

**WEEK 3: REVIEW OF LINEAR ALGEBRA. PART III.  
THE DISCRETE FOURIER TRANSFORM.**

1. FINITE-DIMENSIONAL LINEAR ALGEBRA IN INNER PRODUCT SPACES

We continue with the review of Linear Algebra in finite dimensions from last week discussion and we now talk about properties of Inner Product Vector Spaces, their bases and Spectral Theory on them.

Recall the definition of an inner product  $\langle \cdot, \cdot \rangle$ , the definition of ‘the inner product’ on  $\mathbb{C}^n$  (i.e., the ‘dot product’  $x \cdot y$ ), the definition of the norm induced by an inner product ( $\|\cdot\| = \sqrt{\langle \cdot, \cdot \rangle}$ ), and the Cauchy-Schwarz inequality ( $|\langle x, y \rangle| \leq \|x\| \|y\|$ ). For the remainder of this section, when we discuss an inner product space, we mean a complex inner product space, although most of the results remain true in real inner product spaces.

**Definition 1.1.** Let  $H$  be an inner product space and let  $u, v \in H$ . We say  $u$  and  $v$  are *orthogonal*, and write  $u \perp v$ , if  $\langle u, v \rangle = 0$ .

**Proposition 1.2.** (PYTHAGOREAN THEOREM) *Let  $H$  be an inner product space and suppose that  $u, v \in H$  are orthogonal. Then  $\|u + v\| = \|u\| + \|v\|$ .*

This result also holds for finite linear combinations.

**Definition 1.3.** Let  $H$  be an inner product space. A set  $S \subset H$  is said to be *orthogonal* if any two elements of  $S$  are orthogonal, and  $S$  is *orthonormal* if  $S$  is orthogonal and satisfies  $\|x\| = 1$  for all  $x \in S$ .

**Proposition 1.4.** *Suppose  $S$  is an orthogonal set in an inner product space  $H$ . Then  $S$  is linearly independent.*

**Proposition 1.5.** *Let  $H$  be an inner product space, and  $B = \{u_1, \dots, u_n\}$  be an orthogonal subset of nonzero elements of  $H$ . Then for any  $v$  in the span of  $B$ , we have*

$$v = \sum_{j=1}^n \frac{\langle v, u_j \rangle}{\|u_j\|^2} u_j.$$

Note that if  $B$  is orthonormal, we can leave out the term in the denominator.

**Definition 1.6.** Let  $H$  be an inner product space, and  $B = \{u_1, \dots, u_n\}$  be an orthogonal subset of nonzero elements of  $H$ . Let  $S = \text{span } B$ . For  $v \in H$ , define the *orthogonal projection*  $P_S(v)$  of  $v$  onto  $S$  by

$$P_S(v) = \sum_{j=1}^n \frac{\langle v, u_j \rangle}{\|u_j\|^2} u_j.$$

Technically, since the definition of  $P_S$  depends on the basis  $B$ , we should check that  $P_S$  is well-defined. That is, we should check that if  $B_1$  and  $B_2$  are two orthogonal bases for  $S$ , then  $P_S$  as defined above is the same whether we use  $B_1$  or  $B_2$ . We will not worry about this here, but it is not difficult to show that  $P_S$  is, indeed, well-defined.

It is worth noting that we can actually define the notion of projection on vector spaces which merely have a norm by minimizing a distance function, but it requires more analysis and in any case will not be necessary here.

**Proposition 1.7.** *Let  $H, B, S$  and  $P_S$  be as in Definition 1.6. Then the following hold:*

- (a)  $P_S$  is a linear map.
- (b) The range of  $P_S$  is  $S$ .
- (c) If  $v \in S$ , then  $P_S(v) = v$ .
- (d) For any  $v \in H$  and  $x \in S$ ,

$$(v - P_S(v)) \perp x.$$

(e) For  $v \in H$ ,

$$P_S(v) = \operatorname{argmin}_{x \in S} \|v - x\|.$$

**Definition 1.8.** Let  $H$  be an inner product space. A basis for  $H$  which is also orthonormal is called an *orthonormal basis*.

We know now that any orthogonal set which spans the entire vector space is a basis. Now, the above results show that an orthogonal, or better yet orthonormal, set, is in some ways a particularly nice sort of basis, since it is easy to convert to that basis from another, and easy to compute projections onto certain subspaces. The Gram-Schmidt procedure gives a method for converting any basis for a space into an orthonormal basis.

