UNIVERZITET U NOVOM SADU
PRIRODNO–MATEMATIČKI FAKULTET
INSTITUT ZA MATEMATIKU

MILOVAN VINČIĆ

Involutivne algebre

– DOKTORSKA DISERTACIJA –

Novi Sad, 2001.

Sadržaj

Predgovor

Materijal sadržan u ovoj disertaciji spada u oblast matematike koja se naziva *algebra*. Zadatak savremene algebre, kao matematičke oblasti koja, ne ulazeći u prirodu i građu elemenata posmatrane strukture, ispituje njihovu povezanost i odnose, je da istraži koje su to bitne, apstraktne osobine struktura koje se pojavljuju u različitim ambijentima u matematici.

Tema ovog rada je *involucija* u algebarskim strukturama. Involucije su bijektivna preslikavanja koja se poklapaju sa svojim inverznim funkcijama. Javljaju se u gotovo svim matematičkim disciplinama. Podsetimo se samo projektivne geometrije, teorije algebarskih krivih, inverzije u euklidskoj geometriji i njenog značaja u modelima hiperboličke geometrije, teorije grupa, teorije matrica, teorije operatora i mnogih drugih.

Involucija je važna komponenta u matematičkom izučavanju prirodnih fenomena simetrije. Ta činjenica sigurno dovodi involuciju u prvi plan, kada su savremena istraživanja u pitanju. Zadatak ovog rada se ograničava na to da prikaže teoriju *involutivnih algebri*, odnosno neke rezultate u okvirima ove teorije. Tako, naš je glavni cilj da što podrobnije otkrijemo međudejstva algebarskih zakona i involucije, mnoge načine njihovog kombinovanja koji sinhrono daju jednu novu algebarsku teoriju.

Rad je podeljen na četiri dela. U prvom delu govorimo o *involutivnim Płonkinim sumama* proizvoljnih klasa algebri. Ispostavilo se da su mnoge konstrukcije algebri u klasičnim involutivnim strukturama samo specijalan slučaj ovih suma. Materijal izložen u ovoj glavi je naš skromni doprinos univerzalnoj algebri i dobijen je u saradnji sa I. Dolinkom.

Drugi deo rada govori o *involutivnim polugrupama*. Involutivne polugrupe predstavljaju široko uopštenje pojma grupe. Teorija grupa je do danas ostala najprirodnija, najjača i najbolje izučavana primena involucije u algebri. S druge strane, teorija involutivnih polugrupa se ne može podvesti pod teoriju grupa ili ma koju poznatu algebarsku teoriju, već predstavlja jednu samostalnu, nezavisnu oblast algebre. Veći deo magistarske teze autora ove disertacije bio je posvećen involutivnim polugrupama. Materijal o Baerovim *-polugrupama ovde se iznosi prvi put na našem jeziku. Deo rada, koji se odnosi na globalnu određenost regularnih *-traka, originalni je doprinos autora ovoj problematici, uz doprinose iznete u pomenutoj magistarskoj tezi.

Treći deo rada sadrži problematiku vezanu za *involutivne poluprstene*. Ovaj deo disertacije od originalnih priloga sadrži dokaz globalne neodređenosti involutivnih poluprstena koji je preuzet iz magistarske teze. Veći deo glave sadrži originalne rezultate dr Igora Dolinke, mladog docenta PMF-a u Novom Sadu, čiji su naučni prilozi već poznati van granica Jugoslavije. Takođe, navedeni su rezultati S. Crvenkovića, I. Dolinke i Z. Ésika koji se odnose na algebre formalnih jezika. Ove algebre imaju strukturu poluprstena, a involucija, u ovom ambijentu, jeste pisanje slova date reči obrnutim redom. Ovo je moderna oblast algebre i teorijskog računarstva koja se nalazi u velikom usponu.

Četvrti deo disertacije odnosi se na *involutivne prstene*, temu o kojoj su napisane knjige poznatih autora. Prvo se govori o involutivnim prim prstenima tj. rezultatima I. Hersteina, a zatim o specijalnim involutivnim prstenima i rezultatima M. Yamade. Poslednji deo četvrte glave govori o poddirektno nesvodljivim involutivnim prstenima i poznatoj teoremi N. Jacobsona u ambijentu prstena sa involucijom. Ovaj deo disertacije je originalni doprinos autora navedenoj problematici i dobijen je u saradnji sa S. Crvenkovićem i I. Dolinkom.

Uvodni deo disertacije sadrži *osnovne pojmove* neophodne za razumevanje prezentiranih rezultata i daleko je od sveobuhvatnog. Dati su dokazi nekih elementarnih tvrđenja više kao ilustracije tehnika koje se koriste u radu.

Metodologija našeg rada bila je dvojaka: prezentirane klase algebri su ovde tretirane kako sa stanovišta klasične algebre, tako i korišćenjem aparata univerzalne algebre.

Ispostavlja se da su involutivne algebre lepa i zanimljiva tema toliko široka, da je gotovo možemo nazvati multidisciplinarnom. Iako je reč o oblasti koja je veoma mlada, pošto se punim intenzitetom razvija tek poslednjih dvadesetak godina, ona je brzo izrasla u jednu razuđenu teoriju, koja predstavlja izuzetno široko polje naučnog rada. Iz tog razloga, ovaj rad nema pretenziju da bude sveobuhvatni pregled teorije involutivnih algebri, već predstavlja jedan presek kroz problematiku koji reflektuje lični ukus autora.

Literatura, koja je navedena na kraju rada, takođe je daleko od sveobuhvatne. Skoro sve navedene reference korišćene su u tekstu ili su u tesnoj vezi sa problematikom.

Disertacije su ozbiljni tekstovi, u kojima ne priliči autorima da glasno iskazuju svoje oduševljenje problematikom kojom se bave. Ipak, makar u predgovoru, recimo da nam je veliko zadovoljstvo baviti se ovom prelepom oblašću matematike. Reč *matematika* je čudna samo zato što mnogi od nas ne znaju da potiče od starogrčke reči koja znači *učiti*. Radeći na magistarskoj tezi i ovoj doktorskoj disertaciji, autor je mnogo naučio o matematici, a posebno o algebri. Prirodno-matematički fakultet u Novom Sadu je najjača naučna institucija u Jugoslaviji kada je algebra u pitanju. Ova disertacija samo je mali izraz zahvalnosti za svu onu bratsku, nesebičnu pomoć koju sam dobio na Institutu za matematiku Prirodno-matematičkog fakulteta u Novom Sadu.

Posebnu zahvalnost dugujem prof. dr Siniši Crvenkoviću, mom mentoru, i mom saradniku, doc. dr Igoru Dolinki. Bila mi je velika čast da radim i učim zajedno s njima, i da zajednički ulazimo u tajne involutivnih algebri. Njihova pomoć i uloga u mom matematičkom napredovanju je nemerljiva. Takođe, zahvaljujem se i prof. dr Gradimiru Vojvodiću i prof. dr Đuri Pauniću, na podršci koju su mi neprestano pružali tokom izrade ove disertacije. Najzad, ne mogu a da ne spomenem moje drage kolege, prof. dr Daniela A. Romana i prof. dr Milana Janjića, koji su mi nakon pakla bosnasko-hecegovačkog građanskog rata pružili jednu sasvim novu životnu i profesionalnu šansu u akademskoj sredini Univerziteta u Banja Luci. Njihovo poverenje mi je bila značajna inspiracija tokom mog rada.

Banja Luka, 10. maj 2001.

0.1. Polugrupe

Polugrupa je skup S zajedno sa asocijativnom binarnom operacijom na S. Operacija $S \times S \to S$ polugrupe $\mathbf{S} = (S, \cdot)$ obično se piše kao množenje

$$(x, y) \mapsto xy.$$

Asocijativnost je osobina

$$x(yz) = (xy)z, \quad \text{za sve} \quad x, y, a \in S.$$

Jedinični element polugrupe $\mathbf{S}$ je element $e \in S$ takav da važi

$$ex = xe = x, \quad \text{za sve} \quad x \in S.$$

Polugrupe koje imaju jedinični element zovu se **monoidi**.

Slično, **nulti element** ili **nula** je element $z \in S$ takav da važi

$$S \neq \{z\}, \text{ i } zx = xz = z, \text{ za svako } x \in S.$$

Ako polugrupa $\mathbf{S}$ nema jedinični (nulti) element, onda sa $\mathbf{S}^1$ ($\mathbf{S}^0$) označavamo polugrupu čiji je nosač $S \cup \{1\}$ ($S \cup \{0\}$) i 1 (0) je jedinični (nulti) element za $\mathbf{S}^1$ ($\mathbf{S}^0$).

Polugrupa je **komutativna** ako važi $xy = yx$ za sve $x, y \in S$.

Definicija operacije na polugrupi $\mathbf{S}$ prirodno se proširuje na podskupove nosača S. Ako su $A, B \subseteq S$, onda je po definiciji

$$AB = \{ab \in S \mid a \in A, b \in B\}$$

podskup od S. Singltoni se u proizvodu podskupova pišu bez zagrada, npr. $\{a\}B = aB$.

Idempotent polugrupe $\mathbf{S}$ je element $e \in S$ za koji važi $e^2 = e$. Tada je $e^n = e$, za sve $n > 0$. Jedinični i nulti element, kada postoje, su idempotentni.

Traka je polugrupa u kojoj su svi elementi idempotentni.

PROPOZICIJA 0.1.1. *Komutativna polugrupa* S *u kojoj je svaki element idempotent, može se parcijalno urediti tako da važi:* $a \leq b \Leftrightarrow ab = a$. *Tada je* S *donja polumreža, u kojoj je* $\mathsf{infimum}(a,b) = ab$. *Obratno,* infimum *je u donjoj polumreži asocijativna i komutativna operacija za koju je svaki element idempotent.*

Dokaz. Neka su $a, b \in S$. Tada je $a \leq a$, s obzirom da je a idempotent; $a \leq b \leq a$ implicira $a = b$, s obzirom da je S komutativna polugrupa; $a \leq b \leq c$ implicira $ab = b$, $bc = c$, $ac = abc = ab = a$, pa sledi $a \leq c$. Tako, $\leq$ je relacija parcijalnog uređenja. Za proizvoljne $a, b \in S$ imamo $ab \leq a$, jer je $aba = aab = ab$, i $ab \leq b$. Ako ja sada $x \leq a$ i $x \leq b$, onda je $xab = xb = x$ tj. $x \leq ab$. Sledi, S je donja polumreža u kojoj je $\mathsf{infimum}(a,b) = ab$.

Obrat sledi direktno. □

Uobičajeno je da $\mathsf{infimum}(a,b)$ označavamo sa $a \wedge b$.

Zbog prethodne propozicije koristimo izraz **polumreža** za komutativnu polugrupu u kojoj je svaki element idempotent.

Generatori su elementi polugrupe S takvi da je svaki element iz S proizvod generatora. Svaka polugrupa ima bar jedan skup generatora.

Kongruencije na datoj pougrupi S su realcije ekvivalencije na nosaču S koje su saglasne sa operacijom polugrupe.

Relacija **jednakosti** na skupu X ili **identična** relacija je

$$\Delta_X = \{(x,x) \mid x \in X\}.$$

Na skupu $\mathcal{P}(X \times X)$ svih binarnih relacija na skupu X definišemo operaciju $\circ$ na sledeći način

$$\rho \circ \sigma = \{(x,y) \in X \times X \mid (\exists z \in X)(x,z) \in \rho \text{ i } (z,x) \in \sigma\},$$

za sve $\rho, \sigma \in \mathcal{P}(X \times X)$.

Lako se pokazuje da za sve $\rho, \sigma, \tau \in \mathcal{P}(X \times X)$ važi

$$\rho \subseteq \sigma \Rightarrow \rho \circ \tau \subseteq \sigma \circ \tau \text{ i } \tau \circ \rho \subseteq \tau \circ \sigma.$$

Takođe, jednostavno se pokazuje da je operacija $\circ$ asocijativna u $\mathcal{P}(X \times X)$,

$$(\rho \circ \sigma) \circ \tau = \rho \circ (\sigma \circ \tau).$$

Prema tome, $\mathbf{B}(X) = (\mathcal{P}(X \times X), \circ)$ je **polugrupa binarnih relacija** na X.

Za svako $\rho \in \mathcal{P}(X \times X)$ definišemo ρ^{-1}, **inverz** od ρ, kao

$$\rho^{-1} = \{(x,y) \in X \times X \mid (y,x) \in \rho\}.$$

Lako se pokazuje da je za sve $\rho, \sigma, \rho_1, \rho_2, \ldots, \rho_n \in \mathcal{P}(X \times X)$,

$$\begin{aligned} (\rho^{-1})^{-1} &= \rho, \\ (\rho_1 \circ \rho_2 \circ \ldots \circ \rho_n)^{-1} &= \rho_n^{-1} \circ \ldots \circ \rho_2^{-1} \circ \rho_1^{-1}, \\ \rho \subseteq \sigma &\Rightarrow \rho^{-1} \subseteq \sigma^{-1}. \end{aligned}$$

Relacija $\rho \in \mathcal{P}(X \times X)$ je **relacija parcijalnog uređenja** na X ako važi

$$\begin{array}{rcll} \Delta_X & \subseteq & \rho & \text{– refleksivnost,} \\ \rho \cap \rho^{-1} & = & \Delta_X & \text{– antisimetričnost,} \\ \rho \circ \rho & \subseteq & \rho & \text{– tranzitivnost.} \end{array}$$

Primetimo da se simetričnost relacije $\rho \in \mathcal{P}(X \times X)$ izražava uslovom $\rho = \rho^{-1}$.

Ako je $\rho \in \mathcal{P}(X \times X)$, onda je familija ekvivalencija na X koje sadrže ρ neprazna, s obzirom da je $X \times X$ jedna takva relacija. Sledi da je presek svih relacija ekvivalencija koje sadrže ρ jedinstvena minimalna ekvivalencija **generisana** sa ρ i nju označavamo sa ρ^e.

Neka je $\sigma \in \mathcal{P}(X \times X)$ i $\Delta_X \subseteq \sigma$. Tada imamo

$$\sigma \subseteq \sigma \circ \sigma \subseteq \sigma \circ \sigma \circ \sigma \subseteq \ldots$$

Relacija

$$\sigma^{\infty} = \cup\{\sigma^n \mid n \geq 1\},$$

se naziva **tranzitivno zatvorenje** relacije σ. Lako se pokazuje da je σ^{∞} najmanja tranzitivna relacija na X koja sadrži σ.

PROPOZICIJA 0.1.2. *Za svaku relaciju ρ na skupu X važi*

$$\rho^e = [\rho \cup \rho^{-1} \cup \Delta_X]^{\infty}.$$

Dokaz. Relacija $\varepsilon = [\rho \cup \rho^{-1} \cup \Delta_X]^{\infty}$ je tranzitivna i sadrži ρ. Kako važi

$$\Delta_X \subseteq \rho \cup \rho^{-1} \cup \Delta_X \subseteq \varepsilon,$$

ε je refleksivna. Naravno, relacija $\sigma \subseteq \rho \cup \rho^{-1} \cup \Delta_X$ je simetrična i za svako $n \in \mathbb{N}$ važi

$$\sigma^n = (\sigma^{-1})^n = (\sigma^n)^{-1}.$$

Sledi da je σ^n simetrična relacija. Takođe, $\varepsilon = \sigma^{\infty}$ je simetrična, s obzirom da važi

$$\begin{aligned} (x, y) \in \varepsilon &\Rightarrow (\exists n \in \mathbb{N})(x, y) \in \sigma^n \\ &\Rightarrow (\exists n \in \mathbb{N})(y, x) \in \sigma^n \\ &\Rightarrow (y, x) \in \varepsilon. \end{aligned}$$

Pokazali smo da je ε ekvivalencija koja sadrži ρ.

Pretpostavimo da je τ ekvivalencija koja sadrži ρ. Tada je $\Delta_X \subseteq \tau$ i $\rho^{-1} \subseteq \tau^{-1} = \tau$. Prema tome,

$$\sigma = \rho \cup \rho^{-1} \cup \Delta_X \subseteq \tau.$$

Štaviše,

$$\sigma \circ \sigma \subseteq \tau \circ \tau = \tau,$$

i uopšte, $\sigma^n \subseteq \tau$ za sve $n \geq 1$. Sledi da je $\varepsilon = \sigma^\infty \subseteq \tau$. Ovim smo pokazali da je $\varepsilon = [\rho \cup \rho^{-1} \cup \Delta_X]^\infty$ najmanja ekvivalencija na X koja sadrži ρ. Tako,

$$\rho^e = [\rho \cup \rho^{-1} \cup \Delta_X]^\infty,$$

što je i trebalo dokazati. □

Gornje tvrđenje možemo izraziti na jednostavniji način.

PROPOZICIJA 0.1.3. *Ako je ρ binarna relacija na skupu X i ρ^e najmanja ekvivalencija na X koja sadrži ρ, onda $(x,y) \in \rho^e$ ako i samo ako $x = y$ ili za neko $n \in \mathbb{N}$ postoji niz*

$$x = z_1, z_2, \ldots, z_n = y$$

u kome je za svako $i \in \{1, 2, \ldots, n-1\}$ ili $(z_i, z_{i+1}) \in \rho$, ili $(z_{i+1}, z_i) \in \rho$.

Neka je $\rho \in X \times X$. **Refleksivno-tranzitivno zatvorenje** relacije ρ (u oznaci ρ^{rtc}) jeste najmanja relacija skupa X koja sadrži ρ, refleksivna je i tranzitivna. Po definiciji, dakle, imamo da je

$$\rho^{\mathrm{rtc}} = \cap\{\sigma \subseteq X \times X \mid \rho \subseteq \sigma \text{ i } \Delta_X \subseteq \sigma \text{ i } \sigma \circ \sigma \subseteq \sigma\}.$$

Sledeća propozicija daje konstruktivniji opis refleksivno-tranzitivnog zatvorenja neke relacije.

PROPOZICIJA 0.1.4. *Neka je $\rho \in \mathcal{P}(X \times X)$. Tada za sve $a, b \in X$ važi $(a,b) \in \rho^{\mathrm{rtc}}$ ako i samo ako je $a = b$ ili postoje $z_0, z_1, \ldots, z_n \in X$ tako da je $z_0 = a$, $z_n = b$ i $(z_i, z_{i+1}) \in \rho$ za sve $0 \leq i \leq n$.*

Dokaz. Nije teško dokazati da važi

$$\rho^{\mathrm{rtc}} = \Delta_X \cup \rho \cup \rho^2 \cup \ldots \cup \rho^n \cup \ldots$$

iz čega direktno sledi tvrđenje. □

Neka je $\mathbf{S} = (S, \cdot)$ proizvoljna polugrupa. Preslikavanje $\lambda_a : S \to S$ dato sa $\lambda_a(x) = ax$, gde je $a \in S$ fiksno, naziva se **leva translacija** od $\mathbf{S}$. Jasno, (relacijski) proizvod dve leve translacije jeste leva translacija. Ovo znači da leve translacije čine polugrupu u odnosu na kompoziciju preslikavanja.

Analogno definišemo **desnu translaciju** $\rho_a : x \mapsto xa$.

Označimo sa $T(X)$ skup svih funkcija (transformacija) skupa X u X. Očigedno, važi $T(X) \subseteq \mathcal{P}(X \times X)$. Takođe, $\mathcal{T}(X) = (T(X), \circ)$ je polugrupa koja je, jasno, potpolugrupa od $\mathbf{B}(X)$.

Propozicija 0.1.5. *Svaka polugrupa sa jedinicom je izomorfna nekoj polugrupi transformacija.*

Dokaz. Neka je $(M, \cdot)$ dati monoid sa jedinicom e. Definišimo preslikavanje $\psi : M \to T(M)$ na sledeći način: $\psi(a) = \rho_a$. Treba dokazati da je ψ potapanje, tj. da je homomorfizam i da je "1-1".

Preslikavanje ψ je homomorfizam polugrupe $(M, \cdot)$ u polugrupu $(T(M), \circ)$, jer važi

$$\psi(ab) = \rho_{ab} = \rho_a \circ \rho_b = \psi(a) \circ \psi(b).$$

Zaista, za svako $x \in X$ imamo:

$$\rho_{ab}(x) = x(ab) = (xa)b = \rho_b(xa) = \rho_b(\rho_a(x)) = (\rho_a \circ \rho_b)(x).$$

S druge strane, ψ je "1-1", jer ako je $a \neq b$, onda je $f_a(e) \neq f_b(e)$, pa imamo da je $f_a \neq f_b$. □

Propozicija 0.1.6. *Svaka polugrupa se može potopiti u polugrupu sa jedinicom.*

Dokaz. Neka je $(S, \cdot)$ polugrupa i e neki element $e \notin S$. Definišimo na $S \cup \{e\}$ operaciju $\odot$ tako da se na elementima iz S poklapa sa operacijom $\cdot$, i neka je $x \odot e = e \odot x = x$, za sve $x \in S \cup \{e\}$. Na taj način se dobija monoid, što je lako proveriti. Naravno, preslikavanje $\psi : S \to S \cup \{e\}$ definisano sa $\psi(x) = x$, za sve $x \in S$, jeste potapanje polugrupe $(S, \cdot)$ u polugrupu sa jedinicom $(S \cup \{e\}, \odot)$. □

Teorema 0.1.7. (o reprezantaciji polugrupa) *Svaka polugrupa je izomorfna nekoj polugrupi transformacija.*

Dokaz. Direktna posledica prethodne dve propozicije. □

Ako se na nepraznom skupu S definiše operacija množenja sa $ab = a$ za sve $a, b \in S$, dobijamo **polugrupu levih nula**. Dualno definišemo i polugrupu **desnih nula**.

Direktan proizvod polugrupa S i **T** je polugrupa sa nosačem $S \times T$ na kome je definisana operacija po komponentama. Na primer, ako je **L** polugrupa levih nula i **R** polugrupa desnih nula, njihov proizvod **L** $\times$ **R** je poznat pod imenom **pravougaona traka**, i njegova operacija ima oblik

$$(a,b)(c,d) = (a,d), \quad a,c \in L,\ b,d \in R.$$

Polugrupa S se naziva **normalna** ili **medijalna** ako je $abcd = acbd$, za sve $a, b, c, d \in S$. Idempotentna normalna polugrupa se naziva **normalna traka**.

Desni ideal A polugrupe S je neprazan podskup A od S tako da je $ax \in A$ za sve $a \in A$, $x \in S$. Analogno se definiše **levi ideal** od S. Kažemo da je **A ideal** od S ako je **A** levi i desni ideal od **S**. Kako je S takođe ideal, i presek ideala je ideal, možemo govoriti o idealu generisanom nepraznim podskupom A od S. Ako je $A = \{a\}$ singlton, onda govorimo o **glavnom idealu** generisanom sa a.

Element $x \in S$ je **inverz** za $a \in S$ ako je $a = axa$ i $x = xax$. Skup inverza za a označavamo sa $V(a)$ i a je **regulran** ako je $V(a)$ neprazan skup. Skup regularnih elemenata od **S** označavamo sa $Reg(\mathrm{S})$ i kažemo da je **S regularna** ako je $Reg(\mathrm{S}) = \mathrm{S}$. Jednačina $a = axa$ implicira da $xax \in V(a)$, kao i to da su ax i xa idempotenti. Regularna polugrupa u kojoj svaki element a ima jedinstven inverz a^{-1} zove se **inverzna polugrupa**.

Sa $E(\mathrm{S})$ označavamo skup svih idempotenata polugrupe **S**.

PROPOZICIJA 0.1.8. *Sladeći uslovi su ekvivalentni za polugrupu* S:

(i) S *je regularna i* $E(\mathrm{S})$ *je polumreža;*

(ii) Svaki glavni desni ideal i svaki glavni levi ideal od S *ima jedinstveni idempotentni generator;*

(iii) S *je inverzna polugrupa.*

Dokaz. $(i) \Rightarrow (ii)$. Neka $a \in S$, $a' \in V(a)$; tada je $aS = aa'S$, $Sa = Saa'$, tako da svaki glavni desni i levi ideal ima idempotentni generator. Pretpostavimo da $e, f \in E(\mathrm{S})$ i $eS = fS$. Uzmimo $x, y \in S$ tako da je $ex = f$ i $fy = e$. Kako idempotenti komutiraju, dobijamo

$$e = fy = f^2y = fe = ef = e^2x = ex = f.$$

$(ii) \Rightarrow (iii)$. Neka $a', a'' \in V(a)$, $a \in S$. Tada je $aa'S = aS = aa''S$, što implicira $aa' = aa''$, i dualno $a'a = a''a$. Tada je

$$a' = a'aa' = a'aa'' = a''aa'' = a''.$$

$(iii) \Rightarrow (i)$. Neka $e, f \in E(\mathrm{S})$ i $x = (ef)^{-1}$. Lako se uveravamo da su xe i fx oboje inverzi od ef, i prema tome $x = xe = fx$, pa je $x^2 = x$. Ali, tada je $x = x^{-1} = ef$, tj. $ef \in E(\mathrm{S})$. Možemo, dalje, proveriti da je fe inverz od ef, i prema tome, $ef = fe$ što znači da je $E(\mathrm{S})$ polumreža. □

Regularne polugrupe čiji idempotenti čine traku nazivaju se **ortodoksne**.

PROPOZICIJA 0.1.9. *Sledeći uslovi su ekvivalentni za regularnu polugrupu* S*:*

(i) S *je ortodoksna;*

(ii) Ako $a, b \in S$, $a' \in V(a)$, $b' \in V(b)$, *onda* $b'a' \in V(ab)$*;*

(iii) Ako $e \in E(\mathrm{S})$, $x \in V(e)$, *onda* $x \in E(\mathrm{S})$.

Dalje, u bilo kojoj ortodoksnoj polugrupi $aea', a'ea \in E(\mathrm{S})$ *za sve* $a \in S$, $a' \in V(a)$, $e \in E(\mathrm{S})$.

Dokaz. Poslednje tvrđenje se pokazuje na sledeći način:

$$aea' = aea'aa' = a(ea'a)^2a' = aea'aa' = aea'aea',$$

i na sličan način imamo da je $a'ea$ idempotent.

$(i) \Rightarrow (ii)$. Pošto je S ortodoksna imamo

$$abb'a'ab = aa'abb'a'abb'b = a(a'abb')^2b = aa'abb'b = ab$$

i slično, $b'a'abb'a' = b'a'$.

$(ii) \Rightarrow (iii)$. Kako je $xe, xe \in E(\mathrm{S})$, iz datih osobina sledi da $ex^2e \in V(xe^2x)$. Ali, $x = xe^2x$, što je inverz za ex^2e, i tako

$$x = x(ex^2e)x = (xex)(xex) = (xex)^2 = x^2.$$

$(iii) \Rightarrow (i)$. Neka je $e, f \in E(\mathrm{S})$ i uzmimo $x \in V(ef)$. Rutinski proveravamo da $ef \in V(fxe)$ i da $fxe \in E(\mathrm{S})$, pa $ef \in E(\mathrm{S})$. □

PROPOZICIJA 0.1.10. *Ako je* I *ideal polugrupe* S, *onda je relacija* θ_{I} *definisana sa*

$$a\theta_{\mathrm{I}}b \Leftrightarrow a = b \text{ ili } a, b \in I$$

kongruencija od S.

Dokaz. $a, b \in I$ implicira $xa, xb \in I$ i $ax, bx \in I$, što znači da je relacija ekvivalencije θ_{I} saglasna sa množenjem. □

Kongruencija θ_{I} iz prethodne propozicije je **Reesova kongruencija** ideala I, količnička polugrupa $\mathbf{S}/\mathbf{I} = \mathbf{S}/\theta_{\mathrm{I}}$ je **Reesov količnik** od S u odnosu na I. Ako je $I = \emptyset$, onda je (po definiciji) $\mathrm{S}/\mathrm{I} = \mathrm{S}$. Ako je $\mathrm{I} = \mathrm{S} \neq \emptyset$, onda je $\mathrm{S}/\mathrm{I} = \{\mathrm{I}\}$. Ako je $I \notin \{\emptyset, S\}$, onda je standardna praksa da se poistovećuje θ_{I}-klasa $\{x\} \in S/I$ za svako $x \notin I$ sa $x \in S$, dok se θ_{I}-klasa $I \in S/I$ označava sa 0. Tada je $S/I = S \setminus I \cup \{0\}$, sa množenjem datim na sledeći način:

$$x * y = \begin{cases} xy, & \text{ako } xy \notin I \\ 0, & \text{ako } xy \in I \end{cases}$$

za sve $x, y \in S \setminus I$.

Neka je $X \neq \emptyset$ proizvoljan skup i F_X skup svih n-torki $(x_1, \ldots, x_n)$, $x_1, \ldots, x_n \in X$. Prirodan broj $n \geq 1$ je **dužina** od $(x_1, \ldots, x_n)$. Definišimo operaciju **konkatenacije** na skupu F_X:

$$(x_1, \ldots, x_n)(y_1, \ldots, y_m) = (x_1, \ldots, x_n, y_1, \ldots, y_m).$$

Konkatenacija je asocijativna. Uobičajeno je da se identifikuje svaki element $x \in X$ sa jednoelementnim nizom $(x) \in F_X$. Tada je $X \subseteq F_X$.

PROPOZICIJA 0.1.11. *Svaki element* F_X *se može na jedinstven način napisati kao proizvod elemenata iz* X.

Dokaz. U F_X je $(x_1)(x_2)\ldots(x_n) = (x_1, \ldots, x_n)$. □

Elementi F_X se pišu kao **reči** $(x_1, \ldots, x_n) = x_1 \ldots x_n$ u **azbuci** X. Skup F_X, zajedno sa operacijom konkatenacije, čini **slobodnu polugrupu** $\mathbf{F}_X$.

PROPOZICIJA 0.1.12. *Svako preslikavanje* f *skupa* X *u polugrupu* S *jedinstveno se proširuje do homomorfizma* $\varphi : \mathbf{F}_X \to \mathrm{S}$. *Slika u* S *koja se dobija homomorfizmom* φ *je potpolugrupa od* S *generisana sa* $f(X)$. *Ako je* S *generisana sa* $f(X)$, *onda je* φ *sirjektivno.*

Dokaz. Ako $\varphi : F_X \to S$ proširuje f, onda je nužno

$$\varphi((x_1,\ldots,x_n)) = \varphi(x_1)\ldots\varphi(x_n) = f(x_1)\ldots f(x_n),$$

za sve $x_1,\ldots,x_n \in F_X$. Obratno, preslikavanje $\varphi : F_X \to S$, definisano sa $\varphi(x_1,\ldots,x_n) = f(x_1)\ldots f(x_n)$ za sve $x_1\ldots,x_n \in F_X$, je homomorfizam i proširuje f. Jasno, slika dobijena preslikavanjem φ je potpolugrupa od S generisana sa $f(X)$. □

Posledica 0.1.13. *Svaka polugrupa je homomorfna slika neke slobodne polugrupe.*

Greenove relacije na polugrupi S su sledeće relacije:

$$\begin{aligned} a\mathcal{L}b &\Leftrightarrow S^1a = S^1b \\ a\mathcal{R}b &\Leftrightarrow aS^1 = bS^1 \\ \mathcal{H} &= \mathcal{L}\cap\mathcal{R} \\ a\mathcal{J}b &\Leftrightarrow S^1aS^1 = S^1bS^1 \\ \mathcal{D} &= \mathcal{L}\circ\mathcal{R} \end{aligned}$$

Svaka $\mathcal{D}$-klasa polugrupe S je unija $\mathcal{L}$-klasa i, takođe, unija $\mathcal{R}$-klasa. Presek $\mathcal{L}$-klase i $\mathcal{R}$-klase je ili prazan, ili $\mathcal{H}$-klasa. Iz same definicije relacije $\mathcal{D}$ sledi

$$a\mathcal{D}b \Leftrightarrow R_a \cap L_b \neq \emptyset \Leftrightarrow L_a \cap R_b \neq \emptyset,$$

gde su R_a, R_b, L_a, L_b odgovarajuće $\mathcal{R}$-, odnosno $\mathcal{L}$-klase elemenata $a, b \in S$. Sledi da se svaka $\mathcal{D}$-klasa može prikazivati kao "kutija za jaja", kako su to nazivali Clifford i Preston [12], tj. pravougaonik podeljen na jednake kvadrate, gde svaka kolona predstavlja $\mathcal{L}$-klasu i svaka vrsta $\mathcal{R}$-klasu. Kvadrati onda predstavljaju $\mathcal{H}$-klase.

Polugrupa koja nema nulu zove se **prosta** ako nema pravih ideala. Polugrupa S sa nulom se zove **0-prosta** ako važi

(i) $\{0\}$ i S su jedini ideali,

(ii) $S^2 = \{0\}$.

Lako se vidi da je S prosta ako i samo ako je $\mathcal{J} = S \times S$. Odgovarajući kriterijum za 0-prostu polugrupu S je da je $S^2 \neq \{0\}$ i da su $\{0\}$ i $S \setminus \{0\}$ jedine $\mathcal{J}$-klase.

Postoji prirodno (parcijalno) uređenje među idempotentima proizvoljne polugrupe S. Naime, uočimo uređenje $\leq$ na $E(\mathrm{S})$ definisano sa

$$e \leq f \Leftrightarrow ef = fe = e.$$

Jasno je da važi $e \leq e$ i da $e \leq f$ i $f \leq e$ zajedno impliciraju $e = f$. Da pokažemo tranzitivnost, primetimo da ako je $e \leq f$ i $f \leq g$, tako da je $ef = fe = e$ i $fg = gf = f$, onda važi

$$eg = efg = ef = e \quad \text{i} \quad ge = gfe = fe = e,$$

tj. $e \leq g$.

Neka je $\mathbf{S}$ polugrupa bez nule. Kažemo da je $\mathbf{S}$ **kompletno prosta** ako je $\mathbf{S}$ prosta i sadrži idempotent koji je minimalan u odnosu malopre definisan poredak. Za takav idempotent kažemo da je *primitivan.*

S druge strane, polugrupa sa nulom $\mathbf{S}$ je **kompletno 0-prosta** ako je 0-prosta i sadrži minimalan nenula idempotent.

PROPOZICIJA 0.1.14. *Neka je* $\mathbf{S}$ *polugrupa bez nule. Sledeći uslovi su ekvivalentni:*

(1) $\mathbf{S}$ *je kompletno prosta;*

(2) $\mathbf{S}$ *je regularna, i ima osobinu "slabog skraćivanja"*

$$[ca = cb \text{ i } ac = bc] \Rightarrow a = b. \quad a, b, c \in S;$$

(3) $\mathbf{S}$ *je regularna i za sve* $a \in S$

$$aba = a \Rightarrow bab = b;$$

(4) $\mathbf{S}$ *je regularna i svaki idempotent je primitivan.*

Ako je S nosač polugrupe sa nulom $\mathbf{S}$ i važi

$$S = \bigcup_{i \in I} S_i,$$

$$S_i \cap S_j = S_i S_j = \{0\}, \quad i \neq j,$$

gde su S_i, $i \in I$, nosači potpolugrupa od $\mathbf{S}$, onda kažemo da je $\mathbf{S}$ **0-direktna unija** polugrupa $\mathbf{S}_i$, $i \in I$.

PROPOZICIJA 0.1.15. *Neka je* $\mathbf{S}$ *polugrupa sa nulom. Sledeći uslovi su ekvivalentni:*

(1) $\mathbf{S}$ *je regularna i svaki nenula idempotent od* $\mathbf{S}$ *je primitivan;*

(2) $\mathbf{S}$ *je 0-direktna unija kompletno 0-prostih polugrupa.*

Polugrupa S se naziva **kompletno regularna** ako postoji unarna operacija $a \mapsto a^{-1}$ na S koja ima sledeće osobine:

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

Sledeći rezultat daje dve alternativne definicije.

PROPOZICIJA 0.1.16. *Neka je* S *polugrupa. Sledeći uslovi su ekvivalentni:*

(1) S *je kompletno regularna;*

(2) Svaki element S leži u podgrupi od S*;*

(3) Svaka $\mathcal{H}$-klasa je grupa.

Pogledajmo sada neke veze koje važe među prethodno definisanim klasama polugrupa.

PROPOZICIJA 0.1.17. *Neka je* S *polugrupa. Sledeći uslovi su ekvivalentni:*

(1) S *je kompletno prosta;*

(2) S *je kompletno regularna i za sve $x, y \in S$ važi*

$$xx^{-1} = (xyx)(xyx)^{-1};$$

(3) S *je kompletno regularna i prosta.*

Cliffordova polugrupa se definiše kao kompletno regularna polugrupa S $= (S, \cdot, ^{-1})$ u kojoj je za sve $x, y \in S$,

$$(xx^{-1})(yy^{-1}) = (yy^{-1})(xx^{-1}).$$

U proizvoljnoj polugrupi S element $c \in S$ je **centralan** ako važi $cs = sc$ za sve $s \in S$.

PROPOZICIJA 0.1.18. *Neka je* S *polugrupa sa skupom idempotenata E. Sledeći uslovi su ekvivalentni:*

(1) S *je Cliffordova polugrupa;*

(2) S *je regularna i svi idempotenti od* S *su centralni;*

(3) S *je regularna i $\mathcal{D} \cap (E \times E) = \Delta_E$.*

Neka je **Y** polumreža. Svakom $\alpha \in Y$ pridružimo polugrupu $\mathbf{S}_\alpha$, i pretpostavimo da je $S_\alpha \cap S_\beta = \emptyset$ ako je $\alpha \neq \beta$. Za svaki par $\alpha, \beta \in Y$, $\alpha \geq \beta$, neka je $\varphi_{\alpha,\beta} : S_\alpha \longrightarrow S_\beta$ homomorfizam $\mathbf{S}_\alpha$ u $\mathbf{S}_\beta$, i neka važe sledeći uslovi:

$$\begin{aligned} \varphi_{\alpha,\alpha} &= id_{S_\alpha} \quad (\alpha \in Y), \\ \varphi_{\alpha,\beta} \circ \varphi_{\beta,\gamma} &= \varphi_{\alpha,\gamma} \text{ ako je } \alpha > \beta > \gamma. \end{aligned}$$

Na skupu $S = \bigcup_{\alpha \in Y} S_\alpha$ definišemo množenje sa

$$a \cdot b = \varphi_{\alpha,\alpha\beta}(a)\varphi_{\beta,\alpha\beta}(b),$$

$a \in S_\alpha$, $b \in S_\beta$. Lako pokazujemo da je množenje asocijativno i da se na $\mathbf{S}_\alpha$ poklapa sa množenjem u $\mathbf{S}_\alpha$.

Polugrupa $\mathbf{S} = (S, \cdot)$, gde je $S = \bigcup_{\alpha \in Y} S_\alpha$ i operacija " $\cdot$ " definisana kao u gornjim razmatranjima, naziva se **jaka polumreža polugrupa** $\mathbf{S}_\alpha$.

Bijekcija φ polugrupe **S** na samu sebe koja je antiautomorfizam reda 2, dakle,

$$\begin{aligned} \varphi(ab) &= \varphi(b)\varphi(a), \\ \varphi(\varphi(a)) &= id_S, \end{aligned}$$

$a, b \in S$, naziva se **involucija** i označava se sa *.

Algebru $(S, \cdot, ^*)$, gde je $(S, \cdot)$ polugrupa, a * involucija te polugrupe, zovemo **involutivna polugrupa**.

Idempotent e involutivne polugrupe **S** za koji važi $e^* = e$ zovemo **projekcija**.

TEOREMA 0.1.19. *Neka je* $\mathbf{S} = (S, \cdot, ^*)$ *involutivna polugrupa. Tada su sledeći uslovi ekvivalentni:*

(1) Svaka $\mathcal{L}$-klasa od **S** *sadrži projekciju;*

(2) Za svako $x \in S$, x^* je $\mathcal{L}$-ekvivalentno nekom inverzu od x;

(3) Za svako $x \in S$ važi $xx^*\mathcal{L}x$;

(4) Za svako $x \in S$, x^* je $\mathcal{H}$-ekvivalentno nekom inverzu od x;

(5) Za svako $a \in S$ postoji $x \in S$ tako da važi $axa = a$, $xax = x$, $(ax)^* = ax$ i $(xa)^* = xa$;

(6) Za svako $a \in S$ postoji $x \in S$ tako da je $xx^*a^* = x$ i $xaa^* = a^*$;

(7) Za svako $a \in S$ postoji $y \in S$ tako da je $ay^*y = y$ i $a^*ay = a^*$.

Involutivne polugrupe koje zadovoljavaju bilo koji od uslova prethodne teoreme zovemo ***-regularne polugrupe**.

0.2. Poluprsteni i prsteni

Neka je $S \neq \emptyset$ bilo koji skup i $+, \cdot$ binarne operacije na S koje zovemo **sabiranje** i **množenje**. Strukturu $(S, +, \cdot)$ nazivamo **poluprsten** ako važe sledeći uslovi:

(1) $(S, +)$ je komutativna polugrupa;

(2) $(S, \cdot)$ je polugrupa;

(3) Obe operacije su povezane **distributivnim zakonima**

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

za sve $a, b, c \in S$.

Poluprsten $(S, +, \cdot)$ se naziva **prsten** ako je $(S, +)$ komutativna grupa. Ovaj naziv je najverovatnije uveo D. Hilbert 1897. godine, kada je upotrebio termin *Zahlring*.

Kao što je poznato, u poluprstenu (prstenu) pišemo

$$a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i, \quad n \in \mathbb{N}.$$

Posebno, ako je $a_1 = a_2 = \ldots = a_n$, gornja suma daje element koga definišemo kao $na \in S$. Lako pokazujemo da u bilo kom poluprstenu $(S, +, \cdot)$ važi

$$\begin{aligned} na + ma &= (n + m)a \\ m(na) &= (mn)a \\ n(a + b) &= na + nb, \end{aligned}$$

za sve $a, b \in S$ i $m, n \in \mathbb{N}$.

