Harmonic Analysis on Finite Groups and DSP Applications

William J. DeMeo
williamdemeo@yahoo.com

***Abstract*— \input{DSP/UHEE616-abstract} Underlying most digital signal processing (DSP) algorithms is the group $\mathbb{Z}/N$ of integers modulo N, which is taken as the data indexing set. Translations are defined using addition modulo N, and DSP operations, including convolutions and Fourier expansions, are then developed relative to these translations. Recently, An and Tolimieri [1] considered a different class of index set mappings, which arise when the underlying group is nonabelian, and successfully apply them to 2D image data.**

The present work provides an overview of harmonic analysis on finite groups and group algebras. "Generalized translation," and its consequence, "generalized convolution" are defined. Thereafter, some concrete and simple, yet revealing, examples of nonabelian-group indexing sets are discussed along with their practical DSP implications.

\input{DSP/UHEE616-intro}

I. Introduction

The translation-invariance of most classical signal processing transforms and filtering operations is largely responsible for their widespread use, and is crucial for efficient algorithmic implementation and interpretation of results [1].

DSP on *finite abelian groups* such as $\mathbb{Z}/N$ is well understood and has great practical utility. Translations are defined using addition modulo N, and basic operations, including convolutions and Fourier expansions, are developed relative to these translations [2]. Recently, however, interest in the practical utility of *finite nonabelian groups* has grown significantly. Although the theoretical foundations of nonabelian groups is well established, application of the theory to DSP has yet to become common-place. A notable exception is [1], which develops theory and algorithms for indexing data with nonabelian groups, defining translations with a non-commutative group multiply operation, and performing typical DSP operations relative to these translations.

This paper describes the use of nonabelian groups for indexing one- and two-dimensional signals, and discusses some computational advantages and insights that can be gained from such an approach. A simple but instructive class of nonabelian groups is examined. When elements of such groups are used to index the data, and standard DSP operations are defined with respect to special group binary operators, more general and interesting signal transformations are possible.

A. Preview: Two Distinctions of Consequence

Abelian group DSP can be completely described in terms of a special class of signals called the *characters* of the group. (For $\mathbb{Z}/N$, the characters are simply the exponentials.) Each character of an abelian group represents a one-dimensional translation-invariant subspace, and the set of all characters spans the space of signals indexed by the group; any such signal can be uniquely expanded as a linear combination over the characters.

In contrast, the characters of a nonabelian group G do not determine a basis for the space of signals indexed by G. However, a basis can be constructed by extending the characters of an abelian subgroup A of G, and then taking certain translations of these extensions. Some of the characters of A cannot be extended to characters of G, but only to proper subgroups of G. This presents some difficulties involving the underlying translation-invariant subspaces, some of which are now multi-dimensional. However, it also presents opportunities for alternative views of local signal domain information on these translation-invariant subspaces.

The other abelian/nonabelian distinction of primary importance concerns translations defined on the group. In the abelian group case, translations represent simple linear shifts in space or time. When nonabelian groups index the data, however, translations are no longer so narrowly defined.

\input{DSP/UHEE616-cyclic}

II. Finite Groups

This section summarizes the notations, definitions, and important facts needed below. The presentation style is terse since the goal of this section is to distill from the more general literature only those results that are most relevant to our application. The books [1] and [2] treat similar material in a more thorough and rigorous manner. Throughout, $\mathbb{C}$ denotes complex numbers, G an arbitrary finite (nonabelian) group, and $\mathcal{L}(G)$ the collection of complex valued functions of G.

A. Cyclic Groups

A group C is called a *cyclic group* if there exists $x \in C$ such that every $y \in C$ has the form $y = x^n$ for some integer n. In this case, we call x a *generator* of C. Cyclic groups are frequently constructed as special subgroups of arbitrary groups.

If G is an arbitrary finite group, and $x \in G$, then the set of powers of x,

$$gp_G(x) = \{x^n : n \in \mathbb{Z}\}, \tag{1}$$

is a cyclic subgroup of G called the *group generated by x in G*. If the underlying group is understood, (1) may be denoted $gp(x)$.

It will be convenient to have notation for a cyclic group of order N without reference to a particular underlying group. Let the set of formal symbols

$$C_N(x) = \{x^n : 0 \le n < N\} \tag{2}$$

denote the cyclic group of order N with generator x, and define binary composition by

$$x^m x^n = x^{m+n}, \quad 0 \le m, n < N, \tag{3}$$

where $m + n$ is addition modulo N. Then $C_N(x)$ is a cyclic group of order N having generator x. The identity element of $C_N(x)$ is $x^0 = 1$, and the inverse of x^n in $C_N(x)$ is x^{N-n}.

To say that a group is *abelian* is to specify that the binary composition of the group is commutative, in which case the symbol $+$ is usually used to represent this operation. For nonabelian groups, we write the (non-commutative) binary composition as multiplication. Since our work involves both abelian and nonabelian groups, it is notationally cleaner to write the binary operations of an arbitrary group – abelian or otherwise – as multiplication. The following examples illustrate that additive groups, such as $\mathbb{Z}/N$ with addition modulo N, have simple multiplicative representations.

Example 1 Let $\mathbb{Z}/N = \{0, 1, \ldots, N-1\}$, and let addition modulo N be the binary composition on $\mathbb{Z}/N$. This group is isomorphic to the cyclic group $C_N(x)$,

$$\mathbb{Z}/N = \{n : 0 \le n < N\} \simeq \{x^n : 0 \le n < N\} = C_N(x),$$

and it is by this identification that the binary composition of $\mathbb{Z}/N$ can be written as multiplication. More precisely, by uniquely identifying each element $m \in \mathbb{Z}/N$ with the corresponding element $x^m \in C_N(x)$, the binary composition $m + n$ is replaced with that of (3).

Example 2 Consider the direct product group

$$\mathbb{Z}/M \times \mathbb{Z}/N = \{(m, n) : 0 \le m < M,\, 0 \le n < N\}, \tag{4}$$

each element of which might represent a 2-dimensional spatial coordinate. More generally, identify (4) by isomorphism with the group

$$C_M(x) \times C_N(y) = \{x^m y^n : 0 \le m < M,\, 0 \le n < N\}, \tag{5}$$

and define binary composition as follows:

$$(x^m y^n)(x^j y^k) = x^{m+j} y^{n+k},\ 0 \le m, j < M,\ 0 \le n, k < N,$$

where $m + j$ is addition modulo M and $n + k$ is addition modulo N.

Example 3 For an integer $L \in \mathbb{Z}/N$, denote by $gp_N(x^L)$ the subgroup generated by x^L in $C_N(x)$. If L divides N, then

$$gp_N(x^L) = \{x^{mL} : 0 \le m < M\}, \quad LM = N,$$

and $gp_N(x^L)$ is a cyclic group of order M.

