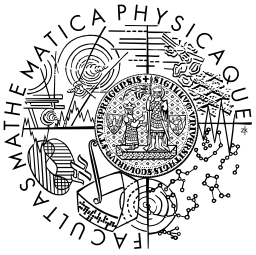

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Ondřej Pudich

Problém izomorfismu pro quandly odvozené z grup

Katedra algebry (301. • 32-KA)

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

Studijní program: Obecná 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

Děkuji svému vedoucímu práce doc. RNDr. Davidu Stanovskému, Ph.D. za obdivuhodnou trpělivost, racionální a individuální přístup a výborný vhled do světa matematika.

Název práce: Problém izomorfismu pro quandly odvozené z grup

Autor: Ondřej Pudich

Katedra: Katedra algebry (301. • 32-KA)

Vedoucí bakalářské práce: doc. RNDr. David Stanovský, Ph.D., Katedra algebry (301. • 32-KA)

Abstrakt: V této práci se budeme zaměřovat na matematickou strukturu nazvanou quandle. Bude nás zajímat, kdy jsou dva principální quandly izomorfní. Nejprve dokážeme abstraktní charakterizaci toho, kdy jsou dva principální quandly izomorfní. Pomocí dokázaných vět si poté ukážeme částečné řešení problému izomorfismu principálních quandlů na dihedrálních grupách.

Klíčová slova: quandly problém izomorfismu

Title: Isomophism problem for quandles derived from groups

Author: Ondřej Pudich

Department: Department of Algebra (301. • 32-KA)

Supervisor: doc. RNDr. David Stanovský, Ph.D., Department of Algebra (301. • 32-KA)

Abstract: In this bachelor thesis, we focus on the mathematical structure called quandle. The point of interest shall be to provide the solution to the isomorphism problem, i.e., to determine exactly when two quandles are isomorphic. We address this problem in the case of principal quandles. Firstly, we prove the abstract characterization of when two principal quandles are isomorphic, and secondly, we imply the results on dihedral groups and obtain a partial classification.

Keywords: quandles isomorphism problem

Obsah

10. května 2023

1. Úvod

1.1 Motivace

Nechť $Q = (Q,*)$ je množina s binární operací $*$, pak Q nazveme quandle (Definice 1), pokud je Q vzhledem k operaci $*$ idempotentní, má jednoznačné řešení $x \in Q$ rovnice $a * x = b$ pro každé $a, b \in Q$ a je zleva distributivní.

Existuje mnoho motivací pro definici quandlu. Nejproslulejší je nejspíše ta z teorie uzlů. Můžeme totiž obarvit oblouky uzlu používajíce prvky quandlu jako barvy pod určitými podmínkami. Počet obarvení je pak invariant a tři axiomy quandlu poté korespondují v určitém smyslu s Redeimeisterovými pohyby [1].

V této práci se budeme soustředit na základní příklady quandlů odvozených z grup, jejichž operace $*$ je definována pomocí vybraného grupového automorfismu f pro $x, y \in Q$ následovně $x * y = xf(x)^{-1}f(y)$. Tyto quandly budeme nazývat principální. Pro tyto quandly nás bude zajímat situace, kdy nastává, že jsou dva různé principální quandly nad stejnou grupou izomorfní vzhledem k operaci $*$. Tento problém je prozkoumaný pro případ principálních quandlů nad abelovskou grupou ([2], [3]), částečně nad symetrickou grupou [4] a pro speciální případ quandlů, které jsou principální a souvislé zároveň. Pro tyto principální a souvislé quandly máme ekvivalentní podmínku, která nám říká, že jsou izomorfní právě tehdy, když jsou automorfismy definující jejich quandlovou operaci konjugované (viz Věta 12). My se v práci zaměříme na případ, kdy quandly souvislé nejsou a odvodíme obecnou větu (Věta 13), která abstraktně charakterizuje, kdy jsou dva obecné principální quandly izomorfní i v případě, že jsou nesouvislé. Větu poté ilustrujeme na principálních quandlech nad dihedrálními grupami.

1.2 Souhrn práce

V první kapitole se soustředíme na základní vlastnosti quandlů. Zavedeme si důležité pojmy a ukážeme si charakterizaci souvislosti principálních quandlů (Tvrzení 8), která nám pomůže vyřešit problém izomorfismu pro souvislé principální quandly.

Ve druhé kapitole nalezneme řešení problému izomorfismu pro souvislé principální quandly (Věta 12) a hlavní výsledek této práce (Věta 13), který řeší problém izomorfismu pro obecné principální quandly.

Třetí kapitolu začneme jednoduchým cvičením z teorie grup, což budou sekce o vlastnostech dihedrálních grup a vlastnostech grup automorfismů dihedrálních grup. To nám pomůže nalézt charakterizaci tříd konjugace grupy automorfismů dihedrálních grup. Tento fakt potřebujeme k tomu, abychom mohli vyloučit případ, kdy jsou quandly izomorfní z již známé teorie (viz Lemma 9). Nakonec odvodíme částečné řešení problému izomorfismu pro principální quandly na dihedrálních grupách. Jako důsledek předešlé teorie dostaneme úplnou klasifikaci pro případ dihedrálních grup D_{2p}, kde p je prvočíslo (Důsledek 32) a pro dihedrální grupu D_8 (Tvrzení 33). Dojdeme k tomu, že v D_{2p} klasifikace odpovídá konjugaci v $\mathrm{Aut}(D_{2p})$ a ve D_8 najdeme izomorfní quandly s navzájem nekonjugovanými automorfismy.

Práce vychází ze základů teorie quandlů tak, jak je popsána například v [5]. Poznamenejme, že všechny důkazy celé práce byly zpracovány samostatně. Některá tvrzení jsou známá (Kapitola 1 od Sekce 1.4, Tvrzení 8, Věta 12, Sekce 3.2, Sekce 3.3), ale stěžejní tvrzení byla nalezena samostatně s důležitými poznatky a radami vedoucího práce (Lemma 10, Věta 13, Důsledek 15, Sekce 3.4, Sekce 3.5).

1.3 Značení

Pro G grupu značíme $\mathrm{Aut}(G)$ množinu všech grupových automorfismů grupy G.

Homomorfismus mezi grupami G,H budeme vždy, pokud nenapíšeme explicitně jinak, značit pomocí malých latinských písmen, například

$$h : G \to H.$$

Fakt, že grupa G je podgrupou H, budeme značit následovně $G \leq H$.

Fakt, že grupa G je izomorfní grupě H, budeme značit následovně $G \simeq H$.

Jednotkový prvek obecné grupy G budeme značit e.

Mějme množinu M prvků G, pak grupu, generovanou prvky M, budeme značit $\langle M \rangle$.

1.4 Zavedení quandlů a quandlových homomorfismů

Definice 1 (quandle)**.** *Dvojici $(Q, *)$ nazveme quandle, pokud Q je množina a $*$ je binární operace splňující následující*

1. $a * a = a$ *pro všechna* $a \in Q$,
2. $a * (b * c) = (a * b) * (a * c)$ *pro všechna* $a, b, c \in Q$,
3. *Pro všechna* $a, b \in Q$ *existuje právě jedno* $x \in Q$ *takové, že* $a * x = b$.

Příklad. Jednoduchý známý příklad quandlu je konjugační quandle. Jedná o situaci, kdy máme grupu G a konjugační quandle je pak $Q = (G, *)$, kde operace $*$ je pro $x, y \in G$ definována následovně $x * y = xyx^{-1}$. Axiomy lze snadno ověřit.

