Analysis on Finite Gel′fand Spaces

by

Michael S. Venn

Bachelor of Arts
University of South Carolina, 1991

Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in the

Department of Mathematics

University of South Carolina

2001

Department of Mathematics
Director of Thesis

Department of Mathematics
Second Reader

Dean of The Graduate School

Acknowledgements

I would like to thank, first, Professor Ralph Howard for introducing finite Gel′fand spaces to me. Further, I am thankful for his mathematical guidance and patience, although I suspect that he would rather be remembered as a difficult and impatient thesis director. So I will thank him then, as well, for being such a peevish and merciless director—although, of course, he was verily rather the opposite of that. Professor Howard is a fine neighbor, an excellent mathematician, and, in the words of Ernest Hemingway, a very good drunk. Next, I appreciate the helpful comments of Professor Konstantin Oskolkov, perhaps the greatest story-teller I have ever met, who gave me valuable advice on the particulars of my defense. Also, Professor George McNulty proved a great help in working out the technical difficulties of typesetting my thesis. Finally, to my wife, Mary Elizabeth Brodie Venn, I give thanks for enduring so many sleepless nights with me and for brooking what must have seemed interminable, senseless half-babble about mathematical places that may, or may not, it turns out, even exist.

Abstract

We consider the discrete analogue, called the *finite Radon transform*, of the classical Radon transform from functional analysis. While others have approached the invertibility question of the finite Radon transform using techniques from graph theory and lattice theory, we approach the problem by considering spaces, which we call *Gel′fand spaces* in which we can show that finite Radon transforms are invertible. We start with a vector space and add some group structure, as well as some representation theory, to build, largely axiomatically, what we call a *convolution algebra* of a finite set. The convolution algebra will serve as a foundation for the Gel′fand space. We also include a few examples of finite Radon transforms and their invertibility formulæ.

Contents

Chapter 1

Introduction

1.1. The Radon Transform

Recall from elementary linear algebra and analysis that we give the name *Hilbert space* to any complete inner product space (See the beginning of Chapter 2 for the definition of an inner product space). Furthermore, recall that a *hyperplane* of an n-dimensional vector space is a subspace of dimension $n-1$. Finally, we will call a subset, A, of a vector space, V, *affine* if there is a vector subspace, W, of V and an element, v, in V such that $A = v + W$. The affine subsets, then, are the translates of the subspaces, and we call the translate of an $(n-1)$-dimensional subspace an *affine hyperplane*. Now let $\phi : \mathbb{R}^n \mapsto \mathbb{C}$ be a complex-valued function on an n-dimensional Hilbert space, where $\mathbb{R}$ and $\mathbb{C}$ denote the real and complex numbers, respectively. Then we will call $T\phi$ the *Radon transform* of ϕ, where $T\phi$ is the complex-valued transformation, defined on the set of affine hyperplanes in $\mathbb{R}^n$ by,

$$(T\phi)(H) = \int_H \phi.$$

We integrate, above, with respect to Lebesgue measure, over the affine hyperplane H.

The Radon transform has enjoyed a position of fundamental importance to many applied problems in mathematics and physics and questions in functional analysis. The problems and applications usually appear in some manifestation of the following question. When can the function, ϕ, be reconstructed from its Radon transform, $T\phi$? The Radon transform gets its name from Johann Radon, who first, in 1917, derived an explicit formula for the function on the plane, if integrals over all lines through the plane are given [**18**]. Since then applications of the Radon formula have appeared in radio astronomy, electron micrography, and many other fields of science and mathematics.

Undoubtedly, however, the most famous application of the Radon transform's invertibility has been in x-ray tomography. In 1970 G. N. Hounsfield and A. M. Cormack introduced a computed tomograph, which physicians could use in a clinical setting, for which, in 1979, they were awarded the Nobel Prize in medicine. For an excellent introduction to the history of the Radon transform in computed tomography, see A. M. Cormack's treatment in [**5**].

1.2. The Finite Radon Transform

But what if we consider the analogues of the Radon transform in the discrete setting? To wit, then, can we define the Radon transform on a function space in which the functions are all defined on a finite set? As the finite analogue of integration is summation, we can rewrite the above definition of the Radon transform.

Let $\mathfrak{C}$ be a collection of subsets of a finite set, X, and let $\ell^2(X)$ denote the set of all complex functions defined on X. (See Section 2.1 for a precise definition of $\ell^2(X)$.) Now if ϕ is in $\ell^2(X)$, then we will call the linear transformation $\mathbf{T} : \ell^2(X) \mapsto \ell^2(\mathfrak{C})$ the *finite Radon transform* defined, for C in $\mathfrak{C}$, by

$$(\mathbf{T}\phi)(C) = \sum_{x \in C} \phi(x).$$

Henceforth, when we refer to the *Radon transform*, we mean the finite Radon transform as defined immediately above, even if we omit the word *finite*, inasmuch as in the following, we work solely with the finite Radon transform.

According to Joseph Kung in [**15**], the first to consider the finite Radon transform was Ethan Bolker *circa* 1976. Bolker writes in [**1**] that, asked by a mathematician working in classical Radon transforms, he began thinking about the Radon transform on finite sets and looking for structure in order "to motivate theorems about the classical Radon transform and its relatives." Bolker's beautifully written mathematics in [**1**] is the most important survey on the topic of the finite Radon transform, and, as Kung states in [**15**],

> Bolker's work is focused on finite analogues of the central ideas in the theory of Radon transforms in analysis: inversion formulas, relation to the Laplacian and other differential operators, ranges of Radon transforms, group actions and homogeneous spaces, and relation to group representation theory.

Kung adds that the importance of Bolker's work in the field "cannot be overemphasized." In [**1**], Bolker explores the relationship between finite Radon transforms and areas of interest to combinatorists, including geometry over finite fields and the Kirkman schoolgirl problem. Bolker continues his work in this area, first, with Eric Grinberg and Kung in [**2**] and then with Patrick O'Neil and Jan Bowman in [**3**].

Kung's own work [**15**] in which he praises Bolker is itself an exceptional overview of the finite Radon transform. Like Bolker, Kung surveys the work in the finite Radon transform in combinatorics, and much of the paper he devotes to applications to lattice theory. Kung ends the paper with an impressive list of unsolved problems, most—if not all—of which, to our knowledge, remain unsolved.

One approach to solving the injectivity question of the finite Radon transform is to convert the question "When can a function, ϕ, be reconstructed from its Radon transform, $T\phi$? " into a question that might be answered through techniques in graph theory. If we look at the matrix of the linear transformation T, relative to the standard basis,

$$\delta_x(y) = \begin{cases} 1 & x = y \\ 0 & x \neq y. \end{cases},$$

then we have the incidence matrix with rows indexed by $\mathfrak{C}$ and columns indexed by C, whose C, x-entry is 1 if x is in C and 0 if x is not in C. Therefore, the study of finite Radon transforms can be reduced to the study of incidence matrices.

Still, as Bolker writes in [**1**], the question "When is the Radon transform injective?" is too hard in its general form. Therefore, we find in the literature answers, rather, to narrower questions of the following sort: "When is a *particular* Radon transform injective?" or "Under what conditions can a function in the image of a Radon transform be recovered?" We take a different approach here. Our question is "Can we build a space in which finite Radon transforms are invertible?" The affirmative answer to that question we present in the following pages, in a more analytic approach than others have employed as regards the finite Radon transform problem. We will consider the case in which we can simplify calculations using symmetry in the form of group actions.

The first step in the construction of such a space, which we will call a *Gel′fand* space, is to find a suitably structured environment in which to start building. We find that a vector space is the environment most suitable and flexible to our needs. Next we will add some group structure, followed by some representation theory to build what we will call a *convolution algebra* of a finite set X. We dedicate Chapter 2 to a largely axiomatic construction of a convolution algebra, which will serve as the keystone for the Gel′fand space, developed in Chapter 3, built on our work with the convolution algebra. We claim now, and will prove presently, that a Gel′fand space is a mathematical structure in which the finite Radon transform is, indeed, invertible. Finally, in Chapter 4, we present our injectivity results in the special case of doubly transitive group actions. We also present two examples, one a special case of the other.

The impetus behind the following pages, as well as, indeed, much of their content, comes from a set of unpublished notes [**13**] written by Ralph Howard and a class, entitled *Groups and Graphs*, he taught at the University of South Carolina in the fall of 2000. We try to provide here a largely axiomatic construction of finite Gel′fand spaces, without assuming that the reader has any prior knowledge of or initiation in their structure or application. Although all of the representation theory and most of the group theory and linear algebra used we try to present from the fundamentals of the definitions that we provide; nevertheless, we do assume that the reader has experience with a few definitions and results from elementary group theory and linear algebra. We find the structure behind the analysis of finite Gel′fand spaces and the proofs supporting that structure, by the nature of the order seemingly inherent in them, often elegant and surprisingly intuitive, with a touch of what seems, at times, an eldritch simplicity. We present then, in the words of the great Twentieth-Century novelist, Salman Rushdie, what we regard as an *eff* of the ineffable.

Chapter 2

The Convolution Algebra of a Finite Set X

2.1. Preliminary Definitions

Let V be a vector space over the field of complex scalars, $\mathbb{C}$. Suppose $\langle \cdot, \cdot \rangle : V \mapsto \mathbb{C}$ is a function that assigns to each ordered pair of vectors v_1 and v_2 in V a scalar $\langle v_1, v_2 \rangle$ in $\mathbb{C}$. Now suppose that our function has the following properties for each v_1, v_2, and v_3 in V and for every c_1, c_2, and c_3 in $\mathbb{C}$: $\langle c_1 v_1 + c_2 v_2, v_3 \rangle = c_1 \langle v_1, v_3 \rangle + c_2 \langle v_2, v_3 \rangle$; $\langle v_1, v_2 \rangle = \overline{\langle v_2, v_1 \rangle}$; and $\langle v_1, v_1 \rangle \geq 0$ with equality precisely when $v_1 = 0$. Then we call the function, $\langle \cdot, \cdot \rangle$, an *inner product*. Further, we shall call any vector space equipped with an inner product an *inner product space*.

Recall that a *basis* of a vector space, V, is a linearly independent spanning set of vectors in V. Also, if the dimension of V is n, then we say that a basis $\{\phi_1, \phi_2, \cdots, \phi_n\}$ is *unitary* or *orthogonal* if

$$\langle \phi_i, \phi_j \rangle = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

We know from elementary linear algebra that any finite-dimensional vector space has a basis, which we can make unitary by the famous Gram-Schmidt process or some similar algorithm.

Let X be a finite set. Then if $\ell^2(X)$ is the set of all complex-valued functions on X and if we equip $\ell^2(X)$ with the standard inner product, $\langle \phi, \psi \rangle = \sum_x \phi(x)\overline{\psi(x)}$, then $\ell^2(X)$ is an inner product space. As usual, we denote the *general linear group*, the group of invertible linear transformations from V to V, by $GL(V)$, where V is a finite-dimensional vector space. We will call a linear operator, T, *unitary* if $T^*T = TT^* = I$. The *unitary group*, denoted $\mathcal{U}(V)$, is the subgroup of $GL(V)$ whose elements are, in addition to being invertible, unitary. Let G be a group and X a set. If we let g be in G and x in X, then we call a map $(g, x) \mapsto gx$ an *action of G on X* if, when e is the identity of G, $ex = x$ for all x in X and $g_1(g_2x) = (g_1g_2)x$ for every g_1 and g_2 in G and x in X. Furthermore, if we have an action of G on X, we often write *G acts on X* and call X a *G-space*. If H is a subgroup of G and $G/H = \{\xi H : \xi \in G\}$ is the set of left cosets, then G/H is a G-space via the action $g(\xi H) = (g\xi)H$.

Let X be a G-space. Then if x is an element of X we call $Gx = \{gx : g \in G\}$ the *orbit of x under G*. Further, we say *G acts transitively on X* or that there is a *transitive group action of G on X*, when all elements of X are in the same orbit under G, or, what is the same, when for all x_1 and x_2 in X, there exists a group element g such that $gx_1 = x_2$. Notice that a set X being a transitive G-space makes no guarantee that the action of a subgroup of G on X will also be transitive. Let us call the number of orbits of a group or a subgroup, H, on X the *rank* of H on X, which we will denote, $\mathrm{Rank}_H(X)$. We next give a name to the set of G-space members that a group element g leaves fixed, or, in symbols, $\{x \in X : gx = x\}$, which we shall denote X^g; these *fixed point sets of g* we extend in a natural way to subsets of G; hence, when we write X^H and H is a subset of G, we mean the set of members of X that the action of every member of H keeps fixed; in symbols, we have, then, $X^H = \{x \in X : gx = x \text{ for all } g \in H\}$.

