UNIVERZITET U BEOGRADU
MATEMATIČKI FAKULTET

Vladimir Božović

Problem izomorfizma u grupnim prstenovima

magistarski rad

Komisija

1. prof. S. Vujošević (mentor)
2. prof. Ž. Mijajlović
3. prof. G. Kalajdžić

Odbrana: 20.03.2003

Beograd 2003.

Pitanja: 1. Šta ako K nije polje ili ako G nije grupa.

2. $K_1(G) \cong K_1(H)$
$K_2(G) \cong K_2(H)$
$\Rightarrow G \cong H$

Sadržaj

UVOD

Grupovna algebra $K[G]$, gdje je K polje, a G multiplikativna grupa, je asocijativna $K-$algebra sa elementima grupe G kao bazom. U literaturi se često za $K[G]$ koristi naziv grupovni prsten, apostrofirajući te dvije strukture kao najznačajnije u njenoj slojevitoj građi. U ovom radu, taj termin je isključivo vezan za $Z-$algebru $Z[G]$, koja se dobija ukoliko polje K u definiciji grupovne algebre zamijenimo prstenom cijelih brojeva Z.

Te dvije strukture su u osnovi interesovanja ovog rada, sa naročitim naglaskom na određenom problemu koji je nastao prije više od šezdeset godina. Britanski matematičar Graham Higman je 1940 godine postavio sljedeći problem: Da li iz $Z[G] \cong Z[H]$ slijedi $G \cong H$. To pitanje je imenovano kao izomorfni problem ili problem izomorfizma grupovnih prstena. Naravno, analogno ovom ubrzo se postavilo i pitanje : Da li iz $K[G] \cong K[H]$ slijedi $G \cong H$, za neko polje K, koji je istaknut kao izomorfni problem grupovnih algebri. Iako u formi slični, načini rješavanja ova dva problema se bitno razlikuju.

Naime, opšti odgovor na problem izomorfizma grupovnih algebri je negativan i relativno lako dostižan, pa se prirodno transformisao u traženje određenih klasa grupa i polja za koje je moguć definitivan zaključak u smislu postavljenog pitanja. Za razliku od ovog, problem izomorfizma grupovnih prstena, nije imao opšti odgovor do unazad pet godina, pa se njegovo rješavanje sastojalo u izdvajanju specifičnih klasa grupa koje su do na izomorfizam određene sa $Z[G]$, odnosno u traganju za kontraprimjerom. Upravo je u tom uspio Martin Hertweck 1997 godine dajući vrlo složen kontraprimjer sa kojim su srušene nade u pozitivan odgovor ovog pitanja, i pored velikog broja indikatora da će se do njega doći. Hertweck, inače, pripada grupi matematičara sa Univerziteta u Štutgartu, koji su se bavili ovim problemom i u tome dobili vrlo zapažene rezultate. Nakon 1997 godine se i problem izomorfizma grupovnih prstena razvija u smislu u kojem je to slučaj za problem izomorfizma grupovnih algebri.

Akcenat u ovom radu je na segmentu problema izomorfizma grupovnih algebri, koji se odnosi na neke klase $p-$grupa konačnog reda i polja čija je karakteristika različita od p. Ta dva uslova obezbjeđuju osobinu da je $K[G]$ poluprost prsten, što je od fundamentalne važnosti u traženju odgovora na postavljeni zadatak.

Poluprosti prsteni (moduli), načini razlaganja, osobine komponenti su elementi sadržani u klasičnoj Vederburnovoj teoriji, koja je uglavnom izložena u prvom poglavlju. Upravo se oslanjajući na nju, u ovom dijelu rada je predstavljen i jedan primjer sa kojim se dolazi do negativnog odgovora na problem izomorfizma grupovnih algebri. Pored niza drugačijih, izloženi primjer je odabran iz razloga što na najbolji način okuplja veoma važne pojmove i teoreme, potrebne u daljim analizama.

Drugo poglavlje, u kojem je na početku dat kratak istorijski osvrt na razvoj oba naznačena problema, predstavlja pregled nekih zanimljivih rezultata do kojih se došlo njihovim rješavanjem. Jedan od njih je svakako da $Q[G]$ do na izomorfizam određuje konačnu Abelovu grupu G. Takođe, predstavljene su i dvije teoreme koje osvjetljavaju problem izomorfizma za $p-$grupe i polja čija je karakteristika p. To se na neki način može shvatiti komplementarnim u odnosu na sadržaj trećeg poglavlja koje se bavi isto $p-$grupama, ali poljima čija je karakteristika različita od p.

Treće poglavlje se u svom uvodnom dijelu, u lemi **3.1.** bavi načinom razlaganja poluproste algebre $K[G]$, za algebarski zatvoreno polje K, čija karakteristika ne dijeli red grupe G. U ovoj lemi je uspostavljena veza između centralnih primitivnih idempotenata algebre $K[G]$ i prostih sumanada u njenom razlaganju, kao i još nekoliko važnih činjenica koje su dokazane na orginalan način. Lema **3.1.** stvara neophodnu osnovu za razumijevanje i dokazivanje teorema u nastavku. Pretpostavka o algebarskoj zatvorenosti polja K se provlači sve do jako važne teoreme **3.14.** u kojoj taj zahtjev nije istaknut. Sva prethodna tvrđenja su u funkciji njenog dokaza. Ova teorema kaže da iz izomorfizma $Q[G] \cong Q[H]$, za konačne grupe G i H, slijedi izomorfizam $K[G] \cong K[H]$ za bilo koje polje K čija karakteristika ne dijeli $|G| = |H|$. U lemi **3.15.** se daje donja ocjena kardinalnosti određene klase neizomorfnih $p-$grupa, reda p^n brojem $M_1 = f(p, n)$, rezultat koji pripada Higmanu. Sljedeći korak se sastoji u traženju najvećeg broja različitih grupovnih algebri tipa $Q[G]$, pri čemu se došlo do broja $M_2 = g(p, n)$, gdje je G određena $p-$grupa, reda p^n iz klase naznačene u lemi **3.15.**.

Pokazuje se da je $M_2 < M_1$. Na osnovu Dirihleovog principa zaključujemo da najmanje M_1/M_2 neizomorfnih p−grupa reda p^n opisane klase ima istu grupovnu algebru $Q[G]$. To znači, na osnovu teoreme **3.14.**, da postoji najmanje M_1/M_2 neizomorfnih p−grupa reda p^n koje imaju istu grupovnu algebru $K[G]$ za svako polje K čija je karakteristika različita od p. Oblik broja M_1 nam nameće ograničenje $n \geq 23$, koje se odražava i na M_2. Prethodno opisani postupak je dio teoreme **3.17.**, ključne za čitavo treće poglavlje i rad u cjelini. Ona govori da problem izomorfizma u odnosu na definisanu klasu grupa i polja ima negativan odgovor, uz kvantitativnu ocjenu tog odnosa. U slučaju $n < 23$, postupak bi se sastojao u konstrukciji kontraprimjera, odnosno u dokazu da je odgovor na problem izomorfizma pozitivan. To bi, ipak, zahtijevalo stvaranje bitno drugačijeg pristupa koji bi mogao biti tema novog rada.

1. POLUPROSTI MODULI. OPŠTI PROBLEM IZOMORFIZMA.

Definicija 1.1. Neka je K polje, a G multiplikativna grupa. Označimo sa $K[G]$ sve konačne, formalne sume oblika:

$$\alpha = \sum_{x \in G} a_x x, \quad (a_x \in K).$$

Uvedimo operaciju $+$ na sljedeći način:

$$\alpha + \beta = (\sum_{x \in G} a_x x) + (\sum_{x \in G} b_x x) = \sum_{x \in G} (a_x + b_x) x,$$

zatim:

$$\alpha \cdot \beta = (\sum_{x \in G} a_x x) \cdot (\sum_{x \in G} b_x x) = \sum_{x, y \in G} (a_x b_y) xy \quad ,$$

kao i:

$$a\alpha = a(\sum_{x \in G} a_x x) = \sum_{x \in G} (a a_x) x, \quad (a \in K).$$

Prethodno definisana struktura predstavlja asocijativnu $K-$algebru, koju nazivamo (**modularnom**) **grupovnom algebrom**.

Suštinski, grupovna algebra predstavlja vektorski prostor nad poljem K i bazom koju sačinjavaju elementi grupe G, uz definisanu operaciju množenja vektora. Ukoliko u prethodnoj definiciji polje K zamijenimo prstenom Z cijelih brojeva, tada se dobija struktura asocijativne $Z-$algebre koju nazivamo **integralnim grupovnim prstenom** ili samo **grupovnim prstenom**. U literaturi se često i jedna i druga struktura imenuju kao grupovni prsten, s tim što se iz konteksta specifira o kojoj se zapravo radi. U daljem tekstu će se čuvati ova terminološka razlika, a iz kog će se uočiti da, naravno, nije samo terminološka.

Veliki broj rezultata u okviru teorije vezane za grupovne algebre odnosi se na traženje svojstava grupe G kako bi $K[G]$ imao neke zahtijevane osobine. Kao ilustraciju tog pristupa možemo navesti neke poznate teoreme:

Teorema 1.1. [1] *$K[G]$ je Artinov zdesna ako i samo ako je grupa G konačna.*

□

Teorema 1.2. [2] *$K[G]$−modul $K[G]$ je injektivan ako i samo ako je grupa G konačna.*

□

Kao što je rečeno, klasična Vederburnova teorija, kao i skup teorema vezanih za poluproste module je od posebnog značaja u pomenutom problemu izomorfizma grupovnih algebri. Stoga slijede definicije i teoreme značajne u daljim analizama.

Definicija 1.2. Modul $M = M_R$ nazivamo prostim ako je $M \neq 0$ i ukoliko je svaki njegov podmodul jednak 0 ili M.

Definicija 1.3. Prsten R nazivamo prostim ako je $R \neq 0$ i ukoliko je svaki njegov dvostrani ideal jednak 0 ili R.

Teorema 1.3. [3] *Za modul $M = M_R$ sljedeći uslovi su ekvivalentni:*

(1) *svaki podmodul u M je suma prostih podmodula.*

(2) *M je suma prostih podmodula.*

(3) *M je direktna suma prostih podmodula.*

(4) *Za svaki pravi podmodul U modula M postoji podmodul U_0 tako da $U \oplus U_0 = M$.*

□

Definicija 1.4. Modul $M = M_R$ se naziva poluprostim ako zadovoljava jedan od uslova navedenih u prethodnoj teoremi. Prsten R nazivamo poluprostim zdesna, odnosno slijeva ako je modul R_R, odnosno ${}_RR$ poluprost.

Teorema 1.4. [3] *(Maške) Neka je $R := K[G]$, gdje je K polje, a G konačna grupa. R_R i ${}_RR$ su poluprosti moduli ako i samo ako karakteristika polja K ne dijeli red grupe G.*

Dokaz. Neka karakteristika K ne dijeli red grupe $n := |G|$. Tada je za $0 \neq k \in K$, element $nk := k + \ldots + k$ invertibilan. Invertibilni element elementu $n1$ zapisivaćemo kao $\frac{1}{n}$, gdje je $1 \in K$. Neka su $g_1, \ldots, g_n$ elementi grupe G. Ukoliko posmatramo R kao desni $K-$ modul, tada je R vektorski prostor nad K. Za svaki $\varphi \in End(R_K)$ definišimo preslikavanje $\hat{\varphi} : R \to R$ formulom:

$$\hat{\varphi}(r) := \frac{1}{n} \sum_{i=1}^{n} \varphi(rg_i)g_i^{-1}, \quad (r \in R).$$

Pokazaćemo da je $\hat{\varphi} \in End(R_R)$. Za proizvoljni $k \in K$ vrijedi:

$$\hat{\varphi}(rk) = \frac{1}{n} \sum_{i=1}^{n} \varphi(rkg_i)g_i^{-1} = (\frac{1}{n} \sum_{i=1}^{n} \varphi(rg_i)g_i^{-1})k = \hat{\varphi}(r)k.$$

Neka je sada $g \in G$. Kako je $\{gg_1, \ldots, gg_n\} = \{g_1, \ldots, g_n\}$, tada je:

$$\hat{\varphi}(rg) = \frac{1}{n} \sum_{i=1}^{n} \varphi(rgg_i)g_i^{-1} = \frac{1}{n} \sum_{i=1}^{n} \varphi(rgg_i)(gg_i)^{-1}g = \hat{\varphi}(r)g.$$

Odavde slijedi da je $\hat{\varphi}(rx) = \hat{\varphi}(r)x$ za proizvoljne $r, x \in R$, čime je pokazano da je $\hat{\varphi} \in End(R_R)$. Neka je sada A podmodul u R_R. Tada je A linearni podprostor u R_K. Znamo da postoji podprostor B tako da $R_K = A \oplus B$. Neka je $\pi : R_K \to R_K$ projekcija na A tj. $\pi(a + b) = a$ za $a \in A$, $b \in B$. Kako je A podmodul R_R to je za proizvoljno $a \in A$:

$$\hat{\pi}(a) = \frac{1}{n} \sum_{i=1}^{n} \pi(ag_i)g_i^{-1} = \frac{1}{n} \sum_{i=1}^{n} ag_ig_i^{-1} = \frac{1}{n}na = a$$

i za $r \in R$ računamo:

$$\hat{\pi}(r) = \frac{1}{n} \sum_{i=1}^{n} \pi(rg_i)g_i^{-1} \in A,$$

jer je $\pi(rg_i) \in A$. Odavde slijedi da je $\hat{\pi}$ projekcija R_R na A i vrijedi:

$$R_R = \hat{\pi}(R) \oplus (1 - \hat{\pi})(R) = A \oplus (1 - \hat{\pi})(R).$$

Slijedi da je R_R poluprost. Dokaz za $_RR$ je analogan. Pretpostavimo sada da karakteristika p polja K dijeli n. Pokazaćemo da za $r_0 := g_1 + \ldots + g_n$, ideal r_0R nije direktni sumand modula R_R. Najprije za $g \in G$ imamo da je $r_0g = r_0$. Odavde slijedi da je $r_0^2 = nr_0 = 0$, kao i $r_0R = r_0K$. Pretpostavimo da je $R_R = r_0R \oplus U$. Tada postoji idempotent e, takav da $eR = r_0R = r_0K$. Ukoliko je $e = r_0k_0$, $(k_0 \in K)$, to imamo da je $e = e^2 = r_0^2k_0^2 = 0$. Slijedi da je $r_0 = 0$.

□

Za razliku od predstavljenog u teoremama **1.1.**, **1.2.** i **1.4.** gdje su osobine grupe G određivale svojstva grupovne algebre $K[G]$ postavlja se obrnuto pitanje: Kako osobine $K[G]$ utiču na karakter grupe G? Tako se dolazi do formulacije opšteg problema izomorfizma grupovnih algebri:

Da li iz izomorfizma $K[G]$ i $K[H]$ kao $K-$algebri slijedi izomorfizam grupa G i H?

Ovaj problem je imenovan kao **problem izomorfizma grupovnih algebri** ili kraće, **izomorfni problem**, podstaknut je u formi sličnim problemom o kom će biti nešto više riječi u sljedećem poglavlju. Opšti odgovor na ovako postavljeno pitanje je negativan, a u svrhu predstavljanja primjera kojim se to dokazuje, neophodne su teoreme klasične Vederburnove teorije. Neka je M_R poluprost modul. Označimo sa Γ skup svih njegovih prostih podmodula:

$$\Gamma = \{E \mid E \text{ prost podmodul modula } M\}$$

Razmotrimo na Γ relaciju ekvivalencije $\cong$. Neka je $\{\Omega_j \mid j \in J\}$ skup odgovarajućih klasa ekvivalencije.

