TU Clausthal

Mathematik-Bericht 2009/3

Metaplectic operators for finite abelian groups and $\mathbb{R}^d$

N. Kaiblinger, M. Neuhauser

März 2009

Institut für Mathematik, Erzstraße 1, 38678 Clausthal-Zellerfeld, Tel. (05323) 72-2413

METAPLECTIC OPERATORS FOR FINITE ABELIAN GROUPS AND $\mathbb{R}^d$

NORBERT KAIBLINGER[1,*] AND MARKUS NEUHAUSER[2]

ABSTRACT. The Segal–Shale–Weil representation associates to a symplectic transformation of the Heisenberg group an intertwining operator, called metaplectic operator. We develop an explicit construction of metaplectic operators for the Heisenberg group $H(G)$ of a finite abelian group G, an important setting in finite time-frequency analysis. Our approach also yields a simple construction for the multivariate Euclidean case $G = \mathbb{R}^d$.

INTRODUCTION

Denote by $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ the cyclic group of order $n \geq 2$. Let G be a finite abelian group, given in generic form

$$G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_d} \ , \qquad \text{where} \ \ n_1 \mid n_2 \mid \cdots \mid n_d \ .$$

Finite abelian groups are self-dual, that is, G is isomorphic to its dual group $\widehat{G}$ consisting of the homomorphisms into the circle group $\mathbb{T} = \{\tau \in \mathbb{C} \colon |\tau| = 1\}$. Specifically, we identify a character $\chi \in \widehat{G}$ with an element $m \in G$ by writing $\chi \colon k \mapsto \langle m, k\rangle$ in terms of the bicharacter

$$\langle m, k\rangle = \exp(2\pi i \cdot m^\top N^{-1} k) \ , \qquad k, m \in G,$$

where

$$N = \operatorname{diag}(n_1, \ldots, n_d).$$

Given $\lambda \in G^2$, the time-frequency shift operator $\pi(\lambda)$ is defined for a complex-valued function v on G, that is for an $n_1 \times \cdots \times n_d$ hypermatrix v, by

$$\pi(\lambda)\, v(k) = \langle m, k\rangle\, v(k - l), \qquad \lambda = (l, m) \in G^2.$$

The Heisenberg group $H(G)$ is the group of operators

$$H(G) := \{\tau\, \pi(\lambda) \colon \lambda \in G^2, \ \tau \in \mathbb{T}\},$$

where $\mathbb{T} = \{\tau \in \mathbb{C} \colon |\tau| = 1\}$ is the circle group.

2000 *Mathematics Subject Classification.* Primary 20C33; Secondary 20K01, 42C15, 81S30.

Key words and phrases. Metaplectic representation, Heisenberg group, extraspecial group, symplectic homomorphism, second degree character, time-frequency shift operator.

[1]Faculty of Mathematics, University of Vienna, Nordbergstraße 15, 1090 Vienna, Austria.

[2]Insitut für Mathematik, TU Clausthal, Erzstr. 1 38678 Clausthal-Zellerfeld, Germany.

[*]Corresponding author.

E-mails: norbert.kaiblinger@univie.ac.at (N. Kaiblinger), neuhauser@math.tu-clausthal.de (M. Neuhauser).

Supported by the Austrian Science Fund FWF grant P 21339 (N.K.) and by the Marie-Curie Excellence Grant MEXT-CT-2004-517154 (M.N.).

Weil's celebrated theory of the metaplectic representation [33] is concerned with a class of automorphisms of the Heisenberg group $H(G)$ for an arbitrary self-dual locally compact abelian group G, see [5]. Especially it contains generalizations of fundamental results that are initially formulated for the case $G = \mathbb{R}^d$, such as the Stone–von Neumann theorem [30]. One of the key results of Weil's theory is the existence of metaplectic operators and applied to the case of the finite abelian group G it is outlined as follows.

By $M_{d,d}(\mathbb{Z})$ denote the set of $d \times d$ matrices with coefficients in $\mathbb{Z}$. We describe the endomorphisms of G by equivalence classes of integer matrices. A representative $[A] = (a_{r,s})$ of A must satisfy the condition that

$$\frac{n_r}{n_s} \text{ divides } a_{r,s} \text{ if } s < r, \qquad r, s = 1, \dots, d,$$

and the entries of any other representative $(a'_{r,s})$ for A satisfy

$$a'_{r,s} = a_{r,s} \bmod n_r, \qquad r, s = 1, \dots, d.$$

The endomorphism ring structure is thus given by the usual matrix operations. This description of $\mathrm{End}(G)$ is standard when G is of prime power order [21]. Our approach does not a priori split G into p-groups, with the advantage that the operators used in the main result need not be factorized.

For $A \in \mathrm{End}(G)$ with representative $[A] \in M_{d,d}(\mathbb{Z})$, the matrix

$$[A]^* = N[A]^\top N^{-1}$$

belongs to $M_{d,d}(\mathbb{Z})$ and it is a representative for the adjoint $A^* \in \mathrm{End}(G)$, so that indeed

$$\begin{aligned} \langle m, Ak \rangle &= \exp(2\pi i \cdot m^\top N^{-1} A\, k) \\ &= \exp\big(2\pi i \cdot (NA^\top N^{-1} m)^\top N^{-1}\, k\big) = \langle A^* m, k \rangle, \qquad k, m \in G. \end{aligned}$$

Notice that the latter formula does not depend on the choice of the representative $[A]$ and in such a situation we usually do not distinguish between $A \in \mathrm{End}(G)$ and a specific representative $[A] \in M_{d,d}(\mathbb{Z})$.

