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

by Norbert Kaiblinger$^a$ and Markus Neuhauser$^b$

$^a$ Faculty of Mathematics, University of Vienna, Nordbergstraße 15, 1090 Vienna, Austria
$^b$ Lehrstuhl A für Mathematik, RWTH Aachen, 52056 Aachen, Germany

Communicated by Prof. M.S. Keane

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 $G = \mathbb{R}^d$.

1. 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

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

Finite abelian groups are self-dual, that is, $G$ is isomorphic to its dual group $\hat{G}$ consisting of the homomorphisms into the circle group $\mathbb{T} = \{ \tau \in \mathbb{C}: |\tau| = 1 \}$.

MSC: 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

$^a$ N. Kaiblinger was supported by the Austrian Science Fund FWF grant P 21339. M. Neuhauser was supported by the Marie-Curie Excellence Grant MEXT-CT-2004-517154.

E-mails: norbert.kaiblinger@univie.ac.at (N. Kaiblinger), markus.neuhauser@matha.rwth-aachen.de (M. Neuhauser).
Specifically, we identify a character $\chi \in \hat{G}$ with an element $m \in G$ by writing $\chi : k \mapsto (m, k)$ in terms of the bicharacter

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

where

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

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

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

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

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

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

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

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

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

$$a'_{r,s} = a_{r,s} \text{ mod } n_r, \quad r, s = 1, \ldots, d.$$

The endomorphism ring structure is thus given by the usual matrix operations. This description of $\text{End}(G)$ 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 $A \in \text{End}(G)$ with representative $[A] \in M_{d,d}(\mathbb{Z})$, the matrix

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

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

$$\langle m, Ak \rangle = \exp(2\pi i \cdot m^T N^{-1} Ak)$$

$$= \exp(2\pi i \cdot (NA^T N^{-1} m)^T N^{-1} k) = \langle A^* m, k \rangle, \quad k, m \in G.$$  

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 $A \in \text{End}(G)$ and a specific representative $[A] \in M_{d,d}(\mathbb{Z})$.

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

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

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

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

that follow since $S \in \text{Sp}(G)$ implies that $S$ is invertible with $S^{-1} = \begin{pmatrix} D^* & -B^* \\ -C^* & A^* \end{pmatrix} \in \text{Sp}(G)$. Then the fundamental result mentioned above reads that there exists a unitary operator $U$ on $\mathbb{C}^{d^2}$, called a metaplectic operator for $S$, such that

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

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

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 2 and proved in Section 4, based on preliminary results which can be found in Section 3. The construction for the continuous-time case $G = \mathbb{R}^d$ is presented in Section 5.
We use the following unitary operators acting on $n_1 \times \cdots \times n_d$ hypermatrices $v \in \mathbb{C}^{n_1 \times \cdots \times n_d}$, viewed as functions on $G$. By $\text{Aut}(G) \subseteq \text{End}(G)$ denote the group of automorphisms of $G$.

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

\begin{align*}
\mathcal{F}v(k) &= \frac{1}{\sqrt{\det N}} \sum_{m \in G} \exp(-2\pi i \cdot k^TN^{-1}m) v(m), \quad k \in G, \\
L_A v(k) &= v(A^{-1}k), \quad k \in G, \\
R_C v(k) &= \psi_C(k) v(k), \quad k \in G,
\end{align*}

where the function $\psi_C$ on $G$ is defined by

$$
\psi_C(k) = \exp(\pi i \cdot k^T(I + N^{-1})C(I + N)k), \quad k \in G.
$$

We remark that the careful definition of $\psi_C$ is one of the crucial steps of our approach, it is shown in Lemma 2 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 $f(k) = \exp(\pi i \cdot k^TN^{-1}[C]k)$ does not work, cf. [6,13]; while $f$ may not be well defined on $G$, we will show that $\psi_C(k) = f((I + N)k)$ 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 $\mathcal{R}(A)$ the image of a given homomorphism $A$.

