Proceedings of the International Symposium on Musical Acoustics, March 31st to April 3rd 2004 (ISMA2004), Nara, Japan

Topics in Nonabelian Harmonic Analysis and DSP Applications

William J. DeMeo

Textron Systems; Hawaii, USA
williamdemeo@yahoo.com

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.

Advantages of indexing signals with nonabelian groups are not limited to image data, but extend to audio signals as well. The present work provides an overview of DSP on finite groups and group algebras. I present the basic nonabelian group theory relevant to DSP, and define a "generalized (nonabelian) translation," and its consequence, "generalized convolution." Thereafter I describe some specific examples of nonabelian-group indexing sets which are simple yet revealing, as well as useful for applications.

1. 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]. Underlying most digital signal processing (DSP) algorithms is the group $\mathbb{Z}/N$ of integers modulo N, which serves as the data indexing set. Translations are defined using addition modulo N, and basic operations, including convolutions and Fourier expansions, are developed relative to these translations.

DSP on *finite abelian groups* such as $\mathbb{Z}/N$ is well understood and has great practical utility. An excellent treatment that is applications oriented while remaining fairly abstract and general, is provided by Tolimieri and An in [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; cf. the NATO ASI "Computational Non-commutative Algebras," Italy, 2003. Another notable exception is the book [1], by An and Tolimieri (2003), 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. The work demonstrates that including nonabelian groups among the possible data indexing strategies significantly broadens the range of useful signal processing techniques.

This paper describes the use of nonabelian groups for indexing 1-dimensional signals, and discusses the computational advantages and insights to be gained from this approach. We examine a simple but instructive class of nonabelian groups – the *semidirect product* groups – and show that, when elements of such groups are used to index the data and standard DSP operations are defined with respect to special group binary operators, interesting and powerful signal transformations are possible.

2. Notation and Background

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 for DSP applications. The books [1] and [2] treat similar material in a more thorough and rigorous manner.

Throughout, $\mathbb{C}$ denotes complex numbers, G an arbitrary (nonabelian) group, and $\mathcal{L}(G)$ the collection of complex valued functions on G.

2.1. 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.

Throughout the following discussion, G is an arbitrary group, not necessarily abelian. For $x \in G$, 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. When G is understood, we simply write $gp(x)$.

It will be convenient to have notation for a cyclic group of order N without reference to a particular un-

derlying 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 (noncommutative) binary composition as multiplication. Since our work involves both abelian and nonabelian groups, it is notationally cleaner to write the binary operations of all groups – whether abelian or not – as multiplications. As the following discussion illustrates, groups such as $\mathbb{Z}/N$ with addition modulo N have a simple multiplicative representation.

Example 2.1 Let

$$\mathbb{Z}/N = \{0, 1, \ldots, N-1\} \tag{4}$$

and let addition modulo N be the binary composition on $\mathbb{Z}/N$. This group is isomorphic to the cyclic group $C_N(x)$; i.e.,

$$\begin{aligned} \mathbb{Z}/N &= \{n : 0 \le n < N\} \\ &\simeq \{x^n : 0 \le n < N\} = C_N(x). \end{aligned} \tag{5}$$

Indeed, it is by identification (5) that the binary composition on $\mathbb{Z}/N$ can be written as multiplication. More precisely, by uniquely identifying each element $m \in \mathbb{Z}/N$ with an element $x^m \in C_N(x)$, the binary composition $m + n$ is replaced with that of equation 3.

Example 2.2 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, say $LM = N$, then

$$gp_N(x^L) = \{x^m L : 0 \le m < M\} \tag{6}$$

is a cyclic group of order M.

2.2. 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 2.3 For $N = 8$,

$$U(8) = \{1, 3, 5, 7\}. \tag{7}$$

2.3. Translation and convolution

2.3.1. General definition of translation

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

$$(\mathsf{T}(y)f)(x) = f(y^{-1}x), \quad x \in G, \tag{8}$$

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

2.3.2. General definition of convolution

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

$$\mathsf{C}(f) = \sum_{y \in G} f(y)\mathsf{T}(y), \quad f \in \mathcal{L}(G), \tag{9}$$

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

$$(\mathsf{C}(f)g)(x) = \sum_{y \in G} f(y)g(y^{-1}x), \quad g \in \mathcal{L}(G). \tag{10}$$

For $f, g \in \mathcal{L}(G)$, the composition

$$f * g = \mathsf{C}(f)g \tag{11}$$

is called the *convolution product*. The vector space $\mathcal{L}(G)$ paired with the convolution product is an algebra, the *convolution algebra over* G.