Let S be an element of the symplectic group $\mathrm{Sp}(G)$ described by $2d \times 2d$ matrices in block form

$$S = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \qquad A, B, C, D \in \mathrm{End}(G),$$

such that $A^*C = C^*A$, $B^*D = D^*B$, and $A^*D - C^*B = I$, with $I \in \mathrm{End}(G)$ the identity, for which the $d \times d$ identity matrix is a representative. For our approach it is preferable to use the equivalent conditions

$$AB^* = BA^*, \quad CD^* = DC^*, \text{ and } AD^* - BC^* = I,$$

that follow since $S \in \mathrm{Sp}(G)$ implies that S is invertible with $S^{-1} = \left(\begin{smallmatrix} D^* & -B^* \\ -C^* & A^* \end{smallmatrix}\right) \in \mathrm{Sp}(G)$. Then the fundamental result mentioned above reads that there exists a unitary operator U on $\mathbb{C}^{n_1 \cdots n_d}$, called a metaplectic operator for S, such that

$$U \pi(\lambda) U^{-1} = \psi(\lambda)\, \pi(S\lambda), \qquad \lambda \in G^2, \tag{1}$$

with some scalar function $\psi \colon G^2 \to \mathbb{T}$.

We describe an explicit construction of metaplectic operators for the case of finite abelian groups G. The finite setting is important in time-frequency analysis [7, 14, 24, 31], particularly for the finite approximation of multivariate Gabor frames [23].

The literature on metaplectic operators in this setting is rich, we mention [1, 2, 4, 8, 11, 13, 19, 20, 25, 27] and the extensive list of references in [32]. On the other hand, the previously known constructions of metaplectic operators in a finite setting are formulated with various restrictions. Typical limitations are the focus on finite fields or strong conditions on S, such as one of its blocks being invertible. Such a restriction on S covers the general case only indirectly, for example by a counting argument in [27], formulated for the finite field setting. A general construction for metaplectic operators for finite cyclic groups is obtained in [13]. The present results cover the case of arbitrary finite abelian groups and we do not impose any restriction on S. Our approach to the finite case also implies a simple construction for the multivariate continuous-time case $G = \mathbb{R}^d$, discussed in a separate section.

The main theorem is stated in Section 1 and proved in Section 3, based on preliminary results which can be found in Section 2. The construction for the continuous-time case $G = \mathbb{R}^d$ is presented in Section 4.

1. Main result

We use the following unitary operators acting on $n_1 \times \cdots \times n_d$ hypermatrices $v \in \mathbb{C}^{n_1 \cdots n_d}$, viewed as functions on G. By $\operatorname{Aut}(G) \subset \operatorname{End}(G)$ denote the group of automorphisms of G.

Let $A \in \operatorname{Aut}(G)$ and $C \in \operatorname{End}(G)$ with $C = C^*$, given in the form of an integer matrix representative $[C] \in M_{d,d}(\mathbb{Z})$ satisfying $[C] = N[C]^\top N^{-1}$. Define the Fourier transform $\mathscr{F}$, the dilation L_A, and the multiplication operator $R_{[C]}$ by

- $$\mathscr{F}v(k) = \frac{1}{\sqrt{\det N}} \sum_{m \in G} \underbrace{\exp(-2\pi i \cdot k^\top N^{-1} m)}_{\overline{\langle k, m \rangle}}\, v(m), \qquad k \in G,$$
- $$L_A v(k) = v(A^{-1}\, k), \qquad k \in G,$$
- $$R_{[C]} v(k) = \psi_{[C]}(k)\, v(k), \qquad k \in G,$$

where the function $\psi_{[C]}$ on G is defined by

$$\psi_{[C]}(k) = \exp\left(\pi i \cdot k^\top (I + N^{-1})\, [C]\, (I + N)\, k\right), \qquad k \in G.$$

We remark that the careful definition of $\psi_{[C]}$ is one of the crucial steps of our approach, it is shown in Lemma 2 below that $\psi_{[C]}$ is a second degree character for C. Second degree characters are a fundamental notion in Weil's theory of the metaplectic representation [33], we refer to [29]; see also [13]. It is important to note that the seemingly more natural assignment $f(k) = \exp(\pi i \cdot k^\top N^{-1}\, [C]\, k)$ does not work, cf. [6, 13]; while f may not be well defined on G, we will show that $\psi_{[C]}(k) = f\big((I + N)k\big)$ works. We also note that the general construction of second degree characters in [3, p. 308] or [29, p. 37], based on Mackey's technique of induced representation, does not directly yield explicit formulas.

The next theorem is our main result and it describes the explicit construction of metaplectic operators U for general finite abelian groups. Denote by $\mathscr{R}(A)$ the image of a given homomorphism A.

Theorem 1. *Let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_d}$ such that $n_1 \mid n_2 \mid \cdots \mid n_d$ and let $S = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}(G)$. For each prime p dividing the group order $|G|$, define $\Theta^{(p)} \in M_{d,d}(\mathbb{Z})$ by the following steps. First, split N into blocks determined by distinct maximal powers of p dividing the diagonal elements,*

$$N = \mathrm{diag}(n_1, \dots, n_d) = \mathrm{diag}(\underbrace{p^{\alpha_1} Q_1, \dots, p^{\alpha_u} Q_u}_{u \le d \ blocks}), \qquad \alpha_1 < \alpha_2 < \cdots < \alpha_u,$$

such that each Q_j is diagonal and invertible modulo p. Then the matrix $(A \bmod p) \in M_{d,d}(\mathbb{Z}_p)$ is block triangular of the form

$$(A \bmod p) = \begin{pmatrix} A_1 & & & * \\ & A_2 & & \\ & 0 & \ddots & \\ & & & A_u \end{pmatrix},$$

