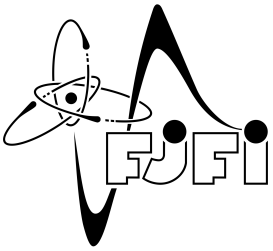
České Vysoké Učení Technické
v Praze

Fakulta jaderná a fyzikálně inženýrská



Bakalářská práce

Struktura Cliffordových grup v konečně-rozměrné kvantové mechanice

Július Kovaľ

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

2020

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze podklady uvedené v přiloženém seznamu.

Nemám závažný důvod proti použití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V praze dne ....

podpis

Poděkování

Chtěl bych poděkovat doktoru Korbelářovi a profesoru Tolarovi za jejich trpělivost a rady.

Obsah

Úvod

Konečně-rozměrná kvantová mechanika se zabývá kvantovými systémy, jejichž stavový prostor je nějaký konečně-rozměrný komplexní Hilbertův prostor $\mathcal{H}_N$. V současnosti je pro rozvoj konečně-rozměrné kvantové mechaniky významnou hnací silou kvantové počítání. Základní jednotkou kvantové informace je qubit, který je reprezentován dvourozměrným Hilbertovým prostorem $\mathcal{H}_2$ a soustava více qubitů je reprezentována tenzorovým součinem $\mathcal{H}_2 \otimes ... \otimes \mathcal{H}_2$.

Zobecněním qubitu je qu*d*it, který je realizován pomocí d-rozměrného kvantového systému. Kvantová logická hradla působící na qudit lze vyjádřit pomocí unitárních matic z $\mathbb{C}^{d,d}$ [1], například zobecněnými Pauliho maticemi.

Nejprve se podíváme na souvislosti mezi klasickou mechanikou, nekonečně-rozměrnou kvantovou mechanikou a konečně-rozměrnou kvantovou mechanikou

Dále se budeme věnovat Weylově-Heisenbergově grupě, což je jistá podgrupa unitárních operátorů tvořena Pauliho X- a Z-maticemi a jejich násobky. Pak se budeme věnovat Cliffordově grupě, což je jistá grupa symetrií Weylovy-Heisenbergovy grupy a blíže se podíváme na její strukturu. Konec této práce je pak věnován tak zvané Weilově reprezentaci pro liché hodnoty dimenze N.

Značení

1. Grupu $(G, \cdot)$ budeme bez zdůraznění její operace značit pouze G, její jednotkový prvek budeme značit 1_G, inverzní prvek k prvku $g \in G$ označíme g^{-1}.

2. Budeme používat braketové značení: $\langle x|y\rangle$ značí skalární součin vektorů $|x\rangle$ a $|y\rangle$. Skalární součin je antilineární v prvním argumentu a lineární ve druhém. Pokud A, B jsou unitární operátory, pak $\langle x|A^\dagger B|y\rangle$ značí skalární součin vektorů $A\,|x\rangle$ a $B\,|y\rangle$.

3. Grupu generovanou prvky $g_1, ..., g_n$ budeme značit $\langle g_1, ..., g_n\rangle$.

4. Direktní součin grup G_1 a G_2 budeme značit $G_1 \times G_2$.

5. To, že H je podgrupa G, budeme značit $H \leq G$.

$\mathcal{H}_N$	komplexní Hilbertův prostor dimenze N
I	Identický operátor na $\mathcal{H}_N$
Id_G	Identický homomorfismus na grupě G
$\mathcal{L}(\mathcal{H}_N)$	grupa lineárních operátorů z $\mathcal{H}_N$ do $\mathcal{H}_N$
$\mathrm{GL}(\mathcal{H}_N)$	grupa $(\{X \in \mathcal{L}(\mathcal{H}_N) \mid X \text{ je regulární }\};\ \circ\ )$
$\mathrm{U}(N)$	grupa $(\{X \in \mathrm{GL}(\mathcal{H}_N) \mid XX^\dagger = I\};\ \circ\ )$
$\mathrm{U}(1)$	grupa $(\{zI \mid z \in \mathbb{C}, \lvert z\rvert = 1\};\ \circ\ )$
$R^{j,k}$	množina všech matic $j \times k$, jejichž prvky patří do okruhu R
$\mathrm{GL(n, R)}$	grupa $(\{A \in R^{n,n} \mid \det(A) \neq 0\};\ \cdot\ )$
$\mathrm{SL}(n, R)$	grupa $(\{A \in R^{n,n} \mid \det(A) = 1\};\ \cdot\ )$

1 Motivace

V hamiltonovské mechanice tvoří význačnou třídu transformací tak zvané kanonické transformace, jelikož zachovávají tvar Hamiltonových kanonických rovnic. Podmínku kanoničnosti transformace lze v obecném $2N$-rozměrném fázovém prostoru vyjádřit pomocí Poissonových závorek, konkrétně

$$\{Q_i, Q_j\}_{q,p} = 0, \qquad \{P_i, P_j\}_{q,p} = 0, \qquad \{Q_i, P_j\}_{q,p} = \delta_{ij}.$$

Jednoduchým výpočtem lze ukázat, že lineární transformace dvourozměrného fázového prostoru, tj. transformace, které lze zapsat ve tvaru

$$\begin{pmatrix} Q \\ P \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} q \\ p \end{pmatrix},$$

jsou kanonické právě tehdy, když matice transformace má determinant 1.

Další význačnou třídu transformací tvoří lineární nehomogenní transformace, které na vektor $v \in \mathbb{R}^N$ působí následovně:

$$v' = Av + b,$$

kde $A \in \mathbb{R}^{N,N}$ a $b \in \mathbb{R}^N$.

Poznámka. Odteď pokud budeme mluvit o lineárních nehomogenních transformacích, budeme předpokládat, že jim příslušející matice jsou regulární.

Speciálně lze lineární nehomogenní transformace dvourozměrného fázového prostoru zapsat ve tvaru

$$\begin{pmatrix} Q \\ P \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} q \\ p \end{pmatrix} + \begin{pmatrix} q_0 \\ p_0 \end{pmatrix}$$

Pokud bychom zkoumali, kdy tyto transformace zachovávají Poissonovy závorky, opět bychom snadným výpočtem zjistili, že musí platit $ad - bc = 1$. Lineární nehomogenní transformaci, jejíž příslušná čtvercová matice je prvkem grupy $\mathrm{SL}(2, \mathbb{R})$, nazveme kanonickou lineární nehomogenní transformací. Regulární lineární transformace a translace jsou de facto speciální případy lineárních nehomogenních transformací, a proto je přirozené se ptát, jaký je mezi nimi vztah. Podívejme se proto na způsob, jakým se lineární nehomogenní transformace skládají:

$$v'' = A'v' + b' = A'(Av + b) + b' = A'Av + A'b + b.$$

Toto skládání odpovídá struktuře semidirektního součtu, což je pojem, který blíže vysvětlíme v podkapitole 3.2. Prozatím řekneme, že grupa $\mathrm{A}(2, \mathbb{R})$ nehomogenních lineárních transformací je semidirektní součin grupy translací a grupy regulárních lineárních transformací, značíme

$$\mathrm{A}(2, \mathbb{R}) = T^2 \rtimes \mathrm{GL}(2, \mathbb{R}),$$

kde T^2 značí grupu translací v $\mathbb{R}^2$. V druhé poznámce pod definicí 3.15 ukážeme, že to skutečně platí. Pro grupu $\widetilde{\mathrm{A}}(2, \mathbb{R})$ kanonických lineárních nehomogenních transformací obdobně platí

$$\widetilde{\mathrm{A}}(2, \mathbb{R}) = T^2 \rtimes \mathrm{SL}(2, \mathbb{R}).$$

V nekonečně-rozměrné kvantové mechanice platí pro operátory polohy a hybnosti komutační relace obdobné Poissonovým závorkám:

$$[\hat{\mathbb{Q}}_i, \hat{\mathbb{Q}}_j] = 0, \qquad [\hat{\mathbb{P}}_i, \hat{\mathbb{P}}_j] = 0, \qquad [\hat{\mathbb{Q}}_i, \hat{\mathbb{P}}_j] = i\hbar\delta_{ij}$$

a navíc jsou operátory polohy a hybnosti provázány Fourierovou transformací:

$$\mathcal{F}^{-1}\hat{\mathbb{Q}}_i\mathcal{F} = \hat{\mathbb{P}}_i.$$

Poznámka. V této práci pracujeme primárně s unitárními operátory Q_N a P_N, kde N značí dimenzi Hilbertova prostoru, na který působí. Abychom se vyhli nejasnostem, značíme samosdružené operátory a matice pomocí samostatného fontu. Odteď budeme také pro jednoduchost psát operátory bez stříšky.

Uvažujme lineární transformaci

$$\begin{pmatrix} \mathbb{Q}' \\ \mathbb{P}' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathbb{Q} \\ \mathbb{P} \end{pmatrix}.$$

Opět lze snadným výpočtem ukázat, že takováto lineární transformace zachová komutátor, právě když matice transformace má determinant 1.

Chtěli bychom, aby komutační vztahy platily i pro konečně-rozměrné operátory polohy a hybnosti. Pro libovolné dvě samosdružené matice $\mathbb{A}, \mathbb{B}$ ale platí $Tr(\mathbb{AB}) = Tr(\mathbb{BA})$, a proto jejich komutátor nemůže být roven násobku jednotkové matice, jelikož musí mít nulovou stopu.

Stoneova věta říká, že každému samosdruženému operátoru lze jednoznačně přiřadit spojitou jednoparametrickou unitární grupu, a proto od operátorů polohy a hybnosti můžeme přejít k jistým unitárním operátorům, konkrétně

$$\mathbb{P} \mapsto U(t) = exp(\tfrac{i}{\hbar}\mathbb{P}t), \qquad \mathbb{Q} \mapsto V(s) = exp(\tfrac{i}{\hbar}\mathbb{Q}s).$$

Pro tyto operátory platí komutační vztah

$$U(t)V(s) = exp(\tfrac{i}{\hbar}st)V(s)U(t),$$

který, jak uvidíme, je analogický vztahu mezi prvky Weylovy-Heisenbergovy grupy.

V kvantové mechanice N-hladinového systému jsou základní operátory zobecněné Pauliho matice [2]. Tyto matice generují určitou konečnou podgrupu Weylovy-Heisenbergovy grupy. Stavový prostor N-hladinového kvantového systému je komplexní N-rozměrný Hilbertův prostor $\mathcal{H}_N$ a pozorovatelné jsou reprezentovány samosdruženými operátory, jejichž vlastní vektory tvoří bázi tohoto prostoru. Proto lze konfigurační prostor tohoto systému ztotožnit s abelovskou grupou řádu N. My se budeme věnovat případu, kdy vlastnostem systému odpovídá grupa $\mathbb{Z}_N$. Fázový prostor pak ztotožňujeme s grupou $\mathbb{Z}_N \times \mathbb{Z}_N$.

Pokusme se nyní najít operátory $\mathbb{Q}_N$ a $\mathbb{P}_N$, které by představovali operátory polohy a hybnosti na $\mathcal{H}_N$. Budeme požadovat, aby byly samosdružené, a proto budou vlastní vektory $\mathbb{Q}_N$, které označíme $|0\rangle, ..., |N-1\rangle$, tvořit ortonormální bázi $\mathcal{H}_N$. Je přirozené operátor $\mathbb{Q}_N$ definovat tak, aby platilo $\mathbb{Q}_N |i\rangle = i\,|i\rangle$ pro všechny $i \in \mathbb{Z}_N$. Operátor hybnosti $\mathbb{P}_N$ pak definujeme pomocí vztahu $\mathbb{P}_N = \mathcal{F}_N^{-1}\mathbb{Q}_N\mathcal{F}_N$, kde $\mathcal{F}_N = \frac{1}{\sqrt{N}}\sum_{i,j=0}^{N-1} |i\rangle\langle j|\,\omega_N^{ij}$ je diskrétní Fourierova transformace a $\omega_N = e^{\frac{2\pi i}{N}}$.

