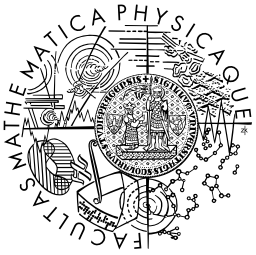

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Filip Filipi

Cykly translací v souvislých quandlech

Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. David Stanovský, Ph.D.

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2023

Prohlašuji, že jsem tuto bakalářskou 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

Rád bych věnoval poděkování svému vedoucímu Davidu Stanovskému za to, že mi dal příležitost pracovat na tak zajímavém problému, že mě uvedl do tématu, že mi poskytl potřebné materiály a že se se mnou na konzultacích dělil i o jeho autorské a jiné zkušenosti.

Název práce: Cykly translací v souvislých quandlech

Autor: Filip Filipi

katedra: Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. David Stanovský, Ph.D., Katedra algebry

Abstrakt: V práci se v kontextu konjugačních quandlů zabýváme Hayashiho domněnkou. Rozebíráme jejich souvislost a pomocí myšlenek podaných Davidem Stanovským a Petrem Vojtěchovským v důkazu tvrzení, že v tomto typu quandlů odvozených ze symetrických grup tato domněnka platí, odvozujeme charakterizaci Hayashiho domněnky pro úzkou třídu quandlů pomocí čistě grupových pojmů. Tato charakterizace mimo jiné říká, že pokud nalezneme konečnou neabelovskou jednoduchou grupu obsahující prvek, který není jednotka a který s každým prvkem své konjugační třídy komutuje v alespoň jedné své netriviální mocnině, pak Hayashiho domněnka neplatí. Dále na zmíněný důkaz navazujeme a dokazujeme, že domněnka platí i pro konjugační quandly odvozené z alternujících a dihedrálních grup. V závěru práce formulujeme atraktivní možnosti, jak ve výzkumu těchto quandlů pokračovat.

Klíčová slova: quandly Hayashiho domněnka konjugace nekomutativita

Title: Cycles in translations in connected quandles

Author: Filip Filipi

Department: Department of Algebra

Supervisor: doc. RNDr. David Stanovský, Ph.D., Department of Algebra

Abstract: In the thesis, we are dealing with Hayashi's conjecture in the context of conjugation quandles. We analyze their connectedness and, by using ideas presented by David Stanovský and Petr Vojtěchovský in the proof of the claim that every quandle of this type, derived from symmetric groups, satisfies this conjecture, we derive a characterization of Hayashi's conjecture for a narrow class of quandles using purely group-theoretic concepts. This characterization states, among other things, that if we find a finite non-abelian simple group containing an element that is not the identity and that commutes with every element of its conjugacy class in at least one of its non-trivial powers, then Hayashi's conjecture does not hold. Furthermore, we follow up on the aforementioned proof and prove that the conjecture also holds for conjugation quandles derived from alternating and dihedral groups. In conclusion, we formulate attractive possibilities for further research on these quandles.

Keywords: quandles Hayashi's conjecture conjugation noncommutativity

Obsah

Kapitola 1

Úvod

1.1 Motivace

Algebraická struktura nazývaná quandl se přirozeně rodí v teorii uzlů. Axiomy této struktury jsou totiž založeny na Reidemeisterových pohybech, což jsou manipulace s uzlovými diagramy, jejichž aplikací neovlivňujeme, jakému uzlu diagram odpovídá. Tento fakt umožňuje quandlům definovat veličiny, které jsou vlastností (orientovaných) uzlů a jsou nezávislé na jejich diagramech. Těmto veličinám se běžně říká invarianty a pomocí nich svedeme v některých případech dokázat, že 2 diagramy popisují různé uzly, což je z charakteru úlohy mnohdy obtížný problém. Volně se dá říci, že quandly svou algebraickou strukturou popisují strukturu orientovaných uzlů.

V případě většího zájmu o zrod a motivaci quandlů doporučujeme přečíst si úvodní část článku [1], který vše zmíněné uceleně, avšak stále stručně, vysvětluje. Více k historii a praktickému významu quandlů se dá najít v [2]. Základní znalosti a pojmy z teorie uzlů lze pak nalézt v knize [3], kde jsou představeny i spousty jiných uzlových invariantů. Mezi takové invarianty patří například speciální uzlové polynomy, různé geometrické vlastnosti a v neposlední řadě právě algebraické struktury podobné quandlům.

1.2 Cíl práce

Cílem této práce je přispět k řešení tzv. Hayashiho domněnky. Jde o problém v teorii quandlů formulovaný v roce 2013, který má pár částečných kladných řešení, avšak principiální důvod, proč by dané tvrzení mělo býti pravdivé stále schází. Domněnka pojednává o strukturální restrikci v tzv. souvislých quandlech. Quandly generované obarveními uzlových diagramů[1] jsou souvislé, a proto jsou z hlediska aplikací v teorii uzlů významné.

V kapitole 2 se seznámíme se základními pojmy z teorie quandlů, v jejím závěru zformulujeme zmíněnou Hayashiho domněnku a shrneme soubor dosažených výsledků. V kapitole 3 pak představíme rodinu quandlů, pro které je domněnka stále otevřená. Rozebereme jejich souvislost, pomocí znalostí [4] představíme vybádané poznatky o vztahu těchto quandlů s Hayashiho domněnkou a díky tomu odvodíme charakterizaci zúžené Hayashiho domněnky, která ji vyjádří

[1] Pro větší detaily k tomu, co to skutečně znamená, viz [1].

v lehce srozumitelném grupovém jazyce. V dalších sekcích pak budeme rozebírat platnost Hayashiho domněnky pro podtřídy těchto quandlů. Navážeme na doposud nepublikovanou práci Davida Stanovského a Petra Vojtěchovského [4], ve které dokázali, že Hayashiho domněnka platí pro podtřídu těchto quandlů svázanou s grupami $\mathbf{S}_n$. My ukážeme, že platí také pro $\mathbf{A}_n$ a $\mathbf{D}_{2n}$. V závěru poté projednáme nově otevřené možnosti, jak ve výzkumu této domněnky v rámci popsané rodiny quandlů pokračovat.

1.3 Značení

V této sekci uceleně zavedeme základní algebraické pojmy, se kterými budeme pracovat. Definujeme jejich značení, které v zájmu snazšího vyjadřování v některých případech mírně zobecníme. U pojmů majících vícero ustálených značení specifikujeme, které z nich budeme využívat. Dále připomeneme podstatné vlastnosti některých objektů, které v textu budeme považovat za samozřejmé. Jako opora pro většinu algebraických a grupových znalostí užitých v tomto textu mohou posloužit učebnice [5] a [6].

Máme-li neprázdnou množinu Q a na ní dánu binární operaci $\star$, pak uspořádanou dvojici $(Q, \star)$ nazýváme *binární algebra*[2]. Jsou-li $\mathbf{Q}_1 := (Q_1, \star_1)$ a $\mathbf{Q}_2 := (Q_2, \star_2)$ binární algebry, pak zobrazení $f : Q_1 \to Q_2$ nazýváme *homomorfismus binárních algeber* $\mathbf{Q}_1$ *a* $\mathbf{Q}_2$, pokud pro každá $a, b \in Q_1$ platí $f(a \star_1 b) = f(a) \star_2 f(b)$. Je-li z kontextu jasné, že na $\mathbf{Q}_1$ a $\mathbf{Q}_2$ nahlížíme jako na binární algebry, pak zkráceně píšeme, že $f : \mathbf{Q}_1 \to \mathbf{Q}_2$ je homomorfismus nebo také, že f je homomorfismus $\mathbf{Q}_1 \to \mathbf{Q}_2$. Pojmy *monomorfismus, epimorfismus, endomorfismus* a *automorfismus* binárních algeber zastupují speciální typy homomorfismů, které zavádíme analogicky jako pro grupy. Poznamenejme, že jsou-li $\mathbf{G}_1$ a $\mathbf{G}_2$ grupy, pak každé f, které je homomorfismem binárních algeber $\mathbf{G}_1$ a $\mathbf{G}_2$, je už dokonce i jejich grupovým homomorfismem, a proto pojmy nemusíme rozlišovat. Dále si ulehčíme vyjadřování tím, že je-li Q třída a $\star : Q \times Q \to Q$ (třídová) binární operace, pak budeme říkat, že se zobrazení $f : Q \to Q$ *chová homomorfně k operaci* $\star$, pokud pro každá $a, b \in Q$ platí $f(a \star b) = f(a) \star f(b)$.

V grupách zavádíme pojem *konjugace*, a to takto: Je-li $\mathbf{G}$ grupa a g její prvek, pak uvažujeme zobrazení $\phi_g : G \to G$ určené předpisem $x \mapsto gxg^{-1}$. Toto zobrazení nazýváme *(levá) konjugace s konjugačním prvkem* g, nebo zkráceně jen *(levá) konjugace prvkem* g. Říkáme, že $\phi_g(x)$ je *prvek získaný konjugací prvku* x *prvkem* g a zavádíme zkratku[3] $x^g := \phi_g(x) = gxg^{-1}$.

Z vlastností grup plyne známý fakt, že pro každé g je ϕ_g automorfismus $\mathbf{G}$. Právě tyto automorfismy nazýváme *vnitřní automorfismy* grupy $\mathbf{G}$. Množina všech vnitřních automorfismů, tj. $\{\phi_g \mid g \in G\}$ spolu s operací skládání množinových zobrazení tvoří podgrupu grupy automorfismů $\mathbf{G}$. Nazýváme ji *grupa vnitřních automorfismů grupy* $\mathbf{G}$ a značíme $\mathrm{Inn}(\mathbf{G})$.

Je-li dán e prvek grupy $\mathbf{G}$ a je-li $\mathbf{H}$ podgrupa $\mathbf{G}$, pak množinu e^H nazýváme *konjugační třída (prvku* e*) daná grupou* $\mathbf{H}$. Konjugační třídy dané podgrupou vždy tvoří disjunktní rozklad původní grupy. Je-li $\mathbf{G}$ grupa a $\mathbf{H}$ její podgrupa,

[2] Někdy také *magma* nebo *grupoid*.

[3] Druhá varianta zkratky ${}^g x := gxg^{-1}$ má hezkou vlastnost při skládání, a sice ${}^h({}^g x) = {}^{hg} x$. Z typografického hlediska je však spíše nepraktická a užívat ji nebudeme.

pak říkáme, že 2 prvky grupy $\mathbf{G}$ jsou *vzájemně konjugované grupou* $\mathbf{H}$, pokud leží ve stejné konjugační třídě dané grupou $\mathbf{H}$. Poznamenejme, že to nastává právě, když existuje prvek grupy $h \in \mathbf{H}$ takový, že jeden z prvků dostaneme z druhého pomocí konjugace prvkem h.

Jak je běžné, pro neprázdné množiny X zavádíme značení S_X zastupující množinu všech bijekcí na X. Její prvky nazýváme *permutace na* X. Množina S_X spolu s operací skládání zobrazení tvoří grupu, kterou nazýváme *symetrická* a značíme ji $\mathbf{S}_X$. Je-li X navíc konečná, pak pro permutace z S_X uvažujeme jejich zápisy jako složení nezávislých cyklů viz [5, str. 95] a tyto zápisy nazýváme *cyklické*. Řekneme, že cyklický zápis je *úplný*, pokud vyobrazuje i všechny cykly délky 1. Nevyobrazuje-li žádný z cyklů délky 1, pak jej nazýváme *redukovaný*. Lze-li permutaci na konečné množině napsat pomocí složení sudého počtu (ne nutně nezávislých) 2-cyklů, pak ji nazýváme *sudá* a pro neprázdnou konečnou množinu X značíme $\mathbf{A}_X$ tzv. *alternující* podgrupu všech sudých permutací grupy $\mathbf{S}_X$. Dále pro každé přirozené n zavádíme zkratky $\mathbf{S}_n$, resp. $\mathbf{A}_n$, zastupující grupy $\mathbf{S}_X$, resp. $\mathbf{A}_X$, pro $X = \{1, 2, \ldots, n\}$.

Je-li dána fixní permutace $\rho \in S_n$, pak mají všechny její úplné cyklické zápisy stejný počet cyklů daných délek. Jsou-li $1 \leq \ell_1 \lneq \ell_2 \lneq \cdots \lneq \ell_n$ všechny tyto délky a $n_{\ell_1}, n_{\ell_2}, \ldots, n_{\ell_n} \in \mathbb{N}$ jejich počty, pak

$$(\underbrace{\ell_1, \ell_1, \ldots, \ell_1}_{n_{\ell_1}}, \underbrace{\ell_2, \ldots, \ell_2}_{n_{\ell_2}}, \ell_3, \ldots\ldots, \ell_{n-1}, \underbrace{\ell_n, \ldots, \ell_n}_{n_{\ell_n}})$$

nazýváme *profil permutace* ρ nebo volně *cyklická struktura* ρ, resp. *struktura cyklů* ρ. Cyklická struktura permutací je v grupě $\mathbf{S}_n$ zachovávána konjugacemi, a dokonce platí, že dvě permutace z S_n jsou vzájemně konjugované grupou $\mathbf{S}_n$ právě tehdy, když mají stejnou strukturu cyklů. Množinu délek všech cyklů značíme $\Lambda(\rho) := \{\ell_i \mid i \in \{1, 2, \ldots, n\}\}$ a nazýváme ji *spektrum permutace* ρ.

Pro každé přirozené $n \geq 3$ definujeme $\mathbf{D}_{2n} \leq \mathbf{S}_{2n}$ jako grupu všech symetrií pravidelného n-úhelníka s vrcholy označenými po řadě $1, 2, \ldots, n$ a nazýváme ji *dihedrální* grupa řádu $2n$. Tuto grupu lze ve smyslu faktorobjektu volné grupy prezentovat jako $\langle r, o \mid o^n = r^2 = u \ \wedge \ ror = o^{-1} \rangle$, kde u značí identický prvek. Grupu $\mathbf{D}_{2n}$ můžeme také reprezentovat pomocí shodností $\mathbb{R}^2$ a ta nám umožňuje disjunktní dělení jejích prvků na přímé a nepřímé, resp. *rotace* a *reflexe*. Zda je výsledkem součinu rotace nebo reflexe se dá určit podle parity počtu součinitelů, které jsou reflexemi. Navíc platí, že rotace mezi sebou vzájemně komutují a každá reflexe má řád 2.

Jako $\mathrm{Z}(\mathbf{G})$ značíme *centrum grupy* $\mathbf{G}$, to je vždy abelovské a jde o normální podgrupu $\mathbf{G}$. Dále je-li dána množina X, její prvek x a grupa $\mathbf{G} \leq \mathbf{S}_X$, pak pomocí $\mathbf{G}_x$ značíme *stabilizátor prvku* x. Ten je vždy podgrupou $\mathbf{G}$. Poznamenejme, že *řád grupy* $\mathbf{G}$ budeme značit jak pomocí $|\mathbf{G}|$, tak $\operatorname{ord} \mathbf{G}$ v závislosti na čitelnosti daného zápisu.

Fakt, že množina X *generuje grupu* $\mathbf{G}$ budeme značit $\langle X \rangle_{\mathbf{G}} = \mathbf{G}$. V takovém případě pak svedeme každý prvek grupy $\mathbf{G}$ vyjádřit jako konečný součin prvků z X a jejich inverzů. To budeme využívat obzvláště často, a proto jsou-li indexové množiny proměnných zřejmé z kontextu, pak je nebudeme uvádět. Například namísto „prvek lze vyjádřit ve tvaru $\prod_{i=1}^{n} c_i$ pro nějaké n přirozené a nějaká c_i prvky množiny e^G nebo jejich inverzy, kde i probíhá prvky množiny $\{1, 2, \ldots, n\}$“ budeme psát pouze „prvek lze vyjádřit ve tvaru $\prod_{i=1}^{n} c_i$ pro nějaké n přirozené

a nějaká c_i prvky množiny e^G nebo jejich inverzy“. Mnohdy bude také z kontextu zřejmé, že dané číslo má být přirozené a tento fakt nebudeme zdůrazňovat. Převážně tomu tak bude při užívání zápisů stylu $1 \leq m \lneq 10$, ze kterých samotných přirozenost m formálně neplyne.

Kapitola 2

Cykly translací v souvislých quandlech

Tato kapitola slouží jako úvod do problematiky, kterou se práce bude následně zabývat. V sekci 2.1 se seznámíme se základními pojmy z teorie quandlů, a to do takové míry, abychom byli schopni navázat sekcí 2.2, kde formulujeme jeden z aktuálních otevřených problémů této teorie. Tomuto problému se budeme blíže věnovat v kapitole 3.