2.2. Representation of a Group on $\ell^2(X)$

Let G be a finite group and V a finite-dimensional vector space. If $\rho : G \mapsto GL(V)$ is a group homomorphism—that is, $\rho(g_1g_2) = \rho(g_1)\rho(g_2)$ for every g_1 and g_2 in G—then we call ρ a *representation of G* or, when there is no confusion about the group to which we refer, a *group representation*. Often we will abuse notation slightly and write g for $\rho(g)$. Our standard example, which will prove useful, of a group representation is the following. Let us assume that X is a G-space; then for x in X and g in G, define $\tau : G \mapsto GL(\ell^2(X))$ by $(\tau_g \phi)(x) = \phi(g^{-1}x)$. Surely, then, the map $\tau_g : \ell^2(X) \mapsto \ell^2(X)$ is linear, as the space $\ell^2(X)$ itself is linear. In addition, τ is a group homomorphism, inasmuch as $(\tau_{g_1})(\tau_{g_2}\phi)(x) = (\tau_{g_2}\phi)({g_1}^{-1}x) = \phi({g_2}^{-1}{g_1}^{-1}x) = \phi((g_1g_2)^{-1}x) = (\tau_{g_1g_2}\phi)(x)$, and thence we have shown that τ is a representation of G. Finally, since τ is a group representation, and therefore a group homomorphism, we have the usual added structural advantage $\tau_g^{-1} = \tau_{g^{-1}}$ for all group elements g, because for any representation ρ of a group G and for any g in G, we have $\rho(g^{-1})\rho(g) = \rho(gg^{-1}) = \rho(e)$, which is the identity element in $GL(V)$. Accordingly, in our example, τ, of a group representation, we know that every τ_g has an inverse, namely, $\tau_{g^{-1}}$, in $GL(\ell^2(X))$.

We will say that a representation $\rho : G \mapsto GL(V)$ is *unitary* if there exists an inner product on V such that $\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle$ for all v and w in V and g in G.

PROPOSITION 2.2.1. If $\rho : G \mapsto GL(V)$ is a representation, then there exists an inner product that makes ρ unitary.

Proof. Let $\langle \cdot, \cdot \rangle_0$ be any inner product on V, and define a new inner product on V by

$$\langle v_1, v_2 \rangle_\nu = \frac{1}{|G|} \sum_{\xi \in G} \langle \rho(\xi)v_1, \rho(\xi)v_2 \rangle_0$$

for v_1 and v_2 in V. We will show, first, that $\langle \cdot, \cdot \rangle_\nu$ is an inner product. Let v_1, v_2 and v_3 be in V and let c_1 and c_2 be in $\mathbb{C}$. Then

$$
\begin{aligned}
\langle c_1v_1 + c_2v_2, v_3\rangle_\nu &= \frac{1}{|G|}\sum_{\xi\in G}\langle \rho(\xi)(c_1v_1 + c_2v_2), \rho(\xi)v_3\rangle_0 \\
&= \frac{1}{|G|}\sum_{\xi\in G}\langle \rho(\xi)c_1v_1 + \rho(\xi)c_2v_2, \rho(\xi)v_3\rangle_0 \\
&= \frac{1}{|G|}\sum_{\xi\in G}\big(\langle \rho(\xi)c_1v_1, \rho(\xi)v_3\rangle_0 + \langle \rho(\xi)c_2v_2, \rho(\xi)v_3\rangle_0\big) \\
&= \frac{1}{|G|}\sum_{\xi\in G}\langle \rho(\xi)c_1v_1, \rho(\xi)v_3\rangle_0 + \frac{1}{|G|}\sum_{\xi\in G}\langle \rho(\xi)c_2v_2, \rho(\xi)v_3\rangle_0 \\
&= c_1\frac{1}{|G|}\sum_{\xi\in G}\langle \rho(\xi)v_1, \rho(\xi)v_3\rangle_0 + c_2\frac{1}{|G|}\sum_{\xi\in G}\langle \rho(\xi)v_2, \rho(\xi)v_3\rangle_0 \\
&= c_1\langle v_1, v_3\rangle_\nu + c_2\langle v_2, v_3\rangle_\nu
\end{aligned}
$$

and, thus, $\langle\cdot,\cdot\rangle_\nu$ satisfies the first property of inner products. For the second, note that

$$
\begin{aligned}
\overline{\langle v_2, v_1\rangle}_\nu &= \frac{1}{|G|}\sum_{\xi\in G}\overline{\langle \rho(\xi)v_2, \rho(\xi)v_1\rangle}_0 \\
&= \frac{1}{|G|}\sum_{\xi\in G}\langle \rho(\xi)v_1, \rho(\xi)v_2\rangle_0 = \langle v_1, v_2\rangle_\nu
\end{aligned}
$$

Finally, we find $\langle v_1, v_1\rangle_\nu \geq 0$ with equality holding precisely when v_1 is the zero vector, because the inner product $\langle\cdot,\cdot\rangle_0$ with which it is defined has the desired property and because $\frac{1}{|G|}$ is never zero if G is nonempty.

Now we will show that $\langle\cdot,\cdot\rangle_\nu$ makes ρ unitary. For g in G we have

$$
\begin{aligned}
\langle \rho(g)v_1, \rho(g)v_2\rangle_\nu &= \frac{1}{|G|}\sum_{\xi\in G}\langle \rho(\xi)\rho(g)v_1, \rho(\xi)\rho(g)v_2\rangle_0 \\
&= \frac{1}{|G|}\sum_{\xi\in G}\langle \rho(\xi g)v_1, \rho(\xi g)v_2\rangle_0 \\
&= \frac{1}{|G|}\sum_{\eta\in G}\langle \rho(\eta)v_1, \rho(\eta)v_2\rangle_0 \text{ if we substitute } \eta g^{-1} \text{ for } \xi
\end{aligned}
$$

$$= \langle v_1, v_2 \rangle_\nu$$

Therefore, our candidate, $\langle \cdot, \cdot \rangle_\nu$, makes ρ unitary, and we have proven the proposition. Q.E.D.

By Proposition 2.2.1, then, every representation of a finite group is unitary. Further, we can represent any finite group, with a group representation, not only as a subset of the general linear group but also as a subset of the unitary group. Now let us reconsider our example, $(\tau_g \phi)(x) = \phi(g^{-1}x)$, of a group representation using the claim that every representation of a finite group is unitary. Hence, we can choose to define our representation, τ, from G to $\mathcal{U}(\ell^2(X))$ instead of to $GL(\ell^2(X))$.

2.3. The Subgroup $G_{\mathbf{o}}$ and G-space Isomorphisms

Now we are ready to provide the basic environment for defining a Gel′fand space, and we establish the convention that any set, X, and any group, G, mentioned henceforth we will assume are finite, unless otherwise specified. Let X be a set on which a group G has a transitive group action. In other words, our set X is a transitive G-space. Now pick any element of X to serve as the origin, and call it $\mathbf{o}$. If $gx = x$ for a given x in X and g in G, we shall call g a *stabilizer* or, in this case, an *x-stabilizer*, and the set of x-stabilizers in G we shall denote G_x. Let $\mathbf{o}$ be any fixed member of X. Now consider the set of $\mathbf{o}$-stabilizers, namely, $G_{\mathbf{o}}$, which comprises the set of all elements of G that leave the origin, $\mathbf{o}$, fixed, or, in symbols, $G_{\mathbf{o}} = \{g \in G : g\mathbf{o} = \mathbf{o}\}$. What should be unsurprising is that the stabilizers in G are subgroups. If g_1 and g_2 are in G_x, we have $g_1 x = g_2 x = x$, and since $(g_1 g_2)x = g_2(g_1 x) = g_2 x = x$, we surely have that G_x is closed. Also, the identity, e, of G is in G_x, as $ex = x$. Now if we demonstrate G_x is closed under taking inverses, as well, we have shown that G_x is a subgroup. To that end, let $g \in G_x$. Then $gx = x$, which implies $g^{-1}gx = g^{-1}x$, and, thence, $x = g^{-1}x$, which, of course, gives us $g^{-1} \in G_x$. Therefore, for any $x \in X$ we know that G_x is a subgroup.

Let X and Y be G-spaces. Then a map $\phi : X \mapsto Y$ is a *G-morphism* if $\phi(gx) = g\phi(x)$ for all x in X and g in G. Furthermore, if there exists a bijective G-morphism ϕ from X into Y, then we call ϕ an *isomorphism* and say *X and Y are isomorphic as G-spaces*. We find, when $G/G_{\mathbf{o}}$ is the quotient of G modulo the subgroup of $\mathbf{o}$-stabilizers, that X and $G/G_{\mathbf{o}}$ are isomorphic as G-spaces. To see this, define $\Phi : G/G_{\mathbf{o}} \mapsto X$ by $\Phi(gG_{\mathbf{o}}) = g\mathbf{o}$, where $gG_{\mathbf{o}}$ is a member of the left cosets of the subgroup $G_{\mathbf{o}}$ and, therefore, a member of the quotient $G/G_{\mathbf{o}}$. Surely, Φ is well-defined, for if $g_1G_{\mathbf{o}}= g_2G_{\mathbf{o}}$ for some g_1 and g_2 in G, then $g_1 = g_2g_0$ for some g_0 in $G_{\mathbf{o}}$. But as g_0 is in $G_{\mathbf{o}}$, we know $g_1\mathbf{o} = g_2g_0\mathbf{o} = g_2\mathbf{o}$, which confirms, indeed, that Φ is well-defined. Now Φ is a G-morphism, inasmuch as

$$\Phi(g_1g_2G_{\mathbf{o}}) = (g_1g_2)\mathbf{o} = g_1(g_2\mathbf{o}) = g_1\Phi(g_2G_{\mathbf{o}}).$$

Next we must show that Φ is injective. To that end, let $\Phi(g_1G_{\mathbf{o}}) = \Phi(g_2G_{\mathbf{o}})$, which means $g_1\mathbf{o} = g_2\mathbf{o}$ and, hence, ${g_2}^{-1}g_1\mathbf{o} = \mathbf{o}$, which, in turn, evinces that ${g_2}^{-1}g_1$ is in $G_{\mathbf{o}}$ or, equivalently, that $g_1G_{\mathbf{o}} = g_2G_{\mathbf{o}}$. Thence we have shown that $\Phi(g_1G_{\mathbf{o}}) = \Phi(g_2G_{\mathbf{o}})$ implies $g_1G_{\mathbf{o}} = g_2G_{\mathbf{o}}$, which reveals that Φ is injective. To show surjectivity, let x be an element of X. Then we know there exists a g in G such that $g\mathbf{o} = x$, for the action of G on X is transitive. But then $\Phi(gG_{\mathbf{o}}) = g\mathbf{o} = x$, which guarantees the surjectivity of Φ and which finishes our justification of the claim that the transitive G-space, X, and the quotient, $G/G_{\mathbf{o}}$, are isomorphic as G-spaces.

2.4. The G-Space $\ell^2(X)$ and its Isotropic Functions

Now we will reconsider $\ell^2(X)$, the set of all complex-valued functions on a set X and claim that if G acts on X, then G acts on $\ell^2(X)$ by $(\tau_g\phi)(x) = (g\phi)(x) = \phi(g^{-1}x)$, where g is in G and $\phi(x)$ is in $\ell^2(X)$. For let $\phi(x)$ be in $\ell^2(X)$. Then $e\phi(x) = \phi(e^{-1}x) = \phi(ex) = \phi(x)$, the last equality holding because X is a G-space. Now let g_1 and g_2 be members of G. We will show $g_1(g_2\phi) = (g_1g_2)\phi$. By the definition of our proposed action of G on $\ell^2(X)$, we have $g_1(g_2\phi)(x) = g_2\phi({g_1}^{-1}x) = \phi({g_2}^{-1}{g_1}^{-1}x)$, which equals $\phi(g_1g_2)^{-1}x = (g_1g_2)\phi(x)$, and gives us $(g_1g_2)\phi$. Hence, if X is, then $\ell^2(X)$ is also, a G-space.

Next we turn our attention to a subspace of the inner product space, $\ell^2(X)$, namely, the set of all functions on X that $G_{\mathbf{o}}$ keeps fixed—that is, $\{\phi \in \ell^2(X) : g\phi = \phi$ for all $g \in G_{\mathbf{o}}\}$. We call these special fixed points in $\ell^2(X)$ *isotropic functions* and write $\ell^2(X)^{G_{\mathbf{o}}}$ for the collection of isotropic functions. We note that although X may be a transitive G-space, and, thus, the action of G on X, by definition, only produces one orbit; nevertheless, the action of $G_{\mathbf{o}}$, a subgroup of G, on X often produces more than one orbit. In fact, we will find, in all cases we consider and, furthermore, in all cases in which $|X| \geq 2$, that $\mathrm{Rank}_{G_{\mathbf{o}}}(X) > 1$, although the number of orbits of X under the transitive action of G is, by definition, 1.

Proposition 2.4.1. The dimension of the subspace of isotropic functions on X is equal to the number of orbits that result when $G_{\mathbf{o}}$ acts on X, or, what is the same, in our notation above, $\dim \ell^2(X)^{G_{\mathbf{o}}} = \mathrm{Rank}_{G_{\mathbf{o}}}(X)$.

Proof. To begin our proof, we claim that the action of a group on a set, X, is an equivalence relation and, thus, partitions the set. To see this, let $\sim_{\mathcal{O}}$ be the relation such that if X is a G-space, then $x_1 \sim_{\mathcal{O}} x_2$ exactly when x_1 and x_2 are in the same orbit under G, or, equivalently, when $gx_1 = x_2$ for some g. We will show that $\sim_{\mathcal{O}}$ is an equivalence relation.