Definicija 1.5. Modul $B_j := \sum_{E \in \Omega_j} E$ nazivamo homogenim komponentama modula M.

Lema 1.5. [3] *Neka je M_R poluprost modul i B_j njegove homogene komponente. Tada vrijedi:*

(1) *Ukoliko je U prost podmodul modula B, tada je $U \in \Omega_j$.*

(2) $M = \bigoplus B_j$.

□

Teorema 1.6. [3] *Neka je R prsten i $R_R = \bigoplus_{i \in I} A_i$ njegovo razlaganje u sumu desnih ideala A_i, $(i \in I)$. Tada vrijede sljedeća tvrđenja:*

(a) *Podskup $I_0 = \{i | i \in I \land A_i \neq 0\}$ je konačan, pa slijedi da je $R = \bigoplus_{i \in I_0} A_i$.*

(b) *Postoje takvi elementi $e_i \in A_i$, $(i \in I_0)$ da:*

(1) $A_i = e_i R \quad (i \in I_0)$

(2) $1 = \sum_{i \in I_0} e_i$

(3) $e_i e_j = \begin{cases} e_i, & i = j \\ 0, & i \neq j \end{cases}$, $(i, j \in I_0)$, *tj.* $\{e_i | i \in I_0\}$ *je skup ortogonalnih idempotenata.*

(c) *Ako su A_i, $(i \in I_0)$ dvostrani ideali, tada su elementi e_i, $(i \in I_0)$ iz (b) u centru prstena R.*

(d) *Obrnuto, ako su dati takvi ortogonalni idempotenti:*

$$e_1, e_2, \dots, e_n \in R,$$

tako da je $1 = \sum_{i=1}^{n} e_i$, tada je $R = \bigoplus_{i=1}^{n} e_i R$, pri čemu su $e_i R$ dvostrani ideali ukoliko e_i pripadaju centru prstena R.

□

Na osnovu leme **1.5.**, teoreme **1.6.** i definicije **1.4.** poluprostog prstena slijedi da se R_R može razložiti na konačan broj homogenih komponenti, tj. $R_R = B_1 \oplus \ldots \oplus B_m$. Dokazuje se da su B_j prosti dvostrani ideali.

Teorema 1.7. [3] *Neka je $R \neq 0$ poluprosti prsten i $R_R = B_1 \oplus \ldots \oplus B_m$ odnosno ${}_R R = C_1 \oplus \ldots \oplus C_n$ razlaganje modula R_R odnosno ${}_R R$ na homogene komponente. Tada vrijedi:*

(a) *$B_j \quad (j = 1, \dots, m)$ su prosti dvostrani ideali u R.*

(b) $n = m$ *i poslije prenumeracije* $B_j = C_j \quad (j = 1, \ldots, m)$.

(c) $B_i B_j = \delta_{ij} B_i \quad (i, j = 1, \ldots, m)$.

(d) B_i, *razmatrani sami za sebe predstavljaju prstene sa jedinicom.*

(e) *Razlaganje* R *u direktnu sumu prostih dvostranih ideala je opredijeljeno jednoznačno sa tačnošću do na poredak.*

□

Kao što se vidi iz prethodne teoreme svaki B_j je prost prsten sa jedinicom. Međutim, iz same definicije homogene komponente B_j jasno je da B_j kao prost prsten ima samo jednu klasu izomorfnih prostih desnih ideala, tj. da su svaka dva prosta desna ideala u B_j izomorfna. Slično se zaključuje da komponente B_j imaju do na izomorfizam jedinstven prost lijevi ideal. Sljedeća teorema upravo govori o prostim prstenima koji imaju do na izomorfizam jedan prosti desni ideal.

Teorema 1.8. [3] *Neka je* R *prosti prsten koji ima do na izomorfizam jedinstven prosti desni ideal* E *u* R. *Neka je* $T := End(E_R)$. *Tada je* T *tijelo,* $E :=_T E$ *konačno generisani lijevi vektorski prostor nad* T *i vrijedi* $R \cong End({}_T E)$.

□

Dualno prethodnom važi tvrđenje za lijeve ideale. Direktne posljedice dvije prethodne teoreme su:

Teorema 1.9. [3] *Svaki poluprosti prsten sa jedinicom je direktna suma prostih prstena, od kojih je svaki izomorfan nekom prstenu matrica nad tijelom.*

□

Teorema 1.10. [3] *Neka je R prosti prsten koji ima do na izomorfizam jedan prosti desni ideal E i neka je R konačno generisana algebra nad poljem K. Tada postoji potpolje T_0 polja $T := End(E_R)$, tako da je $\dim_{T_0} T < \infty$ i $T_0 \cong K$. Ako je K algebarski zatvoreno polje, tad je $K \cong T \cong T_0$.*

□

Lema 1.11. *Prost, komutativan prsten je polje.*

Dokaz. Neka je R prost, komutativan prsten. Neka je $\varphi \in End(R_R)$. Tada je:

$$\varphi(x) = \varphi(1 \cdot x) = \varphi(1)x,$$

tj. svaki endomorfizam modula R_R je oblika $\varphi_r(x) = rx$, $(r \in R)$. Lako se pokazuje da je preslikavanje dato sa $\Phi : R \ni r \to \varphi_r \in End(R_R)$ izomorfizam prstena. Dakle, $R \cong End(R_R)$. Kako je R prost prsten, jasno je da je $End(R_R)$ tijelo, a zbog komutativnosti slijedi da je R polje.

□

Sada su se, konačno, stekli uslovi za konstrukciju najavljenog primjera. Neka je G konačna Abelova grupa, a K algebarski zatvoreno polje karakteristike 0. Na osnovu teoreme **1.4.** slijedi da je prsten $R := K[G]$ poluprost. Kako je već utvrđeno R se može razložiti u direktnu sumu njegovih potprstena. Dakle $R = R_1 \oplus R_2 \ldots \oplus R_m$, pri čemu su sumandi na osnovu teoreme **1.7.** prosti komutativni prsteni, a na osnovu prethodne leme slijedi da su R_i polja. Jasno je da je $K \cong e_i K \subseteq R_i$, gdje je na osnovu teoreme **1.6.** e_i jedinica u R_i. Pozabavimo se sada brojem m tj. brojem sumanada u razlaganju $R := K[G]$. Odgovor na ovo pitanje daje sljedeća teorema.

Teorema 1.12. [4] *Neka je G konačna grupa i neka je K algebarski zatvoreno polje karakteristike 0. Tada je broj neizomorfnih prostih $K[G]-$modula jednak broju klasa konjugacije grupe G.*

□

Pošto je razmatrana grupa G konačna Abelova grupa, to je broj klasa konjugacije jednak $|G|$ tj. redu grupe. Sada je jasno da je $m = |G|$. Kako je $R := K[G]$ vektorski prostor nad poljem K, kao i što je svaki sumand vektorski prostor nad ovim poljem, to je $\dim_K K[G] = |G|$. Tad je:

$$\dim_K K[G] = \dim_K R_1 + \dim_K R_2 + \ldots + \dim_K R_m.$$

Pošto je $m = |G|$ to zaključujemo da je $\dim_K R_i = 1$ odakle proizilazi:

$$R_i \cong K \qquad (i = 1, 2, \ldots, m).$$

Dakle, $K[G] \cong K \oplus K \oplus \ldots \oplus K$, gdje je broj sumanada $|G|$. Ukoliko je H druga Abelova grupa tako da je $|G| = |H|$, tada je $K[G] \cong K[H]$, pri čemu G i H ne moraju biti izomorfne. Ovim je izveden najavljeni primjer i pokazano da je odgovor na opšti problem izomorfizma negativan.

Neka je x proizvoljan element grupe G. Ukoliko je red ovog elementa relativno prost sa p tada kažemo da je $p-$regularan. Kako konjugovani elementi u grupi imaju isti red, možemo na osnovu toga govoriti o $p-$regularnim klasama konjugacije. Sljedeća teorema se bavi istim problemom kao i prethodna, ali u slučaju polja nenulte karakteristike.

Teorema 1.13. [5] *Neka je G konačna grupa, a K algebarski zatvoreno polje karakteristike $p > 0$. Tada je broj neizomorfnih ireducibilnih $K[G]$ modula jednak broju $p-$regularnih klasa konjugacije grupe G.*

□

2. IZOMORFIZAM GRUPOVNIH PRSTENA. REZULTATI.

Interesovanje za opšti problem izomorfizma počinje od uspostavljanja znamenitog problema Grahama Higmana još 1940 godine: Ako su grupe G i H konačne, da li $ZG \cong ZH$ implicira $G \cong H$. Ovaj problem se susreće kao problem izomorfizma **integralnih grupovnih prstena (Higmanov problem)**. Rad mnogih autora na ovom problemu dugo nije ostvario značajniji napredak. Treba izdvojiti važan rezultat do kog je došao Whitcomb 1968 dajući pozitivan odgovor u slučaju kada su G i H konačne, metabelove grupe. Grupa G je **metabelova** ukoliko je grupa $G/C(G)$ Abelova, gdje je $C(G)$ oznaka za centar grupe G. Nakon ovog dostignuća očvrslo je uvjerenje da Higmanov problem ima pozitivan odgovor, pa su se napori razvijali u tom pravcu. Tako je naprimjer dobijen pozitivan odgovor u slučaju kada je G konačno generisana nilpotentna grupa klase 2 [15] i za čitav niz grupa čije su klase određene skupom složenih kriterijuma. Izomorfni problem grupovnih algebri se takođe sužavao na neki specifičniji formalni okvir u kom je bilo moguće doći do konačnog odgovora. Tako je i nastao potproblem, u zapadnoj literaturi imenovan kao **Modular Isomorphism Problem (MIP)**, posmatran nad klasom konačnih $p-$grupa i polja koja se sastoje od p elemenata. Dakle, MIP je sadržan u pitanju da li iz $GF(p)[G] \cong GF(p)[H]$ slijedi $G \cong H$, gdje su G i H konačne $p-$grupe, a $GF(p)$ polje od p elemenata. Između ostalih, dobijen je pozitivan odgovor na MIP za klase sljedećih konačnih $p-$grupa: Abelovih $p-$grupa [17], metacikličnih $p-$grupa [18], $p-$grupa čiji red nije veći od p^4 [19], reda p^5 [Kovacs, Newman], reda 2^6 [20] i reda 2^7 [21] (odgovori dobijeni uz pomoć kompjutera). Zanimljiv rezultat, u smislu veze između Higmanovog i problema izomorfizma grupovnih algebri, ostvario je Dade kada je našao neizomorfne, konačne, metabelove grupe G_1 i G_2, tako da su $K[G_1]$ i $K[G_2]$ izomorfne $K-$algebre za svako polje K, pri čemu $Z[G_1]$ nije izomorfno sa $Z[G_2]$.

Tačka na opšti Higmanov problem stavljena je 1997, kada je Martin Hertweck našao neizomorfne grupe X i Y reda $2^{21} \cdot 97^{28}$ tako da je $ZX \cong ZY$. U ovom poglavlju su predstavljeni neki od rezultata do kojih se došlo rješavanjem pomenutih problema.

Da bi predstavili jedan od zanimljivijih, u okviru problema izomorfizma grupovnih algebri, neophodne su dvije sljedeće leme.

Lema 2.1. *Neka je Ω skup konačnih Abelovih grupa, a S skup cjelobrojnih nizova. Tada je preslikavanje $\Phi : \Omega \to S$ dato sa $\Phi(G) = (|G^{(d)}|)_{d\geqslant 1}$ injektivno do na izomorfizam grupa, pri čemu je $G^{(d)} = \{x^d \mid x \in G\}$.*

Dokaz. Prisjetimo se da svaku konačnu Abelovu grupu G možemo jednoznačno predstaviti na sljedeći način:

$$G \cong Z_{p^{k_1}} \times Z_{p^{k_2}} \times \ldots \times Z_{p^{k_\pi}} \times \ldots \times Z_{q^{l_1}} \times \ldots \times Z_{q^{l_\sigma}},$$

pri čemu su $p < \ldots < q$ jednoznačno određeni prosti djelioci reda grupe, kao što su jednoznačno određeni i brojevi $k_1, \ldots, k_\pi, \ldots, l_1, \ldots, l_\sigma$ do na izomorfizam grupa. Neka su G_1 i G_2 konačne Abelove grupe tako da $\Phi(G_1) = \Phi(G_2)$. Očigledno je $|G_1| = |G_2| = n$. Uočimo p prosti faktor broja n. Predstavimo $G_1 = P_1 \times H_1$, gdje je P_1 Silovljeva p-podgrupa grupe G_1, a H_1 njen p-komplement. Neka je $P_1 = \prod_{i=1}^{m_1}(Z_{p^i})^{\times n_i}$ direktan proizvod cikličnih grupa Z_{p^i} koje se pojavljuju n_i puta. Uočimo da u H_1 nemamo p-elemenata, te je stoga $H_1^{(p^k)} = H_1$ tj.

$$P_1^{(p^k)} = \prod_{i=k+1}^{m_1} (Z_{p^{i-k}})^{\times n_i},$$

odnosno:

$$G_1^{(p^k)} = P_1^{(p^k)} \times H_1.$$

Sada je jasno:

$$|P_1^{(p^k)}| = p^{\sum_{i=k+1}^{m_1}(i-k)n_i},$$

odakle slijedi:

$$\frac{|G_1^{(p^{k-1})}|}{|G_1^{(p^k)}|} = p^{n_k+n_{k+1}+\ldots+n_{m_1}}.$$

Neka je $P_2 = \prod_{i=1}^{m_2}(Z_{p^i})^{\times l_i}$, Silovljeva $p-$podgrupa grupe G_2. Iz činjenice da je: $|G_1^{(p^{m_1})}| = |G_2^{(p^{m_1})}|$, $|G_1^{(p^{m_2})}| = |G_2^{(p^{m_2})}|$, zaključujemo da je $m_1 = m_2$. Pošto je:

$$\frac{|G_1^{(p^{k-1})}|}{|G_1^{(p^k)}|} = \frac{|G_2^{(p^{k-1})}|}{|G_2^{(p^k)}|} \qquad (k = 1,\, 2,\, \ldots\, ,\, m_1),$$

proizilazi:

$$n_i = l_i \qquad (i = 1,\, 2,\, \ldots\, ,\, m_1).$$

Iz prethodnog zaključujemo da je $P_1 \cong P_2$. Nastavljajući ovaj postupak po svim prostim djeliocima broja $|G_1| = |G_2| = n$, proizilazi da je $G_1 \cong G_2$, pa je time lema dokazana.

□

Definicija 2.1. Idempotent $e \neq 0$ u $K-$algebri A je primitivan ukoliko ne postoje dva nenulta ortogonalna idempotenta e_1, e_2 tako da $e_1 + e_2 = e$.