Jak bylo řečeno výše, nebude platit analogie komutačních relací z nekonečněrozměrné kvantové mechaniky, a proto přejděme k operátorům Q_N a P_N definovaným následovně:

$$Q_N = exp(\tfrac{2\pi i}{N}\mathbb{Q}_N), \qquad P_N = exp(\tfrac{2\pi i}{N}\mathbb{P}_N).$$

V příští kapitole dokážeme, že tyto operátory jsou unitární. Ve standardní bázi jsou matice $\mathbb{Q}_N$ a Q_N diagonální:

$$\mathbb{Q}_N = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & N-1 \end{pmatrix}, \qquad Q_N = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \omega_N & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \omega_N^{N-1} \end{pmatrix}.$$

Platí, že $P_N = \exp(\frac{2\pi i}{N}\mathcal{F}_N^{-1}\mathbb{Q}_N\mathcal{F}_N)$ a z definice exponenciály proto plyne, že $P_N = \mathcal{F}_N^{-1}Q_N\mathcal{F}_N$. Pro prvky matice $\mathcal{F}_N$ ve standardní bázi platí $(\mathcal{F}_N)_{i,j} = \frac{1}{\sqrt{N}}\omega_N^{ij}$ a $(\mathcal{F}_N^{-1})_{i,j} = \frac{1}{\sqrt{N}}\omega_N^{-ij}$. Výpočtem dostaneme

$$P_N = \begin{pmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & & & 1 \\ 1 & 0 & \dots & 0 \end{pmatrix}.$$

Tvar $\mathbb{P}_N$ je pro nás nezajímavý a nebudeme ho proto hledat. Operátory Q_N a P_N lze definovat pomocí jejich působení na bázi následovně:

$$Q_N |n\rangle = \omega_N^n |n\rangle,$$
$$P_N |n\rangle = |n - 1 \pmod N\rangle$$

pro všechna $n \in \mathbb{Z}_N$.

Poznámka. Matice Q_N, respektive P_N ve standardní bázi odpovídají Pauliho X-, respektive Z-maticím.

Dále platí pro tyto operátory vztah analogický komutačnímu vztahu mezi $U(t)$ a $V(s)$:

$$P_N^i Q_N^j = \omega_N^{ij} Q_N^j P_N^i,$$

což vyplyne z tvrzení 2.6.

Ve třetí kapitole pak definujeme Cliffordovu grupu jako největší grupu unitárních operátorů zachovávajících Weylovu-Heisenbergovu grupu a později dokážeme, že má strukturu semidirektního součinu.

2 Weylovy-Heisenbergovy grupy

V této kapitole definujeme Weylovu-Heisenbergovu grupu, což je základní pojem v této práci. Pak prozkoumáme některé její vlastnosti a nakonec si ukážeme jak souvisí s grupou $\mathbb{Z}_N \times \mathbb{Z}_N$.

Definice 2.1. *Nechť $\mathcal{B} = \{|n\rangle \mid n \in \mathbb{Z}_N\}$ je ortonormální báze Hilbertova prostoru $\mathcal{H}_N$. Definujme*

$$\omega_N = e^{\frac{2\pi i}{N}}.$$

Dále definujme operátory P_N a Q_N jako v předchozí kapitole:

$$\begin{aligned} Q_N |n\rangle &= \omega_N^n |n\rangle, \\ P_N |n\rangle &= |n-1 \pmod N\rangle \end{aligned}$$

pro všechny $|n\rangle \in \mathcal{B}$.

Poznámka. Lze snadno ověřit, že pro operátory Q_N a P_N platí

$$\begin{aligned} Q_N &= \textstyle\sum_{i\in\mathbb{Z}_N} |i\rangle\, \omega^i \,\langle i|, \\ P_N &= \textstyle\sum_{i\in\mathbb{Z}_N} |i-1\rangle\,\langle i| \end{aligned}$$

Definice 2.2. *Řekneme, že operátor $X \in \mathcal{L}(\mathcal{H}_N)$ je unitární, jestliže platí $X^\dagger = X^{-1}$.*

Poznámka. Operátor $X \in \mathcal{L}(\mathcal{H}_N)$ je unitární právě tehdy, když zachovává skalární součin, tj. platí $\langle x|X^\dagger X|y\rangle = \langle x|y\rangle$ pro všechny $|x\rangle, |y\rangle \in \mathcal{H}_N$.

Tvrzení 2.3. *Operátory P_N, Q_N jsou unitární.*

Důkaz. Nechť $|j\rangle, |k\rangle \in \mathcal{B}$.

$$\begin{aligned} \langle j|P_N^\dagger P_N|k\rangle = \langle j-1|k-1\rangle = \delta_{j-1,k-1} = \delta_{jk} = \langle j|k\rangle, \\ \langle j|Q_N^\dagger Q_N|k\rangle = \omega_N^{k-j}\,\langle j|k\rangle = \omega_N^{k-j}\delta jk = \langle j|k\rangle \end{aligned}$$

Operátory P_N, Q_N tedy zachovávají skalární součin pro bazické vektory. Snadno se pak ukáže, že operátory P_N a Q_N zachovávají skalární součin i pro obecné vektory $|x\rangle, |y\rangle \in \mathcal{H}_N$. □

Tvrzení 2.4. *Pro operátory Q_N a P_N platí*

1. $P_N Q_N = \omega_N Q_N P_N$,

2. $Q_N^N = P_N^N = I$.

Důkaz. Stačí zkoumat působení operátorů na vektory báze.

1. $P_N Q_N |j\rangle = \omega_N^j P_N |j\rangle = \omega_N^j |j - 1 \pmod N\rangle$,
   $\omega_N Q_N P_N |j\rangle = \omega_N Q_N |j - 1 \pmod N\rangle = \omega_N^j |j - 1 \pmod N\rangle$,

2. $Q_N^N |j\rangle = \omega_N^{jN} |j\rangle = |j\rangle$,
   $P_N^N |j\rangle = |j - N \pmod N\rangle = |j\rangle$.

□

Poznámka. Odteď budeme namísto Q_N, P_N, ω_N psát jen Q, P, ω.

Poznámka. Pro zjednodušení zápisu budeme odteď předpokládat, že pro $N > 1$ je sčítání a odčítání v rámci indexace v bra a ketech vždy modulo N.

Definice 2.5. *Weylovu-Heisenbergovu grupu definujeme jako množinu*

$$H(N) := \{zQ^i P^j \mid z \in \mathbb{C}, |z| = 1,\ i, j = 0, ..., N\}.$$

s grupovou operací skládání zobrazení.

Poznámka. Weylova-Heisenbergova grupa je někdy definovaná jako určitá konečná podgrupa $H(N)$, například v [2, 3, 4, 6]. Bývá ale definována zvlášť pro liché a sudé N, což bez dostatečného zdůvodnění působí neintuitivně. My ji definujeme podle [7].

Poznámka. Platí, že $H(N) \leq \mathrm{U}(N)$.

Tvrzení 2.6. *Nechť* $a_1, ..., a_n,\ b_1, ..., b_n \in \mathbb{N} \setminus \{1\}$. *Pak*

$$Q^{a_1} P^{b_1} ... Q^{a_n} P^{b_n} = \omega^{\sum_{1 \leq i < k \leq n} a_k b_i} Q^{\sum_{i=1}^n a_i} P^{\sum_{i=1}^n b_i}.$$

Důkaz. Důkaz provedeme matematickou indukcí. Nejprve tvrzení dokážeme pro n=2.

$$\begin{gathered} Q^{a_1} P^{b_1} Q^{a_2} P^{b_2} = Q^{a_1} P^{b_1 - 1} (PQ) Q^{a_2 - 1} P^{b_2} = Q^{a_1} P^{b_1 - 1} \omega QPQ^{a_2 - 1} P^{b_2} = \\ = Q^{a_1} P^{b_1 - 1} \omega^2 Q^2 P Q^{a_2 - 2} P^{b_2} = ... = \omega^{a_2} Q^{a_1} P^{b_1 - 1} Q^{a_2} P^{b_2 + 1} = ... = \\ = \omega^{2a_2} Q^{a_1} P^{b_1 - 2} Q^{a_2} P^{b_2 + 2} = ... = \omega^{b_1 a_2} Q^{a_1 + a_2} P^{b_1 + b_2}. \end{gathered}$$

Nyní ukážeme, že pokud tvrzení platí pro n, pak platí i pro $n + 1$. Máme

$$Q^{a_1}P^{b_1}...Q^{a_{n+1}}P^{b_{n+1}} = \omega^{\sum_{1\le i<k\le n} a_k b_i} Q^{\sum_{i=1}^{n} a_i} P^{\sum_{i=1}^{n} b_i} Q^{a_{n+1}} P^{b_{n+1}} = \\ = \omega^{\sum_{1\le i<k\le n} a_k b_i} \omega^{(\sum_{i=1}^{n} b_i)a_{n+1}} Q^{\sum_{i=1}^{n+1} a_i} P^{\sum_{i=1}^{n+1} b_i} = \\ = \omega^{\sum_{1\le i<k\le n+1} a_k b_i} Q^{\sum_{i=1}^{n+1} a_i} P^{\sum_{i=1}^{n+1} b_i}.$$

Tím je tvrzení dokázáno. □

Lemma 2.7. *Nechť $X \in \mathrm{GL}(\mathcal{H}_N)$ a nechť $QX = \alpha XQ$ a $PX = \beta XP$, kde $\alpha, \beta \in \mathbb{C} \setminus \{0\}$. Pak existuje $H \in H(N)$ a $z \in \mathbb{C} \setminus \{0\}$ takové, že $X = zH$.*

Důkaz. Důkaz provedeme podle [4]. Nechť $X = \sum_{i,j=0}^{N-1} x_{ij} |i\rangle \langle j|$. Pak

$$QX = (\sum_{i=0}^{N-1} \omega^i |i\rangle \langle i|)(\sum_{j,k=0}^{N-1} x_{kj} |k\rangle \langle j|) = \sum_{i,j,k=0}^{N-1} \omega^i x_{kj} \delta_{ik} |i\rangle \langle j| = \\ = \sum_{i,j=0}^{N-1} \omega^i x_{ij} |i\rangle \langle j|, \\ \alpha XQ = \alpha(\sum_{i,j=0}^{N-1} x_{ij} |i\rangle \langle j|)(\sum_{k=0}^{N-1} \omega^k |k\rangle \langle k|) = \alpha \sum_{i,j=0}^{N-1} x_{ij} \omega^j |i\rangle \langle j|.$$

Porovnáním dostaneme, že $(\omega^{i-j} - \alpha)x_{ij} = 0$ pro všechna i, j. Protože $X \in \mathrm{GL}(\mathcal{H}_N)$, existují i_0, j_0 takové, že $x_{i_0 j_0} \neq 0$ a $\alpha = \omega^{i_0 - j_0}$. Dále platí $x_{ij} = 0$ pro $i - j \neq i_0 - j_0 \pmod N$. Máme tedy $x_{ij} = \delta_{i,j+i_0-j_0} c_i$, kde $c_i \in \mathbb{C}$. Položme $D = \mathrm{diag}(c_0, ..., c_{N-1})$. Lze snadno ověřit, že $X = P^{j_0 - i_0} D$ a $D \neq 0$. Podle předpokladů platí $PX = \beta XP$, a proto i $PD = \beta DP$. Odtud máme

$$PD = (\sum_{i=0}^{N-1} |i-1\rangle \langle i|)(\sum_{j=0}^{N-1} c_j |j\rangle \langle j|) = \sum_{i=0}^{N-1} c_i |i-1\rangle \langle i|, \\ \beta DP = \beta(\sum_{j=0}^{N-1} c_j |j\rangle \langle j|)(\sum_{i=0}^{N-1} |i-1\rangle \langle i|) = \beta \sum_{i=0}^{N-1} c_{i-1} |i-1\rangle \langle i|.$$

Platí proto $c_i = \beta c_{i-1}$ pro všechna i, $c_j = \beta^j c_0$ a $c_0 = \beta^N c_0$. Jelikož $D \neq 0$, máme $c_0 \neq 0$ a $\beta^N = 1$. Proto platí $\beta = \omega^k$ pro nějaké $k \in \{0, ..., N-1\}$ a $D = Q^k(c_0 I)$. Položme nyní $H = P^{j_0 - i_0} Q^k \in H(N)$ a $z = c_0 \in \mathbb{C} \setminus 0$. Dostáváme $X = zH$. □

Poznámka. Pokud zůstaneme při značení z důkazu lemmatu 2.7, pak platí $X = zP^{j_0 - i_0} Q^k$. Pokud bychom předpokládali, že X je unitární, pak by platilo $zI \in \mathrm{U}(1)$, a tedy $X \in H(N)$.

