UNIVERZITET U NOVOM SADU

PAUNIĆ DJURA

ALGEBARSKE N-ARNE STRUKTURE

-DISERTACIJA-

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
INSTITUT ZA MATEMATIKU

PAUNIĆ DJURA

ALGEBARSKE N-ARNE STRUKTURE

- DISERTACIJA -

NOVI SAD, 1987.

S A D R Ž A J

0. UVOD 1

1. n-KVAZIGRUPE 6

2. n-GRUPE 27

3. MULTIKVAZIGRUPE 42

4. (m,n)-PRSTENI 63

5. LITERATURA 89

n-kvazigrupa vrlo brzo razvija, tako da se već 1972. godine pojavljuje monografija V.D.Belousova [2] posvećena isključivo n-kvazigrupama. Osim u algebri, binarne i n-kvazigrupe imaju primenu u kombinatorici i izučavanju geometrijskih konfiguracija.

Jugoslovenski matematičari su takodje dali prilog razvoju kvazigrupa i n-kvazigrupa i to V.Devide, G. Čupona, B.Trpenovski, S.Milić, B.Alimpić, J.Ušan, Z.Stojaković, A.Krapež, S.Krstić, K.Stojmenovski, N.Celakoski, M.Polonijo i drugi.

U prvoj glavi ovoga rada je razmatran sledeći problem: Šta može da se kaže o n-kvazigrupi (Q,f) ako važi

$$(*)\quad f(x_{\sigma(1)},\ldots,x_{\sigma(n)}) = x_{\sigma(n+1)} \Leftrightarrow f(x_1,\ldots,x_n) = x_{n+1}$$

za svako $x_1^{n+1} \in Q$, pri čemu je σ element podgrupe G grupe permutacija S_{n+1} nad skupom $N_{n+1} = \{1,\ldots,n,n+1\}$? Drugim rečima, kakve osobine ima n-kvazigrupa koja je donekle simetrična?

Neki specijalni slučajevi ovakvih n-kvazigrupa su ranije izučavani. Najpre je izučavan slučaj $G = S_{n+1}$ u [2] i [51]. Zatim je posmatran slučaj $G = C_{n+1}$ (tj. ciklična grupa generisana ciklusom (1,2,...,n,n+1)) u [57] i [67] i, konačno, slučaj kad je $G = A_{n+1}$ (alternativna podgrupa grupe S_{n+1}) u [56].

U ovom radu razmatran je opšti slučaj, kada je G proizvoljna podgrupa grupe S_{n+1} ([43]).

U slučaju binarnih kvazigrupa je G podgrupa od S_3, pa se C_3 poklapa sa A_3, dakle u binarnom slučaju za $G = C_3 = A_3$ se dobijaju polusimetrične kvazigrupe koje su izučavane u [47],[48],[49], a dopuštaju i kombinatornu interpretaciju kao Mendelsonovi sistemi trojki [36]. Ako je $G=S_3$ tada se dobijaju totalno simetrične kvazigrupe čija je jedna klasa ekvivalentna sa Štajnerovim sistemima trojki, koji su veoma blisko povezani sa nizom kombinatornih i geometrijskih konstrukcija.

U n-arnom slučaju je najinteresantniji slučaj $G = C_{n+1}$, [57], koji omogućava da se algebarskim metodama proučavaju razna uopštenja nekih poznatih kombinatornih struktura [55]. Samoortogonalne polusimetrične kvazigrupe su izučavane u [4],[35],[37],[47],[54], a ovde su dokazane teoreme ([67]) koje uopštavaju rezultate dobijene u navedenim radovima. Pokazano je da postoji samoortogonalna ciklična n-kvazigrupa za svako $q = p_1^{\alpha_1\beta_1} \dots p_m^{\alpha_m\beta_m}$, gde su $p_1, \dots, p_m$ prosti brojevi, a $\alpha_1, \dots, \alpha_m$ prirodni brojevi takvi da je $p_i^{\alpha_i} \equiv 1 \pmod{s_i}$, gde je $s_i > 1$ delitelj od n+1, i=1, ...,m, a β_i proizvoljni prirodni brojevi.

U drugoj glavi su ispitivane n-grupe (Q,f) koje zadovoljavaju uslov (*). Kako se n-grupa najčešće definiše kao n-kvazigrupa koja je ujedno i n-polugrupa, a pošto ovi uslovi nisu nezavisni, to se može naći ekvivalentna definicija koja zahteva manje provera i prema tome je pogodnija za rad. Naime, ako se pretpostavi da važi asocijativnost, dovoljno je zahtevati jednoznačnu rešivost po x jednačine $f(a_1^{i-1}, x, a_{i+1}^n) = n$ ili (i) za i=1 i i=n, ili (i) za $i \in \{2, \dots, n-1\}$, a ako se pretpostavi kvazigrupnost (jednoznačna rešivost po x jednačine $f(a_1^{i-1}, x, a_{i+1}^n) = b$ za svako i=1,... ...,n) tada je dovoljno zahtevati (i,i+1)-asocijativnost za neko $i \in \{1, \dots, n-1\}$ ili neka kombinacija ta dva ekstremna slučaja (Posledica 2.6.). n-grupe, a samim tim i njihova aksiomatika su veoma izučavane [2],[9],[22],[25],[26],[40], [46],[71].

Ovde je posebno razmatrana klasa G-n-grupa u čijoj definiciji se uslovi za asocijativnost mogu još više oslabiti. Izloženi su slučajevi $G = C_{n+1}$, $G = A_{n+1}$ i $G = \langle (i, i+1, \dots, n+1) \rangle$, za $i \in \{1, \dots, n-1\}$ ([56],[60] i [66]).

Koristeći moćnu Hosu-Gluskinovu teoremu o reprezentaciji operacije n-grupe pomoću binarne grupe([2], [60],[53]) moguće je dati potpun opis G-n-grupa pomoću binarnih grupa i to je izloženo u teoremi 2.18., teoremi 2.20. i teoremi 2.22. ([56],[66]).

Treća glava je posvećena multikvazigrupama. Multikvazigrupe su uvedene u [19] kao prirodno uopštenje pojma n-kvazigrupe. [n,m]-kvazigrupa (ili multikvazigrupa ili vektorsko-vrednosna kvazigrupa) je [n,m]-grupoid koji ispunjava uslove koji predstavljaju uopštenje rešivosti odgovarajućih jednačina. [n,m]-grupoidi su dosta izučavani u [58],[58],[60]. Multikvazigrupe imaju razne interpretacije: Svaka multikvazigrupa je ekvivalentna sistemu od m jako ortogonalnih n-kvazigrupa, a takodje je ekvivalentna i multidimenzionim geometrijskim rešetkama [15],[16],[17],[21], [41],[45],[50],[52],[58],[70].

Ovde je najpre dokazana egzistencija klase nelinearnih multikvazigrupa ([65]), a zatim su razmatrane multikvazigrupe koja zadovoljavaju prirodna uopštenja asocijativnog zakona, komutativnog zakona ili prirodno uopštenje neutralnog sloga ([64]). U nastavku je izložena jedna konstrukcija klase multikvazigrupe koje uopštavaju medijalne n-kvazigrupe ([44]).

U četvrtoj glavi su razmatrani problemi u vezi sa (m,n)-prstenima koji se dosta razlikuju od ranije proučavanih struktura. Naime, u prethodnim glavama su razmatrani algebarski sistemi sa jednom n-arnom operacijom, ili sa više operacija iste vrste definisanih nad jednim istim skupom, dok je (m,n)-prsten algebarska struktura dve operacije: komutativna m-grupa, (koja se obično naziva aditivna m-grupa), i n-polugrupa, (koja se obično naziva multiplikativna n-polugrupa), koje su povezane distributivnošću. (m,n)-prstene je uveo G.Čupona u [14] i D.Boccioni u [5]' pri čemu su u [5] definisani i izučavani (m,2)-prsteni. U [14] su dokazane dve teoreme koje su dva različita uopštenja Postove teoreme o reprezentaciji m-grupne operacije pomoću obične binarne grupe. Prva od njih je dokazana bar još tri puta u literaturi u [5],[11],[34], pri čemu je [5] objavljen 1965, kao i [14], dok je [11] objavljen 1972. a [34] čak 1980. godine. Druga teorema o reprezentaciji iz [14] je data u celosti (teorema 4.16), jer je vrlo interesantna i vrlo malo poznata, što je, po našem mišljenju, velika šteta.

Ovde je posebno izučavana problematika povezana sa homomorfnim preslikavanjem jednog (m,n)-prstena u drugi, tako da se neka multiplikativna n-podpolugrupa prvog (m,n)-prstena preslika u multiplikativnu n-podpolugrupi drugog (m,n)-prstena koja je n-grupa. Kako je pri tom naročito interesantan slučaj kad je homomorfizam monomorfizam, to je izučavan i slučaj kad je multiplikativna n-polugrupa (m,n)-prstena kancelativna u odnosu na neku svoju n-podpolugrupu. Konstrukcija koja je opisana u [42] je uopštenje klasične konstrukcije lokalizacije u binarnom slučaju, a takodje i konstrukcije količničkog (m,n)-prstena opisanog u [12].

Na kraju bih želeo da se zahvalim rukovodiocu ovog rada profesoru Z.Stojakoviću i profesoru G.Čuponi za stalnu podršku i mnogobrojne sugestije koje su mi veoma koristile pri izradi ove disertacije.

I

n - KVAZIGRUPE

Navodimo najpre definicije nekih osnovnih pojmova. Niz $x_m, x_{m+1}, \ldots, x_n$ označavaćemo sa $\{x_i\}_{i=m}^{n}$ ili jednostavnije sa x_m^n. Ako je $m > n$ tada se pod x_m^n podrazumeva prazan niz, a ako je y x_m^n, $x_i = x$, $i = m, m+1, \ldots, n$, tada će se ovaj niz označavati sa $\overset{n-m}{x}$.

DEFINICIJA 1.1. Neka je Q neprazan skup, n prirodan broj $\geqslant 1$ i f funkcija $f: Q^n \to Q$. Algebra (Q,f) se naziva n-grupoid.

DEFINICIJA 1.2. Element $q \in Q$ n-grupoida (Q,f) se naziva idvipotent ako i samo ako je $f(\overset{n}{q}) = q$. Ako za svako $q \in Q$ važi $f(\overset{n}{q}) = q$ n-grupoid se naziva idempotentan.

Sledećom definicijom uvodi se jedno uopštenje pojma izomorfizma koje je veoma značajno u teoriji kvazigrupa.

DEFINICIJA 1.3. n-grupoid (Q,f) je izotopan n-grupoidu (Q,g) ako i samo ako postoji niz bijekcija $T = (\alpha_1^{n+1})$, $\alpha_i : Q \to Q$, $i = 1, \ldots, n$, takvih da je

$$g(x_1^n) = \alpha_{n+1}^{-1} + (\{\alpha_i x_i\}_{i=1}^{n}) \ .$$

T se naziva izotopija, a da je f izotopno g označava se sa $g = f^T$. Ako je $\alpha_{n+1} = id_Q$, pri čemu je sa id_Q označeno identično preslikavanje skupa Q, izotopija se naziva glavna. Sa

T^{-1} se označava izotopija $T^{-1} = (\{\alpha_i^{-1}\}_{i=1}^{n+1})$.

DEFINICIJA 1.4. Neka je (Q,f) n-grupoid takav da za svako $a_1^n, b \in Q$ i svako $i \in \mathbb{N}_n = \{1,\dots,n\}$ jednačine

$$f(a_1^{i-1}, x, a_{i+1}^n) = b$$

ima jednoznačno rešenje po x. Tada se n-grupoid (Q,f) naziva n-kvazigrupa.

Za kvazigrupe je značajan i pojam parastrofije.

DEFINICIJA 1.5. Neka je (Q,f) n-kvazigrupa, σ permutacija skupa $\mathbb{N}_{n+1} = \{1,\dots,n+1\}$ i neka je n-kvazigrupa (Q,f^σ) definisana sa

$$f^\sigma(x_{\sigma(1)}^{\sigma(n)}) = x_{\sigma(n+1)} \iff f(x_1^n) = x_{n+1} \quad .$$

Tada se (Q,f^σ) naziva σ-parastrof (ili jednostavno parastrof ako to ne može da dovede do zabune) n-kvazigrupe (Q,f).

Sa S_n označavaćemo grupu permutacija stepena n.

Neka su $\sigma, \tau \in S_{n+1}$, tada je $f^{(\sigma\tau)} = (f^\sigma)^\tau$.

Parastrof koji odgovara transpoziciji $\pi_i = (i, n+1)$, $i = 1,\dots,n$, se naziva i-ta inverzna operacija.

Sada možemo definisati osnovnu klasu n-kvazigrupa koja se izučava u ovoj glavi, a to su G-n-kvazigrupe.

DEFINICIJA 1.6. [43] Neka je (Q,f) n-kvazigrupa i G podgrupa od S_{n+1}. n-kvazigrupa ako i samo ako je $f = f^\sigma$ za svako $\sigma \in G$.

DEFINICIJA 1.7. Neka je (Q,f) n-kvazigrupa i $\sigma \in S_{n+1}$ takva da je $f^\sigma = f$. Tada se σ naziva autoparastrofija od f. Skup svih autoparastrofija kvazigrupe (Q,f) je podgrupa od S_{n+1} i označava se sa $\Pi(f)$.

Uzimajući za G razne podgrupe od S_{n+1}, dobijaju se sledeće G-n-kvazigrupe koje su izučavane u literaturi.

<u>DEFINICIJA 1.8.</u> G-n-kvazigrupa (Q,f) se naziva totalno simetrična (TS) ako i samo ako je $G = S_{n+1}$.

Totalno simetrične kvazigrupe su prve ispitivane G-n-kvazigrupe.

<u>DEFINICIJA 1.9.</u> G-n-kvazigrupa (Q,f) se naziva alternativno simetrična (AS) ako i samo ako je $G = A_{n+1}$.

AS-kvazigrupe su definisane i ispitivane u [56].

<u>DEFINICIJA 1.10.</u> G-n-kvazigrupa (Q,f) se naziva ciklična ako i samo ako je $G = \langle(1\ 2\ \ldots n{+}1)\rangle \simeq C_{n+1}$.

Ciklične n-kvazigrupe su izučavane u [57].

Ovde je navedena samo definicija G-n-kvazigrupe, medjutim moguće je analogno definisati i G-n-grupoide. Istraživanja u tom pravcu su vršena u [60], [61]

<u>DEFINICIJA 1.11.</u> n-grupoid (Q,f) se naziva G-n-grupoid ako i samo ako važi

$$f(x_1^n) = x_{n+1} \iff f(x_{\sigma(1)}^{\sigma(n)}) = x_{\sigma(n+1)}$$

za svako $\sigma \in G \leqslant S_{n+1}$ i svako $x_1^{n+1} \in Q$.

Interesantno je da ne postoje TS, AS ili ciklički n-grupoidi koji nisu n-kvazigrupe.

<u>TEOREMA 1.1.</u> Neka je (Q,f) G-n-grupoid pri čemu je G tranzitivna grupa permutacija. Tada je (Q,f) n-kvazigrupa.

<u>DOKAZ.</u> Neka je (Q,f) G-n-grupoid sa tranzitivnom grupom permutacija G i neka je data jednačina

$$f(a_1^i, x, a_{i+1}^n) = a_{n+1}.$$

Kako je G tranzitivna grupa permutacija postoji $\sigma \in G$ takvo da je $\sigma(n+1) = i$ pa je

$$f(a_{\sigma(1)}^{\sigma(n)}) = x$$

tj. x je jednoznačno odredjeno.

POSLEDICA 1.2. Svaki TS, AS osnosno ciklički n-grupoid je TS, AS odnosno ciklička n-kvazigrupa respektivno.

DOKAZ. S_{n+1}, A_{n+1}, C_{n+1} su tranzitivne grupe permutacija.

Pošto je $A_3 \cong C_3$ to dobijamo da se u binarnom slučaju klasa alternativno simetričnih i klasa cikličkih kvazigrupa poklapaju. U tom slučaju se dobija klasa polusimetričnih kvazigrupa koje je izučavao A.Sade u vezi sa klasifikacijom latinskih kvadrata i koje imaju velike kombinatorne primene. Idempotentne polusimetrične kvazigrupe su ekvivalentne sa Mendelsonovim sistemom trojki.

U radu [29] je D.G.Hofman dao konstrukciju G-n-kvazigrupe (Q,f) reda mp za svako $m > n$, $p \geqslant 2$ za svako $G \leqslant S_{n+1}$ takve da je $\Pi(f) = G$. Navedimo sada neke konstrukcije kojima se dobijaju pojedine klase G-n-kvazigrupa.

TVRDJENJE 1.3. Neka je $(Q,+)$ binarna abelova grupa, n prirodan broj $\geqslant 2$ i $\varphi : Q \to Q$ automorfizam $(Q,+)$ takav da je za $n = 2k$ $\varphi^{n+1}(x) = -x$, za svako $x \in Q$, a za $n = 2k+1$ $\varphi^{n+1}(x) = x$, za svako $x \in Q$, i $a \in Q$ takav da je $\varphi(a) = -a$. Definišimo $f : Q^n \to Q$ sa

$$f : (x_1, \ldots, x_n) \to \varphi x_1 - \varphi^2 x_2 + \varphi^3 x_3 + \ldots + (-1)^{n+1} \varphi^n x_n + a \ .$$

Tada je (Q,f) ciklična n-kvazigrupa.

TVRDJENJE 1.4. Neka je $(Q,\cdot)$ proizvoljna grupa $\alpha : Q \to Q$ automorfizam takav da je $\alpha^{n+1} = id_Q$, a c centralni element takav da je $\alpha c = c$. Tada je sa

$$f : (x_1, \ldots, x_n) \to \alpha x_1^{-1} \alpha^2 x_2^{-1} \ \ldots \ \alpha^n x_n^{-1} c,$$

definisana ciklična n-kvazigrupa.

POSLEDICA 1.5. Neka je $(R,+,\cdot)$ prsten sa jedinicom i neka je $r \in R$ element za koji važi $r^{n+1} = -1$ ako je $n = 2k$, odnosno $r^{n+1} = 1$ za $n = 2k+1$. Tada je $\varphi : x \to r x$ automorfizam komutativne grupe $(R,+)$ pa je

$$f:(x_1,\dots,x_n)\to rx_1-r^2x_2+r^3x_3-+\dots+(-1)^{n+1}r^nx_n$$

n-arna operacija takva da je (R,f) ciklična n-kvazigrupa.

PRIMER 1.6. Neka je $(Q,+)$ abelova grupa takva da je za svako $x\neq 0$, $x+x\neq 0$. Ako se definiše ternarna operacija f sa

$$f:(x_1,x_2,x_3)\to x_1+x_2-x_3\,,$$

tada je (Q,f) G-3-kvazigrupa pri čemu je G Klajnova četvorna grupa $\{(1),(12)(34),(13)(24),(14)(23)\}$. (Q,f) nije ni TS ni AS, ni ciklična ternarna kvazigrupa.

Neposredno iz definicije G-n-kvazigrupe sledi:

TEOREMA 1.7. n-kvazigrupa (Q,f) je G-n-kvazigrupa ako i samo ako za svako $\sigma\in\Gamma$ i svako $x_1^n\in Q$ važi

$$f(\{x_{\sigma(i)}\}_{i=1}^{k-1},f(x_1^n),\{x_{\sigma(i)}\}_{i=k+1}^{n}) = x_{\sigma(n+1)}\,,$$

pri čemu je $\sigma(k)=n+1$, a Γ je skup generatora grupe G.

Iz teoreme 1.7. se može dobiti niz posledica ako se uoči da je n-kvazigrupa G-n-kvazigrupa ako i samo ako za svako $\sigma\in\Gamma$ zadovoljava identitet naveden u teoremi, tj. G-n-kvazigrupe su varijetet. Iz toga odmah sledi da je na primer direktan proizvod G-n-kvazigrupa opet G-n-kvazigrupa, da je podkvazigrupa G-n-kvazigrupe takodje G-n-kvazigrupa.

Ako se specijalizira grupa G, dobijaju se sledeće posledice:

POSLEDICA 1.8. n-kvazigrupa (Q,f) je AS-kvazigrupa ako i samo ako je zadovoljen bar jedan od sledeća tri sistema identiteta:

(i) $$\begin{cases} f(x_2,x_i,x_3^{i-1},x_1,x_{i+1}^n) = f(x_1^n)\,, & i=3,\dots,n,\\ f(x_2,f(x_1^n),x_3^n) = x_1\,, & \end{cases}$$

(ii) $f(x_1^{i-1}, f(x_1^n), x_{i+1}^{n-1}, x_i) = x_n$, $i = 1,\dots,n-1$,

(iii) $f(x_1^{i-1}, x_n, x_{i+1}^{n-1}, f(x_1^n)) = x_i$, $i = 1,\dots,n-1$.

DOKAZ. Tvrdjenje neposredno sledi iz prethodne teoreme i sledećih generativnih skupova alternativno simetrične grupe:

za (i) $\{(123),(124),\dots,(12,n+1)\}$;

za (ii) $\{(n+1,n,1),(n+1,n,2),\dots,(n+1,n,n-1)\}$,

za (iii) $\{(n,n+1,1),(n,n+1,2),\dots,(n,n+1,n-1)\}$.

POSLEDICA 1.9. n-kvazigrupa (Q,f) je alternativno simetrična ako i samo ako je

$$f^{\pi_i \pi_j} = f$$

za svako $i,j \in \mathbb{N}_n$.

DOKAZ. $S = \{\sigma = \pi_i \pi_j : i,j \in \mathbb{N}_n\} = \{id, (n+1,j,i), i,j \in \mathbb{N}_n, i \neq j\}$ pa S sadrži skup generatora iz stava (ii) prethodnog tvrdjenja.

POSLEDICA 1.10. n-kvazigrupa (Q,f) je ciklična ako i samo ako važi bar jedan od uslova

(i) $f(x_{n+1}, x_1^{n-1}) = x_n$ ako i samo ako je $f(x_1^n) = x_{n+1}$ za svako $x_1^{n+1} \in Q$.

(ii) $f(x_1^n) = x_{n+1}$ ako i samo ako je $f(x_{i+1}^{n+1}, x_1^{i-1}) = x_i$ za svako $x_1^{n+1} \in Q$ i svako $i \in \mathbb{N}_n$ takvo da je $nzd(n+1, i) = 1$,

(iii) $f(f(x_1^n), x_1^{n-1}) = x_n$ za svako $x_1^n \in Q$.

DOKAZ. Sledi iz teoreme 1.7 i činjenice da ciklična grupa ima jednoelementni generativan skup.

POSLEDICA 1.11. n-kvazigrupi (Q,f) je ciklična ako i samo ako je

$$f^{\pi_n \pi_{n-1} \cdots \pi_2 \pi_1} = f.$$

POSLEDICA 1.12. Neka je (Q,f) AS-n-kvazigrupa i $n = 2k$. Tada je (Q,f) ciklična n-kvazigrupa.

DOKAZ. Treba primetiti da je ciklus neparne dužine parna permutacija.

POSLEDICA 1.13. n-kvazigrupa (Q,f) je totalno simetrična ako i samo ako je

$$f^{\pi_i} = f$$

za svako $i \in \mathbb{N}_i$.

Za ispitivanje cikličnih n-kvazigrupa su od posebnog interesa takozvani cirkularni pirostrofi uvedeni u [51].

DEFINICIJA 1.12. Neka je (Q,f) n-kvazigrupa, $\sigma_i \in S_{n+1}$, $i \in \mathbb{N}_{n+1}$, definisana sa $\sigma_i : x \to x+i$, (mod(n+1)). Tada se svaki parastrof (Q, f^{σ_i}), $i = 1,\ldots,n+1$, naziva cirkularni parostrof n-kvazigrupe (Q,f).

Pomoću cirkularnih parastrofa mogu da se daju sledeće karakterizacije cikličkih n-kvazigrupa ([57]).

POSLEDICA 1.14. n-kvazigrupa (Q,f) je ciklična ako i samo ako važi bar jedan od sledeća dva (ekvivalentna) uslova:

(i) f se poklapa sa svojim parastrofom f^{σ_j}, gde je σ_j cirkularan parastrof takav da su j i n+1 uzajamno prosti brojevi.

(ii) f se poklapa sa svim svojim cirkularnim parastrofima.

TVRDJENJE 1.15. Neka je (Q,f) ciklična n-kvazigrupa i neka je (Q, f^{σ}) parastrof takav da je

$$\sigma(t+1) \equiv \sigma(t) + i \bmod(n+1)$$

za neko i i svako t. Tada je (Q, f^{σ}) ciklična n-kvazigrupa.

Cirkularni parastrofi uvek zadovoljavaju uslov teoreme za σ, ali postoje i necirkularni parastrofi koji zadovoljavaju taj uslov. Tako na primer uslov za σ dat u teoremi zadovoljava sve permutacije iz S_3.

Ispitujemo sada kako se G-n-kvazigrupe ponašaju u odnosu na izotopiju. Najpre imamo korisnu posledicu definicija.

Neka je $T = (\alpha_1^{n+1})$ izotopija n-kvazigrupe (Q,f), a $\sigma \in S_{n+1}$. Tada je $(f^T)^\sigma = (f^\sigma)^{T^\sigma}$ gde je $T^\sigma = (\alpha_{\sigma(1)}^{\sigma(n+1)})$.

<u>TVRDJENJE 1.16.</u> [57] Neka je n-kvazigrupa (Q,f) izotopna cikličkoj n-kvazigrupi (Q,g). Tada

(i) (Q,f) je izotopno svakom svom cirkularnom parastrofu (Q,f^{σ_i}).

(ii) Svaki π-parastrof od (Q,f), pri čemu je

$$\pi(t+1) \equiv \pi(t) + j$$

za svako $t \in \mathbb{N}_{n+1}$ i $j \in \mathbb{N}_{n+1}$, je izotop ciklične n-kvazigrupe.

Sada ćemo ispitati šta se može reći ako je $f^\sigma = f^T$ tj. šta se dešava kad je parastrof f^σ jednak izotopu f^T. Najpre slučaj kad je σ ciklus, a zatim opšti slučaj.