Primjetimo da ako je B podalgebra algebre A, da tada primitivni idempotent u B ne mora biti primitivni idempotent u A. Ukoliko je, naprimjer, $G = \{1, x\}$ ciklična grupa reda 2 i $H = \{1\}$ njena podgrupa reda 1, tada je grupovna algebra CH podalgebra grupovne algebre CG, gdje je C je oznaka za polje kompleksnih brojeva. Element $1 \in CH$ je primitivni idempotent u CH. Međutim, nije primitivni idempotent algebre CG, pošto je suma dva ortogonalna, nenulta idempotenta:

$$e_1 = (1/2)(1+x) \text{ i } e_2 = (1/2)(1-x).$$

Lema 2.2. *Neka je A neka $K-$algebra i $e \in A$ idempotent. Tada je e primitivan ako i samo ako se ideal Ae ne može razložiti u direktnu sumu dva nenulta ideala .*

Dokaz. Pretpostavimo da e nije primitivan. To znači da postoje nenulti idempotenti e_1, e_2 tako da je $e = e_1 + e_2$ i $e_1e_2 = 0$. Slijedi:

$$e_1 = e_1 + 0 = e_1^2 + e_1e_2 = e_1(e_1 + e_2) = e_1e,$$

pa time postaje jasno da je $Ae_1 = Ae_1e \subseteq Ae$. Analogno zaključujemo da je $Ae_2 \subseteq Ae$, iz čega proizilazi $Ae_1 + Ae_2 \subseteq Ae$. Kako je suprotna inkluzija očigledna slijedi jednakost $Ae = Ae_1 + Ae_2$. Pošto je $e_i \in Ae_i$ slijedi da su oba sumanda nenulta. Ukoliko pokažemo da je ova suma direktna, to će narušiti pretpostavku o nerazloživosti ideala Ae. Neka je $x \in Ae_1 \cap Ae_2$. Tada je $x = ae_1 = ae_1^2 = (ae_1)e_1 = xe_1$, odnosno $x = xe_2$. Zamjenjujući $x = xe_2 = (xe_1)e_2 = x(e_1e_2) = x0 = 0$. Tako je pokazano da je $Ae_1 \cap Ae_2 = \{0\}$, čime je utvrđena direktnost sume.
Pretpostavimo sada da ideal Ae možemo razložiti u direktnu sumu dva nenulta ideala $Ae = I_1 \oplus I_2$. Kako je $e \in Ae$, to postoje $x \in I_1$, $x \in I_2$ tako da $e = x + y$. Ukoliko je $x = 0$ to znači da je $e = y \in I_2$, iz čega proizilazi $Ae = Ay \subseteq I_2$, odnosno $I_1 \oplus I_2 \subseteq I_2$, što protivrječji pretpostavci da je $I_1 \neq \{0\}$. Slično zaključujemo i za $y \neq 0$. Pošto je $x \in Ae$, slijedi $x = xe$, te zbog toga:

$$(1 - x)x = x - x^2 = xe - x^2 = x(x + y) - x^2 = xy.$$

Kako je $xy \in I_2$, jer je $y \in I_2$, $(1 - x)x \in I_1$, jer je $x \in I_1$, a zbog $I_1 \cap I_2 = \{0\}$ slijedi da je $x - x^2 = xy = 0$. Dalje, $x = x^2$ i $xy = 0$. Mijenjajući x sa y u prethodnom postupku dokazujemo da je $y^2 = y$ i $yx = 0$. Time smo dokazali postojanje nenultih ortogonalnih idempotenata x, y čija je suma jednaka e, tj. e nije primitivan.

□

Sljedeća teorema koju smo već nagovijestili daje odgovor na problem izomorfizma u slučaju kad se radi o Abelovim grupama i polju racionalnih brojeva. U prethodnom razmatranju prilikom konstrukcije primjera u prvom poglavlju došli smo do saznanja da je odgovor na ovo pitanje u slučaju polja karakteristike 0 u opštem slučaju negativan. Međutim kada se radi o polju racionalnih brojeva i klasi Abelovih grupa, odgovor je potvrdan. Razlog za to leži u osobinama ciklotomičnih polja kojim ćemo se baviti u dokazu naredne teoreme.

Teorema 2.3. [6] *Neka je G konačna Abelova grupa, a Q polje racionalnih brojeva. Tada grupovna algebra $Q[G]$ određuje G do na izomorfizam.*

Dokaz. Prema teoremi **1.4.** slijedi da je $Q[G]$ poluprosta, konačnodimenziona, komutativna algebra i prema analizi koju smo sproveli u prvom poglavlju $Q[G]$ je izomorfna direktnoj sumi polja. Neka je $Q[G] = R_1 \oplus \ldots \oplus R_m$ pri čemu su sumandi u ovoj sumi prosti ideali, tj. polja posmatrani sami za sebe. Prema teoremi **1.6.** utvrđujemo postojanje ortogonalnih idempotenata $e_1, e_2, \ldots, e_m$ takvih da je $1 = e_1 + e_2 + \ldots + e_m$, pri čemu je e_i jedinični element polja R_i $(i = 1, \ldots, m)$. Jasno je da vrijedi $e_iQ[G] = R_i$, a prema lemi **2.2.** slijedi da je e_i primitivni ortogonalni idempotent. Dakle, $Q[G] = \sum_{i=1}^{m} e_iQ[G]$, dok je $e_iQ[G] \cong F_i$, za neko polje F_i. Ukoliko je I ideal prstena $Q[G]$ tada je $I = \sum_{i=1}^{m} e_iI$, pri čemu su e_iI ili 0 ili $e_iQ[G]$. Najprije, napravimo nekoliko opservacija na temu ciklotomičnih polja.

Neka je $F = Q(\varepsilon_n)$, gdje je ε_n $n-$ti primitivni korijen jedinice. Zbog činjenice da je $Q(\varepsilon_{2k+1}) = Q(\varepsilon_{4k+2})$ možemo podrazumijevati da je n paran. Sada ćemo dokazati da je n jedinstveno određen poljem F. Neka je A bilo koja konačna multiplikativna podgrupa grupe $F^0 = F\backslash\{0\}$. Tada je $< A, \varepsilon_n >$ takođe konačna podgrupa F^0, a prema poznatom tvrđenju da je svaka konačna podgrupa multiplikativne grupe polja ciklična [11], slijedi da je $< A, \varepsilon_n >$ ciklična. Neka je $< A, \varepsilon_n > = < \delta >$ ciklična grupa reda t. Tada je zbog $F = Q(\delta)$, jasno $\varphi(t) = (F : Q) = \varphi(n)$, gdje je φ Ojlerova funkcija. Zbog $< A, \varepsilon_n > = < \delta >$, $ord(\varepsilon_n) = n$ i $ord(\delta) = t$, zaključujemo da $n|t$. Uzimajući u obzir da je n paran, $\varphi(t) = \varphi(n)$ i $n|t$, slijedi da je $n = t$, iz čega proizilazi $< A, \varepsilon_n > = < \varepsilon_n >$. Drugim riječima, slijedi da je $< \varepsilon_n >$ istovjetna sa multiplikativnom grupom elemenata iz F^0 koji imaju konačan red, pa je shodno tome n jedinstveno određeno i predstavlja broj takvih elemenata. Preciznije, to znači da ako je $F = Q(\varepsilon')$, gdje je ε' primitivni $n'-$ti korijen jedinice, n broj elemenata konačnog reda iz F^0 tada je $n' = n$ ukoliko je n' paran, odnosno $2n' = n$ ukoliko je n' neparan. Naime, u slučaju da je n' neparan, tada vrijedi $F = Q(-\varepsilon')$, a ε' ima paran red $2n'$, odakle je $2n' = n$.

Uvedimo oznaku $\omega(K[G]) = \{\sum a_x x \mid \sum a_x = 0, \, a_x \in K, \, x \in G\}$. Neka je d fiksiran paran broj i neka je $I = \omega(Q[G^{(d)}]) \cdot Q[G]$ ideal prstena $Q[G]$. Pozabavimo se sada sumandima $e_iQ[G] \cong F_i$, odnosno sa e_iI. Pošto množenje sa e_i određuje homomorfizam prstena $Q[G]$ na F_i vidimo da je F_i generisan sa Q i konačnom Abelovom grupom e_iG. Dakle e_iG je multiplikativna, konačna podgrupa polja F_i, pa je zbog već navedenog tvrđenja ciklična. Neka je γ_i generator ove grupe i neka je $ord(\gamma_i) = n_i$. Sada zaključujemo da je $F = Q(\gamma_i)$. Jasno je da je $|e_iG| = n_i$. U slučaju da je n_i paran možemo pisati $F_i = Q(\gamma_i)$, a u slučaju da je n_i neparan, pišemo $F_i = Q(-\gamma_i)$, pri čemu je $ord(-\gamma_i) = 2n_i$. U svakom slučaju, F_i je ciklotomično raširenje polja Q, a n_i tj. $2n_i$ su jedinstveno određeni. Podsjetimo se da je:

$$I = \left\{\sum (a_x x^d)c \mid c \in Q[G],\ a_x \in Q,\ x^d \in G\right\},$$

iz čega proizilazi:

$$e_i \cdot I = \left\{\sum a_x(e_i x^d)c \mid c \in Q[G],\ a_x \in Q,\ x^d \in G\right\}.$$

Sada je $e_i \cdot I = 0 \Leftrightarrow e_i x^d = 1$, odnosno:

$$e_i x^d = 1 \Leftrightarrow (e_i x)^d = 1 \Leftrightarrow (e_i G)^{(d)} = 1.$$

Kako je e_iG ciklična, a red njenog generatornog elementa jednak $|e_iG|$, to slijedi da $|e_iG|$ dijeli d, odnosno da $n_i \mid d$. Dakle $e_iI = 0$ ako i samo ako $n_i \mid d$. Prema tome,

$$I = \sum_{n_i \nmid d} e_i Q[G]$$

je jedinstveno određen ideal prstenom $Q[G]$, jer su n_i jedinstveno određeni poljima F_i, a d je fiksiran paran broj. Kako je :

$$Q[G/G^{(d)}] \cong Q[G]/I = \sum_{n_i \mid d} e_i Q[G],$$

vidimo da je $|G/G^{(d)}| = \dim_Q Q[G/G^{(d)}]$ određen sa $Q[G]$. Prema Lagranžovoj teoremi $|G| = |G/G^{(d)}| \cdot |G^{(d)}|$, a $|G| = \dim_Q Q[G]$, vidimo da je $|G^{(d)}|$ jednoznačno određeno prstenom $Q[G]$ za sve parne brojeve d. Na kraju, neka je $d \geqslant 1$ neparan broj. Neka je $G = P \times H$ gdje P Silovljeva 2-podgrupa, a H njen 2-komplement. Tada je $P^{(d)} = P$ i $H^{(2)} = H$ pa slijedi da je $G^{(d)} = P \times H^{(d)}$, $G^{(2d)} = P^{(2)} \times H^{(d)}$ i $G^{(2)} = P^{(2)} \times H$. Dakle $G/G^{(d)} = H/H^{(d)} = G^{(2)}/G^{(2d)}$, pa je time $|G^{(d)}|$ takođe jednoznačno određeno, jer su nam $|G|$, $|G^{(2)}|$, $|G^{(2d)}|$ već poznati. Zaključujemo da $Q[G]$ određuje $|G^{(d)}|$ za sve $d \geqslant 1$, što prema lemi **2.1.** znači da je G određena jednoznačno do na izomorfizam.

□

Ovaj lijep rezultat je nažalost posljedica prilično jakih pretpostavki među kojim je komutativnost grupe G. Kao što je rečeno odgovor na problem izomorfizma se tražio u okvirima specifičnih klasa grupa i polja. Slijedi nekoliko primjera.

Definicija 2.2. Multiplikativna grupa G u kojoj je jedino 1 konačnog reda je torziono slobodna grupa.

Definicija 2.3. Pod trivijalnim jedinicama grupovne algebre $K[G]$ podrazumijevamo skup $U = \{kg \mid k \in K,\ k \neq 0,\ g \in G\}$.

Teorema 2.4. [7] *Neka je G grupa takva da postoji niz:*

$$\langle 1 \rangle = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_n = G,$$

gdje su G_{i+1}/G_i torziono slobodne Abelove grupe. Ukoliko je K neko polje, tada $K[G]$ nema pravih djelitelja nule i ima samo trivijalne jedinice.

□

Sljedeća teorema odgovara na postavljeni problem izomorfizma pod uslovom da imamo jednu prilično jaku informaciju o grupovnoj algebri $K[G]$ ili samoj grupi G.

Teorema 2.5. [8] *Neka je $K[G] \cong K[H]$ i pretpostavimo da $K[G]$ ima samo trivijalne jedinice. Tada $K[H]$ ima samo trivijalne jedinice i vrijedi $G \cong H$. Posebno, ukoliko su G i H torziono slobodne Abelove grupe tako da $K[G] \cong K[H]$, tada je $G \cong H$.*

Dokaz. Neka je $U = U(K[G])$ grupa jedinica $K[G]$, odnosno prema pretpostavci:

$$U = \{kg \mid k \in K,\ k \neq 0,\ g \in G\}.$$

Neka je $\lambda : K[G] \to K$ bilo koji $K-$homomorfizam. Ako definišemo:

$$U_\lambda = \{i \in U \mid \lambda(i) = 1\},$$

lako se vidi da preslikavanje $G \to U_\lambda$ dato sa $g \to \lambda(g)^{-1}g$ predstavlja izomorfizam i da je time U_λ baza za $K[G]$. Zato što je $K[G] \cong K[H]$, lako slijedi da $K[H]$ ima samo trivijalne jedinice. Tada je:

$$G \cong U_\lambda(K[G]) \cong U_\lambda(K[H]) \cong H,$$

što potvrđuje traženi izomorfizam. Konačno, ukoliko je G, odnosno H torziono slobodna Abelova grupa, onda prethodna teorema implicira da $K[G]$, odnosno $K[H]$ ima samo trivijalne jedinice, odakle slijedi tvrđenje.

□

Naredne dvije teoreme se mogu na neki način shvatiti kao komplementarne sadržaju sljedećeg poglavlja.

Teorema 2.6. [8, 9] *Neka je G prebrojiva Abelova p-grupa, a neka je K polje karakteristike p. Tada je $K[G] \cong K[H]$ ako i samo ako vrijedi $G \cong H$.*

□

Teorema 2.7. [4] *Neka je G konačna $p-$grupa, G' njen komutator, a K polje čija je karakteristika p. Tada grupovna algebra $K[G]$ determiniše do na izomorfizam:*

(1) *faktor grupu G/G',*

(2) *centar grupe G, tj. $C(G)$.*

□

Na osnovu (2) prethodne teoreme slijedi da je svaka Abelova $p-$grupa u potpunosti određena grupovnom algebrom $K[G]$, za polje čija je karakteristika p. Kako je svaka grupa reda p^2 Abelova, to se isti zaključak izvodi i za ovu klasu $p-$grupa. Šta se dešava, ukoliko polje karakteristike p zamijenimo poljem čija je karakteristika različita od p je pitanje kojim se bavi naredno poglavlje.

3. PROBLEM IZOMORFIZMA GRUPOVNIH ALGEBRI ZA NEKE KLASE p–GRUPA I POLJA KARAKTERISTIKE RAZLIČITE OD p.

U ovom poglavlju se konačno bavimo problemom izomorfizma grupovnih algebri $K[G]$, gdje je G neka p-grupa, a K polje karakteristike različite od p. Dakle, ispituje se da li pod prethodnim uslovima iz $K[G] \cong K[H]$ slijedi $G \cong H$. Odgovor bi, naravno, bio obezbjeđen ukoliko bi konstruisali kontraprimjer i to je lakši put do konačnog rješenja. Međutim, pristup koji će ovdje biti predstavljen je više od odgovora na ovaj zadatak. Naime, u ključnoj teoremi ovog poglavlja utvrdiće se, za fiksiran prost broj p, aproksimativna ocjena (N) broja neizomorfnih grupa reda p^n, koje imaju izomorfne grupovne algebre za svako polje K čija je karakteristika različita od p. Pokazaće se da je N oblika $p^{\frac{2}{27}(n^3-23n^2)}$, što nas upućuje na uslov $n \geqslant 23$ pod kojim naznačena teorema ima netrivijalan zaključak. Ipak, to nije ograničenje odgovora za problem koji je definisan na početku, jer se, u stvari, registruje veliki broj neizomorfnih p-grupa čije su grupovne algebre izomorfne. Nažalost, ako je n mali broj, teorija koja je pomogla u definisanju završne teoreme ne može dati određen zaključak. U ovom slučaju, postupak bi se sastojao u konstrukciji specifičnih kontraprimjera, odnosno u dokazu da oni ne postoje. Najveći dio ovog poglavlja je u funkciji dokaza teoreme **3.14.** koja omogućuje da se u tretiranju problema izomorfizma pod navedenim uslovima, ograničimo na grupovne algebre $Q[G]$, odnosno na polje Q racionalnih brojeva kao dobro izučeno. Ta teorema i znameniti Higmanov rezultat dat u lemi **3.15.** čine ostvarivim dokaz teoreme **3.17.** za koju je već rečeno da je ključna teorema poglavlja.

