Dragan Blagojević

STRUKTURA NEKIH KLASA REGULARNIH POLUGRUPA

(doktorska disertacija)

Beograd, 1987

Temu ove disertacije prijavio sam 5. juna 1985. godine Institutu za matematiku OOUR-a za matematiku, mehaniku i astronomiju Prirodno-matematičkog fakulteta u Beogradu.

Na sednici Instituta od 12. septembra 1985. godine, na osnovu izveštaja odgovarajuće komisije, ova tema je prihvaćena, a za rukovodioca pri izradi disertacije određen mi je dr Svetozar Milić.

Disertaciju sam završio i predao krajem aprila 1987. godine.

Zahvaljujem se profesoru dr Svetozaru Miliću na savesnom rukovođenju izradom ove disertacije.

SADRŽAJ

UVOD

Teorija polugrupa je relativno mlada matematička disciplina. Smatra se da je nastala 1928. godine, kada je ruski matematičar Suškevič objavio svoj rad [59] o konačnim prostim polugrupama. Iako su to bili zanimljivi i značajni rezultati, rad nije imao većeg odjeka jer je bio prezentiran u prilično neudobnom obliku. Strukturu jedne šire klase polugrupa od Suškevičevih - klase prostih polugrupa sa primitivnim idempotentima - opisao je Rees 1940. godine u [56] uvodeći pojam matrice nad grupom sa nulom. Odmah zatim 1941. godine Clifford je objavio svoj rad [14] o polumrežnim dekompozicijama nekih klasa polugrupa. Od tog trenutka teorija polugrupa je počela snažno da se razvija. Sledeći značajan impuls razvoju teorije došao je početkom pedesetih godina, kada su, po ugledu na sličnu von Neumannovu [47] definiciju za prstenove, uvedeni pomovi regularnog elementa, odnosno uzajamno inverznih elemenata. Uopšte, prva istraživanja u teoriji polugrupa i prvi značajniji rezultati bili su u velikoj meri motivisani odgovarajućim rezultatima iz tada već dobro razvijenih teorija grupa i prstenova. Kasnije je teorija polugrupa nastavila da se razvija svojim putevima, i sve je teže bilo uspostaviti neku vezu sa grupama i prstenovima. Razlog tome je neophodnost proučavanja kongruencija (Howie [37, predgovor]). U grupi je kongruencija određena ako znamo bar jednu klasu, posebno ako znamo normalnu podgrupu, koja je klasa jedinice. Slično, u prstenovima kongruencija je određena ako znamo ideal koji je kongruencijska klasa nule. U polugrupama uglavnom nema tako srećnih okolnosti. Opisane su kongruencije nekih relativno uskih klasa polugrupa, a tek pre nekoliko godina i kongruencije inverznih i regularnih polugrupa. U oba slučaja je opis prilično složen i sa više parametara. U klasama polugrupa koje nisu regularne nemamo ni toliko. Uopšte, regularne polugrupe su ona klasa polugrupa koja je predstavljala najplodniji teren za istraživanja. Ta klasa je dovoljno široka i dovoljno zanimljiva, tako da su detaljno ispitane njene mnogobrojne potklase. Osnovni instrumenti za ispitivanje strukture svih polugrupa su Greenove ekvivalencije.

Rezultati koji se tiču regularnih polugrupa ne samo da su najmnogobrojniji, nego su i najznačajniji. Iako poslednjih godina pažnju istraživača sve više privlače i druge klase pougrupa, još uvek su regularne polugrupe najzanimljivije.

Stranice koje slede takođe su posvećene istraživanjima strukture nekih klasa regularnih polugrupa. U preliminarnom - nultom odeljku navedeni su neki osnovni pojmovi i rezultati sa ciljem da se da opšta slika dostignuća u toj oblasti teorije polugrupa i da se formuliše neophodni osnovni materijal za dalje izlaganje. To su rezultati za koje bi se već moglo reći da su klasični i dobro poznati. Zato za njih uglavnom i nije navedena referencija ili čak i nisu eksplicitno formulisani u obliku teorema, nego su često samo uzgred pomenuti. Naravno, bilo je nemoguće obuhvatiti sve rezultate kiji su relevantni, jer bi to zahtevalo mnogo više prostora.

Ako se prilikom ispitivanja neke klase polugrupa zaključi da su one unije grupa, tu se obično staje i ne ulazi se u strukturu podgrupa. U ovom radu biće prezentirani rezultati u kojima će se u istraživanju strukture polugrupa ulaziti i u strukturu podgrupa.

U odeljku 1 detaljno je opisana struktura unija diedarskih grupa. Ideju za ovo istraživanje dao mi je profesor dr Svetozar Milić, na čemu mu se najtoplije zahvaljujem. Jednom jednostavnom formulom okarekterisane su unije diedarskih grupa. Posmatranjem jedne lokalne osobine njihovih $\mathcal{H}$-klasa dobijene su trake i Booleove grupe kao ekstremni slučajevi polugrupa sa tom osobinom. Data je efektivna konstrukcija koja pokazuje da $\mathcal{H}$-klase mogu biti dovoljno složene, bar toliko koliko su to komutativne grupe.

Odeljak 2 posvećen je anti-inverznim polugrupama (Sharp [58]) koje su opisali Bogdanović, Milić, Pavlović [12] i Bogdanović [10] karakterišući ih na više načina. Karakterizacija koju dajemo teoremom 2.4 je najpreciznija, i razne druge karakterizacije iz [10], [12], [58] mogu se dobiti kao neposredne posledice (npr. posledice 2.6 i 2.8 i tvrđenja 2.11 i 2.12). Lema 2.3 i posledica 2.7 ovde se pojavljuju prvi put. Materijal koji je izložen u ovom kratkom odeljku služi, uglavnom, kao uvodni za sledeći odeljak, a izdvojen je posebno da bi se istakao paralelizam anti-inverznih polugrupa i unija diedarskih grupa.

Milić, Bogdanović [44] uopštavali su jednu formulu koja karakteriše anti-inverzne polugrupe i ispitivali su slučajeve kada to uopštenje nije pravo. U odeljku 3 taj problem je potpuno rešen i za njihovo uopštenje i za uopštenje koje se može naći u Crvenković [22] .

Odeljak 4 posvećen je traženju anti-inverzne unije diedarskih grupa koja nije Booleova. Pokazano je da najmanja takva polugrupa je grupa sa 32 elementa i detaljno je opisana. Date su ukratko i neke osobine Booleovih polugrupa.

U poslednjem odeljku opisana je struktura slobodne regularne ortokriptogrupe i data je njena konstrukcija u obliku uređenih trojki. To je učinjeno i za opšti slučaj i za slučajeve kad su maksimalne podgrupe iz nekog varijeteta komutativnih grupa. U slučajevima kad je takva polugrupa konačna, dat je broj njenih elemenata u zavisnosti od broja elemenata generatornog skupa.

Većina prezentiranih rezultata iz ove disertacije već je publikovana i to rezultati iz odeljaka 1 i 4 u Blagojević [08] , rezultati iz odeljka 3 i deo iz odeljka 2 u Blagojević [07] , a rezultati iz odeljka 5 u Blagojević, Krapež [09] .

O. OSNOVNI POJMOVI I REZULTATI

Polugrupa je neprazan skup na kome je definisana binarna operacija koja zadovoljava asocijativni zakon

$$(xy)z = x(yz).$$

Ako polugrupa S ima jedinicu 1 zove se monoid i piše se $S = S^1$, a ako nema onda se sa S^1 obeležava polugrupa $S \cup \{1\}$, gde je 1 naknadno dodata jedinica. Slično, sa S^0 označavamo polugrupu sa (eventualno dodatom) nulom. Element e polugrupe S je idempotent ako zadovoljava $e^2 = e$. Ako je A podskup od S onda sa E_A označavamo skup svih idempotenata iz A. Taj skup se može urediti na sledeći način:

(0.1) $\qquad e = f$ ako i samo ako $ef = e = fe$.

Neprazan podskup I polugrupe S je levi ideal od S ako $SI \subseteq I$. Dualno se definiše desni ideal od S. Podskup I je dvostrani ideal (ili samo ideal) ako je levi i desni ideal. Levi (desni, dvostrani) ideal I je pravi ako $I \neq S$. Potpolugrupa B polugrupe S je bi-ideal ((m,n)-ideal) ako je $BSB \subseteq B$ ($B^mSB^n \subseteq B$). Sa $L(a)$, $R(a)$, $J(a)$ označimo glavni levi, desni, dvostrani ideal generisan elementom a; tada je

$$L(a) = S^1a, \quad R(a) = aS^1, \quad J(a) = S^1aS^1.$$

Na polugrupi S definišemo relacije $\mathcal{L}$, $\mathcal{R}$, $\mathcal{J}$ na sledeći način:

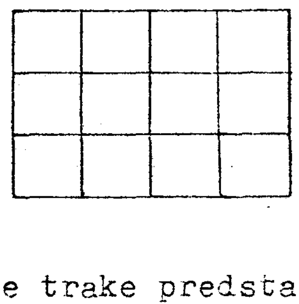
$$a\mathcal{L}b \Leftrightarrow L(a)=L(b),$$
$$a\mathcal{R}b \Leftrightarrow R(a)=R(b),$$
$$a\mathcal{J}b \Leftrightarrow J(a)=J(b).$$

Relacije $\mathcal{L}$, $\mathcal{R}$, $\mathcal{J}$ su ekvivalencije i zovu se Greenove ekvivalencije (relacije). Dokazuje se da ekvivalencije $\mathcal{L}$ i $\mathcal{R}$ komutiraju: $\mathcal{L}\mathcal{R}=\mathcal{R}\mathcal{L}$, što znači da je $\mathcal{R}\mathcal{L}$ takođe relacija ekvivalencije, u oznaci $\mathcal{D}$. Ekvivalencija $\mathcal{D}$ i ekvivalencija $\mathcal{H}=\mathcal{R}\cap\mathcal{L}$ se takođe zovu Greenove ekvivalencije. Navedenih pet ekvivalencija igraju fundamentalnu ulogu u ispitivanju strukture polugrupa. Uveo ih je Green [30].

Sa R_a označićemo klasu ekvivalencije elementa a u odnosu na ekvivalenciju $\mathcal{R}$. Slično definišemo L_a, J_a, D_a, H_a. Za Greenove ekvivalencije važe sledeći odnosi:

$$\mathcal{H}\subseteq \begin{matrix}\mathcal{R}\\ \mathcal{L}\end{matrix} \subseteq\mathcal{D}\subseteq\mathcal{J}.$$

Definicija ekvivalencije $\mathcal{D}$ omogućava da se $\mathcal{D}$-klase zgodno prikažu na sledeći način:



pri čemu horizontalne trake predstavljaju $\mathcal{R}$-klase, vertikalne trake $\mathcal{L}$-klase, a "ćelije" $\mathcal{H}$-klase. Gornja slika može da bude beskonačna po horizontali ili po vertikali, a može i da se redukuje samo na jednu "ćeliju". Dokazuje se da su sve $\mathcal{H}$-klase u okviru iste $\mathcal{D}$-klase istobrojne. To važi i za $\mathcal{R}$-klase i $\mathcal{L}$-klase.

Element a polugrupe S je regularan ako $a = aba$, $b = bab$, za neko b iz S. Tada kažemo da su a i b jedan drugom inverzi. Regularnost je osobina koja se vezuje za $\mathcal{D}$-klase. Naime, u jednoj $\mathcal{D}$-klasi ili su svi elementi regularni ili nije nijedan, pa možemo govoriti o regularnoj $\mathcal{D}$-klasi. Svaka $\mathcal{R}$-klasa i svaka $\mathcal{L}$-klasa regularne $\mathcal{D}$-klase obavezno sadrže idempotent koji funkcioniše kao leva jedinica u svojoj $\mathcal{R}$-klasi, odnosno kao desna jedinica u svojoj $\mathcal{L}$-klasi. One $\mathcal{H}$-klase koje sadrže idempotent su podgrupe, i to maksimalne podgrupe polugrupe. Sve maksimalne podgrupe u istoj $\mathcal{D}$-klasi su izomorfne. Struktura regularnih $\mathcal{D}$-klasa detaljnije je opisana sledećim lemama (Miller, Clifford [45]).

(0.2) LEMA. <u>Za svaka dva elementa</u> a <u>i</u> b <u>polugrupe</u> S <u>važi</u> $ab \in R_a \cap L_b$ <u>ako i samo ako</u> $R_b \cap L_a$ <u>sadrži idempotent</u>. <u>U tom slučaju je</u>

$$aH_b = H_a b = H_a H_b = H_{ab} = R_a \cap L_b .$$

(0.3) LEMA. <u>Neka su</u> a <u>i</u> b <u>elementi regularne</u> $\mathcal{D}$-<u>klase</u> D <u>polugrupe</u> S. <u>Tada</u>:

(a) <u>ako je</u> a' <u>inverz od</u> a, <u>onda</u> $a' \in \mathcal{D}$ <u>i idempotenti</u> aa' <u>i</u> $a'a$ <u>leže u</u> $\mathcal{H}$-<u>klasama</u> $R_a \cap L_{a'}$, <u>odnosno</u> $R_{a'} \cap L_a$;

(b) <u>ako su</u> e <u>i</u> f <u>idempotenti polugrupe</u> S, <u>onda svaki element</u> a <u>iz</u> $R_e \cap L_f$ <u>ima jedinstven inverz</u> a' <u>u</u> $R_f \cap L_e$ <u>i pri tome je</u> $aa' = e$ <u>i</u> $a'a = f$;

(c) <u>svaka</u> $\mathcal{H}$-<u>klasa polugrupe</u> S <u>sadrži najviše jedan inverz od</u> a.

Ako znamo koje $\mathcal{H}$-klase regularne $\mathcal{D}$-klase sadrže idempotente, onda za svaki element te $\mathcal{D}$-klase lako možemo da nađemo sve njegove inverze, koristeći gornje leme i koordinatizaciju $\mathcal{D}$-klase.

Polugrupa bez nule i bez pravih ideala je prosta. Polugrupa S sa nulom je 0-prosta ako joj je $\{0\}$ jedini pravi ideal i $S^2 \neq \{0\}$. Dodavanjem nule prostoj polugrupi dobijamo 0-prostu polugrupu (bez delitelja nule), ali se sve 0-proste polugrupe ne mogu dobiti na ovaj način. Međutim, navedena činjenica omogućuje da se niz rezultata za proste polugrupe dobije kao neposredna posledica odgovarajućih rezultata za 0-proste polugrupe.

Ako polugrupa bez nule ima minimalni ideal (u odnosu na skupovnu inkluziju), onda je on jedinstven i zove se jezgro polugrupe. Jezgro je prosta polugrupa, ako je netrivijalno. Primetimo da 0-prosta polugrupa uvek ima najmanji ideal $\{0\}$.

Idempotent polugrupe je primitivan ako je minimalan u parcijalno uređenom skupu (u odnosu na prirodno uređenje definisano sa (0.1)) svih ne-nula idempotenata. Polugrupa je kompletno 0-prosta ako je 0-prosta i sadrži minimalni idempotent. Važi sledeća teorema:

(0.4) TEOREMA. *Neka je* S *kompletno* 0-*prosta polugrupa. Tada važi*:

(a) S *je regularna*;

(b) $S-\{0\}$ *je* $\mathcal{D}$-*klasa polugrupe* S;

(c) *ako* $a,b \in S$, *onda* $ab=0$ *ili* $ab \in R_a \cap L_b$.

