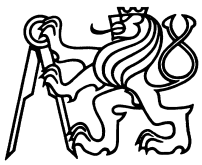
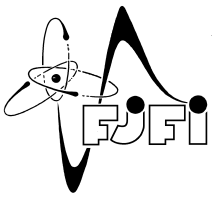


České vysoké učení technické
v Praze
Fakulta jaderná a fyzikálně inženýrská



Bakalářská práce

Teorie grup a kvantové počítání

Pavla Bartoňová

Vedoucí práce: prof. Ing. Jiří Tolar, DrSc.

2017

Název práce:

Teorie grup a kvantové počítání

Autor: Pavla Bartoňová

Obor: Matematické inženýrství

Zaměření: Matematická fyzika

Druh práce: Bakalářská práce

Vedoucí práce: prof. Ing. Jiří Tolar, DrSc.

Konzultanti: Ing. Petr Novotný, PhD.; Mgr. Miroslav Korbelář, PhD.

Abstrakt: V této práci se budeme zabývat Weylovými-Heisenbergovými grupami a Cliffordovými grupami pro jeden qudit. Zavedeme Cliffordovu grupu jako podgrupu normalizátoru Weylovy-Heisenbergovy grupy v grupě unitárních operátorů a ukážeme, jak ke každému jejímu prvku můžeme přiřadit matici z $\mathrm{SL}(2,\mathbb{Z}_d)$. Dále se budeme věnovat grupě vnitřních automorfismů indukovaných některými prvky Weylovy-Heisenbergovy grupy a jejímu normalizátoru. Na závěr se zaměříme na Cliffordovy grupy pro $d = 2$ a $d = 3$.

Klíčová slova: Cliffordova grupa, normalizátor, unitární operátor, vnitřní automorfismus, Weylova-Heisenbergova grupa

Title:

Group Theory and Quantum Computation

Author: Pavla Bartoňová

Abstract: This thesis deals with the Weyl-Heisenberg groups and the Clifford groups on one qudit. We define the Clifford group as a subgroup of the normalizer of the Weyl-Heisenberg group in the group of unitary operators. There exists a correspondence between elements of Clifford group and matrices from $\mathrm{SL}(2,\mathbb{Z}_d)$. Then we describe the group of inner automorphisms induced by some elements of the Weyl-Heisenberg group and the normalizer of this group. Finally, the Clifford groups for $d = 2$ and $d = 3$ are examined.

Key words: Clifford group, inner automorphism, normalizer, unitary operator, Weyl-Heisenberg group

Poděkování

Chtěla bych poděkovat panu profesoru Jiřímu Tolarovi za velkou trpělivost a za to, že mi vždy ochotně poradil a povzbudil mě.

Obsah

Úvod

Podle postulátů kvantové mechaniky je stavovým prostorem uzavřeného kvantového systému Hilbertův prostor $\mathcal{H}$ – úplný lineární vektorový prostor se skalárním součinem. Stav systému je potom popsán vektorem (s normou rovnou jedné) z prostoru $\mathcal{H}$.

Časovému vývoji kvantového systému odpovídá unitární operátor na prostoru $\mathcal{H}$, pozorovatelné se popisují hermitovskými operátory na $\mathcal{H}$.

V této práci se budeme zabývat pouze Hilbertovým prostorem konečné dimenze n nad tělesem $\mathbb{C}$, budeme jej značit $\mathcal{H}_n$.

Základem pro kvantové počítání je qubit (kvantový bit) – kvantový systém, jehož stavovým prostorem je $\mathcal{H}_2$. Pro m qubitů je stavovým prostorem tenzorový součin m dvourozměrných prostorů: $\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_2$.

Qubit je dále možné zobecnit na qu*d*it, kde $d \in \{3, 4, \dots\}$; příslušným stavovým prostorem je pak $\mathcal{H}_d$.

V kvantových počítačích se používají kvantová hradla (podobně jako v klasických počítačích logická hradla). Kvantová hradla pro jeden qubit mohou být reprezentována unitárními maticemi z prostoru $\mathbb{C}^{2,2}$. Příkladem jsou Pauliho matice σ_x, σ_y a σ_z (viz Definice 1.1), dohromady generující Pauliho grupu. Dalšími důležitými hradly jsou Hadamardovo hradlo a fázové hradlo (viz Poznámka 2.5), společně generují Cliffordovu grupu pro jeden qubit.

V 1. kapitole se budeme zabývat Weylovou-Heisenbergovou grupou Π_n [1], [2], [3] – zobecněním Pauliho grupy. Jejími prvky jsou unitární operátory na prostoru $\mathcal{H}_n$, tj. stavovém prostoru jednoho qu*d*itu, kde $d = n$. Ve druhé části této kapitoly zavedeme grupu $\mathcal{P}_n$ [2], [3] – grupu generovanou vnitřními automorfismy indukovanými prvky grupy Π_n.

Ve 2. kapitole se zaměříme na Cliffordovu grupu $\mathcal{C}_n$ – Cliffordovu grupu pro jeden qu*d*it, kde $d = n$. (Často se ovšem symbolem $\mathcal{C}_n$ označuje Cliffordova grupa pro n qubitů.) Je to podgrupa normalizátoru grupy Π_n v grupě unitárních operátorů na prostoru $\mathcal{H}_n$. Ukážeme, že ke každému prvku normalizátoru můžeme přiřadit matici z $\mathrm{SL}(2, \mathbb{Z}_n)$ a dvojici čísel z $\mathbb{Z}_{2n}^2$ [4]. Na konci kapitoly se opět vrátíme ke grupě $\mathcal{P}_n$ a ukážeme, jaký je vztah mezi jejím normalizátorem a grupou $\mathrm{SL}(2, \mathbb{Z}_n)$ [2], [5].

Kapitola 3 pojednává o Cliffordových grupách $\mathcal{C}_2$ [5], [7] a $\mathcal{C}_3$.

Značení

1. Grupu $(G;\cdot)$ budeme značit pouze G, její neutrální prvek označíme e, inverzní prvek k prvku $g \in G$ označíme g^{-1}.

2. Grupu generovanou prvky $a_1, a_2, \ldots, a_m$ budeme značit: $\langle a_1, a_2, \ldots, a_m \rangle$.

3. Kartézský součin grup G_1, G_2 (resp. okruhů R_1, R_2) označíme $G_1 \times G_2$ (resp. $R_1 \times R_2$).

4. Výrazem $H \subset\subset G$ budeme rozumět, že H je podgrupou grupy G.
   Výrazem $H \triangleleft G$ budeme rozumět, že H je normální podgrupou grupy G.

5. Skalární součin na prostoru $\mathcal{H}_n$ budeme značit: $\langle \cdot\,, \cdot \rangle$; je antilineární v prvním argumentu a lineární ve druhém argumentu.

I, $\mathbb{I}$	identický operátor, jednotková matice
O, $\mathbb{O}$	nulový operátor, nulová matice
$\lvert G\rvert$	řád grupy G
$\mathbb{Z}_n$	faktorokruh okruhu $(\mathbb{Z}; +, \cdot)$ podle kongruence mod n
$\mathbb{Z}_n^2$	$\mathbb{Z}_n \times \mathbb{Z}_n$
$\mathbb{Z}_n^{m,m}$	množina všech matic $m \times m$, jejichž prvky patří do $\mathbb{Z}_n$, s operací násobení matic mod n
$\mathcal{Z}_n$	faktorgrupa grupy $(\mathbb{Z}; +)$ podle kongruence mod n
$\mathcal{L}(\mathcal{H}_n)$	množina všech lineárních operátorů $\mathcal{H}_n \to \mathcal{H}_n$
$\mathrm{GL}(\mathcal{H}_n)$	grupa $(\{X \in \mathcal{L}(\mathcal{H}_n) \mid X \text{ je regulární}\}; \circ)$
$\mathrm{U}(n)$	grupa $(\{X \in \mathcal{L}(\mathcal{H}_n) \mid XX^* = \mathrm{I}\}; \circ)$
$\mathrm{SL}(m, \mathbb{Z}_n)$	grupa $(\{M \in \mathbb{Z}_n^{m,m} \mid \det M = 1 \pmod n\}; \cdot \pmod n)$

Kapitola 1

Weylovy-Heisenbergovy grupy

1.1 Definice Weylových-Heisenbergových grup

V této kapitole nejprve definujeme operátory $\hat{Q}_n$ a $\hat{P}_n$, odpovídající zobecněným Pauliho maticím Q_n, P_n. Potom zavedeme Weylovu-Heisenbergovu grupu Π_n.

Definice 1.1. Mějme vektorový prostor $\mathbb{C}^{2,2}$. Matice

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},\ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

se nazývají Pauliho matice.

Definice 1.2. Mějme vektorový prostor $\mathbb{C}^{n,n}$, $n \in \{2, 3, \dots\}$. Označíme

$$\omega_n = \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}.$$

Matice

$$P_n = \begin{pmatrix} 0 & 1 & & & \\ 0 & & 1 & & \\ \vdots & & & \ddots & \\ 0 & & & & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}, \quad Q_n = \begin{pmatrix} 1 & & & & \\ & \omega_n & & & \\ & & {\omega_n}^2 & & \\ & & & \ddots & \\ & & & & {\omega_n}^{n-1} \end{pmatrix},$$

se nazývají zobecněné Pauliho matice.

Poznámka 1.3. Pro n=2 odpovídají zobecněné Pauliho matice P_n, Q_n Pauliho maticím σ_x, σ_z:

$$P_2 = \sigma_x, \quad Q_2 = \sigma_z.$$

Poznámka ke značení 1.4. V této práci budeme symbolem $\mathcal{H}_n$ rozumět Hilbertovův prostor konečné dimenze n nad tělesem $\mathbb{C}$. V něm si pevně zvolíme ortonormální bázi a označíme ji

$$\mathcal{E} = (e_0, e_1, \dots, e_{n-1}).$$

Toto značení budeme zachovávat v celé práci.

Definice 1.5. Mějme vektorový prostor $\mathcal{H}_n$ s ortonormální bází $\mathcal{E}$. Na něm definujeme operátory $\hat{Q}_n, \hat{P}_n \in \mathcal{L}(\mathcal{H}_n) : \ \forall j \in \{0, 1, \ldots, n-1\}$:

$$\hat{Q}_n \, e_j = {\omega_n}^j e_j \,,$$
$$\hat{P}_n \, e_j = e_{j-1(\mathrm{mod}\, n)} \,.$$

Poznámka 1.6. Vyjádřením operátorů $\hat{Q}_n$, $\hat{P}_n$ v bázi $\mathcal{E}$ získáme zobecněné Pauliho matice Q_n, P_n.

Poznámka ke značení 1.7. Nadále nebudeme ve značení rozlišovat mezi operátory a jejich maticemi v bázi $\mathcal{E}$. (Vše budeme psát bez stříšky.)

Tvrzení 1.8. Operátory Q_n, P_n jsou unitární.

Poznámka 1.9. Operátor $X \in \mathcal{L}(\mathcal{H}_n)$ je unitární $\iff \langle Xx, Xy\rangle = \langle x, y\rangle$, $\forall x, y \in \mathcal{H}_n$.

Nechť $\mathcal{X} = (x_0, x_1, \ldots, x_{n-1})$ je báze $\mathcal{H}_n$. Platí:
$\forall x_j, x_k \in \mathcal{X} : \langle Xx_j, Xx_k\rangle = \langle x_j, x_k\rangle \quad \Longrightarrow \quad \forall x, y \in \mathcal{H}_n : \langle Xx, Xy\rangle = \langle x, y\rangle$.

Ověření:

$$\langle Xx, Xy\rangle = \left\langle X\left(\sum\nolimits_j \alpha_j x_j\right), X\left(\sum\nolimits_k \beta_k x_k\right)\right\rangle = \sum\nolimits_j \bar{\alpha}_j \sum\nolimits_k \beta_k \langle Xx_j, Xx_k\rangle =$$
$$= \sum\nolimits_j \bar{\alpha}_j \sum\nolimits_k \beta_k \langle x_j, x_k\rangle = \left\langle \sum\nolimits_j \alpha_j x_j, \sum\nolimits_k \beta_k x_k\right\rangle = \langle x, y\rangle \,.$$

Důkaz Tvrzení 1.8. Pro libovolné $j, k \in \{0, 1, \ldots, n-1\}$:

$$\begin{aligned} \langle Q_n e_j, Q_n e_k\rangle &= \langle \omega_n^j e_j, \omega_n^k e_k\rangle &&= \omega_n^{k-j} \langle e_j, e_k\rangle &&= \langle e_j, e_k\rangle, \\ \langle P_n e_j, P_n e_k\rangle &= \langle e_{j-1}, e_{k-1}\rangle &&= \langle e_j, e_k\rangle. \end{aligned}$$

Odtud již plyne (podle Poznámky 1.9), že Q_n, P_n jsou unitární. □

Tvrzení 1.10. Operátory Q_n, P_n mají následující vlastnosti:

1. $P_n Q_n = \omega_n Q_n P_n$,
2. $(Q_n)^n = (P_n)^n = \mathrm{I}$, kde I je identita na $\mathcal{H}_n$.

Důkaz. Pro libovolné $j \in \{0, 1, \ldots, n-1\}$ platí:

1. $P_n Q_n \, e_j = \omega_n^j P_n \, e_j = \omega_n^j e_{j-1} \,,$
   $\omega_n Q_n P_n \, e_j = \omega_n Q_n \, e_{j-1} = \omega_n^{1+j-1} e_{j-1} = \omega_n^j e_{j-1} \,,$
2. $(Q_n)^n \, e_j = \omega_n^{jn} e_j = e_j,$
   $(P_n)^n \, e_j = e_{j-n} = e_j.$ □

Poznámka 1.11. Grupa $\langle \sigma_x, \sigma_y, \sigma_z\rangle$ se nazývá Pauliho grupa.

Jelikož platí: $\sigma_y = -\mathrm{i}\, \sigma_z \sigma_x$, můžeme Pauliho grupu zapsat také jako

$$\langle -\mathrm{i}\, \mathrm{I}, \sigma_x, \sigma_z\rangle = \langle -\mathrm{i}\, \mathrm{I}, P_2, Q_2\rangle.$$

Definice 1.12 (Weylova-Heisenbergova grupa)**.** Nechť $n \in \{2, 3, 4, \dots\}$. Označíme

$$\tau_n = -\mathrm{e}^{\frac{\pi \mathrm{i}}{n}}.$$

Weylovu-Heisenbergovu grupu Π_n definujeme jako podgrupu grupy $\mathrm{U}(n)$ generovanou operátory $\tau_n \mathrm{I}$, Q_n a P_n, kde grupovou operací je skládání zobrazení:

$$\Pi_n = \langle \tau_n \mathrm{I}, P_n, Q_n \rangle.$$

Poznámka 1.13. Grupa Π_n se také nazývá zobecněná Pauliho grupa.

Tvrzení 1.14. Pro n liché platí: $\{\tau_n, \tau_n^2, \dots, \tau_n^n\} = \{\omega_n, \omega_n^2, \dots, \omega_n^n\}$.

Důkaz. Nechť n je liché, $n > 1$. Vyjádříme τ_n^j pro $j \in \{1, 2, \dots, n\}$:

1. pro j sudé, tj. $j = 2k, k \in \{1, 2, \dots, \frac{n-1}{2}\}$:

   $$\tau_n^j = \tau_n^{2k} = (-1)^{2k}\, \mathrm{e}^{\frac{2k\pi \mathrm{i}}{n}} = \omega_n^k,$$

   a tedy sudé mocniny τ_n odpovídají množině $\{\omega_n, \omega_n^2, \dots, \omega_n^{\frac{n-1}{2}}\}$;

2. pro j liché: $\tau_n = -\mathrm{e}^{\frac{\pi \mathrm{i}}{n}} = \mathrm{e}^{\pi \mathrm{i} + \frac{\pi \mathrm{i}}{n}} = \mathrm{e}^{\frac{(n+1)\pi \mathrm{i}}{n}} = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n} \frac{n+1}{2}} = \omega_n^{\frac{n+1}{2}}$,

   $$\tau_n^j = \omega_n^{\frac{j(n+1)}{2}} = \omega_n^{\frac{(j-1)n}{2}}\, \omega_n^{\frac{n+j}{2}} = \omega_n^{\frac{n+j}{2}}, \tag{1.1}$$

   a proto liché mocniny τ_n odpovídají množině $\{\omega_n^{\frac{n+1}{2}}, \omega_n^{\frac{n+3}{2}}, \dots, \omega_n^{\frac{2n}{2}}\}$.

□

Poznámka 1.15. Podle vztahu (1.1) pro n liché platí:

$$\tau_n^n = \omega_n^{\frac{2n}{2}} = \omega_n^n = 1.$$

Poznámka 1.16. Z Tvrzení 1.10 a 1.14 plyne, že grupu Π_n můžeme zapsat také takto:

$$\Pi_n = \begin{cases} \left\{\omega_n^l\, Q_n^j\, P_n^k \mid j, k, l \in \{0, 1, \dots, n-1\}\right\} & \text{pro } n \text{ liché,} \\ \left\{\tau_n^l\, Q_n^j\, P_n^k \mid j, k \in \{0, 1, \dots, n-1\};\ l \in \{0, 1, \dots, 2n-1\}\right\} & \text{pro } n \text{ sudé.} \end{cases}$$

Tvrzení 1.17.

$$|\Pi_n| = \begin{cases} n^3 & \text{pro } n \text{ liché,} \\ 2n^3 & \text{pro } n \text{ sudé.} \end{cases}$$

Důkaz. Plyne z Poznámky 1.16. □

Poznámka 1.18. V [2], [3] se grupa Π_n definuje pro libovolné n (liché i sudé) pouze jako $\Pi_n = \left\{\omega_n^l\, Q_n^j\, P_n^k \mid l, j, k \in \{0, 1, \dots, n-1\}\right\}$.

Podle [1] můžeme definovat také abstraktní Weylovu-Heisenbergovu grupu.

Definice 1.19 (Abstraktní Weylova-Heisenbergova grupa)**.** Konečnou Weylovu-Heisenbergovu grupu H_n (pro $n \in \{2, 3, \dots\}$) definujeme jako grupu generovanou třemi různými prvky α, Q, P splňujícími následující relace:

- pokud je n liché:
  1. α, Q, P jsou řádu n, (a tedy $\alpha^n = Q^n = P^n = e$),
  2. $\alpha Q = Q\alpha$, $\alpha P = P\alpha$, $\alpha QP = PQ$;
- pokud je n sudé:
  1. α je řádu $2n$; Q, P jsou řádu n, (a tedy $\alpha^{2n} = Q^n = P^n = e$),
  2. $\alpha Q = Q\alpha$, $\alpha P = P\alpha$, $\alpha^2 QP = PQ$.

