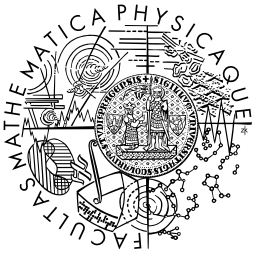

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

DIPLOMOVÁ PRÁCE

Bc. Zuzana Procházková

Význačné prvky grupových okruhů

Katedra algebry

Vedoucí diplomové práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D.

Studijní program: Matematika

Studijní obor: Matematické struktury

Praha 2021

Prohlašuji, že jsem tuto diplomovou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Chtěla bych poděkovat panu docentovi Žemličkovi za jeho odborné vedení, příjemnou spolupráci a pomoc. Dále Mariánovi Popprovi za jeho vtípky a nekonečný optimismus. Poděkování si zaslouží i moji přátelé, bez nich by byl svět šedivý. Pak bych chtěla poděkovat celé mojí rodině za jejich podporu a za to, že pro mě jsou bezednou studnicí inspirace. Také chci poděkovat učitelce matematiky RNDr. Lucii Růžičkové, která mě od fyziky přetáhla k matematice. Následně děkuji Výboru dobré vůle, který při mě stál celé moje studium již od střední školy. Také děkuji Jiřímu Suchému, jehož písničky jsou oázou životního nadšení. A nakonec děkuji sama sobě, že jsem to se sebou vydržela.

Název práce: Význačné prvky grupových okruhů

Autor: Bc. Zuzana Procházková

Katedra: Katedra algebry

Vedoucí diplomové práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Katedra algebry

Abstrakt: Tato diplomová práce se zabývá hledáním idempotentů v grupových okruzích. Jsou v ní popsány tři postupy hledání idempotentů v totálně rozložitelném grupovém okruhu a poslední kapitola popisuje pokusy o hledání idempotentů v grupovém okruhu, který nemusí být totálně rozložitelný. První postup využívá reprezentaci a charaktery grupy. Druhý postup hledá idempotenty pomocí Shodových párů grupy. Třetí postup zvedá idempotenty z faktorokruhu pomocí CNC systémů ideálů, který zobecňuje dlouho známé zvedání idempotentů pomocí nilpotentního ideálu, a je zde rozšířen na grupové okruhy, které tvoří nekomutativní grupa a nekomutativní okruh.

Klíčová slova: grupové okruhy, augmentační zobrazení, Maschkeho věta, Weddernburn - Artinova věta, totálně rozložitelný okruh, idempotenty, reprezentace a charakter grupy, Galoisova grupa, Shodovy páry, nilpotentní ideál, CNC systém ideálů, Cliffordova věta

Title: Distinguished elements of group rings

Author: Bc. Zuzana Procházková

Department: Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: This thesis is about finding idempotents in a group ring. We describe three techniques of finding idempotents in a semisimple group ring and in the last chapter there is an attempt to find idempotents in a group ring that does not have to be semisimple. The first technique uses representations and characters of a group. The second technique finds idempotents through the use of Shoda pairs. The third technique lifts idempotent from the factor ring with the help of CNC system of ideals, which is a generalization of a well-known technique with nilpotent ideals, and it is here extended to group rings formed by non-abelian group and noncommutative ring.

Keywords: group rings, augmentation map, Maschke's theorem, Weddernburn-Artin theorem, semisimple ring, idempotent, representation and character of a group, Galois group, Shoda pair, nilpotent ideal, CNC system of ideals, Clifford's theorem

Obsah

Úvod

Grupové okruhy jsou elegantní kombinací dvou známých struktur: grup a okruhů. Studenti Matematických struktur se většinou setkají s grupovými okruhy skrze teorii reprezentací grup, což by mohlo vést k domněnce, že grupové okruhy se začaly studovat kvůli teorii reprezentací grup. Tak to mu ale není, grupové okruhy byly studovány jako samostatný objekt a jejich studium přispělo k rozšíření teorie reprezentací grup, tyto dva obory se navzájem ovlivňovaly. Vznik grupových okruhů vyšel ze studia komplexních čísel. Při studiu komplexních čísel si matematik William Rowan Hamilton v roce 1837 všiml, že součet $1 + 3i$ není součtem v klasickém slova smyslu jako například $1 + 3$ a že je vhodnější se na něj podívat jako na uspořádanou dvojici. To vedlo k objevení kvaternionů a později k hyperkomplexním systémům, které se už svojí definicí moc od grupových okruhů neliší, nicméně ještě nebyla formální, protože koncept abstraktních grup nebyl formulovaný. Jako první práce o abstraktních grupách se většinou uvádí Cayleyho práce z roku 1854, kde je také první konstrukce grupového okruhu. Formálně je grupový okruh uveden T. Molienem v roce 1897. Asi nejvlivnější článek, často uváděný jako první článek v tomto oboru, byl článek Emmy Noetherové z roku 1929, kde autorka definuje hyperkomplexní systém a uvádí jako jeden z příkladů grupový okruh a ukazuje propojení s reprezentací grup.

Již předtím v roce 1898 Maschke formuloval větu o totální rozložitelnosti, která je základním kamenem teorie hledání idempotentních prvků, jež je v této práci popsána. Z ní víme, kdy je grupový okruh totálně rozložitelný a můžeme na něj, jelikož grupový okruh je také modulem, použít Artin-Weddernburnovu větu. Díky tomu a teorii reprezentací grup jsme schopni zjistit, kolik primitivních centrálních idempotentů nám stačí najít, abychom mohli grupový okruh rozložit na jednoduché moduly.

Pomocí tohoto rozkladu se může zjednodušit hledání invertibilních prvků grupového okruhu, jelikož pro $\{f_1, f_2, \ldots, f_n\}$ kompletní množina ortogonálních primitivních centrálních idempotentů grupového okruhu RG máme rozklad

$$RG \simeq \bigoplus_{j=1}^{n} Rf_j$$

a pokud i_j je invertibilní prvek v Rf_j pro každé $j = 1, \ldots, n$, pak $\bigoplus_{j=1}^{n} i_j$ je invertibilní prvek v RG. Tedy hledání idempotentních prvků je úzce spojené s hledáním invertibilních prvků. Ukazuje se, že oba druhy prvků lze využít při kódování, jak lze třeba najít v Pless et al. [1998] a Guerreiro [2016].

V první kapitole této práce jsou zavedeny základní definice a tvrzení o grupovém okruhu, je dokázána Maschkeho věta a popsáno, jak souvisí rozklad grupového okruhu s idempotenty. V celé práci se využívá Maschkeho věta a předpokládá se, pokud není řečeno jinak, že grupový okruh je totálně rozložitelný. Druhá kapitola shrnuje dlouho známý postup hledání idempotentů pomocí teorie reprezentací grup, je dokázáno, jak najít pomocí charakterů grupy G idempotenty v KG, pro K (algebraicky uzavřené) těleso. V třetí, nejdelší, kapitole popíšeme modernější způsob hledání idempotentů pomocí Shodových párů. V první sekci třetí kapitoly je popsána teorie a postup na hledání idempotentů v grupovém

okruhu $\mathbb{Q}G$ pomocí Shodových párů, v druhé sekci je tento postup zobecněný pro grupový okruh $\mathbb{F}G$, kde $\mathbb{F}$ je konečné těleso. Čtvrtá kapitola obsahuje postup, pro hledání idempotentů pomocí zvedání z faktorokruhu. Je popsán postup hledání idempotentů pomocí CNC-systému ideálů v grupovém okruhu RG, kde G nemusí být komutativní grupa a R je komutativní okruh. V závěru této kapitoly je uvedeno pozorování, kterým se dají spočítat idempotenty pomocí faktorokruhů v grupovém okruhu RG, kde G ani R nemusí být komutativní. V páté kapitole je pokus o hledání idempotentů v obecném grupovém okruhu, který nemusí být totálně rozložitelný. Je popsán postup pro jeden typ grupového okruhu a proč tento postup nelze určitým způsobem zobecnit.

1. Základní definice

Tato kapitola obsahuje základní definice a věty potřebné pro práci s grupovými okruhy a hledání jejich idempotentů. Nejdříve je definován grupový okruh a některé jeho charakteristiky. Tvrzení 3 a Tvrzení 4 jsou potřebná k důkazu Maschkeho věty, Maschkeho věta je zde Větou 5 a říká, kdy je grupový okruh totálně rozložitelný. Poté je popsáno centrum grupového okruhu. Nakonec jsou definovány idempotentní a invertibilní prvky a pomocí Tvrzení 11, Tvrzení 12 a Věty 14 je popsána souvislost (centrálních) idempotentů s rozkladem totálně rozložitelného okruhu. Uvedené věty, definice a důkazy lze najít v Milies César Polcino a Sehgal [2002].

Definice 1. *(Grupový okruh jako formální součet) Nechť R je okruh a G je grupa. Pak* grupový okruh *RG je tvořen konečnými formálními součty tvaru*

$$\sum_{g\in G} r_g g, \quad g \in G, r_g \in R,$$

s operacemi sčítání a násobení definovanými následovně:

$$\sum_{g\in G} r_g g + \sum_{g\in G} s_g g = \sum_{g\in G}(r_g + s_g)g;$$
$$\sum_{g\in G} r_g g \cdot \sum_{g\in G} s_g g = \sum_{g\in G}(\sum_{hh'=g}(r_h s_{h'}))g.$$

Příklad 1. Buď K těleso a G je konečná cyklická grupa, $G = \{1_G, g, g^2, \ldots, g^{n-1}\}$. Mějme zobrazení $\phi : K[x] \to KG$, které pošle x na generátor g, r na r pro všechna $r \in R$. Pak toto zobrazení je surjektivní okruhový homomorfismus a zajímá nás, jak vypadá jeho jádro. Každý polynom p z $K[x]$ můžeme zapsat jako $p = q(x^n - 1) + r$, kde $q, m \in K[x]$ a $\deg(m) < n$. Pokud p leží v jádře ϕ, pak

$$0 = \phi(q(x^n - 1) + m) = \phi(q(x^n - 1)) + \phi(m).$$

Pokud $m \neq 0$, tak $\phi(m) \neq 0$, tedy $m = 0$. Proto p leží v ideálu $(x^n - 1)$. Jelikož $\phi(x^n - 1) = 0$, tak i ideál $(x^n - 1)$ leží v jádře ϕ. Získali jsme, že
$K[x] \big/ (x^n - 1) \simeq KG$.

Okruh R můžeme díky zobrazení $r \mapsto r1_G$ uvažovat jako podokruh RG. Podobně máme zobrazení $g \mapsto 1_R g$ a tedy G můžeme uvažovat jako monoid v RG.

Pokud navíc na RG zadefinujeme skalární násobení prvkem z okruhu R jako

$$s \cdot \sum_{g\in G} r_g g = \sum_{g\in G} s \cdot r_g g,$$

tak se na RG můžeme koukat jako na levý R-modul. Jelikož pak $RG \simeq \bigoplus_{g\in G} Rg$, tak se jedná o volný R-modul a pokud místo okruhu máme těleso K, tak získáme vektorový K-prostor.

V této práci budeme používat definici grupového okruhu pomocí formálních součtů. Hodí se zde pro zajímavost uvést ekvivalentní definici grupového okruhu. Důkaz následujícího tvrzení je technický, proto jej zde nebudeme uvádět, lze jej nalézt například v Milies César Polcino a Sehgal [2002] na začátku kapitoly 3.2.

Tvrzení 2. *(Grupový okruh jako množina zobrazení) Nechť G je grupa a R je okruh. Pak grupový okruh RG reprezentuje množinu zobrazení $G \to R$ s konečným nosičem a s operacemi sčítání, násobení a násobení skalárem definovanými pro $f, g \in RG$, $x \in G$ a $r \in R$:*

$$\begin{aligned}(f+g)(x) &= f(x) + g(x);\\ (f \cdot g)(x) &= \sum_{yy'=x} f(y) \cdot g(y');\\ (r \cdot f)(x) &= r \cdot f(x).\end{aligned}$$

Definice 2. *(Augmentační zobrazení a augmentační ideál) Okruhový homomorfismus $\varepsilon : RG \to R$ daný*

$$\varepsilon(\sum_{g\in G} r_g g) = \sum_{g\in G} r_g$$

nazveme augmentačním zobrazením. *Jeho jádro označíme jako Δ a nazýváme ho* augmentačním ideálem.

Jelikož ε je homomorfismus na ($R \leq RG$), tak platí, že $RG/\Delta \simeq R$.
Pokud prvek $\sum_{g\in G} r_g g$ leží v Δ, pak $\varepsilon(\sum_{g\in G} r_g g) = \sum_{g\in G} r_g = 0$, proto

$$\sum_{g\in G} r_g g = \sum_{g\in G} r_g g - \sum_{g\in G} r_g = \sum_{g\in G} r_g(g-1).$$

Jelikož zjevně všechny prvky tvaru $g-1$, $g \in G$, leží v Δ, tak vidíme, že Δ je ideál v RG generovaný množinou $\{g-1; g \in G\}$.

Definice 3. *(Norma a stopa) Nechť $r = \sum_{g\in G} r_g g \in RG$, pak* normu *prvku r definujeme jako $\delta(r) = \sum_{g\in G} r_g$ a* stopa *prvku r je $tr(r) = r_{1_G}$.*

Tedy augmentační zobrazení je zobrazení, které prvku r z RG přiřazuje jeho normu.

Definice 4. *(Nosič) Nechť $r = \sum_{g\in G} r_g g \in RG$, pak* nosič *prvku r definujeme jako* $\mathrm{Supp}(r) = \{g : r(g) \neq 0\}$ *a grupu generovanou nosičem prvku r označíme jako* $\mathrm{S.G.}(r)$.

Definice 5. *(Anihilátor) Nechť S je okruh a X je podmnožina S. Pak* levý (pravý) anihilátor *podmnožiny X je levý (pravý) ideál $X^l = \{s \in S : sX = 0\}$ ($X^r = \{s \in S : Xs = 0\}$).*

Tvrzení 3. *Nechť RG je grupový okruh a $G = \{1_G, g_2, \ldots, g_n\}$, potom pravý a levý anihilátor augmentačního ideálu Δ splývají, označíme jej jako Δ^*, navíc $\Delta^* = R(1_G + g_2 + \cdots + g_n)$. Pokud je G nekonečná grupa, pak $\Delta^r = \Delta^l = 0$.*

Důkaz. Nechť $G = \{1_G, g_2, \ldots, g_n\}$ a $r = a_1 1_G + a_2 g_2 + \cdots + a_n g_n \in \Delta^l$. Pak

$$\begin{aligned}0 &= r \cdot (1 - g_i)\\ &= (a_1 1_G + a_2 g_2 + \cdots + a_n g_n) \cdot (1 - g_i)\\ &= a_i g_i (1 - g_i) + a_1 1_g (1 - g_i) + \ldots\\ &= a_i g_i - a_1 g_i + \ldots\end{aligned}$$

a proto $a_1 = a_i$ pro každé i. Tedy $\Delta^l \subseteq R(1_G + g_2 + \cdots + g_n)$.

Nechť naopak

$$r = a + ag_2 + \cdots + ag_n \in R(1_G + g_2 + \cdots + g_n),$$

pak

$$\begin{aligned} r \cdot (1 - g_i) &= (a + ag_2 + \cdots + ag_n) \cdot (1 - g_i) \\ &= (a + ag_2 + \cdots + ag_n) - (ag_i + ag_2g_i + \cdots + ag_ng_i) \\ &= 0, \end{aligned}$$

proto $r \in \Delta^l$ a tudíž $\Delta^l = R(1_G + g_2 + \cdots + g_n)$. Stejně by se dokázalo, že $\Delta^r = R(1_G + g_2 + \cdots + g_n)$.

Nechť G je nekonečná a pro spor $x \in \Delta^r \neq 0$. Pak $x = \sum_{g \in G} x_g g$ a

$$(1 - h) \sum_{g \in G} x_g g = 0,$$

tudíž

$$\sum_{g \in G} x_g g = \sum_{g \in G} x_g hg,$$

pro každé $h \in G$. Vezměme $g_0 \in \mathrm{Supp}(x)$. Pak $x_{g_0} \neq 0$ a rovnice výše ukazuje, že i $hg_0 \in \mathrm{Supp}(x)$ pro každé $h \in G$. Ale jelikož G je nekonečná, máme nekonečný $\mathrm{Supp}(x)$, což je spor. Obdobný důkaz funguje pro Δ^l.

□

Tvrzení 4. *Nechť RG je grupový okruh. Pak Δ je direktním sčítancem RG jako levý ideál právě tehdy, když je G konečná grupa a $|G|$ je invertibilní v R.*

Důkaz. Nechť Δ je direktním sčítancem RG. Pak existuje levý ideál J takový, že $RG = \Delta \oplus J$. Pro $x \in \Delta, y \in J$ platí, že $xy \in \Delta \cap J = (0)$, tedy $y \in \Delta^*$ a $J \subset \Delta^*$. Proto je Δ^* nenulový ideál, tudíž G je konečná grupa. Nechť $1 = e_1 + e_2$, kde $e_1 \in \Delta$ a $e_2 \in J$. Pak z Tvrzení 3 plyne, že existuje takové $a \in R$, že $1 = \varepsilon(1) = \varepsilon(e_1) + \varepsilon(e_2) = \varepsilon(e_2) = a \cdot |G|$, tedy $|G| = a^{-1}$.

Buď $G = \{g_1, g_2, \ldots, g_n\}$ konečná grupa a n je invertibilní v R. Pokud $x \in \Delta \cap \Delta^*$, tak $x = a(g_1 + \cdots + g_n)$ a zároveň $\varepsilon(x) = n \cdot a = 0$. Jelikož n je invertibilní, tak $x = 0$, tedy $\Delta \cap \Delta^* = 0$. Zároveň pro $r \in RG$ platí, že

$$\begin{aligned} r &= \sum_{g \in G} r_g g \\ &= \sum_{g \in G} r_g - \sum_{g \in G} r_g(1 - g) \\ &= na - \sum_{g \in G} r_g(1 - g) \\ &= \sum_{g \in G} a - \sum_{g \in G} r_g + \sum_{g \in G} r_g g - \sum_{g \in G} ag + \sum_{g \in G} ag \\ &= \sum_{g \in G} (a - r_g)(1 - g) + \sum_{g \in G} ag \in \Delta + \Delta^*, \end{aligned}$$

kde $\varepsilon(r) = nn^{-1}\varepsilon(r) = na$, pro $a = n^{-1}\varepsilon(r)$. Proto $RG = \Delta \oplus \Delta^*$.

□

Definice 6. *(Jednoduchý, totálně rozložitelný modul) Nechť M je (levý) modul nad okruhem R. Modul M se nazývá* jednoduchý*, pokud $M \neq 0$ a jediné jeho podmoduly jsou 0 a M. M se nazývá* totálně rozložitelný*, pokud existují jednoduché (levé) moduly M_i, $i \in I$, takové, že $M \simeq \bigoplus_{i \in I} M_i$. Okruh R je* totálně rozložitelný*, pokud je totálně rozložitelný jako (levý) modul.*

Věta 5. *(Maschkeho věta) Nechť G je grupa a R okruh. Pak grupový okruh RG je totálně rozložitelný právě tehdy, když:*

- *R je totálně rozložitelný;*
- *G je konečná;*
- *$|G|$ je invertibilní prvek v R.*

Důkaz. Nechť RG je totálně rozložitelný. Pak $RG/\Delta \simeq R$, a tedy R je také totálně rozložitelný. Jelikož RG je totálně rozložitelný, tak Δ je direktním sčítancem jako levý ideál RG a z Tvrzení 4 plyne, že G je konečná a $|G|$ je invertibilní prvek v R.

Naopak uvažujme, že platí všechny tři podmínky. Ukážeme, že každý libovolný RG-podmodul RG je direktním sčítancem RG. Nechť M je RG-podmodul RG. Jelikož R je totálně rozložitelný, tak RG je totálně rozložitelný jako R-modul. Takže existuje R-modul N takový, že

$$RG = M \oplus N.$$

Nechť $\pi : RG \to M$ je projekce z tohoto rozkladu. Pak definujeme $\pi^* : RG \to M$ jako

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \pi(gx).$$

Nyní stačí dokázat, že π^* je RG-homomorfismus, $(\pi^*)^2 = \pi^*$ a $M = \mathrm{Im}(\pi^*)$. Pak $\mathrm{Ker}(\pi^*)$ je RG-modul a $RG = M \oplus \mathrm{Ker}(\pi^*)$. Jelikož je i π^* R-homomorfismus, tak stačí dokázat

$$\pi^*(ax) = a\pi^*(x) \text{ pro každé } x, a \in G.$$

Máme

$$\begin{aligned} \pi^*(ax) &= \frac{1}{|G|} \sum_{g \in G} g^{-1} \pi(gax) \\ &= \frac{a}{|G|} \sum_{g \in G} (ga)^{-1} \pi(gax) \\ &= \frac{a}{|G|} \sum_{t \in G} t^{-1} \pi(tx) \\ &= a\pi^*(x). \end{aligned}$$

Jelikož π je projekce M, tak libovolný prvek $x \in RG$ máme, že $\pi(gx) \in M$, tudíž $\mathrm{Im}(\pi^*(x)) \subseteq M$. Též $\pi(m) = m$ pro každé $m \in M$. Jelikož M je RG-modul, tak $gm \in M$ pro každé $g \in G$. Proto

$$\begin{aligned}\pi^*(m) &= \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gm)\\ &= \frac{1}{|G|}\sum_{g\in G} g^{-1}gm\\ &= m.\end{aligned}$$

Z toho plyne, že $M \subseteq \mathrm{Im}(\pi^*(x))$ a také $(\pi^*)^2 = \pi^*$.