Kad se primeni na proste polugrupe, prethodna teorema daje sledeću posledicu.

(0.5) POSLEDICA. Neka je S kompletno prosta polugrupa. Tada važi:

(a) S je regularna;

(b) S je $\mathcal{D}$-klasa;

(c) ako $a,b \in S$, onda $ab \in R_a \cap L_b$.

Gornja teorema i njena posledica opisuju kompletno (0-) proste polugrupe. Međutim, njihov potpuni opis dat je sledećom konstrukcijom, koja potiče od Reesa [56].

Ako grupi G dodamo nulu, dobićemo grupu sa nulom G^0.

(0.6) Konstrukcija. Neka je G^0 grupa sa nulom, I i M neprazni skupovi i $P: M \times I \to G^0$ funkcija koja zadovoljava sledeći uslov: za svako $\mu \in M$ $(i \in I)$ postoji $i \in I$ $(\mu \in M)$ tako da je $p_{\mu i} \neq 0$, gde je $p_{\mu i}$ oznaka za $p(\mu,i)$. Na skupu $S = (I \times G \times M) \cup \{0\}$, pri čemu $0 \notin I \times G \times M$, definišemo množenje na sledeći način:

$$(i,g,\mu)(j,h,\nu) = \begin{cases} (i,gp_{\mu j}h,\nu), & \text{ako } p_{\mu j} \neq 0 \\ 0, & \text{inače} \end{cases}$$

i neka 0 funkcioniše kao nula u S.

Proverava se da je ovako definisano množenje asocijativno. Dobijena polugrupa se obeležava sa $\mathcal{M}^0(I,G,M;P)$ i zove se Reesova matrična polugrupa nad grupom sa nulom G^0 i sa sendvič-matricom P, ili samo Reesova matrična polugrupa.

Zgodno je funkciju P zamišljati kao matricu tipa

$M \times I$ nad G^0 takvu da u svakoj vrsti i u svakoj koloni ima bar jedan element iz G. Element (i,g,μ) onda treba zamišljati kao matricu tipa $I \times M$ koja na mestu $i\mu$ ima element g iz G, a sve ostalo su nule. Onda je jasno da se množenje dve takve matrice realizuje na uobičajeni način uz posredovanje matrice P.

Važi sledeća teorema (Rees [56]).

(0.7) TEOREMA. Polugrupa je kompletno (0-) prosta ako i samo ako je izomorfna Reesovoj matričnoj polugrupi nad grupom (sa nulom).

U Reesovoj matričnoj polugrupi važi:

$$(i,g,\mu)\mathcal{R}(j,h,\nu) \iff i=j,$$
$$(i,g,\mu)\mathcal{L}(j,h,\nu) \iff \mu=\nu.$$

Dokazuje se da su u kompletno 0-prostoj polugrupi svi ne-nula idempotenti primitivni, tj. da među njima nema uporedivih. Regularna polugrupa sa nulom u kojoj su svi ne-nula idempotenti primitivni ne mora da bude kompletno 0-prosta, ali se dobija uniranjem kompletno 0-prostih, uz identifikovanje svih nula. Da preciziramo, neka je $\{S^0_\alpha, \alpha\in A\}$ neprazna familija polugrupa, svaka sa nulom. Na skupu $S = \bigcup_{\alpha\in A} S^0_\alpha$ identifikujmo sve nule sa 0 i definišimo proizvod dva elementa da bude kao u S_α, ako su oba iz S_α, inače neka bude 0. Tako dobijena polugrupa S zove se ortogonalna suma polugrupa S_α, $\alpha\in A$. Dokazuje se da su u regularnoj polugrupi S^0 sa nulom svi idempotenti primitivni ako i samo ako je S^0 ortogonalna suma kompletno O-prostih polugrupa.

Polugrupa čiji su svi elementi idempotenti zove se traka. Komutativna traka se zove polumreža. Antikomutativna traka, tj. traka koja zadovoljava $xy = yx \Rightarrow x = y$ zove se pravougaona traka. U njoj važi jednakost $x = xyx$, odakle sledi da je svako svakome inverz.

Pored konstrukcije Reesove matrične polugrupe, druga važna konstrukcija u teoriji polugrupa je polumreža polugrupa. Ova konstrukcija se zasniva na činjenici da ako je $\varphi : S \to Y$ homomorfizam polugrupe S na polumrežu Y, onda je $\alpha\varphi^{-1}$ potpolugrupa od S, za svako $\alpha \in Y$. Tada je polugrupa S unija disjunktnih potpolugrupa $S_\alpha = \alpha\varphi^{-1}$ i $S_\alpha S_\beta \subseteq S_{\alpha\beta}$, gde je $\alpha\beta$ proizvod u polumreži Y. Ako su pri tome polugrupe S_α jednostavnije od S, onda imamo motivaciju za sledeću konstrukciju.

(O.8) <u>Konstrukcija</u>. Neka je Y polumreža i neka je $\{S_\alpha : \alpha \in Y\}$ familija disjunktnih polugrupa tipa T indeksiranih elementima iz Y. Za svaki par elemenata α, β iz Y za koje je $\alpha \geq \beta$, neka je $\varphi_{\alpha,\beta} : S_\alpha \to S_\beta$ homomorfizam i neka su pri tome ispunjeni sledeći uslovi: (a) $\varphi_{\alpha,\alpha}$ je identički homomorfizam za svako $\alpha \in Y$; (b) ako su α, β, γ iz Y i $\alpha \geq \beta \geq \gamma$, onda $\varphi_{\alpha,\beta}\varphi_{\beta,\gamma} = \varphi_{\alpha,\gamma}$. Neka je $S = \cup\{S_\alpha : \alpha \in Y\}$. U skupu S definišimo operaciju na sledeći način: ako $a_\alpha \in S_\alpha$ i $b_\beta \in S_\beta$, onda $a_\alpha b_\beta = (a_\alpha \varphi_{\alpha,\alpha\beta})(b_\beta \varphi_{\beta,\alpha\beta})$. Ovako definisana operacija je asocijativna, pa je S polugrupa, u oznaci $S = \mathcal{S}(Y, S_\alpha, \varphi_{\alpha,\beta})$, i zove se jaka polumreža polugrupa tipa T. U sledećoj teoremi pojavljuje se ova konstrukcija.

(0.9) TEOREMA. Za polugrupu S sledeći uslovi su ekvivalentni:

(a) S je regularna polugrupa sa centralnim idempotentima (idempotenti komutiraju sa svakim elementom polugrupe);

(b) S je regularna polugrupa u kojoj je $\mathcal{D} = \mathcal{H}$;

(c) S je polumreža grupa;

(d) S je jaka polumreža grupa.

Ovakve polugrupe su dobile ime po osobini (c).

Svaka polumreža polugrupa ne mora da bude jaka. Struktura kompletno regularnih polugrupa - polugrupa kod kojih svaki element komutira sa nekim od svojih inverza - opisana je sledećom teoremom.

(0.10) TEOREMA. Za polugrupu S sledeći uslovi su ekvivalentni:

(a) S je kompletno regularna;

(b) svaka $\mathcal{J}$-klasa od S je kompletno prosta polugrupa;

(c) S je polumreža kompletno prostih polugrupa;

(d) svaka $\mathcal{H}$-klasa od S je grupa.

Polugrupe koje zadovoljavaju uslove ove teoreme zovu se, na osnovu osobine (d), unije grupa. Kako su kompletno proste polugrupe izomorfne Reesovim matričnim polugrupama nad grupama, uslov (c) se može zameniti uslovom:

(c′) S je polumreža Reesovih matričnih polugrupa nad grupama.

Kako je svaka traka unija trivijalnih grupa, a lako se dokazuje da je traka kompletno prosta ako i samo ako je pravougaona, pa ako prethodnu teoremu primenimo na trake, dobićemo sledeću posledicu.

(0.11) POSLEDICA. *Svaka traka je polumreža pravougaonih traka*.

Polugrupa koja zadovoljava jednakost $xyzx = xzyx$ zove se medijalna. Normalna traka je traka koja je medijalna. Važi sledeća teorema.

(0.12) TEOREMA. *Za polugrupu S sledeći uslovi su ekvivalentni*:

(a) *S je regularna i subdirektni proizvod kompletno prostih polugrupa sa eventualno dodatom nulom*;

(b) *S je normalna traka grupa*;

(c) *S je jaka polumreža kompletno prostih polugrupa*.

Ako ovu teoremu primenimo na trake dobićemo sledeću posledicu.

(0.13) POSLEDICA. *Za polugrupu S sledeći uslovi su ekvivalentni*:

(a) *S je normalna traka*;

(b) *S je jaka polumreža pravougaonih traka*;

(c) *S je subdirektni proizvod pravougaonih traka sa eventualno dodatom nulom*.

Polugrupa je levo (desno) komutativna ako zadovoljava jednakost $xyz = yxz$ $(xyz = xzy)$. Levo (desno) normalna traka je traka koja je levo (desno) komutativna. Dokazuje se da je normalna traka subdirektni priozvod levo normalne i desno normalne trake.

Naveli smo nekoliko rezultata u kojima se pojavljuju jake polumreže nekih polugrupa. Sada ćemo opisati opšti izgled polumreža polugrupa. Za to su nam prethodno potrebni još neki pojmovi.

Neka je S polugrupa i $x,y \in S$. Funkcija λ (ρ) na S zove se leva (desna) translacija ako $\lambda(xy) = (\lambda x)y$ $((xy)\rho = x(y\rho))$[+]. Ako je $x(\lambda y) = (x\rho)y$, onda kažemo da su λ i ρ povezani, a par (λ,ρ) zovemo bitranslacija od S. Skup svih bitranslacija polugrupe S zove se omotač translacija od S, u oznaci $\Omega(S)$, i on je polugrupa u odnosu na koordinatno množenje: $(\lambda,\rho)(\lambda',\rho') = (\lambda\lambda',\rho\rho')$. Leva (desna) translacija λ_s (ρ_s) definisana sa $\lambda_s x = sx$ $(x\rho_s = xs)$ je unutrašnja, a par $(\lambda_s,\rho_s) = \pi_s$ je unutrašnja bitranslacija. Potpolugrupa $\Pi(S) = \{\pi_s : s \in S\}$ je unutrašnji deo od $\Omega(S)$. Proverava se da je preslikavanje $\pi : s \mapsto \pi_s$ homomorfizam, a zove se kanonički, iz polugrupe S na $\Pi(S)$. Polugrupa je slabo reduktivna ako joj je kanonički homomorfizam injektivan.

Sada možemo da damo precizniji opis polumreže slabo reduktivnih polugrupa.

[+] Iz tehničkih razloga operator λ se piše sa leve, a operator ρ sa desne strane argumenta.

(0.14) TEOREMA. Neka je Y polumreža; svakom $\alpha \in Y$ pridružimo jednu slabo reduktivnu polugrupu S_α i pretpostavimo da je $S_\alpha \cap S_\beta = \emptyset$ ako je $\alpha \neq \beta$. Za α, β iz Y i $\alpha \geq \beta$ neka je $\chi_{\alpha,\beta}: S_\alpha \to \Omega(S_\beta)$ funkcija takva da su ispunjeni sledeći uslovi:

(a) $a\chi_{\alpha,\alpha} = \pi_a$, $(a \in S_\alpha)$;

(b) $(S_\alpha \chi_{\alpha,\alpha\beta})(S_\beta \chi_{\alpha,\alpha\beta}) \subseteq \Pi(S_{\alpha\beta})$;

(c) ako je $\alpha\beta > \gamma$, $a \in S_\alpha$, $b \in S_\beta$ onda

$$[(a\chi_{\alpha,\alpha\beta})(b\chi_{\beta,\alpha\beta})]\chi^{-1}_{\alpha\beta,\alpha\beta}\chi_{\alpha\beta,\gamma} = (a\chi_{\alpha,\gamma})(b\chi_{\beta,\gamma}).$$

U skupu $S = \cup\{S_\alpha : \alpha \in Y\}$ definišimo operaciju $*$ na sledeći način:

$$a * b = [(a\chi_{\alpha,\alpha\beta})(b\chi_{\beta,\alpha\beta})]\chi^{-1}_{\alpha\beta,\alpha\beta}, \text{ ako } a \in S_\alpha,\ b \in S_\beta.$$

Tada je S polumreža Y polugrupa S_α, $\alpha \in Y$. Obrnuto, svaka polumreža slabo reduktivnih polugrupa $\{S_\alpha : \alpha \in Y\}$ može ovako da se konstruiše.

Koristeći ovaj rezultat i opis omotača tanslacija kompletno proste polugrupe, može se dati potpuno precizan opis strukture kompletno regularne polugrupe, preko tzv. standardne reprezentacije, a kao posledica dobija se opis strukture traka. Regularna polugrupa kod koje idempotenti čine potpolugrupu zove se ortodoksna. Važi sledeća teorema.

(0.15) TEOREMA. Za regularnu polugrupu S sledeći uslovi su ekvivalentni:

(a) S je ortodoksna;

(b) ako je x' inverz od x i y' inverz od y, onda je $y'x'$ inverz od xy;

(c) inverz idempotenta je i sam idempotent;

(d) ako dva elementa iz S imaju zajednički inverz, onda su im svi inverzi zajednički.

Ortodoksna kompletno regularna polugrupa zove se ortogrupa. Za ortogrupe postoji više teorema strukture. Navodimo jednu od njih.

(0.16) TEOREMA. Neka je $E=(Y,E_\alpha)$ traka i $G=(Y,G_\alpha)$ polumreža grupa. Za svako $g,h\in G$ neka postoji funkcija

$$\delta_{(g,h)}\colon E_\alpha\times E_\beta\to E_{\alpha\beta},\ \text{gde je}\ g\in G_\alpha,\ h\in G_\beta,$$

pri čemu su ispunjeni uslovi:

(a) $\delta_{(g_1g_2,g_3)}(\delta_{(g_1,g_2)}(e_1,e_2),e_3)=\delta_{(g_1,g_2g_3)}(e_1,\delta_{(g_2,g_3)}(e_2,e_3))$;

(b) $\delta_{(1_\alpha,1_\beta)}(e,f)=ef,\quad e\in E_\alpha,\ f\in E_\beta$;

(c) $\delta_{(g,h)}(e,e)=e,\quad g,h\in G_\alpha,\ e\in E_\alpha$.

U skupu $S=\cup\{E_\alpha\times G_\alpha\colon \alpha\in Y\}$ definišimo operaciju $*$ na sledeći način:

$$(e,g)*(f,h)=(\delta_{(g,h)}(e,f),\ gh).$$

Tada je S ortogrupa, $E_S\cong E$, $G_{(e,1_\alpha)}=G_\alpha$ za sve α iz Y i e iz E_α. Obrnuto, svaka ortogrupa je izomorfna nekoj ovako konstruisanoj ortogrupi.

Kriptična polugrupa je ona polugrupa kod koje je relacija $\mathcal{H}$ kongruencija. Kriptogrupa je kompletno regularna kriptična polugrupa. Ako je uz to još i ortodoksna, onda se zove ortokriptogrupa. Uz iste oznake kao u prethodnoj teoremi može se dokazati sledeća teorema.