2.1 Základy teorie quandlů

Definice pojmů zmíněných v této sekci můžeme nalézt například v knize [3]. Jako předloha pro formulace znění tvrzení v této kapitole slouží článek [2]. Poznamenejme však, že ten, na rozdíl od této práce, využívá odlišnou (duální) definici quandlu[1]. My quandl definujeme následovně.

Definice 2.1 (Quandl)**.** Binární algebru $\mathbf{Q} = (Q, \star)$ nazýváme *quandl*, splňuje-li

(i) $(\forall a \in Q)\ a \star a = a$, (idempotence)

(ii) $(\forall a, b \in Q)(\exists! x \in Q)\ a \star x = b$, (levá kvazigrupa)

(iii) $(\forall a, b, c \in Q)\ a \star (b \star c) = (a \star b) \star (a \star c)$. (levá distributivita)

Příklad. Je-li Q množina a $\star : Q \times Q \to Q$ projekce na druhou složku, tj. $a \star b = b$, pak $(Q, \star)$ je quandl. Takovéto quandly nazýváme *projekční*[2]. ■

Příklad. Je-li $\mathbf{G}$ grupa a f její automorfismus, pak množina G spolu s operací $\star : G \times G \to G$ danou vztahem $a \star b := af^{-1}(a)f(b)$, tvoří quandl. Tyto quandly nazýváme *principální*. Je-li $\mathbf{G}$ navíc abelovská, pak se tyto quandly běžně nazývají *afinní* [4][3] a v tomto kontextu se principální quandly považují za zobecněné afinní quandly. ■

Poznamenejme, že jednoznačnost existence řešení rovnic tvaru $a \star x = b$ na množině Q přirozeně definuje druhou binární operaci $\backslash : (a, b) \mapsto a\backslash b$, kde $a\backslash b$

[1] Tj. definici takovou, že quandl je idempotentní, zprava distributivní pravá kvazigrupa.

[2] Někdy také *triviální* [3].

[3] Nebo také *Alexandrovy* [2]. Tento pojem je vyložen i v [3], kde se uvažují moduly nad celočíselnými Laurentovými polynomy. Tyto definice jsou ekvivalentní [2].

je to jediné řešení rovnice $a \star x = b$. Podmínku (ii) dokonce smíme nahradit výrokem, že relace $\setminus := \{((a,b),x) \mid a,b,x \in Q, a \star x = b\}$ je binární operace na Q.

Tímto způsobem můžeme na quandly $\mathbf{Q}_1, \mathbf{Q}_2$ současně nahlížet i jako na množiny se dvěma binárními operacemi, a tedy nemusí být úplně jasné, zda bychom homomorfismus binárních algeber $\mathbf{Q}_1$ a $\mathbf{Q}_2$ měli považovat i za homomorfismus quandlů $\mathbf{Q}_1$ a $\mathbf{Q}_2$.

Je však snadno ověřitelné, že jsou-li $\mathbf{Q}_1 := (Q_1, \star_1)$, $\mathbf{Q}_2 := (Q_2, \star_2)$ quandly a f je homomorfismus binárních algeber $\mathbf{Q}_1$ a $\mathbf{Q}_2$, tak už je f i homomorfismus binárních algeber $(Q_1, \setminus_1)$ a $(Q_2, \setminus_2)$. Pojmy jsou proto v obou interpretacích stejné jako pro binární algebry, a tedy nehrozí nedorozumění, pokud řekneme, že $f : \mathbf{Q}_1 \to \mathbf{Q}_2$ je homomorfismus[4].

Pro binární algebry, a tedy i quandly, má smysl definovat následující pojem. Ten bude, jak v této kapitole uvidíme, hlavním předmětem celé práce.

Definice 2.2 (Levá translace)**.** Je-li $\mathbf{Q} = (Q, \star)$ binární algebra a a její prvek, pak definujeme zobrazení $L_a : Q \to Q$ dané předpisem $x \mapsto a \star x$. Toto zobrazení nazýváme *levá translace určená prvkem* a.

Poznámka. Definice levých translací je závislá na uvažované binární algebře. Nebude-li však blíže specifikováno, tak bude známá z kontextu. Zpravidla půjde o quandl.

Levé translace nám umožňují elegantněji vyjádřit podmínky z definice quandlu.

Pozorování 2.3. *Binární algebra* $\mathbf{Q} = (Q, \star)$ *je*

(i) idempotentní právě, když pro každé $a \in Q$ *platí, že* $L_a(a) = a$,

(ii) levá kvazigrupa právě, když pro každé $a \in Q$ *je* L_a *bijekce na* Q,

(iii) zleva distributivní právě, když pro každé $a \in Q$ *je* L_a *homomorfismus* $\mathbf{Q} \to \mathbf{Q}$.

Důkaz. Všechny implikace zprava doleva plynou přímo z rozepsání výrazu $L_a(x)$ jako $a \star x$. Implikace zleva doprava nejsou o moc složitější: Nechť $a \in Q$ je libovolné, pak

(i) víme, že $a = a \star a = L_a(a)$, kde poslední rovnost je dána definicí L_a.

(ii) chceme ukázat, že L_a je prosté a na Q. Pro tyto účely volme $b \in Q$ libovolně. Víme, že existuje právě jedno $x \in Q$ takové, že $b = a \star x = L_a(x)$. Z existence x plyne, že b je v obrazu L_a, a tedy L_a je na. Kdyby pro spor L_a nebylo prosté, tak nalezneme $b \in Q$ takové, že x není jednoznačné, což by byl spor.

(iii) jsou-li $b, c \in Q$ libovolné prvky, pak víme, že $a \star (b \star c) = (a \star b) \star (a \star c)$. Tuto rovnost svedeme vyjádřit jako $L_a(b \star c) = L_a(b) \star L_a(c)$, což jsme chtěli ukázat.

□

Důsledek 2.3.1. Binární algebra $\mathbf{Q}$ je quandl právě tehdy, když pro každé $a \in Q$ je L_a automorfismus $\mathbf{Q}$ s pevným bodem a.

[4]Není však pravda, že uzavřenost nekonečné podmnožiny quandlu $(Q, \star)$ na operaci $\star$ postačuje k tomu, aby šlo o quandl! Zde je potřeba i uzavřenost na $\setminus$. Pro konečné neprázdné podmnožiny to stačí.

Tento popis quandlů pomocí levých translací svede být v určitých situacích nápomocný. Příkladem takové situace může být ověření toho, že projekční quandly skutečně splňují definici quandlu: Levé translace jsou identitami, a tedy jde o automorfismy, pro něž je dokonce každý prvek pevným bodem.

Už víme, že je-li dán quandl $\mathbf{Q}$, pak je každá jeho levá translace bijekce, tj. permutace na Q. Tímto způsobem smíme levé translace přirozeně reprezentovat jako prvky symetrické grupy $\mathbf{S}_Q$, a to umožňuje definici grupy generované všemi levými translacemi.

Definice 2.4 (Levá multiplikativní grupa)**.** Nechť $\mathbf{Q}$ je quandl. Definujeme *levou multiplikativní grupu quandlu* $\mathbf{Q}$ jako $\mathrm{LMlt}(\mathbf{Q}) := \langle L_a \mid a \in Q \rangle_{\mathbf{S}_Q}$.

Víme, že levé translace jsou v quandlech automorfismy, a platí tedy, že $\{L_a \mid a \in Q\} \subseteq \mathrm{Aut}(\mathbf{Q})$, kde $\mathrm{Aut}(\mathbf{Q})$ značí grupu všech automorfismů quandlu $\mathbf{Q}$. Díky tomu máme, že $\mathrm{LMlt}(\mathbf{Q}) \leq \mathrm{Aut}(\mathbf{Q})$, a tedy speciálně každý prvek grupy $\mathrm{LMlt}(\mathbf{Q})$ je automorfismus.

Poznamenejme, že inverzní zobrazení k levé translaci, ani složení levých translací nemusí být levá translace, a tedy obecně neplatí rovnost $\mathrm{LMlt}(\mathbf{Q})$ a $\{L_a \mid a \in Q\}$.

Definice 2.5 (Souvislý quandl)**.** Quandl $\mathbf{Q}$ nazveme *souvislý*[5], pokud grupa $\mathrm{LMlt}(\mathbf{Q})$ působí tranzitivně na množinu Q při jejím přirozeném působení jako podgrupy $\mathbf{S}_Q$.

Volně řečeno můžeme tuto definici parafrázovat tak, že quandl je souvislý, pokud libovolný jeho bod svedeme pomocí konečně mnoha levých translací a jejich inverzů „posunout“ na libovolný jiný bod v tomto quandlu.

Poznámka. Dle definice je quandl souvislý právě, když má zmíněné působení pouze jednu orbitu. Pro důkaz souvislosti quandlu tedy stačí ukázat, že v něm existuje alespoň jeden prvek, který svedeme pomocí levých translací a jejich inverzů „přesunout“ na libovolný jiný prvek.

V souvislém quandlu platí poměrně překvapivá vlastnost. Všechny jeho levé translace totiž mají stejnou strukturu cyklů. K ukázání tohoto faktu se hodí následující lemma, které je samo o sobě poměrně silným nástrojem v teorii quandlů.

Lemma 2.6. *Nechť* $\mathbf{Q}$ *je quandl,* $\alpha : \mathbf{Q} \to \mathbf{Q}$ *je automorfismus a nechť* a *je prvek množiny* Q*, pak platí, že* $L_{\alpha(a)} = L_a^\alpha$*.*

Důkaz. Je-li x libovolný prvek množiny Q, pak

$$\alpha \circ L_a \circ \alpha^{-1}(x) = \alpha(a \star \alpha^{-1}(x)) = \alpha(a) \star x = L_{\alpha(a)}(x).$$

□

Věta 2.7. *Levé translace v souvislém quandlu mají stejnou strukturu cyklů.*

Důkaz. Nechť $\mathbf{Q}$ je souvislý quandl a nechť a, b jsou prvky množiny Q. Ukážeme, že L_b má stejnou strukturu cyklů jako L_a.

Ze souvislosti $\mathbf{Q}$ plyne, že existuje zobrazení $\rho \in \mathrm{LMlt}(\mathbf{Q}) \leq \mathrm{Aut}(\mathbf{Q})$ takové, že $b = \rho(a)$. Díky lemmatu 2.6 získáváme $L_b = L_{\rho(a)} = L_a^\rho$. Konjugace permutací zachovávají strukturu cyklů, a tedy L_b má stejnou strukturu cyklů jako L_a. □

[5]Nebo také *nerozložitelný* [7].

2.2 Hayashiho domněnka

Věta 2.7 nám říká, že pokud známe strukturu cyklů jedné z levých translací v souvislém quandlu, pak již známe strukturu všech. Tzv. *Hayashiho domněnka* v analogickém znění poprvé zformulovaná v roce 2013 v článku [7] však navrhuje, že možná svedeme říci o jejich struktuře více. Pro účely snazší práce s domněnkou přichází vhod definovat ještě jeden pojem.

Definice 2.8. Nechť ρ je permutace na konečné množině. Řekneme, že ρ *má regulární cyklus*, pokud pro každé $\lambda \in \Lambda(\rho)$ platí $\lambda \mid \max(\Lambda(\rho))$, tj. pokud délka každého jejího cyklu dělí délku jejího nejdelšího cyklu.

Příklad. Permutace $(1\ 2\ 3)(4\ 5) \in S_5$ nemá regulární cyklus, protože délka cyklu $(4\ 5)$ nedělí délku cyklu $(1\ 2\ 3)$. Naopak $(1)(2\ 3)(4\ 5\ 6\ 7) \in S_7$ regulární cyklus má. ■

Domněnka (Hayashi)**.** *Levé translace v konečných souvislých quandlech mají regulární cyklus.*

Pro zajímavost uvádíme její ekvivalentní formulaci užívající čistě grupových pojmů, která je důsledkem [2, Theorem 5.3].

Domněnka. *Nechť* $\mathbf{G}$ *je grupa působící tranzitivně na konečnou množinu* X *a nechť* $e \in X$*. Je-li* $\zeta \in \mathrm{Z}(\mathbf{G}_e)$ *splňující* $\left\langle \zeta^G \right\rangle_{\mathbf{G}} = \mathbf{G}$*, pak má* ζ *regulární cyklus.*

Rozeberme dosažené výsledky částečně zodpovídající tuto domněnku. Seznam je převzat z [8] a lze ho také nalézt v disertační práci Naqeeba ur Rehmana [9].

Hayashiho domněnka byla doposud ověřena pro:

- konečné quandly velikosti nejvýše 47 (užité výpočetní metody byly popsány v [2]),
- quandly, jejichž levé translace mají spektrum velikosti nejvýše 3 [8][6],
- tzv. *primitivní quandly*, tj. quandly $\mathbf{Q}$, v nichž grupa $\mathrm{LMlt}(\mathbf{Q})$ působí primitivně[7] [11],
- afinní quandly [12, 13],
- principální quandly nad konečnými nilpotentními grupami [13],
- principální quandly nad obecnými konečnými grupami při volbě automorfismů, jejichž řád je nesoudělný s řádem této grupy [13].

Dále v textu budeme říkat, že quandl $\mathbf{Q}$ *splňuje Hayashiho domněnku*, pokud s ní není ve sporu. Díky větě 2.7 quandl splňuje Hayashiho domněnku právě, když nesplňuje její předpoklady nebo v něm existuje levá translace mající regulární cyklus.

[6] Méně obecného výsledku bylo poprvé dosaženo v [10].

[7] Definici tohoto pojmu lze nalézt v [11].

Kapitola 3

Cykly translací v konjugačních quandlech

Tato kapitola tvoří páteř celé práce. V kapitole 2 jsme uvedli otevřený problém, který má různá částečná řešení a zde si představíme třídu quandlů, pro již je jeho platnost zatím nejasná.

Lemma 3.1. *Nechť* $\mathbf{G}$ *je grupa a* e *je její prvek. Pak* e^G *spolu s na ní definovanou binární operací* $\star$ *takovou, že* $x \star y := y^x$*, tvoří quandl.*

Důkaz. Dokážeme pomocí důsledku 2.3.1. Nechť x je libovolný prvek množiny e^G. Ukážeme, že L_x je automorfismus $(e^G, \star)$ s pevným bodem x.

Pevnost bodu x je zřejmá: $L_x(x) = x^x = xxx^{-1} = x$.

Dále si všimněme, že translace L_x je na svém definičním oboru, tj. na e^G, definována stejně jako ϕ_x, tj. konjugace prvkem x v grupě $\mathbf{G}$. Konjugace v grupě jsou automorfismy, a to ihned dává, že $L_x = \phi_x{\restriction_{e^G}}$ je prosté a že se chová homomorfně ke grupové operaci.

Pro důkaz toho, že L_x je na, si volme libovolný prvek množiny e^G a ukažme, že je v obrazu L_x, tj. volme libovolné $g \in G$ a ukažme, že je prvek e^g v obrazu L_x. Z toho, že ϕ_x je automorfismus, určitě existuje $y \in G$ takové, že $\phi_x(y) = e^g$. Toto y však dokonce leží v e^G, protože aplikací $(\phi_x)^{-1}$ na obě strany rovnosti získáme

$$y = (\phi_x)^{-1}(e^g) = \phi_{x^{-1}}(e^g) = e^{x^{-1}g} \in e^G.$$

Ve druhé rovnosti jsme užili toho, že $\phi_x \circ \phi_{x^{-1}} = \phi_{xx^{-1}} = \mathrm{id}_{\mathbf{G}}$.

K dokončení důkazu zbývá nahlédnout, že se L_x chová homomorfně i k operaci $\star$. Jsou-li $a, b \in e^G$, pak

$$L_x(a \star b) = L_x(aba^{-1}) = L_x(a)L_x(b)(L_x(a))^{-1} = L_x(a) \star L_x(b)$$

Ve druhé rovnosti jsme užili toho, že se L_x chová homomorfně ke grupové operaci. □

Quandly $(e^G, \star)$ zkonstruované ve smyslu lemmatu 3.1 nazýváme *konjugační* a značíme je $\mathbf{e^G}$. Jak jsme již naznačili, platnost Hayashiho domněnky pro ně doposud nebyla rozhodnuta. Davidu Stanovskému a Petru Vojtěchovskému se však v zatím nepublikované práci [4] podařilo dosáhnout následujícího výsledku.

