Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE

Dominik Lachman

Idempotentní ideály v celočíselné grupové algebře symetrické grupy

Katedra algebry

Vedoucí bakalářské práce:	doc. Mgr. Pavel Příhoda, Ph.D.
Studijní program:	Matematika
Studijní obor:	Obecná matematika

Praha 2015

Rád bych poděkoval svému vedoucímu práce doc. Mgr. Pavlovi Příhodovi, Ph.D. za cenné rady a všechen čas, který mi věnoval.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

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 v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Idempotentní ideály v celočíselné grupové algebře symetrické grupy

Autor: Dominik Lachman

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D., Katedra algebry

Abstrakt: V této práci se zabývám hypotézou, že každý oboustranný idempotentní ideál v grupovém okruhu $\mathbb{Z}S_n$, generuje-li v $\mathbb{Q}S_n$ vlastní ideál, jedná se nutně o takzvaný augmentační ideál. Platnost hypotézy by dávala oslabenou verzi faktu, že v případě řešitelné grupy G, nemá $\mathbb{Z}G$ žádný vlastní oboustranný idempotentní ideál. Nejprve popíši jak idempotentní ideály v $\mathbb{Z}S_n$ spočítat, a následně provedu výpočet pro S_5 a S_7. V prvním případě bude hypotéza platit, v druhém však už nikoli. V teoretické části nejprve přejdu k lokálnímu pohledu a popíši idempotentní ideály v $\mathbb{Z}_{(p)}S_n$, pro p prvočísla dělící řád grupy S_n, jako stopové ideály projektivních $\mathbb{Z}_{(p)}S_n$-modulů. Dále se budu zabývat funktorem $- \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q} : Proj(\mathbb{Z}_{(p)}S_n) \to Mod(\mathbb{Q}S_n)$, ten popíši v řeči Grothendieckových grup maticí E. Matice E se ukáže býti transponovanou dekompoziční maticí, kterou umíme spočítat pomocí Braeurových charakterů.

Klíčová slova: reprezentace Symetrických grup, semiperfektní moduly, modulární reprezentace.

Title: Idempotent ideals in integral group rings

Author: Dominik Lachman

Department: Department of Algebra

Supervisor: doc. Mgr. Pavel Příhoda, Ph.D., Department of Algebra

Abstract: This thesis concerns following hyphotesis: whenever I is two-sided idempotent ideal in group ring $\mathbb{Z}S_n$, such that $I\mathbb{Q}$ is non-trivial ideal of $\mathbb{Q}S_n$, $I\mathbb{Q}$ has to be so called augmentation ideal. The vylidity of this hypothesis would give us weak version of the fact that in the case of solvable group G, there are no two-sided non-trivial idempotent ideals in $\mathbb{Z}G$. At first I desctibe methodt how to calculate idempotent ideals in $\mathbb{Z}S_n$ and then show that hypothesis holds in the case of S_5, but fail in the case of $\mathbb{Z}S_5$. In theoretic part, I firstly switch to local point of view and describe two-sided idempotent ideals in $\mathbb{Z}_{(p)}S_n$, for primes p dividing order of group S_n, as trace ideals of finitely generated projective $\mathbb{Z}_{(p)}S_n$-modules. Next, I describe functor $- \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q} : Proj(\mathbb{Z}_{(p)}S_n) \to Mod(\mathbb{Q}S_n)$ using the language of Grothendiecks groups by matrix E. Matrix E shows to be transposition of decomposition matrix, which we can calculate using Braeur's character.

Keywords: representations of symetric group, semiperfect modules, modular representation

Obsah

Kapitola 1

Idempotentní ideály v grupových algebrách symetrické grupy

1.1 Motivace pro hypotézu

Oboustranné idempotentní ideály v grupovém okruhu $\mathbb{Z}G$, pro G konečnou grupu, úzce souvisí s projektivními $\mathbb{Z}G$-moduly. Víme, že každý zprava konečně generovaný oboustranný idempotentní ideál $I \subseteq \mathbb{Z}G$ lze popsat jako stopový ideál nějakého projektivního $\mathbb{Z}G$-modulu P [8]. Přičemž, je-li P konečně generovaný, je I nutně celý $\mathbb{Z}G$ [1]. V případě že G je řešitelná, je každý konečně negenerovatelný $\mathbb{Z}G$-modul volný [7], jeho stopový ideál je tedy taktéž celý $\mathbb{Z}G$.

V této práci se zabývám případem, kdy G není řešitelná, konkrétně vyšetřuji symetrické grupy S_n, $n \geq 5$. Ty mají jedinou netriviální perfektní normální podgrupu. Je otázka, jak moc se neřešitelnost projeví na struktuře idempotentních ideálů. Jeden vlastní idempotentní ideál umíme přímo zkonstruovat z perfektní podgrupy, budeme mu říkat augmentační. Naivní hypotéza by byla, že se jedná o jediný, my budeme vyšetřovat slabší: každý idempotentní ideál v $\mathbb{Z}S_n$ generuje v $\mathbb{Q}S_n$ buď nevlastní ideál, nebo ten samý jako augmentační.

1.2 Formulace hypotézy a přechod k lokálnímu pohledu

Definice 1. *Nechť G je konečná grupa a R okruh, potom grupovým okruhem RG budeme rozumět množinu všech formálních sum $\sum_{g\in G} r_g g$, kde $r_g \in R$ pro každé $g \in G$. S operací sčítání po složkách a násobením definovaným vztahem:*

$$(\sum_{g\in G} r_g g)(\sum_{h\in G} s_h h) = \sum_{g,h\in G} r_g s_h (g \circ h)$$

Je snadné ověřit že grupový okruh je skutečně okruhem. Navíc, má-li R jednotku 1, je $1id$ jednotka v RG. Grupový okruh RG můžeme zkoumat dvojím způsobem, jednak skrze jeho kategorii RG-modulů a jednak skrze R-reprezentace grupy G. Oba přístupy jsou však analogické: Je-li M R-modul a grupový homomorfismus $\varphi : G \to Aut(M)$ R-reprezentace grupy G, můžeme na M definovat strukturu RG-modulu s násobení skaláry: $m(\sum_{g\in G} r_g g) = \sum_{g\in G} r_g \varphi(g)(m)$. Stejně tak každý pravý RG-modul M zadává R-reprezentaci grupy G v $Aut_R(M)$,

kde každému prvku $g \in G$ přiřazujeme automorfismus definovaný pravým skalárním násobením. Je známý fakt, že tato korespondence zachovává důležité pojmy jako podmodulu a podreprezentace, direktní sumy modulů a direktní sumy reprezentací. V této práci bude teorie budována převážně z pohledu modulárního, kde se nám budou hodit pojmy jako projektivita a semiperfektnost. K reprezentacím přejdu až v závěru, kdy budeme potřebovat charaktery, v jejichž řeči formulujeme vzorce pro závěrečný výpočet.

Značení a konvence: Pro okruh R bude R-modulem myšlen vždy, nebude-li řečeno jinak, pravý R-modul. Stejně tak jednostranné vlastnosti modulů jako Noetherovskost, budeme chápat ve své pravostranné verzi. Dále $Mod(R)$ bude značit kategorii konečně generovaných R-modulů a $Proj(R)$ kategorii konečně generovaných projektivních R-modulů. Symetrickou grupu řádu $n \in \mathbb{N}$ budeme značit S_n.

Pro okruh R označme $Id(R)$ množinu všech jeho oboustranných idempotentních ideálů. Budeme zkoumat zobrazení $i : Id(\mathbb{Z}S_n) \to Id(\mathbb{Q}S_n)$ dané předpisem $i : I \mapsto I \cdot \mathbb{Q}$. Tedy i přiřazuje ideálu $I \in Id(\mathbb{Z}S_n)$ jím generovaný ideál v $\mathbb{Q}S_n$. Je snadno ověřitelné, že $I \cdot \mathbb{Q}$ je idempotentní ideál pro každý $I \in Id(\mathbb{Z}S_n)$, a tedy i je dobře definováno. Díváme-li se na $\mathbb{Q}S_n$ jako na tensorový součin $\mathbb{Z}S_n \otimes_{\mathbb{Z}} \mathbb{Q}$, můžeme psát $i(I) = I \otimes_{\mathbb{Z}} \mathbb{Q}$.

Lemma 1. *V $\mathbb{Z}S_n$, kde $n \geq 5$, existuje vlastní oboustranný idempotentní ideál.*

Důkaz. Označme $A_n < S_n$ alternující podgrupu a uvažme oboustranný ideál I generovaný prvky $\{1 - g | g \in A_n\}$. Je známý fakt, že A_n je pro $n \geq 5$ perfektní, neboli $[A_n,A_n] = A_n$. Proto každý $g \in A_n$ lze vyjádřit ve tvaru $g = g_1 g_2 \cdots g_m$, kde každý g_* je komutátor prvků z A_n. Odtud

$$1 - g = 1 - g_1 + g_1(1 - g_2) + \cdots + g_1 \cdots g_{m-1}(1 - g_m),$$

čili I je generován prvky $\{1 - [g,h] : g,h \in A_n\}$. K důkazu idempotentnosti stačí ukázat, že právě popsané generátory náleží I^2. Buď $g,h \in A_n$, potom:

$$(1 - ghg^{-1}h^{-1})hg = hg - gh = (1 - h)(1 - g) - (1 - g)(1 - h) \in I^2.$$

Vynásobíme-li rovnost zprava prvkem $g^{-1}h^{-1}$, dostaneme dokazované.

❑

Ideál z předchozího lemmatu budeme značit Aug_n. Ideál Aug_n je vlastní, to je okamžitě jasné, uvědomíme-li si, že pro každý jeho prvek $\sum_{g \in S_n} r_g g$ je $\sum_{g \in S_n} r_g = 0$. Neboť tuto vlastnost splňují generátory a je zachována při sčítání i násobení. Zde je přesná formulace hypotézy, kterou budeme vyšetřovat: Nechť I je oboustranný idempotentní ideál grupového okruhu $\mathbb{Z}S_n$, pro n přirozené. Potom $i(I)$, ideál okruhu $\mathbb{Q}S_n$, je jednoho z tvaru:

- 0
- $\mathbb{Q}S_n$
- $Aug_n \cdot \mathbb{Q}$

Definice 2. *Symbolem $\mathbb{Z}_{(p)}$, pro p prvočíslo, budeme značit lokalizaci okruhu $\mathbb{Z}$ v prvoideálu $p\mathbb{Z}$.*

Na okruh $\mathbb{Z}_{(p)}$ se budeme dívat jako na podokruh $\mathbb{Q}$, racionálních čísel, jejichž jmenovatel v redukovaném vyjádření, není dělitelný prvočíslem p. Vzhledem k tomu, že $\mathbb{Z}_p$ je lokalizace Dedekindova oboru, je $\mathbb{Z}_{(p)}$ okruh diskrétní valuace. Tento fakt budeme později potřebovat.

Základním krokem ve vyšetřování hypotézy bude přechod k lokálnímu pohledu. Ukážeme, že každý $I \in Id(\mathbb{Z}S_n)$ je jednoznačně určen ideály, které generuje v okruzích $\mathbb{Z}_{(p)}S_n$, pro prvočísla p dělící řád grupy S_n.

V následující větě budeme potřebovat vědět, že nedělí-li prvočíslo p řád grupy S_n, potom $\mathbb{Z}_{(p)}S_n$ obsahuje všechny centrální idempotenty okruhu $\mathbb{Q}S_n$. To není triviální, ale lze tomu snadno nahlédnout ze známých vzorců pro centrální idempotenty $\mathbb{Q}S_n$, jež jsou k dohledání v [6]. Každý primitivní centrální idempotent $e \in \mathbb{Q}S_n$ je tvaru

$$e = \frac{z}{|S_n|} \sum_i \overline{\chi(i)} C_i,$$

kde $z \in \mathbb{Z}$, index i běží přes třídy konjugace S_n, C_i je součet prvků konjugační třídy i a χ je charakter nějaké ireducibilní reprezentace S_n, který jak víme nabývá celočíselných hodnot. Jediné, co ve vzorci dělá potíže je dělení řádem grupy S_n, což ovšem v $\mathbb{Z}_{(p)}S_n$ pro $p > n$ lze.

Věta 2. *Nechť n je přirozené číslo a pro každé prvočíslo $p \leq n$ mějme idempotentní ideál I_p grupového okruhu $\mathbb{Z}_{(p)}S_n$. Platí-li, že všechny tyto ideály generují v $\mathbb{Q}S_n$ stejný ideál, tedy že pro každé dvě prvočísla $p,q \leq n$ je $\mathbb{Q}I_p = \mathbb{Q}I_q = e\mathbb{Q}S_n$, kde e je nějaký centrální idempotentní prvek $\mathbb{Q}S_n$, potom existuje právě jeden ideál $I \subseteq \mathbb{Z}S_n$ splňující následující:*

- *$\mathbb{Z}_{(p)}I = I_p$ pro každé prvočíslo $p \leq n$,*
- *$\mathbb{Z}_{(p)}I = e\mathbb{Z}_pS_n$ pro každé prvočíslo $p > n$.*

Navíc ideál I je idempotentní.

Důkaz. Prvně poznamenejme, že $\mathbb{Q}S_n$ je dle Maschkeho věty [4, věta 12.8] totálně rozložitelný, každý jeho oboustranný ideál je tedy generován centrálním idempotentem. To nám dává existenci idempotentu e ze znění věty. Úvaha před formulací věty zaručuje, že druhý dokazovaný bod má dobrý smysl.

Dále si všimněme, že pro každé prvočíslo p jsou ideály okruhu $\mathbb{Z}_{(p)}S_n$ konečně generované $\mathbb{Z}_{(p)}$-moduly: $\mathbb{Z}_{(p)}$ je DVR, tedy speciálně Noetherovský okruh. $\mathbb{Z}_{(p)}S_n$ je konečně generovaný $\mathbb{Z}_{(p)}$-modul, tedy je Noetherovský $\mathbb{Z}_{(p)}$-modul. Odtud již plyne, že všechny jeho podmoduly, speciálně i ideály okruhu $\mathbb{Z}_{(p)}S_n$, jsou konečně generované $\mathbb{Z}_{(p)}$-moduly.