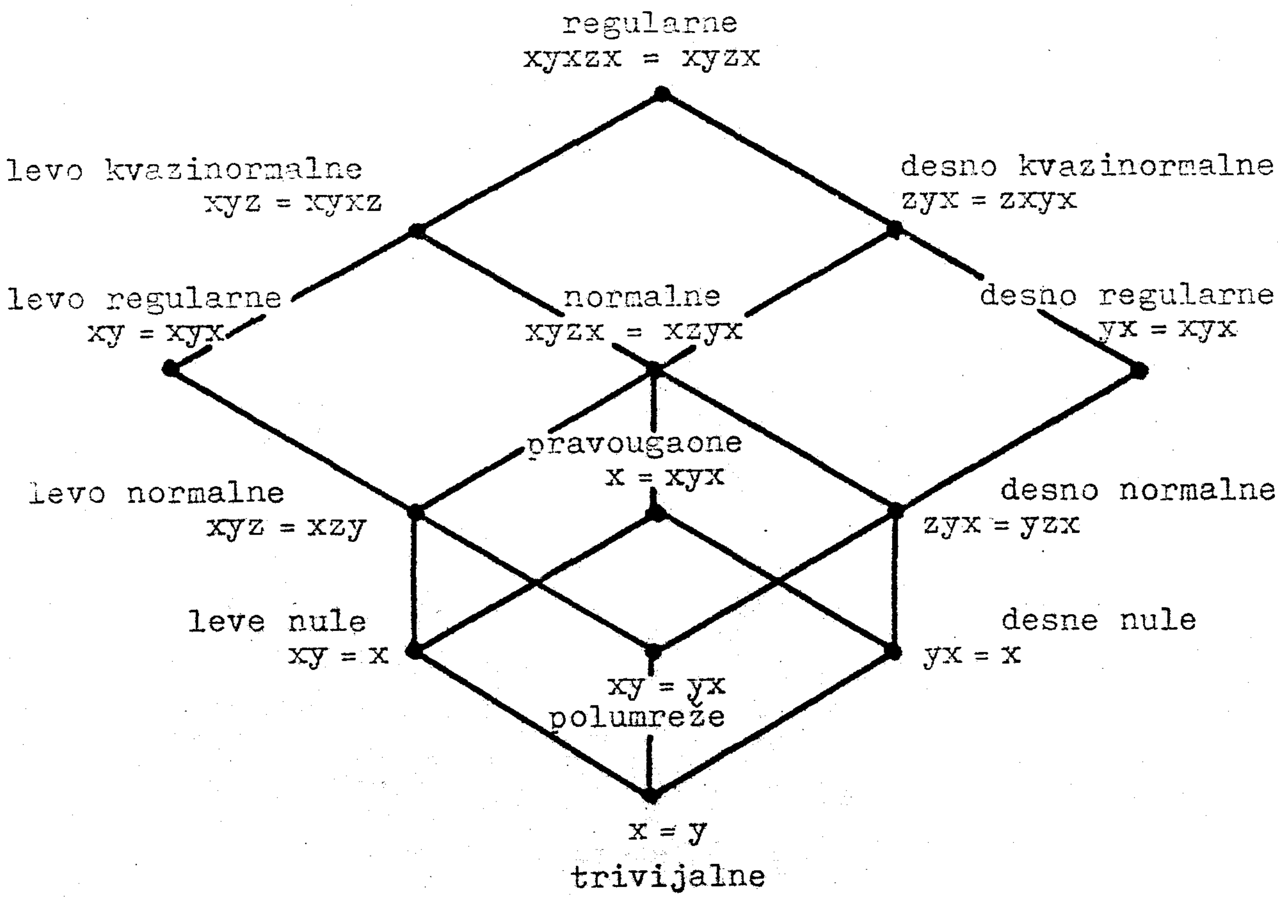
(0.17) TEOREMA. Za ortogrupu S sledeći uslovi su ekvivalentni:

(a) $\mathcal{H}$ je kongruencija na S;

(b) $\delta_{(g,h)}(e,f) = ef$, za svako $e,f \in E_S$;

(c) S je subdirektni proizvod E i G.

Traka koja zadovoljava jednakost $xyxzx = xyzx$ zove se regularna traka, i sve takve trake očigledno formiraju varijetet traka (polugrupa). Na sledećem dijagramu dati su svi podvarijeteti varijeteta regularnih traka sa njihovim nazivima i jednakostima koje ih definišu unutar varijeteta svih traka.



Neka je X proizvoljan neprazan skup. Skup $F(X)$ svih konačnih nizova elemenata iz X čini polugrupu u odnosu na operaciju dopisivanja. To je slobodna polugrupa nad skupom X. Elemente iz $F(X)$ zovemo reči.

Ako je X skup, onda će $|X|$ označavati kardinalni broj skupa X.

Veliki broj matematičara je dao prilog ispitivanju strukture različitih klasa regularnih polugrupa. Većina tih rezultata je sistematizovana u Petrich [54] i materijal za ovaj uvodni odeljak uzet je uglavnom odatle.

1. UNIJE DIEDARSKIH GRUPA

Grupe kije zadovoljavaju jednakost $x^3 = x$ zovu se Booleove grupe i sve su komutativne. Polugrupe koje zadovoljavaju istu jednakost zvaćemo Booleove polugrupe. Lako se vidi da su Booleove polugrupe unije Booleovih grupa, tačnije polumreže Reesovih matričnih polugrupa nad Booleovim grupama.

Grupa generisana sa dva generatora u i v koji zadovoljavaju jednakosti

$$v^2 = 1 = (uv)^2 \tag{1.1}$$

je beskonačna diedarska grupa, D_∞. Ako gornjim jednakostima dodamo jednakost

$$u^n = 1 \tag{1.2}$$

dobićemo konačnu diedarsku grupu D_n sa $2n$ elemenata. Za svaki nenegativni celi broj n grupa D_n je homomorfna slika grupe D_∞ koja nema drugih homomorfnih slika (D_o označava jednoelementnu grupu). Primetimo da su D_2 (Klajnova četvorna grupa), D_1 (grupa reda 2) i D_o jedine komutativne diedarske grupe.

Navedene činjenice o diedarskim grupama su deo folklora teorije grupa, a zainteresovani čitalac može da konsultuje [34].

Sledeća lema se može dobiti kao posledica jednog opštijeg stava za algebre (Graetzer [32, odeljak 45, posledica 2]), ali zbog potpunosti izlaganja dajemo jednostavniji neposredan dokaz.

(1.3) LEMA. <u>Klasa svih polugrupa definisanih formulom</u>

$$\forall x \exists y \,(x = xyy,\ y = xyx) \tag{1.4}$$

<u>zatvorena je za homomorfizme</u>.

<u>Dokaz</u>. Neka je $h\colon S \to T$ homomorfizam polugrupe S koja zadovoljava formulu (1.4) na polugrupu T i neka je $x \in T$. Ako je $u \in h^{-1}(x) \subseteq S$, onda postoji $v \in S$ tako da je $u = uvv$ i $v = uvu$. Stavimo $y = h(v) \in T$. Tada važi

$$x = h(u) = h(uvv) = h(u)h(v)h(v) = xyy,$$

$$y = h(v) = h(uvu) = h(u)h(v)h(u) = xyx,$$

pa polugrupa T zadovoljava formulu (1.4), čime je lema dokazana. ●

Sada možemo da dokažemo sledeću teoremu.

(1.5) TEOREMA. <u>Polugrupa S je unija diedarskih grupa ako i samo ako zadovoljava formulu</u> (1.4).

<u>Dokaz</u>. ($\Rightarrow$) Neka je polugrupa S unija diedarskih grupa i neka je $x \in S$. Tada x pripada nekoj diedarskoj podgrupi D_n (uključujući mogućnost da je $n = \infty$). Dokažimo da svaka diedarska grupa zadovoljava formulu (1.4). Na osnovu prethodne leme, dovoljno je to dokazati za grupu D_∞. Koristeći posledicu $uv = vu^{-1}$ jednakosti (1.1) koje defini-

šu grupu D_∞ generisanu elementima u i v, nalazimo da su svi njeni elementi oblika u^m ili vu^m, gde je m ceo broj. Ako je $x \in D_\infty$ jednog od ovih oblika, onda u oba slučaja možemo uzeti $y = vu^m$ i formula (1.4) biće zadovoljena, jer

$$u^m vu^m vu^m = u^m u^{-m} vvu^m = v^2 u^m = u^m,$$
$$vu^m vu^m vu^m = vu^m u^{-m} vvu^m = vu^m,$$
$$u^m vu^m u^m = vu^{-m} u^m u^m = vu^m.$$

($\Leftarrow$) Neka polugrupa S zadovoljava formulu (1.4) i neka su x i y elementi iz S takvi da je $x = xyy$ i $y = xyx$. Tada je

$$x = xyy = xy(xyx) = x(yxy)x,$$
$$(yxy)x(yxy) = y(xyxyx)y = yxy$$
$$x(yxy) = (xyx)y = yy = y(xyx) = (yxy)x.$$

Prema tome, yxy je inverz elementa x i oni komutiraju. Sledi da je S unija grupa. Osim toga, jasno je da je $x \mathcal{L} y$, a iz $y = xyx$ imamo

(1.6) $$x = xyy = xy(xyx) = (xyx)yx = yyx.$$

Odavde je $x \mathcal{R} y$, pa dakle, i $x \mathcal{H} y$. Zaključujemo da su $\mathcal{H}$-klase grupe koje zadovoljavaju formulu (1.4), a u klasi svih grupa ta formula je očigledno ekvivalentna sa sledećom:

(1.7) $$\forall x \exists y \, (y^2 = 1 = (xy)^2).$$

Dakle, u grupi koja zadovoljava (1.7), za svaki x postoji neki y (ne neophodno različit od x) koji zajedno sa x generiše grupu D_∞ (relacije u (1.7) su definišuće relacije grupe D_∞ generisane elementima x i y) ili neku od njenih homomorfnih slika, na osnovu prethodne leme. Zaključujemo da su grupe koje zadovoljavaju (1.7), odnosno (1.4), unije diedarskih grupa. ●

Ako je $x = xyy$ i $y = xyx$, onda ćemo reći da je y <u>diedarski parnjak</u> za x. Primetimo da element ne mora da bude diedarski parnjak svog diedarskog parnjaka, tj. relacija "biti diedarski parnjak" nije simetrična.

(1.8) <u>Primedba</u>. Pošto svaki element i njegov diedarski parnjak generišu jednu (diedarsku) podgrupu, zaključujemo da element x i svi njegovi diedarski parnjaci pripadaju istoj $\mathcal{H}$-klasi, tj. istoj maksimalnoj podgrupi. Ova činjenica omogućuje da se neka razmatranja o unijama diedarskih grupa podignu na nivo teorije grupa. To znači da možemo da koristimo izraze oblika x^{-3} i slično.

Jedna lokalna osobina $\mathcal{H}$-klasa opisuje se sledećom lemom.

(1.9) LEMA. <u>Ako je</u> y <u>diedarski parnjak za</u> x, <u>onda je to i</u> $x^n y$, <u>za svako</u> n.

<u>Dokaz</u>. Na osnovu primedbe (1.8), dovoljno je dokazati tvrđenje leme za slučaj grupa. Neka je y diedarski parnjak za x u nekoj grupi, tj. neka $x = xyy$ i $y = xyx$. Odavde sledi $yx = x^{-1}y$ i $y^2 = 1$, pa imamo

$$x(x^n y)(x^n y) = xx^n x^{n-1} yy = x,$$
$$x(x^n y)x = xx^n x^{-1} y = x^n y,$$

što znači da je $x^n y$ diedarski parnjak za x. ●

Iz prethodne leme sledi da jedan element može da ima više diedarskih parnjaka. Koliko? Dva ekstremna slučaja opisana su sledećim tvrđenjima.

(1.10) TVRĐENJE. Polugrupa S je unija diedarskih grupa u kojoj je svaki element diedarski parnjak svakog elementa ako i samo ako je S Booleova grupa.

Dokaz. ($\Rightarrow$) Na osnovu primedbe (1.8) polugrupa S ima samo jednu $\mathcal{H}$-klasu, odnosno S je grupa. Pošto je svaki element x sam sebi diedarski parnjak, on zadovoljava jednakost $x^3 = x$, tj. S je Booleova grupa.

($\Leftarrow$) Neka su x i y dva proizvoljna elementa Booleove grupe. Ona je komutativna, pa imamo:

$$x = x \cdot 1 = xy^2, \quad y = y \cdot 1 = yx^2 = xyx,$$

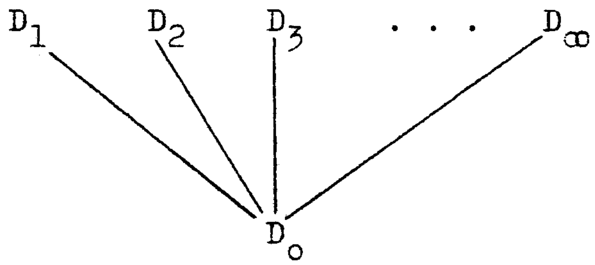
tj. y je diedarski parnjak za x. ●

(1.11) TVRĐENJE. Polugrupa S je unija diedarskih grupa u kojoj svaki element ima jedinstvenog diedarskog parnjaka ako i samo ako je S traka.

Dokaz. ($\Rightarrow$) Dovoljno je dokazati da ako u grupi H svaki element ima jedinstvenog diedarskog parnjaka, onda je H jednoelementna grupa. Neka je 1 jedinica grupe H. Ona ima jedinstvenog diedarskog parnjaka, tj. $1 = 1yy$ i $y = 1y1$, za tačno jedan y iz H. Drugim rečima, postoji samo jedan y iz H koji zadovoljava jednakost $y^2 = 1$. Kako je $1^2 = 1$, zaključujemo da H nema elemenata reda 2. Jedina diedarska grupa bez elemenata reda 2 je D_0. Dakle $H = D_0$.

($\Leftarrow$) Ako je S traka, onda je svaki element x sam sebi diedarski parnjak. Drugih diedarskih parnjaka nema, jer je relacija $\mathcal{H}$ trivijalna. ●

U diedarskoj grupi D_n generisanoj elementima u i v koji zadovoljavaju jednakosti (1.1) i (1.2), element u ima tačno n diedarskih parnjaka. Sada se lako vidi da postoje polugrupe u kojima za svako zadato n (konačno ili prebrojivo) postoji element sa tačno n diedarskih parnjaka. Takva je, naprimer, sledeća polumreža grupa



koja je ortogonalna suma grupa sa nulom $D_1^o, D_2^o, \ldots, D_\infty^o$.

Diedarske grupe nisu suviše složene, naprotiv, pa se prirodno pojavljuje pitanje koliko složene mogu da budu $\mathcal{H}$-klase unija diedarskih grupa. Sledeća konstrukcija pokazuje da one mogu da budu složene bar onoliko koliko su to komutatinve grupe.

(1.12) <u>Konstrukcija</u>. Neka je $(A,+)$ proizvoljna komutativna grupa. U skupu $A \cup \overline{A}$, gde je $\overline{A} = \{\overline{a} : a \in A\}$ definišimo proizvod $*$ na sledeći način:

$$a*b = a+b, \qquad \overline{a}*b = \overline{(a+b)},$$
$$a*\overline{b} = \overline{(b-a)}, \qquad \overline{a}*\overline{b} = b-a.$$

Nije teško (iako nije ni kratko) proveriti da je $*$ asocijativna operacija. Neutralni element je nula grupe $(A,+)$, a inverzi za a i $\overline{a}$ su $-a$, odnosno $\overline{a}$. Dakle, $(A \cup \overline{A}, *)$ je grupa. U njoj važi:

$$\overline{a}*\overline{a} = a-a = 0, \quad a*\overline{a}*a = a*\overline{(a+a)} = \overline{(a+a)-a} = \overline{a},$$

a to znači da je $\overline{a}$ diedarski parnjak i za a i za $\overline{a}$. Prema tome, konstruisana grupa $(A \cup \overline{A}, *)$ je unija diedarskih grupa, a njena podgrupa $(A,*)$ je očigledno izomorfna kopija grupe $(A,+)$.