Uvedimo neke oznake i definicije. Sa $C(R)$ označavamo centar prstena R. U lemama **3.1.**, **3.2.**, **3.3.**, **3.5.**, **3.6.** i **3.10.** ćemo koristiti sljedeće oznake. G je konačna multiplikativna grupa, K_0 je prosto polje, pri čemu karakteristika polja ne dijeli red grupe. $K = \widetilde{K_0}$ je algebarsko zatvorenje K_0. Sa Θ označimo Galoaovu grupu Galoaovog raširenja K/K_0. Jasno je da $K[G] \supseteq K_0[G]$ i da Θ ostavlja fiksnim potprsten $K_0[G]$.

Definicija 3.1. Primitivni idempotent prstena $C(R)$ nazivamo centralnim primitivnim idempotentom prstena R.

Sljedeća lema, kao uvodna u ovom poglavlju čini razumljivijim dokaze teorema u nastavku. Ona se bavi kako načinom razlaganja grupovne algebre $K[G]$, tako i svojstvima komponenti u tom razlaganju. Pokazuje se fundamentalna važnost centralnih primitivnih idempotenata, odnosno njihov direktni uticaj na građu $K[G]$.

Lema 3.1. *Skup centralnih primitivnih idempotenata algebre $K[G]$ je konačan, pri čemu su svaka dva elementa ovog skupa ortogonalna. Ako su $e_1, e_2, \dots, e_m$ svi centralni primitivni idempotenti $K[G]$ tada vrijedi:*

(a) $K[G] = \sum_{i=1}^{m} e_i K[G]$, *pri čemu su $e_i K[G]$ prosti dvostrani ideali prstena $K[G]$.*

(b) $K[G] \cong \sum_{i=1}^{m} M_{d_i}(K)$ *gdje su $M_{d_i}(K)$ prostori matrica dimenzija $d_i \times d_i$ sa elementima iz polja K.*

(c) *Elementi $e_1, e_2, \dots, e_m$ čine bazu K-modula $C(K[G])$.*

Dokaz. Kako je $K[G]$ poluprost prsten, to je $C(K[G])$ kao njegov potprsten takođe poluprost [3], pa prema teoremi **1.7.** vrijedi:

$$C(K[G]) = L_1 \oplus \dots \oplus L_m \quad (1)$$

gdje su $L_1, L_2, \dots, L_m$ prosti dvostrani ($C(K[G])$ je komutativan) ideali $C(K[G])$. Prema teoremi **1.6.** znamo da postoje $e_1, e_2, \dots, e_m$ ortogonalni idempotenti tako da $e_i \in L_i$ i $e_i \cdot C(K[G]) = L_i$. Prema lemi **2.2.** e_i su primitivni u $C(K[G])$, pa su na osnovu toga e_i centralni primitivni idempotenti prstena $K[G]$. Dokažimo da su to svi centralni primitivni idempotenti.

Neka je e proizvoljan centralni primitivni idempotent. Prema teoremi **1.6.** znamo da je $e \cdot C(K[G])$ dvostrani ideal u $C(K[G])$. Na osnovu leme **2.2.** $e \cdot C(K[G])$ je prost ideal. Proizilazi da je $e \cdot C(K[G]) = L_j$, za neki $j \in \{1, 2, \dots, m\}$, jer bi u suprotnom imali:

$$e \cdot C(K[G]) = \sum_{i=1}^{m} (e \cdot C(K[G]) \cap L_i),$$

što bi protivrječilo činjenici da je ovaj ideal prost. Kako je e_j jedinica u L_j, to je:

$$ee_j = e = e_j e. \quad (2)$$

S druge strane $e_j = eg$, $g \in K[G]$. Zaključujemo:

$$e_j e = e^2 g = eg = e_j \quad (3)$$

Iz (2) i (3) slijedi $e = e_j$. Sada je jasno da je broj centralnih primitivnih idempotenata konačan i da su svaka dva elementa tog skupa ortogonalna.
Iz zapisa (1) slijedi da je $1 = e_1 + e_2 + \ldots + e_m$, pa na osnovu tog možemo pisati:

$$K[G] = \sum_{i=1}^{m} e_i K[G].$$

Podsjetimo se da nam teorema **1.6.** obezbjeđuje tvrdnju da su $e_i K[G]$ dvostrani ideali. Dokažimo da su prosti. Prema teoremi **1.7.** znamo da $K[G]$ možemo predstaviti kao sumu prostih dvostranih ideala B_j, tj. $K[G] = \bigoplus_{j=1}^{m_1} B_j$. Za proizvoljno $i \in \{1, 2, \ldots, m\}$ imamo $e_i K[G] = \bigoplus_{j=1}^{m_1} (B_j \cap e_i K[G])$. Pošto su B_j prosti ideali prstena $K[G]$, to je:

$$B_j \cap e_i K[G] = B_j, \text{ ili } B_j \cap e_i K[G] = 0.$$

Slijedi:

$$e_i K[G] = B_{k_1} \oplus B_{k_2} \oplus \ldots \oplus B_{k_t}.$$

Ako su f_i jedinični elementi prstena B_{k_i} to je $e_i = f_1 + f_2 + \ldots + f_t$. Prema teoremi **1.7.**, znamo da je $\{f_1, f_2, \ldots, f_t\}$ skup ortogonalnih idempotenata prstena $K[G]$ što narušava pretpostavljenu primitivnost elementa e_i. Dakle, jasno je da je $t = 1$, pa je time $e_i K[G] = B_{k_1}$. Kako su e_i $(i = 1, 2, \ldots, m)$ nenulti elementi, time su $e_i K[G]$ nenulti prosti dvostrani ideali. Jedno od tvrđenja teoreme **1.7.** jeste jednoznačnost razlaganja prstena $K[G]$ na proste dvostrane ideala do na izomorfizam, pa nakon odgovarajuće prenumeracije zaključujemo $m = m_1$ i $e_i K[G] = B_i$. Time je (a) dokazano. Pošto ideali $e_i K[G]$ imaju do na izomorfizam jedinstven prosti desni ideal E_i, na osnovu teoreme **1.8.** slijedi:

$$e_i K[G] \cong End\,({}_{T_i} E_i) \cong M_{d_i}(T_i),$$

gdje je d_i dimenzija vektorskog prostora $E_i =_{T_i} E_i$, a T_i tijelo definisano kao u naznačenoj teoremi. Znamo da je $e_iK[G]$ konačno generisana algebra nad poljem K koje je algebarski zatvoreno, odakle proizilazi $T_i \cong K$ na osnovu teoreme **1.10.**. Zaključujemo da je:

$$e_iK[G] \cong M_{d_i}(K) \quad (4)$$

$$K[G] \cong \bigoplus_{i=1}^{m} M_{d_i}(K) \quad (5)$$

čime je dokazano (b). Iz (4) slijedi da je $C(e_iK[G]) \cong C(M_{d_i}(K))$, a pošto $C(M_{d_i}(K))$ čine samo skalarne matrice, to je stoga u pitanju jednodimenzioni K-prostor nad jediničnom matricom kao bazom. Jediničnoj matrici u izomorfizmu prstena (4) odgovara centralni primitivni idempotent e_i, što znači da je $C(e_iK[G]) = e_i \cdot K$. Iz ovog i (5) izvodimo zaključak $C(K[G]) = \bigoplus_{i=1}^{m} e_iK$, čime je pokazano da $e_1, e_2, \ldots, e_m$ čini K-bazu $C(K[G])$, pa je i (c) dokazano.

□

U narednoj lemi koristimo prirodno dejstvo grupe Θ na prsten $K[G]$. Orbitu centralnog primitivnog idempotenta e algebre $K[G]$ u odnosu na Θ predstavlja skup:

$$e^{\Theta} = \{\sigma(e) \mid \sigma \in \Theta\}$$

kog čine takođe centralni primitivni idempotenti algebre $K[G]$.

Lema 3.2. [4] *Neka su G i K grupa i polje usklađeni sa prethodno uvedenim oznakama. Tada postoji bijektivna veza između centralnih idempotenata prstena $K_0[G]$ i orbita centralnih primitivnih idempotenata prstena $K[G]$. Preciznije, svakom centralnom primitivnom idempotentu $f \in K_0[G]$ odgovara tačno jedna orbita:*

$$e^{\Theta} = \{e_1, e_2, \ldots, e_r\}$$

centralnog primitivnog idempotenta $e \in K[G]$.
Vrijedi $f \leftrightarrow e^{\Theta} = \{e_1, e_2, \ldots, e_r\}$ ako i samo ako $f = e_1 + e_2 + \ldots + e_r$. Dalje, vrijedi:

$$\dim_{K_0} fK_0[G] = |e^{\Theta}| \cdot \dim_K eK[G],$$

$$\dim_{K_0} C(fK_0[G]) = |e^{\Theta}|,$$

$$\dim_{C(fK_0[G])} fK_0[G] = \dim_K eK[G].$$

Dokaz. Kako je Θ grupa automorfizama na $K[G]$ to ona permutuje konačno mnogo centralnih primitivnih idempotenata ove algebre. Jasno je da su time sve njihove orbite u odnosu na Θ konačne. Neka je f centralni primitivni idempotent u $K_0[G]$. Dakle, f komutira sa svim elementima grupe G. Sada je izvjesno da je $f \in C(K[G])$. Neka su $e_1, e_2, \ldots, e_m$ svi centralni primitivni idempotenti $K[G]$. Prema prethodnoj lemi,

$$f = c_1e_1 + c_2e_2 + \ldots + c_me_m \quad (c_i \in K).$$

Zbog ortogonalnosti elemenata e_i slijedi da je $f^2 = c_1^2e_1 + c_2^2e_2 + \ldots + c_m^2e_m$. Pošto je $f^2 = f$, zaključujemo $c_i^2 = c_i \quad (i = 1, 2, \ldots, m)$. Kako je $c_i \in K$, a K polje, imamo:

$$c_i = 0 \text{ ili } c_i = 1 \quad (i = 1, 2, \ldots, m).$$

Nakon odgovarajuće prenumeracije f možemo zapisati kao:

$$f = e_1 + e_2 + \ldots + e_r.$$

Znajući da je $f \in K_0[G]$, tada:

$$(\forall \sigma \in \Theta) \quad f = f^\sigma = e_1^\sigma + e_2^\sigma + \ldots + e_r^\sigma,$$

odnosno:

$$\{e_1^\sigma, e_2^\sigma, \ldots, e_r^\sigma\} = \{e_1, e_2, \ldots, e_r\},$$

što znači da je $\{e_1, e_2, \ldots, e_r\}$ unija $\Theta-$orbita elemenata ovog skupa. Dokažimo da je Θ tranzitivno na $\{e_1, e_2, \ldots, e_r\}$, tj. da je ovaj skup orbita jednog elementa. Pretpostavimo suprotno. Odgovarajućom prenumeracijom možemo podrazumijevati da su oba skupa $\{e_1, e_2, \ldots, e_s\}$ i $\{e_{s+1}, \ldots, e_r\}$ invarijantni u odnosu na dejstvo Θ. Neka je $f' = e_1 + e_2 + \ldots + e_s$ i $f'' = e_{s+1} + \ldots + e_r$ tako da je $f = f' + f''$ suma dva centralna, ortogonalna idempotenta. Kako su f' i f'' invarijantni u odnosu na Θ to vrijedi $f', f'' \in K_0[G]$ što je u protivrječju sa činjenicom da je f primitivan. Tako je pokazano da je svaki f suma elemenata skupa koga čini $\Theta-$orbita nekog centralnog primitivnog idempotenta e. Kako je $\sum f = 1$, vidimo da ove orbite moraju "pokupiti" sve centralne primitivne idempotente u $K[G]$. Uz činjenicu da su svake dvije orbite disjunktne slijedi da je navedena veza bijektivna. Konačno, zbog $K[G] = K \underset{K_0}{\otimes} K_0[G]$ jasno je da:

$$fK[G] = K \underset{K_0}{\otimes} fK_0[G],$$

pa je $\dim_{K_0} fK_0[G] = \dim_K fK[G]$. Znamo da je $f = e_1 + e_2 + \ldots + e_r$, gdje je $r = |e^{\Theta}|$, a $e \in \{e_1, e_2, \ldots, e_r\}$ proizvoljno. Na osnovu ovog slijedi:

$$fK[G] = e_1K[G] \dotplus \ldots \dotplus e_rK[G].$$

Sumandi $e_iK[G]$ se permutuju tranzitivno od Θ, čime svi imaju iste K-dimenzije. Sada je očigledno:

$$\dim_{K_0} fK_0[G] = \dim_K fK[G] = r \cdot \dim_K eK[G] = |e^{\Theta}| \cdot \dim_K eK[G] \quad (1)$$

Pošto je $fK[G] = K \underset{K_0}{\otimes} fK_0[G]$, to je:

$$C(fK[G]) = K \underset{K_0}{\otimes} C(fK_0[G]),$$

pa iz (1) proizilazi:

$$\dim_{K_0} C(fK_0[G]) = \dim_K C(fK[G]) = r \cdot \dim_K C(eK[G])..$$

Kako je prema lemi **3.1.** $e_iK[G] \cong M_{d_i}(K)$, to je $C(e_iK[G]) \cong C(M_{d_i}(K))$. Na osnovu iste leme utvrdili smo $\dim_K C(M_{d_i}(K)) = 1$, tj. $\dim_K C(e_iK[G]) = 1$, pa zaključujemo $\dim_K C(fK[G]) = r = |e^{\Theta}|$. Prema teoremi **1.4.** $K_0[G]$ je poluprost, a $C(K_0[G])$, kao njegov potprsten takođe. Iz činjenice da je f centralni primitivni idempotent slijedi zaključak da je $f \cdot C(K_0[G])$ prost potprsten prstena $C(K_0[G])$. Pošto je:

$$f \cdot C(K_0[G]) = C(f(K_0[G])),$$

to je prema lemi **1.11.** $C(fK_0[G])$ polje. Sada je:

$$\dim_{C(fK_0[G])} fK_0[G] = (\dim_{K_0} fK_0[G])/(\dim_{K_0}(CfK_0[G])) =$$

$$= r \cdot \dim_K eK[G]/r = \dim_K eK[G].$$

□

Neka je dat $K[G]$-modul V, takav da je $\dim_K V = d$. Neka su $f_1, f_2, \ldots, f_d$ elementi K-baze tog modula. Za svako $l \in K[G]$ možemo formirati preslikavanje:

$$\varphi_l : V \to V, \quad \varphi_l(t) = l \cdot t.$$

Lako je utvrditi da je φ_l $K-$endomorfizam ovog modula kojem u odnosu na pomenutu K-bazu odgovara matrica:

$$\begin{bmatrix} a_{11} & a_{12} \ldots & a_{1d} \\ a_{21} & a_{22} \ldots & a_{2d} \\ \vdots & & \vdots \\ a_{d1} & a_{d2} \ldots & a_{dd} \end{bmatrix} \qquad (a_{ij} \in K).$$

Na ovaj način možemo formirati homomorfizam $\vartheta_V : K[G] \to End_K V$ dat sa:

$$\vartheta_V(l) = \varphi_l,$$

što čini reprezentaciju elemenata prstena $K[G]$ matricama u odnosu na fiksiranu bazu $K[G]-$modula V. Na osnovu ove reprezentacije možemo uvesti preslikavanje $\chi_V : K[G] \to K$ definisano sa:

$$\chi_V(l) = tr(\vartheta_V(l)),$$

gdje je tr trag matrice $\vartheta_V(l)$. Ovako definisano preslikavanje zovemo karakterom $K[G]-$modula V. Primijetimo da ukoliko u V izaberemo neku drugu bazu, matrice koje nastaju ustanovljenom reprezentacijom posmatranog elementa će biti slične. Kako su tragovi sličnih matrica isti, postaje jasno da karakter ne zavisi od baze. Pretpostavimo da su V i W dva izomorfna $K[G]$ modula sa $\mu : V \to W$ kao odgovarajućim izomorfizmom. Ako je $\{v_1, v_2, \ldots, v_d\}$ K-baza za V, tada je $\{\mu(v_1), \ldots, \mu(v_d)\}$ K-baza za W. Slijedi da je matrična reprezentacija u odnosu na ove baze modula V i W ista. Stoga vrijedi $\chi_V = \chi_W$.