such that A_j has the same size as Q_j, for $j = 1, \dots, u$. Next, for each diagonal block A_j, denote by σ_j a set of indices such that the respective columns of A_j form a basis for $\mathscr{R}(A_j)$. Denote by Θ_j the diagonal matrix of the same size as A_j whose diagonal is 0 at the positions indexed by σ_j and 1 otherwise. Finally, let

$$\Theta^{(p)} = \mathrm{diag}\left(\Theta_1, \dots, \Theta_u\right).$$

With $\Theta^{(p)}$ obtained in this way for each prime p dividing $|G|$, define $\Theta \in \mathrm{End}(G)$ diagonal by

$$\Theta = \sum_{\substack{p \ prime, \\ p \mid \nu}} \frac{\nu}{p} \, \Theta^{(p)},$$

where ν denotes the product of all primes p dividing $|G|$. Let $A_0 = A + B\Theta$ and $C_0 = C + D\Theta$. Then A_0 is invertible and the operator $U = U_S$ given by

$$U := R_{[C_0\, A_0^{-1}]} \cdot L_{A_0} \cdot \mathscr{F}^{-1} \cdot R_{[-A_0^{-1} B]} \cdot \mathscr{F} \cdot R_{[-\Theta]}$$

is unitary and satisfies (1), for $\lambda \in G^2$ and some scalar function $\psi \colon G^2 \to \mathbb{T}$.

Remark 1. (i) If in an actual computation some block triangular structure of $(A \bmod p)$ is observed that is finer than the one described in the theorem, it can be used as well. By contrast, a coarser block triangular strucure may not be used, as shown by the following example. Let $G = \mathbb{Z}_p \times \mathbb{Z}_{p^2}$, for some prime p, and let $S = \left(\begin{smallmatrix} A & I \\ -I & 0 \end{smallmatrix}\right)$ with $A = \left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right)$. Notice that $A^* = NA^\top N^{-1} = A$ and hence $S \in \mathrm{Sp}(G)$. Writing $(A \bmod p) = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} A_1 & 1 \\ 0 & A_2 \end{smallmatrix}\right)$ we correctly obtain $\sigma_1 = \sigma_2 = \varnothing$ and $\Theta = \Theta^{(p)} = I$, indeed $A_0 = A + B\Theta = \left(\begin{smallmatrix} 1 & 1 \\ p & 1 \end{smallmatrix}\right)$ is invertible. On the other hand, incorrectly viewing $(A \bmod p)$ as one single block A_1 yields $\sigma_1 = \{2\}$ and thus $\Theta = \Theta^{(p)} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, which does not work, since $A + B\Theta = \left(\begin{smallmatrix} 1 & 1 \\ p & 0 \end{smallmatrix}\right)$ is not invertible.

(ii) The scalar function ψ in the intertwining identity (1) depends on the particular choice of the metaplectic operator U. It is always a second degree character on G^2, see [29, 33] for the details. In this paper we frequently make use of the second degree character $\psi_{[C]}$ on G, notice that in contrast ψ is a function on G^2.

(iii) The construction of Θ in terms of the matrices $\Theta^{(p)}$ is an application of the Chinese remainder theorem so to obtain $(\Theta \bmod p) = (\nu/p)\,\Theta^{(p)}$. Aiming at the plain relations $(\Theta \bmod p) = \Theta^{(p)}$ works as well yet our approach is favorable since the formula for Θ is especially simple. Generally, the theorem also works for other choices of Θ such as Θ multiplied by an any $\Sigma \in \mathrm{Aut}(G)$ in diagonal form.

(iv) We remark that our results also relate to finite Heisenberg groups. Indeed, while $H(G)$ is infinite, with finite time-frequency plane G^2, it is a central extension of the finite Heisenberg group $H_0(G)$ generated by the time-frequency shifts $\pi(\lambda)$, $\lambda \in G^2$,

$$H_0(G) = \{\tau\,\pi(\lambda)\colon \lambda \in G^2,\ \tau \in \mathbb{T}_n\},$$

where $n = n_d$ and $\mathbb{T}_n \subset \mathbb{T}$ consists of the n^{th} roots of unity.

Specifically for $n_1 = \cdots = n_d = p$ prime, where $G = \mathbb{Z}_p^d$ is a homocyclic p-group, the finite Heisenberg group $H_0(\mathbb{Z}_p^d)$ identifies with the extraspecial group p_+^{1+2d} of order p^{1+2d} and plus type, with the notation of [9, Sec. 5.2]. Theorem 1 thus relates to the automorphisms of a class of extraspecial groups, whose structure is analyzed in [34]. See also [17].

2. Preliminary results

For a self-contained presentation of the material, we recall the general decomposition paradigm for metaplectic operators.

Lemma 1. *If $U = U_1$ and $U = U_2$ satisfy (1) for $S = S_1$ and $S = S_2$, respectively, then $U = U_1U_2$ satisfies (1) for $S = S_1S_2$.*

Proof. We have $U_1U_2\pi(\lambda)U_2^{-1}U_1^{-1} = \psi_2(\lambda)U_1\pi(S_2\lambda)U_1^{-1} = \underbrace{\psi_1(S_2\lambda)\psi_2(\lambda)}_{=:\,\psi(\lambda)}\pi(S_1S_2\lambda).$ □

The preparatory material is based on suitable generalizations of the technical steps developed for cyclic groups in [13]. As a key step we verify that $\psi_{[C]}$ is well-defined and that it is indeed a second degree character for $C \in \mathrm{End}(G)$.