Věta 2.8. *Nechť $X \in GL(\mathcal{H}_N)$, $PX = XP$ a $QX = XQ$. Pak existuje $c \in \mathbb{C} \setminus \{0\}$ takové, že $X = cI$.*

Důkaz. Použijeme lemma 2.7 pro případ, kdy $\alpha = \beta = 1$. Máme $X = zQ^i P^j$, kde $z \in \mathbb{C} \setminus \{0\}, i, j \in \{0, ..., N-1\}$. Podle předpokladů dále platí

$$zQ^{i+1}P^j = QX = XQ = zQ^i(P^j Q) = z\omega^j Q^{i+1} P^j, \\ zQ^i P^{j+1} = XP = PX = z(PQ^i)P^j = z\omega^i Q^i P^{j+1},$$

kde poslední rovnosti na obou řádcích se získají opakovaným použitím prvního bodu tvrzení 2.4. Z předpokladů věty dostáváme $i = j = 0 \pmod N$, tedy $X = zI$. □

Definice 2.9. *Nechť G je grupa a $g \in G$. Pak zobrazení $\mathrm{Ad}_g : G \to G$ definované jako $\mathrm{Ad}_g(a) := gag^{-1}$ pro $a \in G$ se nazývá vnitřní automorfismus grupy G. Množina vnitřních automorfismů grupy G tvoří grupu, kterou značíme $\mathrm{Int}(G)$.*

Definice 2.10. *Nechť $N \in \{2, 3, ...\}$. Pak $\mathcal{P}_N$ značí podgrupu $\mathrm{Int}(\mathrm{GL}(\mathcal{H}_N))$ generovanou prvky Ad_Q, Ad_P. Symbolicky*

$$\mathcal{P}_N := \langle Ad_Q,\ Ad_P \rangle.$$

Z fyzikálního hlediska jsou dva kvantové stavy, které se liší jen o fázový faktor, nerozlišitelné, a proto, jak uvidíme v tvrzení 2.20, lze od Weylovy-Heisenbergovy grupy přejít ke grupě $\mathcal{P}_N$. Například v článku [4] se pracuje primárně s tímto alternativním popisem, a proto ho pro úplnost zavádíme.

Tvrzení 2.11. *Nechť $M,\ N \in \mathrm{GL}(\mathcal{H}_N)$. Pak platí*

1. *$Ad_M Ad_N = Ad_{MN}$,*
2. *$Ad_{M^{-1}} = (Ad_M)^{-1}$,*
3. *$Ad_M = Ad_N$ právě tehdy, když existuje $c \in \mathbb{C} \setminus \{0\}$ takové, že $M = cN$.*

Důkaz. 1. Nechť $X \in \mathrm{GL}(\mathcal{H}_N)$. Pak

$$\mathrm{Ad}_M \mathrm{Ad}_N X = \mathrm{Ad}_M(NXN^{-1}) = MNXN^{-1}M^{-1} = MNX(MN)^{-1} = \\ = \mathrm{Ad}_{MN} X.$$

2. Z předchozího bodu plyne, že

$$\mathrm{Ad}_M \mathrm{Ad}_{M^{-1}} = \mathrm{Ad}_{M^{-1}} \mathrm{Ad}_M = \mathrm{Ad}_I = I,$$

tedy $\mathrm{Ad}_{M^{-1}} = (\mathrm{Ad}_M)^{-1}$.

3. $\Leftarrow$: Plyne z toho, že $(cN)^{-1} = \frac{1}{c} N^{-1}$.

$\Rightarrow$: Nechť $\mathrm{Ad}_M X = \mathrm{Ad}_N X$ pro všechna $X \in \mathrm{GL}(\mathcal{H}_N)$. Pak $MXM^{-1} = NXN^{-1}$ a ekvivalentně $N^{-1}MX = XN^{-1}M$. Prvek $N^{-1}M$ tedy komutuje se všemi $X \in \mathrm{GL}(\mathcal{H}_N)$ a speciálně i s Q a P. Z věty 2.8 plyne, že existuje $c \in \mathbb{C} \setminus \{0\}$ tak, že $N^{-1}M = cI$. Platí tedy $M = cN$, čímž je ekvivalence dokázána.

□

Poznámka. Z tvrzení 2.11 plyne, že zobrazení Ad: $G \to \mathrm{Int}(G)$ je grupový homomorfismus pro $G = \mathrm{GL}(\mathcal{H}_N)$. Pro obecnou grupu G to lze dokázat analogicky.

Definice 2.12. *Nechť G je grupa a $H \leq G$. Definujme normalizátor H v G následovně:*

$$\mathcal{N}_G(H) := \{x \in G \mid xHx^{-1} = H\}.$$

Definice 2.13. *Nechť G je grupa a $H \leq G$. Grupu H nazveme normální podgrupou grupy G, pokud $\mathcal{N}_G(H) = G$. Značíme $H \trianglelefteq G$.*

Definice 2.14. *Nechť G je grupa a $H \leq G$ a $g \in G$. Pak množiny $gH = \{gh \mid h \in H\}$, respektive $Hg = \{hg \mid h \in H\}$ nazýváme levé, respektive pravé rozkladové třídy H v G. Libovolný prvek třídy nazveme jejím reprezentantem.*

Tvrzení 2.15. *Nechť G je grupa, $H \leq G$ a $u, v \in G$. Pak $uH = vH$ právě tehdy, když u a v jsou reprezentanti stejné levé rozkladové třídy.*

Důkaz. Důkaz provedeme podle [5]. Nechť $x \in uH \cap vH$. Pak platí

$$x = un = vm$$

pro nějaké $n, m \in H$. Vynásobením rovnosti prvkem n^{-1} zprava dostaneme

$$u = vmn^{-1},$$

kde $mn^{-1} \in H$. Pro libovolné $t \in H$ pak platí

$$ut = v(mn^{-1}t).$$

Proto platí, že $uH \subset vH$. Opačná inkluze se dokáže analogicky. Pokud tedy mají dvě levé rozkladové třídy neprázdný průnik, jsou totožné. Máme tedy, že $uH = vH$ právě tehdy, když $u \in vH$, což je ekvivalentní tomu, že u je reprezentant vH. □

Poznámka. Analogické tvrzení platí pro pravé rozkladové třídy.

Definice 2.16. *Nechť G je grupa a $M, N \subset G$. Pak definujeme součin množin:*

$$M \cdot N := \{mn \mid m \in M, n \in N\}.$$

Tvrzení 2.17. *Nechť G je grupa, $H \trianglelefteq G$. Pak množina levých rozkladových tříd H v G s operací definovanou $uH \cdot vH = (uv)H$ tvoří grupu.*

Důkaz. Nechť $u, v \in G$ a $m, n \in H$. Pak

$$(un)(vm) = (uvv^{-1}n)(vm) = (uv)(v^{-1}nv)m = (uv)n'm,$$

kde $n' \in H$, jelikož $H \trianglelefteq G$. Odtud plyne $uH \cdot vH \subset (uv)H$. Dále máme

$$(uv)m = (uv)(mn)(v^{-1}v)n^{-1} = u(vmnv^{-1})vn^{-1} = um'vn^{-1},$$

kde $m' \in H$. Platí tedy $(uv)H \subset uH \cdot vH$, a proto $(uv)H = uH \cdot vH$. Z této rovnosti podle tvrzení 2.15 plyne, že operace je dobře definovaná.

Odtud plyne, že jednotkový prvek je eH a inverzní prvek k uH je $u^{-1}H$. Asociativita se snadno ověří. □

Poznámka. Pro jednoduchost budeme odteď psát namísto $uH \cdot vH$ psát jen $uHvH$.

Definice 2.18. *Nechť G je grupa, $H \trianglelefteq G$. Grupu definovanou v předchozím tvrzení nazýváme faktorgrupou G podle H, značíme G/H.*

Tvrzení 2.19. *Nechť G, H jsou grupy a $\varphi : G \to H$ je homomorfismus. Pak φ je prostý právě tehdy, když* $\mathrm{Ker}(\varphi) = \{1_G\}$.

Důkaz. Nechť $\mathrm{Ker}(\varphi) = \{1_G\}$ a $g_1, g_2 \in G$ jsou takové, že $g_1 \neq g_2$. Pak

$$\varphi(g_1) = \varphi(g_2 g_2^{-1} g_1) = \varphi(g_2)\varphi(g_2^{-1}g_1) \neq \varphi(g_2),$$

což znamená, že φ je prosté. Ukažme nyní obrácenou implikaci. Pro libovolné $g \in G$ a $g' \in G$ takové, že $\varphi(g') = 1_H$, platí

$$\begin{aligned} \varphi(g)1_H = \varphi(g) = \varphi(g1_G) = \varphi(g)\varphi(1_G), \\ \varphi(g) = \varphi(g)1_H = \varphi(g)\varphi(g') = \varphi(gg'). \end{aligned}$$

První řádek ukazuje, že $\{1_G\} \subset \mathrm{Ker}(\varphi)$ a druhý, že je-li $\varphi(g') = 1_H$, pak $g' = 1_G$ kvůli prostotě φ. Tím je tvrzení dokázáno. □

Tvrzení 2.20. *Platí*

$$H(N)/\mathrm{U}(1) \cong (\mathbb{Z}_N \times \mathbb{Z}_N) \cong \mathcal{P}_N$$

Důkaz. 1. Definujme zobrazení $\theta : (\mathbb{Z}_N \times \mathbb{Z}_N) \to H(N)/\mathrm{U}(1)$ tak, že $\theta(i,j) = Q^i P^j \mathrm{U}(1)$. Pak platí

$$\theta(i+i', j+j') = Q^{i+i'} P^{j+j'} \mathrm{U}(1) = \omega^{-ji'} Q^i P^j Q^{i'} P^{j'} \mathrm{U}(1) = \\ = Q^i P^j Q^{i'} P^{j'} \mathrm{U}(1) = \theta(i,j)\theta(i',j'),$$

kde druhá rovnost plyne z tvrzení 2.6. Všechny prvky $H(N)/\mathrm{U}(1)$ mají tvar $Q^i P^j \mathrm{U}(1)$, a proto $\theta(\mathbb{Z}_N \times \mathbb{Z}_N) = H(N)/\mathrm{U}(1)$. Homomorfismus θ je proto surjektivní. Mějme (k,l) takové, že $\theta(k,l) = \mathrm{U}(1)$, tedy $Q^k P^l \mathrm{U}(1) = \mathrm{U}(1)$. Pak $k = l = 0$, jelikož grupa $\mathrm{U}(1)$ obsahuje jen násobky jednotkového operátoru. Vzor $\mathrm{U}(1)$ je tedy $\{(0,0)\}$, což podle tvrzení 2.19 znamená, že homomorfismus θ je prostý. Celkově $H(N)/\mathrm{U}(1) \cong (\mathbb{Z}_N \times \mathbb{Z}_N)$.

2. Definujme zobrazení $\Theta : (\mathbb{Z}_N \times \mathbb{Z}_N) \to \mathcal{P}_N$ tak, že $\Theta(i,j) = \mathrm{Ad}_{Q^i P^j}$. Pak platí

$$\Theta(i+i', j+j') = \mathrm{Ad}_{Q^{i+i'} P^{j+j'}} = \mathrm{Ad}_{Q^i P^j} \mathrm{Ad}_{Q^{i'} P^{j'}} = \Theta(i,j)\Theta(i',j'),$$

kde ve druhé rovnosti se využije první bod tvrzení 2.4 a první a třetí bod tvrzení 2.11. Zobrazení Θ je tedy homomorfismus. Surjektivita Θ se dokáže podobnou úvahou jako v předchozí části důkazu. Zřejmě platí, že $\Theta(0,0) = \mathrm{Ad}_I$ a z třetího bodu tvrzení 2.11 plyne, že vzor $\mathrm{Ad}_I = \{(0,0)\}$, čímž je dokázána i prostota Θ. Opět tedy máme $\mathcal{P}_N \cong (\mathbb{Z}_N \times \mathbb{Z}_N)$.

□

3 Cliffordovy grupy

V této kapitole budeme zkoumat Cliffordovu grupu, její souvislost s grupou $\mathrm{SL}(2,\mathbb{Z}_N)$, pak definujeme semidirektní součin grup a nakonec se podíváme na to, zda Cliffordova grupa má strukturu semidirektního součinu.

3.1 Cliffordovy grupy

Definice 3.1. *Normalizátor Weylovy-Heisenbergovy grupy v grupě unitárních operátorů* $\mathrm{U}(N)$ *nazveme Cliffordovou grupou, značíme*

$$\mathcal{C}(N) := \mathcal{N}_{\mathrm{U(N)}}(H(N)).$$

Poznámka. Cliffordova grupa $\mathcal{C}(N)$ je grupa unitárních operátorů, jejichž Ad-akce zachovává grupu $H(N)$. Z tvrzení 2.11 plyne, že Ad-akce unitárních operátorů, které se liší o fázový faktor, je stejná, a proto má smysl je ztotožnit. Smysl této definice se ukáže hlavně v kapitole 4.

Definice 3.2. *Projektivní Cliffordovu grupu definujeme následovně:*

$$\widetilde{\mathcal{C}}(N) := \mathcal{C}(N)/\mathrm{U}(1).$$

Zkoumejme nyní působení prvků $\mathcal{C}(N)$ na $H(N)$. Nechť $X \in \mathcal{C}(N)$. Pak platí

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

pro nějaká $a, b, c, d \in \{0, ..., N-1\}$ a $\alpha, \beta \in \mathbb{C}$ taková, že $|\alpha| = |\beta| = 1$.