Neka je $(S, +, \cdot)$ poluprsten. Ako polugrupa $(S, \cdot)$ ima neutralni element e, onda e zovemo **jedinica** poluprstena $(S, +, \cdot)$. Ako polugrupa $(S, +)$ ima neutralni element, onda taj element nazivamo **nula** poluprstena $(S, +, \cdot)$ i označavamo ga sa 0. Mi ćemo u našem radu koristiti termin 'poluprsten' i za poluprstene obogaćene upravo opisanim konstantama, bez opasnosti od zabune (budući da će pristup koji primenjujemo uvek biti jasan iz konteksta). Naravno, za prstene je prirodno istaći neutralni element aditivne Abelove grupe (pa i aditivni inverz) i pisati $\mathbf{R} = (R, +, \cdot, -, 0)$.

Kao prvu posledicu veze sabiranja i množenja u poluprstenima, datu kroz zakone distributivnosti, imamo da za sve $m, n \in \mathbb{N}$, $a_i, b_j \in S$ važi:

$$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}(\sum_{j=1}^{m} a_i b_j) = \sum_{1 \leq i \leq n,\ 1 \leq j \leq m} a_i b_j.$$

Za poluprsten $(S,+,\cdot)$ i neprazne podskupove $A, B \subseteq S$ definišemo sledeće podskupove od S:

$$\begin{aligned}\langle A\rangle &= \{\textstyle\sum_{i=1}^{n} a_i \mid n \in \mathbb{N},\, a_i \in A\},\\ A+B &= \{a+b \mid a \in A,\, b \in B\},\\ A\cdot B &= \{a\cdot b \mid a \in A,\, b \in B\}.\end{aligned}$$

Jasno, $A \cdot B \subseteq \langle A\cdot B\rangle$.

Unarna operacija $^* : A \to A$ je **involucija poluprstena** $\mathbf{A} = (A,+,\cdot)$, ako je $(A,\cdot,^*)$ involutivna polugrupa i za sve $a, b \in A$ važi $(a+b)^* = a^* + b^*$. Tada algebru $(A,+,\cdot,*)$ zovemo **involutivni poluprsten**. Primetimo da, ukoliko poluprsten ima nulu i/ili jedinicu, tada kao posledicu datih uslova imamo $0^* = 0$ i $1^* = 1$. Nije teško videti da je, na primer,

$$(\mathcal{P}(A\times A), \cup, \circ, ^{-1}, \emptyset, \Delta_A)$$

involutivni poluprsten. U teorijskom računarstvu i algebarskoj logici je uobičajeno da algebru

$$\mathbf{Rel}(A) = (\mathcal{P}(A\times A), \cup, \circ, ^{\mathrm{rtc}}, \emptyset, \Delta_A)$$

zovemo **puna Kleenejeva algebra binarnih relacija na skupu** A. Naravno, i ona može biti proširena involutivnom operacijom relacijskog inverza.

Prsten $\mathbf{R} = (R,+,\cdot,-,0)$ je **komutativan** ako zadovoljava $ab = ba$ za sve $a, b \in R$. Komutativan prsten $\mathbf{R}$ je **domen integriteta (integralni domen)** ako i samo ako je proizvod dva nenula elementa iz R takođe nenula element iz R.

Podskup S komutativnog prstena $\mathbf{R}$ je **potprsten** od $\mathbf{R}$ ako je:

(1) $a, b \in S \Rightarrow a - b \in S$;

(2) $a, b \in S \Rightarrow ab \in S$.

Posledica ove definicije je činjenica da je potprsten komutativnog prstena komutativan prsten. Naravno, ovo se moglo iskazati i na drugi način. Najopštiji pristup ovakvim definicijama daćemo u narednom paragrafu.

Ako su a i b elementi komutivnog prstena $\mathbf{R}$, tada kažemo da a **deli** b u $\mathbf{R}$ (ili a je **delitelj** b, ili b je **umnožak** od a), u oznaci $a|b$, ako postoji element $c \in R$ tako da je $b = ca$. Na primer, ako $0|a$, onda je $a = 0\cdot c$ za neko $c \in R$. Kako je $0\cdot c = 0$, sledi da je $a = 0$. Znači, $0|a$ ako i samo ako je $a = 0$. U prstenu racionalnih brojeva $\mathbf{Q} = (\mathbb{Q},+,\cdot,0,1)$ imamo $3|2$, jer važi $2 = 3\cdot\frac{2}{3}$, dok u prstenu $\mathbb{Z}$ ovo nije tačno.

Element u komutativnog prstena $\mathbf{R}$ sa jedinicom se zove **unitaran** ako $u|1$ u $\mathbf{R}$, tj. ako postoji $v \in R$ tako da je $uv = 1$. v se zove **inverz** od u i, s obzirom da je jedinstven, označava se sa u^{-1}.

Propozicija 0.2.1. *Neka je* $\mathbf{R}$ *integralni domen i neka su* $a, b \in R$ *nenula elementi. Tada* $a|b$ *i* $b|a$ *ako i samo ako je* $b = ua$ *za neki unitaran element* $u \in R$.

Dokaz. Ako $a|b$ i $b|a$, tada postoje elementi $u, v \in R$ tako da važi $b = ua$ i $a = vb$. Sledi da je $b = ua = uvb$. Kako je $b = 1 \cdot b$ i $b \neq 0$, zakon skraćivanja u integralnom domenu $\mathbf{R}$ daje $1 = uv$ i u je unitaran.

Obratno, pretpostavimo da je $b = ua$, gde je u unitaran element u $\mathbf{R}$. Jasno, $a|b$. Ako $v \in R$ zadovoljva $uv = 1$, onda je $vb = vua = a$, i prema tome $b|a$. □

Šta su unitarni elementi u $\mathbb{Z}_m$?

Propozicija 0.2.2. *Ako je* a *ceo broj, onda je* $[a]$ *unitaran element u* $\mathbb{Z}_m$ *ako i samo ako su* a *i* m *uzajamno prosti. U stvari, ako je* $sa + tm = 1$, *onda je* $[a]^{-1} = [s]$.

Dokaz. Ako je $[a]$ unitarni element iz $\mathbb{Z}_m$, tada postoji $[s] \in \mathbb{Z}_m$ tako da je $[s][a] = [1]$. Prema tome $sa \equiv 1 \,(\mathrm{mod}\ m)$ i postoji ceo broj t takav da je $sa - 1 = tm$ tj. $1 = sa - tm$. Sledi da su a i m uzajamno prosti.

Obratno, ako su a i m relativno prosti, postoje celi brojevi s i t tako da je $1 = sa + tm$. Sledi $sa \equiv 1 \,(\mathrm{mod}\ m)$ i $[s][a] = [1]$, pa je $[a]$ unitaran u $\mathbb{Z}_m$. □

Posledica 0.2.3. *Ako je* p *prost broj, onda je svaki nenula element* $[a]$ *u* $\mathbb{Z}_p$ *unitaran.*

Dokaz. Ako je $[a] \neq [0]$, onda $a \not\equiv 0 \,(\mathrm{mod}\ p)$ i $p \mid a$. Prema tome, a i p su uzajamno prosti, jer je p prost. □

Polje F je komutativan prsten u kome je svaki element a unitaran. To znači da postoji $a^{-1} \in F$ tako da je $a^{-1}a = 1$.

Propozicija 0.2.4. *Svako polje* $\mathbf{F}$ *je integralni domen.*

Dokaz. Pretpostavimo da je $ab = 0$, gde je $a \neq 0$. Množeći obe starne sa a^{-1} dobijamo $b = a^{-1}ab = a^{-1} \cdot 0 = 0$. □

Propozicija 0.2.5. *Komutativan prsten* $\mathbb{Z}_m$ *je polje ako i samo ako je* m *prost broj.*

Dokaz. Ako je m prost broj, onda na osnovu Posledice 0.2.3 sledi da je $\mathbb{Z}_m$ polje. Obratno, ako je m složen broj, lako pokazujemo da $\mathbb{Z}_m$ nije domen integriteta. Naime, ako je $m = pq$, $p, q < m$, onda je $[p][q] = [m] = [0]$. Prema prethodnoj propoziciji, $\mathbb{Z}_m$ nije polje. □

Ideal komutativnog prstena **R** je podskup $I \subseteq R$ za koji važi

(1) $0 \in I$;

(2) ako $a, b \in I$, onda $a - b \in I$;

(3) ako $a \in I$ i $r \in R$, onda $ra \in I$.

Postoje uvek bar dva ideala komutativnog prstena **R**: prsten **R** i $\{0\}$. Ideal $\mathbf{I} \neq \mathbf{R}$ se zove **pravi ideal**.

Ako je **R** komutativni prsten sa jedinicom i $a_1, a_2, \ldots, a_n \in R$, onda je skup svih linearnih kombinacija

$$I = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \,|\, r_i \in R \text{ za sve } 1 \leq i \leq n,\ n \in \mathbb{N}\}$$

ideal u **R**. Pišemo $\mathbf{I} = (a_1, a_2, \ldots, a_n)$. Posebno ako je $n = 1$, onda je

$$I = (a) = \{ra \,|\, r \in R\} = Ra$$

ideal od **R**, i on se naziva **glavni ideal** generisan sa a.

Ako ideal **I** komutativnog prstena **R** sa jedinicom sadrži 1, onda je $\mathbf{I} = \mathbf{R}$. Pretpostavimo da je prsten **R** polje. Tada **R** nema pravih ideala.

Neka je I ideal komutativnog prstena **R**. Ako ne gledamo operaciju množenja, onda je **I** normalna podgrupa aditivne grupe $(R, +, 0)$; pošto je $(R, +, 0)$ Abelova grupa, podgrupa $(I, +, 0)$ je nužno normalna, i definišemo količničku grupu $\mathbf{R}/\mathbf{I}$ na prirodan način

$$R/I = \{a + I \,|\, a \in R\}$$

$$(a + I) + (b + I) = (a + b) + I.$$

U aditivnoj grupi $\mathbf{R}/\mathbf{I}$ definišemo množenje kao

$$(a + I)(b + I) = ab + I.$$

Lako se uveravamo da je $(R/I, +, \cdot, -, I)$ komutativan prsten koji se naziva **količnički prsten od R modulo** I. Tako, $\mathbb{Z}/(m)$ se poklapa sa $\mathbb{Z}_m$.

Ako u proizvoljnom prstenu $\mathbf{R} = (R, +, \cdot, -, 0)$ postoji pozitivan ceo broj n takav da za svaki element $a \in R$ važi $na = 0$, najmanji takav n se zove **karakteristika** prstena **R** i označava sa $char(\mathbf{R})$. Ako takav broj ne postoji, onda kažemo da je **R** karakteristike 0.

Prsten **R** je **prost** ako nema pravih ideala.

PROPOZICIJA 0.2.6. *Komutativan prsten* **R** *sa jedinicom je polje ako i samo ako je prost.*

Dokaz. Pretpostavimo da je **R** prost i $x \in R$ je nenula element. Ideal Rx je različit od 0 jer je $x = 1x \in Rx$. Kako je **R** prost, $R = Rx$. Sledi da postoji $y \in R$ tako da važi $1 = yx$.

Obratno, pretpostavimo da je **R** polje i **I** nenula ideal. Kako **I** sadrži nenula element x, on takođe sadrži element $r = rx^{-1}x$ za svako $r \in R$ pa je $\mathbf{I} = \mathbf{R}$. □

Element r u prstenu je **nilpotentan** ako je $r^k = 0$ za neko k.

Neka je $\{\mathbf{R}_i | \, i \in J\}$ familija prstena indeksiranih skupom J, i neka imamo funkciju koja elementu $i \in J$ opredeljuje element u R_i. Tako, ako je a takva funkcija, važi $a(i) \in R_i$ za svako $i \in J$. Zbir i proizvod ovakvih funkcija definisan je na uobičajen način:

$$(a+b)(i) = a(i) + b(i), \quad (ab)(i) = a(i)b(i).$$

Lako se pokazuje da je skup svih takvih funkcija prsten. Označimo ovakav prsten sa **R**. Prsten **R** se naziva **(kompletan) direktan proizvod** prstena $\mathbf{R}_i$, $i \in J$. Skup svih funkcija iz **R**, koje imaju vrednost 0 na svim (sem konačno mnogo komponenata), čini potprsten od **R** koji se zove **diskretan direktan proizvod**, ili **direktna suma**. Ako je $J = \{1, 2, ..., n\}$, onda formalno predstavljamo $a \in R$ kao

$$a = (a_1, a_2, ..., a_n), \quad a_i \in R_i, \quad i = 1, 2, ..., n.$$

Ako je **R** direktan proizvod prstena $\mathbf{R}_i$, $i \in J$, svakom $i \in J$ možemo pridružiti preslikavanje

$$\pi_i(a) = a(i).$$

Jasno, $\pi_i(\mathbf{R}) = \mathbf{R}_i$ je homomorfizam **R** na $\mathbf{R}_i$, koji zovemo ***i*-ta projekcija**. Ako je sada **T** potprsten od **R**, $\theta_i(\mathbf{T})$ je potprsten od $\mathbf{R}_i$. Slučaj koji nas najviše interesuje je kada je $\theta_i(\mathbf{T}) = \mathbf{R}_i$ za svako $i \in J$. Tada se **T** naziva **poddirektan proizvod**.

Ako je prsten **R** izomorfan poddirektnom proizvodu **T** prstena $\mathbf{R}_i$, $i \in J$, **T** se naziva **reprezentacija R** poddirektnim proizvodom prstena $\mathbf{R}_i$, $i \in J$.

TEOREMA 0.2.7. *Prsten* **R** *ima reprezentaciju kao poddirektan proizvod prstena* $\mathbf{R}_i$, $i \in J$, *ako i samo ako za svako* $i \in J$ *postoji homomorfizam* ϕ_i *od* **R** *na* $\mathbf{R}_i$ *tako da ako je* $r \neq 0$ *element od* R, *onda je* $\phi_i(r) \neq 0$ *za bar jedno* $i \in J$.

Prsten se zove **poddirektno nesvodljiv** ako nema netrivijalnih reprezentacija kao poddirektan proizvod bilo kojih prstena.

TEOREMA 0.2.8. *Svaki prsten je izomorfan poddirektnom proizvodu poddirektno nesvodljivih prstena.*

TEOREMA 0.2.9. *Prsten* $\mathbf{T}$ *je poddirektno nesvodljiv ako i samo ako presek svih nenula ideala od* $\mathbf{R}$ *jeste nenula ideal.*

Neka je $\mathbf{R}$ proizvoljan komutativan prsten i $\mathbf{I}$ ideal od $\mathbf{R}$. Označimo sa $\sqrt{\mathbf{I}}$ skup svih elemenata $a \in R$ takvih da je $a^i \in I$ za neki pozitivan ceo i, koji zavisi od a. Lako se pokazuje da je $\sqrt{\mathbf{I}}$ ideal. Ovaj ideal zovemo **radikal** ideala $\mathbf{I}$. Radikal nula ideala (0) naziva se **nil-radikal prstena** $\mathbf{R}$, u oznaci $N(\mathbf{R})$.

PROPOZICIJA 0.2.10. *Prsten* $\mathbf{R}/N(\mathbf{R})$ *je izomofan poddirektnom proizvodu integralnih domena.*

Prsten $\mathbf{R}$ se zove **regularan** ako za svaki element $a \in R$ postoji $x \in R$ tako da važi

$$axa = a.$$

TEOREMA 0.2.11. *Svaki netrivijalan komutativan regularan prsten sa jedinicom izomorfan je poddirektnom proizvodu polja.*

TEOREMA 0.2.12. *Komutativan prsten sa jedinicom* $\mathbf{R}$ *sa samo konačno mnogo ideala je regularan ako i samo ako nema nenula nilpotentnih elemenata.*

TEOREMA 0.2.13. *Komutativan prsten sa jedinicom* $\mathbf{R}$ *je regularan prsten ako i samo ako se svaki ideal u* $\mathbf{R}$ *poklapa sa svojim radikalom.*

Za element a prstena $\mathbf{R}$ ($a \neq 0$) kažemo da je **delitelj nule** ako postoji $b \in R$, $b \neq 0$, tako da je $ab = 0$. U tom slučaju kažemo da je a **levi delitelj nule** i b **desni delitelj nule.**

Element prstena $\mathbf{R}$ se zove **pseudoregularan** ako nije ni levi ni desni delitelj nule.

Prsten $Q(\mathbf{R})$, koji sadrži $\mathbf{R}$, naziva se **prsten levih količnika** od $\mathbf{R}$ ako je

(1) Svaki pseudoregularan element iz $\mathbf{R}$ invertibilan u $Q(\mathbf{R})$;

(2) Svaki element $x \in Q(\mathbf{R})$ je oblika $x = a^{-1}b$, gde su $a, b \in R$ i a je pseudoregularan.

Ako je $Q(\mathbf{R})$ levi količnički prsten od $\mathbf{R}$, kažemo da je $\mathbf{R}$ **levi red** u $Q(\mathbf{R})$.

Algebra $\mathbf{R} = (R, +, \cdot, -, 0, ^*)$ je **involutivni prsten** ako je $(R, +, \cdot, -, 0)$ prsten i $(R, +, ^*)$, $(R, \cdot, ^*)$ su involutivne polugrupe. Pri tome je, naravno, $0^* = 0$.

0.3. Algebre

Algebra je uređen par (A, F), gde je $A \neq \emptyset$ i $F = \{F_i \mid i \in I\}$ skup operacija na A. Pri tome, A se naziva **nosač** (**univerzum**) od (A, F), a F_i se zovu **fundamentalne** (**osnovne**) operacije algebre (A, F). Algebre označavamo masnim slovima, npr. $\mathbf{A} = (A, F)$.

Kao što smo ranije videli, uobičajeno je da se za operacije nekih poznatih algebri koriste specijalni simboli: $+, \cdot, \wedge, \vee, \ldots$, itd.

Ako želimo da naglasimo da je operacija $\cdot$ baš operacija date algebre $\mathbf{A}$, onda je pišemo kao $\cdot^{\mathbf{A}}$. Tako, polugrupu definišemo kao algebru $\mathbf{A} = (A, \cdot^{\mathbf{A}})$ na kojoj važi

$$(a \cdot^{\mathbf{A}} b) \cdot^{\mathbf{A}} c = a \cdot^{\mathbf{A}} (b \cdot^{\mathbf{A}} c) \text{ za sve } a, b, c \in A.$$

Naravno, u praksi ovaj eksponent $\mathbf{A}$ izostavljamo.

Ako je $f : A^n \to A$, onda n nazivamo **arnost** operacije f. Za $n = 0$ kažemo da je f **nularna** ili **konstanta**.

Neka je f operacija na nepraznom skupu A arnosti n, i neka je X podskup od A. Kažemo da je X **zatvoreno u odnosu na** f ako i samo ako je

$$f(a_1, a_2, \ldots, a_n) \in X \quad \text{za sve } a_1, a_2, \ldots, a_n \in X.$$

Ako je f konstanta, X je zatvoren u odnosu na f ako i samo ako $f \in X$. Znači, prazan skup je zatvoren u odnosu na svaku operaciju koja nije konstanta.

Neka je $\mathbf{A}$ algebra. Podskup univerzuma A od $\mathbf{A}$ koji je zatvoren u odnosu na svaku fundamentalnu operaciju od $\mathbf{A}$ naziva se **poduniverzum** od $\mathbf{A}$.

Algebra $\mathbf{B}$ je **podalgebra** od $\mathbf{A}$ ako je $\emptyset \neq B \subseteq A$ i skup B je zatvoren u odnosu na fundamentalne operacije algebre $\mathbf{A}$. Kažemo da je $\mathbf{A}$ **ekstenzija od** $\mathbf{B}$.

Neka je I bilo koji skup i neka je A_i skup za svako $i \in I$. Sistem $\mathcal{A} = \{A_i \mid i \in I\}$ zovemo **sistem skupova indeksiranih sa** I. **Izborna funkcija za** $\mathcal{A}$ je funkcija φ čiji je domen I tako da je $\varphi(i) \in A_i$ za sve $i \in I$. **Direktan proizvod** sistema $\mathcal{A}$ je skup svih izbornih funkcija od $\mathcal{A}$. Direktan proizvod označavamo sa

$$\prod \mathcal{A}, \quad \prod_{i \in I} A_i, \quad \text{ili} \quad \prod_I A_i.$$

Ako je data algebra $\mathbf{A} = (A, F)$, $F = \{F_i \mid i \in I\}$, postoji funkcija $\rho : F \to \mathbb{N}$, koju zovemo **rang funkcija**, definisana sa:

$$\rho(F_i) \quad \text{je arnost } F_i^{\mathbf{A}}, \quad \text{za sve } F_i \in F.$$

Rang funkcija neke algebre zove se još i **tip sličnosti**. Algebre **A** i **B** su **slične** ako i samo ako imaju iste rang funkcije.

Neka je $\mathcal{A} = \{\mathbf{A}_i \mid i \in I\}$ sistem sličnih algebri. **Direktan proizvod** od $\{\mathbf{A}_i \mid i \in I\}$ je algebra, koju označavamo sa $\prod \mathcal{A}$, istog tipa sličnosti, čiji univerzum je direktan proizvod familije $\{A_i \mid i \in I\}$, i operacije definisane sa

$$F_t^{\prod \mathbf{A}}(f^0, f^1, \ldots, f^{r-1})(i) = F_t^{\mathbf{A}_i}(f^0(i), f^1(i), \ldots, f^{r-1}(i)),$$

za sve $f^0, f^1, \ldots, f^{r-1} \in \prod \mathcal{A}$, $i \in I$.

Uočimo dve slične algebre **A** i **B** i neka je f operacijski simbol arnosti r. Funkcija h od A u B **očuvava interpretaciju** f ako i samo ako

$$h(f^{\mathbf{A}}(a_0, \ldots, a_{r-1})) = f^{\mathbf{B}}(h(a_0), \ldots, h(a_{r-1})),$$

za sve $a_0, \ldots, a_{r-1} \in A$.

Neka su **A** i **B** slične algebre. Funkcija $h : A \to B$ je **homomorfizam** iz A u B ako h očuvava interpretaciju svakog operacijskog simbola iz **A**.

Neka je $\mathcal{K}$ klasa sličnih algebri. Koristimo sledeću notaciju:

- $\mathsf{H}(\mathcal{K})$ je klasa svih homomorfnih slika elemenata $\mathcal{K}$.
- $\mathsf{S}(\mathcal{K})$ je klasa svih izomorfnih slika podalgebri elemenata $\mathcal{K}$.
- $\mathsf{P}(\mathcal{K})$ je klasa svih izomorfnih slika direktnih proizvoda sistema algebri iz $\mathcal{K}$.

Kažemo da je $\mathcal{K}$ **zatvorena** u odnosu na formiranje homomorfnih slika, podalgebri i direktnih proizvoda ako važi

$$\mathsf{H}(\mathcal{K}) \subseteq \mathcal{K}, \quad \mathsf{S}(\mathcal{K}) \subseteq \mathcal{K}, \quad \mathsf{P}(\mathcal{K}) \subseteq \mathcal{K},$$

respektivno. U tom slučaju kažemo da je klasa $\mathcal{K}$ **varijetet** (ili **mnogostrukost**).

Svaki od navedenih operatora C ima osobine $\mathcal{K} \subseteq \mathsf{C}(\mathcal{K})$, $\mathcal{K}_0 \subseteq \mathcal{K}_1 \Rightarrow \mathsf{C}(\mathcal{K}_0) \subseteq \mathsf{C}(\mathcal{K}_1)$, i $\mathsf{C}(\mathbf{C}(\mathcal{K})) = \mathsf{C}(\mathcal{K})$. Kažemo da su to **operatori zatvorenja**.

LEMA 0.3.1. *Operatori* HS, SP *i* HP *su operatori zatvorenja na klasama algebri. Važi:*

$$\mathsf{SH}(\mathcal{K}) \subseteq \mathsf{HS}(\mathcal{K}), \quad \mathsf{PS}(\mathcal{K}) \subseteq \mathsf{SP}(\mathcal{K}), \quad \mathsf{PH}(\mathcal{K}) \subseteq \mathsf{HP}(\mathcal{K}).$$

Ako je $\mathcal{K}$ klasa algebri istog tipa, onda sa $\mathsf{V}(\mathcal{K})$ označavamo najmanji varijetet koji sadrži $\mathcal{K}$. Kažemo da je $\mathsf{V}(\mathcal{K})$ varijetet **generisan** sa $\mathcal{K}$.

TEOREMA 0.3.2. (Tarski) $\mathsf{V}(\mathcal{K}) = \mathsf{HSP}(\mathcal{K})$.

Dokaz. Iz Leme 0.3.1 sledi $\mathsf{HHSP} = \mathsf{SHSP} = \mathsf{PHSP} = \mathsf{HSP}$. Sledi da je $\mathsf{HSP}(\mathcal{K})$ varijetet koji sadrži $\mathcal{K}$, za svaku klasu $\mathcal{K}$. S druge strane, ako je $\mathcal{V}$ varijetet koji sadrži $\mathcal{K}$, tada je $\mathsf{HSP}(\mathcal{K}) \subseteq \mathsf{HSP}(\mathcal{V}) = \mathcal{V}$. Dakle, $\mathsf{HSP}(\mathcal{K})$ je najmanji varijetet koji sadrži $\mathcal{K}$. □

Najjednostavnija klasifikacija algebri je prema jeziku, tj. prema broju i vrsti algebarskih operacija i konstanti koje učestvuju u njihovoj definiciji. Pod **algebarskim jezikom** podrazumevamo svaki konačan skup simbola

$$L = Const_L \cup Fun_L, \quad Const_L \cap Fun_L = \emptyset,$$

gde je svakom simbolu $f \in Fun_L$ pridružen neki prirodan broj $ar(f)$, tzv. **arnost** simbola f. Elemente skupa $Const_L$ nazivamo **simbolima konstanti**, dok elemente Fun_L nazivamo **operacijskim** ili **funkcijskim znacima**. Simbolima konstanti dogovorno dodeljujemo arnost 0. Skupovi $Const_L$, Fun_L mogu biti i prazni.

Neka je $L = Const_L \cup Fun_L$ algebarski jezik, gde su $Const_L = \{c_1, \dots, c_m\}$ i $Fun_L = \{F_1, \dots, F_k\}$. **Algebra na jeziku** L je svaka algebarska struktura

$$\mathbf{A} = (A, f_1, \dots, f_k, a_1, \dots, a_m),$$

gde je arnost f_i upravo $ar(F_i)$, $1 \leq i \leq k$. U tom slučaju, kažemo da je operacija f_i **intepretacija** operacijskog simbola F_i, dok je konstanta a_j, $1 \leq j \leq m$, interpretacija simbola c_j.

Često se koriste isti simboli za operacijske simbole jezika L i njihove interpretacija u algebrama jezika L. Ovo retko dovodi do zabuna.

U formiranju algebarskih izraza nakog algebarskog jezika L, pored simbola iz L, ključnu ulogu igraju **promenljive**. Pod promenljivama podrazumevamo prebrojiv skup simbola $X = \{x_0, x_1, x_2, \dots\}$.

Definišemo algebraske izraze, tzv. **terme**, na sledeći način:

(1) Sve promenljive $x_0, x_1, x_2, \dots, x_n, \dots$ su termi;

(2) Ako je $f \in Fun_L$ operacijski znak arnosti n, i ako su $u_1, u_2, \dots, u_n$ termi jezika L, onda je $f(u_1, u_2, \dots, u_n)$ term jezika L;

(3) Svaki term jezika L dobija se konačnom primenom pravila (1) i (2).

Kako bismo izračunali **vrednost** terma u nekoj algebri $\mathbf{A} = (A, F)$, neophodno je da najpre definišemo preslikavanje $v : X \to A$, koje zovemo **valuacija**, tj. da promenljivama dodelimo vrednosti iz A. U odnosu na datu valuaciju v, vrednost $t^{\mathbf{A}}(v)$ terma t se izračunava na sledeći način:

(1) Ako je $t = x \in X$, tada je $t^{\mathbf{A}}(v) = v(x)$;

(2) Ako je $t = f(u_1, \ldots, u_n)$, gde je $f \in Fun_L$ operacijski znak arnosti n, tada je $t^{A}(v) = f^{\mathbf{A}}(u_1^{\mathbf{A}}(v), \ldots, u_n^{\mathbf{A}}(v))$.

Ako se u termu t pojavljuje n promenljivih, na gornji način dobijenu operaciju $t^{\mathbf{A}} : A^n \to A$ zovemo **term operacija** indukovana sa t an $\mathbf{A}$.

Algebarski zakon ili identitet jezika L je svaka formula oblika $p = q$, gde su p i q termi. Simbol **semantičke rampe** $\vdash$ se koristi da se označi relacija važenja identiteta u algebri. Naime, za algebru $\mathbf{A}$ i zakon $p = q$ jezika L pišemo $\mathbf{A} \vdash p = q$ ako i samo ako se indukovane term operacije $p^{\mathbf{A}}$ i $q^{\mathbf{A}}$ poklapaju. To znači da za termi p i q imaju istu vrednost u $\mathbf{A}$ za sve valuacije promenljivih.

Algebarska teorija na jeziku L je svaki skup Σ identiteta na jeziku L. U tom slučaju, elementi skupa Σ se zovu još i **aksiomama**.

Neka je Σ algebarska teorija jezika L. Sa $Mod(\Sigma)$ označavamo klasu svih algebri jezika L koje zadovoljavaju zakone Σ.

Ako je dat term p, **podterm** od p se definiše na sledeći način:

(1) p je podterm od p.

(2) Ako je $f(p_1, \ldots, p_n)$ podterm od p i f je n-arni simbol, onda su i p_i podtermi od p, $i = 1, 2, \ldots, n$.

Skup identiteta Σ je zatvoren za **zamenu**, ako je za bilo koji identitet $p = q \in \Sigma$ i bilo koji term r koji sadrži podterm p važi da se zamenom tog podterma p sa q dobija term s tako da

$$r = s \in \Sigma.$$

Skup identiteta Σ je zatvoren u odnosu na **uvrštavanje** ako za svaki identitet $p = q \in \Sigma$ i svaki term r, ako zamenimo svako pojavljivanje neke promenljive x u $p = q$ sa r, onda rezultat zamene opet pripada Σ.

Ako je Σ skup identiteta, tada je **deduktivno zatvorenje** od Σ najmanji skup identiteta $D(\Sigma)$ koji sadrži Σ tako da važi

(1) $p = p \in D(\Sigma)$, za svaki term p,

(2) $p = q \in D(\Sigma) \Rightarrow q = p \in D(\Sigma)$, za sve terme p i q,

(3) $p = q, q = r \in D(\Sigma) \Rightarrow p = r \in D(\Sigma)$, za bilo koje terme p, q, r,

(4) $D(\Sigma)$ je zatvoren za zamenu,

(5) $D(\Sigma)$ je zatvoren za uvrštavanje.

Neka je Σ skup identiteta. Kažemo da

$$\mathbf{A} \vdash \Sigma$$

za neku algebru $\mathbf{A}$, ako svaki identitet iz Σ važi u $\mathbf{A}$. Dalje, imamo

$$\mathcal{K} \vdash p = q$$

ako $p = q$ važi na svakoj algebri iz klase $\mathcal{K}$. Najzad, pišemo

$$\Sigma \vdash p = q$$

ako $\mathbf{A} \vdash \Sigma \Rightarrow \mathbf{A} \vdash p = q$ za proizvoljnu algebru $\mathbf{A}$.

Neka je Σ proizvoljan skup identiteta. Za identitet $p = q$ kažemo da je **sintaktička posledica** Σ i pišemo

$$\Sigma \vdash p = q$$

(čitamo "Σ dokazuje $p = q$"), ako postoji niz identiteta

$$p_1 = q_1, \ p_2 = q_2, \ \ldots, \ p_n = q_n,$$

tako da svaki $p_i = q_i$ pripada Σ, ili je oblika $p = p$, ili je dobijen iz prethodnog skupa identiteta u nizu zamenom, ili uvrštavanjem, ili nekim od pravila (2) i (3) iz definicije deduktivnog zatvorenja. Poslednji identitet $p_n = q_n$ je baš $p = q$. Gornji niz identiteta naziva se **formalno izvođenje** $p = q$. Lako se pokazuje da $p = q$ pripada $D(\Sigma)$ ako i samo ako $\Sigma \vdash p = q$.

Teorema 0.3.3. (Birkhoff) *Ako je Σ skup identiteta i $p = q$ neki identitet, onda*

$$\Sigma \vdash p = q \ \Leftrightarrow \ \Sigma \vdash \ p = q.$$

Identitet $p = q$ je **regularan** (ili **homotipan**) ako se skupovi promenljivih u termovima p i q poklapaju. U suprotnom, on je **neregularan**, ili **heterotipan**.

Neka je $\mathbf{Y} = (Y, \leq)$ parcijalno uređen skup. Pretpostavimo da je za svako $i \in Y$ data algebra $\mathbf{A}_i = (A_i, (F_t^{(i)})_{t \in T})$, pri čemu su sve algebre $\mathbf{A}_i$ istog tipa. Dalje, neka je za svaki par elemenata $i, j \in Y$, gde je $i \leq j$, dat skup homomorfizama $\varphi_{ij} : \mathbf{A}_i \rightarrow \mathbf{A}_j$ koji zadovoljava sledeće uslove:

(1) Za sve $i \leq j \leq k$ važi $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$;

(2) φ_{ii} je identičko preslikavanje za sve $i \in Y$.

Sistem $(\mathbf{Y}, (\mathbf{A}_i)_{i \in I}, (\varphi_{ij})_{i \leq j, i,j \in Y})$ naziva se **direktan sistem** algebri. Ukoliko u parcijalno uređenom skupu $\mathbf{Y} = (Y, \leq)$ svaka dva elementa imaju najveću donju granicu, tj. ako je $\mathbf{Y}$ (donja) polumreža, onda je reč o **polumrežno uređenom** direktnom sistemu algebri. Pri tome možemo pretpostaviti da su univerzumi algebri $\mathbf{A}_i$ disjunktni.

Za svaki takav direktan sistem $\mathcal{A}$ definišemo algebru $\mathbf{A} = \mathcal{S}(\mathcal{A})$. Nosač algebre $\mathbf{A}$ je skup $\bigcup_{i \in I} A_i$, i fundamentalne operacije od $\mathcal{S}(\mathcal{A})$ su definisane sa

$$F_t(x_1, \ldots, x_n) = F_t^{(i_0)}(\varphi_{i_1, i_0}(x_1), \ldots, \varphi_{i_n, i_0}(x_n)),$$

gde je $i_0 = \text{infimum}\{i_1, \ldots, i_n\}$, $x_r \in A_{i_r}$, $r = 1, 2, \ldots, n$ i $t \in T$. Algebra $\mathcal{S}(\mathcal{A})$ naziva se **Płonkina suma** datog polumrežno uređenog sistema algebri.

TEOREMA 0.3.4. *Neka je $\mathcal{A}$ polumrežno uređen direktan sistem algebri koji sadrži bar dve algebre. Tada na $\mathcal{S}(\mathcal{A})$ važe samo regularni identiteti koji važe na svim algebrama sistema $\mathcal{A}$.*

Neka je $\mathbf{A} = (A, (F_t)_{t \in T})$ algebra i neka je $f : A^2 \to A$. Funkciju f zavemo **particiona funkcija** za algebru $\mathbf{A}$ (ili kratko P-**funkcija**) ako važi

(1) $f(f(x, y), z) = f(x, f(y, z))$,

(2) $f(x, x) = x$,

(3) $f(x, f(y, z)) = f(x, f(z, y))$

(4) $f(F_t(x_1, \ldots, x_n), y) = F_t(f(x_1, y), \ldots, f(x_n, y))$,

(5) $f(y, F_t(x_1, \ldots, x_n)) = f(y, F_t(f(y, x_1), \ldots, f(y, x_n)))$,

(6) $f(F_t(x_1, \ldots, x_n), x_k) = F_t(x_1, \ldots, x_n)$, $1 \leq k \leq n$,

(7) $f(y, F_t(y, \ldots, y)) = y$.

Glavni rezultat Płonke iz njegovog poznatog rada [97] koji se odnosi na dekompozicije algebri u Płonkine sume je sledeći.

TEOREMA 0.3.5. *Svakoj P-funkciji f algebre $\mathbf{A} = (A, (F_t)_{t \in T})$ odgovara reprezentacija $\mathbf{A} = \mathcal{S}(\mathcal{A})$ dobijena na sledeći način. Podelimo A na disjunktne podskupove A_i, $i \in Y$, stavljajući $a, b \in A$ u istu klasu A_i ako i samo ako je*

$f(a,b) = a$ i $f(b,a) = b$. Skupovi A_i su zatvoreni u odnosu na fundamentalne operacije od $\mathbf{A}$ i neka su $\mathbf{A}_i = (A_i, (F_t|_{A_i})_{t\in T})$. U skupu Y definišimo relaciju $\leq$ tako da je $i_1 \leq i_2$ ako i samo ako postoje $a \in A_{i_1}$ i $b \in A_{i_2}$ tako da je $f(b,a) = b$. Ova definicija je dobra i Y ima strukturu polumreže. Konačno, definišimo preslikavanja $\varphi_{i_1,i_2} : A_{i_1} \to A_{i_2}$ za $i_1 \leq i_2$ stavljajući da je $\varphi_{i_1,i_2}(a) = f(a,b)$, gde je b proizvoljan element od A_{i_2}. Ovako definisana preslikavanja su homomorfizmi i sistem

$$\mathcal{A} = (\mathbf{Y}, (\mathbf{A}_i)_{i\in Y}, (\varphi_{ij})_{i\leq j,\, i,j\in Y})$$

je polumrežno uređen direktan sistem algebri za koji je $\mathbf{A} = \mathcal{S}(\mathcal{A})$.

Obratno, svaka reprezentacija $\mathbf{A} = \mathcal{S}(\mathcal{A})$ može se dobiti ovom konstrukcijom birajići odgovarajuću P-funkciju.

Štaviše, korspodencija između P-funkcija za $\mathbf{A}$ i reprezentacija $\mathbf{A}$ u obliku $\mathbf{A} = \mathcal{S}(\mathcal{A})$ je "1-1".

Neka je $\mathbf{A} = (A, F)$ algebra. Preslikavanje $\varphi : A \to A$ za koje važi

$$\varphi(\varphi(a)) = a$$

za sve $a \in A$, i

$$\varphi(f^{\mathbf{A}}(a_1, \ldots, a_n)) = f^{\mathbf{A}}(\varphi(a_n), \ldots, \varphi(a_1))$$

naziva se **involutivni antiautomorfizam** algebre $\mathbf{A}$. Ako F sadrži unarnu operaciju φ koja je u isto vreme involutivni antiautomorfizam φ-slobodnog redukta algebre $\mathbf{A}$, onda algebru $\mathbf{A}$ nazivamo **involutivna algebra**. Drugim rečima, budući da je involuciju uobičajeno obeležavati sa *, involutivna algebra je algebarski sistem oblika $\mathbf{A} = (A, F, ^*)$, pri čemu važe seledći identiteti:

$$(x^*)^* = x,$$

i za svaku n-arnu operaciju $f \in F$,

$$(f(x_1, \ldots, x_n))^* = f(x_n^*, \ldots, x_1^*).$$

1.1. Uvod

U prethodnoj glavi smo se upoznali sa konstrukcijom Płonkine sume polumrežno uređenih sistema algebri (videti [97]). Ova konstrukcija se ubraja u fundamentalne konstrukcije u opštoj algebri. Płonkine sume nalaze mnogobrojne primene u mnogim posebnim algebarskim teorijama (videti, na primer, [31, 88, 96]). Inspiracija za ovu konstrukciju najverovatnije dolazi od jake polumreže polugrupa. Na primer, Płonkine sume pravougaonih traka predstavljaju standardan način za konstrukciju normalnih traka.

Naravno, Płonkine sume se mogu takođe primeniti na direktne sisteme algebri sa involucijom. Posmatrajmo proizvoljnu algebru sa involucijom $(A, F, ^*)$ i pretpostavimo da se može predstaviti kao Płonkina suma direktnog sistema algebri sa involucijom. Tada se redukt (A, F) razlaže na Płonkinu sumu redukata gornjih sumanada. Međutim (vraćajući se nazad na polaznu "involutivnu" situaciju), svaki od tih sumanada je zatvoren u odnosu na operaciju involucije *, što ne mora biti tačno za bilo koju dekompoziciju u Płonkinu sumu *-slobodnog redukta proizvoljne algebre sa involucijom.

Kako bismo prebrodili teškoću, nećemo pokušavati da komponujemo algebre koje su već snabdevene involucijom. Umesto toga, mi komponujemo familiju "običnih" algebri (čiji jezik ne sadrži simbol koji odgovara *), indeksiranu involutivnom polumrežom $\mathbf{Y}$, tako da su algebre koje odgovaraju elementima $\alpha, \alpha^* \in Y$, respektivno, antiizomorfne. Neki dodatni uslovi za bijekciju na disjunktnoj uniji posmatrane familije omogućiće nam da pretvorimo tu bijekciju u involuciju. Na ovaj način, dobićemo **involutivnu Płonkinu sumu**.

Ovakav pristup daje neke nove rezultate, koje ćemo prikazati u ovoj glavi. U narednom delu, dajemo glavne konstrukcije i definicije, i dokazujemo osnovnu teoremu o involutivnim Płonkinim sumama i P^*-funkcijama (involutivnim particionim funkcijama). Takođe (u trećem paragrafu), diskutovaće se još neka relevantna pitanja koja se odnose na poddirektna razlaganja involutivnih Płonkinih suma. Ilustrovaćemo naše opšte rezultate involutivnim polugrupama i involutivnim poluprstenima.

1.2. Involutivni direktni sistemi algebri, njihove sume i P^*-funkcije

Razmatraćemo samo algebre koje nemaju konstante tj. nularne operacije. Fiksirajmo neki tip sličnosti T bez simbola konstanti. Dodavanjem ovom tipu simbola unarne operacije * (rezervisanog za involuciju), dobijamo tip sličnosti $T^* = T \cup \{^*\}$.