Lemma 2. *Let $C \in \mathrm{End}(G)$ with $C = C^*$ be given in the form of an integer matrix representative $[C] \in M_{d,d}(\mathbb{Z})$ satisfying $[C] = N[C]^\top N^{-1}$.*

(i) *$\psi_{[C]}$ is well-defined on G, that is, the function does not depend on the choice of the multi-integer representative for the argument $k \in G$.*

(ii) *$\psi_{[C]}$ is a second degree character for C, that is, it satisfies the identity*

$$\psi_{[C]}(k + k') = \psi_{[C]}(k)\,\psi_{[C]}(k')\,\langle k, Ck'\rangle, \qquad k, k' \in G.$$

Proof. First we notice that $(I + N^{-1})[C](I + N)$ is symmetric since $N^{-1}[C] = [C]^\top N^{-1}$.

(i) Let $k \in G$ be given in the form of some representative $[k] \in \mathbb{Z}^d$. Then any other representative of k is of the form $[k]+Nz$, for some $z\in\mathbb{Z}^d$, and we need to verify that $\psi_{[C]}([k]+Nz)=\psi_{[C]}([k])$. Indeed we have

$$\begin{aligned}
&\psi_{[C]}([k]+Nz)\\
&=\exp\big(\pi i\cdot([k]+Nz)^\top(I+N^{-1})\,[C]\,(I+N)\,([k]+Nz)\big)\\
&=\underbrace{\exp\big(\pi i\cdot[k]^\top(I+N^{-1})\,[C]\,(I+N)\,[k]\big)}_{=\psi_{[C]}([k])}\cdot\underbrace{\exp\big(\pi i\cdot z^\top(N+I)\,[C]\,\overbrace{(I+N)\,N}^{\text{even entries}}\,z\big)}_{=1}\cdot\\
&\qquad\times\underbrace{\exp\big(2\pi i\cdot z^\top(N+I)\,[C]\,(I+N)\,[k]\big)}_{=1}\\
&=\psi_{[C]}([k])\ .
\end{aligned}$$

(ii) For $k,k'\in G$, we have

$$\begin{aligned}
&\psi_{[C]}(k+k')\\
&=\exp\big(\pi i\cdot(k+k')^\top\,(I+N^{-1})\,[C]\,(I+N)\,(k+k')\big)\\
&=\underbrace{\exp\big(\pi i\cdot k^\top\,(I+N^{-1})\,[C]\,(I+N)\,k\big)}_{=\psi_{[C]}(k)}\cdot\underbrace{\exp\big(\pi i\cdot k'^\top\,(I+N^{-1})\,[C]\,(I+N)\,k'\big)}_{=\psi_{[C]}(k')}\cdot\\
&\qquad\times\exp\big(2\pi i\cdot k^\top\,(I+N^{-1})\,[C]\,(I+N)\,k'\big)\\
&=\psi_{[C]}(k)\,\psi_{[C]}(k')\,\underbrace{\exp\big(2\pi i\cdot k^\top N^{-1}[C]k'\big)}_{=\langle k,Ck'\rangle}\cdot\underbrace{\exp\big(2\pi i\ \cdot k^\top\overbrace{([C]+N^{-1}[C]N+[C]N)}^{\text{integer entries}}\,k'\big)}_{=1}\\
&=\psi_{[C]}(k)\,\psi_{[C]}(k')\,\langle k,Ck'\rangle,
\end{aligned}$$

where we recall that $\langle k,[C]k'\rangle=\langle k,Ck'\rangle$ does not depend on the choice of a representative $[C]$ for C. □

Remark 2. (i) If n_d is odd, then all n_j are odd and $\psi_{[C]}$ is uniquely determined by C, independent on the choice of the representative $[C]$.

(ii) If n_1 is even, then all n_j are even and there are 2^d possible vectors $\psi_{[C]}$, depending on the choice of $[C]$. Two such vectors $\psi_{[C]_1}\neq\psi_{[C]_2}$ differ by some modulation of the form of a multiplication with ±1 entries.

Lemma 3. *Let $A\in\operatorname{Aut}(G)$ and $C\in\operatorname{End}(G)$ with $C=C^*$, given in the form of an integer matrix representative $[C]\in M_{d,d}(\mathbb{Z})$ satisfying $[C]=N[C]^\top N^{-1}$. The operators $U_1=\mathscr{F}$, $U_2=L_A$, and $U_3=R_{[C]}$ satisfy* (1) *for*

$$S_1=\begin{pmatrix}0&I\\-I&0\end{pmatrix},\quad S_2=\begin{pmatrix}A&0\\0&(A^*)^{-1}\end{pmatrix},\quad\textit{and}\quad S_3=\begin{pmatrix}I&0\\C&I\end{pmatrix},$$

respectively. More precisely, we have

$$\text{(i)}\qquad \mathscr{F}\,\pi(l,m)\,\mathscr{F}^{-1} = \underbrace{\exp(2\pi i\cdot m^\top N^{-1} l)}_{\langle m,l\rangle}\,\pi(m,-l), \qquad l,m\in G,$$

$$\text{(ii)}\qquad L_A\,\pi(l,m)\,L_A^{-1} = \pi\big(Al,(A^*)^{-1}m\big), \qquad l,m\in G,$$

$$\text{(iii)}\qquad R_{[C]}\,\pi(l,m)\,R_{[C]}^{-1} = \underbrace{\exp\big(-\pi i\cdot l^\top (I+N^{-1})\,[C]\,(I+N)\,l\big)}_{\overline{\psi_{[C]}(l)}}\,\pi(l,Cl+m), \qquad l,m\in G.$$

Proof. (i) Use elementary properties of the Fourier transform, first $\mathscr{F}\pi(0,m)=\pi(m,0)\mathscr{F}$, secondly $\mathscr{F}\mathscr{F}v(k)=v(-k)$, and note that $\pi(l,m)\pi(-l,-m)=\langle m,l\rangle$.