**Proposition 1.9.** (GRAM-SCHMIDT PROCEDURE) *Let  $H$  be an inner product space, and  $\{v_1, \dots, v_n\}$  be any linearly independent set in  $H$ . Then there is an orthonormal set  $\{u_1, \dots, u_n\}$  with the same span.*

**Proposition 1.10.** *Let  $H$  be an inner product space with an orthonormal basis  $B = \{u_1, \dots, u_n\}$ . Then for  $v, w \in H$  we have*

(a) *Decomposition in  $B$ :*

$$v = \sum_{j=1}^n \langle v, u_j \rangle u_j.$$

(b) *Parseval's relation:*

$$\langle v, w \rangle = \sum_{j=1}^n \langle v, u_j \rangle \overline{\langle w, u_j \rangle}.$$

(c) *Plancherel's formula:*

$$\|v\|^2 = \sum_{j=1}^n |\langle v, u_j \rangle|^2.$$

**Definition 1.11.** Let  $A = (a_{ij})$  be a matrix over  $\mathbb{C}$  (or  $\mathbb{R}$ ). The *transpose* of  $A$  is the matrix  $A^t = (a_{ji})$  gotten by interchanging the rows and columns of  $A$ , while the *conjugate transpose* of  $A$  is  $A^* = [\bar{a}_{ji}]$ .

**Proposition 1.12.** *Let  $A$  be an  $m \times n$  matrix over  $\mathbb{C}$ . Then  $A^*$  is the unique matrix such that, for any  $z \in \mathbb{C}^n$  and  $w \in \mathbb{C}^m$ ,*

$$\langle Az, w \rangle = \langle z, A^*w \rangle.$$

**Definition 1.13.** An  $n \times n$  matrix  $A$  is *unitary* if  $A$  is invertible and  $A^{-1} = A^*$ .

**Proposition 1.14.** *Suppose  $A$  is an  $n \times n$  matrix over  $\mathbb{C}$ . The following are equivalent:*

- (a)  *$A$  is unitary.*
- (b) *The columns of  $A$  are an orthonormal basis for  $\mathbb{C}^n$ .*
- (c) *The rows of  $A$  are an orthonormal basis for  $\mathbb{C}^n$ .*
- (d)  *$A$  preserves inner products on  $\mathbb{C}^n$ , i.e. for any  $z, w \in \mathbb{C}^n$ ,*

$$\langle Az, Aw \rangle = \langle z, w \rangle.$$

(e)  *$A$  preserves norms, i.e., for any  $z \in \mathbb{C}^n$ ,*

$$\|Az\| = \|z\|.$$

**Proposition 1.15.** *Let  $E = \{e_1, \dots, e_n\}$  be the standard basis for  $\mathbb{C}^n$ , and  $O = \{u_1, \dots, u_n\}$  be any orthonormal basis. Let  $U$  be the matrix whose  $j$ th column is  $u_j$ . Then  $U$  is unitary,  $U$  is the  $O$  to  $E$  change-of-basis matrix, and  $U^*$  is the  $E$  to  $O$  change of basis matrix.*

**Corollary 1.16.** *If  $T : \mathbb{C}^n \rightarrow \mathbb{C}^n$  is linear and  $A$  represents  $T$  with respect to the standard basis, then  $U^*AU$  represents  $T$  with respect to the basis  $O$ .*

**Definition 1.17.** Let  $A$  and  $B$  be  $n \times n$  matrices over  $\mathbb{C}$ .  $A$  and  $B$  are said to be *unitarily similar* if there is a unitary matrix  $U$  such that  $A = U^*BU$ . A matrix which is unitarily similar to a diagonal matrix is *unitarily diagonal*.

**Definition 1.18.** An  $n \times n$  matrix  $A$  is normal if  $A^*A = AA^*$ .

**Theorem 1.19.** (SPECTRAL THEOREM FOR MATRICES) *Let  $A$  be a square complex matrix. The following are equivalent:*

- (a)  $A$  is unitarily diagonalizable.
- (b)  $A$  is normal.
- (c) The eigenvectors of  $A$  form an orthonormal basis of  $\mathbb{C}^n$ .

**Definition 1.20.** A square matrix  $A$  is *Hermitian* if  $A^* = A$ .

**Proposition 1.21.** *Let  $A$  be a square complex matrix. The following are equivalent:*

- (a)  $A$  is Hermitian.
- (b)  $A$  is normal with real eigenvalues.
- (c) There is a unitary matrix  $U$  and a diagonal matrix  $D$ ,  $D$  having only real values, such that  $A = U^*DU$ .