<u>TVRDJENJE 1.17.</u> [57] Neka je (Q,f) n-kvazigrupa izotopna svom parastrofu f^σ izotopijom $T = (\alpha_1^{n+1})$, tj. $f^T = f^\sigma$, gde je $\sigma \in S_{n+1}$ ciklus dužine n+1. Tada postoji bijekcija $\theta : Q \to Q$ i n-kvazigrupa (Q,g) izotopna (Q,f) takva da je $g^\sigma = g^S$ sa izotopijom

$$S = (id,\ldots,id,\theta^{-1}\alpha_{n+1}\alpha_{\sigma(n+1)}\cdots\alpha_{\sigma^n(n+1)}\theta) .$$

<u>TVRDJENJE 1.18.</u> [57] n-kvazigrupa (Q,f) je izotopna cikličkoj n-kvazigrupi (Q,g) ako i samo ako postoji cirkularan parastrof f^{σ_i}, gde su i i $n+1$ uzajamno prosti brojevi takvi da je f izotopno sa f^{σ_i} izotopijom $T = (\alpha_1^{n+1})$ pri čemu je

$$\alpha_{n+1}\alpha_{\sigma_i(n+1)}\alpha_{\sigma_i^2(n+1)}\cdots\alpha_{\sigma_i^n(n+1)} = id .$$

<u>TVRDJENJE 1.19.</u> Neka je (Q,f) n-kvazigrupa izotopna svom parastrofu f^{σ} izotopijom $T=(\alpha_1^{n+1})$, $f^T=f^{\sigma}$, $\sigma\in S_{n+1}$ i neka je $\sigma=(i_1\ldots i_r)(j_1\ldots j_s)\ldots(k_1\ldots k_t)$ razlaganje permutacije σ u v disjunktnih ciklusa (pri čemu su računati i ciklusi dužine 1). Tada postoje permutacije $\theta_1,\ldots,\theta_v$ skupa Q i n-kvazigrupa (Q,g) izotopna (Q,f) takva da je g izotopno g^{σ} izotopijom S

$$S=(id,\ldots,id,\theta^{-1}\alpha_{i_1}\alpha_{\sigma(i_1)}\ldots\alpha_{\sigma^{r-1}(i_1)}\theta_1,id,\ldots$$
$$\ldots,id,\theta_2^{-1}\alpha_{j_1}\alpha_{\sigma(j_1)}\ldots\alpha_{\sigma^{s-1}(j_1)}\theta_2,id,\ldots$$
$$\ldots,id,\theta_v^{-1}\alpha_{k_1}\alpha_{\sigma(k_1)}\ldots\alpha_{\sigma^{t-1}(k_1)}\theta_v,id,\ldots,id),$$

pri čemu su bar $n+1-v$ komponenti identiteta, a najviše po jedna komponenta različita od identične permutacije skupa Q za svaki ciklus permutacije σ. Komponenta različita od identičke permutacije skupa Q koja odgovara ciklusu $(i_1,\ldots,i_r)$ može da se nalazi na bilo kom mestu $i_1,\ldots,i_r$ i analogno za ostale cikluse. Ako je (i_1) ciklus dužine 1 njemu odgovara komponenta $\theta_1^{-1}\alpha_{i_1}\theta_1$ i nalazi se na mestu i_1.

<u>DOKAZ.</u> Neka je g proizvoljan izotop od f, $g=f^S$ gde je $S=(\beta_1^{n+1})$. Kako je $f^T=f^{\sigma}$ to sledi da je

$$((g^{S^{-1}})^T)^{\sigma^{-1}})^S=g\ .$$

Iz definicija izotopije i parastrofije sledi da je $(h^{\sigma^{-1}})^S=$ $=(h^{S^{\sigma}})^{\sigma^{-1}}$ za svaku n-kvazigrupu (Q,h) pa je zato

$$((g^{S^{-1}T})^{S^{\sigma}})^{\sigma^{-1}}=g \quad \text{tj.}\quad g^{S^{-1}TS^{\sigma}}=g^{\sigma}$$

što znači da je svaki izotop g n-kvazigrupe f izotopan svom parastrofu.

Pokažimo sada da postoji izotop g od f takav da je g izotopan g^{σ} izotopijom oblika navedenog u tvrdjenju. Kako je

$$S^{-1}TS^{\sigma} = (\{\beta_i^{-1}\alpha_i\beta_{\sigma(i)}\}_{i=1}^{n+1}) \ ,$$

to iz pretpostavke da je

$$g^{(\{\beta_i^{-1}\alpha_i\beta_{\sigma(i)}\}_{i=1}^{n+1})} = g$$

dobijamo sistem jednačina za prvih n komponenata izotopije

$$(*) \qquad \beta_1^{-1}\alpha_1\beta_{\sigma(1)} = id,\ldots,\beta_n^{-1}\alpha_n\beta_{\sigma(n)} = id,$$

tj.

$$\alpha_1\beta_{\sigma(1)} = \beta_1,\ldots,\alpha_n\beta_{\sigma(n)} = \beta_n \ .$$

Neka je β_{n+1} proizvoljna permutacija skupa Q i pretpostavimo najpre da je σ ciklus dužine $n+1$ tj. da se svaki indeks $i \in \mathbb{N}_n$ može dobiti od $n+1$ primenjujući odgovarajući stepen permutacije σ tada, ako je $i = \sigma^{-1}(n+1)$, imamo $j = \sigma^{-1}(i) = \sigma^{-2}(n+1)$ itd. pa je konačno

$$\beta_{\sigma^{-1}(n+1)} = \alpha_{\sigma^{-1}(n+1)}\beta_{n+1} \ ,$$

$$\beta_{\sigma^{-2}(n+1)} = \alpha_{\sigma^{-2}(n+1)}\beta_{\sigma^{-1}(n+1)} = \alpha_{\sigma^{-1}(n+1)}\alpha_{\sigma^{-1}(n+1)}\beta_{(n+1)}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\beta_{\sigma^{-n}(n+1)} = \alpha_{\sigma^{-n}(n+1)}\alpha_{\sigma^{-n+1}(n+1)}\cdots\alpha_{\sigma^{-1}(n+1)}\beta_{(n+1)} \ .$$

Ako sada sve vrednosti iskoristimo za izračunavanje $n+1$ komponente izotopije $S^{-1}TS^{\sigma}$ dobijamo da je

$$\beta_{n+1}^{-1}\alpha_{n+1}\beta_{\sigma(n+1)} = \beta_{n+1}^{-1}\alpha_{n+1}\beta_{\sigma^{-n}(n+1)} =$$

$$= \beta_{n+1}^{-1}\alpha_{n+1}\alpha_{\sigma^{-n}(n+1)}\beta_{\sigma^{-n+1}(n+1)} = \ldots =$$

$$= \beta_{n+1}^{-1}\alpha_{n+1}\alpha_{\sigma^{-n}(n+1)}\cdots\alpha_{\sigma^{-1}(n+1)}\beta_{n+1} =$$

$$= \beta_{n+1}^{-1}\alpha_{n+1}\alpha_{\sigma(n+1)}\alpha_{\sigma^{2}(n+1)}\cdots\alpha_{\sigma^{n}(n+1)}\beta_{n+1} \ .$$

Kako se sve komponente $\beta_1,\dots,\beta_n$ izražavaju preko alfi i β_{n+1} ako stavimo da je $\theta=\beta_{n+1}$ dobijamo tvrdjenje kad je σ ciklus dužine n+1.

Opšti slučaj se sad lako dobija ako se sistem jednačina (*) razbije na v sistema

$$(m_1)\quad \beta^{-1}_{i_2}\alpha_{i_2}\beta_{\sigma(i_2)}=id,\dots,\beta^{-1}_{i_r}\alpha_{i_r}\beta_{\sigma(i_r)}=id\ ,$$

$$(m_2)\quad \beta^{-1}_{j_2}\alpha_{j_2}\beta_{\sigma(j_2)}=id,\dots,\beta^{-1}_{j_s}\alpha_{j_s}\beta_{\sigma(j_s)}=id\ ,$$

$$\dots\dots\dots\dots\dots\dots\dots$$

$$(m_v)\quad \beta^{-1}_{k_2}\alpha_{k_2}\beta_{\sigma(k_2)}=id,\dots,\beta^{-1}_{k_t}\alpha_{k_t}\beta_{\sigma(k_t)}=id\ ,$$

i ako pretpostavimo da su $\beta_{i_1},\beta_{j_1},\dots,\beta_{k_1}$ proizvoljne permutacije skupa Q tada se sistemi $(m_1),(m_2),\dots,(m_v)$ rešavaju analogno kao što je rešen sistem (*) i tvrdjenje sledi.

<u>TVRDJENJE 1.20.</u> Neka je (Q,f) n-kvazigrupa izotopna n-kvazigrupi (Q,g) takvoj da postoji parastrof $g^\sigma=g$. Tada je f izotopno f^σ izotopijom $T=(\alpha_1^{n+1})$ takvom da je

$$\alpha_{i_1}\alpha_{\sigma(i_1)}\dots\alpha_{\sigma^{r-1}(i_1)}=id$$

za svaki ciklus $(i_1,i_2,\dots,i_r)$ u razlaganju σ na disjunktne cikluse uključujući i cikluse dužine 1 (gde ako je (j) ciklus dužine 1 tada je $\alpha_j=id$).

<u>DOKAZ.</u> Neka je f izotopno n-kvazigrupi g sa izotopijom $S=(\beta_1^{n+1})$, $f^S=g$, takvoj da je $g=g^\sigma$ za neko $\sigma\in S_{n+1}$. Tada je

$$f^S=g=g^\sigma=(f^S)^\sigma=(f^\sigma)^{S^\sigma}$$

pa je

$$f^{S(S^\sigma)^{-1}}=f^\sigma$$

Ako označimo sa T izotopiju $S(S^\sigma)^{-1}$, tj. $T=S(S^\sigma)^{-1}=$ $=(\alpha_1^{n+1})$ imamo da je

$$S^{-1}TS^\sigma=I,$$

tj.

(*) $$\beta_k^{-1}\alpha_k\beta_{\sigma(k)} = id_Q,\ k=1,\dots,n+1.$$

Iz ovog sistema jednačina analognom eliminacijom kao u dokazu prethodne teoreme dobijamo za slučaj kad je σ ciklus

$$\beta_{n+1}^{-1}\alpha_{n+1}\alpha_{\sigma(n+1)}\dots\alpha_{\sigma^n(n+1)}\beta_{n+1} = id\ ,$$

tj.

$$\alpha_{n+1}\alpha_{\sigma(n+1)}\dots\alpha_{\sigma^n(n+1)} = id\ .$$

Ako σ nije ciklus tada se sistem jednačina (*) raspada na podsisteme koji odgovaraju pojedinim ciklusima u razlaganju permutacije σ na disjunktne cikluse i rešavajući te podsisteme, kao što je bilo uradjeno u dokazu prethodne teoreme, dobijamo za ciklus $(i_1,i_2,\dots,i_k)$

$$\beta_{i_1}^{-1}\alpha_{i_1}\alpha_{\sigma(i_1)}\dots\alpha_{\sigma^{r-1}(i_1)}\beta_{i_1} = id\ ,$$

tj.

$$\alpha_{i_1}\alpha_{\sigma(i_1)}\dots\alpha_{\sigma^{r-1}(i_1)} = id\ .$$

Analogno za ostale cikluse i cikluse dužine 1.

TEOREMA 1.21. Ako je $T=(\alpha_1^{n+1})$ autotopija G-n-kvazigrupe (Q,f) i $\sigma\in G\leqslant S_{n+1}$, tada je i $S=T^\sigma=(\{\alpha_{\sigma(i)}\}_{i=1}^{n+1})$ takodje autotopija G-n-kvazigrupe (Q,f).

DOKAZ. Pošto je T autotopija to je $f^T=f$, a kako je (Q,f) G-n-kvazigrupa to je $f^\sigma=f$ pa je i

$$f=(f^T)^\sigma=(f^\sigma)^{T^\sigma}=f^{T^\sigma}$$

tj. T^σ je autotopija od (Q,f).

U specijalnim slučajevima kad je G jedna odredjena podgrupa od S_{n+1} dobijaju se daleko precizniji rezultati.

TVRDJENJE 1.22. Neka je (Q,f) G-n-kvazigrupa i $\tau \in S_{n+1}$ takva da je G invarijantna pri unutrašnjem automorfizmu indukovanim sa τ. Tada je (Q,f^{τ}) G-n-kvazigrupa.

DOKAZ. Kako je G invarijantno pri automorfizmu $\sigma \to \tau\sigma\tau^{-1}$ sledi da za svako $\sigma_i \in G$ postoji $\sigma_j \in G$ takvo da je $\sigma_j = \tau\sigma_i\tau^{-1}$. Otuda sledi da je

$$f^{\tau\sigma_i\tau^{-1}} = f^{\sigma_j} = f \quad \text{pa je} \quad f^{\tau\sigma_i} = f^{\tau}$$

za svako $\sigma_i \in G$ tj. f^{τ} je G-n-kvazigrupa.

POSLEDICA 1.23. Ako je (Q,f) H-kvazigrupa i H je invarijantna podgrupa grupe $G \leqslant S_{n+1}$, tada je svaki parastrof f^{τ}, $\tau \in G$, takodje H-n-kvazigrupa.

TVRDJENJE 1.24. Neka je (Q,f) G-n-kvazigrupa gde je $G = \Pi(f)$. Parastrof f^{τ} je G-n-kvazigrupa ako i samo ako je G invarijantna podgrupa za unutrašnji automorfizam indukovan sa τ.

DOKAZ. Ako $\tau\sigma\tau^{-1} \in G$ za svako $\sigma \in G$ tada zbog tvrdjenja 1.22. sledi da je f^{τ} G-n-kvazigrupa.

Da dokažemo obrnuto neka je f^{τ} G-n-kvazigrupa. Tada za svako $\sigma \in G$ $(f^{\tau})^{\sigma} = f^{\tau}$ tj. $f^{\tau\sigma\tau^{-1}} = f$. Kako je $G = \Pi(f)$ jedini parastrofi jednaki sa f su oni koje indukuju permutacije iz G pa $\tau\sigma\tau^{-1} \in G$ za svako $\sigma \in G$ tj. G je invarijantno za unutrašnji automorfizam indukovan sa τ.

TEOREMA 1.25. Neka je n-kvazigrupa (Q,f) izotopna G-n-kvazigrupa (Q,g). Tada je f izotopno parastrofu f^{σ} za svako $\sigma \in G$ i svaki parastrof f^{τ}, pri čemu je τ permutacija iz S_{n+1} takva da je $\tau G\tau^{-1} = G$, je izotop G-n-kvazigrupe.

DOKAZ. (Q,g) je G-n-kvazigrupa pa je $g = g^{\sigma}$ za svako $\sigma \in G$. Pošto su odgovarajući parastrofi izotopnih n-kvazigrupa izotopni sledi da je i (Q,f^{σ}) izotopno sa $g = g^{\sigma}$

za svako $\sigma \in G$.

Ako je τ takvo da je $G = \tau G \tau^{-1}$ tada iz tvrdjenja 1.23. sledi da je g^{τ} G-n-kvazigrupa. Otuda sledi da je odgovarajući parastrof (Q,f^{τ}) kvazigrupe (Q,f) izotopan G-n-kvazigrupi (Q,g^{τ}).

Postoji tesna veza izmedju AS-n-kvazigrupa i TS-kvazigrupa, naime da za $n \geqslant 3$ svaka AS-n-kvazigrupa definiše familiju TS-(n-2)-kvazigrupa dokazano je u [56], dok se ovde daje malo modifikovana teorema.

<u>TEOREMA 1.26.</u> Neka je (Q,f) AS-n-kvazigrupa, pri čemu je $n \geqslant 4$ i $a \in Q$ proizvoljan element. Tada je (n-2)-kvazigrupa (Q,g) definisana sa

$$g(x_1^{n-2}) = x_{n-1} \text{ ako i samo ako je}$$

$$f(x_1^{i-1},a,x_i^{j-1},a,x_j^{n-2}) = x_{n-1},\ i,j \in \mathbb{N}_{n-1},\ i \neq j,$$

TS-(n-2)-kvazigrupa.

<u>DOKAZ.</u> Dobro je poznato da je $S_{n-2} \to A_n$, naime n-2 elemenata možemo permutovati kako hoćemo, a n-1 i n ili ostavimo na mestu ako je permutacija bila parna, ili n-1 i n zamene mesta ako je bila neparna. Naravno ulogu n-1 i n mogu igrati bilo koja dva elementa iz $\mathbb{N}_n$.

U slučaju AS-n-kvazigrupa je opis autopija precizniji.

<u>TVRDJENJE 1.27.</u> [56] Neka su α i β permutacije skupa Q i $n \geqslant 3$, $n \in \mathbb{N}$. $T = (\alpha,\beta,id,\ldots,id)$ je autopija AS-n-kvazigrupe (Q,f) ako i samo ako važi

(i) $\beta = \alpha^{-1}$

(ii) $f(x_1^{i-1},\alpha x_i,x_{i+1}^n) = f(x_i^{j-1},\alpha x_j,x_{j+1}^n)$ za neko $i,j \in \mathbb{N}_n$, $i \neq j$, i svako $x_1^n \in Q$.

<u>TVRDJENJE 1.28.</u> [56] Neka je $T = (\alpha_1^{n+1})$ autotopija AS-n-kvazigrupe (Q,f). Tada je

(i) Ako je $n \geqslant 2$ tada je za svaka tri, medjusobno različita elementa, $i,j,k \in \mathbb{N}_{n+1}$ ili

$(\alpha_i^{-1}\alpha_j, \alpha_j^{-1}\alpha_k, \alpha_k^{-1}\alpha_i, id, \ldots, id)$ ili

$(\alpha_j^{-1}\alpha_k, \alpha_i^{-1}\alpha_j, \alpha_k^{-1}\alpha_i, id, \ldots, id)$

autotopija od f.

(ii) Ako je $n \geqslant 4$ tada je za svako $i,j \in \mathbb{N}_{n+1}$, $i \neq j$,

$(\alpha_i^{-1}\alpha_j, \alpha_j^{-1}\alpha_i, id, \ldots, id)$

autotopija od f.

<u>TVRDJENJE 1.29</u>. [56] Neka je (Q,f) AS-n-kvazigrupa, $n \geqslant 4$ i $T = (\alpha_1^{n+1})$ autotopija od f. Tada je $T^{\sigma} = (\{\alpha_{\sigma(i)}\}_{i=1}^{n+1})$ autotopija od f za svako $\sigma \in S_{n+1}$.

Alternativno simetrične n-kvazigrupe imaju vrlo interesantnu kombinatornu primenu [63].

Ciklične n-kvazigrupe imaju raznovrsne kombinatorne primene. Veze cikličkih n-kvazigrupa i uopštenja Mendelsovih sistema trojki su date u [55], a sada ćemo izložiti druga njihova kombinatorna svojstva koja se odnose na ortogonalnost.

Binarna kvazigrupa $(Q,\cdot)$ se naziva polusimetrična ako u $(Q,\cdot)$ važi identitet $x(yx) = x$. Ukoliko u $(Q,\cdot)$ važi identitet $x^2 = x$, $(Q,\cdot)$ se naziva idempotentna. Svaka konačna, idempotentna, polusimetrična kvazigrupa je ekvivalentna Mendelsovom sistemu trojki uvedenom u [36]. Kvazigrupa $(Q,*)$ se naziva transpozicija kvazigrupe $(Q,\cdot)$ ako je zvezdica definisana sa $x*y = yx$. Binarna kvazigrupa $(Q,\cdot)$ je samoortogonalna ako je ortogonalna na svoju transpoziciju tj. ako za svako $a,b \in Q$ sistem jednačina $xy = a$, $yx = b$ ima jednoznačno rešenje. Ako je Q konačan skup tada je kvazigrupa $(Q,\cdot)$ samoortogonalna ako i samo ako iz $xy = zu$ i $yx = uz$ sledi da je $x = z$ i $y = u$. Samoortogonalne polusimetrične kvazigrupe su nužno idempotentne.

Samoortogonalne polusimetrične kvazigrupe su izučavane u [4],[28],[37],[47],[54] i dokazano je da one postoje za $q \equiv 1 \pmod 3$ osim za $q = 10$, gde je q red kvazigrupe. Kako ne postoje Mendelsovi sistemi trojki za $q \equiv 2 \pmod 3$ i za $q = 6$ [36] to ne postoje samoortogonalne polusimetrične kvazigrupe tih redova. U [4] je dokazano da ne postoje za $q = 9$ i otvoreno je pitanje da li postoje samoortogonalne polusometrične kvazigrupe za $q \equiv 0 \pmod 3$ $q \geqslant 12$.

Sada ćemo pokazati kako se navedeni rezultati mogu uopštiti na cikličke n-kvazigrupe koje predstavljaju generalizaciju polusimetričnih kvazigrupa.

DEFINICIJA 1.13. Skup $\{(Q,f_1),\dots,(Q,f_n)\}$ od n n-arnih kvazigrupa se naziva ortogonalan ako i samo ako za svako $a_1,\dots,a_n \in Q$ postoji jednoznačno odredjen $(b_1,\dots,b_n) \in Q^n$ takav da je $f_i(b_1,\dots,b_n) = a_i$, $i = 1,\dots,n$.

DEFINICIJA 1.14. Neka je (Q,f) n-kvazigrupa takva da je skup $\{(Q,f),(Q,f_1),\dots,(Q,f_{n-1})\}$ ortogonalan pri čemu su f_i, $i = 1,\dots,n$, parastrofi od f definisani sa $f_i(x_1^n) = f(x_{i+1}^n, x_1^i)$, $i = 1,\dots,n$, tada se n-kvazigrupa (Q,f) naziva samoortogonalna.

TEOREMA 1.30. Neka je $(Q,+)$ abelova grupa, $n \geqslant 2$ i φ automorfizam grupe $(Q,+)$ takav da je $1+\varphi$ bijekcija pri čemu je $1+\varphi : Q \to Q$ definisano sa $1+\varphi : x \to x+\varphi(x)$, i za koji važi

$$\varphi^{n+1}(x) = \begin{cases} -x & \text{za } n = 2k \\ x & \text{za } n = 2k+1 \end{cases}.$$

Ako se definisana operacija $f : Q^n \to Q$ sa

$$f : (x_1,\dots,x_n) \to \varphi x_1 - \varphi^2 x_2 + \varphi^3 x_3 - \dots + (-1)^{n+1}\varphi^n x_n ,$$

tada je (Q,f) samoortogonalna ciklična n-kvazigrupa.

DOKAZ. Na osnovu teoreme 1.3 je (Q,f) ciklična n-kvazigrupa. Neka su $a_1,\dots,a_n \in Q$ i posmatrajmo sistem jednačina

$$f(x_1,\dots,x_n) = a_1$$

$$f_i(x_1,\dots,x_n) = a_{1+i},\ i = 1,\dots,n-1 ,$$

pri čemu su f_i parastrofi od f definisani u teoremi.

Na osnovu definicije operacije f to je u stvari sistem jednačina u grupi $(Q,+)$

$$\begin{aligned}
&\varphi x_1 - \varphi^2 x_2 + \ldots + (-1)^{n+1}\varphi^n x_n = a_1 ,\\
(*) \quad &\varphi x_2 - \varphi^2 x_3 + \ldots + (-1)^n \varphi^{n-1} x_n + (-1)^{n+1}\varphi^n x_1 = a_2 ,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\varphi x_n - \varphi^2 x_1 + \ldots + (-1)^{n+1}\varphi^n x_{n-1} = a_n .
\end{aligned}$$

Ako primenimo φ na drugu jednačinu i dodamo je prvoj dobijamo

$$x_1 + \varphi x_1 = a_1 + \varphi a_2$$

tj.

$$x_1 = (1+\varphi)^{-1}(a_1 + \varphi a_2).$$

Analogno postupku iz i-te i i+1-ve jednačine sistema(*), $i = 2,\ldots,n-1$, dobijamo da je

$$x_i = (1+\varphi)^{-1}(a_i + \varphi a_{i+1}),\ i = 2,\ldots,n-1 ,$$

a iz poslednje i prve jednačine konačno da je

$$x_n = (1+\varphi)^{-1}(a_n + \varphi a_1) .$$

Lako se proverava da je $(1+\varphi)^{-1}$ takodje automorfizam komutativne grupe $(Q,+)$ koji komutira sa φ. Ako se dobijene vrednosti zamene u (*) dobija se da su to rešenja sistema (*). Jasno je da je rešenje jednoznačno.

<u>POSLEDICA 1.31.</u> Neka je n prirodan broj $\geqslant 2$ i $(R,+,\cdot)$ asocijativan prsten sa jedinicom 1, takav da postoji $b \in R$ koji zadovoljava:

(i) b ima inverzni element,

(ii) $1+b$ ima inverzni element,

(iii)
$$b^{n+1} = \begin{cases} -1 & \text{za } n = 2k \\ 1 & \text{za } n = 2k+1 . \end{cases}$$

Ako se definiše u R operacija $f:R^n \to R$ sa

$$f:(x_1,\ldots,x_n) \to bx_1 - b^2x_2 + b^3x_3 - \ldots + (-1)^{n+1}b^n x_n$$

tada je (R,f) samoortogonalna ciklična n-kvazigrupa.

PRIMEDBA. U slučaju kada je prsten konačan dovoljno je u uslovima (i) i (ii) zahtevati samo da b ne bude delitelj nule.

DEFINICIJA 1.14. Prsten $(R,+,\cdot)$ koji zadovoljava uslov posledice 1.31. se naziva C-n-prsten, a element b koren C-n-prstena.

C-n-prsteni su uopštenje S-prstena definisanih u [47].

POSLEDICA 1.32. Neka su R_1 i R_2 C-n-prsteni tada je i direktan proizvod $R_1 \times R_2$ je C-n-prsten čiji je koren (b_1, b_2) ako su b_1 i b_2 koren C-n-prstenovi R_1 i R_2 respektivno.

Sada ćemo odrediti neke vrednosti za n i q za koje postoje C-n-prsteni tj. samoortogonalne cikličke n-kvazigrupe.

POSLEDICA 1.33. Neka su n,q neparni brojevi ≥ 3. Tada postoji samoortogonalna ciklična n-kvazigrupa.

DOKAZ. U prstenu $\mathbb{Z}_q$ ostatak po modulu q, $b = 1$ se koren, jer je $b+1 = 2$ invertibilan element i $b^{n+1} = 1$.

TEOREMA 1.34. Neka je $k > 1$ prirodan broj takav da je $2^k - 1 = rs$, $r,s \in \mathbb{N}$, $s > 1$. Tada za svaki prirodan broj n oblika $ts-1$ gde je $t \geq 1$ postoji samoortogonalna ciklična n-kvazigrupa reda 2^k.

DOKAZ. Neka je G multiplikativna grupa polja Galoa $GF(2^k)$. G je ciklična grupa sa $2^k - 1$ elementom i postoji tačno jedan element takav da je $a+1 = 0$ tj. $a = -1 = 1$ jer je $\mathrm{char}(GF(2^k)) = 2$. Kako 1 očigledno nije generator $(k > 1)$ to postoji generator $b \in G$ takav da je $b+1 \neq 0$.

Za svako $c \in G$, $c \neq 1$ sledi da je $c+1 \neq 0$ pa ako je $2^k - 1 = rs$, $r,s, \in \mathbb{N}$, $s > 1$ tada ke $b^r \neq 1$ i $(b^r)^s = 1$ iz čega sledi da je za svako $t \in \mathbb{N}$ $(b^r)^{st} = 1$. Iz svega dobijamo da je b^r koren C-n-prstena $GF(2^k)$ kad je $n = ts-1$.

