UNIVERZITET U NOVOM SADU

PRIRODNO-MATEMATIČKI FAKULTET

BLAGOJE CEROVIĆ

NEKE KLASE REGULARNIH PRSTENA

(Doktorska disertacija)

NOVI SAD, 1982.

S A D R Ž A J

UVOD

Pojam regularnosti za elemente prstena uveo je J.von Neuman [39] , i od tada klasa regularnih prstena, kao i klasa regularnih semigrupa, zauzima značajno mjesto u teoriji prstena i semigrupa.

U ovome radu ispitivane su neke klase regularnih prstena, i to: klasa prstena za čiji svaki element x važi $x^n=x$, klasa (m,n)-anti-inverznih prstena, kao i klasa anti-inverznih prstena.

Klase (m,n)-anti-inverznih prstena i anti-inverznih prstena i njihova metodologija ispitivanja oslanjaju se na analognim metodama koje su korišćene u [3] , [4] , [5] , [6] , [14] , [34] i [36] za (m,n)-anti-inverzne semigrupe i anti-inverzne semigrupe. Zbog toga su u Glavi I navedeni osnovni pojmovi i glavni rezultati iz ovih radova.

U Glavi I, takodje, navedeni su neki poznati rezultati o prstenima, idealima prstena, semiprostim prstenima i konačnim poljima, koji su korišćeni u narednim glavama ovoga rada. Ovdje su uglavnom korišćene monografije L.A.Kalužnina [29], I, Lambeka [31], V. Perića [43] i [44] i M. Petrića [45].

U Glavi II ispitivana je klasa prstena $\mathfrak{R}_n$, definisana sa

$$Re\,\mathfrak{R}_n \Longleftrightarrow (\forall x\in R)(x^n=x) \quad .$$

Iz Teoreme Jacobsona slijedi da su prsteni iz klase $\mathfrak{R}_n$ komutativni, a iz definicije regularnosti elementa prstena, slijedi da su regularni.

Svaki ideal prstena $Re\mathfrak{R}_n$ je idempotentan (Lema 2.1.5), a odavde slijedi da prsten $Re\mathfrak{R}_n$ nema nilpotentnih ideala različitih od nulaideala, tj. klasa $\mathfrak{R}_n$ je podklasa klase semiprostih prstena (Propozicija 2.1.1).

Aditivna karakteristika elemenata prstena $Re\mathfrak{R}_n$ okarakterisana je sa

$$(\forall x \in R)(\ (2^n-2)x=0)\ ,$$

(Lema 2.1.1).

Za proizvoljan element x prstena $Re\mathfrak{R}_n$ element x^{n-1} je idempotent (Lema 2.2.1). Ova činjenica je dokazana i u [4] za (m,n)-anti-inverzne semigrupe i dokaz je analogan.

Razmatrani su ortogonalni idempotenti prstena $Re\mathfrak{R}_n$ i, u vezi sa tim, dat je potreban i dovoljan uslov kada je prsten $Re\mathfrak{R}_n$ polje (Propozicija 2.2.1).

Posebna pažnja je posvećena *m-skupovima* (skup medjusobno ortogonalnih idempotenata E za koji ne postoji idempotent $e \in R\setminus E$ ortogonalan sa svim idempotentima iz E) i *maksimalnom m-skupu* (m-skup $M=\{e_i : i \in I\}$, takav da za svako $e_i \in M$ jedini idempotenti ideala Re_i su 0 i e_i). Dat je potreban i dovoljan uslov kada je skup medjusobno ortogonalnih idempotenata m-skup (Lema 2.2.3) a zatim je dokazano da ako je $E=\{e_1,\ldots,e_s\}$ m-skup, prsten R je direktna suma ideala $Re_i, e_i \in E$ (Propozicije 2.2.2).

Za slučaj kada idempotent e_i pripada m-skupu E, ideal Re_i nije obavezno minimalan ideal. Medjutim, za svaki idempotent e_i iz maksimalnog m-skupa M ideal Re_i je minimalan i, još više, ideali $Re_i, e_i \in M$, su jedini minimalni ideali prstena R(Propozicija 2.3.1). Na ovaj način pomoću maksimalnog m-skupa M može se okarakterisati skup svih minimalnih ideala prstena $Re\mathfrak{R}_n$. Inače, maksimalan m-skup je jedinstven (Posljedica Propozicije 2.3.1) i za slučaj kada su svi m-skupovi prstena $Re\mathfrak{R}_n$ konačni, maksimalan m-skup je m-skup sa najvećim brojem elemenata.

Prsteni iz klase $\mathfrak{R}_n$, čiji je maksimalan m-skup konačan, mogu se okarakterisati na sljedeći način: ako je maksimalan m-skup prstena $Re\mathfrak{R}_n$ konačan, tada je prsten R direktna suma svih svojih minimalnih ideala (Propozicija 2.3.3). Takodje, prsten $Re\mathfrak{R}_n$ sa konačnim maksimalnim m-skupom je prsten sa jedinicom (Propozicija 2.3.4) i za takve prstene moguće je okarakterisati skup svih idempotenata (Propozicija 2.3.4).

Kako su prsteni iz klase $\mathfrak{R}_n$ semiprosti, to su njihovi minimalni ideali polja, koja takodje pripadaju klasi $\mathfrak{R}_n$. Zbog toga je bilo od značaja odrediti sva polja koja pripadaju klasi $\mathfrak{R}_n$. Prema Lemi 2.1.1, klasi $\mathfrak{R}_n$ ne mogu pripadati beskonačna polja karakteristike nula. U Teoremi 2.4.1 je dokazano da polje $GF(p^m)$ pripada klasi $\mathfrak{R}_n$ ako i samo ako $p|2^n-2$ i ako postoji broj $k \geq 0$, takav da je $n=(k+1)p^m-k$. Na taj način ova teorema predstavlja karakterizaciju konačnih polja iz klase $\mathfrak{R}_n$. U Primjeru 2.4.2 odredjena su sva polja koja pripadaju klasama $\mathfrak{R}_3$, $\mathfrak{R}_4$ i $\mathfrak{R}_5$.

U Glavi III ispitivana je klasa $\mathcal{AR}_{m,n}$ (m,n)-anti-inverznih prstena, definisana sa

$$\text{Re}\ \mathcal{AR}_{m,n} \Longleftrightarrow (\forall x \in R)(\exists y \in R)(x^m = y^m = (xy)^m \wedge x^n = x) \ .$$

Kako je klasa $\mathcal{AR}_{m,n}$ podklasa klase $\mathcal{R}_n$, to su prsteni iz klase $\mathcal{AR}_{m,n}$ komutativni, regularni i semiprosti.

U ovoj glavi je dokazano da za slučaj kada je m> n postoji broj $m' \leq n$, takav da je klasa $\mathcal{AR}_{m,n}$ jednaka klasi $\mathcal{AR}_{m',n}$. Zbog toga je dalje ispitivana klasa $\mathcal{AR}_{m,n}$ za $m \leq n$.

U tački 3.2 Glave III razmatrana su neka svojstva (m,n)--anti-inverznih elemenata. Dokazano je (Propozicija 3.2.1) da je (m,n)-anti-inverznost relacija ekvivalencije prstena R. Dalje je dokazano da je x^m sopstvena jedinica elementa x i ako $y \in A_x$ (A_x skup (m,n)-anti-inverznih elemenata elementa x), tada je $e_x = e_y$. Takodje, (m,n)-anti-inverzni elementi imaju istu aditivnu karakteristiku (Lema 2.3.1).

Prsten $\text{Re}\ \mathcal{AR}_{m,n}$ je polje ako i samo ako je $A_x = R \setminus \{0\}$, za svako $x \in R$ (Propozicija 3.2.2). U Propoziciji 3.2.3 dat je uslov kada iz $y \in A_x$ slijedi $ky \in A_x$ i dokazano je da je skup A_x zatvoren u odnosu na operaciju "·".

Za (m,n)-anti-inverzne semigrupe važi, (Teorema 2.1. 4), da za bilo koji podskup skupa A_x, skup $x \in A_x$ generiše grupu. Za (m,n)-anti-inverzne prstene skup A_x ne generiše polje. Jedino u slučaju kada x^m pripada maksimalnom m-skupu, tada je $A_x \setminus \{0\}$ polje (Propozicija 3.2.4).

U Teoremi 3.3.1 dokazano je da važi $\mathfrak{AR}_{m,n} = \mathfrak{AR}_{m,m+r}$, gdje je $n=mq+r$, $0<r<m$. Sada je bilo moguće odrediti potreban i dovoljan uslov kada Re $\mathfrak{AR}_{m,m+r}$. Naime, prsten Re $\mathfrak{AR}_{m,m+r}$ ako i samo ako za svaki njegov element x važi $x^{m+1}=x$ i $x^r=x$ (Teorema 3.3.2).

Klasa Bulovih prstena $\mathfrak{B}$ je podklasa klase $\mathfrak{AR}_{m,n}$, za sve prirodne brojeve m i n. U tački 3.4 ispitivani su neki slučajevi kada je $\mathfrak{AR}_{m,n}=\mathfrak{B}$. Kako je $\mathfrak{AR}_{m,m}=\mathfrak{B}$, to u Teoremama 3.3.1 i 3.3.2 nije razmatran slučaj kada je r=0.

U Glavi IV ispitivana je klasa $\mathfrak{AR}$ anti-inverznih prstena, definisana sa

$$\mathrm{Re}\,\mathfrak{AR} \iff (\forall x\in R)(\exists\, y\in R)(xyx=y \wedge yxy=x) .$$

Prsteni iz klase $\mathfrak{AR}$ su takodje komutativni i regularni.

U Propoziciji 4.1.1 dat je potreban i dovoljan uslov, kada je Re $\mathfrak{AR}$. Naime, Re $\mathfrak{AR}$ ako i samo ako za svako $x\in R$ važi $x^3=x$. Odavde slijedi da je $\mathfrak{AR}=\mathfrak{AR}_{2,3}$ i da je $y\in R$ anti-inverzan element za $x\in R$ ako i samo ako je y (2,3)-anti-inverzan za element x (Propozicija 4.1.2).

U tački 4.2 odredjeni su neki slučajevi kada je $\mathfrak{AR}_{m,m+r}\subset\mathfrak{AR}$.

U tački 4.3 razmatrana je klasa prstena $Q\mathfrak{AR}$ čiji je svaki pravi potprsten iz $\mathfrak{AR}$. Od polja, jedino polja $GF(2^m)$ i $GF(3^m)$, gdje je m prost broj, pripadaju klasi $Q\mathfrak{AR}$ (Propozicija 4.3.2).

U propoziciji 4.3.3 je dokazano da $R_1 x R_2 e Q\mathfrak{AR}$ ako i samo ako oba prstena R_1 i R_2 pripadaju klasi $\mathfrak{AR}$.

U Teoremi 4.4.1 odredjena je bazisna klasa u smislu Ljapina za klasu $\mathfrak{AR}$ u odnosu na klasu $\mathfrak{R}$ svih prstena. Tu klasu sačinjavaju trivijalan prsten, zatim $Z_2, Z_3, Z_6, R_9, R_{18}$ i R_{36}, gdje su prsteni R_9, R_{18} i R_{36} prsteni od 9,18 odnosno 36 elemenata opisani u tački 4.4.

U tački 4.5 odredjena je bazisna klasa u smislu Ljapina za klasu $\mathfrak{R}_4$ u odnosu na klasu svih prstena $\mathfrak{R}$. Nju sačinjavaju trivijalan prsten, polja Z_2 i GF(4) i prsten $R_8^{\sim}$ od 8 elemenata, koji je opisan u ovome dodatku.

Neki rezultati iz Glave IV objavljeni su u [8].

Profesoru dr Svetozaru Miliću zahvaljujem na pomoći i savjetima koje mi je dao pri izradi ovog rada i koji su mi bili od izuzetne koristi.

GLAVA I

NEKI POJMOVI I REZULTATI O ANTI-INVERZNIM SEMIGRUPAMA I PRSTENIMA

1.1. KLASA ANTI-INVERZNIH SEMIGRUPA

U radovima [3], [5] i [34] razmatrana je klasa $\mathfrak{A}$ *anti--inverznih semigrupa*, tj. klasa takvih semigrupa S za koje važi

$$(\forall x \in S)(\exists y \in S)(xyx = y \wedge yxy = x) .$$

Za element y tada kažemo da je *anti-inverzan* elementu x.

Za klasu $\mathfrak{A}$ važe sljedeće karakterizacije:

Teorema 2.1. [3] Neka je S semigrupa. Tada je

$$S \in \mathfrak{A} \iff (\forall x \in S)(\exists y \in S)(x^2=y^2 \wedge yx=x^3y \wedge x^5 = x) .$$

Teorema 2.2. [3] Neka je S semigrupa. Tada je

$$S \in \mathfrak{A} \iff (\forall x \in S)(\exists y \in S)(x^2=y^2 \wedge x^2=(xy)^2 \wedge x^5=x) .$$

Iz Teoreme 2.1 slijedi:

Posljedica 2.1. [3] (i) Svaka anti-inverzna semigruna je regularna.

(ii) Svaki element anti-inverzne semigrupe ima sopstvenu jedinicu.

(iii) Anti-inverzni elementi semigrupe S imaju istu jedinicu.

(iv) Ako je $x^2=e_x$(e_x sopstvena jedinica elementa x), tada je x permutativan sa anti-inverznim elementom.

(v) Ako su x i y medjusobno anti-inverzni elementi, tada je $x^2y=yx^2$ i $xy^2=y^2x$.

(vi) Ako je element yeS anti-inverzan element elementa xeS, tada su za x anti-inverzni i elementi xy, x^2y i x^3y.

Sljedeća teorema daje potreban i dovoljan uslov kada svaki element anti-inverzne semigrupe ima jedinstven anti-inverzan element:

Teorema ([3] str. 23) Neka je S semigrupa. Svaki element iz S ima jedinstven anti-inverzan element u S ako i samo ako je S idempotentna semigrupa.

Sljedeća teorema daje potreban i dovoljan uslov kada su svaka dva elementa semigrupe medjusobno anti-inverzna:

Teorema ([3] str. 23) Neka je S semigrupa. Svaka dva elementa iz S su anti-inverzna ako i samo ako je S Abelova grupa u kojoj je svaki element sam sebi anti-inverzan.

Neka je P neprazan podskup semigrupe S. Označimo sa [P] podsemigrupu od S generisanu sa skupom P. Označimo sa A_a skup svih anti-inverznih elemenata elementa a semigrupe S, t.j.

$$A_a=\{x\in S \mid axa=x \wedge xax=a\} .$$

Važi:

Teorema 3.1. [3] Neka je S anti-inverzna semigrupa i $a \in S$. Tada za svaki podskup $I_a \subset A_a$, $GI_a = [a \cup I_a]$ je podsemigrupa od S.

Iz Teoreme 3.1. slijedi:

(i) Ako je I_a jednočlan skup i $a \notin A_a$ tada je GI_a grupa kvaterniona.

(ii) Ako $a \in I_a$ i I_a je dvočlan skup, t.j. $I_a = \{a,b\}$, tada je GI_a Kleinova grupa ili ciklična grupa reda 2.

(iii) Ako je $I_a = \emptyset$ i $a^2 \neq e_a$, tada je grupa GI_a ciklična grupa reda 4.

Iz Teoreme 3.1 takodje slijedi da se svaka anti-inverzna semigrupa S prekriva grupama, tj. $S = \bigcup_{a \in S} GI_a$.

Sljedeća teorema daje potreban i dovoljan uslov kada grupa G pripada klasi $\mathcal{A}$.

Teorema 3.3. [3] Neka je G grupa. Tada

$$G \in \mathcal{A} \iff (\forall x \in G)(\exists y \in G)([\{x,y\}] \in \mathcal{A}) .$$

Sljedeću definiciju dao je E.S.Ljapin 32 :

Definicija (bazisne klase) Neka su M,N,P tri klase semigrupa pri čemu je $M \subset N \subset P$. Tada je M *bazisna klasa* za klasu N, u odnosu na klasu P, ako važi:

a) Svaka semigrupa iz N može se predstaviti kao unija svojih podsemigrupa koje su iz klase M.

b) Svaka semigrupa iz P koja se može predstaviti kao unija svojih podsemigrupa iz M je iz P.

c) Nijedna podklasa M′ klase M ne ispunjava uslov a).

Za klasu semigrupa koja je bazisna klasa u smislu prethodne definicije reći ćemo da je bazisna klasa u smislu Ljapina.

Neka je $\mathfrak{B}$ klasa koju sačinjavaju trivijalna grupa, ciklična grupa reda 2 i grupa kvaterniona. Ako je $M=\mathfrak{B}$, $N=\mathfrak{A}$, $P=\mathfrak{C}$, gdje je $\mathfrak{C}$ klasa svih semigrupa, tada važi:

Teorema 3.3. [6] Klasa $\mathfrak{B}$ je bazisna klasa u smislu Ljapina za klasu $\mathfrak{A}$ u odnosu na klasu $\mathfrak{C}$.

1.2. KLASA (m,n)-ANTI-INVERZNIH SEMIGRUPA

U [36] je razmatrana klasa $\mathfrak{C}_{m,n}$ *(m,n)-antiinverznih* semigrupa S za koje važi

$$(\forall x\in S)(\exists y\in S)(x^m=y^m \wedge x^m=(xy)^m \wedge x^n = x) ,$$

gdje su m i n prirodni brojevi.

Za element y kažemo da je *(m,n)-anti-inverzan element* elementa x.

Neposredno slijedi da je $\mathfrak{A} = \mathfrak{C}_{2,5}$.

U [36] je takodje dokazano:

$\mathcal{Y}_{1,n} \subset \mathcal{A}$, $\mathcal{Y}_{2,n} \subset \mathcal{A}$ $(n>1)$, $\mathcal{Y}_{m,2} \subset \mathcal{A}$, $\mathcal{Y}_{m,m} \subset \mathcal{A}$, $\mathcal{Y}_{m,mq} \subset \mathcal{A}$.

U [4] i [34] je razmatrana klasa $\mathcal{Y}^*_{m,n}$ *(m,n)*-anti-inverznih semigrupa*, za koje važi

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

gdje su m i n prirodni brojevi. Za element y u tom slučaju kažemo da je *(m,n)* - anti-inverzan* element za x.

Označimo sa M_a (M^*_a) skup svih (m,n)-anti-inverznih elemenata ((m,n)*-anti-inverznih elemenata) elementa aeS. Tada važi:

Teorema 2.1. [4] Ako $S \in \mathcal{Y}_{m,n}$ $(\mathcal{Y}^*_{m,n})$, tada za svako aeS i svako $I_a \subset M_a$ $(I^*_a \subset M^*_a)$

$$GI_a = [a \cup I_a] \quad (GI^*_a = [a \cup I_a])$$

je grupa.

Takodje, važi:

$$S \in \mathcal{Y}_{m,n} \Longrightarrow S = \bigcup_{a \in S} GI_a$$

$$S \in \mathcal{Y}^*_{m,n} \Longrightarrow S = \bigcup_{a \in S} GI^*_a .$$

Na kraju istaknimo:

Teorema. [34] Podklasa komutativnih semigrupa iz $\mathcal{Y}_{m,n}$ jednaka je podklasi komutativnih semigrupa iz $\mathcal{Y}^*_{m,n}$.

1.3. NEKE DEFINICIJE I SVOJSTVA PRSTENA

U [28] N.Jacobson je dokazao:

Teorema. Ako za svaki element x prstena R postoji broj $n(x) > 1$, koji zavisi od x, takav da važi $x^{n(x)}=x$, tada je R komutativan prsten.

Kako prsteni u glavama II, III i IV zadovoljavaju uslove Jacobsonove teoreme, to ćemo ovdje razmatrati neke definicije i tvrdjenja vezana za komutativne prstene.