Neka je $\mathbf{Y} = (Y, \cdot)$ (donja) polumreža. Podsetimo se, familija disjunktnih algebri $\{\mathbf{A}_\alpha \,|\, \alpha \in Y\}$ (gde je $\mathbf{A}_\alpha = (A_\alpha, F_\alpha)$) i $F_\alpha = \{f^{\mathbf{A}_\alpha} \,|\, f \in T\}$, zajedno sa sistemom homomorfizama $\{\Phi_{\alpha,\beta} \,|\, \alpha, \beta \in \mathbf{Y}, \alpha \geq \beta\}$, zove se **Y-uređen sistem algebri** ako su zadovoljeni sledeći uslovi:

(1) za svako $\alpha \in Y$, $\Phi_{\alpha,\alpha}$ je identičko presilkavanje na A_α,

(2) za sve $\alpha, \beta, \gamma \in Y$ takve da je $\alpha \geq \beta \geq \gamma$ imamo

$$\Phi_{\alpha,\beta} \circ \Phi_{\beta,\gamma} = \Phi_{\alpha,\gamma}.$$

Pretpostavimo da je involucija * definisana na Y, tako da imamo involutivnu polumrežu $(Y, \cdot, ^*)$ u kojoj važi $(\alpha^*)^* = \alpha^*$ i $(\alpha\beta)^* = \beta^*\alpha^*$ za sve $\alpha, \beta \in Y$ (primetimo da je svaka involucija na polumreži ujedno i njen automorfizam). Dalje, pretpostavimo da nam je data bijekcija $\sigma : A \to A$, gde je $A = \bigcup_{\alpha \in Y} A_\alpha$, tako da, kao dodatak gornjim uslovima, imamo

(3) za svako $\alpha \in Y$

$$\sigma|_{A_\alpha} : A_\alpha \to A_{\alpha^*}$$

je antiizmorfizam (posebno, ako je $\alpha^* = \alpha$, onda je $\sigma|_{A_\alpha}$ antiautomorfizam od A_α),

(4) $\Phi_{\alpha^*,\beta^*} = (\sigma|_{A_{\alpha^*}}) \circ \Phi_{\alpha,\beta} \circ (\sigma|_{A_\beta})$ važi za sve $\alpha, \beta \in Y$ tako da je $\alpha \geq \beta$ (ovo implicira da je $\sigma|_{A_\alpha} \circ \sigma|_{A_{\alpha^*}} = id_{A_\alpha}$, tako da je $\sigma \circ \sigma = id_A$).

Tada se sistem koji se sastoji od algebri $\mathbf{A}_\alpha$, homomorfizama $\Phi_{\alpha,\beta}$ i bijekcije σ zove **involutivni polumrežno uređeni sistem algebri**.

Definišimo sada **involutivnu Płonkinu sumu** takvog sistema: to je algebra sa involucijom (tipa T^*), $\mathbf{A} = (A, F, ^*)$, gde je $A = \bigcup_{\alpha \in Y} A_\alpha$ i

$F = \{f^{\mathbf{A}} \mid f \in T\}$, tako da za sve n-arne simbole $f \in T$ i $a_i \in A_{\alpha_i}$, $1 \leq i \leq n$, imamo $(\alpha = \alpha_1 \cdots \alpha_n)$:

$$f^{\mathbf{A}}(a_1, \ldots, a_n) = f^{\mathbf{A}_\alpha}(\Phi_{\alpha_1,\alpha}(a_1), \ldots, \Phi_{\alpha_n,\alpha}(a_n)),$$

gde je involucija definisana sa

$$a^* = \sigma(a)$$

za sve $a \in A$ (involuciju u $\mathbf{Y}$ i $\mathbf{A}$ smo označili istim simbolom, ali to neće zadavati probleme).

Na primer, normalne trake sa involucijom [26, 30] se dobijaju iz pravougaonih traka na gore opisan način.

PROPOZICIJA 1.2.1. *Involutivna polugrupa* $\mathbf{S}$ *je normalna traka sa involucijom ako i samo ako je involutivna Płonkina suma pravougaonih traka.*

Dokaz. Dobro je poznato da su normalne trake Płonkine sume (jake polumreže) pravougaonih traka. Štavše, ako predstavimo $\mathbf{S}$ kao takvu sumu, onda se lako vidi da involucija na $\mathbf{S}$ indukuje involuciju na strukturnoj polumreži $\mathbf{Y}$ od $\mathbf{S}$ (videti [25, Propozicija 4.1]), tako da uslov (3) važi. Uslov (4) važi po Lemi 7.1 iz [30]. Obrat tvrđenja sledi neposredno. □

Podsetimo se da se za algebru (A, F) funkcija $p : A \times A - A$ se zove **P-funkcija (particiona funkcija)** ako za sve $x, y, z \in A$ imamo

$$\begin{aligned} p(x,x) &= x, \\ p(x,p(y,z)) &= p(x,p(z,y)), \\ p(p(x,y),z) &= p(x,p(y,z)), \end{aligned}$$

i za sve n-arne operacije $f \in F$ i sve $x_1, \ldots, x_n, y \in A$ važi

$$\begin{aligned} p(f(x_1,\ldots,x_n),y) &= f(p(x_1,y),\ldots,p(x_n,y)), \\ p(y,f(x_1,\ldots,x_n)) &= p(y,f(p(y,x_1),\ldots,p(y,x_n))) \\ p(f(x_1,\ldots,x_n),x_k) &= f(x_1,\ldots,x_n) \quad (1 \leq k \leq n), \\ p(y,f(y,\ldots,y)) &= y. \end{aligned}$$

Ako je sada $(A, F, ^*)$ algebra sa involucijom, i p particiona funkcija na (A, F), onda se p zove **$\mathbf{P}^*$-funkcija** (ili **involutiva particiona funkcija**) ako se za sve $x, y \in A$ imamo

$$p(x^*, y^*) = (p(x,y))^*.$$

Poznato je (na primer, iz [97, Teorema II]) da su P-funkcije i Płonkine sume povezane, tako da P-funkcija $p(x, y)$ indukuje particiju nosača A algebre $\mathbf{A}$

tako da su $x, y \in A$ u istoj klasi ako i samo ako $p(x,y) = x$ i $p(y,x) = y$. Ova particija je u stvari dekompozicija $\mathbf{A}$ u Płonkinu sumu. Obratno, ako je $\mathbf{A}$ Płonkina suma direktnog sistema algebri $\{\mathbf{A}_\alpha \,|\, \alpha \in Y\}$ (sa oznakama kao u prethodnom delu teksta), i ako $x \in A_\alpha$, $y \in A_\beta$, tada je odgovarajuća P-funkcija data sa

$$p(x,y) = \Phi_{\alpha,\alpha\beta}(x).$$

Pokazaćemo da analogno tvrđenje važi za involutivne algebre.

Teorema 1.2.2. *Neka je* $p : A \times A \to A$ P^**-funkcija algebre sa involucijom* $\mathbf{A} = (A, F,^*)$. *Tada je ova algebra involutivna Płonkina suma involutivnog polumrežno uređenog sistema algebri dobijenog na sledeći način: predstavimo* **-slobodan redukt od* $\mathbf{A}$ *kao Płonkinu sumu algebri* $\mathbf{A}_\alpha$, $\alpha \in Y$, *gde je* $\mathbf{Y}$ *polumreža, sa strukturnim homomorfizmima* $\Phi_{\alpha,\beta}$, *tako da se odgovarajuća particiona funkcija poklapa sa* p. *Tada involucija na* $\mathbf{A}$ *daje* $\mathbf{Y}$ *strukturu involutivne polumreže, i dobijeni polumrežno uređeni sistem algebri je involutivni direktni sistem.*

Obratno, svaka se dekompozicija $\mathbf{A}$ *u involutivnu Płonkinu sumu može dobiti na opisani način polazeći od neke* P^**-funkcije na* $\mathbf{A}$.

Dokaz. Pretpostavimo da je (A, F) Płonkina suma sistema algebri $\mathbf{A}_\alpha$, $\alpha \in Y$, uređenog polumrežom $\mathbf{Y}$. Prvo dokazujemo da $\mathbf{Y}$ nasleđuje involuciju iz $\mathbf{A}$. Uzmimo proizvoljne $x, y \in A_\alpha$ za neko $\alpha \in Y$. Tada je $p(x,y) = x$ i $p(y,x) = y$. Sledi,

$$p(x^*, y^*) = (p(x,y))^* = x^*$$

i

$$p(y^*, x^*) = (p(y,x))^* = y^*,$$

što implicira da x^* i y^* pripadaju istoj algebri $\mathbf{A}_\beta$ za neko $\beta \in Y$. Prema tome, $A_\alpha^* \subseteq A_\beta$, i slično, $A_\beta^* \subseteq A_\alpha$, što nam daje za pravo da definišemo $\beta = \alpha^*$ (pretvarajući $\mathbf{Y}$ u involutivnu polumrežu), i pokazuje u isto vreme da za svako $\alpha \in Y$, preslikavanje $^* : A_\alpha \to A_{\alpha^*}$ mora biti antiizomorfizam. Sada je strukturni homomorfizam u Teoremi II iz [97] konstruisan tako da za sve $x \in A_\alpha$ imamo

$$\Phi_{\alpha,\beta}(x) = p(x,y)$$

za proizvoljni element $y \in A_\beta$, $\alpha \geq \beta$. Prema tome,

$$\Phi_{\alpha^*,\beta^*}(x^*) = p(x^*, y^*) = (p(x,y))^* = (\Phi_{\alpha,\beta}(x))^*,$$

što je baš uslov (4) iz definicije involutivnog polumrežno uređenog sistema algebri.

Obratno, neka je $\mathbf{A}$ suma direktnog sistema algebri uređenog involutivnom polumrežom $\mathbf{Y}$. Tada je *-slobodan redukt od $\mathbf{A}$ dobijen kao Płonkina suma $\mathbf{Y}$-uređenog sistema podalgebri redukta, bazirana na P-funkciji p. Jedina stvar koju moramo pokazati je da je p u stvari P^*-funkcija. Neka je $x \in A_\alpha$ i $y \in A_\beta$. Tada, prema (4), imamo

$$p(x^*, y^*) = \Phi_{\alpha^*,\alpha^*\beta^*}(x^*) = (\Phi_{\alpha,\alpha\beta}(x))^* = (p(x,y))^*.$$

Ovim je teorema dokazana. □

Neka je sada $\mathcal{V}$ varijetet tipa T. Sa $\mathcal{V}^*$ označavamo varijetet tipa T^* koji se sastoji od svih algebri sa involucijom čiji su involutivno-slobodni redukti iz $\mathcal{V}$. Drugim rečima, varijetet $\mathcal{V}^*$ je definisan identitetima varijeteta $\mathcal{V}$ i odgovarajućim involutivnim aksiomama.

Takođe, za proizvoljan varijetet $\mathcal{V}$, definišimo $R(\mathcal{V})$, **regularuzaciju** od $\mathcal{V}$. To je varijetet istog tipa kao i $\mathcal{V}$, definisan samo regularnim identitetima koji važe na $\mathcal{V}$. Primetimo da uvek važi $\mathcal{V} \subseteq R(\mathcal{V})$, i jednakost važi ako i samo ako se $\mathcal{V}$ može definisati skupom regularnih identiteta.

PROPOZICIJA 1.2.3. *Neka je $\mathbf{Y}$ involutivna polumreža i pretpostavimo da je $\mathbf{A}$ suma $\mathbf{Y}$-uređenog sistema algebri (tipa T), tako da sve one pripadaju varijetetu $\mathcal{V}$. Tada $\mathbf{A} \in (R(\mathcal{V}))^*$. Ako se, štaviše, involucija na $\mathbf{Y}$ poklapa sa identičkim preslikavanjem, onda $\mathbf{A} \in R(\mathcal{V}^*)$.*

Dokaz. Involutivno-slobodni redukt od $\mathbf{A}$ se može posmatrati kao obična Płonkina suma odgovarajućih sumanada, $\mathbf{A}_\alpha$, $\alpha \in Y$. Prema tome, po Teoremi I iz [97], taj redukt pripada $R(\mathcal{V})$, pa stoga $\mathbf{A} \in (R(\mathcal{V}))^*$. Ako $\mathbf{Y}$ ima identičko preslikavanje kao involuciju, onda svi sumandi $\mathbf{A}_\alpha$, $\alpha \in Y$, pripadaju $\mathcal{V}^*$, a $\mathbf{A}$ je baš njihova Płonkina suma, te je druga polovina propozicije direktna posledica [97, Teorema I]. □

Gornja propozicija ima obrat u slučaju koji je dobro poznat za obične Płonkine sume. Podsetimo se da je varijetet $\mathcal{V}$ **strogo neregularan** ako postoji term $t(x,y)$ od dve promenljive tako da na $\mathcal{V}$ važi $t(x,y) = x$.

PROPOZICIJA 1.2.4. *Neka je $\mathcal{V}$ strogo neregularan varijetet, za koji važi $t(x,y) = x$, tako da je identitet*

$$t(x^*, y^*) = (t(x,y))^*$$

posledica regularnih identiteta od $\mathcal{V}$ i involutivnih aksioma. Tada za svaku algebru $\mathbf{A} \in (R(\mathcal{V}))^*$ postoji involutivna polumreža $\mathbf{Y}$ tako da je $\mathbf{A}$ suma $\mathbf{Y}$-uređenog sistema algebri iz $\mathcal{V}$. Ako je $\mathbf{A} \in R(\mathcal{V}^*)$, onda je involucija na $\mathbf{Y}$ identičko preslikavanje.

Dokaz. Neka $\mathcal{V}$ zadovoljava identitet $t(x,y) = x$. Tada, kao što je poznato iz dokaza Teoreme I iz [97], $p(x,y) = t^{\mathbf{A}}(x,y)$ je particiona funkcija za svaku algebru iz $R(\mathcal{V})$. Posmatrajmo sada proizvoljnu algebru $\mathbf{A} \in (R(\mathcal{V}))^*$. Malopre definisana funkcija $p(x,y)$ je particiona funkcija *-slobodnog redukta od $\mathbf{A}$. Ostaje da se pokaže da je $p(x,y)$ P^*-funkcija na $\mathbf{A}$. Prema datom uslovu, imamo

$$p(x^*, y^*) = t^{\mathbf{A}}(x^*, y^*) = (t^{\mathbf{A}}(x,y))^* = (p(x,y))^*,$$

s obzirom da $\mathbf{A}$ pripada $(R(\mathcal{V}))^*$. Traženi rezultat sada sledi iz Teoreme 1.2.2. Za drugi deo propozicije, dovoljno je primetiti da ako je $\mathcal{V}$ neregularan varijetet, takav je i $\mathcal{V}^*$. Stoga se, korišćenjem Teoreme I iz [97], pokazuje da je $\mathbf{A}$ obična Płonkina suma algebri sa involucijom iz $\mathcal{V}^*$. □

Kako je regularizacija (strogo neregularnog) varijeteta pravougaonih traka varijetet normalnih traka, rezultat Propozicije 1.2.1 sledi direktno iz gornje propozicije, jer je $(xyx)^* = x^*y^*x^*$ posledica involutivnih aksioma.

Međutim, postoji druga primena gornje propozicije, koja ima naročit značaj u radu [31]. Podsetimo se da je **poluprsten** algebra $(A, +, \cdot)$, gde je $(A, +)$ komutativna polugrupa, $(A, \cdot)$ polugrupa, i $\cdot$ je distributivno u odnosu na $+$. Poluprsten je **distributivan** ako zadovoljava dualni distributivni zakon, tj. ako je $+$ distributivno u odnosu na množenje:

$$x + yz = (x + y)(x + z).$$

Na kraju, poluprsten je **idempotentan** ako su takvi oba njegova polugrupna redukta.

POSLEDICA 1.2.5. *Svaki idempotentan distributivan poluprsten sa involucijom se može predstaviti kao involutivna Płonkina suma involutivnog polumrežno uređenog sistema idempotentnih distributivnih poluprstena koji zadovoljavaju identitet*

$$x + xyx = x.$$

Obratno, involutivna Płonkina suma svakog takvog sistema je idempotentni distributivni poluprsten sa involucijom.

Dokaz. Iz Teoreme 1.6 iz [88] sledi da je svaki idempotentni distributivni poluprsten (ID-poluprsten) Płonkina suma polumrežno uređenog sistema ID-poluprstena za koje važi $x + xyx = x$. Poslednji identitet definiše jako neregularan varijetet $\mathcal{V}$ ID-poluprstena. Iz Teoreme I iz [97] imamo da se $R(\mathcal{V})$ poklapa sa varijetetom svih ID-poluprstena, tako da je $(R(\mathcal{V}))^*$ varijetet svih

ID-poluprstena sa involucijom. Pošto iz komutativnosti + i aksioma involucije imamo

$$(x + xyx)^* = x^* + x^* y^* x^*,$$

rezultat posledice sledi direktno iz Propozicija 1.2.3 i 1.2.4. □

ID-poluprsteni će biti detaljnije izučavani u Glavi 3.

1.3. Poddirektno nesvodljive involutivne Płonkine sume

Ponovimo još jednom, netrivijalna algebra **A** je **poddirektno nesvodljiva** ako za svaku familiju $\{\theta_i \mid i \in I\}$ njenih kongruencija važi sledeća implikacija:

$$\bigcap_{i \in I} \theta_i = \Delta_A \;\Rightarrow\; (\exists i \in I)\theta_i = \Delta_A .$$

Drugim rečima, **A** ima najmanju neidentičku kongruenciju, nazvanu **monolit**. Naravno, monolit mora biti glavna konguencija $\theta(a, b)$ za neke $a, b \in A$.

Važnost poddirektno nesvodljivih algebri leži u činjenici da one sadrže mnoštvo informacija o strukturi varijeteta kome pripadaju. Grubo rečeno, možemo reći da su poddirektno nesvodljive algebre građevinski blokovi zgrade varijeteta.

Lakser, Padmanabhan i Platt su u [71] opisali sve poddirektno nesvodljive Płonkine sume čiji sumandi pripadaju datom varijetetu $\mathcal{V}$. To su poddirektno nesvodlji elementi $\mathcal{V}$ i algebre dobijene dodavanjem apsorptivnog elementa (tj. nule) poddirektno nesvodljivim elementima $\mathcal{V}$ koji nemaju nulu. Jasno, algebra ove vrste je u stvari Płonkina suma čija struktura je bazirana na dvoelementnoj polumreži, gde je "donja" klasa trivijalna algebra. Zadatak ovog paragrafa je da se diskutuju poddirektno nesvodljive involutivne Płonkine sume (gde su sumandi uzeti iz fiksnog varijeteta $\mathcal{V}$ tipa T).

U nameri da dokažu gore navedeno, autori rada [71] prvo pokazuju da ako je Płonkina suma poddirektno nesvodljiva, onda njena strukturna polumreža mora biti ili trivijalna ili poddirektno nesvodljiva. Analogno tvrđenje je tačno za involutivne Płonkine sume i njihove strukturne involutivne polumreže, i delovi argumenata prezentiranih u [71] mogu biti (s mailm prilagođavanjem) primenjeni skoro doslovce.

Lema 1.3.1. *Neka je* **Y** *involutivna polumreža i* **A** *suma involutivnog* **Y**-*uređenog sistema algebri. Ako je* **A** *poddirekntno nesvodljiva, onda je* **Y** *ili trivijalna, ili poddirekntno nesvodljiva.*

Dokaz. Najpre, za kongruenciju θ od $\mathbf{Y}$ definišimo ekvivalenciju $\theta^{\mathbf{A}}$ od A tako da za $x \in A_i$, $y \in A_j$, $i, j \in Y$ imamo $(x, y) \in \theta^{\mathbf{A}}$ ako i samo ako $(i, j) \in \theta$ i postoji $k \in Y$ tako da je $k \leq ij$, $k\theta i\theta j$ i $\Phi_{i,k}(x) = \Phi_{j,k}(y)$. Nije teško proveriti da je $\theta^{\mathbf{A}}$ kongruencija od $\mathbf{A}$. Pokazaćemo da je ona kompatibilna sa *. Jasno, ako je $i\theta j$, onda je i $i^*\theta j^*$, i imamo

$$\Phi_{i^*,k^*}(x^*) = (\Phi_{i,k}(x))^* = (\Phi_{j,k}(y))^* = \Phi_{j^*,k^*}(y^*),$$

što daje $(x^*, y^*) \in \theta^{\mathbf{A}}$.

Dalje, pretpostavimo da je

$$\bigcap_{m \in I} \theta_m = \Delta_Y,$$

gde su θ_m, $m \in I$, sve neidentičke kongruencije na $\mathbf{Y}$. Naš cilj je da dokažemo da je

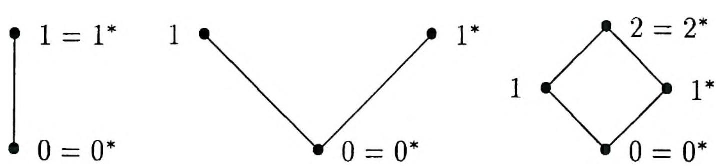
$$\bigcap_{m \in I} \theta_m^{\mathbf{A}} = \Delta_A,$$

što onda daje traženi zaključak. Ako je $(x, y) \in \theta_m^{\mathbf{A}}$ za sve $m \in I$, onda $x, y \in A_i$ za neko $i \in Y$, i prema tome, za svako $m \in I$ postoji $k_m \in Y$ tako da je $k_m \leq i$, $(k_m, i) \in \theta_m$ i $\Phi_{i,k_m}(x) = \Phi_{i,k_m}(y)$. Dokažimo da se može uzeti $m \in I$ tako da je $k_m = i$. Ako ovo nije slučaj, postoje $m_1, m_2 \in I$ tako da je $k_{m_1} \neq k_{m_2}$ i $k_{m_1}k_{m_2} < i$, tako da važi $k_{m_1}k_{m_2} < k_{m_1} < i$.

Posmatrajmo sada glavnu kongruenciju $\theta(k_{m_1}, k_{m_1}k_{m_2})$ od $\mathbf{Y}$. Lako se vidi da ako $(x, i) \in \theta(k_{m_1}, k_{m_1}k_{m_2})$, onda ili je $x = i$, ili $i \leq k_{m_1}$, ili $i \leq k_{m_1}^*$. Drugi slučaj je, jasno, nemoguć. Pretpostavimo da važi treći slučaj. Tada je $i \leq k_{m_1}^* < i^*$, što implicira $i^* < i$, kontradikcija. Prema tome, $\{i\}$ je blok razmatrane kongruencije. Tako, ako je $\theta(k_{m_1}, k_{m_1}k_{m_2}) = \theta_\ell$, onda je $k_\ell = i$. Kontradikcija. Sledi $x = y$, što je i trebalo dokazati. □

Sada, ako je strukturna involutivna polumreža poddirektno nesvodljive Płonkine sume trivijalna, reč je o poddirektno nesvodljivim članovima $\mathcal{V}^*$, i ovaj slučaj naćemo dalje razmatrati.

S druge strane, poddirektno nesvodljive polumreže su poznate iz Teoreme 3.1 u [30]. To su Σ_2^*, Σ_3^*, i Σ_4^*, date na Slici 1.1.



Slika 1.1. Σ_2^*, Σ_3^* i Σ_4^*

Jasno, ovaj rezultat znači da će se naša razmatranja podeliti na tri odvojena slučaja u odnosu na involutivnu polumrežu na kojoj se razmatrana involutivna Płonkina suma bazira. U svim podslučajevima, međutim, odgovarajući sumandi će biti označeni elementima strukturne involutivne polumreže kao što je dato na Slici 1.1. Prema tome, susretaćemo se sa oznakama poput $\mathbf{A}_0$, $\mathbf{A}_{1^*}$ i $\mathbf{A}_2$ (naravno, $\mathbf{A}_0$, na primer, je notacija korišćena sa različitim strukturnim polumrežama, ali neće biti zabune s obzirom da će iz konteksta biti sve jasno; štaviše, ova blaga zloupotreba notacije biće nekad korisna, videti sledeću lemu).

Pre nego što pređemo na glavne rezultate ovog dela, napravićemo jednu važnu primedbu.

LEMA 1.3.2. *Neka je* $\mathbf{A}$ *poddirektno nesvodljiva involutiovna Płonkina suma algebri. Tada je* $\mathbf{A}_0$ *trivijalna algebra, tj.* $|A_0| = 1$.

Dokaz. Neka je θ ekvivalencija na A koja kolapsira A_0 i poklapa se sa identičkom relacijom van A_0. Takođe, definišimo ξ stavljajući $(x, y) \in \xi$ ako i samo ako $\Phi_{i,0}(x) = \Phi_{j,0}(y)$, gde je $x \in A_i$ i $y \in A_j$. Obe ove relacije su kongruencije na $\mathbf{A}$, a uz to su još i kompatibilne sa *, kao što se može videti iz

$$\Phi_{i^*,0}(x^*) = (\Phi_{i,0}(x))^* = (\Phi_{j,0}(y))^* = \Phi_{j^*,0}(y^*).$$

Kako ξ sigurno nije identička relacija, sledi da je $\theta = \Delta_A$, tj. $|A_0| = 1$. □

Razmotrimo prvi (i daleko najlakši) od svih slučajeva. Ako je $\mathbf{A}$ algebra, sa $\mathbf{A}^0$ označavamo algebru dobijenu dodavanjem apsortivnog elementa 0 algebri $\mathbf{A}$. Drugim rečima, operacije algebre $\mathbf{A}^0$ definisane su na sledeći način

$$f^{\mathbf{A}^0}(a_1, \ldots, a_n) = \begin{cases} 0, & 0 \in \{a_1, \ldots, a_n\}, \\ f^{\mathbf{A}}(a_1, \ldots, a_n), & \text{inače}. \end{cases}$$

Posebno, ako je $\mathbf{A}$ algebra sa involucijom, u $\mathbf{A}^0$ imamo $0^* = 0$.

TEOREMA 1.3.3. *Neka je algebra* $\mathbf{A}$ *suma* Σ_2^**-uređenog sistema algebri iz* $\mathcal{V}$. *Tada je* $\mathbf{A}$ *poddirektno nesvodljiva ako i samo ako je* $\mathbf{A} = \mathbf{B}^0$, *gde je involutivna algebra* $\mathbf{B} \in \mathcal{V}^*$ *ili trivijalna, ili poddirektno nesvodljiva bez apsorptivnih elemenata.*

Dokaz. Kako se suma od Σ_2^*-uređenog sistema algebri tipa T poklapa sa običnom Płonkinom sumom sistema algebri sa involucijom (tipa T^*) koji je uređen dvoelementnom polumrežom, tvrđenje ove teoreme je posledica glavnog rezultata iz [71]. □

Dalje, neka je $\mathbf{A}$ algebra (tipa T). Definišimo **0-direktnu uniju** $I_0^*(\mathbf{A})$ od $\mathbf{A}$ sa svojom antiizomorfnom kopijom $\mathbf{A}^*$ (imamo fiksan antiizomorfizam $a \mapsto a^*$) na skupu $\{0\} \cup A \cup A^*$ tako da su operacije rezultujućeg sistema date sa

$$f^{I_0^*(\mathbf{A})}(a_1, \ldots, a_n) = \begin{cases} f^{\mathbf{A}}(a_1, \ldots, a_n), & a_1, \ldots, a_n \in A, \\ f^{\mathbf{A}^*}(a_1, \ldots, a_n), & a_1, \ldots, a_n \in A^*, \\ 0, & \text{inače.} \end{cases}$$

Algebra $I_0^*(\mathbf{A})$ je baš suma Σ_3^*-uređenog sistema algebri u kome je klasa koja odgovara $0 \in \Sigma_3^*$ trivijalna. Osobine involutivnih polugrupa dobijenih na ovaj način proučavane su u radu [18].

Teorema 1.3.4. *Neka je algebra* $\mathbf{A}$ *suma* Σ_3^**-uređenog sistema algebri iz* $\mathcal{V}$. *Ako je* $\mathbf{A}$ *poddireknto nesvodljiva, onda je* $\mathbf{A} = I_0^*(\mathbf{B})$, *gde je* $\mathbf{B} \in \mathcal{V}$ *ili trivijalna, ili poddirektno nesvodljiva bez apsorptivnih elemenata. Ako tip* T *sadrži najmanje jedan simbol arnosti* ≥ 2, *onda je i obrat tačan. Ako je* T, *međutim, unaran tip, onda je* $I_0^*(\mathbf{B})$ *poddirektno nesvodljiva ako i samo ako je* $\mathbf{B}$ *trivijalna.*

Dokaz. ($\Rightarrow$) Prema Lemi 1.3.2, algebra $\mathbf{A}_0$ mora biti trivijalna. Sledi da ako je $\mathbf{B} = \mathbf{A}_1$, onda je $\mathbf{A} = I_0^*(\mathbf{B})$. Sada treba pokazati da je $\mathbf{B}$ poddirektno nesvodljiv član $\mathcal{V}$ koji nema apsortivni element.

Za kongruenciju θ od $\mathbf{B}$ definišimo $\theta^* = \{(b_1^*, b_2^*) \mid (b_1, b_2) \in \theta\}$. Lako je videti da je θ^* kongruencija od $\mathbf{B}^*$. Štaviše, ako je

$$\theta' = \theta \cup \theta^* \cup \{(0,0)\},$$

onda je θ' kongruencija od $I_0^*(\mathbf{B})$.

Tako, pretpostavimo da je $\{\theta_i \mid i \in I\}$ skup kongruencija od $\mathbf{B}$ čiji je presek Δ_B. Onda je presek svih θ_i, $i \in I$, očigledno Δ_{B^*}, pa je

$$\bigcap_{i \in I} \theta_i' = \Delta_A.$$

Sledi da je $\theta_j' = \Delta_A$ za neko $j \in I$, odakle je $\theta_j = \Delta_B$, i $\mathbf{B}$ je poddirektno nesvodljiva.

Konačno, pretpostavimo da $\mathbf{B}$ ima apsorptivni element ∞ i da ∞ nije jedini element od $\mathbf{B}$. Tada je ekvivalencija θ, čiji je jedan od blokova $\{0, \infty, \infty^*\}$, dok su svi ostali su jednoelementni, očigledno kongruencija od $\mathbf{A} = I_0^*(\mathbf{B})$, kao i ξ, čiji su blokovi B, B^* i $\{0\}$. Kako važi $\theta \cap \xi = \Delta_A$, došli smo do kontadikcije, i prema tome, ako je $\mathbf{B}$ netrivijalna, ne može imati nulu.

S druge strane, ako radimo sa unarnim algebrama, posmatramo ekvivalenciju χ od A, čiji su blokovi $\{0\}$ i svi parovi $\{b, b^*\}$, $b \in B$, Lako se vidi da je χ kongruencija od $\mathbf{A}$. Međutim, presek χ sa malopre definisanom kongruencijom ξ je baš Δ_A, tako da je $\xi = \Delta_A$, što znači da $\mathbf{B}$ mora biti trivijalna.

($\Leftarrow$) Razmotrimo prvo slučaj kada $\mathcal{V}$ nije varijetet unarnih algebri. Pretpostavimo da je $\mathbf{B}$ netrivijalna, u protivnom, situacija je jasna. Neka je $\theta(a,b)$, $a, b \in B$, monolit od $\mathbf{B}$. Dokazujemo da je $(\theta(a,b))'$ monolit od $\mathbf{A} = I_0^*(\mathbf{B})$. Očigledno, dovoljno je pokazati da svaka glavna kongruencija od $\mathbf{A}$ sadrži par (c,d) gde su $c, d \in B$, $c \neq d$. Kako važi $\theta^{\mathbf{A}}(x,y) = \theta^{\mathbf{A}}(x^*,y^*)$ za sve $x, y \in A$, i kako za sve $x \in B$, $y^* \in B^*$ lako dobijamo

$$(0,z) \in \theta(x,y^*)$$

za $z = f^{\mathbf{B}}(x,\ldots,x)$ i $f \in T$ tako da $ar(f) \geq 2$, možemo se ograničiti na glavne kongruencije oblika $\theta^{\mathbf{A}}(0,\beta)$, $\beta \in B$.

Kako $\mathbf{B}$ nema apsorptivni element, mora postojati $f \in T$ arnosti n, $1 \leq k \leq n$ i $b_1, \ldots, b_{k-1}, b_{k+1}, \ldots, b_n \in B$, tako da je

$$\alpha = f^{\mathbf{B}}(b_1, \ldots, b_{k-1}, \beta, b_{k+1}, \ldots, b_n) \neq \beta.$$

S obzirom da je $f^{\mathbf{A}}(b_1, \ldots, b_{k-1}, 0, b_{k+1}, \ldots, b_n) = 0$, imamo $(0,\alpha) \in \theta^{\mathbf{A}}(0,\beta)$ i tako $(\alpha,\beta) \in \theta^{\mathbf{A}}(0,\beta)$, kao što je i traženo.

Ostaje da se primeti da ako je $\mathbf{B}$ trivijalna unarna algebra, onda je mreža kongruencija od $I_0^*(\mathbf{B})$ troelementni lanac, pa je time dokaz teoreme kompletiran. □

Konačno, razmotrimo poddirektno nesvodljive sume bazirane na Σ_4^*. Kako bismo rešili ovaj slučaj, treba nam novi pojam. Neka je $\mathbf{A}$ algebra (tipa T) i neka je $a, b \in A$. Kažemo da je par (a,b) **razdvojiv** ako postoji unarni polinom π algebre $\mathbf{A}$ tako da je

$$\pi(a) \neq \pi(b).$$

Algebra $\mathbf{A}$ ima **osobinu razdvajanja** ako je svaki par njenih različitih elemenata razdvojiv. Varijetet ima osobinu razdvajanja ako tu osobinu imaju svi njegovi članovi.

PRIMER 1.3.5. Svaka netrivijalna algebra $\mathbf{A}$ koja ima idempotentnu i komutativnu operaciju $q = q(x,y)$ ima osobinu razdvajanja. Pretpostavimo da nema. Tada za $a \in A$ definišimo unarni polinom π_a od $\mathbf{A}$ sa $\pi_a(x) = q(x,a)$. Za bilo koje $a, b \in A$, $a \neq b$ imamo $a = q(a,a) = \pi_a(a) = \pi_a(b) = q(b,a) =$

$\pi_b(a) = \pi_b(b) = q(b,b) = b$, kontradikcija. Tako, svaki varijetet koji ima term $t(x,y)$ za koji važe identiteti

$$t(x,x) = x, \quad t(x,y) = t(y,x),$$

ima osobinu razdvajanja.

Teorema 1.3.6. *Neka je algebra* $\mathbf{A}$ *suma* Σ_4^**-uređenog sistema algebri iz varijeteta* $\mathcal{V}$*, sa strukturnim homomorfizmom* $\Phi_{2,1} : \mathbf{A}_2 \to \mathbf{A}_1$ *(što, prema uslovu (4), jedinstveno određuje homomorfizam* $\Phi_{2,1^*} : \mathbf{A}_2 \to \mathbf{A}_{1^*}$*, po formuli* $\Phi_{2,1^*}(x) = (\Phi_{2,1}(x^*)^*)$*. Ako je* $\mathbf{A}$ *poddirektno nesvodljiva, onda važe sledeća dva uslova:*

(1) $I_0^*(\mathbf{A}_1)$ *(podalgebra od* $\mathbf{A}$ *sa univezumom* $A_0 \cup A_1 \cup A_{1^*}$*) je jedna od poddirektno nesvodljivih iz Teoreme 1.3.4;*

(2) Za sve $a,b \in A_2$*, ako* $(\Phi_{2,1}(a), \Phi_{2,1}(b))$ *i* $(\Phi_{2,1}(a^*), \Phi_{2,1}(b^*))$ *nisu razdvojivi u* $\mathbf{A}_1$*, onda je* $a = b$*.*

Obrat je takođe tačan, pod uslovom da $\mathbf{A}$ *nije unarna algebra. S druge strane, ako se tip* T *sastoji od unarnih operacijskih simbola, onda nijedna suma* Σ_4^**-uređenog sistema algebri tipa* T *nije poddirektno nesvodljiva.*

Dokaz. Kratkoće radi, označimo $\mathbf{B} = \mathbf{A}_1$ i $\mathbf{C} = \mathbf{A}_2$, dok se $\mathbf{C}^*$ odnosi na algebru $\mathbf{C}$ snabdevenu involucijom nasleđenom od $\mathbf{A}$. Takođe, označimo sa $\mathbf{D}$ podalgebru od $\mathbf{A}$ sa univezumom $A_0 \cup A_1 \cup A_{1^*}$.

($\Rightarrow$) (1) Za kongruenciju θ od $\mathbf{D}$, označimo sa $\theta' = \theta \cup \Delta_{A_2}$. Jasno, θ' je kongruencija od $\mathbf{A}$. Prema tome, ako je θ_i $i \in I$, familija kongruencija od $\mathbf{D}$ čiji je presek Δ_D, onda je presek svih θ_i', $i \in I$, jednak Δ_A. Sledi, za neko $j \in I$ imamo $\theta_j' = \Delta_A$, što implicira $\theta_j = \Delta_D$. Tako, $\mathbf{D}$ je poddirektno nesvodiva.

(2) Pretpostavimo da su $a,b \in C$, $a \neq b$, takvi da je $\pi(\Phi_{2,1}(a), c) = \pi(\Phi_{2,1}(b), c)$ i $\pi(\Phi_{2,1}(a^*), c) = \pi(\Phi_{2,1}(b^*), c)$ za sve binarne polinomne operacije π od $\mathbf{B}$ i sve $c \in B$. Posmatrajmo ekvivalenciju $\chi = \theta^{\mathbf{C}^*}(a,b) \cup \Delta_D$. Naš cilj je da dokažemo da je χ kongruencija od $\mathbf{A}$, što je dovoljno da se dokaže direktni deo teoreme. Naravno, ako je μ monolit od $\mathbf{D}$ i $\mu' = \mu \cup \Delta_C$, onda je μ' kongruencija od $\mathbf{A}$ i

$$\chi \cap \mu' = \Delta_A,$$

što je kontradikcija.

Stoga pretpostavimo da $(c,d) \in \chi$, $c \neq d$. Neka je $f \in T^*$ simbol arnosti n. Dalje, neka je $1 \leq k \leq n$ i neka su $a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n \in A$ proizvoljni. Dokazujemo da

$$(f^{\mathbf{A}}(a_1, \ldots, a_{k-1}, c, a_{k+1}, \ldots, a_n), f^{\mathbf{A}}(a_1, \ldots, a_{k-1}, d, a_{k+1}, \ldots, a_n)) \in \chi,$$

što je dovoljno da se dobije traženi rezultat. Gornje tvrđenje je, jasno, tačno ako ili svi a_i pripadaju C, ili ako je neki od njih 0. Situacija je ista ako $a_i \in B$ i $a_j^* \in B$ za neke i, j. U protivnom, pretpostavimo, na primer, da za sve i imamo $a_i \in B \cup C$, sa bar jednim od razmatranih elemenata iz B. Pokazaćemo da je $\Phi_{2,1}(c) = \Phi_{2,1}(d)$, pa nije teško dobiti traženi zaključak.

Pre svega, primetimo da se proizvoljan unarni polinom π tipa T^* može napisati u formi $\pi(x) = q_\pi(x, x^*)$, gde je q_π polinom tipa T (ne sadrži *). Pošto je $\Phi_{2,1}$ homomorfizam (T-algebri), za svaku unarnu polinomsku operaciju $\pi(x)$ algebre $\mathbf{C}^*$ postoji binarna polinomska operacija $q'_\pi(x, y)$ od $\mathbf{B}$ (koja je tipa T) tako da imamo

$$\Phi_{2,1}(\pi(x)) = q'_\pi(\Phi_{2,1}(x), \Phi_{2,1}(x^*))$$

za sve $x \in C$. Sada prema teoremi o generisanju kongruencija (videti, [77, Teorema 4.19]) nalazimo prirodan broj m, elemente $z_1, \ldots, z_m, z_{m+1} \in C$, kao i unarne polinome $\pi_1, \ldots, \pi_m$ od $\mathbf{C}^*$ tako da je $z_1 = c$, $z_{m+1} = d$ i $\{z_r, z_{r+1}\} = \{\pi_r(a), \pi_r(b)\}$ za sve $1 \leq r \leq m$. Prema učinjenim pretpostavkama, sledi da je

$$\begin{aligned} \Phi_{2,1}(\pi_r(a)) &= g'_{\pi_r}(\Phi_{2,1}(a), \Phi_{2,1}(a^*)) = \\ &= g'_{\pi_r}(\Phi_{2,1}(b), \Phi_{2,1}(a^*)) = \\ &= g'_{\pi_r}(\Phi_{2,1}(a), \Phi_{2,1}(b^*)) = \Phi_{2,1}(\pi_r(b)) \end{aligned}$$

(gde smo koristili unarne polinome $q'_{\pi_r}(x, \Phi_{2,1}(a^*))$ i $q'_{\pi_r}(\Phi_{2,1}(b), x)$ od $\mathbf{B}$), što implicira

$$\Phi_{2,1}(z_r) = \Phi_{2,1}(z_{r+1})$$

za sve $1 \leq r \leq m$. Prema tome, imamo $\Phi_{2,1}(c) = \Phi_{2,1}(d)$, kao što je traženo.

($\Leftarrow$) Pretpostavimo da (1) i (2) važe u $\mathbf{A}$. Slično kao u Teoremi 1.3.4, dovoljno je dokazati da svaka glavna kongruencija $\theta(a, b)$ od $\mathbf{A}$, $a \neq b$, sadrži par (c, d), $c \neq d$, tako da $c, d \in D$. Naravno, ako $a, b \in D$, nema šta da se dokazuje.

Pretpostavimo da $a, b \in C$. Prema (2), postoji unarni polinom π od $\mathbf{B}$ tako da je ili $\pi(\Phi_{2,1}(a)) \neq \pi(\Phi_{2,1}(b))$, ili važi $\pi(\Phi_{2,1}(a^*)) \neq \pi(\Phi_{2,1}(b^*))$. U svakom slučaju upravo smo našli različite elemente $c, d \in B \subseteq D$ tako da $(c, d) \in \theta(a, b)$. Ako je $a = 0$ i $b \in C$, onda birajući $x \in B$ i $f \in T$, $ar(f) \geq 2$, na proizvoljan način, imamo $c = f^{\mathbf{A}}(b, x, \ldots, x) \in B$ i $(0, c) \in \theta(0, b)$. Na kraju, ako je $a \in B$ (slučaj $a^* \in B$ je analogan) i $b \in C$, izaberimo $y \in A_{1^*}$ i $f \in T$ kao malopre. Imamo

$$\begin{aligned} f^{\mathbf{A}}(a, y, \ldots, y) &= 0, \\ c = f^{\mathbf{A}}(b, y, \ldots, y) &\in B^*, \end{aligned}$$

i $(0,c) \in \Theta(a,b)$, kao što smo tražili.