Dokažme jednoznačnost ideálu I, splňujícího oba dokazované body. Mějme dva takové ideály I, J okruhu $\mathbb{Z}S_n$, můžeme BÚNO předpokládat $I \subseteq J$, jinak berme I a $I + J$. Stačí dokázat opačnou inkluzi.

Volme pevně j, libovolný prvek v J. Pro každé prvočíslo p nalezneme $d_p \in \mathbb{Z}$, že $\mathrm{NSD}(d_p,p) = 1$ a $d_pj \in I$. Nechť tedy p je prvočíslo, ze znění dokazovaného lemmatu dostáváme rovnost $\mathbb{Z}_{(p)}I = \mathbb{Z}_{(p)}J$. Proto musí existovat $i_1,\ldots,i_r \in I$ a $c_1,\ldots,c_r \in \mathbb{Z}_{(p)}$, že:

$$\sum_{\alpha=1}^{r} c_\alpha i_\alpha = j. \tag{1.1}$$

Označme $d_p \in \mathbb{Z}$ součin všech jmenovatelů prvků $c_1,...,c_r$. Protože všechny jmenovatelé prvků c_i jsou z definice okruhu $\mathbb{Z}_{(p)}$ nesoudělné s p, platí $NSD(d_p,p) = 1$. Přenásobíme-li obě strany rovnosti (1.1) číslem d_p, dostaneme na levé straně celočíselnou lineární kombinaci prvků $i_1,..., i_r$, tedy prvek ideálu I. Odtud $d_p j \in I$.

Uvažme nyní prvky d_p zkonstruované pro všechna prvočísla a podívejme se na jimi generovaný ideál K okruhu celých čísel. $\mathbb{Z}$ je $OIHI$, proto je K tvaru $c\mathbb{Z}$, pro nějaké $c \in \mathbb{Z}$. Číslo c nemá žádného prvočíselného dělitele q, neboť kdyby $q|c$, pak $q|d_q$, což je spor. Proto $K = \mathbb{Z}$ a existuje P, konečná množina prvočísel, a celá čísla a_p, $p \in P$, taková, že $1 = \sum_{p\in P} a_p d_p$. Pak ale

$$j = \sum_{p\in P} a_p d_p j \in I.$$

Odtud $J \subseteq I$ a rovnost ideálů je dokázaná.

Nyní dokážeme existenci ideálu I. Pro každý ideál I_p ze znění věty definujme $J_p = \mathbb{Z}S_n \cap I_p$. Jistě platí $\mathbb{Z}_{(p)}J_p = I_p$. Dále vezměme $p,q \leq n$ různá prvočísla. $\mathbb{Z}_{(q)}J_p$ má konečnou množinu generátorů $g_1,..,g_t$ jakožto $\mathbb{Z}_{(q)}$-modul. Platí:

$$\mathbb{Q}(\mathbb{Z}_{(q)}J_p) = \mathbb{Q}J_p = \mathbb{Q}(\mathbb{Z}_{(p)}J_p) = \mathbb{Q}I_p = \mathbb{Q}I_q.$$

Odtud pro každé g_j existují $i_1, \ldots, i_s \in I_q$ a $a_1, \ldots, a_s \in \mathbb{Q}$, že $g_j = \sum_{\alpha=1}^{s} a_\alpha i_\alpha$. Volme λ_j takovou mocninu prvočísla q, že všechna λa_α jsou prvky $\mathbb{Z}_{(q)}$, jinak řečeno λ_j je dostatečně velká mocnina q, aby pokrátila u všech a_α mocniny q ve jmenovatelích. Pro takové λ_j platí $\lambda_j g_j = \sum_{\alpha=1}^{s} \lambda_j a_\alpha i_\alpha \in I_q$. Definujme nyní $\lambda_{p,q}$ jako největší prvek množiny $\{\lambda_1,...,\lambda_t\}$. Pro takto definované $\lambda_{p,q}$ platí $\lambda_{p,q} g_j \in I_q$ pro všechny generátory $g_1,...,g_t$, a tedy

$$\mathbb{Z}_{(q)}\lambda_{p,q}J_p \subseteq I_q. \tag{1.2}$$

Navíc $\lambda_{p,q}$ je v $\mathbb{Z}_{(p)}$ jakožto mocnina prvočísla q invertibilní, proto:

$$\mathbb{Z}_{(p)}\lambda_{p,q}J_p = \mathbb{Z}_{(p)}J_p = I_p. \tag{1.3}$$

Nyní sestrojme $\lambda_{p,q}$ pro všechny uspořádané dvojice různých prvočísel $p,q \leq n$ a konečně definujme $\Lambda_p = \prod_{q\in\mathbb{P},p\neq q\leq n} \lambda_{p,q}$. Protože Λ_p dostaneme z $\lambda_{p,q}$ vynásobením prvky invertibilními jak v $\mathbb{Z}_{(p)}$ tak v $\mathbb{Z}_{(q)}$, vzorce (1.2) a (1.3) zůstanou platnými, přepíšeme-li $\lambda_{p,q}$ na Λ_p. Položíme-li

$$I_0 = \sum_{p\in\mathbb{P},p\leq n} \Lambda_p J_p,$$

dostaneme z pravidel aritmetiky ideálů $\mathbb{Z}_{(p)}I_0 = I_p$, pro každé prvočíslo $p \leq n$.

Nyní ať je p prvočíslo větší než n. V $\mathbb{Q}S_n$ existuje centrální idempotent f, že $e + f = 1$ a $ef = 0$. Dle úvahy na začátku e i f náleží $\mathbb{Z}_{(p)}S_n$, čili $\mathbb{Z}_{(p)}S_n = e\mathbb{Z}_{(p)}S_n \oplus f\mathbb{Z}_{(p)}S_n$. Ideál $\mathbb{Z}_{(p)}I_0$ musí být tedy nutně obsažen v ideálu $e\mathbb{Z}_{(p)}S_n$. Protože $e \in \mathbb{Q}I_0$, existují $i_1, \ldots, i_m$ prvky ideálu I_0 a racionální čísla $q_1, \ldots, q_m$, že

$$e = \sum_{j=1}^{m} q_j i_j. \tag{1.4}$$

Označme q natolik velké prvočíslo, že pro všechna prvočísla $p \geq q$ už $\mathbb{Z}_{(p)}$ obsahuje všechna q_j ze (1.4), čili $\mathbb{Z}_{(q)}I_0 = e\mathbb{Z}_{(q)}S_n$. Nyní pro každé prvočíslo p, $n < p < q$

označme $J_p = \mathbb{Z}S_n \cap e\mathbb{Z}_{(p)}S_n$ a podobně jako výše sestrojme Λ_p, součin mocnin prvočísel menších nebo rovných n, aby $\mathbb{Z}_{(r)}\Lambda_p J_p \subseteq I_r$, pro každé prvočíslo $r \leq n$. Definujme

$$I = I_0 + \sum_{p\in\mathbb{P}, n<p<q} \Lambda_p J_p.$$

Ideál I bude generovat ideály I_* ze zadání. Pro každé prvočíslo p, $n < p < q$ je $\mathbb{Z}_{(p)}\Lambda_p J_p = e\mathbb{Z}_{(p)}S_n$, výše jsme dokázali inkluzi $\mathbb{Z}_{(p)}I_0 \subseteq e\mathbb{Z}_{(p)}S_n$ a podobným argumentem se dokáže i $\mathbb{Z}_{(p)}\Lambda_r J_r \subseteq e\mathbb{Z}_{(p)}S_n$, pro každé prvočíslo $r \neq p$, $n < r < q$, to dohromady dává $\mathbb{Z}_p I = e\mathbb{Z}_{(p)}S_n$. A konečně vzhledem k předpokladu na q, bude druhý dokazovaný bod platit i pro prvočísla větší nebo rovna q.

Idempotentnost ideálu I snadno plyne z jednoznačnosti, neboť pro každé prvočíslo $p \leq n$ platí $\mathbb{Z}_{(p)}I^2 = (\mathbb{Z}_{(p)}I)^2 = I_p$ a podobně pro prvočísla větší než n. ❑

Každý $I \in Id(\mathbb{Z}S_n)$ generuje v $Z_{(*)}S_n$ idempotentní ideály splňující předpoklady věty. Můžeme proto přejít od zkoumání zobrazení $i : Id(\mathbb{Z}S_n) \to Id(\mathbb{Q}S_n)$, ke zkoumání zřejmým způsobem definovaných zobrazení $i_p : Id(\mathbb{Z}_{(p)}S_n) \to (\mathbb{Q}S_n)$, pro prvočísla $p \leq n$. Hlavním přínosem tohoto přechodu je, že $\mathbb{Z}_{(p)}S_n$ jsou semiperfektní okruhy a oboustranné idempotentní ideály v nich umíme popsat.

Bohužel nám věta 2 nedává jednoznačnost ideálu I jen na základě znalosti ideálů I_p, neboť si v důkazu jednoznačnosti navíc klademe požadavek druhého dokazovaného bodu. Zatím tedy nemůžeme říci, že existuje bijekce mezi množinami $Id(\mathbb{Z}S_n)$ a $\prod_{p\in\mathbb{P}, p|n} Id(\mathbb{Z}_{(p)}S_n)$, později však tento nedostatek odstraníme.

V následujících dvou sekcích se budeme zabývat popisem $Id(\mathbb{Q}S_n)$ a $Id(\mathbb{Z}_{(p)}S_n)$.

1.3 Oboustranné idempotentní ideály v totálně rozložitelném okruhu

Množinu $Id(\mathbb{Q}S_n)$ lze snadno popsat, neboť podle Maschkeho věty [4, věta 12.8] je $\mathbb{Q}S_n$ totálně rozložitelný okruh. Protože teorie totálně rozložitelných okruhů je poměrně známá, následující výklad bude stručný. Prvně z definice totálně rozložitelných okruhů je každý ideál direktním sčítancem regulárního modulu $\mathbb{Q}S_{n\mathbb{Q}S_n}$ a podle [2, lemma 7.1] je generován idempotentním prvkem. Čili každý ideál okruhu $\mathbb{Q}S_n$ je idempotentní. Z totální rozložitelnosti dále víme, že $\mathbb{Q}S_{n\mathbb{Q}S_n}$ lze vyjádřit jako direktní sumu jednoduchých pravých ideálů, těch musí být nutně konečně mnoho, protože $\mathbb{Q}S_n$ je Artinovský. Podle [4, lemma 25.10] je každý jednoduchý $\mathbb{Q}S_n$-modul izomorfní nějakému minimálnímu pravému ideálu. Existuje proto konečná sada až na izomorfismus všech jednoduchých pravých $\mathbb{Q}S_n$-modulů, označme je Z_1,...,Z_s, a jim izomorfní minimální ideály označme L_1,...,L_s. Dále ať B_i je součet všech pravých ideálů izomorfních s L_i. B_i je podle [4, lemma 25.15] oboustranný ideál a platí

$$\mathbb{Q}S_n = B_1 \oplus ... \oplus B_s. \tag{1.5}$$

Podle [4, lemma 25.21] je každý oboustranný ideál okruhu $\mathbb{Q}S_n$ součtem ideálů B_i, neboli v $\mathbb{Q}S_n$ existuje právě 2^s oboustranných idempotentních ideálů.

Oboustranné ideály nyní popíšeme jako stopové ideály:

Definice 3. *Buď R okruh a M libovolný R-modul, definujme $Tr_R(M)$ stopový ideál modulu M vzorcem*

$$Tr_R(M) = \sum_{\alpha \in Hom_R(M,R_R)} \alpha(M).$$

Lemma 3. *Pro libovolný okruh R a R-modul M je $Tr_R(M)$ oboustranný ideál okruhu R.*

Důkaz. Přímo z definice se jedná o podmodul R_R a podmoduly regulárního modulu jsou právě pravé ideály okruhu R. Dále, je-li $\alpha \in Hom_R(M,R_R)$ a $r \in R$ je $r \cdot \alpha : m \mapsto r\alpha(m)$ také prvek $Hom_R(M,R_R)$, proto $r\alpha(m) \in Tr_R(M)$ pro každé $m \in M$, čili $Tr_R(M)$ je i levý ideál.

❑

Lemma 4 ([2], lemma 8.18)**.** *Jsou-li M a N dva R-moduly, pak $Tr_R(M \oplus N) = Tr_R(M) + Tr_R(N)$.*

Pro každé $i = 1, \ldots, s$ je z definice ideálu B_i zřejmá inkluze $B_i \subseteq Tr_R(Z_i)$. Platí i opačná: Protože Z_i je jednoduchý, je každý nenulový $\alpha \in Hom_R(Z_i,R_R)$ prostý, a tedy $Im(\alpha) \cong Z_i \cong L_i$. Vidíme, že ideál $Im(\alpha)$ je izomorfní L_i, musí být proto obsažen v B_i. Tím je dokázána rovnost $Tr_R(Z_i) = B_i$. Protože každý oboustranný ideál v $\mathbb{Q}S_n$ je součtem některých ideálů B_i, lze podle lemmatu 4 každý oboustranný ideál popsat jako stopový ideál direktní sumy některých z modulů Z_i. Můžeme tedy říci, že každý oboustranný idempotentní ideál okruhu $\mathbb{Q}S_n$ je stopovým ideálem konečně generovaného $\mathbb{Q}S_n$-modulu.