Tvrzení 3.2. *V konjugačních quandlech tvaru* $\mathbf{e^{S_n}}$ *má* L_e *regulární cyklus.*

Tvrzení 3.2 ověřuje Hayashiho domněnku pro třídu všech konjugačních quandlů tvaru $\mathbf{e^{S_n}}$, protože říká, že nehledě na souvislost v těchto quandlech nalezneme levou translaci mající regulární cyklus, a tedy s jistotou už tyto quandly splňují Hayashiho domněnku. Sekce 3.1 nám později dokonce ukáže, že velkou část této třídy skutečně tvoří souvislé quandly.

V sekci 3.1 pomocí vypozorované věty 3.3 rozebere souvislost quandlů, kterými se budeme dále zabývat. V sekcích 3.2 a 3.3 následně budeme stavět na znalosti důkazu tvrzení 3.2 z osobních poznámek Davida Stanovského a Petra Vojtěchovského [4]. Strukturu jejich důkazu v naší práci kopíruje posloupnost znění lemmat 3.6, 3.7, tvrzení 3.8, 3.10 a nekonstruktivní části důkazu lemmatu 3.14. Tyto jejich myšlenky doplníme o důkazy jejich korektnosti a v sekci 3.2 je mírně zobecníme tak, abychom spolu s naším rozborem souvislosti ze sekce 3.1 obdrželi větu 3.9, která nám dává poměrně jednoduše formulovatelnou ekvivalentní vyjádření Hayashiho domněnky v jazyku teorie grup. V sekci 3.3 navážeme na zmíněný důkaz tvrzení 3.2 a ukážeme, že dokonce platí i jeho analogie pro konjugační quandly odvozené z alternujících grup, tj. tvrzení 3.15. V sekci 3.4 pak využijeme téměř všech nabytých znalostí, abychom Hayashiho domněnku ověřili i pro konjugační quandly odvozené z dihedrálních grup, konkrétně dokážeme tvrzení 3.19.

3.1 Souvislost konjugačních quandlů

Ne každý konjugační quandl musí být souvislý. Příklad jednoho takového nalezneme dokonce ve třídě konjugačních quandlů tvaru $\mathbf{e^{A_n}}$. Ve stručnosti si jej předveďme.

Příklad. Uvažme quandl $\mathbf{e^{A_4}}$ s $e = (1\ 2)(3\ 4)$. Získáme, že

$$e^{A_4} = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Každý z těchto prvků je v grupě $\mathbf{A}_4$ řádu 2, což má za následek, že inverz každé translace L_a je sama translace L_a [1] a kvůli tomu, že součinem každých dvou různých prvků z e^{A_4} získáme zbylý prvek, budou levé translace v tomto quandlu identity. Tím pádem působení grupy $\mathrm{LMlt}\left(\mathbf{e^{A_4}}\right) = \mathbf{1}$ na množinu e^G nebude tranzitivní, protože každý prvek bude tvořit izolovanou orbitu. ■

Může být rozumné se nejprve ptát, zda je netriviální množství konjugačních quandlů skutečně souvislých a má vůbec smysl se jimi v kontextu Hayashiho domněnky zabývat. Odpovědí je, že ano, jak nám ukáže věta 3.3.

Věta 3.3. *Nechť* $\mathbf{G}$ *je grupa a nechť* e *je její prvek takový, že* $\left\langle e^G \right\rangle_{\mathbf{G}} = \mathbf{G}$. *Pak je konjugační quandl* $\mathbf{e^G}$ *souvislý.*

Důkaz. Nechť e^g je libovolný prvek množiny e^G. Dle poznámky za definicí souvislosti quandlu stačí ukázat, že existuje způsob, jak se pomocí levých translací a jejich inverzů „přesunout“ z e na e^g.

Daný prvek $g \in \mathbf{G} = \left\langle e^G \right\rangle_{\mathbf{G}}$ svedeme vyjádřit ve tvaru $\prod_{i=1}^{n} c_i$ pro nějaké n přirozené a nějaká c_i prvky množiny e^G nebo jejich inverzy. Kdyby všechna c_i ležela v e^G, tak bychom měli již hotovo, protože bychom směli psát, že $e^g =$

[1] Quandly, co toto splňují se v anglicky psané literatuře nazývají *involutory quandles* nebo také *kei* [3].

$e^{\prod_{i=1}^{n} c_i} = \phi_{c_1} \circ \phi_{c_2} \circ \cdots \circ \phi_{c_n}(e) = L_{c_1} \circ L_{c_2} \circ \cdots \circ L_{c_n}(e)$. Pokud však některé $c_i \notin e^G$, tak bohužel požadovanou translaci L_{c_i} nemáme definovanou. Nicméně je pak nutně c_i inverzem nějakého prvku z e^G, a tedy $c_i^{-1} \in e^G$. Teď již smíme psát $\phi_{c_i} \circ L_{c_i^{-1}} = \mathrm{id}_{e^G}$ a z toho máme $\phi_{c_i}{\restriction}_{e^G} = L_{c_i^{-1}}^{-1}$.

Celkově získáváme to, co jsme ukázat, a sice:

$$e^g = L_{c_1^{s_1}}^{s_1} \circ L_{c_2^{s_2}}^{s_2} \circ \cdots \circ L_{c_n^{s_n}}^{s_n}(e), \text{ kde } s_i = \begin{cases} 1, & \text{pokud } c_i \in e^G, \\ -1, & \text{pokud } c_i \notin e^G. \end{cases}$$

□

Věta 3.3 má poměrně elegantní důsledek, který formulujeme jako větu 3.5. K důkazu nám přijde vhod následující nepřekvapivé lemma.

Lemma 3.4. *Nechť* $\mathbf{G}$ *je grupa a nechť* e *je její prvek, pak* $\mathbf{H} := \left\langle e^G \right\rangle_{\mathbf{G}}$ *je normální podgrupa grupy* $\mathbf{G}$.

Důkaz. Vezměme libovolné prvky $h \in H, g \in G$. Z definice $\mathbf{H}$ lze h vyjádřit jako konečný součin prvků množiny e^G a jejich inverzů. Rovnosti $e^g(e^{-1})^g = 1$ platící pro každé $g \in G$ ukazují, že inverzy prvků z e^G jsou právě prvky z $(e^{-1})^G$. Celkově tedy víme, že existuje n přirozené a $g_i \in G, e_i \in \{e, e^{-1}\}$ taková, že

$$h = \prod_{i=1}^{n} e_i^{g_i}.$$

Teď už jednoduše získáváme

$$h^g = g(\Pi_{i=1}^n e_i^{g_i})g^{-1} = \Pi_{i=1}^n g e_i^{g_i} g^{-1} = \Pi_{i=1}^n e_i^{gg_i} \in \left\langle e^G \right\rangle_{\mathbf{G}} = \mathbf{H},$$

a tedy podgrupa $\mathbf{H}$ je skutečně normální. □

Věta 3.5. *Nechť* $\mathbf{G}$ *je jednoduchá grupa a nechť* e *je nějaký její prvek. Pak je konjugační quandl* $\mathbf{e^G}$ *souvislý.*

Důkaz. Označme $\mathbf{H} := \left\langle e^G \right\rangle_{\mathbf{G}}$. Je-li $\mathbf{H}$ triviální, pak je quandl jednoprvkový, a tedy triviálně souvislý. V opačném případě díky lemmatu 3.4 víme, že $\mathbf{H}$ je netriviální normální podgrupa jednoduché grupy $\mathbf{G}$, a tedy už nutně $\mathbf{H} = \mathbf{G}$. To nám umožňuje aplikovat větu 3.3 a získat, že je $\mathbf{e^G}$ skutečně souvislý. □

S využitím jednoho důležitého výsledku z teorie grup [6, Theorem 3.11], a sice, že pro $n \geq 5$ je $\mathbf{A}_n$ jednoduchá grupa, nám věta 3.5 říká, že pro $n \geq 5$ je každý konjugační quandl tvaru $\mathbf{e^{A_n}}$ souvislý. Poznamenejme, že analogické tvrzení pro $n = 4$ neplatí, o čemž jsme se přesvědčili na začátku této sekce.

Podobně z teorie grup víme [6, Exercise 3.21], že pro $n \geq 5$ jsou $\mathbf{1}, \mathbf{A}_n$ a $\mathbf{S}_n$ jediné normální podgrupy $\mathbf{S}_n$. Vezmeme-li tedy libovolné $e \in S_n \setminus A_n$, pak opět díky lemmatu 3.4 je $\left\langle e^G \right\rangle_{\mathbf{S}_n}$ už nutně rovna $\mathbf{S}_n$, a tedy dle věty 3.3 je quandl $\mathbf{e^{S_n}}$ souvislý.

Věta 3.3 nám také říká něco o souvislosti konjugačních quandlů odvozených z dihedrálních grup. Nechť je dáno j přirozené, $n := 2j + 1$ a reflexe $e \in D_{2n}$. Budeme zkoumat souvislost quandlu $\mathbf{e^{D_{2n}}}$. Vezměme nějakou rotaci $o \in D_{2n}$ řádu n, pak nám platí, že $e^{D_{2n}} \ni e' := oeo^{-1} = oe(eoe) = o^2 e$ a následně také

$\left\langle e^{D_{2n}} \right\rangle_{\mathbf{D}_{2n}} \ni (ee')^j = (eo^2e)^j = (o^{-2})^j = o^{-2j} = o^{-2j+n} = o$. Grupa $\left\langle e^{D_{2n}} \right\rangle_{\mathbf{D}_{2n}}$ tedy obsahuje prvek e řádu 2 a prvek o lichého řádu n. Nutně pak číslo $2n$ dělí její řád, takže speciálně $\operatorname{ord}\left\langle e^{D_{2n}} \right\rangle_{\mathbf{D}_{2n}} \geq 2n = \operatorname{ord}\mathbf{D}_{2n}$. Tím jsme ukázali, že $\left\langle e^{D_{2n}} \right\rangle_{\mathbf{D}_{2n}} = \mathbf{D}_{2n}$, a tedy dle věty 3.3 je quandl $\mathbf{e^{D_{2n}}}$ souvislý.

Ukázali jsme si, že téměř všechny konjugační quandly tvaru $\mathbf{e^{A_n}}$ jsou souvislé a neformálně řečeno[2] alespoň polovina těch tvaru $\mathbf{e^{S_n}}$ je souvislých. Dále jsme ukázali, že pro lichá $n \geq 3$ a reflexe $e \in \mathbf{e^{D_{2n}}}$ jsou quandly $\mathbf{e^{D_{2n}}}$ souvislé. Neformálně řečeno to znamená, že alespoň čtvrtina konjugačních quandlů odvozených z dihedrálních grup je souvislých.

Poznamenejme, že, jak na začátku sekce 3.4 uvidíme, quandly tvaru $\mathbf{e^{D_{2n}}}$, kde e je rotace, jsou až na izomorfismus pouze 2. Tento problém ale v žádném z případů, co jsme právě ověřili v takové míře nenastává, protože je-li e fixní, tak zvětšováním n zpravidla zvětšujeme i velikost odpovídajícího quandlu. V tomto kontextu[3] by se dalo říci, že ověřených konjugačních quandlů odvozených z dihedrálních grup je dokonce spíše alespoň polovina, nežli čtvrtina.

3.2 Cykly translací v konjugačních quandlech

Jedním ze stěžejních obratů v [4] dokazujících tvrzení 3.2 je řetězec grupových izomorfismů, který v mírně obecnější podobě vyslovujeme formou následujícího lemmatu. Jeho důkaz je spíše formální záležitostí a sám o sobě není ničím zajímavý.

Lemma 3.6. *Nechť* $\mathbf{G}$ *je grupa,* e *je její prvek a* $\mathbf{H} := \left\langle e^G \right\rangle_{\mathbf{G}}$. *Pak* $\operatorname{Inn}(\mathbf{H})\restriction_{e^G} := \{\phi_h\restriction_{e^G} \mid h \in H\}$ *tvoří se skládáním zobrazení grupu a platí následující řetězec grupových izomorfismů*

$$\mathbf{H}\!\diagup_{\mathrm{Z}(\mathbf{H})} \overset{\text{(iii)}}{\simeq} \operatorname{Inn}(\mathbf{H}) \overset{\text{(ii)}}{\simeq} \operatorname{Inn}(\mathbf{H})\restriction_{e^G} \overset{\text{(i)}}{=} \operatorname{LMlt}\left(\mathbf{e^G}\right).$$

Navíc máme izomorfismus $\psi : \mathbf{H}\!\diagup_{\mathrm{Z}(\mathbf{H})} \to \operatorname{LMlt}\left(\mathbf{e^G}\right)$ *definovaný tak, že kdykoliv je* n *přirozené a pro každé* $i = 1, 2, \ldots, n$ *jsou* $h_i \in e^G, s_i \in \{\pm 1\}$, *pak*

$$\left(\prod_{i=1}^{n} h_i^{s_i}\right) \mathrm{Z}(\mathbf{H}) \mapsto L_{h_1}^{s_1} \circ L_{h_2}^{s_2} \circ \cdots \circ L_{h_n}^{s_n}.$$

Důkaz. Důkaz jednotlivých izomorfismů provádíme v opačném pořadí, než by se mohlo zdát být přirozené. Děláme to tak proto, abychom již z rovnosti (i) mohli vyvodit, že $\operatorname{Inn}(\mathbf{H})\restriction_{e^G}$ je skutečně grupa a tento fakt směli použít v bodě (ii).

(i): Pomocí dvou vzájemných inkluzí ukážeme, že si jsou výrazy množinově rovny. Díky tomu, že operace je na obou stranách definována stejně, bez námahy získáme dokonce i grupovou rovnost, které chceme docílit. Speciálně budeme také vědět, že $\operatorname{Inn}(\mathbf{H})\restriction_{e^G}$ je grupa.

Už jsme v důkazu věty 3.3 narazili na to, že pro libovolné $a \in e^G$ nám platí $L_a = \phi_a\restriction_{e^G}$ a $L_a^{-1} = \phi_{a^{-1}}\restriction_{e^G}$. Pro libovolné přirozené n a $h_i \in e^G$, $s_i \in \{\pm 1\}$ nám proto platí

$$L_{h_1}^{s_1} \circ L_{h_2}^{s_2} \circ \cdots \circ L_{h_n}^{s_n} = \phi_{h_1^{s_1}}\restriction_{e^G} \circ \phi_{h_2^{s_2}}\restriction_{e^G} \circ \cdots \circ \phi_{h_n^{s_n}}\restriction_{e^G} = \phi_{\prod_{i=1}^{n} h_i^{s_i}}\restriction_{e^G}. \tag{3.1}$$

[2] Ve smyslu relativního počtu voleb parametrů e a n, kde $n \leq k$ pro $k \to \infty$.

[3] Tentokrát již nezaloženém na počtu parametrů, ale počtu výsledných quandlů.

Levý výraz rovnice (3.1) vždy leží v LMlt $\left(\mathbf{e^G}\right)$ a současně pravý výraz (3.1) v $\mathrm{Inn}(\mathbf{H})\restriction_{e^G}$. Svedeme-li tedy každý prvek grupy LMlt $\left(\mathbf{e^G}\right)$ vyjádřit výrazem vlevo, pak získáme jednu z inkluzí a svedeme-li vyjádřit každý prvek grupy $\mathrm{Inn}(\mathbf{H})\restriction_{e^G}$ výrazem vpravo, pak získáme druhou z inkluzí. První plyne z toho, že $\{L_a \mid a \in e^G\}$ generuje LMlt $\left(\mathbf{e^G}\right)$ a druhá z toho, že e^G generuje $\mathbf{H}$.

(ii): Uvažme zobrazení $\psi_{(ii)} : \mathrm{Inn}(\mathbf{H}) \to \mathrm{Inn}(\mathbf{H})\restriction_{e^G}$ takové, že $\phi_h \mapsto \phi_h\restriction_{e^G}$. Ověříme, že jde o izomorfismus a tím dokážeme bod (ii).

- Je to homomorfismus: Pro libovolná $h, k \in H$ platí $\psi_{(ii)}(\phi_h) \circ \psi_{(ii)}(\phi_k) = \phi_h\restriction_{e^G} \circ \phi_k\restriction_{e^G} = \phi_{hk}\restriction_{e^G} = \psi_{(ii)}(\phi_h \circ \phi_k)$.
- Je na: Plyne přímo z definice $\psi_{(ii)}$ a grupy $\mathrm{Inn}(\mathbf{H})$, resp. $\mathrm{Inn}(\mathbf{H})\restriction_{e^G}$.
- Je prosté: Díky tomu, že jde o homomorfismus, tak stačí ukázat, že má triviální jádro. Máme-li $h \in H$ takové, že $\phi_h\restriction_{e^G} = \mathrm{id}_{e^G}$, pak se ϕ_h na množině generátorů grupy $\mathbf{H}$ shoduje se zobrazením $\mathrm{id}_H \in \mathrm{Inn}(\mathbf{H})$, a tedy už nutně $\phi_h = \mathrm{id}_H$.