□

Důsledek 6. *Uvažujme grupový okruh nad tělesem K. Pokud je G konečná a charakteristika tělesa K nedělí řád G, tak pak z Maschkeho věty přímo plyne, že KG je totálně rozložitelný okruh.*

Příklad 7. Navážeme na Příklad 1. Nechť K je těleso, G je konečná cyklická grupa řádu n a navíc charakteristika tělesa K nedělí n. Pak víme, že

$$K[x] \big/ (x^n - 1) \simeq KG.$$

Nechť $x^n - 1 = f_1 f_2 \dots f_k$ je rozklad na ireducibilní polynomy v $K[x]$. Jelikož $\mathrm{char}(K)$ nedělí $|G|$, tak $x^n - 1$ nemá násobné kořeny, a proto $f_i \nmid f_j$ pro $i \neq j$. Pak máme

$$KG \simeq K[x] \big/ (x^n - 1) \simeq K[x] \big/ (f_1) \oplus K[x] \big/ (f_2) \oplus \dots \oplus K[x] \big/ (f_k).$$

Nechť ξ_i je kořen polynomu f_i, pak $K[x] \big/ (f_i) \simeq K(\xi_i)$, pro f_i, $1 \leq i \leq k$. Tím jsme získali rozklad

$$KG \simeq K(\xi_1) \oplus K(\xi_2) \oplus \dots \oplus K(\xi_k).$$

Definice 7. *(Centrum okruhu)* Centrum okruhu R *je množina prvků $x \in R$, pro které platí $rx = xr$, pro všechna $r \in R$. Budeme jej značit jako $Z(R)$. $Z(R)$ je komutativní podokruh R.*

Tvrzení 8. *Buď R okruh a G konečná grupa s konjugačními třídami $C_1, \dots, C_k$. Pak $Z(RG)$ je volný $Z(R)$-modul s bázemi $b_1, \dots, b_k$, kde $b_i = \sum_{c\in C_i} c$.*

Důkaz. Nejdříve dokážeme, že $\langle b_1, \dots, b_k\rangle_{Z(R)} \subseteq Z(RG)$. Nechť $x = \sum_{i=1}^{k} r_i b_i$, kde $r_i \in Z(R)$, a $r = \sum_{g\in G} r_g g \in RG$. Pak

$$r \cdot x = r \cdot \sum_{i=1}^{k} r_i b_i = \sum_{i=1}^{k} r_i r b_i = \sum_{i=1}^{k} r_i b_i r = x \cdot r,$$

protože

$$\begin{aligned} gb_i &= g \sum_{g_i \in C_i} g_i \\ &= \sum_{g_i \in C_i} g g_i g^{-1} g \\ &= \sum_{g_j \in C_i} g_j g \\ &= b_i g, \end{aligned}$$

a potom

$$\begin{aligned} rb_i &= (\sum_{g \in G} r_g g) b_i \\ &= \sum_{g \in G} r_g b_i g \\ &= b_i r. \end{aligned}$$

Nyní chceme $Z(RG) \subseteq \langle b_1, \ldots, b_k \rangle_{Z(R)}$. Nechť $x = \sum_{g \in G} x_g g \in Z(RG)$, pak pro každé $r \in R$ platí, že

$$\begin{aligned} (\sum_{g \in G} x_g g) r &= r (\sum_{g \in G} x_g g), \\ \sum_{g \in G} x_g r g &= \sum_{g \in G} r x_g g, \end{aligned}$$

tedy $x_g r = r x_g$ pro každé $g \in G$ a $r \in R$. Proto $x_g \in Z(R)$ pro každé $g \in G$. Dále chceme dokázat, že koeficienty u prvků každé konjugační třídy jsou stejné. Nechť $x \in Z(RG)$, $x = \sum_{g \in G} x_g g$, a pro každé $r \in RG$ platí

$$x \cdot r = r \cdot x,$$

speciálně i pro $r = h \in G$. Pak máme $h^{-1} x h = \sum_{g \in G} x_g h^{-1} g h = \sum_{g \in G} x_g g$. Proto prvky ve stejné konjugační třídě mají stejný koeficient a tedy $x \in \langle b_1, \ldots, b_k \rangle_{Z(R)}$. □

Důsledek 9. *Nechť RG je grupový okruh, kde R je komutativní okruh, G je konečná grupa a G má konjugační třídy $C_1, \ldots, C_k$. Pak centrum $Z(RG)$ je jako modul nad R generovaný množinou $\{b_1, \ldots, b_k\}$, kde $b_i = \sum_{g \in C_i} g$.*

Definice 8. *(Idempotentní, invertibilní prvek) Nechť R je okruh.* Idempotentní prvek $r \in R$ *je takový prvek, pro který platí $r^2 = r$. Prvek $u \in R$ je* invertibilní, *pokud existuje prvek $v \in R$ takový, že $uv = vu = 1_R$.*

Příklad 10. Nechť G obsahuje konečnou podgrupu H, R je okruh a $|H|$ je invertibilní v R. Pak

$$r = \frac{1}{|H|} \sum_{h \in H} h$$

je idempotentní prvek okruhu RG. Vskutku

$$\begin{aligned}\frac{1}{|H|}\sum_{h\in H} h \cdot \frac{1}{|H|}\sum_{h\in H} h &= \frac{1}{(|H|)^2}(\sum_{h\in H} h)\cdot(\sum_{h\in H} h)\\ &= \frac{|H|}{(|H|)^2}(\sum_{h\in H} h)\\ &= \frac{1}{|H|}(\sum_{h\in H} h),\end{aligned}$$

kde předposlední rovnost plyne z toho, že $hH = H$ pro každé $h \in H$. Tento idempotent označíme jako $\widehat{H}$. Prvek $\widehat{H}$ je centrální idempotent právě tehdy, když $H \trianglelefteq G$. Pro $g \in G$ značíme $\widehat{\langle g\rangle}$ zkráceně jako $\widehat{g}$.

Následující tvrzení jsou známá, důkazy by nebylo zde zajímavé uvádět, lze je nalézt například v [Milies César Polcino a Sehgal, 2002].

Tvrzení 11. *Nechť R je okruh. Pak R je totálně rozložitelný právě tehdy, když každý jeho levý ideál L je tvaru $L = Re$, kde $e \in R$ je idempotent.*

Tvrzení 12. *Nechť $R = \bigoplus_{i=1}^{n} L_i$ je rozklad totálně rozložitelného okruhu R na direktní součet minimálních levých (oboustranných) ideálů. Pak existuje množina $\{e_1, e_2, \ldots, e_n\}$ prvků z R, pro kterou platí:*

(i) $e_i \neq 0$ *je (centrální) idempotent pro každé i;*

(ii) pokud $i \neq j$, pak $e_i e_j = 0$;

(iii) $1 = e_1 + \cdots + e_n$;

(iv) e_i *nelze zapsat jako $e_i = e_i' + e_i''$, kde e_i' a e_i'' splňují podmínky (i) a (ii).*

A naopak, pokud existuje množina $\{e_1, e_2, \ldots, e_n\}$ prvků z R, která splňuje podmínky (i)-(iv), pak levé (oboustranné) ideály $L_i = Re_i$ jsou minimální a $R = \bigoplus_{i=1}^{n} L_i$.

(Centrální) idempotenty splňující podmínku (ii) nazýváme (centrální) *ortogonální* a pokud splňují podmínku (iv), tak jsou (centrální) *primitivní*. Množinu $\{e_1, \ldots, e_n\}$ splňující všechny podmínky (i)-(iv) nazveme *kompletní množinou ortogonálních primitivních (centrálních) idempotentů*.

Příklad 13. Nechť G je cyklická grupa řádu 7 generovaná prvkem a a $K = \mathbb{Q}$. Prvek $e_1 = \frac{1}{7}(1 + a + \cdots + a^6)$ je primitivní idempotent a stejně tak $e_2 = 1 - e_1$. Pak množina $\{e_1, e_2\}$ splňuje vlastnosti z Tvrzení 6 a tedy máme rozklad

$$\mathbb{Q}G \simeq \mathbb{Q}Ge_1 \oplus \mathbb{Q}Ge_2.$$

Zároveň ale také máme

$$\mathbb{Q}G \simeq \mathbb{Q}[x] \big/ (x^7 - 1).$$

V $\mathbb{Q}$ můžeme rozložit polynom na ireducibilní polynomy

$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

Pokud ξ značí kořen polynomu $(x^6+x^5+x^4+x^3+x^2+x+1)$, tak máme rozklad

$$\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q}(\xi).$$

Jak spolu tyto dva rozklady souvisí? Z jednoznačnosti rozkladu víme, že $\mathbb{Q} \simeq \mathbb{Q}Ge_1$, nebo $\mathbb{Q} \simeq \mathbb{Q}Ge_2$. Jelikož $e_1 = \frac{1}{7}(1 + a + \cdots + a^6) \in \Delta^*$, tak $\mathbb{Q}Ge_1 \simeq \Delta^* \simeq \mathbb{Q}$. Z toho plyne, že $\mathbb{Q}Ge_2 \simeq \mathbb{Q}(\xi)$.

Věta 14. *(Wedderburn-Artin) Okruh R je totálně rozložitelný právě tehdy, když existuje $k \in \mathbb{N}_0, n_1, n_2, \ldots, n_k \in \mathbb{N}$ a (obecně nekomutativní) tělesa $D_1, D_2, \ldots, D_k$ tak, že*

$$R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k).$$

Pokud R je konečně dimenzionální algebra nad algebraicky uzavřeným tělesem K, tak pak za $D_1, \ldots, D_k$ můžeme volit K.

Důkaz. Načrtneme pouze důkaz jedné implikace pro spojení této věty s idempotenty. Nechť

$$R = L_{11} \oplus \cdots \oplus L_{1r_1} \oplus L_{21} \oplus \cdots \oplus L_{2r_2} \oplus \cdots \oplus L_{s1} \oplus \cdots \oplus L_{sr_s}$$

je rozklad na direktní součet minimálních levých ideálů, poskládaný tak, že jednotlivé skupiny tvoří izomorfní levé ideály. Každý minimální levý ideál je generován primitivním idempotentem. Definujme jednoduchou komponentu jako $A_i = \bigoplus_{j=1}^{r_i} L_{ij}$. Pak $R = \bigoplus_{j=1}^{s} A_j$ je rozklad R na direktní součet oboustranných ideálů a platí, že $A_i \simeq M_n(D_i)$, pro určité (nekomutativní) těleso D_i. Každá jednoduchá komponenta je generována primitivním centrálním idempotentem.

□

Důsledek 15. *Nechť K je algebraicky uzavřené těleso, G je konečná grupa taková, že KG je totálně rozložitelný okruh. Pak*

$$KG \simeq M_{n_1}(K) \times M_{n_2}(K) \times \cdots \times M_{n_k}(K),$$

pro nějaká $k \in \mathbb{N}_0$, $n_1, \ldots, n_k \in \mathbb{N}$, kde $M_{n_i}(K)$ je algebra matic $n_i \times n_i$ nad tělesem K.

Důsledek 16. *Nechť R je konečný okruh, G je konečná grupa taková, že RG je totálně rozložitelný okruh. Pak*

$$KG \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k),$$

pro nějaká $k \in \mathbb{N}_0$, $n_1, \ldots, n_k \in \mathbb{N}$, kde $D_1, \ldots, D_k$ jsou konečná, tedy komutativní, tělesa, která jsou rozšířením okruhu R.

Důsledek 17. *Nechť R je konečný a totálně rozložitelný okruh, pak*

$$R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k),$$

kde $D_1, \ldots, D_k$ jsou konečná komutativní tělesa.

2. Idempotenty pomocí charakterů

V této kapitole je popsán postup, jak najít idempotenty grupového okruhu KG pro (algebraicky uzavřené) těleso K a grupu G pomocí charakterů grupy. Nejdříve jsou sepsané základní definice a vlastnosti reprezentace grupy a charakterů, Tvrzení 19, 20, 21, 22 jsou bez důkazů, jelikož patří do základů teorie reprezentací, důkazy lze najít v Milies César Polcino a Sehgal [2002]. Věta 23 ukazuje, jak můžeme najít primitivní centrální idempotenty KG pro K algebraicky uzavřené, důkaz je přepsán do našeho značení, v jiném značení jej lze najít v páté kapitole v Milies César Polcino a Sehgal [2002]. Tvrzení 24 a 25 jsou jednoduchá pozorování o idempotentech v libovolném okruhu, která se použijí dále v textu. Nakonec Věta 26 obsahuje postup, jak najít pomocí charakterů grupy G primitivní centrální idempotenty v KG, kde K nemusí být algebraicky uzavřené těleso, důkaz je podrobněji rozepsaný důkaz z první kapitoly v Yamada [1974].

V této kapitole bude K značit obecné těleso, které nemusí být nutně algebraicky uzavřené.

Definice 9. *(Reprezentace grupy a charaktery) Nechť G je grupa, K je těleso a V je konečně dimenzionální vektorový prostor nad K. Pak* reprezentace grupy G nad tělesem K *je homomorfismus*

$$\varphi : G \to \mathrm{Aut}_K(V),$$

kde $\mathrm{Aut}_K(V)$ *je grupa (okruh) automorfismů. Tedy musí platit, že*

$$\varphi(g_1 g_1) = \varphi(g_1)\varphi(g_2),$$

pro všechna $g_1, g_2 \in G$.

Stupněm reprezentace *nazýváme* $\deg_K(V)$. *Stopa zobrazení* $\psi \in \mathrm{Aut}_K(V)$ *je stopa matice automorfismu* ψ *vůči nějaké bázi* B *prostoru* V*:*

$$\mathrm{Tr}(\psi) := \mathrm{Tr}([\psi]_B^B).$$

Definice není závislá na volbě báze B, protože stopy podobných matic si jsou rovné.

Charakter reprezentace φ *je funkce* $\chi_\varphi : G \to K$ *definovaná jako*

$$\chi_\varphi(g) := \mathrm{Tr}(\varphi(g)),$$

kde Tr *značí stopu zobrazení.*

Kategorii reprezentací grupy G nad tělesem K budeme značit jako $Rep_K(G)$.

Příklad 18. Nechť $\varphi : G \to \mathrm{Aut}_K(V)$ je reprezentace grupy G nad tělesem K. Pak V má strukturu KG-modulu:

$$r \cdot v = \sum_{g \in G} r_g \varphi(g)(v).$$

Naopak nechť V je KG-modul. Pak $\varphi(g) : v \mapsto g \cdot v$ je K-lineární invertibilní zobrazení z V do V a

$$\begin{aligned} \varphi : G &\to \mathrm{Aut}_K(V) \\ g &\mapsto \varphi(g) \end{aligned}$$

je reprezentace grupy G.

Pokud V je KG-modul, tak *charakter odpovídající* tomuto modulu V je charakter reprezentace grupy dané modulem V, která je popsaná výše.

Tvrzení 19. *Kategorie $Rep_K(G)$ je izomorfní kategorii KG-modulů, které mají konečnou K-dimenzi. Konkrétně nerozložitelné reprezentace odpovídají nerozložitelným modulům.*

Definice 10. *Nechť $\phi_1 : G \to \mathrm{Aut}_K(V_1)$ a $\phi_2 : G \to \mathrm{Aut}_K(V_2)$ jsou dvě reprezentace grupy G nad tělesem K. Řekneme, že ϕ_1 a ϕ_2 jsou* ekvivalentní*, pokud existuje $\Phi : V_1 \to V_2$ izomorfismus vektorových prostorů nad K takový, že $\phi_2(g) = \Phi\phi_1(g)\Phi^{-1}$.*

Tvrzení 20. *Buď G konečná grupa, K algebraicky uzavřené těleso,* $\mathrm{char}(K) \nmid |G|$ *a ϕ, ψ jsou nerozložitelné reprezentace grupy G. Pak platí, že*

$$\frac{1}{|G|}\sum_{g\in G}\chi_\phi(g)\chi_\psi(g^{-1}) = 0, \qquad \text{pokud } \psi \text{ a } \phi \text{ nejsou ekvivalentní reprezentace;}$$
$$\frac{1}{|G|}\sum_{g\in G}\chi_\phi(g)\chi_\psi(g^{-1}) = 1_K, \qquad \text{pokud } \psi \text{ a } \phi \text{ jsou ekvivalentní reprezentace.}$$

Tvrzení 21. *Nechť G je konečná grupa. Potom*

$$\sum_{\varphi\in \mathrm{Irr}(G)}\chi_\varphi(g)\chi_\varphi(h^{-1}) = \begin{cases} 0, & \text{pokud } g, h \text{ nejsou ve stejné konjugační třídě,} \\ \dfrac{|G|}{|C|}, & \text{když } g, h \text{ leží ve stejné konjugační třídě } C. \end{cases}$$

Tvrzení 22. *Buď G konečná grupa, K algebraicky uzavřené těleso a* $\mathrm{char}(K) \nmid |G|$*, $\phi : G \to V$ nerozložitelná reprezentace grupy G. Pak platí, že* $\mathrm{char}(K) \nmid \dim_K(V)$.

Poznámka. Nechť $\varphi : G \to \mathrm{Aut}_K(V)$ je reprezentace grupy G nad tělesem K. Pak φ^* lze přirozeně rozšířit na okruhový homomorfismus $\varphi^* : KG \to \mathrm{Aut}_K(V)$ tak, že

$$\varphi^*(\sum_{g\in G}(r_g g)) := \sum_{g\in G}(r_g\varphi(g)).$$

Stejně tak definujeme charakter $\chi^*_\varphi : KG \to K$ jako

$$\chi^*_\varphi(\sum_{g\in G}(r_g g))) := \mathrm{Tr}(\sum_{g\in G}(r_g\varphi(g))) = \sum_{g\in G}(r_g\chi_\varphi(g)).$$

Věta 23. *Buď K algebraicky uzavřené těleso, G konečná grupa a* $\mathrm{char}(K) \nmid |G|$*, I_j je minimální levý ideál v jednoduché komponentě A_j okruhu KG. Potom $A_j = KGe_j$ pro jednoznačný primitivní centrální idempotent e_j okruhu KG a platí, že*

$$e_j = \frac{\chi_j(1_G)}{|G|} \sum_{g \in G} \chi_j(g^{-1}) g,$$

kde χ_j je charakter odpovídající I_j.

Důkaz. Jelikož K je algebraicky uzavřené těleso a $\mathrm{char}(K) \nmid |G|$, tak

$$KG = KGe_1 \oplus KGe_2 \oplus \cdots \oplus KGe_s$$

je rozklad KG na jednoduché moduly s ortogonálními primitivními centrálními idempotenty $e_1, \ldots, e_s$, kde s je počet konjugačních tříd $C_1, \ldots, C_s$ grupy G, plyne z Věty (27.24) v Curtis and Reiner [2006].

Nechť φ_j je nerozložitelná reprezentace grupy G odpovídající I_j, $e_k = \sum_{g \in G} d_g g$ a mějme $v = \sum_{g \in G} r_g g e_j \in I_j$. Pak

$$\begin{aligned}
\varphi_j^*(e_k)(v) &= \varphi_j^*(\sum_{g \in G} d_g g)(v) \\
&= \sum_{g \in G} d_g \varphi_j(g)(v) \\
&= \sum_{g \in G} d_g g \cdot \sum_{h \in G} r_h h e_j \\
&= e_k e_j \sum_{h \in G} r_h h \\
&= \delta_{kj} v.
\end{aligned}$$

Takže $\varphi_j^*(e_k) = \delta_{kj} \,\mathrm{id}_{I_j}$.

Nechť b_i je jako v Tvrzení 8, tedy $b_i = \sum_{c \in C_i} c$, a podívejme se nyní na $\varphi_j^*(b_i)$. Jelikož b_i leží v centru okruhu KG, tak z Weddernburn-Artinovy věty plyne, že $\varphi_j^*(KG) \simeq \mathrm{Aut}_K(I_j)$. Tudíž $\varphi_j^*(b_i)$ leží v centru $\mathrm{Aut}_K(I_j)$ a proto $\varphi_j^*(b_i) = \omega_j^i \,\mathrm{id}_{I_j}$ pro nějaké $\omega_j^i \in K$. Z toho plyne, že $\mathrm{Tr}(\varphi_j(b_i)) = \omega_j^i \dim_K(I_j)$.

Buď $\chi_j^*(b_i) = \chi_j^*(\sum_{c \in C_i} c) = |C_i| \chi_j(c_i)$, kde $c_i \in C_i$. Jelikož $\chi_j^*(b_i) = \mathrm{Tr}(\varphi_j^*(b_i))$, tak máme

$$\varphi_j^*(b_i) = \frac{|C_i| \chi_j(c_i)}{\dim_K(I_j)} \,\mathrm{id}_{I_j}.$$

Díky Tvrzení 22 nedělíme ve zlomku 0. Jelikož $e_1, \ldots, e_s$ tvoří také bázi centra KG, tak lze b_i vyjádřit jako K-lineární kombinaci $e_1, \ldots, e_s$. Nechť $b_i = \sum_{k=1}^{s} a_k e_k$. Pak

$$\frac{|C_i| \chi_j(c_i)}{\dim_K(I_j)} \,\mathrm{id}_{I_j} = \varphi_j^*(b_i) = \varphi_j^*(\sum_{i=1}^{s} a_k e_k) = \sum_{i=1}^{s} a_k \varphi_j^*(e_k) = \sum_{k=1}^{s} a_k \delta_{kj} \,\mathrm{id}_{I_j}.$$

Získali jsme, že

$$b_i = \sum_{k=1}^{s} \frac{|C_i| \chi_k(c_i)}{\dim_K(I_k)} e_k.$$

Proto

$$\begin{aligned}\frac{\dim_K(I_j)}{|G|}\sum_{i=1}^{s}\chi_j(c_i^{-1})b_i &= \frac{\dim_K(I_j)}{|G|}\sum_{i=1}^{s}\chi_j(c_i^{-1})\sum_{k=1}^{s}\frac{|C_i|\chi_k(c_i)}{\dim_K(I_k)}e_k\\ &= \frac{\dim_K(I_j)}{|G|}\sum_{i,k=1}^{s}\frac{|C_i|\chi_j(c_i^{-1})\chi_k(c_i)}{\dim_K(I_k)}e_k\\ &= \dim_K(I_j)\sum_{k=1}^{s}\frac{e_k}{\dim_K(I_k)}\frac{1}{|G|}\sum_{i=1}^{s}(|C_i|\chi_j(c_i^{-1})\chi_k(c_i))\\ &= \dim_K(I_j)\sum_{k=1}^{s}\frac{e_k}{\dim_K(I_k)}\delta_{jk}\\ &= e_j,\end{aligned}$$

kde předposlední rovnost plyne z Tvrzení 20 a z faktu, že hodnota charakteru je stejná na konjugační třídě. A jelikož

$$\frac{\dim_K(I_j)}{|G|}\sum_{i=1}^{s}\chi_j(c_i^{-1})b_i = \frac{\chi_j(1_G)}{|G|}\sum_{g\in G}\chi_j(g^{-1})g,$$

tak je důkaz hotov.

