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. 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, "generalized translations," and their consequences, "generalized convolutions." Thereafter, some specific, simple examples of nonabelian-group indexing sets are discussed along with their practical implications.

## 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].

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 noncommutative group multiply operation, and performing typical DSP operations relative to these translations.

This paper describes the use of nonabelian groups for indexing 1-dimensional signals, and discusses computational advantages and insights thus gained. 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.

## 2. Notation and Background

This section summarizes the notations, definitions, and important facts needed below. The presentation style is terse since the goal is to distill from the literature only those results that are most relevant for DSP applications. The books [1] and [2] treat the same 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, $x$ is a *generator* of $C$.

Let the set

$$C_N(x) = \{x^n : 0 \leq n < N\} \tag{1}$$

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

$$x^m x^n = x^{m+n}, \quad 0 \leq m, n < N, \tag{2}$$

where $m + n$ is addition modulo $N$. In $C_N(x)$, the identity element is $x^0 = 1$, and the inverse of $x^n$ 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 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 $\mathbb{Z}/N = \{0, 1, \ldots, N-1\}$, and let addition modulo $N$ be the binary composition on $\mathbb{Z}/N$. This group is isomorphic to the cyclic group $C_N(x)$; indeed, it is by this identification that the binary composition on $\mathbb{Z}/N$ can be written as multiplication. More precisely, uniquely identifying each $m \in \mathbb{Z}/N$ with $x^m \in C_N(x)$, the binary composition $m + n$ is replaced with that of (2).

### 2.2. Group of Units

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

### 2.3. Generalized Translation and Convolution

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

$$(\mathsf{T}(y)f)(x) = f(y^{-1}x), \quad x \in G, \tag{3}$$

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

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

$$\mathsf{C}(f) = \sum_{y \in G} f(y)\mathsf{T}(y), \quad f \in \mathcal{L}(G), \tag{4}$$

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

$$(\mathsf{C}(f)g)(x) = \sum_{y \in G} f(y)g(y^{-1}x), \quad g \in \mathcal{L}(G). \tag{5}$$

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* $G$.

**Example 2.3** 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, (3) becomes

$$(\mathsf{T}(y)f)(x) = f(x - y), \qquad x \in G, \tag{6}$$

and (5) becomes

$$(\mathsf{C}(g)f)(x) = \sum_{y \in G} g(y)f(x - y). \tag{7}$$

### 2.4. The Group Algebra $\mathbb{C}G$

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

$$f = \sum_{x \in G} f(x)x, \quad f(x) \in \mathbb{C}, \tag{8}$$

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

$$f + g = \sum_{x \in G} (f(x) + g(x))x, \tag{9}$$

$$\alpha f = \sum_{x \in G} (\alpha f(x))x, \quad \alpha \in \mathbb{C}, \tag{10}$$

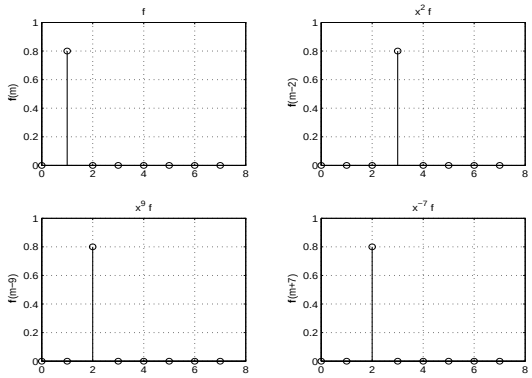


*Figure 1: An impulse $f \in \mathbb{C}A$ and a few abelian group translates, $x^2 f, x^9 f, x^{-7} f$.*

$$fg = \sum_{x \in G} \left( \sum_{y \in G} f(y)g(y^{-1}x) \right) x. \tag{11}$$

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,

$$yf = \mathsf{L}(e_y)f = \sum_{x \in G} f(y^{-1}x)x. \tag{12}$$

In relation to translation of $\mathcal{L}(G)$, (12) is the $\mathbb{C}G$ analog.

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

$$\Theta(f) = \sum_{x \in G} f(x)x, \quad f \in \mathcal{L}(G), \tag{13}$$

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 $f \in \mathbb{C}G$.

### 2.5. Translation-Invariant Subspaces

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

$$u\mathcal{V} = \{uf : f \in \mathcal{V}\} \subset \mathcal{V}, \quad u \in G. \tag{14}$$

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.

## 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 $\varrho(xy) = \varrho(x)\varrho(y)$, $x, y \in G$. Let $G^*$ denote the set of all characters of $G$.