## 2. INTRODUCTION TO THE DISCRETE FOURIER TRANSFORM

Before we begin this section, we need to introduce some notation. First, we define the group  $\mathbb{Z}_N$  to be the group of integers  $\{0, \dots, N-1\}$  under addition modulo  $N$ . Hence, if  $m, n \in \mathbb{Z}_N$ , we define the addition  $m +_N n := m +_N n$  to be the unique integer of the set  $\{n + m + rN : r \in \mathbb{Z}\}$  such that  $m +_N n \in \{0, \dots, N-1\}$ . From now on, we will simply write  $m +_N n = m + n$  when it is understood that the addition is in  $\mathbb{Z}_N$ . This addition has a kind of ‘wrap-around’ effect at the ends of  $\mathbb{Z}_N$ . For example,  $(N-1) + 1 = 0$ , and  $0 - n = N - n$  for  $0 \leq n \leq N$ . Also, we will allow our vectors to take indexes in all of  $\mathbb{Z}$  range by letting  $z(n) = z(n')$ , where  $n' \equiv n \pmod{N}$ . Thus, for example, if  $n \in \mathbb{Z}_N$ , then  $z(-n) = z(N-n)$ , and  $z(n+N) = z(n)$ .

Next, we replace the usual notation for complex vectors  $\mathbb{C}^n$  with the notation  $\ell^2(\mathbb{Z}_N)$ . We do this because we want to stress that a vector is a function on  $\mathbb{Z}_N$  in order to emphasize that the Fourier transform should be thought of as an operator between function spaces, in this case taking the space of complex-valued functions on  $\mathbb{Z}_N$  to itself. We use the notation  $\ell^2(\mathbb{Z}_N)$  to represent this function space mainly because it coincides with later notation when we discuss Fourier analysis on ‘square integrable’ spaces.

We remark that, in making the argument of a vector  $\mathbb{Z}_N$ , we have altered the usual indexing. Instead of the indexes running from 1 to  $N$  as they usually would, they now run from 0 to  $N-1$ . Throughout this section, we retain the usual convention of writing elements of  $\ell^2(\mathbb{Z}_N)$  as row vectors to save space, i.e.,  $z \in \ell^2(\mathbb{Z}_N)$  means  $z = (z(0), z(1), z(2), \dots, z(N-1))$ , but still treating them as column vectors when we wish to multiply them by matrices. And since we have altered the usual indexing on the vectors by subtracting 1 from all the indexes, we do the same with matrices, letting the top left element of an  $N \times N$  matrix be the  $(0, 0)$  element, and the bottom-right element be the  $((N-1), (N-1))$  element.

Observe that  $\ell^2(\mathbb{Z}_N)$  is a vector space. Moreover, with the dot product  $z \cdot w = \sum_{n=0}^{N-1} z(n)\bar{w}(n)$  used as an inner product, this vector space becomes an Inner Product Space. It is also a normed space with the norm induced by the inner product, namely,  $\|z\|_{\ell^2(\mathbb{Z}_N)} = \sqrt{\langle z, z \rangle}$ . A standard basis for  $\ell^2(\mathbb{Z}_N)$  is the Euclidean basis

$$\mathcal{E} = \{e_0, e_1, \dots, e_{N-1}\},$$

where  $e_k(n) = 1$  if  $n = k$ , and  $e_k(n) = 0$  if  $n \neq k$ .

Our discussion of the discrete Fourier transform is adapted from M. Frazier’s *An Introduction to Wavelets Through Linear Algebra*.

### 2.1. The Discrete Fourier Transform.

**Proposition 2.1.** *For  $0 \leq k \leq N-1$ , define  $B_k \in \ell^2(\mathbb{Z}_N)$  by*

$$B_k(m) = \frac{1}{\sqrt{N}} e^{2\pi i k m / N}.$$

*Then the set  $\{B_0, \dots, B_{N-1}\}$  is an orthonormal basis for  $\ell^2(\mathbb{Z}_N)$ .*

*Proof.* Since  $\ell^2(\mathbb{Z}_N)$  is  $N$ -dimensional, we need only prove that  $\langle B_j, B_k \rangle$  is 1 when  $j = k$  and 0 when  $j \neq k$ . So, let  $j, k \in \mathbb{Z}_N$ . Then

$$\begin{aligned} \langle B_j, B_k \rangle &= \sum_{n=0}^{N-1} \frac{1}{\sqrt{N}} e^{2j\pi in/N} \overline{\frac{1}{\sqrt{N}} e^{2k\pi ik/N}} \\ &= \frac{1}{N} \sum_{n=0}^{N-1} e^{2\pi i(j-k)n/N} \\ &= \frac{1}{N} \sum_{n=0}^{N-1} \left( e^{2\pi i(j-k)/N} \right)^n. \end{aligned}$$

If  $j = k$ , then the above sum is clearly 1, since  $e^0 = 1$ , while for  $j \neq k$  the last line above is a partial sum of a geometric series, and therefore, is equal to

$$(2.1) \quad \frac{1 - \left( e^{2\pi i(j-k)/N} \right)^N}{1 - e^{2\pi i(j-k)/N}}.$$