Poznámka ke značení 1.20. V dalším textu budeme někdy index n (např. u operátorů Q_n, P_n nebo konstant τ_n, ω_n) vynechávat.

Na závěr uvedeme dvě lemmata, týkající se operátorů Q_n a P_n. Využijeme je především až ve 2. kapitole.

Lemma 1.21. Platí: $Q^j P^k Q^l P^m = \omega^{kl} Q^{j+l} P^{k+m}$.

Důkaz.

$$\begin{aligned} Q^j P^k Q^l P^m &= Q^j P^{k-1} PQ\, Q^{l-1} P^m && = \omega\, Q^j P^{k-1} QP\, Q^{l-1} P^m \\ &= \omega\, Q^j P^{k-2} PQ\, PQ^{l-1} P^m && = \omega^2\, Q^j P^{k-2} Q\, P^2 Q^{l-1} P^m \\ &= \ \dots && = \omega^k\, Q^{j+1} P^k Q^{l-1} P^m \\ &= \omega^{2k}\, Q^{j+2} P^k Q^{l-2} P^m && = \ \dots \\ &= \omega^{kl}\, Q^{j+l} P^{k+m} \end{aligned}$$

□

Lemma 1.22. Platí: $(Q^j P^k)^l = \tau^{jkl(l-1)}\, Q^{jl} P^{kl}$.

Důkaz.

$$\begin{aligned} (Q^j P^k)^l &= Q^j P^k Q^j P^k (Q^j P^k)^{l-2} && \overset{(a)}{=} \omega^{jk}\, Q^{2j} P^{2k} (Q^j P^k)^{l-2} && = \\ &= \omega^{jk}\, Q^{2j} P^{2k} Q^j P^k (Q^j P^k)^{l-3} && \overset{(a)}{=} \omega^{jk+2jk}\, Q^{3j} P^{3k} (Q^j P^k)^{l-3} && = \\ &\overset{(a)}{=} \dots \overset{(a)}{=} \omega^{jk+2jk+\cdots+(l-1)jk}\, Q^{jl} P^{kl} && = \tau^{2jk(1+2+\cdots+(l-1))}\, Q^{jl} P^{kl} && = \\ &= \tau^{jkl(l-1)}\, Q^{jl} P^{kl} \end{aligned}$$

V rovnostech označených (a) jsme použili Lemma 1.21. □

1.2 Grupa $\mathcal{P}_n$

Přejdeme od prvků grupy $\mathrm{GL}(\mathcal{H}_n)$ (tj. operátorů na $\mathcal{H}_n$) k jejím vnitřním automorfismům. Zavedeme grupu $\mathcal{P}_n$ obsahující vnitřní automrfismy indukované operátory Q_n a P_n a nakonec ukážeme, jaká je souvislost mezi grupami Π_n a $\mathcal{P}_n$.

Definice 1.23. Nechť G je grupa, $a \in G$. Zobrazení $\mathrm{Ad}_a : G \to G : g \mapsto aga^{-1}$ nazveme vnitřním automorfismem grupy G (indukovaným prvkem a).

Definice 1.24. Grupu $\mathrm{Int}(G) = \{\mathrm{Ad}_a \mid a \in G\}$ nazveme grupou vnitřních automorfismů grupy G.

Poznámka ke značení 1.25. Pro každé $X \in \mathrm{GL}(\mathcal{H}_n)$ budeme výrazem Ad_X rozumět vnitřní automorfismus grupy $\mathrm{GL}(\mathcal{H}_n)$.

Definice 1.26 (Grupa $\mathcal{P}_n$)**.** Nechť $n \in \{2, 3, 4, \dots\}$. Grupu $\mathcal{P}_n$ definujeme jako podgrupu grupy $\mathrm{Int}(\mathrm{GL}(\mathcal{H}_n))$ generovanou automorfismy $\mathrm{Ad}_{Q_n}, \mathrm{Ad}_{P_n}$, kde grupovou operací je skládání zobrazení:

$$\mathcal{P}_n = \langle \mathrm{Ad}_{Q_n}, \mathrm{Ad}_{P_n} \rangle.$$

Lemma 1.27. Nechť $X \in \mathrm{GL}(\mathcal{H}_n)$ a platí následující vztahy: $Q_n X = \alpha X Q_n$ a $P_n X = \beta X P_n$, kde $\alpha, \beta \in \mathbb{C} \setminus \{0\}$. Potom existují $\gamma \in \mathbb{C} \setminus \{0\}$ a $Y \in \Pi_n$ takové, že $X = \gamma Y$.

Důkaz. Důkaz provedeme podle [3].

Označíme $X_i^{(j)} = \langle e_i, X e_j \rangle$. Pro libovolné $i, j \in \{0, 1, \dots, n-1\}$ platí:

$$\begin{aligned} \langle e_i, QXe_j \rangle &= \langle Q^{-1} e_i, Xe_j \rangle &&= \omega^i \langle e_i, Xe_j \rangle &&= \omega^i X_i^{(j)}, \\ \langle e_i, XQe_j \rangle &= \omega^j \langle e_i, Xe_j \rangle &&= \omega^j X_i^{(j)}. \end{aligned}$$

S využitím předpokladu $QX = \alpha XQ$ získáme:

$$\begin{aligned} \omega^i X_i^{(j)} &= \alpha \omega^j X_i^{(j)} \\ (\omega^i - \alpha \omega^j) X_i^{(j)} &= 0. \end{aligned} \tag{1.2}$$

Jelikož $X \neq \mathrm{O}$, musí existovat nějaké $\tilde{j}$ takové, že $Xe_{\tilde{j}} \neq 0$. Pak existuje také $\tilde{i}$ takové, že $\langle e_{\tilde{i}}, Xe_{\tilde{j}} \rangle = X_{\tilde{i}}^{(\tilde{j})} \neq 0$.

$$\begin{aligned} (\omega^{\tilde{i}} - \alpha \omega^{\tilde{j}}) X_{\tilde{i}}^{(\tilde{j})} &= 0 \\ \omega^{\tilde{i}} - \alpha \omega^{\tilde{j}} &= 0 \\ \omega^{\tilde{i} - \tilde{j}} &= \alpha \end{aligned}$$

Zjistili jsme, že α musí být nějakou mocninou ω. Dosadíme za α do (1.2).

$$(\omega^i - \omega^{\tilde{i} - \tilde{j} + j}) X_i^{(j)} = 0$$

Odtud plyne, že pokud $i \neq \tilde{i} - \tilde{j} + j \pmod n$, potom $X_i^{(j)} = 0$. Tudíž platí:

$$Xe_j = \sum_{k=0}^{n-1} X_k^{(j)} e_k = X_{\tilde{i} - \tilde{j} + j}^{(j)} e_{\tilde{i} - \tilde{j} + j}. \tag{1.3}$$

Označíme $X^{(j)} = X^{(j)}_{\tilde{i}-\tilde{j}+j}$. Pro každé $j \in \{0, 1, \ldots, n-1\}$ platí:

$$PXe_j = X^{(j)}Pe_{\tilde{i}-\tilde{j}+j} = X^{(j)}e_{\tilde{i}-\tilde{j}+j-1}\,,$$
$$XPe_j = Xe_{j-1} = X^{(j-1)}e_{\tilde{i}-\tilde{j}+j-1}\,.$$

Využitím předpokladu $PX = \beta XP$ získáme:

$$\begin{aligned} X^{(j)}e_{\tilde{i}-\tilde{j}+j-1} &= \beta X^{(j-1)}e_{\tilde{i}-\tilde{j}+j-1} \\ (X^{(j)} - \beta X^{(j-1)})e_{\tilde{i}-\tilde{j}+j-1} &= 0 \\ X^{(j)} &= \beta X^{(j-1)}. \end{aligned} \tag{1.4}$$

Odtud

$$\begin{aligned} X^{(j)} = \beta X^{(j-1)} = \beta^2 X^{(j-2)} = \ldots = \beta^j X^{(0)}, \\ X^{(0)} = \beta X^{(n-1)} = \ldots = \beta^n X^{(0)} \\ (1-\beta^n)X^{(0)} = \mathrm{O}. \end{aligned} \tag{1.5}$$

Jelikož $X \neq \mathrm{O}$, existuje nějaké k tak, že $X^{(k)} \neq 0$. Aby to bylo splněno, musí platit: $X^{(0)} \neq 0$. Potom

$$\beta^n = 1,$$

a tedy existuje nějaké l takové, že

$$\beta = \omega_n^l.$$

Dosadíme za β do (1.5):

$$X^{(j)} = \omega^{lj}X^{(0)}.$$

Potom se (1.3) změní na

$$Xe_j = \omega^{lj}X^{(0)}e_{\tilde{i}-\tilde{j}+j} = X^{(0)}P^{\tilde{j}-\tilde{i}}Q^l e_j,$$

a proto

$$X = X^{(0)}P^{\tilde{j}-\tilde{i}}Q^l.$$

Zřejmě platí: $X^{(0)} \in \mathbb{C} \setminus \{0\}$ a $P^{\tilde{j}-\tilde{i}}Q^l \in \Pi_n$. Položíme $\gamma = X^{(0)}$ a $Y = P^{\tilde{j}-\tilde{i}}Q^l$. □

Lemma 1.28. Nechť $X \in \mathrm{GL}(\mathcal{H}_n)$ a platí následující vztahy: $Q_nX = XQ_n$ a $P_nX = XP_n$. Potom $X = \delta\,\mathrm{I}$, kde $\delta \in \mathbb{C} \setminus \{0\}$.

Důkaz. Vyjdeme z důkazu Lemmatu 1.27 – v něm položíme $\alpha = 1$ a $\beta = 1$. Vztah (1.2) se změní na

$$(\omega^i - \omega^j)X_i^{(j)} = 0.$$

Odtud plyne: pokud $i \neq j \pmod n$, pak $X_i^{(j)} = 0$. Vyjádříme Xe_j:

$$Xe_j = \sum_{k=0}^{n-1} X_k^{(j)} e_k = X_j^{(j)} e_j.$$

Označíme $X^{(j)} = X_j^{(j)}$. Vztah (1.4) se (po dosazení $\beta = 1$, $\tilde{i} - \tilde{j} = 0$) změní na

$$(X^{(j)} - X^{(j-1)})e_{j-1} = 0.$$

Odtud

$$X^{(j)} = X^{(j-1)},$$
$$X^{(n-1)} = X^{(n-2)} = \cdots = X^{(0)};$$

a protože $X \neq \mathrm{O}$, musí platit: $X^{(0)} \neq 0$. Pak

$$Xe_j = X^{(j)} e_j = X^{(0)} e_j,$$

a tedy

$$X = X^{(0)}\mathrm{I}.$$

Nyní už jen položíme $\delta = X^{(0)}$. □

Poznámka 1.29. Pokud budeme v Lemmatu 1.27 (resp. 1.28) předpokládat, že $X \in \mathrm{U}(n)$, získáme, že existuje $\gamma \in \mathbb{C}, |\gamma| = 1$ a $Y \in \Pi_n$ tak, že $X = \gamma Y$ (resp. existuje $\delta \in \mathbb{C}, |\delta| = 1$ tak, že $X = \delta\mathrm{I}$).

Vnitřní automorfismy grupy $\mathrm{GL}(\mathcal{H}_n)$ mají následující vlastnosti [3]:

Tvrzení 1.30. Mějme libovolné $A, B \in \mathrm{GL}(\mathcal{H}_n)$. Pak platí:

1. $\mathrm{Ad}_A \mathrm{Ad}_B = \mathrm{Ad}_{AB}$;
2. $(\mathrm{Ad}_A)^k = \mathrm{Ad}_{A^k}$, $k \in \mathbb{N}$;
3. $(\mathrm{Ad}_A)^{-1} = \mathrm{Ad}_{A^{-1}}$;
4. $\mathrm{Ad}_A = \mathrm{Ad}_B \Leftrightarrow \exists\, c \in \mathbb{C} \setminus \{0\} : A = cB$.

Důkaz. Pro libovolné $X \in \mathrm{GL}(\mathcal{H}_n)$ platí:

1. $\mathrm{Ad}_A \mathrm{Ad}_B X = \mathrm{Ad}_A(BXB^{-1}) = ABXB^{-1}A^{-1} = ABX(AB)^{-1} = \mathrm{Ad}_{AB} X$;
2. $(\mathrm{Ad}_A)^k X = A^k X (A^{-1})^k = A^k X (A^k)^{-1} = \mathrm{Ad}_{A^k} X$;

3. $\mathrm{Ad}_{A^{-1}}\mathrm{Ad}_A = \mathrm{Ad}_{A^{-1}A} = \mathrm{Ad}_{\mathrm{I}} = \mathrm{I} = \mathrm{Ad}_A\mathrm{Ad}_{A^{-1}}$, (v první rovnosti jsme využili vlastnost 1.);

4. Pokud $A = cB$, pak $\mathrm{Ad}_A X = \mathrm{Ad}_{cB}X = cBXc^{-1}B^{-1} = BXB^{-1} = \mathrm{Ad}_B X$.

   Pokud $\mathrm{Ad}_A = \mathrm{Ad}_B$, potom pro každé $X \in \mathrm{GL}(\mathcal{H}_n)$ platí:

$$\mathrm{Ad}_A X = AXA^{-1} = BXB^{-1} = \mathrm{Ad}_B X.$$
$$B^{-1}AX = XB^{-1}A$$

   Označíme $C = B^{-1}A$. Máme tedy $CX = XC, \forall X \in \mathrm{GL}(\mathcal{H}_n)$. Potom jistě platí: $CQ = QC$ a $CP = PC$. Podle Lemmatu 1.28 existuje $\delta \in \mathbb{C} \setminus \{0\}$ tak, že $C = \delta\,\mathrm{I}$. Je zřejmé, že operátor $\delta\mathrm{I}$ komutuje i se všemi ostatními $X \in \mathrm{GL}(\mathcal{H}_n)$. Položíme $c = \delta$.

$$C = c\,\mathrm{I} = B^{-1}A$$
$$A = cB \qquad \square$$

Tvrzení 1.31. Grupa $\mathcal{P}_n$ je komutativní.

Důkaz. Stačí ověřit, že spolu komutují generátory $\mathcal{P}_n$. Podle Tvrzení 1.30 a vztahu $\omega_n Q_n P_n = P_n Q_n$:

$$\mathrm{Ad}_P\mathrm{Ad}_Q = \mathrm{Ad}_{PQ} = \mathrm{Ad}_{\omega QP} = \mathrm{Ad}_{QP} = \mathrm{Ad}_Q\mathrm{Ad}_P. \qquad \square$$

Poznámka 1.32. Z Tvrzení 1.10 a z komutativity grupy $\mathcal{P}_n$ plyne, že můžeme její libovolný prvek napsat ve tvaru: $\mathrm{Ad}_Q^j\mathrm{Ad}_P^k$, pro nějaké $j, k \in \{0, 1, \ldots, n-1\}$, a proto

$$\mathcal{P}_n = \left\{\mathrm{Ad}_{Q_n}^j\mathrm{Ad}_{P_n}^k \mid j, k \in \{0, 1, \ldots, n-1\}\right\}.$$

Tvrzení 1.33. $|\mathcal{P}_n| = n^2$.

Důkaz. Plyne z Poznámky 1.32. $\square$

Definice 1.34. Centrum grupy G je podgrupa

$$Z(G) = \{z \in G \mid \forall g \in G :\ zg = gz\}.$$

Poznámka 1.35. $Z(G) \triangleleft G$.
Ověření: $\forall z \in Z(G) : \forall g \in G :\ gzg^{-1} = zgg^{-1} = z \in Z(G)$.

Tvrzení 1.36.

$$Z(\Pi_n) = \begin{cases} \left\{\omega_n^j\,\mathrm{I} \mid j \in \{0, 1, \ldots, n-1\}\right\} & \text{pro } n \text{ liché,} \\ \left\{\tau_n^j\,\mathrm{I} \mid j \in \{0, 1, \ldots, 2n-1\}\right\} & \text{pro } n \text{ sudé.} \end{cases}$$

Důkaz. ($\subset$) Pokud $z \in Z(\Pi_n)$, tj. z komutuje se všemi prvky grupy Π_n, pak podle Lemmatu 1.28 platí, že existuje $\gamma \in \mathbb{C}\backslash\{0\}$ tak, že $z = \gamma \mathrm{I}$. Zároveň víme, že $z \in \Pi_n$, tudíž z může být jedině tvaru $\tau_n^k \mathrm{I}$, kde $k \in \{0, 1, \ldots, n-1$ (resp. $2n-1)\}$.

($\supset$) Pro každé $k \in \{0, 1, \ldots, n-1$ (resp. $2n-1)\}$ platí: pokud $z = \tau_n^k \mathrm{I}$, pak určitě komutuje se všemi prvky Π_n.

Pro n liché nyní ještě využijeme Tvrzení 1.14. □

Tvrzení 1.37. $\Pi_n / Z(\Pi_n) \cong \mathcal{P}_n \cong \mathcal{Z}_n \times \mathcal{Z}_n$.

Důkaz. Prvky grupy $\Pi_n / Z(\Pi_n)$ jsou rozkladové třídy. Označíme

$$[Q^j P^k] = Q^j P^k \, Z(\Pi_n).$$

Pro násobení ve faktorgrupě platí:

$$[Q^j P^k][Q^l P^m] = [Q^j P^k Q^l P^m] \overset{(a)}{=} [\omega^{kl} Q^{j+l} P^{k+m}] \overset{(b)}{=} [Q^{j+l} P^{k+m}],$$

kde v rovnosti (a) jsme využili Lemma 1.21, v rovnosti (b) : $\omega^{kl} \mathrm{I} \in Z(\Pi_n)$.

1. Definujeme zobrazení $h_1 : \Pi_n / Z(\Pi_n) \to \mathcal{P}_n : [Z] \mapsto \mathrm{Ad}_Z$.

   Podle Tvrzení 1.30 je zobrazení h_1 prosté:

   $$\mathrm{Ad}_{Z_1} = \mathrm{Ad}_{Z_2} \Longrightarrow Z_1 = c Z_2 \Longrightarrow [Z_1] = [Z_2],$$

   a tudíž je to také bijekce. Ověříme, že h_1 je homomorfismus:

   $$h_1([Z_1][Z_2]) = h_1([Z_1 Z_2]) = \mathrm{Ad}_{Z_1 Z_2} \overset{(c)}{=} \mathrm{Ad}_{Z_1} \mathrm{Ad}_{Z_2} = h_1([Z_1]) h_1([Z_2]),$$

   kde v rovnosti (c) jsme využili Tvrzení 1.30.