Prethodna teorem se može formulisati u sledećem obliku, gde je n fiksno.

TEOREMA 1.35. Neka je $n \geq 2$ prirodan broj takav da je $n+1 \equiv 0 \pmod{s}$ gde je s prirodan broj >1. Tada za svako $k > 1$ takav da je $2^k \equiv 1 \pmod{s}$ postoji samoortogonalna ciklična n-kvazigrupa reda 2^k.

TEOREMA 1.36. Neka je $k \in \mathbb{N}$, p neparan prost broj takav da je $(p^k-1)/2 = rs$, gde su $r,s \in \mathbb{N}$, a s neparan broj >1. Tada za svaki prirodan broj $n = ts-1$, gde je t neparan prirodan broj postoji samoortogonalna ciklična n-kvazigrupareda p^k.

DOKAZ. Neka je G multiplikativna grupa polja Galoa $GF(p^k)$ i neka je b generator grupe $(G,\cdot)$ takav da je $b \neq -1$. Dokaz da takav generator postoji se dokazuje analogno kao u teoremi 1.34: Jednačina $x^2 = 1$ u G ima rešenje -1, a kako je G ciklična grupa jedini elementi u G koji su rešanje su 1 ili $b^{(p^k-1)/2}$ pa je

$$b^{(p^k-1)} = -1 .$$

Ako je $(p^k-1)/2 = rs$, $r,s \in \mathbb{N}$ i s neparan >1, tada je $b^r \neq -1$ i $(b^r)^s = -1$ pa je $(b^r)^{st} = -1$ za svaki neparan broj t. Otuda je za $n = ts-1$, b^r koren C-n-prstena $GF(p^k)$.

Ako se prethodna teorema formuliše za fiksno n tada se dobija

TEOREMA 1.37. Neka je n paran prirodan broj takav da je $n+1 \equiv 0 \pmod{s}$ gde je s prirodan broj >1. Tada za svaki prirodan broj k i svaki neparan prost broj p takav da je $p^k \equiv 1 \pmod{s}$ postoji samoortogonalna ciklična n-kvazigrupa reda p^k.

Ako se iskoristi posledica 1.32. dobija se sledeća opšta teorema.

TEOREMA 1.38. Neka je n paran prirodan broj, $p_1,\dots,p_m$ prosti brojevi, a $\alpha_1,\dots,\alpha_m$ prirodni brojevi takvi da je $p_i^{\alpha_i} \equiv 1 \pmod{s_i}$, gde je $s_i > 1$ delitelj od $n+1$, $i = 1,\dots,m$. Tada za proizvoljne nenegativne cele brojeve β_i, $i = 1,\dots,m$, postoji samoortogonalna ciklična n-kvazigrupa reda q

$$q = p_1^{\alpha_1\beta_1} \cdots p_m^{\alpha_m b_m} .$$

Ova teorema predstavlja uopštenje većeg broja autora [35],[36],[37],[47] čiji su rezultati objedinjeni u sledećoj teoremi:

TEOREMA 1.39. [4] Neka su $p_1,\dots,p_r$ prosti brojevi $\equiv 1 \pmod 3$, neka su $q_1,\dots,q_s$ prosti brojevi $\equiv 2 \pmod 3$ i neka je

$$q = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{2\beta_1} \cdots q_s^{2\beta_s} ,$$

gde su α_i, β_i nenegativni celi brojevi. Tada postoji samoortogonalna polusimetrična kvazigrupa reda q.

Teorema 1.39. je specijalan slučaj teoreme 1.38. Zaista za $n=2$ je $n+1 = 3$ prost broj, pa je u teoremi 1.38. $s_i = 3$ za svako $i=1,\dots,m$. Ako je q_j prost broj $\equiv 2 \pmod 3$ tada je $q_j^2 \equiv 1 \pmod 3$ pa je teorema 1.39. posledica teoreme 1.38.

LEMA 1.40. Neka je n prirodan broj $\geqslant 2$, a p prost broj $p > n+1$. Neka je $p(x)$ polinom

$$(*) \quad p(x) = x^n - \binom{n+1}{1} x^{n-1} + \binom{n+1}{2} x^{n-2} + \dots + (-1)^n \binom{n+1}{n} \in \mathbb{Z}_p[x]$$

tada rešenje jednačine $p(x) = 0$ nisu 0 ni 1.

DOKAZ. Kako je $p > n+1$ jasno je da 0 nije rešenje, a kako je $xp(x) = (x-1)^{n+1} - (-1)^{n+1}$ sledi da ni 1 nije rešenje.

TEOREMA 1.41. Neka je n prirodan broj, a p prost broj takav da je $p > n+1$. Neka je $r(x)$ nesvodljivi faktor, nad $\mathbb{Z}_p$, polinoma (*) i neka je k stepen polinoma $r(x)$. Tada postoji samoortogonalna ciklična n-kvazigrupa reda p^k.

DOKAZ. Neka je $R = \mathbb{Z}_p[\alpha]$ gde je α koren polinoma $r(x)$. Tada je zbog Leme1.40 $\alpha \neq 0$ pa α ima inverzni, a i $\beta = \alpha-1 \neq 0$ pa i β ima inverzni. Izračunajmo β^{n+1}

$$\beta^{n+1} = (\alpha-1)^{n+1} = \alpha p(\alpha) + (-1)^{n+1} = (-1)^{n+1} .$$

$1+\beta = \alpha$ je invertibilan pa je β koren C-n-prstena R reda $q = p^k$.

Koristeći posledicu 1.32. dobija se teorema

TEOREMA 1.42. Neka je prirodan broj $n \geq 2$ i neka su $p_1,\dots,p_s$ prosti brojevi takvi da je $p_i > n+1$, $i=1,\dots,s$. Tada postoje prirodni brojevi $k_1,\dots,k_s$, $1 \leq k_i \leq n$, $i=1,\dots,s$ takvi da za svaki prirodan broj α_i, $i=1,\dots,s$ postoji samoortogonalna ciklična n-kvazigrupa reda

$$q = q_1^{\alpha_1} \cdots q_s^{\alpha_s} ,$$

gde su $q_i = p_i^{k_i}$, $i=1,\dots,s$.

II

n-GRUPA

U odnosu na n-kvazigrupe struktura n-grupa može da se opiše pomoću binarne grupe nad istim nosačem, što omogućava da se svaki problem sa n-grupama svede na problem sa binarnim grupama koje su mnogo bolje izučena algebarska struktura. Najpre su navedene teoreme koje daju nekoliko jednostavnijih uslova za proveru, od definicije, kada je n-kvazigrupa, odnosno n-polugrupa, n-grupa i teoreme o reprezentaciji, a zatim se prelazi na osnovnu temu izučavanja ove teze, G-n-grupe.

<u>DEFINICIJA 2.1.</u> n-grupoid (Q,f) se naziva (i,j)-asocijativan ako i samo ako važi identitet

$$f(x_1^{i-1}, f(x_i^{i+n-1}), x_{i+n}^{2n-1}) = f(x_1^{j-1}, f(x_j^{j+n-1}), x_{j+n}^{2n-1}) .$$

<u>DEFINICIJA 2.2.</u> n-grupoid (Q,f) se naziva n-polugrupa ako i samo ako je (j,i)-asocijativan za svako $i,j \in \mathbb{N}_n$.

<u>DEFINICIJA 2.3.</u> n-polugrupa (q,f) se naziva n-grupa ako i samo ako je (Q,f) i n-kvazigrupa.

Za $n \geqslant 3$ nisu svi uslovi ((i,j)-asocijativnost za svako $i,j \in \mathbb{N}_n$ i jednoznačna rešivost $f(a_1^{k-1},x,a_k^{n-1}) = b$ za svako $k \in \mathbb{N}_n$) nezavisni. Naime, važi ([46],[40],[9]).

TEOREMA 2.1. Neka je (Q,f) n-polugrupa, $n \geqslant 3$. Tada je (Q,f) n-grupa ako i samo ako je ispunjen jedan od uslova

(i) Postoji bar jedno $i \in \{2,3,\ldots,n-1\}$ takvo da jednačina

$$f(a_1^{i-1},x,a_i^{n-1}) = b$$

ima jednoznačno rešenje za svako $a_1^{n-1}, b \in Q$.

(ii) Jednačine

$$f(x,a_1^{n-1}) = b, \quad i \quad f(a_1^{n-1},y) = b$$

imaju jednoznačna rešenja za svako $a_1^{n-1}, b \in Q$.

DEFINICIJA 2.4. Neka je (Q,f) n-grupoid. Niz $(e_1,e_2,\ldots,e_{n-1})$ se naziva i-ti jedinični slog ako i samo ako za svako $x \in Q$ važi

$$f(e_1^{i-1},x,e_i^{n-1}) = x \ .$$

Za $i = n$ (e_1^{n-1}) se naziva levi jedinični slog, a za $i=1$ se (e_1^{n-1}) naziva desni jedinični slog. Ako je (e_1^{n-1}) i levi i desni jedinični slog i ako je svaka ciklična permutacija od (e_1^{n-1}) takodje i levi i desni jedinični slog tada se (e_1^{n-1}) naziva $(n-1)$-adski jedinični slog ili prosto jedinični slog ako to ne može da dovede do zabune.

U slučaju kada je $e_i = e$, $i=1,\ldots,n-1$, tada se element e naziva i-ti jedinični element, levi jedinični element, desni jedinični element. Ako je e i-ti jedinični element za svako $i \in \mathbb{N}_n$ tada se e naziva jedinični element ili prosto jedinica.

Iz dokaza teoreme 2.1. dobijamo

POSLEDICA 2.2. Neka je (Q,f) n-grupa. Da bi slog (e_1^{n-1}) bio jedinični slog dovoljno je da postoji bar jedan element $x \in Q$ takav da je

$$\text{(i)} \quad f(e_1^{n-1},x) = x ,$$

ili

$$\text{(ii)} \quad f(x,e_1^{n-1}) = x.$$

Dakle u n-grupi jedinični slog može da se izabere posebno jednostavno, jer za svako $e_1^{n-2} \in Q$ postoji e_{n-1} tako da važi (i) ili (ii).

DEFINICIJA 2.5. Neka je (Q,f) n-grupa. Tada se rešenje jednačine

$$f(a,\ldots,a,x) = a$$

naziva kosim elementom elementa a i označava sa $\bar{a}$.

Iz posledice 2.2. se dobija

TEOREMA 2.3. Neka je (Q,f) n-grupa i $\bar{a}$ kosi element za element $a \in Q$. Tada je za svako $i \in \mathbb{N}_n$

$$f(\overset{i-1}{a}, \bar{a}, \overset{n-i}{a}) = a.$$

POSLEDICA 2.4. Neka je (Q,f) n-grupa i $a \in Q$. Tada je za svako $x \in Q$ i svako $i \in \mathbb{N}_n$

$$f(x, \overset{i-1}{a}, \bar{a}, \overset{n-i-1}{a}) = x \quad \text{i} \quad f(\overset{i-1}{a}, \bar{a}, \overset{n-i-1}{a}, x) = x,$$

Ako se pretpostavi kvazigrupnost operacije f (rešivost $f(a_1^{i-1},x,a_i^{n-1}) = b$ za svako $i \in \mathbb{N}_n$) tada, da bi (Q,f) bila grupa ne moramo pretpostaviti (i,j)-asocijativnost za svako $i,j \in \mathbb{N}_n$. Naime, imamo sledeću teoremu [53]. Navešćemo dokaz ove teoreme, jer iz njega sledi nešto opštija posledica koja je najpogodnija za primenu.

TEOREMA 2.5. Neka je (Q,f) n-kvazigrupa $n \geq 3$. Tada je (Q,f) n-grupa ako i samo ako je $(i,i+1)$-asocijativna za neko $i \in \mathbb{N}_{n-1}$.

DOKAZ. Neka je a proizvoljan element iz Q. Tada iz $(i,i+1)$-asocijativnosti sledi

$$f(\overset{i-1}{a},f(x_1^{i},f(x_{i+1}^{i+n}),x_{i+n+1}^{2n-1}),\overset{n-i}{a}) =$$
$$= f(\overset{i-1}{a},x_1,f(x_2^{i},f(x_{i+1}^{i+n}),x_{i+n+1}^{2n-1},a),\overset{n-i-1}{a}) ,$$

pa ako sada na unutrašnji izraz desne strane ponovo primenimo $(i,i+1)$-asocijativnost dobijamo da je

$$f(\overset{i-1}{a},x_1,f(x_2^{i},f(_{i+1}^{i+n}),x_{i+n+1}^{2n-1},a),\overset{n-i-1}{a}) =$$
$$= f(\overset{i-1}{a},x_1,f(x_2^{i+1},f(x_{i+2}^{i+n+1}),x_{i+n+2}^{2n-1},a),\overset{n-i-1}{a}) .$$

Primenimo sada na desnu stranu $(i,i+1)$-asocijativnost tako da od operacije na $i+1$-vom mestu dobijemo operaciju na i-tom mestu pa je

$$f(\overset{i-1}{a},x_1,f(x_2^{i+1},f(x_{i+2}^{i+n+1}),x_{i+n+2}^{2n-1},a),\overset{n-i-1}{a}) =$$
$$= f(\overset{i-1}{a},f(x_1^{i+1},f(x_{i+2}^{i+n+1}),x_{i+n+2}^{2n-1}),\overset{n-i}{a})$$

tj. iz $(i,i+1)$-asocijativnosti sledi $(i+1,i+2)$-asocijativnost pa na osnovu tranzitivnosti dobijamo $(i,i+2)$-asocijativnost itd.

Dokažimo sada $(i-1,i)$-asocijativnost.

$$f(\overset{i}{a},f(x_1^{i-1},f(x_i^{i+n+1}),x_{i+n}^{2n-1}),\overset{n-i-1}{a}) =$$
$$= f(\overset{i-1}{a},f(a,x_1^{i-1},f(x_i^{i+n-1}),x_{n+1}^{2n-2}),x_{2n-1},\overset{n-i-1}{a}) =$$
$$= f(\overset{i-1}{a},f(a,x_1^{i-2},f(x_{i-1}^{i+n-2}),x_{i+n-1}^{2n-2}),x_{2n-1},\overset{n-i-1}{a}) =$$
$$= f(\overset{i}{a},f(x_1^{i-2},f(x_{i-1}^{i+n-2}),x_{i+n-1}^{2n-1}),\overset{n-i-1}{a})$$

pa je zbog jednoznačnosti rešenja $f(a_1^{i},x,a_{i+1}^{n-1}) = b$ sledi da je

$$f(x_1^{i-1},f(x_i^{i+n-1}),x_{i+n}^{2n-1}) = f(x_1^{i-2},f(x_{i-1}^{i+n-2}),x_{i+n-1}^{2n-2})$$

tj. $(i-1,i)$-asocijativnost i nastavljajući $(i-2,i)$-asocijativnost itd. Dakle iz $(i,i+1)$-asocijativnosti sledi (i,j) -asocijativnost za svako $j \in \mathbb{N}_n$, a takodje i (i,k)-asocijativnost za svako $j,k \in \mathbb{N}_n$, čime je dokaz završen.

Iz dokaza prethodne teoreme sledi da je za dokaz (i,j)-asocijativnosti za $j > i$ dovoljna jednoznačna rešivost $f(a_1^{i-1},x,a_i^{n-1}) = b$ na i-tom mestu, a za (j,i)-asocijativnost je dovolja rešivost $f(a_1^i,x,a_{i+1}^{n-1}) = b$ na $(i+1)$-vom mestu pa imamo sledeću posledicu kombinujući teoreme 2.1 i 2.5.

POSLEDICA 2.6. Neka je (Q,f) n-grupoid. (Q,f) je n-grupa ako i samo ako je zadovoljen bar jedan od uslova:

(i) (Q,f) je $(i,i+1)$-asocijativan za $i \in \{2,\ldots,\ldots,n-2\}$ i jednačina
$$f(a_1^{k-1},x,a_k^{n-1}) = b$$
ima jednoznačno rešenje za $k=i$ i za bar još jedno $k > i$.

(ii) (Q,f) je $(1,2)$-asocijativan i $f(a_1^{k-1},x,a_k^{n-1}) = b$ ima rešenje za $k=n$ i ima jednoznačno rešenje za $k=1$.

(iii) (Q,f) je $(n-1,n)$-asocijativan i $f(a_1^{k-1},x,a_k^{n-1}) = b$ ima rešenje za $k=1$ i ima jednoznačno rešenje za $k=n$.

Pri izračunavanju n-grupa su važne dve teoreme o reprezentaciji n-arne operacije pomoću binarnih operacija, teorema Posta [46] i teorema Hosu-Gluskina [36]. Pošto ćemo u daljem izlaganju koristiti teoremu Hosu-Gluskina nju ćemo dati sa dokazom dok ćemo teoremu Posta samo formulisati.

TEOREMA 2.7. (Post [46]. Neka je (Q,f) n-grupa Tada:

(i) Postoji binarna grupa $(G,\cdot)$ čiji je skup generatora Q takav da G sadrži normalnu podgrupu N takvu da je $N = Q^{n-1}$

(ii) $f(x_1^n) = x_1 x_2 \ldots x_n$, $x_i \in Q$, $i=1,\ldots,n$.

(iii) Faktorgrupa G/N je ciklična grupa reda $n-1$.

(iv) G je jednoznačno odredjena (do na izomorfizam).

TEOREMA 2.8. (Hosu-Gliskin) Neka je (Q,f) n-grupa $n \geq 3$. Tada postoji binarna grupa $(Q,\cdot)$ i njen automorfizam takav da je

$$f(x_1^n) = x_1 \varphi(x_2) \varphi^2(x_3) \ldots \varphi^{n-2}(x_{n-1}) \varphi^{n-1}(x_n) c ,$$

pri čemu je c fiksan element iz Q takav da je

$$\varphi(c) = c \quad \text{i} \quad \varphi^{n-1}(x) = c x c^{-1} .$$

DOKAZ. Definišimo operaciju $\cdot$ i preslikavanje φ sa

$$xy = f(x, \overset{n-2}{a}, y) ,$$

$$\varphi(x) = f(\bar{a}, x, \overset{n-2}{a}).$$

Tada je

$$(xy)z = f(f(x, \overset{n-2}{a}, y), \overset{n-2}{a}, z) =$$

$$= f(x, \overset{n-2}{a}, f(y, \overset{n-2}{a}, z)) = x(yz)$$

pa je $(Q,\cdot)$ podgrupa

$$bx = c \Leftrightarrow f(b, \overset{n-2}{a}, x) = c ,$$

$$yb = c \Leftrightarrow f(y, \overset{n-2}{a}, b) = c$$

imaju jednoznačna rešenja, jer je (Q,f) n-kvazigrupa pa je $(Q,\cdot)$ grupa. Neposredno sledi da je jedinica grupe $(Q,\cdot)$ $\bar{a}$, kosi element od a.

Izračunajmo sada $\varphi(xy)$.

$$\varphi(xy) = f(\bar{a}, f(x, \overset{n-2}{a}, y), \overset{n-2}{a}) = f(f(\bar{a}, x, \overset{n-2}{a}), y, \overset{n-2}{a}) =$$

$$= f(\varphi(x), y, \overset{n-2}{a}) .$$

Kako je za svako $y \in Q$ (posledica 2.4)

$$f(\overset{n-2}{a}, \bar{a}, y) = y$$

to je

$$f(\varphi(x),y,\overset{n-2}{a}) = f(\varphi(x),f(\overset{n-2}{a},\bar{a},y),\overset{n-2}{a}) =$$

$$= f(\varphi(x),\overset{n-2}{a},f(\bar{a},y,\overset{n-2}{a})) =$$

$$= f(\varphi(x),\overset{n-2}{a},\varphi(y)) = \varphi(x)\varphi(y)$$

pa je φ homomorfizam koji je bijekcija pa je φ automorfizam.

Neka je

$c = f(\bar{a},\ldots,\bar{a})$. Tada je

$$\varphi(c) = f(\bar{a},c,\overset{n-2}{a}) = f(c,\bar{a},\overset{n-2}{a}) = c\ .$$

Konačno

$$cx = f(c,\overset{n-2}{a},x) = f(\bar{a},\ldots,\bar{a},x) =$$

$$= f(\bar{a},\ldots,\bar{a},f(x,\overset{n-2}{a},\bar{a})) = f(\bar{a},\ldots,\bar{a},\varphi(x),\bar{a}) =$$

$$= f(\bar{a},\ldots,\bar{a},\varphi^2(x),\bar{a},\bar{a}) = \ldots =$$

$$= f(\varphi^{n-1}(x),\bar{a},\ldots,\bar{a}) =$$

$$= f(f(\varphi^{n-1}(x),\overset{n-2}{a},\bar{a}),\bar{a},\ldots,\bar{a}) =$$

$$= f(\varphi^{n-1}(x),\overset{n-2}{a},f(\bar{a},\ldots,\bar{a})) =$$

$$= f(\varphi^{n-1}(x),\overset{n-2}{a},c) = \varphi^{n-1}(x)c$$

pa je

$$\varphi^{n-1}(x) = c\,x\,c^{-1}\ .$$

Izračunajmo sada $f(x_1^n)$.

$$f(x_1^n) = f(x_1^{n-1},f(x_n,\overset{n-2}{a},\bar{a})) = f(x_n^{n-1},f(f(\overset{n-2}{a},\bar{a},x_n,),\overset{n-2}{a},\bar{a}))=$$

$$= f(x_1^{n-1},f(\overset{n-2}{a},\varphi(x_n),\bar{a})) = f(x_1^{n-2},x_{n-1}\,\varphi(x_n),\bar{a}) =$$

$$= f(x_1^{n-3},x_{n-2}\varphi(x_{n-1}\varphi(x_n)),\bar{a},\bar{a}) = \ldots =$$

$$= f(x_1\varphi(x_2)\ldots\varphi^{n-1}(x_n),\bar{a},\ldots,\bar{a}) =$$

$$= f(f(x_1\varphi(x_2)\ldots\varphi^{n-1}(x_n),\overset{n-2}{a},\bar{a}),\bar{a},\ldots,\bar{a}) =$$

$$= f(x_1\varphi(x_2)\ldots\varphi^{n-1}(x_n,\overset{n-2}{a},c) = x_1\varphi(x_2)\ldots\varphi^{n-1}(x_n)c\ .$$

<u>PRIMEDBA.</u> Grupa $(Q,\cdot)$ je odredjena jednoznačno (do na izomorfizam).

Prećićemo sad na osnovni objekt našeg izučavanja: G-n-grupe.

DEFINICIJA 2.6. n-grupa (Q,f) se naziva G-n-grupa ako i samo ako je $f = f^{\sigma}$ za svaku permutaciju σ grupe permutacija G, gde je G podgrupa od S_{n+1}.

Ako sada specijaliziramo grupu permutacija G dobijamo niz klasa n-grupa koje mogu da se definišu nekim identitetima.

DEFINICIJA 2.7. n-grupa (Q,f) se naziva C-n-grupa ako i samo ako je f ciklična n-kvazigrupa.

DEFINICIJA 2.8. n-grupa (Q,f) se naziva AS-n-grupa ako i samo ako je f AS-n-kvazigrupa.

DEFINICIJA 2.9. n-grupa (Q,f) se naziva i-permutabilna n-grupa ako i samo ako je G-n-grupa za $G = \langle(i,i+1,\ldots$ $\ldots,n,n+1)\rangle$.

Za ove klase n-grupa možemo još oslabiti kvazigrupnost ili asocijativnost. Naime, za C-n-grupe važi sledeća teorema.

TVRDJENJE 2.9. Neka je (Q,f) (i,j)-asocijativna ciklična n-kvazigrupa. Tada je (Q,f) $(i+1,j+1)$-asocijativna (pri čemu su $i+1$, $j+1$ redukovani po modulu n).

DOKAZ. Neka je $i,j \neq n$. Ako primenimo cikličnost na (i,j)-asocijativnost dobijamo da je

$$f(x_1^{i-1},f(x_i^{i+n-1}),x_{i+n}^{2n-1}) = x_{2n}$$

ekvivalentno sa

$$f(x_{2n},x_1^{i-1},f(x_i^{i+n-1}),x_{i+n}^{2n-2}) = x_{2n-1}\ ,$$

a zbog cikličnosti je i

$$f(x_1^{j-1},f(x_j^{j+n-1}),x_{j+n}^{2n-1}) = x_{2n}$$

ekvivalentno sa

$$f(x_{2n},x_1^{j-1},f(x_j^{j+n-1}),x_{j+n}^{2n-2}) = x_{2n-1}\ ,$$

pa je otuda

$$f(x_{2n},x_1^{i-1},f(x_i^{i+n-1}),x_{i+n}^{2n-2}) = f(x_{2n},x_1^{j-1},f(x_j^{j+n-1}),x_{j+n}^{2n-2})$$

tj. u ovom slučaju je f $(i+1,j+1)$-asocijativno.

Neka je sada $i=n$, $j \neq n$. Tada je

$$f(x_1^{i-1},f(x_i^{i+n-1}),x_{i+n}^{2n-1}) = x_{2n}$$

zbog cikličnosti ekvivalentno sa

$$f(x_{2n},x_1^{i-1},f(x_i^{i+n-1}),x_{i+n}^{2n-2}) = x_{2n-1}$$

dok na

$$f(x_1^{j-1},f(x_j^{2n-1})) = x_{2n}$$

dva puta primenimo cikličnost pa dobijamo

$$f(f(x_{2n},x_1^{j-1}),x_j^{2n-2}) = x_{2n-1} ,$$

pa je konačno

$$f(x_{2n},x_1^{i-1},f(x_i^{i+n-1}),x_{i+n}^{2n-2}) = f(f(x_{2n},x_1^{j-1}),x_j^{2n-2}) ,$$

što je i trebalo dokazati.

<u>POSLEDICA 2.10.</u> Neka je (Q,f) (i,j)-asocijativna ciklička n-kvazigrupa. Tada je (Q,f) $(i+m,j+m)$-asocijativna n-kvazigrupa (pri čemu je $i+m$, $j+m$ redukovano po modulu n).

Koristeći ovu posledicu dobijamo sledeću karakterizaciju C-n-grupa.

<u>TEOREMA 2.11.</u> Neka je (Q,f) (i,j)-asocijativna ciklična n-kvazigrupa. Ako je $j-i$ uzajamno prosto sa n tada je (Q,f) C-n-grupa.