By the definition of group action we have $ex = x$ for all x; thence $x \sim_{\mathcal{O}} x$ and, accordingly, $\sim_{\mathcal{O}}$ is reflexive. Next, suppose $x_1 \sim_{\mathcal{O}} x_2$. Then $gx_1 = x_2$ for some g, which means, after multiplication on both sides by the group element g^{-1}, that $g^{-1}gx_1 = g^{-1}x_2$, which reduces to $x_1 = g^{-1}x_2$, which, in turn, tells us $g^{-1}x_2 = x_1$;

hence $x_2 \sim_{\mathcal{O}} x_1$. We have shown, then, that $\sim_{\mathcal{O}}$ is symmetric. Now we check the transitivity of $\sim_{\mathcal{O}}$. Let $x_1 \sim_{\mathcal{O}} x_2$ and $x_2 \sim_{\mathcal{O}} x_3$. We will show $x_1 \sim_{\mathcal{O}} x_3$. Since $x_1 \sim_{\mathcal{O}} x_2$, we know $g_1x_1 = x_2$, and since $x_2 \sim_{\mathcal{O}} x_3$, we have $g_2x_2 = x_3$, whence $x_2 = g_2^{-1}x_3$. Now substituting this value for x_2 into the equation $g_1x_1 = x_2$, we get $g_1x_1 = g_2^{-1}x_3$, which is the same as $(g_2g_1)x_1 = x_3$ and, since G is a group and is therefore closed, setting $g_3 = g_2g_1$ evinces $g_3x_1 = x_3$. Therefore, $x_1 \sim_{\mathcal{O}} x_3$. Reflexivity, symmetry and transitivity hold, and thence, $\sim_{\mathcal{O}}$ is, indeed, an equivalence relation.

Therefore, we know that if $X_1 = \{\mathbf{o}\}, X_2, \cdots, X_r$ form a partition of X, then $X_1 = \{\mathbf{o}\}, X_2, \cdots, X_r$ are disjoint. Now let

$$\phi_i(x) = \begin{cases} 1 & x \in X_i \\ 0 & x \notin X_i, \end{cases}$$

with $1 \leq i \leq r$. Inasmuch as the sets $X_1 = \{\mathbf{o}\}, X_2, \cdots, X_r$ are disjoint, then, surely, $\{\phi_1, \phi_2, \cdots, \phi_r\}$ are linearly independent, since we can think of each ϕ_{i_0}—if $|X| = n$, where $|X|$ denotes the number of elements in X—as an n-dimensional column vector in $\ell^2(X)^{G_\mathbf{o}}$ with entries of ones and zeros. The set of all such vectors, that is, $\{\phi_1, \phi_2, \cdots, \phi_r\}$, is linearly independent, inasmuch as $X_1, X_2, \cdots, X_r$ are disjoint sets. Our column vector interpretation also reveals that the vectors $\{\phi_i : 1 \leq i \leq r\}$ span $\ell^2(X)^{G_\mathbf{o}}$, and because there are r vectors in the linearly independent spanning set, $\{\phi_i\}$, we have shown that $\{\phi_i\}$ forms an r-dimensional basis for $\ell^2(X)^{G_\mathbf{o}}$ and, in so doing, have shown that $\dim \ell^2(X)^{G_\mathbf{o}} = r = \mathrm{Rank}_{G_\mathbf{o}}(X)$. Q.E.D.

2.5. G-invariant Subspaces of $\ell^2(X)$

We call a linear transformation from V into V a *linear operator*. Let $\mathfrak{C}$ be a collection of linear operators on a finite-dimensional vector space. Then we say that a subspace,

W, of V is *invariant under* $\mathfrak{C}$ if $C[W] \subseteq W$ for all C in $\mathfrak{C}$. Furthermore, we say, in a natural extension of the definition of invariant subspaces above, that, if G acts on V, then a subspace W for which $gw \in W$, for all w in W and g in G, is *G-invariant.* Next we prove a proposition that guarantees every G-invariant subspace of $\ell^2(X)$ whose members $G_{\mathbf{o}}$ leaves fixed is not the trivial subspace, $\{0\}$.

PROPOSITION 2.5.1. Let $W \neq \{0\}$ be a G-invariant subspace of $\ell^2(X)$. Then $W^{G_{\mathbf{o}}} = \{\phi \in W : g\phi = \phi \text{ for all } g \in G_{\mathbf{o}}\} \neq \{0\}$. In fact, there exists a ϕ in $W^{G_{\mathbf{o}}}$ with $\phi(\mathbf{o}) = 1$.

Proof. If we let ϕ_0 be in W and stipulate that $\phi_0 \neq 0$, then because W is G-invariant and the action of G on X is transitive, we can assume, with no loss of generality, that $\phi_0(\mathbf{o}) \neq 0$. For if $\phi_0(\xi) \neq 0$ for some ξ in $G_{\mathbf{o}}$, then $\xi^{-1}\phi(\mathbf{o}) \neq 0$, and, therefore, we could simply replace ϕ_0 with $\xi^{-1}\phi_0$. Now let

$$\phi(x) = \frac{1}{|G_{\mathbf{o}}|} \sum_{g \in G_{\mathbf{o}}} \phi_0(g^{-1}x).$$

If ξ is in $G_{\mathbf{o}}$, then

$$\begin{aligned}
(\xi\phi)(x) &= \frac{1}{|G_{\mathbf{o}}|} \sum_{g \in G_{\mathbf{o}}} \phi_0(g^{-1}\xi^{-1}x) \\
&= \frac{1}{|G_{\mathbf{o}}|} \sum_{g \in G_{\mathbf{o}}} \phi_0\left((\xi g)^{-1}x\right) \\
&= \frac{1}{|G_{\mathbf{o}}|} \sum_{(\xi^{-1}g) \in G_{\mathbf{o}}} \phi_0\left(\xi\xi^{-1}g)^{-1}x\right), \\
&\quad \text{by substitution of } (\xi^{-1}g) \text{ for } g, \\
&= \frac{1}{|G_{\mathbf{o}}|} \sum_{g \in G_{\mathbf{o}}} \phi_0(g^{-1}x),
\end{aligned}$$

inasmuch as summing over $(\xi^{-1}g)$ is the same as summing over g, since G_0 is a subgroup and is, accordingly, closed. But as

$$\frac{1}{|G_{\mathbf{o}}|}\sum_{g\in G_{\mathbf{o}}}\phi_0(g^{-1}x)=\phi(x),$$

we have shown that $\phi(x)$ is in W^{G_0}.

Furthermore,

$$\begin{aligned}\phi(\mathbf{o}) &= \frac{1}{|G_{\mathbf{o}}|}\sum_{g\in G_{\mathbf{o}}}\phi_0(g^{-1}\mathbf{o}) \\ &= \frac{1}{|G_{\mathbf{o}}|}\sum_{g\in G_{\mathbf{o}}}\phi_0(\mathbf{o})\end{aligned}$$

because, as $G_{\mathbf{o}}$ is a subgroup of G, $g \in G_{\mathbf{o}}$ implies g^{-1} is in $G_{\mathbf{o}}$ and thence we know $g^{-1}\mathbf{o} = \mathbf{o}$. But

$$\frac{1}{|G_{\mathbf{o}}|}\sum_{g\in G_{\mathbf{o}}}\phi_0(\mathbf{o})=\phi_0(\mathbf{o}),$$

which, by our construction, is not equal to 0, nor is, in that case, ϕ, and we have shown that $W^{G_0} \neq \{0\}$. Finally, the element $\frac{1}{\phi(\mathbf{o})}\phi$ has the value 1 at $\mathbf{o}$, as required. Q.E.D.

2.6. Schur's Lemma

From elementary linear algebra we recall that if T is a linear transformation, then $\mathrm{Im}(T)$ and $\mathrm{Ker}(T)$ are subspaces, where $\mathrm{Im}(T)$ and $\mathrm{Ker}(T)$ represent the image of T and the kernel of T, respectively. Now we prove that under certain conditions $\mathrm{Im}(T)$ and $\mathrm{Ker}(T)$ are G-invariant.

Lemma 2.6.1. If $T : V_1 \mapsto V_2$ is a G-morphism, then $\mathrm{Im}(T)$ and $\mathrm{Ker}(T)$ are G-invariant subspaces.

Proof. First, we will show that $\mathrm{Ker}(T)$ is G-invariant. Let v_1 be in $\mathrm{Ker}(T)$, which is a subspace of V_1. Then $Tv_1 = 0$, as v_1 is in $\mathrm{Ker}(T)$. Now we know that, since T is a G-morphism,

$$T(gv_1) = gTv_1 = g0 = 0,$$

if g is in G. Thence, gv_1 is in $\mathrm{Ker}(T)$ and so $\mathrm{Ker}(T)$ is G-invariant. Now to show that $\mathrm{Im}(T)$ is G-invariant, let v_2 be in $\mathrm{Im}(T)$, which is a subspace of V_2. Consequently, we have that, for some v in V_1,

$$gv_2 = gTv = T(gv),$$

which is, indeed, a member of the image of T; therefore, we have shown that $\mathrm{Im}(T)$ is G-invariant. *Q.E.D.*

We will call a representation $\rho : G \mapsto GL(V)$ *irreducible* if the only subspaces of V invariant under G are $\{0\}$ and V. If $\rho_1 : G \mapsto GL(V_1)$ and $\rho_2 : G \mapsto GL(V_2)$ are two representations of G, then we say ρ_1 and ρ_2 are *equivalent* if there exists an invertible linear transformation $L : V_1 \mapsto V_2$ so that $L\rho_1(g) = \rho_2(g)L$ for all g in G, or, what is the same, if $\rho_1(g)$ and $\rho_2(g)$ are similar for all g in G. In this case, we call L an *equivalence* between ρ_1 and ρ_2.

Schur's Lemma. Let $\rho_1 : G \mapsto GL(V_1)$ and $\rho_2 : G \mapsto GL(V_2)$ be two irreducible representations of G. Then any G-invariant linear transformation $L : V_1 \mapsto V_2$ is either the zero transformation, $L = 0$, or is an equivalence between ρ_1 and ρ_2. To wit, L is either an isomorphism or the zero transformation.

Proof. If $L = 0$, then there is nothing to prove. Assume, then, $L \neq 0$. Now by Lemma 2.6.1, we know $\mathrm{Ker}(L)$ is a G-invariant subspace of V_1, and, as $L \neq 0$, we know $\mathrm{Ker}(L) \neq V_1$. Because V_1 is irreducible, $\mathrm{Ker}(L) = \{0\}$, and, thence, L is injective. Similarly, $\mathrm{Im}(L)$ is a G-invariant subspace of V_2 and $\mathrm{Im}(L) \neq \{0\}$, since $L \neq 0$ and, thus, L is surjective. Therefore, L is bijective and is an equivalence between ρ_1 and ρ_2. Q.E.D.

2.7. An Injectivity Theorem

We use Lemma 2.6.1 to prove the following theorem, which will prove useful when we try to determine whether or not a linear transformation in general, and, specifically, when a Radon Transform, from $\ell^2(X)$ to a vector space is injective and, therefore, invertible.

Theorem 2.7.1. Let $\rho : G \mapsto GL(V)$ be a representation and $T : \ell^2(X) \mapsto V$ be a G-morphism. Then T is injective if and only if $T\big|_{\ell^2(X)^{G_o}}$ is injective.

Proof. That T is injective evidently guarantees that $T\big|_{\ell^2(X)^{G_o}}$ is injective. To prove the converse, assume to the contrary that $T\big|_{\ell^2(X)^{G_o}}$ is, but T is not, injective. Then $\mathrm{Ker}(T) \neq \{0\}$. From Lemma 2.6.1 we know that the subspace, $\mathrm{Ker}(T)$, is G-invariant, and, consequently, by Proposition 2.5.1, $\mathrm{Ker}(T)^{G_0} \neq \{0\}$, a result that produces the following contradiction:

$$\{0\} \neq \mathrm{Ker}(T)^{G_0} \subseteq \mathrm{Ker}\left(T\big|_{\ell^2(X)^{G_o}}\right) = \{0\},$$

which proves the assertion that $T\big|_{\ell^2(X)^{G_o}}$ is injective implies T is injective. Q.E.D.

2.8. Radon Transforms Between Finite Grassmanians

As an application, we consider, from [**13**], Radon transforms between finite Grassmanians. Let $\mathbb{F}$ be a finite field and $\mathbb{F}^n$ the vector space of dimension n over $\mathbb{F}$. Then $GL(\mathbb{F}^n)$ is the group of all invertible linear transformations of $\mathbb{F}^n$ and $\mathrm{Aff}(\mathbb{F}^n)$ is the group of all invertible affine transformations of $\mathbb{F}^n$. The set of all k-dimensional linear subspaces of $\mathbb{F}^n$ we denote $G_k(\mathbb{F}^n)$ and call the *Grassmanian of k-dimensional subspaces*. With this notation the n-dimensional projective space over $\mathbb{F}$ is $G_1(\mathbb{F}^{n+1})$. Also, $AG_k(\mathbb{F}^n)$ is the set all k-dimensional affine subspaces of $\mathbb{F}^n$ and is called the *Grassmanian of affine k-planes*. Recall from elementary linear algebra that if V and W are two inner product spaces and $T : V \mapsto W$ is a linear transformation, then the transformation $T^* : W \mapsto V$ for which $\langle Tv, w\rangle = \langle v, T^*w\rangle$ for all v in V and w in W is the *adjoint of T*.