**Theorem 1.** Let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_d}$ such that $n_1 | n_2 | \cdots | n_d$ and let $S = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{Sp}(G)$. 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,

$$
N = \text{diag}(n_1, \ldots, n_d) = \text{diag}(p^{\alpha_1}Q_1, \ldots, p^{\alpha_u}Q_u), \quad \alpha_1 < \alpha_2 < \cdots < \alpha_u,
$$

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

$$
(A \mod p) = \begin{pmatrix}
A_1 & \ast & & \\
& A_2 & & \\
& & \ddots & \\
& & & A_u
\end{pmatrix}.
$$
such that \( A_j \) has the same size as \( Q_j \), for \( j = 1, \ldots, u \). Next, for each diagonal block \( A_j \), denote by \( \sigma_j \) a set of indices such that the respective columns of \( A_j \) form a basis for \( \mathcal{R}(A_j) \). Denote by \( \Theta_j \) the diagonal matrix of the same size as \( A_j \) whose diagonal is 0 at the positions indexed by \( \sigma_j \) and 1 otherwise. Finally, let

\[
\Theta(p) = \text{diag}(\Theta_1, \ldots, \Theta_u).
\]

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

\[
\Theta = \sum_{\substack{p \text{ prime, } \nu \mid v \atop p \neq v}} \frac{\nu}{p} \Theta(p),
\]

where \( \nu \) 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

\[
U := R_{[C_0A_0^{-1}]} \cdot L_{A_0} \cdot \mathcal{F}^{-1} \cdot R_{[-A_0^{-1}B]} \cdot \mathcal{F} \cdot R_{[-\Theta]}
\]

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

**Remark 1.** (i) If in an actual computation some block triangular structure of \((A \text{ mod } p)\) is observed that is finer than the one described in the theorem, it can be used as well. By contrast, a coarser block triangular structure 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 \( S = \left( \begin{smallmatrix} A & 0 \\ 1 & 0 \end{smallmatrix} \right) \) with \( A = \left( \begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix} \right) \). Notice that \( A^* = NA^TN^{-1} = A \) and hence \( S \in \text{Sp}(G) \). Writing \((A \text{ mod } p) = \left( \begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix} \right) = \left( \begin{smallmatrix} A_1 & 1 \\ 0 & A_2 \end{smallmatrix} \right) \) we correctly obtain \( \sigma_1 = \sigma_2 = \emptyset \) and \( \Theta = \Theta(p) = I \), indeed \( A_0 = A + B\Theta = \left( \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right) \) is invertible. On the other hand, incorrectly viewing \((A \text{ mod } p)\) as one single block \( A_1 \) yields \( \sigma_1 = \{2\} \) and thus \( \Theta = \Theta(p) = \left( \begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix} \right) \), which does not work, since \( A + B\Theta = \left( \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right) \) is not invertible.

(ii) The scalar function \( \psi \) 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 \( \psi \) is a function on \( G^2 \).

(iii) The construction of \( \Theta \) in terms of the matrices \( \Theta(p) \) is an application of the Chinese remainder theorem so to obtain \((\Theta \text{ mod } p) = \nu/p)\Theta(p)\). Aiming at the plain relations \((\Theta \text{ mod } p) = \Theta(p)\) works as well yet our approach is favorable since the formula for \( \Theta \) is especially simple. Generally, the theorem also works for other choices of \( \Theta \) such as \( \Theta \) multiplied by an any \( \Sigma \in \text{Aut}(G) \) 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 \( \pi(\lambda), \lambda \in G^2 \),

\[
H_0(G) = \{ \tau \pi(\lambda): \lambda \in G^2, \tau \in \mathbb{T}_n \},
\]

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, Section 5.2]. Theorem 1 thus relates to the automorphisms of a class of extraspecial groups, whose structure is analyzed in [34]. See also [17].

3. 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 \( U = U_1 U_2 \) satisfies (1) for \( S = S_1 S_2 \).