Definice 2 (Quandlový homomorfismus)**.** *Mějme quandly $(Q_1, *_1), (Q_2, *_2)$, řekneme, že zobrazení*

$$\alpha : Q_1 \to Q_2$$

je quandlový homomorfismus, jestliže pro všechna x,$y \in Q_1$ platí

$$\alpha(x *_1 y) = \alpha(x) *_2 \alpha(y).$$

Pokud je α bijekce, tak ho budeme nazývat quandlový izomorfismus. Grupu generovanou všemi quandlovými izomorfismy budeme značit

$$\mathrm{Aut}(Q).$$

Quandlové homomorfismy budeme nadále značit řeckými písmeny a fakt, že jsou quandly $(Q_1, *_1), (Q_2, *_2)$ izomorfní, budeme značit

$$Q_1 \simeq Q_2.$$

Definice 3 (Levá translace)**.** *Mějme quandle $(Q, *)$, pak levou translací prvkem $a \in (Q, *)$ myslíme zobrazení*

$$L_a : Q \to Q, \quad x \mapsto a * x.$$

Dále si označíme

$$\langle L_a : a \in Q \rangle := \mathrm{LMlt}(Q).$$

Lemma 1. *Mějme quandle $(Q, *)$, pak platí*

$$\mathrm{LMlt}(Q) \leq \mathrm{Aut}(Q).$$

Důkaz. Z třetího bodu definice quandlu platí, že L_a jsou prosté a surjektivní zobrazení do sebe sama. Navíc je zobrazení quandlový homomorfismus, protože díky druhého bodu definice quandlu platí

$$L_a(y * z) = L_a(y) * L_a(z).$$

□

Definice 4 (Pravá translace)**.** *Mějme quandle $(Q, *)$, pak pravou translací prvkem $a \in (Q, *)$ myslíme zobrazení*

$$P_a : Q \to Q, \quad x \mapsto x * a.$$

Tvrzení 2 (Invariantní vlastnosti quandlů)**.** *Mějme quandlový izomorfismus $\alpha : Q_1 \to Q_2$ mezi quandly Q_1, Q_2, pak pro α platí*

(1) $|\{L_a; a \in Q_1\}| = |\{L_a; a \in Q_2\}|$,

(2) $ord(L_a) = ord(L_{\alpha(a)})$.

Důkaz.

(1) Pro spor předpokládejme, že Q_2 má méně levých translací než Q_1. Pro levou translaci L_a na Q_1 a pro libovolné $x \in G$ platí, že $\alpha(L_a(x)) = \alpha(a * x) = \alpha(a) * \alpha(x)$, a tedy levá translace L_a se zobrazí po prvcích na levou translaci $L_{\alpha(a)}$ na quandlu Q_2. Kdyby tedy bylo v Q_2 méně levých translací, pak by se dvě různé levé translace L_a, L_b na Q_1 musely zobrazit na jednu stejnou levou translaci $L_{\alpha(a)} = L_{\alpha(b)}$ na Q_2, a tedy by platilo $L_{\alpha(a)} = L_{\alpha(b)}$ pro $L_a \neq L_b$, což je spor, protože by existovalo $x \in G$ takové, že

$$L_a(x) = (a * x) \neq (b * x) = L_b(x)$$

a zároveň

$$\alpha(a * x) = \alpha(b * x),$$

takže by se nejednalo o quandlový izomorfismus, jelikož by zobrazení nebylo prosté.

(2) Přímo plyne z homomorfní vlastnosti, jelikož máme, že pokud pro každé $x \in G$ platí $a * a * a * ... * x = x$, pak platí také

$$\alpha(a) * \alpha(a) * \alpha(a)...\alpha(x) = \alpha(a * a * a * ... * x) = \alpha(x).$$

□

1.5 Souvislé a principální quandly

Definice 5 (Souvislý quandle)**.** *Quandle $Q = (Q, *)$ nazveme souvislý, pokud* $\mathrm{LMlt}(Q)$ *působí na Q tranzitivně.*

Definice 6 (Principální quandle)**.** *Dvojici $Q = (G, f)$, kde G je grupa, $f \in \mathrm{Aut}(G)$ a f tvoří binární operaci definovanou pro $a, b \in G$ následovně*

$$a * b = af(a)^{-1}f(b),$$

nazveme principální quandle.

Lemma 3. *Principální quandle splňuje definici quandlu.*

Důkaz.

- Ověříme první bod definice. Máme $a * a = af(a)^{-1}f(a) = a$.

- Pro druhý bod máme

$$a * (b * c) = af(a)^{-1}f(b)f((f(b))^{-1})f(f(c))$$

a zároveň

$$\begin{aligned}(a * b) * (a * c) &= (af(a)^{-1}f(b)) * (af(a)^{-1}f(c)) \\ &= af(a)^{-1}f(b)f(af(a)^{-1}f(b))^{-1}f(af(a)^{-1}f(c)) \\ &= af(a)^{-1}f(b)f(f(b))^{-1}f(f(a))f(a)^{-1}f(a)f(f(a))^{-1}f(f(c)) \\ &= af(a)^{-1}f(b)f((f(b))^{-1})f(f(c)),\end{aligned}$$

tudíž jsme došli k rovnosti.

- Pro libovolně zvolené pevné $a, b \in Q$ zvolíme za x prvek $f^{-1}(f(a)a^{-1}b)$, pak skutečně platí
$$a * x = af(a)^{-1}f(f^{-1}(f(a)a^{-1}b)) = b,$$
a tedy takové x skutečně existuje. Dokážeme, že je jednoznačeně určeno. Kdyby pro $x \neq y$ platilo
$$a * x = a * y = b,$$
pak
$$af(a)^{-1}f(x) = af(a)^{-1}f(y),$$
ale pokud rovnost zleva vynásobíme $(af(a)^{-1})^{-1}$, tak dostaneme
$$f(x) = f(y),$$
a tudíž, jelikož je f grupový automorfismus, máme
$$x = y.$$

□

1.6 Charakterizace souvislosti principálních quandlů

Značení. Pro tuto podsekci si označíme pro principální quandle $Q = Q(G,f)$ $\mathrm{M} := \langle xf(x)^{-1}; x \in G\rangle$.

Lemma 4. *Mějme $Q = Q(G,f)$ principální quandle, pak pro libovolnou translaci L_a platí*
$$L_a^{-1}(x) = af^{-1}(a^{-1}x).$$

Důkaz. Z definice pro $x \in G$ libovolné máme $L_a(x) = af(a)^{-1}f(x)$, a platí
$$af^{-1}(a^{-1}L_a(x)) = af^{-1}(a^{-1}af(a)^{-1}f(x)) = x,$$
a tedy platí naše tvrzení.

□

Lemma 5. *Mějme $Q = Q(G,f)$ principální quandle, pak pro $m \in \mathrm{M}$ platí, že prvky $f(m), f^{-1}(m) \in \mathrm{M}$.*

Důkaz. Prvky $m \in \mathrm{M}$ jsou tvaru
$$m = \prod_{i=1}^{k}(a_i f(a_i)^{-1})^{i_j}, a_i \in Q, i_j \in \{+1, -1\}.$$
Nalezneme a_i, tak aby pro m libovolné, které je tvaru výše, platilo
$$f(m), f^{-1}(m) \in M.$$

- $f(m) = \prod_{i=1}^{k}(f(a_i)f(f(a_i)^{-1}))^{i_j} \in \mathrm{M}$, protože můžeme zvolit místo a_i prvek $f(a_i)$,
- $f^{-1}(m) = \prod_{i=1}^{k}(f^{-1}(a_i)(a_i)^{-1})^{i_j} \in \mathrm{M}$, protože můžeme zvolit místo a_i prvek $f^{-1}(a_i)$.

Poznamenejme, že používáme faktu, že f, f^{-1} jsou grupové automorfismy.

□

Lemma 6. *Mějme $Q = Q(G,f)$ principální quandle, pak pro libovolné $\alpha \in \mathrm{LMlt}(Q)$ platí $\alpha(\mathrm{M}) \subseteq \mathrm{M}$.*

Důkaz. Libovolné $\alpha \in \mathrm{LMlt}(Q)$ je složení L_a a L_a^{-1} pro různé $a \in Q$ a tyto zobrazení zobrazí $m \in \mathrm{M}$ na prvek z M, protože

- $L_a(m) = af(a)^{-1}f(m) \in \mathrm{M}$ podle Lemma 5,
- $L_a^{-1}(m) = af^{-1}(a^{-1}m) = af^{-1}(a^{-1})f^{-1}(m) \in \mathrm{M}$,

kde v první rovnosti využíváme Lemma 4, a poté v inkluzi využíváme Lemma 5, faktu, že M je grupa a toho, že $af^{-1}(a^{-1}) \in \mathrm{M}$, což platí, protože je to inverz prvku $xf(x)^{-1} \in \mathrm{M}$ pro $x = f^{-1}(a)$.