(iii): Uvažme zobrazení $\psi'_{(iii)} : H \to \mathrm{Inn}(\mathbf{H})$ takové, že $h \mapsto \phi_h$. Toto zobrazení má následující vlastnosti.

- Je to homomorfismus: Pro $h, k \in H$ máme $\psi'_{(iii)}(hk) = \phi_{hk} = \phi_h \circ \phi_k = \psi'_{(iii)}(h) \circ \psi'_{(iii)}(k)$.
- Je na: Plyne přímo z definice $\psi'_{(iii)}$ a grupy $\mathrm{Inn}(\mathbf{H})$.
- Jeho jádro je rovno $\mathrm{Z}(\mathbf{H})$: Prvek $h \in H$ leží v jádru $\psi'_{(iii)}$, tj. splňuje, že $\psi'_{(iii)}(h) = \mathrm{id}_H$ právě, když pro všechna $h' \in H$ platí $h' = \mathrm{id}_H(h') = \psi'_{(iii)}(h)(h') = \phi_h(h') = hh'h^{-1}$ a to platí právě, když pro všechna $h' \in H$ máme $h'h = hh'$, tj. h je v centru $\mathbf{H}$.

S užitím 1. věty o izomorfismu grup k našemu $\psi'_{(iii)}$ dostáváme, že zobrazení $\psi_{(iii)} : \mathbf{H}/\mathrm{Z}(\mathbf{H}) \to \mathrm{Inn}(\mathbf{H})$ definované vztahem $h\,\mathrm{Z}(\mathbf{H}) \mapsto \psi'_{(iii)}(h) = \phi_h$ je dobře definovaný izomorfismus, jehož existence dokazuje, co jsme si přáli.

Složením nalezených izomorfismů $\psi := \psi_{(ii)} \circ \psi_{(iii)}$ získáme grupový izomorfismus $\mathbf{H}/\mathrm{Z}(\mathbf{H}) \to \mathrm{Inn}(\mathbf{H})\restriction_{e^G} \overset{\text{(i)}}{=} \text{LMlt } \left(\mathbf{e^G}\right)$ takový, že pro každé n přirozené a každá $h_i \in e^G, s_i \in \{\pm 1\}$, kde $i = 1, 2, \ldots, n$, platí

$$\left(\prod_{i=1}^{n} h_i^{s_i}\right) \mathrm{Z}(\mathbf{H}) \overset{\psi_{(iii)}}{\mapsto} \phi_{\prod_{i=1}^{n} h_i^{s_i}} \overset{\psi_{(ii)}}{\mapsto} \phi_{\prod_{i=1}^{n} h_i^{s_i}}\restriction_{e^G} \overset{\text{(i)}}{=} L_{h_1}^{s_1} \circ L_{h_2}^{s_2} \circ \cdots \circ L_{h_n}^{s_n}.$$

□

Lemma 3.6 nám dává strukturální vztah mezi $\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{G}}\right)$ a grupou $\mathbf{G}$ samotnou. Dále prozkoumejme podmínku míti regulární cyklus po vzoru [4].

Lemma 3.7. [4] *Je-li* $\mathbf{Q}$ *konečný quandl a* $\pi \in \mathrm{LMlt}(\mathbf{Q})$*, pak jsou následující podmínky ekvivalentní.*

(i) permutace π *má regulární cyklus,*

(ii) v permutaci π *existuje cyklus o délce jejího řádu v* $\mathrm{LMlt}(\mathbf{Q})$*,*

(iii) existuje $z \in Q$ *takové, že* $(\mathrm{LMlt}(\mathbf{Q}))_z \cap \langle \pi \rangle_{\mathrm{LMlt}(\mathbf{Q})} = \mathbf{1}$.

Důkaz. Pro $\pi = \mathrm{id}_Q$ jsou všechny podmínky splněny. Od tohoto momentu dále uvažujme fixní $\mathrm{id}_Q \neq \pi \in \mathrm{LMlt}(\mathbf{Q})$. Pro každý prvek $x \in Q$ označme ℓ_x to nejmenší přirozené číslo, že $\pi^{\ell_x}(x) = x$, tj. ℓ_x je délka toho cyklu π, ve kterém se nachází x. Navíc označme $\mathscr{o}$ řád permutace π v grupě $\mathrm{LMlt}(\mathbf{Q})$.

(i) ⇒ (ii): Permutace π má regulární cyklus, a tedy pro každé $y \in Q$ platí $\ell_y \mid \max(\{\ell_x \mid x \in Q\})$. Volbou z jako prvku z nějakého nejdelšího cyklu π, tj. $\ell_z = \max(\{\ell_x \mid x \in Q\})$, získáme, že pro všechna $y \in Q$ máme $\ell_y \mid \ell_z$. Následně pak díky tomu, že $\pi^{\ell_y}(y) = y$, máme $\pi^{\ell_z}(y) = \pi^{\ell_z \bmod \ell_y}(y) = \pi^0(y) = y$ pro všechna y, což znamená, že $\pi^{\ell_z} = \mathrm{id}_Q$. Z minimality $\mathscr{o}$ plyne $\mathscr{o} \leq \ell_z$. Současně však $\pi^{\mathscr{o}}(z) = z$, a tak z minimality ℓ_z nutně také $\ell_z \leq \mathscr{o}$. Celkově získáváme $\ell_z = \mathscr{o}$, tj. z je prvkem cyklu, jehož délka je rovna řádu permutace π jako prvku grupy $\mathrm{LMlt}(\mathbf{Q})$.

(ii) ⇒ (i): Z předpokladu existuje prvek $z \in Q$ takový, že $\ell_z = \mathscr{o}$. Pro každé $y \in Q$ platí $y = \mathrm{id}_Q(y) = \pi^{\mathscr{o}}(y) = \pi^{\mathscr{o} \bmod \ell_y}(y)$. Zajisté $\mathscr{o} \bmod \ell_y \in \{0, 1, \ldots, \ell_y - 1\}$. Z minimality ℓ_y víme, že $\pi^m(y) \neq y$ pro všechna $1 \leq m \lneq \ell_y$, a tedy nutně $\mathscr{o} \bmod \ell_y = 0$. To nám dává, že pro každé $y \in Q$ platí $\ell_y \mid \mathscr{o} = \ell_z$. Zbývá říci, že $\ell_z = \max(\{\ell_x \mid x \in Q\})$, to však plyne z toho, že pokud $\ell_y \mid \ell_z$, pak už $\ell_y \leq \ell_z$. Délka každého cyklu dělí délku nejdelšího cyklu, a tedy π má regulární cyklus.

(ii) ⇒ (iii): Z předpokladu existuje prvek $z \in Q$ takový, že $\ell_z = \mathscr{o}$. Pak z definice ℓ_z, kdykoliv si vezmeme $1 \leq m \lneq \ell_z = \mathscr{o}$, tak $\pi^m(z) \neq z$, a tedy $(\mathrm{LMlt}(\mathbf{Q}))_z \cap \{\pi^m \mid 1 \leq m \lneq \mathscr{o}\} = \emptyset$. Nutně už pak průnik grup $(\mathrm{LMlt}(\mathbf{Q}))_z$ a $\langle \pi \rangle_{\mathrm{LMlt}(\mathbf{Q})}$ obsahuje právě identitu na Q.

(iii) ⇒ (ii): Pro $z \in Q$ dané z předpokladu platí, že pro všechna $1 \leq m \lneq \mathscr{o}$ je $\pi^m \notin \mathbf{1} = (\mathrm{LMlt}(\mathbf{Q}))_z \cap \langle \pi \rangle_{\mathrm{LMlt}(\mathbf{Q})}$, a tedy $\pi^m(z) \neq z$. Z toho plyne, že $\ell_z \geq \mathscr{o}$. Víme, že $\pi^{\mathscr{o}}(z) = \mathrm{id}_Q(z) = z$, a tak z minimality ℓ_z současně $\ell_z \leq \mathscr{o}$. Celkově máme $\ell_z = \mathscr{o}$, tj. z je prvkem cyklu, jehož délka je rovna řádu permutace π. □

Tvrzení 3.8. *Je-li* $\mathbf{G}$ *grupa, e její prvek,* $\mathbf{Q} := \mathbf{e}^{\mathbf{G}}$ *konečný konjugační quandl a* $\mathbf{H} := \left\langle e^G \right\rangle_{\mathbf{G}}$ *grupa mající triviální centrum. Pak má* L_e *regulární cyklus právě tehdy, když existuje* $z \in e^G$*, které silně nekomutuje s* e*, tj. pro každé* $1 \leq k \lneq \mathrm{ord}_{\mathbf{G}}(e)$ *platí* $e^k z \neq z e^k$.

Důkaz. Ztotožněme prvky h grupy $\mathbf{H}$ s prvky $h\,\mathrm{Z}(\mathbf{H}) = h\mathbf{1}$ grupy $\mathbf{H}/\mathrm{Z}(\mathbf{H}) = \mathbf{H}/\mathbf{1}$. Dle lemmatu 3.7 má L_e regulární cyklus právě, když existuje $z \in e^G$ takové, že

$$(\mathrm{LMlt}(\mathbf{Q}))_z \cap \langle L_e \rangle_{\mathrm{LMlt}(\mathbf{Q})} = \mathbf{1}.$$

[4] Jak je vidět z důkazu, při zobecnění pojmu $\mathrm{LMlt}(\mathbf{Q})$ toto lemma platí dokonce i pro konečné levé kvazigrupy.

Označme ψ grupový izomorfismus ze znění lemmatu 3.6 a získáme, že tato rovnost platí právě, když platí rovnost

$$\psi^{-1}\left(\mathrm{LMlt}\left(\mathbf{Q}\right)\right)_z \cap \langle L_e\rangle_{\mathrm{LMlt}(\mathbf{Q})}) = \psi^{-1}\left(\mathbf{1}\right) = \mathbf{1}.$$

Množinové vzory se k chovají homomorfně k průnikům, a díky tomu

$$\psi^{-1}((\mathrm{LMlt}\left(\mathbf{Q}\right))_z \cap \langle L_e\rangle_{\mathrm{LMlt}(\mathbf{Q})}) = \psi^{-1}((\mathrm{LMlt}\left(\mathbf{Q}\right))_z) \cap \psi^{-1}(\langle L_e\rangle_{\mathrm{LMlt}(\mathbf{Q})}).$$

První výraz z průniku se za užití rovnosti z lemmatu 3.6 upraví

$$\begin{aligned}\psi^{-1}(\mathrm{LMlt}\left(\mathbf{Q}\right)_z) &= \psi^{-1}\left((\mathrm{Inn}(\mathbf{H})\restriction_Q)_z\right) = \left\{\psi^{-1}(\phi_h\restriction_Q) \mid h \in \mathbf{H} \ \wedge \ hz = zh\right\} \\ &= \{h\,\mathrm{Z}(\mathbf{H}) \mid h \in H \ \wedge \ hz = zh\} = \{h \in H \mid hz = zh\}.\end{aligned}$$

A protože obraz grupy je grupa generovaná obrazy jejích generátorů, tak pro druhý výraz máme

$$\psi^{-1}(\langle L_e\rangle_{\mathrm{LMlt}(\mathbf{Q})}) = \left\langle \psi^{-1}(L_e)\right\rangle_{\mathbf{G}} = \langle e\rangle_{\mathbf{G}}.$$

Celkově má L_e regulární cyklus právě tehdy, když existuje $z \in e^G$ takové, že

$$\{h \in H \mid hz = zh\} \cap \langle e\rangle_{\mathbf{G}} = \mathbf{1}. \tag{3.2}$$

Pro $e \neq 1_{\mathbf{G}}$ rovnost (3.2) říká právě to, pro každé $1 \leq k \lneq \mathrm{ord}_{\mathbf{G}}(e)$ nenastane $e^k z = ze^k$, jinak by prvek $e^k \neq 1_{\mathbf{G}}$ ležel v průniku. Případ $e = 1_{\mathbf{G}}$ je s tímto také konzistentní, protože ten splňuje obě podmínky z triviálních důvodů. □

Poznamenejme, že dle naší definice skutečně platí, že jednotka grupy silně nekomutuje sama se sebou. Jednotka nás v tomto kontextu zpravidla zajímat nebude, a proto tuto vadu definice kompenzovat nebudeme.

Naše věta 3.5 spolu se zpracováním myšlenek, které v [4] podali Stanovský a Vojtěchovský k důkazu tvrzení 3.2, nám dává následující větu!

Věta 3.9. *Je-li* $\mathbf{G}$ *konečná neabelovská jednoduchá grupa a* e *její prvek, pak jsou následující podmínky ekvivalentní.*

(i) konjugační quandl $\mathbf{e^G}$ *splňuje Hayashiho domněnku,*

(ii) existuje $z \in e^G$*, které silně nekomutuje s* e*.*

Důkaz. V případě, že $e = 1_{\mathbf{G}}$, jsou obě podmínky splněny triviálně. Nechť je dále $1_{\mathbf{G}} \neq e \in G$.

Grupa $\mathbf{H} := \left\langle e^G\right\rangle_{\mathbf{G}}$ je dle lemmatu 3.4 netriviální normální podgrupa jednoduché grupy $\mathbf{G}$, a tedy už nutně $\mathbf{H} = \mathbf{G}$. Centrum grupy $\mathbf{H} = \mathbf{G}$ je normální podgrupou jednoduché neabelovské grupy $\mathbf{G}$, a tedy je nutně triviální. Tím jsme ověřili předpoklady tvrzení 3.8, které nám říká, že translace L_e má regulární cyklus právě, když existuje $z \in e^G$, které silně nekomutuje s e.

Quandl $\mathbf{e^G}$ je konjugační quandl odvozený z jednoduché grupy, a tedy dle věty 3.5 je souvislý. Tím pádem díky lemmatu 2.7 konečný quandl $\mathbf{e^G}$ splňuje Hayashiho domněnku právě, když L_e má regulární cyklus, tj. právě, když existuje $z \in e^G$, které silně nekomutuje s e. □

Věta 3.9 dává charakterizaci speciálního případu Hayashiho domněnky ve smyslu čistě grupových pojmů. Při snaze ji vyvrátit, nám díky ní stačí najít konečnou neabelovskou jednoduchou grupu takovou, že v ní existuje prvek, který není jednotka a který s každým prvkem jeho konjugační třídy komutuje v alespoň jedné netriviální mocnině.

3.3 Cykly translací v konjugačních quandlech typu $\mathbf{e^{S_n}}$ a $\mathbf{e^{A_n}}$

V sekci 3.2 jsme uvedli poměrně obecnou teorii, která v některých případech konjugačních quandlů pomocí vlastností jejich definující grupy charakterizuje stav, kdy má translace L_e regulární cyklus. V této sekci bude naším cílem ověřit Hayashiho domněnku pro konjugační quandly typu $\mathbf{e^{A_n}}$ a $\mathbf{e^{S_n}}$. Věta 3.9 nám spolu s tvrzením 3.5 dává charakterizaci pro quandly typu $\mathbf{e^{A_n}}$, tj. tvrzení 3.11. Důsledkem tvrzení 3.8 je pak i charakterizace platnosti Hayashiho domněnky pro $\mathbf{e^{S_n}}$ popsaná v tvrzení 3.10.