<u>DOKAZ.</u> Neka je $j-i=k$. Tada je (Q,f) $(i,i+k)$ - asocijativna n-kvazigrupa. Na osnovu prethodne posledice imamo da je (Q,f) $(i+mk,i+(m+1)k)$-asocijativna, pri čemu se svi brojevi redukuju po modulu n. Odatle sledi da je (Q,f)

$(i,i+mk)$- asocijativno za svaki prirodan broj m. No medjutim, $i+mk(\mathrm{mod}\ n)$ daje potpun sistem ostataka jer $(k,n)=1$. Otuda dobijamo da je (Q,f) (i,j)-asocijativno za svako $i,j \in \mathbb{N}_n$.

U slučaju i-permutabilnih n-grupa imaćemo sledeću karakterizaciju.

TEOREMA 2.12. Neka je (Q,f) i-permutabilan n-grupoid i neka su $1 \leqslant i \leqslant j < k < n$ prirodni brojevi. Grupoid (Q,f) je (j,k)-asocijativan ako i samo ako je $(j+1,k+1)$-asocijativan.

DOKAZ. Neka je (Q,f) i-permutabilan (j,k)-asocijativan n-grupoid, $1 \leqslant i \leqslant j < k < n$. Tada je za svako $x_1^{2n} \in Q$

$$f(x_1^{j-1}, f(x_j^{j+n-1}), x_{j+n}^{2n-1}) = x_{2n}$$

ako i samo ako je

$$f(x_1^{k-1}, f(x_k^{k+n-1}), x_{k+n}^{2n-1}) = x_{2n}$$

pa je zbog i-permutabilnosti

$$f(x_1^{i-1}, x_{2n}, x_i^{j-1}, f(x_j^{j+n-1}), x_{j+n}^{2n-2}) = x_{2n-1}$$

ako i samo ako je

$$f(x_1^{i-1}, x_{2n}, x_i^{k-1}, f(x_k^{k+n-1}), x_{k+n}^{2n-2}) = x_{2n-1}$$

tj, za svako $x_1^{2n-2}, x_{2n} \in Q$ je

$$f(x_1^{i-1}, x_{2n}, x_i^{j-1}, f(x_j^{j+n-1}), x_{j+n}^{2n-2}) =$$

$$= f(x_1^{i-1}, x_{2n}, x_i^{k-1}, f(x_k^{k+n-1}), x_{k+n}^{2n-2}),$$

tj. (Q,f) je $(j+1,k+1)$-asocijativan. Jasno je da ćemo se, ponavljajući gornju postupak dovoljan broj puta, ponovo vratiti na identitet (j,k)-asocijativnosti, pa sledi da polazeći od $(j+1,k+1)$-asocijativnosti možemo dobiti (j,k)-asocijativnost.

POSLEDICA 2.13. Neka je (Q,f) i-permutabilan n-grupoid i $1 \leqslant i \leqslant j < k \leqslant n$. Tada je (Q,f) (j,k)-asocijativan ako i samo ako je $(j-1,k-1)$-asocijativan.

POSLEDICA 2.14. Neka je (Q,f) i-permutabilan n-grupoid koji je (j,k)-asocijativan gde je $1 \leqslant i \leqslant j < k \leqslant n$. Tada:

(i) Ako je $k < n$ tada je (Q,f) $(i+s,k+s)$-asocijativan za svako $s \in \mathbb{N}_{n-k}$.

(ii) Ako je $i < j$ tada je (Q,f) $(j-t,k-t)$-asocijativan za svako $t \in \mathbb{N}_{j-i}$.

Koristeći prethodnu teoremu i njene posledice imamo

TEOREMA 2.15. Neka je (Q,f) i-permutabilna n-kvazigrupa koja je (j,k)-asocijativna za $1 \leqslant i \leqslant j < k < n$. Tada je (Q,f) n-grupa ako i samo ako je (p,m)-asocijativna, pri čemu je $i \leqslant p < m < n$ i $k-j = m-p\pm 1$.

DOKAZ. Neka je (Q,f) i-permutabilna n-kvazigrupa koja je (j,k) i (p,m)-asocijativna za $i \leqslant j < k < n$ i $i \leqslant p < m < n$. Kako je tada (Q,f) takodje $(j+s,k+s)$- i $(p+t,m+t)$-asocijativna za svako $s \in \mathbb{N}_{n-k}$ i $t \in \mathbb{N}_{n-m}$ pa ako je $k-j = m-p\pm 1$ tada je (Q,f) $(r,r+1)$-asocijativna za neko $r \in \mathbb{N}_{n-j}$, što je dovoljno za asocijativnost na osnovu teoreme 2.5.

Koristeći posledicu 2.6 dobijamo sledeće tvrdjenje.

TEOREMA 2.16. Neka je (Q,f) i-permutabilan n-grupoid. Tada je (Q,f) n-grupa ako i samo ako je zadovoljen bar jedan od sledećih uslova:

(i) Ako je $i=1$ tada je dovoljno da je $(j,j+1)$-asocijativan za neko $j \in \mathbb{N}_{n-1}$.

(ii) Ako je $i \in \{2,\dots,n-2\}$ tada je dovoljno da je $(j,j+1)$-asocijativan za neko $j \in \{i,i+1,\dots,\dots,n-2\}$.

(iii) Ako je $i = n-1$ ili $i=n$ tada je dovoljno da je $(n-1,n)$-asocijativan i da jednačina $f(a_1^{k-1},x,a_k^{n-1}) = b$ ima rešenje za $k=1$, (rešenje ne mora biti jedinstveno).

Ako iskoristimo teoremu 2.1 dobijamo

TEOREMU 2.17. Neka je (Q,f) i-permutabilna n-polugrupa gde je $i \in \mathbb{N}_{n-1}$. Tada je (Q,f) n-grupa.

U slučaju AS-n-grupa, iz Hosu-Gluskinove teoreme (teorema 2.8) se dobija opis strukture operacije f AS-n-grupe.

TEOREMA 2.18. [56] Neka je (Q,f) n-grupa. (Q,f) je AS-n-grupa ako i samo ako postoji komutativna binarna grupa $(Q,+)$ takva da je za svako $x \in Q$, $x+x = 0$ i

$$f(x_1^n) = x_1 + x_2 + \ldots + x_n + c\ ,$$

pri čemu je c fiksan element skupa Q.

Koristeći poznati rezultat o konačnim bulovim grupama (tj. grupama u kojima za svako x važi $x+x = 0$) dobija se

POSLEDICA 2.19. [56] Neka je (Q,f) konačna AS-n-grupa. Tada je $|Q|$ jedinica ili stepen dvojke.

Ako iskoristimo Hosu-Gluskinovu teoremu u slučaju C-n-grupa dobijamo

TEOREMA 2.20. Neka je (Q,f) n-grupa pri čemu je n paran broj. n-grupa (Q,f) je C-n-grupa ako i samo ako postoji abelova grupa $(Q,+)$ takva da je $x+x = 0$ za svako $x \in Q$ i

$$f(x_1^n) = \sum_{k=1}^{n} x_k + c$$

gde je c fiksan element skupa Q.

DOKAZ. Neka je (Q,f) C-n-grupa. Na osnovu Hosu-Gluskinove teoreme postoji binarna grupa $(Q,\cdot)$, njen automorfizam φ i element $c \in Q$ tako da je

$$f(x_1^n) = x_1\varphi(x_2)\ldots\varphi^{n-1}(x_n)c ,$$

gde je $\varphi(c) = c$ i $\varphi^{n-1}(x) = cxc^{-1}$. Koristeći tu reprezentaciju za identitet

$$f(f(x_1^n), x_1^{n-1}) = x_n$$

koji važi u C-n-grupama dobijamo

$$(*) \quad x_1\varphi(x_2)\ldots\varphi^{n-1}(x_n)c\varphi(x_1)\varphi^2(x_2)\ldots\varphi^{n-1}(x_{n-1})c = x_n .$$

Ako sada u (*) stavimo $x_i = e$, $i=1,\ldots,n$, gde je e neutralni element od $(Q,\cdot)$ dobijamo da je $c^2 = e$.

Stavimo sada $x_i = e$, $i=2,\ldots,n$, u (*) dobijamo da je

$$x_1\varphi(x_1) = e \quad \text{tj.} \quad \varphi(x) = x^{-1} ,$$

a ako stavimo $x_i = e$, $i=1,\ldots,n-1$, dobijamo

$$\varphi^{n-1}(x) = x,$$

a kako je n parno to je

$$(x^{-1})^{n-1} = x^{-1} = x$$

pa je

$$x^2 = e.$$

Grupa u kojoj je za svako x, $x^2 = e$ je na osnovu poznatog rezultata komutativna pa je u jednom pravcu dokaz završen.

Drugi deo tvrdjenja se proverava direktnim izračunavanjem.

<u>POSLEDICA 2.21.</u> Neka je (Q,f) C-n-grupa i n paran broj. Tada je Q red grupe (Q,f) ili jedinica ili stepen dvojke.

<u>TEOREMA 2.22.</u> Neka je (Q,f) n-grupa pri čemu je n neparno. n-grupa (Q,f) je C-n-grupa ako i samo ako postoji abelova grupa $(Q,+)$ takva da je

$$f(x_1^n) = x_1 - x_2 + x_3 - + \ldots + x_n + c \;,$$

pri čemu je c fiksan element iz Q za koji važi $c = -c$.

DOKAZ. Koristeći se postupkom korišćenim u dokazu teoreme 2.20 se dobija da je $\varphi(x) = x^{-1}$ pa je

$$f(x_1^n) = x_1 x_2^{-1} x_3 \ldots x_{n-1}^{-1} x_n c$$

za elemente binarne grupe $(Q,\cdot)$ pri čemu je $c = c^{-1}$ i $\varphi^{n-1}(x) = c\,x\,c^{-1}$ pa je $x\,c = c\,x$.

Ako sad u identitetu (*) dokaza teoreme 2.20 stavimo $x_i = e$, $i=2,\ldots,n-1$ i iskoristimo $c^2 = e$ i $c\,x = x\,c$ dobijamo

$$x_1 x_n x_1^{-1} = x_n$$

tj.

$$x_1 x_n = x_n x_1$$

i grupa $(Q,\cdot)$ je komutativna.

Dokaz u suprotnom smeru se dobija direktnom proverom.

POSLEDICA 2.23. Neka je n neparan prirodan broj. Tada za svaki prirodan broj $q \in \mathbb{N}$ postoji C-n-grupa (Q,f) takva da je $|Q| = q$.

POSLEDICA 2.24. Neka je (Q,f) AS-n-grupa ili C-n-grupa pri čemu je n parno. Tada n-grupa (Q,f) ima jedinstven jedinični element.

DOKAZ. Na osnovu teoreme 2.20 sledi da je

$$f(x_1^n) = x_1 + x_2 + \ldots + x_n + c$$

pri čemu je $x+x = 0$ za svako $x \in Q$. Na osnovu posledice 2 (i) dovoljno je rešiti

$$x_1 = x_1 + x + \ldots + x + c,$$

kako je n parno tada je

$x + c = 0$ tj. $x = c$.

POSLEDICA 2.25. Neka je (Q,f) AS-n-grupa ili C-n-grupa pri čemu je n neparno. Ako je y reprezentaciji operacije f $c = 0$ tada je

(i) $x = \bar{x}$ za svako $x \in Q$.

(ii) Za svako $x \in Q$ je $f(\overset{n}{x}) = x$.

POSLEDICA 2.26. Neka je (Q,f) AS-n-grupa pri čemu je n neparno. Ako je u reprezentaciji operacije f $c = 0$ tada je svaki element $x \in Q$ jedinični element za (Q,f).

III

MULTIKVAZIGRUPE

Od svih n-arnih algebarskih struktura razmatranih u ovoj tezi, (n,m)-kvazigrupe ili jednostavnije multikvazigrupe, su se najkasnije pojavile, uvedene su 1980. godine u [19]. Kao što se kvazigrupe dobijaju kao podklasa grupoida u kojoj jednačine $ax = b$ i $ya = b$ imaju jednoznačna rešenja po x i y, tako su i multikvazigrupe podklasa (n,m)-grupoida u kojoj sistem uopštenih jednačina ima jednoznačno rešenje. Kako se u ovoj tezi po prvi put izlaže algebarska teorija multikvazigrupa to se, zbog celovitosti, navodi nešto više rezultata drugih autora nego što je u tezama uobičajeno.

DEFINICIJA 3.1. Neka je Q neprazan skup, a n i m prirodni brojevi $n,m \geqslant 1$ i f funkcija $f:Q^n \to Q^m$. Tada se algebra (Q,f) naziva (n,m)-grupoid ili jednostavno multigrupoid ako to ne dovodi do zabune.

DEFINICIJA 3.2. (n,m)-grupoid se naziva (n,m) kvazigrupa ako i samo ako za svako $a_1^n \in Q^n$ i svaku injekciju $\varphi: \mathbb{N}_n \to \mathbb{N}_{n+m}$ postoji jednoznačno odredjena (m+n)-torka $(b_1^{n+m}) \in Q^{n+m}$ takva da je

$$\text{(i)} \quad a_i = b_{\varphi(i)} \ , \ i=1,\dots,n \ ,$$

$$\text{(ii)} \quad f(b_1^n) = (b_{n+1}^{n+m}) \ .$$

Ako to ne dovodi do zabune (n,m)-kvazigrupa se naziva multikvazigrupa.

DEFINICIJA 3.3. Neka je (Q,f) (n,m)-grupoid i neka je $f:(x_1,\dots,x_n) \to (y_1,\dots,y_m)$. Funkcije $f_i : Q^n \to Q$ definisanje sa $f_i : (x_1,\dots,x_n) \to y_i$, $i = 1,\dots,m$, se nazivaju komponente operacije f i to se označava sa $f = (f_1,\dots,f_m)$.

Koristeći pojam komponente operacije dobija se sledeća definicija multikvazigrupe.

DEFINICIJA 3.4. (n,m)-grupoid (Q,f) se naziva (n,m)-kvazigrupa ako i samo ako za svako $(a_1,\dots,a_n) \in Q^n$ i i svaku injekciju $\varphi : \mathbb{N}_n \to \mathbb{N}_{n+m}$ postoji jednoznačno odredjen $(b_1,\dots,b_{n+m}) \in Q^{n+m}$ takav da je

(i) $a_i = b_{\varphi(i)}$, $i = 1,\dots,n$,

(ii) $f_i(b_1,\dots,b_n) = b_{n+i}$, $i = 1,\dots,m$.

Postoji tesna veza izmedju multivkazigrupa i skupa ortogonalnih n-arnih operacija.

DEFINICIJA 3.5. Skup n-arnih operacija $\{g_1,\dots$ $\dots,g_{n+m}\}$ definisanih nad nepraznim skupom Q se naziva ortogonalan skup n-arnih operacija ako i samo ako za svaki $(a_1,$ $,\dots,a_n)$ Q^n i svaku injekciju φ, $\varphi : \mathbb{N}_n \to \mathbb{N}_{n+m}$ postoji jednoznačno odredjen $(c_1,\dots,c_n) \in Q^n$ takav da je

$$g_{\varphi(i)}(c_1,\dots,c_n) = a_i, \quad i = 1,\dots,n .$$

DEFINICIJA 3.6. Skup n-arnih operacija $\{f_1,\dots,f_m\}$ nad nepraznim skupom Q se naziva skup jako ortogonalnih operacija nad skupom Q ako i samo ako za svako $(a_1,\dots,a_n) \in Q^n$ i svaku injekciju $\varphi : \mathbb{N}_n \to \mathbb{N}_{n+m}$ postoji jednoznačno odredjen $(b_1,\dots,b_{n+m}) \in Q^{n+m}$ takav da je

(i) $a_i = b_{\varphi(i)}$, $i = 1,\dots,n$,

(ii) $f_i(a_1,\dots,a_n) = b_{n+i}$, $i = 1,\dots,m$.

TEOREMA 3.1. [19] Neka je (Q,f) (n,m)-grupoid. (Q,f) je (n,m)-kvazigrupa ako i samo ako nad Q postoji ortogonalan skup n-arnih operacija $\{g_1,\dots,g_{n+m}\}$ takav da je

$f(x_1,\dots,x_n) = (x_{n+1},\dots,x_{n+m})$ ekvivalentno sa

postoji $(t_1,\dots,t_n) \in Q^n$ takvo da je $x_i = g_i(t_1,\dots,t_n)$ za svako $i = 1,\dots,n+m$.

DOKAZ. Neka je (Q,f) (n,m)-kvazigrupa gde je $f = (f_1,\dots,f_m)$. Definišimo skup od $n+m$ n-arnih operacija na sledeći način:

$$(*) \qquad \begin{cases} g_i(x_1,\dots,x_n) = x_i, & i = 1,\dots,n, \\ g_{n+i}(x_1,\dots,x_n) = f_i(x_1,\dots,x_n), & i = 1,\dots,m. \end{cases}$$

Zbog definicije 3.4 sledi da su $g_1,\dots,g_{n+m}$ ortogonalne operacije i obrnuto ako su $g_1,\dots,g_{n+m}$ ortogonalne operacije onda se lako proverava da operacije $f_1,\dots,f_m$ zadovoljavaju definiciju 3.4.

POSLEDICA 3.2. Skup n-arnih operacija $\{f_1,\dots,f_m\}$ nad nepraznim skupom Q je jako ortogonalan skup operacija ako i samo ako je skup $\{g_1,\dots,g_n, f_1,\dots,f_m\}$ skup ortogonalnih operacija pri čemu je g_i definisano sa

$$g_i : Q^n \to Q, \quad g_i : (x_1,\dots,x_n) \to x_i, \quad i = 1,\dots,n.$$

Za $n=2$ su pojmovi skupa jako ortogonalnih operacija i skupa ortogonalnih operacija ekvivalentni. Za $n>2$ skup ortogonalnih operacija ne mora da bude skup jako ortogonalnih operacija. Zaista, ako je $\{f_1,\dots,f_m\}$ skup ortogonalnih binarnarnih operacija, tada je i skup $\{g_1,g_2, f_1,\dots,f_m\}$ ortogonalan jer ako sistem $f_i(c_1,c_2) = a_1$, $f_j(c_1,c_2) = a_2$ ima rešenje za svako $i,j=1,\dots,m$, jasno je da će i sistem $g_1(a_1,c_2) = a_1$, $f_i(c_1,c_2)=a_2$ imati rešenje, jer iz činjenice da je f_i kvazigrupa sledi da jednačina $f_i(a_1,c_2)=a_2$ ima jednoznačno rešenje. Analogno se dokazuje za g_2 $(g_2(c_1,c_2)=c_2)$

Da za $n>2$ ne mora da bude skup ortogonalnih n-arnih operacija istovetno i skup jako ortogonalnih operacija sledi iz sledećeg primera.

Neka je Q skup od 3 elementa i identifikujemo ga sa $\mathbb{Z}_3=\{0,1,-1\}$. Definišimo ternarne operacije f_1,f_2,f_3 sa

$$f_1(x,y,z)=x+y+z,\quad f_2(x,y,z)=x-y+z,\quad f_3(x,y,z)=x+y-z .$$

Tada sistem

$$\begin{aligned} x+y+z &= a_1,\\ x-y+z &= a_2,\\ x+y-z &= a_3, \end{aligned}$$

ima jednoznačno rešenje

$$x=-a_2-a_3,\quad y=a_2-a_1,\quad z=a_3-a_1,$$

dok sistem

$$\begin{aligned} x+y+z &= a_1\ ,\\ x-y+z &= a_2\ ,\\ y &= a_3\ , \end{aligned}$$

nema jednoznačno rešenje za $a_3=0$ i $a_1=a_2=1$.

Primenjujući teoremu 3.1. na skup operacija $\{g_1,\dots,g_{n+m}\}$ definisanih nad komutativnim prstenom R pri čemu je $g_i:R^n\to R$ definisano sa $g_i:(x_1,\dots,x_n)\to a_{1i}x_1+\dots+a_{ni}x_n$ dobijamo sledeću posledicu

<u>POSLEDICA 3.3.</u> [18] Neka je $A=[a_{ij}]$ matrica formata $n\times(n+m)$ sa elementima iz komutativnog prstena R takva

da je svaka kvadratna podmatrica A reda n invertibilna. Neka je $f: R^n \to R^m$ funkcija definisana sa

$$f(x_1,\dots,x_n) = (x_{n+1},\dots,x_{n+m}) \iff (x_1,\dots,x_{n+m}) =$$

$$= (t_1,\dots,t_n)A \text{ za neko } (t_1,\dots,t_n) \in R^n .$$

Tada je (R,f) (n,m)-kvazigrupa.

DOKAZ. Neka je $\underline{C} = (c_1,\dots,c_n) \in R^n$ i $\varphi: \mathbb{N} \to \mathbb{N}_{n+m}$ injekcija. Matrice $B = [b_{ij}]$ formata $n \times n$ definisana sa $b_{ij} = a_{i\varphi(j)}$ je invertibilna po pretpostavci pa sistem linearnih jednačina $(c_1,\dots,c_n) = (t_1,\dots,t_n)B$ ima jednoznačno rešenje $(t_1,\dots,t_n) = (c_1,\dots,c_n)B^{-1}$. Tako dobijamo da postoji $(b_1,\dots,b_{n+m})$ tako da je $b_{\varphi(i)} = c_i$, $i = 1,\dots,n$, i $(b_1,\dots,b_{n+m}) = (t_1,\dots,t_n)A$.

DEFINICIJA 3.7. Multikvazigrupe koje pripadaju klasi multikvazigrupa opisanoj u posledici 3.3. se nazivaju linearne multikvazigrupe.

DEFINICIJA 3.8. Matrica A formata $m \times n$ sa elementima iz komutativnog prstena se nazivaju jako regularna ako i samo ako je svaka kvadratna podmatrica reda k, $k = 1,\dots,\min(n,m)$, invertabilna.

Iz posledice 3.2 dobijamo

POSLEDICA 3.4. Neka je $A = [a_{ij}]$ jako regularna matrica formata $n \times m$ sa elementima iz komutativnog prstena R. Ako je funkcija $f: R^n \to R$ definisana sa

$$f: (x_1,\dots,x_n) \to (y_1,\dots,y_m) \iff (y_1,\dots,y_m) = (x_1,\dots,x_n)A,$$

tada je (R,f) (n,m)-kvazigrupa.

POSLEDICA 3.5. Neka je $A = [a_{ij}]$ jako regularna matrica formata $n \times m$ sa elementima iz komutativnog prstena R. Tada:

(i) Transponovana matrica A' matrica A definiše (m,n)-kvazigrupu.

(ii) Svaka podmatrica B formata $p \times q$ matrice A definiše (p,q)-kvazigrupu.

Ako se umesto komutativnog prstena R uzme polje F dobija se klasa multikvazigrupa, koja je naročito interesantna kada je polje F konačno.

U sledećim primerima su date linearne multikvazigrupe konstruisane nad malim poljima. Primeri su iz [18].

PRIMER 3.1.

$$F = GF(3) = \{0,1,-1\},\ n = m = 2,\ A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$f(x,y) = (x+y,\ x-y)\ .$$

PRIMER 3.2

$$F = GF(5) = \{0,1,2,-1,-2\},\ n = 3,\ m = 2,\ A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 1 & -1 \end{bmatrix},$$

$$f(x,y,z) = (x+y+z,\ x+2y-z)\ .$$

PRIMER 3.3.

$$F = GF(5),\ n = 2,\ m = 3,\quad A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & -1 \end{bmatrix},$$

$$f(x,y) = (x+y, x+2y, x-y).$$

PRIMER 3.4.

$$F = GF(5),\quad n = m = 3,\quad A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix},$$

$$f(x,y,z) = (2x+y+z, x+2y+z, x+y+2z)\ .$$

Sledeća teorema iz [18] povezuje arnost multikvazigrupe i kardinalnost skupa Q.

TEOREMA 3.6. Neka je F konačno polje sa q elemenata i neka su m i n prirodni brojevi takvi da je

$$\binom{n+m}{n} < q\ .$$

Tada postoji jako regularna matrica A formata $n \times m$ sa elementima iz F, tj. postoji (n,m)-kvazigrupa nad skupom od q elemenata.

Ako se celobrojna matrica A posmatra kao matrica sa elementima iz $\mathbb{Z}_q$ dobija se sledeće tvrdjenje.

TVRDJENJE 3.7. [18] Ako postoji celobrojna matrica A formata $n \times m$ takva da je svaki minor matrice A uzajamno prost sa prirodnim brojem q, tada postoji (n,m)-kvazigrupa reda q.

Neposredno se dobijaju sledeće posledice.

POSLEDICA 3.8. Neka je $q = 2k+1$, $k = 1,2,\ldots$ tada je matrica $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ jako regularna pa postoje (2,2)-kvazigrupe svakog neparnog reda.

POSLEDICA 3.9. Matrica $A = \begin{bmatrix} -2 & 1 & -1 \\ -1 & 2 & -1 \\ 1 & -1 & 2 \end{bmatrix}$ je jako regularna za svako q uzajamno prosto sa 6 pa postoje (2,3)- (3,2)- i (3,3)-kvazigrupe reda q za svaki prirodan broj q uzajamno prost sa 6.

Slično kao i kod n-arnih grupoida i kod multigrupoida se uvodi pojam izotopije.

DEFINICIJA 3.9. (n,m)-grupoidi (Q,f) i (Q,g) se nazivaju izotopnim ako i samo ako postoji niz $(\varphi_1,\ldots,\varphi_{n+m})$ permutacija skupa Q takav da je

$$f(x_1,\ldots,x_n) = (x_{n+1},\ldots,x_{n+m}) \text{ ako i samo ako je}$$

$$g(\varphi_1(x_1),\ldots,\varphi_n(x_n)) = (\varphi_{n+1}(x_{n+1}),\ldots,\varphi_{n+m}(x_{n+m})) .$$

Multigrupoid (Q,g) se naziva izotop multigrupoida (Q,f), a niz permutacija $T = (\varphi_1,\ldots,\varphi_{n+m})$ se naziva izotopija multigrupoida (Q,f) u multigrupoid (Q,g) i to se obeležava sa $g = f^T$.

DEFINICIJA 3.10. Ako postoji izotopija $T = (\varphi_1,\ldots$ $\ldots,\varphi_{n+m})$ multigrupoid (Q,f) u multigrupoid (Q,g) takav da je $\varphi_1 = \varphi_2 = \ldots = \varphi_n = \varphi_{n+1}^{-1} = \ldots = \varphi_{n+m}^{-1}$ tada je multigrupoid (Q,g) izomorfan multigrupoidu (Q,f).

Iz definicije izotopije neposredno sledi.

TVRDJENJE 3.10. Neka su multigrupoidi (Q,f) i (Q,g) izotopni. (Q,f) je multikvazigrupa ako i samo ako je (Q,g) multikvazigrupa.

TVRDJENJE 3.11. Izotopija je relacija ekvivalencije u skupu svih (n,m)-kvazigrupa definisanih nad istim skupom Q.