B. Group of Units

Multiplication modulo N is a ring product on the group of integers $\mathbb{Z}/N$. An element $m \in \mathbb{Z}/N$ is called a *unit* if there exists an $n \in \mathbb{Z}/N$ such that $mn = 1$. The set $U(N)$ of all units in $\mathbb{Z}/N$ is a group with respect to multiplication modulo N, and is called the *group of units*.The group of units can be described as the set of all integers $0 < m < N$ such that m and N are relatively prime.

Example 4 For $N = 8$, $U(8) = \{1, 3, 5, 7\}$.

C. Quotient Groups

In image processing applications the set used to index the data is an important factor influencing performance of the resulting algorithms. Typically image data are indexed by elements of direct products of cyclic groups, such as (5). Implicit in our present treatment of such direct product groups are some standard identifications, such as $x^1 y^0 = (x, 1) = x$, and $x^0 y^1 = (1, y) = y$. There is no ambiguity in this representation, though it may take some getting used to. The unaccustomed reader is well-advised to consult [1] for reassurance.

Let $A = C_N(x) \times C_N(y)$ and suppose B is the subgroup of A with elements in

$$gp_N(x^L) \times gp_N(y^L) = \{x^{pL} y^{qL} : 0 \le p, q < M\},$$

where $LM = N$. The group B is a direct product of cyclic groups of order M. The *quotient group* A/B is given by

$$A/B = \{x^j y^k B : 0 \le j, k < L\}.$$

Each member of A/B is a direct product of cyclic subgroups of A, called a *B-coset of A*. More specifically, the member $x^j y^k B \in A/B$ is called the *B-coset of A with representative $x^j y^k$*. The elements within a particular coset are called *equivalent modulo B*. A complete set of *B-coset representatives in A* is $H = \{x^j y^k : 0 \le j, k < L\} = C_L(x) \times C_L(y)$. Thus, H is a direct product of cyclic groups of order L. Furthermore, any element $a \in A$ can be uniquely written as

$$a = hb, \qquad h \in H,\ b \in B,$$

where h specifies that a belongs to the coset hB, and b identifies a within that coset. We give concrete examples of B-cosets for a few special cases.

Example 5 For $N = 8$, $M = 2$, $L = 4$,

$$A = C_8(x) \times C_8(y) = \{x^m y^n : 0 \le m, n < 8\}, \tag{6}$$

and

$$B = gp_8(x^4) \times gp_8(y^4) = \{x^{p4} y^{q4} : 0 \le p, q < 2\}.$$

In the following table, the numbers denote exponents mn on the elements $x^m y^n \in A$ in (6).

m \ n	0	1	2	3	4	5	6	7
0	**00**	01	02	03	**04**	05	06	07
1	10	11	12	13	14	15	16	17
2	20	21	22	23	24	25	26	27
3	30	31	32	33	34	35	36	37
4	**40**	41	42	43	**44**	45	46	47
5	50	51	52	53	54	55	56	57
6	60	61	62	63	64	65	66	67
7	70	71	72	73	74	75	76	77

For illustrative purposes, the exponents belonging to the B-coset with representative x^0y^0 are set in bold font; that is,

$$x^0y^0B = B = \begin{bmatrix} 00 & 04 \\ 40 & 44 \end{bmatrix}.$$

The B-coset with representative x^1y^0 is

$$x^1y^0B = xB = \begin{bmatrix} 10 & 14 \\ 50 & 54 \end{bmatrix}.$$

A few more examples are the B-cosets

$$yB = \begin{bmatrix} 01 & 05 \\ 41 & 45 \end{bmatrix}, \quad xyB = \begin{bmatrix} 11 & 15 \\ 51 & 55 \end{bmatrix}$$

$$x^2B = \begin{bmatrix} 20 & 24 \\ 60 & 64 \end{bmatrix}, \quad x^2yB = \begin{bmatrix} 21 & 25 \\ 61 & 65 \end{bmatrix}$$

which have B-coset representatives x^0y^1, x^1y^1, x^2y^0, and x^2y^1, respectively.

```
\input{DSP/UHEE616-trans}
```

III. Translation Invariance

A. Generalized Translation and Convolution

For $y \in G$, the mapping $\mathsf{T}(y)$ of $\mathcal{L}(G)$ defined by

$$(\mathsf{T}(y)f)(x) = f(y^{-1}x), \quad x \in G, \tag{7}$$

is a linear operator of $\mathcal{L}(G)$ called *left translation by* y.

The mapping $\mathsf{C}(f)$ of $\mathcal{L}(G)$ defined by

$$\mathsf{C}(f) = \sum_{y \in G} f(y)\mathsf{T}(y), \quad f \in \mathcal{L}(G), \tag{8}$$

is a linear operator of $\mathcal{L}(G)$ called *left convolution by* f. By definition, for $x \in G$,

$$(\mathsf{C}(f)g)(x) = \sum_{y \in G} f(y)g(y^{-1}x), \quad g \in \mathcal{L}(G). \tag{9}$$

For $f, g \in \mathcal{L}(G)$, the composition $f * g = \mathsf{C}(f)g$ is called the *convolution product*. The vector space $\mathcal{L}(G)$ paired with the convolution product is an algebra, the *convolution algebra over* G.

To gain some familiarity with the general definitions of translation and convolution, it helps to verify that these definitions agree with what we expect when G is a familiar abelian group.

Example 6 If $G = \mathbb{Z}/N$, then (7) becomes

$$(\mathsf{T}(y)f)(x) = f(x - y), \qquad x \in G, \tag{10}$$

and (9) becomes

$$(\mathsf{C}(g)f)(x) = \sum_{y \in G} g(y)f(x - y). \tag{11}$$

Example 7 If $G = \mathbb{Z}/M \times \mathbb{Z}/N$, then translation of $\mathcal{L}(G)$ by $y \in G$ is given by

$$(\mathsf{T}(y)f)(x) = f(x_1 - y_1, x_2 - y_2), \qquad x \in G.$$

while convolution of $\mathcal{L}(G)$ by $g \in \mathcal{L}(G)$ is given by

$$\mathsf{C}(g)f = \sum_{y \in G} g(y)\mathsf{T}(y)f, \qquad f \in \mathcal{L}(G).$$

Evaluated at a point $x = (x_1, x_2) \in G$,

$$(\mathsf{C}(g)f)(x) = \sum_{y_1=0}^{M-1} \sum_{y_2=0}^{N-1} g(y_1, y_2)f(x_1 - y_1, x_2 - y_2).$$

```
\input{DSP/UHEE616-ga}
```

B. The Group Algebra $\mathbb{C}G$

The *group algebra* $\mathbb{C}G$ is the space of all formal sums

$$f = \sum_{x \in G} f(x)x, \quad f(x) \in \mathbb{C}, \tag{12}$$

with the following operations for $f, g \in \mathbb{C}G$:

$$f + g = \sum_{x \in G} (f(x) + g(x))x, \tag{13}$$

$$\alpha f = \sum_{x \in G} (\alpha f(x))x, \quad \alpha \in \mathbb{C}, \tag{14}$$

$$fg = \sum_{x \in G} \left(\sum_{y \in G} f(y)g(y^{-1}x) \right) x. \tag{15}$$

The mapping $\mathsf{L}(g)$ of $\mathbb{C}G$ defined by $\mathsf{L}(g)f = gf$ is a linear operator on the space $\mathbb{C}G$ called *left multiplication by* g. Since $y \in G$ can be identified with the formal sum $e_y \in \mathbb{C}G$ consisting of a single nonzero term,

$$yf = \mathsf{L}(e_y)f = \sum_{x \in G} f(y^{-1}x)x. \tag{16}$$

In relation to translation of $\mathcal{L}(G)$, (16) is the $\mathbb{C}G$ analog. Fig. 1 illustrates.