Since

$$\left( e^{2\pi i(j-k)/N} \right)^N = e^{2\pi i(j-k)} = 1,$$

the expression in (2.1) is zero, which finishes the proof.  $\square$

The orthonormal basis defined above turns out to not be the most useful basis, primarily because computing  $\sqrt{N}$  in all the numerical calculations wastes computer power and can increase machine error. So the Fourier basis for  $\ell^2(\mathbb{Z}_N)$  is defined slightly differently as an orthogonal but not orthonormal basis:

**Definition 2.2.** The *Fourier basis* for  $\ell^2(\mathbb{Z}_N)$  is the orthonormal set

$$\mathcal{F} = \{F_0, \dots, F_{N-1}\},$$

where

$$F_k(n) = e^{2m\pi in/N}.$$

Note that for each  $k \in \mathbb{Z}_N$ ,  $\|F_k\|_{\ell^2(\mathbb{Z}_N)} = \sqrt{N}$ .

The Discrete Fourier Transform is simply the algorithm for converting a vector to the Fourier basis; this is a simple consequence of the fact that the Fourier basis is an orthogonal basis.

**Definition 2.3.** Let  $z \in \ell^2(\mathbb{Z}_N)$ . The *discrete Fourier transform* (DFT) of  $z$  is the vector  $\hat{z} \in \ell^2(\mathbb{Z}_N)$  defined by

$$(2.2) \quad \hat{z}(n) = \sum_{m=0}^{N-1} z(m) e^{-2\pi imn/N}.$$

Observe that  $\hat{z}(n)$  is simply the inner product of  $z$  and  $F_n$ , i.e.,  $\hat{z}(n) = \langle z, F_n \rangle$ . Hence,  $\hat{z}$  is  $[z]_{\mathcal{F}}$ , i.e.,  $\hat{z}$  is the representation of  $z$  in terms of the Fourier Basis:

$$(2.3) \quad \hat{z} = \sum_{n=0}^{N-1} \langle z, F_n \rangle F_n.$$

The algorithm given in the definition of the DFT is the usual theoretical way of looking at the DFT, but we know from basic linear algebra (we reviewed last week) that, since the DFT is a change-of-basis, it can be expressed in terms of multiplication by an orthogonal matrix. Let  $\omega_N = e^{-2\pi i/N}$ . Define an  $N \times N$  matrix  $W_N = (\omega_N^{nm})$  (recall that we are now letting the indexes range from 0 to  $N-1$ ), here,  $\omega_N^{nm} = (e^{2\pi i/N})^{n \cdot m} = e^{2\pi inm/N}$ . Then it is easy to check that pre-multiplication by  $W_N$  converts  $z$  to  $\hat{z}$ .

**Proposition 2.4.** Let  $z \in \ell^2(\mathbb{Z}_N)$ . We have

i. (*Fourier Inversion Formula*)

$$z(n) = \frac{1}{N} \sum_{m=0}^{N-1} \hat{z}(m) e^{2\pi inm/N}.$$

ii. (*Parseval's relation*) For any  $w \in \ell^2(\mathbb{Z}_N)$ ,

$$\langle z, w \rangle = \frac{1}{N} \sum_{n=0}^{N-1} \hat{z}(n) \overline{\hat{w}(n)} = \frac{1}{N} \langle \hat{z}, \hat{w} \rangle.$$

iii. (*Plancherel's formula*)

$$\|z\|^2 = \frac{1}{N} \sum_{n=0}^{N-1} |\hat{z}(n)|^2 = \frac{1}{N} \|\hat{z}\|^2.$$

*Proof.* These follow from the general results regarding orthonormal bases in inner product spaces, i.e., Proposition 1.10, and the fact that the Fourier basis is just a constant multiple by  $\sqrt{N}$  of an orthonormal basis.  $\square$

The inversion formula leads to the next definition:

**Definition 2.5.** Let  $w \in \ell^2(\mathbb{Z}_N)$ . The *inverse discrete Fourier transform* of  $w$  is the vector  $\check{w} \in \ell^2(\mathbb{Z}_N)$  defined by

$$\check{w}(n) = \frac{1}{N} \sum_{m=0}^{N-1} w(m) e^{2\pi i n m / N}.$$

Thus,  $(\hat{z})^\sim = z$ .

It follows from the theory of finite-dimensional changes-of-bases that the IDFT is given by premultiplication with  $W_N^{-1}$ . Thus, without having to invert the matrix directly, we see that  $W_N^{-1} = (\overline{\omega_N^{nm}}/N)$ .