TVRDJENJE 3.12. Skup svih izotopija multikvazigrupe (Q,f) je grupa u odnosu na kompoziciju izotopija koja je definisana na sledeći način: $S = (\varphi_1,\dots,\varphi_{n+m})$, $T = (\psi_1,\dots,\psi_{n+m})$. $S \circ T = (\varphi_1\psi_1,\dots,\varphi_{n+m}\psi_{n+m})$.

DEFINICIJA 3.11. Neka su (Q,f) i (Q,g) multikvazigrupe takve da je $(Q,g) = (Q,f^T)$ gde je $T = (\varphi_1,\dots,\varphi_{n+m})$ pri čemu je $\varphi_{n+1} = \dots = \varphi_{n+m} = id$. Tada se (Q,g) naziva glavni izotop multikvazigrupe (Q,f), a izotopija glavna izotopija.

TVRDJENJE 3.13. Neka je (Q,f) (n,m)-kvazigrupa i $(Q,g) = (Q,f^T)$ gde je $T = (\varphi_1,\dots,\varphi_{n+m})$. (Q,g) je izomorfan glavnom izotopu multikvazigrupe (Q,f) ako i samo ako je $\varphi_{n+1} = \dots = \varphi_{n+m}$.

Jedno od primarnih pitanja koje se postavlja prilikom izučavanja multikvazigrupa je da li postoje multikvazigrupe koje nisu linearne. Na to pitanje daćemo odgovor konstruišući klasu konačnih multikvazigrupa koje nisu linearne. U tom cilju ćemo najpre dokazati dva stava iz teorije brojeva.

Nad konačnim poljem F je svaka funkcija $f:F\to F$ jednoznačno odredjena svojim interpolacionim polinomom ako je stepen interpolacionog polinoma $<\mathrm{Card}(F)$. Zbog toga ćemo permutaciju konačnog polja F zvati linearnom ili nelinearnom već prema tome da li je interpolacioni polinom najnižeg stepena koji je odredjuje linearan ili nelinearan.

TVRDJENJE 3.14. Za svako konačno polje $F = GF(p^k)$ $F \neq GF(2)$ i $F \neq GF(3)$, postoji $p^k(p^k-1)((p^k-2)!-1)$ permutacija skupa F koje nisu linearne funkcije.

DOKAZ. Pošto postoji $p^k(p^k-1)$ linearnih funkcija $f(x) = ax+b$, $(a \neq 0)$ i kako postoji $(p^k)!$ permutacija polja F, to ako je $p^k! > p^k(p^k-1)$ tada postoji $p^k(p^k-1)((p^k-2)!-1)$ nelinearna permutacija nad skupom F. Za $k = 1$, $p^k! > p^k(p^k-1)$ za $p \geqslant 5$, a ako je $k > 1$ tada nejednakost važi za svaki prost broj.

Lako se proverava da su sve permutacije nad $GF(2)$ i $GF(3)$ linearne funkcije.

TVRDJENJE 3.15. Neka je F polje Galoa $F \neq GF(2)$, $F \neq GF(3)$.

(i) Ako je $F = GF(p)$ tada je $\varphi(x) = x^{p-2}$ nelinearna permutacija.

(ii) Ako je $F = GF(p^k)$, $k \geqslant 2$ tada je $\varphi(x) = x^p$ nelinearna permutacija.

DOKAZ. Neka je $F = GF(p^k)$.

(i) $k = 1$. Neka je $\varphi(x) = x^{p-2}$. Zbog uslova teoreme je $p-2 \geqslant 3$, a zbog male Fermatove teoreme je $x^{p-1} = 1$ za $x \neq 0$ pa je $\varphi(x) = x^{-1}$ za $x \neq 0$, a $\varphi(0) = 0$ tj. φ je permutacija. Pretpostavimo da je φ linearna tj. da za neko $a,b \in F$, $a \neq 0$ važi $x^{p-2} - ax - b = 0$ za svako $x \in GF(p)$. Tada bi polinom stepena $p-2$ imao u polju $GF(p)$ p rešenja, a to je nemoguće.

(ii) $k > 1$. Neka je $\varphi(x) = x^p$. Preslikavanje φ je automorfizam $GF(p^k)$ pa je bijekcija. Neka je opet $x^p-ax-b = 0$ za svako $x \in GF(p^k)$. Tada bi jednačina stepena p imala u polju p^k $(k > 1)$ rešenja što je opet nemoguće.

TEOREMA 3.16. Za svaku linearnu (n,m)-kvazigrupu (F,f) definisanu nad poljem Galoa $F = GF(p^k)$, $F \neq GF(2)$ i $F \neq GF(3)$ postoji bar $(p^k!)^m - (p^k(p^k-1))^m$ različitih nelinearnih (n,m)-kvazigrupa koje su izotopne sa (F,f).

<u>DOKAZ.</u> Neka je $F = GF(p^k)$ polje Galoa koje zadovoljava uslove teoreme i neka je (F,f) linearna multikvazigrupa takva da je

$$f(x_1,\dots,x_n) = \left(\sum_{k=1}^{n} \ell_{1k}x_k,\dots,\sum_{k=1}^{n} \ell_{mk}x_k\right),$$

pri čemu je matrica $L = [\ell_{ij}]$ jako regularna matrica formata $n \times m$.

Posmatrajmo izotop (F,g) multikvazigrupe (F,f) dobijen izotopijom $T = (\varphi_1,\dots,\varphi_{n+m})$ gde su $\varphi_1 = \dots = \varphi_n = id_F$, a φ_{n+i}, $i = 1,\dots,m$, neke permutacije skupa F. Na osnovu tvrdjenja 3.10. je (F,g) multikvazigrupa i dovoljno je dokazati da je bar jedna od funkcija φ_{n+i}, $i = 1,\dots,m$, nelinearna.

Svako preslikavanje polja Galoa F je jednoznačno odredjeno svojim interpolacionim polinomom, jer je stepen interpolacionog polinoma koji prolazi kroz p^k tačka najviše p^k-1, a različiti polinomi stepena najviše p^k-1 uvek definišu različite funkcije, jer $x^s \neq x$ za svako $s < p^k$, Kako su $\sum_{k=1}^{n} \ell_{ik}x_k$, $i = 1,\dots,m$, linearne funkcije to je stepen polinoma $\varphi_j(x)$ isti kao i stepen $\varphi_j\left(\sum_{k=1}^{n} \ell_{jk}x_k\right)$, $j = 1,\dots,m$. To znači da ako je funkcija φ_j nelinearna, nelinearna je i $\varphi_j\left(\sum_{k=1}^{n} \ell_{jk}x_k\right)$ pa

$$g(x_1,\dots,x_n) = \left(\varphi_{n+1}\left(\sum_{k=1}^{n} \ell_{1k}x_k\right),\dots,\varphi_{n+m}\left(\sum_{k=1}^{n} \ell_{mk}x_k\right)\right),$$

ne može biti linearna (n,m)-kvazigrupa.

Neka su φ_j i ψ_j različite permutacije nad F, tada je

$$\varphi_j\left(\sum_{k=1}^{n} \ell_{jk}x_k\right) \neq \psi_j\left(\sum_{k=1}^{n} \ell_{jk}x_k\right).$$

Neka su $T = (\varphi_1,\dots,\varphi_{n+m})$ gde je $\varphi_1 = \dots = \varphi_n = id_F$ i $S = (\psi_1,$ $\dots,\psi_{n+m})$ gde je $\psi_1 = \dots = \psi_n = id_F$ dve različite izotopije

(n,m)-kvazigrupe (F,f) pa su i (n,m)-kvazigrupe (F,f^T) i (F,f^S) različite. Zbog tvrdjenja 3.14. sledi da postoji $(p^k!)^m-(p^k(p^k-1))^m$ različitih izotopija oblika $(id_F,\dots,id_F,\varphi_{n+1},\dots,\varphi_{n+m})$ kod kojih je bar jedno φ_{n+j} nelinearno. Tako dobijamo da za linearnu multikvazigrupu (F,f) postoji bar $(p^k!)^m-(p^k(p^k-1))^m$ nelinearnih multikvazigrupa koje su joj izotopne.

Koristeći prethodna dva stava se mogu lako konstruisati primeri nelinearnih multikvazigrupa.

PRIMERI.

1. Posmatrajmo sledeću linearnu $(2,4)$-kvazigrupu $(GF(5),f)$ gde je f definisano sa

$$f:(x,y)\to(2x+2y,x+4y,x+3y,3y+y).$$

Primenimo izotopiju $T=(\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6)$ gde je

$$\varphi_1=\varphi_2=id,\ \varphi_3(x)=x^3,\ \varphi_4(x)=2x^3+1,\ \varphi_5(x)=3x,$$
$$\varphi_6(x)=4x+2.$$

Dobijamo nelinearnu multikvazigrupu $(GF(5),g)$ gde je g definisano sa

$$g:(x,y)\to(3x^3+4x^2y+4xy^2+3x^3,2x^3+4x^2y+xy^2+3y^3+1,$$
$$2x+3y+2).$$

2. Neka je $F=GF(4)=GF(2)[t]/(t^2+t+1)$. Tada je $GF(4),f)$ $(2,2)$-kvazigrupa ako je f definisano sa

$$f:(x,y)\to(x+y,\ x+ty).$$

Primenimo izotopiju $T=(\varphi_1,\varphi_2,\varphi_3,\varphi_4)$ definisanu sa $\varphi_1=\varphi_2=id$, $\varphi_3(x)=x^2$, $\varphi_4(x)=x^2+t$. Dobijamo nelinearnu multikvazigrupu $(GF(4),g)$ pri čemu je g definisano sa

$$g:(x,y)\to(x^2+y^2,\ x^2+(t+1)y^2+t).$$

Multikvazigrupe dozvoljavaju i geometrijsku interpolaciju pomoću koje se dobija vrlo interesantan rezultat o broju ortogonalnih n-arnih operacija nad konačnim skupovima.

DEFINICIJA 3.12. Neka su P i B neprazni skupovi neka je B disjunktna unija m+n nepraznih skupova $B = B_1 \cup \ldots$ $\ldots \cup B_{n+m}$, $n \geq 2$, $m \geq 1$, a I podskup od $P \times B$. Struktura $(P; B_1, \ldots, B_{n+m}; I)$ se naziva n-dimenziona (n+m)-mreža ili (n,n+m)-mreža ako i samo ako važi:

(i) Ako je $p \in P$ tada postoji tačno jedan niz $B_1, \ldots, B_{n+m} \in B$ takav da $(p, B_i) \in I$, $B_i \in B_i$, $i = 1, \ldots, n+m$.

(ii) Ako je $\varphi : \mathbb{N}_n \to \mathbb{N}_{n+m}$ injekcija i $B_i \in B_{\varphi(i)}$ tada postoji jedinstveno $p \in P$ takvo da je $(p, B_i) \in I$ za svako $i = 1, \ldots, n$.

Elementi skupa P se još nazivaju tačke, dok se elementi skupa B nazivaju blokovi ili linije.

TEOREMA 3.17. [18] Neka je (Q,f) (n,m)-kvazigrupa pri čemu skup Q ima bar dva elementa. Tada multikvazigrupa (Q,f) definiše (n,n+m)-mrežu.

DOKAZ. Neka je (Q,f) multikvazigrupa koja zadovoljava uslove teoreme. Definišimo skup tačaka sa

$$P = \{(x_1, \ldots, x_{n+m}) \in Q^{n+m} \mid f(x_1, \ldots, x_n) = $$
$$= (x_{n+1}, \ldots, x_{n+m})\} .$$

Ako $q \in Q$, a $i \in \mathbb{N}_{n+m}$ tada definišemo blok sa

$$B_i^q = \{(x_1, \ldots, x_{n+m}) \in P \mid x_i = q\} ,$$

dok je skup blokova

$$B = \{B_i^q \mid q \in Q,\ i \in \mathbb{N}_{n+m}\} .$$

Particiju skupa B, $B = B_1 \dot\cup \ldots \dot\cup B_{n+m}$ definišemo sa

$$B_i = \{B_i^q \mid q \in Q\}, \quad i = 1, \ldots, n+m .$$

Relaciju incidencije I definišemo sa

$$I = \{(p,B_i^q) \in \mathcal{P} \times \mathcal{B} \mid p \in B_i^q,\ i \in \mathbb{N}_{n+m},\ q \in Q\}\ .$$

Iz definicije (n,m)-kvazigrupe neposredno sledi da je definisana struktura n-dimenziona (n+m)-mreža.

TEOREMA 3.18. [18] Svaka (n,n+m)-mreža definiše (n,m)-kvazigrupu.

DOKAZ. Neka je $(\mathcal{P}; \mathcal{B}_1,\ldots,\mathcal{B}_{n+m}; I)$ (n,n+m)-mreža. Najpre ćemo dokazati da su svi skupovi $\mathcal{B}_1,\ldots,\mathcal{B}_{n+m}$ iste kardinalnosti.

Primetimo da iz (i) definicije 3.12. sledi da ako je $\mathcal{P} \neq \emptyset$ tada je $\mathcal{B}_i \neq \emptyset$, za $i = 1,\ldots,n+m$.

Neka su $r,s \in \mathbb{N}_{n+m}$ $r \neq s$ i neka je $\mathbb{N}^*_{r,s} = \{i_2,\ldots$ $\ldots,i_n\} \subseteq \mathbb{N}_{n+m}$ podskup koji sadrži n-1 element i ne sadrži ni r ni s. Za svako $B \in \mathcal{B}_r$ zbog uslova (ii) definicije 3.12. sledi da postoji tačno jedna tačka p takva da $p \in B$ i $p \in B_k$ za svako $k \in \mathbb{N}^*_{r,s}$, a tada iz uslova (i) definicije (n,n+m)-mreže sledi da postoji jednoznačno odredjen $B' \in \mathcal{B}_s$ takav da je $(p,B') \in I$. Na taj način se definiše preslikavanje $\psi_{sr}: B \to B'$ iz $\mathcal{B}_r$ u $\mathcal{B}_s$. Analogno se definiše preslikavanje $\psi_{rs}: \mathcal{B}_s \to \mathcal{B}_r$. Neposredno sledi da je

$$\psi_{rs}\psi_{sr} = id_{\mathcal{B}_r} \quad i \quad \psi_{sr}\psi_{rs} = id_{\mathcal{B}_s}$$

tj. ψ_{rs} je bijekcija.

Pošto svi $\mathcal{B}_i$, $i = 1,\ldots,n+m$, imaju isti broj elemenata možemo izabrati skup Q i bijekcije $\varphi_i: Q \to \mathcal{B}_i$, $i = 1,\ldots,n+m$. Definišemo funkciju $f: Q^n \to Q^m$ sa

$$f:(x_1,\ldots,x_n) \to (x_{n+1},\ldots,x_{n+m}) \text{ ako i samo ako}$$

$$(\exists p \in \mathcal{P})(\forall i \in \mathbb{N}_{n+m})((p,\varphi_i(x_i)) \in I)\ .$$

Neposredno iz definicije 3.9. sledi da je (Q,f) (n,m)-kvazigrupa.

POSLEDICA 3.19. Neka je data (n,n+m)-mreža (P; $B_1,\dots,B_{n+m}$,I). Ako se na nju primeni postupak iz teoreme 3.19, a na dobijenu multikvazigrupu postupak iz teoreme 3.18 dobija se (n,n+m)-mreža izomorfna sa polaznom.

TVRDJENJE 3.20. Neka (n,n+m)-mreža indukuje dve multikvazigrupe (Q_1,f_1) i (Q_2,f_2). Tada su (Q_1,f_1) i (Q_2,f_2) izotopne multikvazigrupe.

TVRDJENJE 3.21. [18] Neka su n,m,q prirodni brojevi $\geqslant 2$. Ako postoji (n,m)-kvazigrupa (Q,f) reda q tada je

$$m \leqslant q-1$$

POSLEDICA 3.22. Ako su m,n prirodni brojevi $\geqslant 2$ tada ne postoji (n,m)-kvazigrupa reda 2.

Iz teoreme 3.21 sledi važno tvrdjenje o broju ortogonalnih operacija nad skupom od q elemenata.

TEOREMA 3.23. [18] Neka su n,q prirodni brojevi $\geqslant 2$ i $(f_1,\dots,f_k)$ sistem ortogonalnih n-arnih operacija definisanih nad skupom Q od q elemenata. Tada je

$$k \leqslant n+q-1.$$

DEFINICIJA 3.13. Sa $\omega_n(q)$ označićemo maksimalan broj ortogonalnih n-arnih operacija nad skupom sa q elemenata, a sa $\pi_n(q)$ maksimalan broj ortogonalnih n-arnih kvazigrupa nad skupom sa q elemenata.

TEOREMA 3.24. Neka su n,q prirodni brojevi $\geqslant 2$. Tada je

$$\pi_n(q) \leqslant \omega_n(q) \leqslant n+q-1 .$$

Ova teorema u nizu slučajeva poboljšava rezultat iz [20] str. 186 koji daje da je

$$\pi_n(q) \leqslant (n-1)(q-1) .$$

Teorija n-kvazigrupa koje zadovoljavaju pojedine identitete je veoma razvijena i dobijen je niz zajedničkih rezultata za klase kvazigrupa definisanih pomoću identiteta. Sada ćemo razmotriti pitanje kako se pojedini identiteti mogu uopštiti na multikvazigrupe i dokazati da prirodna uopštenja zakona asocijativnosti, komutativnosti i neutralnog elementa (ili sloga) ne daju rezultate u teoriji multikvazigrupa.

DEFINICIJA 3.14. Neka je (Q,f) (n,m)-grupoid takav da je $n > m$. Multigrupoid (Q,f) se naziva (i,j)-asocijativan ako i samo ako važi sledeći identitet:

$$f(x_1^{i-1}, f(x_i^{i+n-1}), x_{i+n}^{2n-m}) = f(x_1^{j-1}, f(x_j^{j+n-1}), x_{j+n}^{2n-m}).$$

Sa

$$f(_1^{i-1}, f(x_i^{i+n-1}), x_{i+n}^{2n-m}) \text{ je označen}$$

$$f(x_1^{i-1}, y_1^m, x_{i+n}^{2n-m}) \text{ gde je } f(x_i^{i+n-1}) = (y_1, \ldots y_m).$$

DEFINICIJA 3.15. (n,m)-grupoid (Q,f) $(n > m)$ koji je (i,j)-asocijativan za svako $i,j = 1,\ldots,n-m$ se naziva (n,m)-polugrupa. (n,m)-polugrupe su ispitivane u radu [16]

TEOREMA 3.25. Neka su n,m prirodni brojevi takvi da je $n > m \geqslant 2$ i neka su i,j medjusobno različiti prirodni beojevi takvi da je $1 \leqslant i,j \leqslant n-m$. Ako je (Q,f) (i,j)-asocijativna (n,m)-kvazigrupa tada skup Q ima samo jedan element.

DOKAZ. Neka je (Q,f) (i,j)-asocijativna (n,m)-kvazigrupa i neka je $i < j$. Kako je $n > m$ tada je $j < i+n-1$. Uvedimo sledeće oznake $k = n-m$, $\ell = j-i$.

Najpre posmatrajmo jednakost

$$\text{(i)} \quad f(x_i, x_{i+1}, \ldots, x_{i+n-1}) = (y_1, \ldots, y_m).$$

Ako u (i) stavimo $x_p = a_p$, $p = i,\ldots,k+i-1$, $y_q = a_{i+q-1}$, $q = 1,\ldots,m$, gde su a_p, $p=1,\ldots,\max(k+i-1, i+m-1)$ proizvoljni fiksni elementi iz Q dobijamo

$$f(a_i^{k+i-1}, x_{k+i}^{i+n-1}) = (a_i^{i+m-1}) .$$

Kako je (Q,f) (n,m)-kvazigrupa postoji jednoznačno odredjena m-torka $(b_{k+1}^{i+n-1}) \in Q^m$ takva da je

$$\text{(ii)} \qquad f(a_i^{k+i-1}, b_{k+i}^{i+n-1}) = (a_i^{i+m-1}) .$$

Ako su u identitetu (i,j)-asocijativnosti stavimo $x_p = a_p$, $p=i,\ldots,k+i-1$, $x_r = b_r$, $r=k+i,\ldots,i+n-1$ dobija se

$$\text{(iii)} \qquad f(x_1^{i-1}, f(a_i^{k+i-1}, b_{k+i}^{i+n-1}), x_{i+n}^{2n-m}) =$$

$$= f(x_1^{i-1}, a_i^{j-1}, f(c_j,\ldots,b_{i+n-1}, x_{i+n}^{j+n-1}), x_{j+n}^{2n-m})$$

gde je $c_t = \begin{cases} a_t & \text{ako je } t \leq k+i-1 \\ b_t & \text{ako je } t > k+i-1 \end{cases}$. Iz (ii) i (iii) sledi

$$\text{(iv)} \qquad f(x_1^{i-1}, a_i^{i+m-1}, x_{i+n}^{2n-m}) =$$

$$= f(x_1^{i-1}, a_i^{j-1}, f(c_j,\ldots,b_{i+n-1}, x_{i+n}^{j+n-1}), x_{j+n}^{2n-m}) .$$

Ako sad u $f(x_j^{j+n-1}) = (z_1^m)$ stavimo $x_j = c_j,\ldots,x_{j+n-1} = b_{i+n-1}$, $z_1 = a$, $z_2 = a_{j+1},\ldots,z_\ell = a_{j+\ell-1}$ pri čemu su a i a_s, $s = \max(k+i-1,\ i+m-1),\ldots,j+\ell-1$, proizvoljni elementi iz Q tada sledi da postoji jednoznačno odredjena m-torka

$$(b_{i+n},\ldots,b_{j+n-1}, d_1,\ldots,d_{m-\ell}) \in Q^m \text{ takva da je}$$

$$f(c_j,\ldots,b_{j+n-1}) = (a, a_{j+1},\ldots,a_{j+\ell-1}, d_1,\ldots,d_{m-\ell}).$$

Ako u (iv) stavimo da je $x_{i+n} = b_{i+n},\ldots,x_{j+n-1} = b_{j+n-1}$, dobija se

$$\text{(v)} \qquad f(x_1^{i-1}, a_i^{i+m-1}, b_{i+n}^{j+n-1}, x_{j+n}^{2n-m}) =$$

$$= f(x_1^{i-1}, a_i^{j-1}, a, a_{j+1}^{j+\ell-1}, d_1^{m-\ell}, x_{j+n}^{2n-m}) .$$

U prethodnom identitetu (v) su bar n-m odgovarajućih komponenata dveju n-torki jednaki. To su $x_1,\dots,x_{i-1}$, $a_i,\dots,a_{k+i-1}$, $x_{j+n},\dots,x_{2n-m}$, a kako je (Q,f) multikvazigrupa to i sve ostale odgovarajuće komponente moraju da budu medjusobno jednake pa je $a = a_j$. No a i a_j su bili proizvoljni elementi iz Q , tj. svi elementi iz Q su medjusobno jednaki .

POSLEDICA 3.26. Ako je (Q,f) (n,m)-kvazigrupa, gde je $n > m \geq 2$, koja je i (n,m)-polugrupa tada je Q jednoelementni skup.

DEFINICIJA 3.16. Neka je $\sigma \in S_n$. (n,m)-grupoid (Q,f) se naziva σ-komutativan ako i samo ako u (Q,f) važi identitet

$$f(x_1,\dots,x_n) = f(x_{\sigma(1)},\dots,x_{\sigma(n)}) .$$

DEFINICIJA 3.17. (n,m)-grupoid (Q,f) se naziva komutativan ako i samo ako je σ-komutativan za svako $\sigma \in S_n$.

TEOREMA 3.27. Neka je $\sigma \in S_n$ takva permutacija da postoje i,j, $i \neq j$, $1 \leq i,j \leq n$, takav da je $\sigma(i) = j$ i $\sigma(j) = i$. Ako je (Q,f) σ-komutativno (n,m)-kvazigrupi pri čemu je $m \geq 2$ tada je Q jednoelementni skup.

DOKAZ. Neka je (Q,f) multikvazigrupa koja zadovoljava uslove teoreme, i neka je $i < j$.

Ako se u identitet

$$f(x_1^n) = f(x_{\sigma(1)}^{\sigma(i-1)}, x_j, x_{\sigma(i+1)}^{\sigma(j-1)}, x_i, x_{\sigma(j+1)}^{\sigma(n)})$$

stavi $x_k = a$, $k=1,\dots,i-1,i+1,\dots,n$, gde je a proizvoljan fiksan element iz Q dobija se

$$f(a,\dots,a,\overset{i}{x_i},a,\dots,a) = f(a,\dots,a,\overset{j}{x_i},a,\dots,a).$$

U ovom identitetu su bar n-m odgovarajućih komponenata jednake pa kako je (Q,f) multikvazigrupa sledi da je $x_i = a$, tj. da je Q jednoelementni skup.

<u>POSLEDICA 3.28.</u> Ako je (Q,f) komutativna (n,m)-kvazigrupa i $m \geqslant 2$ tada je Q jednoelementni skup.

<u>DEFINICIJA 3.18.</u> Neka je (Q,f) (n,m)-grupoid i neka je $n > m$. $(n-m)$-torka (e_1^{n-m}) se naziva i-ti neutralni slog za (Q,f) ako i samo ako za svaku m-torku $(x_1,\dots,x_m) \in Q^m$ važi

$$f(e_1,\dots,e_{i-1},x_1,\dots,x_m,e_i,\dots,e_{n-m}) = (x_1,\dots,x_m).$$

$(e_1,\dots,e_{n-m})$ se naziva neutralni slog ako i samo ako je i-ti neutrani slog za svako $i=1,\dots,n-m+1$.

<u>DEFINICIJA 3.19.</u> Element $e \in Q$ se naziva i-ti neutralni element (n,m)-grupoida (Q,f) ako i samo ako je $(e,\dots,e) \in Q^{n-m}$ i-ti neutralni slog. Element $e \in Q$ je neutralni element ako i samo ako je i-ti neutralni element za svako $i=1,\dots,n-m+1$.

<u>TEOREMA 3.29.</u> Neka je (Q,f) (n,m)-kvazigrupa i $n > m$. Ako je $(e_1,\dots,e_{n-m})$ i-neutralan i $(i+1)$-neutralan slog tada je Q jednoelementni skup.

<u>DOKAZ.</u> Za svaku n-torku $(x_1,\dots,x_m)$ važi

$$f(e_1,\dots,e_{i-1},x_1,\dots,x_m,e_i,\dots,e_{n-m}) = (x_1,\dots,x_m).$$

Stavimo $x_1 = e_i$. Tada se dobija

$$f(e_1,\dots,e_{i-1},e_i,x_2,\dots,x_m,e_i,e_{i+1},\dots,e_{n-m}) =$$
$$= (e_i,x_2,\dots,x_m) = (x_2,\dots,x_m,e_i)$$

jer je $(e_1,\dots,e_{n-m})$ takodje i $(i+1)$-neutralni slog pa je $x_2 = e_i$ tj. Q je jednoelementni skup, jer x_2 može da bude proizvoljan element iz Q.