**Proof.** We have

\[
U_1 U_2 \pi(\lambda) U_2^{-1} U_1^{-1} = \psi_2(\lambda) U_1 \pi(\lambda) U_1^{-1} = \psi_1(S_2 \lambda) \psi_2(\lambda) \pi(S_1 S_2 \lambda).
\]

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 \( C \in \text{End}(G) \).

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

(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

\[
\psi_C(k + k') = \psi_C(k) \psi_C(k') \psi_C(Ck'k), \quad k, k' \in G.
\]

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

(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

\[
\psi_{[C]}([k] + Nz) = \exp(\pi i \cdot ([k] + Nz)^T (I + N^{-1})[C](I + N)([k] + Nz))
\]

\[
= \exp(\pi i \cdot [k]^T (I + N^{-1})[C](I + N)[k])
\]

\[
= \psi_{[C]}([k])
\]

\[
\times \exp(\pi i \cdot z^T (N + I)[C](I + N)Nz)
\]

\[
= 1
\]

\[
\times \exp(2\pi i \cdot Z^T (N + I)[C](I + N)[k])
\]

\[
= 1
\]

\[
= \psi_{[C]}([k]).
\]

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

\[
\psi_{[C]}(k + k') = \exp(\pi i \cdot (k + k')^T (I + N^{-1})[C](I + N)(k + k'))
\]

\[
= \exp(\pi i \cdot k^T (I + N^{-1})[C](I + N)k)
\]

\[
= \psi_{[C]}(k)
\]

\[
\times \exp(\pi i \cdot k'^T (I + N^{-1})[C](I + N)k')
\]

\[
= \psi_{[C]}(k')
\]

\[
\times \exp(2\pi i \cdot k^T (I + N^{-1})[C](I + N)k')
\]

\[
= \psi_{[C]}(k) \psi_{[C]}(k') \exp(2\pi i \cdot k^T N^{-1}[C]k')
\]

\[
= (k,Ck')
\]

\[
\times \exp(2\pi i \cdot k^T ([C] + N^{-1}[C]N + [C]N)k')
\]

\[
= 1
\]

\[
= \psi_{[C]}(k) \psi_{[C]}(k')(k, Ck'),
\]

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

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

respectively. More precisely, we have

(i) $\mathcal{F} \pi(l, m) \mathcal{F}^{-1} = \exp(2\pi i \cdot m^	op N^{-1}l) \pi(m, -l)$, \quad $l, m \in G$,

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

(iii) $R_{[C]} \pi(l, m) R_{[C]}^{-1} = \exp(-\pi i \cdot l^\top (I + N^{-1})[C](I + N)l) \pi(l, Cl + m)$, \quad $l, m \in G$.

Proof. (i) Use elementary properties of the Fourier transform, first $\mathcal{F} \pi(0, m) = \pi(m, 0) \mathcal{F}$, secondly $\mathcal{F} v(k) = v(-k)$, 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

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

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

$$R_{[C]} \pi(l, 0) v(k) = \psi_{[C]}(k) v(k - l) = \psi_{[C]}(l + (k - l)) v(k - l) = \psi_{[C]}(l) \psi_{[C]}(k - l) v(k - l) = \psi_{[C]}(l) (Cl, k - l) \psi_{[C]}(k - l) v(k - l) = \overline{\psi_{[C]}(l) \pi(l, Cl) R_{[C]} v(k)},$$

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

4. PROOF OF THEOREM 1

We prepare the matrix block structure used in Theorem 1.

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

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

with $u \leq d$, such that each $Q_j$ is invertible modulo $p$. Then we have:
(i) For $A \in \text{End}(G)$, 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,

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

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 $A_j Q_j B_j^T = B_j Q_j A_j^T$ and $A_j Q_j D_j^T - B_j Q_j C_j^T = Q_j$, 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 $A^* \in \text{End}(G)$ the observation in (i) also applies to $A^*$. Next, the diagonal blocks of $(A^* \bmod p)$ correspond to those parts of $A^* = N A^T N^{-1}$ where the following cancellation of powers of $p$ is in effect, $(A^*)_j = (N A^T N^{-1})_j = Q_j A_j^T Q_j^{-1}$.