2. Definujeme zobrazení $h_2 : \Pi_n / Z(\Pi_n) \to \mathcal{Z}_n \times \mathcal{Z}_n : [Q^j P^k] \mapsto (j, k)$.

   Je to zřejmě bijekce. Ukážeme, že je to homomorfismus:

   $$\begin{aligned} h_2([Q^j P^k]\,[Q^l P^m]) &= h_2([Q^{j+l} P^{k+m}]) = (j + l,\, k + m) = (j, k) + (l, m) \\ &= h_1([Q^j P^k])\; h_2([Q^l P^m]). \end{aligned}$$ □

Kapitola 2

Cliffordovy grupy

Cliffordova grupa se někdy (např. v [1], [4]) definuje jako normalizátor grupy Π_n v grupě $\mathrm{U}(n)$ všech unitárních operátorů na prostoru $\mathcal{H}_n$:

$$\tilde{\mathcal{C}}_n = \mathcal{N}_{\mathrm{U}(n)}(\Pi_n).$$

V této práci budeme ale Cliffordovou grupou $\mathcal{C}_n$ rozumět pouze jistou konečně generovanou podgrupu grupy $\mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$, (jak je to uvedeno v Definici 2.11).

Definice 2.1. Nechť G je grupa, H její podgrupa. Normalizátor H v grupě G je podgrupa

$$\mathcal{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Poznámka 2.2. Ověříme, že normalizátor je opravdu podgrupa.

1. Je zřejmé, že $e \in \mathcal{N}_G(H)$. 2. $n \in \mathcal{N}_G(H) \Rightarrow nHn^{-1} = H \Rightarrow H = n^{-1}Hn \Rightarrow n^{-1} \in \mathcal{N}_G(H)$. 3. $n_1, n_2 \in \mathcal{N}_G(H) \Rightarrow n_1 n_2 H n_2^{-1} n_1^{-1} = n_1 H n_1^{-1} = H \Rightarrow n_1 n_2 \in \mathcal{N}_G(H)$.

Poznámka 2.3. Z definice normalizátoru plyne, že $H \triangleleft \mathcal{N}_G(H)$.

2.1 Definice a vlastnosti Cliffordových grup

Definice 2.4. Mějme vektorový prostor $\mathcal{H}_n$ nad $\mathbb{C}$ s ortonormální bází $\mathcal{E}$. Definujeme operátory $S_n, D_n \in \mathcal{L}(\mathcal{H}_n) : \ \forall j \in \{0, 1, \ldots, n-1\}$:

$$S_n\, e_j = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \omega_n^{kj}\, e_k; \tag{2.1}$$

$$D_n\, e_j = \begin{cases} \tau_n^{j(1-j)}\, e_j & \text{pro } n \text{ liché,} \\ \tau_n^{j(n-j)}\, e_j & \text{pro } n \text{ sudé.} \end{cases} \tag{2.2}$$

Poznámka 2.5. Jak bylo zmíněno v úvodu, důležitými hradly pro kvantové počítače jsou kromě Pauliho hradel (ty jsou reprezentovány Pauliho maticemi) také

Hadamardovo hradlo a fázové hradlo. Jim odpovídající matice označíme po řadě $\tilde{S}_2$ a $\tilde{D}_2$:

$$\tilde{S}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \tilde{D}_2 = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}.$$

Snadno se přesvědčíme, že pro $n = 2$ odpovídá matice operátoru S_n v bázi $\mathcal{E}$ matici $\tilde{S}_2$. Operátor S_n se také nazývá n-rozměrná diskrétní Fourierova transformace.

Fázovému hradlu pro jeden qu*d*it (kde $d = n$) odpovídá operátor $\tilde{D}_n$:

$$\tilde{D}_n\, e_j = \tau^{j(n+j)}\, e_j,$$

ten souvisí s operátorem D_n následovně:

1. pro n sudé: $\tilde{D}_n = D_n^{-1}$,

$$D_n \tilde{D}_n e_j = \tau_n^{j(n+j)} D_n e_j = \tau_n^{j(n+j)+j(n-j)} e_j = \tau_n^{2jn} e_j = e_j,$$

2. pro n liché: $\tilde{D}_n = D_n^{-1} Q_n^{\frac{n+1}{2}}$,

$$D_n \tilde{D}_n e_j = \tau_n^{j(n+j)} \tilde{D}_n e_j = \tau_n^{j(n+j)+j(1-j)} e_j = \tau_n^{(n+1)j} e_j = \omega_n^{\frac{(n+1)j}{2}} e_j = Q_n^{\frac{n+1}{2}} e_j.$$

Poznámka 2.6. V několika následujících důkazech se nám bude hodit znát rovnost

$$\frac{1}{n} \sum_{l=0}^{n-1} \omega^{lp} = \begin{cases} \text{pro } p = 0 \pmod n\text{:} & = \dfrac{1}{n} \displaystyle\sum_{l=0}^{n-1} 1 \qquad\quad = 1, \\[2ex] \text{pro } p \neq 0 \pmod n\text{:} & = \dfrac{1}{n}\, \dfrac{1-\omega^{np}}{1-\omega^{p}} \quad = 0, \end{cases}$$

kde $p \in \mathbb{Z}$.

Tvrzení 2.7. Operátory S_n, D_n jsou unitární.

Důkaz. $\forall j, k \in \{0, 1, \ldots, n-1\}$:

$$\begin{aligned} &\langle Se_j, Se_k \rangle = \\ &= \left\langle \frac{1}{\sqrt{n}} \sum_{l=0}^{n-1} \omega^{lj} e_l,\ \frac{1}{\sqrt{n}} \sum_{m=0}^{n-1} \omega^{mk} e_m \right\rangle = \frac{1}{n} \sum_{l=0}^{n-1} \omega^{-lj} \left\langle e_l,\ \sum_{m=0}^{n-1} \omega^{mk} e_m \right\rangle \\ &= \frac{1}{n} \sum_{l=0}^{n-1} \omega^{-lj} \sum_{m=0}^{n-1} \omega^{mk} \langle e_l,\ e_m \rangle = \frac{1}{n} \sum_{l=0}^{n-1} \omega^{-lj} \omega^{lk} = \frac{1}{n} \sum_{l=0}^{n-1} \omega^{l(k-j)} \\ &\overset{(a)}{=} \langle e_j, e_k \rangle, \end{aligned}$$

kde rovnost (a) plyne z Poznámky 2.6: pro $k = j$ se výraz před označeným rovnítkem rovná 1, pro $k \neq j$ se rovná 0;

$$\langle De_j, De_k\rangle = \left\langle \tau^{j(\varepsilon-j)}e_j, \tau^{k(\varepsilon-k)}e_k \right\rangle = \tau^{-j(\varepsilon-j)+k(\varepsilon-k)}\langle e_j, e_k\rangle$$
$$= \begin{Bmatrix} \text{pro } j=k: & =\tau^0 = 1 \\ \text{pro } j\neq k: & =0 \end{Bmatrix} = \langle e_j, e_k\rangle.$$

Odtud podle Poznámky 1.9 plyne, že oba operátory jsou unitární. □

Tvrzení 2.8. Řád operátoru S_n je pro $n = 2$ roven 2 a pro $n > 2$ roven 4.

Důkaz. $\forall j, m \in \{0, 1, \ldots, n-1\}$:

$$\langle e_m, S^2 e_j\rangle = \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\omega^{kj}\langle e_m, Se_k\rangle = \frac{1}{n}\sum_{k=0}^{n-1}\omega^{kj}\sum_{l=0}^{n-1}\omega^{lk}\langle e_m, e_l\rangle = \frac{1}{n}\sum_{k=0}^{n-1}\omega^{kj}\omega^{km}$$
$$= \frac{1}{n}\sum_{k=0}^{n-1}\omega^{k(j+m)} \overset{(a)}{=} \langle e_m, e_{n-j}\rangle,$$

kde rovnost (a) plyne z Poznámky 2.6 (stačí dosadit $p = j + m$).

Odtud plyne: $\forall j \in \{0, 1, \ldots, n-1\}$:

$$S^2 e_j = e_{n-j}, \tag{2.3}$$

a dále

$$S^4 e_j = S^2 e_{n-j} = e_j. \tag{2.4}$$

Ukázali jsme, že $S_n^4 = \mathrm{I}$ pro libovolné n. Pokud dosadíme $n = 2$ do rovnosti (2.3), získáme:

$$S^2 e_0 = e_0, \quad S^2 e_1 = e_1,$$

neboli

$$S_2^2 = \mathrm{I}.$$ □

Tvrzení 2.9. Řád operátoru D_n je pro n liché roven n a pro n sudé roven $2n$.

Důkaz. $\forall j \in \{0, 1, \ldots, n-1\}, \varepsilon \in \{1, n\}$:

$$D^k e_j = \tau^{kj(\varepsilon-j)}e_j.$$

Hledáme k takové, aby platilo

$$\forall j: \ \tau^{kj(\varepsilon-j)} = 1. \tag{2.5}$$

1. Nejprve se podíváme na n liché (tj. $\varepsilon = 1$, τ je řádu n). Máme:

$$\forall j: \ kj(1-j) = 0 \pmod{n}. \tag{2.6}$$

Položíme $j = 2$, potom $2k = 0 \pmod{n}$. Odtud plyne (protože n je liché):

$$k = 0 \pmod{n}.$$

Snadno ověříme, že pokud $k = 0 \pmod{n}$, podmínka (2.6) je splněna pro každé $j \in \{0, 1, \ldots, n-1\}$.

2. Zbývá nám provést důkaz pro n sudé (tj. $\varepsilon = n$, τ je řádu $2n$). Víme:

$$\forall j: \ kj(n-j) = 0 \pmod{2n}. \tag{2.7}$$

Položíme $j = 1$, potom $k(n-1) = 0 \pmod{2n}$. Jelikož výraz $(n-1)$ je lichý, musí platit, že hledané k je sudé, (aby mohlo být dělitelné sudým číslem). Pro sudé k můžeme zjednodušit podmínku (2.7):

$$\forall j \ : kj^2 = 0 \pmod{2n}.$$

Opět dosadíme $j = 1$, a dostaneme:

$$k = 0 \pmod{2n}.$$

Je zřejmé, že takové k vyhovuje podmínce (2.7) pro každé $j \in \{0, 1, \ldots, n-1\}$.

□

Tvrzení 2.10. Operátory S_n, D_n patří do $\mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$.

Důkaz. Ukážeme, že platí následující vztahy:

$$SQS^{-1} = P, \qquad SPS^{-1} = Q^{-1}; \tag{2.8}$$

$$DQD^{-1} = Q, \qquad DPD^{-1} = \begin{cases} QP & \text{pro } n \text{ liché}, \\ \tau^{n+1} QP & \text{pro } n \text{ sudé}. \end{cases} \tag{2.9}$$

1. $SQS^{-1} = P \ \Leftrightarrow \ SQ = PS$.

Pro každé $j \in \{0, 1, \ldots, n-1\}$:

$$SQe_j = \omega^j Se_j = \frac{1}{\sqrt{n}} \omega^j \sum_{k=0}^{n-1} \omega^{kj} e_k = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \omega^{(k+1)j} e_k, \tag{2.10}$$

$$\begin{aligned} PSe_j &= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \omega^{kj} Pe_k = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \omega^{kj} e_{k-1} = \frac{1}{\sqrt{n}} \left(e_{n-1} + \sum_{k=1}^{n-1} \omega^{kj} e_{k-1} \right) \\ &= \frac{1}{\sqrt{n}} \left(e_{n-1} + \sum_{k=0}^{n-2} \omega^{(k+1)j} e_k \right) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \omega^{(k+1)j} e_k. \end{aligned} \tag{2.11}$$

Pravé strany (2.10) a (2.11) se rovnají, a tedy platí $SQ = PS$.

2. Vyjdeme z právě dokázaného vztahu $SQS^{-1} = P$, $\Rightarrow S^2QS^{-2} = SPS^{-1}$. Jelikož $S^4 = \mathrm{I}$, platí $S^{-2} = S^2$; potom $SPS^{-1} = S^2QS^2$.

   $\forall j \in \{0, 1 \ldots, n-1\}$:

   $$S^2QS^2e_j = S^2Qe_{n-j} = \omega^{-j}S^2e_{n-j} = \omega^{-j}e_j = Q^{-1}e_j.$$

   Ukázali jsme, že $SPS^{-1} = Q^{-1}$.

3. Pro každé $j \in \{0, 1, \ldots, n-1\}$:

   $$DQD^{-1}e_j = \omega^j e_j = Qe_j.$$

4. Pro každé $j \in \{0, 1, \ldots, n-1\}$, pro $\varepsilon \in \{1, n\}$:

   $$\begin{aligned} DPD^{-1}e_j &= \tau^{-j(\varepsilon-j)}DPe_j = \tau^{-j(\varepsilon-j)}De_{j-1} \\ &= \tau^{-j(\varepsilon-j)}\tau^{(j-1)(\varepsilon-(j-1))}\, e_{j-1} = \tau^{2j-\varepsilon-1}\, e_j = \omega^{j-1}\,\tau^{-\varepsilon+1}\, e_{j-1} \\ &= \begin{cases} \omega^{j-1}\, e_{j-1}, \\ \tau^{-n+1}\,\omega^{j-1}\, e_{j-1} = \tau^{n+1}\,\omega^{j-1}\, e_{j-1}, \end{cases} \end{aligned}$$

   $QPe_j = Qe_{j-1} = \omega^{j-1}\, e_{j-1}$.

   Odtud plyne, že pro n liché $DPD^{-1} = QP$ a pro n sudé $DPD^{-1} = \tau^{n+1}QP$.

□

Definice 2.11 (Cliffordova grupa)**.** Cliffordovu grupu $\mathcal{C}_n$ definujeme jako podgrupu grupy $\mathrm{U}(n)$ generovanou operátory Q_n, P_n, S_n a D_n, kde grupovou operací je skládání zobrazení:

$$\mathcal{C}_n = \langle Q_n, P_n, S_n, D_n \rangle.$$

Tvrzení 2.12. $\mathcal{C}_n \subset\subset \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$.

Důkaz. Víme, že $\mathcal{C}_n$ je podle definice grupa, $Q_n, P_n \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ a podle Tvrzení 2.10 také $S_n, D_n \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$. □

Tvrzení 2.13. $\Pi_n \subset\subset \mathcal{C}_n$.

Důkaz. Podle Definice 2.11 patří do $\mathcal{C}_n$ libovolné kombinace mocnin operátorů Q_n a P_n. Stačí tedy ukázat, že také $\tau_n\mathrm{I} \in \mathcal{C}_n$.

1. Pro n liché využijeme Tvrzení 1.14 – libovolnou mocninu τ_n lze zapsat jako nějakou mocninu ω_n, přesněji platí: $\tau_n = \omega_n^{\frac{n+1}{2}}$. Dále podle Tvrzení 1.10:

   $$\begin{aligned} P_nQ_n = \omega_nQ_nP_n. \iff P_nQ_nP_n^{-1}Q_n^{-1} = \omega_n\mathrm{I} \implies \\ \implies \left(P_nQ_nP_n^{-1}Q_n^{-1}\right)^{\frac{n+1}{2}} = \tau_n\mathrm{I}. \end{aligned}$$

   Tímto jsme ukázali, že $\tau_n\mathrm{I}$ patří do grupy $\mathcal{C}_n$.

2. Pro n sudé vyjdeme ze vztahu (2.9):

$$DPD^{-1} = \tau^{n+1}QP. \iff DPD^{-1}P^{-1}Q^{-1} = \tau^{n+1}\mathrm{I} \implies$$
$$\implies \left(DPD^{-1}P^{-1}Q^{-1}\right)^{n+1} = \tau^{(n+1)^2}\mathrm{I} = \tau^{n^2+2n+1}\,\mathrm{I} = \tau\mathrm{I},$$

a tedy operátor $\tau_n\mathrm{I}$ patří do $\mathcal{C}_n$. □

Tvrzení 2.14. $\Pi_n \triangleleft \mathcal{C}_n$.

Důkaz. Podle Poznámky 2.3 platí: $\Pi_n \triangleleft \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$. Odtud plyne:

$$\forall a \in \mathcal{C}_n \subset \mathcal{N}_{\mathrm{U}(n)}(\Pi_n),\ \forall p \in \Pi_n : apa^{-1} \in \Pi_n,$$

a proto je Π_n normální podgrupou grupy $\mathcal{C}_n$. □

Tvrzení 2.15. Pokud je n liché, platí:

$$\mathcal{C}_n = \langle S_n, D_n \rangle.$$

Důkaz. Ukážeme, že platí

$$Q_n = {S_n}^2 {D_n}^{n-1} {S_n}^2 D_n. \tag{2.12}$$

Pro každé $j \in \{0, 1, \ldots, n-1\}$ platí:

$$\begin{aligned} S^2D^{n-1}S^2De_j &= \tau^{j(1-j)}S^2D^{n-1}S^2e_j &&= \tau^{j(1-j)}S^2D^{n-1}e_{n-j} \\ &= \tau^{j(1-j)}\tau^{-(n-j)(1-(n-j))}S^2e_{n-j} &&= \tau^{j(1-j)}\tau^{j(1+j)}S^2e_{n-j} \\ &= \tau^{2j}e_j &&= \omega^j e_j \\ &= Qe_j \end{aligned}$$

Nyní ze známých vztahů $SQS^{-1} = P$ a $S^{-1} = S^3$ vyjádříme:

$$P = S^3D^{n-1}S^2DS^3.$$

Ukázali jsme, že operátory Q_n, P_n lze vyjádřit pomocí operátorů S_n a D_n, a proto $\langle Q_n, P_n, S_n, D_n \rangle = \langle S_n, D_n \rangle$. □

2.2 Normalizátor grupy Π_n

Podle článku [4] ukážeme, jak ke každému prvku $\mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ můžeme přiřadit matici z grupy $\mathrm{SL}(2, \mathbb{Z}_n)$ a dvojici čísel z okruhu $\mathbb{Z}_{2n}^2$, a jaké má toto přiřazení vlastnosti. Stejným způsobem lze přiřazení zavést také pro prvky grupy $\mathcal{C}_n$, toho se týká následující poznámka.

Poznámka 2.16. V Tvrzeních 2.22, 2.24, 2.25, 2.30, 2.32, Důsledku 2.26 a Lemmatu 2.34 můžeme předpoklad $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ zaměnit za předpoklad $X \in \mathcal{C}_n$, (neboť $\mathcal{C}_n \subset \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$).

Pro libovolný operátor $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ platí:

$$X\tau^l Q^j P^k X^{-1} \in \Pi_n.$$

Potom jistě existují α, β, a, b, c, d taková, že

$$XQX^{-1} = \tau^\alpha Q^a P^b\,, \tag{2.13}$$
$$XPX^{-1} = \tau^\beta Q^c P^d\,. \tag{2.14}$$

Poznámka 2.17. Prvek gupy $\mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ není konstantami α, β, a, b, c, d určen jednoznačně.