Pošto se klasa unija diedarskih grupa može definisati univerzalno-egzistencijalnom formulom prvog reda sa pozitivnom hornovskom matricom, ona nije zatvorena samo za homomorfizme (lema 1.3), nego i za direktne proizvode i direktne unije (Graetzer [32, odeljci 45,46]). Dakle, i ove standardne algebarske konstrukcije mogu da se koriste za dobijanje složenijih unija diedarskih grupa, polazeći od jednostavnijih.

Na osnovu (1.6) zaključujemo da u formuli (1.4) na desnoj strani jednakosti možemo izvršiti manju permutaciju slova, pa da dobijena formula i dalje definiše klasu unija diedarskih grupa. Ovu činjenicu ćemo formulisati u obliku tvrđenja.

(1.13) TVRĐENJE. <u>Polugrupa S je unija diedarskih grupa ako i samo ako zadovoljava formulu</u>

(1.14) $$\forall x \exists y\, (x = yyx,\ y = xyx).$$

Ako nastavimo da permutujemo promenljive u formuli (1.14), onda će se situacija promeniti, pa imamo

(1.15) TVRĐENJE. U klasi svih polugrupa jednakost $x^3 = x$ ekvivalentna je svakoj od sledećih formula:

$$\forall x \exists y\,(x = yxy,\ y = yxx), \tag{1.16}$$

$$\forall x \exists y\,(x = yxy,\ y = xxy), \tag{1.17}$$

$$\forall x \exists y\,(x = xyy,\ y = yxx), \tag{1.18}$$

$$\forall x \exists y\,(x = xyy,\ y = xxy), \tag{1.19}$$

$$\forall x \exists y\,(x = yyx,\ y = yxx), \tag{1.20}$$

$$\forall x \exists y\,(x = yyx,\ y = xxy). \tag{1.21}$$

Dokaz. Jasno je da jednakost $x^3 = x$ povlači svaku od formula (1.16) - (1.21); dovoljno je za y uzeti x. Obrnuto, da formula (1.n) povlači jednakost $x^3 = x$, može se videti iz računanja (1.n′) u sledećem nizu ($n \in \{16,17,18,19,20,21\}$):

$$x = yxy = yx(yxx) = (yxy)xx = x^3, \tag{1.16′}$$

$$x = yxy = (xxy)xx = xx(yxy) = x^3, \tag{1.17′}$$

$$x = xyy = xy(yxx) = (xyy)xx = x^3, \tag{1.18′}$$

$$x = xyy = x(xxy)y = xx(xyy) = x^3, \tag{1.19′}$$

$$x = yyx = y(yxx)x = (yyx)xx = x^3, \tag{1.20′}$$

$$x = yyx = (xxy)yx = xx(yyx) = x^3. \tag{1.21′}$$ ●

Gledajući formule (1.4),(1.14) i (1.16) - (1.21), može se primetiti da nedostaje formula $\forall x \exists y\,(x = yxy,\ y = xyx)$. Njome su definisane tzv. anti-inverzne polugrupe, a o njima će kasnije biti više reči. Sada dajemo još jednu karakterizaciju unija diedarskih grupa, ali prethodno nam je potrebna sledeća lema, koju je dokazao Clifford [14] za ideale, ali ona se jednostavno proširuje na (m,n)-ideale, za svako m,n.

(1.22) LEMA. _Ako (m,n)-ideal polugrupe sadrži element neke njene podgrupe, onda sadrži i celu tu podgrupu._

Dokaz. Neka je S polugrupa, H njena podgrupa, I (m,n)-ideal, $a \in H \cap I$ i $b \in H$. Ako sa a^{-1} označimo inverz elementa a u podgrupi H, onda

$$b = a^m a^{-m} b a^{-n} a^n \in B^m S B^n \subseteq B,$$

odakle $H \subseteq B$. ●

Sada možemo da dokažemo

(1.23) TVRĐENJE. _Za svako $m,n \geq 0$ važi: polugrupa S je unija diedarskih grupa ako i samo ako su joj svi (m,n)-ideali unije diedarskih grupa._

Dokaz. $(\Longrightarrow)$ Neka je S unija diedarskih grupa i I njen (m,n)-ideal. Prema prethodnoj lemi, iz $a \in I$ sledi $H_a \subseteq I$, jer je H_a grupa, pa je I unija $\mathcal{H}$-klasa. Kako su $\mathcal{H}$-klase unije diedarskih grupa, sledi da je i I takođe unija diedarskih grupa.

$(\Longleftarrow)$ U ovom smeru dokaz je trivijalan. ●

Pojam bazisne klase polugrupa uveo je Ljapin sledećom definicijom.

(1.24) _Definicija._ Neka su C_1, C_2, C_3 tri klase polugrupa i $C_1 \subseteq C_2 \subseteq C_3$. Za klasu polugrupa C_1 kažemo da je bazisna klasa klase C_2 u odnosu na klasu C_3, ako su ispunjeni sledeći uslovi: (a) svaka polugrupa iz C_2 je unija polugrupa iz C_1; (b) svaka polugrupa iz C_3 koja može da se predstavi kao unija polugrupa iz C_1, pripada C_2; (c) ako neka klasa C_1' polugrupa zadovoljava uslove (a) i (b), onda je $C_1 = C_1'$.

Na osnovu dosadašnjih rezultata možemo da nađemo bazisnu klasu (u Ljapinovom smislu) unija diedarskih grupa u odnosu na klasu svih polugrupa.

(1.25) TVRĐENJE. Bazisna klasa unija diedarskih grupa u odnosu na klasu svih polugrupa je $\{D_0, D_1, D_3, D_4, D_5, \dots, D_\infty\}$.

Dokaz. Uslov (a) definicije je očigledno ispunjen.

(b) Pošto grupa D_2 zadovoljava jednakost $x^2 = 1$, ona je unija dvoelementnih grupa D_1, pa je i uslov (b) definicije ispunjen.

(c) Diedarska grupa D_n sadrži element reda n (uključujući mogućnost da je $n = \infty$) i ne sadrži element reda većeg od n, izuzev za $n = 1$: grupa D_1 ima element reda 2. Zato se grupa D_n ne može prikazati kao unija manjih diedarskih grupa, izuzev za $n = 2$: grupa D_2 je unija grupa D_1. Sledi minimalnost. ●

Svi rezultati iz ovog odeljka su originalni. Materijal je uglavnom iz Blagojević [08].

2. ANTI-INVERZNE POLUGRUPE

Grupa generisana sa dva generatora x i y koji zadovoljavaju jednakosti

$$x^2 = (xy)^2 = y^2 \tag{2.0}$$

je kvaternionska grupa Q i ima 8 elemenata. Njene netrivijalne prave podgrupe su ciklička grupa reda 4 i grupa reda 2, a njene netrivijalne homomorfne slike su grupa reda 2 i četvorna grupa D_2. Grupa Q je najmanja Hamiltonova grupa, tj. najmanja nekomutativna grupa čije su sve podgrupe komutativne

Za dva elementa x i y neke polugrupe reći ćemo da su jedan drugom anti-inverzi ako zadovoljavaju jednakosti

$$x = yxy, \quad y = xyx. \tag{2.1}$$

Polugrupa je anti-inverzna ako zadovoljava formulu

$$\forall x \, \exists y \, (x = yxy, \; y = xyx), \tag{2.2}$$

tj. ako svaki njen element ima anti-inverz.

Važi sledeća lema.

(2.3) LEMA. Klasa svih polugrupa definisanih formulom (2.2) zatvorena je za homomorfizme.

Dokaz ne navodimo jer je skoro identičan dokazu leme 1.3. Štaviše, slično kao i u odeljku 1, osim zatvorenosti za homomorfizme, klasa anti-inverznih polugrupa je zatvorena i za direktne proizvode i direktne sume.

Sada možemo da dokažemo sledeću teoremu.

(2.4) TEOREMA. <u>Polugrupa</u> S <u>je unija homomorfnih slika kvaternionske grupe ako i samo ako je anti-inverzna</u>.

<u>Dokaz</u>. ($\Rightarrow$) Neposrednom proverom nalazimo da kvaternionska grupa zadovoljava formulu (2.2), tj. da je anti-inverzna. Prema prethodnoj lemi, takve su i njene homomorfne slike. Anti-inverz nekog elementa u nekoj podgrupi polugrupe je takođe anti-inverz u celoj podgrupi, pa je S anti-inverzna.

($\Leftarrow$) Neka je S anti-inverzna polugrupa i neka su x i y elementi iz polugrupe S koji zadovoljavaju (2.1). Tada imamo

$$(2.5) \qquad x = yxy = (xyx)(yxy)(xyx) = x(yxy)x(yxy)x = x^5,$$

odakle sledi da je S unija grupa. Dalje, očigledno je da iz (2.5) sledi $x\mathcal{R}y$ i $x\mathcal{L}y$, pa $x\mathcal{H}y$, što znači da anti-inverzni elementi pripadaju istoj maksimalnoj podgrupi. S druge strane, jednakosti (2.1) u klasi svih grupa ekvivalentne su jednakostima (2.0), koje definišu kvaternionsku grupu. Dakle, svaki par anti-inverznih elemenata generiše kvaternionsku grupu ili neku njenu homomorfnu sliku. Sledi da je S unija homomorfnih slika kvaternionske grupe. ●

Na osnovu ove teoreme lako se mogu dokazati sledeće posledice.

(2.6) POSLEDICA. Polugrupa je anti-inverzna ako i samo ako je (disjunktna) unija anti-inverznih grupa.

(2.7) POSLEDICA. Za svako $m,n>0$ važi: polugrupa je anti-inverzna ako i samo ako su joj svi (m,n)-ideali anti-inverzni.

Dokazi ovih zvrđenja su slični dokazima odgovarajućih tvrđenja za unije diedarskih grupa, pa ih ne navodimo.

(2.8) POSLEDICA. Grupe D_0, D_1, Q čine bazisnu klasu anti-inverznih polugrupa u odnosu na klasu svih polugrupa.

Dokaz sledi iz činjenice da su D_0, D_1, D_2, Q jedine homomorfne slike grupe Q i iz činjenice da je D_2 unija grupa D_1. (Uporedi sa dokazom sličnog tvrđenja 1.17 za unije diedarskih grupa.)

Kako je inverzna unija grupa polumreža grupa, lako se dobija i sledeće tvrđenje.

(2.9) TVRĐENJE. Anti-inverzna polugrupa je inverzna ako i samo ako je polumreža anti-inverznih grupa.

(2.10) Komentar. S obzirom na prethodno tvrđenje, izraz "anti-inverzna polugrupa" možda nije najsrećnije izabran, mada je svakako bolji od izraza "anti-regularna polugrupa", koji je bio prvi naziv za ove polugrupe. Imajući u vidu teoremu 2.4, najtačnije bi bilo govoriti o "unijama homomorfnih slika kvaternionske grupe", što je, iako precizno, ipak suviše dugačko i glomazno. Tako se opet vraćamo izrazu "anti-inverzne polugrupe" kao najprihvatljivijem. Pri tome treba imati u vidu i sličnu situaciju sa binarnim relacijama: naime, postoje relacije koje su i simetrične i anti-simetrične.

I sledeća dva tvrđenja su slična odgovarajućim tvrđenjima za unije diedarskih grupa i slično se dokazuju, pa ih navodimo bez dokaza.

(2.11) TVRĐENJE. <u>U polugrupi</u> S <u>svaki element ima jedinstven anti-inverz ako i samo ako je</u> S <u>traka</u>.

(2.12) TVRĐENJE. <u>U polugrupi</u> S <u>svi elementi su jedan drugom anti-inverzi ako i samo ako je</u> S <u>Booleova grupa</u>.

Anti-inverzne polugrupe definisao je Sharp [58] pod imenom anti-regularne polugrupe. Njihovu strukturu su ispitivali Bogdanović, Milić, Pavlović [12] i Bogdanović [10]. U ovim radovima se mogu naći razne karakterizacije anti-inverznih polugrupa. Karakterizacija data teoremom 2.4 je najpreciznija i ostale se mogu izvesti iz nje. Posledice 2.6 i 2.8 su iz Bogdanović [10, teoreme 4.3 i 3.3]. Tvrđenja 2.11 i 2.12 su iz Sharp [58, teoreme 2 i 3]. Vidi takođe Blagojević [07]. Lema 2.3 i posledica 2.7 su novi.

U ovom kratkom odeljku sadržan je uvodni materijal za sledeći odeljak, a posebno je izdvojen da bi se istakao paralelizam unija diedarskih grupa i anti-inverznih polugrupa.

3. NEKA UOPŠTENJA ANTI-INVERZNIH POLUGRUPA

Teorema kojom započinjemo ovaj odeljak daje još neke karakterizacije anti-inverznih polugrupa.

(3.1) TEOREMA. <u>U klasi svih polugrupa sledeće formule su ekvivalentne:</u>

(a) $\forall x \exists y \, (x = yxy, \; y = xyx)$

(b) $\forall x \exists y \, (x^2 = (xy)^2 = y^2, \; x^5 = x)$

(c) $\forall x \exists y \, (x^2 = y^2, \; yx = x^3 y, \; x^5 = x)$

Drugim rečima, polugrupa je anti-inverzna ako zadovoljava bar jednu od formula (b) ili (c).

Karakterizacija anti-inverznih polugrupa data formulom (b) uopštava se u radu Milić, Bogdanović [44] i posmatraju se polugrupe definisane formulom

(3.2) $$\forall x \exists y \, (x^m = (xy)^m = y^m, \; x^{n+1} = x)$$

Obeležimo sa $S_{m,n}$ klasu polugrupa definisanih formulom (3.2). U pomenutom radu se rešava sledeći problem: koje od klasa $S_{m,n}$ sadrže jedino anti-inverzne polugrupe, i daje se algoritam koji daje odgovor na postavljeno pitanje. U ovom odeljku daćemodrugo rešenje tog problema koje će biti jednostavnije i potpunije, u smislu da ćemo tačno odrediti sadržaj klase $S_{m,n}$ ako je ona anti-inverzna.

Da bismo pojednostavili izražavanje, uvedimo oznake: $\mathbf{A}$ za klasu svih anti-inverznih polugrupa, $\mathbf{G}$ za klasu grupa i $\mathbf{B}$ za klasu traka.

(3.3) LEMA. <u>Za svako</u> m,n <u>je</u> $\mathbf{B} \subseteq \mathbf{S}_{m,n}$.

<u>Dokaz</u>. Lako se vidi da je $\mathbf{B} \subseteq \mathbf{S}_{1,1} \subseteq \mathbf{S}_{m,n}$ i tvrđenje leme odmah sledi. ●

Sledeća teorema bliže opisuje polugrupe iz klase $\mathbf{S}_{m,n}$.

(3.4) TEOREMA. <u>Polugrupa</u> S <u>pripada klasi</u> $\mathbf{S}_{m,n}$ <u>ako i samo ako je</u> S <u>polumreža Reesovih matričnih polugrupa nad grupama iz</u> $\mathbf{S}_{m,n}$.

<u>Dokaz</u>. ($\Rightarrow$) Jednostavno se proverava da je $\mathbf{S}_{m,1} \subseteq \mathbf{B}$. Međutim, svaka traka je polumreža Reesovih matričnih polugrupa nad trivijalnim grupama - jedinim grupama u $\mathbf{S}_{m,1} = \mathbf{B}$.