1.4 Oboustranné idempotentní ideály v semiperfektním Noetherovském okruhu

Definice 4. *Okruh R nazveme semiperfektním, je-li $R/J(R)$ totálně rozložitelný a pro každý idempotentní prvek $e \in R/J(R)$ existuje idempotentní prvek $f \in R$, že $e = f + J(R)$.*

Budeme potřebovat následující dvě vlastnosti semiperfektních okruhů (jejich důkaz lze nalézt v [5, teorém 3.6]). Nechť tedy R je semiperfektní okruh:

- každý konečně generovaný R-modul má projektivní pokrytí
- v R existuje rozklad jednotky $1 = f_1 + \ldots + f_m$, kde $\{f_i\}_{i=1}^m$ jsou primitivní ortogonální idempotentní prvky (čili $f_i f_j = 0$ pro $i \neq j$ a žádný z f_* nemá netriviální rozklad na součet dvou idempotentů).

V této sekci dokážeme, že semiperfektní okruh R, který je navíc Noetherovský, má konečnou sadu až na izomorfismus všech konečně generovaných nerozložitelných projektivních modulů. Pomocí zobrazení stopy pak, analogicky jako v případě totálně rozložitelného okruhu, popíšeme všechny idempotentní oboustranné ideály, jako stopové ideály konečně generovaných projektivních R-modulů. V dalším bude R vždy značit semiperfektní Noetherovský okruh a $\pi : R \longrightarrow R/J(R)$ přirozenou projekci.

Nejprve ověřme noetherovskost a semiperfektnost u okruhu $\mathbb{Z}_{(p)}S_n$. Okruh $\mathbb{Z}_{(p)}$ je jakožto okruh diskrétní valuace Noetherovský, a tedy i $\mathbb{Z}_{(p)}S_n$ je jakožto konečně generovaný $\mathbb{Z}_{(p)}$-modul Noetherovský, tím spíš je Noetherovský jakožto $\mathbb{Z}_{(p)}S_n$-modul. Dokázat semiperfektnost je podstatně těžší a je k tomu potřeba rozkladovost tělesa $\mathbb{Q}$ pro S_n, viz následující definice.

Definice 5. *Těleso T nazveme rozkladovým pro grupu G, jestliže pro každé tělesové rozšíření konečného stupně $S \geq T$ a jednoduchý TG-modul M, je $M \otimes_T S$ jednoduchý SG-modul.*

Lemma 5 ([6], teorém 2.1.12)**.** *Každé těleso je rozkladové pro grupu S_n, kde n je libovolné přirozené číslo.*

V následující kapitole ukáži (lemma 2.1), že pro okruh diskrétní valuace R platí $J(R)G \subseteq J(RG)$. Projekce $RG \to RG/J(RG)$ se proto faktorizuje přes $RG/J(R)G \cong (R/J(R))G$. V případě okruhu $\mathbb{Z}_{(p)}$ je $R/J(R) \cong \mathbb{Z}_p$ a grupový okruh $\mathbb{Z}_pS_n$ je jak vidíme konečný, tedy triviálně semiperfektní (každý konečný okruh je Artinovský a každý Artinovský okruh je semiperfektní). Stačí proto dokázat, že každý idempotent v $\mathbb{Z}_pS_n$ je projekcí idempotentu z $\mathbb{Z}_{(p)}S_n$. K důkazu by bylo třeba zavézt pojmy p-adické topologie a p-adického zúplnění. Odkáži se proto raději na cvičení 6.16 v [3], kde je ve velmi podrobném návodu toto ukázáno v obecném případě. Tedy pro grupový okruh RG, kde R je DVR, jehož podílové těleso je rozkladové pro grupu G (což je splněno v případě $\mathbb{Z}_{(p)}S_n$).

Zaveďme několik pojmů týkajících se teorie projektivních modulů.

Definice 6. *R-modul P nazveme projektivním, jestliže pro každý surjektivní modulový homomorfismus $f : M \to N$ a každý modulový homomorfismus $g : P \to N$ existuje homomorfismus $h : P \to M$, že $fh = g$. Ekvivalentně R-modul P je projektivní, je-li direktním sčítancem nějakého volného R-modulu.*

Důkaz ekvivalence obou definicí lze nalézt v [2, lemma 17.2].

Definice 7. *Projektivním pokrytím nazveme surjektivní homomorfismus $\varphi : P \to M$, kde P a M jsou R-moduly, P navíc projektivní, jehož jádro splňuje následující podmínku: pro každý $N \leq P$ je-li $N + ker\varphi = P$, pak $N = P$.*

Podmínku na $ker\varphi$ z předchozí definice budeme značit $ker\varphi \ll P$.

Lemma 6 (jednoznačnost projektivního pokrytí)**.** *[[5], věta 3.1] Jsou-li $\varphi : P \to M$ a $\psi : Q \to M$ projektivní pokrytí R-modulu M, potom P a Q jsou izomorfní.*

Lemma 7 ([5], věta 3.2)**.** *Jsou-li $\varphi_i : P_i \to M_i$, pro $i = 1, \ldots, m$ projektivní pokrytí, potom zobrazení $\varphi : P_1 \oplus \cdots \oplus P_m \to M_1 \oplus \cdots \oplus M_m$, přirozeně definované po složkách, je projektivní pokrytí.*

Lemma 8 (Nakayamovo)**.** *[[2], důsledek 15.13] Je-li M konečně generovaný R-modul, potom $MJ(R) \ll M$.*

Nakayamovo lemma nám říká, že pro P konečně generovaný projektivní R-modul, je přirozená projekce $P \to P/PJ(R)$ projektivní pokrytí.

Lemma 9 (jednoznačnost pokrývaného)**.** *Nechť P je konečně generovaný projektivní R-modul a $\varphi : P \to S$ je projektivní pokrytí polojednoduchého R-modulu S, potom $S \cong P/PJ(R)$.*

Důkaz. P je spolu s přirozenou projekcí π projektivním pokrytím polojednoduchého modulu $P/PJ(R)$. Je jasné, že $PJ(R) \leq ker\varphi$ neboť $\varphi(PJ(R)) = \varphi(P)J(R) = SJ(R) = 0$, poslední rovnost plyne z polojednoduchosti S. Z věty o homomorfismu je S homomorfním obrazem $P/PJ(R)$ a tedy izomorfní nějakému podmodulu $P/PJ(R)$, protože $P/PJ(R)$ je polojednoduchý. Polojednoduchost $P/PJ(R)$ nám dále dává existenci R-modulu S_1, že $P/PJ(R) \cong S_1 \bigoplus S$. Označme P_1 projektivní R-modul příslušný projektivnímu pokrytí S_1, jeho existence plyne z vlastností semiperfektního okruhu. Z lemmatu 7 je $P \oplus P_1$ projektivním pokrytím S a lemma 6 dává izomorfismus $P \cong P \bigoplus P_1$. Protože P je jakožto konečně generovaný modul Noetherovského okruhu Noetherovský, musí být $P_1 = 0$, proto i $S_1 = 0$ což dává dokazovaný izomorfismus $P/PJ(R) \cong S$. ❑

Z definice semiperfektního modulu je $R/J(R)$ totálně rozložitelný okruh. To nám dává existenci konečné množiny až na izomorfismus všech po dvou neizomorfních jednoduchých $R/J(R)$-modulů (zkráceně: kompletní sady jednoduchých $R/J(R)$-modulů) S_1,...,S_r a přirozená čísla λ_1,...,λ_r, že:

$$R/J(R)_{R/J(R)} \cong S_1^{\lambda_1} \oplus ... \oplus S_r^{\lambda_r}.$$

Izomorfismus je ve smyslu $R/J(R)$-modulů. Moduly S_i jsou i jednoduchými R-moduly a opačně každý jednoduchý R-modul je nulován ideálem $J(R)$, je tedy i jednoduchým $R/J(R)$-modulem, čili je izomorfní některému S_i jakožto R-modul i $R/J(R)$-modul. Můžeme proto považovat S_1,...,S_r i za kompletní sadu jednoduchých R-modulů. Přirozené číslo r a jednoduché R-moduly S_1,..., S_r budou mít v dalším právě popsaný význam.

Věta 10. *Existuje sada konečně generovaných nerozložitelných projektivních R-modulů P_1,...,P_r, že každý konečně generovaný projektivní R-modul P lze vyjádřit jako direktní suma*

$$P \cong P_1^{\alpha_1} \oplus ... \oplus P_r^{\alpha_r}. \tag{1.6}$$

Toto vyjádření je jednoznačné až na pořadí sčítanců. Navíc každý P_i je izomorfní pravému ideálu okruhu R, který je generovaný primitivním idempotentním prvkem.

Důkaz. Z vlastností semiperfektního okruhu existuje rozklad

$$R_R = f_1R \oplus \cdots \oplus f_mR, \tag{1.7}$$

kde f_i jsou primitivní idempotentní prvky. Primitivnost f_i dává nerozložitelnost f_iR vůči direktní sumě. Nakayamovo lemma říká, že přirozená projekce f_iR na f_iR/J_i, kde $J_i = J(R) \cap f_iR = f_iJ$, je projektivní pokrytí. Ať $i \in \{1, \ldots, m\}$, dokáži že i f_iR/J_i je nerozložitelný. Pro spor předpokládejme, že $f_iR/J_i = M_1 \oplus M_2$ je netriviální rozklad. Z konečné generovanostif_iR/J_i můžeme odvodit, že i M_1,M_2 jsou konečně generované. Existují proto projektivní pokrytí $\phi_i : P_i \to M_i$, $i = 1$,2. Z jednoznačnosti projektivního pokrytí je $P_1 \oplus P_2$ netriviální rozklad f_iR, což je spor. Navíc f_iR/J_i je anihilován ideálem $J(R)$, čili se jedná o jednoduchý R-modul.

Lemma 7 a vzorec (1.7) dávají projektivní pokrytí $\phi : R_R \to f_1R/J_1 \oplus \cdots \oplus f_mR/J_m$, z lemmatu 9 pak dostáváme izomorfismus

$$f_1R/J_1 \oplus \cdots \oplus f_mR/J_m \cong R/J(R) \cong S_1^{\lambda_1} \oplus \cdots \oplus S_r^{\lambda_r}.$$

Podle výše dokázané nerozložitelnosti f_iR/J_i a jednoznačnosti rozkladu polojednoduchých modulů, můžeme uspořádat idempotenty f_i tak, že pro $i = 1,...,r$ je $f_iR/J_i \cong S_i$. Definujme $P_i = f_iR$.

Je-li P libovolný konečně generovaný projektivní R-modul, pak $P/PJ(R)$ je jakožto polojednoduchý R-modul tvaru $S_1^{\alpha_1} \oplus \cdots \oplus S_r^{\alpha_r}$. Z jednoznačnosti projektivního pokrytí platí $P \cong P_1^{\alpha_1} \oplus \cdots \oplus P_r^{\alpha_r}$. Vyjádření (1.6) je jednoznačné, neboť $P_1^{\alpha_1} \oplus \cdots \oplus P_r^{\alpha_r} \cong P_1^{\beta_1} \oplus \cdots \oplus P_r^{\beta_r}$ nám dává z lemmat 7 a 9 izomorfismus $S_1^{\alpha_1} \oplus \cdots \oplus S_r^{\alpha_r} \cong S_1^{\beta_1} \oplus \cdots \oplus S_r^{\beta_r}$. Rovnosti $\alpha_i = \beta_i$ pak plynou z jednoznačnosti rozkladu polojednoduchých modulů.

❑

Projektivním modulům z předchozího lemmatu budeme říkat *kompletní sada nerozložitelných konečně generovaných projektivních R-modulů*. Z důkazu je patrné, že kompletní sadu nerozložitelných konečně generovaných projektivních R-modulů můžeme zkonstruovat i jako projektivní pokrytí kompletní sady jednoduchých R-modulů.

Lemma 11. *Ať I,K jsou oboustranné idempotentní ideály okruhu R. Platí-li $\pi(I) = \pi(K)$, pak $I = K$.*

Důkaz. Označme $L = I + K$, snadno se odvodí, že i L je idempotentní ideál. Předpoklad $\pi(I) = \pi(K)$ můžeme přepsat do tvaru $I + J(R) = K + J(R)$, odtud $L + J(R) = I + J(R)$. Aritmetikou ideálů spočtěme:

$$L = L(L + J(R)) = L(I + J(R)) = I + LJ(R).$$

Poslední rovnost dostáváme z: $LI \subseteq RI = I$ a $LI \supseteq I^2 = I$. Noetherovskost R zaručuje konečnou generovanost L, můžeme na něj proto aplikovat Nakayamovo lemma, což nám dá $L = I$. Analogicky se dokáže $K = L$. To dohromady dává dokazovaný vztah $L = K$.

❑

Lemma 12. *V R existuje 2^r idempotentních ideálů.*

Důkaz. Protože $R/J(R)$ je totálně rozložitelný okruh, má podle teorie polojednoducých okruhů, kterou jsme pro speciální případ $\mathbb{Q}S_n$ popsali v předchozí sekci, právě 2^r oboustranných idempotentních ideálů. Stačí tedy dokázat, že zobrazení $\Pi : Id(R) \to Id(R/J)$, které každému idempotentnímu ideálu I v R přiřadí jeho projekci $\pi(I)$, je bijekcí. Je snadné si rozmyslet, že pro každé $I \in Id(R)$ je $\pi(I)$ prvek $Id(R/J)$ (π je surjektivní okruhový homomorfismus). Prostota zobrazení Π je dokázána v předchozím lemmatu. Víme, že každý oboustranný ideál totálně rozložitelného okruhu R/J můžeme zapsat ve tvaru eR/J, kde e je centrální idempotent. Z definice semipefektních okruhů má e při zobrazení π vzor f, idempotentní prvek v R. RfR je jistě idempotentní ideál a

$\pi(RfR) = (R/J)e(R/J) = e(R/J).$

❑

Nyní odstraním nedostatek věty 2, o němž se zmiňuji v komentáři za jejím důkazem. Buď $p > n$ prvočíslo, podle [3, důsledek 17.11] je r, počet různých jednoduchých $\mathbb{Z}_pS_n$-modulů, roven počtu tříd konjugace S_n odpovídajících prvkům řádu nedělitelného prvočíslem p, což splňují všechny prvky grupy S_n. Počet různých jednoduchých $\mathbb{Q}S_n$-modulů je ale podle [4, věta 27.22] taktéž roven počtu tříd konjugace S_n, tedy číslu r. Z teorie vybudované v minulé sekci víme, že v $\mathbb{Q}S_n$ je právě 2^r oboustranných idempotentních ideálů. Množiny $Id(\mathbb{Z}_{(p)}S_n)$ a $Id(\mathbb{Q}S_n)$ jsou tedy stejně veliké. Každý $I \in Id(\mathbb{Q}S_n)$ je generován centrálním idempotentem, který je podle úvahy předcházející větě 2 prvkem okruhu $\mathbb{Z}_{(p)}S_n$, čili v něm generuje oboustranný idempotentní ideál I_p, pro který platí $I_p\mathbb{Q} = I$. Vidíme, že $i_p : Id(\mathbb{Z}_{(p)}S_n) \to Id(\mathbb{Q}S_n)$ je zobrazení mezi stejně velkými konečnými množinami a je na, nutně proto musí být bijekcí. Odvodili jsme, že pro každé dva $I, J \in Id(\mathbb{Z}S_n)$ platí:

$$\mathbb{Q}I = \mathbb{Q}J \Rightarrow \mathbb{Z}_{(p)}I = \mathbb{Z}_{(p)}J.$$

Skutečně tedy existuje přirozeně definovaná bijekce mezi množinami $Id(\mathbb{Z}S_n)$ a $\prod_{p\in\mathbb{P},p|n} Id(\mathbb{Z}_pS_n)$.