Definujme zobrazení

$$\phi : X \mapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix},$$

kde $X \in \mathcal{C}(N)$ a $a, b, c, d \in \mathbb{Z}_N$.

Tvrzení 3.3. *Zobrazení* ϕ *je homomorfismus z* $\mathcal{C}(N) \to SL(2,\mathbb{Z}_N)$.

Důkaz. Nechť $X, X' \in \mathcal{C}(N)$. Dále nechť X působí na Q a P jako výše a

$$X'QX'^{-1} = \alpha' Q^{a'} P^{b'},\ X'PX'^{-1} = \beta' Q^{c'} P^{d'}.$$

Pak platí

$$\begin{gathered} XX'Q(XX')^{-1} = X(X'QX'^{-1})X^{-1} = X(\alpha' Q^{a'} P^{b'})X^{-1} = \\ = \alpha'(\alpha Q^a P^b)^{a'}(\beta Q^c P^d)^{b'} = \alpha'\alpha^{a'}\beta^{b'}\omega^{\frac{a'(a'-1)}{2}ab} Q^{aa'} P^{ba'} \omega^{\frac{b'(b'-1)}{2}cd} Q^{cb'} P^{db'} = \\ = \alpha'\alpha^{a'}\beta^{b'}\omega^{\frac{a'(a'-1)}{2}ab + \frac{b'(b'-1)}{2}cd + ba'cb'} Q^{aa'+cb'} P^{ba'+db'}, \end{gathered}$$

kde v posledních dvou rovnostech jsme použili tvrzení 2.6. Podobně dostaneme

$$XX'P(XX')^{-1} = \beta'\alpha^{c'}\beta^{d'}\omega^{\frac{c'(c'-1)}{2}ab + \frac{d'(d'-1)}{2}cd + bcc'd'} Q^{ac'+cd'} P^{bc'+dd'}.$$

Platí tedy

$$\phi(XX') = \begin{pmatrix} aa'+cb' & ac'+cd' \\ ba'+db' & bc'+dd' \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \phi(X)\phi(X'),$$

a ϕ je proto homomorfismus. Dále platí

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

kde poslední rovnosti na obou řádcích plynou z tvrzení 2.6. Podle tvrzení 2.4 platí $PQ = \omega QP$ a porovnáním výrazů výše dostaneme

$$\omega^{ad} = \omega^{1+bc}.$$

Odtud plyne, že $\det(\phi(X)) = ad - bc = 1 \pmod N$ pro všechna $X \in \mathcal{C}_N$. □

Podívejme se nyní, čemu se rovná $\phi(H(N))$. Nechť $\gamma \in \mathrm{U}(1)$ a $i, j \in \mathbb{Z}_N$. Pak

$$\begin{aligned} \gamma Q^i P^j Q(\gamma Q^i P^j)^{-1} = \gamma Q^i (P^j Q)\gamma^{-1} P^{-j} Q^{-i} = Q^i(\omega^j Q P^j) P^{-j} Q^{-i} = \omega^j Q, \\ \gamma Q^i P^j P \gamma^{-1} P^{-j} Q^{-i} = (Q^i P) Q^{-i} = (\omega^{-i} P Q^i) Q^{-i} = \omega^{-i} P, \end{aligned}$$

kde druhá rovnost na obou řádcích plyne z tvrzení 2.4. Zřejmě tedy pro libovolné $H \in H(N)$ platí $\phi(H) = I$ a jelikož ϕ je homomorfismus, platí také pro libovolné $X \in \mathcal{C}(N)$

$$\phi(XH) = \phi(X)\phi(H) = \phi(X)I = \phi(X).$$

Z hlediska jejich ϕ-obrazu lze tedy všechny prvky $\mathcal{C}(N)$, které se liší jen o násobek prvkem $H(N)$, ztotožnit.

Definice 3.4. *Faktorgrupu Cliffordovy grupy podle Weylovy-Heisenbergovy grupy značíme*

$$\mathcal{C}'(N) = \mathcal{C}(N)/H(N).$$

Poznámka. Jednotkový prvek v grupě $\mathcal{C}'(N)$ je $H(N)$.

Chtěli bychom nyní zavést homomorfismus $\Phi : \mathcal{C}'(N) \to \mathrm{SL}(2, \mathbb{Z}_N)$ podobně jako výše. Z úvah nad definicí 3.4 plyne, že při počítání výrazů XQX^{-1} a XPX^{-1}, kde X je tentokrát nějaká rozkladová třída z $\mathcal{C}'(N)$, stačí vybrat jejího libovolného reprezentanta. Zobrazení Φ je proto dobře definováno.

Tvrzení 3.5. *Zobrazení $\Phi : \mathcal{C}'(N) \to \mathrm{SL}(2, \mathbb{Z}_N)$ je homomorfismus.*

Důkaz. Důkaz je zcela analogický důkazu tvrzení 3.3, pouze X a X' budou prvky $\mathcal{C}'(N)$, z nichž vybereme nějaké fixní reprezentanty a s nimi budeme počítat. □

Lemma 3.6. *Homomorfismus Φ je prostý.*

Důkaz. Podle tvrzení 2.19 stačí ukázat, že $\mathrm{Ker}(\Phi) = \{H(N)\}$. Z úvah nad definicí 3.4 plyne $\{H(N)\} \subset \mathrm{Ker}(\Phi)$. Stačí proto ukázat, že platí opačná inkluze. Nechť $X' \in \mathrm{Ker}(\Phi), X \in X'$. Pak platí

$$XQX^{-1} = \alpha Q,$$
$$XPX^{-1} = \beta P$$

pro nějaké $\alpha, \beta \in \mathrm{U}(1)$. Podle lemmatu 2.7 a poznámky pod ním platí, že $X \in H(N)$. Platí proto $\mathrm{Ker}(\Phi) \subset \{H(N)\}$, čímž je důkaz ukončen. □

Nyní podle [2] definujeme operátory S_N a D_N, jejichž význam se ukáže v tvrzení 3.10.

Definice 3.7. *Nechť $\mathcal{B} = \{|0\rangle, ..., |N-1\rangle\}$ je ortonormální báze $\mathcal{H}_N$. Definujme*

$$\tau_N = -e^{\frac{\pi i}{N}}.$$

Dále definujeme operátory S_N, D_N následovně:

$$S_N \left|j\right\rangle = \tfrac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} \left|k\right\rangle,$$

$$D_N \left|j\right\rangle = \begin{cases} \tau_N^{j(1-j)} \left|j\right\rangle & \textit{pro } N \textit{ liché} \\ \tau_N^{j(N-j)} \left|j\right\rangle & \textit{pro } N \textit{ sudé.} \end{cases}$$

Poznámka. Operátor S_N odpovídá diskrétní Fourierově transformaci.

Poznámka. Odteď budeme namísto S_N, D_N, τ_N psát jen S, D, τ.

Poznámka. Pro $k \in \mathbb{N}$ platí

$$\frac{1}{N} \sum_{i=0}^{N-1} \omega^k = \begin{cases} 1 & \text{pro } k = 0 \pmod N \\ \frac{1}{N} \frac{\omega^{kN}-1}{\omega^k-1} = 0 & \text{pro } k \ \neq 0 \pmod N. \end{cases}$$

Tvrzení 3.8. *Operátory S, D jsou unitární.*

Důkaz. Stačí ukázat, že operátory zachovávají skalární součin. Máme

$$\langle j|S^\dagger S|k\rangle = \tfrac{1}{N} \sum_{m,n=0}^{N-1} \omega^{-mj} \omega^{nk} \langle m|n\rangle = \tfrac{1}{N} \sum_{n=0}^{N-1} \omega^{n(k-j)} = \delta_{jk} = \langle j|k\rangle,$$
$$\langle j|D^\dagger D|k\rangle = \tau^{-j(x-j)} \tau^{j(x-j)} \langle j|k\rangle = \langle j|k\rangle,$$

kde $x = 1$ pro N liché a $x = N$ pro N sudé. □

Tvrzení 3.9. *Platí následující vztahy:*

$$SQS^{-1} = P,$$
$$SPS^{-1} = Q^{-1},$$
$$DQD^{-1} = Q,$$

$$DPD^{-1} = \begin{cases} QP & \textit{pro } N \textit{ liché} \\ \tau^{N+1} QP & \textit{pro } N \textit{ sudé.} \end{cases}$$

Důkaz. Stačí zkoumat působení operátorů na bazické vektory.

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

$$SQ \left|j\right\rangle = \omega^j S \left|j\right\rangle = \tfrac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{j(k+1)} \left|k\right\rangle,$$
$$PS \left|j\right\rangle = \tfrac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} P \left|k\right\rangle = \tfrac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} \left|k-1\right\rangle =$$
$$= \tfrac{1}{\sqrt{N}} (\sum_{k=1}^{N-1} \omega^{jk} \left|k-1\right\rangle + \left|N-1\right\rangle) = \tfrac{1}{\sqrt{N}} (\sum_{k=0}^{N-2} \omega^{j(k+1)} \left|k\right\rangle + \left|N-1\right\rangle) =$$
$$= \tfrac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{j(k+1)} \left|k\right\rangle.$$

Porovnáním dostaneme $SQ = PS$.

2. $SPS^{-1} = Q^{-1} \iff SP = Q^{-1}S$.

$$SP\,|j\rangle = S\,|j-1\rangle = \tfrac{1}{\sqrt{N}} \textstyle\sum_{k=0}^{N-1} \omega^{(j-1)k}\,|k\rangle,$$
$$Q^{-1}S\,|j\rangle = \tfrac{1}{\sqrt{N}} \textstyle\sum_{k=0}^{N-1} \omega^{jk} Q^{-1}\,|k\rangle = \tfrac{1}{\sqrt{N}} \textstyle\sum_{k=0}^{N-1} \omega^{(j-1)k}\,|k\rangle.$$

Porovnáním dostaneme $SP = Q^{-1}S$.

3. $DQD^{-1} = Q \iff DQ = QD$. Nechť $x = 1$ pro N liché a $x = N$ pro N sudé. Pak

$$DQ\,|j\rangle = \omega^j D\,|j\rangle = \omega^j \tau^{j(x-j)}\,|j\rangle,$$
$$QD\,|j\rangle = \tau^{j(x-j)} Q\,|j\rangle = \omega^j \tau^{j(x-j)}\,|j\rangle.$$

Porovnáním dostaneme $QD = DQ$.

4. $DPD^{-1} = \tau^{\alpha(N+1)}QP \iff DP = \tau^{\alpha(N+1)}QPD$, kde $\alpha = 0$ pro N liché a $\alpha = 1$ pro N sudé.

Nejprve nechť N je liché. Pak

$$DP\,|j\rangle = D\,|j-1\rangle = \tau^{(j-1)(1+1-j)}\,|j-1\rangle = \tau^{(j-1)(2-j)}\,|j-1\rangle,$$
$$QPD\,|j\rangle = \tau^{j(1-j)} QP\,|j\rangle = \tau^{j(1-j)} Q\,|j-1\rangle = \tau^{j(1-j)}\omega^{j-1}\,|j-1\rangle =$$
$$= \tau^{-j(j-1)}\tau^{2(j-1)}\,|j-1\rangle = \tau^{(j-1)(2-j)}\,|j-1\rangle.$$

Porovnáním dostaneme $DP = QPD$. Nyní nechť je N sudé. Pak platí

$$DP\,|j\rangle = D\,|j-1\rangle = \tau^{(j-1)(N+1-j)}\,|j-1\rangle = \tau^{-j^2+2j+Nj-1-N}\,|j-1\rangle,$$
$$\tau^{N+1}QPD\,|j\rangle = \tau^{N+1}\tau^{j(N-j)} QP\,|j\rangle = \tau^{N+1}\tau^{j(N-j)} Q\,|j-1\rangle =$$
$$= \tau^{N+1}\tau^{j(N-j)}\tau^{2(j-1)}\,|j-1\rangle = \tau^{-j^2+2j+Nj-1+N}.$$

Podle definice 3.7 platí, že $\tau^{2N} = 1$, a proto dostáváme $DP = \tau^{N+1}QPD$.