Nechť $X, Y \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$. Předpokládejme, že platí

$$XQX^{-1} = \tau^\alpha Q^a P^b = YQY^{-1}\,,$$
$$XPX^{-1} = \tau^\beta Q^c P^d = YPY^{-1}\,.$$

Potom

$$Y^{-1}XQ = QY^{-1}X,$$
$$Y^{-1}XP = PY^{-1}X.$$

Podle Lemmatu 1.28 a Poznámky 1.29 existuje $\delta \in \mathbb{C}, |\delta| = 1$ takové, že $Y^{-1}X = \delta\,\mathrm{I}$, neboli

$$X = \delta Y.$$

Definice 2.18. Označíme $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, $h = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.

Nechť $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ a nechť platí vztahy (2.13), (2.14).

1. Definujeme zobrazení $\Theta_1 : \mathcal{N}_{\mathrm{U}(n)}(\Pi_n) \to \mathbb{Z}_n^{2,2} : X \mapsto C$.
2. Definujeme zobrazení $\Theta_2 : \mathcal{N}_{\mathrm{U}(n)}(\Pi_n) \to \mathbb{Z}_{2n}^{2} : X \mapsto h$.

Poznámka ke značení 2.19. Až do konce této podkapitoly budeme automaticky předpokládat, pokud není uvedeno jinak, že složky h (resp. h') jsou označeny řeckými písmeny α, β (resp. α', β') a prvky matice C (resp. C') písmeny a, b, c, d (resp. a', b', c', d') tak, jak je to zavedeno v Definici 2.18.

Poznámka ke značení 2.20. Výrazem $\Theta(X) = (C, h)$ se rozumí:

$$\Theta_1(X) = C \quad \text{a} \quad \Theta_2(X) = h.$$

Poznámka 2.21. Pokud nás zajímají pouze prvky Cliffordovy grupy, můžeme zavést zúžení zobrazení Θ_1, Θ_2:

$$\Theta_1/_{\mathcal{C}_n} : \mathcal{C}_n \to \mathbb{Z}_n^{2,2} : X \mapsto C,$$
$$\Theta_2/_{\mathcal{C}_n} : \mathcal{C}_n \to \mathbb{Z}_{2n}^{2} : X \mapsto h.$$

Tvrzení 2.22. Nechť $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ a $\Theta(X) = (C, h)$. Potom pro libovolné $u_1, u_2 \in \mathbb{Z}_n$, $\delta \in \mathbb{Z}_{2n}$ platí:

$$X\,\tau^{\delta} Q^{u_1} P^{u_2}\, X^{-1} = \tau^{\varepsilon} Q^{v_1} P^{v_2}, \tag{2.15}$$

kde

$$\begin{aligned} v &= Cu \pmod n, \\ \varepsilon &= \delta + h^T u - \begin{pmatrix} ab \\ cd \end{pmatrix}^T u + u^T \begin{pmatrix} ab & 2bc \\ 0 & cd \end{pmatrix} u \pmod{2n}; \end{aligned}$$

kde $u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$, $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$.

Důkaz.

$$\begin{aligned} & X\,\tau^{\delta} Q^{u_1} P^{u_2}\, X^{-1} = \\ &= \tau^{\delta} \underbrace{XQX^{-1} \dots XQX^{-1}}_{u_1\text{-krát}} \underbrace{XPX^{-1} \dots XPX^{-1}}_{u_2\text{-krát}} \\ &= \tau^{\delta} (\tau^{\alpha} Q^a P^b)^{u_1} (\tau^{\beta} Q^c P^d)^{u_2} \\ &\overset{(a)}{=} \tau^{\delta+\alpha u_1+\beta u_2+abu_1(u_1-1)+cdu_2(u_2-1)}\, Q^{au_1} P^{bu_1}\, Q^{cu_2} P^{du_2} \\ &= \tau^{\delta+\alpha u_1+\beta u_2+abu_1(u_1-1)+cdu_2(u_2-1)}\, \omega^{bu_1 cu_2}\, Q^{au_1+cu_2} P^{bu_1+du_2} \\ &= \tau^{\delta+\alpha u_1+\beta u_2+abu_1(u_1-1)+cdu_2(u_2-1)+2bcu_1u_2}\, Q^{au_1+cu_2} P^{bu_1+du_2}, \end{aligned} \tag{2.16}$$

rovnost (a) plyne z Lemmatu 1.22.

Nakonec porovnáním pravých stran (2.15) a (2.16) získáme:

$$\begin{aligned} v &= \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} au_1 + cu_2 \\ bu_1 + du_2 \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = Cu \pmod n, \\ \varepsilon &= \delta + \alpha u_1 + \beta u_2 - abu_1 - cdu_2 + abu_1^2 + cdu_2^2 + 2bcu_1u_2 \\ &= \delta + \begin{pmatrix} \alpha \\ \beta \end{pmatrix}^T \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} - \begin{pmatrix} ab \\ cd \end{pmatrix}^T \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} + \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}^T \begin{pmatrix} ab & 2bc \\ 0 & cd \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \\ &= \delta + h^T u - \begin{pmatrix} ab \\ cd \end{pmatrix}^T u + u^T \begin{pmatrix} ab & 2bc \\ 0 & cd \end{pmatrix} u \pmod{2n}. \end{aligned}$$

□

Poznámka ke značení 2.23. Mějme libovolnou matici A rozměru $m \times m$. Označíme $\mathcal{V}_{\mathrm{diag}}(A) = \begin{pmatrix} A_{11} & A_{22} & \dots & A_{mm} \end{pmatrix}^T$.

Tvrzení 2.24. Nechť $X, X' \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$, $\Theta(X) = (C, h)$, $\Theta(X') = (C', h')$. Pokud $X'' = X'X$, $\Theta(X'') = (C'', h'')$, pak

$$C'' = C'C \pmod n, \tag{2.17}$$

$$h'' = h + C^T h' - C^T \begin{pmatrix} a'b' \\ c'd' \end{pmatrix} + \mathcal{V}_{\mathrm{diag}} \left(C^T \begin{pmatrix} a'b' & 2b'c' \\ 0 & c'd' \end{pmatrix} C \right) \pmod{2n}. \tag{2.18}$$

Důkaz.

$$X''QX''^{-1} = X'XQX^{-1}X'^{-1} = \tau^{\alpha} X'Q^{a}P^{b}X'^{-1} =$$
$$= \tau^{\left\{\alpha+h'^{T}\begin{pmatrix}a\\b\end{pmatrix}-\begin{pmatrix}a'b'\\c'd'\end{pmatrix}^{T}\begin{pmatrix}a\\b\end{pmatrix}+\begin{pmatrix}a\\b\end{pmatrix}^{T}\begin{pmatrix}a'b' & 2b'c'\\0 & c'd'\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}\right\}} Q^{a'a+c'b}P^{b'a+d'b},$$

v poslední rovnosti jsme využili Tvrzení 2.22. Stejným postupem získáme:

$$X''PX''^{-1} =$$
$$= \tau^{\left\{\beta+h'^{T}\begin{pmatrix}c\\d\end{pmatrix}-\begin{pmatrix}a'b'\\c'd'\end{pmatrix}^{T}\begin{pmatrix}c\\d\end{pmatrix}+\begin{pmatrix}c\\d\end{pmatrix}^{T}\begin{pmatrix}a'b' & 2b'c'\\0 & c'd'\end{pmatrix}\begin{pmatrix}c\\d\end{pmatrix}\right\}} Q^{a'c+c'd}P^{b'c+d'd}.$$

Potom

$$C'' = \begin{pmatrix}a'a+c'b & a'c+c'd\\ b'a+d'b & b'c+d'd\end{pmatrix} = \begin{pmatrix}a' & c'\\ b' & d'\end{pmatrix}\begin{pmatrix}a & c\\ b & d\end{pmatrix} = C'C\,,$$
$$h'' \overset{(a)}{=} \begin{pmatrix}\alpha\\\beta\end{pmatrix} + \begin{pmatrix}a & b\\ c & d\end{pmatrix}h' - \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}a'b'\\c'd'\end{pmatrix} + \mathcal{V}_{\mathrm{diag}}\left(C^{T}\begin{pmatrix}a'b' & 2b'c'\\0 & c'd'\end{pmatrix}C\right)$$
$$= h + C^{T}h' - C^{T}\begin{pmatrix}a'b'\\c'd'\end{pmatrix} + \mathcal{V}_{\mathrm{diag}}\left(C^{T}\begin{pmatrix}a'b' & 2b'c'\\0 & c'd'\end{pmatrix}C\right).$$

Rovnost (a) jsme získali využitím následujících vztahů:

$$\begin{pmatrix}a\\b\end{pmatrix} = \begin{pmatrix}a & c\\ b & d\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = C\begin{pmatrix}1\\0\end{pmatrix}, \qquad \begin{pmatrix}c\\d\end{pmatrix} = \begin{pmatrix}a & c\\ b & d\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = C\begin{pmatrix}0\\1\end{pmatrix},$$

a tedy

$$\begin{pmatrix}a\\b\end{pmatrix}^{T}\begin{pmatrix}a'b' & 2b'c'\\0 & c'd'\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}^{T}C^{T}\begin{pmatrix}a'b' & 2b'c'\\0 & c'd'\end{pmatrix}C\begin{pmatrix}1\\0\end{pmatrix} =$$
$$= \left[C^{T}\begin{pmatrix}a'b' & 2b'c'\\0 & c'd'\end{pmatrix}C\right]_{11},$$

$$\begin{pmatrix}c\\d\end{pmatrix}^{T}\begin{pmatrix}a'b' & 2b'c'\\0 & c'd'\end{pmatrix}\begin{pmatrix}c\\d\end{pmatrix} = \left[C^{T}\begin{pmatrix}a'b' & 2b'c'\\0 & c'd'\end{pmatrix}C\right]_{22}.$$

□

Tvrzení 2.25. Nechť $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$, $\Theta(X) = (C,h)$. Pak $\det(C) = 1 \pmod n$.

Důkaz.

$$XPQX^{-1} = XPX^{-1}XQX^{-1} = \tau^{\alpha+\beta}\,Q^{c}P^{d}\,Q^{a}P^{b} = \tau^{\alpha+\beta}\,\omega^{ad}\,Q^{a+c}P^{b+d}$$
$$= \omega\,XQPX^{-1} = \omega\,\tau^{\alpha+\beta}\,Q^{a}P^{b}\,Q^{c}P^{d} = \tau^{\alpha+\beta}\,\omega^{1+bc}\,Q^{a+c}P^{b+d}$$

Odtud:

$$\omega^{ad} Q^{a+c} P^{b+d} = \omega^{1+bc} Q^{a+c} P^{b+d}$$
$$(\omega^{ad} - \omega^{1+bc}) Q^{a+c} P^{b+d} = \mathrm{O}$$
$$\omega^{ad} = \omega^{1+bc}$$
$$ad = 1 + bc \pmod{n},$$

a tedy

$$\det(C) = ad - bc = 1 \pmod{n}. \qquad \square$$

Důsledek 2.26. Nechť $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$, $\Theta_1(X) = C$. Potom $C \in \mathrm{SL}(2, \mathbb{Z}_n)$.

Poznámka 2.27. Jinými slovy, zobrazení Θ_1 zobrazuje do $\mathrm{SL}(2, \mathbb{Z}_n)$:

$$\Theta_1 : \mathcal{N}_{\mathrm{U}(n)}(\Pi_n) \to \mathrm{SL}(2, \mathbb{Z}_n).$$

Stejně tak to platí i pro zúžení Θ_1:

$$\Theta_1/_{\mathcal{C}_n} : \mathcal{C}_n \to \mathrm{SL}(2, \mathbb{Z}_n).$$

Důsledek 2.28. Zobrazení Θ_1 je homomorfismus grup.

Důkaz. Využijeme Tvrzení 2.24: pro libovolné $X, X' \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ platí, že $\Theta_1(X'X) = C'C = \Theta_1(X')\Theta_1(X)$. $\square$

Poznámka 2.29. Zobrazení $\Theta_1/_{\mathcal{C}_n}$ je také homomorfismus.

Tvrzení 2.30. Nechť $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$. Potom $\Theta(X^{-1}) = (C', h')$, kde

$$C' = C^{-1} \pmod{n},$$
$$h' = -C^{-T} \left[h + \mathcal{V}_{\mathrm{diag}} \left(C^T \begin{pmatrix} -bd & 2bc \\ 0 & -ac \end{pmatrix} C \right) \right] + \begin{pmatrix} -bd \\ -ac \end{pmatrix} \pmod{2n}.$$

Poznámka 2.31. Z Tvrzení 2.25 plyne, že pro každé $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ je matice C regulární, a tedy existuje C^{-1};

$$C^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}. \tag{2.19}$$

Důkaz. Označíme $\tilde{X} = X^{-1}X$, $\Theta(\tilde{X}) = (\tilde{C}, \tilde{h})$. Všimneme si, že $\tilde{X} = \mathrm{I}$. Dále zřejmě platí:

$$\Theta(\tilde{X}) = \Theta(\mathrm{I}) = \left(\mathbb{I}, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right). \tag{2.20}$$

1. Podle (2.17) platí: $\tilde{C} = C'C \pmod{n}$, a současně podle (2.20) platí: $\tilde{C} = \mathbb{I}$. Dohromady máme:

$$C'C = \mathbb{I} \pmod{n}. \quad \Longrightarrow \quad C' = C^{-1} \pmod{n}.$$

2. Podle (2.18) platí:

$$\tilde{h} = h + C^T h' - C^T \begin{pmatrix} a'b' \\ c'd' \end{pmatrix} + \mathcal{V}_{\text{diag}} \left(C^T \begin{pmatrix} a'b' & 2b'c' \\ 0 & c'd' \end{pmatrix} C \right) \pmod{2n},$$

a současně podle (2.20) platí: $\tilde{h} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Dohromady máme:

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = h + C^T h' - C^T \begin{pmatrix} a'b' \\ c'd' \end{pmatrix} + \mathcal{V}_{\text{diag}} \left(C^T \begin{pmatrix} a'b' & 2b'c' \\ 0 & c'd' \end{pmatrix} C \right) \pmod{2n}.$$

Člen $C^T h'$ převedeme na levou stranu, a pak rovnici zleva vynásobíme maticí $(-C^{-T})$:

$$h' = -C^{-T} h + \begin{pmatrix} a'b' \\ c'd' \end{pmatrix} - C^{-T} \mathcal{V}_{\text{diag}} \left(C^T \begin{pmatrix} a'b' & 2b'c' \\ 0 & c'd' \end{pmatrix} C \right) \pmod{2n}. \tag{2.21}$$

Nyní využijeme 1. bod důkazu ($C' = C^{-1}$) a rovnost (2.19):

$$C' = \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = C^{-1};$$

odtud dosadíme za a', b', c',d' do (2.21):

$$h' = -C^{-T} h + \begin{pmatrix} -bd \\ -ac \end{pmatrix} - C^{-T} \mathcal{V}_{\text{diag}} \left(C^T \begin{pmatrix} -bd & 2bc \\ 0 & -ac \end{pmatrix} C \right) \pmod{2n}.$$

Malou úpravou již získáme požadovaný výsledek:

$$h' = -C^{-T} \left[h + \mathcal{V}_{\text{diag}} \left(C^T \begin{pmatrix} -bd & 2bc \\ 0 & -ac \end{pmatrix} C \right) \right] + \begin{pmatrix} -bd \\ -ac \end{pmatrix} \pmod{2n}.$$

□

Tvrzení 2.32. Nechť $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$, $\Theta(X) = (C, h)$. Potom platí:

$$h + (n-1) \begin{pmatrix} ab \\ cd \end{pmatrix} = 0 \pmod{2}. \tag{2.22}$$

Důkaz. Víme, že operátory Q, P jsou řádu n (podle Tvrzení 1.10), potom také XQX^{-1}, XPX^{-1} jsou řádu n:

$$(XQX^{-1})^n = XQX^{-1} \dots XQX^{-1} = XQ^n X^{-1} = XX^{-1} = \mathrm{I},$$

a stejně tak

$$(XPX^{-1})^n = \mathrm{I}.$$

Operátory XQX^{-1}, XPX^{-1} můžeme vyjádřit podle (2.13), (2.14) jako:

$$XQX^{-1} = \tau^{\alpha}\, Q^a P^b, \quad XPX^{-1} = \tau^{\beta}\, Q^c P^d;$$

potom

$$\mathrm{I} = (XQX^{-1})^n = (\tau^{\alpha}\, Q^a P^b)^n, \tag{2.23}$$

$$\mathrm{I} = (XPX^{-1})^n = (\tau^{\beta}\, Q^c P^d)^n. \tag{2.24}$$

Použijeme Lemma 1.22 na rozepsání pravé strany rovnice (2.23):

$$(\tau^{\alpha}\, Q^a P^b)^n = \tau^{\alpha n + ab\, n(n-1)}\, Q^{an} P^{bn} = \tau^{n(\alpha + ab\,(n-1))}\, \mathrm{I}\,. \tag{2.25}$$

Porovnáním (2.23) a (2.25) získáme:

$$\tau^{n(\alpha+ab\,(n-1))}\, \mathrm{I} = \mathrm{I}\,.$$
$$n(\alpha + ab\,(n-1)) = 0 \pmod{2n}$$
$$\alpha + ab\,(n-1) = 0 \pmod 2$$

Stejným postupem (s využitím rovnice (2.24)) získáme:

$$\beta + cd\,(n-1) = 0 \pmod 2.$$

Celkem máme: $h + (n-1)\begin{pmatrix} ab \\ cd \end{pmatrix} = 0 \pmod 2$. □

Poznámka ke značení 2.33. V následujícím textu se budeme několikrát odkazovat na podmínku (2.22). Její znění ovšem závisí na prvcích jisté matice (v případě Tvrzení 2.32 je to matice C); tuto závislost budeme značit následujícím způsobem:

Nechť $M \in \mathrm{SL}(2, \mathbb{Z}_n)$, (její prvek v i-tém řádku a j-tém sloupci označíme M_{ij}). Pokud řekneme, že nějaké $g \in \mathbb{Z}_{2n}^2$ splňuje podmínku $(2.22)(M)$, je tím myšleno, že platí:

$$g + (n-1)\begin{pmatrix} M_{11}M_{21} \\ M_{12}M_{22} \end{pmatrix} = 0 \pmod 2.$$

Lemma 2.34. Nechť $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$, $\Theta(X) = (C, h)$. Potom platí:

1. $\Theta(XQ) = (C, h')$, kde $h' = \begin{pmatrix} \alpha \\ \beta - 2 \end{pmatrix} \pmod{2n}$;
2. $\Theta(XP) = (C, h')$, kde $h' = \begin{pmatrix} \alpha + 2 \\ \beta \end{pmatrix} \pmod{2n}$;
3. $\Theta(XQ^{\gamma}P^{\delta}) = (C, h')$, kde $h' = \begin{pmatrix} \alpha + 2\delta \\ \beta - 2\gamma \end{pmatrix} \pmod{2n}$.