Celkově tedy máme, že i složení těchto zobrazení zobrazí m na prvek z M.

□

Lemma 7. *Mějme $Q = Q(G,f)$ principální quandle, pak pro libovolné $\alpha \in \mathrm{LMlt}(Q)$ platí $f \circ \alpha, \alpha \circ f^{-1} \in \mathrm{LMlt}(Q)$.*

Důkaz. Tvrzení stačí dokázat pro generátory, a tedy mějme $L_a \in \mathrm{LMlt}(Q)$, pak platí

$$f \circ L_a = L_e \circ L_a,$$

protože pro každé $x \in Q$ platí $L_e(x) = ef(e)^{-1}f(x) = f(x)$, tedy $f \circ \alpha \in \mathrm{LMlt}(Q)$. Druhá část tvrzení je inverz pro $f \circ \alpha^{-1}$, takže tam musí být, jelikož $\mathrm{LMlt}(Q)$ je podgrupa podle Lemma 1.

□

Tvrzení 8 (Ekvivalence pro souvislost principálních quandlů)**.** *Mějme principální quandle $Q = Q(G,f)$, pak je souvislý právě tehdy, když platí rovnost*

$$\langle xf(x)^{-1}; x \in G\rangle = G.$$

Důkaz.

($\Rightarrow$)
Nejprve mějme $g \in G$ libovolné, chceme dokázat, že platí
$g \in \mathrm{M} = \langle xf(x)^{-1}; x \in G\rangle$. Protože je Q souvislý můžeme zvolit $\alpha \in \mathrm{LMlt}(Q)$ takové, že $\alpha(e) = g$, ale $\alpha(e) \in \mathrm{LMlt}(Q)$ podle Lemma 6, a tedy platí rovnost z tvrzení.

($\Leftarrow$)

Mějme $g, m \in G$ libovolné, chceme dokázat, že existuje $\alpha \in \mathrm{LMlt}(Q)$, takové, že $\alpha(m) = g$. Stačí ovšem, pokud nalezneme $\alpha \in \mathrm{LMlt}(Q)$, takové, že $\alpha(e) = g$. Pokud se nám toto povede pro libovolné g, pak $\beta \in \mathrm{LMlt}(Q)$ takové, že $\beta(m) = g$ bychom našli složením inverzu $\gamma^{-1} \in \mathrm{LMlt}(Q)$ takového, že $\gamma(e) = m$ a α. Poznamenejme, že podle tvrzení je g tvaru

$$g = \prod_{i=1}^{k} (a_i f(a_i)^{-1})^{j_i}, a_i \in Q, j_i \in \{+1, -1\}.$$

Zvolíme α takové, že

$$\alpha(x) = (L^{j_1}_{f^{-j_1}(a_1)} \circ f^{-j_1} \circ L^{j_2}_{f^{-j_2}(a_2)} \circ f^{-j_2} ... \circ L^{j_{k-1}}_{f^{-j_{k-1}}(a_{k-1})} \circ f^{-j_{k-1}} \circ L^{j_k}_{f^{-j_k}(a_k)})(x),$$

pak máme

$$\alpha(e) = (L^{j_1}_{f^{-j_1}(a_1)} \circ f^{-j_1} \circ L^{j_2}_{f^{-j_2}(a_2)} \circ f^{-j_2} ... \circ L^{j_{k-1}}_{f^{-j_{k-1}}(a_{k-1})} \circ f^{-j_{k-1}} \circ L^{j_k}_{f^{-j_k}(a_k)})(e),$$

což je ekvivalentní.

$$\alpha(e) = (a_1 * e)^{j_1} (a_2 * e)^{j_2} ... (a_{k-1} * e)^{j_{k-1}} (a_k * e)^{j_k} = g.$$

Navíc zřejmě $\alpha \in \mathrm{LMlt}(Q)$, a tedy jsme dokázali tvrzení.

□

2. Problém izomorfismu pro principální quandly

Problémem izomorfismu myslíme to, že máme quandly Q_1, Q_2 a chceme vědět, kdy platí, že jsou quandlově izomorfní $Q_1 \simeq Q_2$. V našem případě prozkoumáme principální quandly a budeme se snažit najít charakterizaci případu, kdy jsou navzájem izomorfní, pomocí grupových vlastností.

Lemma 9. *Mějme principální quandly $Q(G,f)$,$Q(G,g)$, pak jestliže existuje $h \in \mathrm{Aut}(G)$ takové, že $hfh^{-1} = g$, pak platí*

$$Q(G,f) \simeq Q(G,g).$$

Důkaz. Ukážeme, že h je hledaný izomorfismus. Jelikož se jedná o automorfismus, tak je prostý a na. Ověříme homomorfní vlastnost. Mějme $x, y \in G$, pak platí

$$h(x * y) = h(xf(x)^{-1}f(y)) = h(x)h(f(x)^{-1})h(f(y)) = h(x)gh(x^{-1})gh(y)$$
$$= h(x) * h(y).$$

□

Lemma 10. *Mějme principální quandly $Q(G,f), Q(G,g)$ a zobrazení $\alpha : \mathrm{G} \to \mathrm{G}$, pak následující tvrzení jsou ekvivalentní.*

(i) Platí, že α je quandlový izomorfismus mezi $Q(G,f)$ a $Q(G,g)$ takový, že

$$\alpha(e) = e.$$

(ii) Pro α platí

(1) $g = \alpha \circ f \circ \alpha^{-1}$,
(2) $\alpha(xf(x)^{-1}) = \alpha(x)\alpha(f(x))^{-1}$, $x \in G$,
(3) $\alpha(mx) = \alpha(m)\alpha(x)$ pro $x \in G, m \in \langle xf(x)^{-1}, x \in G\rangle$.

Důkaz.
$(i) \Rightarrow (ii)$
Nejprve ukážeme pro důkaz první vlastnosti ekvivalentně, že $\alpha \circ f = g \circ \alpha$, protože pro každé $x \in G$ máme

$$\alpha(f(x)) = \alpha(e * x) = \alpha(e) * \alpha(x) = \alpha(e)g(\alpha(e))^{-1}g(\alpha(x)) = g(\alpha(x)).$$

Nyní si všimněme pro důkaz druhé vlastnosti, že platí

$$\alpha(xf(x)^{-1}f(e)) = \alpha(x * e) = \alpha(x) * \alpha(e) = \alpha(x)g(\alpha(x))^{-1}g(\alpha(e))$$
$$\overset{(1)}{=} \alpha(x)\alpha(f(x))^{-1}.$$

Nakonec třetí vlastnost také platí. Označme

$$H = \{u \in G : \alpha(uz) = \alpha(u)\alpha(z) \forall z \in G\}.$$

Ukážeme, že H je podgrupa G.

- Platí $e \in H$, protože $\alpha(ez) = \alpha(z) = \alpha(e)\alpha(z)$.
- Pokud $x, y \in H$, pak platí $xy \in H$, protože pro každé $z \in G$ máme

$$\alpha(xyz) = \alpha(x)\alpha(yz) = \alpha(x)\alpha(y)\alpha(z) = \alpha(xy)\alpha(z).$$

- Také pokud $x \in H$, pak $x^{-1} \in H$, protože

$$\alpha(xx^{-1}) = \alpha(x)\alpha(x^{-1}) = \alpha(e) = e = \alpha(x)\alpha(x)^{-1},$$

kde v první rovnosti využívám toho, že $x \in H$. Máme tudíž

$$\alpha(x^{-1}) = \alpha(x)^{-1}$$

a zároveň platí

$$\alpha(z) = \alpha(x)\alpha(x)^{-1}\alpha(z) = \alpha(xx^{-1}z) = \alpha(x)\alpha(x^{-1}z).$$

Pokud rovnost nyní vynásobíme pomocí $\alpha(x)^{-1}$ zleva, tak máme pro každé $z \in G$ rovnost

$$\alpha(x^{-1}z) = \alpha(x^{-1})\alpha(z),$$

a tedy $x^{-1} \in H$ z čehož plyne, že H je podgrupa G.