Tvrzení 3.10. *Nechť $n \geq 5$ a $e \in S_n$. Pak má v konjugačním quandlu $\mathbf{e^{S_n}}$ translace L_e regulární cyklus právě tehdy, když existuje $z \in e^{S_n}$, které silně nekomutuje s e.*

Důkaz. Z lemmatu 3.4 víme, že je grupa $\mathbf{H} := \left\langle e^{S_n} \right\rangle_{\mathbf{S}_n}$ normální podgrupa $\mathbf{S}_n$. Pro $n \geq 5$ jsou $\mathbf{1}, \mathbf{A}_n$ a $\mathbf{S}_n$ jediné normální podgrupy $\mathbf{S}_n$, a tedy $\mathbf{H}$ je jedna z nich. Centrum grupy $\mathbf{H}$ je normální podgrupou $\mathbf{H}$. S užitím znalosti normálních podgrup $\mathbf{S}_n$ a jednoduchosti $\mathbf{A}_n$ pro $n \geq 5$ svedeme říci, že i $\mathrm{Z}(\mathbf{H}) \in \{\mathbf{1}, \mathbf{A}_n, \mathbf{S}_n\}$. Centrum je vždy abelovská grupa, ale $\mathbf{A}_n$ ani $\mathbf{S}_n$ abelovské nejsou: Permutace (1 2 3)(1 2 4) zobrazuje prvek 1 na 3, zatímco (1 2 4)(1 2 3) zobrazuje prvek 1 na 4, a tedy (1 2 3) $\in A_n \subseteq S_n$ a (1 2 4) $\in A_n \subseteq S_n$ vzájemně nekomutují. Tím jsme ukázali, že už nutně $\mathrm{Z}(\mathbf{H}) = \mathbf{1}$ a tvrzení 3.8 přesně říká, co jsme chtěli ukázat. □

Tvrzení 3.11. *Nechť $n \geq 5$ a $e \in A_n$. Pak má v konjugačním quandlu $\mathbf{e^{A_n}}$ translace L_e regulární cyklus právě tehdy, když existuje $z \in e^{A_n}$, které silně nekomutuje s e.*

Důkaz. Z věty 3.5 víme, že jsou tyto quandly souvislé. Jak jsme viděli v důkaze věty 3.9 existence silně nekomutujícího prvku je ekvivalentní tomu, že quandl $\mathbf{e^{A_n}}$ splňuje Hayashiho domněnku a to je ze souvislosti a konečnosti díky lemmatu 2.7 ekvivalentní, že translace L_e má regulární cyklus. □

Posledním dílem k ověření Hayashiho domněnky pro konjugační quandly typu $\mathbf{e^{A_n}}$ a $\mathbf{e^{S_n}}$ pro $n \geq 5$ je nalezení zmíněných prvků z, které silně nekomutují s prvkem e. Stanovský a Vojtěchovský v [4] přišli na to, jaké vlastnosti po prvku z v případě quandlů $\mathbf{e^{S_n}}$ požadovat, aby se zmíněné nekomutativity dosáhlo. Existence prvku s vyžádanými vlastnostmi byla v jejich případě zřejmá z faktu, že permutace jsou vzájemně konjugované grupou $\mathbf{S}_n$ právě tehdy, když mají stejnou strukturu cyklů.

Doposud jsme ověřili, že postup, který Stanovský a Vojtěchovský v [4] použili ve svém důkazu pro $\mathbf{e^{S_n}}$, funguje do tohoto bodu i pro $\mathbf{e^{A_n}}$. Během ukazování existence silně nekomutujícího prvku z se nám, až na jeden výjimečný případ (konkrétně případ $\ell_1 \geq 4, t = 1$ v důkazu lemmatu 3.14), podaří zachovat seznam vlastností, které po něm požadovali ve svém důkazu i oni. Jeho existence však již nebude zřejmá, protože jej nebudeme hledat v konjugační třídě grupy $\mathbf{S}_n$, nýbrž $\mathbf{A}_n$. V té už není pravda, že by dvě permutace byly vzájemně konjugované právě, když mají stejnou strukturu cyklů. Důkaz existence provedeme konstrukcí. Tato konstrukce bude dokonce fungovat pro quandly $\mathbf{e^{A_n}}$ a $\mathbf{e^{S_n}}$ současně.

Myšlenku celé konstrukce založíme na následujícím lemmatu. To nám spolu s jednou jeho interpretací umožní s permutacemi pracovat více hmatatelně a poskytne nám nadhled nad daným problémem.

Lemma 3.12. *Nechť $n \geq 3$ a nechť $\rho, e \in S_n$. Pak $\rho \in e^{A_n}$ právě, když existuje n přirozené a 3-cykly $m_i \in S_n$ takové, že $\rho = \phi_{m_1} \circ \phi_{m_2} \circ \cdots \circ \phi_{m_n}(e)$.*

Důkaz. Víme [6, Exercise 2.7], že pro každé $n \geq 3$ je grupa $\mathbf{A}_n$ generovaná množinou všech 3-cyklů, označme ji M. Pro naše $\rho \in e^{A_n}$, existuje $\sigma \in A_n$ takové, že $\rho = e^\sigma$ a pro to zase existuje n přirozené a $m_i \in M \cup M^{-1}$ taková, že $\sigma = \prod_{i=1}^n m_i$. Inverz 3-cyklu je opět 3-cyklus, a proto m_i jsou 3-cykly a my získáváme žádané

$$\rho = e^\sigma = e^{\prod_{i=1}^n m_i} = \phi_{m_1} \circ \phi_{m_2} \circ \cdots \circ \phi_{m_n}(e).$$

Implikace zprava doleva je triviální, protože 3-cykly jsou sudé permutace a jejich složení už jsou nutně také sudé permutace. □

Definice 3.13. Je-li dáno n přirozené a po dvou různé prvky $a, b, c \in \{1, 2, \ldots, n\}$, pak

- pojmem 3-*cyklická substituce* $a \mapsto b \mapsto c \mapsto a$ myslíme konjugaci 3-cyklem $(a\ b\ c) \in S_n$.
- pojmem 3-*cyklická rotace* $a \to b \to c \to a$ myslíme konjugaci 3-cyklem $(a\ b\ c)^{-1} \in S_n$.

Právě jsme zavedli dva nové pojmy pro jednu již existující akci, tj. konjugaci 3-cyklem. Tyto definice však mají smysl, protože slouží k definování přirozenějšího pohledu na provádění zmíněné konjugace. Tento pohled vychází ze známého faktu [5, str. 96], a sice: Jsou-li $e, \alpha \in S_n$ permutace takové, že e má cyklický zápis

$$(u_{1,1}\ u_{1,2} \cdots u_{1,m_1})(u_{2,1} \cdots u_{2,m_2}) \cdots (u_{m,1} \cdots u_{m,m_m}) \in S_n, \tag{3.3}$$

pak má permutace e^α cyklický zápis

$$(\alpha(u_{1,1})\ \alpha(u_{1,2}) \cdots \alpha(u_{1,m_1}))\,(\alpha(u_{2,1}) \cdots \alpha(u_{2,m_2})) \cdots (\alpha(u_{m,1}) \cdots \alpha(u_{m,m_m}))\,. \tag{3.4}$$

Tato identita nám umožňuje konjugaci 3-cyklem provádět úpravou zápisů, které právě nazýváme 3-cyklická substituce a 3-cyklická rotace. Vysvětleme jejich interpretaci a význam.

Máme-li e stejně jako v (3.3) a máme-li 3-cyklus $(a\ b\ c) \in S_n$, pak si konjugaci prvku e pomocí 3-cyklu $(a\ b\ c)$ můžeme představit jako nahrazování znaků způsobem stejným jako v (3.4). Provedení této konjugace tedy znamená v daném (úplném) cyklickém zápise permutace e „přepsat“ prvek a na prvek b, ten na prvek c a ten na prvek a, zatímco všechny ostatní prvky zůstanou nepozměněny. Svým způsobem to tedy znamená, že na znaky tohoto zápisu aplikujeme 3-cyklické nahrazení $a \mapsto b \mapsto c \mapsto a$, tj. náš pojem 3-cyklická substituce. Uveďme si jeden konkrétní příklad.

Příklad. Nechť $(1\ 2\ 3)(4)$ je nějaký z cyklických zápisů permutace z S_4. Aplikujeme-li na něj substituci $1 \mapsto 4 \mapsto 2 \mapsto 1$, tak získáme zápis $(4\ 1\ 3)(2)$, který tentokrát odpovídá jiné permutaci z S_4, konkrétně té permutaci, kterou lze z původní získat konjugací 3-cyklem $(1\ 4\ 2)$. ■

Máme-li e stejně jako v (3.3) a máme-li 3-cyklickou rotaci $a \to b \to c \to a$, pak z její definice tato rotace odpovídá konjugaci 3-cyklem $(a\ b\ c)^{-1}$, tj. 3-cyklické substituci $a \mapsto c \mapsto b \mapsto a$. Opět tedy její aplikací na zápis permutace e dojde k zachování pozic všech prvků různých od a, b, c, ale prvky a, b, c se tentokrát budou „přepisovat“ opačným směrem. To prakticky znamená, že se prvek a „přesune“ na původní pozici prvku b, ten na pozici prvku c a ten na pozici prvku a. Nahlédnout, že toto je skutečně to, co se děje, se dá tak, že následnou aplikací 3-cyklické substituce, která odpovídá konjugaci inverzním 3-cyklem, tj. provedením substituce $a \mapsto b \mapsto c \mapsto a$, dostaneme zpět původní zápis permutace e (prvek a se přesunul na pozici prvku b a tam byl nahrazen prvkem b, apod.). Tyto operace jsou skutečně inverzní, a proto jsme 3-cyklickou rotaci interpretovali správně. Provádění 3-cyklických rotací je pro nás, jak bylo právě vysvětleno, jinou myšlenkovou interpretací konjugace 3-cyklem. Opět si uveďme konkrétní příklad.

Příklad. Nechť $(1\ 2\ 3)(4)$ je nějaký z cyklických zápisů permutace z S_4. Aplikujeme-li na něj rotaci $1 \mapsto 2 \mapsto 4 \mapsto 1$, tak provádíme cyklický posun znaků v tomto zápise naznačený v (3.5).

$$(\overleftarrow{1\ \overrightarrow{2}\ 3)(\overrightarrow{4}}) \rightsquigarrow (4\ 1\ 3)(2). \tag{3.5}$$

získáme zápis $(4\ 1\ 3)(2)$, který tentokrát odpovídá jiné permutaci z S_4, konkrétně té permutaci, kterou lze z původní získat konjugací 3-cyklem $(1\ 2\ 4)^{-1}$. ■

Substituce je vhodná ve chvílích, kdy chceme z daného zápisu permutace přímo určit výsledný zápis po konjugaci daným 3-cyklem. Rotace zase lépe ukazuje, co se v zápise permutace při konjugaci skutečně děje, ale její představa často vyžaduje nakreslení šipek jako v (3.5).

Dále poznamenejme, že budeme pracovat výhradně s úplnými cyklickými zápisy permutací. V těch se vyskytují všechny symboly, na kterých odpovídající permutace koná akci. Zápis $(1\ 2\ 3)(4\ 5)$ pro nás tedy v tomto kontextu reprezentuje konkrétní permutaci z S_5, avšak neodpovídá úplnému cyklickému zápisu žádné z permutací v S_6 a vyšších. Užíváním úplných cyklických zápisů se tak vyhneme rozpakům v případě aplikace rotace, resp. substituce, která užívá prvky, jež v zápisu nejsou znázorněny.

Aplikace 3-cyklických substitucí a 3-cyklických rotací jsou jen jiné interpretace konjugací pomocí 3-cyklů. Svedeme-li tedy ze zápisu permutace e tímto způsobem získat zápis permutace z, pak dle lemmatu 3.12 platí, že $z \in e^{A_n}$. Tuto skutečnost budeme dále v textu považovat za samozřejmou a nebudeme se na ni odkazovat. Poznamenejme ještě, že platí i opačná implikace, tj. pokud leží permutace ve stejné konjugační třídě dané grupou $\mathbf{A}_n$, pak taková posloupnost aplikací 3-cyklických substitucí nebo 3-cyklických rotací existuje. Tuto implikaci však v textu nevyužijeme.

Zavedený jazyk nám umožňuje vyložit důkaz následujícího tvrzení v intuitivní a přirozené formě.

Lemma 3.14. *Nechť $n \geq 5$ a nechť $e \in \mathbf{S}_n$, pak existuje $z \in e^{A_n}$, které silně nekomutuje s e.*

Důkaz. Pro $e = \mathrm{id}_{\{1,2,\ldots,n\}}$ je znění splněno. Nechť je dále $\mathrm{id}_{\{1,2,\ldots,n\}} \neq e \in S_n$ fixní. V důkaze rozebereme tři případy v závislosti na spektru permutace ρ. Pro

každý z těchto případů vyslovíme soubor vlastností, které budeme požadovat po hledaném prvku z (stejně jako v [4]). Ukážeme, že tyto vlastnosti zajistí silnou nekomutativitu a následně provedeme konstrukci nějakého takového prvku, čímž ověříme jeho náležení do množiny e^{A_n}.

Nechť $t := |\Lambda(e)|$. Pro zkrácení zápisu, kdykoliv budeme psát x, pak myslíme, že jde o prvek množiny $\{1, 2, \ldots, n\}$ a kdykoliv budeme psát i, pak jde o prvek množiny $\{1, 2, \ldots, t\}$. Z toho, že $e \neq \mathrm{id}_{\{1,2,\ldots,n\}}$, nutně $\ell_t \gneq 1$. Stejně jako tomu bylo v důkaze lemmatu 3.7, budeme značit ℓ_x délku cyklu permutace e, v níž se nachází prvek x. Struktura grupy nezávisí na pojmenování prvků, a tedy bez újmy na obecnosti můžeme předpokládat, že

$$\ell_1 \lneq \ell_2 \lneq \cdots \lneq \ell_t. \tag{3.6}$$

Tím jsme bez opakování vyčerpali všechny délky cyklů, a tedy pro každé x najdeme právě jedno i, že $\ell_x = \ell_i$. Označme i_x toto i příslušné prvku x. Dále pro každé $j = 1, 2, \ldots, \ell_{t-1}$ označme $x_j := e^j(t)$. Permutace e tedy obsahuje cyklus $(t\ x_1\ x_2\ \ldots\ x_{\ell_t-1})$.

Případ $\ell_1 = 1$: Zkoumejme $z \in S_n$ taková, že

$$z(t) = t - 1, z(t-1) = t - 2, \ldots, z(2) = 1.$$

Nechť je dáno $1 \leq k \lneq \mathrm{ord}_{\mathbf{S}_n}(e)$. Kdyby pro všechna i platilo, že $\ell_i \mid k$, pak by pro každé x bylo $e^k(x) = e^{k \bmod \ell_{i_x}}(x) = e^0(x) = x$, a tedy $e^k = \mathrm{id}_{\{1,2,\ldots,n\}}$, což by byl spor s minimalitou $\mathrm{ord}_{\mathbf{S}_n}(e) \gneq k$. To nám umožňuje uvážit $i_{\min}$, to nejmenší takové i, že $e^k(i) = e^{k \bmod \ell_i}(i) \neq i$. Předpokládáme, že $\ell_1 = 1 \mid k$, a tedy $i_{\min} \gneq 1$. Z minimality $i_{\min}$ plyne, že $e^k(i_{\min} - 1) = i_{\min} - 1$. Teď již máme

$$e^k z(i_{\min}) = e^k(i_{\min} - 1) = i_{\min} - 1 = z(i_{\min}) \neq z e^k(i_{\min}),$$

kde poslední nerovnost víme z toho, že z je bijekce a $e^k(i_{\min}) \neq i_{\min}$. Tím jsme ukázali, že taková z splňují, co požadujeme. Pokročme ke konstrukci.

Kdyby bylo e složeno z právě 2 (nezávislých) cyklů, pak už $\ell_t = \ell_2 = n - 1 \geq 3$, a proto smíme provést rotaci $1 \to x_1 \to x_2 \to 1$, jak je naznačeno v (T).

$$(\overbrace{1)(2\ x_1\ x_2}\ \ldots) \rightsquigarrow (x_2)(2\ 1\ x_1\ \ldots) \tag{T}$$

Tímto získáme z s hledanou vlastností a z konstrukce $z \in e^{A_n}$.