□

Poznámka. Z předchozího tvrzení vyplývá, že $S, D \in \mathcal{C}_N$ a $SH(N)$, $DH(N) \in \mathcal{C}'(N)$. Dále platí

$$\phi(S) = \Phi(SH(N)) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \phi(D) = \Phi(DH(N)) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Tvrzení 3.10. *Platí, že* $\mathrm{SL}(2,\mathbb{Z}_N) = \langle A, B\rangle$, *kde*

$$A = \Phi(DH(N)), \qquad B = \Phi(SH(N)).$$

Důkaz. Důkaz lze najít v [8]. □

Lemma 3.11. *Homomorfismus* Φ *je surjektivní.*

Důkaz. Nechť $C \in \mathrm{SL}(2,\mathbb{Z}_N)$. Pak podle tvrzení 3.10 existují čísla $i_1, ..., i_k, j_1, ..., j_k$ taková, že $C = \Phi(DH(N))^{i_1}\Phi(SH(N))^{j_1}...\Phi(DH(N))^{i_k}\Phi(SH(N))^{j_k}$. Navíc Φ je homomorfismus a proto

$$C = \Phi(DH(N))^{i_1}\Phi(SH(N))^{j_1}...\Phi(DH(N))^{i_k}\Phi(SH(N))^{j_k} = \\ = \Phi(D^{i_1}S^{j_1}...D^{i_k}S^{j_k}H(N)).$$

Pro každé $C \in \mathrm{SL}(2,\mathbb{Z}_N)$ tedy existuje $X \in \mathcal{C}'(N)$ takové, že $C = \Phi(X)$. □

Poznámka. Podobně platí, že ϕ je surjektivní.

Věta 3.12. *Platí* $\mathcal{C}'(N) \cong \mathrm{SL}(2,\mathbb{Z}_N)$.

Důkaz. Zobrazení Φ je podle tvrzení 3.5 homomorfismus, podle lemmatu 3.6 je prosté a podle lemmatu 3.11 surjektivní. □

3.2 Semidirektní součin

Nyní definujeme pojem semidirektního součtu dvou grup. Dokážeme tvrzení z první kapitoly, že grupa lineárních nehomogenních transformací je semidirektní součin grupy translací a grupy regulárních lineárních transformací a nakonec se podíváme, zda je možné vyjádřit projektivní Cliffordovu grupu jako semidirektní součin dvou jiných grup.

Náš postup zavedení semidirektního součinu je podobný postupu v [5].

Definice 3.13. *Nechť* G *je grupa. Grupu automorfismů grupy* G *značíme* $\mathrm{Aut}(G)$.

Tvrzení 3.14. *Nechť* H *a* K *jsou grupy a nechť* $\varphi : K \to \mathrm{Aut}(H)$ *je homomorfismus. Nechť* G *je množina uspořádaných dvojic* (h,k), *kde* $h \in H$ *a* $k \in K$. *Na* G *definujeme operaci*

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2).$$

Pak

1. *G s touto operací je grupa s jednotkovým prvkem $(1_H, 1_K)$ a $(h, k)^{-1} =$ $= (\varphi(k^{-1})(h^{-1}), k^{-1})$. Platí navíc $|G| = |H||K|$.*

2. *Označme $\widetilde{H} = \{(h, 1_K) \mid h \in H\}$. Pak $\widetilde{H} \trianglelefteq G$.*

Důkaz. Pro zjednodušení zápisu budeme namísto $\varphi(k)$ psát φ_k.

1. Uzavřenost G vůči zavedené operaci je zřejmá. Nechť $(h, k) \in G$. Pak

$$\begin{aligned}(h, k)(1_H, 1_K) &= (h\varphi_k(1_H), k1_K) = (h1_H, k1_K) = (h, k),\\ (1_H, 1_K)(h, k) &= (1_H\varphi_{1_K}(h), 1_Kk) = (1_H, 1_Kk) = (h, k),\end{aligned}$$

   $(1_H, 1_K)$ je tedy jednotkový prvek na G. Dále

$$\begin{gathered}(\varphi_{k^{-1}}(h^{-1}), k^{-1})(h, k) = (\varphi_{k^{-1}}(h^{-1})\varphi_{k^{-1}}(h), k^{-1}k) = (\varphi_{k^{-1}}(h^{-1}h), 1_K) =\\ = (\varphi_{k^{-1}}(1_H), 1_K) = (1_H, 1_K),\\ (h, k)(\varphi_{k^{-1}}(h^{-1}), k^{-1}) = (h\varphi_k(\varphi_{k^{-1}}(h^{-1})), kk^{-1}) =\\ = (h\varphi_{kk^{-1}}(h^{-1}), 1_K) = (hh^{-1}, 1_K) = (1_H, 1_K).\end{gathered}$$

   Platí tedy $(h, k)^{-1} = (\varphi(k^{-1})(h^{-1}), k^{-1})$. Nechť $(a, x), (b, y), (c, z) \in G$. Pak platí

$$\begin{gathered}((a, x)(b, y))(c, z) = (a\varphi_x(b), xy)(c, z) = (a\varphi_x(b)\varphi_{xy}(c), xyz) =\\ = (a\varphi_x(b)(\varphi_x \circ \varphi_y)(c), xyz) = (a\varphi_x(b)\varphi_x(\varphi_y(c)), xyz) =\\ = (a\varphi_x(b\varphi_y(c)), xyz) = (a, x)(b\varphi_y(c), yz) = (a, x)((b, y)(c, z)).\end{gathered}$$

   Operace je tedy asociativní a G je grupa. Řád G je zřejmý.

2. Nechť $(a, x) \in G$. Pak

$$\begin{gathered}(a, x)(h, 1_K)(a, x)^{-1} = (a\varphi_x(h), x1_K)(\varphi_{x^{-1}}(a^{-1}), x^{-1}) =\\ = (a\varphi_x(h)\varphi_x(\varphi_{x^{-1}}(a^{-1})), xx^{-1}) = (a\varphi_x(h)a^{-1}, 1_K) \in \widetilde{H}.\end{gathered}$$

   Platí proto $\widetilde{H} \trianglelefteq G$.

□

Definice 3.15. *Nechť H a K jsou grupy a $\varphi : K \to \mathrm{Aut}(H)$ je homomorfismus. Grupa popsaná v předchozím tvrzení se nazývá semidirektní součin H a K vzhledem k φ a značí se $H \rtimes_\varphi K$.*

Poznámka. Pokud bude φ zřejmé nebo pokud nás nebude zajímat, budeme namísto $H \rtimes_\varphi K$ psát jen $H \rtimes K$.

Poznámka. Uvažujme grupu translací v dvourozměrném prostoru T^2, speciální lineární grupu $\mathrm{SL}(2,\mathbb{R})$ a definujme $\varphi : \mathrm{SL}(2,\mathbb{R}) \to \mathrm{Aut}(T^2)$ tak, že $\varphi(A)(v) = Av$ pro všechna $A \in \mathrm{SL}(2,\mathbb{R})$ a $v \in T^2$, přičemž v značí translaci i její příslušný vektor. Matice A jsou regulární, a proto je $\varphi(A)$ skutečně automorfismus grupy T^2. Dále nechť $(v, A), (v', A') \in T^2 \rtimes_\varphi \mathrm{SL}(2,\mathbb{R})$. Pak platí

$$(v', A')(v, A) = (v' + \varphi(A')(v), A'A) = (v' + A'v, A'A),$$

což odpovídá skládání lineárních nehomogenních transformací. Proto skutečně platí $\widetilde{\mathrm{A}}(2,\mathbb{R}) = T^2 \rtimes \mathrm{SL}(2,\mathbb{R})$, respektive $\mathrm{A}(2,\mathbb{R}) = T^2 \rtimes \mathrm{GL}(2,\mathbb{R})$, jak bylo řečeno v první kapitole.

Tvrzení 3.16. *Mějme grupy $G,\ H,\ K$ takové, že $H \trianglelefteq G$ a nechť existuje epimorfismus $\pi : G \to K$ takový, že $\mathrm{Ker}(\pi) = H$. Pokud existuje homomorfismus $\sigma : K \to G$ takový, že $\pi \circ \sigma = Id_K$, pak $G \cong H \rtimes_\varphi K$, kde $\varphi : K \to \mathrm{Aut}(H)$ je homomorfismus takový, že platí $\varphi(k)(h) = \sigma(k)h\sigma(k)^{-1}$ pro $k \in K,\ h \in H$.*

Důkaz. Pro zjednodušení zápisu budeme opět namísto $\varphi(k)(h)$ psát $\varphi_k(h)$. Nejprve si uvědomme, že $H \trianglelefteq G$, a proto skutečně platí, že zobrazení $\varphi : K \to \mathrm{Aut}(H)$ je dobře definované a podle poznámky pod tvrzením 2.11 je to homomorfismus. Mějme zobrazení $\alpha : H \rtimes_\varphi K \to G$ takové, že $\alpha(h,k) = h\sigma(k)$ pro $h \in H,\ k \in K$. Nejprve ukažme, že α je homomorfismus. Nechť $h_1, h_2 \in H,\ k_1, k_2 \in K$. Pak

$$\begin{aligned}\alpha((h_1,k_1)(h_2,k_2)) &= \alpha(h_1\varphi_{k_1}(h_2), k_1k_2) = \alpha(h_1\sigma(k_1)h_2\sigma(k_1)^{-1}, k_1k_2) = \\ &= h_1\sigma(k_1)h_2\sigma(k_1)^{-1}\sigma(k_1)\sigma(k_2) = h_1\sigma(k_1)h_2\sigma(k_2) = \alpha(h_1,k_1)\alpha(h_2,k_2).\end{aligned}$$

Zobrazení α je tedy skutečně homomorfismus. Nyní dokažme, že α je prosté. Nechť $(h,k) \in H \rtimes_\varphi K$ takové, že $\alpha(h,k) = h\sigma(k) = 1_G$. Určitě platí $\pi(1_G) = 1_K$, jelikož π je homomorfismus. Pak

$$1_K = \pi(1_G) = \pi(h\sigma(k)) = \pi(h)\pi(\sigma(k)) = 1_K k = k,$$

kde $\pi(h) = 1_K$ platí, protože $\mathrm{Ker}(\pi) = H$ a využili jsme toho, že $\pi \circ \sigma = Id_K$. Platí, že $\sigma(1_K) = 1_G$, a proto $h = 1_H = 1_G$. Odtud máme $\mathrm{Ker}(\alpha) = \{(1_H, 1_K)\}$, což znamená, že α je prosté.

Zbývá ukázat, že α je surjektivní. Nechť $a \in G$. Platí, že $\mathrm{Ker}(\pi) = H$, takže $a \in H \iff \pi(a) = 1_K$. Zřejmě $g\sigma(\pi(g^{-1})) \in G$ pro libovolné $g \in G$. Pro π-obraz tohoto prvku platí

$$\pi(g\sigma(\pi(g^{-1}))) = \pi(g)\pi(\sigma(\pi(g^{-1}))) = \pi(g)\pi(g^{-1}) = \pi(gg^{-1}) = 1_K,$$

kde druhá rovnost plyne z toho, že $\pi \circ \sigma = Id_K$. Z úvah výše vyplývá, že $g\sigma(\pi(g^{-1})) \in H$. Spočítejme $\alpha(g\sigma(\pi(g^{-1})), \pi(g))$:

$$\alpha(g\sigma(\pi(g^{-1})), \pi(g)) = g\sigma(\pi(g)^{-1})\sigma(\pi(g)) = g\sigma(\pi(g)^{-1}\pi(g)) = g\sigma(1_K) = g.$$

Pro libovolný prvek $g \in G$ lze tedy najít $(h, k) \in H \rtimes_\varphi K$ takové, že $\alpha(h, k) = g$, čímž je dokázána surjektivita α. Celkově tedy platí $G \cong H \rtimes_\varphi K$. □

4 Weilova reprezentace pro liché N

V minulé kapitole jsme mluvili o Cliffordově grupě a o její souvislosti s grupou $\mathrm{SL}(2,\mathbb{Z}_N)$. Nyní by nás zajímalo, zda Cliffordova grupa má strukturu semidirektního součinu. Podle výsledků z předchozí kapitoly proto budeme hledat vhodný homomorfismus z $\mathrm{SL}(2,\mathbb{Z}_N)$ do $\mathcal{C}(N)$, respektive $\widetilde{\mathcal{C}}(N)$. Pro liché N jsou tyto homomorfismy známy jako Weilova reprezentace, respektive projektivní Weilova reprezentace.

Problematikou Weilovy reprezentace se zabývají například články [7, 9, 10], přičemž autoři těchto článků zřejmě pracovali nezávisle na sobě, jelikož byl všude použit zcela jiný postup. Náš postup v této kapitole vychází z [10].

4.1 Weylovy posunovací operátory

Nejprve zavedeme tak zvané Weylovy posunovací operátory, které generují jistou konečnou podgrupu Weylovy-Heisenbergovy grupy.

Definice 4.1. *Definujme množinu* $\mathcal{I} = \{0, 1, ..., N-1\}$.

Poznámka. Pokud nebude řečeno jinak, budeme v této kapitole sčítat vždy přes $\mathcal{I}$.