It is worth noting that the physical frequencies of the Fourier basis vectors  $F_k$  do not actually increase with  $k$ . Rather, they increase with  $k$  for  $k < N/2$ , and then decrease when  $k > N/2$ . This occurs because, although the oscillations of the continuous functions in the formula of  $F_k$  increase with  $k$ ,  $F_k$  only includes points at the integers. An example of this appears in the MATLAB exercises. Because of the way that the frequencies peak at  $k = N/2$ , some authors prefer to use a 'zero-centered' DFT, where the indexes range from  $-N/2$  to  $N/2$  if  $N$  is even and  $-(N-1)/2$  to  $(N+1)/2$  if  $N$  is odd. Although this gives a better physical description of the phenomenon, however, the notation becomes inconvenient because the range of the index then depends on whether  $N$  is even or odd.

Now we will define some useful operators and obtain how they behave under the DFT.

**Definition 2.6.** Let  $z \in \ell^2(\mathbb{Z}_N)$  and  $k \in \mathbb{Z}$ . The *translation by  $k$  operator*  $R_k$  is defined from  $\ell^2(\mathbb{Z}_N)$  to itself by setting

$$R_k z(n) = z(n - k),$$

where the subtraction should be viewed as subtraction modulo 2. So if  $k \geq 0$ , then  $R_k$  translates  $z$  to the right by  $k$  units, with the familiar 'wrap-around' effect at the ends.

**Proposition 2.7.** Let  $z \in \ell^2(\mathbb{Z}_N)$ . Then

$$\widehat{R_k z}(n) = e^{-2\pi i n k / N} \hat{z}(n).$$

*Proof.* The proof is a straightforward computation. We change variables in the (finite) sum defining the Fourier Transform and, using the periodic nature of addition modulo  $N$ , to get

$$\begin{aligned}
 \widehat{R_k z}(n) &= \sum_{m=0}^{N-1} R_k z(m) e^{-2\pi i n m / N} \\
 &= \sum_{m=0}^{N-1} z(m-k) e^{-2\pi i n m / N} \\
 &= \sum_{l=0}^{N-1} z(l) e^{-2\pi i (l+k) / N} \\
 &= e^{-2\pi i n k / N} \sum_{m=0}^{N-1} R_k z(n) e^{2\pi i n l / N} \\
 &= e^{-2\pi i n k / N} \widehat{z}(n).
 \end{aligned}$$

□

**Definition 2.8.** The *conjugate* of a complex-valued function  $f$  on a domain  $X$  is the function  $\bar{f}$  whose value at each  $x \in X$  is  $\overline{f(x)}$ . This applies to functions on  $\mathbb{Z}_N$ , so when we write  $\bar{z}$  for some  $z \in \ell^2(\mathbb{Z}_N)$ , we mean the vector whose  $j$ -th coordinate is the complex conjugate of the  $j$ th coordinate of  $z$ , i.e.,  $\bar{z} = (\bar{z}(0), \bar{z}(1), \dots, \bar{z}(N-1))$ .

**Proposition 2.9.** Let  $z \in \ell^2(\mathbb{Z}_N)$ . Then

$$(2.4) \quad \widehat{\bar{z}}(n) = \overline{\widehat{z}(-n)} = \overline{\widehat{z}(N-n)}.$$

*Proof.* Using properties of conjugation and the  $N$ -periodicity of all functions involved, we obtain

$$\begin{aligned}
 \widehat{\bar{z}}(n) &= \sum_{m=0}^{N-1} \bar{z}(m) e^{-2\pi i n m / N} \\
 &= \sum_{m=0}^{N-1} \overline{z(m) e^{-2\pi i n m / N}} \\
 &= \overline{\sum_{m=0}^{N-1} z(m) e^{2\pi i n m / N}} \\
 &= \overline{\sum_{m=0}^{N-1} z(m) e^{-2\pi i (N-n) m / N}} \\
 &= \overline{\widehat{z}(N-n)}.
 \end{aligned}$$

□

**Corollary 2.10.** Let  $z \in \ell^2(\mathbb{Z}_N)$ . Then  $z$  is real if and only if  $\widehat{z}(n) = \overline{\widehat{z}(N-n)}$  for all  $n$ .

*Proof.* This follows immediately from the fact that if  $z$  is real, then  $z(n) = \bar{z}(n)$ . Now apply (2.4) to obtain the conclusion. □

## 2.2. The DFT and Shift-Invariant Linear Operators.

Translation-invariant linear operators cover a very broad range of operations, both theoretical and practical. Differentiation, for example, is a translation-invariant linear operator. So is any real-world linear filter of a signal in which a delay in the input does not change the output except to delay it. This covers many processes in electrical systems, physics, and other fields. A classic example is the sound amplifier; if the amplifier is working correctly, then it should be roughly linear, at least within the volume range it was designed for, and it should certainly be shift-invariant; that is, if the input signal of the amplifier is delayed by a second, the only effect should be to delay the output by one second. Otherwise, music would be very difficult to enjoy, indeed!