Osim multikvazigrupa koje zadovoljavaju uopšteni asocijativni i komutativni proučavane su i multikvazigrupe koje su uopštenje medialnih n-kvazigrupa ([44]). Naime, n-kvazigrupa (Q,f) se naziva medialna ako i samo ako u (Q,f) važi sledeći identitet.

$$f(\{f(x_{1i}^{n})\}_{i=1}^{n}) = f(\{f(x_{i1}^{n})\}_{i=1}^{n}) .$$

Strukturu medialnih n-kvazigrupa prikazuje sledeća teorema [2] str. 47.

TEOREMA (Tojoda) Neka je (Q,f) medialna n-kvazigrupa. Tada postoji binarna komutativna grupa $(Q,+)$ takva da je

$$f(x_1^n) = \sum_{i=1}^{n} \varphi_i(x_i) + c ,$$

gde su φ_i, $i=1,\dots,n$, automorfizmi grupe $(Q,+)$ takvi da je $\varphi_i\varphi_j = \varphi_j\varphi_i$, $i,j=1,\dots,n$, a c neki fiksan element skupa Q.

DEFINICIJA 3.20. Neka je (Q,f) (n,m)-kvazigrupa pri čemu je $f=(f_1,\dots,f_m)$. Multikvazigrupa (Q,f) se naziva medialna (n,m)-kvazigrupa ako i samo ako važi

$$f_i(f_j(x_{11},\dots,x_{1n}),\dots,f_j(x_{n1},\dots,x_{nn})) =$$

$$= f_i(f_j(x_{11},\dots,x_{n1}),\dots,f_j(x_{1n},\dots,x_{nn}))$$

za svako $x=[x_{k\ell}]$, $k,\ell=1,\dots,n$ i svako $i,j=1,\dots,m$.

Iz definicije neposredno sledi

TVRDJENJE 3.31. [44] $(1,m)$-kvazigrupa (Q,f) gde je $f=(f_1,\dots,f_m)$ je medijalna ako i samo ako su $f_1,\dots,f_m$ bijekcije skupa Q za koje važi $f_if_j = f_jf_i$ za svako $i,j=1,\dots$ $\dots,m$.

TVRDJENJE 3.32. [44] Neka su (Q,f) i (Q,g) dve medialne n-kvazigrupe za koje važi

$$f(g(x_{11},\dots,x_{1n}),\dots,g(x_{n1},\dots,x_{nn})) =$$

$$= g(f(x_{11},\dots,x_{n1}),\dots,f(x_{1n},\dots,x_{nn})) .$$

Tada postoji komutativna grupa $(Q,+)$ takva da je

(i) $\quad f(x_1,\ldots,x_n) = \alpha_1(x_1) + \ldots + \alpha_n(x_n) + v$,

(ii) $\quad g(x_1,\ldots,x_n) = \beta_1(x_1) + \ldots + \beta_n(x_n) + w$

gde su $\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n$ fiksni automorfizmi grupe $(Q,+)$ koji komutiraju po parovima, a v i w su dva fiksna elementa iz Q.

Sledeća teorema neposredno sledi iz Tojodine teoreme i prethodnog stava.

TEOREMA 3.33. [44] Neka je (Q,f) medijalna (n,m)-kvazigrupa, $n\geq 2$. Tada postoji abelova grupa $(Q,+)$ takva da je

$$f_i(x_1,\ldots,x_n) = \alpha_{i1}(x_1) + \ldots + \alpha_{in}(x_n) + w_i ,$$

za svako $x_1,\ldots,x_n \in Q$, $i=1,\ldots,m$ gde su α_{ij} $(i=1,\ldots,m,$ $j=1,\ldots,n)$ fiksni automorfizmi grupe $(Q,+)$ koji komutiraju po parovima, a w_i, $i=1,\ldots,m$ su fiksni elementi iz Q.

Ako se sa funkcijske oznake $y = f(x)$ predje na ekvivalentnu relacijsku oznaku $(x,f(x))$ dobija se, u slučaju (n,m)-kvazigrupa, sledeća ekvivalentna definicija [19].

DEFINICIJA 3.21. Neka je $\rho \subseteq Q^{n+m}$ relacija arnosti $n+m$ nad nepraznim skupom Q. Relacija ρ se naziva (n,m)-kvazigrupna relacija ako i samo ako za svako $(a_1,\ldots,a_n) \in Q^n$ i svaku injekciju $\varphi:\mathbb{N}_n \to \mathbb{N}_{n+m}$ postoji jednoznačno odredjen $(b_1,\ldots,b_{n+m}) \in \rho$ takav da je $a_i = b_{\varphi(i)}$, $i=1,\ldots,n$.

Iz definicije 3.4 i 3.21 se neposredno dobija:

TVRDJENJE 3.33. (n,m)-grupoid (Q,f) je (n,m)-kvazigrupa ako i samo ako je relacija ρ, arnosti $n+m$, definisana sa

$$(x_1,\ldots,x_{n+m}) \in \rho \text{ ako i samo ako } f(x_1,\ldots,x_n) = (x_{n+1},\ldots,x_{n+m})$$

(n,m)-kvazigrupa relacija.

Ako je ρ definisano kao u prethodnom tvrdjenju tada ćemo (Q,f) obeležavati sa (Q,ρ).

Relacijska definicija multikvazigrupa je vrlo pogodna, jer se pomoću nje mogu zgodno definisati parcijalne multikvazigrupe.

DEFINICIJA 3.22. Neka je $\rho \subseteq Q^{n+m}$ relacija arnosti $n+m$ nad nepraznim skupom Q, a $\varphi: \mathbb{N}_n \to \mathbb{N}_{n+m}$ injekcija. Struktura (Q,ρ) se naziva parcijalna (n,m)-kvazigrupa ako i samo ako iz

$$(x_1,\dots,x_{n+m}) \in \rho,\ (y_1,\dots,y_{n+m}) \in \rho \text{ i } x_{\varphi(i)} = y_{\varphi(i)},$$

$$i=1,\dots,n, \quad \text{sledi} \quad x_j = y_j,\ j=1,\dots,n+m.$$

Parcijalna (n,m)-kvazigrupa (Q,ρ) se naziva parcijalna multikvazigrupa (n,m)-kvazigrupe (R,σ) ako i samo ako je $Q \subseteq R$ i $\rho \subseteq \sigma$. (n,m)-kvazigrupa (R,σ) se naziva proširenje (n,m)-kvazigrupe (Q,ρ).

Parcijalna multikvazigrupa je prirodno uopštenje multikvazigrupe u sledećem smislu. Ne zahteva da se za svaki izbor od n elemenata postoji m jednoznačno odredjenih elemenata tako da $(x_1,\dots,x_{n+m}) \in \rho$, nego samo da ako za neki izbor od n elemenata postoji $(x_1,\dots,x_{n+m}) \in \rho$ tada su preostali elementi jednoznačno odredjeni. Koristeći pojam parcijalne multikvazigrupe se dokazuje sledeća važna teorema.

TEOREMA 3.34. [19] Za svaku parcijalnu (n,m)-kvazigrupu (Q,ρ) postoji (n,m)-kvazigrupa (R,σ) koja je proširenje parcijalne multikvazigrupe (Q,ρ).

IV

(m,n)-PRSTENI

Iako su (m,n)-prsteni vrlo prirodno uopštenje binarnih prstena, oni su uvedeni tek 1965. godine ali je posebno značajno da ih je definisao i ispitivao naš matematičar Dj.Čupona. U ovoj tezi će se ispitivati lokalizacija u komutativnim (m,n)-prstenima tako da su navedeni i neki rezultati o kancelativnosti i komutativnosti u n-polugrupama i n-grupama.

DEFINICIJA 4.1. n-grupoid (Q,f) se naziva σ-komutativan ako i samo ako je

$$f(x_1,\ldots,x_n) = f(x_{\sigma(1)},\ldots,x_{\sigma(n)})$$

gde je σ permutacija skupa $\mathbb{N}_n$. Ako je (Q,f) σ-komutativan za svako $\sigma \in S_n$ tada se (Q,f) naziva komutativan n-grupoid.

TVRDJENJE 4.1. Neka je (Q,f) komutativna n-grupa Tada su sledeća tvrdjenja ekvivalentna

(i) e je idempotent.

(ii) $e = \bar{e}$.

(iii) e je jedinični element.

DEFINICIJA 4.2. Neka su (Q,f) i (R,g) n-grupoidi i φ preslikavanje skupa Q u skup R. Preslikavanje φ se naziva homomorfizam ako i samo ako je

$$\varphi(f(x_1^n)) = g(\{\varphi(x_i)\}_{i=1}^n)$$

za svako $x_1^n \in Q$.

TVRDJENJE 4.2. Neka su (Q,f) i (R,g) n-grupe i φ homomorfizam Q u R. Tada je $\varphi(\bar{x}) = \overline{\varphi(x)}$.

TVRDJENJE 4.3. Neka je (Q,f) komutativna n-grupa. Tada je

$$\overline{f(x_1^n)} = f(\bar{x}_1^n).$$

DEFINICIJA 4.3. Neka je (Q,f) n-polugrupa. Element $z \in Q$ se naziva nula te polugrupe ako i samo ako je

$$f(z,x_1^{n-1}) = f(x_1,z,x_2^{n-1}) = \ldots = f(x_1^{n-1},z) = z,$$

za svako $x_1^n \in Q$.

Sa Q^* ćemo označiti podskup elemenata od Q različitih od nule. Ako Q nema nulu tada je $Q^* = Q$.

TVRDJENJE 4.4. Neka je (Q,f) n-polugrupa sa nulom. Tada je nula jedinstvena.

DEFINICIJA 4.4. n-polugrupa (Q,f) se naziva i-kancelativna u odnosu na skup $M \subseteq Q$ ako i samo ako za svako $a_1^{n-1} \in M$ iz

$$f(a_1^{i-1},x,a_i^{n-1}) = f(a_1^{i-1},y,a_i^{n-1}) \quad \text{sledi} \quad x = y.$$

Ako je $i=1$ tada se (Q,f) naziva desno kancelativna u odnosu na M, a ako je $i=n$ tada se naziva levo kancelativna u odnosu na M. Ako je (Q,f) i-kancelativna u odnosu na M za svako $i \in \mathbb{N}_n$ tada se naziva kancelativna u odnosu na M.

Ako je $M = Q^*$ tada se naziva samo i-kancelativna, levo kancelativna, desno kancelativna odnosno kancelativna respektivno.

TVRDJENJE 4.5. Neka je (Q,f) n-polugrupa $n > 2$, Tada su sledeća tvrdjenja ekvivalentna:

(i) Q je kancelativna n-polugrupa.

(ii) Q je levo i desno kancelativna n-polugrupa.

(iii) Q je i-kancelativna n-polugrupa za neko $i \in \{2,\dots,n-1\}$.

DOKAZ. Očigledno (i) $\Rightarrow$ (ii).

Neka važi (ii) i neka je

$$f(a_1^{i-1},x,a_i^{n-1}) = f(a_1^{i-1},y,a_i^{n-1}).$$

Tada je za neko $b_1^{n-1} \in Q^*$

$$f(b_i^{n-1},f(a_1^{i-1},x,a_i^{n-1}),b_1^{i-1}) =$$

$$= f(b_i^{n-1},f(a_1^{i-1},y,a_i^{n-1}),b_1^{i-1})$$

pa je zbog asocijativnosti

$$f(f(b_i^{n-1},a_1^{i-1},x),a_i^{n-1},b_1^{i-1}) =$$

$$= f(f(b_i^{n-1},a_1^{i-1},y),a_i^{n-1},b_1^{i-1}).$$

Zbog leve i desne kancelativnosti dobijamo da je $x = y$, tj. (iii).

(iii) $\Rightarrow$ (i). Dokažimo j-kancelativnost. Neka je $j > i$ i neka je

$$f(a_1^{j-1},x,b_j^{n-1}) = f(a_1^{j-1},y,a_j^{n-1}).$$

Neka $b_1^{n-1} \in Q^*$ i neka je $k = n+i-j-1$. Tada je

$$f(b_1^k,f(a_1^{j-1},x,a_j^{n-1}),b_{k+1}^{n-1}) =$$

$$= f(b_1^k,f(a_1^{j-1},y,a_j^{n-1}),b_{k+1}^{n-1}) ,$$

zbog asocijativnosti sledi

$$f(b_1^{i-2},f(b_{i-1}^k,a_j^{j-1}),x,a_j^{n-1},b_{k+1}^{n-1}) =$$

$$= f(b_1^{i-2},f(b_{i-1}^k,a_1^{j-1}),y,a_j^{n-1},b_{k+1}^{n-1})$$

pa je sada zbog i-kancelativnosti $x = y$.

Ako je $j < i$ tada treba uzeti $k = i-j-1$.

TVRDJENJE 4.6. Neka je $(Q,\cdot)$ n-polugrupa i $(S,\cdot)$ n-polugrupa takva da je $(S,\cdot)$ n-grupa i neka je zadovoljen jedan od uslova

(i) Q ima bar jedan jedinični slog e_1^{n-1} takav da $e_1^{n-1} \in S$.

(ii) Za svako $x \in Q$ postoje $s,t \in S$ i $u_2^n, v_1^{n-1} \in Q$ takvi da je

$$x = su_2 \dots u_n \quad \text{i} \quad x = v_1 \dots v_{n-1}t.$$

Tada je $(Q,\cdot)$kancelativno u odnosu na S.

DOKAZ. Neka je zadovoljen uslov (i). Dokazaćemo levu kancelativnost, dok se desna kancelativnost dokazuje analogno. Neka je

(*) $\quad a_1a_2 \dots a_{n-1}x = a_1a_2 \dots a_{n-1}y, \quad a_1^{n-1} \in S.$

Pošto je S n-grupa to je

$$e_1 \dots e_{n-1}(a_{n-1})^{n-3}\bar{a}_{n-1} \dots (a_2)^{n-3}\bar{a}_2(a_1)^{n-3}\bar{a}_1(a_1a_2 \dots a_{n-1}x) =$$

$$= e_1 \dots e_{n-1}(a_{n-1})^{n-3}\bar{a}_{n-1} \dots (a_2)^{n-3}\bar{a}_2((a_1)^{n-3}\bar{a}_1a_1a_2)a_3 \dots a_{n-1}x =$$

$$= e_1 \dots e_{n-1}(a_{n-1})^{n-3}\bar{a}_{n-1} \dots (a_2)^{n-3}\bar{a}_2a_2a_3 \dots a_{n-1}x = \dots =$$

$$= e_1 \dots e_{n-2}(e_{n-1}(a_{n-1})^{n-3}\bar{a}_{n-1}a_{n-1})x = e_1 \dots e_{n-1}x = x,$$

a analogno se dobija da je desna strana jednakosti (*) y pa je $x = y$. Ako je $n = 3$ tada se izostavlja član $(a_i)^{n-3}$, $i=1,\dots,n-1$.

Neka je (ii) i (*). Dokažimo opet levu kancelativnost. Analogno se dobija da je

$$(a_{n-1})^{n-3}\bar{a}_{n-1} \dots (a_1)^{n-3}\bar{a}_1(a_1a_2 \dots a_{n-1}x) = (a_{n-1})^{n-3}\bar{a}_{n-1}a_{n-1}x =$$

$$= (a_{n-1})^{n-3}\bar{a}_{n-1}a_{n-1}(su_2 \dots u_n) = ((a_{n-1})^{n-3}\bar{a}_{n-1}a_{n-1}s)u_2 \dots u_n = su_2 \dots u_n = x,$$

pa je $x=y$. Koristeći prethodno tvrdjenje tada je $(Q,\cdot)$ kancelativna n-polugrupa u odnosu na S.

DEFINICIJA 4.5. Algebra (R,f,g) se naziva (m,n)-prsten ako i samo ako je

(i) (R,f) je komutativna n-grupa, $m \geq 2$.

(ii) (R,g) je n-polugrupa, $n \geq 2$.

(iii) Za svako $i \in \mathbb{N}_n$ važi sledeći distributivan zakon za svako $a_1^n, b_1^m \in R$

$$g(a_1^{i-1}, f(b_1^m), a_i^{n-1}) = f(\{g(a_1^{i-1}, b_j a_i^{n-1})\}_{j=1}^m).$$

Kako su oznake u prethodnoj definiciji komplikovane i nepregledne koristićemo i sledeće oznake:

$$f(x_1^m) = x_1 + x_2 + \ldots + x_m$$

i operaciju f ćemo nazivati m-arno sabiranje (ili prosto sabiranje ako to ne dovodi do zabune) pri čemu treba voditi računa da je $x_1 + \ldots + x_k$ dopušten izraz ako i samo ako je $k \equiv 1 \mod (m-1)$.

Analogno ćemo operaciju g nazivati n-arno množenje (ili samo množenje ako to ne dovodi do zabune) i označavati je sa

$$g(x_1^n) = x_1 x_2 \ldots x_n$$

pri čemu treba voditi računa da je $x_1 x_2 \ldots x_r$ definisano ako i samo ako je $r \equiv 1 \mod (n-1)$. Ako je $x_1 = x_2 = \ldots = x_n = x$ tada ćemo $x_1 x_2 \ldots x_n$ označavati sa $(x)^n$.

Komutativnu m-grupu (R,f) ćemo zvati aditivna m-grupa (m,n)-prstena, a n-polugrupu (R,g) ćemo zvati multiplikativna n-podgrupa (m,n)-prstena.

Neka je $T \subseteq S$. Ako je (T,f,g) (m,n)-prsten tada se (T,f,g) naziva (m,n)-podprsten od (R,f,g).

TVRDJENJE 4.7. Neka je (R,f,g) (m,n)-prsten i $a_1^n \in R$. Tada je za svako $i \in \mathbb{N}_n$

$$\overline{g(a_1^n)} = g(a_1^{i-1}, \bar{a}_i, a_{i+1}^n).$$

DEFINICIJA 4.6. Neka je (Q,f,g) (m,n)-prsten. Rećićemo da je (Q,f,g) (m,n)-prsten sa nulom ako i samo ako multiplikativna n-polugrupa (Q,g) ima nulu. Nulu prstena označićemo sa 0_R (ili prosto 0).

TVRDJENJE 4.8. Neka je (R,f,g) (m,n)-prsten. Ako (m,n)-prsten R ima jedinstven aditivan idempotent e tada je e nula.

DEFINICIJA 4.7. Neka je (R,f,g) (m,n)-prsten sa nulom. Element $a \in R^*$ se naziva i-ti delitelj nule ako i samo ako postoje $b_1^{n-1} \in R^*$ takvi da je $g(b_1^{i-1},a,b_i^{n-1}) = 0$. Ako je i-ti delitelj nule za svako $i \in \mathbb{N}_n$ tada se a naziva delitelj nule.

DEFINICIJA 4.8. (m,n)-prsten se naziva i-kancelativan ako i samo ako je njegova multiplikativna n-podgrupa i-kancelativna, levo kancelativna, desno kancelativna ili kancelativna respektivno.

DEFINICIJA 4.9. (m,n)-prsten se naziva σ-komutativan odnosno komutativan ako i samo ako mu je multiplikativna n-polugrupa σ-komutativna odnosno komutativna.

DEFINICIJA 4.10. (m,n)-prsten (Q,f,g) se naziva (m,n)-domen integriteta (ili integralni (m,n)-domen) ako i samo ako je komutativan i kancelativan.

TVRDJENJE 4.11. Neka je (R,f,g) (m,n)-prsten sa nulom. Tada su sledeći uslovi ekvivalentni:

(i) (R^*,g) je n-polugrupa, tj. R nema delitelja nule.
(ii) (R^*,g) je kancelativna n-polugrupa.
(iii) (R,f,g) je kancelativan (m,n)-prsten.

TVRDJENJE 4.12. Neka je (R,f,g) kancelativan (m,n)-prsten. Tada je zadovoljan jedan i samo jedan od uslova:

(i) R nema aditivnih idempotenata.
(ii) R ima nulu.
(iii) svaki element R je aditivan idempotent.

DEFINICIJA 4.11. Neka (R,f,g) (m,n)-prsten ako multiplikativna n-polugrupa (R,g) ima n-podpolugrupu (S,g) takvu da je (S,g) n-grupa tada se multiplikativni kosi element elementa a označava $\underline{a}$.

DEFINICIJA 4.12. Neka je (R,f,g) (m,n)-prsten, a skup $I \subseteq T$. I se naziva ideal (m,n)-prstena (R,f,g) ako i samo ako je

(i) (I,g) je n-podgrupa aditivne n-grupe od R.

(ii) Za svako $r_1^{n-1} \in R$, svako $a \in I$ i svako $i \in \mathbb{N}_n$

$$g(r_1^{i-1}, a, r_i^{n-1}) \in I.$$

DEFINICIJA 4.13. Neka je (R,f,g) (m,n)-prsten i $S_1^k \subseteq R$ pri čemu je $k \equiv 1 \bmod (m-1)$. Tada je

$$S_1 + \ldots + S_k \overset{\text{def}}{=} \{x \in R \mid x = a_1 + \ldots + a_k,\ a_i \in I_i,\ i \in \mathbb{N}_k\}.$$

TVRDJENJE 4.13. Neka je (R,f,g) (m,n)-prsten i neka su I_1^k ideali (m,n)-prstena R, pri čemu je $k \equiv 1 \bmod (m-1)$. Tada je $I_1 + \ldots + I_k$ ideal (m,n)-prstena R.

DEFINICIJA 4.14. Neka je (R,f,g) (m,n)-prsten i $S_1^t \subseteq R$ pri čemu je $t \equiv 1 \bmod (n-1)$. Tada je

$$S_1 \ldots S_t = \{x \in R \mid x = a_{11} \ldots a_{1t} + \ldots + a_{k1} \ldots$$

$$\ldots a_{kt},\ a_{ij} \in S_j,\ i \in \mathbb{N}_k,\ j \in \mathbb{N}_t,\ k \equiv 1 \bmod (m-1)\}.$$

TVRDJENJE 4.14. Neka je (R,f,g) komutativan (m,n)-prsten i neka su I_1^t ideali (m,n)-prstena R, pri čemu je $t \equiv 1 \bmod (n-1)$. Tada je $I_1 \ldots I_t$ ideal (m,n)-prstena R.

Za (m,n)-prstene može da se dokaže teorema analogna Postovoj teoremi za n-arne grupe. Prvi je dokazao tu teoremu Dj.Čupona 1965. [14], a posle toga je dokazana bar još tri puta ([5],[11],[34]). Ovu teoremu ćemo navesti bez dokaza.

TEOREMA 4.15. (Čupona) Neka je (R,f,g) (m,n)-prsten. Tada

(i) Postoji komutativna binarna grupa $(K,+)$ koja je skup generatora R takva da K sadrži podgrupu N gde je $N=(m-1)R$.

(ii) $f(x_1^m) = x_1 + x_2 + \dots + x_n$, $x_i \in R$, $i=1,\dots,m$.

(iii) Faktorgrupa K/N je ciklična grupa reda $m-1$.

(iv) U grupi $(K,+)$ može da se definiše n-arno množenje h tako da je $(K,+,h)$ $(2,n)$-prsten.

(v) Podgrupa N je ideal u R, a R je koset u faktor prstenu K/N.

(vi) Restrikcija h na R je g.

(vii) $(K,+,h)$ je jednoznačno odredjen (do na izomorfizam).

Navešćemo još jednu teoremu Dj.Čupone koja zaslužuje da bude poznatija.

TEOREMA 4.16. (Čupona) Neka je $(R,\oplus,g)$ $(2,n)$-prsten. Tada postoji binaran prsten $(Q,+,\cdot)$ takav da je:

(i) $R \subseteq Q$,

(ii) $(R,\oplus)$ je podgrupa grupe $(Q,+)$,

(iii) $g(x_1^n) = x_1 x_2 \dots x_n$, $x_i \in R$, $i \in \mathbb{N}_n$.

DOKAZ. Neka je $(S,\cdot)$ univerzalna pokrivajuća polugrupa n-polugrupe. Podsetimo [13] da je

$$S = \{a_1 a_2 \dots a_p \mid a_i \in R,\ 1 \leqslant p < n\},$$

da je pri tom iz

$$a_1 \dots a_p = b_1 \dots b_q, \quad 1 \leqslant p \leqslant q < n \quad \text{sledi } p = q$$

i da za $1 \leqslant p < n$ važi

$$(a_1 \dots a_p)(a_{p+1} \dots a_n) = g(a_1^n).$$

Neka je $(T,+,\cdot)$ podgrupni prsten konstruisan nad $(S,\cdot)$, tj. $(T,+)$ je slobodna komutativna grupa za koju je S skup slobodnih generatora, dok se množenje definiše produžavanjem po distributivnosti. Na taj način se svaki element od T može predstaviti kao zbir konačno mnogo sabiraka oblika

$$\varepsilon a_1 a_2 \dots a_k, \text{ gde je } \varepsilon = \pm 1,\ 1 \leqslant k \leqslant n-1 .$$

Definišimo preslikavanje φ iz S u R sa:

$$\varphi(a) = a, \quad \text{za} \quad a \in R ,$$

$$\varphi(a_1 a_2 \dots a_k) = \hat{0}, \text{ za } 2 \leqslant k \leqslant n-1, \quad a_i \in R ,$$

gde je sa $\hat{0}$ označena nula prstena $(R,\oplus,g)$. Kako je T polugrupni prsten to postoji jedinstven homomorfizam

$$\psi: (T,+) \to (R,\oplus),$$

takav da je restrikcija od ψ na S baš φ. (Uočimo da ψ nije "prstenski" homomorfizam).

Označimo sa A skup svih onih elemenata iz T oblika

$$a_1 \dots a_i\,(d-b-c)a_{i+1} \dots a_k$$

gde je $k \geqslant 0$, $a_i, b, c, d \in R$ i važi $d = b \oplus c$ u $(R,\oplus,g)$. Neposredno sledi da je podgrupa I, grupe $(T,+)$ generisana sa A, ideal prstena $(T,+,\cdot)$. Naime, I je definisano sa

$$I = \{ \sum_{i=1}^{p} \varepsilon_i u_i \mid \varepsilon_i = \pm 1,\ u_i \in A,\ p \geqslant 1 \} .$$

Neka je u proizvoljan element A tj.

$$u = a_1 \dots a_i (d-b-c) a_{i+1} \dots a_k =$$

$$= a_1 \dots a_i d a_{i+1} \dots a_k - a_1 \dots a_i b a_{i+1} \dots a_k -$$

$$- a_1 \dots a_i c a_{i+1} \dots a_k ,$$

i neka je $k \equiv \alpha$ (mod n-1). Tada po definiciji homomorfizma imamo da je za $\alpha > 0$, $\psi(u) = \hat{0}$, dok je za $\alpha = 0$

$$\psi(u) = \psi(a_1 \ldots a_i d a_{i+1} \ldots a_k)\ \theta\ \psi(a_1 \ldots a_i b a_{i+1} \ldots a_k)\ \theta$$

$$\theta\ \psi(a_1 \ldots a_i c a_{i+1} \ldots a_k) = a_1 \ldots a_i d a_{i+1} \ldots a_k\ \theta$$

$$\theta\ a_1 \ldots a_i b a_{i+1} \ldots a_k\ \theta\ a_1 \ldots a_i c a_{i+1} \ldots a_k =$$

$$= a_1 \ldots a_i (d\ \theta\ b\ \theta\ c) a_{i+1} \ldots a_k =$$

$$= a_1 \ldots a_i\ \hat{0}\ a_{i+1} \ldots a_k = \hat{0}\ ,$$

gde je sa θ označena inverzna operacija za $\oplus$.