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

\[
(AB^* \bmod p) = (A \bmod p)(B^* \bmod p)
\]

\[
= \begin{pmatrix}
A_1 Q_1 B_1^T Q_1^{-1} & * \\
& A_2 Q_2 B_2^T Q_2^{-1} & \\
& & \ddots \\
& & & A_u Q_u B_u^T Q_u^{-1}
\end{pmatrix}
\]

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 $R(A) + R(B) = \mathbb{Z}_p^d$ 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 $\Theta$ diagonal, that works if $AB^T$ 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 \( \mathcal{R}(A) \). Let \( \Phi \in M_{d,d}(\mathbb{Z}_p) \) be a diagonal matrix whose diagonal consists of zeros at \( \sigma \) and invertible elements at the complementary set of indices \( \mathbb{C} \sigma = \{1, \ldots, d\} \setminus \sigma \). Then for any \( B \in M_{d,d}(\mathbb{Z}_p) \) such that \( \mathcal{R}(A) + \mathcal{R}(B) = \mathbb{Z}_p^d \) 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 \( A_\sigma \) denote the \( d \times |\sigma| \) matrix formed of those columns of \( A \) indexed by \( \sigma \).

Since \( \sigma \) and \( \mathbb{C} \sigma \) are complementary index sets, we have

\[
(2) \quad BA^\top = B_\sigma A_\sigma^\top + B_{\mathbb{C} \sigma} A_{\mathbb{C} \sigma}^\top.
\]

Since \( A_\sigma \) is injective, \( A_\sigma^\top \) is surjective and thus

\[
(3) \quad \mathcal{R}(B_\sigma) = \mathcal{R}(B_\sigma A_\sigma^\top).
\]

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

\[
\mathcal{R}(B_\sigma) = \mathcal{R}(B_\sigma A_\sigma^\top) = \mathcal{R}(BA^\top - B_{\mathbb{C} \sigma} A_{\mathbb{C} \sigma}^\top) \\
\subseteq \mathcal{R}(BA^\top) + \mathcal{R}(B_{\mathbb{C} \sigma} A_{\mathbb{C} \sigma}^\top) \\
\subseteq \mathcal{R}(AB^\top) + \mathcal{R}(B_{\mathbb{C} \sigma} A_{\mathbb{C} \sigma}^\top) \\
\subseteq \mathcal{R}(A) + \mathcal{R}(B_{\mathbb{C} \sigma})
\]

(4)

Since the columns of \( A_\sigma \) are a basis for \( \mathcal{R}(A) \) we have

\[
(5) \quad \mathcal{R}(A_{\mathbb{C} \sigma}) \subseteq \mathcal{R}(A) = \mathcal{R}(A_\sigma).
\]

Noticing that \( \mathcal{R}(B_{\mathbb{C} \sigma}) = \mathcal{R}((B\Phi)_{\mathbb{C} \sigma}) \) and making use of (4) and (5) we observe that

\[
\mathcal{R}(A) + \mathcal{R}(B) = \mathcal{R}(A) + \mathcal{R}(B_\sigma) + \mathcal{R}(B_{\mathbb{C} \sigma}) \\
\subseteq \mathcal{R}(A) + \mathcal{R}(B_{\mathbb{C} \sigma}) \\
= \mathcal{R}(A) + \mathcal{R}((B\Phi)_{\mathbb{C} \sigma}) \\
= \mathcal{R}(A) + \mathcal{R}(A_{\mathbb{C} \sigma} + (B\Phi)_{\mathbb{C} \sigma}) \\
= \mathcal{R}(A_\sigma) + \mathcal{R}(A_{\mathbb{C} \sigma} + (B\Phi)_{\mathbb{C} \sigma}) \\
= \mathcal{R}(A + B\Phi).
\]

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

\[
A_j Q_j B_j^\top = B_j Q_j A_j^\top
\]

242
\[ A_jQ_jD_j^T - B_jQ_jC_j^T = Q_j \quad \text{for } j = 1, \ldots, u. \]