□

Poznámka. Nechť je χ je nerozložitelný charakter (charakter nerozložitelné reprezentace) grupy G do algebraicky uzavřeného tělesa K, pak odpovídající primitivní idempotent popsaný ve Větě 23 označíme jako $e(\chi)$. Pokud K není algebraicky uzavřené těleso a χ je nerozložitelný charakter grupy G do algebraického uzávěru $\overline{K}$, pak $e(\chi)$ značí odpovídající primitivní idempotent v grupovém okruhu $\overline{K}G$.

Poznámka. Nechť χ je nerozložitelný charakter grupy G nad algebraickým uzávěrem tělesa K. Pak $K(\chi)$ je těleso K rozšířené o obraz charakteru χ.

Poznámka. Nechť $\sigma \in \mathrm{Gal}(\overline{K}/K)$, tak lze σ rozšířit na automorfismus okruhu $\overline{K}G$:

$$\sigma(\sum_{g\in G} r_g g) = \sum_{g\in G}\sigma(r_g)g.$$

Tvrzení 24. *Nechť R je okruh, $\{e_1,\ldots,e_s\}$ je kompletní posloupnost ortogonálních primitivních centrálních idempotentů okruhu R a f je idempotent v R. Pak $f = \sum_{j\in J} e_j$ pro nějaké $J \subseteq \{1,\ldots,s\}$ a pokud je $\{d_1,\ldots,d_l\}$ množina různých primitivních centrálních idempotentů, pak platí*

$$d_j e_i = 0, \text{ nebo } d_j e_i = d_j.$$

pro každé i,j.

Tvrzení 25. *Nechť f je centrální idempotent okruhu R. Pak platí, že*

- *g je centrální idempotent okruhu R právě tehdy, když fg je centrální idempotent a také $(1-f)g$ je centrální idempotent.*

- *g je primitivní centrální idempotent okruhu R právě tehdy, když je fg primitivní centrální idempotent a $(1-f)g = 0$, nebo $(1-f)g$ je primitivní centrální idempotent a $fg = 0$.*

Důkaz. Nechť g je centrální idempotent okruhu R, pak ekvivalence vyplývá z toho, že $g = fg + (1-f)g$.

Nechť g je primitivní centrální idempotent. Pak opět máme $g = fg + (1-f)g$ a z předchozího tvrzení platí, že buď $fg = g$, nebo $(1-f)g = g$. Pro druhou implikaci předpokládejme, že fg je primitivní centrální idempotent a $(1-f)g = 0$, pak $g = fg$ a g je primitivní centrální idempotent.

□

Věta 26. *Nechť K je těleso, $\overline{K}$ je jeho algebraický uzávěr takový, že $\mathrm{char}(K) \nmid |G|$, G konečná grupa a χ je nerozložitelný charakter grupy G nad algebraickým uzávěrem K. Pak*

$$e_K(\chi) = \sum_{\sigma \in \mathrm{Gal}(K(\chi)/K)} \sigma(e(\chi)))$$

je primitivní centrální idempotent okruhu KG.

Důkaz. Jelikož $e(\chi)$ je primitivní centrální idempotent v $\overline{K}G$ a σ je automorfismus, $\sigma(e(\chi))$ je primitivní centrální idempotent $\overline{K}G$ pro každé $\sigma \in \mathrm{Gal}(K(\chi)/K)$. Podívejme se na předpis $e_K(\chi)$:

$$\begin{aligned} e_K(\chi) &= \sum_{\sigma \in \mathrm{Gal}(K(\chi)/K)} \sigma(e(\chi))) \\ &= \frac{\chi(1_G)}{|G|} \sum_{\sigma \in \mathrm{Gal}(K(\chi)/K)} \sigma(\sum_{g \in G} \chi(g^{-1})g)) \\ &= \frac{\chi(1_G)}{|G|} \sum_{g \in G} \sum_{\sigma \in \mathrm{Gal}(K(\chi)/K)} \sigma(\chi(g^{-1}))g. \end{aligned}$$

Ale

$$\sum_{\sigma \in \mathrm{Gal}(K(\chi)/K)} \sigma(\chi(g^{-1})) \in \mathrm{Fix}_{K(\chi)/K}(\mathrm{Gal}(K(\chi)/K)) = K,$$

tedy $e_K(\chi) \in KG$. Takže $e_K(\chi)$ je centrální idempotent v KG a tudíž také v $\overline{K}G$. Nyní chceme dokázat, že je primitivní.

Pokud $\sigma \neq \mathrm{id}_{K(\chi)} \in \mathrm{Gal}(K(\chi)/K)$, tak

$$K \subseteq \mathrm{Fix}_{K(\chi)/K}(\langle\sigma\rangle) \subset K(\chi).$$

Jelikož $e(\chi) = \dfrac{\chi(1_G)}{|G|} \displaystyle\sum_{g \in G} \chi(g^{-1})g$, tak $\sigma(e(\chi))$ bude mít minimálně jeden koeficient jiný než $e(\chi)$. Takže množina $\{\sigma(e(\chi)); \sigma \in \mathrm{Gal}(K(\chi)/K)\}$ je množina navzájem různých ortogonálních centrálních primitivních idempotentů $\overline{K}G$.

Pokud by tedy nebyl idempotent $e_K(\chi)$ primitivní v KG, pak by nebyl primitivní ani v $\overline{K}G$. Dále z Tvrzení 24 plyne, že by existovaly dvě podmnožiny I, J Galoisovy grupy $\mathrm{Gal}(K(\chi)/K)$ takové, že $I \cap J = \varnothing$, $I \cup J = \mathrm{Gal}(K(\chi)/K)$ a

$$e_K(\chi) = \sum_{\sigma \in I} \sigma(e(\chi)) + \sum_{\sigma \in J} \sigma(e(\chi)),$$

kde $\sum_{\sigma \in I} \sigma(e(\chi)), \sum_{\sigma \in J} \sigma(e(\chi)) \in KG$. Nechť $\mathrm{id}_{K(\chi)} \in I, \tau \in J$, pak

$$\sum_{\sigma \in I} \sigma(e(\chi)) = \tau(\sum_{\sigma \in I} \sigma(e(\chi))) = \sum_{\sigma \in I} \tau\sigma(e(\chi)),$$

kde první rovnost platí, protože koeficienty $\sum_{\sigma \in I} \sigma(e(\chi))$ leží v K. Pak ale $\tau \in I$, což je spor.

□

Poznámka. Pokud $K(\chi) = K$, tak $e_K(\chi) = e(\chi)$.

Příklad 27. Mějme grupu kvaternionů

$$Q_8 = \langle \overline{e}, i, j, k : \overline{e}^2 = e, i^2 = j^2 = k^2 = ijk = \overline{e} \rangle,$$

kde e je jednotkový prvek a $\overline{e}i$ označíme jako $\overline{i}$, stejně tak pro j, k. Chceme spočítat idempotenty pomocí charakterů. Q_8 má 5 konjugačních tříd $\{e\}$,$\{\overline{e}\}, \{i, \overline{i}\}, \{j, \overline{j}\}$, $\{k, \overline{k}\}$, takže hledáme 5 idempotentů, 5 charakterů. Jako první máme triviální reprezentaci $\phi_{\mathrm{triv}} : \ Q_8 \to \mathbb{Q}$, $\phi_{\mathrm{triv}}(g) = 1$ pro každé $g \in Q_8$. Jelikož

$$|Q_8| = d_1^2 + d_2^2 + d_3^2 + d_4^2 + d_5^2,$$

kde d_i jsou stupně jednotlivých reprezentací a $d_1 = 1$, tak $d_2 = d_3 = d_4 = 1$ a $d_5 = 2$. Např. $\{i, \overline{i}\}$ je konjugační třída, takže $\chi_i(i) = \chi_i(\overline{i})$ a $\chi_i(\overline{e}) = 1$, pro každé $i \in \{2, 3, 4\}$. Jelikož $ijk = \overline{e}$, tak máme následující tabulku charakterů.

char/hodnoty	e	$\overline{e}$	i, $\overline{i}$	j, $\overline{j}$	k, $\overline{k}$
χ_{triv}	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	1	-1
χ_5	2	?	?	?	?

Pak z ortogonálních vztahů charakterů (Tvrzení 20 a Tvrzení 21) vyplývá:

char/hodnoty	e	$\overline{e}$	i, $\overline{i}$	j, $\overline{j}$	k, $\overline{k}$
χ_{triv}	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	1	-1
χ_5	2	-2	0	0	0

Získali jsme idempotenty:

$$\begin{aligned}
e_{\text{triv}} &= \frac{1}{8}(e+\overline{e}+i+\overline{i}+j+\overline{j}+k+\overline{k}),\\
e_2 &= \frac{1}{8}(e+\overline{e}-i-\overline{i}-j-\overline{j}+k+\overline{k}),\\
e_3 &= \frac{1}{8}(e+\overline{e}+i+\overline{i}-j-\overline{j}-k-\overline{k}),\\
e_4 &= \frac{1}{8}(e+\overline{e}-i-\overline{i}+j+\overline{j}-k-\overline{k}),\\
e_5 &= \frac{2}{8}(2e-2\overline{e}) = \frac{1}{2}(e-\overline{e}).
\end{aligned}$$

3. Idempotenty pomocí Shodových párů

Tato kapitola je souhrnem článků Jespers et al. [2003], [Olivieri et al., 2004], [Broche and Río, 2007], Bakshi and Kaur [2019] s podrobněji rozepsanými důkazy a přidaným technickým Tvrzením 33. V první části této kapitoly je nejdříve popsán způsob, jakým lze spočítat idempotenty grupového okruhu $\mathbb{Q}G$, pro G konečnou grupu, pomocí speciálních párů podgrup grupy G, tzv. Shodových párů. V druhé části je tento postup rozšířen pro výpočet idempotentů grupového okruhu $\mathbb{F}G$, pro G konečnou grupu a konečné těleso $\mathbb{F}$, pro které $\mathbb{F}G$ je totálně rozložitelný okruh.

3.1 Idempotenty $\mathbb{Q}G$

V této sekci je nejdříve definován prvek $\varepsilon(G, N)$ pro G konečnou grupu a N její normální podgrupu a pomocí Tvrzení 28 je tato definice propojena s idempotentem $e_{\mathbb{Q}}(\chi)$ pro lineární charakter χ. Následuje definice indukovaného modulu, resp. indukované reprezentace grupy, a dvě tvrzení z teorie reprezentací grup, která jsou bez důkazu. Tvrzení 29 je technické tvrzení potřebné k důkazu Tvrzení 33, Tvrzení 30 je potřeba v příkladu na konci kapitoly. Poté je uvedena Shodova věta, která je stavebním kamenem této teorie. Její důkaz je technický a pro další výpočty není potřeba, proto zde není. Dále je definován Shodův pár podgrup a v Důsledku 32 je popsáno, jak tato definice souvisí se Shodovou větou. Tvrzení 33 je technické a potřebné pro důkaz hlavní Věty 34. Po důkazu hlavní věty jsou popsány její důsledky, které vedou k definici silného Shodova páru. Tvrzení 38 a 39 jsou technická a vedou k důkazům Tvrzení 40 a 41, která popisují propojení Shodových párů a silných Shodových párů a také popisují, k čemu jsou silné Shodovy páry dobré. Důsledek 42 a Tvrzení 46 se hodí pro výpočet příkladů. Nakonec jsou spočítány primitivní centrální idempotenty pro grupové okruhy $\mathbb{Q}Q_8$ a $\mathbb{Q}D_{12}$ a je ukázáno propojení postupu pomocí Shodových párů a pomocí charakterů grup.

V této kapitole budeme pracovat s konečnou grupou G a okruhem $\mathbb{Q}$, s reprezentacemi a lineárními charaktery (definováno níže) G nad $\mathbb{C}$, neboť pro lineární charakter χ tyto výsledky lze použít i pro $\mathbb{Q} \leq \overline{\mathbb{Q}}$, protože $\mathbb{Q}(\chi)$ je pro konečnou grupu a lineární charakter algebraické rozšíření. Nechť $\mathcal{M}(G)$ značí množinu minimálních netriviálních normálních podgrup G, pak definujeme

$$\varepsilon(G) = \prod_{M \in \mathcal{M}(G)} (1 - \widehat{M}).$$

Pokud $N \trianglelefteq G$, pak jádro zobrazení

$$\begin{aligned} \varepsilon_N : \mathbb{Q}G &\longrightarrow \mathbb{Q}(G/N) \\ \sum_{g \in G} r_g g &\mapsto \sum_{g \in G} r_g N g \end{aligned}$$

je $\mathbb{Q}G(1 - \widehat{N})$ a to indukuje izomorfismus $\mathbb{Q}G\widehat{N} \simeq \mathbb{Q}(G/N)$. Pak definujeme zobecnění definice výše

$$\varepsilon(G,N) = \begin{cases} \widehat{N}, & \text{pro } N = G, \\ \prod\limits_{M/N \in \mathcal{M}(\mathcal{G}/\mathcal{N})} (\widehat{N} - \widehat{M}), & \text{pro } N \neq G. \end{cases}$$

Dále definujeme *lineární charakter* jako charakter reprezentace stupně 1 grupy G nad tělesem $\mathbb{C}$, tedy se jedná o grupový homomorfismus z grupy G do multiplikativní grupy tělesa $\mathbb{C}$. A nakonec definujme značení, pro $x \in RG$, libovolný okruh R, a $g \in G$: $x^g := g^{-1}xg$.

Pokud χ je lineární charakter konečné grupy G nad $\mathbb{C}$ a $H = \ker(\chi)$, tak G/H je cyklická grupa, jelikož každá konečná podgrupa $\mathbb{C}^*$ je cyklická a v lineárním případě je charakter homomorfismus.

Tvrzení 28. *Pokud χ je lineární charakter konečné grupy G a $H = \ker(\chi)$, pak $e_{\mathbb{Q}}(\chi) = \varepsilon(G,H)$.*

Důkaz. Pokud A je konečná cyklická grupa, tak $\varepsilon(A)$ je primitivní centrální idempotent $\mathbb{Q}A$. To plyne z Lemma 1.2 a Věty 1.4 v Goodaire et al. [1996]. Speciálně pokud G/N je konečná cyklická grupa, tak $\varepsilon(G/N)$ je primitivní centrální idempotent a tedy i $\varepsilon(G,N)$ je primitivní centrální idempotent v $\mathbb{Q}G$. Nechť $G/H = \langle gH \rangle$ a $[G:H] = n$, pak $\chi(g) = \xi$, kde ξ je n-tá primitivní odmocnina z 1. Minimální podgrupy G/H jsou tvaru $M_p/H = \langle g^{\frac{n}{p}}, H \rangle$, kde p je prvočíselný dělitel n. Pak χ rozšíříme na χ^* na celý okruh $\mathbb{C}G$ jako v Poznámce před Větou 23. Potom

$$\begin{aligned} \chi^*(\widehat{H} - \widehat{M_p}) &= \frac{1}{|H|} \sum_{h \in H} h - \frac{1}{|M_p|} \sum_{i=1}^{p} \chi(g^{\frac{n}{p}i}) \\ &= 1 - \frac{1}{p} \sum_{i=0}^{p-1} (\xi^{\frac{n}{p}i}) = 1, \end{aligned}$$

protože součet $\sum\limits_{i=0}^{p-1} (\xi^{\frac{n}{p}i})$ je roven 0. Proto

$$\chi^*(\varepsilon(G,H)) = (\prod_{p|n} \chi^*(\widehat{H} - \widehat{M_p})) = 1.$$

Ale jelikož $e_{\mathbb{Q}}(\chi)$ je jediný primitivní centrální idempotent e, pro který $\chi(e) = 1$, tak

$$e_{\mathbb{Q}}(\chi) = \varepsilon(G,H).$$

Tím je důkaz hotov.

□

Definice 11. *Nechť R je okruh, G grupa, H podgrupa grupy G a M je levý RH-modul, tedy reprezentace podgrupy H nad R. Pak*

$$M^G = RG \otimes_{RH} M$$

je levý RG-modul indukovaný modulem M, *neboli* reprezentace grupy G indukovaná reprezentací grupy H.

Poznámka. Nechť φ_H je reprezentace podgrupy H grupy G nad okruhem R. Pak indukovanou reprezentaci grupy G značíme jako φ_H^G.

Následující dvě tvrzení lze nalézt v Curtis and Reiner [2006] na začátku 6. kapitoly a v odstavci 12.26, Shodova věta je ve stejném zdroji jako Důsledek 45.4. Tvrzení patří k teorii reprezentací a důkazy nejsou uvedeny, protože patří do základů teorie reprezentací a nejsou pro další konstrukce a výpočty potřebné.

Tvrzení 29. *Nechť φ_H je reprezentace podgrupy H grupy G nad $\mathbb{C}$ s charakterem χ_H. Pak charakter indukované reprezentace χ_H^G je charakter grupy G a lze jej spočítat jako*

$$\chi_H^G(g) = \frac{1}{|H|} \sum_{t \in G} \chi_H(tgt^{-1}),$$

kde $\chi_H(g) = 0$, pokud $g \in G \setminus H$.

Tvrzení 30. *Nechť φ_H je reprezentace podgrupy H grupy G nad okruhem R. Pak*

$$\deg_R(\varphi_H^G) = [G : H] \deg_R(\varphi_H).$$

Věta 31. *(Shodova věta) Nechť χ je lineární charakter definovaný na podgrupě K grupy G. Pak indukovaný charakter χ^G je nerozložitelný právě tehdy, když pro každé $g \in G \setminus K$ existuje $k \in K \cap K^g$ takové, že $\chi(gkg^{-1}) \neq \chi(k)$.*

Definice 12. *Pár podgrup (K, H) grupy G je* Shodův pár, *pokud splňuje následující podmínky:*

(S1) $H \trianglelefteq K$,

(S2) K/H je cyklická grupa,

(S3) pokud $g \in G$ a $[K, g] \cap K \subseteq H$, pak $g \in K$.

Důsledek 32. *Shodovu větu můžeme pomocí definice výše přepsat takto: pokud je χ lineární charakter na podgrupě K grupy G s jádrem H, pak indukovaný charakter χ^G je nerozložitelný právě tehdy, když (K, H) je Shodův pár.*

Mějme dvě podgrupy H a K grupy G takové, že $H \trianglelefteq K$, pak definujeme

$$e(G, K, H) = \sum_{t \in T} \varepsilon(K, H)^t,$$

kde T je pravá transverzála $\mathrm{Cen}_G(\varepsilon(K, H))$ v G. Pak vidíme, že $e(G, K, H)$ je v $Z(\mathbb{Q}G)$. A pokud pro každé $t \neq k \in T$ platí, že $\varepsilon(K, H)^t \varepsilon(K, H)^k = 0$, tak $e(G, K, H)$ je centrální idempotent v $\mathbb{Q}G$.
Dokažme nyní pomocné technické tvrzení, které nebylo dokázáno v původním článku, a používá se v důkazu Věty 34.