Prema tome, imamo da je $\psi(u) = \hat{0}$ za svako $u \in A$, pa je tada i $\psi(u) = \hat{0}$ za svako $u \in I$, tj. $I \subseteq \ker(\psi)$.

Posmatrajmo faktor prsten $(R^1,+,\cdot) = (T/I,+,\cdot)$. Jasno je da je kanoničko preslikavanje

$$\pi_I : R \to R^{\hat{}}\ ,$$

definisano sa

$$\pi_I : x \to x + I\ ,$$

homomorfizam (2,n)-prstena $(R,\oplus,g)$ u (2,n)-prsten $(R^{\hat{}},\oplus,g')$ gde je g' definisano sa $g'(x_1^n) = x_1 x_2 \ldots x_n$.

Ako je pri tom $\pi_I(a) = \pi_I(b)$, za neko $a,b \in R$, tada je $b \in a+I$, tj. $b = a+u$ za neko $u \in I$, pa je

$$b = \psi(b) = \psi(a) + \psi(u) = a + \hat{0} = a\ ,$$

tj. π_I je monomorfizam.

Stavljajući da je $Q = R^{\hat{}}$, dobija se tvrdjenje teoreme. Naime, lako se proverava da dobijeni prsten $(R^{\hat{}},+,\cdot)$ ima sledeće "univerzalno svojstvo":

Ako je $(Q,+,\cdot)$ proizvoljan prsten koji zadovoljava uslove (i), (ii) i (iii) teoreme, tada postoji jedinstven homomorfizam $\xi : R^{\hat{}} \to Q$, takav da je $\xi(a) = a$, za svako $a \in R$.

<u>DEFINICIJA 4.15.</u> Neka je $(R,+,\cdot)$ komutativan (n, m)-prsten i neka je $(S,\cdot)$ n-podpolugrupa multiplikovane n-polugrupe (m,n)-prstena R. Nad skupom $R \times S^{n-1}$ definišemo rela-

ciju sa

$(r_1^n) \sim (s_1^n)$ ako i samo ako postoji

$t_2^n \in S$ tako da je

$r_1 s_2 \ldots s_n t_2 \ldots t_n = s_1 r_2 \ldots r_n t_2 \ldots t_n$.

TEOREMA 4.17. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten. Tada je relacija $\sim$ definisana u definiciji 4.1. relacija ekvivalencije.

DOKAZ. Dokaz reflektivnosti i simetrije sledi neposredno iz definicije. Dokažimo tranzitivnost. Neka je

$(r_1^n) \sim (s_1^n)$ i $(s_1^n) \sim (u_1^n)$.

Na osnovu definicije 4.15 je tada

(1) $r_1 s_2 \ldots s_n t_2 \ldots t_n = s_1 r_2 \ldots r_n t_2 \ldots t_n$ za neko $t_2^n \in S^{n-1}$ i

(2) $s_1 u_2 \ldots u_n v_2 \ldots v_n = u_1 s_2 \ldots s_n v_2 \ldots v_n$ za neko $v_2^n \in S^{n-1}$.

Iz (1) i (2) slede

$$r_1 s_2 \ldots s_n t_2 \ldots t_n u_2 \ldots u_n v_2 \ldots v_n =$$
$$= s_1 r_2 \ldots r_n t_2 \ldots t_n u_2 \ldots u_n v_2 \ldots v_n \text{ i}$$

$$s_1 u_2 \ldots u_n v_2 \ldots v_n r_2 \ldots r_n t_2 \ldots t_n =$$
$$= u_1 s_2 \ldots s_n v_2 \ldots v_n r_2 \ldots r_n t_2 \ldots t_n$$

pa je

$$r_1 s_2 \ldots s_n t_2 \ldots t_n u_2 \ldots u_n v_2 \ldots v_n =$$
$$= u_1 s_2 \ldots s_n v_2 \ldots v_n r_2 \ldots r_n t_2 \ldots t_n \text{ .}$$

Koristeći asocijativnost i komutativnost n-arnog množenja dobijamo da je

$$(r_1 u_2 \ldots u_n)(s_2 \ldots s_n t_2)(t_3 \ldots t_n v_2 v_3) v_4 \ldots v_n =$$
$$= (u_1 r_2 \ldots r_n)(s_2 \ldots s_n t_2)(t_3 \ldots t_n v_2 v_3) v_4 \ldots v_n \text{ ,}$$

pa je

$$(r_1^n) \sim (u_1^n)$$

tj. $\sim$ je $R\,S\,T$ relacija.

DEFINICIJA 4.16. Neka je $\sim$ relacija ekvivalencije opisana u definiciji 4.15 i teoremi 4.17. Tada se klasa ekvivalencije koja odgovara (s_1^n) u odnosu na relaciju $\sim$ označava sa $[s_1^n]$, a skup klasa ekvivalencije $R \times S^{n-1}/\sim$ sa $S^{-1}R$. Ako je $T \subseteq R$ tada se skup klasa ekvivalencije $[s_1^n]$ pri čemu $s_1 \in T$ i $s_2^n \in S$ označava sa $S^{-1}T$.

PRIMEDBA. Ako je n-polugrupa R kancelativna u odnosu na S tada se $(a_1^n) \sim (b_1^n)$ svodi na $a_1b_2 \ldots b_n = b_1a_2 \ldots$ $\ldots a_n$, relacija, koja je uvedena u [12]

TEOREMA 4.18. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten i $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe. Definišimo u skupu $S^{-1}R$, klasa ekvivalencije po relaciji operacije na sledeći način:

(i) Neka je $[a_1^n],[b_1^n],[c_1^n],\ldots,[d_1^n],[e_1^n]$ m elemenata skupa $S^{-1}R$. Definišimo

$$[a_1^n]+[b_1^n]+[c_1^n]+\ldots+[d_1^n]+[e_1^n] =$$

$$= [(a_1b_2 \ldots b_n \ldots e_2 \ldots e_n + b_1a_2 \ldots a_nc_2 \ldots c_n \ldots e_2 \ldots e_n + \ldots$$

$$\ldots + e_1a_2 \ldots a_n \ldots d_2 \ldots d_n)x_{12} \ldots x_{1n} \ldots x_{k2} \ldots x_{kn},$$

$$a_2b_2 \ldots d_2e_2x_{12} \ldots x_{k2}, \ldots, a_nb_n \ldots d_ne_nx_{1n} \ldots x_{kn}] .$$

gde je k prirodan broj takav da reči $a_ib_i \ldots d_ie_ix_{1i} \ldots x_{ki}$ postanu dopustive za multiplikativnu n-polugrupu, a $x_{ij} \in S$, $i \in \mathbb{N}_k$, $j \in \mathbb{N}_n$, su proizvoljni.

(ii) Neka su $[a_1^n]$, $[b_1^n],\dots,[e_1^n]$ i elemenata skupa $S^{-1}R$, definišemo

$$[a_1^n][b_1^n]\dots[e_1^n] = [a_1b_1\dots e_1,\dots,a_nb_n\dots e_n] .$$

Tada je $(S^{-1}R,+,\cdot)$ komutativan (m,n)-prsten.

DOKAZ. Dokaz se svodi na direktnu verifikaciju. Da ne bismo preterano opterećivali notaciju dokazećemo tvrdjenje za $(3,4)$-prsten.

Najpre dokazujemo da je ternarno sabiranje dobro definisano. Neka su

$$(a_1^4)\sim(\alpha_1^4),\ (b_1^4)\sim(\beta_1^4) \quad \text{i} \quad (c_1^4)\sim(\gamma_1^4)$$

treba pokazati da je

$$[a_1^4]+[b_1^4]+[c_1^4] = [\alpha_1^4]+[\beta_1^4]+[\gamma_1^4] ,$$

a da bismo to dokazali dovoljno je da dokažemo da je

$$(*) \qquad [a_1^4]+[b_1^4]+[c_1^4] = [\alpha_1^4]+[b_1^4]+[c_1^4] ,$$

jer se potpuno analogno dokazuje

$$[\alpha_1^4]+[b_1^4]+[c_1^4] = [\alpha_1^4]+[\beta_1^4]+[c_1^4]$$

i

$$[\alpha_1^4]+[\beta_1^4]+[c_1^4] = [\alpha_1^4]+[\beta_1^4]+[\gamma_1^4]$$

pa željeno tvrdjenje sledi iz tranzitivnosti.

Da se dokeže $(*)$ treba pokazati da je

$$((a_1b_2b_3b_4c_2c_3c_4+b_1a_2a_3a_4c_2c_3c_4 +$$
$$+ c_1a_2a_3a_4b_2b_3b_4)x_{12}x_{13}x_{14},$$
$$, a_2b_2c_2x_{12}, a_3b_3c_3x_{13}, a_4b_4c_4x_{14})\sim$$
$$\sim ((\alpha_1b_2b_3b_4c_2c_3c_4+b_1\alpha_2\alpha_3\alpha_4c_2c_3c_4 +$$
$$+ c_1\alpha_2\alpha_3\alpha_4b_2b_3b_4)y_{12}y_{13}y_{14},$$

$$,\alpha_2 b_2 c_2 y_{12}, \alpha_3 b_3 c_3 y_{13}, \alpha_4 b_4 c_4 y_{14})$$

ako je $(\alpha_1^4) \sim (a_1^4)$.

Neka je

$$\alpha_1 a_2 a_3 a_4 t_2 t_3 t_4 = a_1 \alpha_2 \alpha_3 \alpha_4 t_2 t_3 t_4 ,$$

za neko $t_2^4 \in S$. Tada je zbog distributivnosti i komutativnosti

$$(a_1 b_2 b_3 b_4 c_2 c_3 c_4 + b_1 a_2 a_3 a_4 c_2 c_3 c_4 + c_1 a_2 a_3 a_4 b_2 b_3 b_4)$$

$$x_{12} x_{13} x_{14} \alpha_2 \alpha_3 \alpha_4 b_2 b_3 b_4 c_2 c_3 c_4 y_{12} y_{13} y_{14} t_2 t_3 t_4 =$$

$$= (a_1 \alpha_2 \alpha_3 \alpha_4 t_2 t_3 t_4 b_2 b_3 b_4 c_2 c_3 c_4 + b_1 a_2 a_3 a_4 c_2 c_3 c_4 \alpha_2 \alpha_3 \alpha_4 t_2 t_3 t_4 +$$

$$+ c_1 a_2 a_3 a_4 b_2 b_3 b_4 \alpha_2 \alpha_3 \alpha_4 t_2 t_3 t_4) x_{12} x_{13} x_{14} b_2 b_3 b_4 c_2 c_3 c_4 y_{12} y_{13} y_{14} =$$

$$= (\alpha_1 a_2 a_3 a_4 t_2 t_3 t_4 b_2 b_3 b_4 c_2 c_3 c_4 + b_1 a_2 a_3 a_4 t_2 t_3 t_4 \alpha_2 \alpha_3 \alpha_4 c_2 c_3 c_4 +$$

$$+ c_1 a_2 a_3 a_4 t_2 t_3 t_4 \alpha_2 \alpha_3 \alpha_4 b_2 b_3 b_4) x_{12} x_{13} x_{14} b_2 b_3 b_4 c_2 c_3 c_4 y_{12} y_{13} y_{14} =$$

$$= (\alpha_1 a_2 a_3 a_4 b_2 b_3 b_4 + b_1 \alpha_2 \alpha_3 \alpha_4 c_2 c_3 c_4 + c_1 \alpha_2 \alpha_3 \alpha_4 b_2 b_3 b_4) y_{12} y_{13} y_{14}$$

$$\cdot\ a_2 a_3 a_4 b_2 b_3 b_4 c_2 c_3 c_4 x_{12} x_{13} x_{14} t_2 t_3 t_4 ,$$

a to je i trebalo dokazati.

Dokažimo sad (1,2)-asocijativnost.

$$([a_1^4] + [b_1^4] + [c_1^4]) + [d_1^4] + [e_1^4] =$$

$$= [(a_1 b_2 b_3 b_4 c_2 c_3 c_4 + b_1 a_2 a_3 a_4 c_2 c_3 c_4 + c_1 a_2 a_3 a_4 b_2 b_3 b_4) x_{12} x_{13} x_{14} ,$$

$$, a_2 b_2 c_2 x_{12}, a_3 b_3 c_3 x_{13}, a_4 b_4 c_4 x_{14}] + [d_1^4] + [e_1^4] =$$

$$= [((a_1 b_2 b_3 b_4 c_2 c_3 c_4 + b_1 a_2 a_3 a_4 c_2 c_3 c_4 + c_1 a_2 a_3 a_4 b_2 b_3 b_4)$$

$$x_{12} x_{13} x_{14} d_2 d_3 d_4 e_2 e_3 e_4 + d_1 a_2 a_3 a_4 b_2 b_3 b_4 c_2 c_3 c_4 x_{12} x_{13} x_{14} e_2 e_3 e_4 +$$

$$+ e_1 a_2 a_3 a_4 b_2 b_3 b_4 c_2 c_3 c_4 x_{12} x_{13} x_{14} d_2 d_3 d_4) y_{12} y_{13} y_{14} ,$$

$$, a_2 b_2 c_2 d_2 e_2 x_{12} y_{12}, a_3 b_3 c_3 d_3 e_3 x_{13} y_{13}, a_4 b_4 c_4 d_4 e_4 x_{14} y_{14}] ,$$

dok je

$$[a_1^4]+([b_1^4]+[c_1^4]+[d_1^4])+[e_1^4] =$$

$$= [a_1^4] + [(b_1c_2c_3c_4d_2d_3d_4+c_1b_2b_3b_4d_2d_3d_4+$$

$$+ d_1b_2b_3b_4c_2c_3c_4)x_{12}x_{13}x_{14}, b_2c_2d_2x_{12}, b_3c_3d_3x_{13}, b_4c_4d_4x_{14}] +$$

$$+ [e_1^4] = [(a_1b_2b_3b_4c_2c_3c_4d_2d_3d_4x_{12}x_{13}x_{14}e_2e_3e_4 \quad +$$

$$+ (b_1c_2c_3c_4d_2d_3d_4+c_1b_2b_3b_4d_2d_3d_4+d_1b_2b_3b_4c_2c_3c_4)\cdot$$

$$\cdot x_{12}x_{13}x_{14}a_2a_3a_4e_2e_3e_4+e_1b_2b_3b_4c_2c_3c_4d_2d_3d_4x_{12}x_{13}x_{14}a_2a_3a_4)$$

$$y_{12}y_{13}y_{14}, a_2b_2c_2d_2e_2x_{12}y_{12}, a_3b_3c_3d_3e_3x_{13}y_{13}, a_4b_4c_4d_4e_4x_{14}y_{14}].$$

Koristeći distributivnost, komutativnost i asocijativnost po prvoj komponenti se vidi da je $S^{-1}R$ (1,2)-asocijativan.

Da bismo rešili jednačinu $[a_1^4]+[b_1^4]+[x_1^4] = [c_1^4]$ dokažimo jednu jednostavnu formulu.

Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten. Tada je za svako $a_1^m \in R$ i svako $b_2^n \in S$

$$(**) \qquad [a_1, b_2^n] + \ldots + [a_m, b_2^n] = [a_1 + \ldots + a_m, b_2^n] .$$

$$[a_1, b_2^n] + \ldots + [a_m, b_2^n] = [(a_1(b_2 \ldots b_n)^{m-1} + \ldots$$

$$\ldots + a_m(b_2 \ldots b_n)^{m-1})x_{12} \ldots x_{1n} \ldots x_{k2} \ldots$$

$$\ldots x_{kn}, (b_2)^m x_{12} \ldots x_{1n}, \ldots, (b_n)^m x_{1n} \ldots x_{kn}] =$$

$$= [a_1 + \ldots + a_m, b_2^n] ,$$

jer je

$$(a_1+\ldots+a_m)(b_2)^m \ldots (b_n)^m x_{12} \ldots x_{k2} \ldots x_{1n} \ldots x_{kn} =$$

$$= (a_1(b_2 \ldots b_n)^{m-1} + \ldots + a_m(b_2 \ldots b_n)^{m-1})x_{12} \ldots x_{k2} \ldots$$

$$\ldots x_{1n} \ldots x_{kn} b_2 \ldots b_n .$$

Sada lako možemo rešiti

$$[a_1^4] + [b_1^4] + [x_1^4] = [c_1^4]$$

Naime za neko $n \in S$ je

$$[a_1^4] = [a_1 b_2 b_3 b_4 c_2 c_3 c_4 u^3, a_2 b_2 c_2 u, a_3 b_3 c_3 u, a_4 b_4 c_4 u] ,$$

$$[b_1^4] = [b_1 a_2 a_3 a_4 c_2 c_3 c_4 u^3, a_2 b_2 c_2 u, a_3 b_3 c_3 u, a_4 b_4 c_4 u] ,$$

$$[c_1^4] = [c_1 a_2 a_3 a_4 b_2 b_3 b_4 u^3, a_2 b_2 c_2 u, a_3 b_3 c_3 u, a_4 b_4 c_4 u] ,$$

pa ako stavimo da je

$$x_2 = a_2 b_2 c_2 u, \quad x_3 = a_3 b_3 c_3 u, \quad x_4 = a_4 b_4 c_4 u$$

dobijamo da treba rešiti,

$$a_1 b_2 b_3 b_4 c_2 c_3 c_4 u^3 + b_1 a_2 a_3 a_4 c_2 c_3 c_4 +$$

$$+ x_1 = c_1 a_2 a_3 a_4 b_2 b_3 b_4 u^3$$

pa x_1, a to je uvek moguće, jer je $(R,+)$ n-grupa.

Da je $(S^{-1}R,\cdot)$ polugrupa se proverava bez problema, jer je množenje definisano po komponentama, a takodje i komutativnost množenja.

Dokažimo distributivnost

$$([a_1^4]+[b_1^4]+[c_1^4])[d_1^4][e_1^4][f_1^4] =$$

$$= [(a_1 b_2 b_3 b_4 c_2 c_3 c_4 + b_1 a_2 a_3 a_4 c_2 c_3 c_4 + c_1 a_2 a_3 a_4 b_2 b_3 b_4) x_{12} x_{13} x_{14},$$

$$, a_2 b_2 c_2 x_{12}, a_3 b_3 c_3 x_{13}, a_4 b_4 c_4 x_{14}][d_1^4][e_1^4][f_1^4] =$$

$$= [(a_1 b_2 b_3 b_4 c_2 c_3 c_4 + b_1 a_2 a_3 a_4 c_2 c_3 c_4 + c_1 a_2 a_3 a_4 b_2 b_3 b_4) x_{12} x_{13} x_{14} d_1 e_1 f_1,$$

$$, a_2 b_2 c_2 x_{12} d_2 e_2 f_2, a_3 b_3 c_3 x_{13} d_3 e_3 f_3, a_4 b_4 c_4 x_{14} d_4 e_4 f_4] =$$

$$= [((a_1 d_1 e_1 f_1) b_2 b_3 b_4 c_2 c_3 c_4 + (b_1 d_1 e_1 f_1) a_2 a_3 a_4 c_2 c_3 c_4 +$$

$$+ (c_1 d_1 e_1 f_1) a_2 a_3 a_4 b_2 b_3 b_4) x_{12} x_{13} x_{14}, (a_2 d_2 e_2 f_2) b_2 c_2 x_{12},$$

$$(a_3d_3e_3f_3)b_3c_3x_{13},(a_4d_4e_4f_4)b_4c_4x_{14}] =$$

$$= [\{a_id_ie_if_i\}_{i=1}^4] + [\{b_id_ie_if_i\}_{i=1}^4] + [\{c_id_ie_if_i\}_{i=1}^4] =$$

$$= [a_1^4][d_1^4][e_1^4][f_1^4] + [b_1^4][d_1^4][e_1^4][f_1^4] + [c_1^4][d_1^4][e_1^4][f_1^4] \ ,$$

čime je dokaz završen.

Formulišimo formulu (**) posebno

POSLEDICA 4.19. Neka je $(R,+,\cdot)$ komutativan (m, n)-prsten i neka je $(S,\cdot)$ n-podpolugrupa multiplikativne n-podgrupe. Tada je za svako $a_1^m \in R$ i svako $b_2^n \in S$

$$[a_1,b_2^n] + \ldots + [a_m,b_2^n] = [a_1+\ldots+a_m,b_2^n] \ .$$

DEFINICIJA 4.17. Neka je $(R,+,\cdot)$ komutativan (m, n)-prsten i $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe. (m,n)-prsten $(S^{-1}R,+,\cdot)$ definisan u teoremi 4.17 se naziva lokalizacija (m,n)-prstena R sa S.

POSLEDICA 4.20. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten i $(S,\cdot)$ n-podgrupa multiplikativne n-polugrupe. Ako je I ideal (m,n)-prstena $(R,+,\cdot)$ tada je $S^{-1}I$ ideal u (m,n)-prstenu $S^{-1}R$.

DOKAZ. Iz dokaza teoreme 4.18 sledi da je $(S^{-1}I,+)$ aditivna m-podgrupa komutativne m-grupe $(S^{-1}R,+)$ ako je $(I,+)$ m-podgrupa m-grupe (R,f) dok stabilnost u odnosu na n-arno množenje sledi direktno iz definicije n-arnog množenja u $(S^{-1}R\ ,\cdot)$.

POSLEDICA 4.21. Neka je $(R,+,\cdot)$ komutativan (m, n)-prsten, $(S,\cdot)$ n-podgrupa multiplikativne n-polugrupe i $I_1,\ldots,I_k$ ideali (m,n)-prstena R pri čemu je $k \equiv 1 \bmod(m-1)$. Tada je

$$S^{-1}(I_1+\ldots+I_k) = S^{-1}I_1+\ldots+S^{-1}I_k \ .$$

DOKAZ. Neposredno sledi iz definicije sume ideala i posledice 4.19.

POSLEDICA 4.22. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten, $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe i $J_1,\dots,J_i$ ideali (m,n)-prstena R pri čemu je $i \equiv 1 \mod(n-1)$. Tada je

$$S^{-1}(J_1\dots J_i) = (S^{-1}J_1)\dots(S^{-1}J_i) .$$

DOKAZ. Dokaz sledi ako se u dokazu teoreme 4.17 stavi

$$a_1 = r_{11}\dots r_{1i},\ b_1 = r_{21}\dots r_{2i}\ ,\ c_1 = r_{31}\dots r_{3i},\dots$$

$$,\ d_1 = r_{m-1,1}\dots r_{m-1,i},\ e_1 = r_{m1}\dots r_{mi}\ , \quad \text{pri čemu}$$

pri čemu $r_{st} \in J_t$, $s \in \mathbb{N}_m$, $t \in \mathbb{N}_i$, i zatim primeni posledica 4.19.

Takodje se dobija

POSLEDICA 4.23. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten, $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe i I,J ideali (m,n)-prstena R. Tada je

$$S^{-1}(I\cap J) = S^{-1}I \cap S^{-1}J.$$

TEOREMA 4.24. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten i $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe. Tada je $(S^{-1}S,\cdot)$ n-grupa.

DOKAZ. Neka je data jednačina

$$x[a_1^n]\ \dots\ [t_1^n] = [a_1^n]\ ,$$

pri čemu $[s_1^n],\dots,[t_1^n],[a_1^n] \in S^{-1}S$. Tada je

$$x = [a_1 s_2\dots s_n\dots t_2\dots t_n, a_2 s_1\dots t_1, a_3,\dots,a_n]$$

rešenje, jer je

$$x[s_1^n]\dots[t_1^n] = [a_1 s_1\dots s_n\dots t_1\dots t_n, s_1\dots t_1 a_2 s_2\dots$$

$$\dots t_2, a_3 s_3\dots t_3,\dots,a_n s_n\dots t_n] = [a_1^n]\ .$$

TEOREMA 4.25. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten i $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe. Tada je (m,n)-prsten $(S^{-1}R,+,\cdot)$ kancelativan u odnosu na elemente skupa $S^{-1}S$.

DOKAZ. Pošto je R komutativan (m,n)-prsten dovoljno je dokazati 1-kanvelativnost. Neka je

$$[x_1^n][a_1^n]\ldots[c_1^n] = [y_1^n][a_1^n]\ldots[c_1^n] .$$

Tada je za neko $t_2^n \in S$

$$(x_1a_1\ldots c_1y_2a_2\ldots y_na_n\ldots c_n)t_2\ldots t_n =$$

$$= (y_1a_1\ldots c_1x_2a_2\ldots c_2\ldots x_na_n\ldots c_n)t_2\ldots t_n ,$$

pa je zbog komutativnosti

$$(x_1y_2\ldots y_n)a_1\ldots c_1a_2\ldots a_n\ldots c_2\ldots c_nt_2\ldots t_n =$$

$$= (y_1x_2\ldots x_n)a_1\ldots c_1a_2\ldots a_n\ldots c_2\ldots c_nt_2\ldots t_n .$$

Kako je $(S,\cdot)$ n-podpolugrupa to je

$$a_1\ldots c_1a_2\ldots a_n\ldots c_2\ldots c_nt_2 = u_2$$

$$t_i = u_i \ , \ \text{za } i=2,\ldots,n \ ;$$

pa je

$$[x_1^n] = [y_1^n].$$

TEOREMA 4.26. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten i neka je $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe. Tada je preslikavanje

$$\pi_s : R \to S^{-1}R ,$$

definisano sa

$$\pi_s : a \to [as_2\ldots s_n, s_2^n], \ s_i \in S, \ i=2,\ldots,n,$$

homomorfizam (m,n)-prstena $(R,+,\cdot)$ u (m,n)-prsten $(S^{-1}R,+,\cdot)$.

DOKAZ. Dokažimo najpre da je π_s dobro definisano.

Neka je $t_2^n \in S$. Tada se lako vidi da je

$$(as_2 \dots s_n, s_2^n) \sim (at_2 \dots t_n, t_2^n),$$

pa je π_s dobro definisano preslikavanje.

Iz posledice 4.19 odmah sledi da je

$$\pi_s(a_1 + \dots + a_m) = \pi_s(a_1) + \dots + \pi_s(a_m),$$

pa je π_s aditivan homomorfizam.