Nyní si všimněme, že platí

$$\alpha(xf(x)^{-1}f(y)) = \alpha(x * y) = \alpha(x) * \alpha(y) = \alpha(x)g(\alpha(x))^{-1}g(\alpha(y))$$

$$= \alpha(x)\alpha(f(x))^{-1}\alpha(f(y)).$$

Speciálně pro $y = e$ máme rovnost

$$\alpha(xf(x)^{-1}) = \alpha(x)\alpha(f(x))^{-1}.$$

Díky této rovnosti můžeme odvodit, že

$$xf(x)^{-1} \in H,$$

protože platí

$$\alpha(xf(x)^{-1}f(y)) = \alpha(x) * \alpha(y) = \alpha(x)g(\alpha(x))^{-1}g(\alpha(y))$$

$$= \alpha(x)\alpha(f(x))^{-1}\alpha(f(y)) = \alpha(x(f(x))^{-1})\alpha(f(y))$$

pro $y \in G$, kde ve druhé rovnosti využíváme toho, že $\alpha \circ f = g \circ \alpha$ a v poslední rovnosti využíváme odvozené rovnosti výše, navíc f je grupový automorfismus, speciálně je tedy na, takže skutečně platí $xf(x)^{-1} \in H$. Celkově jsme dokázali, že $\langle xf(x)^{-1}, x \in G\rangle \subseteq H$, a tedy platí třetí vlastnost.

$(ii) \Rightarrow (i)$

Abychom ukázali, že α je skutečně quandlový homomorfismus, tak stačí nahlédnout pomocí vlastností, že

$$\alpha(x * y) = \alpha(xf(x)^{-1}f(y)) \overset{(3)}{=} \alpha(x(f(x))^{-1})\alpha(f(y)) \overset{(2)}{=} \alpha(x)\alpha(f(x))^{-1}\alpha(f(y))$$

$$\overset{(1)}{=} \alpha(x)g(\alpha(x))^{-1}g(\alpha(y)) = \alpha(x) * \alpha(y),$$

kde ve druhé rovnosti jsme využili třetí vlastnost, ve třetí rovnosti druhou vlastnost a ve čtvrté rovnosti první vlastnost. Také pro α musí platít podle druhé vlastnosti následující

$$\alpha(e) = \alpha(e(f(e))^{-1}) \overset{(2)}{=} \alpha(e)\alpha((f(e))^{-1}) = \alpha(e)\alpha(e),$$

a tedy musí platít, $\alpha(e) = e$.

□

Lemma 11. *Jestliže jsou principální quandly $Q(G,f), Q(G,g)$ quandlově izomorfní, pak existuje quandlový izomorfismus $\alpha : \mathrm{G} \to \mathrm{G}$ takový, že*

$$\alpha(e) = e.$$

Důkaz. Mějme libovolný quandlový izomorfismus $\omega : G \to G$ a nechť $\omega(a) = e$. Pokud $a = e$, tak jsme hotovi, jinak definujme zobrazení

$$\beta : Q(G,f) \to Q(G,f), \quad x \mapsto ax.$$

Platí, že β je quandlový automorfismus, protože

$$\beta(x * y) = \beta(xf(x)^{-1}f(y)) = axf(x)^{-1}f(y) = axf(x^{-1}y) = axf(x^{-1}a^{-1}ay)$$

$$= axf(ax)^{-1}f(ay) = \beta(x) * \beta(y).$$

Navíc je β levá grupová translace, a tedy je speciálně bijekcí. Nyní pokud označíme

$$\gamma := \omega \circ \beta,$$

tak platí $\gamma(e) = \omega(a) = e$ a zároveň se jedná o quandlový izomorfismus, jelikož máme složení quandlových izomorfismů.

□

Věta 12 (Charakterizace izomorfismu souvislých principálních quandlů)**.** *Mějme souvislé principální quandly $Q(G,f), Q(G,g)$, pak platí $Q(G,f) \simeq Q(G,g)$ právě tehdy, když existuje $h \in Aut(G)$ takové, že $hfh^{-1} = g$.*

Důkaz.

($\Leftarrow$)
Plyne přímo z Lemmatu 9.

($\Rightarrow$)
Díky Lemmatu 11 můžeme zvolit quandlový izomorfismus takový, že $h(e) = h(e)$, pak z Lemmatu 10 víme z třetí podmínky, že pro $x \in G, m \in \langle xf(x)^{-1}, x \in G\rangle$ platí

$$h(mx) = h(m)h(x).$$

Z Tvrzení 8 ovšem máme, že $xf(x)^{-1}$ generují celou grupu G, a tedy je h grupový automorfismus, protože $\langle xf(x)^{-1}, x \in G\rangle = G$.

□

Věta 13 (Charakterizace izomorfismu obecných principálních quandlů)**.** *Mějme dva principální quandly $Q_1 = Q(G,f), Q_2 = Q(G,g)$, pak platí $Q_1 \simeq Q_2$ právě tehdy, když existuje zobrazení $\alpha : \mathrm{G} \to \mathrm{G}$ takové, že*

(1) $g = \alpha \circ f \circ \alpha^{-1}$,

(2) $\alpha(xf(x)^{-1}) = \alpha(x)\alpha(f(x))^{-1}$, $x \in G$,

(3) $\alpha(mx) = \alpha(m)\alpha(x)$ *pro* $x \in G, m \in \langle xf(x)^{-1}, x \in G\rangle$.

Důkaz. Podle Lemma 11 platí, že pokud jsou quandly izomorfní, pak existuje quandlový izomorfismus α takový, že $\alpha(e) = e$, a tedy podmínka (i) Lemma 10 je ekvivalentní s existencí libovolného quandlového izomorfismu, a tedy platí tvrzení.

□

Lemma 14 (Charakterizace operace principálního quandlu pomocí translací)**.** *Mějme $Q = Q(G,f)$ principální quandle, pak pro všechny $a, b \in G$ platí rovnost*

$$a * b = P_e(a)L_e(b).$$

Důkaz. Snadno ověříme, že

$$a * b = (af(a)^{-1})(f(b)) = (a * e)(e * a) = P_e(a)L_e(b).$$

□

Důsledek 15 (Charakterizace quandlového izomorfismu na principálních quandlech)**.** *Mějme dva principální quandly $Q_1 = Q(G,f), Q_2 = Q(G,g)$ a označme $P_e^{Q_1}, P_e^{Q_2}$ pravou translaci pomocí prvku e v quandlu Q_1, respektivě Q_2 a $L_e^{Q_1}, L_e^{Q_2}$ levou translaci pomocí prvku e v quandlu Q_1, respektivě Q_2, pak bijekce $\alpha : Q_1 \to Q_2$ je quandlový izomorfismus takový, že $\alpha(e) = e$ právě tehdy, když platí podmínky*

(1) $P_e^{Q_2} = \alpha \circ P_e^{Q_1} \circ \alpha^{-1}$,

(2) $L_e^{Q_2} = \alpha \circ L_e^{Q_1} \circ \alpha^{-1}$,

(3) $\alpha(mx) = \alpha(m)\alpha(x)$ *pro* $x \in G, m \in \{xf(x)^{-1}, x \in G\}$.

Důkaz.

($\Rightarrow$)
Pro pravou translaci $P_e^{Q_1}$ máme pro $a \in G$ libovolné

$$\alpha(P_e^{Q_1}(a)) = \alpha(a * e) = \alpha(a) * \alpha(e) = P_e^{Q_2}(\alpha(a)).$$

Pro levou translaci $L_e^{Q_1}$ máme pro $a \in G$ libovolné

$$\alpha(L_e^{Q_1}(a)) = \alpha(e * a) = \alpha(e) * \alpha(a) = L_e^{Q_2}(\alpha(a)).$$

Jelikož $a \in G$ bylo libovolné, tak rovnosti platí na definičním oboru, a tedy platí první dvě rovnosti ze tvrzení. Třetí rovnost je speciální případ třetí podmínky Lemma 10.