Tvrzení 33. *Buď χ lineární charakter podgrupy K grupy G nad $\mathbb{C}$ a $\{g_1, \ldots, g_k\}$ je pravá transverzála K v G. Pak*

$$\chi^G(g) = \sum_{i=1}^{k} \chi(g_i g g_i^{-1}).$$

Navíc platí, že

$$e(\chi^G) = \sum_{i=1}^{k} (g_i^{-1} e(\chi) g_i).$$

Důkaz. Použijeme předpis pro χ^G z Tvrzení 29:

$$\chi^G(g) = \frac{1}{|K|} \sum_{t \in G} \chi(tgt^{-1}),$$

kde $\chi(g) = 0$ pro $g \notin K$. Pak si všimněme, že

$$\chi(kgk^{-1}) = \chi(g), \text{ pro každé } k \in K,$$

neboť pro $g \in G \setminus K$ jsou obě strany rovny 0 a pokud $g \in K$, tak jsou si strany také rovny, jelikož charakter má stejnou hodnotu na konjugační třídě. Pak tedy pro $kg_i \in Kg_i$ a $g \in G$ platí, že

$$\chi(kg_i g g_i^{-1} k^{-1}) = \chi(g_i g g_i^{-1}).$$

Tudíž můžeme indukovaný charakter upravit a získáme první část tvrzení.

$$\begin{aligned}
\chi^G(g) &= \frac{1}{|K|} \sum_{t \in G} \chi(tgt^{-1}) \\
&= \frac{1}{|K|} \sum_{t \in Kg_1 \cup \cdots \cup Kg_k} \chi(tgt^{-1}) \\
&= \frac{1}{|K|} \Big(\sum_{t \in Kg_1} \chi(tgt^{-1}) + \cdots + \sum_{t \in Kg_k} \chi(tgt^{-1}) \Big) \\
&= \frac{1}{|K|} \big(|Kg_1| \chi(g_1 g g_1^{-1}) + \cdots + |Kg_k| \chi(g_k g g_k^{-1}) \big) \\
&= \sum_{i=1}^{k} \chi(g_i g g_i^{-1})
\end{aligned}$$

Upravíme pomocí tohoto vzorce předpis pro $e(\chi^G)$.

$$\begin{aligned}
e(\chi^G) &= \frac{\chi^G(1_G)}{|G|}(\sum_{g\in G}\chi^G(g)g^{-1}) \\
&= \frac{[G:K]}{|G|}(\sum_{g\in G}(\sum_{i=1}^{k}\chi(g_igg_i^{-1}))g^{-1}) \\
&= \frac{1}{|K|}(\sum_{i=1}^{k}(\sum_{g\in G}\chi(g_igg_i^{-1}))g^{-1}) \\
&= \frac{1}{|K|}(\sum_{i=1}^{k}(\sum_{g_igg_i^{-1}\in K}\chi(g_igg_i^{-1})g^{-1}), \quad \text{jelikož } \chi(g_igg_i^{-1})\neq 0 \Leftrightarrow g_igg_i^{-1}\in K, \\
&= \frac{1}{|K|}(\sum_{i=1}^{k}(\sum_{h_i\in K}\chi(h_i)g_i^{-1}h_i^{-1}g_i), \qquad \text{pro } h_i := g_igg_i^{-1}, \\
&= \sum_{i=1}^{k}g_i^{-1}\frac{1}{|K|}(\sum_{h_i\in K}\chi(h_i)h_i^{-1})g_i \\
&= \sum_{i=1}^{k}(g_i^{-1}e(\chi)g_i)
\end{aligned}$$

A důkaz je hotov.

□

Věta 34. *Nechť G je konečná grupa, K je podgrupa G, χ je lineární charakter K a χ^G je indukovaný charakter χ na G. Pokud χ^G je nerozložitelný charakter, pak*

$$e_{\mathbb{Q}}(\chi^G) = \frac{[\mathrm{Cen}_G(\varepsilon(K,H)):K]}{[\mathbb{Q}(\chi):\mathbb{Q}(\chi^G)]}e(G,K,H),$$

kde H je jádro χ.

Důkaz. Na $\mathbb{C}G$ můžeme definovat dvě akce. Nejdříve pravou akci grupy G tak, že g působí na e konjugací e^g pro $e\in\mathbb{C}G, g\in G$. Pak pro $\mathcal{A}=\mathrm{Aut}(\mathbb{C})$

$$\sigma\cdot e = \sum_{g\in G}\sigma(e_g)g,$$

pro $e\in\mathbb{C}G$ a $\sigma\in\mathcal{A}$, je levá akce $\mathcal{A}$ na $\mathbb{C}G$. Když na prvek $e\in\mathbb{C}G$ působí obě množiny, tak platí

$$(\sigma\cdot e)^g = \sigma\cdot(e^g).$$

Tudíž můžeme zadefinovat levou akci grupy $\mathcal{A}\times G$ na $\mathbb{C}G$:

$$(\sigma,g)\cdot e = \sigma\cdot e^g.$$

Mějme idempotent $e=e(\chi)\in\mathbb{C}G$, na který necháme působit $\mathcal{A}\times\mathcal{G}$. Nechť $T_{\mathcal{A}}=\{\sigma_1,\sigma_2,\ldots,\sigma_n\}$ je levá transverzála stabilizátoru $\mathcal{A}_e$ a $T_G=\{g_1,g_2,\ldots,g_k\}$ je pravá transverzála stabilizátoru G_e. Pak působení $\mathcal{A}\times G$ vytvoří orbity, jejichž reprezentanty můžeme v tabulce zapsat takto:

$\sigma_1 \cdot e^{g_1}$	$\sigma_1 \cdot e^{g_2}$	$\dots$	$\sigma_1 \cdot e^{g_k}$
$\sigma_2 \cdot e^{g_1}$	$\sigma_2 \cdot e^{g_2}$	$\dots$	$\sigma_2 \cdot e^{g_k}$
$\dots$	$\dots$	$\dots$	$\dots$
$\sigma_n \cdot e^{g_1}$	$\sigma_n \cdot e^{g_2}$	$\dots$	$\sigma_n \cdot e^{g_k}$

Jako levou transverzálu stabilizátoru $\mathcal{A}_e$ můžeme vzít $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$, jelikož χ je lineární charakter a tedy $\mathbb{Q}(\chi)$ je algebraické rozšíření a také $e = e(\chi)$. Protože χ^G je nerozložitelná reprezentace, tak ze Shodovy věty plyne, že pokud

$$\chi(g^{-1}kg) = \chi(k),$$

tak $g \in K$, a proto $G_e = K$. Pak je T_G pravá transverzála K v G. Uděláme nyní součty všech sloupců a všech řádků tabulky. Z Tvrzení 33 plyne, že součet i-tého řádku je $\sigma_i \cdot e(\chi^G)$ a z definice $e_{\mathbb{Q}}(\chi)$ (Věta 26 a Věta 23) a Tvrzení 28 plyne, že součet každého sloupce je $\varepsilon(K,H) \cdot g_i$.

$\sigma_1 \cdot e^{g_1}$	$\sigma_1 \cdot e^{g_2}$	$\dots$	$\sigma_1 \cdot e^{g_k}$	$\sigma_1 \cdot e(\chi^G)$
$\sigma_2 \cdot e^{g_1}$	$\sigma_2 \cdot e^{g_2}$	$\dots$	$\sigma_2 \cdot e^{g_k}$	$\sigma_2 \cdot e(\chi^G)$
$\dots$	$\dots$	$\dots$	$\dots$	
$\sigma_n \cdot e^{g_1}$	$\sigma_n \cdot e^{g_2}$	$\dots$	$\sigma_n \cdot e^{g_k}$	$\sigma_n \cdot e(\chi^G)$
$\varepsilon(K,H) \cdot g_1$	$\varepsilon(K,H) \cdot g_2$	$\dots$	$\varepsilon(K,H) \cdot g_k$	$*$

Pak

$$* = \sum_{i=1}^{m} (\sigma_i \cdot e(\chi^G)) = \sum_{j=1}^{k} \varepsilon(K,H) \cdot g_i.$$

Galoisovu grupu $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ můžeme zapsat jako rozklad na pravé rozkladové třídy podgrupy $\mathrm{Gal}(\mathbb{Q}(\chi^G)/\mathbb{Q})$:

$$\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}) = \alpha_1 \,\mathrm{Gal}(\mathbb{Q}(\chi^G)/\mathbb{Q}) \cup \cdots \cup \alpha_m \,\mathrm{Gal}(\mathbb{Q}(\chi^G)/\mathbb{Q}),$$

kde $\alpha_i \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}(\chi^G))$, pro každé $i \in \{1, \dots, m\}$, a $m = [\mathbb{Q}(\chi) : \mathbb{Q}(\chi^G)]$. Takže první sumu ve výpočtu $*$ můžeme upravit:

$$\begin{aligned}\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})} \sigma \cdot e(\chi^G) &= \sum_{\sigma \in \alpha_1 \,\mathrm{Gal}(\mathbb{Q}(\chi^G)/\mathbb{Q})} \sigma \cdot e(\chi^G) + \cdots + \sum_{\sigma \in \alpha_m \,\mathrm{Gal}(\mathbb{Q}(\chi^G)/\mathbb{Q})} \sigma \cdot e(\chi^G) \\ &= \sum_{i \in \{1,\dots,m\}} \alpha_i \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi^G)/\mathbb{Q})} \sigma \cdot e(\chi^G),\end{aligned}$$

jelikož $\alpha_i \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}(\chi^G))$. Dále

$$\begin{aligned}\sum_{i \in \{1,\dots,m\}} \alpha_i \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi^G)/\mathbb{Q})} (\sigma \cdot e(\chi^G)) &= [\mathbb{Q}(\chi) : \mathbb{Q}(\chi^G)] \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi^G)/\mathbb{Q})} \sigma e(\chi^G) \\ &= [\mathbb{Q}(\chi) : \mathbb{Q}(\chi^G)] e_{\mathbb{Q}}(\chi^G).\end{aligned}$$

Z definice $e(G,K,H) = \sum_{g \in T} \varepsilon(K,H)^g$, T je pravá transverzála $\mathrm{Cen}_G(\varepsilon(K,H))$ v G. Tedy v $*$ každý člen $e(G,K,H)$ je $[\mathrm{Cen}_G(\varepsilon(K,H)) : K]$-krát, proto je druhá suma rovna

$$[\mathrm{Cen}_G(\varepsilon(K,H)) : K] e(G,K,H).$$

Z toho plyne dokazovaný vztah.

□

Důsledek 35. *Pokud je (K, H) Shodův pár grupy G, pak existuje jedinečné $\alpha \in \mathbb{Q}$ takové, že $\alpha e(G, K, H)$ je primitivní centrální idempotent $\mathbb{Q}G$.*

Nabízí se otázka: kdy je každý primitivní centrální idempotent výše uvedeného tvaru? Tato otázka vede k použití definice monomiální grupy.

Definice 13. *Konečná grupa G je* monomiální*, pokud každý její nerozložitelný charakter je indukovaný lineárním charakterem nějaké její podgrupy.*

Příklad 36. Monomiální grupy jsou například nilpotentní grupy, metabelovské grupy, super-řešitelné grupy. [Bakshi and Kaur, 2017]

Důsledek 37. *Konečná grupa G je monomiální právě tehdy, když každý primitivní centrální idempotent grupového okruhu $\mathbb{Q}G$ je tvaru $\alpha e(G, K, H)$ pro $\alpha \in \mathbb{Q}$ a Shodův pár (H, K) grupy G.*

Nyní víme, že pro monomiální grupy umíme najít všechny primitivní centrální idempotenty pomocí Shodových párů, pro nemonomiální umíme najít nějaké primitivní centrální idempotenty pomocí Shodových párů. Hodilo by se však, aby v předpisu idempotentu nebyl nevkusný koeficient α. Tím je inspirovaná definice silného Shodova páru.

Definice 14. Silný Shodův pár *grupy G je pár (K, H) podgrup grupy G takový, že splňuje:*

(SS1) $H \trianglelefteq K \trianglelefteq N_G(H)$,

(SS2) K/H je cyklická grupa a maximální abelovská podgrupa v $N_G(H)/H$,

(SS3) pro každé $g \in G \setminus N_G(H)$ platí, že $\varepsilon(K, H)\varepsilon(K, H)^g = 0$.

Tvrzení 38. *Nechť G je konečná grupa a e je primitivní centrální idempotent $\mathbb{Q}G$. Pak $\{g \in G : eg = e\} = \{1_G\}$ právě tehdy, když $\varepsilon(G)e = e$. Speciálně, pokud G má věrnou, tedy injektivní, nerozložitelnou reprezentaci, tak $\varepsilon(G) \neq 0$.*

Důkaz. Mějme M normální podgrupu G, pak $\widehat{M}e = e$ právě tehdy, když $M \subseteq \{g \in G : eg = e\}$. Jelikož $\varepsilon(G)$ je centrální idempotent a e je primitivní centrální idempotent, tak $\varepsilon(G)e$ může být rovno e, nebo 0. Máme

$$\varepsilon(G)e = \prod_{M \in \mathcal{M}(G)} (1 - \widehat{M})e = \prod_{M \in \mathcal{M}(G)} (e - \widehat{M}e).$$

Ze stejného argumentu může platit pouze to, že $(1 - \widehat{M})e$ je rovno buď e, nebo 0, a jelikož $\{g \in G : eg = e\}$ je normální podgrupa a pokud není triviální, tak obsahuje minimální normální podgrupu, tak $\{g \in G : eg = e\} = \{1\}$ právě tehdy, když $\varepsilon(G)e = e$. Nyní dokážeme poslední část. Nechť G má věrnou nerozložitelnou reprezentaci. Tedy máme nerozložitelný modul I, pro který platí $Ie = I$, kde e je primitivní centrální idempotent (jinak by modul nebyl nerozložitelný, protože bychom jej pomocí primitivních centrálních idempotentů rozložit), a reprezentace

odpovídající tomuto modulu, označme ji ϕ, je věrná (připomeňme Příklad 18). Že se jedná o věrnou reprezentaci znamená, že pokud $\phi(g) = \mathrm{id}_{Ie}$, tak $g = 1_G$. Z Příkladu 18 víme, že reprezentace $\phi(g)$ vypadá takto:

$$\phi(g) : ve \mapsto g \cdot ve,$$

kde $ve \in Ie$. Proto když $\phi(g) = \mathrm{id}_{Ie}$, tak musí platit $ge = e$. Takže pokud je reprezentace věrná, tak $\{g \in G : eg = e\} = \{1_G\}$.

□

Tvrzení 39. *Nechť $H \trianglelefteq K \leq G$.*

- *Pokud $K \trianglelefteq N_G(H)$, pak $N_G(H) \leq \mathrm{Cen}_G(\varepsilon(K, H))$.*
- *Pokud K/H je cyklická grupa, pak $\mathrm{Cen}_G(\varepsilon(K, H)) \leq N_G(H)$ a následující podmínky jsou ekvivalentní pro $g \in G$:*

  (i) $g \in H$,
  (ii) $g\varepsilon(K, H) = \varepsilon(K, H)$,
  (iii) $\widehat{g}\varepsilon(K, H) = \varepsilon(K, H)$.

Důkaz. Nechť g leží $N_G(H)$, pak $gH = Hg$. A protože $K \trianglelefteq N_G(H)$, tak $\varepsilon(K^g, H^g) = \varepsilon(K, H)$. Zároveň ale platí, že $\varepsilon(H, K)^g = \varepsilon(K^g, H^g)$, tím je dokázaná první část tvrzení.

Nejdříve dokážeme ekvivalenci podmínek a potom ukážeme, jak z toho plyne druhé vnoření grup.

Z definice

$$\varepsilon(K, H) = \prod_{M/H \in \mathcal{M}(K/H)} (\widehat{H} - \widehat{M})$$

a platí, že $g\widehat{H} = \widehat{H}$ a $g\widehat{M} = \widehat{M}$, proto $(i) \Rightarrow (ii)$. Jelikož z definice $\widehat{g} = \widehat{\langle g \rangle}$, tak

$$\widehat{g}\varepsilon(K, H) = \frac{1}{\mathrm{ord}(g)} \sum_{i=1}^{\mathrm{ord}(g)} g^i \varepsilon(K, H) = \varepsilon(K, H)$$

a proto $(ii) \Rightarrow (iii)$. Pokud platí (iii), tak

$$\widehat{g} \prod_{M/H \in \mathcal{M}(K/H)} (\widehat{H} - \widehat{M}) = \prod_{M/H \in \mathcal{M}(K/H)} (\widehat{H} - \widehat{M}),$$

tedy např. $\widehat{g}\widehat{H} = \widehat{H}$ a pak $g\widehat{H} = g\widehat{g}\widehat{H} = \widehat{g}\widehat{H} = \widehat{H}$, tudíž $g\varepsilon(K, H) = \varepsilon(K, H)$. Jelikož K/H má věrnou nerozložitelnou reprezentaci, tak díky předchozímu tvrzení víme, že $\varepsilon(K, H) \neq 0$. Chceme dokázat (ii) implikuje (i). Ať platí, že $g\varepsilon(K, H) = \varepsilon(K, H)$. Protože $\varepsilon(K, H) \in \mathbb{Q}K$, tak $g \in K$. Mějme $g \in K \setminus H$ a vezměme $M/H \in \mathcal{M}(\langle g, H \rangle / H)$. Pak také $M/H \in \mathcal{M}(K/H)$. Též platí, že $\langle g, H \rangle = \langle g, M \rangle$ a proto máme rovnost $\widehat{g}\widehat{H} = \widehat{\langle g, H \rangle} = \widehat{\langle g, M \rangle} = \widehat{g}\widehat{M}$. Z toho plyne rovnost $\varepsilon(K, H) = \widehat{g}\varepsilon(K, H) = 0$, což je spor.

Zbývá dokázat, že $\mathrm{Cen}_G(\varepsilon(K, H)) \leq N_G(H)$. Nechť $g \in \mathrm{Cen}_G(\varepsilon(K, H))$, pak z ekvivalence mezi $(i) \Leftrightarrow (iii)$ plyne, že $g \in H \leq N_G(H)$.

□

Tvrzení 40. *Nechť (K, H) je dvojice podgrup grupy G, pak následující tvrzení jsou ekvivalentní:*

(i) (K, H) *je silný Shodův pár grupy* G*;*

(ii) (K, H) *je Shodův pár grupy* G*,* $K \trianglelefteq N_G(H)$ *a všechny* G*-konjugace* $\varepsilon(K, H)$ *jsou ortogonální.*

Navíc, pokud podmínky platí, tak $\mathrm{Cen}_G\varepsilon(K, H) = N_G(H)$ *a* $e(G, K, H)$ *je primitivní centrální idempotent v* $\mathbb{Q}G$*.*

Důkaz. Nejdříve se podívejme na implikaci $(ii) \Rightarrow (i)$. Z podmínky (ii) je splněna podmínka $(SS1)$ a z předchozího tvrzení plyne, že $\mathrm{Cen}_G(K, H) = N_G(H)$, a proto platí i podmínka $(SS3)$. Zbývá dokázat podmínku $(SS2)$. Nechť K/H není největší abelovskou podgrupou v $N_G(H)/H$ a L/K je největší abelovská podgrupa v $N_G(H)/H$. Pak existuje $l \in L$, tedy $l \in N_G(H)$, a zároveň $l \notin K$. Jelikož $K \trianglelefteq N_G(H)$, tak $[K, l] \cap K = K$ a tedy podmínka $(S3)$ z definice Shodova páru není splněna a to je spor.

Předpokládejme, že je splněná první podmínka. Pak jsou splněné podmínky $(S1), (S2)$ a z předešlého tvrzení plyne, že $N_G(H) = \mathrm{Cen}_G(\varepsilon(K, H))$ a všechny G-konjugace $\varepsilon(K, H)$ jsou ortogonální. Zbývá dokázat podmínku $(S3)$. Mějme $g \in G$ takové, že $[K, g] \cap K \subseteq H$. Chceme dokázat, že $g \in K$. Nechť χ je lineární charakter grupy K s jádrem H. Pokud $g^{-1}kg \in K$ pro nějaké $k \in K$, pak $[k, g] \in [K, g] \cap K \subseteq H$ a tedy $\chi([k, g]) = 1$. Podíváme se na součin $e(\chi)(e(\chi) \cdot g)$, připomeneme, že $\cdot g$ působí na $e(\chi)$ konjugací. Tedy

$$e(\chi)(e(\chi) \cdot g) = \frac{1}{|K|^2} \sum_{k_1, k_2 \in K} \chi(k_1)\chi(k_2^{-1})k_1^{-1}g^{-1}k_2 g.$$

Koeficient u 1_G je roven

$$\frac{1}{|K|^2} \sum_{k, gkg^{-1} \in K} \chi(k)\chi(gk^{-1}g^{-1}) = \frac{1}{|K|^2} \sum_{k, g^{-1}kg \in K} \chi([k, g]^{-1}) = \frac{|K \cap K^g|}{|K|^2} \neq 0,$$

proto $e(\chi)(e(\chi) \cdot g) \neq 0$. Jelikož

$$\varepsilon(K, H) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})} \sigma e(\chi)$$

a $\varepsilon(K, H)$ je z Tvrzení 28 primitivní centrální idempotent $\mathbb{Q}K$, tak různé $\sigma e(\chi)$ jsou ortogonální a $\sigma e(\chi) = e(\chi)$ pro $\sigma = \mathrm{id}_{\mathbb{Q}(\chi)} \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$. Proto

$$\begin{aligned} e(\chi)\varepsilon(K, H)\varepsilon(K, H)^g(e(\chi) \cdot g) &= e(\chi)\varepsilon(K, H)g^{-1}\varepsilon(K, H)g(g^{-1}e(\chi)g) \\ &= e(\chi)\varepsilon(K, H)g^{-1}\varepsilon(K, H)e(\chi) \cdot g \\ &= e(\chi)(e(\chi)g) \neq 0 \end{aligned}$$

a $\varepsilon(K, H)\varepsilon(K, H)^g \neq 0$. Tudíž z $(SS3)$ plyne, že $g \in N_G(H)$. Díky podmínce $(SS1)$ platí, že $[K, g] \subseteq K$. Pak z $[K, g] \subseteq H$ plyne, že $\langle K, g\rangle/H$ je abelovská grupa a z $(SS2)$ leží g v K.

Jelikož (K, H) je Shodův pár, tak z Důsledku 32 plyne, že χ^G je nerozložitelný charakter. Proto z Věty 34 máme

$$e_{\mathbb{Q}}(\chi^G) = \frac{[\mathrm{Cen}_G(\varepsilon(K,H)) : K]}{[\mathbb{Q}(\chi) : \mathbb{Q}(\chi^G)]} e(G,K,H),$$

ale zároveň $e(G,K,H)$ je idempotent. Takže $e_{\mathbb{Q}}(\chi^G) = e(G,K,H)$ a proto $e(G,K,H)$ je primitivní centrální idempotent $\mathbb{Q}G$.

□

Tvrzení 41. *Nechť (K,H) je pár podgrup konečné grupy G, který splňuje tyto podmínky:*

- $H \trianglelefteq K \trianglelefteq G$;
- *K/H je cyklická grupa a maximální abelovská podgrupa $N_G(H)/H$.*

Pak (K,H) je silný Shodův pár a tedy $e(G,K,H)$ je primitivní centrální idempotent $\mathbb{Q}G$.