**Definition 2.11.** A linear transformation  $T : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$  is said to be *translation invariant* (or *shift invariant*) if it commutes with translation, that is, if for any  $z \in \ell^2(\mathbb{Z}_N)$ ,

$$TR_k z = R_k Tz.$$

Our ultimate goal in this section is to prove the following central theorem from signal analysis:

**Theorem 2.12.** *Let  $T : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$  be a linear operator. Then the following are equivalent:*

- (a)  $T$  is translation invariant.
- (b) The matrix  $A_{T,E}$  representing  $T$  in the standard basis is circulant.
- (c)  $T$  is a convolution operator.
- (d)  $T$  is a Fourier multiplier operator.
- (e) The matrix  $A_{T,F}$  representing  $T$  in the Fourier basis  $F$  is diagonal.

We will prove the above theorem, along with some useful specific formulas, in a piece-by-piece manner, beginning by defining the unfamiliar terms below.

**Definition 2.13.** An  $N \times N$  matrix is *circulant* for any  $m, n \in \mathbb{Z}_N$  and  $k \in \mathbb{Z}$ , we have

$$a_{n+k, m+k} = a_{n, m},$$

where the addition should be interpreted as  $N$ -periodic addition, that is, as addition modulo  $N$ .

By an easy recursive argument, an  $N \times N$  matrix is circulant if and only if for any  $m, n \in \mathbb{Z}_N$ , we have  $a_{n+1, m+1} = a_{n, m}$ .

**Definition 2.14.** Let  $z, w \in \ell^2(\mathbb{Z}_N)$ . The *convolution* of  $z$  and  $w$  is the vector  $z * w \in \ell^2(\mathbb{Z}_N)$  defined by

$$z * w(n) = \sum_{n=0}^{N-1} z(m-n)w(n).$$

It should be clear that convolution is linear in both arguments; it is also commutative, and associative, as can be seen by a simple change of variables in the first case and interchange of order of summation in the second, both of which we can do without worrying about changing the sum because the sums are finite.

**Definition 2.15.** A linear transformation  $T : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$  is said to be a *convolution operator* if there is a  $w \in \ell^2(\mathbb{Z}_N)$  such that  $T$  is given by

$$Tz = z * w \text{ for any } z \in \ell^2(\mathbb{Z}_N).$$

In this case, we denote  $T$  by  $T_w$ .

**Definition 2.16.** A linear transformation  $T : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$  is said to be a *Fourier multiplier operator* if there is a  $w \in \ell^2(\mathbb{Z}_N)$  such that  $T$  is given by

$$\widehat{Tz}(n) = w(n)\widehat{z}(n) \text{ for any } z \in \ell^2(\mathbb{Z}_N).$$

In this case, we denote  $T$  by  $T_{(w)}$ , where the parentheses distinguish  $T_{(w)}$  from the convolution operator  $T_w$ .

For notational convenience, we will denote by  $mz$  the vector given by  $mz(n) = m(n)z(n)$ , so that the definition of a Fourier multiplier operator reduces to

$$\widehat{T_{(w)}z} = w\widehat{z}.$$

We now proceed to prove Theorem 2.12 in a series of lemmas:

**Lemma 2.17.** *Let  $T : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$  be a shift-invariant linear operator. Then the matrix  $A_{T,E}$  representing  $T$  in the standard basis is circulant.*

*Proof.* Fix  $m, n \in \mathbb{Z}_N$ . Then

$$\begin{aligned} a_{n+1, m+1} &= (Te_{m+1})(n+1) \\ &= (TR_{-1}e_m)(n+1) \\ &= (R_{-1}Te_m)(n+1) \\ &= (Te_m)_n, \end{aligned}$$

where the first equality is the definition of the matrix  $A_{T,E}$ , and the other inequalities come from the definitions of translations and shift-invariant operators.  $\square$

**Lemma 2.18.** *Let  $T : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$  be represented in the standard basis by a circulant matrix  $A_{T,E}$ . Let  $a \in \ell^2(\mathbb{Z}_N)$  be defined by  $a(k) = a_{0,k}$ , the first row of  $A_{T,E}$ . Then  $T$  is a convolution operator, and  $T = T_a$ , that is  $T$  is given by convolution with the first row of  $A_{T,E}$ .*

*Proof.* Let  $z \in \ell^2(\mathbb{Z}_N)$ . Then

$$\begin{aligned} Tz(n) &= \sum_{m=0}^{N-1} a_{n,m}z(m) \\ &= \sum_{m=0}^{N-1} a_{0,m-n}z(m) \\ &= \sum_{m=0}^{N-1} a(m-n)z(m) \\ &= z * a(n), \end{aligned}$$

where the first equality follows from the definition of matrix multiplication, the second is the definition of a circulant matrix, the third is the definition of  $a$ , and the fourth is the definition of convolution.  $\square$