($\Leftarrow$)
Pokud platí podmínky, tak máme pro libovolné $a, b \in G$ rovnost

$$\alpha(a*b) \overset{\text{Lemma 14}}{=} \alpha((a*e)(e*a)) \overset{(3)}{=} \alpha(a*e)\alpha(e*a) \overset{(1)(2)}{=} (\alpha(a)*\alpha(e))(\alpha(e)*\alpha(a))$$

$$\overset{\text{Lemma 14}}{=} \alpha(a)*\alpha(b),$$

kde ve první rovnosti využíváme Lemma 14, ve druhé rovnosti využíváme podmínku (3), ve třetí rovnosti používáme podmínku (1) a (2) a ve čtvrté rovnosti využíváme Lemma 14. Celkově tedy máme bijekci, která je homomorfismus, takže je i izomorfismus. Navíc $\alpha(e) = e$, protože podle podmínky (3) máme

$$\alpha(e) = \alpha(ef(e)^{-1}) = \alpha(e)\alpha(e).$$

Z čehož plyne $\alpha(e) = e$.

□

3. Problém izomorfismu pro principální quandly na dihedrálních grupách

3.1 Značení

Pro celou práci dihedrální grupu o $2n$ prvcích značíme D_{2n} a předpokládáme $n > 2$ přirozené. Rotaci o a vrcholů doprava značíme r^a, speciálně $r^1 = r$. Skládání prvků $d_1, d_2 \in D_{2n}$, budeme zapisovat jako násobení

$$d_2 \circ d_1 = d_1 d_2,$$

speciálně pro rotace r^a, r^b, budeme značit

$$r^b \circ r^a = r^a r^b = r^{a+b \, mod(n)} := r^{a+b}.$$

Reflexe značíme cr^a, kde c je námi vybraná pevná reflexe a $a \in \mathbb{Z}_n$ a identitu budeme značit podle potřeby jako id nebo jako triviální rotaci o 0 kroků r^0.

Značením $\phi(n)$ standardně myslíme Eulerovu funkci.

Semidirektní součin grup G, H značíme

$$G \rtimes_\omega H,$$

kde ω je grupový homomorfismus $\omega : H \to Aut(G)$.
Zbytek značení zůstává stejný jako v minulé kapitole.

3.2 Vlastnosti dihedrálních grup

Lemma 16 (Generátory dihedrálních grup a vlastnosti skládání prvků)**.** *Pro dihedrální grupu D_{2n} platí*

$$D_{2n} = \langle r^b, c \rangle,$$

kde $b \in \{0, 1...n-1\}$ takové, že $\mathrm{NSD}(b, n) = 1$ a c je libovolná reflexe.

Důkaz. Máme $\mathrm{NSD}(b, n) = 1$, a tedy můžeme pomocí r^b nagenerovat každou rotaci $r^a, a \in \{0, 1...n-1\}$, jelikož skládání rotací je izomorfní sčítání modulo $\mathbb{Z}_n$. Každá z těchto rotací generuje podgrupu velikosti n, a tudíž platí $\langle r^b, c \rangle = D_{2n}$, jelikož dostaneme podgrupu řádu vyššího než polovina řádu celé grupy.

□

Pozorování 17 (Vlastnosti skládání prvků dihedrální grupy)**.** *Složení dvou reflexí je rotace a pro libovolnou rotaci $r^a, a \in \{0, 1...n-1\}$ a reflexi c platí $cr^a c = r^{-a}$.*

Důkaz. Složení dvou reflexí je rotace, protože platí, že determinant matice reflexí je -1, rotací je 1. Složení dvou reflexí odpovídá součinu dvou matic a z věty o determinantu součinu matic dostaneme tvrzení, navíc platí $cr^a cr^a = id$, protože cr^a je reflexe a ta má vždy řád 2.

□

3.3 Grupy automorfismů dihedrálních grup

V této sekci jsou všechny homomorfismy grupové.

Lemma 18. *Automorfismy $f \in \mathrm{Aut}(D_{2n})$ jsou právě homomorfismy $f_{a,b}$ takové, že*

$$f_{a,b} : D_{2n} \to D_{2n}, \quad r \mapsto r^b; \quad c \mapsto cr^a,$$

kde $a, b \in \{0, 1...n-1\}$ a zároveň $\mathrm{NSD}(b, n) = 1$.

Důkaz. Ukážeme, že libovolný automorfismus f zobrazuje reflexi na reflexi a rotaci na rotaci. Toto platí, jelikož $\mathrm{ord}(r) = n$ a v grupě D_{2n} mají řád n pouze rotace $r^b, b \in \{0, 1...n-1\}$ takové, že $\mathrm{NSD}(b, n) = 1$, a tedy každou rotaci můžeme nagenerovat pomocí mocnění obrazu $f(r)$, protože automorfismy zachovávají řád prvků. Nyní ukážeme, že každé takové zobrazení

$$f_{a,b} : D_{2n} \to D_{2n}, \quad r \mapsto r^b; \quad c \mapsto cr^a,$$

kde $a, b \in \{0, 1...n-1\}$ a zároveň $\mathrm{NSD}(b, n) = 1$, které je na zbytku prvků homomorfně zadefinováno je automorfismus.
Pro dvě rotace je zobrazení homomorfní, protože

$$f_{a,b}(r^m r^n) = r^{bm} r^{bn} = f_{a,b}(r^m) f_{a,b}(r^n).$$

Pro dvě reflexe je zobrazení homomorfní, jelikož

$$f_{a,b}(cr^m cr^n) = cr^a r^{bm} cr^a r^{bn} = f_{a,b}(cr^m) f_{a,b}(cr^n).$$

Nakonec pro rotaci a reflexi platí

$$f_{a,b}(cr^m r^n) = f_{a,b}(cr^{m+n}) = cr^a r^{b(m+n)} = cr^a r^{bm} r^{bn} = f_{a,b}(cr^m) f_{a,b}(r^n).$$

Z čehož máme, že se skutečně jedná o homomorfismus. Tento homomorfismus je zřejmě na, protože generátory se zobrazí na generátory. Prostota plyne z toho, že každé rotaci je přiřazena právě jedna rotace a toto přiřazení odpovídá translaci prvkem $\mathbb{Z}_n^*$ na prvcích grupy $\mathbb{Z}_n$, jelikož podgrupa rotací grupy D_{2n} je izomorfní grupě $\mathbb{Z}_n$ a takové přiřazení je automorfismus, speciálně je tedy prosté. U reflexí musí platit to samé, jelikož si každou reflexi můžeme vyjádřit jako složení jedné pevné reflexe s vhodnou rotací.

□

Důsledek 19. *Platí $|\mathrm{Aut}(D_{2n})| = n\phi(n) = |\mathbb{Z}_n||\mathbb{Z}_n^*|$.*

Poznámka 1. *Nadále až do konce práce budeme značit stejně jako ve znění Lemma 18 automorfismy na dihedrálních grupách $f_{a,b}$.*

Věta 20 (Izomorfismus grupy automorfismů dihedrálních grup)**.** *Mezi následujícími grupami platí vztah izomorfismu*

$$\mathrm{Aut}(D_{2n}) \simeq \mathbb{Z}_n \rtimes_\omega \mathbb{Z}_n^*,$$

kde grupová operace semidirektního součinu je definovaná následovně

$$(a,b) * (c,d) = (a + bc, bd),$$

kde $a,c \in \mathbb{Z}_n$ a $b,d \in \mathbb{Z}_n^*$. Nakonec grupový homomorfismus ω je definován následovně

$$\omega : \mathbb{Z}_n^* \to \mathrm{Aut}(\mathbb{Z}_n), \quad b \mapsto f;$$
$$f : \mathbb{Z}_n \to \mathbb{Z}_n, \quad a \mapsto ba.$$

Důkaz. Nejprve se podíváme na to, jak funguje skládání prvků v $\mathrm{Aut}(D_{2n})$. Mějme $f_{a,b}, f_{c,d} \in \mathrm{Aut}(D_{2n})$, pak platí

$$f_{a,b}(f_{c,d}(r)) = f_{a,b}(r^d) = r^{bd}, \tag{3.1}$$
$$f_{a,b}(f_{c,d}(c)) = f_{a,b}(cr^c) = f_{a,b}(c) f_{a,b}(r^c) = cr^a r^{bc} = cr^{a+bc}. \tag{3.2}$$

Nyní mějme $\mathbb{Z}_n \rtimes_\omega \mathbb{Z}_n^*$, dokážeme, že ω je správně definovaný. Zobrazení ω přiřadí prvku $b \in \mathbb{Z}_n^* \mapsto f \in \mathrm{Aut}(\mathbb{Z}_n)$, kde $f(a) = ba, a \in \mathbb{Z}_n$, a tedy obraz prvku je skutečně automorfismus, jelikož se jedná o levou translaci generátorem. Navíc se zřejmě jedná o homomorfismus, jelikož $\omega(1)(a) = a$ a $\omega(bd)(c) = bdc = \omega(b)(\omega(d)(c))$.