Důkaz. Podmínky $(SS1)$ a $(SS2)$ jsou zjevně splněné. Zbývá dokázat podmínku $(SS3)$. Nechť $g \in G \setminus N_G(H)$. Z Tvrzení 39 plyne, že $N_G(H) = \mathrm{Cen}_G(\varepsilon(K,H))$, a platí, že $\varepsilon(K,H)^g = \varepsilon(K^g, H^g) = \varepsilon(K, H^g)$. Pak K/H^g je cyklická grupa a $\varepsilon(K,H^g)$ je z Tvrzení 28 primitivní centrální idempotent $\mathbb{Q}K$, stejně jako $\varepsilon(K,H)$. A protože $g \in G \setminus N_G(H)$, tak $\varepsilon(K,H^g)$ a $\varepsilon(K,H)$ jsou dva rozdílné primitivní centrální idempotenty v $\mathbb{Q}K$ a tak jejich součin je 0.

□

Důsledek 42. *Nechť G je konečná grupa. Pokud $K = G$, pak (G,H) je silný Shodův pár právě tehdy, když $H \trianglelefteq G$ a G/H je cyklická grupa.*

Toto tvrzení lze najít v Olivieri and Ángel Del [2003] jako Tvrzení 2.1 a je zde uvedeno kvůli příkladům níže.

Tvrzení 43. *Nechť G' je derivovaná grupa grupy G a $G' \leq H \leq K$, pak (K,H) je Shodův pár právě tehdy, když $K = G$ a G/H je cyklická grupa. Pak je (G,H) silný Shodův pár a $e(G,G,H) = \varepsilon(G,H)$.*

Příklad 44. Mějme opět grupu kvaternionů Q_8. Chceme spočítat idempotenty pomocí Shodových párů. Grupa Q_8 má 5 konjugačních tříd, takže hledáme 5 centrálních primitivních idempotentů. Derivovaná grupa Q_8' je $\{e, \overline{e}\}$. Mějme podgrupy:

$$H_1 = \{e, \overline{e}, i, \overline{i}\},$$
$$H_2 = \{e, \overline{e}, j, \overline{j}\},$$
$$H_3 = \{e, \overline{e}, k, \overline{k}\}.$$

Pak $Q_8/H_m \simeq C_2$ pro každé $m \in \{1,2,3\}$, takže z tvrzení výše plyne, že (Q_8, H_1), (Q_8, H_2), (Q_8, H_3) jsou silné Shodovy páry. Stejně tak podle stejného tvrzení je

(Q_8, Q_8) silný Shodův pár. Našli jsme tedy idempotenty:

$$\begin{aligned}
\varepsilon(Q_8, Q_8) &= \widehat{G} = \frac{1}{8}(e + \overline{e} + i + \overline{i} + j + \overline{j} + k + \overline{k}) \\
\varepsilon(Q_8, H_1) &= \prod_{M/H_1 \in \mathcal{M}(Q_8/H_1)} (\widehat{H_1} - \widehat{M}) \\
&= \widehat{H_1} - \widehat{Q_8} \\
&= \frac{1}{4}(e + \overline{e} + i + \overline{i}) - \frac{1}{8}(e + \overline{e} + i + \overline{i} + j + \overline{j} + k + \overline{k}) \\
&= \frac{1}{8}(e + \overline{e} + i + \overline{i} - j - \overline{j} - k - \overline{k}) \\
\varepsilon(Q_8, H_2) &= \frac{1}{8}(e + \overline{e} + j + \overline{j} - i - \overline{i} - k - \overline{k}) \\
\varepsilon(Q_8, H_3) &= \frac{1}{8}(e + \overline{e} + k + \overline{k} - i - \overline{i} - j - \overline{j}).
\end{aligned}$$

Poslední idempotent spočítáme pomocí čtyř předchozích:

$$1 - \varepsilon(Q_8, Q_8) - \varepsilon(Q_8, H_1) - \varepsilon(Q_8, H_2) - \varepsilon(Q_8, H_3) = 1 - \tfrac{1}{2}(e + \overline{e}).$$

Vidíme, že první čtyři idempotenty dokážeme jednoduše pomocí Tvrzení 28 propojit s charaktery z výpočtu pomocí charakterů v Příkladu 27.

Trochu zajímavější je případ posledního idempotentu. Jelikož grupa Q_8 je nilpotentní (a tedy monomiální), tak existuje lineární charakter χ_K nějaké podgrupy K takový, že $\chi_K^{Q_8} = \chi_5$. Chceme tedy najít, jak vypadá původní charakter χ_K, respektive reprezentace $\varphi_K : K \to \mathbb{C}$, kde K je podgrupa grupy Q_8. Z Tvrzení 30 víme, že $\deg_{\mathbb{C}}(\varphi_K^{Q_8}) = [Q_8 : K] \deg_{\mathbb{C}}(\varphi_K)$.

My víme, že $\deg_{\mathbb{C}}(\varphi_K^{Q_8}) = 2$ (z Příkladu 27) a $\deg_{\mathbb{C}}(\varphi_K) = 1$ (jelikož to je lineární charakter), takže $[Q_8 : K] = 2$, proto hledáme $|K| = 4$. Ze vzorce pro výpočet indukovaného charakteru

$$\chi_K^{Q_8}(e) = \frac{1}{|K|} \sum_{x \in G} \chi_K(xex^{-1})$$

je vidět, že $\chi_K(e) = 1$ a $\chi_K(\overline{e}) = -1$. Zvolíme $\chi_K(i) = i$ a $\chi_K(\overline{i}) = -i$. Pak

$$\begin{aligned}
\chi_K^{Q_8}(i) &= 0, \\
\chi_K^{Q_8}(j) &= 0, \\
\chi_K^{Q_8}(k) &= 0,
\end{aligned}$$

takže $\chi_K^{Q_8} = \chi_5$ a $K = \{e, \overline{e}, i, \overline{i}\}$. Označíme $H = \{e\}$. Z Věty 34 plyne, že

$$e_{\mathbb{Q}}(\chi_K^{Q_8}) = \frac{[\mathrm{Cen}_{Q_8}(\varepsilon(K, H)) : K]}{[\mathbb{Q}(\chi) : \mathbb{Q}(\chi^{Q_8})]} e(Q_8, K, H),$$

je primitivní centrální idempotent, který odpovídá Shodovu páru (K, H). Jelikož $\mathrm{Cen}_G(\varepsilon(K, H)) = Q_8$ a $[\mathbb{Q}(\chi_K) : \mathbb{Q}(\chi_K^{Q_8})] = 2$, tak

$$e_{\mathbb{Q}}(\chi_K^{Q_8}) = e(G, K, H) = \varepsilon(K, H) = 1 - \tfrac{1}{2}(e + \overline{e}).$$

Příklad 45. Mějme dihedrální grupu $D_{12} = \langle a, b : a^6 = b^2 = 1, bab = a^{-1}\rangle$. Nejdříve spočítáme idempotenty $\mathbb{Q}D_{12}$ pomocí Shodových párů a pak to porovnáme s charaktery grupy D_{12}.

Konjugační třídy D_{12}: $\{e\}, \{a^3\}, \{a, a^5\}, \{a^2, a^4\}, \{b, a^2b, a^4b\}, \{ab, a^3b, a^5b\}$, proto hledáme 6 idempotentů. První silný Shodův pár je triviální pár (D_{12}, D_{12}). Podgrupy $H_1 = \{e, a^2, a^4, b, a^2b, a^4b\}$, $H_2 = \{e, a^2, a^4, ab, a^3b, a^5b\}$, $\mathbb{Z}_6 \simeq \langle a\rangle$ jsou normální grupy a jejich faktorgrupy jsou izomorfní $\mathbb{Z}_2$, tedy cyklické grupy. Podle Tvrzení 41 se jedná o silný Shodův pár. Z Tvrzení 41 plyne, že další silný Shodův pár je $(\langle a\rangle, Z(D_{12}) = \langle a^3\rangle)$. Tím už jsme našli 5 idempotentů:

$$\begin{aligned}
\varepsilon(D_{12}, D_{12}) &= \widehat{D_{12}} \\
&= \frac{1}{12}(e + a + a^2 + a^3 + a^4 + a^5 + b + ab + a^2b + a^3b + a^4b + a^5b), \\
\varepsilon(D_{12}, H_1) &= \widehat{H_1} - \widehat{D_{12}} \\
&= \frac{1}{12}(e - a + a^2 - a^3 + a^4 - a^5 + b - ab + a^2b - a^3b + a^4b - a^5b), \\
\varepsilon(D_{12}, H_2) &= \widehat{H_2} - \widehat{D_{12}} \\
&= \frac{1}{12}(e - a + a^2 - a^3 + a^4 - a^5 - b + ab - a^2b + a^3b - a^4b + a^5b), \\
\varepsilon(D_{12}, \langle a\rangle) &= \widehat{\langle a\rangle} - \widehat{D_{12}} \\
&= \frac{1}{12}(e + a + a^2 + a^3 + a^4 + a^5 - b - ab - a^2b - a^3b - a^4b - a^5b), \\
\varepsilon(\langle a\rangle, Z(D_{12})) &= \widehat{Z(D_{12})} - \widehat{\langle a\rangle} \\
&= \frac{1}{6}(2e - a - a^2 + 2a^3 - a^4 - a^5).
\end{aligned}$$

Poslední idempotent dopočítáme jako doplněk:

$$\begin{aligned}
&1 - \varepsilon(D_{12}, H_1) - \varepsilon(D_{12}, H_2) - \varepsilon(D_{12}, \langle a\rangle) - \varepsilon(\langle a\rangle, Z(D_{12})) \\
&= 1 - (\frac{1}{6}(4e - a + a^2 + 2a^3 + a^4 - a^5)) \\
&= \frac{1}{6}(6e - 4e + a - a^2 - 2a^3 - a^4 + a^5) \\
&= \frac{1}{6}(2e + a - a^2 - 2a^3 - a^4 + a^5).
\end{aligned}$$

Nyní se podíváme na tabulku charakterů. První charakter je triviální, další tři odvodíme z faktu, že faktorové grupy podgrup $H_1, H_2, \langle a\rangle$ jsou cyklické grupy, a proto udávají lineární reprezentaci, ve kterých jsou $H_1, H_2, \langle a\rangle$ jádra.

char/hodnoty	e	a^3	a, a^5	a^2, a^4	b, a^2b, a^4b	ab, a^3b, a^5b
χ_{triv}	1	1	1	1	1	1
χ_{H_1}	1	-1	-1	1	1	-1
χ_{H_2}	1	-1	-1	1	-1	1
$\chi_{\langle a\rangle}$	1	1	1	1	-1	-1
χ_4	?	?	?	?	?	?
χ_5	?	?	?	?	?	?

Jelikož pro stupně reprezentací platí, že

$$\begin{aligned}|D_{12}| &= \deg_{\mathbb{C}}(\chi_{H_1})^2 + \deg_{\mathbb{C}}(\chi_{H_2})^2 + \deg_{\mathbb{C}}(\chi_{\langle a\rangle})^2 + \deg_{\mathbb{C}}(\chi_4)^2 + \deg_{\mathbb{C}}(\chi_5)^2 \\ &= 4 + \deg_{\mathbb{C}}(\chi_4)^2 + \deg_{\mathbb{C}}(\chi_5)^2,\end{aligned}$$

tak $\deg_{\mathbb{C}}(\chi_4) = \deg_{\mathbb{C}}(\chi_5) = 2$. Z Tvrzení 21 použitého na χ_4, χ_5 a Tvrzení 20 použitého na 1. a 2. sloupec plyne, že $\chi_4(a^3) = \pm 2$ a $\chi_5(a^3) = \mp 2$. Zvolíme, že $\chi_4(a^3) = 2$ a $\chi_5(a^3) = -2$. Zároveň z Tvrzení 21 plyne, že $\chi_4(b) = \chi_5(b) = \chi_4(ab) = \chi_5(ab) = 0$, takže máme tabulku charakterů:

char/hodnoty	e	a^3	a, a^5	a^2, a^4	b, a^2b, a^4b	ab, a^3b, a^5b
χ_{triv}	1	1	1	1	1	1
χ_{H_1}	1	-1	-1	1	1	-1
χ_{H_2}	1	-1	-1	1	-1	1
$\chi_{\langle a\rangle}$	1	1	1	1	-1	-1
χ_4	2	2	?	?	0	0
χ_5	2	-2	?	?	0	0

Z Tvrzení 21 použitého na charakter χ_4, χ_5 plyne, že

$$\begin{aligned}\chi_4(\{a, a^5\}) &= \pm 1, \\ \chi_5(\{a, a^5\}) &= \pm 1, \\ \chi_4(\{a^2, a^4\}) &= \pm 1, \\ \chi_5(\{a^2, a^4\}) &= \pm 1.\end{aligned}$$

Z Tvrzení 20 použitého na 2., 3. a 4. sloupec určíme znaménka a máme výslednou tabulku charakterů:

char/hodnoty	e	a^3	a, a^5	a^2, a^4	b, a^2b, a^4b	ab, a^3b, a^5b
χ_{triv}	1	1	1	1	1	1
χ_{H_1}	1	-1	-1	1	1	-1
χ_{H_2}	1	-1	-1	1	-1	1
$\chi_{\langle a\rangle}$	1	1	1	1	-1	-1
χ_4	2	2	-1	-1	0	0
χ_5	2	-2	1	-1	0	0

Opět jsou první čtyři charaktery spojeny se Shodovými páry pomocí Tvrzení 28. D_{12} je monomiální grupa, takže každý nerozložitelný charakter je indukovaný lineárním charakterem nějaké její podgrupy. Shodův pár $(\langle a\rangle, Z(D_{12}))$ odpovídá charakteru χ_4, který je indukovaný charakter lineárního charakteru podgrupy $\langle a\rangle$ s jádrem $Z(D_{12})$. Charakter χ_5 je indukovaný charakter lineárního charakteru podgrupy $\langle a\rangle$ s jádrem e, takže odpovídá Shodově párů $(\langle a\rangle, e)$. Že $(\langle a\rangle, e)$ je silný Shodův pár, opět potvrzuje Tvrzení 41.

3.2 Idempotenty $\mathbb{F}_q G$

V této kapitole se zobecní využití (silných) Shodových párů pro konečná tělesa. Nejdřív je definován prvek $\varepsilon_{\mathcal{C}}(K, H)$ a další nutné pojmy. V prvním tvrzení

této kapitoly je tento prvek propojen s primitivním centrálním idempotentem v $\mathbb{F}G$ pro jednoduchý případ konečné abelovské grupy G. Tvrzení 47 tento postup zobecňuje pro libovolnou konečnou grupu G. Následuje popis konjugace prvku $\varepsilon_{\mathcal{C}}(K,H)$ a technické tvrzení, jež potřebujeme k Tvrzení 49, které popisuje propojení prvku $\varepsilon(K,H)$ z předchozí části kapitoly a $\varepsilon_{\mathcal{C}}(K,H)$. Kapitola končí Větou 50, která popisuje použití silných Shodových párů pro nalezení centrálních primitivních idempotentů $\mathbb{F}G$ a popisuje i to, jak souvisí s centrálními primitivními idempotenty $\mathbb{Q}G$.

Nechť $\mathbb{F}_q$ je konečné těleso s q prvky a G je konečná grupa řádu n taková, že $\gcd(q,n)=1$, tedy $\mathbb{F}_qG$ je totálně rozložitelný okruh.

Mějme pár podgrup (K,H) grupy G, který splňuje podmínky $(S1)$ a $(S2)$, pak $\mathrm{Irr}(K/H)$ značí množinu nerozložitelných charakterů K/H do algebraického uzávěru $\overline{\mathbb{F}_q}$. Pokud $[K:H]=m$, tak ξ_m značí m-tou primitivní odmocninu z 1 v $\overline{\mathbb{F}_q}$ a pak Galoisova grupa $\mathrm{Gal}(\mathbb{F}_q(\xi_m)/\mathbb{F}_q)$ přirozeně působí na množinu $\mathrm{Irr}(K/H)$. Orbity tohoto působení nazveme q-cyklotomické třídy. Jako $\mathcal{C}_q(K/H)$ označíme ty q-cyklotomické třídy, které obsahují generátory $\mathrm{Irr}(K/H)$, což jsou věrné reprezentace. Pokud nebude řečeno jinak, tak budeme q v názvech pro zjednodušení vynechávat a předpokládat, že $\mathbb{F}G$ je totálně rozložitelný okruh.

Definice 15. *Nechť $T/\mathbb{F}$ je Galoisovo rozšíření těles a $x \in T$, pak*

$$\mathrm{tr}(x) = \sum_{\sigma \in \mathrm{Gal}(T/K)} \sigma(x)$$

je stopa *tohoto rozšíření.*

Nechť $\mathcal{C} \in \mathcal{C}_q(K/H)$ a $\chi \in \mathcal{C}$, pak definujeme

$$\varepsilon_{\mathcal{C}}(K,H) = \frac{1}{|K|}\sum_{k\in K} \mathrm{tr}(\chi(kH))k^{-1},$$

$$e_{\mathcal{C}}(G,K,H) = \text{součet všech rozdílných G-konjugací } \varepsilon_{\mathcal{C}}(K,H),$$

kde tr je stopa Galoisova rozšíření $\mathbb{F}_q(\xi_m)/\mathbb{F}_q$. Proto

$$\varepsilon_C(K,H) = \frac{1}{|K|}\sum_{k\in K} \mathrm{tr}(\chi(kH))k^{-1} = \frac{1}{|K|}\sum_{k\in K}\sum_{\sigma\in \mathrm{Gal}(\mathbb{F}_q(\xi_m)/\mathbb{F}_q)} (\sigma(\chi(kH)))k^{-1}.$$

Prvek $\varepsilon_{\mathcal{C}}(K,H)$ můžeme také upravit díky tomu, že hodnoty koeficientů jsou u rozkladových tříd stejné a celá grupa K je disjunktní sjednocení tříd:

$$\begin{aligned}\varepsilon_C(K,H) &= \frac{1}{|K:H|}\frac{1}{|H|}\sum_{h\in H} h \sum_{x\in K/H} \mathrm{tr}(\chi(x))x_K^{-1} \\ &= \frac{1}{|K:H|}\widehat{H}\sum_{x\in K/H} \mathrm{tr}(\chi(x))x_K^{-1},\end{aligned}$$

kde x_K je reprezentant prvku x v K. Z tohoto zápisu vidíme, že $\varepsilon_{\mathcal{C}}(K,H)$ leží v $\mathbb{F}K\widehat{H}$.

Připomeňme, že pokud je G abelovská grupa, pak každý charakter χ této grupy je lineární. Plyne to z faktu, že počet nerozložitelných reprezentací je roven počtu konjugačních tříd a zároveň $|G| = \sum_{i\in I} d_i^2$, kde d_i jsou stupně nerozložitelných reprezentací.

Tvrzení 46. *Nechť G je konečná abelovská grupa a $\mathbb{F}$ je konečné těleso takové, že $\mathbb{F}G$ je totálně rozložitelný okruh. Buď $N \trianglelefteq G$ taková, že G/N je cyklická grupa, a $\mathcal{C} \in \mathcal{C}(G/N)$. Pak $\varepsilon_{\mathcal{C}}(G,N)$ je primitivní centrální idempotent $\mathbb{F}G$ a každý primitivní centrální idempotent má tento tvar, který je jednoznačně určen podgrupou N a $\mathcal{C} \in \mathcal{C}(G/N)$.*

Důkaz. Buď e primitivní centrální idempotent $\mathbb{F}G$, pak existuje nerozložitelný charakter χ grupy G takový, že $e = e(\chi)$, jako primitivní centrální idempotent v $\overline{F}G$. Jelikož G je abelovská grupa, tak χ je lineární. Vezměme $N = \ker(\chi)$ a charakter $\overline{\chi}$ cyklické grupy G/N takový, že $\overline{\chi}(\overline{g}) = \chi(g)$. Potom $\overline{\chi}$ je věrný charakter grupy G/N, který patří do nějaké cyklotomické třídy $\mathcal{C}$, jež leží v $\mathcal{C}_q(K/H)$. Potom z Věty 23 a Věty 26 máme

$$\begin{aligned} e_{\mathbb{F}}(\chi) &= \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}(\chi)/\mathbb{F})} \sigma e(\chi) \\ &= \frac{1}{|G|} \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}(\chi)/\mathbb{F})} \sum_{g \in G} \sigma\chi(g) g^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}(\chi)/\mathbb{F})} \sigma\chi(g) g^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}(\chi(g)) g^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}(\overline{\chi}(\overline{g})) g^{-1} \\ &= \varepsilon_{\mathcal{C}}(G,N). \end{aligned}$$

Nechť N_1, N_2 jsou dvě normální podgrupy grupy G takové, že G/N_i je cyklická grupa, $\chi_i \in \mathcal{C}_i \in \mathcal{C}_q(G/N_i)$ a $\varepsilon_{\mathcal{C}_1}(G,N_1) = \varepsilon_{\mathcal{C}_2}(G,N_2)$. Chceme dokázat, že $\mathcal{C}_1 = \mathcal{C}_2$ a $N_1 = N_2$. Vezměme $\overline{\chi_i} = \chi_i \circ \pi_i$, kde $\pi_i : G \twoheadrightarrow G/N_i$ je projekce. Pak z výpočtu výše platí, že

$$e_{\mathbb{F}}(\overline{\chi_1}) = \varepsilon_{\mathcal{C}_1}(G,N_1) = \varepsilon_{\mathcal{C}_2}(G,N_2) = e_{\mathbb{F}}(\overline{\chi_2}).$$

Jelikož pro $\sigma \in \mathrm{Gal}(\mathbb{F}(\overline{\chi_1})/\mathbb{F})$ platí, že $\sigma(e_{\mathbb{F}}(\overline{\chi_1})) = e_{\mathbb{F}}(\overline{\chi_1})$, tak $\mathbb{F}(\overline{\chi_1}) = \mathbb{F}(\overline{\chi_2})$. Navíc $\overline{\chi_1} = \sigma\overline{\chi_2}$ pro nějaké $\sigma \in \mathrm{Gal}(\mathbb{F}(\overline{\chi}_1)/\mathbb{F})$, jelikož $e_{\mathbb{F}}(\overline{\chi_1}) = e_{\mathbb{F}}(\overline{\chi_2})$. A díky tomu, že χ_1, χ_2 jsou věrné reprezentace, platí $N_1 = N_2$. Z definice cyklotomické třídy plyne, že $\mathcal{C}_1 = \mathcal{C}_2$.