For $0 \leq k < l \leq n-1$ define the Radon transform $R_{k,l} : \ell^2(AG_k(\mathbb{F}^n)) \mapsto \ell^2(AG_l(\mathbb{F}^n))$ and its dual, $R^*_{k,l} : \ell^2(AG_l(\mathbb{F}^n)) \mapsto \ell^2(AG_k(\mathbb{F}^n))$, by

$$(R_{k,l}\phi)(P) = \sum_{x \subset P} \phi(x)$$

and

$$(R^*_{k,l}F)(x) = \sum_{P \supset x} F(P),$$

respectively. Likewise, for $1 \leq k < l \leq n-1$ the projective versions of these transforms, $P_{k,l} : \ell^2(G_k(\mathbb{F}^n)) \mapsto \ell^2(G_l(\mathbb{F}^n))$ and $P^*_{k,l} : \ell^2(G_l(\mathbb{F}^n)) \mapsto \ell^2(G_k(\mathbb{F}^n))$, we define by

$$(P_{k,l}\phi)(L) = \sum_{x \subset L} \phi(x)$$

and

$$(P^*_{k,l}F)(x) = \sum_{L \subset x} F(L),$$

respectively.

Define an inner product $\ell^2(X)$ in the usual manner:

$$\langle \phi_1, \phi_2 \rangle := \sum_{x \in X} \phi_1(x)\phi_2(x).$$

Then the linear transformations $R_{k,l}$ and $R_{k,l}^*$ are adjoint in the sense that

$$\langle R_{k,l}\phi, F \rangle = \sum_{P \subset Q} \phi(P)F(Q) = \langle \phi, R_{k,l}^* F \rangle.$$

Therefore, $R_{k,l}$ is injective if and only if $R_{k,l}^*$ is surjective and $R_{k,l}$ is surjective if and only if $R_{k,l}^*$ is injective. Likewise, the maps $P_{k,l}$ and $P_{k,l}^*$ are adjoint.

Theorem 2.8.1. Let $0 \leq k < l \leq n-1$.

(a) If $k + l \leq n$, then $R_{k,l} : \ell^2(AG_k(\mathbb{F}^n)) \mapsto \ell^2(AG_l(\mathbb{F}^n))$ is injective, and the dual map $R_{k,l}^* : \ell^2(AG_l(\mathbb{F}^n)) \mapsto \ell^2(AG_k(\mathbb{F}^n))$ is surjective.

(b) If $k + l \geq n$ then $R_{k,l} : \ell^2(AG_k(\mathbb{F}^n)) \mapsto \ell^2(AG_l(\mathbb{F}^n))$ is surjective, and the dual map $R_{k,l}^* : \ell^2(AG_l(\mathbb{F}^n)) \mapsto \ell^2(AG_k(\mathbb{F}^n))$ is injective.

Theorem 2.8.2. Let $1 \leq k < l \leq n-1$.

(a) If $k + l \leq n$, then $P_{k,l} : \ell^2(G_k(\mathbb{F}^n)) \mapsto \ell^2(G_l(\mathbb{F}^n))$ is injective, and the dual map $P_{k,l}^* : \ell^2(G_l(\mathbb{F}^n)) \mapsto \ell^2(G_k(\mathbb{F}^n))$ is surjective.

(b) If $k + l \geq n$ then $P_{k,l} : \ell^2(G_k(\mathbb{F}^n)) \mapsto \ell^2(G_l(\mathbb{F}^n))$ is surjective, and the dual map $P_{k,l}^* : \ell^2(G_l(\mathbb{F}^n)) \mapsto \ell^2(G_k(\mathbb{F}^n))$ is injective.

We defer the proof of Theorems 2.8.1 and 2.8.2 until the next section.

2.9. Radon Injectivity Results for Grassmanians

Continuing our example from [**13**], we claim that the group $GL(\mathbb{F}^n)$ has a transitive action on $G_k(\mathbb{F}^n)$. Fix L_0 in $G_k(\mathbb{F}^n)$, and let $K = \{a \in GL(\mathbb{F}^n) : aL_0 = L_0\}$ be the stabilizer of L_0.

Proposition 2.9.1. The orbits of $G_k(\mathbb{F}^n)$ under the action of K are

$$X_i = \{L : \dim(L \cap L_0) = i\} \qquad \text{for} \qquad \max(0, 2k-n) \le i \le k.$$

Accordingly, the number of orbits of $G_k(\mathbb{F}^n)$ under K is $k+1$ for $1 \le k \le n/2$ and $2k-n+1$ for $n/2 < k \le n-1$. In other notation, $\text{Rank}_K(G_k(\mathbb{F}^n)) = k+1$ if $1 \le k \le n/2$ and $\text{Rank}_K(G_k(\mathbb{F}^n)) = 2k-n+1$ if $n/2 < k \le n-1$.

Proof. We will merely sketch the straightforward proof of the proposition. For some L_1 and L_2, say, we can extend a basis of $L_0 \cap L_1$ to a basis, call it $\{v_i\}$, for L_0. Similarly, we extend a basis of $L_0 \cap L_2$ to a basis, call it $\{u_i\}$, for L_0, keeping, all the while, the spans of $\{u_i\}$ and $\{v_i\}$ equal. Then we define a unique linear transformation, $\mathcal{H}$, so that $\mathcal{H}v_i = u_i$, whence we determine that $\mathcal{H}$ is in K. Q.E.D.

The affine Grassmanians, $AG_k(\mathbb{F}^n)$, are somewhat more complicated. Every P in $AG_k(\mathbb{F}^n)$ is the translation of some k-dimensional linear subspace of $\mathbb{F}^n$. Let $\boldsymbol{\mathcal{L}}(P)$ in $G_k(\mathbb{F}^n)$ be the translate of P that contains the origin and is, therefore, a linear subspace of $\mathbb{F}^n$. Choose P_0 in $AG_k(\mathbb{F}^n)$ with 0 in P_0 so that $\boldsymbol{\mathcal{L}}(P_0) = P_0$, and let $K = \{a \in \text{Aff}(\mathbb{F}^n) : aP_0 = P_0\}$ be the stabilizer of P_0.

Proposition 2.9.2. The orbits of $AG_k(\mathbb{F}^n)$ under the action of K are

$$X_{0,i} = \{P : P \cap P_0 = \emptyset, \quad \dim(\boldsymbol{\mathcal{L}}(P) \cap P_0) = i\}$$
$$X_{1,i} = \{P : P \cap P_0 \neq \emptyset, \quad \dim(\boldsymbol{\mathcal{L}}(P) \cap P_0) = i\}$$

where $\max(0, 2k-n) \le i \le k$. Hence, $\text{Rank}_K(AG_k(\mathbb{F}^n)) = 2(k+1)$ if $0 \le k \le n/2$ and $\text{Rank}_K(AG_k(\mathbb{F}^n)) = 2(2k-n+1)$ if $n/2 < k \le n-1$.

Proof. This follows from the last proposition by considering the two cases where $P \cap P_0 = \emptyset$ and $P \cap P_0 \neq \emptyset$. Q.E.D.

Now we return to the proof of the theorems we deferred from the previous section.

Proof of Theorem 2.8.1. We first prove (a). Let $k+l \leq n$ and $0 \leq k < l \leq n-1$. Choose P_0 in $AG_k(\mathbb{F})$ to use as an origin. We assume that 0 in P_0 so that $\boldsymbol{\mathcal{L}}(P_0) = P_0$, and let K be the stabilizer of P_0. Let $X_{0,i}$ and $X_{1,i}$ be as in (2.9.2). Define functions ϕ_i for $0 \leq i \leq 2k+1$ by

$$\phi_i(P) := \begin{cases} 1 & 0 \leq i \leq k \text{ and } P \in X_{0,i} \\ 1 & k+1 \leq i \leq 2k+1 \text{ and } P \in X_{1,i-(k+1)} \\ 0 & \text{otherwise.} \end{cases}$$

These are the functions that are 1 on precisely one orbit of K and 0 on all other orbits. Because of the condition $k+l \leq n$ we can choose $Q_j \in AG_l(\mathbb{F}^n)$ such that $Q_j \cap P_0 = \emptyset$ and $\dim(\boldsymbol{\mathcal{L}}(Q_j) \cap P_0) = j$ for $0 \leq j \leq k$ and so that if $k+1 \leq j \leq 2k+1$, then Q_j contains 0 and, hence, $\boldsymbol{\mathcal{L}}(Q_j) = Q_j$ and $\dim(P_0 \cap Q_j) = j - (k+1)$. If $P \in AG_k(\mathbb{F}^n)$, $P \in Q_j$, and $i > j$, then $\phi_i(P) = 0$. For example, if $k \geq i > j$ then $P \subset Q_j$ implies $P \cap P_0 = \emptyset$ and $\boldsymbol{\mathcal{L}}(P) \cap P_0 \subseteq \boldsymbol{\mathcal{L}}(Q) \cap P_0$; thence, $\dim(\boldsymbol{\mathcal{L}}(P) \cap P_0) \leq \dim(\boldsymbol{\mathcal{L}}(Q_j) \cap P_0) = j < i$. Thus, P is not in $X_{0,i}$, so that $\phi_i(P) = 0$. Similar considerations work in the cases $j \leq k < i$ and $k \leq j < i$. Therefore, $R_{k,l}\phi_i(Q_j) = 0$ whenever $j < i$. On the other hand, when $0 \leq i \leq k$, we have $c_i = |\{P \subset Q_j : P \in X_{0,i}\}| > 0$ and when $k+1 \leq i \leq 2k+1$, we also have $c_i = |\{P \subset Q_j : P \in X_{1,i-(k+1)}\}| > 0$. Therefore, the matrix $[R_{k,l}\phi_i(Q_j)]$ is triangular, namely,

$$[R_{k,l}\phi_i(Q_j)] = \begin{bmatrix} c_0 & 0 & 0 & \cdots & 0 \\ * & c_1 & 0 & \cdots & 0 \\ * & * & c_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ * & * & * & \cdots & c_{2k+1} \end{bmatrix}$$

and, as the c_i are nonzero, this matrix is nonsingular. But then the functions $R_{k,l}\phi_i$, when $i = 0, \cdots, 2k-1$, are linearly independent (If $\sum_{i=0}^{2k+1} a_i\phi_i = 0$, then by evaluating at the Q_js we get a nonsingular system for the a_is). As the functions $\phi_0, \cdots, \phi_{2k+1}$ are a basis of $\ell^2(\mathbb{F}^n)^K$, the restriction of $R_{k,l}$ to $\ell^2(\mathbb{F}^n)^K$, or, in other notation, $R_{k,l}\big|_{\ell^2(\mathbb{F}^n)^K}$, is injective. Therefore, by Theorem 2.7.1, $R_{k,l}$ is injective, and $R^*_{k,l}$ surjective, when $k+l \leq n$.

Now assume $0 \leq k < l \leq n-1$ and $k+l \geq n$. We will show $R^*_{k,l}$ is injective. These conditions imply $l \geq n/2$. Let Q_0 in $AG_l(\mathbb{F}^n)$ be so that 0 is in Q_0 and, thus, $\boldsymbol{\mathcal{L}}(Q_0) = Q_0$. Also, let $K = \{a \in \text{Aff}(\mathbb{F}^n) : aQ_0 = Q_0\}$ be the stabilizer of Q_0. Then $l \leq n/2$ implies K has $(2l-n+1)$ orbits on $AG_l(\mathbb{F}^n)$. To simplify notation let $r = 2n - l$ be the codimension of Q_0. Then proposition 2.9.2 implies that the orbits of K are

$$Y_{0,i} = \{Q : Q \cap Q_0 \neq \emptyset, \quad \dim(\boldsymbol{\mathcal{L}}(Q) + Q_0) = l + i\}$$

$$Y_{1,i} = \{Q : Q \cap Q_0 = \emptyset, \quad \dim(\boldsymbol{\mathcal{L}}(Q) + Q_0) = l + (i - r - 1)\}$$

for $0 \leq i \leq r$. Define functions F_i on $AG_l(\mathbb{F}^n)$ by

$$F_i(Q) := \begin{cases} 1 & 0 \leq i \leq r \text{ and } Q \in Y_{0,i} \\ 1 & r+1 \leq i \leq 2r+1 \text{ and } P \in Y_{1,i-(r+1)} \\ 0 & \text{otherwise.} \end{cases}$$

Then $F_0, \cdots, F_{2k+1}$ is a basis of the isotropic functions $\ell^2(AG_l(\mathbb{F}^n))^K$. Because of the dimension restriction, $k+l \geq n$, we can choose elements P_j in $AG_k(\mathbb{F}^n)$ so that $P_j \cap Q_0 \neq \emptyset$, $\dim(\boldsymbol{\mathcal{L}}(P_j) + Q_0) = l + j$ for $0 \leq j \leq r$ and $P_j \cap Q_0 = \emptyset$, $\dim(\boldsymbol{\mathcal{L}}(P_j) + Q_0) = l + (j - r - 1)$ for $r+1 \leq j \leq 2r+1$. But then by considering the cases $0 \leq i < j \leq r$, $0 \leq i \leq r < j \leq 2r+1$ and $r+1 \leq i < j \leq 2r+1$, we determine that if $i < j$ and $Q \supset P_j$, then $F_i(Q) = 0$. Thence, $i < j$ implies $R^*_{k,l}F_i(P_j) = 0$. But clearly $R^*_{k,l}F_i(P_i) \neq 0$; whence, $[R^*_{k,l}F_i(Q_j)]$ is a triangular matrix with non-zero elements along the diagonal and is, accordingly, nonsingular, which implies, just as in the previous case, that $R^*_{k,l}F_0, \cdots, R^*_{k,l}F_{2r+1}$ are independent which, in turn, implies the restriction of $R^*_{k,l}$ to the isotropic functions $\ell^2(\mathbb{F}^n)^K$, or, equivalently, $R^*_{k,l}\big|_{\ell^2(\mathbb{F}^n)^K}$, is injective. Therefore, Theorem 2.7.1 implies $R^*_{k,l}$ is injective, and $R_{k,l}$ is surjective by duality. Q.E.D.