The mapping $\Theta : \mathcal{L}(G) \to \mathbb{C}G$ defined by

$$\Theta(f) = \sum_{x \in G} f(x)x, \quad f \in \mathcal{L}(G), \tag{17}$$

is an algebra isomorphism of the convolution algebra $\mathcal{L}(G)$ onto the group algebra $\mathbb{C}G$. Thus we can identify $\Theta(f)$ with f, using context to decide whether f refers to the function in $\mathcal{L}(G)$ or the formal sum in $\mathbb{C}G$.

An important aspect of the foregoing isomorphism is the correspondence between the translations of the spaces. Translation of $\mathcal{L}(G)$ by $y \in G$ corresponds to left multiplication of $\mathbb{C}G$ by $y \in G$. Convolution of $\mathcal{L}(G)$ by $f \in \mathcal{L}(G)$ corresponds to left multiplication of $\mathbb{C}G$ by $f \in \mathbb{C}G$.

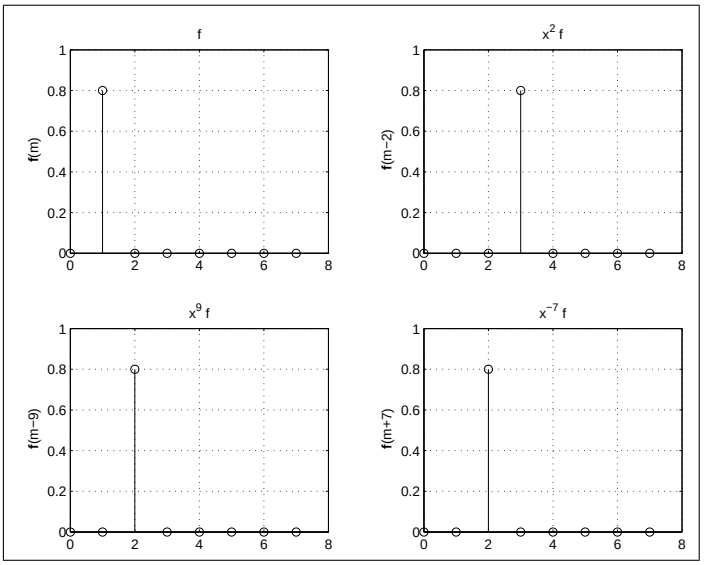

Fig. 1. An impulse $f \in \mathbb{C}A$ and a few abelian group translates, $x^2 f, x^9 f, x^{-7} f$.

C. Ideals: Translation-Invariant Subspaces

A subspace $\mathcal{V}$ of the space $\mathbb{C}G$ is called a *left ideal* if

$$u\mathcal{V} = \{uf : f \in \mathcal{V}\} \subset \mathcal{V}, \quad u \in G. \tag{18}$$

A left ideal of $\mathbb{C}G$ corresponds to a subspace of $\mathcal{L}(G)$ invariant under all left translations.

If $\mathcal{V}$ is a left ideal, then, by linearity, $g\mathcal{V} \subset \mathcal{V}$ for all $g \in \mathbb{C}G$. The set $\mathbb{C}Gg$, defined by $\{fg : f \in \mathbb{C}G\}$, is a left ideal of $\mathbb{C}G$, called *the left ideal generated by* g in $\mathbb{C}G$. A left ideal $\mathcal{V}$ of $\mathbb{C}G$ is called *irreducible* if the only left ideals of $\mathbb{C}G$ contained in $\mathcal{V}$ are $\{0\}$ and $\mathcal{V}$. The sum of two distinct, irreducible left ideals is always a direct sum.

For *abelian* group A, the group algebra $\mathbb{C}A$ of signals is decomposed into a direct sum of irreducible ideals. Since multiplication of $\mathbb{C}A$ by elements of A corresponds to translation, ideals represent translation-invariant subspaces. Furthermore, in the abelian case, such translation-invariant subspaces are one-dimensional.

Similarly, for *nonabelian* group G, the group algebra $\mathbb{C}G$ is decomposed into a direct sum of left ideals. Here, again, the ideals are translation-invariant subspaces. However, some of these subspaces must now be multi-dimensional, and herein lies the potential advantage of using nonabelian groups for indexing the data. The left translations are more general and represent a broader class of transformations. Therefore, projections of data into the resulting left ideals can reveal more complicated partitions and structures in the data as compared with the Fourier components in the abelian group case.

```
\input{DSP/ideals}
```

D. Translation-Invariant Subspaces

A subspace $\mathcal{V}$ of the space $\mathbb{C}G$ is called a *left ideal* if

$$u\mathcal{V} = \{uf : f \in \mathcal{V}\} \subset \mathcal{V}, \quad u \in G. \tag{19}$$

A left ideal of $\mathbb{C}G$ corresponds to a subspace of $\mathcal{L}(G)$ invariant under all left translations. If $\mathcal{V}$ is a left ideal, then, by linearity, $g\mathcal{V} \subset \mathcal{V}$ for all $g \in \mathbb{C}G$. The set $\mathbb{C}Gg$, defined by $\{fg : f \in \mathbb{C}G\}$, is a left ideal of $\mathbb{C}G$, called *the left ideal generated by* g in $\mathbb{C}G$. A left ideal $\mathcal{V}$ of $\mathbb{C}G$ is called *irreducible* if the only left ideals of $\mathbb{C}G$ contained in $\mathcal{V}$ are $\{0\}$ and $\mathcal{V}$. The sum of two distinct, irreducible left ideals is always a direct sum.

For *abelian* group A, the group algebra $\mathbb{C}A$ of signals is decomposed into a direct sum of irreducible ideals. Since multiplication of $\mathbb{C}A$ by elements of G corresponds to translation, ideals represent translation-invariant subspaces. Furthermore, in the abelian case, such translation-invariant subspaces are one-dimensional.

Similarly, for *nonabelian* group G, the group algebra $\mathbb{C}G$ is decomposed into a direct sum of left ideals and, again, the ideals are translation-invariant subspaces. However, some of them must now be multi-dimensional, and herein lies the potential advantage of using nonabelian groups for indexing the data. The left translations are more general and represent a broader class of transformations. Therefore, projections of data into the resulting left ideals can reveal more complicated partitions and structures as compared with the Fourier components in the abelian group case.