S druge strane, ako je $\mathcal{V}$ varijetet unarnih algebri, onda primetimo da za bilo koju kongruenciju θ od $\mathbf{C}$, ekvivelencija $\theta' = \theta \cup \Delta_D$ jeste kongruencija od $\mathbf{A}$. U tom slučaju, ako je $\mu' = \mu \cup \Delta_C$, gde je μ monolit od $\mathbf{D}$, onda je $\theta' \cap \mu' = \Delta_A$, i prema tome, $\theta' = \Delta_A$, što povlači da je Δ_C jedina kongruencija od $\mathbf{C}$, što je nemoguće osim ako $\mathbf{C}$ nije trivijalna (recimo, $C = \{\top\}$). Primetimo da je ekvivalencija ξ, koja kolapsira 0 i $\top$ dok su druge klase jednoelmentne, kao i ξ', čiji blokovi su $\{\top\}$ i $A \setminus \{\top\} = \{0\} \cup B \cup B^*$, kongruencije od $\mathbf{A}$. Pošto obe relacije ξ i ξ' nisu identičke, i pošto je $\xi \cap \xi' = \Delta_A$, dobili smo kontadikciju. □

Uslov (2) gornje teoreme implicira da preslikavanje $c \mapsto (\Phi_{2,1}(c), \Phi_{2,1^*}(c))$, $c \in C$, mora biti injektivno. Prema tome, lako dokazujemo sledeće tvrđenje.

POSLEDICA 1.3.7. *Koristeći istu notaciju kao u gornjoj teoremi, ako je* $|B| \leq k$, *onda je* $|C| \leq k^2$. *Štaviše, algebra* $\mathbf{C}$ *može imati najviše* k *fiksnih tačaka involucije. Sledi da ako* $\mathcal{V}$ *zadovolajva uslove Propozicije 1.2.4 i ako je rezidualno* $\leq k$, *onda je* $(R(\mathcal{V}))^*$ *rezidualno* $\leq (k+1)^2$.

Pošto sve pravougaone trake imaju osobinu razdvojivosti (dovoljno je uzeti $\pi(x,y) = xyx$ u Primeru 1.3.5), rezultati Glave 7 u [30], koji daju kompletnu listu poddirektno nesvodljivih normalnih traka sa involucijom, su više ili manje neposredna posledica teorema ovog paragrafa. Takođe, ove teoreme služe kao glavna pomoć u nalaženju poddirketno nerazloživih ID-poluprstena sa involucijom u [31]. U stavri, kao što ćemo videti i Glavi 3, određivanje mreže varijeteta ID-poluprstena sa involucijom — što je glavni rezultat [31] — je skoro kompletno zasnovano na rezultatima prezentiranim u ovoj glavi.

2.1. Istorijski pregled

Kao samostalna algebarska disciplina, involutivne polugrupe počinju svoj razvoj radovima D. J. Foulisa o Baerovim *-polugrupama početkom šezdesetih godina prošlog veka. Baerove *-polugupe javljaju se u fizici, algebri i geometriji [39]. Krajem sedamdesetih godina pojavljuju se radovi T. E. Nordahla i H. E. Scheiblicha [84], M. P. Drazina [33], N. Reillyja [102]. Početkom osamdesetih K. S. S. Nambooripad i F. J. Pastijn štampaju svoj rad *Regular involution semigroups* [81]. Posle toga, sledi serija radova o tzv. *-regularnim polugrupama i srodnim temama [1, 14, 126].

Na našim prostorima involutivnim polugrupama su se bavili S. Crvenković [14], J. Cvetković [22], I. Dolinka [23, 29, 25, 26, 30] i autor ovoga rada [18, 19, 32, 121].

O polugrupama binarnih relacija ima takođe dosta radova. Na našem jeziku, ovoj temi je posvećena knjiga R. Sz. Madarász i S. Crvenkovića *Relacione algebre* [73]. Značajan doprinos u zasnivanju teorije polugrupa binarnih relacija dali su B. M. Schein [111] i njegov učenik D. A. Bredikhin [11]. Spomenimo da je aksiomatizaciju klase $\mathcal{R}el(\cdot,^{-1})$ svih involutivnih polugrupa binarnih relacija dao R. McKenzie 1966. godine u svojoj doktorskoj disertaciji [75]. Kasnije, Schein je dokazao da ova klasa nije varijetet [111].

2.2. *-regularne polugrupe

Označimo sa $M_n(C)$ prsten kompleksnih matrica formata $n \times n$. **Uopštena inverzna matrica** X za matricu A se dobija kao rešenje sledećeg sistema matričnih jednačina:

$$AXA = A, \quad XAX = X, \quad (AX)^* = AX, \quad (XA)^* = XA,$$

gde je * operator transponovanja i konjugovanja. Matrica $X \in M_n(C)$ koja je rešenje gornjeg sistema (koje postoji za sve $A \in M_n(C)$), naziva se još i **Moore-Penrose-Stojaković inverz** za matricu A. U literaturi se ovo jedinstveno rešenje označava sa A^+.

Napisano je više od 2000 radova na temu uopštenja inverzne matrice, kao i dvadesetak knjiga. Ove knjige i radovi sa bave različitim pristupima teoriji matrica i njenim primenama u raznim oblastima matematike: teoriji klasičnih algebarskih struktura, linearnom i nelinearnom programiranju, algebarskoj geometriji, statistici, kvantnoj mehanici, itd.

Pojam *-regularnosti za polugrupe uveo je M. P. Drazin 1979. godine, motivisan prstenom $M_n(C)$. U radu [81], Nambooripad i Pastijn uvode novu definiciju *-regularnosti za polugrupe, ekvivalentnu Drazinovoj. Treba reći da je L. A. Skornjakov u knjizi [112] definisao prstene sa unarnom operacijom * tako da su zadovoljeni sledeći identiteti:

$$\begin{aligned} (xy)^* &= y^*x^*, \\ (x^*)^* &= x, \\ (x+y)^* &= x^* + y^*, \end{aligned}$$

kao i kvazi-identitet

$$xx^* = 0 \Rightarrow x = 0.$$

Multiplikativni redukti ovih prstena su *-regularne polugrupe sa nulom.

*-regularne polugrupe se definišu kao involutivne polugrupe $\mathbf{S} = (S, \cdot, ^*)$ u kojima za svako $a \in S$ postoji $x \in S$ tako da je $axa = a$, $xax = x$, $(ax)^* = ax$, $(xa)^* = xa$. Lako se pokazuje da je ovo x jedinstveno. Ekvivalentno, involutivna polugrupa je *-regularna ako svaka njena $\mathcal{L}$-klasa sadrži (jedinstvenu) projekciju, idempotent fiksiran involucijom.

PRIMER 2.2.1. Involutivna polugrupa zadata tablicom

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

i involucijom * za koju važi $a^* = b$, $b^* = a$, $c^* = c$, $d^* = d$ je nekomutativna *-regularna polugrupa sa netrivijalnom involucijom, koja nije grupa.

Uopšteni inverz u *-regularnim polugrupama je jedinstven, pa imamo alternativnu definiciju *-regularne polugrupe kao algebre sa jednom binarnom i dve unarne operacije $\mathbf{S} = (S, \cdot, ^*, ^+)$, koja pripada varijetetu definisanom identitetima

$$\begin{aligned} (xy)z &= x(yz), \\ (xy)^* &= y^*x^*, \\ (x^*)^* &= x, \\ xx^+x &= x, \\ x^+xx^+ &= x^+, \\ (xx^+)^* &= xx^+, \\ (x^+x)^* &= x^+x, \end{aligned}$$

Ovako zadate *-regularne polugrupe imaju sledeće osobine.

TEOREMA 2.2.2. ([14], [81]) *Ako je* $\mathbf{S} = (S, \cdot, ^*, ^+)$ **-regularna polugrupa, onda za sve $a \in S$ važi:*

(1) $(a^+)^+ = a$,

(2) $(a^+)^* = (a^*)^+$,

(3) $(a^*a)^+ = a^+(a^*)^+$,

(4) $a^+(a^*)^+a^* = a^+ = a^*(a^*)^+a^+$,

(5) $a^+aa^* = a^* = a^*aa^+$.

TEOREMA 2.2.3. (S. Crvenković, [14]) *Ako u *-regularnoj polugrupi* $\mathbf{S}$ *važi $xaa^* = a^*$ i $a^*ay = a^*$ za neke $a, x, y \in S$, tada je $a^+ = xay$.*

TEOREMA 2.2.4. (S. Crvenković, [14]) *Neka je* $\mathbf{S}$ *konačna *-reguarna polugrupa. Tada za sve $a \in S$ postoji $n \in \mathbb{N}$ tako da je $a^+ = (a^*a)^{n-1}a$.*

Sledeće tvrđenje je poslužilo kao inspiracija za rad [23].

TEOREMA 2.2.5. (S. Crvenković, [14]) *Involutivna polugrupa* $\mathbf{S} = (S, \cdot, ^*)$ *je *-regularna ako i samo ako za sve $a \in S$ jednačina*

$$aa^*ax = a$$

ima najmanje jedno rešenje. U tom slučaju, $a^+ = (ax)^*$.

Međutim, rešenje gornje jednačine ne mora biti jedinstveno u *-regularnim polugrupama.

PRIMER 2.2.6. Gornja jednačina nema jedinstevno rešenje svakoj *-regularnoj polugrupi sa nulom. Drugi primer *-regularne polugrupe u kojoj gornja jednačina nema rešenje je polugrupa kompleksnih kvadratnih matrica. Jednačina

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}^*\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

ekvivalentna je sledećem sistemu

$$\begin{aligned} 4x_1 + 4x_3 &= 1, \\ 4x_2 + 4x_4 &= 1, \end{aligned}$$

čija rešenja nisu jedinstvena.

TEOREMA 2.2.7. (I. Dolinka, [23]) *Neka je* $\mathbf{S} = (S, \cdot, ^*)$ *involutivna polugrupa tako da za svako* $a \in S$ *postoji jedinstveno* $x \in S$ *za koji važi*

$$aa^*ax = a.$$

Tada $\mathbf{S}$ *zadovoljava sledeće uslove.*

(1) Za sve $a \in S$, *jednačina* $ax = a$ *ima jedinstveno rešenje.*

(2) Svi idempotenti $e \in S$ *su projekcije, tj.* $e^* = e$.

(3) Ako su $e, f \in S$ *idempotenti, onda* $L_e \leq L_f$ *ako i samo ako* $R_e \leq R_f$.

(4) Svake dve različite $\mathcal{L}$*−klase(*$\mathcal{R}$*−klase) od* S *su neuporedive.*

(5) Sve $\mathcal{H}$*-klase od* $\mathbf{S}$ *su grupe.*

(6) Sve $\mathcal{H}$*-klase od* $\mathbf{S}$ *su fiksirane involucijom* *.

(7) $\mathbf{S}$ *ima jedinstven idempotent.*

(8) $(S, \cdot, ^+)$ *je grupa.*

2.3. Regularne *-polugrupe

Involutivna polugrupa $\mathbf{S} = (S, \cdot, ^*)$ se naziva **regularna *-polugrupa** ako zadovoljava

$$xx^*x = x.$$

Klasu (varijetet) regularnih *-polugrupa uveli su T. E. Nordahl i H. E. Scheiblich 1978. godine u radu [84]. Ova klasa, koju označavamo sa $\mathcal{S}^{\text{reg}}$, jeste prirodno uopštenje grupa. Naime, regularna *-polugrupa je grupa ako i samo ako zadovoljava identitet

$$xx^* = yy^*.$$

PRIMER 2.3.1. Neka je X neprazan skup a $Y = X \times X$. Polugrupa $\mathbf{Y} = (Y, \cdot)$ u kojoj važi $(x, y) \cdot (r, s) = (x, s)$ je pravougaona traka. Definišimo $(x, y)^* = (y, x)$. Lako se proverava da je $(Y, \cdot, ^*)$ regularna *-polugrupa. Primetimo da $\mathbf{Y}$ nije inverzna polugrupa.

Potklasa klase regularnih *-polugrupa su i **specijalne regularne involutivne polugrupe** koje zadovoljavaju još i uslov

$$xyy^*x^* = xx^*.$$

Ove polugrupe okarakterisao je N. Reilly u radu [102].

Regularna polugrupa $\mathbf{S}$ je **ortodoksna** ako skup idempoteneta $E = E(\mathbf{S})$ polugrupe $\mathbf{S}$ čini potpolugrupu od $\mathbf{S}$.

TEOREMA 2.3.2. ([84]) *Regularna *-polugupa $\mathbf{S}$ je ortodoksna ako i samo ako $\mathbf{S}$ zadovoljava identitet*

$$[(xx^*)(yy^*)(zz^*)]^2 = [(xx^*)(yy^*)(zz^*)].$$

Polugrupa $\mathbf{S}$ je **uopšteno inverzna** ako je ortodoksna i ako je traka E normalna, tj. važi $eghf = ehgf$ za sve $e, g, h, f \in E$. Strukturu svih uopšteno inverznih polugrupa opisao je M. Yamada [124], pomoću inverznih polugrupa i normalnih traka. U svojoj doktorskoj disertaciji [1], Celia L. Adair je 1979. godine pokazala da je *-regularna polugrupa uopšteno inverzna ako i samo ako zadovoljava identitet

$$a(xx^*)(x^*x)b = a(x^*x)(xx^*)b.$$

2.4. Kompletno regularne *-polugrupe

Mario Petrich je u radu [95] razmatrao regularne *-polugrupe koje se mogu dobiti od kompletno regularnih polugrupa. Kompletno regularne polugrupe se mogu smatrati algebrama sa jednom binarnom asocijativnom operacijom i jednom unarnom operacijom $^{-1}$, u kojima važe zakoni

$$xx^{-1}x = x, \quad xx^{-1} = x^{-1}x, \quad (x^{-1})^{-1} = x.$$

Naime, u kompletno regularnim polugrupama x^{-1} predstavlja inverz od x u maksimalnoj podgrupi kojoj pripada x. Jasno je da ove polugrupe ne moraju biti involutivne. Uzmimo samo dva elementa a, b iz različitih maksimalnih podgrupa. Tada $(ab)^{-1}$ ne mora biti $b^{-1}a^{-1}$.

Međutim, M. Petrich je otkrio da za bilo koji varijetet $\mathcal{V}$ kompletno regularnih polugrupa, klasa svih (kompletno) regularnih *-polugrupa čiji polugrupni redukti (zajedno sa induciranom operacijom inverzije) pripadaju $\mathcal{V}$, čine podvarijetet od $\mathcal{S}^{\mathrm{reg}}$. Ovo sledi iz sledećeg rezultata.

LEMA 2.4.1. *Za svaku kompletno regularnu *-polugrupu* S *i* $x \in S$ *važi*

$$x^{-1} = xx^*x^*x^*x.$$

Drugim rečima, inverzija je u kompletno regularnim *-polugrupama izraziva pomoću *. Prema tome, moguće je ispitivati varijetete kompletno regularnih *-polugrupa.

TEOREMA 2.4.2. (M. Petrich, [95]) *Varijetet kompletno regularnih *-polugrupa je određen unutar* $\mathcal{S}^{\text{reg}}$, *identitetom*

$$xx^* = xxx^*x^*,$$

*dok je varijetet kompletno prostih regularnih *-polugrupa definisan bilo kojim od identiteta*

$$\begin{aligned} xyy^*x^* &= xx^* \\ xyxx^*y^*x^* &= xx^*. \end{aligned}$$

Dalje, Petrich daje jednakosni opis jednog broja varijeteta kompletno regularnih *-polugrupa, sa različitim restrikcijama za grupe koje su u igri, kao i za njihove strukturne veze. Primetimo da se involucija na grupi ne poklapa obavezno sa grupnim inverzom. Lako se pokazuje da se bilo koja grupna involucija * može izraziti kao $x^* = \varphi(x^{-1})$, gde je φ neki automorfizam razmatrane grupe. Ako, međutim, radimo sa regularnom involucijom, inverz je jedina takva involucija na grupi.

Sledeća teorema sumira rezultate rada [95].

TEOREMA 2.4.3. (M. Petrich, [95]) *Sledeća lista daje jednakosnu aksiomatizaciju za nekoliko podvarijeteta varijeteta kompletno regularnih *-polugrupa:*

- *grupe:* $xx^* = yy^*$,
- *Abelove grupe:* $x = yxy^*$,
- *Booleove grupe:* $x = xy^2$,
- *pravougaone grupe:* $xx^* = xyy^*y^*yx^*$,
- *pravougaone Abelove grupe:* $x = xyx^*y^*x$,
- *pravougaone Booleove grupe:* $x = xy^2x^2$,
- *kompletno proste regularne *-polugrupe sa Abelovim podgrupama:* $xx^* = x^2yxx^*x^*y^*x^*$,

- *kompletno proste regularne *-polugrupe sa Booleovim podgrupama:* $x = xyxyx$,
- *polumreže grupa:* $xx^* = x^*x$,
- *polumreže Abelovih grupa:* $xy = yx$,
- *polumreže Booleovih grupa:* $x = x^*$,
- *normalne trake:* $xyx = xyy^*x$,
- *normalne trake grupa:* $xyy^*x = xy^*yx$,
- *normalne trake Abelovih grupa:* $x^2x^*x^*xyxzx = xzxyx$,
- *normalne trake Booleovih grupa:* $x^3yxzx = xzxyx$,
- *ortodoksne normalne trake grupa:* $xyy^*x = x^2x^*y^*yx^*$,
- *ortodoksne normalne trake Abelovih grupa:* $xyzx = xzyx$,
- *ortodoksne normalne trake Booleovih grupa:* $xyx = xy^*x$.

Svi ovi varijeteti čine "kostur" donjih slojeva mreže varijeteta kompletno regularnih *-polugrupa.

2.5. Inverzne polugrupe

Inverzne polugrupe su, posle grupa, najznačajnija i najviše izučavana klasa u teoriji polugrupa. Američki matematičar M. Petrich je 1984. godine napisao knjigu *Inverse Semigroups* od 670 strana. Jasno, inverzne polugrupe, kao i involutivne polugrupe, predstavljaju uopštenje grupa. Takođe, inverzne polugrupe čine pravu potklasu klase svih involutivnih polugrupa.

Istorijski gledano, inverzne polugrupe su se razvijale u dve škole: ruskoj i zapadnoj školi, čiji su predstavnici bili Vagner u Rusiji, i Preston na Zapadu.

Polugrupa **S** se naziva **inverzna** ako za svako $a \in S$ postoji jedinstven inverzni element, tj. element $a^{-1} \in S$ tako da važi

$$aa^{-1}a = a, \quad a^{-1}aa^{-1} = a^{-1}.$$

Lako se pokazuje da za sve $a, b \in S$ važi

$$\begin{aligned} (a^{-1})^{-1} &= a, \\ (ab)^{-1} &= b^{-1}a^{-1}, \end{aligned}$$

tj. da je svaka inverzna polugrupa involutivna polugrupa, pa samim tim i regularna *-polugrupa. Položaj varijeteta inverznih polugrupa unutar klase regularnih *-polugrupa određuje sledeća

TEOREMA 2.5.1. (Schein, [109]) *Varijetet inverznih polugrupa je definisan unutar varijeteta regularnih *-polugrupa identitetom*

$$xx^*x^*x = x^*xxx^*.$$

Označimo sa $\mathcal{J}(X)$ skup svih parcijalnih injektivnih transformacija skupa X ("parciajlnih" znači da transformacija može biti definisana samo na delu skupa X). Važi sledeća teorema reprezentacije za inverzne polugrupe.

TEOREMA 2.5.2. (Vagner, Preston [12, 56]) *Svaka inverzna polugrupa se može potpiti u $\mathcal{J}(X)$ za neki skup X.*

2.6. Involutivne polugrupe i 0-direktne unije

Podsetimo se, za datu polugrupu $\mathrm{S} = (S, \cdot)$ sa S^0 označavamo polugrupu $(S \cup \{0\}, \cdot)$ (pri čemu $0 \notin S$), gde je $x \cdot 0 = 0 \cdot x = 0$ za sve $x \in S$. Kao što je to opisano u prethodnoj glavi, $I_0^*(\mathrm{S})$ je 0-direktna unija polugrupe S sa svojom antiizomorfnom kopijom S^*, pri čemu se involucija posmatra kao fundamentalna operacija.

Označimo aksiome involucije (na polugrupama) sa

$$Inv = \{(xy)^* = y^*x^*, (x^*)^* = x\}.$$

TEOREMA 2.6.1. (Crvenković, Dolinka, Vinčić, [18]) *Neka je Σ skup svih identiteta koji važe na polugrupi $I_0(\mathrm{S})$, polugrupnom reduktu od $I_0^*(\mathrm{S})$ (on predstavlja najveći podskup skupa svih regularnih identiteta koji važe na* S *zatvoren za inverziju). Dalje, neka je E skup koji sa sastoji od sledećih identiteta:*

$$\begin{aligned} xx^*y &= xx^*, \\ xyx^* &= xx^*. \end{aligned}$$

Tada $\Sigma \cup Inv \cup E$ aksiomatizuje jednakosnu teoriju involutivne polugrupe $I_0^*(\mathrm{S})$.

TEOREMA 2.6.2. (Crvenković, Dolinka, Vinčić, [18]) *Neka je* S *polugrupa čiji su identiteti zatvoreni za inverziju (specijalno,* S *može biti redukt involutivne polugrupe). Tada S^0 ima konačnu bazu identiteta ako i samo ako involutivna polugrupa $I_0^*(\mathrm{S})$ ima konačnu bazu identiteta.*

Polugrupa data tablicom

	0	1	a	b	c	d
0	0	0	0	0	0	0
1	0	1	a	b	c	d
a	0	a	a	b	0	0
b	0	b	0	0	a	b
c	0	c	c	d	0	0
d	0	d	0	0	c	d

naziva se **Brandtov monoid** $\mathbf{B}_2^1$. Ona je izomorfna polugrupi koja se dobija dodavanjem jedinice polugrupi prezentiranoj sa

$$\langle x, y \mid x^2 = y^2 = 0,\ xyx = x,\ yxy = y \rangle.$$

Lako se pokazuje da je polugrupa $\mathbf{B}_2^1$ izomorfna multiplikativnoj polugrupi koju čine matrice

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

POSLEDICA 2.6.3. (Crvenković, Dolinka, Vinčić, [18]) *13-toelementna involutivna polugrupa* $\mathbf{I}_0^*(\mathbf{B}_2^1)$ *nema konačnu bazu identiteta.*

2.7. Atomi u mreži varijeteta involutivnih polugrupa

Mreža podvarijeteta varijetata svih involutivnih polugrupa još uvek nije dovoljno ispitana. Ova mreža nema maksimalne elemente, kao što je pokazano u [120], ali je neke donje delove ove mreže opisao I. Dolinka u radovima [29, 25, 26]. Atomi ove mreže su poznati još od 1972. godine. Njih je odredio poljski matematičar S. Fajtlowicz u radu [37].

Uvedimo sledeće oznake:

- $\mathcal{RB} = [xyx = x]$, varijetet pravougaonih involutivnih traka;
- $\mathcal{SL}^{\mathrm{id}} = [xy = yx,\ x^* = x]$, varijetet polumreža sa trivijalnom involucijom;
- $\mathcal{SL}^0 = [xy = yx,\ xx^*y = xx^*]$;
- $\mathcal{C}^{\mathrm{id}} = [xy = zt,\ x^* = x]$, varijetet koji se sastoji od svih konstantnih polugrupa sa trivijalnom involucijom;

- Za svaki prost broj p, varijetet
$$\mathcal{A}_p^{\mathrm{id}} = [xy = yx,\ x^p y = y,\ x^* = x]$$
Abelovih grupa eksponenta p sa trivijalnom involucijom;

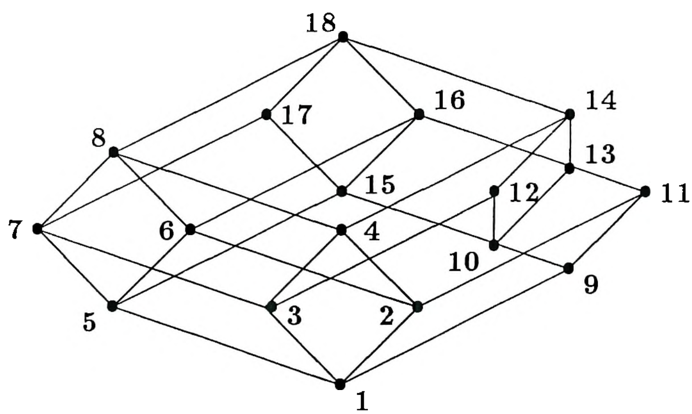
- Za svaki prost broj p, varijetet
$$\mathcal{A}_p = [xy = yx,\ x^p y = y,\ x^* = x^{p-1}]$$
Abelovih grupa eksponenta p sa grupnom inverzijom kao involucijom;

- Sa $\mathcal{A}_n$ označavamo varijetet Abelovih grupa eksponenata n, a sa $\mathcal{A}_n^{\mathrm{id}}$ varijetet Abelovih grupa eksponenta n sa trivijalnom involucijom;

- Najzad, sa $\mathcal{A}_n^{r,s}$ označavamo varijetet svih Abelovih grupa eksponenta n sa involucijom koja zadovoljava $(x^*)^r = x^s$, dok je $\mathcal{A}_n^*$ varijetet svih involutivnih Abelovih grupa eksponenta n. Tako, imamo $\mathcal{A}_n^{1,1} = \mathcal{A}_n^{\mathrm{id}}$ i $\mathcal{A}_n^{1,n-1} = \mathcal{A}_n$.

TEOREMA 2.7.1. (Fajtlowicz, [37]) *Minimalni varijeteti involutivnih polugrupa jesu* $\mathcal{RB}^*$, $\mathcal{SL}^{\mathrm{id}}$, $\mathcal{SL}^0$, $\mathcal{C}^{\mathrm{id}}$ *i* $\mathcal{A}_p^{\mathrm{id}}, \mathcal{A}_p$ *za sve proste brojeve* p.

TEOREMA 2.7.2. (Dolinka, [29]) *Mreža varijeteta involutivnih polugrupa generisana negrupnim atomima ima 18 elmenata, i ona je data sledećim dijagramom.*



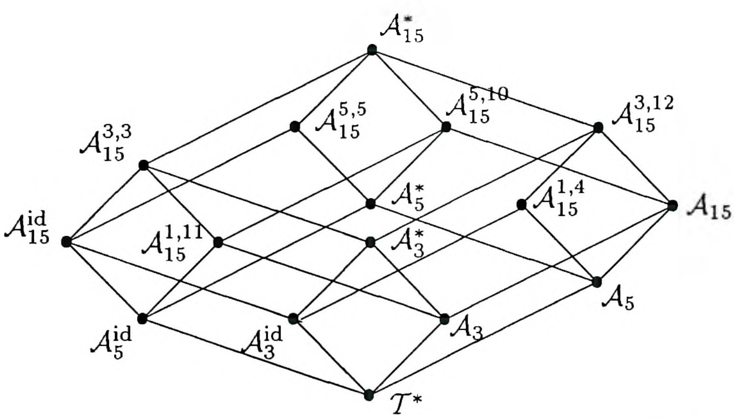
Slika 2.1. Mreža varijeteta involutivnih polugrupa generisana negrupnim atomima

Brojevi 1–18 *na gornjem dijagramu označavaju sledeće varijetete:*

Oznaka	Varijetet (dat preko definišićih idewntiteta)
1	$x = y$
2	$x^2 = x,\ xy = yx,\ x^* = x$
3	$x^2 = x,\ xy = yx,\ xx^*y = xx^*$
4	$x^2 = x,\ xy = yx,\ xx^*y = xx^*y^*$
5	$x^2 = x,\ xyz = xz$
6	$x^2 = x,\ xyzt = xzyt,\ xyz = xy^*z$
7	$x^2 = x,\ xyzt = xzyt,\ xyy^*ut = xzz^*vt$
8	$x^2 = x,\ xyzt = xzyt,\ xyy^*zt = xyzz^*t$
9	$xy = zt,\ x^* = x$
10	$xy = zt$
11	$x^2y = xy = yx,\ x^* = x$
12	$x^2y = xy = yx,\ xx^*y = xx^*$
13	$x^2y = xy = yx,\ xy = xy^*$
14	$x^2y = xy = yx,\ xx^*y = xx^*y^*$
15	$xyz = xz$
16	$x^2y = xy^2 = xy,\ xyzt = xzyt,\ xyz = xy^*z$
17	$x^2y = xy^2 = xy,\ xyzt = xzyt,\ xyy^*ut = xzz^*vt$
18	$x^2y = xy^2 = xy,\ xyzt = xzyt,\ xyy^*zt = xyzz^*t$

TEOREMA 2.7.3. (Dolinka, [29]) *Podmrežu mreže varijeteta involutivnih polugrupa, generisanu involutivno-grupnim atomima $\mathcal{A}_p$ i $\mathcal{A}_p^{\mathrm{id}}$ za sve proste brojeve p, čine sledeći varijeteti: trivijalni varijetet, $\mathcal{A}_m$, $\mathcal{A}_n^{\mathrm{id}}$ i $\mathcal{A}_m \vee \mathcal{A}_n^{\mathrm{id}}$, gde su $m, n \geq 2$ proizvoljni kvadratno slobodni celi brojevi . Štaviše, ta podmreža je izomorfna mreži konačnih podskupova prebrojivo beskonačnog skupa.*

Mreža generisana grupnim atomima $\mathcal{A}_3, \mathcal{A}_3^{\mathrm{id}}, \mathcal{A}_5$ i $\mathcal{A}_5^{\mathrm{id}}$ data je sledećom slikom.



Slika 2.2. Mreža varijeteta involutivnih polugrupa generisana sa $\mathcal{A}_3$, $\mathcal{A}_3^{\mathrm{id}}$, $\mathcal{A}_5$ i $\mathcal{A}_5^{\mathrm{id}}$

2.8. Neki varijeteti involutivnih traka

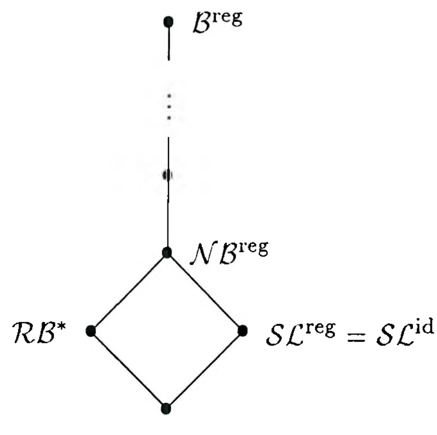
Neka je $\mathcal{V}$ proizvoljni polugrupni varijetet. Uvedimo sledeće oznake:

- $\mathcal{V}^*$ označava varijetet svih involutivnih polugrupa čiji polugrupni redukti leže u $\mathcal{V}$ (tako, $\mathcal{V}^*$ je definisan identitetima za $\mathcal{V}$ i involutivnim aksiomama);
- $\mathcal{V}^{\mathrm{reg}}$ označava podvarijetet od $\mathcal{V}^*$ definisan identitetom $xx^*x = x$, tj. varijetet regularnih *-polugrupa iz $\mathcal{V}^*$;
- $\mathcal{V}^0$ je podvarijetet od $\mathcal{V}^*$ definisan identitetima $xx^*y = xx^* = xyx^*$. Imajući u vidu Teoremu 2.6.1, ako je jednakosna teorija varijeteta $\mathcal{V}$ zatvorena na inverziju identiteta, i ako je $\mathcal{V}$ generisan polugrupom S, tada je $\mathcal{V}^0$ generisan involutivnom polugrupom $I_0^*(\mathrm{S})$.

Primetimo da je, na primer, $\mathcal{SL}^{\mathrm{reg}} = \mathcal{SL}^{\mathrm{id}}$, dok je $\mathcal{RB}^{\mathrm{reg}} = \mathcal{RB}^*$, gde $\mathcal{SL}, \mathcal{RB}$ označavaju redom varijetete polumreža, odnosno pravougaonih traka.

1982, Celia L. Adair je odredila mrežu svih podvarijeteta od $\mathcal{B}^{\mathrm{reg}}$, varijeteta regularnih *-traka.

TEOREMA 2.8.1. (Adair, [2]) *Svi podvarijeteti od $\mathcal{B}^{\mathrm{reg}}$ su iscrpljeni varijetetima oblika $\mathcal{V}^{\mathrm{reg}}$, gde je $\mathcal{V}$ centralni varijetet traka (zatvoren na inverziju identiteta). Stoga je mreža ovih podvarijeteta data sledećim dijagramom.*



Slika 2.3. Mreža svih varijeteta regularnih *-traka

Kasnije, Yamada je odredio kardinalnost konačno generisanih slobodnih algebri varijeteta $\mathcal{B}^{\mathrm{reg}}$. Označimo sa $f_n(\mathcal{B}^{\mathrm{reg}})$ kardinalnost n-generisane slobodine algebre u razmatranom varijetetu (ovaj niz se obično zove *slobodni spektar*). Kao i u slučaju varijeteta traka, slobodni spektar za $\mathcal{B}^{\mathrm{reg}}$ se sastoji od konačnih brojeva. Tačnije imamo sledeći rezultat.

Teorema 2.8.2. (Yamada, [125])

$$f_n(\mathcal{B}^{\mathrm{reg}}) = \sum_{k=1}^{n} \binom{n}{k} 4^{2^k-1} \prod_{i=0}^{k-1} (k-i)^{2^i+1}.$$

Struktura slobodnih regularnih *-traka je izučavana u radu Gerharda i Petricha [43], a srodna problematika je razmatrana i u [42].

Nakon ovih rezultata, logično je da se pažnja usmeri na širu mrežu, mrežu svih varijeteta involutivnih traka. Međutim, ispostavlja se da varijeteti oblika $\mathcal{V}^{\mathrm{reg}}$ i $\mathcal{V}^0$, gde je $\mathcal{V}$ neki (centralni) varijetet traka, imaju naročit značaj i posebnu ulogu.

Lema 2.8.3. (Dolinka, [25]) *Neka je $\mathcal{V}$ centralan, homotipan varijetet traka. Tada je $\mathcal{V}^0$ sadržan u svakom varijetetu involutivnih traka čiji se polugrupni deo jednakosne teorije poklapa sa jednakosnom teorijom od $\mathcal{V}$, osim u $\mathcal{V}^{\mathrm{reg}}$.*

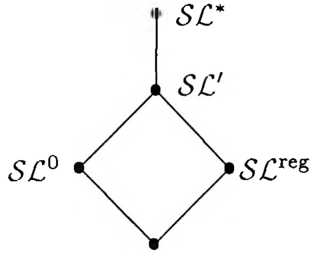
Posledica 2.8.4. *Podvarijeteti od $\mathcal{B}^0$ su tačno varijeteti oblika $\mathcal{V}^0$, gde je $\mathcal{V}$ centralan i homotipan varijetet traka. Stoga je mreža podvarijeteta od $\mathcal{B}^0$ beskonačni (prebrojiv) lanac sa vrhom.*

I. Dolinka je u radu [25] opisao mrežu svih podvarijeteta od $\mathcal{B}^{\mathrm{reg}} \vee \mathcal{B}^0$, ujedinjujući tako rezultat Adair [2] i prethodnu posledicu. On je pokazao da je, unutar $\mathcal{B}^*$, ovaj varijetet definisan identitetima

$$xx^*xyy^*y = xy(xy)^*xy = xx^*xy = xyy^*y.$$

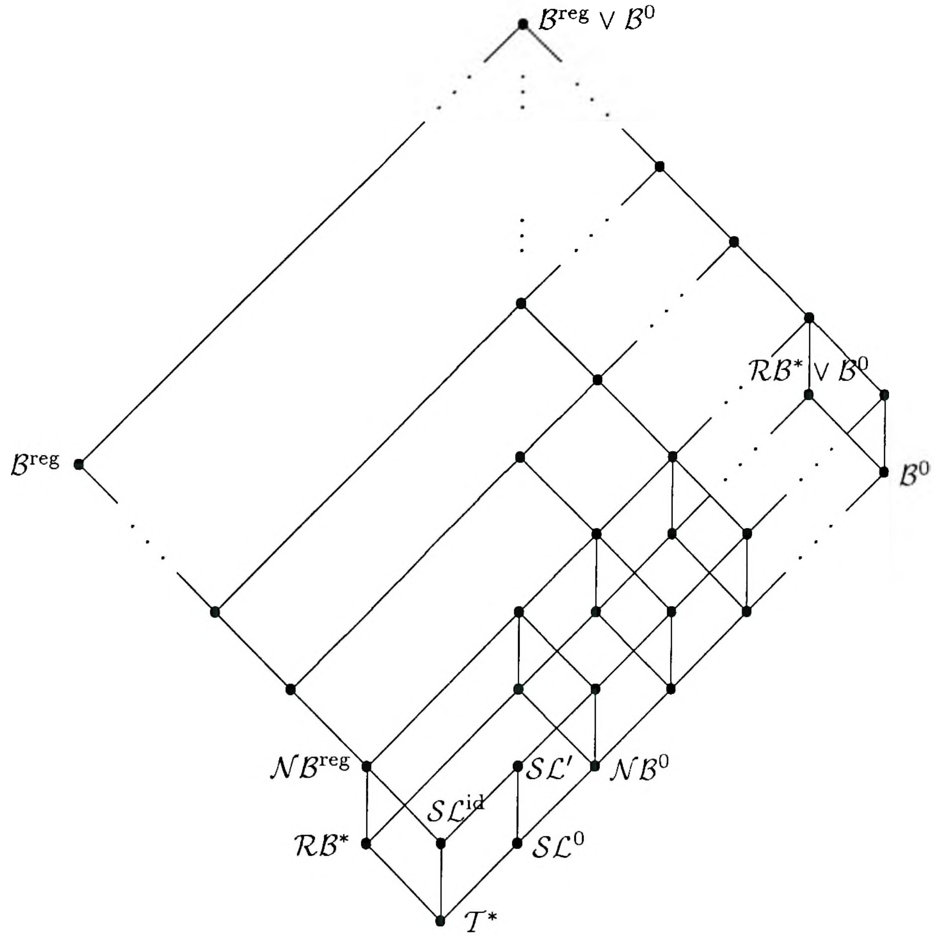
Ali, najpre su određeni svi varijeteti involutivnih polumreža.

Teorema 2.8.5. (Dolinka, [25]) *Postoji tačno četiri netrivijalna varijeteta involutivnih polumreža: $\mathcal{SL}^{\mathrm{reg}}$, $\mathcal{SL}^0$, $\mathcal{SL}' = \mathcal{SL}^{\mathrm{reg}} \vee \mathcal{SL}^0$ (nije teško videti da je on opisan identitetom $xx^*y = xx^*y^*$), i $\mathcal{SL}^*$, pa je tako mreža podvarijeteta od $\mathcal{SL}^*$ data sledećim dijagramom.*



Slika 2.4. Svi varijeteti involutivnih polumreža

TEOREMA 2.8.6. (Dolinka, [25]) *Mreža svih podvarijeteta od* $\mathcal{B}^{\mathrm{reg}} \vee \mathcal{B}^0$ *je data sledećom slikom.*



Slika 2.5. Svi podvarijeteti od $\mathcal{B}^{\mathrm{reg}} \vee \mathcal{B}^0$

Gornja teorema pokazuje kako je struktura mreže podvarijeteta od $\mathcal{B}^*$ daleko komplikovanija od strukture mreže svih varijeteta traka. Na primer, za razliku od potonje mreže, gornja mreža nema konačnu širinu. Takođe, gornja mreža nije modularna, dok je mreža svih varijeteta traka čak distributivna.

Najzad, mrežu svih varijeteta normalnih traka sa involucijom, samo dno mreža podvarijeteta od $\mathcal{B}^*$, odredio je Dolinka u radu [26]. Taj cilj je postignut klasifikacijom svih involutivno-polugrupnih identiteta unutar klase $\mathcal{NB}^*$.

TEOREMA 2.8.7. (Dolinka, [26]) *Za svaki involutivno-polugrupni identitet* $p = q$, *u* $\mathcal{NB}^*$ *važi jedan od sledećih uslova:*

(1) $p = q$ *je trivijalan (u smislu da sledi iz aksioma normalnih traka sa involucijom),*

(2) $p = q \;\Rightarrow\; xy = yx$,

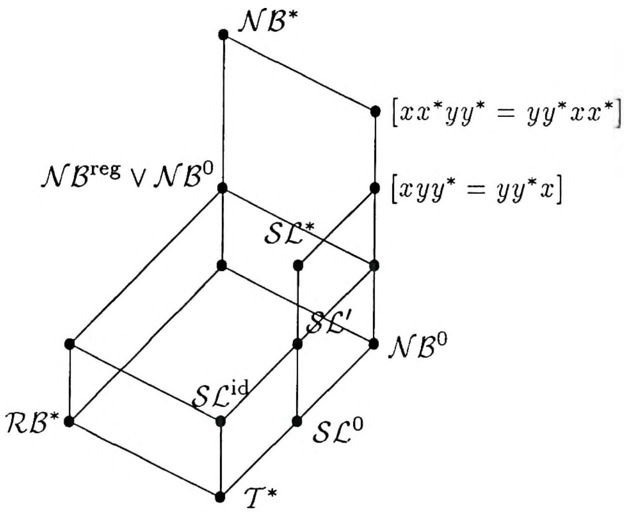
(3) $p = q \;\Rightarrow\; xyy^* = xx^*yy^*$,

(4) $p = q \;\Leftrightarrow\; xyy^* = yy^*x$,

(5) $p = q \;\Leftrightarrow\; xx^*yy^* = yy^*xx^*$.