Věta 13. *Nechť P je projektivní konečně generovaný R-modul, potom $Tr_R(P)$ je oboustranný idempotentní ideál. Každý oboustranný idempotentní ideál je tohoto tvaru.*

Důkaz. Volme P libovolný konečně generovaný projektivní R-modul. Z lemmatu 3 je $Tr_R(P)$ oboustranný ideál. Dokáži idempotentnost: Z ekvivalentní definice projektivního R-modulu existuje n přirozené a R-modul $\tilde{P}$, že $P \oplus \tilde{P} \cong R_R^n$. Označme $\sigma : R_R^n \to P$ přirozenou projekci a e_1,...,e_n nějakou bázi R_R^n. Pro každé $i = 1, \ldots, n$ definujme $p_i = \sigma(e_i)$, homomorfismus $\sigma_i : R_R^n \to R_R$ jako projekci na i-tou složku a homomorfismus α_i jako restrikci σ_i na P. Berme p libovolný prvek v P, můžeme jej vyjádřit vůči zvolené bázi ve tvaru $p = \sum_i e_i\alpha_i(p)$. Snadno se odvodí:

$$p = \sigma(p) = \sum \sigma(e_i)\alpha_i(p) = \sum p_i\alpha_i(p). \tag{1.8}$$

Zvolme α libovolný prvek $Hom_R(P,R_R)$. Užitím vzorce (1.8) spočtěme:

$$\alpha(p) = \sum \alpha(p_i)\alpha_i(p) \in Tr_R(P)^2.$$

Protože prvek p a homomorfismus α jsme volili libovolně, platí $Tr_R(P) \subseteq Tr_R(P)^2$, čímž je idempotentnost ideálu $Tr_R(P)$ dokázána.

Uvažme nyní libovolný oboustranný idempotentní ideál $I \leq R$, jeho projekce $\pi(I)$ je oboustranný idempotentní ideál okruhu $R/J(R)$, je tedy tvaru $eR/J(R)$, kde e je centrální idempotentní prvek okruhu $R/J(R)$. $eR/J(R)$ je konečně generovaný R-modul a má proto projektivní pokrytí $\varphi : P \to e(R/J(R))$. Nechť $f \in P$ je takový, že $\varphi(f) = e$, potom $fR + ker\varphi = P$, a protože $ker\varphi \ll P$, je $P = fR$. Odtud P je konečně generovaný.

Chceme dokázat, že $Tr_R(P) = I$. K tomu nám podle lemmatu 11 stačí ověřit rovnost $\pi(Tr_R(P)) = \pi(I)$. Buď $\beta_0 : P \to R$ libovolný homomorfismus a označme

$\beta = \pi \circ \beta_0$. Podobným argumentem jako v lemmatu 9 se dokáže, že $ker\beta \supseteq PJ(R)$ a $\beta(P)$ je izomorfní nějakému podideálu $\pi(I)$. Ideál $\pi(I)$ je jakožto $R/J(R)$-modul totálně rozložitelný, proto existuje nějaký homomorfismus $\psi : \pi(I) \to \beta(P)$ představující projekci na $\beta(P)$. Odtud

$$\beta(P) = \psi(\pi(I)) = \psi(eeR/J(R)) = \psi(e)eR/J(R) \subseteq eR/J(R) = \pi(I). \tag{1.9}$$

V poslední rovnosti jsme užili toho, že e je centrální idempotent. Protože homomorfismus β_0 jsme volili libovolně, ze vzorce (1.9) snadno vyvodíme inkluzi $\pi(Tr_R(P)) \subseteq \pi(I)$. K dokončení důkazu stačí ověřit druhou inkluzi.

Protože $\pi : I \to eR/J$ je surjektivní homomorfismus pravých R-modulů, existuje z definice projektivního modulu homomorfismus $\alpha : P \to I$ takový, že $\pi \circ \alpha = \varphi$. Přejdeme-li k obrazům těchto zobrazení, dostaneme $\pi(Tr_R(P)) \supseteq \pi(I)$.

❑

Označme P_1,...,P_r projektivní R-moduly z věty 10. Pro každý $I \in Id(R)$, nám předchozí věta zaručuje existenci konečně generovaného projektivního R-modulu P, že $I = Tr_R(P)$. Z věty 10 musí být P direktní sumou některých modulů P_*. Protože stopa převádí direktní sumy na součty (lemma 4), musí se I rovnat součtu některých ideálů $Tr_R(P_*)$. Uvážíme-li, že v R existuje dle lemmata 12 právě 2^r oboustranných idempotentních ideálů, lze si snadno uvědomit, že každý ideál $Tr_R(P)$ je jednoznačně určen podmnožinou $\Lambda \subseteq \{P_1,...,P_r\}$ projektivních R-modulů, vyskytujících se jako direktní sčítanci v P.

Lemma 14. *Pro ideál okruhu R tvaru eR, kde e je idempotentní prvek, je $Tr_R(eR) = ReR$.*

Důkaz. Pro každý modulový homomorfismus $\alpha : eR \to R$ je $\alpha(eR) = \alpha(e)eR \subseteq ReR$, odtud $Tr_R(eR) \subseteq ReR$. Naopak, je-li $r \in R$, potom násobení prvkem r zleva zadává homomorfismus posílající e na re. Protože prvky tvaru re generují ReR jakožto pravý ideál, platí i $Tr_R(eR) \supseteq ReR$

❑

Komutativita diagramu v následující větě nám říká, že hledání popisu zobrazení $i : Id(\mathbb{Z}_{(p)}S_n) \mapsto Id(\mathbb{Q}S_n)$ je ekvivalentní zkoumání funktoru $- \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q} : Proj(\mathbb{Z}_{(p)}S_n) \to Mod(\mathbb{Q}S_n)$, neboť podle předchozího dostaneme přechodem k stopovým ideálům kompletní popis zobrazení $i_p : Id(\mathbb{Z}_{(p)}S_n) \to Id(\mathbb{Q}S_n)$.

Věta 15. *Následující diagram komutuje*

$$\begin{tikzcd}
Proj(\mathbb{Z}_{(p)}S_n) \arrow[r, "-\otimes_{\mathbb{Z}_{(p)}}\mathbb{Q}"] \arrow[d, "Tr_{\mathbb{Z}_{(p)}S_n}(-)"'] & Mod(\mathbb{Q}S_n) \arrow[d, "Tr_{\mathbb{Q}S_n}(-)"] \\
Id(\mathbb{Z}_{(p)}S_n(-)) \arrow[r, "-\cdot\mathbb{Q}"] & Id(\mathbb{Q}S_n)
\end{tikzcd}$$

Důkaz. Volme P konečně generovaný projektivní R-modul, podle věty 10 je tvaru $P = P_1^{\alpha_1} \oplus \cdots \oplus P_r^{\alpha_r}$. Navíc můžeme předpokládat, že každé P_i, pro $i = 1, \ldots, r$, je izomorfní ideálu generovaným idempotentním prvkem e_i.

Počítejme nejprve *levou dolní cestu*:

$$Tr_{\mathbb{Z}_{(p)}S_n}(P) = \sum_{\alpha_i \neq 0} Tr_{\mathbb{Z}_{(p)}S_n}(P_i) = \sum_{\alpha_i \neq 0} Tr(e_i \mathbb{Z}_{(p)} S_n) = \sum_{\alpha_i \neq 0} \mathbb{Z}_{(p)} S_n e_i \mathbb{Z}_{(p)} S_n.$$

Což nám v $\mathbb{Q}S_n$ generuje ideál $\sum_{\alpha_i \neq 0} \mathbb{Q}S_n e_i \mathbb{Q}S_n$.

Horní pravá cesta: protože tensorový součin zachovává direktní sumy, je $P \otimes \mathbb{Q} \cong (P_1 \otimes \mathbb{Q})^{\alpha_1} \oplus ... \oplus (P_r \otimes \mathbb{Q})^{\alpha_r}$. Z lemmatu 4 dostáváme:

$$Tr_{\mathbb{Q}S_n}((P_1 \otimes \mathbb{Q})^{\alpha_1} \oplus ... \oplus (P_r \otimes \mathbb{Q})^{\alpha_r}) = \sum_{\alpha_i \neq 0} Tr_{\mathbb{Q}S_n}(P_i \otimes \mathbb{Q}).$$

Platí $P_i \otimes \mathbb{Q} \cong e_i \mathbb{Z}_{(p)} S_n \otimes \mathbb{Q} \cong e_i \mathbb{Q} S_n$, což spolu s faktem, že izomorfní moduly dávají stejný stopový ideál a každý e_i je i idempotentním prvkem okruhu $\mathbb{Q}S_n$, dává $Tr_{\mathbb{Q}S_n}(P_i \otimes \mathbb{Q}) = \mathbb{Q}S_n e_i \mathbb{Q}S_n$. Tím je komutativita diagramu dokázána.

❑

Diagram má dokonce vlastnost aditivity: pro $P = P_1^{\alpha_i} \oplus ... \oplus P_r^{\alpha_r}$ a $\acute{P} = P_1^{\beta_i} \oplus ... \oplus P_r^{\beta_r}$ je:

$$\mathbb{Q} \cdot Tr(P \oplus \acute{P}) = \sum_{\alpha_i + \beta_i \neq 0} \mathbb{Q}S_n e_i \mathbb{Q}S_n =$$

$$\sum_{\alpha_i \neq 0} \mathbb{Q}S_n e_i \mathbb{Q}S_n + \sum_{\beta_i \neq 0} \mathbb{Q}S_n e_i \mathbb{Q}S_n = \mathbb{Q} \cdot Tr(P) + \mathbb{Q} \cdot Tr(\acute{P}).$$

Stačí nám proto spočítat pouze $P \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q}$ pro P nerozložitelné.

Kapitola 2

Modulární reprezentace

V předchozí kapitole jsme zkoumání zobrazení $i : Id(\mathbb{Z}S_n) \to Id(\mathbb{Q}S_n)$ převedli na zkoumání funktoru $- \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q} : Proj(\mathbb{Z}_{(p)}S_n) \to Mod(\mathbb{Q}S_n)$. V této kapitole půjdeme ještě dál a převedeme jej do abstraktního rámce Grothendieckových grup, kde nám definuje grupový homomorfismus e. V předchozích dvou sekcích jsme ukázali, že obě kategorie $Mod(\mathbb{Q}S_n)$ a $Proj(\mathbb{Z}_{(p)}S_n)$ mají ve vágním smyslu báze. To nabude formálně správného smyslu v jazyce Grothendieckových grup. Zobrazení e bude tedy homomorfismus volných abelovských grup, čili ho budeme moci popsat celočíselnou maticí E. Zároveň ukážeme, že obě kategorie jsou natolik hezké, že přechodem k e neztratíme žádnou informaci. V druhé sekci pak ukážeme, že $E = D^t$, kde D je takzvaná dekompoziční matice, tu již jak ukážeme ve třetí sekci umíme spočítat pomocí Braeurových charakterů.

2.1 p-modulární systém a redukce modulo N

Definice 8. *Trojici* (k,R,K) *nazveme p-modulárním systémem, je-li:* R *obor diskrétní valuace s maximálním ideálem* $N = \rho R$, K *jeho podílové těleso charakteristiky 0 a* $k = R/N$ *těleso charakteristiky* p.

p-modulární systém budeme zkoumat v souvislosti s konečnou grupou G, řádu dělitelného prvočíslem p. Navíc budeme předpokládat, že K je rozkladové pro grupu G a RG je semiperfektní (to máme ověřeno v případě $\mathbb{Z}_{(p)}S_n$), čili pro něj můžeme užít teorii vybudovanou v předchozí kapitole. Označme pro tuto kapitolu pevně (k, R, K) nějaký p-modulární systém pro grupu G. Pro zkoumání hypotézy pak užijeme vybudovanou teorii na p-modulární systém $(\mathbb{Z}_p, \mathbb{Z}_{(p)}, \mathbb{Q})$, s grupou S_n, kde p je prvočíslo menší nebo rovno n.

Označme ve shodě s notací v [3]:

- $P_1, \ldots, P_r$ kompletní sadu konečně generovaných nerozložitelných projektivních RG-modulů (dané větou 10 pro semiperfektní okruh RG).
- $F_1, \ldots, F_r$ kompletní sadu jednoduchých RG-modulů, indexované tak, že $F_i \cong P_i/P_iJ(RG)$
- $Z_1, \ldots, Z_s$ kompletní sadu jednoduchých KG-modulů

Přirozeně definovaná projekce z RG do kG má jádro NG, odtud NG je ideál a

$$kG \cong RG/NG. \tag{2.1}$$

Máme-li RG-modul M, můžeme se dívat na

$$\overline{M} = M/(M \cdot NG)$$

jako na kG-modul. Této operaci budeme říkat redukce modulo N a prvek $m + M \cdot NG$ modulu $\overline{M}$ budeme zkráceně značit $\overline{m}$.