2.3.3. Translation and convolution of abelian groups

In applications such as audio and image processing, data are often indexed by elements of abelian groups. Two canonical examples are $\mathbb{Z}/N$ of equation (5), and

$$\begin{aligned} \mathbb{Z}/M \times \mathbb{Z}/N &= \{(m, n) : 0 \le m < M,\ 0 \le n < N\} \\ &= \{x^m y^n : 0 \le m < M,\ 0 \le n < N\} \\ &\simeq C_M(x) \times C_N(y). \end{aligned} \tag{12}$$

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 the familiar abelian group $\mathbb{Z}/N$. Indeed, for this special case, (8) becomes

$$(\mathsf{T}(y)f)(x) = f(x - y), \qquad x \in G, \tag{13}$$

and (10) becomes

$$(\mathsf{C}(g)f)(x) = \sum_{y \in G} g(y)f(x - y). \tag{14}$$

2.4. The group algebra $\mathbb{C}G$

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

$$f = \sum_{x \in G} f(x)x, \quad f(x) \in \mathbb{C}, \tag{15}$$

with the following operations:

$$f + g = \sum_{x \in G} (f(x) + g(x))x, \quad f, g \in \mathbb{C}G, \tag{16}$$

$$\alpha f = \sum_{x \in G} (\alpha f(x))x, \quad \alpha \in \mathbb{C}, f \in \mathbb{C}G, \tag{17}$$

$$fg = \sum_{x \in G} \left(\sum_{y \in G} f(y) g(y^{-1}x) \right) x, \quad f, g \in \mathbb{C}G. \tag{18}$$

For $g \in \mathbb{C}G$, the mapping $\mathsf{L}(g)$ of $\mathbb{C}G$ defined by

$$\mathsf{L}(g)f = gf, \quad f \in \mathbb{C}G, \tag{19}$$

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,

$$yf = \mathsf{L}(e_y)f = \sum_{x \in G} f(y^{-1}x)x. \tag{20}$$

In relation to translation of $\mathcal{L}(G)$, (20) is the $\mathbb{C}G$ analog.

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

$$\Theta(f) = \sum_{x \in G} f(x)x, \quad f \in \mathcal{L}(G), \tag{21}$$

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 $f \in \mathbb{C}G$. We state these relations symbolically as follows:

$$\begin{array}{ccc} \mathcal{L}(G) & \simeq & \mathbb{C}G \\ \mathsf{T}(y) & \leftrightarrow & \mathsf{L}(y) \\ \mathsf{C}(f) & \leftrightarrow & \mathsf{L}(f) \end{array}$$

2.4.1. Translation-invariant subspaces

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

$$u\mathcal{V} = \{uf : f \in \mathcal{V}\} \subset \mathcal{V}, \quad u \in G. \tag{22}$$

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.

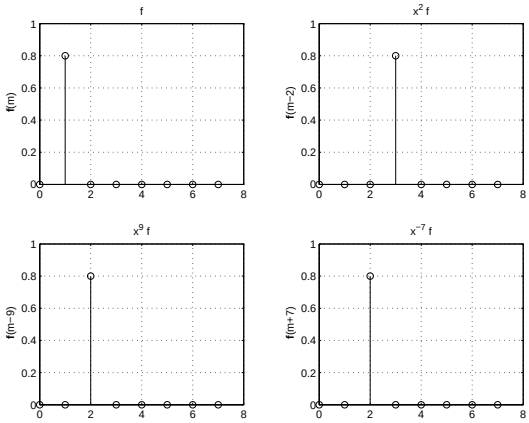

Figure 1: An impulse $f \in \mathbb{C}A$ and a few abelian group translates, $x^2 f, x^9 f, x^{-7} f$.