Kao posledica ove klasifikacije, dobija se

TEOREMA 2.8.8. (Dolinka, [26]) *Mreža svih varijeteta involutivnih normalnih traka je data dijagramom na Slici 2.6.*



Slika 2.6. Svi podvarijeteti od $\mathcal{NB}^*$

2.9. Problemi globalne određenosti

Neka je $\mathbf{A} = (A, F)$ proizvoljna algebra. **Algebra kompleksa** od $\mathbf{A}$ (ili **global** od $\mathbf{A}$) je algebra $\Gamma(\mathbf{A})$, istog tipa kao i $\mathbf{A}$, čiji su elementi neprazni podskupovi od A, dok su njene operacije, za sve $f \in F$, definisane sa

$$f(A_1, \ldots, A_n) = \{f(a_1, \ldots, a_n) \mid a_i \in A_i,\ 1 \le i \le n\},$$

za sve neprazne $A_1, \ldots, A_n \subseteq A$. Jasno, izomorfne algebre indukuju izomorfne globale. Postavlja se pitanje kada je tačan obrat. Stoga kažemo da je klasa istotipnih algebri $\mathcal{K}$ **globalno određena** ako za sve $\mathbf{A}, \mathbf{B} \in \mathcal{K}$ iz $\Gamma(\mathbf{A}) \cong \Gamma(\mathbf{B})$ sledi $\mathbf{A} \cong \mathbf{B}$.

Probleme u vezi sa globalnom određenošću pokrenuli su šezdesetih godina B. M. Schein i T. Tamura. Na primer, Tamura i Shafer [114] su pokazali da su grupe (prsteni) globalno određeni, dok je Kobayashi [63] dokazao da to isto važi i za polumreže. S druge strane, Mogiljanskaja [80] i Važenjin [119] su dali primere parova neizomorfnih polugrupa koje indukuju izomorfne globale.

Primetimo da je za svaku involutivnu polugrupu $\mathbf{S} = (S, \cdot, {}^*)$ njen global $\Gamma(\mathbf{S})$ takođe involutivna polugrupa, pošto važi

$$\begin{aligned} (AB)^* &= \{ab \mid a \in A,\, b \in B\}^* = \{(ab)^* \mid a \in A,\, b \in B\} \\ &= \{b^*a^* \mid a \in A,\, b \in B\} = B^*A^*, \end{aligned}$$

i slično,

$$(A^*)^* = \{(a^*)^* \mid a \in A\} = \{a \mid a \in A\} = A,$$

za sve neprazne $A, B \subseteq S$.

Teorema 2.9.1. (Crvenković, Dolinka, Vinčić, [18]) *Postoje involutivne polugrupe* $\mathbf{A}$ *i* $\mathbf{B}$, *obe sa netrivijalnom involucijom, tako da je* $\Gamma(\mathbf{A}) \cong \Gamma(\mathbf{B})$, *ali* $\mathbf{A} \not\cong \mathbf{B}$.

U preostalom delu ovog paragrafa, prikazaćemo detaljno rezultat iz [121] koji predstavlja originalni doprinos autora disertacije problematici globalne određenosti. Naime, ispostavlja se da je varijetet $\mathcal{B}^{\mathrm{reg}}$ svih regularnih *-traka globalno određena klasa. Dokaz koji sledi je inspirisan radom Y. Kobayashija [63], koji je pokazao da je klasa svih polumreža globalno određena, analizirajući neke osobine parcijalnog uređenja polumreža. Kako se svaka traka može prirodno pretvoriti u parcijalno uređen skup definišući

$$a \leq b \Leftrightarrow ab = ba = a,$$

interesantno je videti do koje mere se metoda Kobayashija može primeniti na neke opštije situacije. Ispostavilo se da regularne *-trake daju mogućnost za uspešnu primenu tih metoda. Podsetimo se, regularna involucija na polumreži je nužno trivijalna, tako da najavljeni rezultat zaista uopštava Kobayashijev.

Za bilo koju involutivnu polugrupu $\mathbf{S}$, sa $Su(\mathbf{S})$ označavamo skup svih involutivnih potpolugrupa od $\mathbf{S}$. Polazimo od sledeće činjenice.

Lema 2.9.2. *Za bilo koju traku* $\mathbf{B}$, $Su(\mathbf{B})$ *se poklapa sa skupom svih projekcija (idempotenata fiksiranih involucijom) od* $\Gamma(\mathbf{B})$. *Prema tome, ako su* $\mathbf{B}_1$, $\mathbf{B}_2$ *involutivne trake, bilo koji izomorfizam* $\varphi : \Gamma(\mathbf{B}_1) \to \Gamma(\mathbf{B}_2)$ *inducira (restrikcijom) bijekciju* $Su(\mathbf{B}_1) \to Su(\mathbf{B}_2)$.

Dokaz. Pre svega, primetimo da za sve $X \subseteq B$ imamo $(X^*)^* = X$, i zbog idempotencije, $X \subseteq X^2$. Prema tome, $X \in Su(\mathbf{B})$ ako i samo ako je $X^2 \subseteq X$ i $X^* \subseteq X$, što je ekvivalentno sa $X = X^2 = X^*$. □

Dalje, izdvajamo jednu posebnu podfamiliju od $Su(\mathbf{B})$:

$$Ch(\mathbf{B}) = \{X \in Su(\mathbf{B}) \,|\, X = Y^2 \Rightarrow X = Y\}.$$

Jasno, kao u prethodnoj lemi, bilo koji izomorfizam $\Gamma(\mathbf{B}_1)$ i $\Gamma(\mathbf{B}_2)$ definiše bijekciju između $Ch(\mathbf{B}_1)$ i $Ch(\mathbf{B}_2)$. Dajemo opis elemenata $Ch(\mathbf{B})$ na sledeći način.

LEMA 2.9.3. *Neka je* $\mathbf{B}$ *regularna* **-traka. Tada* $X \in Ch(\mathbf{B})$ *ako i samo ako je* X *lanac projekcija.*

Dokaz. Uzmimo da $xy \notin \{x, y\}$ za neke $x, y \in X$. Tada $x, y \in X \setminus \{xy\}$ i prema tome, $xy \in (X \setminus \{xy\})^2$. Kako je $X \setminus \{xy\} \subseteq (X \setminus \{xy\})^2$, sledi $(X \setminus \{xy\})^2 = X$, jer je $(X \setminus \{xy\})^2 \subseteq X^2 = X$. Sledi da $X \notin Ch(\mathbf{B})$. Sada za svako $x \in X$ imamo $xx^* \in \{x, x^*\}$, što implicira da je x projekcija. Konačno, s obzirom da $xy \in \{x, y\}$ za sve $x, y \in X$ i x, y su projekcije, xy mora biti projekcija i prema tome, $xy = yx$. Imamo da je X lanac.

Obratno, neka je X lanac projekcija i $X = Y^2$ za neki podskup $Y \subseteq B$. Tada je $Y \subseteq X$, i pošto je svaki podskup lanca njegova potpolugrupa, dobijamo $Y = Y^2 = X$. □

Ranije smo pomenuli relaciju parcijalnog uređenja koja se može definisati za bilo koju traku $\mathbf{B}$. Na analogan način, definišemo parcijalno uređenje na $Su(\mathbf{B})$ kao restrikciju prirodnog uređenja na skupu idempotenata od $\Gamma(\mathbf{B})$:

$$X \leq Y \Leftrightarrow XY = YX = X.$$

Činjenicu da y pokriva x u B (tj. ako je $x < y$ i ne postoji $z \in B$ tako da je $x < z < y$) označavamo sa $x \to y$. Međutim, kada su u pitanju elementi $Su(\mathbf{B})$, koristićemo dve vrste strelica. Ako Y pokriva X u $Su(B)$, onda pišemo $X \Rightarrow Y$. S druge strane, slabije tvrđenje da je $X < Y$ i da nema elemenata $Ch(\mathbf{B})$ između X i Y označavamo sa $X \to Y$.

Sledeći Kobayashijevu terminologiju [63], niz $Y_1, \ldots, Y_n$ elemenata familije $Ch(\mathbf{B})$ nazivamo **izdanak** od X (dužine n) ako

$$X \Rightarrow Y_1 \Rightarrow \ldots \Rightarrow Y_n.$$

Gornji izdanak je **maksimalan** ako se ne može produžiti do izdanka dužine $n+1$. Konačno, četvorka X, Y, Z, T različitih elemenata od $Ch(\mathbf{B})$ naziva se **poklopac** od X ako važe sledeće relacije

$$\begin{array}{ccccc} Y & \Rightarrow & T & \Leftarrow & Z \\ & \nwarrow & & \nearrow & \\ & & X & & \end{array}$$

Glavna teorema iz [63], koja dozvoljava da se dokaže globalna određenost polumreža, je sledeća.

TEOREMA 2.9.4. (Kobayashi, [63]) *Neka je* $\mathbf{S}$ *polumreža i* X *lanac u* $\mathbf{S}$. *Tada je* $|X| = 1$ *ako i samo ako* X *nema poklopce i izdanke duže od* 1.

Naš cilj je da dokažemo analogno tvrđenje za regularne *-trake.

Dobro je poznato (npr. iz [1, 2, 25]) da ako je $\mathbf{\Omega}$ najveća polumrežna slika regularne *-trake $\mathbf{B}$, onda je svaka $\mathcal{D}$-klasa od $\mathbf{B}$ zatvorena za *, odakle sledi da ove klase (koje su inače pravougaone trake) moraju biti kvadrati. Drugim rečma, $\mathbf{B}$ je polumreža involutivnih pravougaonih traka. Neka je $\sigma : \mathbf{B} \to \mathbf{\Omega}$ odgovarajući sirjektivni homomorfizam. Sledeća jednostavna primedba omogućava nam da koristimo Lemu 1 iz [63] za regularne *-trake.

LEMA 2.9.5. *Neka je* $\mathbf{B}$ *regularna* **-traka. Ako su* $X, Y \in Ch(\mathbf{B})$ *takvi da je* $X < Y$ *i* $\sigma(X) \Rightarrow \sigma(Y)$ $(\sigma(X) \to \sigma(Y))$ *važi u* $\Gamma(\mathbf{\Omega})$, *onda* $X \Rightarrow Y$ $(X \to Y)$.

Dokaz. Pretpostavimo da postoji $Z \in Su(\mathbf{B})$ $(Z \in Ch(\mathbf{B}))$ tako da je $X < Z < Y$. Tada, jasno, $\sigma(X) < \sigma(Y) < \sigma(X)$. Lema sada lako sledi iz primedbe da je $\sigma(Z)$ polumreža (podlanac) od $\mathbf{\Omega}$. □

Ovo odmah daje sledeći rezultat.

LEMA 2.9.6. *Neka je* $X \in Ch(\mathbf{B})$, *gde je* $\mathbf{B}$ *regularna* **-traka. Ako* $x \in X$ *nije maksimalan element od* X, *onda* $X \Rightarrow X \setminus \{x\}$.

Dokaz. Pošto je restrikcija σ na dati lanac projekcija (u ovom slučaju X) izomorfizam X i $\sigma(X)$, i pošto po Lemi 1 iz [63] imamo $\sigma(X) < \sigma(X) \setminus \{\sigma(x)\} = \sigma(X \setminus \{\sigma(x)\})$, sledi da je $X < X \setminus \{x\}$. Traženi zaključak sada sledi iz pretodne leme i Leme 1 iz [63]. □

Potrebne su nam još dve leme, koje su analogoni (ali važno je naglasiti, *ne* posledice) Leme 2 i Leme 3 iz [63].

Lema 2.9.7. *Za regularnu* **-traku* $\mathbf{B}$, *neka je* $X \in Ch(\mathbf{B})$ *i pretpostavimo da* X *ima najveći element* x'. *Ako, štaviše, postoji projekcija* $y \in B$ *tako da* $x' \to y$, *onda* $X \to X \cup \{y\}$.

Dokaz. Kako je $X(X \cup \{y\}) = (X \cup \{y\})X = X$, imamo $X < X \cup \{y\}$. Pretpostavimo da je $X \leq Y \leq X \cup \{y\}$ za neko $Y \in Ch(\mathbf{B})$. Tada je $XY = YX = X$ i

$$Y = (X \cup \{y\})Y = XY \cup \{y\}Y = X \cup \{y\},$$

pa je $X \leq Y$. Slično, $Y = X \cup Y\{y\}$. Sada, ako je $X \neq Y$, neka $z \in Y \setminus X$. Onda je $x' < z$, jer bi inače bilo $z = x'z \in XY = X$.

S druge strane, z pripada $\{y\}Y \cap Y\{y\}$, tj. $z = yu = vy$ važi za neke $u, v \in Y$, i prema tome $yz = zy = z$, $z \leq y$. Ali mi imamo da $x' \to y$, pa sledi $y = z$. Prema tome, $Y = X \cup \{y\}$. □

Lema 2.9.8. *Neka je* $\mathbf{B}$ *regularna* **-traka i* $x \in B$ *projekcija. Ako* $\{x\} \to Y$ *za neko* $Y \in Ch(\mathbf{B})$, *onda je* $Y = \{x, y\}$, *gde* $x \to y$.

Dokaz. Pre svega, znamo da je $\{x\}Y = Y\{x\} = \{x\}$. Drugim rečima, za sve $y \in Y$ imamo $xy = yx = x$, tj. $x \leq y$. Prema tome, ako je $Y' = \{x\} \cup Y$, sledi

$$YY' = Y(\{x\} \cup Y) = \{x\} \cup Y = Y',$$

i slično, $YY' = Y$ i $\{x\}Y' = Y'\{x\} = \{x\}$, tj. $\{x\} < Y' \leq Y$, što znači da je $Y = Y'$, odnosno $x \in Y$.

Izaberimo sada $z \in Y \setminus \{x\}$ na proizvoljan način i posmatrajmo lanac projekcija $Z = \{y \in Y \mid y \leq z\}$. Jasno, imamo $\{x\}Z = Z\{x\} = \{x\}$ i $YZ = ZY = Z$, tako da $\{x\} < Z \leq Y$, što implicira $Z = Y$. Ovo pokazuje da Y ima samo dva elementa, $Y = \{x, y\}$. Moramo imati $x \to y$, jer inače, ako je $x < u < y$, imamo $\{x\} < \{x, u\} < Y$, kontradikcija. □

Pređimo sada na glavni deo dokaza globalne određenosti regularnih *-traka.

Propozicija 2.9.9. *Neka je* $X \in Ch(\mathbf{B})$ *za regularnu* **-traku* $\mathbf{B}$ *tako da* $|X| \geq 3$. *Tada* X *ima poklopac.*

Dokaz. Pretpostavimo da X sadrži elemente $x < y < z$. Tada prema Lemi 2.9.6, X ima poklopac

$$\begin{array}{ccccc} X \setminus \{x\} & \Rightarrow & X \setminus \{x, y\} & \Leftarrow & X \setminus \{y\} \\ & \nwarrow & & \nearrow & \\ & & X & & \end{array}$$

(štaviše, obične strelice $\to$ su u stvari $\Rightarrow$), i propozicija je dokazana. □

PROPOZICIJA 2.9.10. *Ako je X involutivni podlanac regularne *-trake* B *sa tačno dva elementa, onda on ima ili maksimalni izdanak dužine* 1, *ili poklopac.*

Dokaz. Neka je $X = \{x, x'\}$ i $x < x'$. Prema Lemi 2.9.6, imamo $X \Rightarrow X \setminus \{x\} = \{x'\}$. Ako bi se ovaj izdanak mogao produžiti, onda Lema 2.9.8 daje projekciju $y \in B$ tako da $x' \to y$ i $\{x'\} \Rightarrow \{x', y\}$. Sada prema Lemi 2.9.7 imamo $X \to X \cup \{y\} = \{x, x', y\}$, i $\{x, x', y\} \Rightarrow \{x', y\}$, prema Lemi 2.9.6. Prema tome, upravo smo konstruisali poklopac

$$\begin{array}{ccc} \{x'\} \Rightarrow \{x', y\} & \Leftarrow & X \cup \{y\} \\ \nwarrow & & \nearrow \\ & X & \end{array}$$

i traženi zaključak sledi. □

Konačno, dajemo dokaz glavnog tvrđenja.

TEOREMA 2.9.11. *Neka je $X \in Ch(\mathrm{B})$, gde je* B *regularna *-traka. Tada je $|X| = 1$ ako i samo ako X nema ni maksimalne izdanke dužine* 1, *ni poklopce.*

Dokaz. ($\Rightarrow$) Pre svega, jasno je da ako $X = \{x\}$ ima izdanak dužine 1, $\{x\} \Rightarrow Y$, onda prema lemi 2.9.8 on mora biti oblika $\{x\} \Rightarrow \{x, y\}$, sa $x \to y$. Očigledno, on može se produžiti, jer prema Lemi 2.9.6, $\{x, y\} \Rightarrow \{y\}$.

Pretpostavimo da $\{x\}$ ima poklopac oblika

$$\begin{array}{ccc} Y \Rightarrow & T & \Leftarrow Z \\ \nwarrow & & \nearrow \\ & \{x\} & \end{array}$$

Tada je $Y = \{x, y\}$ i $Z = \{x, z\}$ (prema Lemi 2.9.8), i imamo $x \to y$, $x \to z$, $y \neq z$, tako da je $yz = zy = x$. Sada se argument sa dna stranice 220 u radu [63] primenjuje doslovno, kako bismo dokazali da važi $Y, Z < \{x, y, z\} < T$, što sprečava postojanje gornjeg poklopca.

($\Leftarrow$) Ovo sledi direktno iz Propozicija 2.9.9 i 2.9.10. □

TEOREMA 2.9.12. *Varijetet svih regularnih *-traka je globalno određen.*

Dokaz. Prema prethodnoj teoremi i primedbama nakon definicije $Ch(\mathbf{B})$, ako su $\mathbf{B}_1$ i $\mathbf{B}_2$ regularne *-trake, onda bilo koji izomorfizam $\phi : \Gamma(\mathbf{B}_1) \to$

$\Gamma(\mathbf{B}_2)$ definiše bijekciju među jednoelementnim podskupovima od B_1 i B_2 koji sadrže projekcije. Primetmo da je u bilo kojoj regularnoj *-traci svaki element x proizvod dve projekcije, naime xx^* i x^*x, s obzirom da je $(xx^*)(x^*x) = xx^*x = x$. Prema tome, ako $x \in B_1$, onda je $x = pq$ za neke projekcije $p, q \in B_1$, i

$$\phi(\{x\}) = \phi(\{pq\}) = \phi(\{p\}\{q\}) = \phi(\{p\})\phi(\{q\}) = \{p'\}\{q'\} = \{p'q'\},$$

što implicira da ϕ definiše injekciju familije jednoelementnih podskupova od B_1 u odgovarajuću familiju jednoelementnih podskupova od B_2. Naravno, ovaj zaključak važi i za inverzno preslikavanje ϕ^{-1}, tako da su jednoelementni podskupovi od B_1 i B_2 u bijektivnoj korespodenciji indukovanoj sa ϕ. Sada se direktno može proveriti da je preslikavanje $\psi : B_1 \to B_2$ definisano sa

$$\psi(x) = x' \quad \text{ako i samo ako} \quad \phi(\{x\}) = \{x'\}$$

izomorfizam. Prema tome, $\mathbf{B}_1 \cong \mathbf{B}_2$. □

2.10. Baerove *-polugrupe

Neka je S involutivna polugrupa. Skup svih projekcija od S označavamo sa $Pr(\mathrm{S})$. Definišimo uređenje u $Pr(\mathrm{S})$ sa $e \leq f$ ako i samo ako je $ef = e$ (ili ekvivalentno $fe = e$). Lako se uveravamo da je $Pr(\mathrm{S})$ parcijalno uređen skup. Ako S ima 0, onda je 0 najmanji element od $Pr(\mathrm{S})$, i ako S ima jedinicu 1, onda je 1 najveći element $Pr(\mathrm{S})$.

LEMA 2.10.1. ([74]) *Neka su e i f projekcije u involutivnoj polugrupi* S. *Tada je $eS \subseteq fS$ ako i samo ako je $e \leq f$.*

Dokaz. Ako je $e \leq f$, onda pošto je $e = fe$, imamo $eS \subseteq fS$. Obratno, ako je $eS \subseteq fS$, onda pošto je $e = ee \in eS \subseteq fS$, postoji $x \in S$ tako da je $e = fx$. Prema tome,

$$fe = ffx = fx = e,$$

što se i tražilo. □

Involutivna polugrupa S sa 0 se zove **Baerova *-polugrupa** ako za svaki element $a \in S$ postoji projekcija $e \in S$ tako da je

$$\{x \in S \mid ax = 0\} = eS.$$

Iz prethodne leme sledi da je e jedinstveno određeno sa a. Takvo e označavamo sa a'.

LEMA 2.10.2. ([74]) *Svaka Baerova *-polugrupa* S *ima dvostranu jedinicu* 1 *i važi da je* $0' = 1$ *i* $1' = 0$.

Dokaz. Kako je $0'S = \{x \in S \mid 0x = x\} = S$, imamo da za svako $s \in S$ postoji $t \in S$ tako da važi $0't = s$, odnosno $0'0't = 0's$ tj. $0's = s$. Dalje, imamo $s0' = (0's^*)^* = (s^*)^* = s$. Sladi da je $0'$ jedinica polugrupe S. Takođe, važi $1' = 0$ jer je $1'S = \{x \in S \mid 1x = 0\} = \{0\}$. □

LEMA 2.10.3. ([74]) *Neka su a i b elementi Baerove *-polugrupe* S *i neka su e i f projekcije iz* S. *Tada važi*

(1) $aa' = 0$ *i* $a'a^* = 0$;

(2) $ae = 0 \Rightarrow e \leq a'$;

(3) $a' \leq (ba)'$;

(4) $e \leq f \Rightarrow f' \leq e'$;

(5) $a = aa''$ *i* $e \leq e''$;

(6) $a' = a'''$;

(7) $ab = 0$ *ako i samo ako* $a''b = 0$;

(8) $ea = ae \Rightarrow e'a = ae'$.

Dokaz. (1) $aa' = 0$, jer $a' \in a'S$ i $a'a^* = (aa')^* = 0$.

(2) Ako je $ae = 0$, onda $e \in a'S$ pa je $a'e = e$ tj. $e \leq a'$.

(3) $baa' = 0$ po (1), pa je $a' \leq (ba)'$ po (2).

(4) Ako je $e \leq f$, onda je po (3) $f' \leq (ef') = e'$.

(5) Kako je $a'a^* = 0$ po (1), imamo da $a^* \in a''S$. Prema tome, $aa'' = (a''a^*)^* = (a^*)^* = a$. Specijalno, $ee'' = e$, pa sledi $e \leq e''$.

(6) $a' \leq a'''$ prema (5). S druge strane, pošto $a''x = 0$ implicira $ax = aa''x = 0$ prema (5), imamo da je $a'''S \subseteq a'S$, što daje $a''' \leq a'$.

(7) Prema (6), imamo $\{x \in S \mid ax = 0\} = a'S = a'''S = \{x \in S \mid a'''x = 0\}$.

(8) Ako je $ea = ae$, onda pošto je $eae' = aee' = 0$ prema (1), imamo da $ae' \in e'S$. Sledi da važi $e'ae' = ae'$. Kako je $ea^* = (ae)^* = (ea)^* = a^*e$, slično pokazujemo da važi $e'a^*e' = a^*e'$, tj. $e'ae' = ae'$. Prema tome, $ae' = e'a$. □

Neka je S Baerova *-polugrupa. Projekcija $e \in S$ je **zatvorena** ako je $e = e''$. Prema (6) iz prethodne leme, projekcija e je zatvorena ako i samo ako je $e = a'$ za neko $a \in S$. Skup svih zatvorenih projekcija označavamo sa $Pr'(\mathrm{S})$. Skup $Pr'(\mathrm{S})$ ima parcijalno uređenje indukovano onim iz $Pr(\mathrm{S})$.

LEMA 2.10.4. ([74]) *Neka su e i f projekcije Baerove *-polugrupe* S. *Ako je $ef = fe$, onda je $ef = e \wedge f =$ infimum$\{e, f\}$ u $Pr(\mathrm{S})$. Ako su e i f zatvorene, onda je ef zatvorena i $ef = e \wedge f$ u $Pr'(\mathrm{S})$.*

Dokaz. Očigledno je da je ef projekcija i $ef \leq e$, $ef \leq f$. Ako je g projekcija iz S tako da $g \leq e$ i $g \leq f$, onda imamo $g = eg = efg$, tj. $g \leq ef$. Sledi $ef = e \wedge f$, u $Pr(\mathrm{S})$.

Ako su e i f zatvorene, onda prema (3) i (4) iz prethodne leme imamo $(ef)'' = (fe)'' \leq e'' = e$. Naime, $ef \leq e$ pa je, na osnovu (4), $e' \leq (ef)'$ tj. $(ef)'' \leq e''$. Takođe, $(ef)'' \leq f'' = f$, pa je $(ef)'' \leq ef$. S obzirom da prema (5) važi $ef \leq (ef)''$, projekcija ef je zatvorena i prema tome, $ef = e \wedge f$ u $Pr(\mathrm{S})$. □

TEOREMA 2.10.5. ([74]) *Neka je* S *Baerova *-polugrupa. Skup $Pr'(\mathrm{S})$, zatvorenih projekcija od* S *čini ortomodularnu mrežu sa ortokomlpementiranjem $e \to e'$, i u $Pr'(\mathrm{S})$ važi*

$$e \wedge f = e(f'e)' = (f'e)'e.$$

Dokaz. Neka je $e, f \in Pr'(\mathrm{S})$ i označimo $a = f'e$. Pokazaćemo da $e \wedge f$ postoji u $Pr'(\mathrm{S})$, i da važe gornji uslovi. Imamo da je $e' \leq a'$, prema (3), i e' komutitra sa a'. Kako $e = e''$ komutira sa a' prema (8), imamo da je $ea' = e \wedge a'$ u $Pr'(\mathrm{S})$, prema prethodnoj lemi. Štaviše, s obzirom da je $fea' = aa'x$, imamo $ea' \leq f'' = f'$ prema (2). Sledi da je ea' donja granica za $\{e, f\}$. Ako je $g \in Pr'(\mathrm{S})$ donja granica za $\{e, f\}$, onda je $ag = f'eg = f'g = f'fg = 0$, pa je $g \leq a'$. Prema tome, $g \leq e \wedge a' = ea'$. Sledi $ea' = e \wedge f$ u $Pr'(\mathrm{S})$.

Preslikavanje $e \to e'$ je involutivni dualni automorfizam u $Pr'(\mathrm{S})$, tj. važi $(e' \wedge f')' = e \vee f$. Prema tome, $Pr'(\mathrm{S})$ čini mrežu. Štaviše, $e \wedge e' = 0$ za svako $e \in Pr'(\mathrm{S})$, pošto $ee' = e'e = 0$. Sledi da je $e \to e'$ ortokomplementiranje u $Pr'(\mathrm{S})$.

S obzirom da je $e' \wedge f' = e'(fe')' = e' \wedge (fe')'$, za sve $e, f \in Pr'(\mathrm{S})$ prema prethodnom imamo

$$e \vee f = e \vee (fe')''.$$

Ako je $e \leq f$, onda s obzirom da f komutira sa e' prema (8), imamo $(fe')'' = fe' = f \wedge e'$. Prema prethodnom je

$$f = e \vee f = e \vee (f \wedge e').$$

Sledi da je $Pr'(\mathrm{S})$ ortomodularna mreža. □

D. J. Foulis je 1960. godine u radu [39] pokazao da je svaka ortomodularna mreža izomorfna mreži zatvorenih projekcija neke Baerove *-polugrupe.

PRIMER 2.10.6. Involutivna polugrupa svih binarnih relacija na nepraznom skupu X, $\mathbf{B}(X) = (\mathcal{P}(X \times X), \circ, ^{-1})$ je primer Baerove *-polugrupe. Neka je, na primer, $\rho = A \times B \subseteq X \times X$. Tada je

$$\{\sigma \subseteq X \times X \mid \rho \circ \sigma = \emptyset\} = \Delta_{\bar{B}}(\mathbf{B}(X)),$$

što se lako proverava.

Posledica ovog je činjenica da svaka polugrupa može biti izomorfna potpolugrupi polugrupnog redukta Baerove *-polugrupe.

Pogledajmo još jednu konstrukciju Baerove *-polugrupe koja se dobija iz proizvoljne polugrupe $\mathbf{S}$. Definišimo skup Q na sledeći način.

$$Q = S \cup S^* \cup \{e, f, 0, 1\},$$

gde je $\mathbf{S}^*$ antiizomorfna kopija od $\mathbf{S}$, e je spoljna jedinica za S^*, a f spoljna jedinica za $\mathbf{S}$. Neka su 0 i 1 redom spoljna nula i spoljna jedinica za Q. Neka je, dalje, $ea = ae = 0$ za sve $a \in S$, $fa^* = a^*f = 0$ za sve $a^* \in S^*$, i

$$e^* = e = ee, \quad f^* = f = ff, \quad ef = fe = 0.$$

Jasno, $0^* = 0$ i $1^* = 1$. Posmatrajmo skupove

$$A_0 = \{x \in Q \mid 0x = 0\} = 1Q,$$

$$A_1 = \{x \in Q \mid 1x = 0\} = \{0\} = 0Q,$$

za svako $a^* \in S^*$,

$$A_{a^*} = \{x \in Q \mid a^*x = 0\} = S \cup \{f, 0\} = fQ,$$

za svako $a \in S$,

$$A_a = \{x \in Q \mid ax = 0\} = S^* \cup \{e, 0\} = eQ,$$

i najzad,

$$A_e = \{x \in Q \mid ex = 0\} = S \cup \{f, 0\} = fQ,$$

$$A_f = \{x \in Q \mid fx = 0\} = S^* \cup \{e, 0\} = eQ.$$

Na osnovu date konstrukcije sledi da je $\mathbf{Q} = (Q, \cdot, ^*)$ Baerova *-polugrupa i $\mathbf{S}$ je potpolugrupa polugrupe $(Q, \cdot)$.

3.1. Varijeteti involutivnih poluprstena

Podsetimo se, *poluprsten sa involucijom* je algebra $\mathbf{A} = (A, +, \cdot, ^*)$ takva da je $(A, +, \cdot)$ poluprsten i sledeći identiteti važe na $\mathbf{A}$:

$$\begin{aligned} (x+y)^* &= x^* + y^*, \\ (xy)^* &= y^* x^*, \\ (x^*)^* &= x. \end{aligned}$$

Tipičan primer poluprstena je $(\mathbb{N}, +, \cdot)$ gde je $\mathbb{N} = \{0, 1, 2, \ldots\}$. Veoma važan poluprsten u teoriji formalnih jezika je Booleov poluprsten $\mathbf{B}_2 = (\{0,1\}, +, \cdot)$ gde je $1+1 = 1 \cdot 1 = 1$. Jasno, svi prsteni se mogu posmatrati kao poluprsteni, npr. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Neka je $\mathbb{N}^\infty = \mathbb{N} \cup \{\infty\}$. Tada je $(\mathbb{N}^\infty, +, \min)$ poluprsten, i on se u literaturi naziva **tropski poluprsten**. Osim toga, još neki poluprsteni brojeva (prirodni, celi) prošireni beskonačnim elementom (sa raznim operacijama) se zovu tropski poluprsteni, i oni igraju važnu ulogu u najnovijim istraživanjima u algebarskoj teoriji automata, dok su prvi put korišćeni u operacionim istraživanjima i teoriji optimizacije.

Svi gore navedeni primeri su komutativni, pa samim tim i involutivni poluprsteni sa identičkom involucijom.

Primer nekomutativnog poluprstena je poluprsten binarnih relacija

$$(\mathcal{P}(X \times X), \cup, \circ, \emptyset, \Delta_X),$$

gde su $\emptyset$ i Δ_X nula i jedinica ovog poluprstena. Naravno, algebra

$$(\mathcal{P}(X \times X), \cup, \circ, ^{-1}, \emptyset, \Delta_X),$$

gde je $\rho^{-1} = \{(a,b) \in X \times X \mid (b,a) \in \rho\}$, je involutivni poluprsten. Od naročitog je interesa proširiti skup operacija ovih algebri operacijom refleksivno-tranzitivnog zatvorenja relacija. Na taj način se dobijaju RTC-poluprsteni, odnosno involutivni RTC-poluprsteni binarnih relacija. Kao što smo ranije već pomenuli, ovakve strukture imaju svoj poseban naziv u literaturi. Naime, u teorijskom računarstvu i algebarskoj logici [58] je uobičajeno da algebru

$$\mathbf{Rel}(X) = (\mathcal{P}(X \times X), \cup, \circ, ^{rtc}, \emptyset, \Delta_X),$$

zovemo **puna Kleenejeva algebra binarnih relacija na skupu** X. Sve podalgebre punih Kleenejevih algebri nazivamo **standardne** ili **reprezentabilne Kleenejeve algebre**. Ukoliko razmatramo i inverz relacija kao osnovnu operaciju, koristimo istu terminologuju sa razlikom da umesto Kleenejevih algebri govorimo o involutivnim Kleenejevim algebrama, dok odgovarajuće pune involutivne Kleenejeve algebre binarnih relacija označavamo sa $\mathbf{Rel}^{-1}(X)$. Najzad, **Kleenejeve algebre (sa inverzijom)** su članovi varijeteta generisanog svim algebrama oblika $\mathbf{Rel}(X)$ $(\mathbf{Rel}^{-1}(X))$. Taj varijetet označavamo sa $\mathcal{KA}$ (odnosno $\mathcal{KA}^{-1}$).

Varijeteti poluprstena (sa involucijom) i njihove mreže su predmet savremenih algebarskih istraživanja. Za poluprstene, atome u mreži podvarijeteta odredioje S. V. Polin 1980. godine [100], dok je atome u mreži involutivnih poluprstena odredio I. Dolinka 2000. godine u radu [27].

Podsetimo se Polinovog rezultata, koji daje listu svih minimalnih varijeteta poluprstena. Definišimo prvo nekoliko binarnih i unarnih operacija na izvesnim konačnim skupovima.

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

$\circ$	0	1
0	0	0
1	0	0

$*_\ell$	0	1
0	0	0
1	1	1

$*_r$	0	1
0	0	1
1	0	1

$\wedge_3$	0	1	2
0	0	0	0
1	0	1	0
2	0	0	2

$\circ_3$	0	1	2
0	0	0	0
1	0	0	0
2	0	0	0

$\diamond$	0	1	2	3
0	0	1	2	3
1	1	1	3	3
2	2	3	2	3
3	3	3	3	3

$\square$	0	1	2	3
0	0	1	0	1
1	0	1	0	1
2	2	3	2	3
3	2	3	2	3

a	0	1	2
$\bar{a}$	0	2	1

a	0	1	2	3
$\bar{a}$	0	2	1	3

Teorema 3.1.1. (Polin, [100]) *Varijetet poluprstena je minimalan ako i samo ako je generisan jednim od sledećih poluprstena:*

(1) $(\{0,1\},\circ,\wedge)$, $(\{0,1\},\circ,\circ)$, $(\{0,1\},\vee,\vee)$, $(\{0,1\},\vee,\wedge)$, $(\{0,1\},\vee,\circ)$, $(\{0,1\},\wedge,\circ)$,

(2) $(\{0,1\},\vee,*_\ell)$, $(\{0,1\},\vee,*_r)$,

(3) $\mathbb{Z}_p = (\{0,1,\ldots,p-1\},+_p,\cdot_p$, *gde je* p *prost broj, a* $+_p$ *i* $\cdot_p$ *su respektivno sabiranje i množenje po modulu* p.

(4) $\mathbb{N}_p = (\{0,1,\ldots,p-1\},+_p,\circ_p)$, *gde je* p *prost broj, a* $\circ_p$ *je nula množenje u skupu* $\{0,1,\ldots,p-1\}$.

Varijeteti involutivnih poluprstena sa trivijalnom involucijom su upravo komutativni varijeteti. Ovo važi i za minimalne varijetete, pa (1), (3) i (4) iz poslednje teoreme daju tačno minimalni varijetete poluprstena sa identičkom involucijom. Stoga, ako razmatramo involutivne poluprstene i njihove minimalne varijetete, možemo se ograničiti na one sa netrivijalnom involucijom, tj. na nekomutativne poluprstene. Tako, sledeća lema nam pruža važna ograničenja u potrazi za takvim varijetetima.

LEMA 3.1.2. ([27]) *Neka involutivni poluprsten* $\mathbf{A}$ *generiše minimalni varijetet* $\mathcal{V}$. *Pretpostavimo da* $\mathbf{A}$ *ima element fiksiran involucijom koji nije ni aditivno ni multiplikativno idempotentan. Tada se* $\mathcal{V}$ *sastoji od komutativnih poluprstena sa trivijalnom involucijom.*

Dokaz. Pretpostavimo da postoji $a \in A$ tako da je $a^* = a$ i tako da važi $a + a \neq a$ i $aa \neq a$. Zbog ovih različitosti, involutivni poluprsten $\mathbf{B} \leq \mathbf{A}$ generisan sa a je netrivijalan, pa $\mathbf{B}$ mora generisati isti varijetet kao $\mathbf{A}$. Lako se pokazuje da $a^* = a$ implicira da je involucija na $\mathbf{B}$ trivijalna. Prema tome, imamo monogeni poluprsten snabdeven identičkim preslikavanjem kao involucijom, koji očigledno mora biti komutativan. □

Zbog prethodne leme, možemo pretpostaviti da je bilo koja fiksna tačka involucije u involutivnim poluprstenima koji generišu minimalni varijetet istovremeno aditivno i multiplikativno idempotentan (primetimo da svaki involutivni prsten ima elemente fiksirane involucijom, npr. $a+a^*$ i aa^*). Poluprsten (sa involucijom) je **aditivno idempotentan** ako zadovoljava identitet

$$x + x = x.$$

LEMA 3.1.3. ([27]) *Neka je* $\mathbf{A}$ *poluprsten sa involucijom koji nije aditivno idempotentan i koji pripada minimalnom varijetetu. Tada* $\mathbf{A}$ *ima samo jednu fiksnu tačku involucije* e *koji je multiplikativna nula, i koji je u isto vreme ili aditivna jedinica ili aditivna nula u* $\mathbf{A}$.

Dokaz. Pre svega, primetimo da je $B = \{a \in A \mid a + a = a\}$ nosač podalgebre $\mathbf{B} \leq \mathbf{A}$, koja zadovoljava identitet $x + x = x$. Po pretpostavci leme, $\mathbf{B}$ mora biti prava podalgebra od $\mathbf{A}$, i kao takva generiše netrivijalan podvarijetet varijeteta kome pripada $\mathbf{A}$. Kako $\mathbf{A}$ pripada minimalnom varijetetu, sledi da $\mathbf{B}$ sadrži samo jedan element. Jasno, ovo je jedinstvena fiksna tačka involucije u $\mathbf{A}$ (jer smo pretpostavili da su svi elementi fiksirani involucijom idempotentni). Dalje, za svako $a \in A$ imamo $ea + ea = (e + e)a = ea$, pa je $ea \in B = \{e\}$. Sledi da je $ea = e$ (slično $ae = e$), tj. e je multiplikativna nula od $\mathbf{A}$. Posmatrajmo preslikavanje $\psi : A \to A$ dato sa $\psi(a) = e + a$. Ovo je očigledno idempotentni endomorfizam od $\mathbf{A}$. Prema tome, imamo da je $\psi(A) = e + A = \{e\}$ (tako da je e aditivna nula), ili pak podalgebra $\mathbf{A}$ čiji nosač je $e + A$ generiše tačno isti varijetet kao $\mathbf{A}$. Kako za svako $x \in e + A$ imamo $e+x = x$, zbog jedinstvenosti fiksne tačke involucije e imamo $x+x^* = e$, pa sledi $x + x^* + x = x$. Ovaj identitet mora važiti na celom poluprstenu $\mathbf{A}$, što znači da je tada e aditivna jedinica. □

Dalje, u [27] je pokazano da ukoliko je element e iz prethodne leme aditivna jedinica u involutivnom poluprstenu $\mathbf{A}$ koji generiše minimalni varijetet, tada zbog $x + x^* = e$ dobijamo da je $\mathbf{A}$ zapravo prsten (sa aditivnim inverzom a^*). Štaviše, tada za sve $a \in A$ važi

$$e = ae = a(a + a^*) = a^2 + e = a^2,$$

pa prema poznatom opisu svih minimalnih varijeteta prstena (koji je dao A. Tarski), sledi da se razmatrani varijetet poklapa sa onim koji je generisan nula-prstenom $\mathbf{N}_p$ (za $p \geq 3$, pošto razmatramo samo nekomutativni slučaj).

S druge strane, ako je pomenuti element e aditivna nula, nakon dužih razmatranja i prilagođavanja nekih Polinovih pomoćnih rezultata involutivnom "ambijentu", dobija se da uočeni minimalni varijetet mora biti jedinstven, i on je generisan troelementnim involutivnim poluprstenom $(\{0, 1, 2\}, \circ_3, \wedge_3, ^-)$.

Tako, preostaju aditivno idempotentni poluprsteni sa involucijom. U [27] se sada razmatraju dva slučaja. Ako je minimalni varijetet generisan involutivnim poluprstenom $\mathbf{A}$ koji ima jedinstvenu fiksnu tačku involucije, on mora biti jedan od varijeteta koji su redom generisani algebrama $(\{0, 1, 2\}, \wedge_3, \circ_3, ^-)$, $(\{0, 1, 2\}, \wedge_3, \wedge_3, ^-)$. S druge strane, ako $\mathbf{A}$ ima bar dva elementa fiskirana involucijom, onda $\mathbf{A}$ sadrži podalgebru izomorfnu sa $(\{0, 1, 2, 3\}, \diamond, \square, ^-)$. Na kraju se, dakle, dobija sledeće tvrđenje.