□

Tvrzení 47. *Nechť $N \trianglelefteq G$ a G/N je cyklická grupa, $\mathcal{C} \in \mathcal{C}(G/N)$. Potom $\varepsilon_{\mathcal{C}}(G,N)$ je primitivní centrální idempotent $\mathbb{F}G$ a pokud $\mathcal{D} \in \mathcal{C}(G/N)$, pak*

$$\varepsilon_{\mathcal{C}}(G,N) = \varepsilon_{\mathcal{D}}(G,N)$$

právě tehdy, když $\mathcal{D} = \mathcal{C}$.

Důkaz. Máme izomorfismus $\phi : \mathbb{F}G\widehat{N} \simeq \mathbb{F}(G/N)$ indukovaný projekcí $G \to G/N$. Jelikož prvek $\varepsilon_{\mathcal{C}}(G,N)$ leží v $\mathbb{F}G\widehat{N}$, tak na něj můžeme použít ϕ:

$$\phi(\varepsilon_{\mathcal{C}}(G,N)) = \varepsilon_{\mathcal{C}}(G/N,1)$$

a $\varepsilon_{\mathcal{C}}(G/N, 1)$ je z předchozího tvrzení primitivní centrální idempotent $\mathbb{F}(G/N)$, proto $\varepsilon_{\mathcal{C}}(G, N)$ je primitivní centrální idempotent $\mathbb{F}G\widehat{N}$. Jelikož $\widehat{N}$ je centrální idempotent a $\widehat{N}\varepsilon_{\mathcal{C}}(G, N) = \varepsilon_{\mathcal{C}}(G, N)$ je primitivní centrální idempotent $\mathbb{F}G\widehat{N}$, tak můžeme použít Tvrzení 25 a toho plyne, že $\varepsilon_{\mathcal{C}}(G, N)$ je primitivní centrální idempotent v $\mathbb{F}G$ a $\varepsilon_{\mathcal{C}}(G, N) = \varepsilon_{\mathcal{D}}(G, N)$ právě tehdy, když $\mathcal{C} = \mathcal{D}$, díky Tvrzení 46.

□

Nechť K je podgrupa grupy G s lineárním charakterem χ a $\ker(\chi) = H$. Mějme $g \in G$, pak můžeme definovat χ^g jako $\chi^g(h) = \chi(ghg^{-1})$ pro $h \in K^g$ (jedná se o speciální případ pro Definici 11 a Tvrzení 29). Potom $\ker(\chi^g) = H^g$. Proto zobrazení $\chi \to \chi^g$ definuje bijekci mezi lineárními charaktery K s jádrem H a lineárními charaktery K^g s jádrem H^g. Toto zobrazení indukuje bijekci mezi $\mathcal{C}_q(K/H)$ a $\mathcal{C}(K^g/H^g)$, obraz $\mathcal{C} \in \mathcal{C}(K/H)$ označíme jako $\mathcal{C}^g$. Pak platí

$$\varepsilon_{\mathcal{C}}(K, H)^g = \varepsilon_{\mathcal{C}^g}(K^g, H^g).$$

Mějme $H \trianglelefteq K \leq G$ takové, že K/H je cyklická grupa, a $N = N_G(H) \cap N_G(K)$, N pak působí na prvky v $\mathcal{C}(K/H)$ jako popsáno výše. Nechť $g \in N$ stabilizuje q-cyklotomickou třídu $\mathcal{C} \in \mathcal{C}(K/H)$, tedy $\mathcal{C}^g = \mathcal{C}$, a $\chi \in \mathcal{C}$. Pro každé $k \in K$ platí

$$\begin{aligned}\chi^g(kH) &= \chi(gkHg^{-1}) \\ &= \chi(gkg^{-1}H).\end{aligned}$$

A zároveň

$$\begin{aligned}\chi^g(kH) &= \sigma\chi(kH), \qquad \text{jelikož } \mathcal{C}^g = \mathcal{C}, \\ &= \chi(kH)^n \\ &= \chi((k^nH)),\end{aligned}$$

kde $\sigma \in \mathrm{Gal}(\mathbb{F}(\xi_{[K:H]})/\mathbb{F})$ a $n \in \mathbb{N}$ je takové, že $\sigma(\xi_{[K:H]}) = \xi_{[K:H]}^n$. A jelikož χ je věrná reprezentace, tak $gkg^{-1} = k^n$ a tedy g stabilizuje i jakoukoli jinou cyklotomickou třídu $\mathcal{C}$. Takže stabilizátory různých cyklotomických tříd při této akci jsou jedna stejná množina a tu označíme jako $E_G(K/H)$.

Tvrzení 48. *Nechť $H \trianglelefteq K \leq G$ a K/H je cyklická grupa, $\mathcal{C} \in \mathcal{C}(K/H)$.*

1. *Následující tvrzení jsou ekvivalentní pro $x \in G$:*

   (i) $x \in H$,

   (ii) $x\varepsilon_{\mathcal{C}}(K, H) = \varepsilon_{\mathcal{C}}(K, H)$,

   (iii) $\widehat{x}\varepsilon_{\mathcal{C}}(K, H) = \varepsilon_{\mathcal{C}}(K, H)$.

2. *Pokud $K \trianglelefteq N_G(H)$, pak* $\mathrm{Cen}_G(\varepsilon_{\mathcal{C}}(K, H)) = E_G(K, H)$.

Důkaz. Důkaz je analogický důkazu Tvrzení 39 a lze jej najít v [Broche and Río, 2007].

□

Nechť p je prvočíselný dělitel q a $\mathbb{Z}_{(p)}$ je lokalizace $\mathbb{Z}$ v p. Pak $\mathbb{F}_p \simeq \mathbb{Z}_{(p)}/m$, kde

m je maximální ideál, a $\overline{x} \in \mathbb{F}_p$ je obraz $x \in \mathbb{Z}_{(p)}$ a toto značení rozšíříme na projekci $\mathbb{Z}_{(p)}G$ do $\mathbb{F}_pG$.

Všimněme si, že pro Shodův pár (K, H) leží $\varepsilon(K, H)$ v $\mathbb{Z}_{(p)}G$ a tedy tam leží i $e(G, K, H)$. Proto je $\overline{\varepsilon(K, H)}$ idempotent v $\mathbb{F}_pG$ a pokud je (K, H) silný Shodův pár, tak $\overline{e(G, K, H)}$ je centrální idempotent v $\mathbb{F}_pG$.

Tvrzení 49. *Nechť (K, H) je silný Shodův pár grupy G, pak*

$$\overline{\varepsilon(K, H)} = \sum_{\mathcal{C} \in \mathcal{C}(K/H)} \varepsilon_{\mathcal{C}}(K, H),$$

a existuje množina R taková, že

$$\overline{e(G, K, H)} = \sum_{\mathcal{C} \in R} e_{\mathcal{C}}(G, K, H).$$

Důkaz. Jelikož $\varepsilon(K, H)$ i $\varepsilon_{\mathcal{C}}(K, H)$ leží v $\mathbb{F}K\widehat{H} \simeq \mathbb{F}(K/H)$, tak můžeme uvažovat, že $H = 1$ a tedy K je cyklická grupa. Z Tvrzení 46 víme, že každý primitivní centrální idempotent $\mathbb{F}K$ má tvar $\varepsilon_{\mathcal{C}}(K, H)$, kde H je libovolná podgrupa K (protože K již je cyklická) a $\mathcal{C} \in \mathcal{C}(K/H)$. Z Tvrzení 24 plyne, že $\overline{\varepsilon(K, 1)}$ je idempotent a tedy je součtem $\varepsilon_{\mathcal{C}_i}(K, H_i)$ pro nějaké podgrupy H_i a $\mathcal{C}_i \in \mathcal{C}_q(K/H_i)$. Proto stačí dokázat, že $\overline{\varepsilon(K, 1)}\varepsilon_{\mathcal{C}}(K/H) \neq 0$, pro $H \leq K$ a $\mathcal{C} \in \mathcal{C}(K/H)$, právě tehdy, když $H = 1$.
Nechť $H = 1$, vezměme $1 \neq x \in K$, pak z předchozího tvrzení plyne, že

$$(1 - \widehat{x})\varepsilon_{\mathcal{C}}(K, 1) \neq 0.$$

Jelikož $(1 - \widehat{x})$ je také idempotent, tak $(1 - \widehat{x})\varepsilon_{\mathcal{C}}(K, 1) = \varepsilon_{\mathcal{C}}(K, 1)$. Ale $\overline{\varepsilon(K, 1)}$ je přesně součinem prvků tvaru $(1 - \widehat{x})$. Tedy $\overline{\varepsilon(K, 1)}\varepsilon_{\mathcal{C}}(K, 1) \neq 0$.
Naopak, nechť $1 \neq H \leq G$, pak existuje $h \in H$ takové, že $\langle h \rangle$ je minimální grupa grupy K, tedy $1 - \widehat{h}$ je jeden ze součinů v $\varepsilon(K, 1)$. Ale zároveň $(1 - \widehat{h})\varepsilon_{\mathcal{C}}(K, H) = 0$ z předchozího tvrzení, tedy $\overline{\varepsilon(K, 1)}\varepsilon_{\mathcal{C}}(K, H) = 0$.

Nechť $N = N_G(H) \cap N_G(K) = N_G(H)$, jelikož $K \trianglelefteq N_G(H)$, a $E = E_G(K/H)$, T_N je pravá transverzála N v G a T_E je pravá transverzála E v N. Pak $\{hg : h \in T_E, g \in T_N\}$ je pravá transverzála E v G. Z Tvrzení 39 víme, že $N = \mathrm{Cen}_G(\varepsilon(K, H))$ a proto $e(G, K, H) = \sum_{t \in T_N} e(K, H)^t$. Když necháme N působit na $\mathcal{C}(K/H)$, tak

$$\mathcal{C}(K/H) = \dot{\bigcup}_{C \in R} \{C^t : t \in T_E\},$$

kde R je množina reprezentantů akce grupy N na $\mathcal{C}(K/H)$. Následně rozepíšeme z definice $\overline{e(G, K, H)}$:

$$\begin{aligned}
\overline{e(G, K, H)} &= \sum_{g \in T_N} \overline{\varepsilon(K, H)^g} \\
&= \sum_{g \in T_N} \sum_{\mathcal{C} \in \mathcal{C}(K/H)} \varepsilon_{\mathcal{C}}(K, H)^g, && \text{z první části tvrzení,} \\
&= \sum_{g \in T_N} \sum_{\mathcal{C} \in R} \sum_{t \in T_E} \varepsilon_{\mathcal{C}^t}(K, H)^g, && \text{díky rozkladu popsanému výše,} \\
&= \sum_{\mathcal{C} \in R} \sum_{g \in T_N} \sum_{t \in T_E} \varepsilon_{\mathcal{C}}(K, H)^{tg}, && \text{prohodíme pořadí součtu,} \\
&= \sum_{\mathcal{C} \in R} e_{\mathcal{C}}(G, K, H), && \text{díky Tvrzení 46,}
\end{aligned}$$

a tím je důkaz hotov.

□

Věta 50. *Nechť G je konečná grupa a $\mathbb{F}$ konečné těleso takové, že $\mathbb{F}G$ je totálně rozložitelný okruh.*

- *Buď (K, H) silný Shodův pár a $\mathcal{C} \in \mathcal{C}(K/H)$. Pak $e_{\mathcal{C}}(G, K, H)$ je primitivní centrální idempotent $\mathbb{F}G$.*
- *Buď X množinou silných Shodových párů grupy G. Když je každý primitivní centrální idempotent $\mathbb{Q}G$ tvaru $e(G, K, H)$ pro nějaký pár $(K, H) \in X$, tak je každý primitivní centrální idempotent $\mathbb{F}G$ tvaru $e_{\mathcal{C}}(G, K, H)$ pro nějaký pár $(K, H) \in X$ a nějaké $\mathcal{C} \in \mathcal{C}(K/H)$.*

Důkaz. Nechť $E = E_G(K/H)$, pak z Tvrzení 48 víme, že $\mathrm{Cen}_G(\varepsilon_{\mathcal{C}}(K, H)) = E$ a nechť T je pravá transverzála E v G. Pak

$$e_{\mathcal{C}}(G, K, H) = \sum_{t \in T} \varepsilon_{\mathcal{C}}(K, H)^t.$$

Z Tvrzení 39 víme, že $N_G(H) = \mathrm{Cen}_G(\varepsilon(K, H))$. Chceme dokázat, že

$$\varepsilon_{\mathcal{C}}(K, H)\varepsilon_{\mathcal{C}}(K, H)^t = 0$$

pro $t \in G \setminus E$. Jelikož $\varepsilon_{\mathcal{C}}(K, H)$ i $\overline{\varepsilon(K, H)}$ leží v $\mathbb{F}K$, kde $\varepsilon_{\mathcal{C}}(K, H)$ je primitivní centrální idempotent, a

$$\overline{\varepsilon(K, H)} = \sum_{\mathcal{C} \in \mathcal{C}(K/H)} \varepsilon_{\mathcal{C}}(K, H).$$

Proto

$$\varepsilon_{\mathcal{C}}(K, H)\varepsilon_{\mathcal{C}}(K, H)^t = \varepsilon_{\mathcal{C}}(K, H)\overline{\varepsilon(K, H)\varepsilon(K, H)^t}\varepsilon_{\mathcal{C}}(K, H)^t.$$

Pokud $t \in G \setminus N_G(H)$, tak z definice silného Shodova páru $\overline{\varepsilon(K, H)\varepsilon(K, H)^t} = 0$, proto $\varepsilon_{\mathcal{C}}(K, H)\varepsilon_{\mathcal{C}}(K, H)^t = 0$.
Nechť $t \in N_G(H) \setminus E$. Pak $\varepsilon_{\mathcal{C}}(K, H)^t = \varepsilon_{\mathcal{C}^t}(K, H)$, ale protože $t \notin E$, tak $\varepsilon_{\mathcal{C}^t}(K, H)$ a $\varepsilon_{\mathcal{C}}(K, H)$ jsou z Tvrzení 47 dva různé primitivní centrální idempotenty v $\mathbb{F}K$ a tedy jejich součin je 0.

Z předpokladu existuje podmnožina Y množiny X taková, že $\{e(G, K, H) : (K, H) \in Y\}$ je kompletní množina primitivních centrální idempotentů $\mathbb{Q}G$. Pak $\{\overline{e(G, K, H)} : (K, H) \in X\}$ je kompletní množina ortogonálních centrálních idempotentů, které ale nemusí být primitivní. Pak podle předchozí části tvrzení a Tvrzení 49 je $\{e_{\mathcal{C}}(G, K, H) : (K, H) \in X, \mathcal{C} \in R\}$ množina primitivních centrálních idempotentů $\mathbb{F}G$, kde R je množina z předchozího tvrzení.

□

4. Idempotenty pomocí ideálů okruhu

Tato kapitola vychází z článku de Melo Hernández et al. [2020]. V tomto článku je definován soubor ideálů splňující CNC-podmínky a je popsáno, jak se dá využít ke zvedání idempotentů v grupovém okruhu RG, kde G a R jsou komutativní. V této kapitole se díky Tvrzení 56 rozšíří použití této techniky i na grupové okruhy RG, kde R je komutativní, G ale nemusí být, a je nastíněno, jak by se dalo pokračovat i pro nekomutativní okruh R. Pokud nebude řečeno jinak, tak budeme uvažovat oboustranné ideály.

První tvrzení popisuje známý způsob zvedání idempotentů pro nilpotentní ideál N. Věta 52 ukazuje, že pokud jsou splněné podmínky centrality, tak je zvednutý idempotent určený jednoznačně. Tvrzení 53, 54, 55 popisují, jak se zachovávají vlastnosti primitivnosti, ortogonality a součtu. Tvrzení 56 je důležité a ukazuje, proč a jak centrální idempotent $\overline{f}$ v RG/NG můžeme zapsat jako $f+NG$, kde f je centrální, což je potřeba v následujících důkazech. Věta 57 je technická a ukazuje, jak lze při určitých podmínkách zvednutý idempotent spočítat jednodušeji. Definice 16 zavádí systém CNC ideálů, který zobecňuje nilpotentní ideál. Věta 58 popisuje, jak lze idempotenty zvedat pomocí systému CNC ideálů. Tvrzení 59 propojuje CNC ideály R s CNC ideály RG. Věta 60 spojuje výsledky 56 a Věty 58 a ukazuje, jak je použít na grupový okruh. Tvrzení 61 je technické a využije se na Tvrzení 62, což vede k důsledku 63. Ten se využije na konkrétní případ grupového okruhu Z_mG ve Větě 64. Důsledek 65 použije výsledky kapitoly na popis idempotentů RG pro R komutativní artinovský okruh. Nakonec Věta 60 ukazuje, jak se jinak může popsat centrum RG a jak to lze využít pro hledání centrálních idempotentů, což je ukázáno v příkladu na konci kapitoly.

Tvrzení 51. *Nechť N je nil oboustranný ideál okruhu R a $\overline{R} = R/N$. Buď $\overline{f} = f + N$ idempotent okruhu $\overline{R}$, pro nějaké f v R. Pak existuje $e \in R$ takové, že e je idempotent okruhu R a zároveň $\overline{e} = \overline{f}$. Navíc pokud f je centrální, pak umíme nalézt e centrální.*

Důkaz. Jelikož $\overline{f}$ je idempotent v $\overline{R}$, tak i $\overline{1-f}$ je idempotent v $\overline{R}$ a $\overline{f}+\overline{1-f} = \overline{1}$. Proto $f - f^2 = f(1-f) \in N$ a pak existuje $s \in \mathbb{N}$ takové, že $f^s(1-f)^s = 0$, jelikož N je nilpotentní. Zároveň platí, že

$$\overline{f}^s + (\overline{1-f})^s = \overline{1},$$

definujme $w := 1 - f^s - (1-f)^s \in N$. Tedy existuje $k \in \mathbb{N}$ takové, že $w^k = 0$. Pak má $1 - w$ inverzní prvek

$$t := (1 + w + w^2 + \cdots + w^{k-1}).$$

Takže

$$1 = tf^s + t(1-f)^s$$

a

$$tf^s = (tf^s)^2 + tf^s t(1-f)^s.$$

Jelikož t komutuje s f^s a $f^s(1-f)^s = 0$, tak je druhý člen roven nule a našli jsme idempotent. Navíc

$$\overline{tf^s} = \overline{(1 + w + w^2 + \cdots + w^{k-1})f^s} = \overline{f},$$

takže tf^s je hledaný prvek e. Z jeho konstrukce vyplývá, že pokud f je centrální, tak i e je centrální.

□

Věta 52. *Buď R okruh a N je jeho nil ideál. Pokud $\overline{f}$ je centrální idempotent R/N a e, f jsou centrální idempotenty v R takové, že $e + N = f + N = \overline{f}$, pak $e = f$.*

Důkaz. Nechť $f = e + n$ je také idempotent, kde $n \in N$. Pak z $(e+n)^2 = (e+n)$ a centrality e máme, že $(1-2e)n = n^2$. Tudíž $n^3 = (1-2e)n^2 = (1-2e)^2 n$ a indukcí máme $n^{k+1} = (1-2e)^k n$. Ale $(1-2e)^2 = 1 - 4e + 4e = 1$, takže $n = 0$, jelikož $n \in N$ a N je nilpotentní, a $e + n = e$.

□

Poznámka. Nechť $\overline{f} = f + N$ je centrální idempotent, f je centrální prvek. Pak e získaný algoritmem z důkazu Tvrzení 51 je centrální a podle předchozí věty je jednoznačně určený, budeme jej nazývat *zvednutým idempotentem* a značit jako e_f.

Tvrzení 53. *Pokud $\overline{f} = f + N$ je primitivní centrální idempotent v R/N, pro N nil ideál a f centrální, pak i e_f je primitivní centrální idempotent okruhu R.*

Důkaz. Nechť $\overline{f}$ je primitivní centrální idempotent a e_f není primitivní. Pak $e_f = g + h$, kde g, h jsou centrální idempotenty. Tedy $\overline{f} = \overline{e_f} = \overline{g} + \overline{h}$ a musí platit, že buď $g \in N$, nebo $h \in N$. Ale jelikož N je nilpotentní, tak buď $g = 0$, nebo $h = 0$, což je spor.

□

Tvrzení 54. *Pokud $\overline{f_1} = f_1 + N, \overline{f_2} = f_2 + N$ jsou ortogonální centrální idempotenty v R/N, kde N je nil ideál a f_1, f_2 centrální, pak i e_{f_1} a e_{f_2} jsou ortogonální centrální idempotenty v R.*

Důkaz. Jelikož $\overline{0} = \overline{f_1 f_2} = e_{f_1} e_{f_2} + N$, tak $e_{f_1} e_{f_2} \in N$, ale zároveň $e_{f_1} e_{f_2}$ je centrální idempotent, tedy musí být roven 0.