Neka je sada $n \geq 2$, $S \in \mathbf{S}_{m,n}$, $x \in S$. Iz $x^{n+1} = x$ imamo

$$x^{n-1}xx^{n-1} = x^{n+1}x^{n-2} = xx^{n-2} = x^{n-1},$$

$$x = xx^{n-1}x, \qquad xx^{n-1} = x^{n-1}x$$

pa je S kompletno regularna, tj. polumreža Reesovih matričnih polugrupa . Za dato $x \in S$, na osnovu (3.2) postoji y takvo da je $x^m = (xy)^m = y^m$, odakle dobijamo $x^{m+k} = y^m x^k$. Za pogodno izabrano k (recimo $k = n - \mathrm{rest}(m,n)$, gde je $\mathrm{rest}(m,n)$ ostatak pri deljenju m sa n) dobijamo $x = x^{m+k} = y^m x^k$, i i slično $y = y^{m+k} = x^m y^k$. Prema tome, $x \mathcal{R} y$ i dualno $x \mathcal{L} y$, a odavde $x \mathcal{H} y$. Zaključujemo da su $\mathcal{H}$-klase grupe iz $\mathbf{S}_{m,n}$.

($\Leftarrow$) Obrnuto, neka je $S = S(Y, G_0)$ polumreža Y Reesovih matričnih polugrupa nad grupama G_α, $\alpha \in Y$ iz klase

$\mathbb{S}_{m,n}$ i neka je $x \in S$. Kako je klasa H_x izomorfna nekoj grupi G_o, ona je iz $\mathbb{S}_{m,n}$. Zato u H_x, pa dakle i u S, postoji neki y kojim je zadovoljena formula (3.2). Prema tome, i S je iz $\mathbb{S}_{m,n}$. ●

Na osnovu prethodne teoreme biće dovoljno da naša dalja razmatranja ograničimo na klasu $\mathbb{G}_{m,n} = \mathbb{G} \cap \mathbb{S}_{m,n}$ grupa. Naravno, pri tome možemo da koristimo i jezik teorije grupa, tj. izraze oblika 1, x^{-5} i slično.

(3.5) LEMA. <u>Važi:</u> $\mathbb{G}_{m,n} = \mathbb{G}_{d,n}$, <u>gde je</u> $d = \mathrm{nzd}(m,n)$ <u>najveći zajednički delilac za</u> m <u>i</u> n.

<u>Dokaz</u>. Pošto $x^d = (xy)^d = y^d$ povlači $x^m = (xy)^m = y^m$, onda očigledno $\mathbb{G}_{d,n} \subseteq \mathbb{G}_{m,n}$. Dokažimo i obrnutu inkluziju. Ako je $d = \mathrm{nzd}(m,n)$, onda postoje celi brojevi k i l takvi da je $d = km - ln$ (dobro poznata činjenica iz elementarne teorije brojeva). Iz $x^m = (xy)^m = y^m$ imamo $x^{km} = (xy)^{km} = y^{km}$, odnosno $x^{d+ln} = (xy)^{d+ln} = y^{d+ln}$. Kako je $x^n = (xy)^n = y^n = 1$, prethodne jednakosti postaju $x^d = (xy)^d = y^d$. Dakle, formula

$$\forall x \, \exists y \, (x^d = (xy)^d = y^d, \; x^n = 1)$$

povlači formulu

$$\forall x \, \exists y \, (x^m = (xy)^m = y^m, \; x^n = 1)$$

odakle sledi da je $\mathbb{G}_{m,n} \subseteq \mathbb{G}_{d,n}$. ●

Prethodna lema nam omogućuje da učinimo dalja ograničenja i posmatramo samo klase $\mathbb{G}_{p,pq}$.

(3.6) LEMA. <u>Ciklička grupa reda</u> r <u>pripada klasi</u> $\mathbb{G}_{p,pq}$ <u>ako i samo ako</u> r <u>deli</u> p.

Dokaz. ($\Rightarrow$) Neka je $C_r = \{z, z^2, \ldots, z^r = 1\}$ ciklička grupa reda r. Pošto C_r pripada klasi $\mathbb{G}_{p,pq}$, ona zadovoljava formulu

(3.7) $$\forall x \exists y \, (x^p = (xy)^p = y^p).$$

Svaki x iz C_r je oblika z^a, gde je $1 \le a \le r$, pa uslov (3.7) primenjen na C_r daje

$$(\forall a \le r)(\exists b \le r)(z^{ap} = z^{(a+b)p} = z^{bp}),$$

odakle imamo

$$(\forall a \le r)(\exists b \le r)(z^{ap+bp} = z^{bp}),$$

a to implicira

$$(\forall a \le r)(z^{ap} = 1).$$

Odavde sledi

$$(\forall a \le r)(a \text{ deli } p),$$

pa zaključujemo da r deli p.

($\Leftarrow$) Ako r deli p, onda očigledno važi

$$x^p = (xy)^p = y^p = x^{pq} = 1,$$

za svaki x iz C_r, pa $C_r \in \mathbb{G}_{p,pq}$. ●

Prethodne dve leme daju sledeću posledicu.

(3.8) POSLEDICA. $\mathbb{G}_{p,pq} \subseteq \mathbb{A}$ ako i samo ako $p \le 2$. Štaviše:

(i) $\mathbb{G}_{1,q}$ sadrži samo trivijalnu grupu;

(ii) $\mathbb{G}_{2,2q}$, za q neparno je klasa svih Booleovih grupa;

(iii) $\mathbb{G}_{2,4q}$ je klasa svih anti-inverznih grupa.

Dokaz. ($\Rightarrow$) Prema lemi 3.6, klasa $\mathbb{G}_{p,pq}$ sadrži grupu C_p koja nije anti-inverzna za $p > 2$. Prema tome $p \le 2$.

($\Leftarrow$) Neka je $p=2$. Sve grupe iz $\mathbb{G}_{2,2q}$ su anti--inverzne jer $x^2=(xy)^2=y^2$ povlači $x=yxy$, $y=xyx$. Za $p=1$ je $\mathbb{G}_{1,q}\subseteq\mathbb{G}_{2,2q}$, pa su i grupe iz $\mathbb{G}_{1,q}$ takođe anti-inverzne.

(i) Grupe iz $\mathbb{G}_{1,q}$ zadovoljavaju formulu

$$\forall x\,\exists y\,(x=xy=y).$$

Odavde sledi $\forall x\,(x^2=x)$, odnosno $\forall x\,(x=1)$, tj. $\mathbb{G}_{1,q}$ sadrži samo trivijalnu grupu.

(ii) Očigledno je da svaka grupa koja zadovoljava jednakost $x^2=1$ pripada klasi $\mathbb{G}_{2,2q}$. Obrnuto, neka je $G\in\mathbb{G}_{2,2q}$. Videli smo da je ona tada anti-inverzna, pa, prema teoremi 3.1.b, primenjenoj na grupe, zadovoljava jednakost $x^4=1$. Iz $x^4=1$ i $x^{2q}=1$ dobijamo $x^{nzd(4,2q)}=1$; međutim, $nzd(4,2q)=2$, jer je q neparan. Dakle, svaka grupa iz $\mathbb{G}_{2,2q}$ zadovoljava jednakost $x^2=1$, tj. Booleova je.

(iii) Na osnovu teoreme 3.1 jasno je da je $\mathbb{G}_{2,4}$ klasa svih anti-inverznih grupa i $\mathbb{G}_{2,4}\subseteq\mathbb{G}_{2,4q}$. Obrnuto, ako je grupa G iz $\mathbb{G}_{2,4q}$, onda ona zadovoljava

$$\forall x\,\exists y\,(x^2=(xy)^2=y^2),$$

što je u klasi grupa ekvivalentno sa (2.2), tj. G je anti-inverzna grupa, pa imamo $\mathbb{G}_{2,4}=\mathbb{G}_{2,4q}=\mathbb{A}\cap\mathbb{G}$. ●

Sada se vratimo klasama $\mathbb{S}_{m,n}$ polugrupa. Kombinujući prethodne rezultate možemo da dokažemo sledeću teoremu.

(3.9) TEOREMA. (1) $\mathbb{B}\leq\mathbb{S}_{m,n}$, <u>za svako</u> m,n.

(2) <u>Neka je</u> $n=1$. <u>Tada</u> $\mathbb{S}_{m,n}\subseteq\mathbb{A}$ <u>ako i samo ako</u> $nzd(m,n)=2$. <u>Štaviše</u>:

(2i) $\mathbb{S}_{m,n} = \mathbb{B}$ ako i samo ako $nzd(m,n) = 1$;

(2ii) $\mathbb{S}_{m,n}$ je klasa svih Booleovih polugrupa ako i samo ako $nzd(m,n) = 2$ i $n \in 4\mathbb{N} - 2$;

(2iii) $\mathbb{S}_{m,n}$ je klasa svih anti-inverznih polugrupa ako i samo ako $nzd(m,n) = 2$ i $n \in 4\mathbb{N}$.

(3) $\mathbb{S}_{1,0}$ je klasa svih traka; ako $m > 0$, onda $\mathbb{S}_{m,0}$ nije klasa anti-inverznih polugrupa.

Dokaz. (1) Lema 3.3.

(2) Svaka polugrupa S iz $\mathbb{S}_{m,n}$ je polumreža Reesovih matričnih polugrupa nad grupama iz $\mathbb{S}_{m,n}$, na osnovu teoreme 3.4, a po lemi 3.5 sve ove grupe su u $\mathbb{G}_{nzd(m,n),n}$. Sada posledica 3.8 može da se primeni, pa tvrđenje sledi.

(3) Već smo videli da je $\mathbb{S}_{1,0} = \mathbb{B}$. Za $m = 2$ klasa $\mathbb{S}_{m,0}$ sadrži cikličku grupu reda m, a takođe i sve konstantne polugrupe (to su polugrupe definisane jednakošću $xy = uv$), i zato to nije klasa anti-inverznih polugrupa. ●

Slično uopštavanje formule (3.1.c) je izvršeno u radovima Bogdanović, Crvenković [11] i Crvenković [22] i posmatrane su klase polugrupa $\mathbb{S}^*_{m,n}$ definisane formulom

$$(3.10) \qquad \forall x \, \exists y \, (x^m = y^m, \ yx = x^{m+1}y, \ x^{n+1} = x)$$

$m \geq 1$, $n \geq 0$ i posmatrane su razne karakterizacije polugrupa iz tih klasa. Koristeći metode slične onima koje smo upotrebljavali u ispitivanju klasa $\mathbb{S}_{m,n}$, daćemo i za klase $\mathbb{S}^*_{m,n}$ odgovor na pitanje koje od njih su anti-inverzne, i tačno odrediti sadržaj odgovarajućih klasa. Dobijeni rezultati su su slični onoma za klase $\mathbb{S}_{m,n}$. To važi i za neke dokaze.

Takve dokaze nećemo navoditi, nego ćemo samo formulisati odgovarajuća tvrđenja, a dokazivaćemo uglavnom, samo ona kod kojih se dokazi ne mogu dobiti jednostavnim preformulacijama dokaza odgovarajućih tvrđenja za klase $\mathbb{S}_{m,n}$. Započinjemo sledećom teoremom koja je analogna teoremi 3.4.

(3.11) TEOREMA. <u>Polugrupa</u> S <u>pripada klasi</u> $\mathbb{S}^*_{m,n}$ <u>ako i samo ako je polumreža Reesovih matričnih polugrupa nad grupama iz</u> $\mathbb{S}^*_{m,n}$.

Opet je zgodno umesto klasa $\mathbb{S}^*_{m,n}$ posmatrati klase $\mathbb{G}^*_{m,n} = \mathbb{S}^*_{m,n} \cap \mathbb{G}$ grupa.

Lema 3.5 se ne može dokazati ako se umesto klasa $\mathbb{G}_{m,n}$ posmatraju klase $\mathbb{G}^*_{m,n}$. Međutim, važi tvrđenje slično lemi 3.6, koje dokazujemo.

(3.12) LEMA. <u>Ciklička grupa</u> C_r <u>reda</u> r <u>pripada klasi</u> $\mathbb{G}^*_{m,n}$ <u>ako i samo ako</u> r <u>deli</u> m <u>i</u> n.

<u>Dokaz</u>. ($\Rightarrow$) Neka je $C_r = \{z, z^2, \dots, z^r = 1\} \in \mathbb{G}^*_{m,n}$. Pošto C_r zadovoljava jednakost $x^n = 1$, sledi da r deli n. Dalje, C_r mora da zadovoljava formulu

$$\forall x \exists y (yx = x^{n+1}y),$$

što, primenjeno na C_r, daje

$$(\forall p \le r)(\exists q \le r)(z^q z^p = z^{(m+1)p} z^q),$$

odakle dobijamo

$$(\forall p \le r)(\exists q \le r)(z^{mp} = 1),$$

odnosno

$$(\forall p \le r)(z^{mp} = 1)$$

a odatle sledi $z^m = 1$. Zaključujemo da r deli m.

($\Leftarrow$) Obrnuto, neka r deli m i n. Tada $m = ra$, $n = rb$, za neke a i b. Grupa C_r zadovoljava formulu (3.10) ako zadovoljava

$$(\forall p \leq r)(\exists q = r)(z^{ar(p-q)} = 1,\ z^{apr} = 1,\ z^{bqr} = 1),$$

a to će sigurno biti ispunjeno jer je $z^r = 1$. ●

Tvrđenje koje sledi je analogno posledici 3.8 leme 3.6 za klase $\mathbb{G}_{m,n}$, ali ne više kao jednostavna posledica prethodne leme. Zato dokaz dajemo u potpunosti.

(3.13) TVRĐENJE. $\mathbb{G}^*_{m,n} \subseteq \mathbb{A}$ <u>ako i samo ako</u> $\text{nzd}(m,n) \leq 2$. <u>Štaviše</u>: (i) $\mathbb{G}^*_{m,n}$ <u>je klasa trivijalnih grupa ako i samo ako su</u> m <u>i</u> n <u>uzajamno prosti</u>;

(ii) $\mathbb{G}^*_{m,n}$ <u>je klasa svih Booleovih grupa ako i samo ako je</u> $\text{nzd}(m,n) = 2$ <u>i</u> $n \in 4\mathbb{N} - 2$;

(iii) $\mathbb{G}^*_{m,n}$ <u>je klasa svih anti-inverznih grupa ako i samo ako je</u> $\text{nzd}(m,n) = 2$ <u>i</u> $n \in 4\mathbb{N}$.

<u>Dokaz</u>. Neka je u daljem $d = \text{nzd}(m,n)$. Neka je $\mathbb{G}^*_{m,n} \subseteq \mathbb{A}$. Kako, na osnovu leme 3.12, klasa $\mathbb{G}^*_{m,n}$ sadrži cikličku grupu reda d, koja nije anti-inverzna za $d > 2$, sledi da je $d \leq 2$. Iz istih razloga, ako je $\mathbb{G}^*_{m,n}$ klasa trivijalnih grupa, onda je $d = 1$.