Neka je (R,+,.), dalje ćemo pisati samo R, komutativan prsten. Za element $x \in R$ kažemo da je *djeljitelj nule* ako postoji element $y \in R$, $y \neq 0$, takav da je $xy=0$.

Element $0 \in R$ je sigurno djeljitelj nule i naziva se *trivijalni* djeljitelj nule.

Komutativni prsten sa jedinicom koji nema netrivijalnih djeljitelja nule naziva se *oblast cijelih*.

Za element $x \in R$ kažemo da je *nilpotentan*, ako postoji prirodan broj n takav da je $x^n=0$.

Svaki nilpotentni element prstena je očigledno djeljitelj nule. Obrnuto, u opštem slučaju ne važi.

Za element $e \in R$ kažemo da je *idempotent* prstena R, ako važi $e^2=e$.

Za idempotente $e_1, e_2 \in R$ kaže se da su *ortogonalni* ako važi $e_1 e_2 = 0$.

Za nas će od posebnog značaja biti sistem medjusobno ortogonalnih idempotenata $e_1, e_2, \ldots, e_n$ prstena R, (znači $e_i^2 = e_i$, $e_i e_j = 0$ za $i \neq j, i, j = 1, 2, \ldots, n$), pri čemu je $e_i \neq o, i = 1, 2, \ldots, n$.

Neka je R prsten i I podskup od R. Ako je:

1. (I,+) podgrupa grupe (R,+);
2. $(\forall x \in R)(\forall y \in I)(xy \in I)$, tj. $RI \subset I$;

tada se I naziva *ideal* prstena R.

Neka je $a \in R$. Neposredno se provjerava da je $Ra = \{ra : r \in R\}$ ideal prstena R. Ideal Ra nazivamo *glavni ideal* prstena R generisan elementom a. često se označava i sa (a).

Ideal (0), označavaćemo ga sa 0, sastoji se samo od elemenata 0 i zvaćemo ga *nulaideal* prstena R.

Prsten R je takodje svoj ideal, i ako je R prsten sa jedinicom 1, važi R=(1).

Ako je I ideal prstena R, tada je $R/I = \{x+I : x \in R\}$ prsten, gdje je

$$(x+I)+(y+I) = (x+y)+I, \quad (x+I)(y+I) = xy+I.$$

Prsten R/I nazivamo *faktor prsten*.

Za ideal I prstena R, pri čemu je $I \neq R$, kažemo da je *prost*, ako važi

$$(\forall x,y\in R)(xy\in I \Longrightarrow x\in I \vee y\in I) \ .$$

Ideal M prstena R, $M\neq R$, je *maksimalan*, ako ne postoji ideal $M'\neq R$ takav da je $M\subset M'$.

Važi:

(a) Ideal I prstena R je prost ako i samo ako je prsten R/I oblast cijelih.

(b) Ideal M prstena R je maksimalan ako i samo ako je prsten R/M polje.

Odavde neposredno slijedi da je svaki maksimalan ideal prstena R prost.

Takodje važi da je svaki ideal prstena R sadržan u nekom maksimalnom idealu prstena R.

Za ideal prstena R kažemo da je *minimalan* ako ne postoji ideal $I'\neq 0$, takav da je $I'\subset I$.

Ako su I_1 i I_2 ideali prstena R, tada je skup svih konačnih suma proizvoda $xy, x\in I_1, y\in I_2$, takodje idaal prstena R. Ovaj ideal nazivamo *proizvod* ideala I_1 i I_2 i označava se I_1I_2.

Analogno se definiše proizvod bilo koje konačne familije ideala prstena R.

Za ideal I prstena R kažemo da je *idempotentan*, ako važi $I^2=I$.

Lema 1.3.1. Svaki idempotentan minimalan ideal prstena R je generisan idempotentom.

D o k a z. Neka je I idempotentan minimalan ideal prstena R. Tada postoji element aeI takav da je Ia≠0. Naime, ako bi za svako aeI važjelo Ia=0, tada bi bilo $I^2=0$, što je u kontradikciji sa pretpostavkom da je I idempotentan ideal.

Kako je I minimalan ideal, to je Ia=I. Dalje, postoji element eeI takav da je ea=a. Posmatrajmo homomorfizam ideala I definisan sa $\varphi(x)=xa$. Tada je $I'=\{xeI: \varphi(x)=0\}$ ideal prstena R sadržan u I. Kako je $\varphi(e)=ea=a$, to $e\notin I'$, a kako je I minimalan ideal to važi $I'=0$. Dalje je $\varphi(e^2-e)=(e^2-e)a=e^2a-ea=a-a=0$, pa e^2-eeI', odakle je $e^2-e=0$, tj. $e^2=e$. Znači, e je idempotent.

Kako je Ie≠0 i kako je $Ie\subset I$, to je Ie=I. Dalje je Re=I, tj. ideal I je generisan idempotentom e.

Za ideal I prstena R kažemo da je *nilpotentan*, ako postoji prirodan broj n takav da je $I^n=0$.

Presjek bilo koje familije ideala prstena R je ideal prstena R.

Presjek svih prostih (maksimalnih) ideala prstena R nazivamo *nilradikal (radikal Jacobsona)* prstena R.

Za prsten R kažemo da je *regularan* u smislu Nojmana, ili prosto regularan, ako važi

$$(\forall x\in R)(\exists y\in R)(xyx=x)\ ,$$

t.j. ako je prsten R komutativan, ako važi

$$(\forall x\in R)(\exists y\in R)(x^2y=x) \ .$$

Od značaja su u daljem sljedeća svojstva komutativnih regularnih prstena:

Propozicija 1.3.1. Ako je R komutativan regularan prsten sa jedinicom, tada važi:

1. Svaki neinvertibilni element prstena R je djeljitelj nule;

2. Svaki prost ideal je maksimalan;

3. Prsten R je poluprimitivan, tj. Jacobsonov radikal prstena R je 0.

1.4. DIREKTNA SUMA IDEALA

Neka je $I_j, j\in J$, familija ideala prstena R. Ako je I skup svih suma $\Sigma x_j, x_j\in I_j$, pri čemu je $x_j\neq 0$ samo u konačno mnogo slučajeva, tada se lako provjerava da je I takodje ideal prstena R.

Ideal I nazivamo *suma* ideala $I_j, j\in J$ i označava se $I=\Sigma I_j$.

Ako je još za svako $i\in J$

$$I_i \cap \Sigma I_j = 0 \ , \tag{1.4.1}$$

tada kažemo da je I *direktna suma* ideala I_j, $j\in J$, i piše se $I=\bigoplus_{j\in J} I_j$.

Ako je $R = \bigoplus_{j\in J} I_j$, tada kažemo da je prsten R direktna suma ideala $I_j, j\in J$.

Neposredno se provjerava da je uslov (1.4.1) ekvivalentan sa uslovom: ako je $\sum_{j\in J} x_j = 0, x_j \neq 0$ samo u konačno mnogo slučajeva, tada je $x_j = 0$ za svako $j\in J$.

Odavde slijedi da je R direktna suma ideala $I_j, j\in J$, ako i samo ako, se svaki element $x\in R$ na jedinstven način može napisati u obliku $x = \sum_{j\in J} x_j, x_j \in I_j, x_j \neq 0$ samo u konačno mnogo slučajeva.

Ako je R direktna suma konačno mnogo ideala $I_j, j=1,2,\ldots,n$, tada se piše $R = \sum_{j=1}^{n} I_j$.

Uočimo jednu mogućnost razlaganja prstena R u direktnu sumu svojih ideala:

<u>Propozicija 1.4.1.</u> Neka su $e_1, e_2, \ldots, e_n$ medjusobno ortogonalni idempotenti prstena R. Tada su $I_k = Re_k$, $k=1,2,\ldots,n$, ideali prstena R. Takodje

$$I_o = \{x\in R: xe_k = 0, k=1,2,\ldots,n\}$$

je ideal prstena R i prsten R je direktna suma ideala $I_o, I_1, \ldots, I_n$.

D o k a z. Neposredno se provjerava da su $I_k = Re_k, k=1,\ldots,n$, i I_o ideali prstena R.

Neka je x proizvoljni element prstena R. Tada $x - \sum_{k=1}^{n} xe_k \in I_o$, jer

$$(x-\sum_{j=1}^{n} xe_k)e_j=xe_j-xe_j=0,\ j=1,2,\ldots,n\ .$$

Dalje je

$$(1.4.2)\qquad x=(x-\sum_{k=1}^{n} xe_k)+\sum_{k=1}^{n} xe_k \in \sum_{k=o}^{n} I_k\ ,$$

t.j. prsten R je suma ideala $I_k, k=1,2,\ldots,n$.

Dokažimo da je prikaz (1.4.2) jedinstven. Neka je $x = \sum_{k=o}^{n} x_k$, $x_k \in I_k, k=0,1,2,\ldots,n$. Kako $x_k \in Re_k$, to je $x_k=y_k e_k, y_k \in R, e_k \in I_k$, $k=1,2,\ldots,n$. Dalje, kako su idempotentni $e_k, k=1,2,\ldots,n$, medjusobno ortogonalni i kako je $x_o e_k=0$, to je $xe_k=y_k e_k=x_k$, $k=1,2,\ldots,n$. Još je

$$x_o=x-(x_1+\ldots+x_n)=x-\sum_{k=1}^{n} xe_k\ .$$

Dakle, prikaz (1.4.2) je jedinstven, pa je R direktna suma ideala $I_k, k=0,1,\ldots,n$.

1.5. SEMIPROSTI PRSTENI

Za prsten R kažemo da je *semiprost* ako ne postoji ideal $I\neq 0$ prstena R koji je nilpotentan.

Lema 1.5.1. Ako je R semiprost prsten, tada je svaki minimalni ideal I prstena R generisan idempotentom.

D o k a z . Neka je $I\neq 0$ minimalan ideal semiprostog prstena R. Zbog $I^2 \subset I$ važi $I^2=0$ ili $I^2=I$. No, ne može biti $I^2=0$, jer

je R semiprost prsten. Dakle, I je idempotentan ideal.

Sada, tvrdjenje slijedi iz Leme 1.3.1.

Lema 1.5.2. Neka je R prsten. Ako je I neprazan podskup od R takav da za svako aeI, a≠0, važi Ra=I, tada je I minimalan ideal prstena R. Obrnuto tvrdjenje važi ako je R semiprost prsten, tj. ako je R semiprost prsten i I minimalan ideal prstena R, tada za svako aeI, a≠0, važi Ra=I.

D o k a z. Neka je I neprazan podskup prstena R koji zadovoljava uslove Leme. Neposredno slijedi da je I ideal. Pretpostavimo da je I′≠0 ideal prstena R takav da je I′⊂ I. Tada za svako aeI′, a≠0, važi I=Ra⊂ I′, tj. I′= I i ideal I je minimalan.

Neka je sada R semiprost prsten i I minimalan ideal prstena R. Za proizvoljan element aeI, a≠0, ideal Ra je sadržan u I. Kako je I minimalan ideal, to je Ra=I ili Ra=0. Medjutim, ne može biti Ra=0. Naime, tada bi element a pripadao nilpotentnom idealu {reR:xr=0} , za svako xeR i prsten R nebi bio semiprost.

Dakle, Ra=I za svako aeI, a≠0.

Lema 1.5.3. Neka je R komutativan semiprost prsten i e idempotent prstena R. Tada je ideal Re minimalan ideal ako i samo ako je Re polje.

D o k a z. Neka je Re minimalan ideal prstena R. Za proizvoljno xeRe važi x=re, reR, pa je xe=(re)e=re^2=re=x, tj. e je

jedinični element u Re. Kako je Re minimalan ideal semiprostog prstena R, to prema Lemi 1.5.2, za svako aeRe, a≠0, važi Ra=Re. Znači, postoji element reR takav da je ra=e.Sada je e=ra=e(ra)= =(re)a, tj. element re je inverzan elementu aeRe. Dakle, Re je polje.

Neka je sada Re polje i aeRe, a≠0. Tada postoji element ye Re takav da je ya=e. Sada, za proizvoljno ceRe. važi c=ce= =cyaeRa, tj. Re⊂Ra. Kako je Ra⊂Re, to je Ra=Re za svako aeRe,a≠0. Odavde, zbog Leme 1.5.2 slijedi da je Re minimalan ideal.

1.6. KONAČNA POLJA

Ovdje ćemo navesti neke definicije i tvrdjenja vezana za konačna polja, (tj. polja Galoa kako se često nazivaju), sa posebnim osvrtom na ona tvrdjenja koja ćemo kasnije koristiti.

Za polje P kažemo da je *prosto*, ako ne postoji pravo potpolje polja P.

Za prosto polje važi da je ono izomorfno sa poljem racionalnih brojeva ili sa poljem Z_p za neki prost broj p.

Presjek svih potpolja polja K je neprazan skup, jer taj presjek sadrži obavezno elemente 0 i 1. No, taj presjek P je takodje potpolje polja K i to je jedinstveno prosto potpolje polja K. Dakle:

Propozicija 1.6.1. Svako polje K sadrži tačno jedno prosto potpolje P.

Ako je prosto potpolje P polja K izomorfno sa poljem racionalnih brojeva, kažemo da je polje K *karakteristike* 0, a ako je P izomorfno sa Z_p, kažemo da je K polje *karakteristike* p.

Neka je K polje karakteristike $p \neq 0$. Tada je njegovo prosto potpolje P izomorfno sa Z_p i zbog toga važi $p \cdot 1 = 1+1+\ldots+1 = 0$. No, tada za svaki element $x \in K$ važi $px = (p \cdot 1)x = 0 \cdot x = 0$, tj. svaki element polja karakteristike p ima aditivni red p.

Sada je moguće okarakterisati konačna polja. Neka je K konačno polje. Tada je njegovo prosto potpolje izomorfno sa Z_p, gdje je p prost broj. Dakle, polje K je karakteristike p. Dalje, polje K može se shvatiti kao vektorski prostor nad poljem P i, kako je K konačno polje, dimenzija tog prostora je konačan broj m. Znači, broj elemenata polja K je p^m. Dakle:

Propozicija 1.6.2. Svako konačno polje ima p^m elemenata, gdje je p prost broj i $m > 0$. Karakteristika polja K je p.

Neka je K konačno polje, Za multiplikativnu grupu $(K^*, \cdot)$, važi:

Propozicija 1.6.3. Ako je K polje od $q = p^m$ elemenata, tada je multiplikativna grupa K^* ciklična grupa reda q-1.

D o k a z. Multiplikativna grupa K^* je Abelova grupa reda q-1. Označimo sa k eksponent grupe K^*, tj. k je najmanji broj za koji važi $x^k=1$, za svako $x \in K^*$. Tada je $k < q-1$. No, kako su svi elementi grupe K^* korjeni polinoma x^k-1, tj. kako polinom x^k-1 ima najmanje q-1 različitih korjena, to je $k > q-1$. Dakle, $k=q-1$. Znači, postoji element $g \in K^*$ reda q-1 i svi elementi $g^0=1, g, g^2, \ldots, g^{q-2}$ su različiti i iscrpljuju grupu K^*, tj. K^* je ciklična grupa generisana elementom g.

Vidjeli smo da svako konačno polje ima p^m elemenata, gdje je p prost broj i $m > 0$. Medjutim, važi i obrnuto, što ovdje nećemo dokazivati, tj. za svaki prost broj p i svaki broj $m > 0$ postoji polje od p^m elemenata. To polje je jedinstveno do izomorfizma.

Polje Galoa od p^m elemenata označavaćemo $GF(p^m)$.

Za dalje, trebaće nam opis svih potpolja konačnog polja.

Propozicija 1.6.4. Ako je $GF(p^m)$ konačno polje, tada za svaki djeljitelj d broja m postoji tačno jedno potpolje polja $GF(p^m)$.

D o k a z. Neka je K potpolje polja $GF(p^m)$. Prosto potpolje polja $GF(p^m)$ je istovremeno i potpolje polja K, pa je $K=GF(p^d)$. Kako je $GF(p^m)$ konačnodimenzionalni vektorski prostor nad poljem K, to postoji broj $r > 0$ takav da je $p^m=(p^d)^r$, a odavde slijedi da je d djelilac broja m.

Multiplikativna grupa K^* polja K je podgrupa grupe $GF(p^m)^*$, koja, kao što smo vidjeli, je ciklična grupa reda p^m-1. Kako ciklična grupa sadrži tačno jednu podgrupu datog reda, koji dijeli red grupe, to grupa $GF(p^m)^*$ sadrži tačno jednu podgrupu reda p^d, tj. polje K je jedinstveno.

GLAVA II

O KLASI PRSTENA ZA ČIJI SVAKI ELEMENT x VAŽI $x^n=x$

U ovoj glavi razmatraćemo klasu prstena $\mathfrak{AR}_n$, kojoj pripadaju prsteni za čiji svaki element x važi $x^n=x$. Dokazuje se da su prsteni iz ove klase komutativni, regularni i semiprosti. Takodje, daje se opis aditivne karakteristike elemenata prstena Re $\mathfrak{R}_n$ (Lema 2.1.1).

Dalje se uvodi pojam *m-skupa i maksimalnog m-skupa*. Pomoću maksimalnog m-skupa daje se karakterizacija svih minimalnih ideala prstena Re $\mathfrak{R}_n$ (Propozicija 2.3.1).

Za slučaj kada je maksimalan m-skup prstena Re $\mathfrak{R}_n$ konačan, prsten R je direktna suma svih svojih minimalnih ideala, i na taj način okarakterisani su prsteni Re $\mathfrak{R}_n$ sa konačnim maksimalnim m-skupom (Propozicija 2.3.3).Takodje, u slučaju kada je maksimalan m-skup prstena Re $\mathfrak{R}_n$ konačan, moguće je dati karakterizaciju svih idempotenata prstena R(Propozicija 2.3.4).

Ovdje se takodje,razmatraju neki slučajevi kada je prsten Re $\mathfrak{R}_n$ polje. Tako na primjer, ako je Re $\mathfrak{R}_n$ prsten sa jedinicom i ako je R oblast cijelih, tada je R polje (Lema 2.1.3). Pomoću ortogonalnih idempotenata prstena Re $\mathfrak{R}_n$ daje se potreban i dovoljan uslov kada je prsten R sa jedinicom polje. (Propozicija 2.2.1). Konačno, u Teoremi 2.4.1 daje se potreban i dovoljan

uslov kada polje od p^m elemenata pripada klasi $\mathfrak{R}_n$. Na osnovu postupka koji daje ova teorema za odredjivanje svih polja koja pripadaju klasi $\mathfrak{R}_n$, za svaki fiksirani broj n, odredjena su sva polja koja pripadaju klasama $\mathfrak{R}_3$, $\mathfrak{R}_4$ i $\mathfrak{R}_5$.

2.1. DEFINICIJA I NEKA SVOJSTVA

Neka je $(R,+,\cdot)$ prsten takav da važi

$$(2.1) \qquad (\forall x\in R)(x^n=x) \ ,$$

pri čemu je $n>1$.

Klasu prstena sa svojstvom (2.1) označimo $\mathfrak{R}_n$.

Prema Teoremi N.Jacobsona, [28], prsten $R\in\mathfrak{R}_n$ je komutativan.

Takodje, iz definicije regularnosti elementa prstena slijedi da je prsten $R\in\mathfrak{R}_n$ regularan. Naime, za svaki element $x\in R$ važi $xx^{n-2}x=x$, za $n>2$, odnosno $xxx=x$ za $n=2$.

Navešćemo neke primere prstena iz klase $\mathfrak{R}_n$.