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.

3. 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].

3.1. Main theorems

A *character* of G is a group homomorphism of G into $\mathbb{C}^\times$, where $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. In other words, the mapping $\varrho : G \to \mathbb{C}^\times$ is a character of G if it satisfies $\varrho(xy) = \varrho(x)\varrho(y), x, y \in G$. There is always at least one character, the *trivial character*, which is 1 for all $y \in G$. Let G^* denote the set of all characters of G.

By the identification (21) between $\mathcal{L}(G)$ and $\mathbb{C}G$, a

[1] A few notable exceptions are [1, 3, 2, 4]

character $\varrho \in G^*$ can be viewed as a formal sum,

$$\varrho = \sum_{x \in G} \varrho(x) x. \tag{23}$$

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

Theorem 3.1 If ϱ is a character of G, then

$$y\varrho = \varrho y = \varrho(y^{-1})\varrho, \quad y \in G. \tag{24}$$

Proof: By a change of variables,

$$\varrho y = \sum_{x \in G} \varrho(x)xy = \sum_{x \in G} \varrho(xy^{-1})x, \quad y \in G. \tag{25}$$

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

$$\varrho y = \sum_{x \in G} \varrho(x)\varrho(y^{-1})x = \varrho(y^{-1})\varrho, \quad y \in G. \tag{26}$$

A similar change of variables argument shows

$$y\varrho = \sum_{x \in G} \varrho(y^{-1}x)x = \varrho(y^{-1})\varrho, \quad y \in G. \tag{27}$$

□

Theorem 3.2 For $\varrho \in G^*$,

$$\frac{1}{|G|} \sum_{x \in G} \varrho(x) = \begin{cases} 1, & \varrho(x) = 1, \forall x \in G, \\ 0, & \text{otherwise.} \end{cases} \tag{28}$$

where $|G|$ is the order of G.

Proof: By a change of variables,

$$\varrho(y) \sum_{x \in G} \varrho(x) = \sum_{x \in G} \varrho(yx) = \sum_{x \in G} \varrho(x), \quad y \in G. \tag{29}$$

Therefore, either (a) $\varrho(x) = 1, \forall x \in G$, or (b) $\sum \varrho(x) = 0$.

□

Theorem 3.1 shows that every character is an eigenvector of left-multiplication by elements of the group G, so we call them $L(G)$-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 restated more formally as the following formula for the G-*spectral components* of f:

Corollary 3.1 If $\varrho \in G^*$ and $f \in \mathbb{C}G$, then

$$f\varrho = \varrho f = \hat{f}(\varrho)\varrho, \tag{30}$$

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

Proof: By Theorem 3.1,

$$f\varrho = \sum_{y \in G} f(y) y\varrho = \sum_{y \in G} f(y)\varrho(y^{-1})\varrho \tag{31}$$

Similarly for ϱf, mutatis mutandis. □

The functions which make up the standard Fourier basis – the exponential functions – are eigenvectors of the standard convolution. However, as seen in the proof of 3.2, this is merely a consequence of the fact that the exponential functions satisfy properties which allow us to call them characters. The notion of a character basis generalizes the exponential basis to include bases which can diagonalize any linear combination of left group multiplications.

Corollary 3.2 If $\lambda, \tau \in G^*$, then

$$\lambda\tau = \begin{cases} |G|\lambda, & \tau = \lambda, \\ 0, & \tau \neq \lambda. \end{cases} \tag{32}$$

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,

$$\hat{\lambda}(\tau) = \sum_{x \in G} \lambda(x)\tau(x^{-1}) = \sum_{y \in G} \lambda(y^{-1})\tau(y) = \hat{\tau}(\lambda) \tag{33}$$

By (30), $\hat{\lambda}(\tau)\tau = \lambda\tau = \tau\lambda = \hat{\tau}(\lambda)\lambda$. 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 3.2 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 $e_1 e_2 = e_2 e_1 = 0$. Corollary 3.2 says that

$$\left\{ \frac{1}{|G|}\rho : \rho \in G^* \right\} \tag{34}$$

is a set of pairwise orthogonal idempotents.