TEOREMA 3.1.4. (Dolinka, [27]) *Varijetet poluprstena sa netrivijalnom involucijom je minimalan ako i samo ako je generisan jednim od sledećih involutivnih poluprstena:*

(1) $(\{0,1,2\},\wedge_3,\wedge_3,\bar{\ })$, $(\{0,1,2\},\wedge_3,\circ_3,\bar{\ })$, $(\{0,1,2\},\circ_3,\wedge_3,\bar{\ })$,

(2) $(\{0,1,2\},\diamond,\square,\bar{\ })$,

(3) $(\{0,1,\ldots,p-1\},+_p,\circ_p,-_p)$, *gde je* $-_p$ *operacija aditivnog inverza po modulu prostog broja* $p\geq 3$.

3.2. Idempotentni distributivni involutivni poluprsteni

Poluprsten $(S,+,\cdot)$ je **idempotentan** ako su obe njegove operacije idempotentne. Očigledno, uslov idempotencije daje da je $(S,+)$ polumreža. Kažemo da je poluprsten **distributivan** ako je $+$ distributivan u odnosu na $\cdot$, tj. važi zakon dualne distributivnosti:

$$x+yz=(x+y)(x+z).$$

Idempotentni i distributivni poluprsteni se kraće zovu **ID-poluprsteni**. ID-poluprsteni čiji su aditivni redukti polumreže (budući da se kod nekih autora komutativnost sabiranja ne uzima kao aksioma) su razmatrani od strane F. J. Pastijna i A. Romanovske u radu [88] i A. Romanovske u radovima [103, 104].

Ispitivanje ID-poluprstena počelo je u kasnim šezdesetim godinama [60, 96] sa ispitivanjem distributivnih bipolumreža (pod *bipolumrežom* podrazumevamo komutativni idempotentni poluprsten). Međutim, pravi ID-poluprsteni počinju ozbiljnije da se ispituju tek početkom osamdesetih u pomenutim radovima F. J. Pastijna i A. Romanovske [86, 88, 103, 104]. Posebno, mreža svih varijeteta ID-poluprstena je data u [104]. Reč je o četvorodimenzionalnoj kocki. Nedavno su M. Kuřil i L. Polák u radu [70] našli način da opišu sve varijetete idempotentnih poluprstena (bez zahteva za distributivnošću $+$ nad $\cdot$). F. J. Pastijn i Y. Q. Guo su u radu [87] opisali mrežu svih ID-poluprstena pod uslovom da $+$ nije komutativna operacija. Ova mreža je prebrojivo beskonačna i distributivna (videti takođe i [89]).

Sa stanovišta teorije varijeteta, istraživanja vezana za poluprstene sa involucijom su tek u povoju, i praktično prve razultate (prezentirane u prethodnom paragrafu) je dobio Dolinka [27]. Ovde kratko prikazujemo rezultate njegovog rada [31], gde je opisana mreža svih varijeteta ID-poluprstena sa involucijom. Ispostavilo se da postoji tačno 64 takva varijeteta.

U radu [88] je dokazano da je u bilo kom ID-poluprstenu $(S,+,\cdot)$ (sa komutativnim sabiranjem), redukt $(S,\cdot)$ normalna traka ($x^2=x$, $xyzu=xzyu$). Sledeći rezultat daje strukturu ID-poluprstena sa involucijom kao involutivne Płonkine sume specijalnih poluprstena.

TEOREMA 3.2.1. ([31, 32]) *Svaki ID-poluprsten sa involucijom je predstavljiv kao involutivna Płonkina suma involutivno-polumrežno uređenog sistema ID-poluprstena koji zadovoljavaju identitet $x + xyx = x$. Obratno, involutivna Płonkina suma svakog takvog sistema je ID-poluprsten sa involucijom.*

U radu [104], A. Romanovska je dokazala da je svaki ID-poluprsten koji zadovoljava identitet $x + xyx = x$ suma distributivno-mrežno uređenog **m-sistema** pravougaonih ID-poluprstena (tj. poluprstena sa pravougaonim multiplikativnim reduktom). To znači da imamo sistem disjunktnih poluprstena $\mathbf{S}_i$ indeksiranih distributivnom mrežom $(D, \vee, \wedge)$ (tako da $i \in D$), i za svako $i, j \in D$ takve da je $i \geq j$, potapanje

$$\psi_{i,j} : S_i \to S_j$$

takvo da važi

(i) $\psi_{i,i}$ je identičko preslikavanje na S_i za sve $i \in D$,

(ii) $\psi_{i,j} \circ \psi_{j,k} = \psi_{i,k}$ za sve $i, j, k \in D$ takve da je $i \geq j \geq k$,

(iii) $\psi_{i,i\wedge j}(S_i) + \psi_{j,i\wedge j}(S_j) \subseteq \psi_{i\vee j,i\wedge j}(S_{i\vee j})$.

Suma ovog sistema definisana je tako da su operacije u rezultujućem poluprstenu $(S, +, \cdot)$ (gde je $S = \bigcup_{i\in D} S_i$) date sa

$$\begin{aligned} a_i b_j &= \psi_{i,i\wedge j}(a_i)\psi_{j,i\wedge j}(b_j), \\ a_i + b_j &= \psi_{i\vee j}^{-1}(\psi_{i,i\wedge j}(a_i) + \psi_{j,i\wedge j}(b_j)), \end{aligned}$$

gde je $a_i \in S_i$, $b_j \in S_j$.

Familiju poluprstena $\mathbf{S}_i$ indeksiranu distributivnom mrežom sa involucijom $(D, \wedge, \vee, ^*)$ zvaćemo **m^*-sistem poluprstena**, ukoliko je ona snabdevena poluprstenskim potapanjima

$$\psi_{i,j} : S_i \to S_j$$

za svaki par $i \geq j$ i bijekcijom * na $\bigcup_{i\in D} S_i$ tako da su gornji uslovi (i)–(iii) zadovoljeni, kao i sledeći uslovi:

(iv) $^* : S_i \to S_{i^*}$ je poluprstenski antiizomorfizam za sve $i \in D$,

(v) $\psi_{i^*,j^*}(x) = (\psi_{i,j}(x^*))^*$, za sve $i, j \in D$ tako da je $i \geq j$ i za sve $x \in S_{i^*}$,

što izražava simetriju m^*-sistema u odnosu na involuciju i respektivno, kompatibilnost * sa strukturom m^*-sistema.

Teorema 3.2.2. ([31]) *Algebra* $(S, +, \cdot, ^*)$ *je ID-poluprsten sa involucijom koji zadovoljava identitet* $x + xyx = x$ *ako i samo ako je on suma* m^**-sistema pravougaonih ID-poluprstena.*

Pogledajmo detaljnije šta su to zapravo pravougaoni poluprsteni. Podsetimo se konstrukcije koja je dobro poznata u univerzalnoj algebri [54]. Ona se zove *matrični stepen.* Naime, za svaku univezalnu algebru (A, F) (gde je F familija operacija na A) i $n \in \mathbb{N}$, n-ti matrični stepen je definisan na skupu

$$A^n = A \times A \times \cdots \times A$$

tako da su sve fundamentalne operacije originalne algebre nasleđene primenjujući ih po koordinatama u A^n, i dodate su još dve operacije: n-arna **dijagonalna operacija** d data sa

$$d(\mathbf{x}_1, \ldots, \mathbf{x}_n) = (x_{11}, x_{22}, \ldots, x_{nn}),$$

gde su $\mathbf{x}_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ za sve $1 \leq i \leq n$, i unarna operacija p definisana sa

$$p((x_1, x_2, \ldots, x_n)) = (x_2, \ldots, x_n, x_1).$$

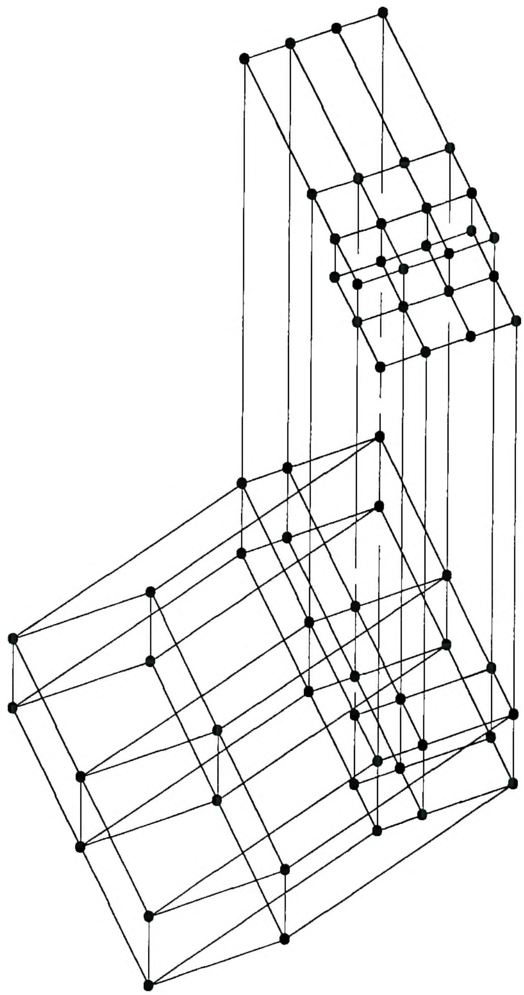
Poznato je da za svaki varijetet $\mathcal{V}$ i dati pozitivan broj n, sve izomorfne kopije svih n-tih matričnih stepena elemenata $\mathcal{V}$ takođe čine varijetet, koji označavamo sa $\mathcal{V}^{[n]}$. Takođe, poznato je da ova konstrukcija očuvava jednakosnu kompletnost, tj. minimalnost varijeteta [76].

Sledeće tvrđenje nema svoj neinvolutivni analogon.

Propozicija 3.2.3. ([31]) *Svaki pravougaoni ID-poluprsten sa involucijom je matrični kvadrat neke polumreže i obratno, svaki matrični kvadrat polumreže je pravougaoni ID-poluprsten sa involucijom. Drugim rečima, varijetet pravougaonih ID -poluprstena sa involucijom je* $\mathcal{SL}^{[2]}$ *i prema tome, on nema pravih podvarijeteta.*

U radu [31], I. Dolinka je pokazao da postoji tačno 17 netrivijalnih poddirektno nesvodljivih ID-poluprstena sa involucijom, koristeći upravo opšte rezultate iz [32] dobijene zajedno sa autorom ove diseratacije (prikazane u Glavi 1), kao i Teoremu 3.2.1. Njegov glavni rezultat je sledeći.

Teorema 3.2.4. (I. Dolinka, [31]) *Postoji tačno 64 varijeteta ID-poluprstena sa involucijom i njihova mreža je data sledećom slikom.*



Slika 3.1. Mreža svih varijeteta ID-poluprstena sa involucijom

3.3. Involutivni poluprsteni binarnih relacija i jezika

Kao što smo to već opisali u prvom paragrafu ove glave, polazeći od poluprstena binarnih relacija na nekom skupu X i dodajući mu operaciju refleksivno-tranzitivnog zatvorenja, dobijamo

$$\mathbf{Rel}(X) = (\mathcal{P}(X \times X), \cup, \circ, ^{\mathrm{rtc}}, \emptyset, \Delta_X),$$

punu Kleenejevu algebru binarnih relacija na skupu X, koju možemo dopuniti operacijom inverza relacija, tako da dobijamo involutivnu Kleenejevu algebru

$\mathbf{Rel}^{-1}(X)$. Algebre $\mathbf{Rel}(X)$ ($\mathbf{Rel}^{-1}(X)$) generišu varijetet $\mathcal{KA}$ ($\mathcal{KA}^{-1}$), i članovi tog varijeteta se nazivaju Kleenejeve algebre (sa inverzijom).

Varijetet Kleenejevih algebri se može, međutim, dobiti i na sasvim drugačiji način. Označimo sa Σ proizvoljan konačan skup. Slobodan monoid nad Σ označavamo sa $\mathbf{\Sigma}^\star$. Njegov nosač se sastoji od svih reči nad Σ, uključujući i praznu reč λ kao jedinicu ovog monoida. Članovi skupa $\mathcal{P}(\Sigma^\star)$ nazivaju se **jezici**. Unija jezika $L_1, L_2 \in \mathbf{P}(\Sigma^\star)$ se iz tradicionalnih razloga označava sa $L_1 + L_2$. Takođe, posmatra se **konkatenacija** ovih jezika

$$L_1L_2 = \{w_1w_2 \mid w_1 \in L_1, w_2 \in L_2\},$$

kao i **Kleenejeva zvezda**, koja sa za $L \in \mathcal{P}(\Sigma^\star)$ definiše sa

$$L^\star = \{\lambda\} \cup L \cup L^2 \cup \ldots = \bigcup_{n\geq 0} L^n,$$

pošto po dogovoru uzimamo da je $L^0 = \{\lambda\}$. Kako bismo izbegli zabunu, u ovom paragrafu involuciju označavati sa $^{-1}$, za razliku od operacije * koja nastaje apstrakcijom refleksivno-tranzitivnog zatvorenja, odnosno Kleenejeve zvezde (primetimo da za tu operaciju koristimo petokraku zvezdicu *, za razliku od šestokrake zvezdice * koja u ostalom delu disertacije označava involuciju).

Operacija **inverza jezika** L definiše se na sledeći način:

$$L^{-1} = \{w^{-1} \mid w \in L\},$$

gde w^{-1} označava reč koja se dobija obrtanjem reči w. Na taj način smo dobili **algebru jezika nad** Σ,

$$\mathbf{Lang}_\Sigma = (\mathbf{P}(\Sigma^\star), +, \cdot, ^\star, \emptyset, \{\lambda\}),$$

odnosno **algebru jezika sa inverzijom**

$$\mathbf{Lang}_\Sigma^{-1} = (\mathbf{P}(\Sigma^\star), +, \cdot, ^\star, ^{-1}, \emptyset, \{\lambda\}).$$

LEMA 3.3.1. *Neka je* $\mathbf{S}$ *proizvoljna polugrupa. Tada je algebra*

$$\mathbf{M}(\mathbf{S}) = (\mathbf{P}(S^1), \cup, \cdot, ^\star, \emptyset, \{\lambda\}),$$

pri čemu je $\cdot$ *množenje kompleksa,* * *operacija generisanja podmonoida, standardna Kleenejeva algebra.*

Dokaz. Posmatrajmo preslikavanje $\xi : \mathcal{P}(S^1) \to \mathcal{P}(S^1 \times S^1)$ definisano za sve $A \subseteq S^1$ sa

$$\xi(A) = \{(s, sa) \mid s \in S^1, a \in A\} = \bigcup_{a \in A} \rho_A,$$

gde ρ_A označava desnu translaciju monoida $\mathbf{S}^1$ u odnosu na $a \in S^1$. Lako se pokazuje da je ξ u stvari potapanje algebre $\mathbf{M}(\mathbf{S})$ u $\mathbf{Rel}(S^1)$. □

Gornje tvrđenje ima jednu značajnu posledicu. Naime, ako uzmemo $\mathbf{S} = \mathbf{\Sigma}^\star$, tada je

$$\mathbf{M}(\mathbf{\Sigma}^\star) = \mathbf{Lang}_\Sigma.$$

Ovo znači da se svaki jezik može posmatrati kao binarna relacija, tačnije kao unija desnih translacija na slobodnom monoidu. Time je dokazana

PROPOZICIJA 3.3.2. *Svaka algebra jezika je standardna Kleenjeva algebra.*

PROPOZICIJA 3.3.3. *Varijetet $\mathcal{L}$ generisan svim algebrama jezika je podvarijetet varijeteta Kleenejevih algebri $\mathcal{KA}$.*

Veza algebri jezika i Kleenejevih algebri je još jača. Ovo sledi iz fundamentalnog tvrđenja, poznatog kao **Kozen-Nemetijeva teorema**. Ovu teoremu je prvi dokazao Kozen 1979. godine u radu [64], u kontekstu dinamičkih algebri. Međutim, ovaj rad je bio u formi IBM-ovog tehničkog izveštaja i nikad nije bio objavljen. Dokaz je prvi publikovao Németi tri godina kasnije u radu [82]. Označimo sa $\mathbf{Reg}_\Sigma = (Reg(\Sigma), +, \cdot, ^\star, \emptyset, \{\lambda\})$ podalgebru algebre $\mathbf{Lang}_\Sigma$ generisanu jezicima $\{a\}$, $a \in \Sigma$. Njeni elementi su **regularni jezici**. Po čuvenoj Kleenejevoj teoremi, regularni jezici su tačno jezici konačnih automata.

TEOREMA 3.3.4. (Kozen, Németi) *Algebra* $\mathbf{Reg}_\Sigma$ *je slobodna Kleenejeva algebra nad* Σ, *slobodno generisana preslikavanjem* $a \mapsto \{a\}$, $a \in \Sigma$.

PROPOZICIJA 3.3.5. $\mathcal{L} = \mathcal{KA}$.

Dokaz. Iz Posledice 3.3.3 imamo da je $\mathcal{L} \leq \mathcal{KA}$. S druge strane algebre (regularnih jezika) $\mathbf{Reg}_\Sigma$ su podalgebra algebri jezika, pa je varijetet generisan njima sadržan u $\mathcal{L}$. Međutim, algebre regularnih jezika su slobodne Kleenejeve algebre, pa one generišu $\mathcal{KA}$. Sledi da je $\mathcal{KA} \leq \mathcal{L}$. □

Klasa Kleenejevih algebri nema konačnu bazu identiteta. Ovo je dokazao V. N. Redko 1964. godine u radu [101]. Prvu eksplicitnu jednakosnu aksiomatizaciju za varijetet $\mathcal{L} = \mathcal{KA}$ dao je D. Krob 1991. godine u radu *Complete* *systems of $\mathcal{B}$-rational identities.* Ovim radom D. Krob je potvrdio hipotezu J. H. Conwaya iz [13].

Nakon što je Redko dokazao da jednakosna teorija regularnih jezika nema konačnu bazu identiteta, krenulo se u potragu za konačnim opisom ove klase algebri. Pokazalo se da postoje teorije kvaziidentiteta sa konačnom bazom, čije su jednakosne posledice upravo identiteti algebri regularnih jezika, odnosno Kleenejevih algebri. Ovo znači da postoje konačno aksiomatizovani kvazivarijeteti $\mathcal{Q}$ koji generišu $\mathcal{KA}$, tj. $\mathcal{KA} = \mathsf{HSP}(\mathcal{Q})$.

Svaka algebra jezika zadovoljava **Conwayeve identitete**

$$\begin{aligned}(x+y)^\star &= (x^\star y)^\star x^\star,\\ (xy)^\star &= 1 + x(yx)^\star y.\end{aligned}$$

Poluprstene sa nulom i jedinicom i dodatnom unarnom operacijom * u kojima važe gornji identiteti zovemo **Conwayevi *-poluprsteni**. Conwayevi identiteti opisuju dejstvo unarne operacije * na zbir i konkatenaciju jezika. U algebrama jezika takođe imamo

$$\begin{aligned}0^\star &= 1,\\ 1^\star &= 1.\end{aligned}$$

Drugi od ova dva identiteta zovemo **ω-idempotentni zakon** (primetimo da iz ovih zakona sledi $(x^\star)^\star = x^\star = x^\star x^\star$). Prema tome, svaka algebra jezika je ω-idempotentni Conwayev *-poluprsten.

TEOREMA 3.3.6. (Krob, [68]) *Kvazivarijetet $\mathcal{Q}$ definisan identitetima koji definišu Conwayeve *-poluprstene zajedno sa $1+1=1$ i kvaziidentitetom*

$$x^2 = x \;\Rightarrow\; x^\star = 1 + x$$

generiše $\mathcal{KA}$.

TEOREMA 3.3.7. (Kozen, [66]) *Kvazivarijetet $\mathcal{Q}'$ definisan identitetima koji definišu Conwayeve *-poluprstene zajedno sa $1+1=1$ i kvaziidentitetima*

$$\begin{aligned}a + bx \leq x &\;\Rightarrow\; b^\star a \leq x,\\ a + xb \leq x &\;\Rightarrow\; ab^\star \leq x\end{aligned}$$

generiše $\mathcal{KA}$.

Neka je A matrica formata $n \times n$ čiji su elementi regularni izrazi (tj. termi na jeziku Kleenejevih algebri). Definišimo matricu $A^\star$ (istog formata) indukcijom po n.

- Za $n = 1$, $A = [r]$, definišemo $A^\star = [r^\star]$.
- Neka je $n = k+1$, $k \geq 1$. Podelimo matricu na blokove

$$A = \begin{bmatrix} P & Q \\ R & S \end{bmatrix},$$

gde je P matrica formata $k \times k$, S matrica formata 1×1, dok su Q i R redom odgovarajuće vektor kolone i vektor vrste. Sada definišemo

$$A^\star = \begin{bmatrix} (P+QS^\star R)^\star & (P+QS^\star R)^\star QS^\star \\ (S+RP^\star Q)^\star RP^\star & (S+RP^\star Q)^\star \end{bmatrix}.$$

Neka je $\mathbf{G} = (\{g_1, \ldots, g_n\}, \cdot)$ proizvoljna konačna grupa. Definisaćemo matricu $A_{\mathbf{G}} = [\alpha_{ij}]_{n\times n}$ pridruženu ovoj grupi, čiji su elementi promenljive iz skupa $X = \{x_k \mid k \geq 1\}$, na sledeći način:

$$\alpha_{ij} = x_k \Leftrightarrow g_i g_k = g_j \; (\Leftrightarrow g_i^{-1} g_j = g_k).$$

Dalje, neka $\mathbf{v}_n^{(1)}$ označava vrstu dužine n čiji je prvi element 1, a ostali 0, dok $\mathbf{s}_n$ označava kolonu visine n čiji su svi elementi 1. Identitet

$$\mathbf{v}_n^{(1)} A_{\mathbf{G}}^\star \mathbf{s}_n = (x_1 + \ldots + x_n)^\star$$

zovemo **grupni matrični identitet pridružen grupi G** i označavamo ga sa $P(\mathbf{G})$. Leva strana ovog identiteta je u stvari zbir prve vrste matrice $A_{\mathbf{G}}^\star$.

TEOREMA 3.3.8. (Krob, [68]) *Identiteti ω-idempotentnih Conwayevih *-poluprstena, zajedno sa matričnim identitetima $P(\mathbf{G})$ pridruženim svakoj konačnoj grupi $\mathbf{G}$, čine bazu zakona algebri jezika (tj. bazu identiteta za $\mathcal{KA}$).*

Ispostavilo se da se gornje tvrđenje može pojačati u smislu da **G** pripada nekoj klasi konačnih grupa. Kažemo da grupa **H** deli grupu **G** ako je **H** izomorfna faktor-grupi neke podgrupe od **G**.

TEOREMA 3.3.9. (Bloom, Ésik, [7]) *Neka je $\mathcal{G}$ neka klasa konačnih grupa. Aksiome ω-idempotentnih Conwayevih *-poluprstena i identiteti $P(\mathbf{G})$, $\mathbf{G} \in \mathcal{G}$, čine bazu identiteta za $\mathcal{KA}$ ako i samo ako svaka konačna prosta grupa deli neku grupu iz $\mathcal{G}$.*

D. A. Bredikhin je 1993. postavio pitanje da li varijetet generisan algebrama binarnih relacija

$$(\mathcal{P}(A \times A), \circ, ^{\mathrm{rtc}})$$

(proširene, eventualno, konstantama $\emptyset, \Delta_A$) ima konačnu jednakosnu bazu. Reč je, naravno, o multiplikativnim reduktima punih Kleenejevih relacionih algebri. U radu [17] dat je negativan odgovor na ovo pitanje. Za proizvoljni skup A definišimo algebru

$$\mathbf{UFRel}(A) = (\mathcal{P}(A \times A), \circ, ^{\mathrm{rtc}}, \emptyset, \Delta_A),$$

koju zovemo **puna multiplikativna Kleenejeva relaciona algebra**. Varijetet generisan ovim algebrama označavamo sa $\mathcal{UF}$, a njegovi članovi su **multiplikativne Kleenejeve algebre.**

Lako se uveravamo da je $\cup$-slobodni redukt Kleenejeve algebre $\mathrm{M}(\mathrm{S})$ kompleksa monoida S^1, multiplikativna Kleenejeva algebra. Specijalno, ako je $\mathbf{S} = \mathbf{\Sigma}^\star$ slobodan monoid, dobijamo redukt algebre jezika bez $+$,

$$\mathbf{UFLang}_\Sigma = (\mathcal{P}(\Sigma^\star), \cdot, ^\star, \emptyset, \{\lambda\}).$$

Sa $\mathbf{UFReg}_\Sigma$ označavamo podalgebru od $\mathbf{UFLang}_\Sigma$ generisanu jezicima $\{a\}$, $a \in \Sigma$. Elementi ove algebre su **multiplikativni regularni jezici**.

PROPOZICIJA 3.3.10. ([17]) *Jednakosna teorija $Eq(\mathcal{UF})$ se poklapa sa skupom identiteta iz $Eq(\mathcal{KA})$ koji ne sadrže $+$.*

Adaptacijom Kozen-Németijeve teoreme dobija se

PROPOZICIJA 3.3.11. ([17]) $\mathbf{UFReg}_\Sigma$ *je $\mathcal{UF}$-slobodna algebra nad Σ, slobodno generisana preslikavanjem $a \mapsto \{a\}$, $a \in \Sigma$.*

TEOREMA 3.3.12. (Crvenković, Dolinka, Ésik, [17]) *Ne postoji konačan skup identiteta koji važe na $\mathcal{KA}$ iz kojeg se mogu izvesti svi identiteti od jedne promenljive koji važe na $\mathcal{UF}$. Stoga, varijetet $\mathcal{UF}$ nema konačnu bazu identiteta.*

Vratimo se sada algebrama jezika sa inverzijom

$$\mathbf{Lang}_\Sigma^{-1} = (\mathbf{P}(\Sigma^\star), +, \cdot, ^\star, ^{-1}, \emptyset, \{\lambda\}).$$

Varijetet generisan svim ovakvim algebrama označavamo sa $\mathcal{L}^{-1}$. Međutim, za razliku od slučaja Kleenejevih algebri bez inverzije, $\mathcal{KA}^{-1} \neq \mathcal{L}^{-1}$. Posmatrajmo identitet

$$x + xx^{-1}x = xx^{-1}x.$$

On važi na svim algebrama $\mathbf{Rel}^{-1}(X)$, a time i na celom varijetetu $\mathcal{KA}^{-1}$. Ali, on očigledno ne važi na algebrama jezika $\mathbf{Lang}_\Sigma^{-1}$, a time ni na $\mathcal{L}^{-1}$.

Definišimo skup Σ' tako što se svakom elementu $a \in \Sigma$ obostrano jednoznačno pridružuje slovo $a' \in \Sigma'$. Za jezik $L \subseteq (\Sigma \cup \Sigma')^*$ definišemo

$$L^{-1} = \{w^{-1} \mid w \in L\},$$

gde je za $w = a_1 \dots a_n$, $w^{-1} = a_n^{-1} \dots a_1^{-1}$, pri čemu je za $x \in \Sigma \cup \Sigma'$,

$$x^{-1} = \begin{cases} x' & x \in \Sigma \\ y, & x = y' \in \Sigma'. \end{cases}$$

Dobijamo algebru

$$\mathbf{L}^{-1}(\Sigma, \Sigma') = (\mathcal{P}((\Sigma \cup \Sigma')^*), +, \cdot, ^*, ^{-1}, \emptyset, \{\lambda\}).$$

Propozicija 3.3.13. ([17]) *Za sve azbuke* Σ, $\mathbf{L}^{-1}(\Sigma, \Sigma') \in \mathcal{L}^{-1}$.

Neka je $\mathbf{R}^{-1}(\Sigma, \Sigma')$ podalgebra od $\mathbf{L}^{-1}(\Sigma, \Sigma')$ generisana jezicima $\{x\}$, $x \in \Sigma \cup \Sigma'$.

Teorema 3.3.14. (Bloom, Ésik, Stefanesku, [8]) $\mathbf{R}^{-1}(\Sigma, \Sigma')$ *je* $\mathcal{L}^{-1}$*-slobodna algebra nad* Σ. *Stoga baza identiteta za* $\mathcal{KA}$, *zajedno sa identitetima*

$$\begin{aligned} (x+y)^{-1} &= x^{-1} + y^{-1}, \\ (xy)^{-1} &= y^{-1}x^{-1}, \\ (x^*)^{-1} &= (x^{-1})^*, \\ (x^{-1})^{-1} &= x, \end{aligned}$$

čini bazu identiteta za $\mathcal{L}^{-1}$. *Drugima rečima,* $\mathcal{L}^{-1}$ *je upravo varijetet svih Kleenejevih algebri sa involucijom.*

Kažemo da je jezik $L \subseteq (\Sigma \cup \Sigma')^*$ **zatvoren** ako za svaku reč $w \in L$ oblika $w = u_1 v v^{-1} v u_2$ važi $u_1 v u_2 \in L$. Najmanji zatvoren jezik koji sadrži L (koji postoji pošto je $(\Sigma \cup \Sigma')^*$ zatvoren jezik i pošto se zatvorenost čuva presecima) je **zatvorenje** od L, koje označavamo sa $cl(L)$. Jasno, jezik je zatvoren ako i samo ako je $L = cl(L)$. Definišimo relaciju ρ na sledeći način

$$(L_1, L_2) \in \rho \Leftrightarrow cl(L_1) = cl(L_2).$$

Lako se pokazuje da je ρ kongruencija na $\mathbf{Reg}_\Sigma$ ali i na $\mathbf{R}^{-1}(\Sigma, \Sigma')$, pa dobijamo faktor algebru

$$\mathbf{CR}^{-1}(\Sigma, \Sigma') = \mathbf{R}^{-1}(\Sigma, \Sigma')/\rho.$$

TEOREMA 3.3.15. (Bloom, Ésik, Stefanesku, [8]) $\mathbf{CR}^{-1}(\Sigma, \Sigma')$ *je* $\mathcal{KA}^{-1}$-*slobodna algebra nad* Σ.

Rezultati dobijeni u radu [8] omogućili su Z. Ésiku i L. Bernátskom da u [35] dobiju sledeći rezultat.

TEOREMA 3.3.16. (Ésik, Bernátsky, [35]) *Identitet*

$$x + xx^{-1}x = xx^{-1}x$$

definiše $\mathcal{KA}^{-1}$ *unutar varijeteta* $\mathcal{L}^{-1}$.

Na osnovu jedne opšte teoreme o jednakosnim teorijama involutivnih algebri iz rada [18] (koja je prikazana u magistarskoj tezi autora [120]), dobijamo sledeće rezultate.

TEOREMA 3.3.17. (Crvenković, Dolinka, Ésik, [16]) *Varijetet* $\mathcal{L}^{-1}$ *nema konačnu bazu identiteta.*

TEOREMA 3.3.18. (Crvenković, Dolinka, Ésik, [16]) *Varijetet* $\mathcal{KA}^{-1}$ *nema konačnu bazu identiteta.*

Za bilo koji skup A, $\mathbf{UFRel}^{-1}(A)$ je algebra koja se dobija od $\mathbf{UFRel}(A)$ proširivanjem operacijom inverzije relacija,

$$\mathbf{UFRel}^{-1}(A) = (\mathcal{P}(A \times A), \circ, {}^{\mathrm{rtc}}, {}^{-1}, \emptyset, \Delta_A).$$

Varijetet generisan ovakvim algebrama označavamo sa $\mathcal{UF}^{-1}$. Članovi ovog varijeteta su **multiplikativne Kleenejeve algebre sa inverzijom**.

TEOREMA 3.3.19. (Crvenković, Dolinka, Ésik, [17]) *Ne postoji konačan skup identiteta koji važe na* $\mathcal{KA}^{-1}$ *iz koga se mogu izvesti svi identiteti od jedne promenljive koji važe na* $\mathcal{UF}^{-1}$. *Stoga varijetet* $\mathcal{UF}^{-1}$ *nema konačnu bazu identiteta.*

TEOREMA 3.3.20. (Crvenković, Dolinka, Ésik, [17]) *Varijetet generisan multiplikativnim Kleenejevim algebrama sa inverzijom* $\mathbf{UFLang}_{\Sigma}^{-1}$ *nema konačnu bazu identiteta.*

Napominjemo da je materijal koji se odnosi na poluprstene relacija i jezika ovde iznet u sažetom obliku. Detalji dokaza navedenih tvrđenja mogu se naći u doktorskoj disertaciji I. Dolinke [24].

3.4. Globalna neodređenost involutivnih poluprstena

Involutivni poluprsteni nisu globalno određeni. Ovo je pokazano u radovima [21] i [120]. Dokaz globalne neodređenosti involutivnih poluprstena bazira se na Teoremi 2.9.1.

TEOREMA 3.4.1. (Crvenković, Dolinka, Vinčić, [21]) *Varijetet involutivnih poluprstena nije globalno određen.*

Dokaz. Dajemo postupak kojim se proizvoljna involutivna polugrupa S pretvara u involutivni poluprsten $\sigma(\mathrm{S})$. Dodajmo novu nulu 0 (čak i ako S već ima nulu) tako da je $0^* = 0$. Definišimo komutativnu operaciju $+$ na $S \cup \{0\}$ tako da je $a + 0 = a$ za sve $a \in S \cup \{0\}$ i $a + b = 0$ za sve $a, b \in S$. Nije teško videti da je sada $\sigma(\mathrm{S})$ involutivni poluprsten.

Posmatrajmo $\sigma(\mathbf{A})$ i $\sigma(\mathbf{B})$, gde su $\mathbf{A}$ i $\mathbf{B}$ involutivne polugrupe iz Teoreme 2.9.1. Jasno, $\sigma(\mathbf{A}) \cong \sigma(\mathbf{B})$, pošto je svaki izomorfizam involutivnih poluprstena ujedno i izomorfizam odgovarajućih involutivnih polugrupa. S druge strane, ako je $\varphi : \Gamma(\mathbf{A}) \to \Gamma(\mathbf{B})$ izomorfizam iz već pomenute teoreme, proširimo ga do preslikavanja $\psi : \Gamma(\mathbf{A} \cup \{0_{\mathbf{A}}\}) \to \Gamma(\mathbf{B} \cup \{0_{\mathbf{B}}\})$ tako da imamo $\psi(0_{\mathbf{A}}) = \{0_{\mathbf{B}}\}$ i za sve neprazne $C \subseteq A$:

$$\psi(C \cup \{0_{\mathbf{A}}\}) = \varphi(C) \cup \{0_{\mathbf{B}}\}.$$

Jasno, ψ je bijekcija. Takođe, lako se vidi da je ψ izomorfizam involutivnih poluprstena $\Gamma(\sigma(\mathbf{A}))$ i $\Gamma(\sigma(\mathbf{B}))$. Ovo se može proveriti koristeći činjenicu da je sabiranje kompleksa (npr. u $\sigma(\mathbf{A})$) dato sa ($C, D \subseteq A \cup \{0_{\mathbf{A}}\}$):

$$C + D = \begin{cases} \{0_{\mathbf{A}}\}, & 0_{\mathbf{A}} \notin C \cup D, \\ D \cup \{0_{\mathbf{A}}\}, & 0_{\mathbf{A}} \in C,\ 0_{\mathbf{A}} \notin D, \\ C \cup \{0_{\mathbf{A}}\}, & 0_{\mathbf{A}} \notin C,\ 0_{\mathbf{A}} \in D, \\ C \cup D \cup \{0_{\mathbf{A}}\}, & 0_{\mathbf{A}} \in C \cap D. \end{cases}$$

Zbog toga je $\Gamma(\sigma(\mathbf{A})) \cong \Gamma(\sigma(\mathbf{B}))$. □

POSLEDICA 3.4.2. ([21]) *Varijetet poluprstena nije globalno određen.*

4.1. Istorijski pregled

Teorija prstena je jedna od najrazvijenijih i najznačajnijih oblasti algebre. U okviru ove teorije razvija se i teorija prstena sa involucijom. Do sada je napisano više knjiga na temu involutivnih prstena od kojih su najznačajnije knjige I. N. Hersteina [52] i S. K. Berberiana [3]. Takođe, delovi nekih poznatih monografija posvećeni su prstenima sa involucijom. Kao što je rečeno u delu o *-regularnim polugrupama, knjiga L. A. Skornjakova [112] sadrži vrlo interesantna razmatranja prstena sa involucijom. Spomenimo i knjigu I. N. Hersteina [49], koja u Poglavlju II govori o prostim prstenima sa involucijom. Veza involutivnih prstena i simetričnih mreža data je u knjizi [74]. Interesantna veza Baerovih *-polugrupa, odnosno Baerovih *-prstena, i ortomodularnih mreža data je u knjizi [9].

Spomenimo još i poznate radove o involutivnim prstenima [53, 72, 126].

Jedna od poznatijih teorema algebre je teorema Jacobsona koja kaže da je svaki prsten u kome za neko $n \in \mathbb{N}$ važi identitet $x^{n+1} = x$ komutativan (videti [48, 51, 57]). Jedan od načina da se dokaže Jacobsonova teorema je da se pokaže da svaki poddirektno nesvodljiv prsten koji zadovoljava identitet gornjeg oblika mora biti polje. U ovoj disertaciji ćemo opisati involutivne prstene koji su poddirektno nesvodljivi i zadovoljavaju identitet $x^{n+1} = x$ za neko $n \in \mathbb{N}$. Koristeći ovaj rezultat, bićemo u mogućnosti da konstruišemo mreže varijeteta involutivnih prstena koji zadovoljavaju ovakve identitete.

4.2. Involutivni prim prsteni

Involutivne prim prstene ispitivali su mnogi autori (videti, na primer, radove [50, 72]). Ovde ćemo razmotriti neke osobine involutivnih prim prstena izučavane u radu [50]. Podsetimo se, prsten $\mathbf{R}$ je **prim** ako za sve $a, b \in R$ takve da je $aRb = 0$ važi $a = 0$ ili $b = 0$.

Neka je $\mathbf{R}$ prsten sa involucijom *. Označimo $S = \{x \in R \mid x^* = x\}$ i $K = \{x \in R \mid x^* = -x\}$ i nazovimo elemente S **simetričnim**, a elemente K **antisimetričnim elementima** od $\mathbf{R}$. Sa Z ili $Z(\mathbf{R})$ označavamo **centar** od $\mathbf{R}$. Prsten $\mathbf{R}$ ćemo zvati **domen** (čak i ako nije komutativan), ako $ab = 0$ u $\mathbf{R}$ implicira $a = 0$ ili $b = 0$.

LEMA 4.2.1. ([50]) *Neka je* $\mathbf{R}$ *prsten sa involucijom* *, *i neka je* $U \neq 0$ *ideal u* $\mathbf{R}$ *tako da je* $U^* = U$. *Ako je* $U \cap S = 0$, *tj.* U *nema simetričnih elemenata, onda je* $U^3 = 0$.

Dokaz. Ako je $0 \neq x \in U$, onda $x^* \in U^* = U$ pa važi $x + x^* \in U \cap S = 0$. Sledi $x^* = -x$, za svako $x \in U$. Posebno, s obzirom da je $U \cap S = 0$, imamo da $2x = 0$ povlači $x = 0$ za sve $x \in U$, kao i da za sve $x \in U$ važi $(x^2)^* = x^2$. Ovo znači da $x^2 \in S$, pa kako je U ideal, $x^2 \in U$, tj. $x^2 = 0$. Dalje, za sve $x, y \in U$ imamo

$$xy = (-x)(-y) = x^*y^* = (yx)^* = -yx,$$

pa sledi

$$xyz = x(yz) = -x(zy) = -(xz)y = zxy.$$

Iz prethodnog imamo

$$xyz - zxy = 0,$$

što uz $-z(xy) = (xy)z$ daje

$$xyz + xyz = 0,$$

tj.

$$2xyz = 0.$$

Sledi $xyz = 0$ tj. $U^3 = 0$. □

Ideale $\mathbf{I}$ involutivnog prstena $\mathbf{R}$ fiksirane involucijom, $I^* = I$ (kao što je to U u gornjoj lemi), zvaćemo ***-ideali**.

Kažemo da je podskup $A \subseteq R$ **Liejev potprsten** od $\mathbf{R}$ ako je A aditivna podgrupa od $\mathbf{R}$ tako da za svako $a, b \in A$, $ab - ba \in A$. Ako je $\mathbf{A}$ Liejev potprsten od $\mathbf{R}$, aditivna podgrupa $U \subseteq A$ se zove *Liejev ideal* od A ako važi

$$u \in U,\ a \in A \Rightarrow [u, a] = ua - au \in U.$$

LEMA 4.2.2. *Neka je* $\mathbf{R}$ *prsten bez nenula nilpotentnih ideala u kome važi da* $2x = 0$ *implicira* $x = 0$. *Pretpostavimo da je* $U \neq \{0\}$ *potprsten od* $\mathbf{R}$ *koji je ujedno i njegov Liejev ideal. Tada je ili* $U \subseteq Z(\mathbf{R})$, *ili* U *sadrži nenula ideal od* $\mathbf{R}$.

Dokaz. Pretpostavimo da U, kao potprsten, nije komutativan. Tada za neke $x, y \in U$, $xy - yx \neq 0$. Za bilo koje $r \in R$, $x(yr) - (yr)x \in U$. To znači da je $(xy - yx)r + y(xr - rx) \in U$. Drugi sabirak je iz U, jer $y, xr - rx \in U$. Sledi da je $(xy - yx)r \in U$. Imamo da je $(xy - yx)R \subseteq U$. Ali, tada za $r, s \in R$, $((xy - yx)r)s - s((xy - yx)r) \in U$, što daje $R(xy - yx)R \subseteq U$. Ako je $R(yx - xy)R = 0$, onda je $(R(xy - yx))^2 = 0$, suprotno pretpostavci za $\mathbf{R}$.