Takodje je

$$\pi_s(a_1) \dots \pi_s(a_n) = [a_1 s_2 \dots s_n, s_2^n] \dots$$

$$\dots [a_n s_2 \dots s_n, s_2^n] = [a_1 \dots a_n (s_2)^n \dots (s_n)^n, (s_2)^n, \dots$$

$$\dots, (s_n)^n] = [a_1 \dots a_n s_2 \dots s_n, s_2^n]$$

što se lako proverava pa je

$$\pi_s(a_1) \dots \pi_s(a_n) = \pi_s(a_1 \dots a_n).$$

DEFINICIJA 4.18. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten, a $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe $(R,\cdot)$. Tada se homomorfizam π_s (m,n)-prstena $(R,+,\cdot)$ u (m,n)-prsten $(S^{-1}R,+,\cdot)$ definisan u teoremi 4.25 naziva kanonički homomorfizam (m,n)-prstena $(R,+,\cdot)$ u (m,n)-prsten $(S^{-1}R,+,\cdot)$.

TEOREMA 4.27. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten i $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe $(R,\cdot)$. Ako je $(R,\cdot)$ kancelativna n-polugrupa u odnosu na S tada je kanonički homomorfizam π_s (m,n)-prstena $(R,+,\cdot)$ u (m,n)-prsten $(S^{-1}R,+,\cdot)$ monomorfizam.

DOKAZ. Neka je

$$[as_2 \dots s_n, s_2^n] = [bs_2 \dots s_n, s_2^n], \quad s_2^n \in S,$$

tada je

$$as_2 \dots s_n s_2 \dots s_n t_2 \dots t_n = bs_2 \dots s_n s_2 \dots s_n t_2 \dots t_n$$

za neko $t_2^n \in S$, a kako je R kancelativno u odnosu na S to je

$a = b$.

TEOREMA 4.28. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten i $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe takva da je $(S,\cdot)$ n-grupa i da $(R,\cdot)$ zadovoljava bar jedan od uslova tvrdjenja 4.6. Tada je kanonički homomorfizam π_S izomorfizam (m,n)-prstena $(R,+,\cdot)$ i $(S^{-1}R,+,\cdot)$.

DOKAZ. S obzirom na tvrdjenje 4.6 i teoremu 4.27 dovoljno je da dokažemo da je π_S surjektivno. Neka je $[t,u_2^n]$, $t\in R$, $u_2^n\in S$, proizvoljan element iz $S^{-1}R$. Da bi π_S bilo surjektivno tada, na osnovu definicije preslikavanja π_S, treba da postoji bar jedan element $s\in R$ takav da je

$$[ss_2\ldots s_n, s_2^n] = [t,u_2^n]$$

ili ekvivalentno

$$ss_2\ldots s_n u_2\ldots u_n x_2\ldots x_n = ts_2\ldots s_n x_2\ldots x_n,$$

za neko $x_2^n\in S$.

Neka je

$$s = t(u_2)^{n-3}\underline{u}_2\ldots(u_n)^{n-3}\underline{u}_n,$$

pri čemu se za $n=3$ izostavljaju članovi $(u_i)^{n-3}$, $i=2,\ldots,n$. Pošto je $(S,\cdot)$ komutativna n-grupa to je $(u_i)^{n-2}\underline{u}_i y = y$ za svako y S pa je

$$(t(u_2)^{n-3}\underline{u}_2\ldots(u_n)^{n-3}\underline{u}_n)u_2\ldots u_n s_2\ldots s_n = ts_2\ldots s_n,$$

tj. π_S je surjektivno.

TEOREMA 4.29. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten i $(S,\cdot)$ n-podpolugrupa multiplikativne n-polugrupe takva da je $(S,\cdot)$ n-grupa i da $(R,\cdot)$ zadovoljava bar jedan od uslova tvrdjenja 4.6. Neka je $(T,+,\cdot)$ (m,n)-prsten i neka je φ homomorfizam (m,n)-prstena $(R,+,\cdot)$ u (m,n)-prsten $(T,+,\cdot)$ takav da je $\varphi(S)$ n-grupa u multiplikativnoj n-polugrupi $(T^*,\cdot)$.

Tada postoji jednoznačno odredjen homomorfizam $\bar{\varphi}$ (m,n)-prstena $(S^{-1}R,+,\cdot)$ u (m,n)-prsten $(T,+,\cdot)$ takav da je $\bar{\varphi}\pi_s=\varphi$.

DOKAZ. Definišimo preslikavanje $\bar{\varphi}:S^{-1}R\to T$ sa

$$\bar{\varphi}:[r,s_2^n]\to\varphi(r)(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\dots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)}\ .$$

pri čemu se za n=2 članovi $(\varphi(s_i))^{n-3}$ izostavljaju. Tada je zbog posledice 4.19.

$$\varphi([r_1,s_2^n]+\dots+[r_m,s_2^n])=\varphi([r_1+\dots+r_m,s_2^n])=$$

$$=\varphi(r_1+\dots r_m)(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\dots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)}=$$

$$=(\varphi(r_1)+\dots+\varphi(r_m))(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\dots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)}=$$

$$=\varphi(r_1)(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\dots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)}+\dots$$

$$\dots+\varphi(r_m)(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\dots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)}=$$

$$=\varphi([r_1,s_2^n])+\dots+\varphi([r_m,s_2^n]).$$

Neka su sada $[r_1,s_2^n],\dots,[r_n,t_2^n]$ n elemenata $S^{-1}R$. Tada je

$$\varphi([r_1,s_2^n]\dots[r_n,t_2^n])=\varphi([r_1\dots r_n,s_2\dots t_2,\dots,s_n\dots t_n])=$$

$$=\varphi(r_1\dots r_n)(\varphi(s_2\dots t_2))^{n-3}\underline{\varphi(s_2\dots t_2)}\dots(\varphi(s_n\dots t_n))^{n-3}$$

$$\underline{\varphi(s_n\dots t_n)}=\varphi(r_1)(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\dots$$

$$\dots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)}\dots\varphi(r_n)(\varphi(t_2))^{n-3}\underline{\varphi(t_2)}\dots$$

$$\dots(\varphi(t_n))^{n-3}\underline{\varphi(t_n)}=\varphi([r_1,s_2^n])\dots\varphi([r_n,t_2^n])$$

pri čemu je korišćeno da je $\underline{\varphi(x_1\dots x_n)}=\underline{\varphi(x_1)}\dots\underline{\varphi(x_n)}$ što je neposredna posledica tvrdjenja 4.2 i 4.3.

Izračunajmo sada $\bar{\varphi}(\pi_s(r))$ za $r\in R$. Tada po definiciji π_s i ako (R,g) zadovoljava uslov (i) tvrdjenja 4.6 imamo

$$\bar{\varphi}(\pi_s(r))=\bar{\varphi}([rs_2\dots s_n,s_2^n])=$$

$$=\varphi(re_2\dots e_ns_2\dots s_n)(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\dots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)}=$$

$$= \varphi(r)\varphi(e_2)\ldots\varphi(e_n)\varphi(s_2)\ldots\varphi(s_n)(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\ldots$$

$$\ldots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)} = \varphi(r)\varphi(e_3)\ldots$$

$$\ldots\varphi(e_n)(\varphi(e_2)(\varphi(s_2))^{n-2}\underline{\varphi(s_2)})\ldots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)} =$$

$$= \ldots = \varphi(r)\varphi(e_2)\ldots\varphi(e_n) = \varphi(re_2\ldots e_n) = \varphi(r) \ .$$

Ako $(R,\cdot)$ zadovoljava uslov (ii), tj. $r = b_1\ldots b_{n-1}t$, $t \in S$, $b_1^{n-1} \in R$, tada je

$$\varphi(r)(\varphi(s_n))^{n-2}\underline{\varphi(s_n)} = \varphi(b_1\ldots b_{n-1}t)(\varphi(s_n))^{n-2}\underline{\varphi(s_n)} =$$

$$= \varphi(b_1)\ldots\varphi(b_{n-1})(\varphi(t)(\varphi(s_n)^{n-2}\underline{\varphi(s_n)})) = \varphi(b_1)\ldots$$

$$\ldots\varphi(b_{n-1})\varphi(t) = \varphi(b_1\ldots b_{n-1}t) = \varphi(r) \ .$$

Neka je ψ neki drugi homomorfizam $\psi : S^{-1}R \to T$ takav da je $\psi\pi_s = \varphi$. Tada za svako $s \in S$, $\psi(\pi_s(s))$ ima multiplikativan kosi element u T i tada je $\underline{\psi(\pi_s(s))} = \psi(\underline{\pi_s(s)})$.

Zamenom se lako proverava da je $x = [r,s_2^n]$ rešenje jednačine

$$x[s_2t_2\ldots t_n,t_2^n]\ldots[s_nt_2^n] = [rt_2\ldots t_n,t_2^n] \ .$$

Označimo $[s_it_2\ldots t_n,t_2^n] = u_i$ tada je po definiciji π_s, $\pi_s(s_i) = u_i$, $i=2,\ldots,n$. Ako su u_i elementi n-grupe tada je i

$$y = [rt_2\ldots t_n,t_2^n](u_2)^{n-3}\underline{u_2}\ldots(u_n)^{n-3}\underline{u_n}$$

takodje rešenje, pri čemu se za $n=3$ izostavljaju članovi $(u_i)^{n-3}$, $i=2,\ldots,n$, ako važi uslov (i) tvrdjenja 4.6 o jediničnom slogu. Naime

$$[rt_2\ldots t_n,t_2^n](u_2)^{n-3}\underline{u_2}\ldots(u_n)^{n-3}\underline{u_n}u_2\ldots u_n =$$

$$= [rt_2\ldots t_ne_2\ldots e_n,t_2e_2\ldots e_n,\ldots,t_ne_2\ldots e_n](u_2)^{n-2}\underline{u_2}\ldots$$

$$\ldots(u_n)^{n-2}\underline{u_n} = [rt_2\ldots t_n,t_2^n][\overset{n}{e_2}]\ldots[\overset{n}{e_n}](u_2)^{n-2}\underline{u_2}\ldots(u_n)^{n-2}\underline{u_n} =$$

$$= [rt_2\ldots t_n, t_2^n][e_3^n]\ldots[e_n^n]([e_2^n](u_2)^{n-2}\underline{u_2})\ldots(u_n)^{n-2}\underline{u_n} =$$

$$= \ldots = [rt_2\ldots t_n, t_2^n][e_2^n]\ldots[e_n^n] = [rt_2\ldots t_n e_2\ldots e_n, t_2 e_2\ldots e_n, \ldots$$

$$\ldots, t_n e_2\ldots e_n] = [rt_2\ldots t_n, t_2^n] .$$

Ako je zadovoljen uslov (ii) tvrdjenja 4.6 tada je $r = tb_2\ldots b_n$, $t \in S$, $b_2^n \in R$ pa je

$$[rt_2\ldots t_n, t_2^n](u_2)^{n-3}\underline{u_2}\ldots(u_n)^{n-3}u_n u_2\ldots u_n =$$

$$= [tb_2\ldots b_n t_2\ldots t_n, t_2^n](u_2)^{n-2}\underline{u_2}\ldots(u_n)^{n-2}\underline{u_n} =$$

$$= [b_2 t_2\ldots t_n, t_2^n]\ldots[b_n t_2\ldots t_n, t_2^n][tt_2\ldots t_n, t_2^n](u_2)^{n-2}\underline{u_2}\ldots$$

$$\ldots(u_n)^{n-2}\underline{u_n} = [b_2 t_2\ldots t_n, t_2^n]\ldots[b_n t_2\ldots t_n, t_2^n][tt_2\ldots t_n, t_2^n] =$$

$$= [tb_2\ldots b_n t_2\ldots t_n, t_2^n] = [rt_2\ldots t_n, t_2^n]$$

pri čemu je korišćena komutativnost i činjenica da je

$$[a_1 t_2\ldots t_n, t_2^n][a_2 t_2\ldots t_n, t_2^n]\ldots[a_n t_2\ldots t_n, t_2^n] =$$

$$= [a_1\ldots a_n (t_2)^n\ldots(t_n)^n, (t_2)^n, \ldots, (t_n)^n] =$$

$$= [a_1\ldots a_n t_2\ldots t_n, t_2^n]$$

za svako $a_1^n \in R$.

U oba slučaja imamo da je

$$[rt_2\ldots t_n, t_2^n](u_2)^{n-3}\underline{u_2}\ldots(u_n)^{n-3}\underline{u_n} = [r, s_2^n]$$

zbog kancelativnosti, jer u_2^n pripadaju n-grupi. Ako sada primenimo ψ dobijamo

$$\psi([r, s_2^n]) = \psi([rt_2\ldots t_n, t_2^n](u_2)^{n-3}\underline{u_2}\ldots(u_n)^{n-3}\underline{u_n}) =$$

$$= \psi([rt_2\ldots t_n, t_2^n])(\psi(u_2))^{n-3}\underline{\psi(u_2)}\ldots(\psi(u_n))^{n-3}\underline{\psi(u_n)} =$$

$$= \psi(\pi_s(r))(\psi(\pi_s(s_2)))^{n-3}\underline{(\psi(\pi_s(s_2)))}\ldots(\psi(\pi_s(u_n)))^{n-3}\underline{\psi(\pi_s(u_n))} =$$

$$= \varphi(r)(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\ldots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)} = \bar{\varphi}([r, s_2^n]),$$

pa je $\psi = \bar{\varphi}$, pri čemu je korišćeno da je $\psi\pi_s = \varphi$, da je $\pi_s(s_i) = u_i$, $i = 2,\ldots,n$ i definicija preslikavanja $\bar{\varphi}$.

TEOREMA 4.30. Neka je $(R,+,\cdot)$ komutativan (m,n)-prsten, a $(S,\cdot)$ i $(T,\cdot)$ n-podpolugrupe multiplikativne n-polugrupe takve da $S \subseteq T$ i da ili u S postoji jedinični slog $e_2^n \in S$ takvo da je e_2^n ujedno jedinični slog u $(R,\cdot)$, ili za svako $r \in R$ postoji $s \in S$ i $a_2^n \in R$ takvi da je $r = sa_2\ldots a_n$. Tada

(i) Postoji jednoznačno odredjen homomorfizam φ (m,n)-prstena $(S^{-1}R,+,\cdot)$ u (m,n)-prsten $(T^{-1}R,+,\cdot)$ takav da je $\pi_T = \varphi\pi_S$.

(ii) $S^{-1}T$ je n-podpolugrupa multiplikativne n-polugrupe (m,n)-prstena $(S^{-1}R,+,\cdot)$.

(iii) (m,n)-prsteni $T^{-1}R$ i $(\pi_s(T))^{-1}(S^{-1}R)$ su izomorfni.

(iv) (m,n)-prsteni $(\pi_s(T))^{-1}(S^{-1}R)$ i $(S^{-1}T)^{-1}(S^{-1}R)$ su izomorfni.

DOKAZ. Da dokažemo (i), neka su $t_2^n \in T$, $s_2^n \in S$ i kako je $S \subseteq T$, pa kao i u dokazu teoreme 4.26 sledi da ako $s \in S$ da tada

$$\pi_T(s) = [st_2\ldots t_n, t_2^n] = [ss_2\ldots s_n, s_2^n] \in S^{-1}S$$

pa kako je na osnovu teoreme 4.22. $S^{-1}S$ n-grupa to možemo da primenimo teoremu 4.29, pa postoji jednoznačni homomorfizam φ takav da je $\pi_T = \varphi\pi_S$.

Dokaz (ii) sledi nrposredno iz definicije.

Da dokažemo (iii) primetimo da se $(\pi_s(T))^{-1}(S^{-1}R)$ dobija kompozicijom homomorfizama π_s i $\pi_{\pi_s(T)}$ pošto je $\pi_s(T) = S^{-1}T$ n-podpolugrupa multiplikativne n-polugrupe $(S^{-1}R,\cdot)$ na osnovu (ii). Dakle važi

$$R \xrightarrow{\pi_s} S^{-1}R \xrightarrow{\pi_{\pi_s(T)}} (\pi_s(T))^{-1}(S^{-1}R),$$

pa $(\pi_s(T))^{-1}(S^{-1}R)$ takodje ima univerzalnu osobinu iz teoreme 4.29, tj. za svaki element $t \in T$, $\pi_{\pi_s(T)}(\pi_s(T))$ je sadržano u n-grupi.

Kako su univerzalni objekti jednoznačno odredjeni do na izomorfizam to sledi da su (m,n)-prsteni $T^{-1}R$ i $(\pi_s(T))^{-1}(S^{-1}T)$ izomorfni.

(iv) se dokazuje slično kao i (iii).

L I T E R A T U R A

[1] Alimpić B., Izotopija jedne klase kvazigrupa, Disertacija, Beograd, 1972.

[2] Белоусов В.Д., n-арные квазигруппы , Штиинца, Кишинев, 1972.

[3] Белоусов В.Д., Сандик М.Д., n-арные квазигруппы и лупы , Сиб.Мат. Жур. 7 (1966), 31-54.

[4] Bennett F.E., Self orthogonal semisymetric quasigroups, J.Comb. Theory, ser. A, 33 (1982), 117-119.

[5] Boccioni D., Caratterizzazione di una classe di anelli generalizati, Rend.Sem.Mat.Univ.Padova, 35(1965), 116-127.

[6] Boccioni D., Simmetrizzazione di una operazione n-aria, Rend.Sem.Mat.Univ. Padova, 35(1965), 82-106.

[7] Bruck R.H., A survey of binary systems, Springer Verlag, Berlin, 1958.

[8] Celakoski N., On (F,G)-rings, Год.зб.матем.фак. Скопје, 28(1977), 5-15.

[9] Celakoski N., On some axiom systems for n-groups, Билтен ДМФ СРМ Скопје, 27(1977), 5-14.

[10] Crombez G., On (n,m)-rings, Abh.Math.Sem.Univ. Hamburg, 37(1972), 180-199.

[11] Crombez G., The Post coset theorem for (n,m)-rings, Atti Inst. Veneto, 131(1972-73), 1-7.

[12] Crombez G., Timm J., On (n,m)-quotient rings, Abh.Mat. Sem.Univ. Hamburg, 37(1972), 200-203.

[13] Чупона Г., За асоцијативните конгруенции, Билтен ДМФ НРМ Скопје, 13(1962), 5-12.

[14] Чупона Г., За [m,n]-прстените, Билтен ДМФ СРМ Скопје, 16 (1965), 5-10.

[15] Чупона Г., Една класа делумни алгебри, Год.зб.прир.мат. фак. Скопје, 22(1972), 5-37.

[16] Čupona G., Vector valued semigroups, Semigroup Forum, 26(1983), 65-74.

[17] Čupona G., Dimovski D., On a class of vector valued groups Proc.Conf.Algebra and Logic, Zagreb 1984, Novi Sad, 1985, 29-37.

[18] Čupona G., Stojaković Z., Ušan J., On finite multiquasigroups, Publ.Inst.Mat. Belgrade, 29(43)(1981), 53-59.

[19] Čupona G., Ušan J., Stojaković Z., Multiquasigroups and some related Structures, MANU Contributions, I2 (1980), 5-12.

[20] Denes J., Keedwel A.D., Latin squares and their applications, Akademiai Kiado, Budapest, 1974.

[21] Dimovski D., Some existence conditions for vector valued groups, Год. зб.мат.фак. Скопје, 33-34(1982-83) 99-103.

[22] Dörnte W., Untersuchungen über einen verallgemeinerten Gruppenbegriff, Math.Zeit.,29(1928), 1-19.

[23] Dudek W.A., Autodistributive n-groups, Ann.Soc.Math. Polonae, 33(1983), 1-11.

[24] Dudek W.A., On the divisibiliti theory in (m,n)-rings, Demonstratio Math., 14(1981), 19-32.

[25] Dudek W.A., Remarks on n-groups, Demonstratio Math., 13(1980), 165-181.

[26] Dudek W.A., Glazek K., Gleichgewicht B., A note on the axioms of n-groups, Coll.Math.Soc.J.Bolyai, 29 Universal Algebra (Esztergom) 1977, 195-202.

[27] Evans T., Abstract mean value, Duke Math.J., 30(1963), 331-347.

[28] Evans T., Latin cubes orthogonal to their transposes-a ternary analogue of Stein quasigroups, Aeq.Math. 9(1973), 296-297.

[29] Hoffman D.G., On the spectrum of n-quasigroups with given conjugate invariant subgroup, J.Comb.Theory, ser A, 35(1983), 98-99.

[30]Hosszú M., On the explicit form of n-group operations, Publ.Math. Debrecen, 10(1963), 88-92.

[31] Krapež A., Prilog teoriji funkcionalnih jednačina na kvazigrupama, Disertacija, Beograd, 1980.

[32] Krstić S., Kvadratni kvazigrupni identiteti, Disertacija, Beograd 1985.

[33] Курош А.Г., Общая алгебра, лекции 1969-1970 учебного года, Наука, Москва, 1974.

[34] Leeson J.J., Butson A.T., On the general theory of (m, n)rings, Alg. Universalis, 11(1980), 42-76.

[35] Lindner C.C., Mendelsohn N.S., Construction of perpendicular Steiner quasigroups, Aeq.Math., 9(1973), 150-156.

[36] Mendelsohn N.S., A natural generalization of Steiner triple systems, In Computer in Number Theory (Proc.Sci.Res.Council Atlas Sympos. No.2, Oxford, 1969), Academic Press, London, 1971, 323-338.

[37] Mendelsohn N.S., Orthogonal Steiner systems, Aeq. Math. 5(1970), 268-272.

[38] Milić S., Prilog teoriji kvazigrupa, Disertacija, Beograd 1971.

[39] Milić S., On GD-groups with application to n-ary quasigroups, Publ.Inst.Math.Belgrade, 13(27)(1972), 65-76.

[40] Monk J.D., Sioson F.M., On the general theory of m-groups, Fund. Math., 72(1971), 233-244.

[41] Одобеску С.С., Изотопия мультиопераций, Ислед. по теор. квазигрупп и луп, Штиинца, Кишинев, 1973, 127-132.

[42] Paunić Dj., Localization in (m,n)-rings, Proc.Conf. Algebra and Logic Zagreb, 1984, Novi Sad, 1985, 123-133.

[43] Paunić Dj., Stojaković Z., Parastrophy invariant n-quasigroups, Univ. u Novom Sadu, Zbornik radova Prir.-mat. fak. ser.mat., 13(1983), 251-257.

[44] Polonio M., Medial multiquasigroups, MANU Contributions, III2 (1982), 31-41.

[45] Polonio M., On C^{n+1}-systems and [m,n]-groups, Proc. Thirs Alg. Conf. Belgrade 1982, 111-116.

[46] Post E., Polyadic groups, Trans.Am.Math.Soc., 48(1940), 208-350.

[47] Radó F., On semi-symmetric quasigroups, Aeq.Math., 11 (1974), 250-255.

[48] Sade A., Critéres d'isotopie d'un quasigroupe avec un quasigroupe demi-symétrique, Univ.Lisabon Revista Fac.Ci.Lisaboa 11(1964), 121-136.

[49] Sade A., Quasigroups demi-symetriques, Ann.Soc.Sci. Bruxelles, 79(1965), 133-143.

[50] Сандик М.Д., Обратимые мультиопераций и подстановки, Acta.Sci.Math., 39(1977), 153-162.

[51] Сандик М.Д., Соколов Е.И., Тотально-симметричные n-квазигруппы, Мат. исследования, Кишинев, Том III, вып. 2, 1968, 170-182.

[52] Schweizer B., Sklar A., The algebra of multiplace vector-valued functions, Bull.Am.Math.Soc., 73 (1967), 510-515.

[53] Соколов Е.И., О теореме Глускина-Хоссу для n-групп Дернте, Мат.Исследования, вып. 39(1976),187-189.

[54] Steedly D., Separable quasigroups, Aeq.Math. 11(1974), 189-195.

[55] Stojaković Z., A generalization of Mendelsohn triple systems, Ars. Combinatoria, 18(1984), 131-138.

[56] Stojaković Z., Alternating symmetric n-quasigroups, Univ. u Novom Sadu, Zbornik radova Prir.-mat. fak., ser.mat., 13(1983), 259-272.

[57] Stojaković Z., Cyclic n-quasigroups, Univ. u Novom Sadu, Zbornik radova Prir.-mat.fak., ser.mat., 12(1982), 407-415.

[58] Stojaković Z., On a class of bisymmetric [n,m]-grupoids, Proc.Third alg.conf. Belgrade 1982, 139-143.

[59] Stojaković Z., On bisymmetric [n,m]-grupoids, Univ. u Novom Sadu, Zbornik radova Prir.-mat.fak., ser. mat., 12(1982), 399-405.

[60] Stojaković Z., Dudek W.A., Permutable n-grupoids, Univ. u Novom Sadu, Zbornik radova Prir.-mat.fak., ser., mat., 14/2(1984), 155-166.

[61] Stojaković Z., Dudek W.A., On σ-permutable n-grupoids, Univ. u Novom Sadu, Zbornik radova Prir.-mat.fak., ser.mat., 15/1(1985), 189-198.

[62] Stojaković Z., Dudek W.A., On σ-permutable n-groups, Publ.Inst.Math., Belgrade, 40(54)(1986), 49-55.

[63] Stojaković Z., Madaras R., On tetrahedral quadruple systems, Utilitas math., 29(1986), 19-26.

[64] Stojaković Z., Paunić Dj., Identities on multiquasigroups, Proc.Symp. n-ary Structures, Skopje 1982, 195-200.

[65] Stojaković Z., Paunić Dj., Nonlinear multiquasigroups, Univ. u Novom Sadu, Zbornik radova Prir.-mat. fak., ser.mat., 10(1980), 145-148.

[66] Stojaković Z., Paunić Dj., On a class of n-grups, Univ. u Novom Sadu, Zbornik radova Prir.-mat.fak., ser.mat., 14/2(1984), 147-154.

[67] Stojaković Z., Paunić Dj., Self-orthogonal cyclic n-quasigroups, Aeq.Math., 30(1986), 252-257.

[68] Стојменовски К., За [m,n]-квазигрупите, Год. зб. Мат. фак. Скопје, 28(1978), 33-37.

[69] Toyoda K., On axioms of linear functions, Proc.Imp. Acad. Tokyo, 17(1941), 221-227.

[70] Трпеновски Б., Чупона Г., [m,n]-групоиди, Билтен ДМФ СРМ Скопје, 22(1972), 5-37.

[71] Ушан Я., Одно определение группы и его обобщение на n-арний случай, Матем.Вестн., 5(1968), 145-149.

[72] Ушан Я., Ассоциативные в целом системы n-арных квазигрупп, Publ.Inst.Math.Belgrade, 17(31)(1974), 173-182.

[73] Ušan J., Uvod v teorija kvazigrup, I del. DMFA SR Slovenije, Ljubljana, 1986.