By the identification (13) between $\mathcal{L}(G)$ and $\mathbb{C}G$, a character $\varrho \in G^*$ can be viewed as a formal sum,

$$\varrho = \sum_{x \in G} \varrho(x) x. \tag{15}$$

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

**Theorem 3.1** If $\varrho$ is a character of $G$, then

$$y\varrho = \varrho y = \varrho(y^{-1})\varrho, \quad y \in G. \tag{16}$$

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

$$\frac{1}{|G|} \sum_{x \in G} \varrho(x) = \begin{cases} 1, & \varrho(x) = 1, \forall x \in G, \\ 0, & \text{otherwise.} \end{cases} \tag{17}$$

where $|G|$ is the order of $G$. 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 re-stated 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

$$f\varrho = \varrho f = \hat{f}(\varrho)\varrho, \tag{18}$$

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

**Proof:** By Theorem 3.1,

$$f\varrho = \sum_{y \in G} f(y) y\varrho = \sum_{y \in G} f(y)\varrho(y^{-1})\varrho \tag{19}$$

Similarly for $\varrho f$, mutatis mutandis. □

The functions which make up the standard Fourier basis are eigenvectors of standard convolution. As seen in the proof of 3.2, this is merely a consequence of the fact that exponential functions satisfy properties which allow us to call them 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 3.2** If $\lambda, \tau \in G^*$, then

$$\lambda\tau = \begin{cases} |G|\lambda, & \tau = \lambda, \\ 0, & \tau \neq \lambda. \end{cases} \tag{20}$$

## 4. Semidirect Product Groups

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

$$\Psi_z(x) = zxz^{-1}, \quad z \in K, x \in H \tag{21}$$

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

$$x_1 x_2 = (y_1 z_1)(y_2 z_2) = y_1 \Psi_{z_1}(y_2) z_1 z_2, \tag{22}$$

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

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

### 4.1. Simplest Nonabelian Example

If the mapping $\Psi$ given in (21) is defined over $K = U(N)$, then $\Psi$ 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 $K = \{k_u^j : 0 \le j < J\}$. 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 (22) as follows:

$$zy = (x^m k_u)(x^n k_v) = x^{m+un} k_u k_v, \tag{23}$$

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

$$G = \{x^n k_u^j : 0 \le n < N, 0 \le j < J\}. \tag{24}$$

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

$$f = \sum_{y \in G} f(y) y = \sum_{n,j} f(x^n k_u^j) x^n k_u^j, \tag{25}$$

As above, translations of $\mathbb{C}G$ are defined as left-multiplication by elements of $G$. For semidirect product (24) 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 $x$ (Figure 1). By change of variables,

$$x^m f = \sum_{n,j} f(x^{n-m} k_u^j) x^n k_u^j, \tag{26}$$

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 $k_v \in K$.

$$k_v f = \sum_{n,j} f(k_v^{-1} x^n k_u^j) x^n k_u^j. \tag{27}$$

[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 $C_N(x)$.

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

$$k_v f = \sum_{n,j} f(x^{wn} k_u^{\ell+j}) x^n k_u^j \tag{28}$$

From equation (28) 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 $z^{-1} = x^{N-wm} k_w$ we derive rules for generalized translations.

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

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

## 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 Example[3]

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 of $N$-samples.

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.

Multiplication on $G_2$ obeys the following relations:

$$x^N = k_{N-1}^2 = 1, \tag{29}$$

$$x^m k_{N-1}^{j+1}\, x^n k_{N-1}^j = \begin{cases} x^{m-n}, & j = 0, \\ x^{m+n}, & j = 1. \end{cases} \tag{30}$$

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

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

$$f = \sum_n f(x^n) x^n + f(x^n k_{N-1}) x^n k_{N-1}. \tag{31}$$

By (29), the nonabelian translate $k_{N-1} f$ is given by

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

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

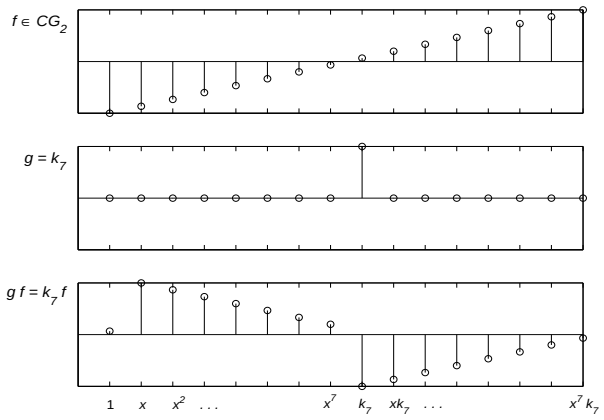


*Figure 2: A linear signal $f \in \mathbb{C}G_2$, where $N = 8$ (left); the element $k_{N-1} \in G_2$ (middle) – as an element of the group algebra, $k_{N-1}$ is the "impulse function" $g \in \mathbb{C}G_2$ with one nonzero coefficient, $g(k_{N-1}) = 1$; the product $gf = k_{N-1}f$ (right) is, in general,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

which is equivalent to

$$\sum_n f(x^{N-n}k_{N-1})x^n + f(x^{N-n})x^n k_{N-1}. \qquad (32)$$

Comparing (31) and (32), 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. For a simple linear function, this special translation is illustrated in Figure 2.

## 6. Summary and Conclusions

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. 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.