Nyní najdeme izomorfismus mezi dvěmi grupami, zvolme

$$\Pi : \mathrm{Aut}(D_{2n}) \to \mathbb{Z}_n \rtimes_\omega \mathbb{Z}_n^*, \quad f_{i,k} \mapsto (i,k).$$

Ukážeme, že Π je izomorfismus. Platí následující

$$\Pi(f_{a,b}) = (a,b),$$
$$\Pi(f_{c,d}) = (c,d),$$
$$\Pi(f_{a,b} \circ f_{c,d}) \overset{3.1,\,3.2}{=} (a + bc, bd) = (a,b) * (c,d),$$

protože $\mathbb{Z}_n^*$ je komutativní. Navíc pokud $(a,b) = (c,d)$, pak se zobrazení $f_{a,b}, f_{c,d}$ rovnají na generátorech, tudíž jsou si rovné. Z tohoto plyne, že Π je prosté a zřejmě je také na, protože je to prosté zobrazení mezi stejně mohutnými množinami podle Důsledku 19.

□

Poznámka 2. *Nadále až do konce práce budeme myslet semidirektním součinem $\mathbb{Z}_n \rtimes_\omega \mathbb{Z}_n^*$ ten z Věty 20.*

Pozorování 21. *Inverz prvku (a,b) v grupě $\mathbb{Z}_n \rtimes_\omega \mathbb{Z}_n^*$ je tvaru $(-b^{-1}a, b^{-1})$.*

Důkaz. Přímým výpočtem platí $(a,b)*(-b^{-1}a,b^{-1}) = (a+b(-b^{-1}a),bb^{-1}) = (0,1)$. □

Tvrzení 22 (Třídy konjugace automorfismů dihedrálních grup)**.** *Mějme $\mathbb{Z}_n \rtimes_\omega \mathbb{Z}_n^*$, pak prvek (c,d) je ve stejné konjugační třídě jako prvek (a,b) právě tehdy, když $d = b$ a zároveň platí*

$$c \in (a + (b-1)\mathbb{Z}_n)\mathbb{Z}_n^*.$$

Důkaz. Platí, že $(a,b),(c,d)$ jsou konjugované právě tehdy, když existuje (x,y) takové, že

$$(a,b)(x,y) = (x,y)(c,d),$$

což nastává právě tehdy, když

$$(a + bx, by) = (x + yc, yd),$$

ovšem $\mathbb{Z}_n^*$ je abelovská grupa, a tedy pravá složka $by = yd$ je ekvivalentní s $b = d$, protože y nemůže být nulové. Pro levou složku rovnosti platí

$$a + bx = x + yc,$$

což si můžeme ekvivalentně upravit na

$$c = (a + bx - x)y^{-1} = (a + (b-1)x)y^{-1},$$

jelikož $y \in \mathbb{Z}_n^*$, a tedy celkově

$$(a + bx, by) = (x + yc, yd)$$

nastává právě tehdy, když $b = d$ a zároveň platí, že existuje $x \in \mathbb{Z}_n, y \in \mathbb{Z}_n^*$ takové, že $c = (a + (b-1)x)y^{-1}$, což existují právě tehdy, když

$$c \in (a + (b-1)\mathbb{Z}_n)\mathbb{Z}_n^*.$$

□

Důsledek 23. *Mějme $\mathbb{Z}_p \rtimes_\omega \mathbb{Z}_p^*$ pro p prvočíslo, pak prvek $(c,d) \neq (0,1)$ je ve stejné konjugační třídě jako jiný prvek $(a,b) \neq (0,1)$ právě tehdy, když $d = b$. Prvek $(0,1)$ je v konjugační třídě sám.*

Důkaz. Přímý důsledek Tvrzení 22.

□

Pro znázornění si tedy můžeme třídy ekvivalnece znázornit v následující tabulce, kde řádky nám určují první složku a sloupce druhou složku a písmeny označíme různé konjugační třídy.

	1	2	...	...	(p-1)
0	A	C	D	...	X
1	B	C	D	...	X
...	B	C	D	...	X
...	...	...	...	...	...
(p-1)	B	C	D	...	X

3.4 Vlastnosti principálních quandlů na dihedrálních grupách

Značení. Principální quandle $Q(D_{2n}, f_{a,b})$ budeme nadále značit $Q_{a,b}$, navíc pro principální quandle $Q_{a,b}$ označíme

$$M_{a,b} := \langle x f_{a,b}(x)^{-1}; x \in D_{2n} \rangle = D_{2n}.$$

Tvrzení 24. *Mějme principální quandle $Q_{a,b} = Q(D_{2n}, f_{a,b})$, pak pro všechna $x \in D_{2n}$ platí $x f_{a,b}(x)^{-1}$ je rotace a různých levých translací je tedy maximálně n.*

Důkaz. Pro automorfismus $f_{a,b}$ musí platit podle Lemma 18, že rotace se zobrazí na rotaci a reflexe na reflexi z čehož plyne, že pro rotaci x platí $x f_{a,b}(x)^{-1}$ je rotace, jelikož inverz rotace je rotace a pro reflexi x platí $x f_{a,b}(x)^{-1}$ je rotace, protože inverz reflexe je stejná reflexe a složení dvou reflexí je vždy rotace podle Pozorování 17. Celkově tedy máme, že $x f_{a,b}(x)^{-1}$ jsou pouze rotace.

□

Tvrzení 25. *Mějme principální quandle $Q_{a,b} = Q(D_{2n}, f_{a,b})$, pak tento quandle není souvislý pro žádné $n \in \mathbb{N}, n > 2$.*

Důkaz. Dokážeme sporem pomocí Tvrzení 8 tak, že vyvrátíme ekvivalentní podmínku. Kdyby totiž platilo

$$M_{a,b} = D_{2n},$$

pak reflexe $c \in M_{a,b}$, ale $x f_{a,b}(x)^{-1}$ je rotace pro všechna $x \in D_{2n}$ a inverzem rotace dostaneme opět rotaci a skládání rotací nám dá opět rotaci, tedy platí

$$M_{a,b} = \langle x f_{a,b}(x)^{-1}; x \in D_{2n} \rangle \neq D_{2n},$$

a tedy quandle Q není souvislý.

□

Lemma 26. *Mějme dihedrální quandle $Q_{a,b} = Q(D_{2n}, f_{a,b})$, pak pro rotace r^i, r^j platí $r^i * r^j = r^j * r^i$ právě tehdy, když pro reflexe cr^i, cr^j platí $cr^i * cr^j = cr^j * cr^i$, což platí právě tehdy, když nad $\mathbb{Z}_n$ platí rovnost*

$$i(1 - 2b) = j(1 - 2b).$$

Nikdy neplatí pro reflexi a rotaci rovnost $r^i * cr^j = cr^j * r^i$.

Důkaz.

- Pro dvě rotace máme rovnost $r^i * r^j = r^j * r^i$ ekvivalentní $r^i r^{-bi} r^{bj} = r^j r^{-bj} r^{bi}$, což nastává právě tehdy, když $i - bi + bj = j - bj + bi$ z čehož již dostáváme rovnost z tvrzení

$$i(1-2b) = j(1-2b).$$

- Pro dvě reflexe máme rovnost $cr^i * cr^j = cr^j * cr^i$ ekvivalentní rovnosti $cr^i cr^{a+bi} cr^{a+bj} = cr^j cr^{a+bj} cr^{a+bi}$, což můžeme ekvivalentně upravit na rovnost $r^{-i} r^{a+bi} cr^{a+bj} = r^{-j} r^{a+bj} cr^{a+bi}$, což podle Pozorování 17 nastává právě tehdy, když $i - a - bi + a + bj = j - a - bj + a + bi$, což již můžeme upravit na rovnost z tvrzení

$$i(1-2b) = j(1-2b).$$

- Mějme rotaci a reflexi, pak rovnost $r^i * cr^j = cr^j * r^i$ nastává právě tehdy, když $r^i r^{-bi} cr^{a+bj} = cr^j cr^{a+bj} r^{bi}$, což nemůže nastat, protože na levé straně máme rotaci a na pravé straně podle Pozorování 17 reflexi a reflexe nikdy nemůže být rovna rotaci.