Důkaz. 1. Abychom získali $\Theta(XQ)$, podíváme se, jak operátor XQ konjugovaně působí na operátory Q a P:

$$\begin{aligned} XQ\,Q\,(XQ)^{-1} &= XQ\,Q\,Q^{-1}X^{-1} &= XQX^{-1} &= \tau^{\alpha}\,Q^{a}P^{b}, \\ XQ\,P\,(XQ)^{-1} &= XQ\,P\,Q^{-1}X^{-1} &= \omega^{-1}XPX^{-1} &= \tau^{\beta-2}\,Q^{c}P^{d}. \end{aligned}$$

Těmito vztahy jsou (podle Definice 2.18) $\Theta_1(X)$ a $\Theta_2(X)$ již určeny.

2. Budeme postupovat stejně jako v 1. části důkazu:

$$\begin{aligned} XP\,Q\,(XP)^{-1} &= XP\,Q\,P^{-1}X^{-1} &= \omega XQX^{-1} &= \tau^{\alpha+2}\,Q^{a}P^{b}, \\ XP\,P\,(XP)^{-1} &= XP\,P\,P^{-1}X^{-1} &= XPX^{-1} &= \tau^{\beta}\,Q^{c}P^{d}. \end{aligned}$$

3. Důsledek 1. a 2. bodu.

□

Tvrzení 2.35. Nechť $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$, $\Theta_1(X) = C$. Potom k libovolnému $\tilde{h} \in \mathbb{Z}_{2n}^2$ vyhovujícímu podmínce (2.22)(C) existuje $\tilde{X} \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ takové, že $\Theta(\tilde{X}) = (C, \tilde{h})$.

Důkaz. Označíme $g = \Theta_2(X)$. Z Tvrzení 2.32 víme, že g musí vyhovovat podmínce (2.22)(C):

$$g + (n-1)\begin{pmatrix} ab \\ cd \end{pmatrix} = 0 \pmod 2.$$

Nyní uvažujme libovolné $\tilde{h} \in \mathbb{Z}_{2n}^2$ splňující (2.22)(C):

$$\tilde{h} + (n-1)\begin{pmatrix} ab \\ cd \end{pmatrix} = 0 \pmod 2.$$

Odečtením obou rovnic dostaneme:

$$\tilde{h} - g = 0 \pmod 2.$$

Zjistili jsme, že $\tilde{h}$ musí splňovat:

$$\tilde{h} = g + \begin{pmatrix} 2k_1 \\ 2k_2 \end{pmatrix}, \quad k_1, k_2 \in \mathbb{Z}\,. \tag{2.26}$$

Pro libovolné $\tilde{h}$ splňující (2.26) položíme

$$\tilde{X} = XQ^{-k_2}P^{k_1}.$$

Určitě platí, že $\tilde{X} \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$. Využijeme 3. bod Lemmatu 2.34, a získáme: $\Theta_1(\tilde{X}) = C,\ \Theta_2(\tilde{X}) = g + \begin{pmatrix} 2k_1 \\ 2k_2 \end{pmatrix}$. □

Poznámka 2.36. Předpokládejme, že $X \in \mathcal{C}_n$, $\Theta_1(X) = C$. Potom k libovolnému $\tilde{h} \in \mathbb{Z}_{2n}^2$ vyhovujícímu podmínce (2.22)(C) existuje $\tilde{X} \in \mathcal{C}_n$ takové, že $\Theta(\tilde{X}) = (C, \tilde{h})$.

Podle důkazu Tvrzení 2.35 totiž platí: $\tilde{X} = XQ^{-k_2}P^{k_1} \in \mathcal{C}_n$.

Lemma 2.37. $\mathrm{SL}(2, \mathbb{Z}_n) = \langle A, B \rangle$, kde $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Důkaz. Důkaz provedeme podle [2].

Označíme $C = A^T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Platí:

$$C = B^3 A^{n-1} B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & n-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Libovolný prvek $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}_n)$ můžeme rozepsat následovně:

$$\begin{aligned} \begin{pmatrix} a & c \\ b & d \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & c \\ b-a & d-c \end{pmatrix} &&= C \begin{pmatrix} a & c \\ b-a & d-c \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a-b & c-d \\ b & d \end{pmatrix} &&= A \begin{pmatrix} a-b & c-d \\ b & d \end{pmatrix}. \end{aligned}$$

Nyní použijeme Eukleidův algoritmus na hledání největšího společného dělitele dvou celých čísel. V našem případě budeme hledat největší společný dělitel čísel a, b – označíme jej písmenem s. Nechť např. $b \geq a$, pak existují $k_1, b_1 \in \mathbb{N}_0$, $b_1 < a$ takové, že $b = k_1 a + b_1$. Dále postupujeme podle Eukleidova algoritmu:

$$\begin{gathered} b = k_1 a + b_1 \\ a = l_1 b_1 + a_1 \\ b_1 = k_2 a_1 + b_2 \\ a_1 = l_2 b_2 + a_2 \\ \vdots \\ \swarrow \quad \searrow \\ b_{p-1} = k_p\, s + 0 \qquad b_{p-1} = k_p a_{p-1} + s \\ \qquad\qquad\qquad\quad a_{p-1} = l_p\, s + 0 \end{gathered},$$

kde $p \in \mathbb{N}$, $\forall i \in \{1, \ldots, p\} : k_i, l_i \in \mathbb{N}_0$; $b_1 > a_1 > \cdots > b_{p-1} > a_{p-1} > 0$.

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} = C \begin{pmatrix} a & c \\ b-a & d-c \end{pmatrix} = C^{k_1} \begin{pmatrix} a & c \\ b-k_1a & d-k_1c \end{pmatrix} = C^{k_1} \begin{pmatrix} a & c \\ b_1 & d-k_1c \end{pmatrix} =$$
$$= C^{k_1} A \begin{pmatrix} a-b_1 & c(1+k_1)-d \\ b_1 & d-k_1c \end{pmatrix} = C^{k_1} A^{l_1} \begin{pmatrix} a_1 & c(1+l_1k_1)-l_1d \\ b_1 & d-k_1c \end{pmatrix} =$$
$$= \cdots = \begin{cases} C^{k_1} A^{l_1} \dots C^{k_p} \begin{pmatrix} s & t \\ 0 & u \end{pmatrix} = C^{k_1} A^{l_1} \dots C^{k_p} T_1, \\ \\ C^{k_1} A^{l_1} \dots C^{k_p} A^{l_p} \begin{pmatrix} 0 & v \\ s & w \end{pmatrix} = C^{k_1} A^{l_1} \dots C^{k_p} A^{l_p} T_2, \end{cases} \tag{2.27}$$

kde $t, u, v, w \in \mathbb{Z}_n$. Dále musí platit: $\det T_1 = su = \det T_2 = -sv = 1 (\mathrm{mod}\, n)$, (protože A, C patří do $\mathrm{SL}(2, \mathbb{Z}_n)$ a matice na levé straně rovnosti (2.27) také).

Nyní ukážeme, že libovolnou matici typu T_1 nebo T_2 lze vyjádřit pomocí matic A, B, C. Platí:

$$\begin{pmatrix} s & t \\ 0 & u \end{pmatrix} = A^{s(t-1)} C^u B^3 C^s \,. \tag{2.28}$$

Ověření:

$$\begin{aligned} A^{s(t-1)} C^u B^3 C^s &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{s(t-1)} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^u \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^s \\ &= \begin{pmatrix} 1 & s(t-1) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1+su(t-1) & s(t-1) \\ u & 1 \end{pmatrix} \begin{pmatrix} s & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} ts-s(t-1) & t \\ su-1 & u \end{pmatrix} = \begin{pmatrix} s & t \\ 0 & u \end{pmatrix}. \end{aligned}$$

Dále platí:

$$\begin{pmatrix} 0 & v \\ s & w \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} s & w \\ 0 & -v \end{pmatrix} = B \begin{pmatrix} s & w \\ 0 & -v \end{pmatrix},$$

odtud s využitím vztahu (2.28) dostaneme:

$$\begin{pmatrix} 0 & v \\ s & w \end{pmatrix} = B A^{s(w-1)} C^{-v} B^3 C^s \,.$$

Dokázali jsme, že libovolnou matici z $\mathrm{SL}(2, \mathbb{Z}_n)$ lze rozepsat na součin matic A a B, a proto A, B grupu $\mathrm{SL}(2, \mathbb{Z}_n)$ generují. □

Poznámka 2.38. Podle vztahů (2.8), (2.9) určíme obraz operátorů S a D při zobrazení Θ_1:

$$\Theta_1(S) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = B, \qquad \Theta_1(D) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = A.$$

Tvrzení 2.39. Zobrazení Θ_1 je epimorfismus.

Důkaz. Již víme, že zobrazení Θ_1 je homomorfismus, stačí tedy ukázat, že Θ_1 je surjektivní. Chceme ukázat: $\forall M \in \mathrm{SL}(2,\mathbb{Z}_n),\ \exists X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n) :\ \Theta_1(X) = M$.

Podle Lemmatu 2.37 můžeme libovolné $M \in \mathrm{SL}(2,\mathbb{Z}_n)$ vyjádřit jako součin matic $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ a $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, tj. $M = A^{j_1}B^{k_1}A^{j_2}B^{k_2}\ldots A^{j_m}B^{j_m}$, kde $\forall i \in \{1,2,\ldots,m\} : j_i, k_i \in \mathbb{Z}$.

Položíme $X = D^{j_1}S^{k_1}\ldots D^{j_m}S^{k_m}$. Pak

$$\begin{aligned} \Theta_1(X) \quad &= \Theta_1(D^{j_1}S^{k_1}\ldots D^{j_m}S^{k_m}) \quad &&= \Theta_1(D)^{j_1}\Theta_1(S)^{k_1}\ldots\Theta_1(D)^{j_m}\Theta_1(S)^{k_m} \\ &= A^{j_1}B^{k_1}\ldots A^{j_m}B^{j_m} \quad &&= M. \end{aligned}$$

□

Poznámka 2.40. Z důkazu Tvrzení 2.39 vyplývá, že ke každému $M \in \mathrm{SL}(2,\mathbb{Z}_n)$ najdeme $X \in \mathcal{C}_n$ takové, že $\Theta_1(X) = M$. (Nalezené X lze vyjádřit pomocí operátorů S a D, a proto náleží do Cliffordovy grupy $\mathcal{C}_n$.)

Tudíž platí, že zobrazení

$$\Theta_1/_{\mathcal{C}_n} : \mathcal{C}_n \to \mathrm{SL}(2,\mathbb{Z}_n) \text{ je epimorfismus.}$$

Důsledek 2.41. Ke každé matici $M \in \mathrm{SL}(2,\mathbb{Z}_n)$ a ke každému $g \in \mathbb{Z}_{2n}^2$ splňujícímu podmínku $(2.22)(M)$ existuje operátor $X \in \mathcal{C}_n$ takový, že $\Theta(X) = (M,g)$.

Důkaz. Podle Poznámky 2.40 najdeme $X' \in \mathcal{C}_n$ takové, že $\Theta_1(X') = M$; a podle Poznámky 2.36 najdeme $X \in \mathcal{C}_n$ takové, že $\Theta(X) = (M,g)$. □

Tvrzení 2.42. Ke každému prvku $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$ existují konstanta $\gamma \in \mathbb{C}$, $|\gamma| = 1$ a prvek $Y \in \mathcal{C}_n$ takové, že $X = \gamma Y$.

Důkaz. Mějme libovolné $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$, označíme $C = \Theta_1(X)$, $h = \Theta_2(X)$; (víme tedy, že h splňuje podmínku $(2.22)(C)$). Podle Důsledku 2.41 existuje operátor $Y \in \mathcal{C}_n$ takový, že $\Theta(Y) = (C,h)$. Platí tedy: $\Theta(X) = \Theta(Y)$.

Pak podle Poznámky 2.17 existuje $\gamma \in \mathbb{C}, |\gamma| = 1$ takové, že $X = \gamma Y$. □

2.3 Normalizátor grupy $\mathcal{P}_n$

Poznámka ke značení 2.43. Označíme $\mathcal{M}(n)$ grupu obsahující všechny vnitřní automorfismy Ad_A grupy $\mathrm{GL}(\mathcal{H}_n)$ takové, že $A \in \mathrm{U}(n)$.

Nyní se budeme zabývat normalizátorem grupy $\mathcal{P}_n$ v grupě $\mathcal{M}(n)$. Připomeňme, že z definice normalizátoru plyne, že pro libovolný prvek $\psi \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$ a libovolný prvek $\alpha \in \mathcal{P}_n$ platí:

$$\psi\,\alpha\,\psi^{-1} \in \mathcal{P}_n\,;$$

a tedy také existují čísla $a,b,c,d \in \mathbb{Z}_n$ taková, že

$$\psi\,\mathrm{Ad}_Q\,\psi^{-1} = \mathrm{Ad}_{Q^aP^b}\,, \tag{2.29}$$

$$\psi\,\mathrm{Ad}_P\,\psi^{-1} = \mathrm{Ad}_{Q^cP^d}\,. \tag{2.30}$$

Tvrzení 2.44. $\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)/\mathcal{P}_n \cong \mathrm{SL}(2,\mathbb{Z}_n)$.

Důkaz. Důkaz provedeme podle [2].

1. Definujeme zobrazení $\Phi : \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n) \to \mathrm{SL}(2,\mathbb{Z}_n)$ následovně:

$$\forall \psi \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n) : \ \Phi(\psi) = \begin{pmatrix} a & c \\ b & d \end{pmatrix},$$

kde a, b, c, d jsou určeny vztahy (2.29) a (2.30).

2. Ukážeme, že zobrazení Φ je dobře definované, tj. že obraz $\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$ při zobrazení Φ je podmnožinou $\mathrm{SL}(2,\mathbb{Z}_n)$. Stačí ověřit podmínku:

$$\forall \psi \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n) \text{ platí: } \quad \det(\Phi(\psi)) = \det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = ad - bc = 1 \,(\mathrm{mod}\, n).$$

Nechť $A \in \mathrm{U}(n)$, označíme $\psi = \mathrm{Ad}_A$.

Nechť $\Phi(\mathrm{Ad}_A) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, pak platí:

$$\mathrm{Ad}_A \mathrm{Ad}_Q \mathrm{Ad}_A^{-1} = \mathrm{Ad}_{AQA^{-1}} = \mathrm{Ad}_{Q^a P^b},$$
$$\mathrm{Ad}_A \mathrm{Ad}_P \mathrm{Ad}_A^{-1} = \mathrm{Ad}_{APA^{-1}} = \mathrm{Ad}_{Q^c P^d}.$$

Odtud plyne podle 4. bodu Tvrzení 1.30

$$AQA^{-1} = \alpha Q^a P^b, \tag{2.31}$$
$$APA^{-1} = \beta Q^c P^d, \tag{2.32}$$

kde $\alpha, \beta \in \mathbb{C} \setminus \{0\}$.

Z rovnic (2.31), (2.32) plyne:

$$AQA^{-1}APA^{-1} = \alpha\beta Q^a P^b Q^c P^d$$
$$AQPA^{-1} = \alpha\beta \omega^{cb} Q^{a+c} P^{b+d}$$
$$APA^{-1}AQA^{-1} = \alpha\beta Q^c P^d Q^a P^b$$
$$APQA^{-1} = \alpha\beta \omega^{ad} Q^{a+c} P^{b+d}.$$

Dále platí:

$$APQA^{-1} = \omega AQPA^{-1}$$
$$\alpha\beta\omega^{ad} Q^{a+c} P^{b+d} = \alpha\beta\omega^{1+cb} Q^{a+c} P^{b+d}$$
$$(\omega^{ad} - \omega^{1+bc}) Q^{a+c} P^{b+d} = \mathrm{O}$$
$$\iff \omega^{ad} = \omega^{1+bc} \iff ad = 1 + bc \,(\mathrm{mod}\, n) \iff ad - bc = 1 \,(\mathrm{mod}\, n).$$

Ukázali jsme, že pro každé $\psi \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$ platí $\Phi(\psi) \in \mathrm{SL}(2,\mathbb{Z}_n)$, a tedy zobrazení Φ je dobře definované.

3. Ukážeme, že $\Phi : \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n) \to \mathrm{SL}(2,\mathbb{Z}_n)$ je homomorfismus grup.
   Nechť $\psi_1, \psi_2 \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$. Zajímá nás, jestli platí: $\Phi(\psi_1 \circ \psi_2) = \Phi(\psi_1)\Phi(\psi_2)$.
   Předpokládejme, že $\Phi(\psi_j) = \begin{pmatrix} a_j & c_j \\ b_j & d_j \end{pmatrix}$, $j \in \{1,2\}$.

$$
\begin{aligned}
&(\psi_1\psi_2)\mathrm{Ad}_Q(\psi_1\psi_2)^{-1} = \\
&= \psi_2(\psi_1 \mathrm{Ad}_Q \psi_1^{-1})\psi_2^{-1} = \psi_2\, \mathrm{Ad}_{Q^{a_1}P^{b_1}}\, \psi_2^{-1} = \psi_2\, \mathrm{Ad}_{Q^{a_1}} \mathrm{Ad}_{P^{b_1}} \psi_2^{-1} = \\
&= \underbrace{\psi_2\, \mathrm{Ad}_Q\, \psi_2^{-1} \ldots \psi_2\, \mathrm{Ad}_Q\, \psi_2^{-1}}_{a_1-\text{krát}} \underbrace{\psi_2\, \mathrm{Ad}_P\, \psi_2^{-1} \ldots \psi_2\, \mathrm{Ad}_P\, \psi_2^{-1}}_{b_1-\text{krát}} = \\
&= (\mathrm{Ad}_{Q^{a_2}P^{b_2}})^{a_1} (\mathrm{Ad}_{Q^{c_2}P^{d_2}})^{b_1} = \mathrm{Ad}_{(Q^{a_2}P^{b_2})^{a_1}} \mathrm{Ad}_{(Q^{c_2}P^{d_2})^{b_1}} = \\
&= \mathrm{Ad}_{(Q^{a_2}P^{b_2})^{a_1}(Q^{c_2}P^{d_2})^{b_1}} = \mathrm{Ad}_{Q^{a_1a_2+b_1c_2}P^{a_1b_2+b_1d_2}}
\end{aligned}
$$

$$
\begin{aligned}
&(\psi_1\psi_2)\mathrm{Ad}_P(\psi_1\psi_2)^{-1} = \\
&\qquad = \psi_2(\psi_1\, \mathrm{Ad}_P\, \psi_1^{-1})\psi_2^{-1} && = \psi_2\, \mathrm{Ad}_{Q^{c_1}P^{d_1}}\, \psi_2^{-1} \\
&\qquad = (\mathrm{Ad}_{Q^{a_2}P^{b_2}})^{c_1} (\mathrm{Ad}_{Q^{c_2}P^{d_2}})^{d_1} && = \mathrm{Ad}_{(Q^{a_2}P^{b_2})^{c_1}(Q^{c_2}P^{d_2})^{d_1}} \\
&\qquad = \mathrm{Ad}_{Q^{c_1a_2+d_1c_2}\, P^{c_1b_2+d_1d_2}}
\end{aligned}
$$

   Odtud plyne, že $\Phi(\psi_1 \circ \psi_2) = \begin{pmatrix} a_1a_2 + c_1b_2 & a_1c_2 + c_1d_2 \\ b_1a_2 + d_1b_2 & b_1c_2 + d_1d_2 \end{pmatrix}$.
   Zároveň platí:

$$\Phi(\psi_1)\Phi(\psi_2) = \begin{pmatrix} a_1 & c_1 \\ b_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & c_2 \\ b_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + c_1b_2 & a_1c_2 + c_1d_2 \\ b_1a_2 + d_1b_2 & b_1c_2 + d_1d_2 \end{pmatrix},$$

   a tedy $\Phi(\psi_1 \circ \psi_2) = \Phi(\psi_1)\Phi(\psi_2)$, a Φ je homomorfismus.