(ii) Notice that $L_A\pi(l,0)=\pi(Al,0)L_A$ and $\pi(0,m)L_A=L_A\pi(0,A^*m)$, indeed

$$\begin{aligned}\pi(0,m)\,L_A\,v(k) &= \langle m,k\rangle\,v(A^{-1}k)\\ &= \langle A^*m,A^{-1}k\rangle\,v(A^{-1}k)\\ &= L_A\,\pi(0,A^*m)\,v(k)\ .\end{aligned}$$

(iii) Observe that $R_{[C]}\pi(0,m)=\pi(0,m)R_{[C]}$ and $R_{[C]}\pi(l,0)=\psi_{[C]}(l)\,\pi(l,Cl)R_{[C]}$, indeed

$$\begin{aligned}R_{[C]}\,\pi(l,0)\,v(k) &= \psi_{[C]}(k)\,v(k-l)\\ &= \psi_{[C]}\big(l+(k-l)\big)\,v(k-l)\\ &= \psi_{[C]}(l)\,\psi_{[C]}(k-l)\,\langle l,C(k-l)\rangle\,v(k-l)\\ &= \psi_{[C]}(l)\,\langle Cl,k-l\rangle\,\psi_{[C]}(k-l)\,v(k-l)\\ &= \overline{\psi_{[C]}(l)}\,\pi(l,Cl)\,R_{[C]}v(k),\end{aligned}$$

as follows from Lemma 2(ii) and the fact that $\psi_{[C]}(l)\,\langle Cl,-l\rangle=\overline{\psi_{[C]}(l)}$. □

3. Proof of Theorem 1

We prepare the matrix block structure used in Theorem 1.

Lemma 4. *Given a prime p dividing $|G|$, split $N=\operatorname{diag}(n_1,\ldots,n_d)$. into blocks*

$$N=\operatorname{diag}(p^{\alpha_1}Q_1,\ldots,p^{\alpha_u}Q_u),\qquad \alpha_1<\alpha_2<\cdots<\alpha_u,$$

with $u\le d$, such that each Q_j is invertible modulo p.

(i) *For $A\in\operatorname{End}(G)$, the matrix $(A \bmod p)$ has a block triangular form*

$$(A \bmod p)=\begin{pmatrix}A_1 & & * \\ & A_2 & \\ 0 & & \ddots \\ & & & A_u\end{pmatrix},$$

such that A_j has the same size as Q_j, for $j=1,\ldots,u$.

(ii) $(A \bmod p)$ *is invertible if and only if all diagonal blocks* A_j *are invertible.*

(iii) *The matrix* $(A^* \bmod p)$ *has a corresponding block triangular structure, with diagonal blocks determined as follows,*

$$(A^* \bmod p) = \begin{pmatrix} Q_1 A_1^\top Q_1^{-1} & & & * \\ & Q_2 A_2^\top Q_2^{-1} & & \\ & 0 & \ddots & \\ & & & Q_u A_u^\top Q_u^{-1} \end{pmatrix}$$

modulo p*, where* Q_j^{-1} *is the inverse of* Q_j *modulo* p*.*

(iv) *If* $AB^* = BA^*$ *and* $AD^* - BC^* = I$*, then the respective diagonal blocks of* $(A \bmod p)$*,* $(B \bmod p)$*,* $(C \bmod p)$*, and* $(D \bmod p)$ *satisfy* $A_j Q_j B_j^\top = B_j Q_j A_j^\top$ *and* $A_j Q_j D_j^\top - B_j Q_j C_j^\top = Q_j$*, for* $j = 1, \ldots, u$*.*

Proof. (i) Write $A = (a_{r,s})$. Suppose $s < r$. If the greatest power of p dividing n_r coincides with the greatest power of p dividing n_s, then the indices r and s designate the same diagonal block. Otherwise we have that p divides n_r/n_s and thus $a_{r,s} \bmod p = 0$, which yields the zero blocks.

(ii) The reduction to the diagonal blocks follows from the block triangular form observed in (i).

(iii) Since $A^* \in \operatorname{End}(G)$ the observation in (i) also applies to A^*. Next, the diagonal blocks of $(A^* \bmod p)$ correspond to those parts of $A^* = NA^\top N^{-1}$ where the following cancellation of powers of p is in effect, $(A^*)_j = (NA^\top N^{-1})_j = Q_j A_j^\top Q_j^{-1}$.

(iv) Notice that both $(A \bmod p)$ and $(B^* \bmod p)$ have the same block triangular structure and thus

$$\begin{aligned}(AB^* \bmod p) &= (A \bmod p)(B^* \bmod p) \\ &= \begin{pmatrix} A_1 Q_1 B_1^\top Q_1^{-1} & & & * \\ & A_2 Q_2 B_2^\top Q_2^{-1} & & \\ & 0 & \ddots & \\ & & & A_u Q_u B_u^\top Q_u^{-1} \end{pmatrix}\end{aligned}$$

modulo p, which verifies the first claim, and the second claim follows similarly. □

The next lemma is the final preparation for the proof of Theorem 1. Given $A, B \in M_{d,d}(\mathbb{Z}_p)$ such that $\mathscr{R}(A)+\mathscr{R}(B) = \mathbb{Z}_p^d$ there always exists $\Theta \in M_{d,d}(\mathbb{Z}_p)$ such that $A+B\Theta$ is invertible. The lemma is a specific construction with Θ diagonal, that works if $AB^\top$ is symmetric.