Definice 4.2. *Definujme Weylův posunovací operátor*

$$W_{m,n} := \omega^{2mn} Q^{2m} P^{2n},$$

kde $m, n \in \mathcal{I}$.

Poznámka. Weilova reprezentace je pojmenována po francouzském matematikovi Andrém Weilovi, zatímco Weylovy posunovací operátory jsou pojmenovány po německém matematikovi a fyzikovi Hermannovi Weylovi.

Tvrzení 4.3. *Operátory* $W_{m,n}$ *generují grupu* $\{\omega^i Q^j P^k \mid i, j, k \in \mathcal{I}\}$.

Důkaz. Pro důkaz stačí ukázat, že $\omega I, Q, P$ lze vyjádřit pomocí Weylových posunovacích operátorů. Operátor Q dostaneme volbou $m = \frac{N+1}{2},\ n = 0$ a P dostaneme pro $m = 0,\ n = \frac{N+1}{2}$. Podle tvrzení 2.4 platí $PQ = \omega QP$, odtud $\omega I = PQP^{-1}Q^{-1}$. □

Poznámka. Předchozí tvrzení platí, protože násobení číslem 2 je v $\mathbb{Z}_N$ bijekce pro liché N. To pro sudé N neplatí, a proto by pomocí operátorů $W_{m,n}$ nebylo možné vytvořit všechny možné mocniny operátorů Q a P. Proto postup v této kapitole není možné použít pro sudé N.

Poznámka. Připomínáme, že pro operátory Q a P platí

$$Q = \sum_{i\in\mathcal{I}} |i\rangle\, \omega^i\, \langle i|$$
$$P = \sum_{i\in\mathcal{I}} |i-1\rangle\, \langle i|$$

Tvrzení 4.4. *Nechť $n \in \mathbb{Z}$. Pak platí*

$$Q^n = \sum_k |k\rangle\, \omega^{kn}\, \langle k|,$$
$$P^n = \sum_k |k-1\rangle\, \langle k+n-1|.$$

Důkaz. Můžeme se omezit na případ , kdy $n \in \mathcal{I}$. Vztahy dokážeme matematickou indukcí. Pro $n = 0$ oba vztahy zřejmě platí. Nechť první vztah platí pro dané n. Potom

$Q^{n+1} = Q^n Q = (\sum_k |k\rangle\, \omega^{nk}\, \langle k|)(\sum_l |l\rangle\, \omega^l\, \langle l|) = \sum_{k,l} |k\rangle\, \omega^{nk+l}\, \langle k|l\rangle\, \langle l| =$
$= \sum_{k,l} |k\rangle\, \omega^{nk+l}\delta_{kl}\, \langle l| = \sum_k |k\rangle\, \omega^{(n+1)k}\, \langle k|.$

Tímto je vztah dokázán. Dále nechť druhý vztah platí pro dané n. Potom

$$P^{n+1} = P^n P = (\sum_k |k-1\rangle\, \langle k+n-1|\, (\sum_l |l-1\rangle\, \langle l|) =$$
$$= \sum_{k,l} |k-1\rangle\, \langle k+n-1|l-1\rangle\, \langle l| = \sum_{k,l} |k-1\rangle\, \delta_{k+n,l}\, \langle l| =$$
$$= \sum_k |k-1\rangle\, \langle k+n|.$$

Tímto je vztah dokázán. □

Tvrzení 4.5. *Nechť $m, n \in \mathcal{I}$. Potom platí*

$$W_{m,n} = \sum_j |j\rangle\, \omega^{2m(j+n)}\, \langle j+2n|.$$

Důkaz. Podle předchozího tvrzení platí

$$W_{m,n} = \omega^{2mn}(\sum_j |j\rangle\, \omega^{2mj}\, \langle j|)(\sum_k |k-1\rangle\, \langle k+2n-1|) =$$
$$= \omega^{2mn} \sum_{j,k} |j\rangle\, \omega^{2mj}\, \langle j|k-1\rangle\, \langle k+2n-1| =$$
$$= \omega^{2mn} \sum_j |j\rangle\, \omega^{2mj}\, \langle j+2n| = \sum_j |j\rangle\, \omega^{2m(j+n)}\, \langle j+2n|.$$

Tím je tvrzení dokázáno. □

4.2 Projektivní Weilova reprezentace

Jak bylo řečeno na začátku kapitoly, zajímá nás homomorfismus z grupy $\mathrm{SL}(2,\mathbb{Z}_N)$ do projektivní Cliffordovy grupy. Nejprve definujeme pojem reprezentace.

Definice 4.6. *Nechť G je grupa a V vektorový prostor nad tělesem $\mathbb{F}$. Pak homomorfismus $\rho : G \to \mathrm{GL}(V)$ nazýváme reprezentace grupy G. Projektivní reprezentace grupy G je homomorfismus $\rho' : G \to \mathrm{GL}(V)/\mathbb{F}^*$, kde $\mathbb{F}^*$ je grupa tvořená násobky jednotkového operátoru prvky tělesa $\mathbb{F}$.*

Poznámka. Nechť $\rho : G \to \mathrm{GL}(V)$ je zobrazení a nechť existuje zobrazení $\alpha : G \times G \to \mathbb{F} \setminus \{0\}$ takové, že platí $\rho(g)\rho(h) = \alpha(g,h)\rho(gh)$ pro všechna $g, h \in G$. Pak zobrazení $g \mapsto \rho(g)\mathbb{F}^*$ je projektivní reprezentace grupy G.

Definice 4.7. *Nechť $S \in \mathrm{SL}(2,\mathbb{Z}_N)$. Mějme zobrazení $U : \mathrm{SL}(2,\mathbb{Z}_N) \to \mathrm{U}(N)$ takové, že platí*

$$U(S)W_{m,n}U^\dagger(S) = W_{S\cdot(m,n)}$$

pro všechna $m, n \in \mathcal{I}$, kde $S\cdot(m,n)$ značí násobení matice S vektorem $(m,n)^T$. Zobrazení $\widetilde{\psi} : \mathrm{SL}(2,\mathbb{Z}_\mathrm{N}) \to \widetilde{\mathcal{C}}(N)$, $\widetilde{\psi}(S) = U(S)\mathrm{U}(1)$ říkáme projektivní Weilova reprezentace.

Poznámka. Musíme dokázat, že zobrazení $\widetilde{\psi}$ je homomorfismus, aby bylo jeho pojmenování oprávněné. Navíc zatím ani nevíme, zda takové zobrazení existuje. Dále poznamenejme, že zobrazení U, pokud existuje, kvůli tvrzení 4.3 zobrazuje do $\mathcal{C}(N)$ a proto zobrazení $\widetilde{\psi}$ skutečně zobrazuje do $\widetilde{\mathcal{C}}(N)$.

Tvrzení 4.8. *Pokud výše popsané zobrazení U existuje, pak zobrazení $\widetilde{\psi} : \mathrm{SL}(2,\mathbb{Z}_\mathrm{N}) \to \widetilde{\mathcal{C}}(N)$, $\widetilde{\psi}(S) = \mathrm{U}(S)\mathrm{U}(1)$, kde $S \in \mathrm{SL}(2,\mathbb{Z}_N)$, je homomorfismus a U je jednoznačné až na fázový faktor.*

Důkaz. Nechť $S, S', S'' \in \mathrm{SL}(2,\mathbb{Z}_N)$ jsou takové, že $S'' = S'S$. Pak platí, že

$$\begin{aligned} U(S'')W_{m,n}U^\dagger(S'') = W_{S''\cdot(m,n)} = W_{S'\cdot(S\cdot(m,n))} = U(S')W_{S\cdot(m,n)}U^\dagger(S') = \\ = U(S')U(S)W_{m,n}U^\dagger(S)U^\dagger(S'). \end{aligned}$$

Odtud dostáváme

$$U^\dagger(S'')U(S')U(S)W_{m,n} = W_{m,n}U^\dagger(S'')U(S')U(S).$$

To platí pro všechny $W_{m,n}$ a speciálně tedy i pro Q a P podle tvrzení 4.3. Podle věty 2.8 jediné unitární operátory, které komutují s Q a P, jsou jednotkové operátory vynásobené nějakým fázovým faktorem. Proto platí

$$U(SS') = e^{i\nu(S,S')}U(S)U(S').$$

Podle poznámky pod definicí 4.6 je $\widetilde{\psi}$ homomorfismus. Ukažme nyní jednoznačnost zobrazení U. Nechť U' je jiné zobrazení vyhovující naší definici. Pak

$$U'^{\dagger}(S)U(S)W_{m,n}U^{\dagger}(S)U'(S) = W_{S^{-1}S\cdot(m,n)} = W_{m,n}.$$

Podobným argumentem jako výše dostaneme

$$U'(S) = e^{i\nu'(S)}U(S).$$

□

Následující věta ukazuje význam definice projektivní Weilovy reprezentace.

Tvrzení 4.9. *Pokud projektivní Weilova reprezentace $\widetilde{\psi}$ existuje, pak platí, že*

$$\widetilde{\phi} \circ \widetilde{\psi} = Id_{\mathrm{SL}(2,\mathbb{Z}_N)},$$

kde $\widetilde{\phi} : \widetilde{\mathcal{C}}(N) \to \mathrm{SL}(2,\mathbb{Z}_N)$ je zobrazení definované tak, že pro každou rozkladovou třídu $\widetilde{X} \in \widetilde{\mathcal{C}}(N)$ platí $\widetilde{\phi}(\widetilde{X}) = \phi(X)$, kde X je libovolný reprezentant $\widetilde{X}$ a ϕ je homomorfismus z tvrzení 3.3.

Důkaz. Podle poznámky pod definicí 3.1 je zobrazení $\widetilde{\phi}$ dobře definované a snadno se ukáže, že je to homomorfismus. Mějme matici

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}_N).$$

Podle definice Weylových posunovacích operátorů platí $W_{\frac{N+1}{2},0} = Q$ a $W_{0,\frac{N+1}{2}} = P$. Platí

$$\begin{aligned} U(A)W_{\frac{N+1}{2},0}U(A)^{-1} &= W_{a\frac{N+1}{2},c\frac{N+1}{2}}, \\ U(A)W_{0,\frac{N+1}{2}}U(A)^{-1} &= W_{b\frac{N+1}{2},d\frac{N+1}{2}}. \end{aligned}$$

Pokud tyto vztahy přepíšeme pomocí operátorů $Q,\ P$ a ωI, dostaneme

$$\begin{aligned} U(A)QU(A)^{-1} &= \omega^{ac\frac{(N+1)^2}{2}}Q^aP^c, \\ U(A)PU(A)^{-1} &= \omega^{bd\frac{(N-1)^2}{2}}Q^bP^d. \end{aligned}$$

Podle definice homomorfismu $\widetilde{\phi}$ máme

$$\widetilde{\phi}(\widetilde{\psi}(A)) = A.$$

Proto platí $\widetilde{\phi} \circ \widetilde{\psi} = Id_{\mathrm{SL}(2,\mathbb{Z}_N)}$. □

Poznámka. Platí, že $\mathrm{Ker}(\widetilde{\phi}) = H(N)/\mathrm{U}(1)$. Důkaz je analogický důkazu lemmatu 3.6.

Nyní postoupíme k důkazu existence zobrazení U.

Definice 4.10. *Definujme matice*

$$h_+ = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \qquad h_- = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Poznámka. Zřejmě $h_+, h_- \in \mathrm{SL}(2, \mathbb{Z}_N)$.

Poznámka. Podle tvrzení 3.10 matice

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generují grupu $\mathrm{SL}(2, \mathbb{Z}_N)$. Lze snadno ověřit, že $A = h_-^{N-1}$ a $B = h_+^{N-1} h_- h_+^{N-1}$, takže platí, že

$$\mathrm{SL}(2, \mathbb{Z}_N) = \langle h_-, h_+ \rangle.$$

Poznámka. Platí, že pokud $|0\rangle, \ldots, |N-1\rangle$ je ortonormální báze prostoru $\mathcal{H}_N$, pak $\sum_i |i\rangle \langle i| = I$.

Dále pokud $\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{C}$ a $A = \sum_{i,j} |i\rangle \omega^{\alpha(i,j)} \langle j|$, $B = \sum_{p,q} |q\rangle \omega^{-\alpha(p,q)} \langle p|$, pak $B = A^\dagger$.

Jde o základní tvrzení z lineární algebry a proto je uvádíme bez důkazu.

Tvrzení 4.11. *Nechť h_+, h_- je definováno jako výše. Definujme operátory*

$$U_{h_-} = \textstyle\sum_i |i\rangle \omega^{\frac{i}{2}(i+N)} \langle i|,$$
$$U_{h_+} = \frac{1}{\sqrt{N}} \textstyle\sum_{i,k} |i\rangle \omega^{\frac{1}{2}(i-k)(i-k+N)} \langle k|.$$

Tyto operátory jsou unitární.