Primjer 2.1.1. a) Prsten Z_6 i polja Z_2 i Z_3 pripadaju klasi $\mathfrak{R}_3$.

b) Polje $GF(4)\in\mathfrak{R}_4$.

Primjer 2.1.2. a) Neka je E proizvoljan skup. Bulov

prsten (P(E),+,.), gdje je "+" simetrična razlika i "." presjek skupova, pripada klasi $\mathcal{R}_n$ za svaki prirodan broj n.

b) Neka je $Re\,\mathcal{R}_n$ i P(E) prsten iz prethodnog razmatranja. Prsten RxP(E) takodje pripada klasi $\mathcal{R}_n$, jer za proizvoljni element $(x,y)\in RxP(E)$ važi $(x,y)^n=(x^n,y^n)=(x,y)$.

Lema 2.1.1. *Ako je* $Re\,\mathcal{R}_n$ *tada važi*

$$(2.2)\qquad (\forall x\in R)((2^n-2)x = 0)\ .$$

D o k a z. Za proizvoljne elemente $x,y\in R$ važi

$$x+y+\sum_{k=2}^{n-1}\binom{n}{k}x^{n-k}y^k=x^n+y^n+\sum_{k+1}^{n-1}\binom{n}{k}x^{n-k}y^k=(x+y)^n=x+y\ .$$

Odavde je

$$\sum_{k=1}^{n-1}\binom{n}{k}x^{n-k}y^k = 0\ .$$

Za x=y dobija se

$$\sum_{k=1}^{n-1}\binom{n}{k}x^n = 0\ ,$$

odakle slijedi (2.2).

Lema 2.1.2. *Neka je* $Re\,\mathcal{R}_n$ *prsten sa jedinicom i neka je I ideal prstena R. Sledeća tvrdjenja su ekvivalentna:*

(a) I je maksimalan ideal prstena R;

(b) I je prost ideal prstena R;

(c) Za proizvoljan element $x \in R$ *važi*

$$(x^{n-1} \in I \wedge 1-x^{n-1} \notin I) \vee (x^{n-1} \notin I \wedge 1-x^{n-1} \in I) \quad .$$

D o k a z . Neka $R \in \mathfrak{R}_n$. Kako je R regularan prsten to iz Propozicije 1.3.1. slijedi ekvivalentnost tvrdjenja (a) i (b).

Za proizvoljan element $x \in R$ važi $x^{n-1}+(1-x^{n-1})=1 \notin I$, tj. elementi x^{n-1} i $1-x^{n-1}$ ne pripadaju istovremeno idealu I. Dalje je $x^{n-1}(1-x^{n-1})=0 \in I$, i kako je I prost ideal, to važi (c).

(c) => (a) Za proizvoljan element $x \in R \setminus I$ iz $xx^{n-1}=x$ sledi $x^{n-1} \notin I$. Tada $1-x^{n-1} \in I$. Dalje je $1=(1-x^{n-1})+x^{n-1} \in I+x^{n-1}R \subset I+xR$. Neka je P ideal prstena R koji strogo sadrži ideal I. Za element $x \in P \setminus I$ važi $I+xR \subset P$. No, kako $1 \in I+xR$, to je P=R, tj. I je maksimalan ideal prstena R.

Lema 2.1.3. Neka je $R \in \mathfrak{R}_n$ *prsten sa jedinicom. Ako je R oblast celih, tada je R polje.*

D o k a z . Neka je $x \neq 0$ proizvoljan element oblasti R. Tada iz $x^n=x$ sledi $x(x^{n-1}-1)=0$, a odavde je $x^{n-1}=1$. Dakle, svaki element $x \neq 0$ oblasti R je invertibilan i njemu inverzan element je x^{n-2} za $n > 2$, odnosno sam element x, ako je n=2.

Lema 2.1.4. Neka je $R \in \mathfrak{R}_n$ i $x \in R$. Tada

$$x^t=x \iff x^{n-t+1}=x, \quad 1 < t < n.$$

D o k a z. Iz $x^t=x$ sledi $x^t x^{n-t}=xx^{n-t}$, odakle je $x^n=x^{n-t+1}$, odnosno $x^{n-t+1}=x$.

Obrnuto, neka je $x^{n-t+1}=x$. Odavde je $x^{n-t+1}x^{t-1}=xx^{t-1}$, odakle je $x^n=x^t$, odnosno $x^t=x$.

Posledica. *Neka je* $R \in \mathcal{R}_n$. *Tada* R *je Bulov prsten ako i samo ako za svaki element* $x \in R$ *važi* $x^{n-1}=x$.

Lema 2.1.5. *Neka je* $R \in \mathcal{R}_n$. *Svaki ideal* I *prstena* R *je idempotentan.*

D o k a z. Ako je n=2, neposredno sledi da je $I^2=I$.

Neka je sada $n>2$. Trivijalno je $I^2 \subset I$. Neka $x \in I$. Tada $x^{n-1} \in I$ i važi $x=x^{n-1}x \in I^2$. Dakle, $I \subset I^2$, tj. $I=I^2$.

Propozicija 2.1.1. *Prsten* $R \in \mathcal{R}_n$ *je semiprost prsten.*

D o k a z. Neka je I nilpotentan ideal prstena R, tj. takav ideal da za neko m važi $I^m=0$. Prema Lemi 2.1.5 je $I^2=I$, odakle je $I^m=I$. Dakle, I=0, pa prsten R nema nenultih nilpotentnih ideala, tj. R je semiprost prsten.

2.2. O NEKIM SVOJSTVIMA IDEMPOTENATA

Lema 2.2.1. *Ako je* $R \in \mathcal{R}_n$ *i* $x \in R$, *tada je* x^{n-1} *idempotent.*

D o k a z. Ako je n=2, tj. ako je R Bulov prsten, tvrdjenje neposredno sledi.

Neka je sada $n>2$. Tada je

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

pa je x^{n-1} idempotent.

Za dalje, pogotovo za opis minimalnih ideala prstena iz klase $\mathcal{R}_n$, od značaja su medjusobno ortogonalni idempotenti, tj. takvi idempotenti e_1 i e_2, $e_1 \neq o_1 e_2 \neq o$, za koje važi $e_1 e_2 = 0$.

Pomoću ortogonalnih idempotenata dajemo potreban i dovoljan uslov, kada je prsten iz klase $_n$ polje. Naime, važi:

Propozicija 2.2.1. *Prsten* $R \in \mathcal{R}_n$ *sa jedinicom, je polje ako i samo ako R nema ortogonalnih idempotenata.*

D o k a z. Ako je R polje, tada očigledno R nema ortogonalnih idempotenata.

Neka sada R nema ortogonalnih idempotenata. Tada je R prsten bez djeljitelja nule. Naime, ako bi za neko $x, y \in R$, $x \neq 0$, $y \neq 0$, važelo $xy=0$, tada bi važelo i $x^{n-1}y^{n-1}=0$. Dalje je $x^{n-1} \neq 0$ i $y^{n-1} \neq 0$, jer bi inače bilo $x=0$ i $y=0$. No, to bi značilo da prsten R ima ortogonalne idempotente x^{n-1} i y^{n-1}, što je suprotno pretpostavci.

Sada, iz Leme 2.1.3 slijedi da je R polje.

Neka je E skup medjusobno ortogonalnih idempotenata prstena R. Za skup E kažemo da je *m-skup*, ako ne postoji idempotent iz $R \setminus E$ koji je ortogonalan sa svim idempotentima skupa E.

P r i m j e r 1.2.1. Posmatrajmo prsten $(R,+,\cdot)$, gdje je $R=\{0,1,2,3,4,5,6,7,8,9,10,11\}$ i operacije "+" i "." definisane na sljedeći način:

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	3	5	4	2	0	10	11	9	8	7	6
2	2	5	3	0	1	4	7	8	6	10	11	9
3	3	4	0	2	5	1	8	6	7	11	9	10
4	4	2	1	5	0	3	9	10	11	6	7	8
5	5	0	4	1	3	2	11	9	10	8	6	7
6	6	10	7	8	9	11	0	2	3	4	1	5
7	7	11	8	6	10	9	2	3	0	1	5	4
8	8	9	6	7	11	10	3	0	2	5	4	1
9	9	7	10	11	6	8	4	1	5	0	2	3
10	10	8	11	9	7	6	1	5	4	2	3	0
11	11	6	9	10	8	7	5	4	1	3	0	2

.	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	2	3	0	3	0	2	3	0	2	3
3	0	3	3	2	0	2	0	3	2	0	3	2
4	0	4	0	0	4	4	6	6	6	9	9	9
5	0	5	3	2	4	1	6	8	7	9	11	10
6	0	6	0	0	6	6	6	6	6	0	0	0
7	0	7	2	3	6	8	6	7	8	0	2	3
8	0	8	3	2	6	7	6	8	7	0	3	2
9	0	9	0	0	9	9	0	0	0	9	9	9
10	0	10	2	3	9	11	0	2	3	9	10	11
11	0	11	3	2	9	10	0	3	2	9	11	10

Za prsten R m-skupovi su {2,4}, {6,10}, {7,9} i {2,6,9} .

Lema 2.2.2. *Neka je* $\mathrm{Re}\,\mathfrak{R}_n$ *nenulti prsten sa jedinicom. Tada je R polje ili R ima ortogonalne idempotente (znači i m-skupove).*

D o k a z. Neka je $\mathrm{Re}\,\mathfrak{R}_n$ nenulti prsten sa jedinicom i neka R nije polje. Neka je $x\in R$ i $x\neq 0$. Prema Lemi 2.2.1, element x^{n-1} je idempotent. Dalje je $1-x^{n-1}\neq 0$. Naime, ako bi bilo $1-x^{n-1}=0$, tj. $x^{n-1}=1$, tada bi za $x\neq 0$ iz $xy=0$ sledilo $x^{n-1}y=0$, odnosno $y=0$, pa prsten R nebi imao djelitelja nule, tj. R bi bilo polje.

Iz

$$(1-x^{n-1})^2=1-2x^{n-1}+(x^{n-1})^2=1-x^{n-1}\ ,$$

slijedi da je element $1-x^{n-1}$ idempotent, a iz

$$x^{n-1}(1-x^{n-1})=x^{n-1}-(x^{n-1})^2=0,$$

slijedi da su idempotenti x^{n-1} i $1-x^{n-1}$ ortogonalni.

Lema 2.2.3. *Neka je E neprazan skup medjusobno ortogonalnih idempotenata prstena* $\mathrm{Re}\,\mathfrak{R}_n$ i

$$I_0=\{x\in R/xe=0, e\in E\}\ .$$

Tada je E m-skup ako i samo ako je $I_0=0$.

D o k a z. Neka je E m-skup. Pretpostavimo da je $I_0\neq 0$. Tada postoji element $x\neq 0$ ideala I_0. Dalje je $x^{n-1}\in I_0$ i $x^{n-1}\neq 0$, (jer bi inače bilo $x=x^{n-1}x=0$). Takodje je $x^{n-1}\neq e$, za svako $e\in E$. Naime, ako bi za neko $e\in E$ važjelo $x^{n-1}=e$, tada bi bilo $e=ee=$ $=x^{n-1}e=x^{n-2}xe=0$.

Sada, kako je x^{n-1} idempotent koji nije iz E i kako za svako $e\in E$ važi $x^{n-1}e=0$, to E nije m-skup, što je suprotno pretpostavci. Dakle, $I_o= 0$.

Neka je sada $I_o= 0$. Tada, ako je $e\in E$ idempotent ortogonalan na svaki idempotent iz E, onda $e\in I_o$, tj. e=0. Dakle, E je m-skup.

Ako je R proizvoljan prsten i $e_1,e_2,\ldots,e_s$ skup medjusobno ortogonalnih idempotenata prstena R, tada je, kao što smo vidjeli u Propoziciji 1.4.1, prsten R direktna suma ideala I_o i Re_k, k=1,2,...,s, gdje je I_o ideal iz Leme 2.2.3.

Sada, iz Leme 2.2.3 slijedi:

<u>*Propozicija 2.2.2.*</u> *Ako je* $E=\{e_1,e_2,\ldots,e_s\}$ *m-skup prstena* $Re\Re_n$, *tada je R direktna suma svih ideala* $Re_i, e_i\in E$.

Primjer 2.2.2. a) Neka je P(S) prsten iz Primjera 2.1.2, gdje je S konačan skup. Tada je skup svih jednočlanih podskupova skupa S m-skup prstena P(S). Ideal generisan idempotentom a , $a\in S$ je

$$\{ A\cap \{a\} : A\in P(S)\} =\{\emptyset,\{a\}\}$$

i prsten P(S) je direktna suma ovih ideala.

b) Neka je R prsten iz Primjera 2.2.1. Kako idempotenti 2,4,6,7,9,10 redom generišu ideale

$\{0,2,3\},\{0,4,6,9\},\{0,6\},\{0,2,3,6,7,8\},\{0,9\},\{0,2,3,9,10\}$.

Dalje, kako su {2,4},{6,10},{7,9} i {2,6,9} m-skupovi prstena R, to je prsten R direktna suma ideala

$$\{0,2,3\},\ \{0,4,6,9\}\ ,$$

odnosno ideala

$$\{0,6\},\{0,2,3,9,10\}\ ,$$

odnosno ideala

$$\{0,9\},\ \{0,2,3,6,7,8\}\ ,$$

odnosno ideala

$$\{0,2,3\},\ \{0,6\},\ \{0,9\}\ .$$

Primijetimo da je E ={2,6,9} m-skup sa najvećim brojem elemenata i da su jedino tada odgovarajući ideali minimalni ideali prstena R. U ovome ćemo naći motiv za sljedeća razmatranja.

2.3. MAKSIMALNI m-SKUPOVI PRSTENA $Re\mathfrak{R}_n$

Definicija 2.3.1. Za m-skup $M = \{e_i : i \in I\}$ prstena $Re\mathfrak{R}_n$ kažemo da je *maksimalan* ako za svaki idempotent $e_i \in M$ jedini idempotenti ideala Re_i su 0 i e_i.

Primjer 2.3.1. a) Neka je P(S) prsten iz Primjera 2.1.2. Skup svih jednočlanih podskupova skupa S je m-skup prstena P(S). Ovaj m-skup je maksimalan, jer za svako $a \in S$, idempotent {a} generiše ideal

$$\{\ A \cap \{a\} : A \in P(S)\} = \{\emptyset, \{a\}\},$$

čiji su jedini idempotenti Ø i {a}.

b) U prstenu R iz Primjera 2.2.1 i 2.2.2 m-skup {2,6,9} je maksimalan m-skup, jer ideali {0,2,3}, {0,6},{0,9}, generisani redom idempotentima 2,6 i 9 imaju idempotente 0 i 2, odnosno 0 i 6, odnosno 0 i 9.

Skup {2,4} nije maksimalan m-skup, jer ideal {0,4,6,9}, generisan idempotentom 4, pored idempotenata 0 i 4 sadrži idempotente 6 i 9.

Slično se provjerava da m-skupovi {6,10} i {7,9} nijesu maksimalni m-skupovi, tj. da jedini maksimalni m-skup prstena R je {2,6,9}.

Propozicija 2.3.1. *Neka je* $Re\,\mathcal{R}_n$ *i neka je* $M=\{e_i : i\in I\}$ *maksimalan m-skup prstena R. Ideali* $Re_i, i\in I$, *su jedini minimalni ideali prstena R.*

D o k a z. Prema Lemi 2.2.1, za proizvoljan element $x\in Re_i$ element x^{n-1} je idempotent prstena R. Kako $x^{n-1}e\, Re_i$ i kako je M maksimalan m-skup prstena R, to za $x\neq 0$ važi $x^{n-1}=e_i$. Tada je $Re_i=Rx^{n-1}\subset Rx$, a kako je još $Rx\subset Re_i$, to je $Rx=Re_i$. Odavde, zbog Leme 1.5.2, slijedi da je Re_i minimalan ideal prstena R za svako $e_i\in M$.

Neka je sada $I\neq 0$ minimalan ideal prstena R različit od Re_i, i $\in I$. Kako je R semiprost prsten, to je, prema Lemi 1.5.1 ideal I generisan idempotentom $e'\neq 0$. Kako su I i $Re_i, i\in I$, minimalni ideali, to je $I\cap Re_i = 0$ za svako $i\in I$, pa je $e'e_i=0$ za svako $i\in I$. Znači idempotent e' je ortogonalan sa svim idempotentima $e_i\in M$, što je u kontradikciji sa činjenicom da je M m-skup.

Dakle, ne postoji minimalan ideal $I \neq 0$ prstena R različit od ideala $Re_j, i \in I$.

Posljedica. *Maksimalan m-skup prstena* $Re\mathcal{R}_n$ *je jedinstven.*

D o k a z. Neka je $M=\{e_i : i \in I\}$ maksimalan m-skup prstena R. pretpostavimo da postoji još jedan maksimalan m-skup $F=\{f_j : j \in J\}$.

Prema prethodnoj Propoziciji ideali $Re_i, i \in I$, su jedini minimalni ideali prstena R. No, kako su prema istoj Propoziciji ideali $Rf_j, j \in J$, takodje minimalni ideali prstena R, to za svako $j \in J$ postoji $i \in I$ tako da je $Rf_j = Re_i$. Prema Definiciji 2.3.1 važi $f_j = e_k$. Dakle, svaki od idempotenata $f_j, j \in J$, jednak je nekom od idempotenata $e_i, i \in I$, tj. maksimalan m-skup prstena $Re\mathcal{R}_n$ je jedinstven.

Propozicija 2.3.2. Ako je $Re\mathcal{R}_n$ prsten takav da je maksimalan m-skup M prstena R konačan, tada ne postoji m-skup E prstena R takav da je card E > card M.

D o k a z. Neka je $M = \{e_i : i \in I\}$ maksimalan m-skup prstena R. Pretpostavimo da postoji m-skup $E=\{f_j : j \in J\}$, takav da je card E > card M.

Kako su ideali $Re_i, i \in I$ minimalni, to za svako $i \in I$ i svako $j \in J$ važi $Re_i \cap Rf_j = 0$ ili $Re_i \cap Rf_j = Re_i$. Označimo sa J_0 skup indeksa iz J takvih da za $j \in J_0$ postoji $i \in I$, tako da je $Re_i \cap Rf_j = Re_i$. Kako je $Rf_k \cap Rf_s = 0$ za $k \neq s$, to za fiksirani ideal Re_i postoji najviše jedan ideal Rf_j takav da je $Re_i \cap Rf_j = Re_i$. Znači, važi card J_0 < card E. Sobzirom da je card J > card I, to je $J \setminus J_0 \neq \emptyset$, pa

postoji indeks $j_o \in J$ J_o, takav da je $Re_i \ R_{j_o} = 0$ za svako $i \in I$. Tada je $f_{j_o} \neq e_i$ i $e_i f_{j_o} = 0$, za svako $i \in I$, pa M nije m-skup, što je suprotno pretpostavci.

Dakle, ako je $Re\mathfrak{R}_n$ prsten sa konačnim maksimalnim m-skupom, tada su svi m-skupovi prstena R konačni i maksimalni m-skup je upravo onaj m-skup sa najvećim brojem elemenat, i on je prema Posljedici Propozicije 2.3.1 jedinstven

Iz Propozicije 2.2.2 i Propozicije 2.3.1 slijedi:

Propozicija 2.3.3. *Ako je maksimalni m-skup prstena* $Re\mathfrak{R}_n$ *konačan, tada je prsten R direktna suma svih svojih minimalnih ideala.*

Primijetimo da ako je maksimalan m-skup $M=\{e_i : i \in I\}$ prstena $Re\mathfrak{R}_n$ beskonačan, tada je direktna suma ideala Re_i, $i \in I$, ideal prstena R.

