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. "Generalized translation," and its consequence, "generalized convolution" are defined. Thereafter, some specific, simple, yet revealing, 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]. 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 [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 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, 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.

```
\input{DSP/hafg-prelim}
```

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 (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

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

is a cyclic subgroup of G called the *group generated by*

x in G. When G is understood, we will write $gp_G(x)$ as $gp(x)$.

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

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

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

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

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 a 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 nonabelian – 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 $C_N(x)$,

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

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 an element $x^m \in C_N(x)$, the binary composition $m + n$ is replaced with that of equation 2.

Example 2.2 Consider the direct product group

$$\mathbb{Z}/M \times \mathbb{Z}/N = \{(m, n) : 0 \le m < M,\ 0 \le n < N\}, \tag{3}$$

each element of which represents a 2-dimensional spatial coordinate. More generally, identify (3) by isomorphism with the group

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

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 2.3 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

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

and $gp_N(x^L)$ 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 2.4 For $N = 8$, $U(8) = \{1, 3, 5, 7\}$.

2.3. 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

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

Implicit in our discussions of this set will be some standard identifications, such as $x^1 y^0 = (x, 1) = x$, and $x^0 y^1 = (1, y) = y$. This representation is not ambiguous, 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 2.5 For $N = 8$, $M = 2$, $L = 4$,

$$A = C_8(x) \times C_8(y) = \{x^m y^n : 0 \le m, n < 8\}, \quad (4)$$

and

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

In the following figure, the numbers denote exponents mn on the elements $x^m y^n \in A$ in (4).

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

The boldface exponents comprise the B-coset with representative x^0y^0; 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 sets

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

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

which are the B-cosets with representatives x^0y^1, x^1y^1, x^2y^0, and x^2y^1, respectively.

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

2.4. Translation and convolution

2.4.1. General definition of translation

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

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

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

2.4.2. General definition of convolution

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

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

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

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

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.

2.4.3. Translation and convolution of abelian groups.

In many applications, such as audio and image processing, data are often indexed by elements of abelian groups such as

$$\mathbb{Z}/N = \{n : 0 \le n < N\}$$

or

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

Consider the translation and convolution operations for the special case $A = \mathbb{Z}/M \times \mathbb{Z}/N$. Translation of $\mathcal{L}(A)$ by $y \in A$ is defined by

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

Convolution of $\mathcal{L}(A)$ by $g \in \mathcal{L}(A)$ is defined by

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

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

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

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

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

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

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

with the following operations:

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

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

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

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

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

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, then

$$yf = \mathsf{L}(e_y)f = \sum_{x\in G} f(y^{-1}x)x. \tag{5}$$

In relation to translation of $\mathcal{L}(G)$, (5) is the $\mathbb{C}G$ analog.

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

$$\Theta(f) = \sum_{x\in G} f(x)x, \quad f \in \mathcal{L}(G) \tag{6}$$

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:

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

2.4.5. Translation-invariant subspaces

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

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

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.

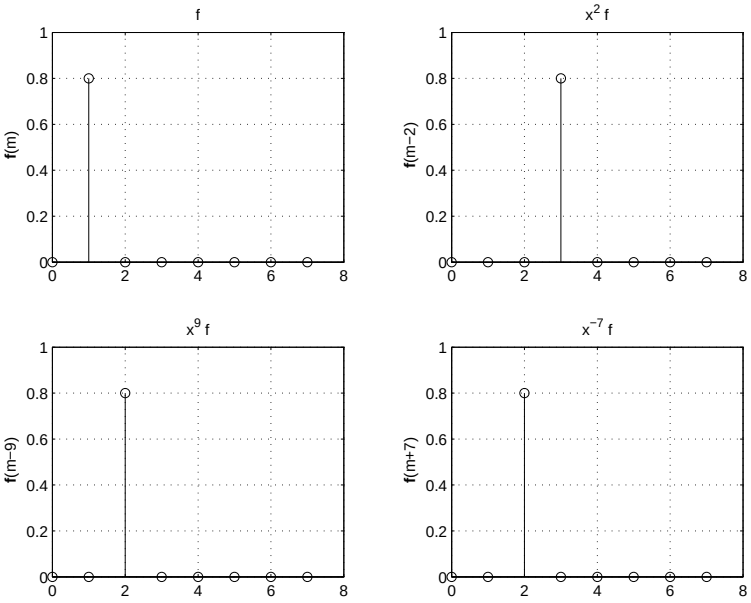

Figure 1: An impulse $f \in \mathbb{C}A$ and a few abelian group translates, $x^2 f, x^9 f, x^{-7} f$.

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]

```
\input{DSP/hafg-nonabelian}
```

3.1. 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.[2] At various places it might aid intuition to compare with the abelian group analogs and

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

[2] The exception is the book by An and Tolimieri citeAn:2003, which was solely responsible for introducing the authors to the viewpoint described in this section.

examples provided in Section **??**.

3.1.1. Characters

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

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

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

Theorem 3.1 If ϱ is a character of G, then

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

Proof: By a change of variables,

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

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

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

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

Proof: By a change of variables,

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

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 the characters $L(G)$-eigenvectors. By linearity, the characters are also 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

$$f\varrho = \varrho f = \hat{f}(\varrho)\varrho, \tag{7}$$

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

Proof: By Theorem 3.1,

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

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 qualify them as 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

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

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,

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

By (7), $\hat{\lambda}(\tau)\tau = \lambda\tau = \tau\lambda = \hat{\tau}(\lambda)\lambda$. 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 $e_1e_2 = e_2e_1 = 0$. Corollary 3.2 says that

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

is a set of pairwise orthogonal idempotents.