Důkaz. Máme

$$\begin{aligned} U_{h_+} U_{h_+}^\dagger &= \tfrac{1}{N} \Big(\textstyle\sum_{i,k} |i\rangle \omega^{\frac{1}{2}(i-k)(i-k+N)} \langle k|\Big)\Big(\sum_{p,q} |q\rangle \omega^{-\frac{1}{2}(p-q)(p-q+N)} \langle p|\Big) = \\ &= \tfrac{1}{N} \textstyle\sum_{i,k,p} |i\rangle \omega^{\frac{1}{2}[(i-k)(i-k+N)-(p-k)(p-k+N)]} \langle p| = \\ &= \tfrac{1}{N} \textstyle\sum_{i,k,p} |i\rangle \omega^{\frac{1}{2}(i^2-2ik+k^2+Ni-Nk-p^2+2pk-k^2+Nk-Np)} \langle p| = \\ &= \tfrac{1}{N} \textstyle\sum_{i,p} |i\rangle \omega^{\frac{1}{2}(i^2-p^2+Ni-Np)} \langle p| \sum_k \omega^{k(p-i)} \ . \end{aligned}$$

Z toho, že $\omega^N = 1$ a ze vzorce pro součet geometrické posloupnosti plyne, že suma přes k bude nenulová právě tehdy, když $i = p$, tedy

$$U_{h_+} U_{h_+}^\dagger = \tfrac{1}{N} |i\rangle \omega^0 \langle i| \sum_k 1 = \sum_i |i\rangle \langle i| = I.$$

Dále platí

$$\begin{gathered} U_{h_-} U_{h_-}^\dagger = (\textstyle\sum_i |i\rangle \omega^{\frac{i}{2}(i+N)} \langle i|)(\sum_k |k\rangle \omega^{-\frac{k}{2}(k+N)} \langle k|) = \\ = \textstyle\sum_{i,k} |i\rangle \omega^{\frac{1}{2}[i(i+N)-k(k+N)]} \delta_{ik} \langle k| = \sum_i |i\rangle \langle i| = I. \end{gathered}$$

Pracujeme s konečně-rozměrným prostorem, a proto automaticky platí i $U_{h_+}^\dagger U_{h_+} = U_{h_-}^\dagger U_{h_-} = I$. □

Tvrzení 4.12. *Pro operátory U_{h_-}, U_{h_+} platí*

$$\begin{aligned} U_{h_-} W_{m,n} U_{h_-}^\dagger &= W_{h_- \cdot (m,n)}, \\ U_{h_+} W_{m,n} U_{h_+}^\dagger &= W_{h_+ \cdot (m,n)} \end{aligned}$$

pro všechna m, $n \in \mathcal{I}$.

Důkaz. Máme

$$\begin{gathered} U_{h_-} W_{m,n} U_{h_-}^\dagger = U_{h_-} (\textstyle\sum_j |j\rangle \omega^{2m(j+n)} \langle j+2n|)(\sum_k |k\rangle \omega^{-\frac{k}{2}(k+N)} \langle k|) = \\ = (\textstyle\sum_i |i\rangle \omega^{\frac{i}{2}(i+N)} \langle i|)(\sum_{j,k} |j\rangle \omega^{2m(j+n)-\frac{k}{2}(k+N)} \delta_{j+2n,k} \langle k|) = \\ = (\textstyle\sum_i |i\rangle \omega^{\frac{i}{2}(i+N)} \langle i|)(\sum_j |j\rangle \omega^{2m(j+n)-\frac{1}{2}(j^2+4nj+4n^2+jN+2nN)} \langle j+2n|) = \\ = \textstyle\sum_{i,j} |i\rangle \omega^{\frac{i}{2}(i+N)} \delta_{ij} \omega^{2m(j+n)-\frac{1}{2}(j^2+4nj+4n^2+jN+2nN)} \langle j+2n| = \\ = \textstyle\sum_i |i\rangle \langle i+2n| \omega^{\frac{i^2}{2}+\frac{Ni}{2}+2mi+2mn-\frac{i^2}{2}-2ni-2n^2-\frac{Ni}{2}+nN} = \\ = \textstyle\sum_i |i\rangle \langle i+2n| \omega^{2(m-n)(n+i)+nN} = \sum_i |i\rangle \langle i+2n| \omega^{2(m-n)(i+n)} = \\ = W_{h_- \cdot (m,n)}, \end{gathered}$$

protože $h_- \cdot (m,n) = (m-n,n)^T$.

Dále platí

$$\begin{gathered} U_{h_+} W_{m,n} U_{h_+}^\dagger = \\ = \tfrac{1}{\sqrt{N}} \textstyle\sum_i |i\rangle (\sum_k \omega^{\frac{1}{2}(i-k)(i-k+N)} \langle k|)(\sum_j |j\rangle \langle j+2n| \omega^{2m(j+n)}) U_{h_+}^\dagger = \\ \tfrac{1}{N} \textstyle\sum_i |i\rangle (\sum_k \omega^{\frac{1}{2}(i-k)(i-k+N)+2m(k+n)} \langle k+2n|)(\sum_p |p\rangle (\sum_q \omega^{-\frac{1}{2}(q-p)(q-p+N)} \langle q|)) = \\ = \tfrac{1}{N} \textstyle\sum_i |i\rangle (\sum_k \omega^{\frac{1}{2}(i-k)(i-k+N)+2m(k+n)})(\sum_q \omega^{-\frac{1}{2}(q-k-2n)(q-k-2n+N)} \langle q|) = \\ = \tfrac{1}{N} \textstyle\sum_{i,q} |i\rangle \langle q| \sum_k \omega^{\frac{1}{2}(i-k)(i-k+N)+2m(k+n)-\frac{1}{2}(q-k-2n)(q-k-2n+N)} = \\ = \tfrac{1}{N} \textstyle\sum_{i,q,k} |i\rangle \langle q| \omega^{\frac{1}{2}((i-k)^2+(i-k)N+4m(k+n)-(k+(2n-q))^2-(q-k-2n)N)} = \\ = \tfrac{1}{N} \textstyle\sum_{i,q,k} |i\rangle \langle q| \omega^{\frac{1}{2}(i^2-2ik+k^2+(i-k-q+k+2n)N+4m(k+n)-k^2-2k(2n-q)-(2n-q)^2)} = \\ = \tfrac{1}{N} \textstyle\sum_{i,q} |i\rangle \langle q| \omega^{\frac{1}{2}(i^2+iN-qN+2nN+4mn-(2n-q)^2)} \sum_k \omega^{\frac{1}{2}(-2ik+4mk-2k(2n-q))} = \\ = \tfrac{1}{N} \omega^{nN+2mn} \textstyle\sum_{i,q} |i\rangle \langle q| \omega^{\frac{1}{2}(i^2+iN-qN-(2n-q)^2)} \sum_k \omega^{k(-i+q+2m-2n)}. \end{gathered}$$

Podobnou úvahou jako v předchozím důkazu dostaneme, že suma přes k je nenulová právě tehdy, když $i - 2m + 2n = q$. Po dosazení dostáváme

$$\begin{gathered}\tfrac{1}{N}\omega^{2mn}\textstyle\sum_i |i\rangle\langle i-2m+2n|\,\omega^{\frac{1}{2}(i^2+(i-i+2m-2n)N-(i-2m)^2)}\sum_k 1 = \\ = \omega^{2mn}\textstyle\sum_i |i\rangle\langle i-2m+2n|\,\omega^{\frac{1}{2}(i^2+2mN-2nN-i^2+4mi-4m^2)} = \\ = \omega^{(m-n)N}\textstyle\sum_i |i\rangle\langle i-2m+2n|\,\omega^{2m(i+n-m)} = \\ = \textstyle\sum_i |i\rangle\langle i+2(n-m)|\,\omega^{2m(i+n-m)} = W_{h_+\cdot(m,n)},\end{gathered}$$

protože $h_+ \cdot (m,n) = (m, n-m)^T$. Tím je tvrzení dokázáno. □

Lemma 4.13. *Existuje zobrazení $U : \mathrm{SL}(2,\mathbb{Z}_N) \to \mathcal{C}(N)$ takové, že pro libovolné $m,n \in \mathcal{I}$ platí*

$$U(S)W_{m,n}U^\dagger(S) = W_{S\cdot(m,n)}.$$

Důkaz. Podle druhé poznámky pod definicí 4.10 platí, že $\mathrm{SL}(2,\mathbb{Z}_N) = \langle h_-, h_+\rangle$. Mějme nyní libovolnou matici $S \in \mathrm{SL}(2,\mathbb{Z}_N)$. Existují čísla $i_1,...,i_k,j_1,...,j_k$ taková, že $S = h_-^{i_1}h_+^{j_1}...h_-^{i_k}h_+^{j_k}$. Definujme zobrazení $U : \mathrm{SL}(2,\mathbb{Z}_N) \to \mathrm{U(N)}$, $U(S) = U_{h_-}^{i_1}...U_{h_+}^{j_k}$. Podle předchozího tvrzení pak platí

$$\begin{gathered}U(S)W_{m,n}U^\dagger(S) = U_{h_-}^{i_1}...U_{h_+}^{j_k}W_{m,n}(U_{h_+}^\dagger)^{j_k}...(U_{h_-}^\dagger)^{i_1} = W_{h_-^{i_1}h_+^{j_1}...h_-^{i_k}h_+^{j_k}\cdot(m,n)} = \\ = W_{S\cdot(m,n)}.\end{gathered}$$

Zobrazení U má tedy požadovanou vlastnost a podle tvrzení 4.3 zobrazuje do $\mathcal{C}(N)$. □

Věta 4.14. *Projektivní Weilova reprezentace, tedy zobrazení $\widetilde{\psi}$ popsané v definici 4.7, existuje.*

Důkaz. Podle předchozího lemmatu existuje zobrazení U popsané v definici 4.7, podle poznámky pod definicí 4.7 je zobrazení $\widetilde{\psi}$ dobře definované a podle tvrzení 4.8 jde o projektivní reprezentaci. □

Věta 4.15. *Platí $\widetilde{\mathcal{C}}(N) \cong (\mathbb{Z}_N \times \mathbb{Z}_N) \rtimes \mathrm{SL}(2,\mathbb{Z}_N)$.*

Důkaz. Pokud $H \in H(N)$ a $X \in \mathcal{C}(N)$, pak platí, že

$$X\mathrm{U}(1)H\mathrm{U}(1)X^{-1}\mathrm{U}(1) = XHX^{-1}\mathrm{U}(1) = H'\mathrm{U}(1),$$

kde $H' \in H(N)$, z čehož plyne $H(N)/\mathrm{U}(1) \trianglelefteq \widetilde{\mathcal{C}}(N)$. Dále podle tvrzení 4.9 platí, že $\widetilde{\phi} \circ \widetilde{\psi} = Id_{\mathrm{SL}(2,\mathbb{Z}_N)}$, z poznámky pod lemmatem 3.11 plyne, že $\widetilde{\phi}$ je surjektivní a podle poznámky nad definicí 4.10 platí, že $\mathrm{Ker}(\widetilde{\phi}) = H(N)/\mathrm{U}(1)$. Definujme zobrazení $\theta' : (\mathbb{Z}_N \times \mathbb{Z}_N) \to H(N)/\mathrm{U}(1)$

tak, že $\theta'(i,j) = Q^{2i}P^{2j}\mathrm{U}(1)$ pro libovolné $i,j \in \mathbb{Z}_N$. Násobení číslem 2 je v $\mathbb{Z}_N$ pro liché N bijekce a to, že je to homomorfismus se dokáže jako v důkazu tvrzení 2.20. Proto platí, že $H(N)/\mathrm{U}(1) \cong \mathbb{Z}_N \times \mathbb{Z}_N$ a z tvrzení 3.16 plyne, že $\widetilde{\mathcal{C}}(N) \cong (\mathbb{Z}_N \times \mathbb{Z}_N) \rtimes \mathrm{SL}(2,\mathbb{Z}_N)$. □

Poznámka. Zdůrazňujeme, že předchozí větu jsme dokázali jen pro liché N.

Podívejme se nyní, jak se skládají prvky grupy $(\mathbb{Z}_N \times \mathbb{Z}_N) \rtimes \mathrm{SL}(2,\mathbb{Z}_N)$.