Za slučaj, kada je maksimalan m-skup prstena R konačan, moguće je opisati skup svih idempotenata prstena R:

Propozicija 2.3.4. *Neka je* $M=\{e_1, e_2, \ldots, e_t\}$ *maksimalan m-skup prstena* $Re\mathfrak{R}_n$. *Element* $a \in R$, $a \neq 0$, *je idempotent ako i samo ako je element a jednak zbiru različitih elemenata iz skupa M.*

D o k a z. Neka je $a = e_{i_1} + e_{i_2} + \ldots + e_{i_m}$, pri čemu je $e_{i_k} \in M, k=1,2,\ldots,m$ i $e_{i_r} \neq e_{i_s}$ za $r \neq s$. Tada je

$$a^2=(e_{i_1}+e_{i_2}+\ldots+e_{i_m})^2=e_{i_1}+e_{i_2}+\ldots+e_{i_m} = a,$$

tj. a je idempotent prstena R.

Obrnuto, neka je aeR idempotent. Kako je prsten R direktna suma svojih minimalnih ideala $Re_i, i=1,2,\ldots,t$, to je

$$a=r_1e_1+r_2e_2+\ldots+r_te_t, r_i\epsilon R, i=1,2,\ldots,t .$$

Kako je a idempotent, važi

$$(r_1e_1+r_2e_2+\ldots+r_te_t)^2=r_1e_1+r_2e_2+\ldots+r_te_t ,$$

odnosno

$$r_1^2e_1+r_2^2e_2+\ldots+r_t^2e_t = r_1e_1+r_2e_2+\ldots+r_te_t .$$

Ako pomnožimo lijevu i desnu stranu zadnje jednakosti sa $e_i, i=1,2,\ldots,t$, dobijamo

$$r_i^2e_i, \text{ odnosno } (r_ie_i)^2=r_ie_i .$$

Dakle, element $r_ie_i\epsilon Re_i$ je idempotent. Kako je M maksimalan m-skup, to je $r_ie_i=0$ ili $r_ie_i=e_i$, $i=1,2,\ldots,t$, pa je idempotent a jednak zbiru različitih elemenata iz M.

Posljedica. *Neka je* $M=\{e_1,e_2,\ldots,e_t\}$ *maksimalan m-skup prstena* $Re\mathfrak{R}_n$. *Tada prsten R ima* 2^t *idempotenata.*

D o k a z. Prema prethodnoj Propoziciji svaki idempotent a prstena R je oblika $a=r_1e_1+r_2e_2+\ldots r_te_t$, gdje je $r_ie_i=0$ ili

$r_i e_i = e_i$, $i=1,2,\ldots,t$. Znači, prsten R ima 2^t idempotenata.

Već smo vidjeli da prsten $Re\mathfrak{R}_n$ sa jedinicom, koji nije polje, ima ortogonalnih idempotenata. Za slučaj kada su m-skupovi prstena R konačni, važi i obrnuto tvrdjenje.

Propozicija 2.3.5. *Prsten $Re\mathfrak{R}_n$ koji ima konačan maksimalan m-skup je prsten sa jedinicom.*

D o k a z. Neka je $M=\{e_1,e_2,\ldots,e_t\}$ maksimalan m-skup prstena R. Tada je prsten R direktna suma minimalnih ideala Re_i, $i=1,2,\ldots,t$. Element $e=e_1+e_2+\ldots+e_t$ je jedinica prstena R. Naime, za proizvoljni element $x\in R$ važi $x=x_1+x_2+\ldots+x_t$, $x_i\in Re_i$, $i=1,2,\ldots,t$, pa je

$$xe=(x_1+x_2+\ldots+x_t)(e_1+e_2+\ldots+e_t)=$$
$$=x_1e_1+x_2e_2+\ldots+x_te_t=x_1+x_2+\ldots+x_t=x.$$

2.4.0 KONAČNIM POLJIMA ZA ČIJI SVAKI ELEMENT x VAŽI $x^n=x$

Kako su prsteni iz klase $\mathfrak{R}_n$ semiprosti, to su njihovi minimalni ideali polja. Prema Propoziciji 2.3.3, prsten $Re\mathfrak{R}_n$ koji ima maksimalan m-skup, je direktna suma svih svojih minimalnih ideala. Drugim riječima prsten $Re\mathfrak{R}_n$ koji ima maksimalan m-skup je direktna suma polja i, jasno, ta polja su iz klase $\mathfrak{R}_n$. Zbog toga je od značaja odrediti sva polja, koja za fiksiran broj n pripadaju klasi $\mathfrak{R}_n$.

Ako je P beskonačno polje karakteristike nula, tada zbog Leme 2.1.1 ono ne može zadovoljavati uslov (2.1).

Ovdje ćemo dati kriterijum za odredjivanje konačnih polja koja pripadaju klasi $\mathcal{R}_n$.

Teorema 2.4.1. *Neka je P polje od p^m elemenata. Tada su ekvivalentni iskazi:*

(a) $(\forall x \in P)(x^n = x)$

(b) $p \mid 2^n - 2$ *i postoji cio broj* $k \geq 0$ *takav da je*

$n = (k+1)p^m - k$.

D o k a z. (a) $\Rightarrow$ (b) Ako važi (a), prema Lemi 2.1.1 je $p \mid 2^n - 2$.

Kako polje P ima p^m elemenata, to za svako $x \in P$ važi $x^{p^m} = x$. Iz $x^{p^m} = x^n$ slijedi $x^{n-p^m} = 1$, a odavde je $n - p^m \equiv 0 \pmod{p^m - 1}$. To znači da postoji cio broj k takav da je $n - p^m = k(p^m - 1)$, odakle se dobija $n = (k+1)p^m - k$. Kako je $n - p^m \geq 0$ i $p^m - 1 > 0$, to je $k \geq 0$.

(b) $\Rightarrow$ (a) Kako polje P ima p^m elemenata to za svaki element $x \in P$ važi $x^{p^m - 1} = 1$. Sada je

$$x^n = x^{(k+1)p^m - k} = x^{k(p^m - 1)} x^{p^m} = x^{p^m} = x \ .$$

Primjer 2.4.1. a) Odredimo sva konačna polja za čiji svaki element x važi $x^3 = x$. Prema Lemi 2.1.1 za svaki element x takvih polja važi $2 \cdot 3x = 0$, tj. ta polja moraju biti karakteristike 2 ili 3, tj. to su polja od 2^m odnosno 3^m elemenata.

Kako je $3 \geqslant 2^m$ tačno samo za m=1, to od polja karakteristike 2 jedino polje Z_2 može imati traženo svojstvo. Iz $(k+1)\cdot 2-k=3$, dobija se k=1, pa za svaki element $x \in Z_2$ važi $x^3=x$.

Kako je $3 \geqslant 3^m$ takodje tačno samo za m=1, to opet treba provjeriti da li za svako $x \in Z_3$ važi $x^3=x$. Kako je jednakost $(k+1)\cdot 3-k=3$ tačna za k=0, to i polje Z_3 ima traženo svojstvo.

Dakle, jedina polja za čiji svaki element x važi $x^3=x$ su Z_2 i Z_3.

b) Odredimo sada sva polja za čiji svaki element x važi $x^4=x$.

Prema Lemi 2.1.1 za svaki element x takvog polja važi $2\cdot 7x=0$, pa su ta polja karakteristike 2 ili 7. Medjutim, relacija $4 \geqslant 7^m$ nije tačna ni za jedan prirodan broj m, pa ne postoji polje karakteristike 7, koje ima traženo svojstvo.

Nejednakost $4 \geqslant 2^m$ je tačna za m=1 i m=2. Kako je relacija $(k+1)2-k=4$ tačna za k=2 i relacija $(k+1)2^2-k=4$ tačna za k=0, to polja Z_2 i GF(4), i samo ona, zadovoljavaju uslov da za svaki njihov element x važi $x^4=x$.

c) Sasvim analogno se dobija da jedino polja Z_2, Z_3 i Z_5 su jedina polja za čiji svaki element x važi $x^5=x$.

GLAVA III

KLASA (m,n)-ANTI-INVERZNIH PRSTENA

U ovoj glavi razmatraćemo klasu $\mathcal{AR}_{m,n}$ (m,n)-*anti-inverznih* prstena, kojoj pripadaju prsteni (R,+,·) kod kojih je semigrupa (R,·) (m,n)-anti-inverzna. Kako je $\mathcal{AR}_{m,n} \subset \mathcal{R}_n$, to su prsteni iz klase $\mathcal{AR}_{m,n}$ komutativni, regularni i semiprosti.

Kako je $\mathcal{AR}_{m,n} = \mathcal{AR}_{m-kn+k,n}$, za m-kn >o, (Posljedica Leme 3.1.1), i kako je za slučaj kada je m > n, moguće odrediti broj k tako da je $0 < m-kn+k \leq n$, to su dalje ispitivane klase $\mathcal{AR}_{m,n}$, za koje je $m \leq n$.

U tački 3.2 razmatrana su neka svojstva (m,n)-anti-inverznih elemenata prstena R i skupa A_x svih elemenata (m,n)-anti-inverznih elementu x∈R. Prije svega, relacija (m,n)-anti-inverznosti je relacija ekvivalencije prstena R (Propozicija 3.2.1).

Takodje, (m,n)-anti-inverzni elementi imaju istu sopstvenu jedinicu i jednake aditivne karakteristike. (Lema 2.3.1). Dalje, prsten Re $\mathcal{AR}_{m,n}$ sa jedinicom je polje ako i samo ako za svaki element x∈R je $A_x = R \setminus \{0\}$ (Propozicija (3.2.2).

U Teoremi 3.3.1 dokazano je da važi $\mathcal{AR}_{m,n} = \mathcal{AR}_{m,m+r}$, gdje je $n=mq+r, 0<r<m$, a zatim u Teoremi 3.3.2 dat je potreban i dovoljan uslov kada Re $\mathcal{AR}_{m,m+r}$.

Takodje, odredjeni su neki slučajevi kada je $\mathcal{AR}_{m,m+r} \subset \mathcal{AR}_{m,m+t}$ kao i neki slučajevi kada je $\mathcal{AR}_{m,m+r} = \mathcal{B}$.

3.1. DEFINICIJE I NEKA SVOJSTVA

Definicija 3.1.1. Za prsten $(R,+,\circ)$ kaže se da je (m,n)-*-anti-inverzan,* ako važi

$$(3.1) \quad (\forall x\in R)(\exists y\in R)(x^m=y^m=(xy)^m \wedge x^n=x) .$$

Klasu (m,n)-anti inverznih prstena označavaćemo $\mathcal{AR}_{m,n}$.

Neka $x\in R$ i Re $\mathcal{AR}_{m,n}$. Za element $y\in R$ koji zadovoljava (3.1) kažemo da je (m,n)-*anti-inverzan* elementu x. Skup (m,n)-anti-inverznih elemenata elementa $x\in R$ označavaćemo A_x.

Kako je $\mathcal{AR}_{m,n} \subset \mathcal{R}_n$, to su prsteni iz klase $\mathcal{AR}_{m,n}$ komutativni, regularni i semiprosti.

Primjer 3.1.1. Prsten $Z_6 \in \mathcal{AR}_{2,3}$, što se neposredno provjerava. Dalje je $A_0=\{0\}$, $A_1=A_5=\{1,5\}$, $A_2=A_4=\{2,4\}$, $A_3=\{3\}$.

Neka je R prsten takav da za svaki element $x\in R$ važi $x^n=x$. Neka je dalje $m-kn>0$. Tada je

$$x^m = x^{m-kn}x^{kn} = x^{m-kn}(x^n)^k = x^{m-kn}x^k = x^{m-kn+k} ,$$

tj. važi:

Lema 3.1.1. *Ako je R prsten takav da za svaki element* $x \in R$ *važi* $x^n = x$ *i ako je* $m-kn > 0$, *tada je* $x^{m-kn+k} = x^m$.

Posledica. *Ako je* $m-kn > 0$, *tada je* $\mathcal{AR}_{m,n} = \mathcal{AR}_{m-kn+k,n}$.

Dokaz sledi neposredno iz Leme 2.1.1.

Kako je za slučaj kada je $m > n, n > 1$, uvijek moguće naći broj k takav da je $n \geq m-kn+k > 0$, i kako je, prema prethodnoj posledici $\mathcal{AR}_{m,n} = \mathcal{AR}_{m-kn+k,n}$, to ćemo dalje razmatrati klase $\mathcal{AR}_{m,n}$, za koje je $m \leq n$.

Neka $R \in \mathcal{AR}_{m,n}$. Kako je R komutativan prsten, to za proizvoljan element $x \in R$, iz $x^m = y^m = (xy)^m$, slijedi

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

tj. važi:

Lema 3.1.2. *Ako* $R \in \mathcal{AR}_{m,n}$, *tada važi*

$$(\forall x \in R)(x^{2m} = x^m).$$

Propozicija 3.1.1. *Ako* $R \in \mathcal{AR}_{m,n}$, *tada za proizvoljan element* $x \in R$ *važi:*

a) $x^{m+1} = x$, b) $x^{n-m} = x$, $(m < n)$ c) $x^{n+m} = x$.

D o k a z. a) Neka je prvo $m = n$. Tada iz $x^m = y^m = (xy)^m$,

$x^m=x, y^m=y$, slijedi $x=y=xy$, tj. $x^2=x$, odakle je $x^{m+1}=x$.

Neka je sada $m<n$. Uz korišćenje Leme 3.1.2, za proizvoljan element $x\in R$ dobija se

$$x=x^n=x^{n-m+m}=x^{n-m}x^m=x^{n-m}x^{2m}=x^{n+m}=x^nx^m=xx^m=x^{m+1}\ .$$

b) Ako je $n=m+1$, tačnost tvrdjenja slijedi neposredno. Neka je sada $n>m+1$. Za proizvoljni element $x\in R$ važi

$$x=x^n=x^{n-m-1}x^{m+1}=x^{n-m-1}x=x\ .$$

c) Uz korišćenje tvrdjenja a) za proizvoljni element $x\in R$ važi

$$x^{n+m}=x^nx^m=xx^m=x^{m+1}=x\ .$$

Propozicija 3.1.2. *Ako za svaki element x prstena R važi $x^n=x, n>1$, tada $R\in AR_{n-1,n}$.*

D o k a z. Ako je $n=2$, tj. ako je $x^2=x$ za svako $x\in R$, tada za $y=x$ važi $x=y=xy$, pa je tvrdjenje tačno i svaki element je sam sebi (1,2)-anti-inverzan.

Neka je $n>2$. Za proizvoljan element $x\in R$ stavimo $y=x^{n-1}$.

Tada važi

$$y^{n-1}=(x^{n-1})^{n-1}=x^{n(n-2)}x=x^{n-2}x=x^{n-1}$$

i

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

tj. element $y=x^{n-1}$ je $(n-1,n)$-anti-inverzan elementu x. Dakle,

$Re\ \mathcal{AR}_{n-1,n}$.

Iz Propozicije 3.1.1 i 3.1.2 sljedi:

Posledica. *Za proizvoljne prirodne brojeve m i n važi* $\mathcal{AR}_{m,n} \subset \mathcal{AR}_{m,m+1}$.

3.2. NEKA SVOJSTVA (m,n)-ANTI-INVERZNIH ELEMENATA

Propozicija 3.2.1. *Relacija* $\sim$ *definisana na prstenu* $Re\ \mathcal{AR}_{m,n}$ *na sledeći način*

$$(\forall x,y\in R)(x\sim y \Leftrightarrow x^m=y^m=(xy)^m).$$

je relacija ekvivalencije prstena R.

D o k a z. Prema Lemi 3.1.2, za proizvoljan element $x\in R$ važi $x^{2m}=x$, pa je $(xx)^m=x^m$, tj. svaki element $x\in R$ je sam sebi (m,n)-anti-inverzan.

Kako je $Re\ \mathcal{AR}_{m,n}$ komutativan prsten, to neposredno sledi da je relacija $\sim$ simetrična.

Neka je $x\sim y$ i $y\sim z$. Tada je $x^m=y^m=(xy)^m$ i $y^m=z^m=(yz)^m$. Odavde je $x^m=z^m$. Dalje je

$$(xz)^m=x^mz^m=x^mx^m=x^{2m}=x^m\ ,$$

pa je $x\sim z$.

Lema 3.2.1. *a) Neka* $R \in \mathcal{AR}_{m,n}$ *i* $x \in R$. *Tada je* $e_x = x^m$ *i ako* $y \in A_x$ *tada je* $e_x = e_y$.

b) Ako $y \in A_x$ *tada je* $px = 0$ *ako i samo ako je* $py = 0$.

D o k a z. a) Prema Propoziciji 3.2.1, za proizvoljni element $x \in R$ važi $x^{m+1} = x$. Odavde je $x = x^m x$, tj. $e_x = x^m$.

Ako $y \in A_x$, tada je $e_x = x^m = y^m = e_y$.

b) Ako je $y \in A_x$, tada je $x = x^{m+1} = x^m x = y^m x$. Slično je $y = x^m y$. Sada iz $px = 0$ slijedi $p(x^m y) = 0$, tj. $py = 0$. Slično, iz $py = 0$ slijedi $p(y^m x) = 0$, tj. $px = 0$.

Propozicija 3.2.2. Prsten $R \in \mathcal{AR}_{m,n}$ sa jedinicom je polje ako i samo ako za svaki element $x \in R$, $x \neq 0$, važi $A_x = R \setminus \{0\}$.

D o k a z. Neka je $R \in \mathcal{AR}_{m,n}$ polje. Za proizvoljan element $x \in R$ važi $x^{m+1} = x$, odakle je, za $x \neq 0$, $x^m = 1$. Tada za svaka dva elementa $x, y \in R \setminus \{0\}$ važi $x^m = y^m = (xy)^m = 1$, tj. za svaki element $x \in R \setminus \{0\}$ važi $A_x = R \setminus \{0\}$.

Obrnuto, neka je $R \in \mathcal{AR}_{m,n}$ prsten sa jedinicom i neka za svaki element $x \in R \setminus \{0\}$ važi $A_x = R \setminus \{0\}$. Prema Propoziciji 2.2.1 dovoljno je dokazati da prsten R nema ortogonalnih idempotenata. Pretpostavimo suprotno da su $e_1, e_2 \in R$, $e_1 \neq 0$, $e_2 \neq 0$ ortogonalni idempotenti, tj. da važi $e_1 e_2 = 0$. Kako $e_1 \in A_{e_2}$, to je $e_1^m = e_2^m = (e_1 e_2)^m = 0$, tj. $e_1 = e_2 = 0$, što je suprotno pretpostavci da je $e_1 \neq 0$ i $e_2 \neq 0$. Dakle, R nema ortogonalnih, pa je R polje.

Propozicija 3.2.3. *Neka* $R \in \mathcal{AR}_{m,n}$ *i* $x \in R$. *Tada:*

a) Ako je $px=0$ i ako $y \in A_x$, tada $ky \in A_x$ ako i samo ako je $k^m-1 \equiv 0 (mod\ p)$.

b) Ako $y, z \in A_x$ tada $yz \in A_x$.

D o k a z. a) Primijetimo prvo da ako je x element prstena $Re\ \mathfrak{R}_{m,n}$, tada je $px=0$ ako i samo ako je $px^m=0$, $1<m<n$. Iz $px=0$ neposredno slijedi $px^m=0$. Ako je $px^m=0$ tada je $px=px^n=px^m \cdot x^{n-m}=0$.

Kako za $y \in A_x$ je $(ky)^m=k^m y^m=k^m x^m$, to $ky \in A_x$ ako i samo ako je $k^m x^m=x^m$, odnosno ako i samo ako je $(k^m-1)x^m=0$, tj. ako i samo ako je $k^m-1 \equiv 0 (mod\ p)$.

b) Iz $y, z \in A_x$ slijedi $x^m=y^m=(xy)^m$ i $x^m=z^m=(xz)^m$. Tada je, uz korišćenje Leme 3.1.2,

$$(yz)^m=y^m z^m=x^m x^m=x^{2m}=x^m$$

i

$$(xyz)^m=x^m(yz)^m=x^m x^m=x^{2m}=x^m \ ,$$

tj. $yz \in A_x$.