Ako je U komutativan, želimo da pokažemo da on leži u centru od $\mathbf{R}$. Neka je $a \in U$, $x \in R$. Tada je $ax - xa \in U$. Sada za $x, y \in R$ imamo

$$a(a(xy) - (xy)a) = (a(xy) - (xy)a)a.$$

Prikazujući $a(xy) - (xy)a$ kao $(ax - xa)y + x(ay - ya)$, i koristeći činjenicu da a komutira sa ovim elementom, kao i sa $ax - xa$ i $ay - ya$, dobijamo

$$2(ax - xa)(ay - ya) = 0$$

za sve $x, y \in R$. Izaberimo $y = ax$. Ovo daje

$$(ax - xa)a(ax - xa) = 0.$$

Sledi da je $ax - xa = 0$, pa je $ax = xa$. □

Teorema 4.2.3. ([50]) *Neka je* $\mathbf{R}$ *involutivni prim prsten čiji nijedan nenula simetričan element nije nilpotentan. Tada važi bar jedan od uslova:*

(1) $xx^* = 0 \Rightarrow x = 0$;

(2) $S \subseteq Z(\mathbf{R})$ *i prsten* $\mathbf{R}$ *je red u prstenu* $\mathbf{F}_2$ *svih* 2×2 *matrica nad nekim poljem* $\mathbf{F}$.

Dokaz. Pretpostavimo da je $xx^* = 0$ za neko $x \neq 0$ iz R. Želimo da pokažemo da je $S \subseteq Z(\mathbf{R})$ i da je $\mathbf{R}$ red u $\mathbf{F}_2$.

Najpre, imamo $x^*Sx \subseteq S$, i iz $xx^* = 0$ sledi da je kvadrat svakog elementa iz x^*Sx jednak 0. Prema tome, iz pretpostavke o $\mathbf{R}$ sledi $x^*Sx = 0$. Ako je $r \in R$, onda je $x^*(r^* + r)x = 0$, pa imamo da važi

$$x^*r^*x = -x^*rx,$$

što znači da je x^*rx antisimetričan za svako $r \in R$. S obzirom da je $\mathbf{R}$ prim prsten, sledi da je za neko $r \in R$, $x^*rx \neq 0$. Sada $\mathbf{R}$ ne može biti karakteristike 2. Naime, ako označimo $k = x^*rx$ i ako bi bilo $k + k = 0$, imamo $k = -k$, tj.

$$k^* = (x^*rx)^* = x^*r^*x = -x^*rx = -k = k,$$

pa bismo imali da je k simetričan element, što je nemoguće, imajući u vidu da je $k^2 = -kk^* = 0$ i pretpostavku teoreme o simetričnim elementima. Dalje, iz gornjih relacija imamo $kSk = 0$. Ako je $s \in S$, onda $ks - sk \in S$, ($k^* = -k$ i $(-s)^* = -s$). Štaviše, s obzirom da je $k^2 = 0$, $s, s^2 \in S$ i $kSk = 0$, vidimo da je $(ks - sk)^2 = 0$. Naša hipoteza za $\mathbf{R}$ daje $ks - sk = 0$ za sve $s \in S$. Dakle, k komutira sa svakim elementom potprstena $\langle S \rangle$ od $\mathbf{R}$ generisanog sa S.

Sada, ako $s \in S$ i $y \in R$, onda $sy - ys = sy + y^*s - (y + y^*)s$ pripada $\langle S \rangle$. To znači da je $\langle S \rangle$ Liejev ideal od $\mathbf{R}$. S obzirom da je $\mathbf{R}$ 2-torziono slobodan i nema nilpotentnih ideala, po prethodnoj lemi je ili $S \subseteq Z(\mathbf{R})$, ili $\langle S \rangle$ sadrži nenula ideal U od $\mathbf{R}$. Ova poslednja mogućnost znači da k komutira sa elementima nenula ideala U. U prim prstenu to znači da $k \in Z(\mathbf{R})$. Međutim, kako je $k \neq 0$ i $k^2 = 0$, $krk = 0$, što u prim prstenu forsira da je $k = 0$.

Sledi da je jedina mogućnost $S \subseteq Z(\mathbf{R})$.

Tvrdimo da ovo znači da je $\mathbf{R}$ red u $\mathbf{F}_2$ za neko polje $\mathbf{F}$. Kako važi $S \subseteq Z(\mathbf{R})$ i elementi $Z(\mathbf{R})$ nisu delitelji nule u $\mathbf{R}$, možemo lokalizovati $\mathbf{R}$ tako da dobijemo prsten

$$T = \{r/s \mid r \in R, s \neq 0 \in S\}.$$

$\mathbf{T}$ je prim prsten sa involucijom. Štaviše, nenula simetrični elementi su invertibilni u $\mathbf{T}$. Tvrdimo da je $\mathbf{T}$ prost kao prsten. Ako je $V \neq 0$ ideal od $\mathbf{T}$, onda je $U = VV^* \neq 0$ i $U^* = U$. Prema Lemi 4.2.1, U ima nenula simetričan element. Ovaj element je invertibilan u $\mathbf{T}$, pa je $U = T$. Pošto je $U \subseteq V$, imamo da je $V = T$. Sledi da je $\mathbf{T}$ prost (nema netrivijalnih idela). Simetrični elementi iz T leže u centru od $\mathbf{T}$, pa je $\mathbf{T}$ 4-dimenzionalan nad svojim centrom. Prsten $\mathbf{T}$ ima delitelje 0 ($x^*x = 0$), pa nije telo. Po poznatim rezultatima iz teorije prstena, sledi da je $\mathbf{T} \cong \mathbf{F}_2$ za neko polj $\mathbf{F}$. Po konstrukciji, $\mathbf{R}$ je red u $\mathbf{T}$. □

Lema 4.2.4. ([50]) *Neka je* $\mathbf{R}$ *prim prsten sa involucijom u kome je* $ab \neq 0$ *ako su* $a \neq 0$ *i* $b \neq 0$ *u* S. *Tada važi bar jedan od sledeća dva uslova:*

(1) $\mathbf{R}$ *je domen;*

(2) $S \subseteq Z(\mathbf{R})$ *i prsten* $\mathbf{R}$ *je red u prstenu* $\mathbf{F}_2$ *svih* 2×2 *matrica nad nekim poljem* $\mathbf{F}$.

Dokaz. Pretpostavimo da $\mathbf{R}$ nije red u $\mathbf{F}_2$. Prema prethodnoj teoremi, $xx^* = 0$ implicira $x = 0$ u $\mathbf{R}$. Pretpostavimo da je $uv = 0$, $u, v \in R$. Tada je $(u^*u)(vv^*) = 0$ i kako $u^*u, vv^* \in S$, onda je ili $u^*u = 0$, ili $vv^* = 0$. Prema tome, ili je $u = 0$, ili $v = 0$. Sledi da je $\mathbf{R}$ domen. □

Kažemo da je prsten *poluprim* ako nema nenula nilpotentnih ideala. Ako želimo da Lemu 4.2.4 uopštimo na poluprim prstene sa involucijom u kojima je $ab \neq 0$ ako su $a \neq 0$ i $b \neq 0$ u S, možemo pretpostaviti da postoje ideali $A \neq 0$ i $B \neq 0$ u $\mathbf{R}$ tako da je $AB = 0$.

Tvrdimo da je $A^*a = 0$. Sigurno važi $A^*aB = 0$, pa je $0 = (A^*aB)^* = B^*a^*a$. S obzirom da je $\mathbf{R}$ poluprim prsten, ova relacija implicira da važi $A^*aB^* = 0$. Prama tome $(A^*a)(B + B^*) = 0$. Ako je $A^*a \neq 0$ onda, s obzirom da je $\mathbf{R}$ poluprim, prema Lemi 4.2.1 postoji element $u \in A^*a$, $u \neq 0$, tako da je $u^* = u$. Slično, u $B + B^*$ postoji $v \neq 0$ tako da važi $v^* = v$. Iz $A^*a(B + B^*) = 0$ imamo da je $uv = 0$, što protivreči našoj hipotezi o S. Sledi da ako je $AB = 0$ i $A, B \neq 0$, onda je $A^*a = 0$. Primetimo da u poluprim prstenu $\mathbf{R}$ iz $A^*a = 0$ sledi $A \cap A^* = 0$.

Neka je $M = \{x \in R \,|\, xA = 0\}$. M je ideal od $\mathbf{R}$ i $A^* \subseteq M$. Kako je $MA = 0$, prema prethodnom je $M^*M = 0$. S obzirom da je $\mathbf{R}$ poluprim prsten, ovo daje $MM^* = 0$. Ako je $Mx = 0$, onda je $A^*x = 0$, jer je $A^* \subseteq M$. Sledi $x^*A = 0$, pa je $x^* \in M$. Drugim rečima $\mathbf{M}^*$ je anihilator $\mathbf{M}$ u $\mathbf{R}$.

Tvrdimo da je $\mathbf{R}/\mathbf{M}^*$ domen. Prvo primetimo da M nema nenula nilpotentnih elemenata. Ako je, na primer, $u^2 = 0$, gde je $u \in M$, onda s obzirom da važi $uu^* \in MM^* = 0$ i $u^*u \in M^*M = 0$, dobijamo $(u + u^*)^2 = 0$. Pošto S nema nilpotentnih elemenata, sledi $u + u^* = 0$ i $u = -u^* \in M \cap M^* = 0$. Dalje, tvrdimo da je M domen. Ako je $uv = 0$, $u, v \in M$, onda pošto je $(vu)^2 = 0$, $vu = 0$. Sada je $(u + u^*)(v + v^*) = 0$, jer je $uv = 0$, $u^*v^* = (vu)^* = 0$, $uv^* = 0$ i $u^*v = 0$, s obzirom da svi ovi elementi leže u $MM^* = 0$ i $M^*M = 0$. Naša pretpostavka o S forsira da je $u + u^* = 0$ ili $v = v^* = 0$. Zbog $M \cap M^* = 0$ imamo da je ili $u = 0$, ili $v = 0$. Sledi da je $\mathbf{M}$ domen.

Pretpostavimo da je $xy \in M^*$. Ako $m_1, m_2 \in M$, onda $(m_1x)(ym_2) \in M \cap M^* = 0$. Međutim, $\mathbf{M}$ je domen i $m_1x, ym_2 \in M$, pa sledi da je $m_1x = 0$ ili $ym_2 = 0$. Ovo odmah daje $Mx = 0$ ili $yM = 0$. Ako je $yM = 0$, onda, zbog činjenice da je $\mathbf{R}$ poluprim, $My = 0$. Drugim rečima, $xy \in M^*$ implicira $Mx = 0$. Dakle, $xy \in M^*$ implicira $x \in M^*$ ili $y \in M^*$, što praktično znači da je $\mathbf{R}/\mathbf{M}^*$ domen. Slično, $\mathbf{R}/\mathbf{M}$ je domen.

Kako je $M \cap M^* = 0$, $\mathbf{R}$ je poddirektan proizvod $\mathbf{R}/\mathbf{M}$ i $\mathbf{R}/\mathbf{M}^*$ i involucija razmenjuje komponente ovog poddirektnog proizvoda. Ovim je pokazana

TEOREMA 4.2.5. (Lanski, [72]). *Ako je* $\mathbf{R}$ *poluprim prsten sa involucijom tako da je* $ab \neq 0$ *za* $a \neq 0$ *i* $b \neq 0$ *u* S, *onda važi bar jedan od uslova:*

(1) $\mathbf{R}$ *je domen;*

(2) $S \subseteq Z(\mathbf{R})$ *i prsten* $\mathbf{R}$ *je red u prstenu* $\mathbf{F}_2$, *svih* 2×2 *matrica nad nekim poljem* $\mathbf{F}$*;*

(3) $\mathbf{R}$ *je poddirektan proizvod domena i njegove antiizomorfne kopije, sa involucijom koja razmenjuje komponente.*

4.3. Specijalni regularni *-prsteni

Jedna od (istorijski) najvažnijih klasa involutivnih prstena je klasa **regularnih *-prstena.** U stvari, **regularni prsteni**, koje je definisao J. von Neumann, u fundamentalnom delu [122], bili su polazna tačka (i glavna motivacija) za čitavu teoriju regularnih polugrupa. Regularni prsteni i regularni *-prsteni su na jedan zanimljiv način čvrsto povezani sa (ortokomplementiranim) modularnim mrežama, a na taj način i sa projektivnim geometrijama. Ova veza je data u poznatoj von Neumannovoj teoremi koordinatizacije, koja uopštava klasične teoreme koordinatizacije projektivnih prostora.

TEOREMA 4.3.1. (von Neumann, [122]) *Neka je* $\mathbf{M}$ *(ortokomplementirana) modularna mreža. Tada postoji ragularan prsten (sa involucijom)* $\mathbf{R}$ *čiji glavni desni ideali čine mrežu, koja je izomorfna sa* $\mathbf{M}$. *Štaviše,* $\mathbf{R}$ *se može dobiti kao prsten matrica (konačne dimenzije) nad prstenom* $\mathbf{D}$ *tako da je* $D \subseteq M$ *i prstenske operacije od* $\mathbf{D}$ *su izražene kao polinomi mreže* $\mathbf{M}$. *U slučaju ortomreža, ortokomplementiranje je jedinstveno određeno involucijom na* $\mathbf{R}$.

Lako se pokazuje da je uslov regularnosti za *-prsten ekvivalentan uslovu da je svaki glavni ideal generisam projekcijom, idempotentom fiksiranim involucijom. Prema tome, u ortokomplementiranoj verziji gornje teoreme, možemo zameniti mrežu glavnih ideala od $\mathbf{R}$ mrežom projekcija od $\mathbf{R}$ u odnosu na parcijalno uređenje definisano sa $e \leq f$ ako i samo ako je $ef = e$. Sledi, svaka se modularna ortomreža može reprezentovati projekcijama nekog regularnog *-prstena. Pri tome, polugrupni redukti odgovarajućih prstena su Baerove *-polugrupe, pa je reč o **Baerovim *-prstenima.**

Dalje, može se pokazati da je regularnost *-prstena $\mathbf{R}$ ekvivalentna implikaciji

$$rr^* = 0 \Rightarrow r = 0,$$

za sve $r \in R$. Sledeći Yamadu [126], involutivni prsten u kome važi identitet

$$xx^*x = x,$$

nazivamo **specijalni regularni *-prsten.** Kažemo da je element prstena **centralan** ako komutira sa svim elementima prstena.

LEMA 4.3.2. ([45]) *Ako je e idempotent u regularnom prstenu* $\mathbf{R}$*, onda su sledeći uslovi ekvivalentni:*

(1) e je centralan;

(2) e komutira sa svakim idempotentom u $\mathbf{R}$*;*

(3) eR je dvostrani ideal od $\mathbf{R}$*;*

(4) Re je dvostrani ideal od $\mathbf{R}$*;*

(5) Za bilo koje $xe \in Re$, $xe - ex = 0$, $x \in R$;

(6) Za bilo koje $ex \in eR$, $ex - xe = 0$, $x \in R$.

Koristeći ovaj rezultat, lako dobijamo sledeću lemu.

LEMA 4.3.3. ([126]) *Neka je* $\mathbf{R}$ *regularan prsten. Tada su sledeći uslovi ekvivalentni:*

(1) Multiplikativna polugrupa $(R, \cdot)$ je inverzna polugrupa;

(2) Svaki idempotent od $(R, \cdot)$ je centralan;

(3) $(R, \cdot)$ je Cliffordova polugrupa, tj. polumreža grupa.

Dokaz. Skup idempotenata $E(\mathbf{R})$ inverzne polugrupe $(R, \cdot)$ čini polumrežu, pa (1) $\Rightarrow$ (2) sledi iz Leme 4.3.1. Implikacije (2) $\Rightarrow$ (3) i (3) $\Rightarrow$ (1) su očigledne. □

Uslov (2) prethodne leme znači da je $\mathbf{R}$ Abelov regularan prsten.

Vidimo da je multiplikativna polugrupa $(R, \cdot)$ specijalnog *-regularnog prstena Cliffordova polugrupa. Sledi da se specijalna involucija * poklapa sa inverznom operacijom $^{-1}$ u inverznoj polugrupi $(R, \cdot)$ i da važi $xx^{-1} = x^{-1}x$ za sve elemente x. Sada imamo

$$2x = (2x)(2x)^*2x = 8xx^*x = 8x,$$

pa je $6x = 0$. Prema tome, $6R = \{6x \,|\, x \in R\} = 0$. Dalje, neka je $x, y \in R$. Kako važi $(x+y)(x+y)^{-1}(x+y) = x+y$, imamo

$$xy^{-1}x + yx^{-1}y + 2xx^{-1}y + 2yy^{-1}x = 0.$$

Označimo sa $R_2 = \{x \in R \,|\, 2x = 0\}$ i $R_3 = \{y \in R \,|\, 3y = 0\}$. Lako se uveravamo da su R_2 i R_3 ideali od $\mathbf{R}$ koji su zatvoreni za operaciju $^{-1}$ (tj. $(R_2, +, \cdot, ^{-1})$ i $(R_3, +, \cdot, ^{-1})$ su specijalni *-regularni prsteni). Zatim, imamo

$$R_2 \cap R_3 = 0 \quad \text{i} \quad R_2 + R_3 = R.$$

Sledi da je $\mathbf{R} = \mathbf{R}_2 \bigoplus \mathbf{R}_3$. Ovim smo dokazali naredni rezultat.

LEMA 4.3.4. ([126]) *Svaki specijalni *-regularni prsten je direktna suma* $\mathbf{A} \bigoplus \mathbf{B}$ *specijalnih *-regularnih prstena* $\mathbf{A}$ *i* $\mathbf{B}$, *od kojih je jedan karakteristike 2, a drugi karakteristike 3.*

Obratno, lako se vidi da ako je $\mathbf{R}$ direktna suma (odnosno, direktan proizvod, što je u ovom slučaju svejedno, s obzirom na konačan broj sumanada) specijalnih *-regularnih prstena $\mathbf{A}$ i $\mathbf{B}$, onda je $\mathbf{R}$ takođe specijalan *-regularan prsten.

Posmatrajmo sada specijalni *-regulani prsten $\mathbf{R} = \mathbf{R}_2 \bigoplus \mathbf{R}_3$, gde su $\mathbf{R}_2$ i $\mathbf{R}_3$ prethodno pomenuti prsteni. Stavimo $y = xx^{-1}$ u formuli

$$xy^{-1}x + yx^{-1}y + 2xx^{-1}y + 2yy^{-1}x = 0.$$

Tada je

$$x^2 + x^{-1} + 2xx^{-1} + 2x = 0.$$

Ako je $x \in R_2$, onda je $x^2 + x^{-1} = 0$ tj. $x^4 = x$. S druge strane, ako je $x \in R_3$, onda je $x^3 - x^2 - x + xx^{-1} = 0$. Sledi $x(x^2 - xx^{-1}) = x^2 - xx^{-1}$, odnosno,

$$\begin{aligned}
x^2(x^2 - xx^{-1}) &= x(x^2 - xx^{-1}) = x^2 - xx^{-1}, \\
(x^2 - xx^{-1})^2 &= x^4 - 2xx^{-1} + (xx^{-1})^2 = \\
&= x^4 - 2xx^{-1}x^2 + xx^{-1} = \\
&= x^4 - 2x^2 + xx^{-1} = \\
&= x^4 - x^2 - (x^2 - xx^{-1}) = \\
&= x^4 - x^2 - (x^4 - x^2) = \\
&= 0.
\end{aligned}$$

Kako je $(R, \cdot)$ Cliffordova polugrupa, sledi $x^2 = xx^{-1}$ tj. $x^3 = x$. Prema već navedenoj teoremi Jacobsona, $\mathbf{R}_2$ i $\mathbf{R}_3$ su komutativni i prema tome, $\mathbf{R}$ je komutativan. Na osnovu prethodnog se dobija

TEOREMA 4.3.5. (Yamada, [126]) *Svaki specijalni regularni *-prsten je komutativan.*

Za regularne prstene karakteristike 2 i 3 imamo sledeće tvrđenje.

LEMA 4.3.6. ([126]) *U regularnom prstenu* $\mathbf{R}$ *karakteristike 2, sledeći uslovi su ekvivalentni:*

(1) $(R, \cdot)$ *je inverzna polugrupa i* $\mathbf{R}$ *je specijalni *-prsten;*

(2) $(R, \cdot)$ *je inverzna polugrupa i važi* $xy^{-1}x = yx^{-1}y$ *za sve* $x, y \in R$;

(3) $(R,\cdot)$ *zadovoljava identitet* $x^4 = x$;

(4) $(R,\cdot)$ *je polumreža Abelovih grupa eksponenta 3.*

Dokaz. (1) $\Leftrightarrow$ (2) Pošto je $\mathbf{R}$ karakteristike 2, iz identiteta

$$xy^{-1}x + yx^{-1}y + 2xx^{-1}y + 2yy^{-1}x = 0,$$

sledi da je $\mathbf{R}$ specijalni regularni *-prsten, pa je $xy^{-1}x = yx^{-1}y$ za sve $x, y \in R$. Obratno, lako se uveravamo da (2) implicira

$$(x+y)(x^{-1}+y^{-1})(x+y) = x+y$$

i

$$(x^{-1}+y^{-1})(x+y)(x^{-1}+y^{-1}) = x^{-1}+y^{-1},$$

pa imamo da je $\mathbf{R}$ specijalni regularni *-prsten.

(2) $\Rightarrow$ (3) Pošto je $(R,\cdot)$ inverzna polugrupa, iz Leme 4.3.3 sledi da je svaki idempotent centralan. Prema tome, $xf^{-1}x = fx^{-1}f$. Kako je $f^{-1} = f$, imamo da je $x^2 f = x^{-1}f$, $x \in R$, $f \in E(\mathbf{R})$. S obzirom da je $(R,\cdot)$ polumreža grupa (prema Lemi 4.3.3), imamo da važi $xx^{-1} = x^{-1}x$. Neka je $f = xx^{-1}$. Sledi $x^2 = x^{-1}$ tj. $x^4 = x$.

(3) $\Rightarrow$ (4) $\mathbf{R}$ zadovoljava $x^4 = x$, pa je $(R,\cdot)$ komutativna inverzna polugrupa. Zaključujemo da je $(R,\cdot)$ polumreža Abelovih grupa $\mathbf{G}_\lambda$. Kako u $\mathbf{G}_\lambda$ važi $x^4 = x$, $\mathbf{G}_\lambda$ je eksponenta 3.

(4) $\Rightarrow$ (2) Po pretpostavci, $(R,\cdot)$ je polumreža $\mathbf{\Lambda}$ Abelovih grupa $\{\mathbf{R}_\lambda \mid \lambda \in \Lambda\}$ eksponenta 3. Jasno, $(R,\cdot)$ je inverzna polugrupa. Neka je $x \in R_\alpha$ i $y \in R_\beta$. Tada je $xy^{-1} \in R_{\alpha\beta}$. Sada je $(xy^{-1})^3 = e_{\alpha\beta}$, gde je $e_{\alpha\beta}$ jedinica $\mathbf{R}_{\alpha\beta}$, i pošto je svaki idempotent centralan, sledi da je $xy^{-1}x = yx^{-1}y$. Naime, $xy^{-1}x \in R_{\alpha\beta}$, $yx^{-1}x \in R_{\alpha\beta}$ i $xy^{-1}xy^{-1}xy^{-1} = e_{\alpha\beta}$, pa je

$$(xy^{-1}x)(yx^{-1}y)^{-1} = e_{\alpha\beta},$$

što daje

$$xy^{-1}x = yx^{-1}y.$$

Lema je dokazana. □

LEMA 4.3.7. ([126]) *Regularni prsten* $\mathbf{R}$ *karakteristike 3 je specijalni regularni* **-prsten ako i samo ako* $(R,\cdot)$ *zadovoljava identitet* $x^3 = x$. *U tom slučaju,* $(R,\cdot)$ *je inverzna polugrupa i* $\mathbf{R}$ *je specijalni* **-prsten. Drugim rečima,* $(R,\cdot)$ *je polumreža Abelovih grupa eksponenta 2 (tj. Booleovih grupa).*

Dokaz. ($\Rightarrow$) Ovo je već pokazano u prethodnom.

($\Leftarrow$) Pretpostavimo da je $(R,\cdot)$ inverzna polugrupa. Sledi da je $(R,\cdot)$ polumreža Λ Abelovih grupa $\{\mathbf{R}_\lambda \mid \lambda \in \Lambda\}$. Kako je $x^3 = x$ za sve $x \in R$, svaka grupa $\mathbf{R}_\lambda$ ima eksponent 2. Prema tome, važi $x = x^{-1}$ za sve $x \in R$. Tako, $\mathbf{R}$ zadovoljava

$$xy^{-1}x + yx^{-1}y + 2xx^{-1}y + 2yyx^{-1} = 3x^2y + 3y^2x = 0$$

za sve $x, y \in R$. Ovo znači da važi

$$(x+y)(x^{-1}+y^{-1})(x+y) = x+y,$$

za sve $x, y \in R$. Kao i ranije, poslednji identitet implicira da je $\mathbf{R}$ specijalni regularni *-prsten. □

Nula-prsten je, jasno, specijalni involutivni prsten. Takođe, očigledno je da je svaki (nenula) specijalni regularni *-prsten poluprim (u stvari, svi regularni prsteni su poluprim prsteni). Dalje, lako se proverava da ako je (nenula) specijalni regularni *-prsten prim, onda je on polje.

Lema 4.3.8. ([126]) *Polje je specijalni regularni *-prsten ako i samo ako ima 2,3 ili 4 elementa, pri čemu je involucija data sa $x^* = x^{-1}$ za $x \neq 0$ i* $0^* = 0$.

Dokaz. Lema se dokazuje direktnim proveravanjem svih slučajeva. U slučaju karakteristike 3, identitet $x^3 = x$ implicira da polje ima (najviše) 3 elementa. U slučaju karakteristike 2, identitet $x^4 = x$ implicira da polje ima (najviše) 4 elementa, i prema tome ima 2 ili 4 elementa. □

Neka je $\mathbf{R}$ nenula specijalni regularni *-prsten karakteristike 2 ili 3. Videli smo da on uvek zadovoljava identitet oblika $x^{n+1} = x$, i stoga, kao što je to već napomenuto, on jeste (kao prsten) poddirektan proizvod polja (videti [77]). Štaviše, nije teško pokazati da se specijalna involucija (što je zapravo involucija polja) slaže sa takvim poddirektnim proizvodima, tj. da ako $(a_i)_{i\in I}$ pripada posmatranom poddirektom proizvodu, tada to važi i za $(a_i^*)_{i\in I}$. Stoga se $\mathbf{R}$ može razložiti na poddirektan proizvod polja sa involucijom iz prethodne leme, tj. ta involutivna polja su jedini poddirektno nesvodljivi specijalni regularni *-prsteni. Tačnije, važi

Teorema 4.3.9. (Yamada, [126]) *Svaki specijalni regularni *-prsten $\mathbf{R}$ je direktna suma $\mathbf{R}_2 \bigoplus \mathbf{R}_3$ specijalnog regularnog *-prstena $\mathbf{R}_2$ karakteristike 2 i specijalnog regularnog *-prstena $\mathbf{R}_3$ karakteristike 3. Dalje, ako je $\mathbf{R}_2 \neq 0$,* *onda je* $\mathbf{R}_2$ *izomorfan poddirektnom proizvodu polja sa 2 i 4 elementa, dok ako je* $\mathbf{R}_3 \neq 0$, *onda je* $\mathbf{R}_3$ *izomorfan poddirektnom stepenu troelementnog polja (sa involucijama naznačenim u prethodnoj lemi).*

Napominjemo da je materijal u delu o specijalnim regularnim *-prstenima većinom preuzet iz rada M. Yamade [126]. Ovaj rad (naročito gornja teorema) bio je inspiracija za rezultate koje ćeme izložiti u narednom delu o poddirektnoj dekompoziciji i varijetetima proizvoljnih (a ne samo specijalnih) involutivnih prstena koji zadovoljavaju Jacobsonov identitet $x^{n+1} = x$ za neki prirodan broj n.

4.4. Poddirektna razlaganja

U teoriji prstena, kao što je poznato, posebnu ulogu igra čuvena teorema N. Jacobsona koja kaže da je svaki prsten na kome je zadovoljen identitet $x^{n+1} = x^n$, $n \in \mathbb{N}$, komutativan, ili opštije, ako je prsten $\mathbf{R}$ takav da za svako $x \in R$ postoji ceo broj $n(x) > 1$ tako da je $x^{n(x)} = x$, tada je $\mathbf{R}$ komutativan prsten.

Teorema Jacobsona široko uopštava poznatu Wedderburnovu teoremu prema kojoj je svako konačno telo komutativno, tj. polje. Iako Jacobsonova teorema daje samo dovoljan uslov za komutativnost prstena i primenjiva je na relativno usku klasu prstena, njen značaj je u tome što se iz algebarskih osobina elemenata izvodi komutativnost, pa je ta ideja iskorišćena za dobijanje velikog broja opštijih teorema o komutativnosti prstena. Od naših matematičara zapažene rezultate u tom smeru su dobili M. Janjić i V. Perić [91].

Postoji više dokaza Jacobsonove teoreme, i svi ti dokazi se više ili manje svode na činjenicu da je svaki poddirektno nesvodljiv prsten koji za neko n zadovoljava identitet $x^{n+1} = x$ polje.

Naš cilj je da problem poddirektnog razlaganja rešimo za involutivne prstene u kojima važi identitet $x^{n+1} = x$, gde je n fiksan prirodan broj. Ovaj rezultat primenićemo kod konstrukcije mreža varijeteta prstena sa involucijom koji zadovoljavaju zakone datog tipa.

Pošto radimo isljučivo sa komutativnim prstenima, pojmovi antiautomorfizma i automorfizma će se poklapati. Ispostavlja se da konačna polja (sa involucijom) nisu jedini poddirektno nesvodljivi prsteni sa involucijom u kojima važi $x^{n+1} = x$, tako da gore navedeni rezultat (za obične prstene) više ne važi. Pored "internog" fenomena involucije na polju, mi ćemo sresti drugi tip, "spoljašnji", koji opisujemo u kratkim crtama.

Naime, neka je $\mathbf{R}$ prsten, i neka je $\mathbf{R}'$ njegova izomorfna kopija (nad istim nosačem R kao i $\mathbf{R}$). Posmatrajmo direktnu sumu $\mathbf{R} \bigoplus \mathbf{R}'$ i definišimo unarnu operaciju * na toj sumi tako da za sve $r, s \in R$ imamo

$$(r,s)^* = (s,r).$$

Lako se proverava da je na ovaj način direktna suma $\mathbf{R} \bigoplus \mathbf{R}'$ pretvorena u prsten sa involicijom, koji ćemo označavati sa $Ex(\mathbf{R})$. Opisana involucija se često naziva i **razmenjujuća involucija** (videti [106]). Susretaćemo se sa sledećom tipičnom situacijom: prsten sa involucijom $\mathbf{R}$ ima ideal $\mathbf{I}$ tako da je $\mathbf{R}$ direktna suma $\mathbf{I}$ i $\mathbf{I}^*$ (što je takođe ideal u $\mathbf{R}$). Tada je $\mathbf{R} = Ex(\mathbf{I})$. Naravno pod idealom podrazumevamo prstenski ideal (ideale zatvorene za * smo još ranije nazvali *-idealima).

U prvoj glavnoj teoremi ovog paragrafa dokazaćemo da je prsten sa involucijom koji zadovoljava $x^{n+1} = x$ za neki ceo broj $n \geq 1$ poddirektno nesvodljiv ako i samo ako je ili konačno polje sa involucijom (u kom slučaju ćemo diskutovati sve moguće involucije), ili oblika $Ex(\mathbf{F})$ za neko konačno polje $\mathbf{F}$ u kojem važi navedeni identitet. Kasnije, daćemo jedan primer kako se ova informacija može primeniti na konstrukciju mreža podvarijeteta varijeteta involutivnih prstena koji zadovoljavaju $x^{n+1} = x$ za dato n. Naš primer uljučuje sve varijetete specijalnih regularnih *-prstena iz prethodnog paragrafa (naime, posmatraćemo slučaj $n = 6$).

Poznato je da su kongruencije i ideali u "1-1" korespodenciji tako da kongruencija θ u prstenu daje ideal $\mathbf{I}$ od $\mathbf{R}$ tako da $a \in I$ ako i samo ako $(0, a) \in \theta$, i obratno, za svaki ideal $\mathbf{I}$ od $\mathbf{R}$ imamo kongruenciju θ definisanu sa $(a, b) \in \theta$ ako i samo ako $a - b \in I$. Primetimo da se slična simetrija pojavljuje u prstenima sa involucijom što se tiče njihovih *-kongruencija i *-ideala. Naravno, ako je θ *-kongruencija od $\mathbf{R}$, onda je ideal konstruisan kao gore *-ideal, pošto ako $a \in I$, onda $(0, a) \in \theta$, što daje $(0, a^*) \in \theta$ (pošto imamo $0^* = 0$) i onda $a^* \in I$. Obratno, ako je $\mathbf{I}$ *-ideal i θ odgovarajuća kongruencija, onda $(a, b) \in \theta$ implicira $a - b \in I$, tako da je $a^* - b^* = (a - b)^* \in I$. Sledi $(a^*, b^*) \in \theta$. Ova razmatranja sumira

LEMA 4.4.1. *Neka* $\mathbf{R}$ *prsten sa involucijom. Onda su* **-kongruencije i* **-ideali u "1-1" korespondenciji, tako da ideal* $\mathbf{R}$ *nastao iz njegove* **-kongruencije jeste* **-ideal, i obratno.*

Naš glavni rezultat, koji uopštava Yamadinu Teoremu 4.3.9 za proizvoljne involutivne prstene sa identitetom oblika $x^{n+1} = x$, je sledeći.

TEOREMA 4.4.2. *Prsten sa involucijom* $\mathbf{R}$ *je poddirektno nesvodljiv i zadovoljava zakon* $x^{n+1} = x$ *ako i samo ako postoji prost broj* p *i ceo broj* $k \geq 1$ *za koje je* $(p^k - 1)|n$*, tako da je* $\mathbf{R}$ *izomorfan jednoj od sledećih algebri:*

(1) $\mathbf{GF}(p^k)$ *(konačno polje od* p^k *elemenata), sa identičkom involucijom,*

(2) $\mathbf{GF}(p^k)$ *sa involucijom definisanom sa* $x^* = x^{p^m}$*, gde je* k *parno,* $k = 2m$ *(ovo ćemo označavati sa* $\mathbf{GF}^*(p^k)$*),*

(3) $Ex(\mathbf{GF}(p^k))$.

Najpre ćemo izložiti neka pomoćna tvrđenja. Ona čine prve korake ka našem cilju.

Lema 4.4.3. *Neka je* $\mathbf{R}$ *prost prsten takav da je* $R^2 = R$*. Tada* $\mathbf{R}$ *ima jedinicu ako i samo ako je njegov centar* $Z(\mathbf{R})$ *netrivijalan.*

Dokaz. Pretpostavimo da je $z \in Z(\mathbf{R})$, $z \neq 0$. Tada je $zR = R$ i postoji $e \in R$ tako da je $z = ze$. Neka je $r \in R$ proizvoljno. Imamo $zr = zer$, i stoga, $z(r - er) = 0$. Međutim, kako je anihilator elementa z trivijalan (jer je $R^2 = R$ i $\mathbf{R}$ je prost prsten), dobijamo $r = er$, i slično, $r = re$. Prema tome, e je jedinica u $\mathbf{R}$. Obrat je očigledan. □

Involutivni prsteni koji su *-prosti (u smislu da nemaju netrivijalnih *-ideala) su razmatrani u radu Birkenmeiera, Groenewalda i Heatherlyja [6]. Jedan od njihovih rezultata je sledeći.

Propozicija 4.4.4. ([6]) *Neka je* $\mathbf{R}$ **-prost involutivni prsten. Tada je* $\mathbf{R}$ *ili prost kao prsten, ili je* $\mathbf{R} \cong Ex(\mathbf{K})$*, gde je* $\mathbf{K}$ *maksimalan i prost ideal u* $\mathbf{R}$*, pri čemu je* $R^2 \neq 0$ *i* $\mathbf{K}, \mathbf{K}^*$ *su jedini netrivijalni ideali u* $\mathbf{R}$*.*

Lema 4.4.5. *Neka je* $\mathbf{R}$ *poddirektno nesvodiljiv involutivni prsten sa netrivijalnim polinomnim identitetom. Tada je* $\mathbf{R}$ **-prost i ima jedinicu.*

Dokaz. Posmatrajmo presek $\mathbf{H}^*(R)$ svih nenula *-ideala od $\mathbf{R}$. Po datom uslovu poddirektne nesvodljivosti, $\mathbf{H}^*(R)$ je nenula i *-prost. Po prethodnoj propoziciji, on je i prost kao psten, ili je $\mathbf{H}^*(\mathbf{R}) \cong Ex(\mathbf{K})$, gde je $\mathbf{K}$ prost prsten. Iz rezultata rada [105] i Leme 4.4.3, $\mathbf{H}^*(\mathbf{R})$ ima jedinicu e. Stoga, imamo prstensko razlaganje $\mathbf{R} = e\mathbf{R} \bigoplus \mathbf{A}$, gde je $e\mathbf{R} = \mathbf{H}^*(\mathbf{R})$, dok je $\mathbf{A}$ anihilator od $\mathbf{H}^*(\mathbf{R})$. Kako je $\mathbf{H}^*(\mathbf{R})$ zapravo *-ideal, to mora biti i $\mathbf{A}$. Stoga, po datim uslovima, anihilator $\mathbf{A}$ mora biti trivijalan, tj. $\mathbf{R} = e\mathbf{R} = \mathbf{H}^*(\mathbf{R})$, što povlači da je $\mathbf{R}$ *-prost. □

Koristeći gornja tvrđenja, krećemo se polako ka dokazu Teoreme 4.4.2.

LEMA 4.4.6. *Neka je* $\mathbf{R}$ *poddirektno nesvodljiv prsten sa involucijom koji zadovoljava identitet* $x^{n+1} = x$ *za neko* $n \geq 1$. *Tada je* $\mathbf{R}$ *ili konačno polje sa involucijom, ili je* $\mathbf{R} = Ex(\mathbf{F})$ *za neko konačno polje* $\mathbf{F}$.

Dokaz. Prema Lemi 4.4.5, $\mathbf{R}$ je *-prost i ima jedinicu. Naravno, $\mathbf{R}$ je komutativan. Ako je $\mathbf{R}$ prost kao prsten, onda je on polje, štaviše, konačno polje, pošto svi njegovi elementi koreni polinoma $x^{n+1} - x = 0$.

S druge strane, pretpostavimo da je $\mathbf{R} \cong Ex(\mathbf{K})$ sa $\mathbf{K}$ opisanim u gornjoj propoziciji. Tada postoje $e, f \in K$ tako da

$$1 = e + f^*.$$

Sada za proizvoljno $a \in K$ imamo

$$a = ae + af^* = ae,$$

pošto je $af^* = 0$. Dakle, e je jedinica u $\mathbf{K}$. Kako je $\mathbf{K}$ prost i komutativan, $\mathbf{K}$ je konačno polje i lema je dokazana. □

Dokaz Teoreme 4.4.2 Naravno, jasno je da konačno polje $GF(p^k)$ zadovoljava identitet $x^{n+1} = x$ ako i samo ako $(p^k - 1)|n$. Prema tome, ako je $\mathbf{R} = Ex(\mathbf{F})$, dobijamo involutivne prstene opisane sa *(3)*.

S druge strane, pretpostavimo da je $\mathbf{R}$ polje sa involucijom. Poznato je iz teorije polja da je grupa automorfizama konačnog polja $\mathbf{GF}(p^k)$ ciklična grupa od k elemenata i njeni elementi su preslikavanja oblika $x \mapsto x^{p^m}$, $1 \leq m \leq k$. Sada treba odabrati koji od ovih su involucije tj. automorfizmi reda 2. Ovo se dobija iz uslova

$$x = (x^{p^m})^{p^m} = x^{p^{2m}}$$

ili ekvivalentno,

$$x \neq 0 \Rightarrow x^{p^{2m}-1} = 1.$$

Kako je multiplikativna grupa svakog konačnog polja ciklična, gornji uslov će važiti ako i samo ako $(p^k - 1)|(p^{2m} - 1)$, tj. $k|2m$. Pošto je $2m \leq 2k$, imamo dve mogućnosti: ili je $2m = 2k$, tj. $m = k$ i odgovarajuća involucija je identička, (kada imamo slučaj *(1)*), ili $2m = k$, što daje situaciju opisanu u *(2)*.

Obratna implikacija je laka, jer je očigledno da su svi navedeni prsteni sa involucijom *-prosti i prema tome, poddirektno nesvodljivi. Tako, naša teorema je dokazana. □

U narednom, konstruisaćemo mrežu svih varijeteta involutivnih prstena koji zadovoljavaju identitet $x^7 = x$. Razlog zbog kojeg smo se operdelili baš za taj identitet (tj. slučaj $n = 6$) leži u činjenici (koju smo izneli u prethodnom paragrafu) da se svaki specijalni regularni *-prsten $\mathbf{R}$ razlaže u direktnu sumu $\mathbf{R}_2 \bigoplus \mathbf{R}_3$, gde su $\mathbf{R}_2$ i $\mathbf{R}_3$ redom ideali 2-torzionih i 3-torzionih elemenata od $\mathbf{R}$. Kao što smo videli, $\mathbf{R}_2$ zadovoljava $x^4 = x$, dok $\mathbf{R}_3$ zadovoljava $x^3 = x$, tako da na svakom specijalnom regularnom *-prstenu važi upravo $x^7 = x$.

Podsetimo se, Yamada je u [126] pokazao da su poddirektno nesvodljivi specijalni involutivni prsteni oni koje mi označavamo sa $\mathbf{GF}(2)$, $\mathbf{GF}(3)$ i $\mathbf{GF}^*(4)$ (imamo da je $\mathbf{GF}^*(2) = \mathbf{GF}(2)$). Ovaj rezultat se sada lako dobija iz naše Teoreme 4.4.2. Kako nas interesuju involutivni prsteni koji zadovoljavaju $x^7 = x$, dovoljno je potražiti proste brojeve p i pozitivne cele k tako da je $(p^k - 1)|6$, tako da dobijamo $p = 2, 3, 7$ za $k = 1$ i $p = 2$ za $k = 2$. Prema tome, imamo 9 poddirektno nesvodljivih u posmatranom varijetetu (dva za svaki prost broj u slučaju $k = 1$ i tri u poslednjem slučaju), i sada lako biramo one koji zadovoljavaju $x = xx^*x$ kao što je navedeno gore. Primetimo da su tri razmatrana polja sa involucijom jedina koja su pokrivena Teoremom 4.4.2 u kojima se involucija poklapa sa inverzom multiplikativne grupe (kompletirana sa $0^* = 0$). Prema tome, dobijamo sledeću posledicu, koja precizira Yamadine rezultate.

