elemenata $2 + \sqrt{2} + \sqrt[3]{2}$ na polju Ra .

Zadatak 90. Polinom

$$p(x) = a_{2n+1}x^{2n+1} + a_{2n}x^{2n} + \ldots + a_1 x + a_0 \quad / a_{2n+1} \neq 0 /$$

na polju Ra je nesvodljiv na polju Ra ako postoji takav prost p da je:

$$a_{2n+1} \not\equiv 0 \pmod p, \quad a_{2n} \equiv \ldots \equiv a_{n+1} \equiv 0 \pmod p,$$

$a_n = a_{n-1} = \ldots = a_o \equiv 0 \bmod p^2$, $a_o \not\equiv 0 \bmod p^3$.

Dokazati.

Zadatak 91. Ispitati svorljivost polinoma u odnosu na navedeno polje:

a/ $x^2 - 1$, $Ra(\sqrt{-2})$; b/ $x^3 + 8x = 2$, $Ra(\sqrt{2})$.

Zadatak 92. Data je jednačina $x^4 - 2x^2 - 9 = 0$ na polju Ra .

1/ Formirati korensko polje N date jednačine .

2/ Naći grupu automorfizama polja N prema polju Ra, sve podgrupe te grupe i odgovarajuća podpolja korenskog polja u kojima su te podgrupe grupe jednačine.

Zadatak 93. Navesti sve automorfizme sledećih polja:

$Ra(\sqrt{-3})$, $Ra(i, \sqrt{5})$, $Ra(\sqrt{2}, \sqrt{3}, \sqrt[3]{5})$.

Zadatak 94. Diskutovati grupu jednačine

$$x^4 + 2ax^2 + b = 0 \quad / a, b \in Ra/$$

u polju Ra.

Zadatak 95. Naći grupu u polju Pa jednačine

$$x^4 + ax^3 + bx^2 + ax + 1 = 0$$

Dokazati da je potreban i dovoljan uslov da grupa jednačine bude Klein - ova vierer grupa da broj $(b + 2a + 2)(b - 2a + 2)$ bude potpun kvadrat.

Zadatak 96. Neka je polje K normalno na polju F i neka F ima nadpolje L koje je podpolje polja $K/F \subset L \subset K/$. Dokazati da je K normalno polje na polju L .

Zadatak 97. Dokazati da je $x^4 - 3$ nesvodljiva na polju Ra (i). Naći grupu jednačine u tom polju.

Zadatak 98. Naći sve nesvodljive kvadratne trinome p/x/ $x^2 + px + q$, na polju J_5. Zadatak 99. Formirati korensko polje jednačine $x^3 + x + 1 = 0$, date u J_3. Zadatak 100. Naći grupu jednačine $x^2 + x + 1 = 0$, u polju J_2.