Podle tvrzení 3.16 je akce (díky izomorfismu θ') definovaná jako $\varphi'(S)(v) = = \theta'^{-1}(\widetilde{\psi}(S)\theta'(v)\widetilde{\psi}(S)^{-1})$ pro $S \in \mathrm{SL}(2,\mathbb{Z}_N)$ a $v \in (\mathbb{Z}_N \times \mathbb{Z}_N)$. Nechť $S, S' \in \mathrm{SL}(2,\mathbb{Z}_N)$ a $v, v' \in (\mathbb{Z}_N \times \mathbb{Z}_N)$. Pak

$$(v', S')(v, S) = (v' + \varphi'(S')(v), S'S) = (v' + \theta'^{-1}(\widetilde{\psi}(S')\theta'(v)\widetilde{\psi}(S')^{-1}), S'S) = \\ = (v' + \theta'^{-1}(W_{S'\cdot v}\mathrm{U}(1)), S'S) = (v' + S'v, S'S),$$

což přesně odpovídá skládání nehomogenních lineárních transformací.

4.3 Weilova reprezentace

V této části kapitoly ukážeme, že zobrazení U lze upravit tak, že už půjde o normální reprezentaci. Tato podkapitola vychází z článku [7].

Tvrzení 4.16. *Definujme operátor*

$$\Delta := \sum_{m,n} W_{m,n}.$$

Pak pro všechny $|i\rangle$ platí

$$\tfrac{1}{N}\Delta\,|i\rangle = |-i\rangle.$$

Důkaz. Podle tvrzení 4.5 máme

$$\begin{aligned}\tfrac{1}{N}\Delta\,|i\rangle &= \tfrac{1}{N}\sum_{j,m,n} |j\rangle\,\langle j+2n|\,\omega^{2m(j+n)}\,|i\rangle = \\ &= \tfrac{1}{N}\sum_{j,n} |j\rangle\,\langle j+2n|i\rangle \sum_m \omega^{2m(j+n)}.\end{aligned}$$

Musí opět platit $n = -j$, aby byl výraz nenulový. Dostáváme

$$\tfrac{1}{N}\Delta\,|i\rangle = \sum_j |j\rangle\,\langle -j|i\rangle = |-i\rangle.$$

□

Definice 4.17. *Definujme operátory*

$$T_+ = \tfrac{1}{2}(I + \tfrac{1}{N}\Delta), \qquad T_- = \tfrac{1}{2}(I - \tfrac{1}{N}\Delta).$$

Dále nechť $|x\rangle$ je libovolný vektor z $\mathcal{H}_N$. Definujme sudou, respektive lichou část vektoru $|x\rangle$ jako

$$|x\rangle_+ = T_+\,|x\rangle, \text{ respektive} \qquad |x\rangle_- = T_-\,|x\rangle.$$

Řekneme, že $|x\rangle$ je sudý, respektive lichý právě tehdy, když

$$|x\rangle \in \mathrm{Im}(T_+) = \mathcal{H}_N^+, \text{ respektive} \qquad |x\rangle \in \mathrm{Im}(T_-) = \mathcal{H}_N^-.$$

Tvrzení 4.18. *Pro vektorové prostory $\mathcal{H}_N^+, \mathcal{H}_N^-$ platí*

$$\dim\mathcal{H}_N^+ = \tfrac{N+1}{2}, \qquad \dim\mathcal{H}_N^- = \tfrac{N-1}{2}.$$

Dále platí

$$\mathcal{H}_N = \mathcal{H}_N^+ \oplus \mathcal{H}_N^-.$$

Důkaz. Podívejme se na to, jak operátory T_+ a T_- zobrazují bazické vektory. Podle předchozí definice a tvrzení 4.17 platí

$$T_+ |i\rangle = \tfrac{1}{2}(|i\rangle + |-i\rangle), \qquad T_- |i\rangle = \tfrac{1}{2}(|i\rangle - |-i\rangle).$$

Pokud $j, k \in \{1, ..., \frac{N-1}{2}\}$ jsou takové, že $j \neq k$, pak $T_+ |j\rangle$ a $T_+ |k\rangle$, respektive $T_- |j\rangle$ a $T_- |k\rangle$ jsou lineárně nezávislé. Dále lze snadno ověřit, že pro $k \in \{0, ..., \frac{N-1}{2}\}$ platí

$$T_+ |\tfrac{N-1}{2} - k\rangle = T_+ |\tfrac{N+1}{2} + k\rangle, \qquad T_- |\tfrac{N-1}{2} - k\rangle = -T_- |\tfrac{N+1}{2} + k\rangle.$$

Navíc $T_+ |0\rangle = |0\rangle$ a $T_- |0\rangle = 0$. Celkově dostáváme

$$\dim\mathcal{H}_N^+ = \tfrac{N+1}{2}, \qquad \dim\mathcal{H}_N^- = \tfrac{N-1}{2}.$$

Dále platí $T_+ + T_- = I$. Odtud $\mathcal{H}_N^+ + \mathcal{H}_N^- = \mathcal{H}_N$. Vzhledem k tomu, že $\dim\mathcal{H}_N^+ + \dim\mathcal{H}_N^- = \dim\mathcal{H}_N$, musí být součet vektorových prostorů direktní. Skutečně tedy platí

$$\mathcal{H}_N = \mathcal{H}_N^+ \oplus \mathcal{H}_N^-.$$

□

Tvrzení 4.19. *Nechť $S \in \mathrm{SL}(2, \mathbb{Z}_N)$. Pak $U(S)$ zobrazuje $\mathcal{H}_N^+$ do $\mathcal{H}_N^+$, respektive $\mathcal{H}_N^-$ do $\mathcal{H}_N^-$.*

Důkaz. Nechť $m, n \in \mathcal{I}$. Pak

$$U(S)W_{m,n} = W_{S\cdot(m,n)}U(S).$$

Zobrazení $(m, n) \mapsto S \cdot (m, n)$ je bijekce, a proto vysčítáním přes m a n dostaneme

$$U(S)\Delta = \Delta U(S).$$

Odtud

$$U(S)T_\pm = T_\pm U(S).$$

Nechť $|x\rangle \in \mathcal{H}_N^+$. Pak existuje $|y\rangle \in \mathcal{H}_N$ takový, že $T_+ |y\rangle = |x\rangle$. Platí

$$U(S) |x\rangle = U(S)T_+ |y\rangle = T_+ U(S) |y\rangle,$$

kde druhá rovnost plyne z úvah výše a poslední výraz je nějaký sudý vektor. Analogicky se tvrzení dokáže pro liché vektory. □

Definice 4.20. *Nechť $S \in \mathrm{SL}(2,\mathbb{Z}_N)$. Pak zúžení $U(S)$ na $\mathcal{H}_N^+$, respektive $\mathcal{H}_N^-$ označíme $U(S)_+$, respektive $U(S)_-$.*

Poznámka. Tvrzení 4.18 a 4.19 nám zaručují, že $U(S)_+$, respektive $U(S)_-$ lze reprezentovat čtvercovými maticemi $\frac{N+1}{2} \times \frac{N+1}{2}$, respektive $\frac{N-1}{2} \times \frac{N-1}{2}$.

Věta 4.21. *Existuje Weilova reprezentace, tj. pro všechny matice $S \in \mathrm{SL}(2,\mathbb{Z}_N)$ existuje $\lambda_S \in \mathbb{C}$ takové, že zobrazení $\psi : \mathrm{SL}(2,\mathbb{Z}_N) \to \mathcal{C}(N),\ \psi(S) = \lambda_S^{-1} U(S)$ je homomorfismus z $\mathrm{SL}(2,\mathbb{Z}_N)$ do $\mathcal{C}(N)$.*

Důkaz. Mějme $S, S' \in \mathrm{SL}(2,\mathbb{Z}_N)$. Pak

$$U(S)U(S') = c(S,S')U(SS'),$$

kde $c(S,S') \in \mathbb{C} \setminus \{0\}$. Analogické výrazy platí pro $U(S)_+$ a $U(S)_-$. Pro jejich determinanty dostaneme

$$\det(U(S)_+)\det(U(S')_+) = c(S,S')^{\frac{N+1}{2}} \det(U(SS')_+),$$
$$\det(U(S)_-)\det(U(S')_-) = c(S,S')^{\frac{N-1}{2}} \det(U(SS')_-).$$

Úpravou dostaneme

$$c(S,S') = \frac{\det(U(S)_+)}{\det(U(S)_-)} \frac{\det(U(S')_+)}{\det(U(S')_-)} \frac{\det(U(SS')_-)}{\det(U(SS')_+)}.$$

Označme $\lambda_S := \frac{\det(U(S)_+)}{\det(U(S)_-)}$. Pak zobrazení $\psi : S \mapsto \lambda_S^{-1} U(S)$ je homomorfismus a jelikož U zobrazuje do $\mathcal{C}(N)$, platí $\psi(S) \in \mathcal{C}(N)$ pro všechny matice $S \in \mathrm{SL}(2,\mathbb{Z}_N)$. □

Tvrzení 4.22. *Pro Weilovu reprezentaci ψ platí, že*

$$\phi \circ \psi = Id_{\mathrm{SL}(2,\mathbb{Z}_N)},$$

kde ϕ je homomorfismus z tvrzení 3.3.

Důkaz. Důkaz je analogický důkazu tvrzení 4.9. □

Věta 4.23. *Platí, že $\mathcal{C}(N) \cong H(N) \rtimes \mathrm{SL}(2,\mathbb{Z}_N)$.*

Důkaz. Zřejmě platí, že $H(N) \trianglelefteq \mathcal{C}(N)$ a podle předchozího tvrzení máme $\phi \circ \psi = Id_{\mathrm{SL}(2,\mathbb{Z}_N)}$. Podle poznámky pod lemmatem 3.11 je ϕ surjektivní a z důkazu lemmatu 3.6 plyne, že $\mathrm{Ker}(\phi) = H(N)$. Podle tvrzení 3.16 platí $\mathcal{C}(N) \cong H(N) \rtimes \mathrm{SL}(2,\mathbb{Z}_N)$. □

Závěr

V této práci jsme prozkoumali Cliffordovu grupu, ukázali, že tato grupa i její projektivní verze mají strukturu semidirektního součtu a dokázali existenci Weilovy reprezentace pro liché N. Nejsou to nové výsledky; je možné je najít v různých článcích, ale většina autorů používá různé definice a značení, a proto je hlavní přínos této práce sepsání těchto výsledků na jednom místě ve společném jazyce.

Na závěr ještě okomentujme otázku existence Weilovy reprezentace pro sudé N. V článku [10] byl nalezen homomorfismus z $\mathrm{SL}(2, \mathbb{Z}_{2N})$ do $\mathrm{U}(N)$, nicméně my bychom potřebovali homomorfismus z $\mathrm{SL}(2, \mathbb{Z}_N)$ do $\mathrm{U}(N)$. V článku [11] se bez důkazu tvrdí, že $(\mathbb{Z}_N \times \mathbb{Z}_N) \rtimes \mathrm{SL}(2, \mathbb{Z}_N)$ a $\widetilde{\mathcal{C}}(N)$ nejsou izomorfní. Tuto otázku tedy ještě bude nutné dál prozkoumat.

Literatura

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge 2010.

[2] J. Tolar, On Clifford groups in quantum computing, *J. Phys.: Conf. Series* **1071** (2018), 012022.

[3] P. Bartoňová: *Teorie grup a kvantové počítání*, bakalářská práce FJFI ČVUT v Praze, 2017.

[4] M. Korbelář, J. Tolar, Symmetries of the finite Heisenberg group for composite systems, *J. Phys. A: Math. Theor.* **43** (No.37) (2010) 375302 (15pp); arXiv: /1006.0328 [quant-ph].

[5] D. S. Dummit, R. M. Foote, *Abstract Algebra*, John Wiley and Sons, New Jersey 2004.

[6] I. Bengtsson, K. Zyczkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, Cambridge University Press, Cambridge 2017.

[7] K. Dutta, A. Prasad, Combinatorics of finite abelian groups and Weil representation, *Pacific J. Math.* **275** (No.2) (2015), 295-324; arXiv: /1010.3528.

[8] M. Havlíček, J. Patera, E. Pelantová, J. Tolar, Automorphisms of the fine gradings of $sl(n, C)$ associated with the generalized Pauli matrices, *Journal of Mathematical Physics* **43** (No.2) (2002), 1083-1094; arXiv: math-ph/0311015.

[9] N. Kaiblinger, M. Neuhauser, Metaplectic operators for finite abelian groups and R^d, *Indag. Mathem., N.S.* **20** (No.2) (2009), 233-246.

[10] D. Watanabe, T. Hashimoto, M. Horibe, A. Hayashi, Covariant projective representation of symplectic group on discrete phase space, *J. Phys.: Conf. Series* **1194** (2019), 012112; arXiv:1802.09891 [quant-ph].

[11] D. M. Appleby, SIC-POVMs and the extended Clifford group, *J. Math. Phys.* **46** (2005) 052107.