4. Definujeme zobrazení $\tilde{\Phi} : \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)/\mathcal{P}_n \to \mathrm{SL}(2,\mathbb{Z}_n)$ následovně:

$$\forall [\psi] \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)/\mathcal{P}_n : \ \tilde{\Phi}([\psi]) = \Phi(\psi),$$

   kde $\psi \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$, $[\psi] = \psi\mathcal{P}_n$ je třída ekvivalence v grupě $\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$.

5. Ověříme, že $\tilde{\Phi}$ je opravdu zobrazení.
   Potřebujeme ukazát, že $\forall \psi, \chi \in \mathcal{N}_{\mathcal{M}}(\mathcal{P}_n)$ platí: $\chi \sim \psi \Rightarrow \Phi(\chi) = \Phi(\psi)$.
   Nechť $\chi \sim \psi$.

$$
\begin{gathered}
\chi \sim \psi \ \Leftrightarrow \ \chi \in \psi\mathcal{P}_n \ \Leftrightarrow \ \exists a, b \in \{0, 1, \ldots, n-1\} : \ \chi = \psi \mathrm{Ad}_{Q^aP^b}\,; \\
\Phi(\chi) = \Phi(\psi \mathrm{Ad}_{Q^aP^b}) = \Phi(\psi)\Phi(\mathrm{Ad}_{Q^aP^b}) = \Phi(\psi),
\end{gathered}
$$

   kde poslední rovnost plyne z komutativity grupy $\mathcal{P}_n$, neboť:

$$\forall \xi \in \mathcal{P}_n : \ \xi\, \mathrm{Ad}_Q\, \xi^{-1} = \mathrm{Ad}_Q, \ \xi\, \mathrm{Ad}_P\, \xi^{-1} = \mathrm{Ad}_P, \text{ tudíž } \Phi(\mathrm{Ad}_{Q^aP^b}) = \mathbb{I}.$$

6. Jelikož Φ je homomorfismus, je také $\tilde{\Phi}$ homomorfismus.

7. Ukážeme, že $\tilde{\Phi}$ je prosté zobrazení.

   Mějme libovolné $\psi, \chi \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$,

   $$\begin{aligned} &\tilde{\Phi}([\psi]) = \tilde{\Phi}([\chi]) \iff \\ \iff &\begin{matrix} \psi \operatorname{Ad}_Q \psi^{-1} = \chi \operatorname{Ad}_Q \chi^{-1} \\ \psi \operatorname{Ad}_P \psi^{-1} = \chi \operatorname{Ad}_P \chi^{-1} \end{matrix} \iff \begin{matrix} \chi^{-1}\psi \operatorname{Ad}_Q = \operatorname{Ad}_Q \chi^{-1}\psi \\ \chi^{-1}\psi \operatorname{Ad}_P = \operatorname{Ad}_P \chi^{-1}\psi \end{matrix} \end{aligned}$$

   Označíme $\chi^{-1}\psi = \operatorname{Ad}_X$. Podle Tvrzení 1.30:

   $$\begin{matrix} \operatorname{Ad}_X \operatorname{Ad}_Q = \operatorname{Ad}_Q \operatorname{Ad}_X \\ \operatorname{Ad}_X \operatorname{Ad}_P = \operatorname{Ad}_P \operatorname{Ad}_X \end{matrix} \iff \begin{matrix} QX = \alpha XQ \\ PX = \beta XP \end{matrix},$$

   kde $\alpha, \beta \in \mathbb{C} \setminus \{0\}$.

   Z Lemmatu 1.27 a Poznámky 1.29 plyne, že existují $\gamma \in \mathbb{C}, |\gamma| = 1$ a $Y \in \Pi_n$ tak, že platí $X = \gamma Y$, a tedy

   $$\chi^{-1}\psi = \operatorname{Ad}_X = \operatorname{Ad}_{\gamma Y} = \operatorname{Ad}_Y \in \mathcal{P}_n \quad \iff \quad \psi \sim \chi \quad \iff \quad [\psi] = [\chi].$$

8. Ukážeme, že $\tilde{\Phi}$ je surjektivní.

   Využijeme známé vztahy (2.8), (2.9) pro operátory S_n a D_n. Platí:

   $$\begin{aligned} \operatorname{Ad}_S \operatorname{Ad}_Q \operatorname{Ad}_S^{-1} &= \operatorname{Ad}_{SQS^{-1}} &&= \operatorname{Ad}_P\,, \\ \operatorname{Ad}_S \operatorname{Ad}_P \operatorname{Ad}_S^{-1} &= \operatorname{Ad}_{SPS^{-1}} &&= \operatorname{Ad}_{Q^{-1}}\,, \\ \operatorname{Ad}_D \operatorname{Ad}_Q \operatorname{Ad}_D^{-1} &= \operatorname{Ad}_{DQD^{-1}} &&= \operatorname{Ad}_Q\,, \\ \operatorname{Ad}_D \operatorname{Ad}_P \operatorname{Ad}_D^{-1} &= \operatorname{Ad}_{DPD^{-1}} &&= \operatorname{Ad}_{QP}\,; \end{aligned}$$

   čímž jsme ukázali, že $\operatorname{Ad}_S, \operatorname{Ad}_D \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$.

   Dále platí, že

   $$\begin{aligned} \tilde{\Phi}([\operatorname{Ad}_S]) &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = B, \\ \tilde{\Phi}([\operatorname{Ad}_D]) &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = A. \end{aligned} \tag{2.33}$$

   Podle Lemmatu (2.37) lze libovolnou matici $M \in \mathrm{SL}(2, \mathbb{Z}_n)$ vyjádřit jako součin matic A a B: $M = A^{j_1}B^{k_1} \ldots A^{j_m}B^{k_m}$, a podle (2.33) existuje $\psi \in \mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$ ($\psi = \operatorname{Ad}_D^{j_1}\operatorname{Ad}_S^{k_1} \ldots \operatorname{Ad}_D^{j_m}\operatorname{Ad}_S^{k_m}$) takové, že $\tilde{\Phi}([\psi]) = M$. Tímto jsme dokázali, že $\tilde{\Phi}$ je surjektivní.

9. Závěr: zobrazení $\tilde{\Phi}$ je izomorfismus mezi $\mathrm{SL}(2, \mathbb{Z}_n)$ a $\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)/\mathcal{P}_n$.

□

Poznámka 2.45. Z důkazu Tvrzení 2.44 plyne, že libovolný prvek $\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)/\mathcal{P}_n$ lze vyjádřit jako nějaký součin $[\mathrm{Ad}_S]$ a $[\mathrm{Ad}_D]$, a tedy libovolný prvek grupy $\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)$ lze zapsat jako nějaké složení prvků $\mathrm{Ad}_S, \mathrm{Ad}_D, \mathrm{Ad}_Q, \mathrm{Ad}_P$:

$$\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n) = \langle \mathrm{Ad}_S, \mathrm{Ad}_D, \mathrm{Ad}_Q, \mathrm{Ad}_P \rangle.$$

Poznámka ke značení 2.46. V následujících tvrzeních budeme předpokládat, že

$$n = \prod_{i=1}^{r} p_i^{k_i},$$

kde $\forall i, j \in \{1, 2, \ldots, r\}$ platí: p_i je prvočíslo, $p_i \neq p_j$, $k_i \in \mathbb{N}$.

Tvrzení 2.47 ([6])**.** Nechť $m, p, q \in \{2, 3, 4, \ldots\}$, p, q jsou nesoudělná. Pak

$$\mathrm{SL}(m, \mathbb{Z}_{pq}) \cong \mathrm{SL}(m, \mathbb{Z}_p) \times \mathrm{SL}(m, \mathbb{Z}_q).$$

Důsledek 2.48. $\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)/\mathcal{P}_n \cong \mathrm{SL}(2, \mathbb{Z}_{p_1^{k_1}}) \times \mathrm{SL}(2, \mathbb{Z}_{p_2^{k_2}}) \times \cdots \times \mathrm{SL}(2, \mathbb{Z}_{p_r^{k_r}})$.

Důkaz. Jelikož pro každé i, j jsou p_i, p_j vzájemně různá prvočísla, jsou čísla $p_i^{k_i}, p_j^{k_j}$ nesoudělná, a proto můžeme aplikovat Tvrzení 2.47. □

V [6] je dokázán vzorec pro řád grupy $\mathrm{SL}(m, \mathbb{Z}_n)$ pro libovolná m, n. Zde jej uvedeme pouze pro případ $m = 2$.

Tvrzení 2.49 ([6])**.** $|\mathrm{SL}(2, \mathbb{Z}_n)| = n^3 \prod_{j=1}^{r} \left(1 - \frac{1}{p_j^2}\right)$.

Důsledek 2.50. $|\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)/\mathcal{P}_n| = n^3 \prod_{j=1}^{r} \left(1 - \frac{1}{p_j^2}\right)$.

Důsledek 2.51. $|\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)| = n^5 \prod_{j=1}^{r} \left(1 - \frac{1}{p_j^2}\right)$.

Důkaz. Podle Lagrangeovy věty platí:

$$|\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)| = |\mathcal{P}_n| \; |\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)/\mathcal{P}_n| = n^2 \; |\mathcal{N}_{\mathcal{M}(n)}(\mathcal{P}_n)/\mathcal{P}_n|,$$

v poslední rovnosti jsme využili Tvrzení 1.33. □

Příklad 2.52.

1. $|\mathcal{N}_{\mathcal{M}(2)}(\mathcal{P}_2)| = 2^5 \, \frac{3}{4} = 24$;
2. $|\mathcal{N}_{\mathcal{M}(3)}(\mathcal{P}_3)| = 3^5 \, \frac{8}{9} = 216$.

Kapitola 3

Výpočet Cliffordových grup pro $n = 2$ a $n = 3$

Nejprve uvedeme několik poznámek pro libovolné $n \in \{2, 3, 4, \dots\}$.

Poznámka 3.1. Nechť $Z \in \Pi_n$, $\gamma \in \mathbb{C} \setminus \{0\}$. Potom platí:

$$\gamma Z Q \gamma^{-1} Z^{-1} = Z Q Z^{-1} = \omega^{l_1} Q,$$
$$\gamma Z P \gamma^{-1} Z^{-1} = Z P Z^{-1} = \omega^{l_2} P,$$

kde l_1, l_2 jsou nějaká čísla z množiny $\{0, 1, \dots, n-1\}$.

Odtud plyne:

$$\Theta_1(\gamma Z) = \mathbb{I}.$$

Poznámka 3.2. Nechť $X, Y \in \mathcal{C}_n$. Uvědomíme si, že

$$\Theta_1(X) = \Theta_1(Y) \iff \begin{matrix} XQX^{-1} = \alpha Y Q Y^{-1} \\ XPX^{-1} = \beta Y P Y^{-1} \end{matrix} \iff \begin{matrix} Y^{-1}XQ = \alpha Y^{-1} X Q \\ Y^{-1}XP = \beta Y^{-1} X P \end{matrix},$$

kde α, β jsou nějaké mocniny τ_n.

Podle Lemmatu 1.27 potom existují $\gamma \in \mathbb{C} \setminus \{0\}$ a $Z \in \Pi_n$:

$$Y^{-1}X = \gamma Z$$
$$X = \gamma Y Z.$$

Zároveň podle Poznámky 3.1 platí, že $\Theta_1(\gamma Z) = \mathbb{I}. \implies \Theta_1(Y^{-1}X) = \mathbb{I} \implies \Theta_1(X) = \Theta_1(Y)$.

Dohromady jsme získali:

$$\Theta_1(X) = \Theta_1(Y) \iff X = \gamma Y Z, \tag{3.1}$$

kde $\gamma \in \mathbb{C} \setminus \{0\}$, $Z \in \Pi_n$.

Označíme $[X] = X\Pi_n$, $[Y] = Y\Pi_n$ prvky faktorgrupy $\mathcal{C}_n/\Pi_n$. Platí:

$$[X] = [Y] \iff Y^{-1}X \in \Pi_n.$$

Vztah (3.1) můžeme nyní přepsat na

$$\Theta_1(X) = \Theta_1(Y) \Longleftrightarrow [X] = [\gamma Y]. \tag{3.2}$$

Poznámka 3.3. Nechť $X, Y \in \mathcal{C}_n$. Podle Poznámky 3.2

$$[X] = [Y] \Longrightarrow \Theta_1(X) = \Theta_1(Y).$$

Obměnou implikace získáme:

$$\Theta_1(X) \neq \Theta_1(Y) \Longrightarrow [X] \neq [Y].$$

Poznámka 3.4. Můžeme zavést zobrazení

$$\tilde{\Theta}_1 : \mathcal{C}_n/\Pi_n \to \mathrm{SL}(2, \mathbb{Z}_n) : [X] \mapsto \Theta_1(X).$$

Zobrazení $\tilde{\Theta}_1$ je dobře definované: z předchozí Poznámky 3.3 totiž plyne, že pro každé $X, Y \in \mathcal{C}_n$ takové, že $X \sim Y$, tj. $[X] = [Y]$, platí: $\Theta_1(X) = \Theta_1(Y)$).

Navíc platí, že $\tilde{\Theta}_1$ je homomorfismus, (neboť zobrazení Θ_1 je homomorfismus).

Poznámka ke značení 3.5. Nechť $X \in \mathcal{N}_{\mathrm{U}(n)}(\Pi_n)$. Až do konce 3. kapitoly budeme symbolem $[X]$ budeme rozumět rozkladovou třídu $[X] = X\Pi_n$, tj. prvek grupy $\mathcal{N}_{\mathrm{U}(n)}(\Pi_n)/\Pi_n$.

3.1 Cliffordova grupa $\mathcal{C}_2$

Poznámka ke značení 3.6. Pokud v této podkapitole nejsou napsány indexy u operátorů Q_n, P_n, D_n, S_n a konstant ω_n, τ_n, myslí se tím, že $n = 2$.

Poznámka 3.7. V případě $n = 2$ lze celou Cliffordovu grupu $\mathcal{C}_2$ vygenerovat pouze pomocí operátorů S_2 a D_2:

$$\mathcal{C}_2 = \langle S_2, D_2 \rangle.$$

Platí totiž:

$$D_2{}^2 = Q_2, \qquad S_2 D_2{}^2 S_2 = P_2.$$

Tyto vztahy snadno ověříme:

1. $\forall j \in \{1, 2\} : D_2{}^2 e_j = \tau^{2j(2-j)} e_j = \tau^{2j^2} e_j = \omega^{j^2} e_j = \omega^j e_j = Q_2\, e_j$.
2. Vyjdeme ze vtahu (2.8): $S_2 P_2 S_2^{-1} = Q_2, \Longrightarrow P_2 = S_2^{-1} Q_2 S_2$. Jelikož operátor S_2 je řádu 2, platí: $S_2^{-1} = S_2$. Nakonec máme: $P_2 = S_2 D_2 S_2$.

Poznámka 3.8.

$$\omega_2 = \mathrm{e}^{\pi \mathrm{i}} = -1, \qquad \tau_2 = -\mathrm{e}^{\frac{\pi \mathrm{i}}{2}} = -\mathrm{i}.$$

Tabulka 3.1: Prvky $\mathcal{C}_2$ reprezentující 6 různých tříd rozkladu $\mathcal{C}_2$ podle Π_2

X	I	D	S	DS	SD	DSD
$\Theta_1(X)$	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$

Nejdříve se zaměříme na faktorgrupu $\mathcal{C}_2/\Pi_2$ a najdeme všechny její prvky (tj. třídy rozkladu grupy $\mathcal{C}_2$ podle Π_2).

Ke každému prvku C grupy $\mathrm{SL}(2,\mathbb{Z}_2)$ – ($|\mathrm{SL}(2,\mathbb{Z}_2)| = 6$) – najdeme nějaké $X \in \mathcal{C}_2$ tak, aby $\Theta_1(X) = C$. Toto přiřazení je zapsáno v Tabulce 3.1.

Označíme:

$$\mathcal{R} = \{\mathrm{I}, D, S, DS, SD, DSD\},$$
$$\eta = \mathrm{e}^{\frac{\pi \mathrm{i}}{4}}.$$

Dále označíme

$$\mathcal{R}_2 = \{[\mathrm{I}], [D], [\eta S], [\eta DS], [\eta SD], [\eta DSD]\}.$$

Lemma 3.9. Množina $\mathcal{R}_2$ je uzavřená na násobení, (kde násobením se myslí operace definovaná ve faktorgrupě $\mathcal{N}_{\mathrm{U}(2)}(\Pi_2)/\Pi_2$).