Lemma 16. *Platí $NG \subseteq J(RG)$ a sjednotíme-li kG s RG/NG skrze izomorfismus* (2.1)*, platí $J(kG) = J(RG)/NG$.*

Důkaz. Dokáži, že ideál NG anihiluje každý jednoduchý RG-modul, což je ekvivalentní s $NG \subseteq J(RG)$. Ať tedy $F = fRG$ je jednoduchý RG-modul, kde $f \in F$. Množina $\{fg : g \in G\}$ generuje F jako R-modul. Protože grupa G je konečná, je F konečně generovaný R-modul. Z Nakayamova lemmatu je $FN = F$ jen pro F nulový. Protože FN je RG-podmodul F a F je jednoduchý, musí $FN = 0$. Druhý vztah snadno plyne z již dokázané inkluze.

❑

Mějme F polojednoduchý RG-modul, F je anihilován $J(RG)$, speciálně je anihilován NG, můžeme se na něj proto dívat jako na kG-modul. Z $J(RG/NG) = J(RG)/NG$ dostáváme $FJ(RG/NG) = 0$, čili F je polojednoduchý kG-modul. Je snadné si uvědomit, že naopak každý polojednoduchý kG-modul je i polojednoduchý RG-modul. Navíc polojednoduchý RG-modul je rozložitelný jako RG-modul, právě když je rozložitelný jako kG-modul. Okruhy RG a kG mají proto totožnou strukturu polojednoduchých modulů a F_1,...F_r je i kompletní sadou jednoduchých kG-modulů.

Dokáži, že redukce modulo N zachovává i strukturu konečně generovaných projektivních modulů. Prvně si uvědomme, že redukce modulo N zachovává direktní sumy: přirozená projekce z $M_1 \oplus M_2$ do $\overline{M_1} \oplus \overline{M_2}$ má jádro

$$M_1NG \oplus M_2NG = (M_1 \oplus M_2)NG.$$

První věta o izomorfismu dává: $\overline{M_1} \oplus \overline{M_2} \cong \overline{M_1 \oplus M_2}$. Každý projektivní RG-modul P je z definice direktním sčítancem volného RG-modulu. Protože redukce modulo N zachovává direktní sumy, je $\bar{P}$ direktním sčítancem volného kG-modulu, tedy je projektivní.

Protože $NG \subseteq J(RG)$, projektivní pokrytí $\pi : P \to P/PJ(RG)$ se faktorizuje přes $\overline{P}$:

$$P \xrightarrow{\pi_1} \overline{P} \xrightarrow{\pi_2} P/PJ(R),$$

kde obě zobrazení jsou přirozené projekce. Jelikož π_1 je surjektivní, lze každý RG-podmodul $\overline{P}$ zapsat ve tvaru $\pi_1(M)$, kde $M \leq P$. Je-li $\pi_1(M) + ker\pi_2 = \overline{P}$, dostaneme přechodem ke vzorům $ker\pi + M = P$, odtud $M = P$ a $\pi_1(M) = \overline{P}$. Dívejme se nyní na π_2 jako na homomorfismus kG-modulů, každý kG-podmodul od $\overline{P}$ je i RG-podmodulem, proto podle výše dokázaného $ker\pi_2 \ll \overline{P}$, čili π_2 je projektivní pokrytí.

Snadným důsledkem lemmatu 16 je, že semiperfektnost RG zaručuje semiperfektnost kG: $kG/J(kG) \cong (RG/NG)/(J(RG)/NG) \cong RG/J(RG)$, kde poslední okruh je totálně rozložitelný, a pro každý idempotent $e \in kG/J(kG)$ existuje $f \in RG$, že $\overline{f} + J(kG) = e$. Protože kompletní sadu nerozložitelných konečně generovaných projektivních kG-modulů dostáváme podle poznámky za větou 10 (zde je potřeba semiperfektnosti kG) jako projektivní pokrytí jednoduchých kG-modulů, což jsou právě $P_1/P_1J(RG)$,...,$P_r/P_rJ(RG)$, jsou $\overline{P_1}$,...,$\overline{P_r}$ kompletní sadou nerozložitelných konečně generovaných projektivních kG-modulů. Budeme je značit $U_i = \overline{P_i}$.

2.2 Grothendieckovy grupy a dekompoziční zobrazení

Konstrukce Grothendieckovy grupy: Nechť S je okruh a C je nějaká kategorie S-modulů, mající malý skelet a v níž máme definovaný pojem krátké exaktní posloupnosti. Definujme F volnou abelovskou grupu generovanou symboly (M), kde M jsou reprezentanti své třídy izomorfismu v C (předpoklad malého skeletu zaručuje, že univerzum F je množina). Podgrupa (relací) F_0 ať je generovaná prvky $(M) - (N) - (L)$ pro každou krátkou exaktní posloupnost $0 \to L \to M \to N \to 0$, kde BÚNO předpokládáme, že K, L a M jsou námi zvolení reprezentanti. Definujme Grothendieckovu grupu kategorie C jako faktorgrupu F/F_0 a pro každý S-modul M, označme $[M]$ prvek F/F_0 příslušný modulu M.

Zde pracujeme zpravidla s kategoriemi konečně generovaných modulů, takové kategorie malý skelet mají. A krátké exaktní posloupnosti budeme chápat tak, jak se klasický zavádí v kategoriích pravých modulů.

Nechť C a D jsou nějaké kategorie modulů né nutně stejného okruhu a G, H jsou jejich Grothendieckovy grupy. Dále mějme funktor $F : C \to D$, budeme říkat, že F definuje homomorfismus Grothendieckových grup, jestliže existuje zobrazení $f : G \to H$, že pro každý M, modul kategorie C, platí

$$f([M]) = [F(M)]. \tag{2.2}$$

Je jasné, že jestliže homomorfismus f existuje, je určen vztahem 2.2 jednoznačně. Má proto dobrý smysl říkat: funktor F definuje homomorfismus f.

Každý exaktní funktor zachovává krátké exaktní posloupnosti, čili zachovává grupy relací, podle níž v definici Grothendieckovy grupy faktorizujeme. Odtud každý exaktní funktor definuje homomorfismus Grothendieckových grup.

Pro okruh S označme $K_0(S)$ Grothendieckovu grupu kategorie konečně generovaných projektivních pravých S-modulů a $G_0(S)$ Grothendieckovu grupu kategorie konečně generovaných pravých S-modulů.

Lemma 17. *Nechť S je Artinovský okruh a V_1,...,V_m je kompletní sada jednoduchých S-modulů, potom*

$$G_0(S) \cong \oplus_{i=1}^{m} \mathbb{Z}[V_i]. \tag{2.3}$$

Důkaz. Celý důkaz je v [3, lemma 16.6], zde dokáži jen jak libovolný $[M]$, kde M je konečně generovaná S-modul, vyjádřit jako $\mathbb{Z}$-kombinaci prvků $\{[V_i]\}_{i=1}^{m}$, což

nám dá představu o významu koeficientů při $[V_i]$. Buď M konečně generovaný S-modul. Protože S je Artinovský, M má konečnou kompoziční řadu $M = M_0 \supseteq M_1 \supseteq ... \supseteq M_t = 0$. Pro $i \in 1,...,t$ nám krátká exaktní posloupnost

$$0 \to M_i \to M_{i-1} \to M_{i-1}/M_i \to 0,$$

kde druhý homomorfismus je inkluze a třetí přirozená projekce, dává vztah $[M_{i-1}] = [M_i] + [M_{i-1}/M_i]$. Snadno se indukcí dokáže, že

$$[M] = [M_0/M_1] + [M_1/M_2] + ... + [M_{t-1}].$$

❑

Zadávají-li dva konečně generované S-moduly, kde S je Artinovský okruh, stejný prvek v $G_0(S)$, nemusí být ještě nutně izomorfní, ale jejich kompoziční řady musí mít až na pořadí stejné faktory (včetně násobností).

Lemma 18 ([3], lemma 16.7)**.** *Nechť S je semiperfektní okruh a $W_1,...,W_r$ je kompletní sadou nerozložitelných konečně generovaných projektivních S-modulů, potom*

$$K_0(S) \cong \oplus_{i=1}^{r} \mathbb{Z}[W_i].$$

Věta 19. *Je-li (k,R,K) p-modulární systém, potom zobrazení*

$$- \otimes_R K : Proj(RG) \to Mod(KG)$$

zadává grupový homomorfismus $e : K_0(RG) \to G_0(KG)$ takový, že $e([M]) = [M \otimes_R K]$.

Důkaz. Protože funktor ve znění věty je zjevně exaktní, je homomorfismus e dobře definován.

❑

KG je podle Maschkeho věty totálně rozložitelný. Z lemmatu 17 je $[Z_1],...,[Z_s]$ volnou bází $G_0(KG)$. Podobně, podle Lemmatu 18 je $[P_1],...,[P_r]$ volnou bází $K_0(RG)$. Označme E matici homomorfismu e z věty 19 vyjádřeného vůči právě popsaným bázím.

Konečně generovaný projektivní RG-modul P má podle věty 10 jednoznačné vyjádření $P \cong P_1^{\alpha_1} \oplus \cdots \oplus P_r^{\alpha_r}$. Z definice Grothendieckovy grupy platí $[P] = \alpha_1[P_1] + \ldots + \alpha_r[P_r]$. Protože $[P_1],...,[P_r]$ je volnou bází, je P až na izomorfismus jednoznačně určen prvkem $[P]$. Z totální rozložitelnosti KG a jednoznačnosti rozkladu na jednoduché KG-moduly lze analogickou úvahou jako výše ověřit, že každý konečně generovaný KG-modul M je až na izomorfismus určen prvkem $[M] \in G_0(KG)$. Proto při přechodu ke Grothendieckovým grupám a zobrazení e neztratíme žádnou informaci o chování funktoru $- \otimes_{\mathbb{Z}_{(p)}} K : Proj(RG) \to Mod(KG)$.

Z definice báze existuje právě jeden homomorfismus $f : K_0(RG) \to K_0(kG)$ definovaný na bázových prvcích vztahem $f[P_i] = [\bar{P}_i] = [U_i]$. Homomorfismus f splňuje $f[P] = [\overline{P}]$, pro každý P konečně generovaný projektivní RG-modul: Je-li $P \cong P_1^{\alpha_1} \oplus ... \oplus P_r^{\alpha_r}$, pak

$$f[P] = f(\sum_{i=1}^{r} \alpha_i[P_i]) = \sum_{i=1}^{r} \alpha_i f([P_i]) = \sum_{i=1}^{r} \alpha_i[\bar{P}_i] = [\oplus_{i=1}^{r} \bar{P}_i^{\alpha_i}].$$

Poslední výraz se rovná $[\overline{P}]$, protože redukce modulo N zachovává direktní sumy. Homomorfismus f je zřejmě izomorfismus. Předefinujme zobrazení e na $e \circ f^{-1}$, kde f je právě popsaný izomorfismus. Protože matice zobrazení f vůči bázím $\{[P_i]\}_{i=1}^r$ a $\{[U_i]\}_{i=1}^r$ je I_r, zůstane matice E pro předefinované zobrazení e nezměněná. Odtud tedy budeme písmenem e značit grupový homomorfismus z $K_0(kG)$ do $G_0(KG)$.

Definice 9. *RG-modul M nazveme RG-mříží, má-li M jakožto R-modul konečnou volnou bázi.*

Z každé RG-mříže M můžeme vytvořit KG-modul $M \otimes_R K$ a kG-modul $\overline{M}$, přičemž oba jsou konečně generované. Stručně popíši jak vypadají jim příslušné reprezentace.

Je-li M RG-mříž s volnou bází $m_1,...,m_l$, pak každý automorfismus R-modulu M můžeme vůči této bázi vyjádřit maticově. Odtud $Aut_R(M) \cong GL(l,R)$. RG-mříž M proto zadává R-reprezentaci φ grupy G, kterou lze vyjádřit v maticové podobě.

Lze dokázat, že v kG-modulu $\overline{M} = M/MN$ jsou prvky $\overline{m_1},...,\overline{m_l}$ volnou k-bází. Označme $\overline{\varphi}$ k-reprezentaci G danou $\overline{M}$. Pro každé $g \in G$ a $m \in M$ je $\overline{\varphi}(g)(\overline{m}) = \overline{\varphi(g)(m)}$. Přejdeme-li do maticového popisu obou reprezentací vůči popsaným bázím, pak redukce modulo N působí po prvcích matic, neboli prvky matice reprezentace po redukci jsou redukce příslušných prvků matice reprezentace před redukcí.

Podobně v KG-modulu $M \otimes_R K$ je $m_1 \otimes 1,...,m_l \otimes 1$ volnou K-bází. K-reprezentace grupy G zadaná modulem $M \otimes_R K$, označme ji psi, splňuje pro každé $g \in G$ vztah $\psi(g) = \varphi(g) \otimes id_K$. Vyjádříme-li ψ maticově vůči bázi $m_1 \otimes 1,...,m_l \otimes 1$, dostaneme pro každý $g \in G$ stejnou matici jako ve vyjádření φ vůči bázi $m_1,...,m_l$. Sjednotíme-li M s $M \otimes 1 \subseteq M \otimes_R K$, pak právě popsaný vztah M a $M \otimes_R K$ vystihuje následující definice.