□

Tvrzení 55. *Pokud $\sum_{i \in I} \overline{f_i} = \sum_{i \in I} f_i + N = 1 + N$, kde $\overline{f_i}$ jsou ortogonální centrální idempotenty v R/N, kde R je okruh a N nil ideál, pak $\sum_{i \in I} e_{f_i} = 1$.*

Důkaz. Z definice e_{f_i} platí, že $\sum_{i\in I} \overline{f_i} = \sum_{i\in I} e_{f_i} + N = 1 + N$, takže $1 - \sum_{i\in I} e_{f_i} \in N$. Jelikož $\overline{f_i}$ byly ortogonální idempotenty, pak z předchozího tvrzení víme, že e_{f_i} jsou ortogonální idempotenty a tedy $1 - \sum_{i\in I} e_{f_i}$ je idempotent ležící v nilpotentním ideálu N, tedy $1 - \sum_{i\in I} e_{f_i} = 0$.

□

Následující tvrzení umožňuje zobecnit tvrzení z článku de Melo Hernández et al. [2020], bez větších úprav důkazů, a dále popsaná metoda zvedání centrálních idempotentů funguje díky tomu pro větší skupinu grupových okruhu RG.

Tvrzení 56. *Nechť R je komutativní okruh a G je konečná grupa, N nilpotentní ideál okruhu R. Nechť $\overline{f} = f + NG$ je centrální idempotent faktorového grupového okruhu $RG/NG \simeq (R/N)G$. Pak f umíme najít centrální v RG a e_f je pak centrální idempotent.*

Důkaz. Nechť $\overline{f}$ je centrální idempotent $RG/NG \simeq (R/N)G$, pak

$$\overline{f} = \sum_{g\in G} \overline{r_g} g$$

a podle Důsledku 9 platí, že koeficienty jsou konstantní na konjugačních třídách grupy G. Zvolme $r_g \in T$, kde T je transverzála N v R, aby

$$\overline{f} = \sum_{g\in G} (r_g + N) g,$$

pak $\overline{f} = \sum_{g\in G} (r_g g + Ng)$, tedy $f = \sum_{g\in G} r_g g$. A opět jsou koeficienty konstantní na konjugačních třídách grupy G. Tudíž f je centrální v RG. Z Tvrzení 51 plyne, že e_f je centrální.

□

Věta 57. *Nechť R je okruh a N je nilpotentní oboustranný ideál s indexem $t \geq 2$ v R a existuje přirozené číslo $s \geq 2$ takové, že $sN = 0$ a všechny prvočíselné činitele s jsou větší nebo rovny indexu t. Pokud $\overline{f} = f + N$ je centrální idempotent okruhu R/N, f je centrální, a e_f je zvednutý centrální idempotent v R, pak*

- *pro libovolné prvočíslo p takové, že $p \geq t$, a pro všechna $n \in N$ existuje $r \in R$ takové, že*

$$(e_f + n)^p = e_f + pnr,$$

- $e_f = f^s$.

Důkaz. Jelikož $n^t = 0$ a $p \geq t$, tak

$$\begin{aligned}(e_f + n)^p &= \sum_{j=0}^{p} \binom{p}{j} e_f^{p-j} n^j \\ &= e_f + \sum_{j=1}^{t-1} \binom{p}{j} e_f n^j \\ &= e_f + p \sum_{j=1}^{t-1} c_j e_f n^j \\ &= e_f + pnr,\end{aligned}$$

kde $c_j = \dfrac{\binom{p}{j}}{p}$ a $r = \sum_{j=1}^{t-1} c_j e_f n^{j-1}$.

Nechť $\{p_1, \ldots, p_m\}$ jsou prvočísla z prvočíselného rozkladu s. Z předpokladu máme, že $\overline{f} = \overline{e_f}$, tedy $f = e_f + n$, pro nějaké $n \in N$. Pak z předchozí části důkazu máme, že

$$f^{p_1} = (e_f + n)^{p_1} = e_f + p_1 n r_1.$$

Ale $p_1 n r_1 \in N$, takže tvrzení můžeme použít znovu.

$$f^{p_1 p_2} = (e_f + p_1 r n)^{p_2} = e_f + p_2 p_1 n r_1 r_2.$$

Takto získáme

$$f^s = f^{p_1 p_2 \cdots p_m} = e_f + s n r_1 r_2 \ldots r_m = e_f,$$

jelikož $s = p_m \ldots p_2 p_1$, $n r_1 r_2 \ldots r_m \in N$ a $sN = 0$.

□

Definice 16. *Řekneme, že soubor $\{N_1, N_2, \ldots, N_k\}$ oboustranných ideálů okruhu R* splňuje CNC-podmínky*, pokud*

(CNC1) $\{0\} = N_k \subset N_{k-1} \subset \cdots \subset N_1 \subset R$,

(CNC2) pro $i = 1, 2, \ldots, k-1$ *existuje celé číslo* $t_i \geq 2$ *takové, že* $N_i^{t_i} \subset N_{i+1}$,

(CNC3) pro $i = 1, 2, \ldots, k-1$ *existuje celé číslo* $s_i \geq 1$ *takové, že* $s_i N_i \subset N_{i+1}$, *navíc všechny prvočíselné činitele* s_i *jsou větší nebo rovny* t_i.

Nejmenší t_i z definice budeme nazývat index nilpotence ideálu N_i nad N_{i+1} a nejmenší s_i z definice nazveme charakteristikou ideálu N_i v N_{i+1}.

Podmínka $(CNC2)$ je ekvivalentní s tím, že pro každé $i = 1, 2, \ldots, k-1$ je N_i/N_{i+1} nilpotentní ideál s indexem t_i v R/N_{i+1}. Podmínka $(CNC3)$ je ekvivalentní s tím, že pro libovolné $i = 1, 2, \ldots, k-1$ existuje s_i takové, že $s(N_i/N_{i+1}) = 0$ v R/N_{i+1}.

Věta 58. *Nechť R je okruh a $\{N_1, N_2, \ldots, N_k\}$ je soubor oboustranných ideálů R, který splňuje CNC-podmínky a s_i je charakteristika N_i nad N_{i+1}. Nechť $f_1 + N_1$, $f_2 + N_1$ jsou centrální idempotenty R/N_1, kde f_1, f_2 jsou centrální.*

- *Pak*

$$f_1^{s_1 s_2 \dots s_{k-1}}$$

je centrální idempotent okruhu R.

- *Pokud $f_1 + N_1$ je primitivní centrální idempotent R/N_1, pak i*

$$f_1^{s_1 s_2 \dots s_{k-1}}$$

je primitivní centrální idempotent R.

- *Pokud $f_1 + N_1$, $f_2 + N_1$ jsou ortogonální centrální idempotenty R/N_1, pak*

$$f_1^{s_1 s_2 \dots s_{k-1}}, f_2^{s_1 s_2 \dots s_{k-1}}$$

jsou ortogonální centrální idempotenty R.

- *Nechť $\{f_1 + N_1, f_2 + N_1, \dots, f_k + N_1\}$ je kompletní množina ortogonálních primitivních centrálních idempotentů R/N_1, kde $f_1, f_2, \dots, f_k$ jsou centrální, pak*

$$\{f_1^{s_1 s_2 \dots s_{k-1}}, f_2^{s_1 s_2 \dots s_{k-1}}, \dots, f_k^{s_1 s_2 \dots s_{k-1}}\}$$

je kompletní množina ortogonálních primitivních centrálních idempotentů v R.

Důkaz. Nechť $f_1 + N_1$ je centrální idempotent R/N_1, pak

$$R/N_1 \simeq \frac{R/N_2}{N_1/N_2}$$

a $(f_1+N_2)+(N_1/N_2)$ je centrální idempotent $\dfrac{R/N_2}{N_1/N_2}$. Jelikož N_1/N_2 je nilpotentní ideál v R/N_2 s indexem t_1 a charakteristikou s_1, tak z předchozí věty víme, že $f_1^{s_1} + N_2$ je centrální idempotent v R/N_2. Obdobně můžeme pokračovat dál pro libovolné $i = 3, \dots, k-1$:

$$f_1^{s_1 s_2 \dots s_i} + N_{i+1}$$

je centrální idempotent v R/N_{i+1}. Dojdeme až k N_k:

$$f_1^{s_1 s_2 \dots s_{k-1}} + N_k = f_1^{s_1 s_2 \dots s_{k-1}}$$

je centrální idempotent v $R/N_k = R$. Tím jsme dokázali první část věty. Zbylé tři části se dokážou analogicky, pouze v dalších krocích použijeme postupně Tvrzení 53, Tvrzení 54 a pro poslední část Tvrzení 55.

□

Tvrzení 59. *Nechť R je komutativní okruh a $\{N_1, N_2, \dots, N_k\}$ je soubor ideálů R, který splňuje CNC-podmínky, G je konečná grupa. Pak $\{N_1G, N_2G, \dots, N_kG\}$ je soubor oboustranných ideálů okruhu RG splňující CNC podmínky.*

Důkaz. Podmínka $(CNC1)$ je splněna z definice N_iG. Mějme $i \in \{1, 2, \ldots, k-1\}$, pak $(N_iG)^{t_i} = N_i^{t_i}G$ a proto $(N_iG)^{t_i} \subset N_{i+1}G$. Podobně pro s_i z podmínky $(CNC3)$: $s_i(N_iG) = (s_iN_i)G$ a proto $s_i(N_iG) \subset N_{i+1}G$.

□

Věta 60. *Nechť R je komutativní okruh a G je konečná grupa, $\{N_1, N_2, \ldots, N_k\}$ je soubor ideálů okruhu R, který splňuje CNC-podmínky, s_i je charakteristika N_i nad N_{i+1} a T je transverzála N_1 v R. Buď $\overline{f} = \sum_{g\in G} \overline{r_g}g$ (primitivní) centrální idempotent okruhu $(R/N_1)G$. Zvolme $r_g \in T, g \in G$ tak, že*

$$\overline{f} = \sum_{g\in G}(r_g + N)g$$

a definujme $f = \sum_{g\in G} r_g g$. Pak

$$f^{s_1 s_2 \ldots s_{k-1}}$$

je (primitivní) centrální idempotent grupového okruhu RG.

Důkaz. Důkaz je spojením důkazu Tvrzení 56, Věty 58 a Tvrzení 59.

□

Tvrzení 61. *Nechť R je okruh a N je nilpotentní ideál s indexem $k \geq 2$ a $s > 1$ je charakteristika okruhu R/N. Pak soubor $\{N, N^2, N^3, \ldots, N^k\}$ ideálů splňuje CNC-podmínky, pro $i = 1, 2, \ldots, k-1$ je $t_i = 2$ a $s_i = s$.*

Důkaz. První podmínka je splněna díky tomu, že N je nilpotentní. Nechť $t_i = 2$ pro každé $i = 1, 2, \ldots, k-1$, pak $(N_i)^{t_i} = (N^i)^2 = N^{2i} \subset N^{i+1}$. Definujme $s_i = s$ pro každé $i = 1, 2, \ldots, k-1$. Jelikož $s(1_R + N) = 0$, tak existuje $n \in N$ takové, že $s1_R = n$, takže $s(N^i) = s1_R(N^i) = n(N^i) \subset N^{i+1}$. A proto, že $t_i = 2$ a $s_i \geq 2$, tak všechny prvočíselné činitele s_i jsou větší nebo rovny t_i.

□

Tvrzení 62. *Nechť R je okruh a N je jeho nilpotentní oboustranný ideál s indexem k v R, s je konečná charakteristika R/N. Pokud $f + N$ je (primitivní) centrální idempotent okruhu R/N, kde f je centrální, pak*

$$f^{s^{k-1}}$$

je (primitivní) centrální idempotent okruhu R.

Důkaz. Z předchozího tvrzení víme, že $\{N, N^2, N^3, \ldots, N^k\}$ je soubor ideálů splňující CNC-podmínky v okruhu R. Můžeme tedy použít Větu 58 a máme, že $f^{s^{k-1}}$ je centrální idempotent R.

□

Důsledek 63. *Nechť R je komutativní okruh a a nilpotentní prvek v R s indexem k, G je konečná grupa, s charakteristika okruhu $R/\langle a\rangle$. Pokud $f+\langle a\rangle G$ je centrální idempotent v $(R/\langle a\rangle)G$, pak*

$$f^{s^{k-1}}$$

je centrální idempotent RG.

Mějme okruh $\mathbb{Z}_{p^k}$, kde p je nějaké prvočíslo a $k > 1$ přirozené číslo. Pak p je nilpotentní prvek v $\mathbb{Z}_{p^k}$ s indexem k a $\mathbb{Z}_{p^k}/\langle p\rangle \simeq \mathbb{Z}_p$.

Věta 64. *Nechť G je konečná grupa a $p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ je prvočíselný rozklad čísla $m \geq 2$. Položme $m_i = m/p_i^{r_i}$ a s_i je takové přirozené číslo, že*

$$s_i m_i \equiv 1 \ mod\ p_i^{r_i}$$

pro $i = 1, 2, \ldots, k$. Pokud $\overline{f_i}$ je centrální idempotent grupového okruhu $\mathbb{Z}_{p_i}G$ pro $i = 1, 2, \ldots, k$ a definujeme $\alpha_i = p_i^{r_i-1}$, pak

$$e = s_1m_1f_1^{\alpha_1} + s_2m_2f_2^{\alpha_2} + \cdots + s_km_kf_k^{\alpha_k}$$

je centrální idempotent okruhu $\mathbb{Z}_mG$.

Důkaz. Z Čínské věty o zbytcích máme, že $\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$ a proto

$$\mathbb{Z}_mG \simeq_\phi \mathbb{Z}_{p_1^{r_1}}G \times \mathbb{Z}_{p_2^{r_2}}G \times \cdots \times \mathbb{Z}_{p_k^{r_k}}G$$

Pokud $\overline{f_i}$ je centrální idempotent $\mathbb{Z}_{p_i}G$ pro každé $i = 1, 2, \ldots, k$, pak podle Důsledku 63 a poznámky před touto větou víme, že $f_i^{\alpha_i}$ je centrální idempotent $\mathbb{Z}_{p_i^{r_i}}$. Pak

$$(f_1^{\alpha_1}, f_2^{\alpha_2}, \ldots, f_k^{\alpha_k})$$

je centrální idempotent $\mathbb{Z}_{p_1^{r_1}}G \times \mathbb{Z}_{p_2^{r_2}}G \times \cdots \times \mathbb{Z}_{p_k^{r_k}}G$, proto $\phi^{-1}((f_1^{\alpha_1}, f_2^{\alpha_2}, \ldots, f_k^{\alpha_k}))$ je centrální idempotent v $\mathbb{Z}_mG$, což můžeme pomocí Čínské věty o zbytcích vyjádřit tak, jako ve znění věty.

□

Důsledek 65. *Nechť R je komutativní artinovský okruh, pak $R \simeq_\phi \prod_{i=1}^{l} R_i$, kde R_i jsou lokální artinovské komutativní okruhy. Každý okruh R_i má právě jeden maximální ideál m_i, který je nilpotentní, jeho index označíme jako k_i a charakteristiku tělesa R_i/m_i označíme jako s_i.*

Pokud $f_i + m_iG$ je centrální idempotent grupového okruhu R_iG/m_iG pro $i = 1, 2, \ldots, l$, pak

$$\phi^{-1}(f_1^{s_1^{k_1-1}}, f_2^{s_2^{k_2-1}}, \ldots, f_l^{s_l^{k_l-1}})$$

je centrální idempotent okruhu RG.

Důkaz. První část věty o rozkladu komutativního artinovského okruhu je známé tvrzení, můžeme jej najít například v Passman [2004]. Druhá část plyne z Tvrzení 59, Tvrzení 61 a Tvrzení 62.

□

Nakonec díky Tvrzení 8 můžeme nastínit, jak lze tuto teorii využít pro nekomutativní okruhy R.

Věta 66. *Nechť R je nekomutativní okruh, G konečná grupa. Pak*

$$Z(RG) = Z(Z(R)G)$$

a ortogonální primitivní centrální idempotenty RG zjistíme tak, že předchozí věty použijeme pro $Z(R)G$.

Důkaz. Nechť má G konjugační třídy $C_1, C_2, \ldots, C_k$. Z Tvrzení 8 víme, že $Z(RG)$ je volný $Z(R)$-modul s bází $\{b_1, \ldots, b_k\}$, kde $b_i = \sum_{c \in C_i} c$. Jelikož $Z(R)$ je komutativní okruh, tak díky Důsledku 9 víme, že $Z(Z(R)G)$ je volný $Z(R)$-modul s bází $\{b_1, \ldots, b_k\}$. Tedy $Z(RG) = Z(Z(R)G)$.

□

Toto pozorování lze využít pro hledání idempotentů v RG, kde G je konečná grupa a R je konečný okruh, který je totálně rozložitelný. Dle Důsledku 17 víme, že

$$R \simeq_\varphi M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$$

pro nějaká komutativní konečná tělesa $D_1, \ldots, D_k$. Tedy podobně jako v Důsledku 65 můžeme najít jednotlivé primitivní centrální idempotenty pro grupové okruhy $M_{n_1}(D_1)G, \ldots, M_{n_k}(D_k)G$ a pomocí izomorfismu φ^{-1} je přenést do RG. Na hledání centrálních idempotentů v $M_{n_i}(D_i)G$ můžeme použít předchozí větu, tudíž nás zajímají centrální idempotenty v $Z(M_{n_i}(D_i))G$. Ale $Z(M_{n_i}(D_i))$ je tvořeno diagonálními maticemi s konstantním prvek v diagonále, tedy $Z(M_{n_i}(D_i)) \simeq D_i$. Takže stačí najít primitivní centrální idempotenty v D_iG pro každé i.

Příklad 67. Nechť $R = \mathrm{Gl}(\mathbb{Z}_9, 2)$ a $G = Q_8$. Pak

$$Z(R) \simeq \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in \mathbb{Z}_9\},$$

$$J(Z(R)) = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in 3\mathbb{Z}_3\},$$

a tak

$$Z(R)/J(Z(R)) \simeq \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in \mathbb{Z}_3\}.$$

Pokud najdeme centrální idempotent f v $(Z(R)/J(Z(R)))Q_8$, tak jej díky Tvrzení 62 dokážeme zvednout do $Z(R)Q_8$ a f bude centrální idempotent okruhu RQ_8. Transverzála $J(Z(R))$ v $Z(R)$ je

$$\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}.$$

$Z(R)/J(Z(R))$ je izomorfní konečnému komutativnímu tříprvkovému tělesu, označíme jej jako $\mathbb{F}_3$, proto můžeme použít výsledky předchozí Kapitoly 3.2, konkrétně Větu 50, k nalezení centrálních idempotentů.

K tomu potřebujeme (silné) Shodovy páry grupy Q_8, ty známe z Příkladu 44. Vezměme silný Shodův pár (Q_8, H_1), kde $H_1 = \{e, \overline{e}, i, \overline{i}\}$. Chceme spočítat $\varepsilon_{\mathcal{C}}(Q_8, H_1)$, podle úvodu v Kapitole 3.2 k tomu potřebujeme cyklotomickou třídu $\mathcal{C}(Q_8/H_1)$.
Podívejme se, jak vypadají $\mathrm{Irr}(Q_8/H_1)$, tedy nerozložitelné reprezentace Q_8/H_1 do algebraického uzávěru $\overline{\mathbb{F}}$. $Q_8/H_1 \simeq C_2$, kde C_2 značí cyklickou grupu řádu 2, proto jsou všechny reprezentace lineární a rovny svému charakteru. Označme jako $\overline{0}, \overline{1}$ dva prvky $Q_8/H_1 \simeq Z_2$. Pak máme tyto reprezentace:

$$\begin{aligned}
\text{triv: } \overline{0} &\longmapsto \overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}, \\
\overline{1} &\longmapsto \overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}, \\
\phi : \overline{0} &\longmapsto \overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}, \\
\overline{1} &\longmapsto \overline{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}}.
\end{aligned}$$

Tedy máme jednu cyklotomickou třídu $\mathcal{C}$ s prezentací ϕ. Jelikož $[Q_8 : H_1] = 2$ a druhá odmocnina z $\overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}$ je $\overline{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}}$ a tedy leží v $\mathbb{F}$, tak $\mathrm{Gal}(\mathbb{F}(\xi_2)/\mathbb{F})$ je triviální grupa. Nyní můžeme spočítat $\varepsilon_{\mathcal{C}}(Q_8, H_1)$:

$$\begin{aligned}
\varepsilon_{\mathcal{C}}(Q_8, H_1) &= \frac{1}{|Q_8|} \sum_{k \in Q_8} \mathrm{tr}(\chi(kH_1))k^{-1} \\
&= \frac{1}{2}\Big(\overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} e + \overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \overline{e} + \overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} i + \overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \overline{i} \\
&+ \overline{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}} j + \overline{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}} \overline{j} + \overline{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}} k + \overline{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}} \overline{k}\Big).
\end{aligned}$$

Jelikož všechny konjugace $\varepsilon_{\mathcal{C}}(Q_8, H_1)$ jsou rovny $\varepsilon_{\mathcal{C}}(Q_8, H_1)$, tak $\varepsilon_{\mathcal{C}}(Q_8, H_1)$ je primitivní centrální idempotent $\mathbb{F}Q_8$ podle Věty 50. Nyní můžeme použít Tvrzení 59 a Tvrzení 60 pro

$$\begin{aligned}
f_1 &= \Big(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} e + \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \overline{e} + \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} i + \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \overline{i} \\
&+ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} j + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \overline{j} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} k + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \overline{k} \\
&= \sum_{q \in Q_8} + \sum_{h \in H_1} .
\end{aligned}$$