Důkaz. Všimneme si, že každý prvek množiny $\mathcal{R}_2$ můžeme zapsat jako nějaký součin prvků $[D]$ a $[\eta S]$, (například $[\eta DSD] = [D][\eta S][D]$). Stačí tedy ověřit, že

$$\forall \varrho \in \mathcal{R}_2 : \varrho[D], \varrho[\eta S] \in \mathcal{R}_2. \tag{3.3}$$

Budou se nám hodit následující vztahy: $D^2 = Q$, $S^2 = \mathrm{I}$. Potom

$$[D]^2 = [\mathrm{I}], \tag{3.4}$$
$$[S]^2 = [\mathrm{I}]. \tag{3.5}$$

Ze vztahu

$$SDS = \mathrm{e}^{\frac{\pi \mathrm{i}}{4}} \frac{1}{\sqrt{2}} \begin{pmatrix}-\mathrm{i} & 1\\ 1 & -\mathrm{i}\end{pmatrix} = \eta\, DSDP \tag{3.6}$$

získáme

$$[SDS] = [\eta DSD]. \tag{3.7}$$

Dále platí: $\eta^2 = \mathrm{e}^{\frac{\pi \mathrm{i}}{2}} = \tau^3$. Víme, že $\tau^3 \mathrm{I} \in \Pi_2$, a proto

$$[\eta^2 \mathrm{I}] = [\tau^3 \mathrm{I}] = [\mathrm{I}]. \tag{3.8}$$

Nyní je třeba postupně projít všechny prvky $\mathcal{R}_2$ a ověřit platnost (3.3). Pomocí vztahů (3.4), (3.5), (3.7), (3.8) to snadno ukážeme. Uvedeme zde pouze případy, které nejsou úplně zřejmé:

$$\begin{aligned}
[\eta DS][\eta S] &= [\eta^2 DS^2] &&= [D] \in \mathcal{R}_2,\\
[\eta SD][\eta S] &= [SDS] &&= [\eta DSD] \in \mathcal{R}_2,\\
[\eta DSD][\eta S] &= [\eta^2 D][SDS] &&= [D][\eta DSD] \quad = [\eta SD] \in \mathcal{R}_2. \qquad \square
\end{aligned}$$

Tvrzení 3.10. $\mathcal{C}_2/\Pi_2 = \left\{[\eta^i X] \mid X \in \mathcal{R}, i \in \{0,1\}\right\}$.

Důkaz. Označíme množinu $\tilde{\mathcal{R}} = \left\{[\eta^i X] \mid X \in \mathcal{R}, i \in \{0,1\}\right\}$.

1. ($\supset$) Ukážeme, že pro každé $X \in \mathcal{R}$ platí: $\eta^i X \in \mathcal{C}_2$.

   Je zřejmé, že každé $X \in \mathcal{R}$ patří do $\mathcal{C}_2$. Stačí tedy ukázat, že do $\mathcal{C}_2$ patří také $\eta\,\mathrm{I}$.

   Připomeneme rovnost (3.6): $SDS = \eta DSDP$. Pak

   $$\mathcal{C}_2 \ni SDSPD^3SD^3 = \eta DSDPPD^3SD^3 = \eta\,\mathrm{I}.$$

   Odtud již plyne, že ηX patří do $\mathcal{C}_2$ (pro každé $X \in \mathcal{R}$), a proto pro každé $i \in \{0,1\} : [\eta^i X] \in \mathcal{C}_2/\Pi_2$.

2. ($\subset$) Ukážeme, že pro každý prvek Y grupy $\mathcal{C}_2$ existuje třída ekvivalence $\varrho \in \tilde{\mathcal{R}}$ tak, že $[Y] = \varrho$.

   Z Poznámky 3.7 a vztahů: $S^2 = \mathrm{I}$, $D^4 = \mathrm{I}$, plyne, že libovolný prvek Y grupy $\mathcal{C}_2$ lze zapsat ve tvaru:

   $$Y = S^{k_0} D^{j_1} S D^{j_2} S \ldots D^{j_m} S D^{j_{m+1}},$$

   kde $\forall i \in \{1,2,\ldots,m\} : j_i \in \{1,2,3\}$; $k_0 \in \{0,1\}$; $j_{m+1} \in \{0,1,2,3\}$.

   Odtud plyne:

   $$\begin{aligned}
   Y &= \eta^{-(k_0+m)} (\eta S)^{k_0} D^{j_1} (\eta S) D^{j_2} (\eta S) \ldots D^{j_m} (\eta S) D^{j_{m+1}},\\
   [Y] &= [\eta^{-(k_0+m)}][\eta S]^{k_0} [D]^{j_1} [\eta S] \ldots [D]^{j_m} [\eta S] [D]^{j_{m+1}}.
   \end{aligned}$$

   Předpokládejme například, že $k_0 = 1$, $j_1 \geq 2$. Potom podle Lemmatu 3.9

   $$\begin{aligned}
   [Y] &= [\eta^{-(1+m)}] \underbrace{\overbrace{[\eta S]}^{\in \mathcal{R}_2}[D]}_{\in \mathcal{R}_2} [D]^{j_1-1} [\eta S] \ldots [D]^{j_m} [\eta S] [D]^{j_{m+1}}\\
   &= [\eta^{-(1+m)}] \underbrace{\overbrace{[\eta SD]}^{\in \mathcal{R}_2}[D]}_{\in \mathcal{R}_2} [D]^{j_1-2} [\eta S] \ldots [D]^{j_m} [\eta S] [D]^{j_{m+1}}\\
   &= [\eta^{-(1+m)}] \underbrace{[\eta S][D]^{j_1} [\eta S] \ldots [D]^{j_m} [\eta S] [D]^{j_{m+1}}}_{\in \tilde{\mathcal{R}}}.
   \end{aligned}$$

   (Pro jiné hodnoty k_0 a j_1 se postupuje stejně.)

   Ukázali jsme, že pro libovolný prvek $Y \in \mathcal{C}_2$ platí: $[Y] \in \tilde{\mathcal{R}}$. $\square$

Poznámka 3.11. 1. Nechť $X \in \mathcal{R}, i, j \in \{0,1\}$. Pak

$$[\eta^i X] = [\eta^j X] \iff \eta^{-j} X^{-1} (\eta^i X) = \eta^{i-j} \mathrm{I} \in \Pi_2 \iff i = j.$$

2. Nechť $X_2, X_2 \in \mathcal{R}, X_1 \neq X_2$. Pak pro každé $i, j \in \{0,1\}$:

$$\Theta_1(\eta^i X_1) = \Theta_1(X_1) \overset{(a)}{\neq} \Theta_1(X_2) = \Theta_1(\eta^j X_2),$$

kde nerovnost (a) plyne z Tabulky 3.1. Odtud podle Poznámky 3.3 plyne:

$$[\eta^i X_1] \neq [\eta^j X_2].$$

Dohromady máme:

$$(i \neq j \vee X_1 \neq X_2) \Longrightarrow [\eta^i X_1] \neq [\eta^j X_2],$$

neboli

$$[\eta^i X_1] = [\eta^j X_2] \Longrightarrow (i = j \wedge X_1 = X_2).$$

Nyní již víme, že libovolný prvek grupy $\mathcal{C}_2$ je možné jednoznačně napsat ve tvaru

$$\eta^i \tau^j X Q^k P^l,$$

kde $i, k, l \in \{0,1\}, j \in \{0,1,2,3\}, X \in \mathcal{R}$.

V Tabulce 3.2 jsou uvedeny matice všech prvků Cliffordovy grupy $\mathcal{C}_2$ – až na násobení konstantou η nebo τ_2 nebo τ_2^2 nebo τ_2^3 – v bázi $\mathcal{E}$.

V tabulce se čte následujícím způsobem: matice v i-tém řádku a j-tém sloupci odpovídá matici operátoru XY, kde X se nachází v 1. sloupci i-tého řádku a Y se nachází v 1. řádku j-tého sloupce.

Tvrzení 3.12. $|\mathcal{C}_2| = 192$.

Důkaz. Z Poznámky 3.11 a Tvrzení 3.10 plyne: $|\mathcal{C}_2/\Pi_2| = 2 \cdot 6 = 12$.
Dále podle Lagrangeovy věty: $|\mathcal{C}_2| = |\Pi_2|\,|\mathcal{C}_2/\Pi_2| = 16 \cdot 12 = 192$. □

Tvrzení 3.13. $\mathcal{C}_2/\Pi_2 \cong \mathcal{Z}_2 \times \mathrm{SL}(2, \mathbb{Z}_2)$.

Důkaz. 1. Označíme: $\mathcal{R}_1 = \{[\mathrm{I}], [\eta\mathrm{I}]\}$.

Definujeme zobrazení $h_1 : \mathcal{R}_1 \to \mathcal{Z}_2 : [\eta^i \mathrm{I}] \mapsto i$.

Je zřejmé, že toto zobrazení je bijekce. Ukážeme, že h_1 je také homomorfismus:

$$h_1([\eta^i][\eta^j]) = h_1([\eta^{i+j(\mathrm{mod}\ 2)}]) = i + j(\mathrm{mod}\ 2) = h_1([\eta^i]) h_1([\eta^j]).$$

Zobrazení h_1 je izomorfismus, (a tudíž $\mathcal{R}_1 \subset\subset \mathcal{C}_2/\Pi_2$).

Tabulka 3.2: Část grupy $\mathcal{C}_2$

	I	Q	P	QP
I	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$
D	$\begin{pmatrix}1 & 0\\ 0 & -\mathrm{i}\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ 0 & \mathrm{i}\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ -\mathrm{i} & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ \mathrm{i} & 0\end{pmatrix}$
S	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}$
DS	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -\mathrm{i} & \mathrm{i}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ -\mathrm{i} & -\mathrm{i}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ \mathrm{i} & -\mathrm{i}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}-1 & 1\\ -\mathrm{i} & -\mathrm{i}\end{pmatrix}$
SD	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -\mathrm{i}\\ 1 & \mathrm{i}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & \mathrm{i}\\ 1 & -\mathrm{i}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}-\mathrm{i} & 1\\ \mathrm{i} & 1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}\mathrm{i} & 1\\ -\mathrm{i} & 1\end{pmatrix}$
DSD	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -\mathrm{i}\\ -\mathrm{i} & 1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & \mathrm{i}\\ -\mathrm{i} & -1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}-\mathrm{i} & 1\\ 1 & -\mathrm{i}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}\mathrm{i} & 1\\ -1 & -\mathrm{i}\end{pmatrix}$

2. Označíme: $\mathcal{R}_2 = \{[\mathrm{I}], [D], [\eta S], [\eta DS], [\eta SD], [\eta DSD]\}$.

   Definujeme zobrazení $h_2 : \mathcal{R}_2 \to \mathrm{SL}(2, \mathbb{Z}_2) : \varrho \mapsto \tilde{\Theta}_1(\varrho)$.

   Z Poznámky 3.1 plyne: $\tilde{\Theta}_1([\eta X]) = \Theta_1(\eta X) = \Theta_1(\eta \mathrm{I})\Theta_1(X) = \Theta_1(X) = \tilde{\Theta}_1([X])$. Odtud s využitím Tabulky 3.1 plyne, že h_2 je bijekce.

   Dále víme (z Lemmatu 3.9), že množina $\mathcal{R}_2$ je uzavřená na násobení, a jelikož zobrazení $\tilde{\Theta}_1$ je homomorfismus, je zřejmé, že h_2 je také homomorfismus.

   Zobrazení h_2 je izomorfismus, (a tudíž $\mathcal{R}_2 \subset\subset \mathcal{C}_2/\Pi_2$).

3. Podle Tvrzení 3.10 a Poznámky 3.11 můžeme libovolný prvek Y grupy $\mathcal{C}_2/\Pi_2$ můžeme zapsat ve tvaru

   $$Y = [\eta^i]\varrho,$$

   kde $i \in \{0, 1\}$ a $\varrho \in \mathcal{R}_2$ jsou určeny jednoznačně.

   Definujeme zobrazení $h : \mathcal{C}_2/\Pi_2 \to \mathcal{Z}_2 \times \mathrm{SL}(2, \mathbb{Z}_2)$:

   $$h(Y) = h([\eta^i]\varrho) = (h_1([\eta^i]), h_2(\varrho)) = (i, \tilde{\Theta}_1(\varrho)).$$

   Zobrazení h je surjektivní, neboť platí:

   $$\forall (i, M) \in \mathcal{Z}_2 \times \mathrm{SL}(2, \mathbb{Z}_2),\ \exists [\eta^i] \in \mathcal{R}_1 \text{ a } \exists \varrho \in \mathcal{R}_2 :$$
   $$h([\eta^i]\varrho) = (h_1([\eta^i]), h_2(\varrho)) = (i, M).$$

   Jelikož řád grupy $\mathcal{C}_2/\Pi_2$ je konečný, plyne odtud, že h je bijekce.

Ukážeme, že je to také homomorfismus:

$$h([\eta^i]\varrho_1[\eta^j]\varrho_2) = h([\eta^{i+j}]\overbrace{\varrho_1\varrho_2}^{\in\mathcal{R}_2}) = (i+j, \tilde{\Theta}_1(\varrho_1\varrho_2)) = (i+j, \tilde{\Theta}_1(\varrho_1)\tilde{\Theta}_1(\varrho_2))$$
$$= (i, \tilde{\Theta}_1(\varrho_1))(j, \tilde{\Theta}_1(\varrho_2)) = h([\eta^i]\varrho_1)h([\eta^j]\varrho_2).$$

Dokázali jsme, že h je izomorfismus. □

Poznámka 3.14. V důkazu Tvrzení 3.13 jsme našli dvě podgrupy grupy $\mathcal{C}_2/\Pi_2$:

$$\mathcal{R}_1 = \langle[\eta\mathrm{I}]\rangle, \qquad \mathcal{R}_2 = \langle[D], [\eta S]\rangle.$$

3.2 Cliffordova grupa $\mathcal{C}_3$

Poznámka ke značení 3.15. Pokud v této podkapitole nejsou napsány indexy u operátorů Q_n, P_n, D_n, S_n a konstant ω_n, τ_n, myslí se tím, že $n = 3$.

Poznámka 3.16. Podle Tvrzení 2.15 platí:

$$\mathcal{C}_3 = \langle S_3, D_3\rangle.$$

Poznámka 3.17.

$$\omega_3 = \mathrm{e}^{\frac{2}{3}\pi\mathrm{i}} = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}, \qquad \tau_3 = -\mathrm{e}^{\frac{1}{3}\pi\mathrm{i}} = \mathrm{e}^{\frac{4}{3}\pi\mathrm{i}} = -\frac{1}{2} - \mathrm{i}\frac{\sqrt{3}}{2} = {\omega_3}^2.$$

Poznámka 3.18. Matice prvků grupy Π_3 v bázi $\mathcal{E}$ vypadají následovně:

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \quad Q^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega \end{pmatrix}, \quad P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$
$$P^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad QP = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \omega \\ \omega^2 & 0 & 0 \end{pmatrix}, \quad Q^2P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \omega^2 \\ \omega & 0 & 0 \end{pmatrix},$$
$$QP^2 = \begin{pmatrix} 0 & 0 & 1 \\ \omega & 0 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix}, \quad Q^2P^2 = \begin{pmatrix} 0 & 0 & 1 \\ \omega^2 & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix},$$

kde libovolná matice může být ještě vynásobena konstantou ω_3 nebo ω_3^2.

Stejně jako v předchozím případě se nejprve podíváme na prvky faktorgrupy $\mathcal{C}_3/\Pi_3$. Pro každou matici $C \in \mathrm{SL}(2, \mathbb{Z}_3)$ – ($|\mathrm{SL}(2, \mathbb{Z}_3)| = 24$) – najdeme jeden prvek $X \in \mathcal{C}_3$ tak, aby $\Theta_1(X) = C$.

Toto přiřazení je zapsáno v následující Tabulce 3.3 – v prvním řádku jsou vybrané prvky grupy $\mathcal{C}_3$, ve druhém jejich matice v bázi $\mathcal{E}$ a ve třetím příslušná matice z grupy $\mathrm{SL}(2, \mathbb{Z}_3)$.

Tabulka 3.3: Prvky $\mathcal{C}_3$ reprezentující 24 různých tříd rozkladu $\mathcal{C}_3$ podle Π_3

I	D	D^2	S
$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&\omega^2\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&\omega\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&1\\1&\omega&\omega^2\\1&\omega^2&\omega\end{pmatrix}$
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\1&0\end{pmatrix}$
S^2	S^3	SD	S^2D
$\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&1\\1&\omega^2&\omega\\1&\omega&\omega^2\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega^2\\1&\omega&\omega\\1&\omega^2&1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&0&\omega^2\\0&1&0\end{pmatrix}$
$\begin{pmatrix}2&0\\0&2\end{pmatrix}$	$\begin{pmatrix}0&1\\2&0\end{pmatrix}$	$\begin{pmatrix}0&2\\1&1\end{pmatrix}$	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$
S^3D	SD^2	S^2D^2	S^3D^2
$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega^2\\1&\omega^2&1\\1&\omega&\omega\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega\\1&\omega&1\\1&\omega^2&\omega^2\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&0&\omega\\0&1&0\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega\\1&\omega^2&\omega^2\\1&\omega&1\end{pmatrix}$
$\begin{pmatrix}0&2\\2&2\end{pmatrix}$	$\begin{pmatrix}0&2\\1&2\end{pmatrix}$	$\begin{pmatrix}2&1\\0&2\end{pmatrix}$	$\begin{pmatrix}0&1\\2&1\end{pmatrix}$
DS	D^2S	DS^3	D^2S^3
$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&1\\1&\omega&\omega^2\\\omega^2&\omega&1\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&1\\1&\omega&\omega^2\\\omega&1&\omega^2\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&1\\1&\omega^2&\omega\\\omega^2&1&\omega\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&1\\1&\omega^2&\omega\\\omega&\omega^2&1\end{pmatrix}$
$\begin{pmatrix}1&2\\1&0\end{pmatrix}$	$\begin{pmatrix}2&2\\1&0\end{pmatrix}$	$\begin{pmatrix}2&1\\2&0\end{pmatrix}$	$\begin{pmatrix}1&1\\2&0\end{pmatrix}$
DSD	DSD^2	DS^3D	DS^3D^2
$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega^2\\1&\omega&\omega\\\omega^2&\omega&\omega^2\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega\\1&\omega&1\\\omega^2&\omega&\omega\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega^2\\1&\omega^2&1\\\omega^2&1&1\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega\\1&\omega^2&\omega^2\\\omega^2&1&\omega^2\end{pmatrix}$
$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}2&0\\2&2\end{pmatrix}$	$\begin{pmatrix}2&2\\2&1\end{pmatrix}$
D^2SD	D^2SD^2	D^2S^3D	$D^2S^3D^2$
$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega^2\\1&\omega&\omega\\\omega&1&\omega\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega\\1&\omega&1\\\omega&1&1\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega^2\\1&\omega^2&1\\\omega&\omega^2&\omega^2\end{pmatrix}$	$\frac{1}{\sqrt{3}}\begin{pmatrix}1&1&\omega\\1&\omega^2&\omega^2\\\omega&\omega^2&\omega\end{pmatrix}$
$\begin{pmatrix}2&1\\1&1\end{pmatrix}$	$\begin{pmatrix}2&0\\1&2\end{pmatrix}$	$\begin{pmatrix}1&2\\2&2\end{pmatrix}$	$\begin{pmatrix}1&0\\2&1\end{pmatrix}$