Pretpostavimo sada da je $G \in \mathbb{G}^*_{m,n}$ i $x, y \in G$ takvi da važi

(3.14) $$x^m = y^m$$

(3.15) $$yx = x^{m+1}y$$

(3.16) $$x^n = 1.$$

Iz (3.14) i (3.15), sa sličnim obrazloženjem kao i u dokazu teoreme 3.4, sledi

$$x^d = y^d. \tag{3.17}$$

Računajući $(x^d y)^d$ prvi put primenom (3.17), dobijamo:

$$\begin{aligned}(x^d y)^d &= (y^d y)^d = y^{(d+1)d} = \\ (y^d)^{d+1} &= (x^d)^{d+1} = x^{d(d+1)},\end{aligned} \tag{3.18}$$

a drugi put primenom (3.15), imamo:

$$\begin{aligned}(x^d y)^d &= x^d y x^d y x^d y \ldots x^d y = \\ &= x^d x^{d(m+1)} y y x^d y \ldots x^d y = \\ &= x^d x^{d(m+1)} x^{d(m+1)^2} y y y \ldots x^d y = \\ &= x^d x^{d(m+1)} x^{d(m+1)^2} \ldots x^{d(m+1)^{d-1}} y^d = \\ &= x^{d+d(m+1)+d(m+1)^2+\ldots+d(m+1)^{d-1}} y^d.\end{aligned} \tag{3.19}$$

Iz (3.18) i (3.19) dobijamo:

$$x^{d^2+d} = x^{d+d(m+1)+d(m+1)^2+\ldots+d(m+1)^{d-1}+d},$$

odnosno

$$\exp_x d^2 = \exp_x d(1+(m+1)+(m+1)^2+\ldots+(m+1)^{d-1}), \tag{3.20}$$

gde smo, zbog jednostavnijeg pisanja, sa $\exp_x A$ označili x^A.

Iz (3.20) sređivanjem i skraćivanjem dobijamo:

$$1 = \exp_x\left[d\,\frac{1-(m+1)^d}{1-(m+1)} - d^2\right] = \exp_x d\left[\frac{(m+1)^d-1}{m} - d\right]. \tag{3.21}$$

Ako je $d=2$, onda (3.21) postaje

$$1 = x^{2m},$$

što, zajedno sa (3.16) daje $x^{nzd(2m,n)} = 1$.

Ako je $n \in 4N-2$, onda je $nzd(2m,n)=2$, pa sve grupe iz $\mathbb{G}^*_{m,n}$ zadovoljavaju jednakost $x^2 = 1$, što znači da su Booleove. Dokažimo da svaka Booleova grupa pripada klasi $\mathbb{G}^*_{m,n}$ za $d = 2$. To sledi iz činjenice da jednakost $x^2 = 1$ trivijalno povlači

$$x^m = y^m \ (=1), \quad yx = x^{m+1}y \ (=xy), \quad x^n = 1,$$

jer su Booleove grupe komutativne. Time je dokazano (ii).

Ako je $n \in 4\mathbb{N}$, onda je $nzd(2m,n) = 4$ i $m = 4k+2$, za neko k iz $\mathbb{N}$, pa jednakost (3.15) postaje

$$yx = x^{m+1}y = x^{4k+3}y = x^3y,$$

jer je $x^{4k} = x^4 = 1$. Sledi da je $\mathbb{G}^*_{m,n} \subseteq \mathbb{A}$. S druge strane, iz $x^2 = y^2$, $yx = x^3y$, $x^4 = 1$ sledi

$$x^{2(2k+1)} = y^{2(2k+1)}, \quad yx = x^{4k+3}y, \quad x^{4l} = 1,$$

za svako k,l iz $\mathbb{N}$, pa $\mathbb{A} \subseteq \mathbb{G}^*_{m,n}$, što dokazuje (iii), a time je kompletiran dokaz celog tvrđenja. ●

Sada se možemo vratiti na klase $\mathbb{S}^*_{m,n}$ polugrupa. Sledeća teorema se lako dobija na osnovu prethodnih rezultata, slično kao što je to bio slučaj sa teoremom 3.9, pa je navodimo bez dokaza.

(3.22) TEOREMA. (1) $\mathbb{B} \subseteq \mathbb{S}^*_{m,n}$, <u>za svako</u> $m \geq 1$ <u>i</u> $n \geq 0$.

(2) <u>Neka je</u> $n > 0$. <u>Onda je</u> $\mathbb{S}^*_{m,n} \subseteq \mathbb{A}$ <u>ako i samo ako je</u> $nzd(m,n) = 2$. <u>Štaviše:</u>

(2i) $\mathbb{S}^*_{m,n} = \mathbb{B}$ <u>ako i samo ako</u> $nzd(m,n) = 1$;

(2ii) $\mathbb{S}^*_{m,n}$ <u>je klasa svih Booleovih polugrupa ako i samo ako je</u> $nzd(m,n) = 2$ <u>i</u> $n \in 4\mathbb{N} - 2$;

(2iii) $\mathbb{S}^*_{m,n}$ <u>je klasa svih anti-inverznih polugrupa ako i samo ako je</u> $nzd(m,n) = 2$ <u>i</u> $n \in 4\mathbb{N}$.

(3) $S^*_{1,0}$ je klasa svih polugrupa koje zadovoljavaju jednakost $x^2 = x^3$; ako je $m \geq 1$, onda $S^*_{m,0}$ nije klasa anti-inverznih polugrupa .

Primetimo da se ova teorema razlikuje od odgovarajuće teoreme 3.9 za klase $S_{m,n}$ u delu (3); naime $S_{1,0} = \mathbb{B}$ i to je prava potklasa klase $S^*_{1,0}$.

Teorema 3.1 je iz Bogdanović, Milić, Pavlović [12, teoreme 2.1 i 2.2]. Izloženi rezultati su, uglavnom, iz Blagojević [07]. Problematiku ovog odeljka započeli su Milić, Bogdanović [44]. Strukturu polugrupa iz $S^*_{m,n}$ ispitivali su Bogdanović, Crvenković [11] i Crvenković [22].

4. ANTI-INVERZNE UNIJE DIEDARSKIH GRUPA

Upoređivanjem unija diedarskih grupa sa anti-inverznim polugrupama, primećuje se da Booleove polugrupe pripadaju i jednoj i drugoj klasi. Prirodno se nameće sledeće pitanje: da li se presek pomenutih dveju klasa polugrupa sastoji samo od Booleovih polugrupa, ili su one prava potklasa tog preseka. Neka je polugrupa S anti-inverzna unija diedarskih grupa. Tada je svaka njena $\mathcal{H}$-klasa takođe anti-inverzna unija diedarskih grupa. Kako su $\mathcal{H}$-klase grupe, jasno je da anti-inverznu uniju diedarskih grupa koja nije Booleova treba prvo tražiti među grupama. Takva grupa bi zadovoljavala jednakost $x^4 = 1$, pa bi ona morala biti 2-grupa sa elementima reda 2 ili 4, a red same grupe bi bio 2^n, za neko n. Zato pokušajmo da takvu grupu nađemo u postojećim tablicama [35] grupa reda 2^n, $n \leq 6$, koji ima 340. Osnovni problem sa tako obimnim tablicama grupa ja kako prepoznati ono što tražimo. Za svaku grupu u tablicama su, među ostalim informacijama, date njene maksimalne prave homomorfne slike i broj elemenata reda 2,4,8,16,32,64. Tražena grupa ne sme imati elemente reda većeg od 4 (da bi bila anti-inverzna) i mora imati elemente reda 4 (da ne bi bila Booleova). Takođe, na osnovu lema 1.3 i 2.3, sve njene homomorfne slike i same moraju biti anti-inverzne unije diedarskih grupa, (ali mogu biti Booleove) i to će nam biti glavni kriterijum eliminacije. Pretražujući tablice na osnovu ovih kriterijima, polazeći od manjih grupa ka većima, nalazimo da je prvi kandidat koji dolazi u obzir, grupa označena sa $32\Gamma_5a_2$ na strani 55. Ona ima 32 elementa i zadata je generatorima b_1,b_2,b_3,b_4,b_5 koji zadovoljavaju relacije:

(4.1) $$b_3b_4=b_4b_3,\ b_2b_5=b_5b_2,\ b_1^2=1=b_5^2,\ b_2^2=b_3^2=b_4^2=b_1.$$

Ova grupa ima 20 elemenata reda 4, ostali su reda 2. Elementi reda 2 su sami sebi anti-inverzi i diedarski parnjaci, pa je potrebno i za elemente reda 4 proveriti da li imaju anti-inverze i diedarske parnjake. To se, naravno, može učiniti, i posle konačno mnogo proveravanja došli bismo do odgovora. Međutim, postupak proveravanja mnogo bi se pojednostavio ako bismo za tu grupu imali neku reprezentaciju koja bi bila simetrična u odnosu na generatore. Pa, pokušajmo.

Posmatrajmo grupu G generisanu elementima c,a_1,a_2,a_3,a_4 koji zadovoljavaju jednakosti:

(4.2) $$a_i^2=c,\ c^2=1,\ a_ia_j=ca_ja_i,\quad i,j\in\{1,2,3,4\},\ i\neq j.$$

Iz (4.2) sledi

(4.3) $$ca_i=a_i^2a_i=a_ia_i^2=a_ic,\quad a_i^{-1}=a_i^3.$$

Neka je $w\in G$. Koristeći jednakosti (4.2) i (4.3), u reči w je moguće:

(i) sve negativne eksponente generatora zameniti pozitivnima - na osnovu $a_i^{-1}=a^3$;

(ii) permutovati generatore a_i tako da odgovarajući niz njihovih indeksa bude neopadajući - na osnovu $a_i a_j = c a_j a_i$ (pri tome će se eventualno pojaviti nekoliko novih slova c;

(iii) sva pojavljivanja slova c premestiti na početak reči - na osnovu $a_i c = c a_i$;

(iv) sve eksponente generatora smanjiti na 1 ili 0 (pri tome je $a_i^0 = c^0 = 1$) - na osnovu $a_i^2 = c$, $c^2 = 1$.

Na osnovu izloženog, svaka reč se može napisati u obliku $c^p a_1^q a_2^r a_3^s a_4^t$, gde su eksponenti p,q,r,s,t iz skupa $\{0,1\}$. Evo i jednog primera

$$\begin{aligned} &a_3 c a_1^{-1} a_2 a_4 a_1 a_2^{-1} = a_3 c a_1^3 a_2 a_4 a_1 a_2^3 = a_3 c c a_1 a_2 a_4 a_1 c a_2 = \\ &a_3 a_1 a_2 a_4 a_1 c a_2 = a_3 a_1 a_2 c a_4 a_1 a_2 = a_3 a_1 a_2 a_1 a_4 a_2 = \\ &a_3 a_1 c a_1 a_2 c a_2 a_4 = a_3 c a_1 a_1 c a_2 a_2 a_4 = a_3 c c c c a_4 = a_3 a_4 . \end{aligned}$$

Prema tome, grupa G ima 32 elementa:

$$\begin{array}{l} 1,\ a_i,\ a_i a_j,\ a_i a_j a_k,\ a_1 a_2 a_3 a_4, \\ c,\ c a_i,\ c a_i a_j,\ c a_i a_j a_k,\ c a_1 a_2 a_3 a_4, \end{array} \qquad 1 \leqslant i < j < k \leqslant 4$$

Elementi a_i, $a_i a_j$, $c a_i$, $c a_i a_j$ su reda 4, ostali su reda 2. Elementi a_i, a_j, a_{ij} su jedan drugom anti-inverzi. Za elemente $a_i a_j$, $c a_i a_j$ diedarski parnjak je c, a za elemente a_i, $c a_i$ diedarski parnjaci su $a_{i+1} a_{i+2} a_{i+3}$, odnosno $c a_{i+1} a_{i+2} a_{i+3}$; pri tome se indeksi sabiraju po modulu 4 i uređuju se u rastući niz, kao što je to već opisano. Za ilustraciju proverimo, naprimer, da je $c a_{i+1} a_{i+2} a_{i+3}$ diedarski parnjak za $c a_i$.

$$\begin{aligned} &c a_i c a_{i+1} a_{i+2} a_{i+3} c a_i = c c a_i a_{i+1} a_{i+2} a_{i+3} a_i c = \\ &c a_{i+1} a_i a_{i+2} a_i a_{i+3} = c a_{i+1} c a_{i+2} a_i a_i a_{i+3} = \\ &c a_{i+1} c a_{i+2} c a_{i+3} = c c c a_{i+1} a_{i+2} a_{i+3} = c a_{i+1} a_{i+2} a_{i+3} , \end{aligned}$$

$$\begin{aligned}
&ca_ica_{i+1}a_{i+2}a_{i+3}ca_{i+1}a_{i+2}a_{i+3} = \\
&ca_ica_{i+1}a_{i+2}a_{i+3}a_{i+2}a_{i+1}a_{i+3} = \\
&ca_ica_{i+1}a_{i+2}a_{i+2}a_{i+3}ca_{i+1}a_{i+3} = \\
&ca_ica_{i+1}ca_{i+3}a_{i+3}a_{i+1} = \\
&ca_ica_{i+1}cca_{i+1} = ca_ica_{i+1}a_{i+1} = ca_icc = ca_i .
\end{aligned}$$

Dakle, svi elementi reda 4 imaju inti-inverz i diedarskog parnjaka. Za elemente reda 2 to je trivijalno ispunjeno, pa je grupa G anti-inverzna unija diedarskih grupa i nije Booleova. Ona je, uz to, izomorfna grupi $32\Gamma_5 a_2$, a izomorfizam je generisan sledećim preslikavanjem:

$$\varphi = \begin{pmatrix} c & a_1 & a_2 & a_3 & a_4 \\ b_1 & b_1b_2b_3b_5 & b_1b_2b_4b_5 & b_1b_3b_4b_5 & b_2b_3b_4b_5 \end{pmatrix}$$

Proverava se da je φ uzajamno jednoznačno preslikavanje i da je inverz zadat sa:

$$\varphi^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 & b_5 \\ c & ca_3a_4 & ca_2a_4 & a_1a_4 & a_1a_2a_3 \end{pmatrix}$$

Takođe važi $\varphi(a_i^2) = \varphi(c)$, $\varphi(c^2) = 1$, $\varphi(a_ia_j) = \varphi(ca_ja_i)$, što znači da je φ zaista homomorfizam.

Ovaj primer pokazuje da su Booleove polugrupe prava potklasa preseka anti-inverznih polugrupa i unija diedarskih grupa. To je ujedno i najmanja (polu)grupa iz tog preseka koja nije Booleova.

Booleove grupe su vrlo jednostavne strukture. One su subdirektni proizvodi dvoelementnih grupa i komutativne su.

Za reprezentaciju (4.2) grupe G zahvalnost dugujem Savi Krstiću iz Matematičkog instituta u Beogradu.

Slobodna Booleova grupa nad nekim skupom X se lako konstruiše: izomorfna je skupu svih konačnih podskupova od X sa simetričnom razlikom kao grupnom operacijom.

Kod Booleovih polugrupa situacija nije ni izbliza tako jednostavna. Naprimer, one ne moraju da budu komutativne. Kombinovanjem nekih poznatih teorema, lako se dokazuje sledeće tvrđenje:

(4.4) TVRĐENJE. Za Booleovu polugrupu S sledeći uslovi su ekvivalentni:

(a) S je komutativna;

(b) S je polumreža grupa;

(c) S je inverzna.

Dokaz. (a) $\Rightarrow$ (b) Booleova polugrupa je unija grupa, a komutativna unija grupa je polumreža grupa.

(b) $\Rightarrow$ (c) Trivijalno.

(c) $\Rightarrow$ (a) Inverzna Booleova polugrupa je polumreža grupa. Svaka grupa u polumreži je Booleova. Booleove grupe su komutativne, a polumteža komutativnih grupa je komutativna.