Podsjetimo se definicije funkcije klasa. Neka je F polje, a G multiplikativna grupa. Funkcija $f : G \to F$ za koju vrijedi $f(xyx^{-1}) = f(y)$ $(\forall x, y \in G)$ zovemo funkcijom klasa grupe G nad poljem F. Na ovaj način funkciju klasa možemo shvatiti kao funkciju na klasama konjugovanih elemenata grupe. Sada možemo linearno raširiti oblast definisanosti funkcije klasa na grupovni prsten. Ukoliko je:

$$\alpha = \sum_{x \in G} a_x x$$

i f funkcija klasa, tada možemo definisati:

$$f(\alpha) = \sum_{x \in G} a_x f(x).$$

Neka je $x_0 \in G$. Pišemo $x \sim x_0$ ako je element $x \in G$ konjugovan sa $x_0 \in G$ tj. ukoliko postoji element $y \in G$ tako da je $x_0 = yxy^{-1}$. Element iz $F[G]$ koji ima oblik:

$$\gamma = \sum_{x \sim x_0} x$$

nazivamo sumom klase konjugovanih elemenata.

Definicija 3.2. Algebarski element nad poljem Q čiji minimalni polinom ima najstariji koeficijent 1, a ostale koeficijente iz prstena cijelih brojeva zovemo cijelim algebarskim elementom.

U sljedećoj lemi se koristi poznato tvrđenje da skup cijelih algebarskih elemenata u bilo kom proširenju polja Q čini prsten [16], kao i teorema da je svaka matrica nad algebarski zatvorenim poljem slična nekoj matrici koja ima gornju trougaonu formu.

Lema 3.3. [4] *Neka je V konačno dimenzioni $K[G]$-modul za koji je $\dim_K V = d$. Tada je $\chi_V : G \to K$ funkcija klasa G nad K i $\chi_V(1) = d$. Ukoliko je G grupa sa periodom n a ε primitivni n-ti korijen jedinice u K, tada za sve $x \in G$ vrijedi:*

$$\chi_V(x) = \varepsilon^{a_1} + \varepsilon^{a_2} + \ldots + \varepsilon^{a_d} \in K_0[\varepsilon],$$

gdje su $a_1, a_2, \ldots, a_d$ odgovarajući cijeli brojevi. Posebno, ukoliko je $K_0 = Q$ tada je $\chi_V(x)$ cijeli algebarski element nad poljem Q, koji je sadržan u ciklotomičnom polju $Q[\varepsilon]$.

Dokaz. Neka je $\vartheta_V : K[G] \to End_K V$ matrična reprezentacija u odnosu na neku K-bazu modula V. Očigledno $\chi_V(1) = d = \dim_K V$, pri čemu je χ_V karakter modula V. Ukoliko su x i y konjugovani elementi grupe G, tada su $\vartheta_V(x)$ i $\vartheta_V(y)$ slične matrice, pa je time $\chi_V(x) = \chi_V(y)$. Ukoliko G ima period n, tada vrijedi $(\forall x \in G)\ x^n = 1$. Prisjetivši se da je ϑ_V homomorfizam, vidimo da je $(\vartheta_V(x))^n = E$, gdje je E jedinična matrica u $M_d(K)$. Kako je K algebarski zatvoreno polje, znamo da postoji baza modula V u kojoj matrica endomorfizma $\vartheta_V(x)$ ima gornju trougaonu formu.

Neka su $\lambda_1, \lambda_2, \ldots, \lambda_d$ elementi na dijagonali matrice endomorfizma u odnosu na posmatranu bazu. Tada je:

$$tr(\vartheta_V(x)) = \lambda_1 + \lambda_2 + \ldots + \lambda_d \quad (\lambda_i \in K),$$

odakle slijedi:

$$tr(\vartheta_V(x))^n = \lambda_1^n + \lambda_2^n + \ldots + \lambda_d^n \Rightarrow tr(E) = \lambda_1^n + \lambda_2^n + \ldots + \lambda_d^n,$$

tj.

$$\lambda_i^n = 1 \quad (i = 1, 2, \ldots, d).$$

Sada shvatamo da postoje $a_1, a_2, \ldots, a_d$ cijeli brojevi tako da:

$$\varepsilon^{a_i} = \lambda_i \quad (i = 1, 2, \ldots, d),$$

pa zaključujemo:

$$tr(\vartheta_V(x)) = \varepsilon^{a_1} + \varepsilon^{a_2} + \ldots + \varepsilon^{a_d} \in K_0[\varepsilon],$$

odnosno:

$$\chi_V(x) = \varepsilon^{a_1} + \varepsilon^{a_2} + \ldots + \varepsilon^{a_d} \in K_0[\varepsilon].$$

Kako je svaki od sabiraka u prethodnoj sumi cijeli algebarski element, to je i $\chi_V(x)$ element prstena cijelih algebarskih elemenata nad poljem Q u ciklotomičnom proširenju $Q[\varepsilon]$.

□

Jedan od rezultata leme **3.1.** odnosi se na K-bazu K-modula $C(K[G])$. Sljedeća lema govori o još jednoj K-bazi centra algebre $K[G]$.

Lema 3.4. [10] *Element iz $F[G]$ je u $C(F[G])$, gdje je F polje, ako i samo ako je predstavljen kao F-linearna kombinacija elemenata oblika:*

$$\gamma = \sum_{x \sim x_0} x \quad (1)$$

(Relacija $\sim$ je relacija konjugacije u grupi G).

Dokaz. Neka je $\alpha = \sum_{x \in G} a_x x$, pri čemu je $(\forall y \in G)\ \alpha y = y\alpha$. Slijedi:

$$\sum_{x \in G} a_x y x y^{-1} = \sum_{x \in G} a_x x$$

Na osnovu ovog zapisa slijedi da $a_x = a_{yxy^{-1}}$ $(\forall y \in G)$, pa time pokazujemo da α mora biti linearna kombinacija elemenata oblika (1), tj. da su elementi oblika (1) F-baza za $C(F[G])$.

□

Na osnovu tvrđenja leme **3.1.** znamo da je $K[G] = \dot{\sum} e_i K[G]$, pri čemu vrijedi $e_i K[G] \cong M_{d_i}(K)$. Svaki od ovih sumanada imaju do na izomorfizam jedan prost desni ideal, tj. $K[G]$-modul V_i, pri čemu je $V_i e_i \neq 0$. Neka je $\chi_i = \chi_{V_i}$. Jasno je:

$$\chi_i(1) = d_i = \dim_K V_i.$$

Označimo sa $\hat{l}_1, \hat{l}_2, \ldots, \hat{l}_m$ sume odgovarajućih klasa konjugacije grupe G. Prema lemi **3.4.** vidimo da ovi elementi čine K-bazu vektorskog prostora $C(K[G])$. Primjetićemo da pod pretpostavkom da char$K \nmid |G|$ datom na početku poglavlja, za algebarski zatvoreno polje K, teorema **1.12.**, odnosno teorema **1.13.** obezbjeđuje da broj centralnih primitivnih idempotenata u $K[G]$ odgovara broju klasa konjugacije grupe G. Stoga je broj centralnih primitivnih idempotenata algebre $K[G]$ takođe m. Pošto skup $\{e_1, e_2, \ldots, e_m\}$ prema lemi **3.1.** čini bazu istog vektorskog prostora $C(K[G])$, to možemo svaki element pojedine baze predstaviti kao K-linearnu kombinaciju elemenata druge baze. O tome nam govori sljedeća lema.

Lema 3.5. [4] *Neka je $K[G]$ usklađeno sa usvojenim oznakama, a $|\hat{l}_i|$ predstavlja broj elemenata u klasi konjugacije kojoj odgovara $\hat{l}_i$. Tada je:*

(1) $\chi_i(1) \neq 0$ u K, $(i = 1, 2, \ldots, m)$

(2) $e_i = \sum_j \frac{\chi_i(1)\chi_i(x_j^{-1})}{|G|}\hat{l}_j$

(3) $\hat{l}_i = \sum_j \frac{|\hat{l}_i|\chi_j(x_i)}{\chi_j(1)}e_j$

Dokaz. Neka je $W = K[G]$ desni $K[G]$–modul i neka je $\psi = \chi_W$. U odnosu na prirodnu bazu G za W svaki element $x \in G$ permutuje ovu bazu. Dalje, $yx = y$ ima rješenje u ovoj bazi ako i samo ako je $x = 1$. U skladu sa tim slijedi da je $\psi(x) = 0$, za $x \neq 1$ i $\psi(1) = |G|$. Neka je $\alpha = \sum a_x x \in K[G]$ proizvoljni element, a $fr(\alpha) := a_1$. Tada je:

$$\psi(\alpha) = \sum a_x \psi(x) = a_1\psi(1) = |G| \cdot a_1 = |G| \cdot fr\alpha$$

Dalje, $W = K[G] = \sum_j e_j K[G]$ i $e_j K[G] \cong M_{d_j}(K)$, pri čemu $e_j K[G]$ ima do na izomorfizam jedan prosti $K[G]$-modul V_j. Svaka od d_j vrsta matrice $M_{d_j}(K)$ je izomorfna V_j, što znači da je:

$$M_{d_j}(K) \cong d_j V_j = V_j \oplus V_j \oplus \ldots \oplus V_j,$$

odnosno $W = \sum_j d_j V_j$. U terminima odgovarajućih karaktera imamo:

$$\psi = \sum_j d_j \chi_j.$$

Fiksirajmo indeks i, pa zapišimo $e_i = \sum b_x x$. Tada za svaki $x \in G$,

$$|G| \cdot b_x = |G| \cdot fr(e_i x^{-1}) = \psi(e_i x^{-1}) = \sum_j d_j \chi_j(e_i x^{-1}).$$

Kako e_i predstavlja nulu na svakom V_j, $j \neq i$, to slijedi da za takve indekse j $\chi_j(e_i x^{-1}) = 0$. Sa druge strane e_i ima ulogu jedinice na V_i pa je: $\chi_i(e_i x^{-1}) = \chi_i(x^{-1})$, odakle proizilazi:

$$|G| \cdot b_x = \sum_j d_j \chi_j(e_i x^{-1}) = d_i \chi_i(x^{-1}).$$

Zato,

$$b_x = \frac{d_i \chi_i(x^{-1})}{|G|} = \frac{\chi_i(1)\chi_i(x^{-1})}{|G|}$$

i

$$e_i = \sum_x \frac{\chi_i(1)\chi_i(x^{-1})}{|G|} \cdot x = \sum_j \frac{\chi_i(1)\chi_i(x_j^{-1})}{|G|} \cdot \hat{l}_j,$$

jer je $\chi_i(x) = \chi_i(x_j)$ ukoliko je $x \sim x_j$. Iz činjenice da je $e_i \neq 0$ vidimo da je $\chi_i(1) \neq 0$ u K. Neka je dato predstavljanje kao u prethodnoj lemi:

$$\hat{l}_i = \sum_j c_j e_j \quad (c_j \in K)$$

Tada je $e_j \hat{l}_i = c_j e_j$, odnosno $\chi_j(c_j e_j) = \chi_j(e_j \hat{l}_i)$. Pošto e_j predstavlja 1 na V_j, slijedi:

$$c_j \chi_j(1) = \chi_j(c_j e_j) = \chi_j(e_j \hat{l}_i) = \chi_j(\hat{l}_i).$$

Kako je $\hat{l}_i$ suma $|\hat{l}_i|$ konjugovanih elemenata sa x_i, koji imaju isti karakter $\chi_j(x_i)$, proizilazi $\chi_j(\hat{l}_i) = |\hat{l}_i| \chi_j(x_i)$, a zbog $\chi_j(1) \neq 0$ u K, zaključujemo:

$$c_j = |\hat{l}_i| \frac{\chi_j(x_i)}{\chi_j(1)}.$$

□

Lema 3.6. [4]

(1) *Za svaki $x \in G$ i indekse i, j vrijedi:*

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g^{-1}) \chi_j(xg) = \delta_{ij} \chi_i(x) / \chi_i(1),$$

gdje je δ_{ij} Kronekerov simbol.

(2) *Ukoliko je $charK = 0$, tada $\chi_i(1)$ dijeli $|G|$.*

Dokaz.

(1) Ukoliko u prethodnoj lemi izmnožimo $e_i e_j$ i sredimo izraz u obliku:

$$\sum_{x \in G} c_{x^{-1}} x^{-1}$$

tada je:

$$c_{x^{-1}} = \sum_{g\in G} \frac{\chi_i(1)\chi_i(g^{-1})}{|G|} \cdot \frac{\chi_j(1)\chi_j(xg)}{|G|} \quad (*)$$

Ukoliko je $i \neq j$ tada je $e_ie_j = 0$, pa je $c_{x^{-1}} = 0$. Kako su $\chi_i(1)$ i $\chi_j(1)$ različiti od nule u K, to je slučaj $i \neq j$ dokazan. U slučaju $i = j$, $e_ie_j = e_i$, pa je:

$$c_{x^{-1}} = \frac{\chi_i(1)\chi_i(x)}{|G|} \quad (**)$$

Upoređujući $(*)$ i $(**)$ lako slijedi rezultat za $i = j$, čime je (1) ukupno dokazano.

(2) Neka je char$K = 0$. Tada je prosto potpolje K_0 polja K u stvari polje racionalnih brojeva Q. Prema lemama **3.3.** i **3.5.** $e_i = \frac{\chi_i(1)}{|G|} \cdot \beta_i$, pri čemu su svi koeficijenti u β_i cijeli algebarski elementi nad poljem Q. Za svaki prirodan broj $t \geqslant 2$ vrijedi:

$$e_i = e_i^t(\frac{\chi_i(1)}{|G|})^t\beta_i^t,$$

a upoređujući koeficijente uz jedinicu u ovom identitetu zaključujemo:

$$\frac{\chi_i(1)^2}{|G|} = \left(\frac{\chi_i(1)}{|G|}\right)^t \gamma_t,$$

gdje je γ_t cijeli algebarski element nad Q. Iz prethodnog zapisa γ_t je i sam racionalan, pa zbog prethodnog, slijedi da je γ_t cio broj. Zbog $|G|^{t-1} = \chi_i(1)^{t-2}\gamma_t$, zaključujemo da $\chi_i(1)^{t-2}$ dijeli $|G|^{t-1}$ za sve $t \geqslant 2$. Neka je p prost broj, a m i n maksimalni prirodni brojevi takvi da p^m, odnosno p^n, dijeli $\chi_i(1)$, odnosno $|G|$. Tada iz prethodnog slijedi da je $m(t-2) \leqslant n(t-1)$ za svaki t. Proizilazi da je $m \leqslant n$, zbog čega $\chi_i(1)$ dijeli $|G|$.