4. 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 problem.

In this section we describe procedures for specifying and studying a simple class of nonabelian groups that have proven useful in applications – the *abelian by abelian semidirect products*. These are perhaps the simplest extension of abelian groups and DSP over such groups closely resembles that over abelian groups. However, the resulting processing tools can have vastly different characteristics.

4.1. Action group

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

$$\Psi_z(x) = zxz^{-1}, \quad z \in K, x \in H \tag{35}$$

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

$$x_1x_2 = (y_1z_1)(y_2z_2) = y_1\Psi_{z_1}(y_2)z_1z_2, \tag{36}$$

$$y_1, y_2 \in H,\ z_1, z_2 \in K.$$

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."

4.2. Simplest nonabelian example

As above, $C_N(x) = \{x^n : 0 \le n < N\}$ denotes the cyclic group of order N with generator x, and $U(N)$ denotes the group of units.

If the mapping Ψ given in (35) 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, we follow [1] and use k_u to denote the element $u \in K$ as this avoids confusion that can arise on occasion.[2]

Without loss of generality, assume 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

$$K = \{k_u^j : 0 \le j < J\}. \tag{37}$$

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 (36) as follows:

$$zy = (x^m k_u)(x^n k_v) = x^{m+un} k_u k_v, \tag{38}$$

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

$$z^{-1} = x^{N-wm} k_w. \tag{39}$$

This is easily verified as follows:

$$\begin{aligned} z^{-1}z &= x^{N-wm}k_w x^m k_v \\ &= x^{N-wm+wm}k_w k_v \equiv 1. \end{aligned} \tag{40}$$

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

$$\begin{aligned} G &= \{x^n k_u^j : 0 \le n < N, 0 \le j < J\} \\ &= \{1, x, \ldots, x^{N-1},\ k, xk, \ldots \\ &\qquad \ldots, x^{N-1}k,\ k_u^2, xk_u^2, \ldots \\ &\qquad\qquad \ldots, x^{N-1}k_u^{J-1}\}. \end{aligned} \tag{41}$$

4.3. Translations on semidirect product groups

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

$$f = \sum_{y \in G} f(y)y = \sum_{n,j} f(x^n k_u^j) x^n k_u^j, \tag{42}$$

where $0 \le n < N$ and $0 \le j < J$. As above, translations of $\mathbb{C}G$ are defined as left-multiplication by elements of G.

The semidirect product in (41) has a very basic form, and there is a simple dichotomy of translation types that arise from left-multiplication by elements of G. Translations of the first type are the familiar "abelian translates," obtained upon left-multiplication by powers of x, as illustrated in Figure 1.

By change of variables,

$$\begin{aligned} x^m f &= \sum_{n,j} f(x^n k_u^j) x^{n+m} k_u^j \\ &= \sum_{n,j} f(x^{n-m} k_u^j) x^n k_u^j \end{aligned} \tag{43}$$

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 of translation arising from left-multiplication by elements of G are the "nonabelian translates." For $k_v \in K$,

$$\begin{aligned} k_v f &= \sum_{n,j} f(x^n k_u^j) k_v x^n k_u^j \\ &= \sum_{n,j} f(k_v^{-1} x^n k_u^j) x^n k_u^j \end{aligned} \tag{44}$$

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

$$\begin{aligned} k_v f &= \sum_{n,j} f(k_w x^n k_u^j) x^n k_u^j \\ &= \sum_{n,j} f(x^{wn} k_u^{\ell+j}) x^n k_u^j \end{aligned} \tag{45}$$

[2] 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 $C_N(x)$.

From equation (45) it is clear that $k_v f$ results in a more complex transformation than $x^m f$.