Posledica 4.4.7. *Prsten sa involucijom je specijalan regularan *-prsten ako i samo ako je on poddirektan proizvod polja sa inverznom involucijom* ($a^* = a^{-1}$ *za sve* $a \neq 0$, *i* $0^* = 0$).

Obratimo sada pažnju na neke metode koje mogu da pomognu da se za dato n konstruiše mreža svih varijeteta prstena sa involucijom koji zadovoljavaju $x^{n+1} = x$. Važno je primetiti da svi prsteni sa involucijom navedeni u Teoremi 4.4.2 imaju prostu karakteristiku, i da ima samo konačno mnogo mogućih karakteristika za poddirektno nesvodljive prstene (se involucijom) koji zadovoljavaju $x^{n+1} = x$. Detaljnije, važi

Posledica 4.4.8. *Neka je* $\mathbf{R}$ *poddirektno nesvodljiv prsten sa involucijom koji zadovoljava* $x^{n+1} = x$. *Tada je karakteristika od* $\mathbf{R}$ *prost broj* p *takav da* $(p-1)|n$.

Prema tome, involutivni prsteni dobijeni u Teoremi 4.4.2 prirodno se raspoređuju u nekoliko grupa prema svojim karakteristikama. Prilično je razumno pretpostaviti da takva klasifikacija mora imati nakog uticaja na strukturu mreže varijeteta, čak i ako razmatramo obične prstene bez involucije. Koliko je taj uticaj jak, pokazuje

TEOREMA 4.4.9. *Neka je n pozitivan ceo broj, i neka je $\{p_1, \ldots, p_k\}$ skup svih prostih brojeva p takvih da $(p-1)|n$. Dalje, neka je $\mathbf{L}$ mreža varijeteta svih prstena (sa involucijom) koji zadovoljavaju $x^{n+1} = x$, i neka za prost broj p kao gore, $\mathbf{L}_p$ označava podmrežu od $\mathbf{L}$ koja se sastoji samo od onih varijeteta u kojima je $px = 0$ (tj. varijeteta karakteristike p). Onda je $\mathbf{L} \cong \mathbf{L}_{p_1} \times \mathbf{L}_{p_2} \times \ldots \mathbf{L}_{p_k}$.*

Dokaz. Nije teško videti da je dovoljno dokazati sledeće tvrđenje: neka su $\mathcal{V}_1, \ldots, \mathcal{V}_k$ varijeteti prstena (sa involucijom) koji zadovoljavaju $x^{n+1} = x$, takvi da je $\mathcal{V}_i$ karakteristike p_i, $1 \leq i \leq k$, i neka je $\mathbf{R}$ poddirektno nesvodljiv član $\mathcal{V}_1 \vee \mathcal{V}_2 \vee \ldots \vee \mathcal{V}_k$; onda $\mathbf{R}$ pripada jednom od $\mathcal{V}_i$, $1 \leq i \leq k$. Opštije, pokazaćemo da ako je karakteristika $char(\mathbf{R}) = p_i$ i $\mathbf{R} \in \mathcal{V}_1 \vee \mathcal{V}_2 \vee \ldots \vee \mathcal{V}_k$, onda je $\mathbf{R} \in \mathcal{V}_i$ čak i bez pretpostavke poddirektne nesvodljivosti $\mathbf{R}$.

Pretpostavimo suprotno: da je $\mathbf{R}$ proste karakteristike p_i, ali $\mathbf{R} \notin \mathcal{V}_i$. Iz univerzalne algebre je poznato da je $\mathbf{R}$ homomorfna slika poddirektnog proizvoda članova $\mathcal{V}_1, \ldots, \mathcal{V}_k$ (primetimo da svi faktori imaju proste karakteristike). Neka je $\mathbf{S}$ taj poddirektan proizvod (tako da je $\mathbf{R} = \psi(\mathbf{S})$ za neki homomorfizam ψ); tada je $\mathbf{S}$ potprsten direktnog proizvoda $\mathbf{R}_1 \times \ldots \times \mathbf{R}_\kappa$, gde za sve $1 \leq j \leq k$, $\mathbf{R}_j \in \mathcal{V}_j$.

Jasno, svaki element $a \in S$ može biti napisan kao

$$a = a_1 + \ldots + a_k,$$

tako da je $p_j a_j = 0$ (tj. a_j je p_j-torzioni): dovoljno je uzeti

$$a_j = (0, \ldots, 0, \pi_j(a), 0, \ldots, 0),$$

gde je π_j j-ta kanonička projekcija posmatranog direktnog proizvoda i gde se $\pi_j(a)$ pojavljuje na j-toj koordinati. Označimo

$$q_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k.$$

Kako je $(p_i, q_j) = 1$, postoji ceo broj ℓ_i tako da je $q_i \ell_i \equiv 1(\text{mod } p_i)$. Očigledno, $q_i \ell_i a \in S$. Međutim, mi takođe imamo da je $q_j a_j = 0$ za sve $j \neq i$, što daje $q_i \ell_i a = q_i \ell_i a_i = a_i$. Prema tome, $a_i \in S$. Ali kako je $\pi_i(S) = R_i$ za sve $1 \leq i \leq k$, lako sledi da je $\mathbf{S} = \mathbf{R}_1 \times \ldots \times \mathbf{R}_k$.

Sada, $\psi(\mathbf{S})$ je karakteristike p_i (po pretpostavci). Prema tome, za svako $a \in S$, imamo $p_i \psi(a) = 0$. Prema kineskoj teoremi o ostacima, pošto je $(p_i, p_j) = 1$ za $j \neq i$, možemo naći ceo broj ℓ koji zadovoljava sistem linearnih kongruencija

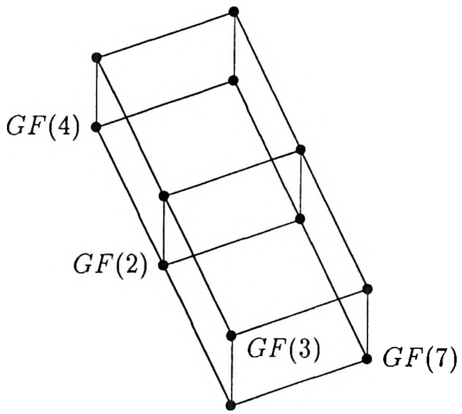
$$p_i \ell \equiv 1(\text{mod } p_i), \quad 1 \leq j \leq k, \ j \neq i.$$

Za takav izbor ℓ, sledi (u odnosu na gornju dekompoziciju za a) $p_i \ell a_i = 0$ i $p_i \ell a_j = a_j$ za sve $j \neq i$, tako da je

$$\begin{aligned} 0 = p_i \ell \psi(a) &= \psi(p_i \ell a) = \psi(a - a_i) = \\ &= \psi(a) - \psi(a_i), \end{aligned}$$

pa je $\psi(a) = \psi(a_i)$. Sledi da se $\mathbf{R} = \psi(\mathbf{S})$ može predstaviti kao homomorfna slika od $\mathbf{R}_i$, što implicira $\mathbf{R} \in \mathcal{V}_i$, kao što se i tražilo. □

Prema tome, zadatak nalaženja mreže varijeteta prstena (sa involucijom) koji zadovoljavaju $x^{n+1} = x$ redukuje se na određivanje struktura mreža varijeteta koji zadovoljavaju $x^{n+1} = x$ i $px = 0$, gde $(p-1)|n$. U primeru koji želimo da prikažemo, imamo $n = 6$, tako da $p \in \{2, 3, 7\}$. Kada razmatramo obične prstene bez involucije, situacija je više ili manje jasna: za $p = 2$ imamo 2 poddirektno nesvodljiva prstena $\mathbf{GF}(2)$ i $\mathbf{GF}(4)$, gde se $\mathbf{GF}(2)$ potapa u $\mathbf{GF}(4)$; za $p = 3$, imamo $\mathbf{GF}(3)$, i za $p = 7$ imamo $\mathbf{GF}(7)$. Prema tome, lako je (koristeći gonju teoremu) videti da postoji 12 varijeteta prstena koji zadovoljavaju $x^7 = x$, i njihov dijagram inkluzije je dat na narednoj slici, koja daje i položaje navedenih polja.



Slika 4.1. Svi varijeteti prstena koji zadovoljavaju $x^7 = x$

Međutim, situacija sa involutivnim prstenima koji zadovoljavaju $x^7 = x$ je nešto komplikovanija, najviše zbog onih karakteristike 2, pošto imamo 5 takvih poddirektno nesvodljivih, dok su karakteristike 3 i 7 lakše za rad. Sledeća lema rešava zadnja dva slučaja.

Lema 4.4.10. *Involutivna polja* $\mathbf{GF}(p^k)$ *i* $\mathbf{GF}^*(p^k)$ *(pod uslovom da ovo poslednje postoji) se mogu potopiti u* $Ex(\mathbf{GF}(p^k))$.

Dokaz. Posmatrajmo sve elemente od $Ex(\mathbf{GF}(p^k))$ koji su fiksirani involucijom. Oni su svi elementi oblika (a,a), $a \in GF(p^k)$, i 0. Lako se pokazuje da ovakvi elementi čine potprsten od $Ex(\mathbf{GF}(p^k))$ snabdeven identičkom involucijom, koji je izomorfan sa $\mathbf{GF}(p^k)$.

S druge strane, pretpostavimo da je $k = 2m$ i označimo $r = p^m$. Posmatrajmo nulu od $Ex(\mathbf{GF}(p^k))$ i elemente ovog involutivnog prstena oblika (a, a^r), $a \in GF(p^k)$. Ovaj skup je očigledno zatvoren u odnosu na množenje i

$$(a,a^r)^* = (a^r, a) = (a^r, a^{r^2}) = (a, a^r)^r.$$

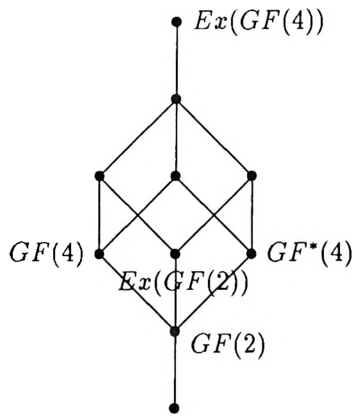
Konačno,

$$(a,a^r) + (b,b^r) = (a+b, a^r + b^r).$$

Međutim, s obzirom da radimo sa karakteristikom p, primenjujući formulu "brucoški san" $(a+b)^p = a^p + b^p$, dobijamo da je $a^r + b^r = (a+b)^r$ i lema je dokazana. □

Iz gornje leme sledi da je mreža varijeteta prstena sa involucijom koji zadovoljavaju $x^7 = x$ i $px = 0$ izomorfna troelementnom lancu kako za $p = 3$, tako i za $p = 7$. Ostaje da se razmotri slučaj $p = 2$, koji je malo složenji.

LEMA 4.4.11. *Mreža varijeteta prstena sa involucijom koji zadovoljavaju $x^7 = x$ i $2x = 0$ data je narednom slikom, sa navedenim položajima poddirektno nesvodljivih.*



Slika 4.2. Svi varijeteti involutivnih prstena koji zadovoljavaju $x^7 = x$ i $2x = 0$

Dokaz. Iz Teoreme 4.4.2 sledi da postoji tačno pet poddirektno nesvodljivih prstena sa involucijom karakteristike 2 koji zadovoljavaju $x^7 = x$. To su: $\mathbf{GF}(2)$, $Ex(\mathbf{GF}(2))$, $\mathbf{GF}(4)$, $\mathbf{GF}^*(4)$ i $Ex(\mathbf{GF}(4))$. Primetimo da svi oni zadovoljavaju $x^4 = x$, pa prema tome možemo raditi sa ovim jednostavnijim zakonom.

Pre svega, $\mathbf{GF}(2)$ se potapa u svaki od četiri preostala prstena sa involucijom sa gornje liste, tako da on generiše jedinstven minimalan varijetet u traženoj mreži.

Da dokažemo da je "srednji deo" Slike 4.2 trodimenzionalna kocka, dovoljno je da dokažemo da za svaki od $Ex(\mathbf{GF}(2))$, $\mathbf{GF}(4)$, $\mathbf{GF}^*(4)$ možemo naći identitet koji ne važi u datoj algebri, ali važi u ostale dve. Razmotrimo sledeće identitete:

(1) $(x^3)^* = x^3$,

(2) $(x^3 + x)^* = x^3 + x^2$,

(3) $(x^3 + x)^* = x^3 + x$.

U $\mathbf{GF}(2)$ imamo $x^3 = x^2 = x$, pa (1) ne važi u $Ex(\mathbf{GF}(2))$, pošto on ima neidentičku involuciju. S druge strane, (1) je tačno u $\mathbf{GF}(4)$ i $\mathbf{GF}^*(4)$, jer za svako a važi $a^3 \in \{0, 1\}$. Tako, a^3 je fiksirano involucijom. Dalje, (2) je očigledno netačno u $\mathbf{GF}(4)$, jer $x = x^2$ nije tačno u ovom polju. Osim toga, (2) važi u $Ex(\mathbf{GF}(2))$, jer se obe strane uvek svode na 0, dok u $\mathbf{GF}^*(4)$ imamo

$$(x^3 + x)^* = (x^3 + x)^2 = x^6 + 2x^4 + x^2 = x^6 + x^2 = x^3 + x^2.$$

Konačno, (3) je tačno u $Ex(\mathbf{GF}(2))$ iz istog razloga kao gore, i trivijalno važi u $\mathbf{GF}(4)$. Međutim, u gornjem lancu idenetiteta se vidi da (3) ne može da važi u $\mathbf{GF}^*(4)$.

Konačno, varijetet $\mathcal{V}$ generisan sa tri malopre razmatrane algebre sadržan je u varijetetu generisanom sa $Ex(\mathbf{GF}(4))$. Da je takva inkluzija prava, pokazuje se identitetom

$$(x^2 + x)^* = x^2 + x,$$

koji važi u $\mathcal{V}$, ali ne važi u $Ex(\mathbf{GF}(4))$, pošto za x možemo uzeti element prvog sumanda u $Ex(\mathbf{GF}(4))$ različit od 0 i jedinice od $\mathbf{GF}(4)$, pa je $x^2 + x$ jedinični element od $\mathbf{GF}(4)$, koji, jasno, nije fiksiran involucijom. Time je lema dokazana. □

Sumirajući, konstruisali smo naš primer, jer je dokazana

TEOREMA 4.4.12. *Varijetet prstena sa involucijom definisan sa $x^7 = x$ ima tačno 90 podvarijeteta, i oni čine mrežu izomorfnu direktnom proizvodu mreže opisane u Lemi 4.4.11 i kvadrata troelementnog lanca.*

Posebno, postoji šest varijeteta prstena sa specijalnom involucijom: to su varijeteti generisani sa **GF**(2), **GF**(3) i **GF***(4), njihov supremum i trivijalan varijetet. Njihova mreža je izomorfna proizvodu dvoelementnog i troelementnog lanca.

Sličnim metodama kao gore prezentiranim, možemo primeniti našu Teoremu 4.4.2 (zajedno sa Teoremom 4.4.9) na nalaženje mreže varijeteta prstena sa involucijom koji zadovoljavaju $x^{n+1} = x$ za proizvoljan pozitivan ceo n.

LITERATURA

[1] Adair, C. L., *Varieties of *-Orthodox Semigroups*, Doktorska disertacija, University of South Carolina, 1979.

[2] Adair, C. L., Bands with an involution, *J. Algebra* **75** (1982), 297–314.

[3] Berberian, S. K., *Baer *-Rings*, Springer-Verlag, Berlin, 1972.

[4] Bernátsky, L., Bloom, S. L., Ésik, Z., Stefanescu, Gh., Equational theories of relations and regular sets, u *Proc. 2nd Int. Colloq. Words, Languages and Combinatorics* (Kyoto, 1992), pp. 40–48, World Scientific, Singapore, 1994.

[5] Birjukov, A. P., Varijeteti idempotentnih polugrupa (ruski), *Algebra i Logika* **9** (1970), 255–273.

[6] Birkenmeier, G. F., Groenewald, N. J., Heatherly, H. E., Minimal and maximal ideals in rings with involution, *Beiträge zur Algebra und Geometrie* **38** (1997), 217–225.

[7] Bloom, S. L., Ésik, Z., Equational axioms for regular sets, *Math. Struct. Comput. Sci.* **3** (1993), 1–24.

[8] Bloom, S.L., Ésik, Z., Stefanescu, Gh., Notes on equational theories of relations, *Algebra Universalis* **33** (1995), 98–128.

[9] Blyth, T. S., Janowitz, M. F., *Residuation Theory*, Pergamon Press, 1972.

[10] Booth, G. L., Groenewald, N. J., Lattices of radicals in involution rings, *Algebra Colloq.* **7** (2000), 17–26.

[11] Bredikhin, D. A., A representation theorem for semilattices, *Proc. Amer. Math. Soc.* **90** (1984), 219–220.

[12] Clifford, A. H., Preston, G. B., *The Algebraic Theory of Semigroups, Vol. I*, Math. Surveys No. 7, Amer. Math. Soc., Providence, 1961.

[13] Conway, J. H., *Regular Algebra and Finite Machines*, Chapman & Hall, London, 1971.

[14] Crvenković, S., On *-regular semigroups, u *Proc. 3rd Algebraic Conf.* (Beograd, 1982), pp. 51–57, Institute of Mathematics, Novi Sad, 1983.

[15] Crvenković, S., Dolinka, I., Varieties of involution semigroups and involution semirings: a survey, u ed. M. Janjić, *Proc. Int. Conf. "Contemporary Developments in Mathematics"* (Banja Luka, 2000), u štampi.

[16] Crvenković, S., Dolinka I., Ésik, Z., The variety of Kleene algebras with conversion is not finitely based, *Theoret. Comput. Sci.* **230** (2000), 235–245.

[17] Crvenković, S., Dolinka, I., Ésik, Z., On equations for union-free regular languages, *Inform. Comput.* **164** (2001), 152–172.

[18] Crvenković, S., Dolinka, I., Vinčić, M., Equational bases for some 0-direct unions of semigroups, *Studia Sci. Math. Hungarica* **36** (2000), 423–431.

[19] Crvenković, S., Dolinka, I., Vinčić, M., On subdirect decomposition and varieties of some rings with involution, *Beiträge zur Algebra und Geometrie*, u štampi.

[20] Crvenković, S., Madarász, R. Sz., On Kleene algebras, *Theoret. Comput. Sci.* **108** (1993), 17–24.

[21] Crvenković, S., Dolinka, I., Vinčić, M., Involution semigroups are not glogaby determined, *Semigroup Forum* **62** (2001), 477–481.

[22] Cvetković, J., *Strukturna svojstva jedne klase polugrupa*, Magistarska teza, Univerzitet u Novom Sadu, 1987.

[23] Dolinka, I., A charaterization of groups in the class of *-regular semigroups, *Novi Sad J. Math.* **29** (1) (1999), 215–219.

[24] Dolinka, I., *O identitetima algebri regularnih jezika*, Doktorska disertacija, Univerzitet u Novom Sadu, Novi Sad, 2000.

[25] Dolinka, I., Remarks on varieties of involution bands, *Comm. in Algebra* **28** (2000), 2837–2852.

[26] Dolinka, I., All varieties of normal bands with involution, *Periodica Math. Hungarica* **40** (2000), 109–122.

[27] Dolinka, I., Minimal varieties of semirings with involution, *Algebra Universalis* **44** (2000), 143–151.

[28] Dolinka, I., On Kleene algebras of ternary co-relations, *Acta Cybernetica* **14** (2000), 583–595.

[29] Dolinka, I., On the lattice of varieties of involution semigroups, *Semigroup Forum* **62** (2001), 438–459.

[30] Dolinka, I., Subdirectly irreducible bands with involution, *Acta Sci. Math. (Szeged)*, u štampi.

[31] Dolinka, I., Idempotent distributive semirings with involution, *priloženo za štampu.*

[32] Dolinka, I., Vinčić, M., Involutorial Płonka sums, *priloženo za štampu.*

[33] Drazin, M. P., Regular semigroups with involution, u *Proc. Symp. on Regular Semigroups* (DeKalb, 1979), pp. 29–46, University of Northern Illinois, DeKalb, 1979.

[34] Easdown, D., Munn, W. D., On semigroups with involution, *Bull. Austral. Math. Soc.* **48** (1993), 93–100.

[35] Ésik, Z., Bernátsky, L., Equational properties of Kleene algebras of relations with conversion, *Theoret. Comput. Sci.* **137** (1995), 237–251.

[36] Evans, T., The lattice of semigroup varieties, *Semigroup Forum* **2** (1971), 1–43.

[37] Fajtlowicz, S., Equationally complete semigroups with involution, *Algebra Universalis* **1** (1972), 355–358.

[38] Fennemore, C. F., All varieties of bands. I, *Math. Nachr.* **48** (1971), 237–252. II, *ibid.*, 253–262.

[39] Foulis, D. J., Baer *-semigroups, *Proc. Amer. Math. Soc.* **11** (1960), 648–655.

[40] Gerhard, J. A., The lattice of equational classes of idempotent semigroups, *J. Algebra* **15** (1970), 195–224.

[41] Gerhard, J. A., Subdirectly irreducible idempotent semigroups, *Pacific J. Math.* **39** (1971), 669–676.

[42] Gerhard, J. A., Petrich, M., Free involutorial completely simple semigroups, *Canad. J. Math.* **37** (1985), 281–295.

[43] Gerhard, J. A., Petrich, M., Free bands and free *-bands, *Glasgow J. Math.* **28** (1986), 161–179.

[44] Golan, J. S., *The Theory of Semirings with Applications in Mathematics and Theoretical Computer Science*, Longman Scientific and Techincal, New York, 1993.

[45] Goodearl, K. R., *von Neumann Regular Rings*, Pitman, San Francisco, 1979.

[46] Graczyńska, E., On normal and regular identities, *Algebra Universalis* **27** (1990), 387–397.

[47] Heatherly, H. E., Lee, E. K. S., Wiegandt, R., Involutions on universal algebras, u eds. Saad, G., Thomsen, M. J, *.Nearrings, Nearfields and K-Loops* (Hamburg, 1995), pp. 269–282, Kluwer, Dordrecht, 1997.

[48] Herstein, I. N., An elementary proof of a theorem of Jacobson, *Duke Math. J.* **21** (1954), 45–48.

[49] Herstein, I. N., *Topics in Ring Theory*, Chicago Lectures in Mathematics, University of Chicago Press, 1969.

[50] Herstein, I. N., On rings with involution, *Canad. J. Math.* **26** (1974), 794–799.

[51] Herstein, I. N., *Topics in Algebra*, John Wiley & Sons, New York, 1975.

[52] Herstein, I. N., *Rings with Involution*, Chicago Lectures in Mathematics, University of Chicago Press, 1976.

[53] Herstein, I. N., Montgomery, S., Invertibile and regular elements in rings with involution, *J. Algebra* **25** (1973), 390–400.

[54] Hobby, D. and McKenzie, R. N., *The Structure of Finite Algebras*, Contemporary Mathematics Series, Vol. 76, Amer. Math. Soc., Providence, 1988.

[55] Hoehnke, H. J., Über antiautomorphe und involutorische primitive Halbgruppen, *Czechoslovak J. Math.* **15 (90)** (1965), 50–63.

[56] Howie, J. M., *Fundamentals of Semigroup Theory*, Oxford University Press, 1995.

[57] Jacobson, N., *Structure of Rings*, AMS Colloq. Publications, Vol. 37, Amer. Math. Soc., Providence, 1956.

[58] Jónsson, B., The theory of binary relations, u eds. Andréka, H. et al., *Algebraic Logic* (Budapest, 1988), Colloq. Math. Soc. János Bolyai, Vol. 54, pp. 245–292, North-Holland, Amsterdam, 1991.

[59] Kalicki, J., Scott, D., Equational completeness of abstract algebras, *Indag. Math.* **17** (1955), 650–659.

[60] Kalman, J. A., Subdirect decomposition of distributive quasilattices, *Fund. Math.* **71** (1971), 161–163.

[61] Kharlampovich, O. G., Sapir M. V., Algorithmic problems in varieties, *Int. J. Algebra Comp.* **5** (1995), 379–602.

[62] Kleiman, E. I., On bases of identities of Brandt semigroups, *Semigroup Forum* **13** (1977), 209–218.

[63] Kobayashi, Y., Semilattices are globaly determinied, *Semigroup Forum* **29** (1984), 127–222.

[64] Kozen, D., A representation theorem for models of *-free PDL, Report RC 7864, IBM Research, Yorktown Heights, 1979.

[65] Kozen, D., On Kleene algebras and closed semirings, u *Mathematical Foundations of Computer Science*, Lecture Notes in Comput. Sci., Vol. 452, pp. 26–47, Springer-Verlag, New York, 1990.

[66] Kozen, D., A completeness thoerem for Kleene algebras and the algebra of regular events, *Inform. Comput.* **110** (1994), 366–390.

[67] Kozen D., *Automata and Computability*, Springer-Verlag, 1997.

[68] Krob, D., Complete systems of $\mathcal{B}$-rational identities, *Theoret. Comput. Sci.* **89** (1991), 207–343.

[69] Kuich, W., Salomaa, A., *Semirings, Automata and Languages*, EATCS Monographs on Theoret. Comput. Sci., Springer-Verlag, New York, 1986.

[70] Kuřil, M., Polák, L., On varietes of semilattice ordered semigroups, *rukopis*.

[71] Lakser, H., Padmanabhan, R., Platt, C. R., Subdirect decomposition of Płonka sums, *Duke Math. J.* **39** (1972), 485–488.

[72] Lanski, C., Rings with involution whose symmetric elements are regular, *Proc. Amer. Math. Soc.* **33** (1972), 264–270.

[73] Madarász, R. Sz., Crvenković, S., *Relacione algebre*, Matematički Institut SANU, Beograd, 1992.

[74] Maeda, F., Maeda S., *Theory of Symetric Lattices*, Springer-Verlag, New York, 1970.

[75] McKenzie, R., *The Representation of Relation Algebras*, Doktorska disertacija, University of Colorado, 1966.

[76] McKenzie, R., An algebraic version of categorical equivalence for varieties and more general algebraic categories, u *Algebra and Logic* (Pontignano, 1994), Lecture Notes in Pure and Appl. Math., Vol. 180, pp. 211–243, Marcel Dekker, New York, 1996.

[77] McKenzie, R., McNulty, G., Taylor, W., *Algebras, Lattices, Varieties, Vol. I*, Wadsworth & Brooks/Cole, Monterey, 1987.

[78] McKenzie, R., Romanowska, A., Varieties of ·-distributive bisemilattices, u *Contributions to General Algebra* (Klagenfurt, 1978), pp. 213–218, Verlag J. Heyn, Klagenfurt, 1979.

[79] Meljnik, I. I., Nilpotentne translacije varijeteta (ruski), *Mat. Zametki* **14** (1973), 703–712.

[80] Mogiljanskaja E. M., Non-isomorphic semigroups with isomorphic semigroups of subsets, *Semigroup Forum* **6** (1973), 330–333.

[81] Nambooripad, K. S. S., Pastijn, F. J., Regular involution semigroups, u eds. Pollák, Gy., Schwarz, Št., Steinfeld, O., *Semigroups* (Szeged, 1981), Colloq. Math. Soc. János Bolyai, Vol. 39, pp. 199–249, North-Holland, Amsterdam, 1985.

[82] Németi, I., Every free algebra in the variety generated by the representable dynamic algebras is separable and representable, *Theoret. Comput. Sci.* **17** (1982), 343–347.

[83] Neumann, H., *Varieties of Groups*, Springer-Verlag, Berlin, 1963.

[84] Nordahl, T. E., Scheiblich, H. E., Regular *-semigroups, *Semigroup Forum* **16** (1978), 369–377.

[85] Pastijn, F. J., Constructions of varieties that satisfy the amalgamation property and the congruence extension property, *Studia Sci. Math. Hungarica* **17** (1982), 101–111.

[86] Pastijn, F., Idempotent distributive semirings II, *Semigroup Forum* **26** (1983), 151–166.

[87] Pastijn, F., Guo, Y. Q., The lattice of idempotent distributive semiring varieties, *Science in China (Ser. A)* **42** (1999), 785–804.

[88] Pastijn, F., Romanowska, A., Idempotent distributive semirings I, *Acta Sci. Math. (Szeged)* 44 (1982), 239–253.

[89] Pastijn, F., Zhao, X., Green's $\mathcal{D}$-relation for the multiplicative reduct of an idempotent semiring, *Arch. Math. (Brno)* **36** (2000) 77–93.

[90] Penrose, R., A generalized inverse for matrices, *Proc. Cambridge Phil. Soc.* **51** (1955), 406–413.

[91] Perić, V., On rings with polynomial identity $x^n - x = 0$, *Publ. Inst. Math. (Beograd)* **34 (48)** (1983), 165–167.

[92] Perkins, P., Bases of equational theories of semigroups, *J. Algebra* **11** (1969), 298–314.

[93] Petrich, M., *Introduction to Semigroups*, Merrill, Columbus, 1973.

[94] Petrich, M., *Inverse Semgroups*, John Wiley & Sons, New York, 1984.

[95] Petrich, M., Certain varieties of completely regular *-semigroups, *Boll. U.M.I., Sect. B (Ser. VI)* **4** (1985), 343–370.

[96] Płonka, J., On distributive quasi-lattices, *Fund. Math.* **60** (1967), 191–200.

[97] Płonka, J., On a method of construction of abstract algebras, *Fund. Math.* **61** (1967), 183–189.

[98] Płonka, J., On equational classes of abstract algebras defined by regular identities, *Fund. Math.* **64** (1969), 241–247.

[99] Polák, L., A solution of the word problem for free *-regular semigroups, *J. Pure Appl. Algebra* **157** (2001), 107–114.

[100] Polin, S. V., Minimalni varijeteti poluprstena (ruski), *Mat. Zametki* **27** (1980), 527–537.

[101] Redko, V. N., O definišućim relacijama za algebru regularnih događaja (ruski), *Ukrain. Mat. Ž.* **16** (1964), 120–126.

[102] Reilly, N. R., A class of regular *-semigroups, *Semigroup Forum* **18** (1979), 385–386.

[103] Romanowska, A., Free idempotent distributive semirings with a semilattice reduct, *Math. Japonica* **27** (1982), 467–481.

[104] Romanowska, A., Idempotent distributive semirings with a semilattice reduct, *Math. Japonica* **27** (1982), 483–493.

[105] Rowen, L. H., Some results on the center of a ring with polynomial identity, *Bull. Amer. Math. Soc.* **79** (1973), 219–223.

[106] Rowen, L. H., *Ring Theory, Vol. I*, Academic Press, London, New York, 1988.

[107] Sapir, M. V., Inherently non-finitely based finite semigroups, *Mat. Sb.* **133** (1987), 154–166.

[108] Scheiblich, H. E., Projective and injective bands with involution, *J. Algebra* **109** (1987), 281–291.

[109] Schein, B. M., O teoriji uopštenih grupa (ruski), *Dokl. Akad. Nauk SSSR* **153** (1963), 296–299.

[110] Schein, B. M., Atomične poluskupine i involutivne polugrupe (ruski). *Izv. Visš. Uč. Zav. Mat.* **3** (1965), 172–184.

[111] Schein, B. M., Representation of involuted semigroups by binary relations, *Fund. Math.* **82** (1974), 121–141.

[112] Skornjakov, L., *Dedekindove mreže sa komplementom i regularni prsteni* (ruski), Gos. Izdat. Fiz. Mat. Lit., Moskva, 1961.

[113] Szendrei, Á., A survey on strictly simple algebras and minimal varieties, u *Universal Algebra and Quasigroup Theory*, pp. 209–239, Heldermann Verlag, Berlin, 1992.

[114] Tamura, T., Shafer, J., Power semigroups, *Math. Japocica* **12** (1967), 25–32.

[115] Tarski, A., Equational logic and equational theories of algebras, u eds. Schnodt, H. A. et al., *Contributions to Mathematical Logic: Proc. Logic Colloq.* (Hanover, 1966), pp. 275–288, North-Holland, Amsterdam, 1968.

[116] Tiščenko, A. V., The finiteness of a base of identities for five-element monoids, *Semigroup Forum* **20** (1980), 171–186.

[117] Trahtman, A. N., Baza identiteta petoelementne Brandtove polugrupe (ruski), *Mat. Zap. Ural. Gos. Univ.* **12** (1981), 147–149.

[118] Vagner, V. V., Uopštene skupine i uopštene grupe sa tranzitivnom relacijom kompatibilnosti (ruski), *Uč. Zap. Saratov. Univ. Meh.-Mat.* **70** (1961), 25–39.

[119] Važenjin, J. M., O globalnoj natpolugrupi simetrične polugrupe (ruski), *Mat. Zap. Ural. Gos. Univ.* **9** (1947), 3–10.

[120] Vinčić, M., *Involutivne polugrupe*, Magistarska teza, Univerzitet u Novom Sadu, Novi Sad, 1999.

[121] Vinčić, M., Global determinism of *-bands, *Facta Univ. Niš, Ser. Math. Inform.*, u štampi.

[122] von Neumann, J., On regular rings, *Proc. Nat. Acad. Sci.* **22** (1936), 707–713.

[123] Wiegandt, R., On the structure of involution rings with chain condition, *Vietnam J. Math.* **21** (1993), 1–12.

[124] Yamada, M., Regular semigroups whose idempotents satisfy permutation identities, *Pacific J. Math.* **21** (1967), 371–392.

[125] Yamada, M., Finitely generated free *-bands, *Semigroup Forum* **29** (1984), 13–16.

[126] Yamada, M., On the multiplicative semigroups of regular rings with special involution, *Simon Stevin* **59** (1985), 51–57.

Indeks

Milovan Vinčić je rođen 11. novembra 1949. u Udetinu kod Dvora na Uni, Republika Hrvatska (tada SR Hrvatska, SFRJ). Osnovnu školu je završio u Rujevcu kod Dvora, a gimnaziju u Bosanskom Novom (sada Novi Grad, Republika Srpska). 1976. završio je teorijsku matematiku (zvanje diplomirani inženjer teorijske matematike) na Prirodno-matematičkom fakultetu u Zagrebu, pri čemu je poslednja godina studija bila uz rad.

Školske 1975/76. godine predavao je matematiku u Školskom Centru u Dvoru na Uni. U toku služenja vojnog roka 1976/77. u Rajlovcu kod Sarajeva, bio je asistent matematike na Vojnoj Akademiji. Bio je profesor matematike u bihaćkoj Gimnaziji u periodu 1977–1992. Učesnik je bosansko-hercegovačkog rata 1992–1995. Oktobra 1995. se zaposlio kao asistent-pripravnik na Mašinskom fakultetu u Banja Luci. Danas radi honorarno i na Šumarskom, Građevinskom i Prirodno-matematičkom fakultetu u Banja Luci. Do novembra 1998. položio je sve ispite predviđene planom poslediplomskih studija, smer Algebra i matematička logika, sa prosekom ocena 9,40. Magistrirao je na Prirodno-matematičkom fakultetu u Novom Sadu 30. juna 1999., sa magistarskim radom "Involutivne polugrupe". Oktobra 1999. izabran je za asistenta Mašinskog fakulteta u Banja Luci.

Autor je ili koautor 9 naučnih radova, više stručnih radova i jednog univerzitetskog udžbenika. Oblasti njegovog naučnog interesovanja obuhvataju univerzalnu algebru, teoriju polugrupa, teoriju poluprstena i prstena i konstruktivističku teoriju skupova.

Otac je dvoje dece.

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
Ključna dokumentacijska informacija

Redni broj (RBR):

Identifikacioni broj (IBR):

Tip dokumentacije (TD): monografska dokumentacija

Tip zapisa (TZ): tekstualni štampani materijal

Vrsta rada (VR): doktorska disertacija

Autor (AU): mr Milovan Vinčić

Mentor (MN): dr Siniša Crvenković, redovni profesor

Naslov rada (NR): "Involutivne algebre"

Jezik publikacije (JP): srpski

Jezik izvoda (JI): srpski/engleski

Zemlja publikovanja (ZP): Republika Srpska, Bosna i Hercegovina

Uže geografsko područje (UGP): -

Godina (GO): 2001.

Izdavač (IZ): autorski reprint

Mesto i adresa (MA): Banja Luka, Tarasa Ševčenka 4

Fizički opis rada (FO): 5/vii+115/126/0/10/0/0

Naučna oblast (NO): matematika

Naučna disciplina (ND): algebra

Predmetna odrednica/Ključne reči (PO): univerzalna algebra; involucija, involutivne algebre, involutivne polugrupe, involutivni poluprsteni, involutivni prsteni, varijetet, mreže varijeteta.

UDK:

Čuva se (ČU): Biblioteka Instituta za matematiku, Prirodno-matematički fakultet, Novi Sad, Trg Dositeja Obradovića 4

Važna napomena (VN): -

Izvod (IZ): Tema ove disertacije je *involucija* u algebarskim strukturama. Involucije su bijektivna preslikavanja koja se poklapaju sa svojim inverznim funkcijama. One se pojavljuju u skoro svim oblastima matematike: podsetimo se samo projektivne geometrije, teorije algebarskih krivih, inverzije u euklidskoj geometriji i njenog značaja za modele hiperboličke geometrije, teorije matrica i drugih disciplina.

Cilj disertacije je da prikaže teoriju involutivnih algebri, tj. neke rezultate u okviru te teorije. Najviše su istraženi odnosi između algebarskih zakona i involucije, i ti odnosi daju jednu sasvim novu algebarsku teoriju.

Materijal je podeljen u četiri dela. U prvom delu se posmatraju tzv. Płonkine sume. Ispostavilo se da su mnoge klasične konstrukcije u algebri samo specijalni slučajevi Płonikih suma. Kako bismo ih prilagodili izučavanju involutivnih algebri, ove sume su modifikovane, tako da dobijamo involutivne Płonkine sume. U radu su ispitane neke osobine takvih suma.

U drugom delu istražujemo involutivne polugrupe. Između ostalog, dokazano je da je klasa regularnih *-traka globalno određena.

Treći deo prikazuje neke od najnovijih rezultata u oblasti involutivnih poluprstena.

Najzad, poslednji, četvrti deo govori o involutivnim prstenima. Posmatrani su neki poddirektno nesvodljivi prsteni sa involucijom, i dokazan je involutivni analogon čuvene teoreme N. Jacobsona.

Datum prihvatanja teme od strane NN Veća (DP): 22.6.2000.

Datum odbrane (DO):

Članovi komisije (KO):

Predsednik: dr Igor Dolinka, docent, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Mentor: dr Siniša Crvenković, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Član: dr Đura Paunić, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Član: dr Gradimir Vojvodić, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Član: dr Milan Janjić, vanredni profesor, Prirodno-matematički fakultet, Univerzitet u Banja Luci

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCE
Key words documentation

Accession number (ANO):

Identification number (INO):

Documentation type (DT): Monographic documentation

Type of record (TR): Textual printed material

Contents code (CC): Ph.D. thesis

Author (AU): Milovan Vinčić, M.Sc.

Mentor (MN): Siniša Crvenković, Ph.D., Full Professor

Title (TI): "Involution Algebras"

Language of text (LT): Serbian

Language of abstract (LA): Serbian/English

Country of publication (CP): Republic of Srpska, Bosnia and Herzegovina

Locality of publication (LP): –

Publication year (PY): 2001

Publisher (PU): Author's reprint

Publication place (PP): Banja Luka, Tarasa Ševčenka 4

Physical description (PD): 5/vii+115/126/0/10/0/0

Scientific field (SF): Mathematics

Scientific discipline (SD): Algebra

Subject/Key words (SKW): Universal Algebra; involution, involution algebras, involution semigroups, involution semirings, involution rings, variety, lattices of varieties.

UC:

Holding data (HD): The Library of the Institute of Mathematics, Faculty of Science, Novi Sad, Trg Dositeja Obradovića 4

Notes (N): –

Abstract (AB): The topic of this dissertation is *involution* in algebraic structures. Involutions are bijective mappings which coincide with their inverse functions. They appear in almost all mathematical disciplines: recall projective geometries, theory of algebraic curves, inversion in euclidean geometry and its importance in the models of hyperbolic geometry, theory of matrices and other parts of mathematics.

The aim of this dissertation is to present the theory of involution algebras, i.e. some results in the frame of that theory. We are investigating the relationship of algebraic laws and involution, which together give a new algebraic theory.

The material is divided into four parts. In the first part, we are considering the so called Płonka sums. It turned out that many classical constructions in algebra are special cases of Płonka sums. We modify these sums in order to make them applicable to involution algebras, and so we obtain the involutorial Płonka sums, whose properties are explored.

In the second part, we investigate involution semigroups. Among other things, it is shown that the class of regular *-bands is globally determined.

The third part is about semirings with involution. We review some of the latest results in the area of involution semirings.

The final, fourth part is about rings with involution. We are considering some subdirectly irreducible involution rings and prove an involutorial analogue of the well-known theorem of N. Jacobson.

Accepted by the Scientific Board of the Faculty on (ASB): June 22, 2000

Defended (DE):

Thesis defend board (DB):

President: dr Igor Dolinka, Assistant Professor, Faculty of Science, University of Novi Sad

Mentor: dr Siniša Crvenković, Full Professor, Faculty of Science, University of Novi Sad

Member: dr Đura Paunić, Full Professor, Faculty of Science, University of Novi Sad

Member: dr Gradimir Vojvodić, Full Professor, Faculty of Science, University of Novi Sad

Member: dr Milan Janjić, Associate Professor, Faculty of Science, University of Banja Luka