Lemma 5. *Given* $A \in M_{d,d}(\mathbb{Z}_p)$*, define* $\sigma \subseteq \{1, \ldots, d\}$ *such that the* j^{th} *columns of* A *with* $j \in \sigma$ *form a basis for* $\mathscr{R}(A)$*. Let* $\Phi \in M_{d,d}(\mathbb{Z}_p)$ *be a diagonal matrix whose diagonal consists of zeros at* σ *and invertible elements at the complementary set of indices* $\complement\sigma = \{1, \ldots, d\} \setminus \sigma$*. Then for any* $B \in M_{d,d}(\mathbb{Z}_p)$ *such that* $\mathscr{R}(A) + \mathscr{R}(B) = \mathbb{Z}_p^d$ *and* $AB^\top = BA^\top$*, we have that the matrix* $A_0 := A + B\Phi$ *is invertible.*

Proof. For a $d \times d$ matrix A, and an index set $\sigma \subseteq \{1, \ldots, d\}$, let A_σ denote the $d \times |\sigma|$ matrix formed of those columns of A indexed by σ.

Since σ and $\complement\sigma$ are complementary index sets, we have

$$BA^\top = B_\sigma A_\sigma^\top + B_{\complement\sigma} A_{\complement\sigma}^\top. \tag{2}$$

Since A_σ is injective, $A_\sigma^\top$ is surjective and thus

$$\mathscr{R}(B_\sigma) = \mathscr{R}(B_\sigma A_\sigma^\top). \tag{3}$$

From (2), (3), and the condition $AB^\top = BA^\top$ we obtain the inclusion

$$\begin{aligned} \mathscr{R}(B_\sigma) = \mathscr{R}(B_\sigma A_\sigma^\top) &= \mathscr{R}(BA^\top - B_{\complement\sigma} A_{\complement\sigma}^\top) \\ &\subseteq \mathscr{R}(BA^\top) + \mathscr{R}(B_{\complement\sigma} A_{\complement\sigma}^\top) \\ &\subseteq \mathscr{R}(AB^\top) + \mathscr{R}(B_{\complement\sigma} A_{\complement\sigma}^\top) \\ &\subseteq \mathscr{R}(A) + \mathscr{R}(B_{\complement\sigma}) \end{aligned} \tag{4}$$

Since the columns of A_σ are a basis for $\mathscr{R}(A)$ we have

$$\mathscr{R}(A_{\complement\sigma}) \subseteq \mathscr{R}(A) = \mathscr{R}(A_\sigma). \tag{5}$$

Noticing that $\mathscr{R}(B_{\complement\sigma}) = \mathscr{R}((B\Phi)_{\complement\sigma})$ and making use of (4) and (5) we observe that

$$\begin{aligned} \mathscr{R}(A) + \mathscr{R}(B) &= \mathscr{R}(A) + \mathscr{R}(B_\sigma) + \mathscr{R}(B_{\complement\sigma}) \\ &\subseteq \mathscr{R}(A) + \mathscr{R}(B_{\complement\sigma}) \\ &= \mathscr{R}(A) + \mathscr{R}\big((B\Phi)_{\complement\sigma}\big) \\ &= \mathscr{R}(A) + \mathscr{R}\big(A_{\complement\sigma} + (B\Phi)_{\complement\sigma}\big) \\ &= \mathscr{R}(A_\sigma) + \mathscr{R}\big(A_{\complement\sigma} + (B\Phi)_{\complement\sigma}\big) \\ &= \mathscr{R}(A + B\Phi). \end{aligned}$$

Hence, $A + B\Phi$ is surjective and thus it is invertible. $\square$

Proof of Theorem 1. Since S is symplectic we have by Lemma 4(iv) that the corresponding diagonal blocks of (A mod p), (B mod p), (C mod p), and (D mod p) satisfy

$$\left.\begin{aligned} &A_j Q_j B_j^\top = B_j Q_j A_j^\top, \text{ and} \\ &A_j Q_j D_j^\top - B_j Q_j C_j^\top = Q_j, \end{aligned}\right. \qquad \text{for } j = 1, \ldots, u.$$

Since the latter of these identities implies $\mathscr{R}(A_j) + \mathscr{R}(B_j Q_j)$ is maximal, the assumptions of Lemma 5 are verified with A given by A_j, with B given by $B_j Q_j$, and with

$$\Phi = \frac{\nu}{p} Q_j^{-1} \Theta_j.$$

Note that the number ν/p is invertible modulo p and the matrix Q_j is invertible modulo p with inverse Q_j^{-1}. Therefore, by Lemma 5, $A_j + B_j(\frac{\nu}{p}\Theta_j)$ is invertible, for any $j = 1, \ldots, u$.

By Lemma 4(ii) we obtain that $(A \bmod p) + (B \bmod p)(\frac{\nu}{p}\Theta^{(p)})$ is invertible. For each prime p dividing $|G|$, we have

$$A_0 \bmod p = (A + B\Theta) \bmod p = (A \bmod p) + (B \bmod p)\ (\tfrac{\nu}{p}\Theta^{(p)}),$$

whence $(A_0 \bmod p)$ is invertible in $M_{d,d}(\mathbb{Z}_p)$. By deducing in this way the invertibility of $(A_0 \bmod p)$ in $M_{d,d}(\mathbb{Z}_p)$, for all prime factors p of $|G|$, we conclude that A_0 is invertible in $\mathrm{End}(G)$.