Proof of Theorem 2.8.2. An easy variant on the last proof. Q.E.D.

2.10. Convolution in $\ell^2(X \times X)$

Let k be a a function from $X \times X$ into $\mathbb{C}$, the complex scalars, or, equivalently, let k be in $\ell^2(X \times X)$. Now define $\mathbf{T}_k : \ell^2(X) \mapsto \ell^2(X)$ by

$$(\mathbf{T}_k \phi)(x) = \sum_y k(x, y)\phi(y).$$

If we view ϕ in $\ell^2(X)$ as a column vector and k as a matrix with entries indexed by $X \times X$, then the linear operator $\mathbf{T}_k$ is matrix multiplication by k.

The following observation will help us prove the subsequent proposition.

Lemma 2.10.1. If $\mathbf{T}_k\phi = 0$ for all ϕ in $\ell^2(X)$, then $k = 0$.

Proof. To see this, let $\mathbf{T}_k\phi = 0$. Then $\mathbf{T}_k\phi = \sum_y k(x, y)\phi(y) = 0$. If we let z be in X and set

$$\phi(y) = \begin{cases} 1 & y = z \\ 0 & y \neq z, \end{cases}$$

then

$$\begin{aligned} 0 &= (\mathbf{T}_k)(x) \\ &= \sum_y k(x, y)\phi(y) = k(x, z). \end{aligned}$$

Hence, $k(x, z) = 0$ for all x and z in X, which guarantees $k = 0$. Q.E.D.

Now define $\Psi : \ell^2(X \times X) \mapsto \operatorname{Hom}(\ell^2(X), \ell^2(X))$ by $\Psi(k) = \boldsymbol{\mathfrak{T}}_k$. Note that $\operatorname{Hom}(\ell^2(X), \ell^2(X))$ represents the set of all linear operators on $\ell^2(X)$. If $\Psi(k) = 0$, then $\boldsymbol{\mathfrak{T}}_k = 0$, which means $\boldsymbol{\mathfrak{T}}_k\phi = 0$ for all ϕ in $\ell^2(X)$. Then, by Lemma 2.10.1, we know that $k = 0$. Furthermore, without difficulty we see not only that $\Psi(k) = 0$ implies $k = 0$, but also that the converse holds: namely, $k = 0$ implies $\Psi(k) = 0$. That $\Psi(k) = 0$ and $k = 0$ are equivalent reveals $\operatorname{Ker}(\Psi) = \{0\}$. Now we make a claim about $\boldsymbol{\mathfrak{T}}_k$. If $\boldsymbol{\mathfrak{L}}$ is a linear operator on $\ell^2(X)$, then there exists a unique k such that $\boldsymbol{\mathfrak{L}} = \boldsymbol{\mathfrak{T}}_k$. The truth of the claim we show by noting that $\dim \ell^2(X \times X) = \dim \operatorname{Hom}(\ell^2(X), \ell^2(X)) = |X|^2$.

Further, from our remarks above, we know that $\operatorname{Ker}(\Psi) = 0$ and, therefore, since $\ell^2(X)$ is finite-dimensional, the dimension of $\operatorname{Im}(\boldsymbol{\mathfrak{L}})$ is $|X|^2$, by a famous theorem from elementary linear algebra, and, thus, we have shown that $\boldsymbol{\mathfrak{L}}$ is surjective. Thence come the existence and uniqueness of k.

Next, define

$$k_1 * k_2(x, z) = \sum_y k_1(x, y) k_2(y, z).$$

We will call the operation, $*$, *convolution* because of analogues from functional analysis, a good treatment of which can be found in [**17**] and [**4**]. If we compose $\boldsymbol{\mathfrak{T}}_{k_1}$ with $\boldsymbol{\mathfrak{T}}_{k_2}$, then we have exactly the operator $\boldsymbol{\mathfrak{T}}_{k_1 * k_2}$ on $\ell^2(X)$, a claim which we prove easily. Let ϕ be in $\ell^2(X)$. Then

$$\begin{aligned}
(\boldsymbol{\mathfrak{T}}_{k_1} \circ \boldsymbol{\mathfrak{T}}_{k_2}\phi)(y) &= \boldsymbol{\mathfrak{T}}_{k_1}(\boldsymbol{\mathfrak{T}}_{k_2}\phi)(y) \\
&= \sum_y k_1(z, y)(\boldsymbol{\mathfrak{T}}_{k_2}\phi)(y) \\
&= \sum_y k_1(z, y) \sum_x k_2(y, x)\phi(x) \\
&= \sum_y \sum_x k_1(z, y) k_2(y, x)\phi(x)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_x \left(\sum_y k_1(z,y) k_2(y,x) \right) \phi(x) \\
&= (\mathbf{T}_{k_1 * k_2} \phi)(y).
\end{aligned}
$$

2.11. The Convolution Ring of X

Now we confirm a few properties of convolution, which afford to the space $\ell^2(X \times X)$ much algebraic structure. The first property is that for all k_1, k_2, and k_3 in $\ell^2(X \times X)$ we have $(k_1 + k_2) * k_3 = k_1 * k_3 + k_2 * k_3$ and $k_1 * (k_2 + k_3) = k_1 * k_2 + k_1 * k_3$. In other words, we must show that convolution distributes over addition. If k_1, k_2, and k_3 are in $\ell^2(X \times X)$, then

$$
\begin{aligned}
k_1 * (k_2 + k_3)(x,y) &= \sum_z k_1(x,z)(k_2 + k_3)(z,y) \\
&= \sum_z k_1(x,z) \left(k_2(z,y) + k_3(z,y) \right) \\
&= \sum_z k_1(x,z) k_2(z,y) + \sum_z k_1(x,z) k_3(z,y) \\
&= k_1 * k_2(x,y) + k_1 * k_3(x,y)
\end{aligned}
$$

Now for the second distributive property:

$$
\begin{aligned}
(k_1 + k_2) * k_3(x,y) &= \sum_z (k_1 + k_2)(x,z) k_3(z,y) \\
&= \sum_z \left(k_1(x,z) + k_2(x,z) \right) k_3(z,y) \\
&= \sum_z k_1(x,z) k_3(z,y) + \sum_z k_2(x,z) k_3(z,y) \\
&= k_1 * k_3(x,y) + k_2 * k_3(x,y)
\end{aligned}
$$

For justification of associativity, recall from above that $\boldsymbol{\mathcal{T}}_{k_1} \circ \boldsymbol{\mathcal{T}}_{k_2} = \boldsymbol{\mathcal{T}}_{k_1 * k_2}$, which we use to show that

$$\boldsymbol{\mathcal{T}}_{(k_1*k_2)*k_3} = \boldsymbol{\mathcal{T}}_{k_1*k_2} \circ \boldsymbol{\mathcal{T}}_{k_3} = (\boldsymbol{\mathcal{T}}_{k_1} \circ \boldsymbol{\mathcal{T}}_{k_2}) \circ \boldsymbol{\mathcal{T}}_{k_3} = \boldsymbol{\mathcal{T}}_{k_1} \circ (\boldsymbol{\mathcal{T}}_{k_2} \circ \boldsymbol{\mathcal{T}}_{k_3}) = \boldsymbol{\mathcal{T}}_{k_1*(k_2*k_3)},$$

and $\boldsymbol{\mathcal{T}}_{(k_1*k_2)*k_3} = \boldsymbol{\mathcal{T}}_{k_1*(k_2*k_3)}$ reveals that, indeed, $(k_1 * k_2) * k_3 = k_1 * (k_2 * k_3)$. In addition to the structure that convolution adds to $\ell^2(X \times X)$, we also know that $\ell^2(X \times X)$ is a group under function addition, which we will not prove here. The properties and structure we have detailed above evince that $(\ell^2(X \times X), +, *)$ form a ring, which we will call the *convolution ring* of X. Of course, we have merely disguised matrix multiplication in a form that will prove useful for later computations.

If V and W are two inner product spaces and $T : V \mapsto W$ is a linear transformation, then the transformation $T^* : W \mapsto V$ for which $\langle Tv, w\rangle = \langle v, T^*w\rangle$ for all v in V and w in W is the *adjoint of* T. Furthermore, if $T^* = T$, then we say that T is *self-adjoint*. When a linear transformation is defined on finite inner product spaces, its adjoint always exists and is always unique, although we will not provide a proof here. We can also extend the definition of *self-adjoint* to make sense in terms of a collection of linear operators. Thus, if $\boldsymbol{\mathcal{A}}$ is a collection of linear operators on a finite-dimensional inner product space, then $\boldsymbol{\mathcal{A}}$ is *self-adjoint* if A is a member of $\boldsymbol{\mathcal{A}}$ if and only if A^* is in $\boldsymbol{\mathcal{A}}$. Finally, we will call a linear operator, T, *unitary* if $T^*T = TT^* = I$.

Next we define, if k is in $\ell^2(X \times X)$, a sort of transpose of k, denoted k^*, such that $k^*(x, y) = \overline{k(y, x)}$. Now since $\boldsymbol{\mathcal{T}}_k$ is a linear operator on $\ell^2(X)$, we know that $\boldsymbol{\mathcal{T}}_k$, because $\dim \ell^2(X) < \infty$, must have an adjoint. We will prove that $\boldsymbol{\mathcal{T}}_k^* = \boldsymbol{\mathcal{T}}_{k^*}$. For the proof, let ϕ_1 and ϕ_2 be in $\ell^2(X)$. Then, using our standard inner product,

$$\langle \boldsymbol{\mathcal{T}}_k \phi_1, \phi_2 \rangle = \sum_x (\boldsymbol{\mathcal{T}}_k \phi_1)(x) \overline{\phi_2(x)}$$

$$
\begin{aligned}
&= \sum_x \left(\sum_y k(x,y)\phi_1(y) \right) \overline{\phi_2(x)} \\
&= \sum_y \phi_1(y) \sum_x k(x,y)\overline{\phi_2(x)} \\
&= \sum_y \phi_1(y) \sum_x \overline{k^*(y,x)}\,\overline{\phi_2(x)} \\
&= \sum_y \phi_1(y) \overline{(\mathbf{T}_{k^*}\phi_2)(y)} = \langle \phi_1, \mathbf{T}_{k^*}\phi_2 \rangle
\end{aligned}
$$

We have already shown that if X is a G-space, then $\ell^2(X)$ is also a G-space. We extend the action of G, presently, a step further by asserting that if $\ell^2(X)$ is a G-space, then $\ell^2(X \times X)$ is likewise. For if X is a G-space, then so is $X \times X$ via $g(x,y) = (gx, gy)$. Thus, $\ell^2(X \times X)$ is a G-space by $(gk)(x,y) = k(g^{-1}x, g^{-1}y)$.

2.12. The Convolution Algebra $\ell^2(X \times X)^G$

Finally, we are in a position to consider the set $\ell^2(X \times X)^G$, which is

$$
\{k \in \ell^2(X \times X) : k(gx, gy) = k(x,y) \text{ for all } x, y \in X \text{ and } g \in G\}.
$$

In words, then, $\ell^2(X \times X)^G$ is the subspace of $\ell^2(X \times X)$ of functions invariant under the group action of G. We conclude easily that $\ell^2(X \times X)^G$ is closed under convolution. For if k_1 and k_2 are in $\ell^2(X \times X)^G$, then

$$
\begin{aligned}
(k_1 * k_2)(gx, gy) &= \sum_z k_1(gx, z) k_2(z, gy) \\
&= \sum_{gz} k_1(gx, gz) k_2(gz, gy) \\
&= \sum_z k_1(gx, gz) k_2(gz, gy) \\
&= \sum_z k_1(x, z) k_2(z, y) = (k_1 * k_2)(x, y).
\end{aligned}
$$

Therefore, the convolution of two functions in $\ell^2(X \times X)^G$ is again in $\ell^2(X \times X)^G$. We present, next, a proposition that guarantees that the action of G commutes with $\mathfrak{T}_k$ if k is in $\ell^2(X \times X)^G$, or, symbolically, $\mathfrak{T}_k g\phi = g\mathfrak{T}_k\phi$ for all g in G and for every ϕ in $\ell^2(X)$.

PROPOSITION 2.12.1. Let k be in $\ell^2(X \times X)$, g in G, and x and y be in X. Suppose X be a G-space. Then the following are equivalent.