IV. Nonabelian Group DSP

This section presents some basic theory of digital signal processing (DSP), but relies on a more general mathematical formalism than that employed by the standard textbooks on the subject.[1]

```
\input{DSP/UHEE616-nonabelianDSP}
```

V. Nonabelian Group DSP

This section presents some basic principles of DSP, but relies on a more general mathematical formalism than that commonly found in textbooks on the subject.[2]

A. The Group of Characters: Main Theorems

A *character* of G is a group homomorphism of G into $\mathbb{C}^\times$, where $\mathbb{C}^\times = \mathbb{C}\backslash\{0\}$. In other words, the mapping $\varrho : G \to \mathbb{C}^\times$ is a character of G if it satisfies $\varrho(xy) = \varrho(x)\varrho(y),\ x, y \in G$. Let G^* denote the set of all characters of G.

By the identification (17) between $\mathcal{L}(G)$ and $\mathbb{C}G$, a character $\varrho \in G^*$ can be viewed as a formal sum,

$$\varrho = \sum_{x \in G} \varrho(x)x. \tag{20}$$

Therefore, $G^* \subset \mathbb{C}G$. Expressing the characters as formal sums leads to simple proofs of important DSP results.

Theorem 1 If ϱ is a character of G, then

$$y\varrho = \varrho y = \varrho(y^{-1})\varrho, \quad y \in G. \tag{21}$$

Proof: By a change of variables,

$$\varrho y = \sum_{x \in G} \varrho(x)xy = \sum_{x \in G} \varrho(xy^{-1})x, \quad y \in G.$$

[1] A few notable exceptions are [1], [2], Chirikjian:2002.

[2] A few notable exceptions are [1], [4], [2], [5].

By homomorphism property, $\varrho(xy^{-1}) = \varrho(x)\varrho(y^{-1})$. Therefore,

$$\varrho y = \sum_{x\in G} \varrho(x)\varrho(y^{-1})x = \varrho(y^{-1})\varrho, \quad y \in G.$$

A similar change of variables argument shows

$$y\varrho = \sum_{x\in G} \varrho(y^{-1}x)x = \varrho(y^{-1})\varrho, \quad y \in G.$$

■

Theorem 2 For $\varrho \in G^*$,

$$\frac{1}{|G|}\sum_{x\in G} \varrho(x) = \begin{cases} 1, & \varrho(x) = 1, \forall x \in G, \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

where $|G|$ is the order of G. *Proof:* By a change of variables,

$$\varrho(y)\sum_{x\in G} \varrho(x) = \sum_{x\in G} \varrho(yx) = \sum_{x\in G} \varrho(x), \quad y \in G. \tag{23}$$

Thus, either $\varrho(x) = 1, \forall x \in G$, or $\sum \varrho(x) = 0$. ■

Theorem 1 shows that every character is an eigenvector of left-multiplication by elements of the group G, so we call them $\mathsf{L}(G)$-eigenvectors. Therefore, by linearity, the characters are eigenvectors of left-multiplication by $f \in \mathbb{C}G$ (convolution by $f \in \mathcal{L}(G)$). This is re-stated more formally as the following formula for the *G-spectral components* of f:

Corollary 1 If $\varrho \in G^*$ and $f \in \mathbb{C}G$, then

$$f\varrho = \varrho f = \hat{f}(\varrho)\varrho, \tag{24}$$

where $\hat{f}(\varrho) = \sum_{y\in G} f(y)\varrho(y^{-1})$.

Proof: By Theorem 1,

$$f\varrho = \sum_{y\in G} f(y)y\varrho = \sum_{y\in G} f(y)\varrho(y^{-1})\varrho \tag{25}$$

Similarly for ϱf, mutatis mutandis. ■

The functions which make up the standard Fourier basis are eigenvectors of standard convolution. As seen in the foregoing proofs, this is merely a consequence of the fact that the exponential functions are characters. *The notion of a character basis generalizes the Fourier basis to include bases which can diagonalize any linear combination of left group multiplications.*

Corollary 2 If $\lambda, \tau \in G^*$, then

$$\lambda\tau = \begin{cases} |G|\lambda, & \tau = \lambda, \\ 0, & \tau \neq \lambda. \end{cases} \tag{26}$$

Proof: Suppose $\tau = \lambda$; then,

$$\lambda\tau = \sum_{x\in G} \lambda(x)\lambda(x^{-1})\lambda = \sum_{x\in G} \lambda(1)\lambda = |G|\lambda$$

Suppose $\tau \neq \lambda$. By definition,

$$\hat{\lambda}(\tau) = \sum_{x\in G} \lambda(x)\tau(x^{-1}) = \sum_{y\in G} \lambda(y^{-1})\tau(y) = \hat{\tau}(\lambda) \tag{27}$$

By (24), $\hat{\lambda}(\tau)\tau = \lambda\tau = \tau\lambda = \hat{\tau}(\lambda)\lambda$. Since $\hat{\lambda}(\tau) = \hat{\tau}(\lambda)$ and $\tau \neq \lambda$, it must be the case that $\hat{\tau} = 0$ and $\lambda\tau = 0$. ■

Corollary 2 can be expressed in the language of *idempotent theory*. A nonzero element $e \in \mathbb{C}G$ is called an *idempotent* if $e^2 = e$. Two idempotents e_1 and e_2 are called orthogonal if $e_1e_2 = e_2e_1 = 0$. Corollary 2 says that

$$\left\{ \frac{1}{|G|}\rho : \rho \in G^* \right\}$$

is a set of pairwise orthogonal idempotents.

```
\input{DSP/SDP}
```

B. Semidirect Product Groups

To determine whether a particular group is useful for a DSP application, we must specify exactly how this group represents the data. The group representation may reduce computational complexity, or it may simply make it easier to state, understand, or model a given signal processing task.

This section describes a simple class of nonabelian groups that have proven useful in applications – *abelian by abelian semidirect products*.

Let G be a finite group of order N, K a subgroup of G, and H a normal subgroup of G. If $G = HK$ and $H \cap K = \{1\}$, then we say that G is the *semidirect product* $G = H \leftthreetimes K$. It can be shown that $G = H \leftthreetimes K$ if and only if every $x \in G$ has a unique representation of the form $x = yz,\ y \in H, z \in K$.

Denote by $Aut(H)$ the set of all *automorphisms* of H. The mapping $\Psi : K \to Aut(H)$ defined by

$$\Psi_z(x) = zxz^{-1}, \quad z \in K, x \in H \tag{28}$$

is a group homomorphism. Define the binary composition in G in terms of Ψ as follows:

$$x_1x_2 = (y_1z_1)(y_2z_2) = y_1\Psi_{z_1}(y_2)z_1z_2, \tag{29}$$
$$y_1, y_2 \in H,\ z_1, z_2 \in K.$$

If K is a normal subgroup of G, then $y^{-1}Ky = K$ for all $y \in G$, and G is simply the cartesian product $H \times K$ with component-wise multiplication. What is new in the semidirect product is the possibility that K acts nontrivially on H. For this reason, K is sometimes called the "action group."