Iz prethodne propozicije se vidi da je skup A_x zatvoren u odnosu na operaciju ".". Medjutim, u opštem slučaju, skup A_x nije zatvoren u odnosu na operaciju "+". Recimo, u primjeru 3.1.1 je $A_5=\{1,5\}$, ali $1+1=2 \notin A_5$.

U opštem slučaju prsten generisan skupom A_x nije polje. Tako u Primjeru 3.1.1 skup A_5 generiše prsten R. Medjutim:

Propozicija 3.2.4. Ako element x^m pripada maksimalnom m-skupu prstena R e $\mathfrak{AR}_{m,n}$, tada je $A_x \cup \{0\} = Rx^m$.

D o k a z. Neka $y \in A_x, y \neq 0$. Tada iz $x^m = y^m$ slijedi $y^{m+1} = yx^m$, odnosno, zbog Propozicije 3.1.1, $y = yx^m$, pa $y \in Rx^m$. Dakle, $A_x \subset Rx^m$.

Neka sada $y \in R^m, y \neq 0$. Kako su y^m i $(xy)^m$ idempotenti ideala Rx^m, to, zbog Propozicije 2.2.2. važi $y^m = (xy)^m = x^m$, pa $y \in A_x$. Dakle, $Rx^m \subset A_x \cup \{0\}$.

Znači, važi $A_x \cup \{0\} = Rx^m$.

3.3. KLASA PRSTENA $\mathfrak{AR}_{m,m+r}$, $0 < r < m$

Teorema 3.3.1. Za proizvoljne prirodne brojeve m i n, gdje je $1<m<n$ i n nije djeljiv sa m, postoji prirodan broj r, $o<r<m$, takav da je

$$\mathfrak{AR}_{m,mq+r} = \mathfrak{AR}_{m,m+r} .$$

D o k a z. Kako je $n>m$ i n nije djeljivo sa m, postoje jedinstveni prirodni brojevi q i r, $o<r<n$, takvi da je $n=mq+r$. Za $q=1$ tvrdjenje je očigledno tačno. Neka je $q > 1$. Za R e $\mathfrak{AR}_{m,mq+r}$ i proizvoljno $x \in R$ postoji $y \in$ R tako da važi

$$x^m = y^m = (xy)^m \wedge x^{mq+r} = x .$$

Još je, prema Propoziciji 3.1.1, $x^{m+1} = x$. Da bi dokazali da R e $\mathfrak{AR}_{m,m+r}$, treba dokazati da još važi $x^{m+r} = x$.

Imamo

$$x = x^{mq+r} = x^{m+1}{}_{x}{}^{(q-1)m+r-1} = xx^{(q-1)m+r-1} = x^{(q-1)m+r} .$$

Ako je $q=2$, važi $x^{m+r}=x$. Ako je $q > 2$, postupak se nastavlja i poslije još $q-2$ koraka dobija se $x^{m+r}=x$.

Dakle, $\mathcal{AR}_{m,mq+r} \subset \mathcal{AR}_{m,m+r}$.

Neka sada $Re\ \mathcal{AR}_{m,m+r}$. Tada za svako $x \in R$ postoji $y \in R$ tako da važi

$$x^m = y^m = (xy)^m \wedge x^{m+r} = x.$$

Da bi važjelo $Re\ \mathcal{AR}_{m,mq+r}$ treba dokazati da je $x^{mq+r}=x$.

Imamo

$$x^{m+r}=x \Rightarrow x^{m+r}{}_{x}{}^{(q-1)m} = xx^{(q-1)m} \Rightarrow x^{mq+r} = x^{(q-1)m+1}.$$

Još je

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

tj. važi $x^{qm+r}=x$. Dakle, $\mathcal{AR}_{m,m+r} \subset \mathcal{AR}_{m,mq+r}$.

Znači, $\mathcal{AR}_{m,mq+r} = \mathcal{AR}_{m,m+r}$.

Zbog Teoreme 3.3.1, dalje ćemo razmatrati klase $\mathcal{AR}_{m,m+r}, 0 < r < m$.

Teorema 3.3.2. *Važi:*

a) $Re\ \mathcal{AR}_{m,m+1} \iff (\forall x \in R)(x^{m+1}=x)$;

b) $Re\ \mathcal{AR}_{m,m+r} \iff (\forall x \in R)(x^{m+1}=x \wedge x^{r}=x),\ (1<r<m)$.

D o k a z. a) Ako $Re\ \mathcal{AR}_{m,m+1}$, tada neposredno slijedi da za proizvoljno $x \in R$ važi $x^{m+1}=x$.

Neka sada za proizvoljno $x \in R$ važi $x^{m+1}=x$. Stavimo $y=x^{m}$. Tada je

$$y^{m}=(x^{m})^{m}=x^{m^{2}}=x^{m^{2}-1}x=(x^{m+1})^{m-1}x=x^{m-1}x=x^{m}$$

i

$$(xy)^{m}=(xx^{m})^{m}=(x^{m+1})^{m}=x^{m}\ .$$

Dakle, važi $Re\ \mathcal{AR}_{m,m+1}$, pri čemu je proizvoljnom elementu $x \in R$ (m,n)-anti-inverzan element $y=x^{m}$.

b) Neka $Re\ \mathcal{AR}_{m,m+r}$ i $x \in R$. Tada je $x^{m+1}=x$ i $x^{m+r}=x$. Dalje je

$$x=x^{m+r}=x^{m+1}x^{r-1}=xx^{r-1}=x^{r}\ .$$

Neka sada za $x \in R$ važi $x^{m+1}=x$ i $x^{r}=x$. Tada je

$$x^{m+r}=x^{m}x^{r}=x^{m}x=x^{m+1}=x.$$

Elementu x je $(m,m+r)$-anti-inverzan element $y=x^{m}$, što se dokazuje sasvim analogno kao u dokazu a).

Lema 3.3.1. Neka $Re\ \mathcal{AR}_{m,m+r}$ i neka je k proizvoljan prirodan broj, takav da je $m-kr+k+1>0$. Tada za proizvoljan element $x \in R$ važi

(3.3.1) $$x^{m-kr+k+1}=x\ .$$

D o k a z. Neka je $m-r+2 > 0$. Tada je

$$x^{m-r+2}=x^{m-r+1}x=x^{m-r+1}x^{r}=x^{m+1}=x,$$

tj. tvrdjenje je tačno za k=1.

Neka je sada $k > 1$ i $m-kr+k+1 > 0$ i neka važi

$$x^{m-kr+k+1}=x.$$

Ako je $m-(k+1)r+k+2 > 0$, tada je

$$x^{m-(k+1)r+k+2}=x^{m-(k+1)r+k+1}x=x^{m-(k+1)r+k+1}x^{r}=x^{m-kr+k+1}=x.$$

Dakle, za svako k za koje je $m-kr+k+1 > 0$, važi (3.3.1).

Sada je moguće odrediti neke slučajeve kada je

$\mathcal{AR}_{m,m+r} \subset \mathcal{AR}_{m,m+t}, 0 < r < m, 0 < t < m.$

Propozicija 3.3.1. *Neka je $m > 1$. Ako je $2r-1=t$ ili $2r-1=m+t$, tada je $\mathcal{AR}_{m,m+r} \subset \mathcal{AR}_{m,m+t}$.*

D o k a z. Neka je $2r-1=t$. Za r=1, dobija se t=1 i tačnost tvrdjenja slijedi neposredno.

Neka je $r > 1$, Re $\mathcal{AR}_{m,m+r}$ i xeR. Tada je, prema Teoremi 3.3.2, $x^{m+1}=x$ i $x^{r}=x$. Dalje je

$$x^{t}=x^{2r-1}=x^{r}x^{r-1}=xx^{r-1}=x^{r}=x.$$

Iz $x^{m+1}=x$ i $x^{t}=x$ za svako xeR, prema Teoremi 3.3.2, slijedi da Re $\mathcal{AR}_{m,m+t}$. Dakle, ako je $2r-1=t$, tada je $\mathcal{AR}_{m,m+r} \subset \mathcal{AR}_{m,m+t}$.

Neka je sada $2r-1=m+t$. Očigledno mora biti $r > 1$, jer bi inače, zbog $m > 1$, bilo $t < 0$. Neka Re $\mathcal{AR}_{m,m+r}$ i $x \in R$. Tada je $x^{m+1}=x$ i $x^r=x$. Ako je $t=1$, prema Teoremi 3.3.2, važi Re $\mathcal{AR}_{m,m+t}$. Neka je $t > 1$. Tada je

$$x^{m+t}=x^{2r-1}=x^r x^{r-1}=xx^{r-1}=x^r=x$$

i

$$x^t=xx^{t-1}=x^{m+1}x^{t-1}=x^{m+t}=x.$$

Iz $x^{m+1}=x$ i $x^t=x$, za proizvoljno $x \in R$, slijedi Re $\mathcal{AR}_{m,m+t}$.

Dakle, ako je $2r-1=m+t$, tada je $\mathcal{AR}_{m,m+r} \subset \mathcal{AR}_{m,m+t}$.

Navešćemo primjer iz kojeg se vidi da u opštem slučaju je $\mathcal{AR}_{m,m+r} \neq \mathcal{AR}_{m,m+t}$, kada m,r i t zadovoljavaju uslove Propozicije 3.3.1.

Primjer 3.3.1. a) Neka je $m=14$, $r=4$ i $t=7$. Tada je $2r-1=t$ i prema Propoziciji 3.3.1 važi $\mathcal{AR}_{14,18} \subset \mathcal{AR}_{14,21}$.

Za proizvoljan element x prstena Z_6 važi $x^3=x$, što se inače lako provjerava. Odavde je $x^7=x$ i $x^{15}=x$, tj. $Z_6 \in \mathcal{AR}_{14,21}$. Medjutim, $Z_6 \notin \mathcal{AR}_{14,18}$, jer je $2^4=4$.

b) Neka je $m=14$, $r=10$ i $t=5$. Tada je $2r-1=m+t$, pa prema

Propoziciji 3.3.1 važi $\mathcal{AR}_{14,24} \subset \mathcal{AR}_{14,19}$. Za proizvoljni element x prstena Z_6 važi $x^{15}=x$ i $x^5=x$, pa $Z_6 \in \mathcal{AR}_{14,19}$. Medjutim, kako je $2^{10}=4$, to $Z_6 \notin \mathcal{AR}_{14,24}$.

Neka $R \in \mathcal{AR}_{m,m+r}$. Tada, prema Teoremi 3.3.2, za svaki element $x \in R$ važi $x^{m+1}=x$, za $r=1$, odnosno $x^{m+1}=x$ i $x^r=x$ za $r>1$. Sada, prema Lemi 2.2.1 važi:

Lema 3.3.2. Ako $R \in \mathcal{AR}_{m,m+r}$, tada za svaki element $x \in R$ je x^m idempotent, ako je $r=1$, odnosno elementi x^m i x^{r-1} su idempotenti, ako je $r>1$.

Iz Teoreme 3.3.2 slijedi da je, za fiksirano m, klasa $\mathcal{AR}_{m,m+r}$ zatvorena u odnosu na formiranje podprstena, direktnih proizvoda i homomorfnih slika. Dakle, klasa $\mathcal{AR}_{m,m+r}$ je mnogostrukost.

3.4. O KLASAMA $\mathcal{AR}_{m,m+r}$, $0 \leq r < m$, ČIJI SU PRSTENI BULOVI

U prethodnim razmatranjima klase $\mathcal{AR}_{m,m+r}$, nije uziman u obzir slučaj kada je $r=0$. Takodje, uvijek je pretpostavljeno

da je $m > 1$. Ovdje ćemo, pored ostalog, razmatrati i takve klase, tj. klase $\mathcal{AR}_{1,n}$ i $\mathcal{AR}_{m,m}$.

Ako je R Bulov prsten, tada Re $\mathcal{AR}_{m,m+r}$ za svaki prirodan broj m. Naime, tada za proizvoljno $x \in R$ važi $x^2=x$, odakle je $x^{m+1}=x$ i $x^r=x$, pa prema Teoremi 3.3.2 slijedi Re $\mathcal{AR}_{m,m+r}$.

Dakle, klasa Bulovih Prstena $\mathcal{B}$ je podklasa klase $\mathcal{AR}_{m,m+r}$.

Propozicija 3.4.1. *Za proizvoljne prirodne brojeve m i n važi:*

a) $\mathcal{AR}_{1,n} = \mathcal{B}$, b) $\mathcal{AR}_{m,m} = \mathcal{B}$.

D o k a z. a) Prema prethodnom razmatranju, treba dokazati da je $\mathcal{AR}_{1,n} \subset \mathcal{B}$. Neka Re $\mathcal{AR}_{1,n}$ i $x \in R$. Tada postoji element $y \in R$ takav da važi $x=y=xy$. Odavde je $x^2=x$, tj. Re $\mathcal{B}$. Dakle, $\mathcal{AR}_{1,n} = \mathcal{B}$.

b) Takodje treba dokazati da je $\mathcal{AR}_{m,m} \subset \mathcal{B}$. Neka Re $\mathcal{AR}_{m,m}$ i $x \in R$. Tada postoji element $y \in R$, tako da je

$$x^m=y^m=(xy)^m \wedge x^m=x \quad .$$

Odavde je $x=y=xy$, t.j. $x^2=x$. Dakle, Re $\mathcal{B}$, t.j. $\mathcal{AR}_{m,m} = \mathcal{B}$.

Moguće je odrediti još neke slučajeve kada je $\mathfrak{AR}_{m,m+r} = \mathfrak{B}$:

Propozicija 3.4.2. Ako postoji broj $k \geq 0$, takav da je tačna jedna od relacija:

(1) $m-kr+k+1=2$;

(2) $m-kr+k+1=r-1$;

(3) $2(m-kr+k+1)=r$,

tada je $\mathfrak{AR}_{m,m+r} = \mathfrak{B}$.

D o k a z. Kako je $\mathfrak{B} \subset \mathfrak{AR}_{m,m+r}$, za svako m i r, to u svakom od ovih slučajeva treba dokazati da važi $\mathfrak{AR}_{m,m+r} \subset \mathfrak{B}$.

Ako $R \in \mathfrak{AR}_{m,m+r}$, tada za svako $x \in R$, prema Lemi 3.3.1, za $m-kr+k+1 > 0$ važi $x^{m-kr+k+1}=x$, a prema Teoremi 3.3.2 važi $x^r=x$.

Sada, ako je $m-kr+k+1=2$, važi

$$x=x^{m-kr+k+1}=x^2 ,$$

tj. $R \in \mathfrak{B}$, odnosno $\mathfrak{AR}_{m,m+r} \subset \mathfrak{B}$.

Ako je $m-kr+k+1=r-1$, tada je $x^{r-1}=x$. Dalje je $x=x^r=x^{r-1}x=x^2$, tj. u ovom slučaju je $R \in \mathfrak{B}$, odnosno $\mathfrak{AR}_{m,m+r} \subset \mathfrak{B}$.

Na kraju, ako je $2(m-kr+k+1)=r$, tada za $x \in R$ važi

$$x=x^r=x^{2(m-kr+k+1)}=(x^{m-kr+k+1})^2=x^2 ,$$

tj. $R \in \mathfrak{B}$, odnosno $\mathfrak{AR}_{m,m+r} \subset \mathfrak{B}$.

GLAVA IV

KLASA ANTI-INVERZNIH PRSTENA

Ovdje ćemo razmatrati klasu prstena $\mathcal{AR}$, kojoj pripadaju prsteni $(R,+,\cdot)$ čija je semigrupa $(R,\cdot)$ anti-inverzna. Kako, prema Teoremi 2.1 iz [3], za svaki element iz R važi $x^5=x$, to su prsteni iz klase $\mathcal{AR}$ komutativni, regularni i semiprosti.

U Propoziciji 4.1.1 dokazuje se da prsten R pripada klasi $\mathcal{AR}$ ako i samo ako za svaki njegov element važi $x^3=x$. Odavde slijedi da je $\mathcal{AR} = \mathcal{AR}_{2,3}$. Dalje, element yeR je anti-inverzan elementu xeR ako i samo ako je y (2,3)-anti-inverzan element elementu x (Propozicija 4.1.2).

U tački 4.2 odredjeni su neki slučajevi kada je $\mathcal{AR}_{m,m+r} \subset \mathcal{AR}$.

U tački 4.3. razmatrana je klasa prstena $Q\mathcal{AR}$ čiji je svaki pravi potprsten iz klase $\mathcal{AR}$. Pored ostalog, odredjen je potreban i dovoljan uslov kada polje od p^m elemenata pripada klasi $Q\mathcal{AR}$.

Posebna pažnja posvećena je odredjivanju bazisne klase u smislu Ljapina za klasu $\mathcal{AR}$ u odnosu na klasu svih prstena $\mathcal{R}$. Tu klasu sačinjavaju trivijalni prsten, polja Z_2 i Z_3, prsteni Z_6, R_9, R_{18} i R_{36}, gdje su prsteni R_9, R_{18} i R_{36} prsteni od 9,18 odnosno 36 elemenata opisani u tački 4.4.

Na kraju, u tački 4.5 odredjena je bazisna klasa u smislu Ljapina za klasu $\mathfrak{AR}_4$ (prsteni iz ove klase nijesu anti-inverzni) u odnosu na klasu svih prstena $\mathfrak{R}$.

4.1. DEFINICIJE I NEKA SVOJSTVA

Definicija 4.1.1. Za prsten $(R,+,\cdot)$ kaže se da je *anti-inverzan, ako važi*

$$(\forall x\in R)(\exists y\in R)(xyx=y \wedge yxy=x) .$$

Za element y tada se kaže da je *anti-inverzan* elementu x. Klasu anti-inverznih prstena označavaćemo sa $\mathfrak{AR}$.

Primjer 4.1.1. Svaki Bulov prsten B je anti-inverzan. Element x je sam sebi anti-inverzan, jer važi xxx=x.

Primjer 4.1.2. Prsten Z_6 je takodje anti-inverzan prsten. Neposredno se provjerava da, recimo, elementi 0 i 3 su sami sebi anti-inverzni, dok su elementi 1 i 5, odnosno 2 i 4 jedan drugom anti-inverzni.

Primjer 4.1.3. Neka je $R\in\mathfrak{AR}$ i P(E) Bulov prsten iz Primjera 2.1.2. Prsten RxP(E) je takodje anti-inverzan prsten. Naime, ako je elementu $x\in R$ anti-inverzan element $x'\in R$, tada je elementu $(x,y)\in RxP(E)$ anti-inverzan element $(x';y)\in RxP(E)$, jer važi

$$(x,y)(x;y)(x,y)=(xx'x,yyy)=(x;y)$$

i

$$(x;y)(x,y)(x;y)=(x'xx;yyy)=(x,y).$$

Prema Teoremi 2.1. iz [3] i Jecobsonove teoreme, slijedi da je svaki anti-inverzni prsten komutativan.

Propozicija 4.1.1. *Neka je R prsten. Tada*

$$R\in\mathfrak{AR} \iff (\forall x\in R)(x^3=x) .$$

D o k a z. Ako za svako $x\in R$ važi $x^3=x$, tada je svaki element $x\in R$ sam sebi anti-inverzan, tj. $R\in\mathfrak{AR}$.