□

U analizi svojstava algebre $K[G]$ značajna su tri njegova potpolja. Prvo, neka je e centralni primitivni idempotent algebre $K[G]$, tada je $K_0(e)$ polje generisano sa K_0 i svim koeficijentima od e. Sljedeće, neka je χ karakter nekog prostog $K[G]$-modula, tada je $K_0(\chi)$ polje generisano sa K_0 i svim $\chi(x)$, $(x \in G)$. Konačno, ukoliko je f centralni primitivni idempotent $K_0[G]$, tada postaje interesantan $C(fK_0[G])$ kao centar prostog sumanda $fK_0[G]$. Navedimo nekoliko tvrđenja iz okvira teorije Galoa koja su nam važna u dokazu leme **3.10.**.

Teorema 3.7. [10] *Neka je F Galuaovo raširenje polja F_0 sa grupom G. Neka je F_1 potpolje, $F_0 \subset F_1 \subset F$ i $H = G(F/F_1)$. F_1 je normalno nad F_0 ako i samo ako je H normalna podgrupa u G.*

□

Lema 3.8. [11] *Neka je L algebarsko proširenje polja F, a M algebarski zatvoreno polje. Tada se svaki monomorfizam $\varphi_0 : F \to M$ može produžiti do monomorfizma $\varphi : L \to M$.*

□

Teorema 3.9. [11] *Neka je L algebarsko proširenje polja F, a M bilo koje proširenje polja L. Ako je polje L invarijantno u odnosu na relativni F-monomorfizam $\varphi : L \to M$, tada je $Im(\varphi) = L$, tj. $\varphi(L) \subseteq L \Rightarrow \varphi(L) = L$.*

Dokaz. Ako je $\beta \in L$ bilo koji element, treba pokazati postojanje $\alpha \in L$ tako da vrijedi $\varphi(\alpha) = \beta$. Stvarno, neka je $f(x) \in F[x]$ minimalni polinom elementa β u odnosu na F, a A skup svih nula $\alpha \in L$ toga polinoma. Kako φ svaku nulu polinoma $f(x)$ prevodi u neku nulu toga polinoma, imamo injektivno preslikavanje $\varphi_A : A \to A$. Skup A je, međutim, konačan, pa je to preslikavanje i sirjektivno. Zato postoji neko $\alpha \in A$ tako da je $\beta = \varphi_A(\alpha) = \varphi(\alpha)$. To znači da je $L = Im(\varphi)$ i teorema je dokazana.

□

Lema 3.10. [4] *Neka je $K[G]$ usklađeno sa oznakama datim na početku poglavlja, a f centralni primitivni idemopotent u $K_0[G]$. Pretpostavimo da je $f \leftrightarrow e^{\Theta}$, a χ karakter koji odgovara prostom modulu $eK[G]$. Tada vrijedi:*

$$K_0(e) = K_0(\chi) = C(fK_0[G]) \quad (1)$$

Ukoliko je G grupa sa periodom n, a ε primitivni n-ti korijen jedinice u K, tada se polje (1) sadrži u $K_0[\varepsilon]$ i predstavlja konačno normalno raširenje polja K_0 sa Abelovom Galoaovom grupom.

Dokaz. Ukoliko primjenimo lemu **3.5.** za $e = e_i$ i $\chi = \chi_i$ imamo:

$$e = \sum_{x \in G} \frac{\chi(1)\,\chi(x^{-1})}{|G|}\,x.$$

Pošto je $\chi(1) \neq 0$ u K i $\dfrac{\chi(1)}{|G|} \in K_0$, na osnovu prethodnog zapisa očigledno je $K_0(e) = K_0(\chi)$. Neka je $F = C(fK_0[G])$. U skladu sa pretpostavkom, f je centralni primitivni idempotent u $K_0[G]$, pa je zapravo $F = f \cdot C\,(K_0[G])$. Kako je e centralni primitivni idempotent algebre $K[G]$, to je preslikavanje:

$$F = fC(K_0[G]) \to e \cdot fC(K_0[G])$$

epimorfizam prstena. Međutim $ef = e$ na osnovu leme **3.2.**, a F je polje, te je stoga prethodno preslikavanje i monomorfizam. Ovo je posljedica tvrđenja da je svaki homomorfizam $F \to L$, gdje je F polje, monomorfizam. Dakle:

$$F \cong e\,C\,(K_0[G]).$$

Na osnovu leme **3.4.** slijedi da je $C\,(K_0[G])$ generisano sumama klasa $\hat{l}_j$ nad K_0, a prema lemi **3.5.** imamo da je $eC(K_0[G])$ generisano elementima:

$$e\hat{l}_j = \frac{|\hat{l}_j|\,\chi(x_j)}{\chi(1)}e,$$

nad poljem K_0. Treba primijetiti da zbog $|G| \neq 0$ u K i toga što $|\hat{l}_j|$ dijeli $|G|$, slijedi $|\hat{l}_j| \neq 0$ u K_0, kao i da je $|\hat{l}_j|/\chi(1) \in K_0$. Vidimo da je $e \cdot C(K_0[G]) = e \cdot K_0(\chi)$, a zbog toga što je $e \cdot C(K_0[G])$ polje i $K_0(\chi) \to e \cdot K_0(\chi)$ epimorfizam proizilazi:

$$e \cdot C(K_0[G]) = e \cdot K_0(\chi) \cong K_0(\chi),$$

odnosno:

$$C(fK_0[G]) \cong K_0(\chi) \quad (1)$$

Prema lemi **3.3.** slijedi $K_0(\chi) \subseteq K_0[\varepsilon]$, dok je $K_0[\varepsilon]$ kao ciklotomično proširenje polja K_0, prema poznatom tvrđenju, Galoaovo sa Abelovom grupom $K_0[\varepsilon]/K_0$. Na osnovu teoreme **3.7.** imamo da je $K_0(\chi)$ normalno proširenje polja K_0.

Neka je $\varphi_0 : K_0(\chi) \to C(fK_0[G])$, K_0-izomorfizam utvrđen u (1). Ako $C(fK_0[G])$ posmatramo kao potpolje algebarski zatvorenog polja K tada nam lema **3.8.** omogućava zaključak o produženju monomorfizma φ_0, do monomorfizma $\varphi : K \to K$. Pošto je K algebarsko proširenje polja $K_0(\chi)$, to je K_0 monomorfizam φ u stvari K_0-automorfizam polja K. Kako smo već urtvrdili da je $K_0(\chi)$ normalno nad K_0, to je zapravo $\varphi(K_0(\chi)) \subseteq K_0(\chi)$ odnosno $\varphi(K_0(\chi)) = K_0(\chi)$, na osnovu teoreme **3.9.**, čime je dokazano i $C(fK_0[G]) = K_0(\chi)$.

□

Neka je e centralni primitivni idempotent algebre $K[G]$. Već je više puta istaknuta posljedica leme **3.1.** u obliku $eK[G] \cong M_d(K)$. Definišimo pojam stepena tog elementa kao:

$$\deg e := d,$$

a sa $\mathrm{Int}Q(e)$ označimo prsten algebarskih elemenata u $Q(e)$ nad poljem Q. Konačno polje od p^n elemenata označavamo sa $GF(p^n)$ i zovemo Galoaovim poljem. Za proizvoljno polje F, sa $\widetilde{F}$ ćemo označavati njegovo algebarsko zatvorenje.

Definicija 3.3. Za potprsten R polja F se kaže da je prsten valuacije polja F ukoliko za svako $x \in F$, $x \notin R$ vrijedi $x^{-1} \in R$.

Lema 3.11. *Neka je R prsten valuacije polja F. Ako sa M označimo skup neinvertibilnih elemenata u R, tada je M jedinstven maksimalni ideal u R.*

Dokaz. Neka su $x, y \in R$. Ako je $xy \in R$ invertibilan element u R, tj. da je injegov inverz u R, tada su i $x \in R$ i $y \in R$ invertibilni u R. To slijedi iz:

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

dok se za y pokazuje analogno s obzirom na to da je množenje u polju komutativno. Ovo zapravo znači da je $MR = RM \subseteq M$. Neka su $x, y \in M$. Posmatrajmo $x - y$.

Ako je jedan od ovih elemenata 0, onda je:

$$x - y \in M.$$

Ako su oba različiti od nule, onda po definiciji slijedi ili $x^{-1}y \in R$ ili $y^{-1}x \in R$, te je stoga:

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

odnosno:

$$x - y \in M.$$

Dakle, M je ideal. Konačno, svaki pravi ideal u R se sastoji od neinvertibilnih elemenata pa se zato i sadrži u M čime je pokazano da je M jedinstven maksimalan ideal u R.

□

Sada možemo prirodni homomorfizam $R \to R/M$ (R je prsten valuacije polja F, a R/M je polje) proširiti na sljedeći način:

$$\varphi_R(x) = \begin{cases} x + M & x \in R \\ \infty & x \in F - R \end{cases}$$

gdje je ∞ neki element koji nije u R/M. Ovakvo preslikavanje $\varphi_R : F \to R/M \cup \{\infty\}$ zovemo valuacionim. Ovaj primjer može poslužiti kao uvod u definiciju valuacionog preslikavanja.

Definicija 3.4. Za preslikavanje $\varphi : F \to F' \cup \{\infty\}$, gdje su F, F' polja, kažemo da je valuaciono ukoliko je $R := \varphi^{-1}(F')$ prsten valuacije polja F, $\varphi : R \to F'$ homomorfizam prstena i vrijedi:

$$\varphi(x) = \infty \text{ ako i samo ako } \varphi(x^{-1}) = 0.$$

Slijedi važna teorema koja govori o produženju homomorfizma iz nekog potprstena polja F u algebarski zatvoreno polje F' do nekog valuacionog preslikavanja iz F u F'.

Teorema 3.12. [4] *Neka je F polje, S njegov potprsten a $\sigma : S \to F'$ homomorfizam u algebarski zatvoreno polje F'. Tada postoji valuaciono preslikavanje:*

$$\varphi_R : F \to F' \cup \{\infty\}$$

takvo da $R \supseteq S$, a koje se sa σ slaže na S.

□

Sljedeća lema ukazuje da valuaciono preslikavanje iz polja $\widetilde{Q}$ u polje $\widetilde{GF}(p)$ ne "deformiše" centralne primitivne idempotente algebre $\widetilde{Q}[G]$. Takođe, vidimo da ovo preslikavanje potprsten $\mathrm{Int}Q(e_i)$ polja $\widetilde{Q}$ "pretvara" u određeno potpolje polja $\widetilde{GF}(p)$.

Lema 3.13. [4] *Neka je G konačna grupa, a p prost broj koji ne dijeli $|G|$ i*

$$\varphi : \widetilde{Q} \to \widetilde{GF}(p) \cup \{\infty\}$$

valuaciono preslikavanje sa prstenom valuacije R. Ako su $e_1, e_2, \ldots, e_m$ centralni primitivni idempotenti algebre $\widetilde{Q}[G]$, tada $e_i \in R[G]$ za svako i, dok su:

$$\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_m)$$

svi centralni primitivni idempotenti algebre $\widetilde{GF}(p)[G]$. Na kraju,

$$\deg \varphi(e_i) = \deg e_i, \quad \varphi(IntQ(e_i)) = GF(p)(\varphi(e_i))$$

Dokaz. Neka je M jedinstveni maksimalni ideal prstena R. Primijetimo da je $Ker(\varphi) = M$. Ako je Z prsten cijelih bojeva, imamo $Z \subseteq R$ i $pZ \subseteq M$. Uostalom, to je vidljivo iz

$$R \cap Q = \left\{ \frac{a}{b} \,|\, a, b \in Z \ i \ p \nmid b \right\},$$

odnosno

$$M \cap Q = \left\{ \frac{a}{b} \,|\, a, b \in Z, \ p \,|\, a, \ p \nmid b \right\}$$

Dokažimo sada tvrdnju da ukoliko je $\alpha \in \widetilde{Q}$ cijeli algebarski element, tada je $\alpha \in R$. Neka je $\alpha^t + a_1\alpha^{t-1} + \ldots + a_t = 0$ jednačina sa cijelim koeficijentima. Pretpostavimo

suprotno, tj. $\varphi(\alpha) = \infty$. Tada je $\varphi\left(\frac{1}{\alpha}\right) = 0$, tako da je $\frac{1}{\alpha} \in M$.
Iz $1 + a_1\alpha^{-1} + \ldots + a_t\alpha^{-t} = 0$ zaključujemo $1 \in M$, što je kontradikcija. Prema lemi **3.5.** vrijedi:

$$e_i = \sum_j \frac{\chi_i(1)\,\chi_i(x_j^{-1})}{|G|}\,\hat{l}_j \quad (1)$$

Zato što p ne dijeli $|G|$, to je $\frac{1}{|G|} \in R \cap Q$. Pošto je $\chi_i(1) \in Z \subseteq R$ slijedi $\chi_i(1)\frac{1}{|G|} \in R$.
Po tvrđenju leme **3.3.** $\chi_i(x_j^{-1})$ su algebarski nad Q, što prema prethodno dokazanoj tvrdnji znači da je $\chi_i(x_j^{-1}) \in R$. Sada je očigledno da je $e_i \in R[G]$.
Iz leme **3.6.**(2) imamo da $\chi_i(1)$ dijeli $|G|$, pa $p \nmid \chi_i(1)$. Analizom koeficijenta uz jedinicu u zapisu (1) zaključujemo da $e_i \notin M(G)$. Iz zapisa centralnog primitivnog idempotenta u lemi **3.5.**, vidimo da je $\{\varphi(e_i) \mid i = 1, 2, \ldots, m\}$ skup nenultih ortogonalnih centralnih idempotenata. Broj m je prema teoremi **1.12.** jednak broju klasa konjugacije grupe G. Prema teoremi **1.13.** slijedi da je broj neizomorfnih prostih (ireducibilnih) $\widetilde{GF}(p)[G]$ modula jednak broju $p-$regularnih klasa konjugacije grupe G. Pošto $p \nmid |G|$, taj broj je takođe m, pa su $\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_m)$ centralni primitivni idempotenti algebre $\widetilde{GF}(p)[G]$. Dokazujemo da su to svi centralni primitivni idempotenti. Naime, ako pretpostavimo da su $p_1, p_2, \ldots, p_m$ neki centralni primitivni idempotenti pomenute algebre, tada je svaki $\varphi(e_i)$ $(i = 1, 2 \ldots, m)$ linearna kombinacija elemenata skupa $\{p_1, p_2, \ldots, p_m\}$, na osnovu leme **3.1.**.
Pretpostavimo da bar u jednoj linearnoj kombinaciji učestvuje više od jednog elementa iz skupa $\{p_1, p_2, \ldots, p_m\}$. Na osnovu Dirhleovog principa slijedi da postoji neprazan skup $A \subseteq \{1, 2, \ldots, m\}$ tako da elementi $\{p_i \mid i \in A\}$ učestvuju u K-linearnoj kombinaciji za bar dva elementa, npr. $\varphi(e_s)$ i $\varphi(e_t)$. Iz ovog slijedi da:

$$\varphi(e_s) \cdot \varphi(e_t) = \sum_{i \in A} p_i \neq 0,$$

jer je $\{p_i \mid i \in A\} \subseteq \{p_1, p_2, \ldots, p_m\}$ K-linearno nezavisan skup, što je u suprotnosti sa činjenicom da su $\varphi(e_i)$ $(i = 1, 2, \ldots, m)$ međusobno ortogonalni. Nakon odgovarajuće prenumeracije slijedi:

$$\varphi(e_i) = p_i \quad (i = 1, 2, \ldots, m)$$

čime je dokazana tvrdnja.