Ve zbylých případech má e alespoň 3 cykly. Ze (3.6) nutně pro každé i platí $\ell_i \geq i$. Permutaci e smíme zapsat ve formě

$$(1)(2\ \ldots) \cdots (t-1\ \ldots)(t\ x_1\ x_2\ \ldots\ x_{\ell_t-1}) \cdots,$$

kde poslední „$\cdots$“ naznačuje zbylé cykly neobsahující žádný z prvků i. Postupně do cyklu obsahujícího t budeme za sebe „skládat“ prvky i rotacemi

$$t - 1 \to x_1 \to x_2 \to t - 1, \tag{T.$t-1$}$$
$$t - 2 \to x_1 \to x_3 \to t - 2, \tag{T.$t-2$}$$
$$\vdots$$
$$t - j \to x_1 \to x_{j+1} \to t - j, \tag{T.$t-j$}$$
$$\vdots$$
$$2 \to x_1 \to x_{t-1} \to 2. \tag{T.2}$$

Poznamenejme, že všechny tyto rotace jsou dobře definované, protože máme k dispozici proměnné $x_1, x_2, \ldots, x_{\ell_t - 1}$ a $\ell_t \geq t$. Definovatelnost rotace „(T.1)“ už však jasná není, s poslední rotací si tedy poradíme jinak. Postupnou aplikací (T.$t-1$) až (T.2) znázorněnou v (T'.$t-1$) až (T'.2)

$$(1)(2\ \ldots)\cdots(t\ \overbrace{t-1\ \ldots)(t\ \overset{\searrow}{x_1}\ \overset{\searrow}{x_2}}\ \ldots)\cdots, \tag{T'.$t-1$}$$

$$(1)(2\ \ldots)\cdots(t\ \overbrace{t-2\ \ldots)\cdots(t\ t-1\ \overset{\searrow}{x_1}\ \overset{\searrow}{x_3}}\ \ldots)\cdots, \tag{T'.$t-2$}$$

$$\vdots$$

$$(1)(2\ \ldots)\cdots(t\ \overbrace{t-j\ \ldots)\cdots(t\ \ldots\ t-j-1\ \overset{\searrow}{x_1}\ \overset{\searrow}{x_{j+1}}}\ \ldots)\cdots, \tag{T'.$t-j$}$$

$$\vdots$$

$$(1)(\overbrace{2\ \ldots)\cdots(t\ \ldots\ t-j-1\ \ldots\ 3\ \overset{\searrow}{x_1}\ \overset{\searrow}{x_{t-1}}}\ \ldots)\cdots \tag{T'.2}$$

obdržíme zápis tvaru

$$(1)\cdots(t\ t-1\ \ldots\ 3\ 2\ x_1\ \ldots)\cdots.$$

Předpokládáme, že e původně měla alespoň 3 cykly, nutně i náš aktuální zápis má alespoň 3. Všechny prvky i a prvek x_1 jsou teď však dohromady obsažené pouze ve 2 cyklech, a my tedy máme k dispozici cyklus, který žádný z nich neobsahuje. Speciálně máme nějaký prvek y tohoto cyklu takový, že $1, x_1$ a y jsou vzájemně různé a že aplikováním rotace $1 \to x_1 \to y \to 1$, jak je znázorněno v (T.1*), nepřemístíme žádný z již „srovnaných“ prvků i. Poznamenejme, že nevíme s jistotou, zda tento cyklus původně obsahoval nějaký prvek i nebo ne a my tedy nevíme, zda ho najdeme v levých „$\cdots$“ nebo v pravých „$\cdots$“. Na tom nám ale nezáleží.

$$(\overbrace{1)\cdots(t\ t-1\ \ldots\ 3\ 2\ \overset{\searrow}{x_1}\ \ldots)\cdots(\ldots\ \overset{\searrow}{y}}\ \ldots)\cdots \tag{T.1*}$$

Výsledný zápis

$$\cdots(t\ t-1\ \ldots\ 2\ 1\ \ldots)\cdots$$

odpovídá permutaci s chtěnou vlastností, kterou budeme považovat za naše z a z konstrukce $z \in e^{A_n}$.

Případ $\ell_1 \neq 1, t \neq 1$: Pro každé $j = 1, 2, \ldots, \ell_1 - 1$ označme $u_j := e^j(1)$. Permutace e tedy obsahuje cyklus $(1\ u_1\ u_2\ \ldots\ u_{\ell_1 - 1})$. Zkoumejme $z \in S_n$ taková, že

$$z(t) = t-1, z(t-1) = t-2, \ldots, z(2) = 1, z(1) = u_1$$

a navíc pro každé $j = 1, 2, \ldots, \ell_1 - 1$ platí

$$z(u_j) \notin \{u_{\bar{j}} \mid \bar{j} \in \{1, 2, \ldots, \ell_1 - 1\}\}.$$

Nechť je dáno $1 \leq k \lneq \mathrm{ord}_{\mathbf{S}_n}(e)$. Stejně jako výše můžeme uvážit $i_{\min}$. Jestliže je $i_{\min} \gneq 1$, pak funguje stejný argument jako výše, protože z speciálně splňuje i vlastnosti z prvního případu. Je-li naopak $i_{\min} = 1$, pak $e^k(1) \neq 1$, a tedy $e^k(1) \in \{u_{\bar{j}} \mid \bar{j} \in \{1, 2, \ldots, \ell_1 - 1\}\}$. Z toho pak víme z vlastností z víme, že $ze^k(1) \notin \{u_{\bar{j}} \mid \bar{j} \in \{1, 2, \ldots, \ell_1 - 1\}\}$. Skládáme-li permutace v druhém pořadí,

tak máme $e^k z(1) = e^k(u_1) \in \{1\} \cup \{u_{\bar{j}} \mid \bar{j} \in \{1, 2, \ldots, \ell_1 - 1\}\}$. Kdyby pro spor platilo, že $e^k z(1) = z e^k(1)$, pak už nutně $z e^k(1) = 1$, tzn. $e^k(1) = z^{-1}(1) = 2$, což je spor s tím, že $e^k(1) \in \{u_{\bar{j}} \mid \bar{j} \in \{1, 2, \ldots, \ell_1 - 1\}\}$. Tím jsme ukázali, že taková z splňují, co požadujeme. Překročme ke konstrukci.

Tentokrát z (3.6) dokonce víme, že $\ell_t \geq \ell_{t-1} + 1 \geq \cdots \geq \ell_1 + (t-1)$. To nám dává, že $\ell_t - 1 \geq \ell_1 + t - 2$, a my tedy máme alespoň $\ell_1 + t - 2$ indexovaných proměnných x. Začněme s obdobným zápisem e jako tomu bylo i posledně.

$$e = (1\ u_1\ u_2\ \ldots\ u_{\ell_1-1})(2\ \ldots) \cdots (t-1\ \ldots)(t\ x_1\ x_2\ \ldots\ x_{\ell_1+t-2}\ \ldots) \cdots$$

Víme, že $\ell_1 \gneq 1$, a proto máme speciálně alespoň t indexovaných proměnných x. To nám umožňuje aplikovat rotace (T.$t-1$) až (T.2) z minulého případu a obdržet permutaci se zápisem

$$(1\ u_1\ \ldots\ u_{\ell_1-1}) \cdots (t\ t-1\ \ldots\ 3\ 2\ x_1\ x_t\ \ldots\ x_{\ell_1+t-2}\ \ldots) \cdots .$$

Rotací $1 \to x_1 \to u_1 \to 1$ znázorněnou v (T.1**) docílíme zápisu (3.7).

$$(\overset{\uparrow}{1}\ \overset{\uparrow}{u_1}\ \ldots\ u_{\ell_1-1}) \cdots (t\ t-1\ \ldots\ 3\ 2\ \overset{\downarrow}{x_1}\ x_t\ \ldots\ x_{\ell_1+t-2}\ \ldots) \cdots \tag{T.1**}$$

$$(u_1\ x_1\ u_2\ \ldots\ u_{\ell_1-1}) \cdots (t\ \ldots\ 2\ 1\ x_t\ x_{t+1}\ \ldots\ x_{\ell_1+t-2}\ \ldots) \tag{3.7}$$

Definujme posloupnost rotací

$$u_3 \to u_2 \to x_t \to u_3, \tag{U.u_3}$$
$$u_5 \to u_4 \to x_{t+2} \to u_5, \tag{U.u_5}$$
$$\vdots$$
$$u_{2j+1} \to u_{2j} \to x_{t+2j-2} \to u_{2j+1}. \tag{U.u_{2j+1}}$$

Postupně pro všechna $j = 1, 2, \ldots$ taková, že $2j + 1 \leq \ell_1 - 1$, tj. taková, že máme definovánu proměnnou u_{2j+1}, proveďme rotaci (U.u_{2j+1}), jak je znázorněno v (U'.u_3) až (U'.u_{2j+1}). Každá z těchto rotací je dobře definována, protože $t + 2j - 2 \leq t + \ell_1 - 4 \leq \ell_t - 3$, a tedy máme definovánu proměnnou x_{t+2j-2} pro všechna užitá j (pokud žádné takové j neexistuje, tj. pokud $\ell_1 - 1 \leq 2$, pak pokračujme dále beze změn).

$$(u_1\ x_1\ \overset{\uparrow}{u_2}\ \overset{\uparrow}{u_3}\ \ldots) \cdots (t\ \ldots\ 2\ 1\ \overset{\downarrow}{x_t}\ x_{t+1}\ \ldots), \tag{U'.u_3}$$
$$(u_1\ x_1\ u_3\ x_t\ \overset{\uparrow}{u_4}\ \overset{\uparrow}{u_5}\ \ldots) \cdots (t\ \ldots\ 2\ 1\ u_2\ x_{t+1}\ \overset{\downarrow}{x_{t+2}}\ \ldots), \tag{U'.u_5}$$
$$\vdots$$
$$(\ldots\ u_{2j-2}\ x_{t+2j-4}\ \overset{\uparrow}{u_{2j}}\ \overset{\uparrow}{u_{2j+1}}\ \ldots) \cdots (t\ \ldots\ x_{t+2j-3}\ \overset{\downarrow}{x_{t+2j-2}}\ \ldots). \tag{U'.u_{2j+1}}$$

- Je-li $\ell_1 - 1$ liché, pak skončíme se zápisem

  $$(u_1\ x_1\ u_3\ x_t\ u_5\ \ldots\ x_{t+\ell_1-6}\ u_{\ell_1-1}\ x_{t+\ell_1-4}) \cdots$$
  $$(t\ \ldots\ 2\ 1\ u_2\ x_{t+1}\ u_4\ x_{t+3}\ \ldots\ x_{t+\ell_1-5}\ u_{\ell_1-2}\ x_{t+\ell_1-3}\ x_{t+\ell_1-2}\ \ldots) \cdots .$$

  To můžeme považovat za naše z. Permutace z má požadované vlastnosti a z konstrukce $z \in e^{A_n}$.

- Je-li $\ell_1 - 1$ sudé, pak skončíme se zápisem

$$(u_1\ x_1\ u_3\ x_t\ u_5\ \dots\ x_{t+\ell_1-5}\ u_{\ell_1-1})\cdots$$
$$(t\ \dots\ 1\ u_2\ x_{t+1}\ u_4\ \dots\ x_{t+\ell_1-6}\ u_{\ell_1-3}\ x_{t+\ell_1-4}\ x_{t+\ell_1-3}\ x_{t+\ell_1-2}\ \dots)\cdots .$$

  V takovém případě ještě nemáme hotovo, protože se prvek u_{ℓ_1-1} zobrazuje na prvek u_1. Provedením substituce $u_{\ell_1-1} \mapsto x_1 \mapsto x_{t+\ell_1-3} \mapsto u_{\ell_1-1}$ již docílíme hledaných vlastností. Poznamenejme, že tento postup zafungoval i pro $\ell_1 - 1 = 2$. Výslednou permutaci tedy označíme z a z konstrukce $z \in e^{A_n}$.

Případ $\ell_1 \neq 1, t = 1$**:** Zde rozebereme 3 případy v závislosti na hodnotě ℓ_1. Všimněme si, že v tomto případě je $\mathrm{ord}_{\mathbf{S}_n}(e) = \ell_1$. Nekomutativitu tedy ověřujeme pro mocniny $1 \leq k \lneq \mathrm{ord}_{\mathbf{S}_n}(e) = \ell_1$.

- Je-li $\ell_1 = 2$, pak díky tomu, že $n \geq 5$, nutně e obsahuje alespoň 3 různé 2-cykly. Označme jejich prvky tak, že je

$$e = (1\ u_1)(u_2\ u_3)(u_4\ u_5)\cdots .$$

  Aplikováním substituce $u_1 \mapsto u_2 \mapsto u_3 \mapsto u_1$ získáme zápis

$$(1\ u_2)(u_3\ u_1)(u_4\ u_5)\cdots$$

  a následnou aplikací $u_3 \mapsto u_1 \mapsto u_4 \mapsto u_3$ obdržíme

$$z := (1\ u_2)(u_1\ u_4)\cdots .$$

  Platí, že $e^1 z(1) = e^1(u_2) = u_3 \neq u_4 = z(u_1) = z e^1(1)$ a z konstrukce $z \in e^{A_n}$.
- Je-li $\ell_1 = 3$, pak nutně e obsahuje alespoň 2 různé 3-cykly. Označme jejich prvky tak, že je

$$e = (1\ u_1\ u_2)(u_3\ u_4\ u_5)\cdots .$$

  Aplikací substituce $u_2 \mapsto u_3 \mapsto u_4 \mapsto u_2$ získáme

$$z := (1\ u_1\ u_3)(u_4\ u_2\ u_5)\cdots .$$

  Platí, že $e^1 z(1) = e^1(u_1) = u_2 \neq u_3 = z(u_1) = z e^1(1)$ a $e^2 z(1) = e^2(u_1) = 1 \neq u_5 = z(u_2) = z e^2(1)$. Z konstrukce současně $z \in e^{A_n}$.
- Je-li $\ell_1 \geq 4$, pak označme prvky, že je

$$e = (1\ u_1\ u_2\ \dots\ u_{\ell_1-1})\cdots$$

  a dále označme $u_0 := 1$. Tím máme

$$e = (u_0\ u_1\ u_2\ \dots\ u_{\ell_1-1})\cdots .$$

  Aplikací substituce $u_0 \mapsto u_1 \mapsto u_2 \mapsto u_0$ získáme

$$z := (u_1\ u_2\ u_0\ u_3\ \dots\ u_{\ell_1-1})\cdots .$$

Vezměme libovolné $1 \leq k \lneq \mathrm{ord}_{\mathbf{S}_n} = \ell_1$. Pro každé $0 \leq j \leq \ell_1 - 1$ nám platí $e^k(u_j) = u_{j+k \bmod \ell_1}$, a tedy $e^k z(u_0) = e^k(u_3) = u_{3+k \bmod \ell_1}$. Naopak

$$ze^k(u_0) = z(u_{k \bmod \ell_1}) = z(u_k) = \begin{cases} u_2, & \text{pokud } k = 1, \\ u_0, & \text{pokud } k = 2, \\ u_{k+1}, & \text{pokud } 3 \leq k \lneq \ell_1 - 1, \\ u_1, & \text{pokud } k = \ell_1 - 1. \end{cases}$$

Poznamenejme, že $k \neq 0$.

Kdyby nastalo, že $e^k z(u_0) = ze^k(u_0)$, pak $u_{3+k \bmod \ell_1} = z(u_k)$, a tedy

$$3 + k \bmod \ell_1 = \begin{cases} 2, & \text{pokud } k = 1, \\ 0, & \text{pokud } k = 2, \\ k+1, & \text{pokud } 3 \leq k \lneq \ell_1 - 1, \\ 1, & \text{pokud } k = \ell_1 - 1. \end{cases}$$

Odečtením $3 + k$ na obou stranách pak v aritmetice $\bmod \ell_1$ získáme

$$0 \equiv_{\ell_1} \begin{cases} -k - 1 \equiv_{\ell_1} -2, & \text{pokud } k = 1, \\ -k - 3 \equiv_{\ell_1} -5, & \text{pokud } k = 2, \\ -2, & \text{pokud } 3 \leq k \lneq \ell_1 - 1, \\ -k - 2 \equiv_{\ell_1} -1, & \text{pokud } k = \ell_1 - 1. \end{cases}$$

Vidíme, že pro $\ell_1 \geq 4$ si všechny případy až na $k = 2 \ \wedge \ \ell_1 = 5$ protiřečí. V takovém případě však $ze^2(u_2) = z(u_4) = u_1 \neq u_2 = e^2(u_0) = e^2 z(u_2)$, a tedy $e^k z \neq ze^k$ pro všechna $1 \leq k \lneq \mathrm{ord}_{\mathbf{S}_n}(e)$. Z konstrukce plyne, že $z \in e^{A_n}$ a my jsme hotovi.

□

Závěrem již smíme vyslovit a dokázat žádané výsledné tvrzení.

Tvrzení 3.15. *V konjugačních quandlech tvaru* $\mathbf{e^{A_n}}$ *a* $\mathbf{e^{S_n}}$ *má* L_e *regulární cyklus.*

Důkaz. K ověření případů $n \geq 5$ využijeme dokázaných výsledků, případy $n \leq 3$ budou příliš malé na to, aby mohly mít regulární cyklus, a případ $n = 4$ rozebereme ručně.

Případ $n \geq 5$**:** Z lemmatu 3.14 existuje $z \in e^{A_n}$, resp. speciálně v e^{S_n}, které silně nekomutuje s e, a tedy dle tvrzení 3.11, resp. 3.10, má L_e regulární cyklus.