Definice 10. *Pro V konečně generovaný KG-modul nazveme RG-mříž $M \subseteq V$ úplnou ve V, jestliže $KM = V$.*

Lemma 20 ([3], lemma 16.15)**.** *Každý konečně generovaný KG-modul má úplnou RG-mříž.*

Neboli, existuje volná báze, vůči níž má K-reprezentace maticové vyjádření s prvky v okruhu R. Čili, každá K-reprezentace grupy G je K-ekvivalentní reprezentaci definované nad R. Obecně neplatí, že každé dvě úplné RG-mříže M_1, M_2 v KG-modulu V jsou izomorfní RG-moduly. Nicméně jejich redukce modulo N mají jakožto kG-moduly stejné kompoziční faktory, čili zadávají stejný prvek v $G_0(kG)$.

Lemma 21 ([3], lemma 16.16)**.** *Buď M_1 a M_2 dvě úplné RG-mříže konečně generovaného KG-modulu V, potom kG-moduly $\overline{M_1}$ a $\overline{M_2}$ zadávají stejný prvek v $G_0(kG)$.*

Věta 22 ([3], lemma 16.17)**.** *Existuje grupový homorfismus $d : G_0(KG) \to G_0(kG)$ takový, že $d : [V] \mapsto [\overline{M}]$ pro M úplnou RG-mříž ve V.*

Definice 11. *Zobrazení d z předchozí věty budeme nazývat dekompoziční zobrazení a matici D danou zobrazením d, vyjádřeného vůči bázím $[Z_1],...,[Z_s]$ a $[F_1],...,[F_r]$, nazveme dekompoziční matice.*

Buď T těleso a M a N ať jsou TG-moduly. Definujme číslo

$$i(M,N) = dim_T Hom_{TG}(M,N).$$

V anglické literatuře se nazývá intertwining number (volný překlad by tedy mohlo být například index splétavosti). Jedná se o modulární analogii skalárního součinu charakterů, klasicky zaváděného v teorii reprezentací. Pomocí indexu splétavosti definujeme dvě bilineární formy na Grothendieckových grupách:

Lemma 23. *Existuje $\mathbb{Z}$-bilineární forma $i_K : G_0(KG) \times G_0(KG) \to \mathbb{Z}$ taková, že pro každé dva KG-moduly M a N platí*

$$i_K([M],[N]) = i(M,N), \tag{2.4}$$

navíc $i_K([Z_i],[Z_j]) = \delta_{i,j}$.

Důkaz. Definujme i_K nejprve na bázových prvcích vztahem (2.4), a pak lineárně dodefinujme na celé $G_0(KG) \times G_0(KG)$. Je třeba ověřit, že pro každé dva konečně generované KG-moduly M a N skutečně platí $i_K([M],[N]) = i(M,N)$. Protože KG je totálně rozložitelný okruh, jsou oba funktory $Hom_{KG}(M,-)$ i $Hom_{KG}(-,M)$ exaktní pro každý konečně generovaný KG-modul M. Navíc v $Mod(KG)$ se každá krátká exaktní posloupnost štěpí, čili oba funktory zachovávají konečné direktní sumy. Proto pro libovolné dva konečně generované KG-moduly $M = \oplus_{i=1}^{s} Z_i^{\alpha_i}$ a $N = \oplus_{i=1}^{s} Z_i^{\beta_i}$ je:

$$Hom_{KG}(M,N) \cong \bigoplus_{i,j=1}^{s} Hom_{KG}(Z_i,Z_j)^{\alpha_i\beta_j}.$$

Přechodem k dimenzím dostaneme

$$i(M,N) = \sum_{i,j=1}^{s} \alpha_i\beta_j \cdot i(Z_i,Z_j) = i_K(M,N).$$

Zbývá dokázat podmínku ortogonality bázových prvků. Pro $i \neq j$ je zřejmě $i(Z_i,Z_j) = 0$. Protože K je rozkladové pro G, je podle [4, lemma 29.13] $Hom_{KG}(Z_i,Z_i) \cong K$, přechodem k K-dimenzi dostaneme $i_K([Z_i],[Z_i]) = 1$.

❑

Lemma 24 ([3], lemma 18.8)**.** *Je-li k rozkladové těleso pro grupu G, pak existuje $\mathbb{Z}$-bilineární forma $i_k : K_0(kG) \times G_0(kG) \to \mathbb{Z}$ taková, že pro každé U a M konečně generované kG-moduly, kde U je navíc projektivní, platí:*

$$i_k([U],[M]) = i(U,M). \tag{2.5}$$

Navíc $i_k([U_i,F_j]) = \delta_{i,j}$, kde $\delta_{i,j}$ je Kroneckerovo delta.

Poznamenám, že bilineární formy z předchozích dvou lemmat jsou vztahy (2.4) a (2.5) definovány jednoznačně. Můžeme proto symboly i_K a i_k pevně označit bilineární formy jednoznačně definované vzorci (2.4) a (2.4). i_K a i_k dávají do souvislosti zobrazení d a e v klíčovém vzorci:

Věta 25 ([3], věta 18.9)**.** *Pro výše definovaná zobrazení e a d platí*

$$i_k(u,d(z)) = i_K(e(u),z),$$

kde u je libovolný prvek $K_0(KG)$ a z libovolný prvek $G_0(KG)$.

Snadným důsledkem je následující lemma.

Lemma 26. *Matici E získáme transponováním matice D, neboli $E = D^T$.*

Důkaz. Přímo z definice matic E a D máme vztahy:

$$e[U_i] = e_{1i}[Z_1] + ... + e_{ji}[Z_j] + ... + e_{si}[Z_s],$$

$$d[Z_j] = d_{1j}[F_1] + ... + d_{ij}[F_i] + ... + d_{rj}[F_r].$$

Z ortogonality bází $\{[Z_i]\}_{i=1}^s$ a $\{[F_i]\}_{i=1}^r$ vůči Z-bilineárním formám i_K a i_k a předchozí věty dostáváme:

$$d_{ij} = i_k([U_i],d[Z_j]) = i_K(e[U_i],[Z_j]) = e_{ji}.$$

❑

Po zbytek této kapitoly se zaměříme na to, jak spočítat dekompoziční matici D.

2.3 Výpočet dekompoziční matice pomocí Braeurových charakterů

Pracujeme pořád s p-modulárním systémem (k, R, K) z předešlých sekcí. Protože každý konečně generovaný KG-modul M zadává K-reprezentaci grupy G konečné dimenze, můžeme definovat charakter modulu M, jako charakter mu příslušné reprezentace. Dále symbolem $cf(KG)$ budeme značit množinu všech funkcí z G do K, konstantních na třídách konjugace grupy G. Na $cf(KG)$ lze zřejmým způsobem definovat strukturu K-vektorového prostoru. Vektorový prostor $cf(KG)$ zahrnuje i všechny charaktery KG-modulů, můžeme proto definovat $ch(KG)$ jako podgrupu aditivní grupy $cf(KG)$, generovanou všemi charaktery modulů z $Mod(KG)$. Symboly $\zeta_1,...,\zeta_s$ označme charaktery KG-modulů $Z_1,...,Z_s$.

Lemma 27 ([3])**.** *Funkce $\zeta_1,...,\zeta_s$ tvoří volnou bázi grupy $ch(KG)$.*

Lemma 28 ([3], lemma 16.10)**.** *Grupy $G_0(KG)$ a $ch(KG)$ jsou izomorfní skrze izomorfismus $\alpha : G_0(KG) \to ch(KG)$, kde α přiřazuje prvku $[M]$, pro libovolný $M \in Mod(KG)$, charakter modulu M.*

Podobný izomorfismus existuje pro grupu $G_0(kG)$ a takzvané Braeurovy charaktery. Aby bylo možné Braeurovy charaktery definovat, musí těleso K obsahovat primitivní m-tou odmocninu z 1, kde $m \in \mathbb{N}$ je největší dělitel řádu grupy G nedělitelný prvočíslem p. V $\mathbb{Q}$ nastane problém už pro grupu S_3, tuto vadu ošetřím v závěru kapitoly přechodem k většímu p-modulárnímu systému, který ovšem zachová matici D. Pracujme tedy nejprve obecně s p-modulárním systémem, kde potřebné odmocniny máme.

Ať G je grupa a p prvočíslo, označme $G_p \subseteq G$ množinu všech prvků majících řád nedělitelný prvočíslem p. Takové prvky budeme nazývat p-regulárními. Vyjádřeme řád grupy G ve tvaru $\mid G \mid = mp^k$, kde p nedělí m a předpokládejme, že K obsahuje primitivní m-tou odmocninu z 1, označme ji ω. Polynom $x^m - 1$ se v $R[x]$ rozkládá na lineární faktory $x^m - 1 = \prod_{i=1}^{m}(x - \omega^i)$, tudíž v $k[x]$ platí $x^m - \overline{1} = \prod_{i=1}^{m}(x - \overline{\omega}^i)$. Protože p, charakteristika tělesa k, nedělí m, jsou kořeny polynomu $x^m - \overline{1}$ po dvou různé (formální derivace nemá s původním polynomem žádný společný kořen). Odtud redukce modulo N definuje izomorfismus cyklických grup $\langle\overline{\omega}\rangle$ a $\langle\omega\rangle$ (daný předpisem $\overline{\omega}^i \mapsto \omega^i$).

Uvažme nyní konečně generovaný kG-modul M, ten dává k-reprezentaci $\overline{\varphi}$ grupy G dimenze d. Písmenem $\overline{\lambda}$ označme její charakterovou funkci. Z definice charakteru víme, že pro každé g, p-regulární prvek grupy G, je $\overline{\lambda}(g) = Tr(\overline{\varphi})$, což je rovno součtu vlastních čísel zobrazení $\overline{\varphi}$, označme je $\{\lambda_j\}_{j=1\ldots,d}$. Dále ze vztahu $id_M = \overline{\varphi}(g)^{mp^k}$ pro každé λ_* platí $1 = \lambda_*^{mp^k} = \lambda_*^m$ (druhá z rovností platí protože počítáme v tělese charakteristiky p). Každé λ_j je tedy tvaru $\overline{\omega}^{i_j}$. Můžeme proto prvku g přiřadit číslo $\lambda(g) = \omega^{i_1} + \ldots + \omega^{i_d}$.

Definice 12. *Buď M kG-modul, právě popsané zobrazení $\lambda : G_p \to K$ nazveme Braeurovým charakterem modulu M.*

Označme $cf_K(G_p)$ K-vektorový prostor všech funkcí z G_p do K, které jsou konstantní na třídách konjugace G. Z konstrukce Braeurových charakterů je zřejmé, že naleží do $cf_K(G_p)$. Dále označme $\varphi_1,\ldots,\varphi_r$ Braeurovy charaktery modulů $F_1,\ldots,F_r$. Následující dvě lemmata jsou analogiemi lemmat 27 a 28 pro Braeurovy charaktery.

Lemma 29 ([3], lemma 17.9)**.** *Funkce $\varphi_1,\ldots,\varphi_r$ jsou K-bázi $cf_K(G_p)$.*

Definice 13. *Podgrupu aditivní grupy $cf_K(G_p)$ generovanou všemi Braeurovými charaktery konečně generovaných kG-modulů budeme značit $Bch(kG)$ a její prvky budeme nazývat virtuální Braeurovy charaktery.*

Lemma 30 ([3], lemma 17.14)**.** *Grupy $G_0(kG)$ a $Bch(kG)$ jsou izomorfní, skrze izomorfismus $\beta : G_0(kG) \to Bch(kG)$, který každému prvku $[M]$, kde M je kG-modul, přiřadí Braeurův charakter modulu M.*

Věta 31 ([3], věta 17.15)**.** *Ať α je izomorfismus z lemmatu 28, β izomorfismus z lemmatu 30 a $d' : Ch(KG) \to Bch(kG)$, zobrazení restrikce na G_p. Potom následující diagram komutuje:*

$$\begin{tikzcd} G_0(KG) \arrow[r, "\alpha"] \arrow[d, "d"'] & Ch(KG) \arrow[d, "d'"] \\ G_0(kG) \arrow[r, "\beta"] & Bch(kG) \end{tikzcd}$$

Poznámka: Každý Braeurův charakter lze podle [3, lemma 18.12] dodefinovat na celé G tak, že výsledná funkce λ lze zapsat jako celočíselnou kombinaci charakterů K-reprezentací, neboli λ je prvek $ch(KG)$. To nám spolu s komutativitou diagramu výše říká, že zobrazení d je na.

Uvažme $\zeta_1',\ldots,\zeta_s'$, restrikce charakterů $\zeta_1,\ldots,\zeta_s$ na p-regulární prvky grupy G (symboly ζ_* jsme na začátku sekce označili charaktery KG-modulů Z_*). Z předchozí věty dostáváme vzorce:

$$\zeta'_j = d_{1j}\varphi_1 + ... + d_{rj}\varphi_r, \tag{2.6}$$

pro každé $j = 1,...,r$. Tyto vzorce již dávají způsob, jak spočítat matici D, a tedy užitím lemmatu 26 i matici E, kterou hledáme.

Pro ošetření faktu, že v $\mathbb{Q}$ nemáme primitivní m-té odmocniny z 1 pro $m \geq 3$, přejdeme k okruhu $\mathbb{Z}_{(p)}[\omega]$, kde ω, je primitivní odmocnina z 1 potřebného řádu. V dalším definuji rozšíření p-modulárního systému konečného stupně a ukáži, že rozkladovost těles $\mathbb{Q}$ a $\mathbb{Z}_p$ pro grupu S_n zaručí, že přechod k rozšířenému p-modulárnímu systému nezmění matici D.