Neka je sada $d_i = \deg e_i$ i $\bar{d}_i = \deg \varphi(e_i)$. Već je utvrđeno da je $e_i \in R[G]$. Posmatrajmo prsten $R[G]$ kao lijevi R-modul sa bazom G. Definišimo preslikavanje $f_{e_i} : R[G] \to R[G]$ sa:

$$f_{e_i}(a) = e_i \cdot a$$

Ovom preslikavanju odgovara matrica S reda $n \times n$ čiji su svi elementi iz R. Međutim,

$$e_i\widetilde{Q}[G] \cong M_{d_i}[\widetilde{Q}],$$

pa matrica S mora imati rang $\leqslant d_i^2$ nad poljem $\widetilde{Q}$. Proizilazi da je determinanta svakog $(d_i^2+1) \times (d_i^2+1)$ minora jednaka nuli. Očigledno je da je matrica za element $\varphi(e_i)$ u analognom preslikavanju na $\widetilde{GF}(p)[G]$ samo homomorfna slika prve matrice u odnosu na φ, pa je stoga determinanta svakog $(d_i^2+1) \times (d_i^2+1)$ minora matrice $\varphi(S)$ takođe nula. Kako je rang druge matrice u stvari $\bar{d}_i^{\,2}$, zaključujemo da je $\bar{d}_i^{\,2} < d_i^2 + 1$ odnosno $\bar{d}_i \leqslant d_i$. S druge strane računajući dimenzije imamo:

$$|G| = \dim_{\widetilde{Q}} \widetilde{Q}[G] = \sum \dim e_i\widetilde{Q}[G] = \sum d_i^2$$

$$|G| = \dim_{\widetilde{GF}(p)} \widetilde{GF}(p)[G] = \sum \dim \varphi(e_i)\widetilde{GF}(p)[G] = \sum \bar{d}_i^{\,2},$$

pa slijedi:

$$\deg e_i = d_i = \bar{d}_i = \deg \varphi(e_i).$$

Neka je $\{e_1, e_2, \dots, e_r\}$ orbita Galoaove grupe Θ . Prema lemama **3.3.** i **3.5.** možemo pisati:

$$|G|e_i = \sum_g c(i,g)g,$$

gdje su $c(i,g)$ cijeli algebarski elementi nad Q, odnosno:

$$|G|\varphi(e_i) = \sum_g \varphi(c(i,g))g.$$

Pošto je $|G| \neq 0$ u $GF(p)$ to je:

$$\varphi(e_i) = \sum_g \frac{1}{|G|}\varphi(c(i,g))g,$$

što znači da je $GF(p)(\varphi(e_1))$ generisan elementima $\varphi(c(1,g))$ nad poljem $GF(p)$. Jasno je da $c(1,g) \in \mathrm{Int}Q(e_1)$, dok je na početku dokaza leme utvrđeno da je

$\mathrm{Int}Q(e_1) \subseteq R$, iz čega proizilazi $\varphi(\mathrm{Int}Q(e_1)) \supseteq GF(p)(\varphi(e_1))$. Za dokaz suprotne inkluzije, primijetićemo da su $\varphi(e_1)$, $\varphi(e_2)$, ..., $\varphi(e_r)$ kao elementi baze centra prstena $\widetilde{GF}(p)[G]$ linearno nezavisni. Stoga matrica reda $r \times |G|$ i oblika:

$$[\varphi(c(i, g))] \quad (i = 1, 2, \ldots, r)$$

ima rang r. Dakle, postoji $\{g_1, g_2, \ldots, g_r\}$, skup r elemenata grupe G, tako da:

$$\det[\varphi(c(i, g_j))] \neq 0 \quad (i = 1, 2, \ldots, r).$$

Zato, ako je $C = [c(i, g)] \in M_r(R)$, tada je:

$$\varphi(\det C) \neq 0 \Rightarrow \det C \notin M \Rightarrow (\det C)^{-1} \in R.$$

Sada ćemo uočiti da su elementi:

$$c(1, g_1),\ c(1, g_2),\ \ldots,\ c(1, g_r) \in Q(e_1)$$

u stvari Q-baza za $Q(e_1)$. Neka je element $f_1 \in Q[G]$ centralni primitivni idempotent koji odgovara elementu e_1 u bijektivnoj vezi $f_1 \leftrightarrow e_1^\Theta$ datoj u lemi **3.2.**. Prema lemi **3.10.** vrijedi, $C(f_1 Q[G]) = Q(e_1)$, dok prema lemi **3.2.** imamo:

$$\dim_Q C(f_1 Q[G]) = |e_1^\Theta|,$$

odnosno:

$$\dim_Q Q(e_1) = r.$$

Neka je:

$$q_1 c(1, g_1) + q_2 c(1, g_2) + \ldots + q_r c(1, g_r) = 0 \quad (q_j \in Q).$$

Ako je $\sigma_i \in \Theta$, tako da je $e_1^{\sigma_i} = e_i$, tada je $c(1, g_j)^{\sigma_i} = c(i, g_j)$. Primjenjujući σ_i na gornju jednakost dobijamo:

$$q_1 c(i, g_1) + q_2 c(i, g_2) + \ldots + q_r c(i, g_r) = 0 \quad (i = 1, 2, \ldots, r).$$

Kako je dokazano da je $\det C \neq 0$, proizilazi $q_j = 0$ za svako j, čime je pokazano da su naznačeni elementi Q-baza za $Q(e_1)$. Konačno, pretpostavimo $\alpha \in \mathrm{Int}Q(e_1)$. Prema prethodnom imamo:

$$\alpha = q_1 c(1, g_1) + q_2 c(1, g_2) + \ldots + q_r c(1, g_r) \quad (q_j \in Q).$$

Ako primijenimo automorfizme σ_i na prethodnu jednakost imamo:

$$\alpha^{\sigma_i} = q_1 c(i, g_1) + q_2 c(i, g_2) + \ldots + q_r c(i, g_r).$$

Ovaj sistem od r jednačina sa r nepoznatih $q_1, q_2, \ldots, q_r$ možemo riješiti Kramerovim pravilom. Tako zaključujemo da je $q_j = \frac{\gamma_j}{\det C}$, gdje je γ_j determinanta matrice čiji su svi elementi algebarski cijeli. Proizilazi da je γ_j algebarski cijeli element, pa i $\gamma_j \in R$. Pošto je $(\det C)^{-1} \in R$ vidimo da je $q_j \in R \cap Q$ i $\varphi(q_j) \in GF(p)$. Zbog:

$$\varphi(\alpha) = \sum_j \varphi(q_j)\varphi(c(1, g_j)) \in GF(p)(\varphi(e_1)),$$

možemo napisati:

$$\varphi(\mathrm{Int}Q(e_1)) \subseteq GF(p)(\varphi(e_1)),$$

čime je lema dokazana.

□

Sljedeća teorema, zasnovana na prethodnim rezultatima, omogućava nam konstrukciju izomorfnih grupovnih algebri ograničavajući pažnju samo na polje Q racionalnih brojeva. Treba naglasiti da se u ovoj teoremi oznaka K ne odnosi na algebarski zatvoreno polje kao u prethodnim lemama.

Teorema 3.14. [12] *Neka su G i H konačne grupe i pretpostavimo da je:*

$$Q[G] \cong Q[H].$$

Za sva polja K čija karakteristika ne dijeli $|G| = |H|$ vrijedi:

$$K[G] \cong K[H].$$

Dokaz. Neka je K_0 prosto potpolje polja K i pretpostavimo da je $K_0[G] \cong K_0[H]$. Pošto se radi o K_0-izomorfizmu imamo:

$$K[G] = K \otimes_{K_0} K_0[G] \cong K \otimes_{K_0} K_0[H] = K[H]$$

što predstavlja $K-$izomorfizam. Prethodno nam ukazuje da je dovoljno pozabaviti se prostim poljima. Kako je slučaj $K = Q$ već dat u pretpostavci teoreme, moramo pokazati da vrijedi $GF(p)[G] \cong GF(p)[H]$ za svaki prosti broj p koji ne dijeli

$|G| = |H|$. Uočimo da je $|G| = |H|$ Q-dimenzija grupovne algebre $Q[G] \cong Q[H]$. Pretpostavimo, da $p \nmid |G|$. Ukoliko pokažemo da $Q[G]$ određuje $GF(p)[G]$ do na izomorfizam, dokazaćemo ukupno tvrđenje teoreme. Kao što znamo, $Q[G] = \bigoplus_{j=1}^{t} S_j$ je jednoznačno predstavljanje prstena $Q[G]$ u obliku direktne sume prostih prstena. Tada je $F = C(S)$, odnosno $\dim_F S$, za svaki $S = S_j$ određen do na izomorfizam. Neka je f centralni primitivni idempotent koji odgovara prstenu S, tj. $S = fQ[G]$, a e njemu odgovarajući centralni primitivni idempotent algebre $Q[G]$ u smislu veze datoj u lemi **3.2.**,

$$f \leftrightarrow e^{\Theta} = \{e_1, e_2, \ldots, e_r\}.$$

Na osnovu iste leme vrijedi $r = |e^{\Theta}| = \dim_Q F$, što je određeno algebrom $Q[G]$, kao i $\deg e$ jer:

$$(\deg e)^2 = \dim_{\widetilde{Q}} e\widetilde{Q}[G] = \dim_{C(fQ[G])} fQ[G] = \dim_F S.$$

Konačno, lema **3.10.** podržava tvrdnju:

$$Q(e) = F.$$

Ovim smo utvrdili da grupovna algebra $Q[G]$ u potpunosti određuje skup uređenih parova (d_i, F_i) $(i = 1, 2, \ldots, m)$ gdje je $d_i = \deg e_i$, a e_i centralni primitivni idempotent algebre $\widetilde{Q}[G]$, a $F_i \subseteq \widetilde{Q}$ odgovarajuća polja $Q(e_i)$. Vidimo da svakom prostom sumandu S_i algebre $Q[G]$ odgovara tačno jedan F_i. Na osnovu teoreme **3.12.** homomorfizam $Z \to Z/pZ \subseteq \widetilde{GF}(p)$ se može produžiti do valuacionog preslikavanja:

$$\varphi : \widetilde{Q} \to \widetilde{GF}(p) \cup \{\infty\}.$$

Pošto $p \nmid |G|$, lema **3.13.** nam omogućava da preko skupa uređenih parova:

$$(d_i, \varphi(\mathrm{Int} F_i)) \quad (i = 1, 2, \ldots, m),$$

dobijemo odgovarajuću informaciju za centralne primitivne idempotente algebre: $\widetilde{GF}(p)[G]$. Ta informacija je, naravno, određena algebrom $Q[G]$ i preslikavanjem φ koje ne zavisi od grupe G. Neka je:

$$L_i = \varphi(\mathrm{Int} F_i).$$

Razmotrimo sada vezu između ovih prstena i prostih sumanada u $GF(p)[G]$. Pretpostavimo da je $\bar{S} = \bar{f} \cdot GF(p)[G]$ prosti sumand konačnog prstena $GF(p)[G]$. $\bar{S}$ je prema teoremi **1.8**. izomorfno nekom $M_d(L)$, gdje je L, na osnovu iste teoreme, konačno tijelo, odnosno polje prema Vederburnovoj teoremi. Svakom prostom sumandu $\bar{S}$ algebre $GF(p)[G]$ odgovara tačno jedan L. Neka je $\bar{f} \leftrightarrow \{\bar{e}_1, \ldots, \bar{e}_k\}$ bijektivna veza data u lemi **3.2.**. Pošto je:

$$\bar{f} \cdot GF(p)[G] \cong M_d(L),$$

slijedi:

$$C(\bar{f} \cdot GF(p)[G]) \cong C(M_d(L)) \cong L \quad (1)$$

Sada je:

$$\deg \bar{e}_i = \sqrt{\dim_{\widetilde{GF(p)[G]}} \bar{e}_i \widetilde{GF}(p)[G]} =$$

$$\sqrt{\dim_{C(\bar{f}GF(p)[G])} \bar{f}GF(p)[G]} = \sqrt{\dim_L M_d(L)} = \sqrt{d^2} = d,$$

$$(i = 1, 2, \ldots, k).$$

Takođe, prema lemi 3.2. imamo:

$$k = \bar{e}_1^{\,?} = \dim_{GF(p)} C(\bar{f}GF(p)[G]) = \dim_{GF(p)} L.$$

Na osnovu leme 3.10. proizilazi:

$$C(\bar{f} \cdot GF(p)[G]) = GF(p)(\bar{e}_i),$$

pa možemo, na osnovu (1), smatrati da je $L = GF(p)(\bar{e}_i) \quad (i = 1, 2, \ldots, k)$. Dakle,

$$L = GF(p)(\varphi(e_i)) = \varphi(\mathrm{Int}Q(e_i)) = \varphi(\mathrm{Int}F_i) \quad (i = 1, 2, \ldots, k),$$

što zaključujemo na osnovu leme **3.13.**. Sada je jasno da jednom prostom sumandu algebre $GF(p)[G]$ za kojeg vezujemo polje L odgovara $k = \dim_{GF(p)} L$ prostih sumanada u razlaganju prstena $Q[G]$, kojima odgovaraju F_i $(i = 1, 2, \ldots, k)$. Na kraju opisujemo način kako na osnovu informacija vezanih za algebru $Q[G]$ određujemo $GF(p)[G]$. Neka je:

$$Q[G] = p_1 B_1 \oplus \ldots \oplus p_m B_m$$

razlaganje prstena $Q[G]$ na proste sumande, pri čemu su isti grupisani. Neka je:

$$F_i = C(B_i), \quad L_i = \varphi(\mathrm{Int}F_i), \quad l_i = \sqrt{\dim_{F_i} B_i}, \quad k_i = \dim_{GF(p)} L_i$$

$$(i = 1, 2, \ldots, m).$$

Prema prethodnoj analizi proizilazi da je:

$$GF(p)[G] \cong \frac{p_1}{k_1} M_{l_1}(L_1) \oplus \ldots \oplus \frac{p_m}{k_m} M_{l_m}(L_m),$$

na osnovu čega zaključujemo da je $GF(p)[G]$ jednoznačno određena informacijama koje su vezane u algebri $Q[G]$, te je time teoreme dokazana.

□

Prije nego što se usresredimo na centralnu teoremu koja rješava problem izomorfizma grupovnih algebri, u odnosu na neke klase p-grupa i polja karakteristike različite od p, mora se uzeti u obzir važan Higmanov rezultat dat u sljedećoj lemi.

Lema 3.15. [13] *Neka je p prost, a n prirodan broj. Postoji najmanje $p^{\frac{1}{27}(2n^3-25n^2)}$ p-grupa reda p^n, klase nilpotencije $\leqslant 2$ i perioda koji dijeli p^2.*

□

Neka je data K-algebra R, a V prosti R-modul sa odgovarajućom reprezentacijom:

$$\rho : R \to End(V).$$

Ukoliko definišemo $D := End(_R V)$, onda je jasno da je D tijelo, s obzirom na to da je V prost. U skladu sa prethodnim može se uvesti Šurov indeks, $m(V) = m(\rho)$ na sljedeći način:

$$m(V) = m(\rho) := \sqrt{\dim_{C(D)} D}.$$

Uvedeni pojmovi se vezuju za naredna tvrđenja.