(1) $\mathfrak{T}_k \circ \tau_g = \tau_g \circ \mathfrak{T}_k$
(2) $k(gx, gy) = k(x, y)$
(3) $k(gx, y) = k(x, g^{-1}y)$

Proof. Suppose, first, that (3) holds. Then

$$k(x, y) = k(g^{-1}gx, y) = k(gx, (g^{-1})^{-1}y) = k(gx, gy);$$

thence, we have shown that (3) implies (2). Next, we suppose that (2) holds. Then $k(gx, y)$=$k(g^{-1}gx, g^{-1}y)$=$k(x, g^{-1}y)$, and we see that, indeed, (3) holds. Finally, we will show that (1) and (3) are equivalent. Let ϕ be in $\ell^2(X)$ and g in G. Note, first, that

$$\begin{aligned}
(\mathfrak{T}_k \circ \tau_g)\phi(x) &= (\mathfrak{T}_k(\tau_g\phi))(x) \\
&= \sum_y k(x, y)\tau_g\phi(y) \\
&= \sum_y k(x, y)\phi(g^{-1}y) \\
&= \sum_y k(x, gy)\phi(g^{-1}gy) \\
&= \sum_y k(x, gy)\phi(y) \\
&= \mathfrak{T}_{k_1}\phi(x)
\end{aligned}$$

where $k_1(x, y) = k(x, gy)$. Likewise,

$$\begin{aligned}(\tau_g \circ \mathbf{T}_k)\phi(x) &= (\mathbf{T}_k\phi)(g^{-1}x)\\ &= \sum_y k(g^{-1}x, y)\phi(y)\\ &= \mathbf{T}_{k_2}\phi(y)\end{aligned}$$

where $k_2(x, y) = k(g^{-1}x, y)$. Therefore, $\mathbf{T}_k \circ \tau_g = \tau_g \circ \mathbf{T}_k$ if and only if $\mathbf{T}_{k_1} = \mathbf{T}_{k_2}$. That is, (1) holds if and only if $k_1 = k_2$, which implies (1) and (3) are equivalent, and we have completed our proof. Q.E.D.

Proposition 2.12.1, in addition to proving that the action, τ, of G commutes with $\mathbf{T}_k$ for k in $\ell^2(X \times X)^G$, gives us different ways to characterize that the action of G commutes with $\mathbf{T}_k$. Considering our work above, we note that the subspace, $\ell^2(X \times X)^G$, of $\ell^2(X \times X)$, inasmuch as it is closed under convolution, is an algebra in which the function

$$\delta(x, y) = \begin{cases} 1 & x = y \\ 0 & x \neq y. \end{cases}$$

serves as the identity. We call the algebra $\ell^2(X \times X)^G$ the *convolution algebra* of X.

2.13. The Relationship Between $\ell^2(X)^{G_\mathbf{o}}$ and $\ell^2(X \times X)^G$

Let us review our basic structural setup so far. We have a finite set, X, which is a transitive G-space. Further, we have fixed a point, call it $\mathbf{o}$, in X as our origin. Then $\ell^2(X)^{G_\mathbf{o}}$ is the subspace of $\ell^2(X)$ consisting of functions that are fixed by the elements of $G_\mathbf{o}$, the $\mathbf{o}$-stabilizers in G. Recall from 2.4.1 that $\dim \ell^2(X)^{G_\mathbf{o}} = \mathrm{Rank}_{G_\mathbf{o}}(X)$, which is the number of orbits that result when $G_\mathbf{o}$ acts on X.

We will proceed to show that the $\mathrm{Rank}_{G_\mathbf{o}}(X) = \dim \ell^2(X)^{G_\mathbf{o}} = r$ is also equal to the dimension of our convolution algebra, $\ell^2(X \times X)^G$. To demonstrate this, we define a linear transformation $E : \ell^2(X)^{G_{\mathbf{o}}} \mapsto \ell^2(X \times X)^G$ by $(E\phi)(x, y) = \phi(\xi^{-1}y)$, where ξ is in G and $\xi\mathbf{o} = x$. We see straightaway that E is well-defined, for if $\xi'\mathbf{o} = x = \xi\mathbf{o}$, then surely $\xi^{-1}\xi' = g_0$ for some g_0 in $G_{\mathbf{o}}$, which gives us $\xi' = \xi g_0$. To finish our demonstration that E is well-defined, we remark that $\phi({\xi'}^{-1}y) = \phi((\xi g_0)^{-1}y)$ from our work above. But $\phi((\xi g_0)^{-1}y) = \phi({g_0}^{-1}\xi^{-1}y) = \phi(\xi^{-1}y)$, the last equality holding because g_0, and therefore ${g_0}^{-1}$, is in $G_{\mathbf{o}}$. Next, consider the linear transformation $F : \ell^2(X \times X)^G \mapsto \ell^2(X)^{G_{\mathbf{o}}}$ defined by $(Fk)(y) = k(\mathbf{o}, y)$, for k in $\ell^2(X \times X)^G$. We will show that F does, in fact, send k to an isotropic function. To that end, let g_0 be in $G_{\mathbf{o}}$ and consider $(Fk)(g_0y)$=$k(\mathbf{o}, g_0y)$=$k({g_0}^{-1}\mathbf{o}, y)$= $k(\mathbf{o}, y) = (Fk)(y)$, and so F behaves correctly. We are in a position, now, to prove a proposition about the linear transformations F and E.

Proposition 2.13.1. F and E, as defined above, are inverses to each other. Therefore, $\dim \ell^2(X)^{G_{\mathbf{o}}} = \dim \ell^2(X \times X)^G = \mathrm{Rank}_{G_{\mathbf{o}}}(X)$.

Proof. Let ϕ be in $\ell^2(X)^{G_{\mathbf{o}}}$, and consider $(FE\phi)(y) = E\phi(\mathbf{o}, y) = \phi(\xi^{-1}y)$, where ξ is in $G_{\mathbf{o}}$. Next, if we set ξ equal to e, the identity in G, which, as $G_{\mathbf{o}}$ is a subgroup of G, is also in $G_{\mathbf{o}}$, we get $\phi(\xi^{-1}y) = \phi((e)^{-1}y) = \phi(ey) = \phi(y)$. Accordingly, $(FE\phi)(y) = \phi(y)$. What remains to be shown is that $(EFk)(x, y) = k(x, y)$. Let k be in $\ell^2(X \times X)$, our convolution algebra, and consider $(EFk)(x, y) = (Fk)(\xi^{-1}y)$ with $\xi\mathbf{o} = x$. Then $(Fk)(\xi^{-1}y) = k(\mathbf{o}, \xi^{-1}y) = k(\xi\mathbf{o}, y) = k(x, y)$. Thence, we have shown that F and E are inverses to each other, and, as $\dim \ell^2(X)^{G_{\mathbf{o}}} = \mathrm{Rank}_{G_{\mathbf{o}}}(X)$, by Proposition 2.4.1, the present proposition holds. Q.E.D.

Chapter 3

Finite Gel′fand Spaces

3.1. Collections of Linear Operators

Let T be a linear operator on a vector space V and λ a complex scalar. If there exists a vector v in V for which the equation $Tv = \lambda v$ holds, then we will call λ an *eigenvalue* and v and *eigenvector* of T. We will always associate eigenvectors to corresponding eigenvalues, and accordingly, we will call the set of all eigenvectors of an eigenvalue, λ, the *eigenspace* of λ. Without proof, we comment that eigenspaces are subspaces. The preceding definitions direct us to the following observation. Let T_1 and T_2 be linear operators on a vector space V. If T_1 and T_2 commute, then any eigenspace of T_1 is invariant under T_2. The claim is easily proven, for if E_λ is the eigenspace corresponding to λ, an eigenvector of T_1—that is, $E_\lambda = \{v \in V \ : \ T_1 v = \lambda v\}$, then $T_1 T_2 v = T_2 T_1 v = T_2 \lambda v$, which evinces that $T_2 v$ is, indeed, in E_λ.

Recall from Chapter 2 that if $\boldsymbol{\mathcal{A}}$ is a collection of linear operators on a finite-dimensional inner product space, then $\boldsymbol{\mathcal{A}}$ is *self-adjoint* if A is a member of $\boldsymbol{\mathcal{A}}$ if and only if A^* is in $\boldsymbol{\mathcal{A}}$.

Proposition 3.1.1. Let $\boldsymbol{\mathcal{A}}$ be a set of commuting linear operators on a vector space, V. Then $\boldsymbol{\mathcal{A}}$ has a common eigenspace, or, in symbols, there exists an eigenspace E corresponding some λ in V, with $E \neq \{0\}$, such that every v in E is an eigenvector for all A in $\boldsymbol{\mathcal{A}}$.

Proof. We proceed with induction on $\dim V$. If $\dim V = 1$, the result is clear. Let us assume, then, that the proposition is true for all spaces of dimension less than $\dim V$. If every A is of the form $A = \alpha I$, where I is the identity in V, then every v in V is an eigenvector of every A in $\boldsymbol{\mathcal{A}}$. In that case, we use $E = V$. Else, there exists an A with an eigenspace, $E_A = \{v \in V : Av = \lambda v\}$, such that $\dim E_A < \dim V$. Now let $\boldsymbol{\mathcal{A}}\big|_{E_A} = \{B\big|_{E_A} : B \in \boldsymbol{\mathcal{A}}\}$. By our claim in the preceding paragraph, E_A is invariant under each B in A, and, therefore, $\boldsymbol{\mathcal{A}}\big|_{E_A}$ is a commuting set of linear operators on E_A. By the induction hypothesis, $\boldsymbol{\mathcal{A}}\big|_{E_A}$ has a common eigenspace, which will also be a common eigenspace for $\boldsymbol{\mathcal{A}}$. Q.E.D.

Let S be a subset of a vector space V. Then we call $\{v \in V : \langle v, s\rangle = 0$ for all s in $S\}$ the *orthogonal complement of* S, which we denote $S^{\perp}$.

PROPOSITION 3.1.2. Let $\boldsymbol{\mathcal{A}}$ be a self-adjoint collection of linear operators on a finite-dimensional inner product space, V. If a subspace, W, of V is invariant under $\boldsymbol{\mathcal{A}}$, then $W^{\perp}$ is also invariant under $\boldsymbol{\mathcal{A}}$.

Proof. Let w_0 be in $W^{\perp}$, w in W, and let A be any member of $\boldsymbol{\mathcal{A}}$. Then $\langle Aw_0, w\rangle = \langle w_0, A^*w\rangle = 0$, as A^* is in $\boldsymbol{\mathcal{A}}$, and, thus, A^*w is in W. Accordingly, $\langle Aw_0, w\rangle = 0$ for all w in W. Thence, we know that Aw_0 is in $W^{\perp}$, and, because we chose A arbitrarily from $\boldsymbol{\mathcal{A}}$, we have shown that $W^{\perp}$ is invariant under $\boldsymbol{\mathcal{A}}$. Q.E.D.

PROPOSITION 3.1.3. If $\rho : G \mapsto GL(V)$ is a unitary representation, then the set of all $\rho(g)$ such that g is in G is self-adjoint collection of linear operators on V.

Proof. Let $\boldsymbol{\mathcal{A}} = \{\rho(g) : g \in G\}$. We will show that for all g in G, we have $\rho(g)^* = \rho(g^{-1}) = \rho(g)^{-1}$. Note that $\rho(g^{-1}) = \rho(g)^{-1}$, as ρ is a representation and, therefore, a homomorphism. Thence,

$$\begin{aligned}\langle \rho(g)w_1, w_2\rangle &= \langle \rho(g^{-1})\rho(g)w_1, \rho(g^{-1})w_2\rangle \\ &= \langle \rho(g^{-1}g)w_1, \rho(g^{-1})w_2\rangle \\ &= \langle \rho(e)w_1, \rho(g^{-1})w_2\rangle \\ &= \langle ew_1, \rho(g^{-1})w_2\rangle \\ &= \langle w_1, \rho(g^{-1})w_2\rangle\end{aligned}$$

which implies $\rho(g)^* = \rho(g^{-1})$. Now $\rho(g)$ is a member of $\boldsymbol{\mathcal{A}}$ if and only if $\rho(g^{-1}) = \rho(g)^*$ is in $\boldsymbol{\mathcal{A}}$. Therefore, $\boldsymbol{\mathcal{A}}$ is self-adjoint. Q.E.D.

As a corollary to the above proposition, we note that if $\rho : G \mapsto GL(V)$ is a unitary representation and W is a subspace of V invariant under ρ, then $W^\perp$ is invariant under ρ.

Let V be an inner product space, and suppose V can be written as a direct sum, $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ with the added property that if v_i is in V_i and v_j in V_j, then $\langle v_i, v_j\rangle = 0$ when $i \neq j$. Then we will call

$$V_1 \oplus V_2 \oplus \cdots \oplus V_r = \bigoplus_{n=1}^{r} V_n$$

the *orthogonal decomposition* of V. We now present the following formulation of the Spectral Theorem from elementary linear algebra.

Spectral Theorem for Commuting, Self-Adjoint Linear Operators. Let V be a finite-dimensional inner product space, and let $\boldsymbol{\mathcal{A}}$ be a self-adjoint and commutative collection of linear operators on V. Then there exist nonzero functionals, $\alpha_1, \cdots, \alpha_r : \boldsymbol{\mathcal{A}} \mapsto \mathbb{C}$, so that if

$$V_{\alpha_i} = \{v \in V : Av = \alpha_i(A)v \text{ for all } A \in \boldsymbol{\mathcal{A}}\},$$

then $V_{\alpha_i} \neq \{0\}$ and there exists the following orthogonal decomposition:

$$V = V_0 \oplus \bigoplus_{i=1}^{r} V_{\alpha_i}$$

where $V_0 = \{v \in V : Av = 0 \text{ for all } A \in \boldsymbol{\mathcal{A}}\}$ and V_0 is, possibly, $\{0\}$.