1) Simplest Nonabelian Example: If the mapping Ψ given in (28) is defined over $K = U(N)$, then Ψ is a group isomorphism. Under this identification, we can form the semidirect product $G = H \leftthreetimes K$, with $H = C_N(x)$ and K a subgroup of $U(N)$. Throughout this section, G will denote such a semidirect product group.

The elements $u \in K$ are integers. However, following [1] we denote by k_u the element $u \in K$, as this avoids confusion that can arise on occasion. This notation is especially useful when K is a cyclic group with generator u. If we denote elements of K by k_u^j, instead of by u^j, it is easier to distinguish them from elements of the abelian group $C_N(x)$.

Suppose the action group K is a cyclic group of order $J = |K|$ with generator u. We identify each element of K with an index, and denote the set of elements by $K = \{k_u^j : 0 \leq j < J\}$. Thus, to each $k_v \in K$, there corresponds a $j \in \mathbb{Z}$ such

that $k_u^j = k_v$. We use $x^n k_v$ and $x^n k_u^j$ to denote typical points of $G = C_N(x) \leftthreetimes K$.

Given two points in G, say $z = x^m k_u$ and $y = x^n k_v$, define multiplication according to (29) as follows:

$$zy = (x^m k_u)(x^n k_v) = x^{m+un} k_u k_v, \tag{30}$$

where $m + un$ is taken modulo N. Since $k_v = k_u^j$ for some $j \in \mathbb{Z}$, then $k_u k_v = k_u^{1+j}$, and $zy = x^{m+un} k_u^{j+1}$.

Let $z = x^m k_v$ and suppose k_w is the inverse of k_v in K. Then the inverse of z must be $z^{-1} = x^{N-wm} k_w$, since this satisfies $z^{-1} z \equiv 1$.

Suppose $K \subset U(N)$ has order $|K| = J$, and consider the semidirect product group with elements

$$G = \{x^n k_u^j : 0 \le n < N, 0 \le j < J\}. \tag{31}$$

For $f \in \mathbb{C}G$,

$$f = \sum_{y \in G} f(y) y = \sum_{n,j} f(x^n k_u^j) x^n k_u^j, \tag{32}$$

As above, translations of $\mathbb{C}G$ are defined as left multiplication by elements of G. For semidirect product (31) there is a simple dichotomy of translation types that arise from left-multiplication by elements of G. First, the familiar "abelian translates" are obtained upon left-multiplication by powers of x (Fig. 1). By change of variables,

$$x^m f = \sum_{n,j} f(x^{n-m} k_u^j) x^n k_u^j, \tag{33}$$

which is simply a right shift of f by m units. Similarly, left-multiplication by powers of x^{-1} effects left shift of f. (Recall, $x^{-1} \equiv x^{N-1}$ and $x^{-m} \equiv x^{N-m}$.)

Of the second type are the "nonabelian translates," obtained upon left-multiplication by $k_v \in K$.

$$k_v f = \sum_{n,j} f(k_v^{-1} x^n k_u^j) x^n k_u^j. \tag{34}$$

Suppose $k_w = k_u^\ell$ is the inverse of k_v in K. Then,

$$k_v f = \sum_{n,j} f(x^{wn} k_u^{\ell+j}) x^n k_u^j \tag{35}$$

From equation (35) it is clear that $k_v f$ results in a more complex transformation than that of $x^m f$ as given by (33).

For the general element $z = x^m k_v \in G$ with inverse $z^{-1} = x^{N-wm} k_w$ we derive rules for generalized translations.

$$zf = \sum_{y \in G} f(z^{-1} y) y = \sum_{n,j} f(x^{N-w(m-n)} k_w k_u^j) x^n k_u^j$$

$$z^{-1} f = \sum_{y \in G} f(zy) y = \sum_{n,j} f(x^{m+vn} k_v k_u^j) x^n k_u^j$$

VI. Examples

As seen above, when varying group structures are placed on indexing sets, and products in the resulting group algebra are computed, interesting signal transforms obtain. In this section, we elucidate the nature of these operations by examining some simple concrete examples in detail.

\input{DSP/Examples}

A. Examples: 1-D Semidirect Product Indexing Sets

As seen above, when varying group structures are placed on indexing sets, and products in the resulting group algebra are computed, interesting signal transforms obtain. In this section, we elucidate the nature of these operations by examining some simple, concrete examples in detail.

Recall, in the notation defined above, the mapping $\Psi : U(N) \to Aut(C_N(x))$ is a group isomorphism. Under this identification, we can form $C_N(x) \leftthreetimes K$ for any subgroup K of $U(N)$. A typical point in $C_N(x) \leftthreetimes K$ is denoted (x^n, u), $0 \le n < N$, $u \in K$ with multiplication given by

$$(x^m, u)(x^n, v) = (x^{m+un}, uv), \quad 0 \le m, n < N,\ u, v \in K$$

where $m + un$ is taken modulo N. We often use k_u to denote the element $u \in K$ as this avoids confusion that can arise at various places.

Example 8 [3] Let G_1 be the abelian group

$$G_1 = C_{2N}(x) = \{x^n : 0 \le n < 2N\}. \tag{36}$$

Let G_2 be the *dihedral group* with elements

$$\begin{aligned} G_2 &= C_N(x) \leftthreetimes \{1, k_{N-1}\} \\ &= \{x^n k_{N-1}^j : 0 \le n < N, 0 \le j < 2\}. \end{aligned}$$

We order the elements of G_2 as follows:

$$\{1, x, \ldots, x^{N-1}, k_{N-1}, x k_{N-1}, \ldots, x^{N-1} k_{N-1}\}$$

Thus, G_2 is divided into two blocks with N-samples per block.

Example 9 Another group, G_3, will be constructed as follows: for some integer $M \ge 2$, define $N = 2^M$, so that $\left(\frac{N}{2} + 1\right)^2 \equiv 1 \mod N$, and $N/2 + 1$ generates a subgroup of $U(N)$ of order 2. Let

$$\begin{aligned} G_3 &= C_N(x) \leftthreetimes \{1, k_{\frac{N}{2}+1}\} \\ &= \{x^n k_{\frac{N}{2}+1}^j : 0 \le n < N, 0 \le j < 2\}. \end{aligned}$$

Note that G_2 and G_3 are isomorphic groups.

Example 8 (cont.) By describing the translations of functions in $\mathbb{C}G_2$, we will see that the nonabelian translates of $\mathbb{C}G_2$ are "intra-block time-reversal" operations. A similar analysis of G_3 shows that the nonabelian translates of $\mathbb{C}G_3$ perform an "intra-block interleave" operation.