Ať (k,R,K) je p-modulární systém. Okruh R je jakožto DVR speciálně Dedekindovým okruhem. Označme $K' = K(\omega)$, jedná se o rozšíření konečného stupně, proto je okruh R_0, definovaný jako celistvý uzávěr R v K', Dedekindovým okruhem. V R_0 volme nějaký maximální ideál N_0, protože R_0 je celistvý uzávěr R v K', je $R \cap N_0 = N$ maximální v R. Dále definujme okruh R' jako lokalizaci R_0 v ideálu N_0. Prvek ω z definice celistvého uzávěru je prvkem okruhu R_0, a tedy i okruhu R'. Protože R_0 je Dedekindův okruh, R' je DVR s maximálním ideálem N'. Definujme $k' = R'/N'$. Dále pak označme $i' : R \to R'$ a $i_0 : R \to R_0$ zobrazení inkluze a $\pi' : R' \to k'$ a $\pi_0 : R_0 \to R_0/N_0$ přirozené projekce. Sjednotíme-li izomorfní residuová tělesa $k' = R'/N' \cong R_0/N_0$, bude platit $\pi' \circ i' = \pi_0 \circ i_0$ a z $R \cap N_0 = N$ je $ker(\pi_0 \circ i_0) = N$. Odtud se $\pi' \circ i'$ faktorizuje přes k a definuje prosté vnoření $k \hookrightarrow k'$. Můžeme se proto dívat na k' jako na tělesové rozšíření $k(\overline{\omega})$. Jistě platí, že K' je podílové těleso R' charakteristiky 0 a k' těleso charakteristiky p. Trojice (k', R', K') je proto p-modulární systém.

Definice 14. *Právě zkonstruovaný p-modulární systém* (k',R',K') *budeme nazývat rozšíření p-modulárního systému* (k,R,K) *konečného stupně.*

Nyní z každého KG-modulu M můžeme pomocí operace rozšíření skalárů vytvořit $K'G$-modul $M \otimes_K K'$ se skalárním násobením: $(m \otimes r)(\sum_{g \in G} r_g g) = \sum_{g \in G} mg \otimes r_g r$. Protože K' je komutativní, jedná se o korektní definici pravého $K'G$-modulu. Analogicky z každého kG-modulu můžeme vytvořit $k'G$-modul.

Lemma 32 ([3], lemma 16.22)**.** *Je-li* (K',R',k') *rozšíření p-modulárního systému* (K,R,k) *konečného stupně, potom operace rozšíření skalárů zadává aditivní homomorfismy*

$$\varphi : G_0(KG) \to G_0(K'G), \chi : G_0(kG) \to G_0(k'G).$$

Tyto homomorfismy jsou navíc prosté.

Označme pro $i = 1, \ldots, s$ $K'G$-moduly $Z'_i = Z_i \otimes_K K'$. Jsou-li $\lambda_1,...,\lambda_s \in \mathbb{N}$ takové, že $KG_{KG} \cong {Z_1}^{\lambda_1} \oplus \cdots \oplus {Z_s}^{\lambda_s}$, je $K'G_{K'G} \cong {Z'_1}^{\lambda_1} \oplus \cdots \oplus {Z'_s}^{\lambda_s}$ (tensorové násobení zachovává direktní sumy). Z rozkladovosti K pro grupu G je každý Z'_i ireducibilní, čili $K'G$-moduly $Z'_1, \ldots, Z'_s$ jsou kompletní sadou jednoduchých $K'G$-modulů. Odtud je φ z předchozího lemmatu na, tedy izomorfismus. Navíc, vyjádříme-li φ maticově vůči bázím $\{Z_i\}_{i=1}^s$ a $\{Z'_i\}_{i=1}^s$, dostaneme jednotkovou matici.

Budeme potřebovat několik vzorců z tensorového násobení. Ať S a T jsou komutativní okruhy a M SG-modul platí:

$$M \otimes_S S \cong M, \tag{2.7}$$

skrze S-izomorfismus posílající $m \otimes s$ na ms. Definujeme-li na levé straně strukturu SG-modulu (podobně jako u operace rozšiřování skalárů), jedná se dokonce o SG-izomorfismus. Dále ať je K (S,T)-bimodul a L levý T-modul. Potom

$$(M \otimes_S K) \otimes_T L \cong M \otimes_S (K \otimes_T L). \tag{2.8}$$

skrze izomorfismus posílající $(m \otimes k) \otimes l$ na $m \otimes (k \otimes l)$, kde izomorfismus je míněn jako izomorfismus pravých S-modulů a levých T-modulů. Vzorec lze opět chápat i jako SG-izomorfismus resp. TG-izomorfismus, dodefinujeme-li na obou stranách zřejmým způsobem násobení prvky G.

Předchozí dva vzorce jsou obecně známé, odvodíme pomocí nich třetí, který se bude hodit v důkazu lemmatu 33. Mějme navíc komutativní okruh U a okruhové homomorfismy $\alpha : S \to T$, $\beta : T \to U$. Čili T i U mají strukturu S-modulu a U má strukturu T-modulu (všechny přirozeně definované). Potom

$$(M \otimes_S T) \otimes_T U \cong M \otimes_S U \tag{2.9}$$

jakožto U-moduly. Použijeme-li na levou stranu vzorec (2.8) a následně na vnitřek závorky analogii (2.7) pro levý modul, dostaneme pravou stranu vzorce (2.9). Izomorfismus je dán vzorcem $(m \otimes t) \otimes u \mapsto m \otimes tu$. A stejně jako u předchozích lze vzorec rozšířit na UG-izomorfismus. Vzorec (2.9) budeme užívat v situacích, kdy volba homomorfismů α, β bude zřejmá: zobrazení inkluze nebo projekce.

Lemma 33. *Nechť (k', R', K') je konečné rozšíření p-modulárního systému (K, R, k). Dále ať φ a χ jsou homomorfismy z lemmatu 32 a d' dekompoziční zobrazení pro rozšířený p-modulární systém. Pak následující diagram komutuje*

$$\begin{tikzcd} G_0(KG) \arrow[r, "\varphi"] \arrow[d, "d"] & G_0(K'G) \arrow[d, "d'"] \\ G_0(kG) \arrow[r, "\chi"] & G_0(k'G) \end{tikzcd}$$

Důkaz. Prvně interpretujeme zobrazení redukce modulo N v řeči tensorů: Mějme R-modul M, je známý fakt, že tensorové násobení je zprava exaktní, proto je posloupnost

$$M \otimes_R N \to M \otimes_R R \to M \otimes_R k \to 0$$

exaktní. Z (2.7) platí $M \otimes_R R \cong M$ skrze izomorfismus posílající $m \otimes r$ na mr. Můžeme proto prostřední člen nahradit RG-modulem M, čímž se obraz prvního homomorfismu stává MN. Užitím exaktnosti v M a první věty o izomorfismu dostáváme $M \otimes_R k \cong M/MN = \overline{M}$. Díváme-li se na vztah jako izomorfismus kG-modulů, dostáváme hledaný popis.

Berme KG-modul V a v něm úplnou RG-mříž M. Dokáži, že $M \otimes_R R'$ je jakožto $R'G$-modul izomorfní úplné $R'G$-mříži v $V \otimes_K K'$: Z definice mříže existuje přirozené λ že $M \cong \oplus_{i=1}^{\lambda} R$ jakožto R-modul. Protože tensorový součin zachovává direktní sumy, platí:

$$M \otimes_R R' \cong (\oplus_{i=1}^{\lambda} R) \otimes_R R' \cong \oplus_{i=1}^{\lambda} (R \otimes_R R') \cong \oplus_{i=1}^{\lambda} R'.$$

Na vzorec se můžeme dívat jako na R'-izomorfismus, odtud plyne existence volné R'-báze.

Uvažme následující $K'G$-izomorfismy dané vzorcem (2.9) a faktem, že M je úplnou RG-mříží ve V, čili $M \otimes_R K \cong V$:

$$(M \otimes_R R') \otimes_{R'} K' \cong M \otimes_R K' \cong (M \otimes_R K) \otimes_K K' \cong V \otimes_K K'.$$

Jejich složením dostaneme $K'G$-izomorfismus F, pro něž je snadné spočítat, že

$$F : (m \otimes r) \otimes t \mapsto m \otimes rt. \tag{2.10}$$

Podle výše dokázaného je $M \otimes_R R'$ jakožto R'-modul volný, speciálně plochý. Jím zadaný funktor $(M \otimes_R R') \otimes_{R'} -$ proto zachovává prostotu homomorfismů. Odtud je $id \otimes i : (M \otimes_R R') \otimes_{R'} R' \to (M \otimes_R R') \otimes_{R'} K'$, kde $i : R' \to K'$ je inkluze, prostý. Složíme-li jej zleva s izomorfismem daným vzorcem (2.7) a zprava s izomorfismem F, chápaným jako $R'G$-izomorfismus, dostaneme prostý $R'G$-homomorfismus $H : M \otimes_R R' \to V \otimes_K K'$. $Im(H)$ je proto $R'G$-mříž, a navíc úplná, protože prvky tvaru $m \otimes rt$, kde $m \in M$, $r \in R'$, $t \in K'$, generují podle (2.10) $Im(F) = V \otimes_K K'$.

Horní pravá cesta v diagramu: Rozepisováním definice a výše dokázaným odvodíme

$$d' \circ \varphi([V]) = d'([V \otimes_K K']) = [\overline{M \otimes_R R'}] = [(M \otimes_R R') \otimes_{R'} k'].$$

Užitím vzorce (2.9) dostaneme $[(M \otimes_R R') \otimes_{R'} k'] = [M \otimes_R k']$.

Druhá cesta: Podobně odvodíme

$$\chi \circ d([V]) = \chi([\overline{M}]) = \chi([M \otimes_R k]) = [(M \otimes_R k) \otimes_k k'].$$

Užitím vzorece (2.9) dostaneme $[(M \otimes_R k) \otimes_k k'] = [M \otimes_R k']$. Protože prvky tvaru $[V]$, kde V je KG-modul, generují grupu $G_0(KG)$, je komutativita dokázána. ❑

Z komutativity snadno plyne, že χ je na, čili izomorfismus: φ je jak jsme již dokázali izomorfismus a d' je podle poznámky za větou 31 na. Vyjádříme-li zobrazení v komutativním diagramu výše maticově vůči bázím $\{Z_i\}_{i=1}^s$, $\{Z'_i\}_{i=1}^s$, $\{F_i\}_{i=1}^r$ a $\{F'_i\}_{i=1}^r$, zobrazení φ a χ dají jednotkové matice I_s a I_r. Matici zobrazení d' označme D'. Z komutativity platí $D' \cdot I_s = I_r \cdot D$, čili $D = D'$.

Kapitola 3

výpočet

Všechny tabulky které ve výpočtu užijeme byly spočteny pomocí on-line kalkulátoru *Magma*, dostupného z *http://magma.maths.usyd.edu.au/calc/*.

3.1 grupa S_7

Ukáži, že v grupovém okruhu $\mathbb{Z}S_7$ existuje vlastní idempotentní ideál, který v $\mathbb{Q}S_n$ generuje vlastní ideál, různý od ideálu z lemmatu 1. Výpočet bude následující: Nejprve užitím vzorce (2.6)

$$\zeta'_j = d_{1j}\varphi_1 + ... + d_{rj}\varphi_r$$

spočítáme dekompoziční matice $D_p = \{d^p_{ij}\}_{ij}$ pro p-modulární systémy ($\mathbb{Z}_p$,$\mathbb{Z}_{(p)}$,$\mathbb{Q}$) s grupou S_7, kde $p \in \{2,3,5,7\}$. Jim příslušné matice E_p dostaneme z lematu 26 transponováním. Dále pomocí věty 15 získáme pro jednotlivá p popis zobrazení $i_p : Id(\mathbb{Z}_{(p)}S_n) \to Id(\mathbb{Q}S_n)$. Nalezneme-li v

$$\bigcap_{p\in\{2,3,5,7\}} Im(i_p)$$

vlastní ideál, různý od těch ve znění hypotézy, dostaneme z věty 2 existenci ideálu vyvracejícího zkoumanou hypotézu.

Z [4, věta 27.22] víme, že $\mathbb{Q}S_7$ má počet různých ireducibilních reprezentací roven počtu tříd konjugace S_7, což je 15. Označme ζ^7_i, $i = 1,\ldots,15$, jim příslušné charaktery, jejich explicitní zápis je v tabulce 4.5. Dále z [3, důsledek 17.11] je r_p, počet různých jednoduchých $\mathbb{Z}_pS_7$-modulů, roven počtu tříd konjugace S_7 odpovídajících p-regulárním prvkům. Čili $r_2 = 5$, $r_3 = 9$, $r_5 = 13$ a $r_7 = 14$. Označme φ^p_i, $i = 1,\ldots,r_p$ Braeurovy charaktery příslušné jednotlivým jednoduchým $\mathbb{Z}_pS_7$-modulům. Explicitní vyjádření lze nalézt v tabulkách 4.1 až 4.4. Dále označme $\{P^p_i\}^{r_p}_{i=1}$ projektivní moduly z věty 10 pro okruh $\mathbb{Z}_pS_7$, indexované tak, že $\overline{P^p_i}$ má Braeurův charakter φ^p_i.

Lemma 29 zaručuje existenci a jednoznačnost prvků d^p_{ij} ve vzorci (2.6). Protože matice D^7_* vychází v tomto případě dosti řídké, lze je ze vzorce (2.6) zcela přímočaře spočítat.

$$E_2^{7T} = D_2^7 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$E_3^{7T} = D_3^7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$E_5^{7T} = D_5^7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$E_7^{7T} = D_7^7 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Při přechodu ke stopovým ideálům nás nezajímají konkrétní hodnoty prvků matic E_*^7, ale pouze zda jsou nulové, či nenulové. Z věty 15 pro každý idempotentní ideál $I_i^p = Tr_{\mathbb{Z}_{(p)}S_7}(P_i^p)$, $i = 1, \ldots, r_p$, platí:

$$\mathbb{Q}I_i^p = \bigoplus_{j=1\ldots,r_p,e_{i,j}^p\geq 1}^{s_p} B_j,$$

kde B_*, jsou oboustranné idempotentní ideály okruhu $\mathbb{Q}S_n$ ze vzorce 1.5, indexované tak, že B_j je stopový ideál $\mathbb{Q}S_7$-modulu s charakterem ζ_j^7.

Neboli sloupce matic E_p^7, respektive řádky matice D_p^7, zadávají ideály $\mathbb{Q}I_i^p$ vyjádřené jako direktní sumy ideálů B_j.