Proof. We prove our Spectral Theorem based on induction on $\dim V$. Surely, the base case of $\dim V = 1$ is true. Assume that $\dim V = n$ and that the result holds on all inner product spaces of dimension less than n. If $\boldsymbol{\mathcal{A}}$ is only scalar multiples of the identity, I_V, then the result is trivial. Let us assume, then, that there exists a A_0 in $\boldsymbol{\mathcal{A}}$ that is not a scalar multiple of I_V and, therefore, has at least one eigenvalue, call it λ. Let E be the eigenspace corresponding to λ. Then $\{0\} \neq E \neq V$. Now for any B in $\boldsymbol{\mathcal{A}}$ and v in E we have $A_0Bv = BA_0v = \lambda Bv$, as all members of $\boldsymbol{\mathcal{A}}$ commute. Thence, E is invariant under all elements of $\boldsymbol{\mathcal{A}}$. Furthermore, by Proposition 3.1.2, $E^{\perp}$ is also invariant under $\boldsymbol{\mathcal{A}}$. Now if we apply the induction hypothesis to $\boldsymbol{\mathcal{A}}\big|_E = \{B\big|_{E^{\perp}} : B \in \boldsymbol{\mathcal{A}}\}$ and $\boldsymbol{\mathcal{A}}\big|_{E^{\perp}}$, we have completed the proof. Q.E.D.

We will say that a linear operator, call it A, is *normal* if $AA^* = A^*A$. Easily, we see that if we let $\boldsymbol{\mathcal{A}} = \{A, A^*\}$, then $\boldsymbol{\mathcal{A}}$ is self-adjoint and we obtain a special case of our Spectral Theorem for normal operators.

3.2. Symmetric G-Spaces

We reconsider, next, our G-space, X, and say that it is *symmetric* if for every x and y in X, there exists an element of G, call it g, such that $gx = y$ and $gy = x$. Restating the definition in plainer terms, we consider a special type of G-space with the property that, given any two elements of X, there exists a group element whose action interchanges them. We call such an X a *symmetric G-space*. We see easily that if X is symmetric, then X is also a transitive G-space. Now we are ready to prove a theorem that relates the symmetry of X with the commutativity of its convolution algebra. The following theorem is attributable to I. M. Gel′fand .

THEOREM 3.2.1. If X is a symmetric G-space, then the convolution algebra of X, $\ell^2(X \times X)^G$, is commutative.

Proof. Let k be a member of $\ell^2(X\times X)^G$ and X be a symmetric G-space. To begin our proof, we will remark that $k(x,y) = k(y,x)$. For $k(x,y) = k(gx,gy) = k(y,x)$, since we have chosen the g in G that interchanges x and y. Now let k_1 and k_2 be in $\ell^2(X \times X)^G$, and consider

$$\begin{aligned}(k_1 * k_2)(x,y) &= \sum_z k_1(x,z)k_2(z,y) \\ &= \sum_z k_2(z,y)k_1(x,z) \\ &= \sum_z k_2(y,z)k_1(z,x) \text{ , by our remark above,} \\ &= (k_2 * k_1)(y,x),\end{aligned}$$

which is again in $\ell^2(X \times X)^G$, as $\ell^2(X \times X)^G$ is closed under convolution. Again, then, by our remark, $(k_2*k_1)(y,x) = (k_2*k_1)(x,y)$, which proves that $(k_1*k_2)(x,y) = (k_2 * k_1)(x,y)$ and, therefore, the theorem. Q.E.D.

We mention, now, a few examples of symmetric G-spaces. The first is the size k subsets of the set of n letters, $\{1, \cdots, n\}$, under the natural action of the group of permutations, S_n. (For the definition of S_n see Section 4.1.) Next, let $G_k(\mathbb{F}^n)$ and $AG_k(\mathbb{F}^n)$ be as in Section 2.8. Then the actions of $GL(\mathbb{F}^n)$ on $G_k(\mathbb{F}^n)$ and $\mathrm{Aff}(\mathbb{F}^n)$ on $AG_k(\mathbb{F}^n)$ are symmetric.

In Chapter 2 we defined, for $k \in \ell^2(X \times X)$, a linear operator, $\mathbf{T}_k$, on $\ell^2(X)$ by

$$(\mathbf{T}_k\phi)(x) = \sum_y k(x,y)\phi(y).$$

Theorem 3.2.1 above shows that the set $\{\mathbf{\mathfrak{T}}_k : k \in \ell^2(X \times X)^G\}$ is a commuting, self-adjoint set of linear operators.

Inspired by Theorem 3.2.1, we formulate the following definition. Let X be a transitive G-space. Then we will call X a *Gel′fand space* if $\ell^2(X \times X)^G$ is commutative. If X is a symmetric G-space, then we know from Theorem 3.2.1 that X is a Gel′fand space.

3.3. The Cartan-Gel′fand Theorem

We now fix and review some notation. As above, let us choose an origin, call it $\mathbf{o}$, in X, and let $G_{\mathbf{o}}$ be the set of $\mathbf{o}$-stabilizers in G. Next, if E is a G-invariant subspace of $\ell^2(X)$, then let

$$E^{G_{\mathbf{o}}} = \{\phi \in E : \tau_g \phi = \phi \text{ for all } g \in G_{\mathbf{o}}\}$$

be the isotropic functions of E. Because $\mathbb{T} = \{\mathbf{\mathfrak{T}}_k : k \in \ell^2(X \times X)^G\}$ is a commuting, self-adjoint set of linear operators, $\ell^2(X)$ can be diagonalized simultaneously or, equivalently, can be decomposed into an orthogonal direct sum by our Spectral Theorem on page 33. We will call a nonzero linear functional $\alpha : \ell^2(X \times X)^G \mapsto \mathbb{C}$ a *weight* if

$$E_\alpha = \{\phi : \mathbf{\mathfrak{T}}_k \phi = \alpha(k)\phi \text{ for all } k \in \ell^2(X \times X)^G\} \neq \{0\}.$$

Therefore, by our Spectral Theorem, we know that if X is a Gel′fand space, then $\mathbb{T}$ is commutative and self-adjoint, and there exist weights, call them $\alpha_1, \cdots, \alpha_r$, such that

$$\ell^2(X) = E_0 \oplus E_{\alpha_1} \oplus \cdots \oplus E_{\alpha_r}$$

where $E_0 = \{\phi \in \ell^2(X) : \mathbf{\mathfrak{T}}_k \phi = 0 \text{ for all } k \in \ell^2(X \times X)^G\} \neq \{0\}$.

Furthermore, we will call E_{α_i}, if $0 \leq i \leq r$, the *weight space* corresponding to α_i.

We provide, now, two lemmata, which we will find useful in our proof of the Cartan-Gel′fand Theorem to follow.

LEMMA 3.3.1. If ϕ is in $E_\alpha^{G_\mathbf{o}}$ and $\phi(\mathbf{o}) = 0$, then $\phi \equiv 0$.

Proof. Let ϕ be in $\ell^2(X)^{G_\mathbf{o}}$. Then we know from remarks leading up to Proposition 2.13.1 that there exists a k_0 in $\ell^2(X \times X)^G$ so that $k_0(\mathbf{o}, y) = \overline{\phi(y)}$. Now

$$0 = \alpha(k_0)\phi(\mathbf{o}) = (\mathfrak{T}_{k_0}\phi)(\mathbf{o}) = \sum_y k_0(\mathbf{o}, y)\phi(y) = \sum_y |\phi(y)|^2,$$

which shows that $\phi \equiv 0$. Q.E.D.

LEMMA 3.3.2. Let ϕ_1 and ϕ_2 be in $\ell^2(X)$. Then there exists a constant $c_\alpha(\phi_1, \phi_2)$ so that for all ϕ in E_α,

$$\sum_{g \in G} \sum_{y \in X} \phi_1(g^{-1}x)\phi_2(g^{-1}y)\phi(y) = c_\alpha(\phi_1, \phi_2)\phi(x).$$

Proof. Suppose $h(x, y) = \sum_{g \in G} \phi_1(g^{-1}x)\phi_2(g^{-1}y)$. We will show that h is in $\ell^2(X \times X)^G$. To that end, let ξ be in G and consider

$$\begin{aligned}
h(\xi x, \xi y) &= \sum_{g \in G} \phi_1(g^{-1}\xi x)\phi_2(g^{-1}\xi y) \\
&= \sum_{g \in G} \phi_1((\xi^{-1}g)^{-1}x)\phi_2((\xi^{-1}g)^{-1}y) \\
&= \sum_{\xi g \in G} \phi_1((\xi^{-1}\xi g)^{-1}x)\phi_2((\xi^{-1}\xi g)^{-1}y), \text{ if we set } g = \xi g \\
&= \sum_{g \in G} \phi_1(g^{-1}x)\phi_2(g^{-1}y) = h(x, y).
\end{aligned}$$

Thence, h is in $\ell^2(X \times X)^G$ as claimed. Therefore, for any ϕ in E_α, we have that $\mathbf{T}_h\phi = \alpha(h)\phi$, which is equivalent to the statement of the lemma, with $c_\alpha(\phi_1, \phi_2) = \alpha(h)$. Q.E.D.

The following theorem is a discrete analogue of the results due to E. J. Cartan and I. M. Gel′fand .

THEOREM 3.3.1. **(Cartan-Gel′fand)** If X is a finite Gel′fand space, then there exist weights, $\alpha_1, \cdots, \alpha_r$, so that

(1) $\ell^2(X) = E_{\alpha_1} \oplus \cdots \oplus E_{\alpha_r}$ *(orthogonal direct sum)*

(2) Each $E_{\alpha_i}^{G_\mathbf{o}}$ is one-dimensional and is spanned by a unique element, p_{α_i}, with $p_{\alpha_i}(\mathbf{o}) = 1$, called the *spherical function* in $E_{\alpha_i}^{G_\mathbf{o}}$.

(3) Each weight space, E_{α_i}, with $1 \leq i \leq r$, is irreducible.

(4) If $i \neq j$, then E_{α_i} and E_{α_j} are not equivalent as representations.

(5) If $E \neq \{0\}$ is any irreducible, G-invariant subspace of $\ell^2(X)$, then $E = E_{\alpha_{i_0}}$ for some i_0.

(6) $r = \mathrm{Rank}_{G_\mathbf{o}}(X)$.

Proof. We already know that $\ell^2(X) = E_0 \oplus E_{\alpha_1} \oplus \cdots E_{\alpha_r}$. Therefore to prove (1), we need merely to show that $E_0 = \{0\}$. Let ϕ be in E_0. Then $\mathbf{T}_k\phi = 0$ for all k in $\ell^2(X \times X)^G$. Now set

$$k(x,y) = \delta(x,y) = \begin{cases} 1 & x = y \\ 0 & x \neq y. \end{cases} ,$$

the identity in the convolution algebra, $\ell^2(X \times X)^G$.

Hence,

$$0 = \mathbf{T}_k\phi(x) \;\; = \;\; \sum_y k(x,y)\phi(y)$$

$$= \sum_y \delta(x,x)\phi(y)$$
$$= \phi(y),$$

whereby we have shown $\phi = 0$ and (1) holds.

To prove that each $E_{\alpha_i}^{G_\mathbf{o}}$ is one-dimensional and is spanned by a unique element we will use Lemma 3.3.1. We know that we can always choose a p_α in $E_{\alpha_i}^{G_\mathbf{o}}$ such that $p_\alpha(\mathbf{o}) = 1$, by Proposition 2.5.1. Now let ϕ be in $E_{\alpha_i}^{G_\mathbf{o}}$. Note that $\phi_1(\mathbf{o}) = \phi(\mathbf{o}) - \phi(\mathbf{o})p_\alpha(\mathbf{o}) = 0$, as $p_\alpha(\mathbf{o}) = 1$. Further, by Lemma 3.3.1, we have shown that $\phi_1 = 0$ and so $\phi = \phi(\mathbf{o})p_\alpha$ and, hence, that (2) holds.

Next, we show that each $E_{\alpha_i}^{G_\mathbf{o}}$ is irreducible. To that end, assume to the contrary that a weight space, $E_{\alpha_{i_0}}$, is reducible. Then we can decompose $E_{\alpha_i}^{G_\mathbf{o}}$ orthogonally as follows, $E_{\alpha_i}^{G_\mathbf{o}} = W_1 \oplus W_2$, where W_1 and W_2 are G-invariant subspaces of $\ell^2(X)$. But we know that ${W_1}^{G_\mathbf{o}} \neq \{0\} \neq {W_2}^{G_\mathbf{o}}$ by Proposition 2.5.1. Therefore, $E_{\alpha_i}^{G_\mathbf{o}} \geq 2$, which is a contradiction, inasmuch as, by (2) above, each E_{α_i} is one-dimensional. Accordingly, we have shown that (3) holds.

Now we show that if α and β are weights, then E_α and E_β are not isomorphic and, therefore, are not equivalent representations. Let ρ be a representation and define $\chi_\rho : G \mapsto \mathbb{C}$ by $\chi_\rho(g) = \text{Trace}(\rho(g))$. Then we call χ_ρ the *character* of ρ. If two linear transformations are isomorphic, then they have the same character, because isomorphic transformations are similar and similar transformations have the same trace.