Multiplication on G_2 obeys the following relations:

$$x^N = k_{N-1}^2 = 1, \tag{37}$$

$$x^m k_{N-1}^{j+1}\ x^n k_{N-1}^j = \begin{cases} x^{m-n}, & j = 0, \\ x^{m+n}, & j = 1. \end{cases} \tag{38}$$

If $z = x^m k_{N-1}$, then $z^2 = 1$, thus $z^{-1} = z$.

For $f \in \mathbb{C}G_2$,

$$f = \sum_n f(x^n) x^n + f(x^n k_{N-1}) x^n k_{N-1}. \tag{39}$$

[3] An and Tolimieri (2003), page 125.

By (37), the nonabelian translate $k_{N-1}f$ is given by

$$\sum_n f(k_{N-1}x^n)x^n + f(k_{N-1}x^n k_{N-1})x^n k_{N-1}$$

which is equivalent to

$$\sum_n f(x^{N-n}k_{N-1})x^n + f(x^{N-n})x^n k_{N-1}. \qquad (40)$$

Comparing (39) and (40), we see that the nonabelian translate of $f \in \mathbb{C}G_2$ swaps the first N samples of f with the remaining N samples, and performs a time-reversal within each sub-block.

To express this another way, define $h = k_{N-1}f$. The first N coefficients of h are defined in terms of f as

$$h(x^n) = f(x^{N-n}k_{N-1}), \quad 0 \le n < N,$$

while the remaining N coefficients are given by

$$h(x^n k_{N-1}) = f(x^{N-n}), \quad 0 \le n < N.$$

For a simple linear function, this special translation is illustrated in Fig. 3.

A similar analysis of $G_3 = C_N(x) \leftthreetimes \{1, k_{\frac{N}{2}+1}\}$ reveals that the nonabelian translates of $\mathbb{C}G_3$ interleave the elements within each N-sample sub-block of G_3, in addition to swapping the two blocks. This is illustrated in Fig. 4.

B. A Few Generalized Convolutions Computed

Fig. 2 illustrates a cyclic convolution of two discrete signals, with 16 samples each, indexed with the abelian group C_{16}. The first graph in Fig. 2 is a graph of the signal f, which is simply an impulse at the 9th sample; i.e., $f(x^8) = 1$ and $f(x^m) = 0$, $m \neq 8$. The second signal, g, appears in the middle graph of Fig. 2. A linearly increasing sequence of 16 numbers ranging from -1 to 1, g can be represented as a vector of values

$$\mathbf{g} = (-1, -0.8\bar{6}, -0.7\bar{3}, \ldots, 0.7\bar{3}, 0.8\bar{6}, 1) \qquad (41)$$

or as an element of the group algebra $\mathbb{C}C_{16}$,

$$g = \sum_{m=0}^{15} g(x^m)x^m,$$

where the coefficients $g(x^m)$ take the values given in (41). The third graph in Fig. 2 shows the result of the convolution $C(f)g = fg$. Evidently, when signals are indexed by elements of the abelian group C_{16}, then the product fg is the familiar cyclic convolution of f and g. (Recall, convolution by an impulse effects a translation.)

Fig. 3 shows the convolution $C(f)g = fg$, where f is an impulse at the 9th sample, with group index k_7, and g is a linearly increasing sequence of 16 numbers ranging from -1 to 1; g can be represented as a vector, or as an element of the group algebra $\mathbb{C}(C_8 \leftthreetimes \{1, k_7\})$,

$$g = \sum_{m=0}^{7}\sum_{j=0}^{1} g(x^m k_7^j)x^m k_7^j$$

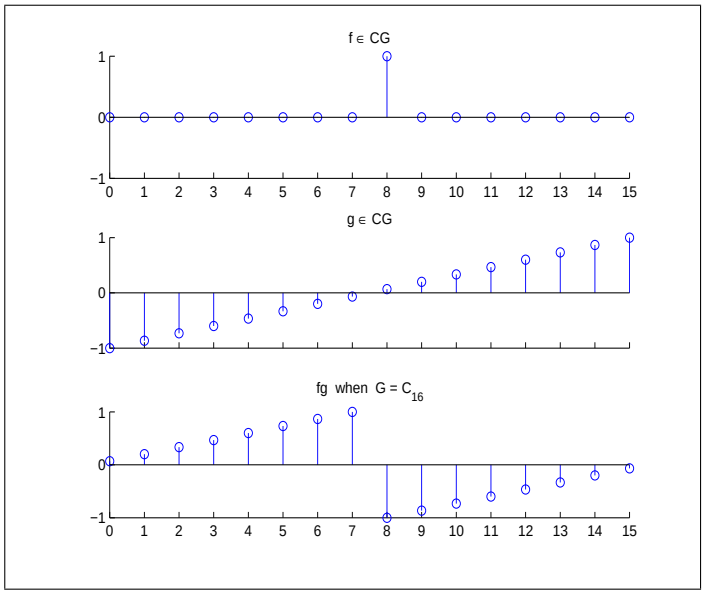

Fig. 2. Convolution of two signals indexed by the abelian group C_{16}.

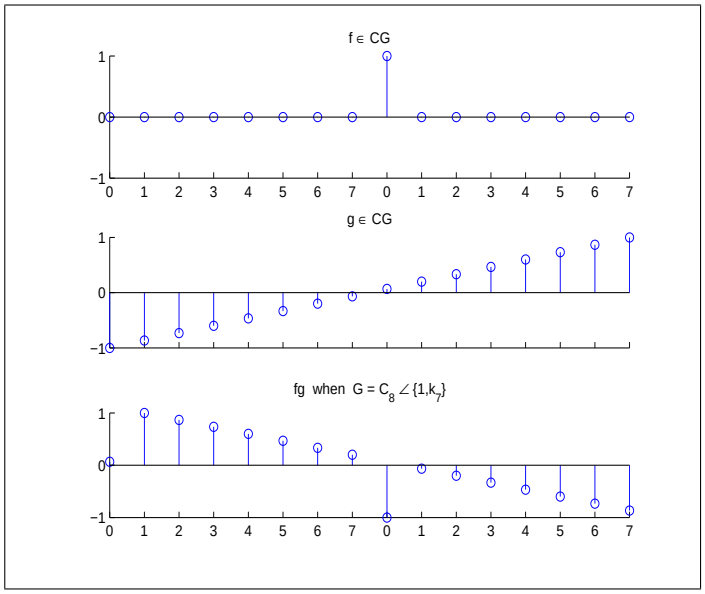

Fig. 3. The element $k_{N-1} \in G$ (top), where $N = 8$ and $G = C_8 \leftthreetimes \{1, k_7\}$ – as an element of the group algebra, $f = k_7 \in \mathbb{C}G$ is the "impulse function" with one nonzero coefficient $f(k_7) = 1$; A linear signal $g \in \mathbb{C}G$ (middle); the product $fg = k_7 g$ (bottom) is, in general, the convolution of g by f, and is implemented by appealing to the convolution theorem and using a generalized FFT algorithm.