**Lemma 2.19.** *Let  $T_w : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$  be a convolution operator. Then  $T$  is shift invariant.*

*Proof.* Using the definitions and a change of variables in the finite sum,

$$\begin{aligned} T_w(R_k z)(n) &= w * (R_k z)(n) \\ &= \sum_{m=0}^{N-1} w(m-n)R_k z(n) \\ &= \sum_{m=0}^{N-1} w(m-n)z(n-k) \\ &= \sum_{m=0}^{N-1} w(m-n+k)z(n) \\ &= \sum_{m=0}^{N-1} w(m-(n-k))z(n) \\ &= w * z(n-k) \\ &= R_k(w * z)(n) \\ &= R_k(T_w z)(n). \end{aligned}$$

$\square$

We have now proved the equivalence of (i)-(iii) in Theorem 2.12. It remains to prove the equivalence of (iv) and (v) to the first three, which will be easy given by a technical lemma. First, we need to define the convolution identity.

**Definition 2.20.** Define the *Dirac delta function* or  $\delta \in \ell^2(\mathbb{Z}_N)$  by  $\delta(0) = 1$ , and  $\delta(n) = 0$  for  $n \neq 0$ . The delta function is also called the *unit impulse function*.

It should be clear from the definition of a convolution that the delta function is an identity for convolutions. Also note that for any shift-invariant linear operator  $T$ , which we know must be a convolution operator  $T_b$  for some  $b \in \ell^2(\mathbb{Z}_N)$ , we have

$$T_b(\delta) = b * \delta = b.$$

For this reason,  $b$  is sometimes called the impulse response.

**Lemma 2.21.** *Let  $z, w \in \ell^2(\mathbb{Z}_N)$ . Then*

$$\widehat{z * w}(n) = \hat{z}(n)\hat{w}(n).$$

*Proof.*

$$\begin{aligned} \widehat{z * w}(n) &= \sum_{m=0}^{N-1} z * w(m) e^{-2\pi i n m / N} \\ &= \sum_{m=0}^{N-1} \sum_{l=0}^{N-1} z(l-m) w(l) e^{-2\pi i n m / N} \\ &= \sum_{m=0}^{N-1} \sum_{l=0}^{N-1} z(l-m) w(l) e^{-2\pi i n (m-l) / N} e^{-2\pi i n l / N} \\ &= \sum_{l=0}^{N-1} \sum_{m=0}^{N-1} z(l-m) w(l) e^{-2\pi i n (m-l) / N} e^{-2\pi i n l / N} \\ &= \sum_{l=0}^{N-1} w(l) e^{-2\pi i n l / N} \sum_{m=0}^{N-1} z(l-m) e^{-2\pi i n (m-l) / N} \\ &= \sum_{l=0}^{N-1} w(l) e^{-2\pi i n l / N} \sum_{k=0}^{N-1} z(k) e^{-2\pi i n (k) / N} \\ &= \hat{z}(n)\hat{w}(n), \end{aligned}$$

where we interchanged order of summation in the fourth line and made the change of variables  $k = l - m$  in the sixth.  $\square$

**Corollary 2.22.** *A convolution operator  $T_b : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$  is also a Fourier multiplier operator, with*

$$T_b = T_{(\hat{b})}.$$

*The converse is also true.*

*Proof.* The statement is immediate from Lemma 2.21, and the converse also follows from Lemma 2.21, along with bijectivity.  $\square$

The final corollary, which completes the proof of Theorem 2.12, follows immediately from the definition of a Fourier multiplier operator, of which the elements of the Fourier basis are automatically eigenvectors, and the fact that by virtue of its being a basis the Fourier basis is automatically a complete set of eigenvectors.

**Lemma 2.23.** *The matrix  $A_{T,F}$  representing a Fourier multiplier operator  $T_{(b)} : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$  is diagonal, with*

$$A_{T,F} = \text{diag}(b),$$

*the matrix with the values of  $b$  along the diagonal and zeros elsewhere.*

### 2.3. The Fast Fourier Transform.

The matrix multiplications defining the Discrete Fourier transform and its inverse, and for that matter the process of computing a convolution, all require  $N^2$  complex multiplications, which is prohibitively large (complex additions are much easier, so an operation's computer complexity is generally measured by counting multiplications and ignoring additions). The usefulness of the DFT in many applied settings comes from the fact that there is a fast algorithm, called the fast Fourier transform, which can dramatically reduce this computational load, making both Fourier transforms, and, via Theorem 2.12, convolutions and shift-invariant linear operations easy to compute quickly.