For the general element $z = x^m k_v \in G$ with inverse $z^{-1} = x^{N-wm} k_w$ (equation (39)), we derive rules for generalized translations with respect to z and z^{-1}.

$$\begin{aligned} zf &= \sum_{y\in G} f(y)zy = \sum_{y\in G} f(z^{-1}y)y \\ &= \sum_{n,j} f(x^{N-wm}k_w\, x^n k_u^j)x^n k_u^j \\ &= \sum_{n,j} f(x^{N-w(m-n)}k_w k_u^j)x^n k_u^j \end{aligned} \quad (46)$$

$$\begin{aligned} z^{-1}f &= \sum_{y\in G} f(y)z^{-1}y = \sum_{y\in G} f(zy)y \\ &= \sum_{n,j} f(x^m k_v x^n k_u^j)x^n k_u^j \\ &= \sum_{n,j} f(x^{m+vn}k_v k_u^j)x^n k_u^j \end{aligned} \quad (47)$$

5. 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.

5.1. Semidirect product examples

Example 5.1 [3] Let G_1 be the abelian group

$$G_1 = C_{2N}(x) = \{x^n : 0 \le n < 2N\}. \quad (48)$$

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:

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

Thus, G_2 is divided into two blocks of N-samples.

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.

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

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.

Note that multiplication on G_2 obeys the following relations:

$$x^N = k_{N-1}^2 = 1, \quad (49)$$

$$x^m k_{N-1}^{j+1}\, x^n k_{N-1}^j = \begin{cases} x^{m-n}, & j = 0, \\ x^{m+n}, & j = 1, \end{cases} \quad (50)$$

and, for any $z = x^m k_{N-1}$,

$$x^m k_{N-1} x^m k_{N-1} = x^{m+(N-1)m} = x^{Nm} = 1. \quad (51)$$

If $f \in \mathbb{C}G_2$, then

$$f = \sum_n f(x^n)x^n + f(x^n k_{N-1})x^n k_{N-1}, \quad (52)$$

where $0 \le n < N$. Since (49) implies $k_{N-1} = k_{N-1}^{-1}$, 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

$$\sum_n f(x^{N-n}k_{N-1})x^n + f(x^{N-n})x^n k_{N-1}. \quad (53)$$

Comparing (52) and (53), 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 $g = k_{N-1}f$. The first N coefficients of g are defined in terms of f as

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

while the remaining N coefficients are given by

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

For a simple linear function, this special translation is illustrated in Figure 2.

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 themselves.

6. Summary and Conclusions

Overall, basic DSP 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

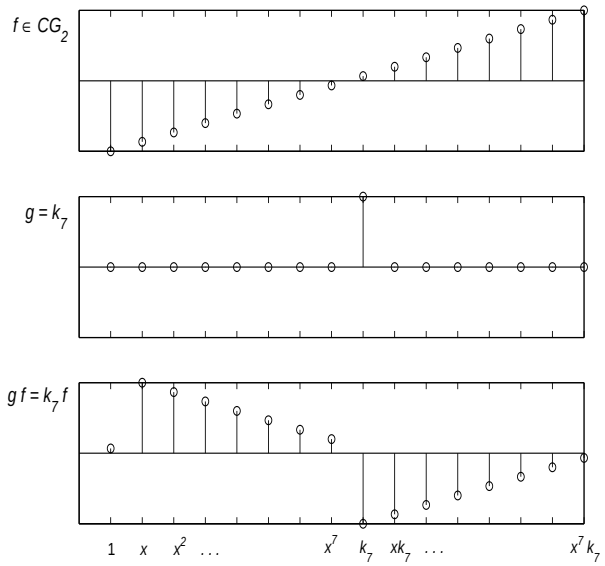

Figure 2: A linear signal $f \in \mathbb{C}G_2$, where $N = 8$ (left); the element $k_{N-1} \in G_2$ (middle) – as an element of the group algebra, k_{N-1} is the "impulse function" $g \in \mathbb{C}G_2$ with one nonzero coefficient, $g(k_{N-1}) = 1$; the product $gf = k_{N-1}f$ (right) is, in general, the convolution product and is implemented by appealing to the convolution theorem and using a generalized FFT algorithm.

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.

References

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

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

[3] G. Chirikjian and A. Kyatkin, *Engineering Applications of Noncommutative Harmonic Analysis*. CRC Press, 2001.

[4] R. Tolimieri, M. An, and C. Lu, *Mathematics of Multidimensional Fourier Transform Algorithms*. New York: Springer-Verlag, 1997.