□

Příklad. Pomocí Lemma 26 můžeme snadno a rychle nahlédnout, že quandly $Q(D_{18}, f_{a,1}), Q(D_{18}, f_{c,2})$, nejsou izomorfní pro žádné $a, c \in \mathbb{Z}_n$, protože pro $b = 1$ máme, že nám nekomutují žádné prvky nikdy, jelikož rovnice $-i = -j$ má pouze triviální řešení $i = j$, ale pro $b = 2$ máme $6i = 6j$ a to má řešení například dvojice $(3, 0), (0, 6)...$, a tedy nemohou být quandly izomorfní. V některých případech nám tedy může Lemma 20 a jeho důsledek vyvrátit možnost izomorfismu pro celé skupiny quandlů najednou.

Důsledek 27. *Mějme dihedrální quandle $Q = Q(D_{2n}, f_{a,b})$, $x, y \in D_{2n}, x \neq y$, pak pro $n = 2^k$, kde $k \in \mathbb{N}$ máme*

$$x * y \neq y * x.$$

Důkaz. Pro $n = 2^k$ máme jako možnosti b pouze lichá čísla, ale pak $(1 - 2b)$ je liché číslo a to je v $\mathbb{Z}_{2^k}$ generátorem, jehož grupová levá i pravá translace je bijekce a speciálně je prostá, a tedy rovnost z přechozího Lemma 26 nastává právě tehdy, když $i = j$.

□

Lemma 28. *Mějme dihedrální quandle $Q_{a,b} = Q(D_{2n}, f_{a,b})$, pak platí, že pro levou translaci L_{r^i} danou rotací r^i a pro každé $x \in D_{2n}$ platí*

$$L_{r^i}(x) = r^{(1-b)i} f_{a,b}(x)$$

a pro levou translaci L_{cr^i} danou reflexí cr^i a pro každé $x \in D_{2n}$ platí

$$L_{cr^i}(x) = r^{a+(b-1)i} f_{a,b}(x).$$

Důkaz. Stačí nahlédnout, že pro rotaci r^i máme

$$L_{r^i}(x) = r^i * x = r^i f_{a,b}(r^i)^{-1} f_{a,b}(x) = r^i r^{-bi} f_{a,b}(x) = r^{(1-b)i} f_{a,b}(x).$$

Pro reflexi cr^i pak máme

$$L_{cr^i}(x) = cr^i f_{a,b}(cr^i) f_{a,b}(x) = cr^i cr^a r^{bi} f_{a,b}(x) = r^{a+(b-1)i} f_{a,b}(x).$$

□

Důsledek 29. *Mějme dihedrální quandle $Q_{a,b} = Q(D_{2n}, f_{a,b})$, pak pro libovolnou rotaci r^i platí*

$$r^i f_{a,b}(r^i)^{-1} = r^{(1-b)i}$$

a pro libovolnou reflexi cr^i platí

$$cr^i f_{a,b}(cr^i)^{-1} = r^{a+(b-1)i}.$$

Speciálně máme, že pokud $b \neq 1$, pak pro $n = p$ prvočíslo je množina

$$\{x f_{a,b}(x)^{-1}, x \in D_{2p}\} = \{r^i, i \in \{0, 1, ..., p-1\}\}.$$

Důsledek 30. *Mějme $Q_{a,b} = Q(D_{2n}, f_{a,b})$, pak počet levých translací quandlu $Q_{a,b}$ je roven velikosti množiny $|\{(1-b)\mathbb{Z}_n\} \cup \{a + (b-1)\mathbb{Z}_n\}|$.*

3.5 Řešení problému izomorfismu pro některé dihedrální quandly

Důsledek 31. *Mějme principální quandly*
$Q_{a,b} = Q(D_{2p}, f_{a,b}), Q_{c,d} = Q(D_{2p}, f_{c,d})$, takové, že $b \neq d$, pak pokud

$$\{L_x(e), x \in D_{2p}, L_x \in \mathrm{LMlt}(Q_{a,b})\} = \{x f_{a,b}(x)^{-1}, x \in D_{2p}\}$$

$$= \{r^i, i \in \{0, 1, ..., p-1\}\}$$

$$= \{x f_{c,d}(x)^{-1}, x \in D_{2p}\} = \{L_x(e), x \in D_{2p}, L_x \in \mathrm{LMlt}(Q_{c,d})\},$$

pak quandly $Q_{a,b}, Q_{c,d}$ nejsou quandlově izomorfní.

Důkaz. Dokážeme sporem. Z Lemma 11 plyne, že aby byly quandly quandlově izomorfní, tak musí existovat quandlový izomorfismus α, takový, že $\alpha(e) = e$, a tedy z podmínky (3) Věty 13 by α zúžené na množinu rotací bylo grupovým automorfismem. Zároveň platí, že grupa automorfismů grupy rotací je komutativní, protože je izomorfní $\mathrm{Aut}(\mathbb{Z}_n)$, a tedy z podmínky (1) Věty 13 máme, že

$$f_{a,b} = \alpha \circ f_{c,d} \circ \alpha^{-1}$$

a z komutativity a podmínky (3) tedy

$$f_{a,b}(x) = f_{c,d}(x),$$

pro všechny rotace x, a tedy $b = d$.

□

Důsledek 32. *Mějme rozdílné principální quandly* $Q_{a,b} = Q(D_{2p}, f_{a,b}), Q_{c,d} = Q(D_{2p}, f_{c,d})$*, kde* p *je prvočíslo, pak tyto quandly jsou quandlově izomorfní právě tehdy, když* $b = d$ *a zároveň* $f_{a,b}$ *ani* $f_{c,d}$ *není identita.*

Důkaz.

($\Leftarrow$)
Různé zobrazení $f_{a,b}, f_{c,d}$ jsou konjugované podle Důsledku 23 a Věty 20 právě tehdy, když $b = d$ a zároveň platí, že ani jeden z dvojice $f_{a,b}, f_{c,d}$ není identita. Speciálně identita $f_{0,1}$ je v konjugační třídě sama a quandly dané automorfismem $f_{a,1}$, pro $a \neq 0$, jsou v jedné konjugační třídě. Ostatní jsou ve stejné konjugační třídě právě tehdy, když $b = d$. Podle Věty 12 jsou všechny navzájem konjugované quandly quandlově izomorfní, čímž jsme dokázali tvrzení.

($\Rightarrow$)
Nyní sporem dokážeme, že pro $1 \neq b \neq d \neq 1$ nejsou quandly $Q_{a,b}, Q_{c,d}$ quandlově izomorfní nikdy. Podle Tvrzení 24 a Důsledku 29 máme, že prvky, které jsou tvaru $xf_{a,b}(x)^{-1}$ nebo tvaru $xf_{c,d}(x)^{-1}$ jsou všechny rotace a podle Důsledku 31 tedy přímo plyne, že quandlově izomorfní nejsou. Navíc pokud je právě jedno z dvojice b, d rovno 1, pak nemohou být izomorfní, protože podle Důsledku 30 by měly různý počet levých translací, což je podle Tvrzení 2 invariant.

□

Tvrzení 33. *Nad grupou* D_8 *je přesně* 5 *tříd ekvivalence vzhledem ke konjugaci* $\mathrm{Aut}(D_8)$*, ale přesně* 4 *navzájem neizomorfní quandly.*

Důkaz. Najdeme řešení problému izomorfismu pro D_8. Nejprve nalezneme pomocí Tvrzení 22 konjugační třídy grupy grupových automorfismů D_8 a dostaneme 5 různých konjugačních tříd, které si znázorníme v tabulce, kde řádky nám určují hodnotu a automorfismu $f_{a,b}$ a sloupce hodnotu b. Písmeny poté označíme konjugační třídy.