Pretpostavimo da $R\in\mathfrak{AR}$. Neka je x proizvoljan element prstena R i $y\in R$ njemu anti-inverzan element. Na osnovu Teoreme 2.1 iz [3] važi $x^2=y^2$. Zbog komutativnosti prstena R iz yxy=x slijedi $y^2x=x$, a odavde je $x^3=x$.

Iz ove Propozicije i Primjera 2.4.1 neposredno slijedi:

Posljedica. *Jedina konačna polja koja pripadaju klasi* $\mathfrak{AR}$ *su* Z_2 *i* Z_3.

Posljedica 2. *Važi* $\mathfrak{AR}=\mathfrak{AR}_{2,3}$.

Još je:

Propozicija 4.1.2. *Neka* $R\in\mathfrak{AR}$ *i neka* $x\in R$. *Element* $y\in R$ *je anti-inverzan element elementa x ako i samo ako je y (2,3)-anti--inverzan elementu x.*

D o k a z. Neka je y anti-inverzan element elementa x. Tada, zbog komutativnosti prstena R, važi $x^2y=y$ i $xy^2=x$.

Odavde je $x^2y^2=y^2$ i $x^2y^2=x^2$, odnosno $x^2=y^2=(xy)^2$, tj. y je anti-inverzan element elementa x.

Neka je sada y (2,3)-anti-inverzan element elementa x. tada iz $x^2=y^2$ sljedi $x^2y=y^3=y$, pa je y anti-inverzan element elementa x.

4.2. NEKE KLASE $\mathcal{AR}_{m,m+r}$ ZA KOJE VAŽI $\mathcal{AR}_{m,m+r}\subset\mathcal{AR}$

Kako je $\mathcal{B}\subset\mathcal{AR}$, to prema Propoziciji 3.4.1 važi $\mathcal{AR}_{1,n}\subset\mathcal{AR}$ i $\mathcal{AR}_{m,m}\subset\mathcal{AR}$, a prema Propoziciji 3.4.2, ako postoji broj $k>0$ takav da važi jedan od uslova $m-kr+k+1=2$, $m-kr+k+1=r-1$ ili $2(m-kr+k+1)=r$, takodje važi $\mathcal{AR}_{m,m+r}\subset\mathcal{AR}$.

Ovdje ćemo odrediti još neke slučajeve kada je $\mathcal{AR}_{m,m+r}\subset\mathcal{AR}$.

Propozicija 4.2.1. Ako postoji broj $k\geq 0$ takav da važi jedan od uslova:

(1) $m-kr+k+1=3$,

(2) $m-kr+k+1=r-2$,

(3) $3(m-kr+k+1)=r$,

(4) $3(m-kr+k+1)=m-1$,

tada je $\mathcal{AR}_{m,m+r}\subset\mathcal{AR}$.

D o k a z. Neka $Re\,\mathcal{AR}_{m,m+r}$. Tada, prema Lemi 3.3.1, za $m-kr+k+1>0$ važi $x^{m-kr+k+1}=x$, a prema Teoremi 3.3.2, važi $x^r=x$.

Sada, ako je $m-kr+k+1=3$, važi

$$x=x^{m-kr+k+1}=x^3\ ,$$

odakle, zbog Propozicije 4.1.1, važi $Re\mathfrak{AR}$.

Uslov (2) ne važi ako je r=1, jer je tada m=-2, što je nemoguće. Za r=2 neposredno slijedi $Re\mathfrak{B}$, odnosno $Re\mathfrak{AR}$. Neka je $r > 2$. Ako je m-kr+k+1=r-2, tada za $x\in R$ važi $x=x^{r-2}$.

Sada je

$$x=x^r=x^{r-2}x^2=xx^2=x^3 \quad ,$$

tj. $Re\mathfrak{AR}$.

Ako je 3(m-kr+k+1)=r, tada za $x\in R$ važi

$$x=x^r=x^{3(m-kr+k+1)}=(x^{m-kr+k+1})^3=x^3,$$

tj. $Re\mathfrak{AR}$.

Neka je sada 3(m-kr+k+1)=m-1 i m > 1, (jer za m=1 neposredno slijedi da $Re\mathfrak{B}$, odnosno $Re\mathfrak{AR}$). Tada za $x\in R$ važi $x^{m-1}=x$.

Dalje je

$$x=x^{m+1}=x^{m-1}x^2=xx^2=x^3 \quad ,$$

tj. i u ovome slučaju važi $Re\mathfrak{AR}$.

4.3. O PRSTENIMA ČIJI JE SVAKI PRAVI PODPRSTEN ANTI-INVERZAN

Ovdje ćemo razmatrati klasu, u oznaci $\mathfrak{QAR}$, onih prstena, čiji je svaki pravi podprsten iz klase $\mathfrak{AR}$.

Neposredno slijedi da je $\mathfrak{AR}\subset\mathfrak{QAR}$. Naime, ako je R anti-inverzan prsten, tada je i svaki njegov pravi podprsten takodje anti-inverzan, tj. $Re\mathfrak{QAR}$, tj. $\mathfrak{AR}\subset\mathfrak{QAR}$.

Primjer 4.3.1. Prsteni $Z_2, Z_3, Z_2 \times Z_3$ i Z_6 su iz klase $\mathfrak{OAR}$, jer su ovi prsteni anti-inverzni.

Primjer 4.3.2. Prsten O_3 zadan sljedećim tablicama

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	0	0
2	0	0	0

je iz klase $\mathfrak{QAR}$. Naime, jedini njegov pravi podprsten je $\{0\}$, i on je anti-inverzan.

Primjer 4.3.3. Takodje, jedini pravi podprsten prstena Z_5 je $\{0\}$, pa $Z_5 \in \mathfrak{QAR}$.

Primjer 4.3.4. Polje GF(4) takodje pripada klasi $\mathfrak{OAR}$. Naime, jedini pravi podprsteni od GF(4) su $\{0\}$ i $\{0,a\}$ i oni su anti-inverzni, što se neposredno provjerava.

Neka je $(O_p, +, \cdot)$ prsten, gdje je $O_p = \{0,1,\ldots,p\}$, operacija "+" sabiranje po modulu p i operacija "." definisana sa $a \cdot b = 0$ za svako $a, b \in O_p$.

U Primjeru 4.3.2 vidjeli smo da $O_3 \in \mathfrak{QAR}$. Za prstene O_p važi:

Propozicija 4.3.1. *Prsten O_p pripada klasi $\mathfrak{QAR}$ ako i samo ako je p=1 ili ako je p prost broj.*

D o k a z. Ako je p=1, tada prsten O_1 nema pravih podprstena, pa $O_p \in \mathfrak{QAR}$. Ako je p prost broj, jedini pravi podprsten prstena O_p je $\{0\}$, pa takodje $O_p \in \mathfrak{QAR}$.

Neka je sada p složen broj i neka je r prost djelilac broja p. Prema Teoremi Silova, postoji podgrupa (R,+) od r elemenata aditivne grupe $(0_p,+)$. Tada je prsten (R,+,.) pravi podprsten prstena 0_p. Medjutim, prsten R nije antiinverzan, jer za $x\in R$, $x\neq 0$ je $x^3=0$. Dakle, ako p nije prost broj prsten 0_p nije iz klase Q.

U Primjerima 4.3.3 i 4.3.4 vidjeli smo da su polja Z_3, Z_5 i GF(4) iz klase QAR . Postavlja se pitanje da li postoje i druga konačna polja koja su iz klase QAR . U tom smislu važi:

Propozicija 4.3.2. *Polje $GF(p^m)$ pripada klasi QAR ako i samo ako je $p=2$ ili $p=3$ i ako je m prost broj.*

D o k a z. Primijetimo prvo, da je svaki nenulti podprsten polja $GF(p^m)$ takodje polje. Naime, prema Propoziciji 1.6.3 slijedi da je multiplikativna grupa $(GF(p^m)^*,\cdot)$ ciklična grupa reda p^m-1 i da prema tome za svako $x\in GF(p^m)^*$ važi $x^{p^m-1}=1$.

Neka je p=2 (odnosno p=3) i m prost broj. Tada, prema Propoziciji 1.6.4 jedino pravo podpolje polja $GF(2^m)$,(odnosno polja $GF(3^m)$ je polje $GF(2)=Z_2$, (odnosno polje $GF(3)=Z_3$). Kako polje Z_2, (odnosno polje Z_3) pripada klasi AR , to je $GF(2^m)$ iz klase QAR , za slučaj kada je m prost broj.

Ako je $p>3$, tada polje $GF(p^m)$ ima podpolje izomorfno sa poljem Z_p. Kako za $p>3$ polje Z_p nije iz AR , to u ovome slučaju $GF(p^m)$ nije iz klase QAR .

Neka sada m nije prost broj i neka je d djelilac broja n,($d\neq 1, d\neq n$). Tada je polje $GF(p^d)$ pravo podpolje polja $GF(p^m)$. Kako polje $GF(p^d)$ nije iz $\mathfrak{AR}$, to polje $GF(p^m)$ nije iz $\mathfrak{Q}$.

Propozicija 4.3.3. *Neka su* R_1 *i* R_2, $R_1\neq\{o\}$, $R_2\neq\{o\}$ *prsteni. Važi*

$$R_1 \times R_2 \in \mathfrak{QAR} \iff R_1 \in \mathfrak{AR} \wedge R_2 \in \mathfrak{AR} .$$

D o k a z. Ako $R_1 \in \mathfrak{AR}$ i $R_2 \in \mathfrak{AR}$, tada $R_1 \times R_2 \in \mathfrak{QAR}$, jer za proizvoljno $(x,y) \in R_1 \times R_2$ važi $(x,y)^3=(x^3,y^3)=(x,y)$. No to znači da $R_1 \times R_2 \in \mathfrak{Q}$.

Neka sada $R_1 \times R_2 \in \mathfrak{QAR}$. Pretpostavimo da jedan od prstena R_1 ili R_2, recimo R_1, nije iz klase $\mathfrak{AR}$. Prsten $P=R_1 \times \{0\}$ je pravi podprsten prstena $R_1 \times R_2$. Kako $R_1 \notin \mathfrak{AR}$, to postoji $x \in R_1$ tako da je $x^3\neq x$. Tada je $(x,0)^3=(x^3,0)\neq(x,0)$; tj. prsten P nije iz $\mathfrak{AR}$. No, to znači da $R_1 \times R_2 \notin \mathfrak{QAR}$, što je u kontradikciji sa pretpostavkom da $R_1 \times R_2 \in \mathfrak{QAR}$.

4.4. O BAZISNOJ KLASI U SMISLU LJAPINA ZA KLASU $\mathcal{AR}$

Konstruisaćemo prvo neke primjere anti-inverznih prstena, koji će biti od značaja za odredjivanje bazisne klase u smislu Ljapina za klasu prstena $\mathcal{AR}$ u odnosu na klasu svih prstena $\mathcal{R}$.

Primjer 4.4.1. Neka $R \in \mathcal{AR}$ i neka $x \in R, x \neq 0$. Neka je dalje $2x=0$. Tada je $(x+x^2)^2=x^2+x^4=x^2+x^2=2x^2=0$, odakle je $x+x^2=0$, odnosno $x^2=x$. Dakle, u ovome slučaju element x generiše anti-inverzni podprsten R_2 sa elementima 0 i x, koji je izomorfan sa prstenom Z_2.

Primjer 4.4.2. Neka $R \in \mathcal{AR}$ i $x \in R$, $x \neq 0$. Neka je dalje $3x=0$. Ako je $x^2=x$, tada element x generiše tročlani podprsten R_3 sa elementima 0,x i 2x:

+	0	x	2x
0	0	x	2x
x	x	2x	0
2x	2x	0	x

·	0	x	2x
0	0	0	0
x	0	x	2x
2x	0	2x	x

a ako je $x^2=2x$ tročlani prsten sa elementima o,x i 2x:

+	0	x	2x
0	0	x	2x
x	x	2x	0
2x	2x	0	x

·	0	x	2x
0	0	0	0
x	0	2x	x
2x	0	x	2x

U oba slučaja dobijaju se prsteni izomorfni sa Z_3.

Primjer 4.4.3. Neka $Re\mathfrak{A}\mathfrak{R}$ i neka $xeR, x\neq 0$, $3x=0$. Neka je dalje $x^2\neq x$ i $x^2\neq 2x$. Kako iz $2x^2=x$ slijedi $x^2=2x$, to je $2x^2\neq x$. Takodje je $2x^2\neq x^2$, jer bi u protivnom važjelo $2x=x$, odnosno $x=0$. Dalje je $2x^2\neq 2x$. Naime, ako bi bilo $2x^2=2x$ važjelo bi $(2x+x^2)^2=x+2x^2=0$, tj. $2x+x^2=0$, odakle je $x^2=x$.

Dalje, zbog

1. $x+x^2=x \Rightarrow x^2=0 \Rightarrow x=0$,
2. $x+x^2=2x \Rightarrow x^2=x$,
3. $x+x^2=x^2 \Rightarrow x=0$,
4. $x+x^2=2x^2 \Rightarrow x^2=x$,
5. $x+2x^2=x \Rightarrow 2x^2=0 \Rightarrow x=0$,
6. $x+2x^2=2x \Rightarrow 2x^2=x$,
7. $x+2x^2=x^2 \Rightarrow 2x^2=x$,
8. $x+2x^2=2x^2 \Rightarrow x=0$,
9. $x+2x^2=x+x^2 \Rightarrow x^2=0 \Rightarrow x=0$,
10. $2x+x^2=x \Rightarrow x^2=2x$,
11. $2x+x^2=2x \Rightarrow x^2=0 \Rightarrow x=0$,
12. $2x+x^2=x^2 \Rightarrow 2x=0 \Rightarrow x=0$,
13. $2x+x^2=2x^2 \Rightarrow x^2=2x$,
14. $2x+x^2=x+x^2 \Rightarrow x=0$,
15. $2x+x^2=x+2x^2 \Rightarrow x^2=x$,
16. $2x+2x^2=x \Rightarrow 2x^2=2x$,
17. $2x+2x^2=2x \Rightarrow 2x^2=0 \Rightarrow x=0$,
18. $2x+2x^2=x^2 \Rightarrow 2x^2=2x$,
19. $2x+2x^2=2x^2 \Rightarrow 2x=0 \Rightarrow x=0$,
20. $2x+2x^2=x+x^2 \Rightarrow x+x^2=0 \Rightarrow x^2=2x$,
21. $2x+2x^2=x+2x^2 \Rightarrow x=0$,
22. $2x+2x^2=2x+x^2 \Rightarrow x^2=0 \Rightarrow x=0$,

važi

1: $x+x^2\neq x$, 7: $x+2x^2\neq x^2$, 13: $2x+x^2\neq 2x^2$, 19: $2x+2x^2\neq 2x^2$,
2: $x+x^2\neq 2x$, 8: $x+2x^2\neq 2x$; 14: $2x+x^2\neq x+x^2$, 20: $2x+2x^2\neq x+x^2$,
3: $x+x^2\neq x^2$, 9: $x+2x^2\neq x+x^2$, 15: $2x+x^2\neq x+2x^2$, 21: $2x+2x^2\neq x+2x^2$,
4: $x+x^2\neq 2x^2$, 10: $2x+2x^2\neq x$, 16: $2x+2x^2\neq x$, 22: $2x+2x^2\neq 2x+x^2$.
5: $x+2x^2\neq x$, 11: $2x+x^2\neq x$, 17: $2x+2x^2\neq 2x$,
6: $x+2x^2\neq 2x$, 12: $2x+x^2\neq x^2$, 18: $2x+2x^2\neq x^2$,

Dakle, u ovome slučaju element x generiše podprsten R_9 od 9 elemenata $0,x,2x,x^2,\ 2x^2,\ x+x^2,x+2x^2,\ 2x+x^2$ i $2x+2x^2$:

+	0	x	2x	x^2	$2x^2$	$x+x^2$	$x+2x^2$	$2x+x^2$	$2x+2x^2$
0	0	x	2x	x^2	$2x^2$	$x+x^2$	$x+2x^2$	$2x+x^2$	$2x+2x^2$
x	x	2x	0	$x+x^2$	$x+2x^2$	$2x+x^2$	$2x+2x^2$	x^2	$2x^2$
2x	2x	0	x	$2x+x^2$	$2x+2x^2$	x^2	$2x^2$	$x+x^2$	$x+2x^2$
x^2	x^2	$x+x^2$	$2x+x^2$	$2x^2$	0	$x+2x^2$	x	$2x+2x^2$	2x
$2x^2$	$2x^2$	$x+2x^2$	$2x+2x^2$	0	x^2	x	$x+x^2$	2x	$2x+x^2$
$x+x^2$	$x+x^2$	$2x+x^2$	x^2	$x+2x^2$	x	$2x+2x^2$	2x	$2x^2$	0
$x+2x^2$	$x+2x^2$	$2x+2x^2$	$2x^2$	x	$x+x^2$	2x	$2x+x^2$	0	x^2
$2x+x^2$	$2x+x^2$	x^2	$x+x^2$	$2x+2x^2$	2x	$2x^2$	0	$x+2x^2$	0
$2x+2x^2$	$2x+2x^2$	$2x^2$	$x+2x^2$	2x	$2x+x^2$	0	x^2	x	$x+x^2$

·	0	x	2x	x^2	$2x^2$	$x+x^2$	$x+2x^2$	$2x+x^2$	$2x+2x^2$
0	0	0	0	0	0	0	0	0	0
x	0	x^2	$2x^2$	x	2x	$x+x^2$	$2x+x^2$	$x+2x^2$	$2x+2x^2$
2x	0	$2x^2$	x^2	2x	x	$2x+2x^2$	$x+2x^2$	$2x+x^2$	$x+x^2$
x^2	0	x	2x	x^2	$2x^2$	$x+x^2$	$x+2x^2$	$2x+x^2$	$2x+2x^2$
$2x^2$	0	2x	x	$2x^2$	x^2	$2x+2x^2$	$2x+x^2$	$x+2x^2$	$x+x^2$
$x+x^2$	0	$x+x^2$	$2x+2x^2$	$x+x^2$	$2x+2x^2$	$2x+2x^2$	0	0	$x+x^2$
$x+2x^2$	0	$2x+x^2$	$x+2x^2$	$x+2x^2$	$2x+x^2$	0	$x+2x^2$	$2x+2x^2$	0
$2x+x^2$	0	$x+2x^2$	$2x+x^2$	$2x+x^2$	$x+2x^2$	0	$2x+x^2$	$x+2x^2$	0
$2x+2x^2$	0	$2x+2x^2$	$x+x^2$	$2x+2x^2$	$x+x^2$	$x+x^2$	0	0	$2x+2x^2$

Lema 4.4.1. *Neka* $R \in \mathcal{R}$ *i neka je* $x \in R$, $x \neq 0$. *Ako je* $5x=0$, $(2x \neq 0, 3x \neq 0)$, *tada važi:*

1. $x^2 \neq 2x$,
2. $x^2 \neq 3x$,
3. $x^2 \neq 4x$,
4. $2x^2 \neq x$,
5. $2x^2 \neq 3x$,
6. $2x^2 \neq 5x$,
7. $3x^2 \neq x$,
8. $3x^2 \neq 2x$,
9. $3x^2 \neq 4x$,
10. $3x^2 \neq 5x$,
11. $4x^2 \neq x$,
12. $4x^2 \neq 3x$,
13. $4x^2 \neq 5x$,
14. $5x^2 \neq 2x$,
15. $5x^2 \neq 3x$,
16. $5x^2 \neq 4x$.