Next, since $A = A_0 - B\Theta$ and $C = C_0 - D\Theta$ we have

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A_0 & B \\ C_0 & D \end{pmatrix} \begin{pmatrix} I & 0 \\ -\Theta & I \end{pmatrix}. \tag{6}$$

Since Θ is symmetric, the second factor of the given matrix product is symplectic. Since $S \in \mathrm{Sp}(G)$, it implies also that the first factor of the product is symplectic. Since we have verified that A_0 is invertible, we thus can make use of the Weil decomposition of a symplectic matrix with invertible upper left block,

$$\begin{pmatrix} A_0 & B \\ C_0 & D \end{pmatrix} = \begin{pmatrix} I & 0 \\ C_0 A_0^{-1} & I \end{pmatrix} \begin{pmatrix} A_0 & 0 \\ 0 & (A_0^*)^{-1} \end{pmatrix} \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix} \begin{pmatrix} I & 0 \\ -A_0^{-1}B & I \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}. \tag{7}$$

Combining (6) and (7) and making use of Lemma 1 and Lemma 3 implies the desired intertwining identity (1). □

4. The continuous case

Our approach also implies a simple explicit formula for the multivariate continuous-time case $G = \mathbb{R}^d$. The continuous-time theory is described in detail in [15] and it is of increasing interest for example in time-frequency analysis, symplectic geometry, and (pseudo-)differential operators, we mention [10, 12, 16, 18]. An explicit formula for metaplectic operators without splitting into simple operators is given in [26], see also [28]. A construction by splitting into simple operators can be obtained by [15, Chapter 4] in conjunction with [22, Section I.6]. Here we obtain a simple, direct construction.

Given $\lambda \in \mathbb{R}^{2d}$, the time-frequency shift operator $\pi(\lambda)$ is defined by

$$\pi(\lambda) f(t) = \exp(2\pi i \cdot \omega^\top t)\, f(t - x), \qquad \lambda = (x, \omega) \in \mathbb{R}^{2d}, \quad t \in \mathbb{R}^d\ .$$

Let $A \in M_{d,d}(\mathbb{R})$ invertible and let $C \in M_{d,d}(\mathbb{R})$ such that $C = C^\top$. The Fourier transform $\mathcal{F}$, the dilation operator $\mathcal{L}_A$, and a suitable second degree character multiplication $\mathcal{R}_C$ are defined for Schwartz functions on $\mathbb{R}^d$ by

- $\mathcal{F} f(t) = \displaystyle\int_{\mathbb{R}^d} \exp(-2\pi i \cdot t^\top \eta)\, f(\eta)\, d\eta, \qquad t \in \mathbb{R}^d,$
- $\mathcal{L}_A f(t) = |\det A|^{-1/2} f(A^{-1} t), \qquad t \in \mathbb{R}^d,$
- $\mathcal{R}_C f(t) = \exp(\pi i \cdot t^\top C t)\, f(t), \qquad t \in \mathbb{R}^d,$

respectively, and they satisfy (see [15], with a slightly different notation)

(i) $\mathcal{F}\,\pi(x,\omega)\,\mathcal{F}^{-1} = \exp(2\pi i\cdot\omega^\top x)\,\pi(\omega,-x), \qquad x,\omega\in\mathbb{R}^d,$

(ii) $\mathcal{L}_A\,\pi(x,\omega)\,\mathcal{L}_A^{-1} = \pi\big(Ax,(A^\top)^{-1}\omega\big), \qquad x,\omega\in\mathbb{R}^d,$

(iii) $\mathcal{R}_C\,\pi(x,\omega)\,\mathcal{R}_C^{-1} = \exp(-\pi i\cdot x^\top C\,x)\,\pi(x,Cx+\omega), \qquad x,\omega\in\mathbb{R}^d.$

The symplectic group $\mathrm{Sp}(\mathbb{R}^d)$ consists of the real $2d\times 2d$ matrices in block form

$$S=\begin{pmatrix}A & B\\ C & D\end{pmatrix}, \qquad A,B,C,D\in M_{d,d}(\mathbb{R}),$$

such that $A^\top C = C^\top A$, $B^\top D = D^\top B$, and $A^\top D - C^\top B = I$, with I the $d\times d$ identity matrix. We obtain the following construction of metaplectic operators for the continuous case. The result follows from the analogy to the special case $G=\mathbb{Z}_p^d$ of the finite abelian group setting discussed in this paper.

Theorem 2. *Let $S=\left(\begin{smallmatrix}A&B\\C&D\end{smallmatrix}\right)\in\mathrm{Sp}(\mathbb{R}^d)$. Define $\sigma\subseteq\{1,\dots,d\}$ such that the columns of A indexed by σ form a basis for $\mathscr{R}(A)$. Denote by $\Theta\in M_{d,d}(\mathbb{Z})$ the diagonal matrix whose diagonal is 0 at σ and 1 at the complementary set of indices $\complement\sigma=\{1,\dots,d\}\setminus\sigma$. Let $A_0=A+B\Theta$ and $C_0=C+D\Theta$. Then A_0 is invertible and the operator $U=U_S$ defined by*

$$U := \mathcal{R}_{C_0\,A_0^{-1}}\cdot\mathcal{L}_{A_0}\cdot\mathcal{F}^{-1}\cdot\mathcal{R}_{-A_0^{-1}B}\cdot\mathcal{F}\cdot\mathcal{R}_{-\Theta}\;.$$

is unitary and satisfies

$$U\pi(\lambda)U^{-1} = \psi(\lambda)\,\pi(S\lambda), \qquad \lambda\in\mathbb{R}^{2d},$$

with some scalar function $\psi\colon\mathbb{R}^{2d}\to\mathbb{T}$.