3.1.2. Semidirect products

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.

3.1.3. 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 $x = yz,\ y \in H, z \in K$.

The mapping $\Psi : K \to Aut(H)$, defined by

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

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

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

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

If $G = H \leftthreetimes K$ and K is a normal subgroup of G, then $y^{-1}Ky = K$ for all $y \in G$, by definition. In that case, G is the usual direct product $H \times K$ (i.e., the cartesian product with component-wise multiplication). What is new in the semidirect product is the possibility that K acts nontrivially on H; thus, we sometimes refer to K an the *action group*.

4. 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/hafg-examples}`

4.1. Examples

We place varying group structures on indexing sets and compute products corresponding to the group algebra.

4.1.1. Semidirect products

Recall the notation of (1) and (**??**) 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 4.1 Let G_1 be the abelian group

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

Let G_2 be the *dihedral group* with elements.

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

Construct the group G_3 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 4.2 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 group* K_c defined by

$$C_M(k_c) = \{k_c^m : 0 \le m < M\}, \quad c = \begin{pmatrix} c_0 & c_1 \\ c_2 & c_3 \end{pmatrix} \in \mathsf{GL}(2, \mathbb{Z}/N).$$

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:

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

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

4.1.2. 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 4.3 (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 $M = 4$.

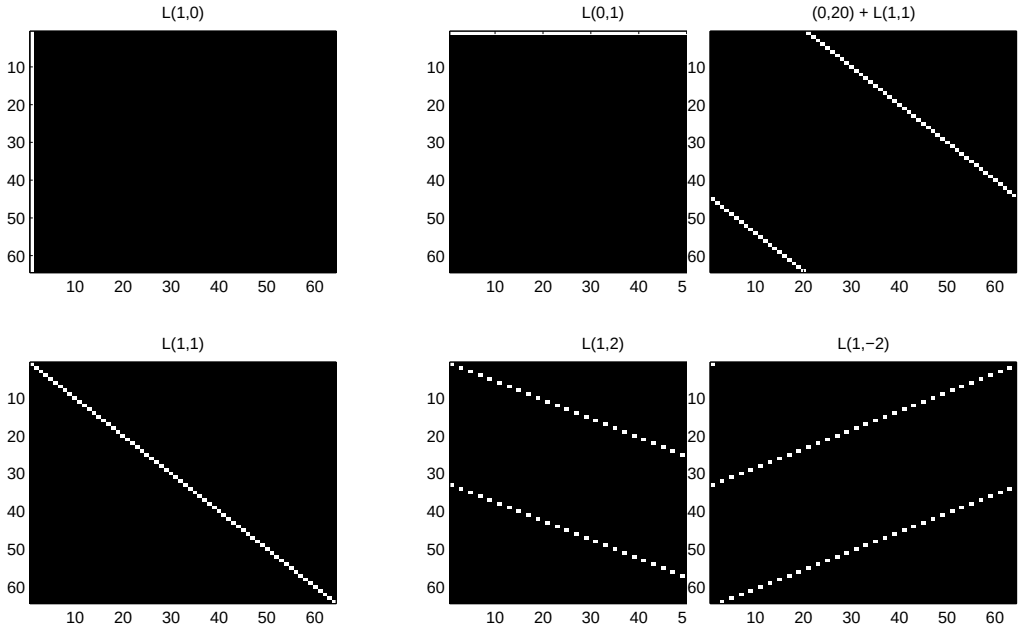

Figure 2: Figures 10.4.1–10.4.3 of An (2003), reproduced with `fline.m` *program.*

Figure 3: Figures 10.4.4–10.4.6 of An (2003) reproduced with `fline.m` *program.*

The semidirect product $A \leftthreetimes K_{c(\theta)}$ has elements $\{x^j y^k k_{c(\theta)}^m : 0 \leq j, k < N, 0 \leq m < M\}$, 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 $|A| = N$.

4.1.3. 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.

5. 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 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. [Online]. Available: www.psypher.net

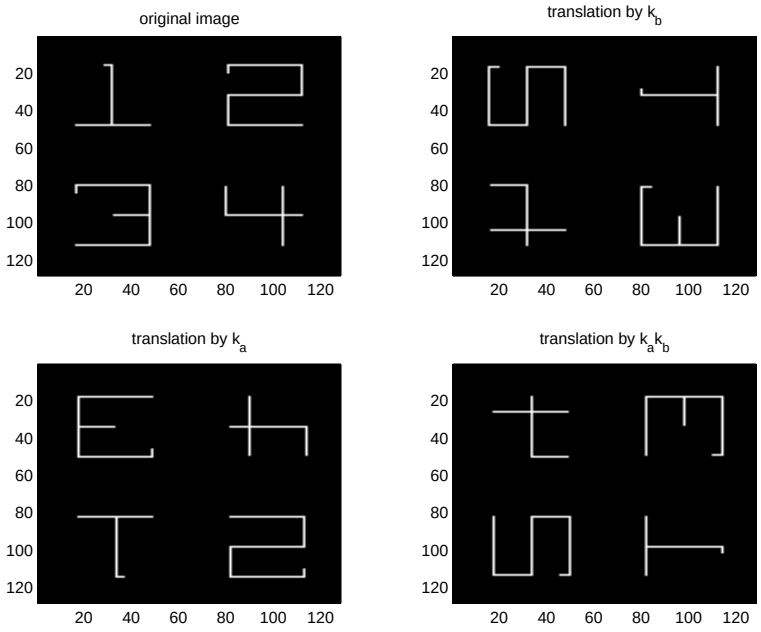

Figure 4: Translates of an image in G_1.

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