D o k a z. Gore navedene relacije važe zbog:

1: $x^2=2x \Rightarrow x^3=2x^2 \Rightarrow x=2x^2 \Rightarrow x=4x \Rightarrow 3x=0$,

2: $x^2=3x \Rightarrow x^3=3x^2 \Rightarrow x=3x^2 \Rightarrow x=9x \Rightarrow 4x=0 \Rightarrow 2x=0$,

3: $x^2=4x \Rightarrow x^3=4x^2 \Rightarrow x=4x^2 \Rightarrow x=16x \Rightarrow 3x=0$,

4: $2x^2=x \Rightarrow 2x^3=x^2 \Rightarrow x^2=2x$,

5: $2x^2=3x \Rightarrow 2x^3=3x^2 \Rightarrow 2x=3x^2 \Rightarrow 4x=6x^2 \Rightarrow 4x=0 \Rightarrow 2x=0$,

6: $2x^2=5x \Rightarrow 2x^3=5x^2 \Rightarrow 2x=5x^2 \Rightarrow 4x=10x^2 \Rightarrow 4x=x \Rightarrow 3x=0$,

7: $3x^2=x \Rightarrow 3x^3=x^2 \Rightarrow x^2=3x$,

8: $3x^2=2x \Rightarrow 3x^3=2x^2 \Rightarrow 2x^2=3x$,

9: $3x^2=4x \Rightarrow 3x^3=4x^2 \Rightarrow 3x=4x^2 \Rightarrow 2x^2=3x$,

10: $3x^2=5x \Rightarrow 3x^3=5x^2 \Rightarrow 3x=5x^2 \Rightarrow x^2=3x$,

11: $4x^2=x \Rightarrow 4x^3=x^2 \Rightarrow x^2=4x$,

12: $4x^2=3x \Rightarrow 4x^3=3x^2 \Rightarrow 4x=5x^2 \Rightarrow x^2=2x$,

13: $4x^2=5x \Rightarrow 4x^3=5x^2 \Rightarrow 4x=5x^2 \Rightarrow x^2=2x$,

14: $5x^2=2x \Rightarrow 5x^3=2x^2 \Rightarrow 2x^2=5x$,

15: $5x^2=3x \Rightarrow 5x^3=3x^2 \Rightarrow 3x^2=5x$,

16: $5x^2=4x \Rightarrow 5x^3=4x^2 \Rightarrow 5x=4x^2 \Rightarrow 2x^2=x$.

Lema 4.4.2. Neka $R \in \mathcal{AR}$ *i* $x \in R, x \neq 0$. *Ako je* $6x=0, (2x\neq 0, 3x\neq 0)$, *tada važi:*

1. $x^2=x \iff 5x^2=5x \iff 2x^2=2x \iff 4x^2=4x$,
2. $x^2=5x \iff 5x^2=x \iff 2x^2=4x \iff 4x^2=2x$.

D o k a z. 1. Zbog $6x=6x^2=0$, neposredno slijedi da je $x^2=x \iff 5x^2=5x$ i $2x^2=2x \iff 4x^2=4x$. Dokazaćemo da je $x^2=x \iff 2x^2=2x$. Iz $x^2=x$ neposredno slijedi $2x^2=2x$. Neka je sada $2x^2=2x$. Tada je $(x+5x^2)^2=4x+2x^2=6x=0$, odakle je $x+5x^2=0$, odnosno $x^2=x$.

2. Zbog $6x=6x^2=0$, važi $x^2=5x \iff 5x^2=x$ i $2x^2=4x \iff 4x^2=2x$. Dokazaćemo da je $x^2=5x \iff 2x^2=4x$. Ako je $x^2=5x$, tada je $2x^2=10x=4x$. Ako je $2x^2=4x$, tada iz $(x+5x^2)^3=4x+2x^2=2x$ slijedi $x+5x^2=2x$, odakle je $x^2=5x$.

P r i m j e r 4.4.4. Neka $R \in \mathcal{AR}$, $x \in R$, $x\neq 0$, $6x=0$, $2x\neq 0$, $3x\neq 0$. Prema Lemi 4.4.1 može da važi $x^2=x$ ili $x^2=5x$.

Ako je $x^2=x$, tada element x generiše prsten R_6 od 6 elemenata $0,x,2x,3x,4x$ i $5x$:

+	0	x	2x	3x	4x	5x
0	0	x	2x	3x	4x	5x
x	x	2x	3x	4x	5x	0
2x	2x	3x	4x	5x	0	x
3x	3x	4x	5x	0	x	2x
4x	4x	5x	0	x	2x	3x
5x	5x	0	x	2x	3x	4x

.	0	x	2x	3x	4x	5x
0	0	0	0	0	0	0
x	0	x	2x	3x	4x	5x
2x	0	2x	4x	0	2x	4x
3x	0	3x	0	3x	0	3x
4x	0	4x	2x	0	4x	2x
5x	0	5x	4x	3x	2x	x

a ako je $x^2=5x$, takodje prsten od 6 elemenata $0,x,2x,3x,4x$ i $5x$:

+	0	x	2x	3x	4x	5x
0	0	x	2x	3x	4x	5x
x	x	2x	3x	4x	5x	0
2x	2x	3x	4x	5x	0	x
3x	3x	4x	5x	0	x	2x
4x	4x	5x	0	x	2x	3x
5x	5x	0	x	2x	3x	4x

·	0	x	2x	3x	4x	5x
0	0	0	0	0	0	0
x	0	5x	4x	3x	2x	x
2x	0	4x	2x	0	4x	2x
3x	0	3x	0	3x	0	3x
4x	0	2x	4x	0	2x	4x
5x	0	x	2x	3x	4x	5x

Oba ova prstena su izomorfna prstenu Z_6.

Primjer 4.4.5. Neka $R \in \mathcal{AR}$, $x \in R, x \neq 0, x^2 \neq x, x^2 \neq 5x, 6x=0$, $2x=0, 3x \neq 0$. Prema Lemi 4.4.1 može da važi $3x^2=3x$. Tada je

$3x+x^2=4x^2$ $\quad 4x+x^2=x+3x+x^2=x+4x^2$ $\quad 5x+x^2=2x+3x+x^2=2x+4x^2$

$3x+2x^2=5x^2$ $\quad 4x+2x^2=x+5x^2$ $\quad 5x+2x^2=2x+5x^2$

$3x+4x^2=x^2$ $\quad 4x+4x^2=x+x^2$ $\quad 5x+4x^2=2x+x^2$

$3x+5x^2=2x^2$ $\quad 4x+5x^2=x+2x^2$ $\quad 5x+5x^2=2x+2x^2$.

Neposredno se provjerava da medju elementima $0,x,2x,3x,4x,5x,$ $x^2,2x^2,4x^2,5x^2,x+x^2,x+2x^2,x+4x^2,x+5x^2,2x+x^2,2x+2x^2,2x+4x^2$ i $2x+5x^2$ nema medjusobno jednakih.

Prema tome u ovom slučaju element x generiše prsten R_{18} od 18 gore navedenih elemenata:

+	0	x	2x	3x	4x	5x	x^2	$2x^2$	$4x^2$	$5x^2$	$x+x^2$	$x+2x^2$	$x+4x^2$	$x+5x^2$	$2x+x^2$	$2x+2x^2$	$2x+3x^2$	$2x+5x^2$
0	0	x	2x	3x	4x	5x	x^2	$2x^2$	$4x^2$	$5x^2$	$x+x^2$	$x+2x^2$	$x+4x^2$	$x+5x^2$	$2x+x^2$	$2x+2x^2$	$2x+4x^2$	$2x+5x^2$
x	x	2x	3x	4x	5x	0	$x+x^2$	$x+2x^2$	$x+4x^2$	$x+5x^2$	$2x+x^2$	$2x+2x^2$	$2x+4x^2$	$2x+5x^2$	$4x^2$	$5x^2$	x^2	$2x^2$
2x	2x	3x	4x	5x	0	x	$2x+x^2$	$2x+2x^2$	$2x+4x^2$	$2x+5x^2$	$4x^2$	$5x^2$	x^2	$2x^2$	$x+4x^2$	$x+5x^2$	$x+x^2$	$x+2x^2$
3x	3x	4x	5x	0	x	2x	$4x^2$	$5x^2$	x^2	$2x^2$	$x+4x^2$	$x+5x^2$	$x+x^2$	$x+2x^2$	$2x+4x^2$	$2x+5x^2$	$2x+x^2$	$2x+2x^2$
4x	4x	5x	0	x	2x	3x	$x+4x^2$	$x+5x^2$	$x+x^2$	$x+2x^2$	$2x+4x^2$	$2x+5x^2$	$2x+x^2$	$2x+2x^2$	x^4	$2x^2$	$4x^2$	$5x^2$
5x	5x	0	x	2x	3x	4x	$2x+4x^2$	$2x+5x^2$	$2x+x^2$	$2x+2x^2$	x^2	$2x^2$	$4x^2$	$5x^2$	$x+x^2$	$x+2x^2$	$x+4x^2$	$x+5x^2$
x^2	x^2	$x+x^2$	$2x+x^2$	$4x^2$	$x+4x^2$	$2x+4x^2$	$2x^2$	$3x^2$	$5x^2$	0	$x+2x^2$	4x	$x+5x^2$	x^2	$2x+2x^2$	5x	$2x+5x^2$	2x
$2x^2$	$2x^2$	$x+2x^2$	$2x+2x^2$	$5x^2$	$x+5x^2$	$2x+5x^2$	3x	$4x^2$	0	x^2	4x	$x+4x^2$	x	$x+x^2$	5x	$2x+4x^2$	2x	$2x+x^2$
$4x^2$	$4x^2$	$x+4x^2$	$2x+4x^2$	x^2	$x+x^2$	$2x+x^2$	$5x^2$	0	$2x^2$	3x	$x+5x^2$	x	$x+2x^2$	4x	$2x+5x^2$	2x	$2x+2x^2$	5x
$5x^2$	$5x^2$	$x+5x^2$	$2x+5x^2$	$2x^2$	$x+2x^2$	$2x+2x^2$	0	x^2	3x	$4x^2$	x	$x+x^2$	$x+3x^2$	$x+4x^2$	2x	$2x+x^2$	5x	$2x+4x^2$
$x+x^2$	$x+x^2$	$2x+x^2$	$4x^2$	$x+4x^2$	$2x+4x^2$	x^2	$x+2x^2$	4x	$x+5x^2$	x	$2x+2x^2$	5x	$2x+5x^2$	2x	$5x^2$	0	$2x^2$	$3x^2$
$x+2x^2$	$x+2x^2$	$2x+2x^2$	$5x^2$	$x+5x^2$	$2x+5x^2$	$2x^2$	4x	$x+4x^2$	x	$x+x^2$	5x	$2x+4x^2$	2x	$2x+x^2$	0	x^2	3x	$4x^2$
$x+4x^2$	$x+4x^2$	$2x+4x^2$	x^2	$x+x^2$	$2x+x^2$	$4x^2$	$x+5x^2$	x	$x+2x^2$	4x	$2x+5x^2$	2x	$2x+2x^2$	5x	$2x^2$	3x	$5x^2$	0
$x+5x^2$	$x+5x^2$	$2x+5x^2$	$2x^2$	$x+2x^2$	$2x+2x^2$	$5x^2$	x	$x+x^2$	4x	$x+4x^2$	2x	$2x+x^2$	5x	$2x+4x^2$	3x	$4x^2$	0	x^2
$2x-x^2$	$2x-x^2$	$4x^2$	$x-x^2$	$2x-4x^2$	x^2	$x-x^2$	$2x+2x^2$	5x	$2x-5x^2$	2x	$5x^2$	0	$2x^2$	3x	$x-5x^2$	x	$x-2x^2$	4x
$2x-2x^2$	$2x-2x^2$	$5x^2$	$x-5x^2$	$2x-5x^2$	$2x^2$	$x-2x$	5x	$2x-4x^2$	2x	$2x-x^2$	0	x^2	3x	$4x^2$	x	$x-x^2$	4x	$x-4x^2$
$2x-4x^2$	$2x-4x^2$	x^2	$x-x^2$	$2x-x^2$	$4x^2$	$x-4x^2$	$2x-5x^2$	2x	$2x-2x^2$	5x	$2x^2$	3x	$5x^2$	0	$x-2x^2$	4x	$x-5x^2$	x
$2x+5x^2$	$2x+5x^2$	$2x^2$	$x+2x^2$	$2x+2x^2$	$5x^2$	$x+5x^2$	2x	$2x+x^2$	5x	$2x+4x^2$	3x	$4x^2$	0	x^2	4x	$x+4x^2$	x	$x+x^2$

·	0	x	2x	3x	4x	5x	x^2	$2x^2$	$4x^2$	$5x^2$	$x+x^2$	$x+2x^2$	$x+4x^2$	$x+5x^2$	$2x+x^2$	$2x+2x^2$	$2x+4x^2$	$2x+5x^2$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x	0	x^2	$2x^2$	3x	$4x^2$	$5x^2$	x	2x	4x	5x	$x+x^2$	$2x+x^2$	$x+4x^2$	$2x+4x^2$	$x+2x^2$	$2x+2x^2$	$x+5x^2$	$2x+5x^2$
2x	0	$2x^2$	$4x^2$	0	$2x^2$	$4x^2$	2x	4x	2x	4x	$2x+2x^2$	$x+5x^2$	$2x+2x^2$	$x+5x^2$	$2x+4x^2$	$x+x^2$	$2x+4x^2$	$x+x^2$
3x	0	3x	0	3x	0	3x	3x	0	0	3x	0	3x	3x	0	3x	0	0	3x
4x	0	$4x^2$	2x2	0	$4x^2$	$2x^2$	4x	2x	4x	2x	$x+x^2$	$2x+4x^2$	$x+x^2$	$2x+4x^2$	$x+5x^2$	$2x+2x^2$	$x+5x^2$	$2x+2x^2$
5x	0	$5x^2$	$4x^2$	3x	$2x^2$	x^2	5x	4x	2x	x	$2x+2x^2$	$x+2x^2$	$2x+5x^2$	$x+5x^2$	$2x+x^2$	$x+x^2$	$2x+4x^2$	$x+4x^2$
x^2	0	x	2x	3x	4x	5x	x^2	$2x^2$	$4x^2$	$5x^2$	$x+x^2$	$x+2x^2$	$x+4x^2$	$x+5x^2$	$2x+x^2$	$2x+2x^2$	$2x+4x^2$	$2x+5x^2$
$2x^2$	0	2x	4x	0	2x	4x	$2x^2$	$4x^2$	$2x^2$	$4x^2$	$2x+2x^2$	$2x+4x^2$	$2x+2x^2$	$2x+4x^2$	$x+5x^2$	$x+x^2$	$x+5x^2$	$x+x^2$
$4x^2$	0	4x	2x	0	4x	2x	$4x^2$	$2x^2$	$4x^2$	$2x^2$	$x+x^2$	$x+5x^2$	$x+x^2$	$x+5x^2$	$2x+4x^2$	$2x+2x^2$	$2x+4x^2$	$2x+2x^2$
$5x^2$	0	5x	4x	3x	2x	x	$5x^2$	$4x^2$	$2x^2$	x^2	$2x+2x^2$	$2x+x^2$	$2x+5x^2$	$2x+4x^2$	$x+2x^2$	$x+x^2$	$x+5x^2$	$x+4x^2$
$x+x^2$	0	$x+x^2$	$2x+2x^2$	0	$x+x^2$	$2x+2x^2$	$x+x^2$	$2x+2x^2$	$x+x^2$	$2x+2x^2$	$2x+2x^2$	0	$2x+2x^2$	0	0	$x+x^2$	0	$x+x^2$
$x+2x^2$	0	$2x+x^2$	$x+5x^2$	3x	$2x+4x^2$	$x+2x^2$	$x+2x^2$	$2x+4x^2$	$x+5x^2$	$2x+x^2$	0	$x+2x^2$	3x	$x+5x^2$	$2x+x^2$	0	$2x+4x^2$	3x
$x+4x^2$	0	$x+4x^2$	$2x+2x^2$	3x	$x+x^2$	$2x+5x^2$	$x+4x^2$	$2x+2x^2$	$x+x^2$	$2x+5x^2$	$2x+2x^2$	3x	$2x+5x^2$	0	3x	$x+x^2$	0	$x+4x^2$
$x+5x^2$	0	$2x+4x^2$	$x+5x^2$	0	$2x+4x^2$	$x+5x^2$	$x+5x^2$	$2x+4x^2$	$x+5x^2$	$2x+4x^2$	0	$x+5x^2$	0	$x+5x^2$	$2x+4x^2$	0	$2x+4x^2$	0
$2x+x^2$	0	$x+2x^2$	$2x+4x^2$	3x	$x+5x^3$	$2x+x^2$	$2x+x^2$	$x+5x^2$	$2x+4x^2$	$x+2x^2$	0	$2x+x^2$	3x	$2x+4x^2$	$x+2x^2$	0	$x+5x^2$	3x
$2x+2x^2$	0	$2x+2x^2$	$x+x^2$	0	$2x+2x^2$	$x+x^2$	$2x+2x^2$	$x+x^2$	$2x+2x^2$	$x+x^2$	$x+x^2$	0	$x+x^2$	0	0	$2x+2x^2$	0	$2x+2x^2$
$2x+4x^2$	0	$x+5x^2$	$2x+4x^2$	0	$x+5x^2$	$2x+4x^2$	$2x+4x^2$	$x+5x^2$	$2x+4x^2$	$x+5x^2$	0	$2x+4x^2$	0	$2x+4x^2$	$x+5x^2$	0	$x+5x^2$	0
$2x+5x^2$	0	$2x+5x^2$	$x+x^2$	3x	$2x+2x^2$	$x+4x^2$	$2x+5x^2$	$x+x^2$	$2x+2x^2$	$x+4x^2$	$x+x^2$	3x	$x+4x^2$	0	3x	$2x+2x^2$	0	$2x+5x^2$

Primjer 4.4.6. Neka $R\in\mathfrak{AR}$, $x\in R, x\neq 0, x^2\neq x, x^2\neq 5x, 6x=0$, $2x\neq 0, 3x\neq 0$. Neka je dalje $3x^2\neq 3x$. Tada, zbog Leme 4.4.1., element x generiše prsten R_{36} od 36 elemenata $0,x,2x,3x,4x,5x,x^2$, $2x^2,3x^2,4x^2,5x^2,x+x^2,x+2x^2,x+3x^2,x+4x^2,x+5x^2,2x+x^2,2x+2x^2$, $2x+3x^2$, $2x+4x^2,2x+5x^2,3x+x^2,3x+2x^2,3x+3x^2,3x+4x^2,3x+5x^2,4x+x^2$, $4x+2x^2,4x+3x^2,4x+4x^2,4x+5x^2,5x+x^2,5x+2x^2,5x+3x^2,5x+4x^2$ i $5x+5x^2$.

Teorema 4.4.1. *Klasa* $\mathfrak{X}=\{R_1,R_2,R_3,R_6,R_9,R_{18},R_{36}\}$ *gdje je* R_1 *trivijalni prsten,* $R_2=Z_2, R_3=Z_3, R_6=Z_6$ *i* R_9,R_{18},R_{36} *prsteni iz Primjera 4.4.3, 4.4.5 i 4.4.6 je bazisna klasa u smislu Ljapina za klasu* $\mathfrak{AR}$ *u odnosu na klasu* $\mathfrak{R}$ *svih prstena.*

D o k a z. (i) Dokazaćemo prvo da je svaki prsten $R\in\mathfrak{AR}$ unija svojih podprstena, koji su izomorfni sa prstenima iz klase $\mathfrak{X}$.

Neka $R\in\mathfrak{AR}$ i neka je $x\neq 0$ proizvoljan element prstena R. Prema Propoziciji 4.1.1 važi $x^3=x$, a tada, prema Lemi 2.1.1 važi $1.2x=0$ ili $2.3x=0$ ili $3.6x=0, (2x\neq 0, 3x\neq 0)$.