with coefficients $g(x^m k_7^j)$ taking the values given in (41); i.e.,

$$g(1) = -1,\ g(x) = -0.8\bar{6}, \ldots, g(x^7) = -0.0\bar{6},$$

$$g(k_7) = 0.0\bar{6},\ g(xk_7) = 0.2, \ldots, g(x^7 k_7) = 1.$$

C. Examples: 2-D Semidirect Product Indexing Sets

Example 10 Recall that $\mathsf{GL}(2, \mathbb{Z}/N)$ denotes the set of all 2×2 invertible matrices with coefficients in $\mathbb{Z}/N$. For $c \in \mathsf{GL}(2, \mathbb{Z}/N)$ such that c^M is the identity, consider the *action*

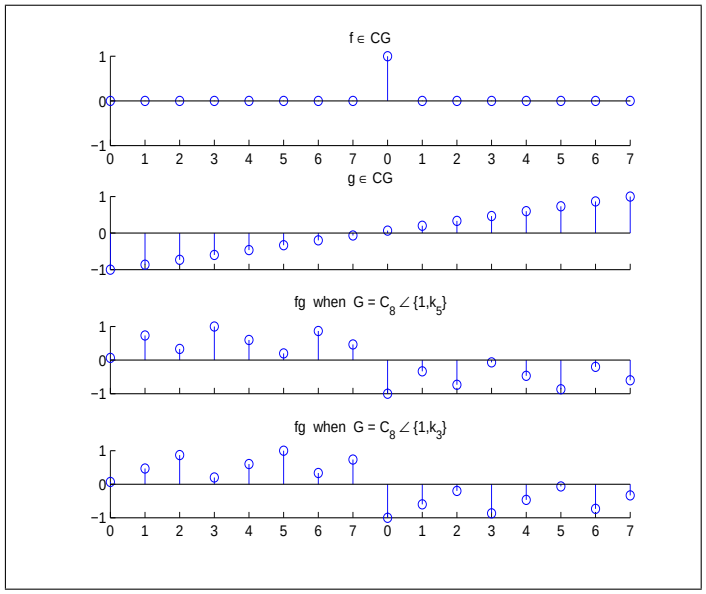

Fig. 4. Convolution of two signals indexed by the nonabelian groups $C_8 \leftthreetimes \{1, k_5\}$ (third graph) and $C_8 \leftthreetimes \{1, k_5\}$ (fourth graph).

group K_c defined by

$$C_M(k_c) = \{k_c^m : 0 \le m < M\}, \quad c = \begin{pmatrix} c_0 & c_1 \\ c_2 & c_3 \end{pmatrix}$$

The semidirect product of H and K_c has elements

$$H \leftthreetimes K_c = \{x^j y^k k_c^m : 0 \le j, k < L, 0 \le m < M\}$$

and binary composition satisfying the following relations:

$$x^L = y^L = k_c^M = 1,$$
$$x^{-1} = x^{L-1}, \quad y^{-1} = y^{L-1}, \quad k_c^{-1} = k_c^{M-1},$$
$$k_c x^j y^k = x^{c_0 j + c_1 k} y^{c_2 j + c_3 k} k_c.$$

where the summands in the exponents are modulo $|H| = L$.

D. Example: 2-D Rotations.

DEBUG this subsection.

Let $A = C_N(x) \times C_N(y)$ with binary composition satisfying

$$(x^m y^j)(x^n y^k) = x^{m+n \bmod N} y^{j+k \bmod N},$$
$$x^N = y^N = 1, \quad x^{-1} = x^{N-1}, \quad y^{-1} = y^{N-1}.$$

Consider the action group K_c, $c \in \mathsf{GL}(2, \mathbb{Z}/N)$, with $c^M = 1$. The group generated by k_c is the cyclic group of order M with elements $C_M(k_c) = \{k_c^m : 0 \le m < M\}$. Now suppose

$$c(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Example 11 (Rotation by $\pi/2$) The action group $K_{c(\pi/2)}$ has

$$c(\pi/2) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Since $c^4(\pi/2)$ is the identity, the group has order $M = 4$.

The semidirect product $A \leftthreetimes K_{c(\theta)}$ has elements $\{x^j y^k k_{c(\theta)}^m : 0 \le j, k < N, 0 \le m < M\}$, and binary composition satisfying

$$x^N = y^N = k_{c(\theta)}^M = 1,$$

$$x^{-1} = x^{N-1}, \quad y^{-1} = y^{N-1}, \quad k_{c(\theta)}^{-1} = k_{c(\theta)}^{M-1},$$

and

$$k_{c(\theta)} x^j y^k = x^{j\cos\theta - k\sin\theta} y^{j\sin\theta + k\cos\theta} k_{c(\theta)},$$

Additive operations in the exponents are modulo $|A| = N$.

We now demonstrate the effect of successive left multiplications by the k_c described above. Suppose an image f has the following array representation:

$$\left(\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 10 & 12 & 2 & 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 0 & 3 & 3 & 3 \\ 0 & 9 & 0 & 3 & 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 0 & 3 & 3 & 3 \\ 0 & 8 & 6 & 4 & 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 0 & 3 & 3 & 3 \end{array}\right)$$

Notice that, in the left-most 4×4 block of this array, there is a 3×3 subarray with entries approximating the locations on the face of an analog clock. Such a configuration facilitate our observation of the local behavior of the non-abelian group translation – that is, the action of k_c on the elements within the given 4×4 block. The subarrays of the three other 4×4 blocks are designed to reveal the global effect of the non-abelian translation. That is, they demonstrate how the blocks shift around (though the elements within each of these blocks undergo the same transformation as those of the first block.)

The following are the array representations of $k_c f$, $k_c^2 f$, and $k_c^3 f$, resp.

$$\left(\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 3 & 3 & 0 & 2 & 3 & 4 & 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 \\ 0 & 3 & 3 & 3 & 0 & 12 & 0 & 6 & 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 \\ 0 & 3 & 3 & 3 & 0 & 10 & 9 & 8 & 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 \end{array}\right)$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 0 & 3 & 3 & 3 & 0 & 4 & 6 & 8 & 0 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 0 & 3 & 3 & 3 & 0 & 3 & 0 & 9 & 0 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 0 & 3 & 3 & 3 & 0 & 2 & 12 & 10 & 0 & 1 & 1 & 1 \end{array}\right)$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 0 & 3 & 3 & 3 & 0 & 8 & 9 & 10 \\ 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 0 & 3 & 3 & 3 & 0 & 6 & 0 & 12 \\ 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 0 & 3 & 3 & 3 & 0 & 4 & 3 & 2 \end{array}\right)$$

E. Digital lines

DEBUG this subsection.