Případ $n \leq 3$**:** Platí, že $|e^{A_n}| \leq |e^{S_n}| \leq 5$, kde poslední nerovnost plyne z toho, že $\{\mathrm{id}_{\{1,2,\ldots,n\}}\}$ vždy tvoří konjugační třídu $\mathbf{S}_n$, a tedy pro každou konjugační třídu platí, že je buďto velikosti 1 nebo je velikosti nejvýše $|S_n| - 1$ a pro $n \leq 3$ jsou obě tyto možnosti ≤ 5. Každá levá translace v quandlu velikosti nejvýše 5 má nutně regulární cyklus: Z idempotentnosti quandlu tato translace obsahuje 1-cyklus, největší možná délka cyklu v této translaci je tedy 4 a ať už je to $4, 3, 2$ nebo 1, tak ji délky všech zbylých cyklů už nutně dělí. Speciálně i L_e má regulární cyklus.

Případ $n = 4$**:** Označme $Q := e^{A_4}$, resp. e^{S_4}. Pak vzhledem k tomu, že řád každého prvku v $\mathbf{S}_4$ je nejvýše 4 a z definice konjugační quandlové operace platí $L_e^{\mathrm{ord}_{\mathbf{S}_4}(e)} = L_{e^{\mathrm{ord}_{\mathbf{S}_4}(e)}} = L_{\mathrm{id}_{\{1,2,3,4\}}} = \mathrm{id}_Q$, tak $\Lambda(L_e) \subseteq \{1,2,3,4\}$. Všimněme si, že jestliže $3 \notin \Lambda(L_e)$, pak už má L_e regulární cyklus, a tedy nechť $3 \in \Lambda(L_e)$. Mohou nastat dva případy.

- Permutace e nemá řád 3, pak má nutně řád 4, protože kdyby měla řád $o \lneq 3$, tak $L_e^o = L_{e^o} = L_{\mathrm{id}_{\{1,2,3,4\}}} = \mathrm{id}_Q$, což by byl spor s tím, že $3 \in \Lambda(L_e)$. Jediné prvky řádu 4 v $\mathbf{S}_4$ jsou 4-cykly. Struktura quandlu nezávisí na pojmenování prvků, a tedy bez újmy na obecnosti nechť $e = (1\ 2\ 3\ 4)$. Provedeme substituci $1 \mapsto 3 \mapsto 2 \mapsto 1$ a získáme, že i $(3\ 1\ 2\ 4) \in e^{A_4} \subseteq Q$. Následně pak

$$(3\ 1\ 2\ 4) \overset{L_e}{\mapsto} (4\ 2\ 3\ 1) \overset{L_e}{\mapsto} (1\ 3\ 4\ 2) \overset{L_e}{\mapsto} (2\ 4\ 1\ 3) \overset{L_e}{\mapsto} (3\ 1\ 2\ 4)$$

  nám definuje 4-cyklus v L_e. Vidíme, že $4 \in \Lambda(e)$, pak ale $\Lambda(e) \supseteq \{1,3,4\}$, a tedy $|Q| \geq 1+3+4 = 8$. To je spor s tím, že $|Q| \leq |e^{S_4}| = \frac{4!}{4} = 6$, kde jsme v předposlední rovnosti užili, že permutace jsou vzájemně konjugované grupou $\mathbf{S}_n$ právě, když mají stejnou strukturu cyklů.

- Permutace e má řád 3, pak jde nutně o 3-cyklus. Bez újmy na obecnosti nechť $e = (1\ 2\ 3)(4)$. Podobně jako výše víme, že $|Q| \leq |e^{S_4}| = \frac{4\cdot3\cdot2}{3} = 8$.

  Buďto $e' := (2\ 1\ 3) \notin Q$, pak je ze symetrií konjugační třída e' stejně velká jako konjugační třída e, tj. $|Q|$. Víme, že $\Lambda(e) \supseteq \{1,3\}$, a tedy $|Q| \geq 1+3 = 4$. Celkově $4 \leq |Q| \leq \frac{|e^{S_4}|}{2} = \frac{8}{2} = 4$, tj. L_e je složení právě jednoho 3-cyklu a jednoho 1-cyklu, tedy má regulární cyklus.

  V opačném případě, kdy $e' := (2\ 1\ 3) \in Q$, provedením substituce $1 \mapsto 4 \mapsto 2 \mapsto 1$ na e a e' získáme, že i $(4\ 1\ 3)(2), (1\ 4\ 3)(2) \in e^{A_4} \subseteq Q$. Následně jsou pak

$$(4\ 1\ 3)(2) \overset{L_e}{\mapsto} (4\ 2\ 1)(3) \overset{L_e}{\mapsto} (4\ 3\ 2)(1) \overset{L_e}{\mapsto} (4\ 1\ 3)(2),$$
$$(1\ 4\ 3)(2) \overset{L_e}{\mapsto} (2\ 4\ 1)(3) \overset{L_e}{\mapsto} (3\ 4\ 2)(1) \overset{L_e}{\mapsto} (1\ 4\ 3)(2)$$

  dva různé 3-cykly L_e. Translace L_e je tedy už nutně složení právě dvou 3-cyklů a dvou 1-cyklů, a proto má regulární cyklus.

□

Poznamenejme, že díky výpočetním metodám popsaných v [2] sice víme, že všechny quandly velikosti nejvýše 47 splňují Hayashiho domněnku, k důkazu našeho tvrzení 3.15 pro případy $n \leq 4$ nám to ale nestačí, protože dokazujeme něco silnějšího, a sice nepředpokládáme souvislost těchto quandlů.

3.4 Cykly translací v konjugačních quandlech typu $\mathbf{e^{D_{2n}}}$

Na konci sekce 3.1 jsme si ukázali, že pro lichá $n \geq 3$ a reflexe $e \in D_{2n}$ jsou konjugační quandly $\mathbf{e^{D_{2n}}}$ souvislé a není těžké si rozmyslet, že pro různá lichá n budou tyto quandly také vzájemně neizomorfní[5]. Doplňme teď, že nehledě

[5]V případě potíží tento fakt plyne z důkazu tvrzení 3.18, kde se vypočítává velikost konjugačních tříd.

na paritu čísla n je naopak pro $e \in D_{2n}$ rotace konjugační quandl $\mathbf{e^{D_{2n}}}$ buďto jednoprvkový nebo dvouprvkový.

Příklad. Nechť $n \geq 3$ a $e \in \mathbf{D}_{2n}$ je rotace. Z vlastností dihedrálních grup jsou konjugace aplikované na rotaci poměrně nezajímavé, a sice platí, že $e^{D_{2n}} = \{e, e^{-1}\}$. Vzhledem k tomu, že levé translace v quandlu $\mathbf{e^{D_{2n}}}$ jsou bijekce na nejvýše 2 prvcích, které mají zaručeně alespoň 1 pevný bod, tak už musí být identity, a tedy $\mathrm{LMlt}\left(\mathbf{e^{D_{2n}}}\right) = \mathbf{1}$. Pokud e není středová symetrie, pak má quandl právě 2 prvky, působení právě 2 orbity a quandl tedy není souvislý. V opačném případě má quandl právě jeden prvek a speciálně je triviálně souvislý. ■

Vybízí se otázka, jak je to se souvislostí těchto quandlů pro sudá n a reflexe e. Uvedeme si příklad malého nesouvislého quandlu tohoto typu.

Příklad. Nechť $e \in e^{D_8}$ je reflexe. Pak buďto tato reflexe prochází dvěma protilehlými vrcholy a jde tedy o 2-cyklus, nebo neprochází žádným z vrcholů, pak jde o složení dvou 2-cyklů. Konjugace zachovávají strukturu cyklů, a tedy tyto reflexe leží v různých konjugačních třídách. Není těžké ověřit, že konjugací pomocí rotace o 90 stupňů se dá získat chybějící reflexe stejného typu a nezávisle na typu e má konjugační třída velikost 2. Stejně jako v příkladě výše jsou levé translace identity a $\mathrm{LMlt}\left(\mathbf{e^{D_8}}\right) = \mathbf{1}$. To má za následek, že její působení má 2 orbity a quandl tedy není souvislý. ■

Naším cílem bude ověřit Hayashiho domněnku pro třídu konjugačních quandlů typu $\mathbf{e^{D_{2n}}}$. V případě quandlů $\mathbf{e^{A_n}}$ jsme si rozmysleli, že jsou pro $n \geq 5$ souvislé, a tedy platnost Hayashiho domněnky byla přímo ekvivalentní tomu, že translace L_e má regulární cyklus. V tomto případě s jistotou nevíme, zda jsou všechny souvislé, ale i přesto k řešení přistoupíme tímto způsobem a uvidíme, že platí i tento obecnější výsledek.

Lemma 3.16. *Pro $n \geq 3$ platí, že*

$$\mathrm{Z}(\mathbf{D}_{2n}) = \begin{cases} \mathbf{1}, & \text{pro } n \text{ liché}, \\ \{\mathrm{id}_{\{1,2,\ldots,n\}}, s\}, & \text{pro } n \text{ sudé}, \end{cases}$$

kde s značí středovou symetrii.

Důkaz. Nechť e je reflexe a o je rotace řádu n, pak

$$e(oe) = o^{-1} \neq o = (oe)e,$$

a tedy $e \notin \mathrm{Z}(\mathbf{D}_{2n})$.

Je-li o rotace, pak pro libovolnou reflexi e platí

$$\begin{aligned} o(o^{-1}e) &= e \\ (o^{-1}e)o &= (eoe)eo = eo^2 \end{aligned}$$

Rovnost nám tedy nastává právě, když $o^2 = \mathrm{id}_{\{1,2,\ldots,n\}}$. Pro liché n jde právě o identitu a pro sudé n jde o identitu a středovou symetrii. O těchto prvcích jsme ukázali, že komutují se všemi reflexemi a díky tomu, že to jsou rotace, tak komutují i se všemi rotacemi. Tím jsme nalezli všechny prvky centra. □

Tvrzení 3.17. *Nechť $n \geq 3$ je liché a $e \in D_{2n}$ je reflexe, pak má translace L_e v konjugačním quandlu $\mathbf{e^{D_{2n}}}$ regulární cyklus.*

Důkaz. Jak jsme již na konci sekce 3.1 ukázali, tak v takovém případě je $\left\langle e^{D_{2n}} \right\rangle_{\mathbf{D}_{2n}} = \mathbf{D}_{2n}$ a dle lemmatu 3.16 má tedy triviální centrum. Tvrzení 3.8 nám pak říká, že L_e má regulární cyklus právě, když existuje $z \in e^{D_{2n}}$ takové, že pro každé $1 \leq k \lneq \mathrm{ord}_{\mathbf{D}_{2n}}(e) = 2$ platí $e^k z \neq z e^k$.

Nechť $o \in D_{2n}$ je rotace řádu n, pak $z := o^2 e = oe(eoe) = oeo^{-1} \in e^{D_{2n}}$ a

$$e^1 z = e(o^2 e) = o^{-2} \neq o^2 = (o^2 e)e = z e^1,$$

protože kdyby bylo $o^{-2} = o^2$, tak pak $o^4 = \mathrm{id}_{\{1,2,\ldots,n\}}$, z čehož plyne, že $n = \mathrm{ord}_{\mathbf{D}_{2n}}(o) \mid 4$, a to je spor s tím, že n je liché a $n \geq 3$. □

Teď již překročíme k tomu zajímavému důkazu této sekce a to k důkazu pro téměř všechna zbylá n (až na $n = 4$).

Tvrzení 3.18. *Nechť $n \geq 3$ a $e \in \mathbf{D}_{4n}$ je reflexe, pak má translace L_e v konjugačním quandlu $\mathbf{e^{D_{4n}}}$ regulární cyklus.*

Důkaz. Nechť $\underline{e} \in \mathbf{D}_{2n}$ je libovolná reflexe, $\underline{o} \in \mathbf{D}_{2n}$ je nějaká rotace řádu n a $o \in \mathbf{D}_{4n}$ je nějaká rotace řádu $2n$. Všimněme si, že každý prvek grupy $\mathbf{D}_{2n}$ lze jednoznačně vyjádřit ve tvaru $\underline{o}^i \underline{e}^j$ pro nějaká $i \in \{0, 1, 2, \ldots, n-1\}, j \in \{0, 1\}$. To dokazovat nebudeme, ale existence zápisu plyne přímo z opakované aplikace pravidla $\underline{e}\underline{o}\underline{e} = \underline{o}^{-1}$ spolu s tím, že $\underline{e} = \underline{e}^{-1}$ a jednoznačnost poté získáme vykrácením společných prvků spolu s následným rozlišením mocnin $\underline{o}$ a odlišením rotací od reflexí. Stejně tak lze libovolný prvek grupy $\mathbf{D}_{4n}$ jednoznačně vyjádřit ve tvaru $o^i e^j$ pro nějaká $i \in \{0, 1, 2, \ldots, 2n-1\}, j \in \{0, 1\}$.

Definujme zobrazení $\phi : D_{4n} \to D_{2n}$ tak, že pro každé $i = 0, 1, \ldots, 2n-1$ a každé $j = 0, 1$ je $\phi(o^i e^j) := \underline{o}^i \underline{e}^j$. Takovéto zobrazení má následující vlastnosti.

- Je to homomorfismus: Pro libovolná $a = o^{i_a} e^{j_a}, b = o^{i_b} e^{j_b} \in D_{4n}$ platí $\phi(ab) = \phi(o^{i_a} e^{j_a} o^{i_b} e^{j_b}) = \phi(o^{i_a}(e^{j_a} o^{i_b} e^{j_a}) e^{j_a} e^{j_b}) = \phi(o^{i_a - i_b} e^{j_a + j_b}) = \underline{o}^{i_a - i_b} \underline{e}^{j_a + j_b} = \cdots = \underline{o}^{i_a} \underline{e}^{j_a} \underline{o}^{i_b} \underline{e}^{j_b} = \phi(a)\phi(b)$.
- Je na: Plyne přímo z definice ϕ a poznámky v prvním odstavci důkazu.
- Jádro ϕ je $\{\mathrm{id}_{\{1,2,\ldots,2n\}}, o^n\}$: Prvek $a = o^i e^j \in \mathbf{D}_{4n}$ je v jádru právě, když $\phi(a) = \underline{o}^i \underline{e}^j = \mathrm{id}_{\{1,2,\ldots,n\}}$. Nutně $j = 0$, protože identita je rotace a dále pak tedy nutně $\underline{o}^i = \mathrm{id}_{\{1,2,\ldots,n\}}$, to nastane právě, když $i \in \{0, n\}$. Vynucenými možnostmi jsou tedy $a = \mathrm{id}_{\{1,2,\ldots,2n\}}$ a $a = o^n$. Obě tyto možnosti se na $\mathrm{id}_{\{1,2,\ldots,n\}}$ skutečně zobrazí, takže $\mathrm{Ker}(\phi) = \{\mathrm{id}_{\{1,2,\ldots,2n\}}, o^n\}$.

Ukažme, že

$$|\underline{e}^{\mathbf{D}_{2n}}| = \begin{cases} n, & \text{pokud je } n \text{ liché,} \\ \frac{n}{2}, & \text{pokud je } n \text{ sudé.} \end{cases}$$

Každý prvek $\underline{e}^{\underline{o}^i \underline{e}^j} \in e^{\mathbf{D}_{2n}}$ svedeme upravit

$$\underline{e}^{\underline{o}^i \underline{e}^j} = \underline{o}^i \underline{e}^j \underline{e} \underline{e}^{-j} \underline{o}^{-i} = \underline{o}^i \underline{e} \underline{o}^{-i} = \underline{o}^i (\underline{e}\underline{o}^{-i}\underline{e})\underline{e} = \underline{o}^{2i}\underline{e},$$

a tedy

$$\underline{e}^{\mathbf{D}_{2n}} = \left\{ \underline{e}^{\underline{o}^i \underline{e}^j} \mid i \in \{0, 1, \ldots, n-1\}, j \in \{0, 1\} \right\} = \left\{ \underline{o}^{2i}\underline{e} \mid i \in \{0, 1, \ldots, n-1\} \right\}.$$

Z jednoznačnosti zápisu a toho, že $\mathrm{ord}_{\mathbf{D}_{2n}}(\underline{o}) = n$, už můžeme usoudit, že v případě, kdy bude n liché, nám každá volba i dá jiný prvek, a bude jich tedy celkem n. V případě, kdy bude n sudé, nám páry hodnot i splynou v jeden prvek $\underline{o}^{2i}\underline{e}$, jinak ale budou po dvou různé, a bude jich celkem $\frac{n}{2}$. Tvrzení funguje pro obecné n a speciálně nám říká, že $|e^{D_{4n}}| = n$.