1. Ako je $2x=0$, tada je, kao što smo vidjeli u Primjeru 4.4.1, $x^2=0$ i element x generiše prsten R_2 izomorfan sa Z_2.

2. Neka je $3x=0$. Ako je $x^2=x$ ili $x^2=2x$, tada,kao što smo vidjeli u Primjeru 4.4.2, element x generiše podprsten R_3 izomorfan sa Z_3.

Ako je $x^2\neq x$ i $x^2\neq 2x$, tada prema Primjeru 4.4.3, element x generiše prsten R_9.

3. Neka je $6x=0,(2x\neq0,3x\neq0)$. Ako je $x^2=x$ ili $x^2=5x$, (prema Lemi 4.4.1 je $x^2\neq2x,x^2\neq3x,x^2\neq4x$), tada prema Primjeru 4.4.4, element x generiše podprsten R_6 izomorfan sa Z_6.

Neka je sada $x^2\neq x,x^2\neq5x$. Zbog Leme 4.4.2, jedino može da važi $3x^2=3x$, i tada prema Primjeru 4.4.5, element x generiše podprsten R_{18}.

Ako je $3x^2\neq3x$, tada prema Primjeru 4.4.6, element x generiše podprsten R_{36}:

Dakle, proizvoljni element xeR pripada nekom podprstenu prstena R koji je izomorfan sa nekim od prstena iz klase $\mathfrak{K}$.

(ii) Ako je prsten R unija svojih podprstena izomorfnih sa prstenima iz klase $\mathfrak{K}$, neposredno slijedi da $R\in AR$.

(iii) Iz dokaza (i) slijedi da ne postoji podklasa klase $\mathfrak{K}$ koja bi zadovoljavala (i).

4.5. BAZISNA KLASA KLASE PRSTENA ZA ČIJI SVAKI ELEMENT VAŽI $x^4=x$

Ovdje ćemo odrediti bazisnu klasu u smislu Ljapina za klasu prstena R_4 sa svojstvom

$$(\forall x\in R)(x^4=x)\ , \tag{4.5.1}$$

tj. za klasu prstena $\mathfrak{R}_4$, mada prsteni iz ove klase nijesu anti-inverzni.

Lema 4.5.1. *Neka je* $R\in\mathfrak{R}_4$. *Za proizvoljni element* $x\in R$ *važi* $2x=0$.

D o k a z. Prema Lemi 2.1.1, za element $x\in R$ važi $2x=0$ ili $7x=0$ ili $14x=0, (2x\neq 0, 7x\neq 0)$.

Predpostavimo da je $7x=0$. Tada je $(3x)^4=4x$, odakle je zbog (4.5.1), $3x=4x$, odnosno $6x=0$, što je za $x\neq 0$ nemoguće. Dakle, $7x\neq 0$.

Pretpostavimo sada da je $14x=0, (2x\neq 0, 7x\neq 0)$. Tada je $(3x)^4=11x$, odakle je, zbog (4.5.1), $3x=11x$, odnosno $6x=0$, što je nemoguće. Dakle $14x\neq 0$.

Prema tome za svako $x\in R$ važi $2x=0$.

Lema 4.5.2. *Neka je* $R\in\mathfrak{R}_4$. *Tada je za svako* $x\in R$

$$x^2=x \iff x^3=x.$$

D o k a z. Ako je $x^2=x$, tada je $x^3=x^2$, odnosno $x^3=x$.

Ako je $x^3=x$, tada je $x^4=x^2$, odakle, zbog $x^4=x$, slijedi $x^2=x$.

Lema 4.5.3. *Neka* $R \in \mathfrak{R}_4$. *Tada za proizvoljno* $x \in R$ *su ekvivalentna tvrdjenja:*

a) $x+x^2+x^3=0$,

b) $x+x^2=x^3$,

c) $x+x^3=x^2$,

d) $x^2+x^3=x$.

D o k a z. Slijedi neposredno, jer je prema Lemi 4.5.1, $2x=0$, a znači i $2x^2=2x^3=0$.

Sada ćemo konstruisati dva prstena iz klase $\mathfrak{R}_4$ koji će biti od značaja za odredjivanje bazisne klase u smislu Ljapina za klasu prstena $\mathfrak{R}_4$ u odnosu na klasu svih prstena.

Primjer 4.5.1. Neka je R prsten iz klase $\mathfrak{R}_4$ i $x \in R, x \neq 0$. Neka dalje važi $x^2 \neq x$, odakle, zbog Leme 4.5.2, slijedi $x^3 \neq x$. Pretpostavimo dalje da je $x+x^2+x^3=0$. Tada je, prema Lemi 4.5.3, $x+x^2=x^3$, $x+x^3=x^2$ i $x^2+x^3=x$.

Značii u ovome slučaju element x generiše podprsten R_4' prstena R, čiji su elementi $0, x, x^2$ i x^3;

+	0	x^3	x^2	x
0	0	x^3	x^2	x
x^3	x^3	0	x	x^2
x^2	x^2	x	0	x^3
x	x	x^2	x^3	0

·	0	x^3	x^2	x
0	0	0	0	0
x^3	0	x^3	x^2	x
x^2	0	x^2	x	x^3
x	0	x	x^3	x^2

Ovaj prsten je izomorfan sa poljem GF(4), što se neposredno provjerava.

Primjer 4.5.2. Neka je $\mathbf{R}e\ \mathcal{R}_4$ i $x\in R, x\neq 0$. Neka je dalje $x^2\neq x$, a znači i $x^3\neq x$, ali neka je sada $x+x^2+x^3\neq 0$. Zbog Leme 4.5.3, tada je $x+x^2\neq x^3$, $x+x^3\neq x^2$ i $x^2+x^3\neq x$.

Dalje, zbog

1: $x+x^2=x \Rightarrow x^2=0 \quad x^4=0 \Rightarrow x=0$,

2: $x+x^2=x^2 \Rightarrow x=0$,

3: $x+x^2=x+x^3 \Rightarrow x^2=x^3 \Rightarrow x^3=x^4 \Rightarrow x^3=x \Rightarrow x^2=x$,

4: $x+x^2=x^2+x^3 \Rightarrow x^3=x \Rightarrow x^2=x$,

5: $x+x^2=x+x^2+x^3 \Rightarrow x^3=0 \Rightarrow x=0$,

6: $x+x^3=x \Rightarrow x^3=0 \Rightarrow x^4=0 \Rightarrow x=0$,

7: $x+x^3=x^3 \Rightarrow x=0$,

8: $x+x^3=x^2+x^3 \Rightarrow x^2=x$,

9: $x+x^3=x+x^2+x^3 \Rightarrow x^2=0 \Rightarrow x^4=0 \Rightarrow x=0$,

10: $x^2+x^3=x^2 \Rightarrow x^3=0 \Rightarrow x=0$,

11: $x^2+x^3=x^3 \Rightarrow x^2=0 \Rightarrow x=0$,

12: $x^2+x^3=x+x^2+x^3 \Rightarrow x=0$,

13: $x+x^2+x^3=x \Rightarrow x^2+x^3=0 \Rightarrow x^3=x^2 \Rightarrow x^3=x$,

14: $x+x^2+x^3=x^2 \Rightarrow x^3+x=0 \Rightarrow x^3=x$,

15: $x+x^2+x^3=x^3 \Rightarrow x+x^2=0 \Rightarrow x^2=x$,

važi:

1. $x+x^2\neq x$,
2. $x+x^2\neq x^2$,
3. $x+x^2\neq x+x^3$,
4. $x+x^2\neq x^2+x^3$,
5. $x+x^2\neq x+x^2+x^3$,
6. $x+x^3\neq x$,
7. $x+x^3\neq x^3$,
8. $x+x^3\neq x^2+x^3$,
9. $x+x^3\neq x+x^2+x^3$,

10. $x^2+x^3 \neq x^2$, 12. $x^2+x^3 \neq x+x^2+x^3$, 14. $x+x^2+x^3 \neq x^2$,
11. $x^2+x^3 \neq x^3$, 13. $x+x^2+x^3 \neq x$, 15. $x+x^2+x^3 \neq x^3$.

Dakle, u ovome slučaju element x generiše podprsten R_8' od 8 elemenata $0, x, x^2, x+x^2, x+x^3, x^2+x^3$ i $x+x^2+x^3$ prstena R:

+	0	x	x^2	x^3	$x+x^2$	$x+x^3$	x^2+x^3	$x+x^2+x^3$
0	0	x	x^2	x^3	$x+x^2$	$x+x^3$	x^2+x^3	$x+x^2+x^3$
x	x	0	$x+x^2$	$x+x^3$	x^2	x^3	$x+x^2+x^3$	x^2+x^3
x^2	x^2	$x+x^2$	0	x^2+x^3	x	$x+x^2+x^3$	x^3	$x+x^3$
x^3	x^3	$x+x^3$	x^2+x^3	0	$x+x^2+x^3$	x	x^2	$x+x^2$
$x+x^2$	$x+x^2$	x^2	x	$x+x^2+x^3$	0	x^2+x^3	$x+x^2$	x^3
$x+x^3$	$x+x^3$	x^3	$x+x^2+x^3$	x	x^2+x^3	0	$x+x^2$	x^2
x^2+x^3	x^2+x^3	$x+x^2+x^3$	x^3	x^2	$x+x^3$	$x+x^2$	0	x
$x+x^2+x^3$	$x+x^2+x^3$	x^2+x^3	$x+x^3$	$x+x^2$	x^3	x^2	x	0

·	0	x	x^2	x^3	$x+x^2$	$x+x^3$	x^2+x^3	$x+x^2+x^3$
0	0	0	0	0	0	0	0	0
x	0	x^2	x^3	x	x^2+x^3	$x+x^2$	$x+x^3$	$x+x^2+x^3$
x^2	0	x^3	x	x^2	$x+x^3$	x^2+x^3	$x+x^2$	$x+x^2+x^3$
x^3	0	x	x^2	x^3	$x+x^2$	$x+x^3$	x^2+x^3	$x+x^2+x^3$
$x+x^2$	0	x^2+x^3	$x+x^3$	$x+x^2$	$x+x^2$	$x+x^3$	x^2+x^3	0
$x+x^3$	0	$x+x^2$	x^2+x^3	$x+x^3$	$x+x^3$	x^2+x^3	$x+x^2$	0
x^2+x^3	0	$x+x^3$	$x+x^2$	x^2+x^3	x^2+x^3	$x+x^2$	$x+x^3$	0
$x+x^2+x^3$	0	$x+x^2+x^3$	$x+x^2+x^3$	$x+x^2+x^3$	0	0	0	$x+x^2+x^3$

Teorema 4.5.1. Klasa $\mathcal{K}' = \{R_1, R_2, R_4', R_8'\}$, gdje je R_1 trivijalan prsten, $R_2 = Z_2$ i prsteni R_4' i R_8' prsteni iz Primjera 4.5.1. i 4.5.2 je bazisna klasa u smislu Ljapina za klasu prstena $\mathfrak{R}_4$ u odnosu na klasu svih prstena $\mathfrak{R}$.

D o k a z. (i) Neka je R prsten iz klase $\mathfrak{R}_4$ i $x \in R$, $x \neq 0$. Prema Lemi 4.5.1, važi $2x = 0$.

Ako je $x^2 = x$, tada element x generiše podprsten prstena R izomorfan sa prstenom Z_2.

Ako je $x^2 \neq x$, a znači prema Lemi 4.5.2 i $x^3 \neq x$, i ako je $x + x^2 + x^3 = 0$, tada prema Primjeru 4.5.1, element x generiše podprsten R_4'. Ako je $x + x^2 + x^3 \neq 0$, tada prema Primjeru 4.5.2, element x generiše prsten R_8'.

Prema tome, proizvoljan element $x \in R$ pripada podprstenu prstena R koji je izomorfan sa nekim od prstena iz klase $\mathcal{K}'$.

(ii) Ako je prsten R unija podprstena izomorfnih sa prstenima iz klase $\mathcal{K}'$, tada neposredno slijedi da $R \in \mathfrak{R}_4$.

(iii) Iz dokaza (i) slijedi da ne postoji prava podklasa klase $\mathcal{K}'$, koja zadovoljava (i).

LITERATURA

[1] G.Birkhoff, ON THE STRUCTURE OF ABSTRACT ALGEBRAS, Proc. Camb.Philos.Soc. 31 (1935), 433-454.

[2] G.Birkhoff, SUBDIRECT UNIONS IN UNIVERSAL ALGEBRA, bull. Amer.Math.Soc, 50 (1944), 764-768.

[3] S.Bogdanović, S.Milić, V.Pavlović, ANTI-INVERSE SEMIGROUPS, Publ.Inst.Math.Beograd, 25 (39), 1979,95-100.

[4] S.Bogdanović, S.Crvenković, ON SOME CLASSES OF SEMIGROUPS, Zbornik radova PMF Novi Sad, 8, 1978, 69-77.

[5] S.Bogdanović, DEUX CARACTERISATIONS DES SEMIGROUPS ANTI-INVERSES, Zbornik radova PMF Novi Sad, 8, 1978, 79-81.

[6] S.Bogdanović, ON ANTI-INVERSE SEMIGROUPS, Publ.Inst.Math. Beograd, 25 (39), 1979, 25-31.

[7] Y.Chow, MODERN ABSTRACT ALGEBRA, Volume 1, Gordon and breach science publishers, 1976.

[8] B.Cerović, ANTI-INVERSE RINGS, Publ.Inst.Math.Beograd, 29 (43), 1981, 45-48.

[9] A.H.Clifford, G.B. Preston, THE ALGEBRAIC THEORI OF SEMIGROUPS (in Russian), "Mup", Moscow, 1972.

[10] P.M.Cohn, UNIVERSAL ALGEBRA, Harper and Row, New York, 1965.

[11] N.H.Mc Coy, THE THEORY OF RINGS, The mac Milan Comp. 1964.

[12] P.Crawley, R.P.Dilworth, ALGEBRAIC THEORY OF LATTICES, Prentice Hall, Englewood Cliffs, 1973.

[13] R.Croisot, DEMI-GROUPES INVERSIF ET DEMI-GROUPES REUNIONS DE DEMI-GROUPES SIMPLES, Ann,Sci.Ecole Norm. Sup. (3), 70 (1953), 361-379.

[14] S.Crvenković, ON SOME PROPERTIES OF A CLASS OF COMPLETELY REGULAR SEMIGROUPS, Zbornik radova PMF Novi Sad, 9 (979), 153-160.

[15] G.Čupona, SEMIGROUPS IN WHICH SOME LEFT IDEAL IS A GROUP, Godišnji zbornik PMF Skopje, T-14 (1963), 15-17.

[16] G.Čupona, ON COMPLETELY SIMPLE SEMIGROUPS, Glasnik Mat.-Fiz. i astr. Skopje, T.18,3 (1963), 159-166.

[17] Г. Чупона, ЗА ЕДЕН ВИД ПОЛИЊА СО КОНЕЧНА КАРАКТЕРИСТИКА, Билт.Друшт.мат.и физ. НР Македоније (1955), 3-5.

[18] D.B. Erickson, ORDERS FOR FIMITE NON-COMMUTATIVE RINGS, Am.Math.Monthly 73, (1966), 376-377.

[19] C.R.Fletcher, RINGS OF SMALL ORDER, The mathematical gazette, 1980, 9-22.

[20] C.R. Fletcher, THE STRUCTURE OF UNIQUE FACTORISATION RINGS, Proc.Cambridge Philos.Soc. 67 (1970), 535-540.

[21] A.Forsythe, N.H.Mc Coy, ON THE COMMUTATIVUY OF CERTAIN RINGS, Bulletin of te Am.Math.Soc. vol. 52(1946), 523-526.

[22] G.Grätzer, UNIVERSAL ALGEBRA, Von Nostrand, Princeton,1960.

[23] G.Grätzer, LATTICE THEORY AN INTRODUCTION, HM.Freeman, San Fancisco, 1971 .

[24] J.A.Green, ON THE STRUCTURE OF SEMIGROUPS, Ann.of Math. 54 (1951), 163-172.

[25] M.Hall., THE THEORY OF GROUPS, New York, 1959.

[26] I.Herstein, TOPICS IN ALGEBRA, Waltham, 1964.

[27] J.M.Howie, AN INTRODUCTION TO SEMIGROUP THEORY, Lond. Math.Soc. 1976.

[28] N.Jacobson, STRUCTURE THEORY FOR ALGEBRAIC ALGEBRAS OF BOUNDED DEGRE, Ann.of math.vol.46 (1945), 695-707.

[29] Л.А. Калужнин, ВВЕДЕНИЕ В ОБЩУЮ АЛГЕБРУ, Москва, 1973.

[30] А.Г.Курош, ЛЕКЦИИ ПО ОБЩЕЙ АЛГЕБРЕ, Москва, 1973.

[31] И.Ламбек, КОЛЬЦА И МОДУЛИ, Москва, 1971,

[32] Е.С. Ляапин, ПОЛУГРУППЮ, ФМ, Москва, 1960.

[33] С.Ленг, АЛГЕБРА, Москва 1968.

[34] S.Milić, ON SOME CLASES OF SEMIGROUPS, Algebraic conf., Skopje 1980, 93-103.

[35] S.Milić, O N-ANTI-INVERZNIM SEMIGRUPAMA, Zbornik radova PMF Novi Sad, 9 (1979), 161-166.

[36] S.Milić, S.Bogdanović, ON A CLASS OF ANTI-INVERSE SEMI-GROUPS, Publ.Inst.Math. Beograd, 25 (39), 1979, 95-100.

[37] S.Milić, V.Pavlović, SEMIGROUPS IN WICH SOME IDEAL IS A COMPLETELY SIMPLE SEMIGROUPS, Algebraic conf. Novi Sad, 1981.

[38] W.D. Neumann, VARIETES OF GROUPS, Springer-verlag, Berlin 1967.

[39] J Von Neumann, ON REGULARE RINGS, Proc. Nat.Acad. Sci. USA 22 (1936), 707-713.

[40] V.Perić, EINE BEMERKUNG ZU DEN INVERTITIEERBAREN UND FAS INVERTIERBAREN IDEALEN, Archiv der Math. Vol XV (1964), 414-417.

[41] V.Perić, ZU DEN FAS INVERTIEBAREN IDEALEN IN KOMUTATIVEN RINGEN UND HALBGRUPPEN, Glasnik matematički 1 (21) (1966), 139-146.

[42] V.Perić, FAST INVERTIEBARE PRIMIDEALE DER KOMUTATIVEN RINGE, Publ. Inst.Math.Beograd, T.7 (21) (1967), 99-109.

[43] V.Perić, ALGEBRA I, Sarajevo 1980.

[44] V.Perić, ALGEBRA II, Sarajevo 1980.

[45] M.Petrich, RINGS AND SEMIGROUPS, Springer-Verlag, New York, 1974.

[46] J.C.Sharp. ANTI-REGULARE SEMIGROUPS, Preliminary report, Notices Amer.Math.Soc.Vol 24.2 (1977), 210-266.

[47] F.A.Szász, NOTE ON RINGS IN WHICH EVERY PROPER LEFT-IDEAL IS CYCLIC, Fund.math., 44(1957), 330-332.

[48] G.Thierrin SUR UNE CONDITION NÉCESSAIRE ET SUFFISANTE POUR QE'UN SEMIGROUPE SOIT UN GROUPE, C.R. Acad. Sci., Paris 232 (1951), 376-378.

[49] G.Thierrin, SUR LES ELEMENT UNITAIRES DÚN DEMI-GRAUPE INVERSIF, C.R.Acad. Sci., Paris, (1952), 234.

[50] B.L. van der Waerden, MODERN Algebra, Vol I, New York 1953.

[51] W.C. Waterhouse, RINGS WITH CYCLIC ADDITIVE GROUP, Am. Math. Monthly, 71, 449-450.