Označíme množinu operátorů z $\mathcal{C}_3$ uvedených v Tabulce 3.3:

$$\mathcal{S} = \big\{\mathrm{I}, D, D^2, S, S^2, S^3, SD, S^2D, S^3D, SD^2, S^2D^2, S^3D^2, DS, D^2S, DS^3,$$
$$D^2S^3, DSD, DSD^2, DS^3D, DS^3D^2, D^2SD, D^2SD^2, D^2S^3D, D^2S^3D^2\big\}.$$

Dále označíme:

$$\zeta = \mathrm{e}^{\frac{\pi\mathrm{i}}{6}}.$$

Poznámka 3.19. Při násobením matic z Tabulky 3.3 můžou vzniknout následující konstanty. Jejich znalost využijeme o něco níž v Poznámce 3.20.

$$\frac{2+\omega}{\sqrt{3}} = \frac{2}{\sqrt{3}} - \frac{1}{2\sqrt{3}} + \mathrm{i}\,\frac{1}{2} = \frac{\sqrt{3}}{2} + \mathrm{i}\,\frac{1}{2} = \mathrm{e}^{\frac{\pi\mathrm{i}}{6}} = \zeta$$
$$\frac{2+\omega^2}{\sqrt{3}} = \mathrm{e}^{-\frac{\pi\mathrm{i}}{6}} = \omega^2\zeta^3$$
$$\frac{1+2\omega}{\sqrt{3}} = \frac{1}{\sqrt{3}} - \frac{1}{\sqrt{3}} + \mathrm{i} = \mathrm{i} = \mathrm{e}^{\frac{\pi\mathrm{i}}{2}} = \zeta^3$$
$$\frac{1+2\omega^2}{\sqrt{3}} = -\mathrm{i} = \mathrm{e}^{-\frac{\pi\mathrm{i}}{2}} = \omega^2\zeta$$

Poznámka 3.20. Platí:

$$SDS = \frac{1}{3}\begin{pmatrix} 2+\omega^2 & 1+2\omega & 2+\omega^2 \\ 1+2\omega & 2+\omega^2 & 2+\omega^2 \\ 2+\omega^2 & 2+\omega^2 & 1+2\omega \end{pmatrix} = \omega^2\zeta^3\,\frac{1}{\sqrt{3}}\begin{pmatrix} 1 & \omega & 1 \\ \omega & 1 & 1 \\ 1 & 1 & \omega \end{pmatrix}$$
$$= \omega^2\zeta^3 D^2SD^2P^2, \tag{3.9}$$
$$SD^2S = \frac{1}{3}\begin{pmatrix} 2+\omega & 2+\omega & 1+2\omega^2 \\ 2+\omega & 1+2\omega^2 & 2+\omega \\ 1+2\omega^2 & 2+\omega & 2+\omega \end{pmatrix} = \zeta\,\frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & \omega^2 \\ 1 & \omega^2 & 1 \\ \omega^2 & 1 & 1 \end{pmatrix}$$
$$= \zeta DS^3D. \tag{3.10}$$

Potom

$$[SDS] = [\zeta^3 D^2SD^2], \tag{3.11}$$
$$[SD^2S] = [\zeta DS^3D]. \tag{3.12}$$

Ještě připomeneme, že pro n liché platí vztah (2.12): $Q_n = {S_n}^2 {D_n}^{n-1} {S_n}^2 D_n$. Po dosazení $n = 3$ získáme:

$$Q = S^2D^2S^2D$$
$$S^2DQ = S^2D$$

Potom

$$[DS^2] = [S^2D]. \tag{3.13}$$

Nakonec se podíváme na konstantu ζ. Platí: $\zeta^2 = \mathrm{e}^{\frac{\pi \mathrm{i}}{3}}$, $\zeta^3 = \mathrm{e}^{\frac{\pi \mathrm{i}}{2}}$, $\zeta^4 = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}} = \omega^2$. Odtud plyne:

$$[\zeta^4 \mathrm{I}] = [\omega^2 \mathrm{I}] = [\mathrm{I}]. \tag{3.14}$$

Označíme

$$\begin{aligned}\mathcal{S}_2 = \big\{&[\mathrm{I}], [D], [D^2], [\zeta S], [\zeta^2 S^2], [\zeta^3 S^3], [\zeta SD], [\zeta^2 S^2 D], [\zeta^3 S^3 D], [\zeta SD^2],\\ &[\zeta^2 S^2 D^2], [\zeta^3 S^3 D^2], [\zeta DS], [\zeta D^2 S], [\zeta^3 DS^3], [\zeta^3 D^2 S^3], [\zeta DSD], [\zeta DSD^2],\\ &[\zeta^3 DS^3 D], [\zeta^3 DS^3 D^2], [\zeta D^2 SD], [\zeta D^2 SD^2], [\zeta^3 D^2 S^3 D], [\zeta^3 D^2 S^3 D^2]\big\}.\end{aligned}$$

Je to množina obsahující prvky tvaru $[\zeta^{f(X)} X]$, kde $X \in \mathcal{S}$ a $f(X) =$ „mocnina prvku S vyskytující se v zápisu prvku X v Tabulce 3.3“; například: $f(D) = 0$, $f(S^2D) = 2$, $f(DS^3D) = 3$.

Lemma 3.21. Množina $\mathcal{S}_2$ je uzavřená na násobení, (kde násobením se myslí operace definovaná ve faktorgrupě $\mathcal{N}_{\mathrm{U}(3)}(\Pi_3)/\Pi_3$).

Důkaz. Všimneme si, že libovolný prvek množiny $\mathcal{S}_2$ lze zapsat jako nějaký součin prvků $[D]$ a $[\zeta S]$, stačí tedy ověřit, že

$$\forall \sigma \in \mathcal{S}_2 : \sigma[D], \sigma[\zeta S] \in \mathcal{S}_2. \tag{3.15}$$

S využitím vztahů (3.11) – (3.14) a vztahů $[S]^4 = [\mathrm{I}]$, $[D]^3 = [\mathrm{I}]$ lze platnost (3.15) ověřit. Nebudeme zde rozepisovat všechny případy, uvedeme pouze některé pro ilustraci:

$$[\zeta^2 S^2 D^2][\zeta S] \overset{(3.13)}{=} [\zeta^3 D^2 S^3] \in \mathcal{S}_2,$$

$$[\zeta^3 S^3 D][\zeta S] = [\zeta^4 S^2][SDS] \overset{(3.11)}{=} [S^2][\zeta^3 D^2 SD^2] \overset{(3.13)}{=} [\zeta^3 D^2 S^3 D^2] \in \mathcal{S}_2,$$

$$[\zeta^3 S^3 D^2][\zeta S] = [\zeta^4 S^2][SD^2 S] \overset{(3.12)}{=} [S^2][\zeta DS^3 D] \overset{(3.13)}{=} [\zeta DS^5 D] = [\zeta DSD] \in \mathcal{S}_2, \tag{$*$}$$

$$[\zeta DSD][\zeta S] = [\zeta^2 D][SDS] \overset{(3.11)}{=} [\zeta^2 D][\zeta^3 D^2 SD^2] = [\zeta^5 D^3 SD^2] = [\zeta SD^2] \in \mathcal{S}_2,$$

$$[\zeta^3 DS^3 D^2][\zeta S] = [\zeta^4 D][S^3 D^2 S] \overset{(*)}{=} [D][\zeta DSD] = [\zeta D^2 SD] \in \mathcal{S}_2.$$

□

Tvrzení 3.22. $\mathcal{C}_3/\Pi_3 = \big\{[\zeta^i X] \mid X \in \mathcal{S}, i \in \{0,1,2,3\}\big\}$.

Důkaz. Budeme postupovat stejným způsobem jako v důkazu Tvrzení 3.10.

Označíme množinu $\tilde{\mathcal{S}} = \big\{[\zeta^i X] \mid X \in \mathcal{S}, i \in \{0,1,2,3\}\big\}$.

1. ($\supset$) Ukážeme, že pro každou třídu $[\zeta^i X] \in \tilde{\mathcal{S}}$ existuje prvek $Y \in \mathcal{C}_3$ takový, že $[Y] = [\zeta^i X]$; (tj. $[\zeta^i X] \in \mathcal{C}_3/\Pi_3$).

   Stačí ukázat, že pro každé $X \in \mathcal{S}$ platí: $\zeta^i X \in \mathcal{C}_3$. Potom už jen položíme $Y = \zeta^i X$. Využijeme vztah (3.10):

   $$SD^2S = \zeta DS^3D.$$

   Pak

   $$\mathcal{C}_3 \ni SD^2SD^2SD^2 = \zeta DS^3DD^2SD^2 = \zeta\,\mathrm{I},$$

   a proto $\forall i \in \{0,1,2,3\}, \forall X \in \mathcal{S}\,(\subset \mathcal{C}_3) : \zeta^i X = (\zeta\mathrm{I})^i X \in \mathcal{C}_3$.

2. ($\subset$) Ukážeme, že pro každý prvek Y grupy $\mathcal{C}_3$ existuje třída ekvivalence $\sigma \in \tilde{\mathcal{S}}$ tak, že $[Y] = \sigma$.

   Z Poznámky 3.16 a vztahů: $S^4 = \mathrm{I}$, $D^3 = \mathrm{I}$, plyne, že libovolný prvek Y grupy $\mathcal{C}_3$ můžeme zapsat ve tvaru:

   $$Y = S^{k_0}D^{j_1}S^{k_1}D^{j_2}S^{k_2}\ldots D^{j_m}S^{k_m}D^{j_{m+1}},$$

   kde $\forall i \in \{1,2,\ldots,m\} : j_i \in \{1,2\}, k_i \in \{1,2,3\}$; $k_0 \in \{0,1,2,3\}$; $j_{m+1} \in \{0,1,2\}$.

   Odtud plyne:

   $$Y = \zeta^{-\kappa}\,(\zeta S)^{k_0}D^{j_1}(\zeta S)^{k_1}D^{j_2}(\zeta S)^{k_2}\ldots D^{j_m}(\zeta S)^{k_m}D^{j_{m+1}},$$

   kde jsme označili $\kappa = \sum_{i=0}^{m} k_i$.

   $$[Y] = [\zeta^{-\kappa}][\zeta S]^{k_0}[D]^{j_1}[\zeta S]^{k_1}\ldots[D]^{j_m}[\zeta S]^{k_m}[D]^{j_{m+1}}.$$

   Předpokládejme například, že $k_0 = 2$. Potom podle Lemmatu 3.21

   $$\begin{aligned}
   [Y] &= [\zeta^{-\kappa}]\overbrace{\underbrace{[\zeta S][\zeta S]}_{\in\mathcal{S}_2}}^{\in\mathcal{S}_2}[D]^{j_1}[\zeta S]^{k_1}\ldots[D]^{j_m}[\zeta S]^{k_m}[D]^{j_{m+1}} \\
   &= [\zeta^{-\kappa}]\overbrace{\underbrace{[\zeta S]^2}_{\in\mathcal{S}_2}[D]}^{\in\mathcal{S}_2}[D]^{j_1-1}[\zeta S]^{k_1}\ldots[D]^{j_m}[\zeta S]^{k_m}[D]^{j_{m+1}} \\
   &= [\zeta^{-\kappa}]\underbrace{[\zeta S]^2[D]^{j_1}[\zeta S]^{k_1}\ldots[D]^{j_m}[\zeta S]^{k_m}[D]^{j_{m+1}}}_{\in\mathcal{S}_2} \in \tilde{\mathcal{S}}.
   \end{aligned}$$

   (Pro jinou hodnotu k_0 se postupuje úplně stejně.)

   Tímto jsme ukázali, že pro libovolný prvek $Y \in \mathcal{C}_3$ platí, že $[Y] \in \tilde{\mathcal{S}}$. □

Poznámka 3.23. Stejným způsobem jako v Poznámce 3.11 se ukáže, že pro každé $X_1, X_2 \in \mathcal{S}$ a pro každé $i, j \in \{0,1,2,3\}$ platí:

$$[\zeta^i X_1] = [\zeta^j X_2] \Longrightarrow (i = j \wedge X_1 = X_2).$$

Tvrzení 3.24. $|\mathcal{C}_3| = 2592$.

Důkaz. Z Tvrzení 3.22 a Poznámky 3.23 získáme: $|\mathcal{C}_3/\Pi_3| = 4 \cdot 24$.
Podle Lagrangeovy věty platí:

$$|\mathcal{C}_3| = |\Pi_3|\ |\mathcal{C}_3/\Pi_3| = 27 \cdot 4 \cdot 24 = 2592. \qquad \square$$

Tvrzení 3.25. $\mathcal{C}_3/\Pi_3 \cong \mathcal{Z}_4 \times \mathrm{SL}(2, \mathbb{Z}_3)$.

Důkaz. Budeme postupovat velmi podobně jako v důkazu Tvrzení 3.13.

1. Označíme: $\mathcal{S}_1 = \big\{[\zeta^i \mathrm{I}] \mid i \in \{0,1,2,3\}\big\}$.
   Definujeme zobrazení $h_1 : \mathcal{S}_1 \to \mathcal{Z}_4 : [\zeta^i \mathrm{I}] \mapsto i$.
   Je zřejmé, že toto zobrazení je bijekce. Ukážeme, že h_1 je také homomorfismus:
   $$h_1([\zeta^i][\zeta^j]) = h_1([\zeta^{i+j(\mathrm{mod}\ 4)}]) = i + j(\mathrm{mod}\ 4) = h_1([\zeta^i])h_1([\zeta^j]).$$
   Zobrazení h_1 je izomorfismus, (a tudíž $\mathcal{S}_1 \subset\subset \mathcal{C}_3/\Pi_3$).

2. Definujeme zobrazení $h_2 : \mathcal{S}_2 \to \mathrm{SL}(2, \mathbb{Z}_3) : \sigma \mapsto \tilde{\Theta}_1(\sigma)$.
   Stejně jako v důkazu Tvrzení 3.13 si uvědomíme, že z Poznámky 3.1 plyne: $\tilde{\Theta}_1([\zeta^i X]) = \tilde{\Theta}_1([X])$. Odtud s využitím Tabulky 3.3 získáme, že h_2 je bijekce.
   Z Lemmatu 3.21 víme, že $\mathcal{S}_2$ je uzavřená na násobení, a protože zobrazení $\tilde{\Theta}_1$ je homomorfismus, je také h_2 homomorfismus.
   Zobrazení h_2 je izomorfismus, (a tudíž $\mathcal{S}_2 \subset\subset \mathcal{C}_3/\Pi_3$).

3. Z Tvrzení 3.22 a Poznámky 3.23 plyne, že libovolný prvek Y grupy $\mathcal{C}_3/\Pi_3$ můžeme zapsat jako
   $$Y = [\zeta^i]\sigma,$$
   kde $i \in \{0,1,2,3\}$ a $\sigma \in \mathcal{S}_2$ jsou určeny jednoznačně.
   Zavedeme zobrazení $h : \mathcal{C}_3/\Pi_3 \to \mathcal{Z}_4 \times \mathrm{SL}(2, \mathbb{Z}_3)$:
   $$h(Y) = h([\zeta^i]\sigma) = (h_1([\zeta^i]), h_2(\sigma)) = (i, \tilde{\Theta}_1(\sigma)).$$
   Zobrazení h je surjektivní. Platí totiž:
   $$\forall (i, M) \in \mathcal{Z}_4 \times \mathrm{SL}(2, \mathbb{Z}_3),\ \exists [\eta^i] \in \mathcal{S}_1 \text{ a } \exists \sigma \in \mathcal{S}_2 :$$
   $$h([\zeta^i]\sigma) = (h_1([\zeta^i]), h_2(\sigma)) = (i, M).$$
   Jelikož řád grupy $\mathcal{C}_3/\Pi_3$ je konečný, plyne odtud, že h je bijekce.
   Ukážeme, že je to také homomorfismus:
   $$h([\zeta^i]\sigma_1[\zeta^j]\sigma_2) = h([\zeta^{i+j}]\overbrace{\sigma_1\sigma_2}^{\in\mathcal{S}_2}) = (i + j, \tilde{\Theta}_1(\sigma_1\sigma_2)) = (i + j, \tilde{\Theta}_1(\sigma_1)\tilde{\Theta}_1(\sigma_2))$$
   $$= (i, \tilde{\Theta}_1(\sigma_1))(j, \tilde{\Theta}_1(\sigma_2)) = h([\zeta^i]\sigma_1)h([\zeta^j]\sigma_2).$$
   Dohromady máme, že h je izomorfismus. $\square$

Poznámka 3.26. V důkazu Tvrzení 3.25 jsme našli dvě podgrupy grupy $\mathcal{C}_3/\Pi_3$:

$$\mathcal{S}_1 = \langle [\zeta \mathrm{I}] \rangle, \qquad \mathcal{S}_2 = \langle [D], [\zeta S] \rangle.$$

Literatura

[1] D. M. Appleby et al., *The monomial representations of the Clifford group*, Quantum Information and Computation **12** (2012), 0404-0431

[2] M. Havlíček, J. Patera, E. Pelantová, J. Tolar, *Automorphisms of the fine grading of sl(n,$\mathbb{C}$) associated with the generalized Pauli matrices*, J. Math. Phys. **43** (2002), 1083-1094

[3] M. Korbelář, J. Tolar, *Symmetries of the finite Heisenberg group for composite systems*, J. Phys. A: Math. Theor. **43** (2010), 375302

[4] E. Hostens, J. Dehaene, B. De Moor, *Stabilizer states and Clifford operations for systems of arbitrary dimensions, and modular arithmetic*, Phys. Rev. A **71** (2005), 042315

[5] J. Tolar, *On the structure of the Clifford groups of finite quantum systems*, rukopis (2016)

[6] P. Novotný, *Počet prvků a akce grupy SL(m, $\mathbb{Z}_n$)*, Výzkumný úkol FJFI ČVUT, Praha (2002)

[7] M. Planat, P. Jorrand, *On group theory for quantum gates and quantum coherence*, J. Phys A: Math. Theor. **41** (2008), 182001

[8] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge (2010)

[9] D. S. Dummit, R. M. Foote, *Abstract algebra*, John Wiley and Sons (2004)

[10] J. Mareš, *Algebra*, skripta ČVUT, Praha (2014)