References

[1] D. M. Appleby, *Symmetric informationally complete-positive operator valued measures and the extended Clifford group*, J. Math. Phys. **46** (2005), no. 5, 052107, 29 pp.

[2] G. G. Athanasiu, E. G. Floratos, and S. Nicolis, *Fast quantum maps*, J. Phys. A **31** (1998), no. 38, L655–L662.

[3] L. Baggett and A. Kleppner, *Multiplier representations of abelian groups*, J. Funct. Anal. **14** (1973), 299–324.

[4] R. Balian and C. Itzykson, *Observations sur la mécanique quantique finie*, C. R. Acad. Sci. Paris Sér. I Math. **303** (1986), no. 16, 773–778.

[5] M. C. Berg, *The Fourier-analytic proof of quadratic reciprocity*, Wiley, New York, 2000.

[6] P. G. Casazza and M. Fickus, *Fourier transforms of finite chirps*, Frames and Overcomplete Representations in Signal Processing, Communications, and Information Theory (eds. R. V. Balan, Y. C. Eldar, and T. Strohmer), Hindawi Publ., 2006, pp. 1–7.

[7] O. Christensen, *An Introduction to Frames and Riesz Bases*, Birkhäuser, Boston, 2003.

[8] G. Cliff, D. McNeilly, F. Szechtman, *Weil representations of symplectic groups over rings*, J. London Math. Soc. **62** (2000), no. 2, 423–436.

[9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Oxford Univ. Press, Eynsham, 1985.

[10] E. Cordero and F. Nicola, *Metaplectic representation on Wiener amalgam spaces and applications to the Schrödinger equation*, J. Funct. Anal. **254** (2008), no. 2, 506–534.

[11] T. Digernes, V. S. Varadarajan, and S. R. S. Varadhan, *Finite approximations to quantum systems*, Rev. Math. Phys. **6** (1994), no. 4, 621–648.
[12] H. G. Feichtinger and K. Gröchenig, *Gabor wavelets and the Heisenberg group: Gabor expansions and short time Fourier transform from the group theoretical point of view*, Wavelets: a Tutorial in Theory and Applications (ed. C. K. Chui), Acad. Press, Boston, 1992, pp. 359–397.
[13] H. G. Feichtinger, M. Hazewinkel, N. Kaiblinger, E. Matusiak, and M. Neuhauser, *Metaplectic operators on* $\mathbb{C}^n$, Quart. J. Math. **59** (2008), no. 1, 15–28.
[14] H. G. Feichtinger, W. Kozek, F. Luef, *Gabor analysis over finite Abelian groups*, Appl. Comput. Harmon. Anal. **26** (2009), no. 2, 230–248.
[15] G. B. Folland, *Harmonic Analysis in Phase Space*, Princeton Univ. Press, 1989.
[16] M. de Gosson, *Symplectic Geometry and Quantum Mechanics*, Birkhäuser, Basel, 2006.
[17] J. Grassberger and G. Hörmann, *A note on representations of the finite Heisenberg group and sums of greatest common divisors*, Discrete Math. Theor. Comput. Sci. **4** (2001), no. 2, 91–100.
[18] K. Gröchenig, *Foundations of Time-Frequency Analysis*, Birkhäuser, Boston, 2001.
[19] S. Gurevich and R. Hadani, *The geometric Weil representation*, Selecta Math. **13** (2007), no. 3, 465–481.
[20] K. C. Hannabuss, *Characters and contact transformations*, Math. Proc. Cambridge Philos. Soc. **90** (1981), no. 3, 465–476.
[21] C. J. Hillar, D. L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly **114** (2007), no. 10, 917–923.
[22] J. Igusa, *Theta Functions*, Springer-Verlag, New York, 1972.
[23] N. Kaiblinger, *Approximation of the Fourier transform and the dual Gabor window*, J. Fourier Anal. Appl. **11** (2005), no. 1, 25–42.
[24] G. Kutyniok and T. Strohmer, *Wilson bases for general time-frequency lattices*, SIAM J. Math. Anal. **37** (2005), no. 3, 685–711.
[25] G. Lion and M. Vergne, *The Weil Representation, Maslov Index and Theta Series*, Birkhäuser, Boston, 1980.
[26] H. ter Morsche and P. J. Oonincx, *On the integral representations for metaplectic operators*, J. Fourier Anal. Appl. **8** (2002), no. 3, 245–257.
[27] M. Neuhauser, *An explicit construction of the metaplectic representation over a finite field*, J. Lie Theory **12** (2002), no. 1, 15–30.
[28] R. Ranga Rao, *On some explicit formulas in the theory of Weil representation*, Pacific J. Math. **157** (1993), no. 2, 335–371.
[29] H. Reiter, *Metaplectic Groups and Segal Algebras*, Lecture Notes in Mathematics, vol. 1382, Springer-Verlag, Berlin, 1989.
[30] J. A. Rosenberg, *A selective history of the Stone–von Neumann theorem*, Operator algebras, quantization, and noncommutative geometry, 331–353, Amer. Math. Soc., Providence, 2004.
[31] T. Strohmer, *Numerical algorithms for discrete Gabor expansions*, Gabor Analysis and Algorithm (eds. H. G. Feichtinger and T. Strohmer), Birkhäuser, Boston, 1998, pp. 267–294.
[32] A. Vourdas, *Quantum systems with finite Hilbert space*, Rep. Progr. Phys. **67** (2004), 267–320.
[33] A. Weil, *Sur certains groupes d'opérateurs unitaires*, Acta Math. **111** (1964), 143–211.
[34] D. L. Winter, *The automorphism group of an extraspecial p-group*, Rocky Mountain J. Math. **2** (1972), no. 2, 159–168.