Z matic E_*^7 lze snadno vyčíst, že ideály

$$I_1 = \oplus_{j=3}^{15} B_j$$

a

$$I_2 = \oplus_{j=5}^{15} B_j$$

dokážeme pro všechna p vyjádřit jako $\mathbb{Q}I_p$, kde I_p je nějaký oboustranný idempotentní ideál v $\mathbb{Z}_{(p)}S_n$. Konkrétně bereme-li za I_p postupně pro $p = 2,3,5,7$ ideály:

$$\begin{aligned}
&\oplus_{i=2}^{5} I_i^2 a \oplus_{i=3}^{5} I_i^2,\\
&\oplus_{i=3}^{9} I_i^3 a \oplus_{i=5}^{9} I_i^5,\\
&\oplus_{i=3}^{13} I_i^5 a \oplus_{i=5}^{13} I_i^5,\\
&\oplus_{i=3}^{14} I_i^2 a \oplus_{i=5}^{14} I_i^2.
\end{aligned}$$

Věta 2 zaručuje existenci oboustranných idempotentních ideálů J_1, J_2 okruhu $\mathbb{Z}S_7$, že $\mathbb{Q}J_1 = I_1$ a $\mathbb{Q}J_2 = I_2$. Oba ideály jsou netriviální, alespoň jeden z nich musí být různý od ideálu z lemmatu 1.

Z matic můžeme vyčíst kolik oboustranných idempotentních ideálů v jednotlivých okruzích $\mathbb{Z}_{(p)}S_7$ generuje celý $\mathbb{Q}S_7$, jednoduchým kombinatorickým cvičením lze spočítat, že ony počty jsou postupně 4, 4, 9 a 3. Z věty 2 existuje v $\mathbb{Z}S_7$ 432 oboustranných idempotentních ideálů generující celé $\mathbb{Q}S_7$.

3.2 grupa S_5

Ukáži, že v případě S_5 hypotéza stále platí. Uvažme značení analogické předchozímu výpočtu, s tím rozdílem, že nás zajímají jen hodnoty $p = 2,3,5$. Čísla s a r_p se změní na: $s = 7$, $r_2 = 3$, $r_3 = 5$ a $r_5 = 6$. Stejným způsobem jako v předchozím spočteme z tabulek 4.6 až 4.9 matice E_2^5, E_3^5 a E_5^5:

$$E_2^{5T} = D_2^5 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$E_3^{5T} = D_3^5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$E_5^{5^T} = D_5^5 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Vlastní oboustranné idempotentní ideály v $\mathbb{Q}S_5$ budeme značit řádkovými vektory 0 a 1 délky 7. Technická pomůcka: budeme říkat, že ideál I dostaneme sečtením nějakých konkrétních řádků některé z matic D_*^5, pokud I dostaneme sečtením stopových ideálů příslušných řádků. Matice D_2^5 nám omezuje počet vlastních ideálů v

$$\bigcap_{p\in\{2,3,5\}} Im(i_p)$$

na 4 kandidáty. Tři dostaneme z jednotlivých řádků a čtvrtý sečtením druhého a třetího řádku:

$$\begin{aligned} I_1 &= \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \\ I_2 &= \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \\ I_3 &= \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \\ I_4 &= \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \end{aligned}$$

.

Abychom I_1 nasčítali z řádků matice D_5^5, museli bychom použít první řádek, ten si ale vynucuje 1 na 3. pozici, I_1 můžeme proto z kandidátů vyloučit. Podobně I_2 očividně nelze nasčítat z řádků D_3^5 ani D_5^5. I_3 si vynucuje v případě D_5^5 užití 3. nebo 4. řádku, oba ale mají 1 mimo poslední 3 pozice. Zbývá I_4, o kterém již víme, že jakožto poslední kandidát, musí být nasčítatelný z řádků všech tří matic. Lze snadno vidět, že to skutečně možné je, a to jediným způsobem. V $\mathbb{Z}S_5$ tedy existuje jediný vlastní oboustranný idempotentní ideál generující v $\mathbb{Q}S_5$ vlastní ideál.

Podíváme-li se kolika způsoby lze z řádků jednotlivých matic nasčítat celý okruh, dostaneme počet vlastních idempotentních oboustranných ideálů generující celé $\mathbb{Q}S_5$. V D_2^5 můžeme a nemusíme použít 3. řádek, to nám dává dvě možnosti. V případě D_3^5 je nutné užít všechny řádky, tedy jediná možnost. Konečně u matice D_5^5 je nutné použít 1., 2., 5., a 6. řádek. Dále pak můžeme použít libovolný z 3. a 4. řádku nebo oba. Máme tedy tři možnosti. Věta 2 zaručuje v $\mathbb{Z}S_5$ existenci šesti vlastních oboustranných idempotentních ideálů generující celý $\mathbb{Q}S_5$. Celkově je tedy $Id(\mathbb{Z}S_5)$ množina velikosti 9.

Kapitola 4

tabulky

$\mathbb{Z}_2$	id	(3)	(3)(3)	(5)	(7)
φ_1^2	1	1	1	1	1
φ_2^2	6	3	0	1	-1
φ_3^2	8	-4	2	-2	1
φ_4^2	14	2	-1	-1	0
φ_5^2	20	-4	-1	0	-1

Tabulka 4.1: Braeurovy charaktery pro $\mathbb{Z}_2 S_7$

$\mathbb{Z}_3$	id	(2)	(2)(2)(2)	(2)(2)	(4)	(4)(2)	(5)	(7)	(5)(2)
φ_1^3	1	1	1	1	1	1	1	1	1
φ_2^3	1	-1	-1	1	-1	1	1	1	-1
φ_3^3	6	4	0	2	2	0	1	-1	-1
φ_4^3	6	-4	0	2	-2	0	1	-1	1
φ_5^3	13	5	1	1	-1	-1	-2	-1	0
φ_6^3	13	-5	-1	1	1	-1	-2	-1	0
φ_7^3	15	5	-3	-1	1	-1	0	1	0
φ_8^3	15	-5	3	-1	-1	-1	0	1	0
φ_9^3	20	0	0	-4	0	0	0	-1	0

Tabulka 4.2: Braeurovy charaktery pro $\mathbb{Z}_3 S_7$

$\mathbb{Z}_5$	id	(2)	(2)(2)(2)	(2)(2)	(3)	(3)(3)	(4)	(4)(2)	(3)(2)(2)	(3)(2)	(6)	(7)	(4)(3)
φ_1^5	1	1	1	1	1	1	1	1	1	1	1	1	1
φ_2^5	1	-1	-1	1	1	1	-1	1	1	-1	-1	1	-1
φ_3^5	6	4	0	2	3	0	2	0	-1	1	0	-1	-1
φ_4^5	6	-4	0	2	3	0	-2	0	-1	-1	0	-1	1
φ_5^5	8	2	2	0	-1	-1	-2	0	3	-1	-1	1	1
φ_6^5	8	-2	-2	0	-1	-1	2	0	3	1	1	1	-1
φ_7^5	13	-3	1	1	-2	1	3	-1	-2	0	1	-1	0
φ_8^5	13	3	-1	1	-2	1	-3	-1	-2	0	-1	-1	0
φ_9^5	15	5	-3	-1	3	0	1	-1	-1	-1	0	1	1
φ_{10}^5	15	-5	3	-1	3	0	-1	-1	-1	1	0	1	-1
φ_{11}^5	20	0	0	-4	2	2	0	0	2	0	0	-1	0
φ_{12}^5	35	5	1	-1	-1	-1	-1	1	-1	-1	1	0	-1
φ_{13}^5	35	-5	-1	-1	-1	-1	1	1	-1	1	-1	0	1

Tabulka 4.3: Braeurovy charaktery pro $\mathbb{Z}_5 S_7$

$\mathbb{Z}_7$	id	(2)	(2)(2)(2)	(2)(2)	(3)	(3)(3)	(4)	(4)(2)	(5)	(3)(2)(2)	(3)(2)	(6)	(5)(2)	(4)(3)
φ_1^7	1	1	1	1	1	1	1	1	1	1	1	1	1	1
φ_2^7	1	-1	-1	1	1	1	-1	1	1	1	-1	-1	-1	-1
φ_3^7	5	3	-1	1	2	-1	1	-1	0	-2	0	-1	-2	-2
φ_4^7	5	-3	1	1	2	-1	-1	-1	0	-2	0	1	2	2
φ_5^7	10	2	-2	-2	1	1	0	0	0	1	-1	1	2	3
φ_6^7	10	-2	2	-2	1	1	0	0	0	1	1	-1	-2	-3
φ_7^7	14	6	2	2	2	-1	0	0	-1	2	0	-1	1	0
φ_8^7	14	-6	-2	2	2	-1	0	0	-1	2	0	1	-1	0
φ_9^7	14	-4	0	2	-1	2	2	0	-1	-1	-1	0	1	-1
φ_{10}^7	14	4	0	2	-1	2	-2	0	-1	-1	1	0	-1	1
φ_{11}^7	21	-1	3	1	-3	0	1	-1	1	1	-1	0	-1	1
φ_{12}^7	21	1	-3	1	-3	0	-1	-1	1	1	1	0	1	-1
φ_{13}^7	35	-5	-1	-1	-1	-1	1	1	0	-1	1	-1	0	1
φ_{14}^7	35	5	1	-1	-1	-1	-1	1	0	-1	-1	1	0	-1

Tabulka 4.4: Braeurovy charaktery pro $\mathbb{Z}_7 S_7$

S_7	id	(2)	(2)(2)(2)	(2)(2)	(3)	(3)(3)	(4)	(4)(2)	(5)	(3)(2)(2)	(3)(2)	(6)	(7)	(5)(2)	(4)(3)
ζ_1^7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
ζ_2^7	1	-1	-1	1	1	1	-1	1	1	1	-1	-1	1	-1	-1
ζ_3^7	6	4	0	2	3	0	2	0	1	-1	1	0	-1	-1	-1
ζ_4^7	6	-4	0	2	3	0	-2	0	1	-1	-1	0	-1	1	1
ζ_5^7	14	6	2	2	2	-1	0	0	-1	2	0	-1	0	1	0
ζ_6^7	14	4	0	2	-1	2	-2	0	-1	-1	1	0	0	-1	1
ζ_7^7	14	-4	0	2	-1	2	2	0	-1	-1	-1	0	0	1	-1
ζ_8^7	14	-6	-2	2	2	-1	0	0	-1	2	0	1	0	-1	0
ζ_9^7	15	5	-3	-1	3	0	1	-1	0	-1	-1	0	1	0	1
ζ_{10}^7	15	-5	3	-1	3	0	-1	-1	0	-1	1	0	1	0	-1
ζ_{11}^7	20	0	0	-4	2	2	0	0	0	2	0	0	-1	0	0
ζ_{12}^7	21	1	-3	1	-3	0	-1	-1	1	1	1	0	0	1	-1
ζ_{13}^7	21	-1	3	1	-3	0	1	-1	1	1	-1	0	0	-1	1
ζ_{14}^7	35	5	1	-1	-1	-1	-1	1	0	-1	-1	1	0	0	-1
ζ_{15}^7	35	-5	-1	-1	-1	-1	1	1	0	-1	1	-1	0	0	1

Tabulka 4.5: charaktery pro $\mathbb{Q}S_7$

S_7	id	(3)	(5)
φ_1^5	1	1	1
φ_2^5	4	1	-1
φ_3^5	4	-2	-1

Tabulka 4.6: Braeurovy charaktery pro $\mathbb{Z}_2 S_5$

S_7	id	(2)	(2)(2)	(4)	(5)
φ_1^3	1	1	1	1	1
φ_2^3	1	-1	1	-1	1
φ_3^3	4	2	0	0	-1
φ_4^3	4	-2	0	0	-1
φ_5^3	6	0	-2	0	1

Tabulka 4.7: Braeurovy charaktery pro $\mathbb{Z}_3 S_5$

S_7	id	(2)	(2)(2)	(3)	(4)	(3)(2)
φ_1^5	1	1	1	1	1	1
φ_2^5	1	-1	1	1	-1	-1
φ_3^5	3	1	-1	0	-1	-2
φ_4^5	3	-1	-1	0	1	2
φ_5^5	5	1	1	-1	-1	1
φ_6^5	5	-1	1	-1	1	-1

Tabulka 4.8: Braeurovy charaktery pro $\mathbb{Z}_5 S_5$

S_7	id	(2)	(2)(2)	(3)	(4)	(5)	(3)(2)
ζ_1^5	1	1	1	1	1	1	1
ζ_2^5	1	-1	1	1	-1	1	-1
ζ_3^5	4	2	0	1	0	-1	-1
ζ_4^5	4	-2	0	1	0	-1	1
ζ_5^5	5	1	1	-1	-1	0	1
ζ_6^5	5	-1	1	-1	1	0	-1
ζ_7^5	6	0	-2	0	0	1	0

Tabulka 4.9: charaktery pro $\mathbb{Q} S_5$

Literatura

[1] Akasaki, T. (1972). *ldempotent Ideals in Integral Group Rings.* JURNAL OF ALGEBRA 23.

[2] Anderson, F. W. a Fuller, K. R. (1991). *Rings and categrories of modules.* Springer-Verlag. ISBN 0-387-97845-3.

[3] Curtis, C. a Reiner, I. (1962). *Methods of representation theory. Vol. I.* Wiley Classics Library. ISBN 0-470-18975-4.

[4] Curtis, C. a Reiner, I. (1962). *Representation theory of finite groups and associative algebras.* Wiley Classics Library. ISBN 0-470-18975-4.

[5] Facchini, A. (1991). *Module theory.* Birkhäuser. ISBN 0-387-97845-3.

[6] James, G. a Kerber, A. (1981). *The representation theory of the symmetric group.* Addison-Wesley.

[7] Swan, R. (1963). *The Grothendieck ring of a finite group.* Topology 2.

[8] Whitehead, J. (1980). *Projective modules and their trace ideals.* Comm. Algebra 8.

Seznam tabulek