Index $J(Z(R))$ v $Z(R)$ je 3 a charakteristika $Z(R)/J(Z(R))$ je také 3. Tedy

$$f_1^9$$

je primitivní centrální idempotent $Z(R)Q_8$. Pomocí skriptu napsaným v Pythonu, který je připojen jako Příloha A.1, lze spočítat, že

$$f_1^9 = \sum_{q\in Q_8} +7 \sum_{h\in H_1}$$

a ověřit, že f_1^9 je skutečně idempotent v $Z(R)Q_8$.
Primitivní idempotenty f_2, f_3 pro silné Shodovy páry (Q_8, H_2) a (Q_8, H_3), kde $H_2 = \{e, \overline{e}, j, \overline{j}\}, H_3 = \{e, \overline{e}, k, \overline{k}\}$, získáme analogicky:

$$f_2 = \sum_{q\in Q_8} + \sum_{h\in H_2} ,$$
$$f_3 = \sum_{q\in Q_8} + \sum_{h\in H_3} .$$

A pak

$$f_2^9 = \sum_{q\in Q_8} +7 \sum_{h\in H_2} ,$$
$$f_3^9 = \sum_{q\in Q_8} +7 \sum_{h\in H_3} .$$

jsou primitivní idempotenty $Z(R)Q_8$. Pak máme silný Shodův pár (Q_8, Q_8), Q_8/Q_8 je triviální grupa, která má pouze triviální charakter. Tedy

$$\begin{aligned}\varepsilon_{\mathcal{C}}(Q_8, Q_8) &= \frac{1}{|Q_8|}\sum_{k\in Q_8} \mathrm{tr}(\chi(kQ_8))k^{-1} \\ &= \frac{1}{2}(\overline{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}e + \overline{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}\overline{e} + \overline{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}i + \overline{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}\overline{i} \\ &+ \overline{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}j + \overline{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}\overline{j} + \overline{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}k + \overline{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}\overline{k}).\end{aligned}$$

Proto

$$f_4 = 2\sum_{g\in Q_8} g$$

a f_4^9 je primitivní idempotent okruhu $Z(R)Q_8$. Skript v příloze A.1 spočítal, že

$$f_4^9 = 8\sum_{g\in Q_8} g$$

a ověřil, že se jedná o idempotent v $Z(R)Q_8$.
Poslední idempotent dopočítáme jako

$$\begin{aligned}1 - f_1^9 - f_2^9 - f_3^9 - f_4^9 &= 1 - (\sum_{q\in Q_8} +7\sum_{h\in H_1} + \sum_{q\in Q_8} +7\sum_{h\in H_2} + \sum_{q\in Q_8} +7\sum_{h\in H_3} +8\sum_{q\in Q_8}) \\ &= 1 - (2\sum_{q\in Q_8} +7\sum_{h\in H_1} +7\sum_{h\in H_2} +7\sum_{h\in H_3}) \\ &= 1 - (5(e+\overline{e})) \\ &= 1 + 4(e+\overline{e}).\end{aligned}$$

5. Obecný případ

Poslední kapitola se snaží o řešení případu, kde KG není totálně rozložitelný okruh. Nejdříve jsou sepsána známá tvrzení o grupách a ideálech v grupových okruzích. Důsledek 73 popisuje triviální případ pro G konečnou p-grupu a K těleso charakteristiky p. Cliffordova věta je uvedena kvůli důkazu Tvrzení 75, které popisuje Jakobsonův radikál KG. Z toho plyne Tvrzení 76, které se snaží trochu popsat zvedání idempotentů v konkrétním případě nerozložitelného grupového okruhu KG. Následuje diskuze, proč tento postup nejde jedním konkrétním způsobem zobecnit. Nakonec je spočítán příklad, proč Tvrzení 76 nelze zjednodušit.

Nechť K je konečné těleso charakteristiky p, kde p je prvočíslo (tedy $\mathbb{F}_{p^n}$), a G je konečná grupa taková, že $\mathrm{char}(K) \mid |G|$, tedy existuje k takové, že $|G| = p^k m$, kde $m \neq 0 \in \mathbb{N}$ a $p \nmid m$.

Následující tři tvrzení můžeme najít v [Milies César Polcino a Sehgal, 2002].

Věta 68. *Nechť G je konečná grupa a p je prvočíslo. Pokud $p^k \mid |G|$, pak G obsahuje podgrupu řádu p^k.*

Tvrzení 69. *Nechť H je podgrupa G, pak $\omega H = \langle 1 - h; h \in H \rangle$ je ideál právě tehdy, když H je normální podgrupa a pak platí, že*

$$K(G/H) \simeq KG/\omega H.$$

Pokud bychom chtěli použít výsledky z předchozí kapitoly, tak nás zajímá, kdy bude ωP nilpotentní ideál, zvlášť v případě, kdy P je normální p-grupa a K má charakteristiku p. Bylo by pěkné, pokud by v takovém případě ωP byla nilpotentní grupa, bohužel tomu tak nemusí být.

Tvrzení 70. *Nechť R je artinovský okruh, pak $J(R)$ je nilpotentní.*

Tvrzení 71. *Nechť K je těleso a G je konečná grupa. Pak KG je artinovský okruh a tedy $J(KG)$ je nilpotentní ideál.*

Důkaz. Lze najít v [Passman, 1977] jako Theorem 1.1 v 10. kapitole. □

Tvrzení 72. *Nechť K je konečné těleso prvočíselné charakteristiky p a G je grupa, pak augmentační ideál $\Delta = \omega G$ je nilpotentní právě tehdy, když G je konečná p-grupa. Pak augmentační ideál a Jakobsonův ideál splývají.*

Důkaz. Toto tvrzení je v Passman [1977] uvedeno jako Lemma 1.6. □

Důsledek 73. *Nechť K je konečné těleso prvočíselné charakteristiky p a G je konečná p-grupa. Pak KG neobsahuje žádné netriviální idempotenty.*

Důkaz. Víme, že $J(KG)$ neobsahuje žádné idempotenty kromě 0 a zároveň je KG lokální, tedy $KG \setminus J(KG)$ je množina invertibilních prvků. Ale pokud x je invertibilní a zároveň idempotent, tak $1 = xx^{-1} = xxx^{-1} = x$.

□

Věta 74. *(Cliffordova věta) Nechť N je normální podgrupa konečné grupy G a S je jednoduchý KG-modul. Pak S má jako KN-modul jednoduchý podmodul W a existují $x_1, \ldots, x_m \in G$, $m \leq |G|$, že $S = \bigoplus_{i=1}^{m} Wx_i$, Wx_i jsou jednoduché KN-moduly.*

Důkaz. Tvrzení je v Passman [1977] jako Theorem 2.16 v 2. kapitole.

□

Následující tvrzení lze najít na [Rickard, 2016] i s diskuzí o důkazu.

Tvrzení 75. *Nechť G je konečná grupa a K těleso prvočíselné charakteristiky p, N je normální p-Sylowa podgrupa grupy G. Mějme homomorfismus $\phi : KG \to K(G/N)$ indukované projekcí $G \to G/N$. Pak Jakobsonův radikál $J(KG)$ je roven* $\ker(\phi)$.

Důkaz. Okruh $K(G/N)$ je totálně rozložitelný, tedy jeho Jakobsonův radikál $J(K(G/N))$ je roven nule. Zároveň $\phi(J(KG)) \subseteq J(K(G/N)) = 0$, tedy $J(KG) \subseteq \ker(\phi)$. Abychom dokázali opačnou inkluzi, tak ukážeme, že $\ker(\phi)$ anihiluje libovolný jednoduchý KG-modul. Pak $\ker(\phi) \subseteq J(KG)$, jelikož $J(KG)$ můžeme také definovat jako průnik všech anihilátorů jednoduchých KG-modulů.

Nechť S je jednoduchý KG-modul. Pak z Cliffordovy věty víme, že S je totálně rozložitelný KN-modul. Jelikož N je p-grupa, pak z Tvrzení 72 plyne, že KN je lokální okruh a maximální ideál je augmentační ideál Δ_{KN}. Pak libovolný jednoduchý KN-modul má tvar $KN/\Delta_{KN} \simeq K$. Tedy N působí na S triviálně, tzn. $ns = s$ pro každé $s \in S, n \in N$. Takže $\ker(\phi) = \omega N$ anihiluje S.

□

Tvrzení 76. *Nechť G je konečná grupa, $|G| = p^k m$, kde p je prvočíselná charakteristika konečného tělesa K a $p \nmid m$, $m \neq 0$. Nechť P je podgrupa grupy G řádu p^k, která je v G normální. Pokud $f + \omega P$ je primitivní centrální idempotent grupového okruhu $K(G/P)$, kde f je centrální, pak existuje přirozené číslo j takové, že f^{p^j} je primitivní centrální idempotent grupového okruhu KG. Pokud f není centrální, tak existuje idempotent $e \in KG$ takový, že $\overline{e} = \overline{f}$.*

Důkaz. Z předchozího tvrzení víme, že $J(KG) = \omega P$ a zároveň $J(KG)$ je nilpotentní ideál z Tvrzení 71. Pak z Tvrzení 61 a Tvrzení 62 plyne, že pokud $f + \omega P$ je primitivní centrální idempotent grupového okruhu $K(G/P) \simeq KG/J(KG)$, pak existuje přirozené číslo j takové, že f^{p^j} je primitivní centrální idempotent grupového okruhu KG, jelikož charakteristika okruhu $KG/J(KG)$ je rovna p. Druhá část věty plyne z Tvrzení 51.

□

Tvrzení 77. *Nechť G je konečná grupa a H je její normální podgrupa, $|G/H| = n$ a $n \neq 0$ v K. Pak*

$$J(KG) = J(KH)KG$$

a navíc $J(KG)$ je nilpotentní právě tehdy, když $J(KH)$ je nilpotentní.

Důkaz. Důkaz můžeme najít v Passman [1971] jako spojení Věty 16.6 a Lemma 16.8..

□

Člověka může napadnout, že by se výše popsaný postup dal zobecnit pomocí konečných řetězců vnořených podgrup. Mějme G konečnou grupu, $|G| = p^k m$, kde p je prvočíselná charakteristika konečného tělesa K a $p \nmid m$, $m \neq 0$. Nechť P je podgrupa grupy G řádu p^k, která není v normální v G, a nechť existuje konečná řada podgrup P_i grupy G:

$$P \lhd P_1 \lhd P_2 \lhd \cdots \lhd P_n \lhd G,$$

pak bychom mohli pomocí předchozího tvrzení najít Jakobsonův ideál. Nicméně tento případ nikdy nenastane, jak dokazuje následující tvrzení a toto zobecnění ve skutečnosti akorát jinak popisuje případ řešený v Tvrzení 76.

Tvrzení 78. *Nechť P je normální p-podgrupa grupy G a G je normální podgrupa H tak, že $p \nmid |H/G|$. Pak P je normální p-podgrupa grupy H.*

Důkaz. Nechť P je normální p-grupa grupy G, G je normální v H. Nechť Q je konjugace grupy P v grupě H. Pak Q je p-podgrupa grupy H, jelikož P je p-grupa v H a každá konjugace p-grupy je p-grupa, a QG/G je p-grupa v H/G. Ale $p \nmid |H/G|$, proto H/G nemá žádnou netriviální p-grupu, tedy $QG \subseteq G$, jinak řečeno $Q \subseteq G$. Ale jediná p-grupa v G je P, tedy $Q = P$. Dokázali jsme tedy, že každá konjugace P v H je rovna P, tedy P je normální v H.

□

Příklad 79. Na tomto příkladu ukážeme, že Tvrzení 76 skutečně musí odlišovat f centrální, f vždy nemusí být centrální. Mějme alternující grupu

$$A_4 = \langle a, b, c : a^2 = c^2 = b^3 = 1, bab^{-1} = ac = ca, bcb^{-1} = a \rangle$$

a konečné těleso $\mathbb{F}_2$. Chceme najít idempotenty grupového okruhu $\mathbb{F}_2 A_4$. Grupa A_4 má Kleinovu 2-podgrupu K, která je generovaná prvky a, c a izomorfní C_2^2, a $A_4/K \simeq C_3 = \langle \bar{b} \rangle$. Protože nyní počítáme idempotenty grupového okruhu s cyklickou grupou, tak můžeme použít výsledky Příkladu 13. Jelikož

$$x^3 - 1 = (x - 1)(x^2 + x + 1),$$

tak stačí najít jeden netriviální primitivní centrální idempotent $\mathbb{F}_2 C_3$. Grupa C_3, generovaná prvkem b, má silný Shodův pár $(C_3, \{e\})$. Chceme najít $\varepsilon_{\mathcal{C}}(C_3, \{e\})$, podle úvodu v Kapitole 3.2, k tomu potřebujeme cyklotomickou třídu $\mathcal{C}(C_3/\{e\})$.

Podívejme se, jak vypadají $\mathrm{Irr}(C_3/\{e\})$, tedy nerozložitelné reprezentace $C_3/\{e\}$ do algebraického uzávěru $\overline{\mathbb{F}_2}$. $C_3/\{e\} \simeq C_3$ a máme reprezentace:

$$\begin{aligned}
\text{triv: } e &\longmapsto 1,\\
c &\longmapsto 1,\\
c^2 &\longmapsto 1,\\
\phi_1 : e &\longmapsto 1,\\
c &\longmapsto \xi_3,\\
c^2 &\longmapsto \xi_3^2,\\
\phi_2 : e &\longmapsto 1,\\
c &\longmapsto \xi_3^2,\\
c^2 &\longmapsto \xi_3.
\end{aligned}$$

Tedy máme cyklotomickou třídu $\{\phi_1, \phi_2\}$ a Galoisovo rozšíření $\mathrm{Gal}(\mathbb{F}_2(\xi_3)/\mathbb{F}_2)$. Vezměme $\chi = \phi_1$. Pak $\mathrm{tr}(e) = 1+1 = 0$, $\mathrm{tr}(b) = \xi_3 + \xi_3^2 = 1$ a $\mathrm{tr}(b) = \xi_3^2 + \xi_3 = 1$. Proto

$$\varepsilon_{\mathcal{C}}(C_3, \{e\}) = b + b^2.$$

Ale b, b^2 netvoří uzavřenou třídu konjugací v A_4, tedy se nejedná o centrální prvek v $\mathbb{F}_2 A_4$.

Závěr

Práce popisuje způsoby, jak nalézt idempotenty v grupovém okruhu. První kapitola obsahuje základní definice a pojmy potřebné pro práci s grupovými okruhy. V druhé kapitole je popsán postup hledání idempotentů pomocí reprezentace grup v grupovém okruhu KG, nejdříve pro algebraicky uzavřené těleso K a pak i pro ne nutně algebraicky uzavřené těleso K, který je již znám od 70. let minulého století, teorie je sjednocená do jednotného značení a důkazy ze zdrojů jsou podrobněji rozepsané, nakonec jsou spočítané idempotenty pomocí tohoto postupu u grupového okruhu $\mathbb{Q}Q_8$ (Příklad 27). Třetí kapitola je kompilací několika článků s podrobněji rozepsanými důkazy z těchto článků a popisuje novější způsob hledání idempotentů pomocí Shodových párů grupy, je v ní přidaný důkaz pomocného technického Tvrzení 33 pro důkaz hlavní Věty 34 a jsou v ní spočítané idempotenty grupových okruhů $\mathbb{Q}Q_8$ (Příklad 44) a $\mathbb{Q}D_{12}$ (Příklad 45), výpočet je porovnaný s postupem uvedeným v druhé kapitole. Čtvrtá kapitola obsahuje největší obsah vlastní práce autorky a je založena na článku de Melo Hernández et al. [2020] z roku 2020. Původní článek se zaměřoval na hledání idempotentů v komutativních okruzích pomocí zvedání idempotentů a na komutativních grupových okruzích, tedy RG pro R i G komutativní, výsledky ukazoval. Ve čtvrté kapitole je tento postup rozšířen na hledání centrálních idempotentů v grupových okruzích RG, kde G již nemusí být komutativní, a je naznačeno, jak by se dalo postupovat také pro R nekomutativní. Tvrzení 56 ukazuje, že pokud $\overline{f}$ je centrální prvek v $(R/N)G$, pak existuje takové centrální $f \in R$, že $\overline{f} = f + N$, a dokonce popisuje, jak takové f najdeme. Díky tomu se celý původní článek může pro grupové okruhy zobecnit i pro G nekomutativní grupu. Nakonec Věta 66 ukazuje souvislost mezi $Z(RG)$ a $Z(Z(R)G$ a tím nastiňuje, jak se předchozí výsledky dají použít i pro práci s nekomutativním okruhem R. To je využito na příkladu, kde jsou spočítané idempotenty grupového okruhu RG pro $R = \mathrm{Gl}(\mathbb{Z}_9, 2)$ a $G = Q_8$, tomuto výpočtu pomáhá krátký skript v Pythonu, přiložený jako příloha A.1. Poslední kapitola se snaží o řešení případu, kde KG není totálně rozložitelný okruh, je v ní popsán možný postup pro zvedání idempotentů v jednom konkrétním případě grupy G.

Literatura

Gurmeet K. Bakshi and Gurleen Kaur. Character triples and shoda pairs. *Journal of Algebra*, 491:447–473, 2017. doi: 10.1016/j.jalgebra.2017.08.016.

Gurmeet K. Bakshi and Gurleen Kaur. Semisimple finite group algebra of a generalized strongly monomial group. *Finite Fields and Their Applications*, 60:101571, 2019. doi: 10.1016/j.ffa.2019.07.001.

Osnel Broche and Ángel Del Río. Wedderburn decomposition of finite group algebras. *Finite Fields and Their Applications*, 13(1):71–79, 2007. doi: 10.1016/j.ffa.2005.08.002.

Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Pub., 2006.

Fernanda D. de Melo Hernández, César A. Hernández Melo, and Horacio Tapia-Recillas. On idempotents of a class of commutative rings. *Communications in Algebra*, 48(9):4013–4026, 2020. doi: 10.1080/00927872.2020.1754424.

Edgar G. Goodaire, Eric Jespers, and Miles César Polcino. *Alternative loop rings*. Elsevier, 1996.

Marinês Guerreiro. Group algebras and coding theory. *São Paulo Journal of Mathematical Sciences*, 10(2):346–371, 2016. doi: 10.1007/s40863-016-0040-x.

Eric Jespers, Guilherme Leal, and Antonio Paques. Central idempotents in the rational group algebra of a finite nilpotent group. *Journal of Algebra and Its Applications*, 02(01):57–62, 2003. doi: 10.1142/s0219498803000398.

Sudarshan K. Milies César Polcino a Sehgal. *An introduction to group rings*. Kluwer Academic Publishers, 2002.

Aurora Olivieri and Río Ángel Del. An algorithm to compute the primitive central idempotents and the wedderburn decomposition of a rational group algebra. *Journal of Symbolic Computation*, 35(6):673–687, 2003. doi: 10.1016/s0747-7171(03)00035-x.

Aurora Olivieri, Ángel Del Río, and Juan Jacobo Simón. On monomial characters and central idempotents of rational group algebras. *Communications in Algebra*, 32(4):1531–1550, 2004. doi: 10.1081/agb-120028797.

Donald S. Passman. *Infinite group rings*. M. Dekker, 1971.

Donald S. Passman. *A course in ring theory*. AMS Chelsea Pub., Providence, RI, 2004.

Ings Passman, Donald S. a Ings. *The Algebraic Structure of Group Rings* -. Wiley, New York, 1977. ISBN 978-0-471-02272-5.

Vera Pless, W. C. Huffman, and Richard A. Brualdi. *Handbook of coding theory*. Elsevier, 1998.

Jeremy Rickard. Computing the jacobson radical of $f[g]$ with $char(f) = p$ and g finite with a normal p-sylow subgroup, Oct 2016. URL https://math.stackexchange.com/questions/2049645/computing-the-jacobson-radical-of-fg-with-charf-p-and-g-finite-with-a?rq=1.

Toshihiko Yamada. *The schur subgroup of the Brauer group*. Springer, 1974.

A. Přílohy

A.1 Skript na spočítání idempotentů k Příkladu 67

```
from sympy import symbols
from sympy import collect
from sympy import Add
from sympy import simplify
from sympy import expand
h, q =symbols('h q')
z=2
a=expand((h+q)**2)
v=(h+q)
for z in [2, 3, 4, 5, 6, 7, 8, 9]:
    w=(h + q)*v
    a=expand(w)
    v=a.subs([(h**2, 4*h), (q**2, 8*q), (h*q, 4*q)])
    collected_h=collect(v, h)
    collected_q=collect(v, q)
    collected_hq=collect(v, h * q)
    koef_h=collected_h.coeff(h, 1)
    koef_q=collected_q.coeff(q, 1)
    koef_hq=collected_hq.coeff(h * q, 1)
    v=v.subs([(koef_q*q, (koef_q%9)*q), (koef_h*h, (koef_h%9)*h)])

w=expand(v**2)
w=w.subs([(h**2, 4*h), (q**2, 8*q), (h*q, 4*q)])
collected_h=collect(w, h)
collected_q=collect(w, q)
collected_hq=collect(w, h*q)
koef_h=collected_h.coeff(h, 1)
koef_q=collected_q.coeff(q, 1)
koef_hq=collected_hq.coeff(h*q, 1)
w=w.subs([(koef_q*q, (koef_q % 9)*q), (koef_h*h, (koef_h % 9)*h)])
if w==v:
    print("Ano")
else:
    print ("Ne")
print(v)
print(w)

v=2*q
for z in [2, 3, 4, 5, 6, 7, 8, 9]:
    w=(2*q)*v
    a=expand(w)
    v=a.subs([(q**2, 8*q)])
    collected_q = collect(v, q)
    koef_q=collected_q.coeff(q, 1)
    v=v.subs([(koef_q*q, (koef_q % 9)*q)])


w=v**2
w=w.subs([(q**2, 8*q)])
collected_q=collect(w, q)
```

```
koef_q=collected_q.coeff(q, 1)
w=w.subs([(koef_q*q, (koef_q % 9)*q)])
if w==v:
    print("Ano")
else:
    print("Ne")
print(v)
print(w)
```