	1	3
0	A	D
1	B	E
2	C	D
3	B	E

Snadno se dá pomocí Lemma 28 ověřit, že počty levých translací, což je invariant podle Tvrzení 2, vyřazuje možnosti, že by byly quandly s automorfismy v konjugačních třídách A, nebo E izomorfní s jakýmikoliv jinými quandly, protože počet levých translací quandlů s automorfismem v konjugační třídě A je 1 a počet levých translací quandlů s automorfismem v konjugační třídě E je 4. U ostatních quandlů máme počet levých translací roven 2.

Ukážeme, že quandly s automorfismem v B a automorfismem v C nejsou izomorfní nikdy pomocí zástupců $Q(D_8, f_{1,1}), Q(D_8, f_{2,1})$. Ukážeme, že nejmenší řád levé translace v quandlu $Q(D_8, f_{2,1})$ je 2, ovšem v quandlu $Q(D_8, f_{1,1})$ jsou všechny řády levé translace vyšší, a tedy podle Tvrzení 2 nemohou být izomorfní. Podíváme-li se na řád levé translace L_{r^2} quandlu $Q(D_8, f_{2,1})$, tak dostaneme, že řád je roven 2, protože pro obecnou rotaci r^i máme

$$r^2 * r^i = r^2 r^{-2} r^i = r^i$$

a zároveň pro reflexi cr^i platí

$$r^2 * (r^2 * cr^i) = r^2 * (r^2 r^{-2} cr^{2+i}) = r^{r^2 r^{-2}} cr^{2+2+i} = cr^i,$$

ale žádná translace quandlu $Q(D_8, f_{2,1})$ nemá řád 2. Například vezmeme-li zástupce L_e, L_c, které jsou zřejmě rozdílné podle Lemma 28, tak pro libovolnou reflexi cr^i platí

$$e * (e * cr^i) = e * (cr^{i+1}) = cr^{i+2} \neq cr^i$$

a pro libovolnou rotaci r^i platí

$$c * (c * r^i) = c * (ccr^{i+1}) = ccrr^{i+1} = r^{i+2} \neq r^i.$$

Nyní nakonec dokážeme, že quandly $(D_8, f_{2,1}), (D_8, f_{0,3})$ jsou quandlově izomorfní tak, že nalezneme vhodný quandlový izomorfismus

$$\alpha : (D_8, f_{2,1}) \to (D_8, f_{0,3}), \quad \alpha(e) = e.$$

Díky Větě 13 podmínky (3) vidíme, že musí platit $\alpha(e) = e, \alpha(r^2) = r^2$ a zároveň se body určující stejnou levou translaci jako e, r^2 v quandlu $(D_8, f_{2,1})$ musí zobrazit v quandlu $(D_8, f_{0,3})$ na body určující stejnou levou translaci jako e, r^2, což nám dává možnosti c, cr^2. Navíc si všimněme, že v obou quandlech platí rovnost $e * cr^3 = cr, e * cr = cr^3$, a tedy zkusíme zadefinovat $\alpha(cr) = cr, \alpha(cr^3) = cr^3$. Zbytek už můžeme zadefinovat pouze 4 možnostmi a dojdeme k řešení

$$\begin{aligned}
\alpha(e) &= e, \\
\alpha(r) &= c, \\
\alpha(r^2) &= r^2, \\
\alpha(r^3) &= cr^2, \\
\alpha(c) &= r, \\
\alpha(cr) &= cr, \\
\alpha(cr^2) &= r^3, \\
\alpha(cr^3) &= cr^3.
\end{aligned}$$

Toto řešení navíc stačí zkontrolovat na $2(2n-1) = 14$ jednoduchých rovnic místo 64, protože máme pouze dvě různé levé translace, které nám už jednoznačně určují celou strukturu quandlu, což nám dává 16 a dvě hodnoty jsou nám známé z idempotence. Dá se ručně ověřit, že skutečně pro všechna $x \in D_8$ platí $\alpha(e * x) = \alpha(e) * \alpha(x)$ a zároveň $\alpha(c * x) = \alpha(c) * \alpha(x)$, z čehož plyne, že jsou skutečně izomorfní, a tedy platí tvrzení. Pro lepší náhlednost uvedeme tabulky obou quandlů. V první buňce vlevo nahoře bude název quandlu. V prvním neohraničeném levém sloupci budou pod názvem prvky, označme je x_i, kde $i \in \{1,...n\}$. Prvky prvního neohraničeného řádku za názvem quandlu označíme y_j, kde $j \in \{1,...n\}$. V již plně ohraničené buňce na pozici (i, j) bude hodnota $x_i * y_j$.

$Q_{2,1}$	$*e$	$*r*$	$*r^2$	$*r^3$	$*c$	$*cr$	$*cr^2$	$*cr^3$
$e*$	e	r	r^2	r^3	cr^2	cr^3	c	cr
$r*$	e	r	r^2	r^3	cr^2	cr^3	c	cr
r^2*	e	r	r^2	r^3	cr^2	cr^3	c	cr
r^3*	e	r	r^2	r^3	cr^2	cr^3	c	cr
$c*$	r^2	r^3	e	r	c	cr	cr^2	cr^3
$cr*$	r^2	r^3	e	r	c	cr	cr^2	r^2
cr^2*	r^2	r^3	e	r	c	cr	cr^2	cr^3
cr^3*	r^2	r^3	e	r	c	cr	cr^2	cr^3

$Q_{0,3}$	$*e$	$*r*$	$*r^2$	$*r^3$	$*c$	$*cr$	$*cr^2$	$*cr^3$
$e*$	e	r^3	r^2	r	c	cr^3	cr^2	cr
$r*$	r^2	r	e	r^3	cr^2	cr	c	cr^3
r^2*	e	r^3	r^2	r	c	cr^3	cr^2	cr
r^3*	r^2	r	e	r^3	cr^2	cr	c	cr^3
$c*$	e	r^3	r^2	r	c	cr^3	cr^2	cr
$cr*$	r^2	r	e	r^3	cr^2	cr	c	cr^3
cr^2*	e	r^3	r^2	r	c	cr^3	cr^2	cr
cr^3*	r^2	r	e	r^3	cr^2	cr	c	cr^3

□

Závěr

Viděli jsme, že problém izomorfismu quandlů je pro souvislé principální quandly právě problém konjugace grupového automorfismu v grupě automorfismů (viz Věta 12). Pro nesouvislé principální quandly je problém řešen, ale věta je podstatně složitější (viz Věta 13).

Také jsme si rozebrali některé příklady problému izomorfismu pro principální quandly na grupě D_{2n}. Pro n prvočíslo, přestože se nejedná o souvislý quandle, je charakterizace stejná jako u souvislých quandlů (viz Důsledek 32). Pro n obecné je problém komplikovanější, jak jsme si ukázali na řešení D_8 (Tvrzení 33), kde jsme explicitně našli izomorfní principální quandly, jejichž automorfismy, které určují jejich quandlovou operaci, nejsou konjugované.

Přirozenou otázkou zůstává jak vyřešit problém pro ostatní D_{2n}. Obzvláště zajímavé budou právě D_{2^n}, protože jsou nilpotentní. Také zůstává otázkou jak vyřešit problém izomorfismu pro principální quandly na rozdílných grupách.

Seznam použité literatury

[1] David Joyce. A classifying invariant of knots, the knot quandle. *Journal of Pure and Applied Algebra*, 23(1):37–65, 1982.

[2] Xiang dong Hou. Automorphism groups of alexander quandles. *Journal of Algebra*, 344(1):373–385, 2011.

[3] Sam Nelson. Classification of finite alexander quandles, 2003.

[4] Akihiro Higashitani and Hirotake Kurihara. Homogeneous quandles arising from automorphisms of symmetric groups. *Communications in Algebra*, 51(4):1413–1430, 2023.

[5] Alexander Hulpke, David Stanovský, and Petr Vojtěchovský. Connected quandles and transitive groups. *Journal of Pure and Applied Algebra*, 220(2):735–758, 2016.