Lema 3.16. [14] *Neka je G konačna nilpotentna grupa, K polje, a V prosti $K[G]$-modul sa odgovarajućom reperzentacijom $\rho : K[G] \to End(V)$. Tada je $m(\rho) = m(V) \leqslant 2$. Ukoliko je $m(V) = 2$, a $D = End(_{K[G]}V)$, tada je Silovljeva 2-podgrupa grupe G nekomutativna, a D je algebra kvaterniona nad poljem $F = C(D)$.*

□

Sada smo prikupili dovoljno rezultata na osnovu kojih dokazujemo najavljenu teoremu, čiji sadržaj govori da ima veoma mnogo p-grupa, a jako malo grupovnih algebri nad tim grupama. Ovom teoremom se pored odgovora na problem izomorfizma koji nam jeste primarni motiv, uspostavljaju i neke kvantifikacijske ocjene.

Teorema 3.17. [12] *Postoji skup od*

$$p^{\frac{2}{27}(n^3-23n^2)}$$

neizomorfnih p-grupa reda p^n koje imaju izomorfne grupovne algebre nad svim poljima čija je karakteristika različita od p.

Dokaz. Neka je G p-grupa čiji je period $\leqslant p^2$ i red p^n. Neka je $S = fQ[G]$ prosti direktni sumand algebre $Q[G]$. Pretpostavimo $f \leftrightarrow e^{\Theta}$ bijektivnu vezu datu u lemi **3.2.**, gdje je Θ grupa automorfizama Galoaovog raširenja $\widetilde{Q}/Q$. Neka je χ karakter koji odgovara elementu e, tj. prostom modulu $eQ[G]$. Prsten S ima prema lemi **1.7.** do na izmorfizam prost lijevi ideal E, pa je na osnovu teorema **1.8.** i **1.9.** $S \cong M_r(L)$, gdje je $L = End(_SE)$. Po lemi **3.10.** slijedi $C(S) = Q(\chi)$. Pošto je svaka konačna p-grupa nilpotentna, to možemo prethodnu lemu primijeniti na $Q[G]$-modul E i grupu G.

Ukoliko je $p > 2$, onda je prema lemi **3.16.** sigurno $m(E) \neq 2$, ($m(E) = \sqrt{\dim_{C(D)} D}$), jer bi u suprotnom postojala Silovljeva 2-podgrupa grupe G što je nemoguće. Dakle, $m(E) = 1$. Kako je $D = End_{Q[G]}E$ tijelo, to je zbog prethodnog $D = C(D)$, pa je D polje. Lako se zaključuje da je $S-$endomorfizam ideala E ujedno $Q[G]-$endomorfizam ideala E i obrnuto, pa se zaključuje da je $D = L$, odakle proizilazi da je i L polje. Dalje imamo:

$$C(S) \cong C(M_r(L)) \cong C(L),$$

a pošto je L polje proizilazi $C(M_r(L)) \cong L$, odnosno $C(S) \cong L$. Na osnovu leme **3.10.** slijedi $C(S) = Q(\chi)$, što zapravo znači:

$$L = C(fQ[G]) = Q(\chi).$$

Pošto je:

$$r^2 = \dim_L M_r(L) = \dim_{C(fQ[G])} fQ[G] = \dim_{\widetilde{Q}} e\widetilde{Q}[G] = \chi(1)^2,$$

to je $r = \chi(1)$. Prema lemi **3.6.** $r = \chi(1)$ dijeli $|G|$, pa je r potencija prostog broja p. U slučaju $p = 2$, iz leme **3.16.** slijedi da je L polje, ili je L algebra kvaterniona nad poljem $C(L) = Q(\chi)$. U slučaju da je L polje vrijedi prethodna analiza, a ako je algebra kvaterniona onda je:

$$(2r)^2 = \dim_{C(L)} M_r(L) = \dim_{C(L)} S = \dim_{\widetilde{Q}} e\widetilde{Q}[G] = \chi(1)^2,$$

pa je r potencija $p = 2$.

Razmotrimo sada polje $Q(\chi)$. Kako G ima period p^2, to lema **3.3.** sugeriše:

$$Q(\chi) \subseteq Q[\varepsilon_2] \quad (1),$$

gdje je ε_2 primitivni p^2-ti korijen jedinice. Pokušajmo dokazati i obrnuto.

Neka je ϑ reprezentacija $\widetilde{Q}[G]$ asocirana sa χ tj. $\vartheta : \widetilde{Q}[G] \to End_{\widetilde{Q}} e\widetilde{Q}[G]$, a neka su: $s_1, s_2, \ldots, s_k$ elementi baze modula $e\widetilde{Q}[G]$ poljem $\widetilde{Q}$.

Razmotrimo posebno slučajeve $\vartheta(G) = \{id\}$ i $\vartheta(G) \neq \{id\}$.

Ukoliko je $\vartheta(G) = \{id\}$, to znači da:

$$x \cdot s_i = s_i, \quad (\forall x \in G),$$

$$(i = 1, 2, \ldots, k),$$

pa proističe da s_i mora biti oblika:

$$q_i(x_1 + x_2 + \ldots + x_n), \quad (q_i \in \widetilde{Q},\ x_j \in G).$$

To znači da je baza $e\widetilde{Q}[G]$ u stvari jednoelementna. Pošto je $e \in e\widetilde{Q}[G]$ imamo:

$$e = q \cdot (x_1 + x_2 + \ldots + x_n),$$

a iz činjenice da je e idempotent zaključujemo $q = \dfrac{1}{n}$. Sada je očigledno da za $\forall \sigma \in \Theta$ vrijedi $\sigma e = e$, jer σ ostavlja fiksnim $Q[G]$. To znači da je $e^{\Theta} = e$, odnosno $e = f$. Lako se pokazuje da je u ovom slučaju $fQ[G] = fQ \cong Q$, odnosno $fQ[G] \cong Q$. Primijetimo da je takođe $C(fQ[G]) \cong Q$, tj.

$$Q(\chi) = Q \quad (2)$$

U slučaju da je $\vartheta(G) \neq \{id\}$ tada je $\vartheta(G)$ p-grupa koja ima netrivijalni centar što proizilazi iz tvrđenja da netrivijalna p-grupa ima netrivijalan centar. Na osnovu

Košijeve teoreme, postoji $g \in G$ tako da je $\vartheta(g)$ centralan u $\vartheta(G)$ i ima red p. U stvari $\vartheta(g)$ je centralan u $\vartheta(\widetilde{Q}[G]) = M_d(\widetilde{Q})$, gdje je $d = \chi(1)$, iz čega slijedi da $\vartheta(g)$ mora biti skalarna matrica $\varepsilon_1 E$, pri čemu je ε_1 primitivni p-ti korijen jedinice. Time je $\chi(g) = d\varepsilon_1$ i $\varepsilon_1 \in Q(\chi) \subseteq \widetilde{Q}$. Dakle imamo:

$$Q[\varepsilon_1] \subseteq Q(\chi) \quad (3)$$

Iz (1) i (3) proizilazi:

$$Q[\varepsilon_1] \subseteq Q(\chi) \subseteq Q[\varepsilon_2]$$

Jasno je $Q[\varepsilon_1] : Q = p - 1$. Minimalni polinom koji anulira ε_2 nad poljem $Q[\varepsilon_1]$ je $x^p - \varepsilon_1$, pa slijedi $Q[\varepsilon_1] : Q[\varepsilon_2] = p$, iz čega proizilazi da među $Q[\varepsilon_1]$ i $Q[\varepsilon_2]$ nema polja. Očigledno je:

$$Q(\chi) = Q[\varepsilon_1] \text{ ili } Q(\chi) = Q[\varepsilon_2] \quad (4),$$

odnosno:

$$\dim_Q Q(\chi) = p - 1 \text{ ili } \dim_Q Q(\chi) = p(p-1).$$

Ukoliko je $p = 2$ vidimo $Q(\chi) = Q$ ili $Q(\chi) = Q[\sqrt{-1}]$. Pošto je u ovom slučaju centar algebre kvaterniona $C(L) = Q(\chi)$, a $\sqrt{-1} \notin C(L)$, to odbacujemo drugu mogućnost. Na osnovu prethodnog i rezultata (2) zaključujemo da je jedina algebra kvaterniona koja se može pojaviti samo ona koja ima polje racionalnih brojeva kao svoj centar. Sada počinjemo računati broj mogućih algebri $Q[G]$ za grupe $|G| = p^n$ i perioda $\leqslant p^2$. Neka je $p > 2$. Ovo je slučaj kad nemamo algebru kvateriona i kad je $L = Q(\chi)$. Podsjetimo se da je svaki prosti sumand $S \cong M_r(L)$, gdje je r oblika p^i. Analiza koja je dovela do zaključka (2) govori da postoji tačno jedan prosti sumand koji je izomorfan Q, tj. $S \cong Q$. U ostalima slučajevima, kao što je pokazano rezultatom (4)

$$L = Q[\varepsilon_1] \text{ ili } L = Q[\varepsilon_2].$$

Dakle, imamo:

$$Q[G] = Q \dot{+} \sum_i (a_i M_{p^i}(Q[\varepsilon_1]) + b_i M_{p^i}(Q[\varepsilon_2]))$$

Pošto je $|G| = p^n$ proizilazi:

$$p^n = \dim_Q Q[G] = 1 + \sum_i (p-1)(a_i + pb_i)p^{2i} \quad (5)$$

Nesumnjivo, a_i i b_i u potpunosti determinišu $Q[G]$. Iz (5) je jasno:

$$0 \leqslant a_i \leqslant \frac{p^n - 1}{(p-1)p^{2i}} \leqslant p^{n-2i} - 1,$$

$$0 \leqslant b_i \leqslant \frac{p^n - 1}{(p-1)p^{2i+1}} \leqslant p^{n-2i-1} - 1,$$

pa je broj mogućih grupovnih algebri $Q[G]$ jednak:

$$\prod_i p^{n-2i} \cdot p^{n-2i-1} = \prod_{j=0}^{n} p^j = p^{\frac{n(n+1)}{2}} \quad (6).$$

Neka je sada $p = 2$. Direktni sumandi $Q[G]$ su oblika:
$M_{2^i}(Q)$, a_i puta,
$M_{2^i}(Q[\sqrt{-1}])$, b_i, puta
$M_{2^i}(D)$, c_i puta,
gdje je D algebra kvanteriniona nad poljem racionalnih brojeva. Stoga je

$$2^n = \sum_i a_i 2^{2i} + \sum_i b_i 2^{2i+1} + \sum_i c_i 2^{2i+2}.$$

Kao i u prethodnom slučaju jedan direktan sumand je upravo Q, te slijedi $a_0 > 0$, tj.
$1 \leqslant a_0 \leqslant 2^n$,
$0 \leqslant a_i \leqslant 2^{n-2i} - 1, \quad (i > 0)$
$0 \leqslant b_i \leqslant 2^{n-2i-1}$,
$0 \leqslant c_i \leqslant 2^{n-2i-2} - 1$.
Dakle, imamo najviše:

$$\{\prod_i 2^{n-2i}\}\{\prod_i 2^{n-2i-1}\}\{\prod_i 2^{n-2i-2}\} \leqslant 2^{\frac{n(n+1)}{2}} \quad (7).$$

grupovnih algebri ovog tipa. Očigledno je da čitava teorema ima netrivijalan sadržaj za veće vrijednosti broja n. Stoga možemo smatrati da je $n \geqslant 6$ i u ovom slučaju vrijedi:

$$\frac{n(n+1)}{2} < 1 + \frac{3n^2}{4} \leqslant \frac{21n^2}{27} \quad (8).$$

Prema lemi **3.15.** znamo da ima najmanje $p^{\frac{1}{27}(2n^3-25n^2)}$ grupa reda p^n i perioda $\leqslant p^2$. Uzimajući u obzir (6), (7) i (8) vidimo da ima najviše $p^{\frac{21}{27}n^2}$ neizomorfnih grupovnih algebri čije su grupe reda p^n i perioda $\leqslant p^2$. Stoga, zaključujemo da ima najmanje:

$$p^{\frac{1}{27}(2n^3-25n^2)}/p^{\frac{21}{27}n^2} = p^{\frac{2}{27}(n^3-23n^2)}$$

neizomorfnih p-grupa reda p^n čiji je period $\leq p^2$ i klasa nilpotencije ≤ 2, koje imaju istu grupovnu algebru $Q[G]$. Konačno, na osnovu teoreme **3.14.** proizilazi da su grupovne algebre ovih grupa takođe izomorfne za sva polja koeficijenata K kod kojih je $char K \neq p$.

□

REFERENCE

[1] Connell, I.G. **On the group ring**, Can.J.Math. 15 (1963), 650-685.

[2] Renault, G. **Sur les anneaux de groupes**, C.R.Acad.Sci.Paris 273 (1971), 84-87.

[3] Kaš, F. **Moduli i prsteni**, Mir, Moskva (1981)

[4] Passman, Donald S. **The Algebraic structure of group rings**. A Wiley-Interscience publication (1977)

[5] Brauer, R. **Zur Darstellungstheorie der Gruppen endlicher Ordnung**, Math.Z. 63 (1956), 406-444.

[6] Perlis, S. Walker, G. **Abelian group algebras of finite order**, Trans.AMS 68 (1950), 420-426.

[7] Bovdi, A.A. **Group rings of torsion free groups**, Sibirsk.Mat.Zh. 1 (1960), 555-558.

[8] Berman, D. **Group algebras of countable abelian p-groups**, Soviet Math.Dokl. 8 (1967), 871-873.

[9] May, W. **Commutative group algebras**, Trans. AMS 136 (1969), 139-149.

[10] Leng, S. **Algebra**, Mir, Moskva (1968)

[11] Perić, Veselin **Algebra II, Opšte algebarske strukture; Teorija polja; Algebarske jednačine**, Sarajevo (1989)

[12] Passman, Donald S. **Isomorphic groups and group rings**, Pac.J.Mathematics 15 (1965), 561-583.

[13] Higman, G. **Enumerating p-groups I: inequalities**, Proc.Lond.Math.Soc. (3) 10 (1960), 24-30.

[14] Roquette, P. **Realisierung von Darstellungen endlicher nilpotenter Gruppen**, Archiv.Math. 9 (1958), 241-250.

[15] Scot, Leonard L. **Recent progress on the Isomorphism Problem**, Proceedings of Symposia in Pure Mathematics, Vol. 47, (1987)

[16] Atiyah, M.F. Macdonald, I.G. **Introducion to commutative algebra.** (1969)

[17] Deskins, W.E. **Finite abelian groups with isomorphic group algebras**. Duke Math J. 23 (1956), 35-40.

[18] Sandling, R. **The modular group algebra problem for metacyclic p-groups**. Proc. A.M.S, 124 (1996), N.5, 1347-1350.

[19] Passman, Donald S. **The group algebra of groups of order p^4 over a modular field**. Michigan Math. Journal 12 (1965), 405-415.

[20] Wursthorn, M. **Isomorphism of modular group algebras: an algorithm and its application to groups of order 2^6**. J.Symbolic Comput. 15 (1993), no 2, 211-227.

[21] Bleher F.M., Kimmerle W., Roggenkamp K.W., Wursthorn M. **Computional aspects of the isomorphism problem. Algorithmic algebra and number theory (Heidelberg, 1997),** Springer, Berlin, 1999, 313-329.