Booleove grupe čine varijetet polugrupa (definisan naprimer jednakostima $x^3 = x$, $x^2 = y^2$) i on je atom u mreži varijeteta polugrupa. Između varijeteta Booleovih grupa i Booleovih polugrupa ima beskonačno mnogo varijeteta polugrupa.

Klasa $\{D_0, D_1\}$ je bazisna klasa u Ljapinovom smislu Booleovih polugrupa u odnosu na klasu svih polugrupa.

Koliko su Booleove polugrupe složenije od Booleovih grupa svedoči i sledeći podatak (Gerhard [26]). Slobodna

Booleova polugrupa sa dva generatora ima 132 elementa, a sa tri generatora $390 + 9 \cdot 2^{388}$ elemenata. Odgovarajuće slobodne Booleove grupe imaju 4, odnosno 8 elemenata.

Glavni primer iz ovog odeljka publikovan je u Blagojević [08] u skraćenoj verziji bez podrobnog ulaženja u detalje.

5. SLOBODNA REGULARNA ORTOKRIPTOGRUPA

U kompletno regularnoj polugrupi se na prirodan način može definisati jedna unarna operacija (obično se zove inverzija) kojom se svakom elementu a pridružuje a^{-1} - njegov grupni inverz u maksimalnoj podgrupi koja sadrži element a. U odnosu na ovako uvedenu unarnu operaciju, kompletno regularne polugrupe zadovoljavaju sledeće jednakosti:

$$xx^{-1}x = x, \quad x^{-1}xx^{-1} = x^{-1}, \quad xx^{-1} = x^{-1}x. \tag{5.1}$$

Polugrupe sa dodatnom unarnom operacijom zovu se unarne polugrupe. Kompletno regularne polugrupe mogu da se definišu kao unarne polugrupe koje zadovoljavaju jednakosti (5.1). To znači da čine varijetet unarnih polugrupa (ali ne i varijetet polugrupa). Neka x^o označava xx^{-1}, ili, što je isto, $x^{-1}x$. Lako se proverava da kriptogrupe čine varijetet kompletno regularnih polugrupa zadat jednakošću

$$(x^oy^o)^o = (xy)^o, \tag{5.2}$$

a da ortokriptogrupe takođe čine varijetet kompletno regularnih polugrupa zadat jednakošću

$$x^oy^o = (xy)^o. \tag{5.3}$$

Regularna ortokriptogrupa je ona ortokriptogrupa čiji idempotenti čine regularnu traku. Regularne ortokriptogrupe obrazuju varijetet kompletno regularnih polugrupa zadat jednakostima (5.2) i (5.3) i jednakošću

$$(xyxzx)^o = (xyzx)^o. \tag{5.4}$$

Slobodna ortokriptogrupa je opisana u radu Gerhard, Petrich [28]. Opis je induktivan, tačnije problem reči se rešava induktivno. Namera nam je da u ovom odeljku, koristeći ideje iz pomenutog rada, i ograničavajući se na regularne ortokriptogrupe, opišemo odgovarajuću slobodnu unarnu polugrupu, izbegavajući pri tome induktivnost i rafinirajući opis. Takođe ćemo posmatrati slučajeve kad su maksimalne podgrupe komutativne.

Osnovu za naš rad predstavljaće slobodna unarna polugrupa. Dajemo njenu konstrukciju. Neka je X proizvoljan skup čije elemente ćemo zvati promenljive, i neka je $F(X)$ slobodna polugrupa nad skupom $X \cup \{(,)^{-1}\}$, gde su (i $)^{-1}$ novi simboli koji nisu u X. Slobodna unarna polugrupa nad skupom X, u oznaci $U(X)$, je najmanja potpolugrupa polugrupe $F(X)$ koja zadovoljava uslove:

(i) $X \subseteq U(X)$;

(ii) ako $u \in U(X)$, onda $(u)^{-1} \in U(X)$;

(iii) ako $u,v \in U(X)$, onda $uv \in U(X)$.

Vidi se da se $U(X)$ sastoji tačno od onih reči iz $F(X)$ kod kojih su zagrade pravilno raspoređene. Prilikom pisanja reči iz $U(X)$ prihvatićemo uobičajene konvencije o ispuštanju zagrada. Slobodni unarni monoid nad skupom X, u oznaci $U^1(X)$, dobija se od polugrupe $U(X)$ kad joj se doda prazna reč θ koja se ponaša kao jedinica: $u\theta = u = \theta u$, za svako u iz $U(X)$.

Podsetimo se nekih standardnih pojmova u vezi sa rečima. Inicijalni deo $i(w)$ reči w je reč koja se dobija iz w zadržavanjem prvog pojavljivanja svake promenljive i brisanjem svega ostalog. Finalni deo $f(w)$ reči w dobija se zadržavanjem samo poslednjeg pojavljivanja svake promenljive. Sadržaj $c(w)$ reči w je skup svih promenljivih iz X koje se pojavljuju u w. Redukovana reč $r(w)$ reči w se dobija iz w brisanjem svih podreči oblika u^0, za neko u iz $U(X)$. Jasno je da se $r(w)$ dobija rešavanjem grupnog problema reči na w.

Sada možemo u polugrupi $U(X)$ da definišemo jednu binarnu relaciju ρ na sledeći način: neka su v i w reči iz $U(X)$; tada

$$v \rho w \quad \text{akko} \quad i(v) = i(w),\ r(v) = r(w),\ f(v) = f(w).$$

Očigledno je da je ρ ekvivalencija. Dokažimo i da je kongruencija. Neka $u,v,w \in U(X)$ i $v \rho w$. Tada važi

$$i(uv) = i(ui(v)) = i(ui(w)) = i(uw),$$
$$r(uv) = r(ur(v)) = r(ur(w)) = r(uw),$$
$$f(uv) = f(uf(v)) = f(uf(w)) = f(uw),$$

tj. $uv \rho uw$, što znači da je ρ leva kongruencija. Dualno se dokazuje da je i desna kongruencija, pa možemo da formulišemo sledeću teoremu.

(5.5) TEOREMA. Polugrupa $U(X)/\rho$ je slobodna regularna ortokriptogrupa nad skupom X.

Dokaz. Sledeće jednakosti su očigledne

$$i(ww^{-1}w) = i(w), \quad r(ww^{-1}w) = r(w), \quad f(ww^{-1}w) = f(w)$$

što znači da je $ww^{-1}w \,\rho\, w$, tj. $U(X)/\rho$ zadovoljava jednakost $xx^{-1}x = x$. Slično se dokazuje da zadovoljava i ostale jednakosti iz (5.1), kao i jednakosti (5.2), (5.3) i (5.4), što znači da je $U(X)/\rho$ regularna ortokriptogrupa. Osim toga, preslikavanje $j\colon a \mapsto a\rho$ je injekcija iz X u $U(X)/\rho$ (jer je, naprimer, $i(a) = i(b)$ ako i samo ako $a = b$) i polugrupa $U(X)/\rho$ je generisana sa $\{a\rho\colon a \in X\}$. Neka je S bilo koja regularna ortokriptogrupa i $\varphi\colon X \to S$ proizvoljno preslikavanje. Definišimo preslikavanje $\psi\colon U(X)/\rho \to S$ na sledeći način:

$$(a\rho)\psi = a \;, \quad \text{ako } a \in X,$$
$$((uv)\rho)\psi = (u\rho)\psi(v\rho)\psi,$$
$$((u^{-1})\rho)\psi = (u\varphi)^{-1}.$$

Lako se proverava da je ψ homomorfizam i da je $j\psi = \varphi$. Dakle, $U(X)/\rho$ je slobodna regularna ortokriptogrupa nad skupom X. ●

Ovaj rezultat omogućuje da se konstruiše model slobodne regularne ortokriptogrupe nad skupom X na sledeći način. Neka je $\bar{U}(X)$ skup svih uređenih trojki oblika

$$(a_1 \ldots a_n,\ g,\ a_{1\pi} \ldots a_{n\pi}), \quad n \in \{1, 2, 3, \ldots\},$$

pri čemu je: $a_i \in X$; $a_i \neq a_j$ za $i \neq j$; $g \in G(X)$, gde je $G(X)$ slobodna grupa nad skupom X; $c(g) \subseteq \{a_1, \ldots, a_n\}$; π je neka permutacija skupa indeksa $\{1, 2, \ldots, n\}$. U skupu svih ovakvih trojki definišemo operaciju na sledeći način:

$$(a_1\ldots a_n,\ g,\ a_{1\pi}\ldots a_{n\pi})(b_1\ldots b_m,\ h,\ b_{1\pi'}\ldots b_{m\pi'}) =$$
$$(i(a_1\ldots a_n b_1\ldots b_m),\ gh,\ f(a_{1\pi}\ldots a_{n\pi} b_{1\pi'}\ldots b_{m\pi'})).$$

Posmatrajmo preslikavanje $\alpha\colon U(X)/\rho \to \bar{U}(X)$ definisano sa $\alpha\colon (w\rho) \mapsto (i(w),\ r(w),\ f(w))$ i preslikavanje $\beta\colon \bar{U}(X) \to U(X)/\rho$ definisano sa

$$(a_1\ldots a_n,\ g,\ a_{1\pi}\ldots a_{n\pi})\beta = ((a_1\ldots a_n)^o g(a_{1\pi}\ldots a_{n\pi})^o)\rho.$$

Neposredno se vidi da: α ne zavisi od izbora w, da su α i β homomorfizmi i da su $\alpha\beta$, odnosno $\beta\alpha$ identička preslikavanja na odgovarajućim skupovima. Dakle, $\bar{U}(X)$ je izomorfna slika (model) slobodne regularne ortokriptogrupe $U(X)/\rho$. Napomenimo još da se uslovi $g \in G(X)$, $c(g) \subseteq \{a_1,\ldots,a_n\}$ u definiciji $\bar{U}(X)$ mogu zameniti uslovom $g \in G(\{a_1,\ldots,a_n\})$, gde je $G(\{a_1,\ldots,a_n\})$ slobodna grupa nad skupom $\{a_1,\ldots,a_n\}$.

Iz ovog modela mogu se dobiti modeli za slobodne objekte u podvarijetetima varijeteta regularnih ortokriptogrupa. Naprimer, ispuštanjem druge komponente, tj identifikovanjem svih drugih komponenti, u elementima iz $\bar{U}(X)$, dobićemo model za slobodnu regularnu traku nad skupom X. Prilično dugačak i zapetljan opis slobodne regularne trake u terminima teorije skupova može se naći kod Längera [61].

Regularne ortokriptogrupe kod kojih su maksimalne podgrupe komutativne, mogu se opisati jednakostima (5.1), (5.2), (5.3), (5.4) i jednakošću (Petrich [52])

$$(5.6)\qquad (xy)^o x(xy)^o y(xy)^o = (xy)^o y(xy)^o x(xy)^o.$$

Međutim

$$\begin{aligned}
(5.6) \Leftrightarrow \quad (xy)^o xx^o y^o y(xy)^o &= x^o y^o y(xy)^o xx^o y \\
\Leftrightarrow \quad (xy)^o xy(xy)^o &= x^{-1}xy(xy)^o xyy^{-1} \\
\Leftrightarrow \quad xy &= x^{-1}xyxyy^{-1} \\
\Leftrightarrow \quad x^2y^2 &= (xy)^2
\end{aligned}$$

Prema tome, umesto jednakosti (5.6), možemo da uzmemo jednakost

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

koja je prostija od (5.6). Napomenimo da jednakosti (5.2), (5.3), (5.4) i (5.7) ne čine minimalni skup jednakosti za ovaj varijetet regularnih polugrupa. Naprimer jednakosti (5.4) i (5.7) mogu se zameniti jednakošću (vidi Petrich [54, str. 319], a takođe Nordahl [48, teorema 2.1])

(5.8) $$(xy)^2 = xy$$

Definišimo $e_a(w)$, eksponent promenljive a u reči w, na sledeći način: $e_a(a) = 1$; $e_a(b) = 0$, ako je b promenljiva različita od a; $e_a(vw) = e_a(v) + e_a(w)$; $e_a(w^{-1}) = -e_a(w)$, gde su v, w iz $U(X)$. U skupu $U(X)$ definišimo relaciju $\bar{\rho}$ na sledeći način: ako su v i w iz $U(X)$, onda

$$v\,\bar{\rho}\,w \quad \text{akko} \quad i(v) = i(w),\ f(v) = f(w),\ e_a(v) = e_a(w),$$
$$\text{za svako } a \text{ iz } X.$$

Primetimo da iz $i(v) = i(w)$ sledi $c(v) = c(w)$, pa se uslov $e_a(v) = e_a(w)$ može ograničiti samo na promenljive a iz $c(v)$, jer je za ostale očigledno $e_a(v) = e_a(w) = 0$.

Ovako definisana relacija $\bar{\rho}$ je ekvivalencija. Proverava se da je i kongruencija, pa možemo da formulišemo sledeću teoremu.

(5.9) TEOREMA. Polugrupa $U(X)/\bar{\rho}$ je slobodna regularna ortokriptogrupa sa komutativnim maksimalnim podgrupama.

Dokaz. Očigledno je da $e_a(w^o) = 0$, za svako a i svako w, pa zaključujemo da $r(v) = r(w)$ implicira $e_a(v) = e_a(w)$, za svako a, odakle sledi $\rho \leq \bar{\rho}$, pa imamo

$$U(X)/\bar{\rho} \cong (U(X)/\rho)/(\bar{\rho}/\rho).$$

Odavde sledi da je $U(X)/\bar{\rho}$ regularna ortokriptogrupa. Kako je $i((xy)^2) = i(x^2y^2)$, $f((xy)^2) = f(x^2y^2)$, $e_a((xy)^2) = e_a(x^2y^2)$, za svako a, znači da polugrupa $U(X)/\bar{\rho}$ zadovoljava jednakost (5.7), a to znači da su joj maksimalne podgrupe komutativne. Preslikavanje $a \mapsto a\bar{\rho}$ iz X u $U(X)/\bar{\rho}$ je injekcija i polugrupa $U(X)/\bar{\rho}$ je generisana sa $\{a\bar{\rho}:\ a \in X\}$. Dokaz da je $U(X)/\bar{\rho}$ slobodna dalje teče slično kao u teoremi 5.5. ●

I za $U(X)/\bar{\rho}$ možemo da napravimo model na sledeći način. Neka je $\bar{U}'(X)$ skup svih trojki oblika

$$(5.10) \qquad (a_1\ldots a_n,\ k_1\ldots k_n,\ a_{1\pi}\ldots a_{n\pi}), \quad n \in \{1,2,\ldots\},$$

pri čemu je: $a_i \in X$; $a_i \neq a_j$ za $i \neq j$; k_i ceo broj; π je neka permutacija skupa indeksa $\{1,2,\ldots,n\}$. U skupu $\bar{U}'(X)$ definišimo operaciju na sledeći način:

$$\begin{aligned}(a_1\ldots a_n,\ k_1\ldots k_n,\ a_{1\pi}\ldots a_{n\pi})(b_1\ldots b_m,\ l_1\ldots l_m,\ b_{1\pi'}\ldots b_{m\pi'})\\ = (i(a_1\ldots a_n b_1\ldots b_m),\ r_1\ldots r_p,\ f(a_{1\pi}\ldots a_{n\pi} b_{1\pi'}\ldots b_{m\pi'})),\end{aligned}$$

gde se brojevi r_j dobijaju odvako: ako je $i(a_1\ldots a_n b_1\ldots b_m) = a_1\ldots a_n b_{q_1}\ldots b_{q_s}$, onda $p = n+s$ i

$$\begin{aligned} r_j &= k_j, && \text{ako } a_j \notin \{b_1,\ldots,b_m\} \\ &= k_j + l_i, && \text{ako } b_i = a_j \text{ za neko } i \\ &= l_{q_{j-n}}, && \text{inače} \end{aligned}$$

Posmatrajmo preslikavanje $\bar{\alpha}$: $(X)/\bar{\rho} \to \bar{U}'(X)$ definisano sa:

$$(w\bar{\rho})\bar{\alpha} = (i(w),\ e_{a_1}(w)\ldots e_{a_n}(w),\ f(w)),$$

gde je $i(w) = a_1 \ldots a_n$ i preslikavanje $\bar{\beta}$: $\bar{U}'(X) \to U(X)/\bar{\rho}$ definisano sa

$$(a_1\ldots a_n,\ k_1\ldots k_n,\ a_{1\pi}\ldots a_{n\pi})\bar{\beta} = (a_1^{k}\ldots a_n^{k}(a_{1\pi}\ldots a_{n\pi})^{o})\bar{\rho}.$$

Proverava se da $\bar{\alpha}$ ne zavisi od izbora w, da su $\bar{\alpha}$ i $\bar{\beta}$ homomorfizmi i da su $\bar{\alpha}\bar{\beta}$ i $\bar{\beta}\bar{\alpha}$ identička preslikavanja na odgovarajućim polugrupama. Zaključujemo da su $U(X)/\bar{\rho}$ i $\bar{U}'(X)$ izomorfne polugrupe.