The details of the fast Fourier transform we will leave, time permitting, to exercises, and otherwise we leave it to the interested reader to read the proofs in Frazier's book or some similar introduction to Fourier analysis, but for the sake of completing our introduction to the DFT, we present the main results in this section.

**Proposition 2.24.** Let  $M \in \mathbb{N}$ , and  $N = 2M$ , and suppose  $z \in \ell^2(\mathbb{Z}_N)$ . Define  $u, v \in \ell^2(\mathbb{Z}_N)$  by

$$u(k) = z(2k), \quad v(k) = z(2k + 1) \text{ for } k = 0, \dots, M - 1.$$

Let  $\hat{z} \in \ell^2(\mathbb{Z}_N)$  be the DFT of  $z$ , and  $\hat{u}, \hat{v} \in \ell^2(\mathbb{Z}_M)$  be the DFT's of  $u$  and  $v$ , respectively. Then for  $m = 0, \dots, M - 1$ ,

$$\hat{z}(m) = \hat{u}(m) + e^{-2\pi im/n} \hat{v}(m)$$

while for  $m = M, \dots, 2M - 1$ ,

$$\hat{z}(m) = \hat{u}(m - M) - e^{-2\pi i(m-M)/n} \hat{v}(m - M).$$

Note that since it only requires  $2M^2$  complex multiplications to compute  $\hat{u}$  and  $\hat{v}$ , much fewer than the  $N^2$  needed to compute  $\hat{z}$  directly if  $N$  is large, and constructing  $\hat{z}$  from  $\hat{u}$  and  $\hat{v}$  requires comparatively few  $N$  calculations, the algorithm above can significantly reduce the time needed to compute a Fourier transform. We get more dramatic improvements come when we use the algorithm recursively. The ideal case is when  $N$  is a power of 2:

**Proposition 2.25.** Let  $N = 2^n$ . Then the DFT on  $\ell^2(\mathbb{Z}_N)$  can be computed in fewer than  $N/2 \log_2 N$  calculations.

The FFT provides a fast, practical way to compute the DFT. Using the identity

$$z * w = (\hat{z}\hat{w})^\sim,$$

where the pointwise product requires only  $N$  multiplications, this also gives a fast way to compute convolutions, and hence, also shift invariant linear transformations.

#### 2.4. Multidimensional DFT.

The discrete Fourier transform can be extended to higher dimensions in a straightforward manner. In what follows we denote by  $\prod_{d=1}^M \mathbb{Z}_{N_d} = \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \mathbb{Z}_{N_3} \times \dots \times \mathbb{Z}_{N_d}$ .

If  $f : \prod_{d=1}^M \mathbb{Z}_{N_d} \rightarrow \mathbb{C}$  is a vector in multiple dimensions, then we define  $\hat{f} \in \ell^2(\prod_{d=1}^M \mathbb{Z}_{N_d})$  by

$$\begin{aligned} \hat{f}(n_1, n_2, \dots, n_d) = \\ \sum_{a=0}^{N_1-1} \sum_{b=0}^{N_2-1} \dots \sum_{m=0}^{N_M-1} f(a, b, \dots, m) e^{-2\pi i(an_1/N_1 + bn_2/N_2 + \dots + mn_M/N_M)}. \end{aligned}$$

A key observation is that we can rearrange this, by splitting up the exponential into  $M$  iterated sums, each containing only the  $M$ th coordinates, and thus evaluate the transform coordinate-wise. That is, we first take the one-dimensional Fourier transform in the  $M$ th coordinate for each value of the 1st through  $(M - 1)$ st coordinates, and then proceed recursively until we are taking the Fourier transform in the first coordinate. This is a general property of Fourier analysis, that the higher-dimensional transformation can be described in terms of iterating the one-dimensional transformations, although in infinite-dimensional settings we have to be more careful about when an interchange of sums or integrals is justified than we do in the finite case.

The inverse Fourier transform in higher dimensions is defined similarly:

$$\begin{aligned} f^\vee(n_1, n_2, \dots, n_d) = \\ \prod_{j=1}^M N_j \sum_{a=0}^{N_1-1} \sum_{b=0}^{N_2-1} \dots \sum_{m=0}^{N_M-1} f(a, b, \dots, m) e^{2\pi i(an_1/N_1 + bn_2/N_2 + \dots + mn_M/N_M)}. \end{aligned}$$

The higher-dimensional discrete Fourier transform and inverse DFT satisfy the same properties as a result of orthogonality that the one-dimensional transform does, namely that they are inverse transformations. This can be seen by directly proving orthogonality, or by noting that the higher-dimensional transform is simply an iteration of the one-dimensional transform, and thus that, by reversing the order of summation, we can invert the transform iteratively as well.