This section defines digital lines and the Matlab routines used to process them. Such examples are useful for demonstrating the nature of the generalized translations and convolutions that are possible when the groups used to index the data are nonabelian.

`\input{DSP/UHEE616-summary}`

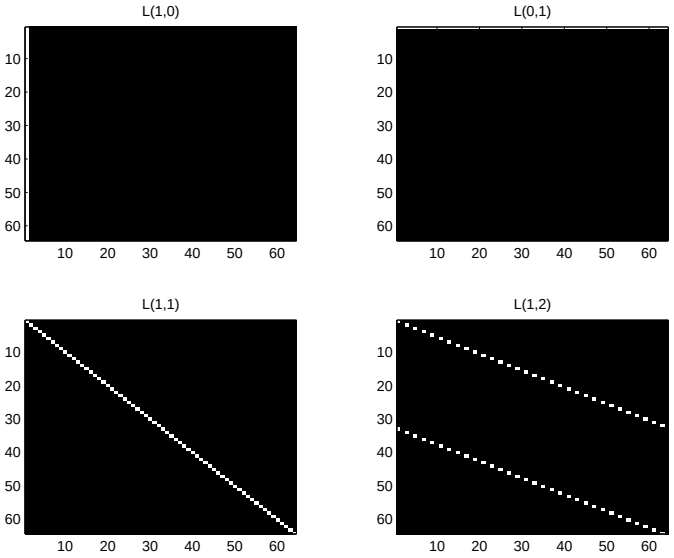

Fig. 5. *Figures 10.4.1–10.4.3 of An (2003), re-produced with* `fline.m` *program.*

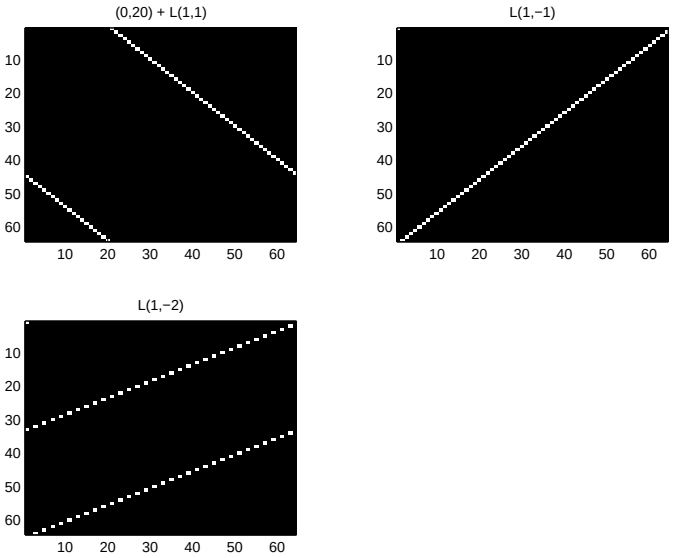

Fig. 6. *Figures 10.4.4–10.4.6 of An (2003) re-produced with* `fline.m` *program.*

VII. Summary and Conclusions

Basic DSP theory was reviewed with a focus on *translation invariance* – translation invariant operators of $\mathcal{L}(G)$, and translation invariant subspaces of $\mathcal{L}(G)$. When such great significance is attached to translation invariance, a deeper understanding of exponential functions, and their unrivaled status in classical DSP, is possible. In particular, exponentials are the *characters* of abelian group indexing sets, such as $\mathbb{Z}/N$, over which classical DSP is performed. Each character of an abelian group represents a one-dimensional translation invariant subspace, and the characters are eigenvectors of translations, therefore, of convolutions.

We described the group algebra $\mathbb{C}G$, the algebra isomorphism $\mathcal{L}(G) \simeq \mathbb{C}G$, and why it is useful for manipulations involving (generalized) translations and convolutions of the space of signals. We saw that, for an abelian group A, translations of $\mathcal{L}(A)$ represent simple linear shifts in space or time, while for a nonabelian group G, translations of $\mathcal{L}(G)$ are more general than simple spatial or temporal shifts. This leads to more interesting translation invariant subspaces.

Motivating many studies in the area of noncommutative harmonic analysis (including this one) is a simple but important fact about the generalized translations that result when a signal is indexed by a nonabelian group. As we have seen, such operations offer more complex and interesting signal transformations. Equally important, however, is the fact that each transformation can be written as a left-multiplication. Thus, the increase in signal transform complexity resulting from a nonabelian indexing scheme comes at no increase in computational complexity.

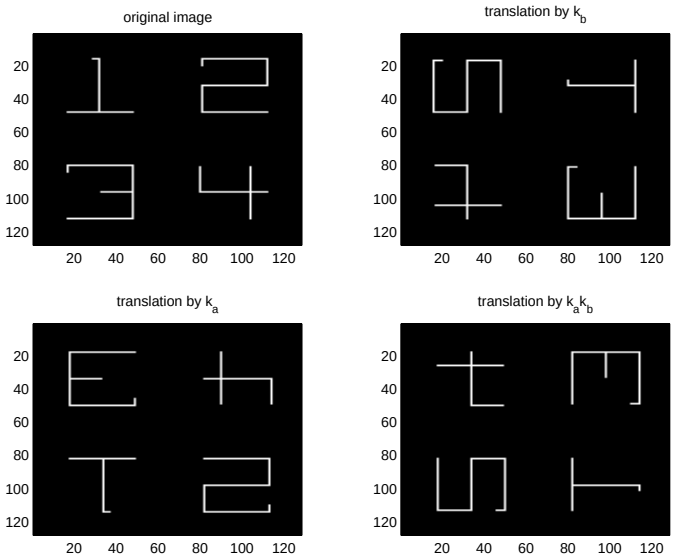

Fig. 7. Translates of an image in $(C_N(x) \times C_N(y)) \leftthreetimes (K_a \times K_b)$.

Acknowledgment

The author would like to thank Textron Systems and the U.S. Navy for supporting this research. This work also owes a great deal to Myoung An and Richard Tolimieri, whose prior contributions to this field are responsible for anything of value in the present work. The author thanks them for many helpful conversations and suggestions, but takes full responsibility for any errors that appear above.

References

[1] M. An and R. Tolimieri, *Group Filters and Image Processing*. Boston: Psypher Press, 2003. [Online]. Available: www.psypher.net

[2] R. Tolimieri and M. An, *Time-Frequency Representations*. Boston: Birkhäuser, 1998.

[3] J. Byrnes and G. Ostheimer, Eds., *Computational Noncommutative Algebra and Applications*. Kluwer Acad., 2004.

[4] R. Tolimieri and M. An, *Group Filters and Image Processing*. Kluwer Acad., 2004.

[5] G. S. Chirikjian and A. B. Kyatkin, *Engineering Applications of Noncommutative Harmonic Analysis: With Emphasis on Rotation and Motion Groups*. CRC Press, 2002.