U slučajevima kad je skup X konačan ili prebrojiv, a ti slučajevi su i najinteresantniji, gornji model se može uprostiti. Neka je, naprimer, $X = \{a_1,\ldots,a_n,\ldots\}$ i neka je $\bar{U}''(X)$ skup svih uređenih trojki oblika

$$(a_{i_1}\ldots a_{i_n},\ l,\ a_{i_1\pi}\ldots a_{i_n\pi})$$

gde je $l = (l_j)$ niz celih brojeva dužine $|X|$, takav da važi: ako je $l_j \neq 0$, onda $a_j \in \{a_{i_1},\ldots,a_{i_n}\}$. Ostalo je slično kao u (5.10). U skupu $\bar{U}''(X)$ definišimo operaciju sa

$$\begin{aligned} &(a_{i_1}\ldots a_{i_n},\ l,\ a_{i_1\pi}\ldots a_{i_n\pi})(a_{j_1}\ldots a_{j_m},\ p,\ a_{j_1\pi'}\ldots a_{j_m\pi'}) = \\ &= (i(a_{i_1}\ldots a_{i_n}a_{j_1}\ldots a_{j_m}),\ l+p,\ f(a_{i_1\pi}\ldots a_{i_n\pi}a_{j_1\pi'}\ldots a_{j_m\pi'})) \end{aligned}$$

gde je $l + p = (l_j + p_j)$. Nije teško proveriti da je $\bar{U}''(X)$ izomorfna sa $\bar{U}'(X)$.

Ako skup X nije prebrojiv, onda prethodna konstrukcija za $\bar{U}''(X)$ i dalje važi, s tom razlikom što niz $1=(1_j)$ mora da bude τ-niz, pri čemu pretpostavljamo da je skup X dobro uređen i da je τ njegov ordinalni tip. Naravno, ovakav model se ne može efektivno konstruisati, tačnije efektivan je onoliko koliko je efektivno dobro uređenje skupa X.

I u ovom slučaju moguće je iz gornjih modela dobiti modele slobodnih objekata u raznim podvarijetetima.

Čak i u slučajevima kad je skup X konačan, slobodne polugrupe u teoremama 5.5 i 5.9 su beskonačne. Ali situacija će se promeniti ako za maksimalne podgrupe zahtevamo da budu iz nekog podvarijeteta varijeteta komutativnih grupa. Svaki od tih podvarijeteta je definisan jednakošću $x^{m+1}=x$. Neka A_m označava odgovarajući varijetet. Ova jednakost, zajedno sa jednakostima (5.2), (5.3), (5.4) i (5.7) definiše varijetet regularnih ortokriptogrupa čije su maksimalne podgrupe u A_m.

U skupu $U(X)$ definišimo relaciju $\bar{\rho}_m$ na sledeći način: za v,w iz $U(X)$ biće

$$v\,\bar{\rho}_m\,w \quad \text{akko} \quad i(v)=i(w),\ f(v)=f(w),\ e_a(v)=e_a(w) \pmod m$$
$$\text{za svako } a \text{ iz } X.$$

Relacija $\bar{\rho}_m$ je kongruencija, pa imamo sledeću teoremu.

(5.11) TEOREMA. <u>Polugrupa</u> $U(X)/\bar{\rho}_m$ <u>je slobodna regularna ortokriptogrupa sa maksimalnim podgrupama iz</u> A_m.

<u>Dokaz</u>. Iz $e_a(v)=e_a(w)$ sledi $e_a(v)=e_a(w)\pmod m$ za svako a,v,w, pa $\bar{\rho}\subseteq\bar{\rho}_m$, tj. $U(X)/\bar{\rho}_m\cong(U(X)/\bar{\rho})/(\bar{\rho}_m/\bar{\rho})$.

Dokaz dalje teče slično kao i u prethodnim teoremama, pa ga ne navodimo.

Ako u konstrukciji modela $U'(X)$ i $U''(X)$ zahtevamo da su brojevi iz srednje komponente iz Z_m, umesto iz Z, i ako se sabiraju po modulu m, odgovarajuće polugrupe $\overline{U}'_m(X)$ i $\overline{U}''_m(X)$ koje se pri tome dobiju, biće modeli za $U(X)/\overline{\rho}_m$. Za konačno X one će biti konačne, pa imamo teoremu:

(5.12) TEOREMA. <u>Ako je skup</u> X <u>konačan</u>, <u>onda</u>

$$\left|\overline{U}'_m(X)\right| = \left|U(X)/\overline{\rho}_m\right| = \sum_{n=1}^{|X|}\binom{|X|}{n}(n!)^2 m^n .$$

<u>Dokaz</u>. Posmatrajmo jednu uređenu trojku oblika (5.10) iz $\overline{U}'(X)$ koja se sastoji od tri konačna n-člana niza. Prvi i treći faktor te trojke su permutacije n-članog skupa; drugi faktor je varijacija s ponavljanjem n-te klase od m elemenata, ako su k_i iz Z_m. Kako su sva tri faktora nezavisni jedan od drugoga, takvih trojki n-članih nizova ima $(n!)^2 m^n$. Dužine pomenutih nizova su određene svim nepraznim podskupovima skupa X, a njih ima, s obzirom da je X konačan, $\sum_{n=1}^{|X|}\binom{|X|}{n}$ i tvrđenje teoreme neposredno sledi. ●

Na sličan način se može izračunati broj elemenata konačno generisane slobodne polugrupe u svim podvarijetetima varijeteta regularnih ortokriptogrupa sa komutativnim maksimalnim podgrupama. Ti varijeteti su ne samo varijeteti unarnih polugrupa, nego i varijeteti polugrupa, a odgovarajuće definišuće jednakosti dobijaju se smenom x^{-1} sa x^{m-1}, ako su u pitanju podgrupe iz A_m.

Većina rezultata iz ovog odeljka, osim konstrukcija za $U'(X)$ i $U''(X)$ su iz Blagojević, Krapež [09].

LITERATURA

01 D. Allen, A generalization of the Rees theorem to a class of regular semigroups, Semigroup Forum 2(1971), 321 - 331.

02 B. Alimpić, Some congruences on generalized inverse semigroups, (4. konf. "Algebra i ligika", Zagreb, 7 - 9 jun 1984), Mat. Inst., Novi Sad, 1985, 1 - 7.

03 ______, Certain idempotent separating congruences on orthodox semigroups, (3. algebarska konf., Beograd, 3 - 4 dec. 1982), Mat. Inst., Novi Sad, 1983, 9 - 16.

04 B. Alimpić, D. Krgović, Idempotent pure congruences on Clifford semigroups, (2. algebarska konf., Novi Sad, 30 maj - 1 jun 1981), Mat. Inst., Novi Sad, 1982,

05 ______, Some congruences on regular semigroups, (Conf. Semigroups, Oberwolfach, feb. 1986), u štampi.

06 J.E. Ault, M. Petrich, The structure of ω-regular semigroups, J. Reine Agnew. Math. 251(1971), 110 - 141.

07 D. Blagojević, More on anti-inverse semigroups, Publ. Inst. Math. (Beograd) 31(45)(1982), 9 - 13.

08 ______, Unions of dihedral semigroups, Semigroup Forum 33(1986), 293 - 298.

09 D. Blagojević, A. Krapež, Free regular orthocryptogroup, (3. algebarska konf., Beograd, 3 - 4 dec. 1982), Mat. Inst., Novi Sad, 1983, 17 - 21.

10 S. Bogdanović, On Anti-inverse semigroups, Publ. Inst. Math. (Beograd) 25(39)(1979), 25 - 41.

11 S. Bogdanović, S. Crvenković, On some classes of semigroups, Zb. Rad. Prirod.-Mat. Fak. Univ. u Novom Sadu 9(1979), 153 - 160.

12 S. Bogdanović, S. Milić, V. Pavlović, Anti-inverse semigroups, Publ. Inst. Math. (Beograd) 24(38)(1978), 19 - 28.

13 T.C. Brown, On the finiteness of semigroups in which $x^r = x$, Math. Proc. Cambridge Phil. Soc. 60(1964), 1028 - 1029.

14 A.H. Clifford, Semigroups admitting relative inverses, Ann. Math. 42(1941), 1037 - 1049.

15 ______, Bands of semigroups, Proc. Amer. Math. Soc. 5(1954), 499 - 504.

16 ______, The structure of orthodox unions of groups, Semigroup Forum 3(1972), 283 - 337.

17 ______, A structure theorem for orthogroups, J. Pure Appl. Algebra 8(1976), 23 - 50.

18 ______, The fundamental representation of a completely regular semigroup, Semigroup Forum 12(1976), 341 - 346.

19 ______, The free completely regular semigroup on a set, J. Algebra 59(1979), 431 - 451.

20 A.H. Clifford, G.B. Preston, The Algebraic Theory of Semigroups, Math. Surveys 7, Amer. Math. Soc., Providence, Vol. I (1960), Vol. II (1967).

21 R. Croisot, Demi-groupes inversifs et demi-groupes rèunions de demi-groupes simples, Ann. Sci. Ecole Norm. Sup. 70(1953), 361 - 379.

22 S. Crvenković, On some properties of a class of completely regular semigroups, Zb. Rad. Prirod.-Mat. Fak. Univ. u Novom Sadu 9(1979), 153 - 160.

23 C. Eberhart, W. Williams, Elementary orthodox semigroups, Semigroup Forum 29(1984), 351 - 364.

24 C.C. Edwards, The structure of L-unipotent semigroups, Semigroup Forum 18(1979), 189 - 199.

25 R. Feigenbaum, Regular semigroup congruences, Semigroup Forum 17(1979), 373 - 377.

26 J.A. Gerhard, The word problem for semigroups satisfying $x^3 = x$, Math. Proc. Cambridge Phil. Soc. 84(1978), 11 - 19.

27 J.A. Gerhard, Free completely regular semigroups; I Representation; II Word problem, J. Algebra, 82(1983), 135-142, 143-156.

28 J.A. Gerhard, M. Petrich, The word problem for orthogroups, Canad. J. Math. 33(1981), 893-900.

29 ______, All varieties of orthogroups, Semigroup Forum 31(1985), 311-352.

30 J.A. Green, On the structure of semigroups, Ann. Math. 54(1951), 163-172.

31 J.A. Green, D. Rees, On semigroups in which $x^r = x$, Proc. Cambridge Phil. Soc. 48(1952), 35-40.

32 G. Grätzer, Universal Algebra, Van Nostrand, 1962.

33 P.A. Grillet, The structure of regular semigroups, I, II, III, IV, Semigroup Forum 8(1974), 177-183, 254-259, 260-265, 368-373.

34 J. Grossman, W. Magnus, Groups and Their Graphs, Random House, New York, 1964.

35 M. Hall, Jr, K. Senior, The Groups of Order 2^n $(n \leq 6)$, Macmillan, New York, 1964.

36 T.E. Hall, On regular semigroups, J. Algebra 34(1975) 375-385.

37 J.M. Howie, An Introduction to Semigroup Theory, Academic Press, London, 1976.

38 D. Krgović, Inverse congruences on orthodox semigroups, (4. konf "Algebra i logika", Zagreb, 7-9 jun 1984), Mat. Inst., Novi Sad, 1985.

39 D. Krgović, Idempotent separating congruences on regular semigroups, (3. algebarska konf., Beograd, 3-4 dec. 1982), Mat. Inst., Novi Sad, 1983.

40 G. Lallement, Structure theorems for regular semigroups, Semigroup Forum 4(1972), 95-123.

41 G. Lallement, M. Petrich, Structure d'une classe de demi--groupes réguliers, J. Math. Pures Appl. 48(1969), 345-397.

42 J. Leech, The structure of a band of groups, Mem. Amer. Math. Soc. 157, Providence, 1975.

43 E.S. Ljapin, Polugruppy, Fizmatgiz, Moskva, 1960.

44 S. Milić, S. Bogdanović, On a class of anti-inverse semigroups, Publ. Inst. Math. (Beograd) 25(39)(1979), 95 - 100.

45 D.D. Miller, A.H. Clifford, Regular D-classes in semigroups, Trans. Amer. Math. Soc. 82(1956), 270 - 280.

46 K.S.S. Nambooripad, Structure of regular semigroups I, II, Semigroup Forum 9(1975), 354 - 371.

47 J. von Neumann, On regular rings, Proc. Nat. Acad. Sci. USA 22(1936), 707 - 713.

48 T. Nordahl, Semigroups satisfying $(xy)^m = x^m y^m$, Semigroup Forum 8(1974), 332 - 346.

49 M. Petrich, Introduction to Semigroups, Merrill, Columbus, Ohio, 1973.

50 ______, Regular semigroups which are subdirect products of a band and a semilattice of groups, Glasgow Math. J. 14(1973), 27 - 49.

51 ______, Structure of completely regular semigroups, Trans. Amer. Math. Soc. 189(1974), 211 - 236.

52 ______, Varieties of orthodox bands of groups, Pacific J. Math. 58(1975), 209 - 217.

53 ______, Lectures in Semigroups, Akademie-Verlag, Berlin, 1977.

54 ______, Structure of Regular Semigroups, Cahiers mathématiques 11, Univ. Sci. Techn. Languedoc, Montpellier, 1977.

55 L. Polák, On varieties of completely regular semigroups, Semigroup Forum 32(1975), 97 -

56 D. Rees, On semi-groups, Proc. Cambridge Phil. Soc. 36(1940), 387 - 400.

57 ______, Note on semi-groups, Proc. Cambridge Phil. Soc. 37(1941), 434 - 435.

58 J.C. Sharp, Jr, Anti-regular semigroups, Publ. Math. Inst. (Beograd) 24(38)(1978), 147 - 150.

59 A.K. Suškevič, Uber die endlichen Gruppen ohne das Gesetz der eindeutinged Umkehrbarkeit, Math. Ann. 99(1928), 30 - 50.

60 R.J. Warne, On the structure of semigroups which are unions of groups, Trans. Amer. Math. Soc. 186(1983), 385 - 401.

61 H. Länger, The free algebra in the variety generated by quasy-trivial semigroups, Semigroup Forum 20(1980), 151 - 156.