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

\[ \Phi = \frac{v}{p}Q_j^{-1}\Theta_j. \]

Note that the number \( v/p \) is invertible modulo \( p \) and the matrix \( Q_j \) is invertible modulo \( p \) with inverse \( Q_j^{-1} \). Therefore, by Lemma 5, \( A_j + B_j(\frac{v}{p}\Theta_j) \) is invertible, for any \( j = 1, \ldots, u \). By Lemma 4(ii) we obtain that \((A \mod p) + (B \mod p)(\frac{v}{p}\Theta^{(p)})\) is invertible. For each prime \( p \) dividing \(|G|\), we have

\[ A_0 \mod p = (A + B\Theta) \mod p = (A \mod p) + (B \mod p)(\frac{v}{p}\Theta^{(p)}), \]

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

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

\[ \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A_0 & B \\ C_0 & D \end{pmatrix} \begin{pmatrix} I & 0 \\ -\Theta & I \end{pmatrix}. \]

Since \( \Theta \) is symmetric, the second factor of the given matrix product is symplectic. Since \( S \in \text{Sp}(G) \), 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,

\[ \begin{pmatrix} A_0 & B \\ C_0 & D \end{pmatrix} \begin{pmatrix} I & 0 \\ -A_0^{-1}B & I \end{pmatrix} = \begin{pmatrix} 0 & -I \\ 0 & I \end{pmatrix} \]

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

5. 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 1.6]. Here we obtain a simple, direct construction.

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

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

Let \( A \in M_{d,d}(\mathbb{R}) \) invertible and let \( C \in M_{d,d}(\mathbb{R}) \) such that \( C = C^T \). 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

\[
\begin{align*}
\mathcal{F} f(t) &= \int_{\mathbb{R}^d} \exp(-2\pi i \cdot t^T \eta)f(\eta) d\eta, & t \in \mathbb{R}^d, \\
\mathcal{L}_A f(t) &= |\det A|^{-1/2} f(A^{-1} t), & t \in \mathbb{R}^d, \\
\mathcal{R}_C f(t) &= \exp(\pi i \cdot t^T C t)f(t), & t \in \mathbb{R}^d,
\end{align*}
\]

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

\[
\begin{align*}
(i) \quad \mathcal{F} \pi(x, \omega) \mathcal{F}^{-1} &= \exp(2\pi i \cdot \omega^T x) \pi(\omega, -x), & x, \omega \in \mathbb{R}^d, \\
(ii) \quad \mathcal{L}_A \pi(x, \omega) \mathcal{L}_A^{-1} &= \pi(Ax, (A^T)^{-1} \omega), & x, \omega \in \mathbb{R}^d, \\
(iii) \quad \mathcal{R}_C \pi(x, \omega) \mathcal{R}_C^{-1} &= \exp(-\pi i \cdot x^T C x) \pi(x, Cx + \omega), & x, \omega \in \mathbb{R}^d.
\end{align*}
\]

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

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

such that \( A^T C = C^T A, B^T D = D^T B, \) and \( A^T D - C^T B = I \), 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 \( S = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{Sp}(\mathbb{R}^d) \). Define \( \sigma \subseteq \{1, \ldots, d\} \) such that the columns of \( A \) indexed by \( \sigma \) form a basis for \( \mathcal{R}(A) \). Denote by \( \Theta \in M_{d,d}(\mathbb{Z}) \) the diagonal matrix whose diagonal is 0 at \( \sigma \) and 1 at the complementary set of indices \( \overline{\sigma} = \{1, \ldots, d\} \setminus \sigma \). 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

\[
U := \mathcal{R}_{C_0} A_0^{-1} \cdot \mathcal{L}_{A_0} \cdot \mathcal{F}^{-1} \cdot \mathcal{R}_{-A_0} \cdot B \cdot \mathcal{F} \cdot \mathcal{R}_{-\Theta}
\]

is unitary and satisfies

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

with some scalar function \( \psi : \mathbb{R}^{2d} \to \mathbb{T} \).

244
REFERENCES


(Received March 2009)