Označme $\mathbf{H} := \left\langle e^{D_{4n}} \right\rangle_{\mathbf{D}_{4n}}$. Ptejme se na obraz této grupy při homomorfismu ϕ. Získáme

$$\phi(\mathbf{H}) = \phi\left(\left\langle e^{D_{4n}} \right\rangle_{\mathbf{D}_{4n}}\right) = \left\langle \phi(e^{D_{4n}}) \right\rangle_{\mathbf{D}_{2n}} = \left\langle \underline{e}^{D_{2n}} \right\rangle_{\mathbf{D}_{2n}},$$

kde poslední rovnosti jsme docílili tím, že jsme si prvky množiny $e^{D_{4n}}$ představili ve tvaru $o^{2i}e^j$, zobrazili je pomocí ϕ a následně převedli zpět na celé $\underline{e}^{D_{2n}}$.

Ukážeme, že řád grupy $\mathbf{H}$ je roven $2n$. Množina $e^{D_{4n}}$, která generuje $\mathbf{H}$, obsahuje pouze reflexe a jejím uzavřením na násobení tedy dojde k přidání alespoň jedné rotace (vezměme druhou mocninu libovolného prvku). Víme, že $n \leq \mathrm{ord}\,\mathbf{H} \mid 4n$ a teď jsme si ukázali, že $|\mathbf{H}| \neq n$. Zbývá rozhodnout, zda $|\mathbf{H}| = 4n$ nebo $|\mathbf{H}| = 2n$, tj. zda $\mathbf{H} = \mathbf{D}_{4n}$ či nikoli. Kdyby pro spor bylo $\mathbf{H} = \mathbf{D}_{4n}$, tak pak by $o \in \mathbf{H}$. To se stát nemůže, protože každý prvek $\mathbf{H}$ lze získat jako konečný součin prvků z $e^{D_{4n}}$ a jejich inverzů. Prvky této množiny jsou reflexe a jsou tedy svými vlastními inverzy. Zkoumejme, jak vypadá součin dvou obecných prvků z $e^{D_{4n}}$. Máme, že

$$(o^{2i}e)(o^{2j}e) = o^{2i}o^{-2j} = o^{2(i-j)}.$$

Indukcí podle počtu prvků v tomto součinu bychom ověřili, že každý prvek $\mathbf{H}$ je buďto tvaru o^{2i}, nebo tvaru $o^{2i}e$, a tedy $o \notin \mathbf{H}$. Tím jsme ukázali, že $|\mathbf{H}| = 2n$.

Řád grupy $\left\langle \underline{e}^{\mathbf{D}_{2n}} \right\rangle_{\mathbf{D}_{2n}}$ získáme pro sudá n naprosto stejně a pro lichá n už při použití argumentu o rozšíření o rotaci. Dostaneme

$$\mathrm{ord}\left\langle \underline{e}^{\mathbf{D}_{2n}} \right\rangle_{\mathbf{D}_{2n}} = \begin{cases} 2n, & \text{pokud je } n \text{ liché,} \\ n, & \text{pokud je } n \text{ sudé.} \end{cases}$$

Případ n je liché: V případě, že n je liché je pak $\phi\restriction_H$ homomorfismus mezi grupami stejné konečné velikosti, který je na. Nutně je už pak i bijekcí, a tedy jde o grupový izomorfismus. Grupa $\mathbf{H}$ je tedy izomorfní grupě $\mathbf{D}_{2n}$ pro liché n a ta má dle lemmatu 3.16 triviální centrum. Aplikací tvrzení 3.8 získáme, že translace L_e má v quandlu $\mathbf{e^{D_{4n}}}$ regulární cyklus právě, když existuje $z \in e^{D_{4n}}$ takové, že pro každé $1 \leq k \lneq \mathrm{ord}_{\mathbf{D}_{4n}}(e) = 2$ platí $e^k z \neq ze^k$. Volbou $z := o^2e = o(eo^{-1}e)e = oeo^{-1} \in e^{D_{4n}}$ dostaneme $e^1 z = e(o^2e) = o^{-2} \neq o^2 = (o^2e)e = ze^1$, protože jinak by $o^4 = \mathrm{id}_{\{1,2,\ldots,n\}}$, takže $2n = \mathrm{ord}_{\mathbf{D}_{4n}}(o) \mid 4$, což by byl spor. Závěrem získáváme, že L_e má regulární cyklus.

Případ n je sudé: V případě, že n je sudé je $\phi\restriction_H$ homomorfismus z grupy o velikosti $2n$ do grupy velikosti n, a tedy má netriviální jádro. My ale víme, že $\mathbf{1} \neq \mathrm{Ker}(\phi\restriction_H) \subseteq \mathrm{Ker}(\phi) = \{\mathrm{id}_{\{1,2,\ldots,2n\}}, o^n\}$, a proto $\mathrm{Ker}(\phi\restriction_H) = \{\mathrm{id}_{\{1,2,\ldots,2n\}}, o^n\}$.

Již jsme si ukázali, že každý prvek grupy $\mathbf{H}$ je vyjádřitelný ve formě o^{2i} nebo $o^{2i}e$. Takových prvku je však v grupě $\mathbf{D}_{4n}$ pouze $2n$, což je řád grupy $\mathbf{H}$, a proto už $\mathbf{H} = \{o^{2i}, o^{2i}e \mid i \in \{0, 1, \ldots, n-1\}\}$. Ukážeme, že $\{\mathrm{id}_{\{1,2,\ldots,2n\}}, o^n\} = \mathrm{Z}(\mathbf{H})$.

Prvky tvaru $o^{2i}e$ v centru neleží, protože volbou $o^2 \in \mathbf{H}$ získáme, že $o^2(o^{2i}e) = o^{2i+2}e \neq o^{2i-2}e = o^{2i}(eo^2e)e = (o^{2i}e)o^2$, kde nerovnost uprostřed plyne z toho, že jinak by $o^4 = \mathrm{id}_{\{1,2,\dots,2n\}}$, což by vedlo k tomu, že $2n = \mathrm{ord}_{\mathbf{D}_{4n}}(o) \mid 4$, tj. spor.

Rotace o^{2i} komutují se všemi ostatními rotacemi a stačí tedy ověřovat reflexe. Je-li $o^{2i'}e$ libovolná reflexe z $\mathbf{H}$, pak

$$\begin{aligned} o^{2i}(o^{2i'}e) &= o^{(2i+2i')}e, \\ (o^{2i'}e)o^{2i} &= o^{2i'}(eo^{2i}e)e = o^{2i'}o^{-2i}e = o^{(2i'-2i)}e. \end{aligned}$$

Rovnost nastává právě, když $o^{2i} = o^{-2i}$, tj. právě, když $2n = \mathrm{ord}_{\mathbf{D}_{4n}}(o) \mid 4i$. To nastane právě pro $i = 0, \frac{n}{2}$, a tedy jádro tvoří právě prvky $o^0 = \mathrm{id}_{\{1,2,\dots,2n\}}$ a $o^{2\frac{n}{2}} = o^n$, jak jsme chtěli ukázat.

Máme surjektivní grupový homomorfismus $\phi\restriction_H : \mathbf{H} \to \left\langle \underline{e}^{D_{2n}} \right\rangle_{\mathbf{D}_{2n}}$, jehož jádro je $\{\mathrm{id}_{\{1,2,\dots,2n\}}, o^n\} = \mathrm{Z}(\mathbf{H})$. Podle první věty o izomorfismu je zobrazení $\Phi : \mathbf{H}/\mathrm{Z}(\mathbf{H}) \to \left\langle \underline{e}^{D_{2n}} \right\rangle_{\mathbf{D}_{2n}}$ určené vztahem $(o^{2i}e^j)\,\mathrm{Z}(\mathbf{H}) \mapsto \underline{o}^{2i}\underline{e}^j$ dobře definovaný izomorfismus grup. Vezměme zobrazení $\Psi := \psi \circ \Phi^{-1} : \left\langle \underline{e}^{D_{2n}} \right\rangle_{\mathbf{D}_{2n}} \to \mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)$, kde ψ je izomorfismus ze znění lemmatu 3.6. Toto zobrazení je grupový izomorfismus určený vztahem $\underline{o}^{2i}\underline{e}^j = L_o^{2i} \circ L_e^j$.

Dle lemmatu 3.7 má translace L_e regulární cyklus právě, když existuje $z \in e^{D_{4n}}$ takové, že

$$\left(\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)\right)_z \cap \langle L_e \rangle_{\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)} = \mathbf{1}.$$

To nastane právě, když

$$\Psi^{-1}\left(\left(\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)\right)_z \cap \langle L_e \rangle_{\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)}\right) = \Psi^{-1}(\mathbf{1}) = \mathbf{1}.$$

Množinové vzory se chovají homomorfně k průnikům, a tedy to nastává právě, když

$$\Psi^{-1}\left(\left(\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)\right)_z\right) \cap \Psi^{-1}\left(\langle L_e \rangle_{\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)}\right) = \mathbf{1}. \tag{3.8}$$

Svedeme vyjádřit

$$\Psi^{-1}\left(\langle L_e \rangle_{\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)}\right) = \left\langle \Psi^{-1}(L_e) \right\rangle_{\mathbf{D}_{2n}} = \langle \underline{e} \rangle_{\mathbf{D}_{2n}} = \{\mathrm{id}_{\{1,2,\dots,n\}}, \underline{e}\}.$$

Trivialita průniku v (3.8) nastane právě, když $\underline{e} \notin \Psi^{-1}\left(\left(\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)\right)_z\right)$, tj. právě, když $\Psi(\underline{e}) \notin \left(\mathrm{LMlt}\left(\mathbf{e}^{\mathbf{D_{4n}}}\right)\right)_z$. Máme, že $\Psi(\underline{e}) = L_e$ a podmínka říká, že $L_e(z) \neq z$.

Získali jsme, že translace L_e má regulární cyklus právě, když existuje $z \in e^{D_{4n}}$ takové, že $L_e(z) \neq z$, tj. $ez \neq ze$. Volbou $z := o^2e = o(eo^{-1}e)e = oeo^{-1} \in e^{D_{4n}}$ získáme $ez = eo^2e = o^{-2} \neq o^2 = (o^2e)e = ze$, protože kdyby tomu tak nebylo, tak by, jak už jsme několikrát viděli, platilo $2n \mid 4$, což by byl spor. Tím jsme ukázali, že je podmínka splněna a díky tomu víme, že L_e skutečně má regulární cyklus. □

Spojme naše poznatky o dihedrálních grupách v následujícím tvrzení.

Tvrzení 3.19. *Nechť $n \geq 3$, pak má translace L_e v konjugačním quandlu $\mathbf{e}^{\mathbf{D_{2n}}}$ regulární cyklus.*

Důkaz. Na začátku této sekce jsme si ukázali, že je-li e rotace, pak je $L_e = \mathrm{id}_{\{1,2,\dots,n\}}$, speciálně má tedy regulární cyklus. Zbývá nám ověřit případy, kdy e je reflexe.

Tvrzení 3.17 nám říká, že je-li n liché, pak má L_e regulární cyklus a tvrzení 3.18 nám dává, že je-li n sudé a různé od 4, pak má L_e regulární cyklus. Případ $n = 4$ jsme rozebrali v příkladě na začátku této sekce a došli jsme k tomu, že nehledě na volbě reflexe e bude $L_e = \mathrm{id}_{\{1,2,\dots,n\}}$ a speciálně tedy bude mít regulární cyklus. □

Kapitola 4

Závěr

V práci jsme pomocí věty 3.3 v sekci 3.1 ukázali, že je neformálně řečeno alespoň polovina quandlů tvaru $\mathbf{e^{S_n}}$ souvislých, že je alespoň čtvrtina[1] quandlů tvaru $\mathbf{e^{D_{2n}}}$ souvislých a že je každý konjugační quandl odvozený z jednoduché grupy souvislý, speciálně pak že jsou téměř všechny konjugační quandly tvaru $\mathbf{e^{A_n}}$ souvislé. V sekci 3.2 jsme rozebrali hlavní myšlenky důkazu tvrzení 3.2 Davida Stanovského a Petra Vojtěchovského v zatím nepublikované práci [4]. Ty jsme mírně zobecnili a spolu s naší větou 3.5 se nám podařilo objevit a dokázat větu 3.9, která dává zajímavé ekvivalentní vyjádření zúžené Hayashiho domněnky v teorii grup. Dále jsme na důkaz z [4] v sekci 3.3 navázali, abychom dokázali tvrzení 3.15. V sekci 3.4 jsme se následně věnovali konjugačním quandlům odvozených z dihedrálních grup, kde se nám podařilo dosáhnout výsledku popsaného v tvrzení 3.19.

Možnosti, jak v práci pokračovat, jsou poměrně široké. Ve větě 3.3 se nám podařilo popsat rozumné množství souvislých konjugačních quandlů. Zajímavým výsledkem by však bylo nalezení chybějící nutné podmínky, a tedy přímo charakterizace souvislosti těchto quandlů. Myšlenka z důkazu v práci [4] popsaná ve znění lemmatu 3.6 dává prostor pro převádění pojmů ze světa quandlů do světa grup. Jeho zajímavou aplikaci jsme mohli vidět v důkazu tvrzení 3.18, kde se nám podařilo domněnku vyřešit pro konjugační quandly odvozené z grup $\mathbf{D}_{4n}$, což jsou grupy s netriviálním centrem. Věta 3.9 nám říká, že nalezením konečné neabelovské jednoduché grupy s vlastností, která je formulací poměrně typickou pro teorii grup, bychom svedli domněnku vyvrátit. V textu jsme ukázali, že jednoduché grupy $\mathbf{A}_n$ tento protipříklad neobsahují. Dalším horkým kandidátem pro výzkum jsou tedy například jednoduché projektivní speciální lineární grupy. V případě, že se bude zdát, že Hayashiho domněnka pro konjugační quandly odvozené z konečných jednoduchých grup skutečně platí, tak pak je ve vzduchu otázka, zda by tento výsledek nešel pomocí lemmatu 3.6 přenést i na třídy nějakých obecnějších grup. Jednoho podobného přenosu se nám podařilo v důkazu zmíněného tvrzení 3.18.

[1] Resp. polovina, viz závěr sekce 3.1.

Seznam použité literatury

[1] Andrew Fish, Alexei Lisitsa a David Stanovský. "A Combinatorial Approach to Knot Recognition". In: *Embracing Global Computing in Emerging Economies*. Ed. Ross Horne. Cham: Springer International Publishing, 2015, s. 64–78. ISBN: 978-3-319-25043-4.

[2] Alexander Hulpke, David Stanovský a Petr Vojtěchovský. "Connected quandles and transitive groups". In: *Journal of Pure and Applied Algebra* 220.2 (2016), s. 735–758. ISSN: 0022-4049. DOI: https://doi.org/10.1016/j.jpaa.2015.07.014. URL: https://www.sciencedirect.com/science/article/pii/S0022404915002017.

[3] Mohamed Elhamdadi. *Quandles. an introduction to the algebra of knots*. American Mathematical Society, 2015, s. 245. ISBN: 978-1-4704-2213-4.

[4] David Stanovský a Petr Vojtěchovský. "Notes on the Hayashi conjecture". nepublikováno. verze 2. 3. říj. 2022.

[5] David Stanovský. *Základy algebry*. 2. vyd. MatfyzPress, 2010. ISBN: 978-80-7378-105-7.

[6] Joseph J. Rotman. *An Indroduction to the Theory of Groups*. 4. vyd. Springer-Verlag New York, Inc., 1999. ISBN: 0-387-94285-8.

[7] Chuichiro Hayashi. "Canonical Forms for Operation Tables of Finite Connected Quandles". In: *Communications in Algebra* 41.9 (2013), s. 3340–3349.

[8] Naqeeb Ur Rehman, David Stanovský a Petr Vojtěchovský. "Notes on the Hayashi conjecture". nepublikováno. verze 5. 3. dub. 2023.

[9] Naqeeb Ur Rehman. "Quandles and Hurwitz Orbits". Dis. pr. University of Glasgow, 2016.

[10] Taisuke Watanabe. "On the structure of the profile of finite connected quandles". In: *Math. J. Okayama Univ.* 61 (2019), s. 85–98.

[11] S. Kayacan. *On a conjecture about profiles of finite racks*. arXiv. eprint: 0902.0885. URL: https://arxiv.org/abs/2006.10327.

[12] Takeshi Kajiwara a Nakayama Chikara. "A large orbit in a finite affine quandle". In: *Yokohama Mathematical Journal* 62 (2016), s. 25–29.

[13] M. V. Horoševskii. "On automorphisms of finite groups". In: *Math. USSR Sbornik* 22.4 (1974), s. 584–594.