Let $\chi_\alpha(g) = \text{Trace}(\tau_g\big|_{E_\alpha})$ and $\chi_\beta(g) = \text{Trace}(\tau_g\big|_{E_\beta})$ be the characters of the representation τ restricted to E_α and E_β. Let $\{\phi_{1\,\alpha}, \phi_{2\,\alpha}, \cdots, \phi_{l\,\alpha}\}$ and $\{\phi_{1\,\beta}, \phi_{2\,\beta}, \cdots, \phi_{m\,\beta}\}$ be unitary bases of E_α and E_β, respectively. Then, since the trace is the sum of the diagonal elements of the matrix of $\tau\big|_{E_\alpha}$, we have that

$$\chi_\alpha(g) = \sum_i \langle \tau_g \phi_{i\,\alpha}, \phi_{i\,\alpha} \rangle.$$

Similarly, we recognize that

$$\chi_\beta(g) = \sum_j \langle \tau_g \phi_{j\,\beta}, \phi_{j\,\beta} \rangle.$$

Consider, next,

$$\begin{aligned}
\langle \chi_\alpha, \chi_\beta \rangle &= \sum_{g \in G} \chi_\alpha(g) \overline{\chi_\beta(g)} \\
&= \sum_{g \in G} \sum_i \sum_j \langle \tau_g \phi_{i\,\alpha}, \phi_{i\,\alpha} \rangle \overline{\langle \tau_g \phi_{j\,\beta}, \phi_{j\,\beta} \rangle} \\
&= \sum_{g \in G} \sum_i \sum_j \sum_x \sum_y \phi_{i\,\alpha}(g^{-1}x) \overline{\phi_{i\,\alpha}(x)}\, \overline{\phi_{j\,\beta}(g^{-1}y)} \phi_{j\,\beta}(y) \\
&= \sum_i \sum_j \sum_x \left(\sum_{g \in G} \sum_y \phi_{i\,\alpha}(g^{-1}x) \overline{\phi_{j\,\beta}(g^{-1}y)} \phi_{j\,\beta}(y) \right) \overline{\phi_{i\,\alpha}(x)} \\
&= \sum_i \sum_j \sum_x c_\alpha(\phi_{i\,\alpha}, \overline{\phi}_{j\,\beta}) \phi_{j\,\beta}(x) \overline{\phi_{i\,\alpha}(x)}, \quad \text{by Lemma 3.3.2,} \\
&= \sum_i \sum_j c_\alpha(\phi_{i\,\alpha}, \overline{\phi}_{j\,\beta}) \sum_x \phi_{j\,\beta}(x) \overline{\phi_{i\,\alpha}(x)} \\
&= \sum_i \sum_j c_\alpha(\phi_{i\,\alpha}, \overline{\phi}_{j\,\beta}) \langle \phi_{j\,\beta}, \phi_{i\,\alpha} \rangle \\
&= 0,
\end{aligned}$$

since $\phi_{j\,\beta}$ is in E_β and $\phi_{i\,\alpha}$ is in E_α and E_α is orthogonal to E_β. Now suppose to the contrary that E_α and E_β are isomorphic. Then $\chi_\alpha = \chi_\beta$. But then

$$0 = \sum_{g \in G} |\chi_\alpha(g)|^2 > 0,$$

a contradiction, which evinces, then, that E_α and E_β are not isomorphic, or, what is the same, E_α and E_β are not equivalent as representations; thus, (4) holds.

Let us suppose that $E \neq \{0\}$ is an irreducible, G-invariant subspace of $\ell^2(X)$, and let $\pi_i : \ell^2(X) \mapsto E_{\alpha_i}$ be the orthogonal projection. Then π_i is G-invariant. As E is a G-invariant subspace of $\ell^2(X)$, we know by Schur's Lemma that for each i, the projection restricted to E, $\pi\big|_E : E \mapsto E_{\alpha_i}$, is either an isomorphism or the zero transformation. Because $E \neq \{0\}$ and, by (4), no two weight spaces are isomorphic, we conclude that for every i but one, call it i_0, $\pi_i = 0$ and π_{i_0} is an isomorphism. Therefore, $E = E_{\alpha_{i_0}}$, and we have proven (5).

To prove (6), we recall from Proposition 2.4.1 that $\mathrm{Rank}_{G_{\mathbf{o}}}(X) = \dim \ell^2(X)^{G_{\mathbf{o}}}$. Now $\dim \ell^2(X)^{G_{\mathbf{o}}} = \dim(E_{\alpha_1} \oplus \cdots \oplus E_{\alpha_r})^{G_{\mathbf{o}}}$ by (1) above. Further,

$$\dim(E_{\alpha_1} \oplus \cdots \oplus E_{\alpha_r})^{G_{\mathbf{o}}} = \dim(E_{\alpha_1}^{G_{\mathbf{o}}} \oplus \cdots \oplus E_{\alpha_r}^{G_{\mathbf{o}}}) = r,$$

inasmuch as, by (3), we know that each of the weight spaces, E_{α_i}, where $1 \leq i \leq r$, is one-dimensional, and we have, indeed, shown that (6) holds. Accordingly, we have proven the Cartan-Gel′fand Theorem.

3.4. *G*-Invariant Linear Operators and Inversion Formulae

We next turn our attention to results obtained when we consider the G-invariant operators in the mathematical setting described in Theorem 3.3.1, the Cartan-Gel′fand Theorem, and we will use the notation of that theorem throughout the following. First, we see that if L is a G-invariant linear operator on $\ell^2(X)$ and X is a Gel′fand space, then we can realize the restriction of L on E_{α_i} by scalar multiplication and find an explicit inverse for L.

Theorem 3.4.1. Let X be a Gel′fand space and let $L : \ell^2(X) \mapsto \ell^2(X)$ be a G-invariant linear operator—that is, $L\tau_g = \tau_g L$ for all g in G. Then for all i, $LE_{\alpha_i} \subseteq E_{\alpha_i}$ holds and $L\big|_{E_{\alpha_i}} = c_i I_{E_{\alpha_i}}$, where $c_i = (Lp_{\alpha_i})(\mathbf{o})$. In particular, L is invertible if and only if $(Lp_{\alpha_i})(\mathbf{o}) \neq 0$ for all i. In this case, the inverse of L is given by

$$L^{-1} = \sum_{i=1}^{r} \frac{1}{Lp_{\alpha_i}(\mathbf{o})} \pi_i,$$

where $\pi_i : \ell^2(X) \mapsto E_{\alpha_i}$ is an orthogonal projection.

Proof. Because LE_{α_i} is a G-invariant subspace of $\ell^2(X)$ and, as E_{α_i} is irreducible, LE_{α_i} is either $\{0\}$ or is an isomorphic to E_{α_i}. Suppose, first, that $LE_{\alpha_i} = \{0\}$. Then $LE_\alpha \subseteq E_{\alpha_i}$ and, therefore, $L\big|_{E_{\alpha_i}} = 0I_{E_{\alpha_i}}$. The first part of the theorem, then, holds for the case $LE_{\alpha_i} = \{0\}$.

Now let us consider the case when LE_{α_i} is isomorphic to E_{α_i}. Then $LE_{\alpha_i} = E_{\alpha_i}$ by parts (4) and (5) of Theorem 3.3.1. Note that $\tau_g L p_{\alpha_i} = L\tau_g p_{\alpha_i} = Lp_{\alpha_i}$, for g in $G_{\mathbf{o}}$, the last equality holding because p_{α_i} is in $E_{\alpha_i}^{G_{\mathbf{o}}}$. Thence, Lp_{α_i} is in $E_{\alpha_i}^{G_{\mathbf{o}}}$, and because $E_{\alpha_i}^{G_{\mathbf{o}}}$ is one-dimensional, $Lp_{\alpha_i} = c_i p_{\alpha_i}$ for some scalar c_i. Then $\ker(L\big|_{E_{\alpha_i}} - c_i I_{E_{\alpha_i}})$ is a G-invariant subspace of E_{α_i}, and since E_{α_i} is irreducible, we know that $\ker(L\big|_{E_{\alpha_i}} - c_i I_{E_{\alpha_i}}) = E_{\alpha_i}$; hence, $\ker(L\big|_{E_{\alpha_i}} - c_i I_{E_{\alpha_i}})$ must be the zero transformation, and we $L\big|_{E_{\alpha_i}} = c_i I_{E_{\alpha_i}}$. From above we know that $Lp_{\alpha_i}(\mathbf{o}) = c_i p_{\alpha_i}(\mathbf{o})$, and so $c_i = (Lp_{\alpha_i})(\mathbf{o})$ follows, as $p_{\alpha_i}(\mathbf{o}) = 1$.

We will show, next, that the inverse of L is as claimed in the statement of the theorem. Let

$$S = \sum_{i=1}^{r} \frac{1}{Lp_{\alpha_i}(\mathbf{o})}\pi_i.$$

Then

$$\begin{aligned}
LS &= \sum_{i=1}^{r} c_i\pi_i \sum_{j=1}^{r} \frac{1}{Lp_{\alpha_j}(\mathbf{o})}\pi_j \\
&= \sum_{i=1}^{r} c_i\pi_i \sum_{j=1}^{r} \frac{1}{c_j}\pi_j, \qquad \text{since} \quad Lp_{\alpha_j}(\mathbf{o}) = c_j, \\
&= \sum_{i=1}^{r} \frac{c_i}{c_i}{\pi_i}^2, \quad \text{because} \quad \pi_i\pi_j = 0 \text{ for } i \neq j \\
&= \sum_{i=1}^{r} \pi_i, \qquad \text{as} \quad \pi_i \text{ is a projection}, \\
&= I_{\ell^2(X)}.
\end{aligned}$$

Similarly, $SL = I_{\ell^2(X)}$ and, therefore, the inverse of L is given by

$$L^{-1} = \sum_{i=1}^{r} \frac{1}{Lp_{\alpha_i}(\mathbf{o})} \pi_i,$$

as claimed. Q.E.D.

Let V and W be inner product spaces and $L : V \mapsto W$ be a linear transformation. We claim that L is injective if and only if L^*L, a linear operator on V, is injective; for $Lv = 0$ is equivalent to $\|Lv\|^2 = 0$, where $\|v_0\|$, called the *norm* of v_0, we define, as usual, to be $\sqrt{\langle v_0, v_0 \rangle}$. Now $\|Lv\|^2 = 0$ is the same as $\langle Lv, Lv \rangle = 0$. Finally, we have $0 = \langle Lv, Lv \rangle = \langle L^*Lv, v \rangle$, which proves the claim, which, in turn, we use in the proof of the theorem that follows.

THEOREM 3.4.2. Let $L : \ell^2(X) \mapsto V$ be a G-invariant linear transformation. Then the following are equivalent.

(1) L is injective

(2) $Lp_{\alpha_i}(\mathbf{o}) \neq 0$, if $1 \leq i \leq r$

(3) The restriction, $L\big|_{\ell^2(X)^{G_\mathbf{o}}}$, of L to the isotropic functions, $\ell^2(X)^{G_\mathbf{o}}$, is injective.

Furthermore, if L is injective, any ϕ in $\ell^2(X)$ is recovered from $L\phi$ by

$$\phi = \left(\sum_{i=1}^{r} \frac{1}{L^*Lp_{\alpha_i}(\mathbf{o})} \pi_i L^* \right) L\phi.$$

Proof. By Theorem 2.7.1 , we have already shown that (1) is equivalent to (3). Now by the claim above, we know that L is injective if and only if L^*L is injective, which is equivalent to the statement

$$(L^*Lp_{\alpha_i})(\mathbf{o}) \neq 0, \quad 1 \leq i \leq r.$$

To prove that the inversion formula holds, let L be injective. Now if we apply the inversion results in Theorem 3.4.1 to the linear operator, L^*L, on $\ell^2(X)$, then

$$(L^*L)^{-1} = \left(\sum_{i=1}^{r} \frac{1}{L^*Lp_{\alpha_i}(\mathbf{o})} \pi_i L^* \right) L.$$

Therefore,

$$\phi = (L^*L)^{-1}\phi = \left(\sum_{i=1}^{r} \frac{1}{L^*Lp_{\alpha_i}(\mathbf{o})} \pi_i L^* \right) L\phi.$$

and we have proven the theorem.   Q.E.D.

Chapter 4

Doubly Transitive Group Actions

4.1. Introduction and Definitions

Heretofore we have been interested in transitive group actions on sets and have constructed our injectivity theorems under the assumption that the set X with which we have been working is a transitive G-space. Now let X be a G-space, and suppose that, for all (x_1, x_2) and (y_1, y_2) in $X \times X$ such that $x_1 \neq y_1$ and $x_2 \neq y_2$, there exists a g in G such that $gx_1 = x_2$ and $gy_1 = y_2$. Then we will say that the action of G on X is *doubly transitive* and will call X a *doubly transitive G-space.*

Evidently, if X is a doubly transitive G-space, then X is a symmetric G-space. Consequently, by Theorem 3.2.1, if the action of G on X is doubly transitive, then X is a Gel′fand space. Therefore, the injectivity and orthogonal decomposition results from Chapter 3 hold. As in the previous chapters, fix some $\mathbf{o}$ in X to serve as the origin, and let $G_{\mathbf{o}} = \{g \in G : g\mathbf{o} = \mathbf{o}\}$ be the $\mathbf{o}$-stabilizers in G. Then we claim that X is a doubly transitive G-space if and only if there are exactly two orbits of X under the action of the $\mathbf{o}$-stabilizers, $G_{\mathbf{o}}$: namely, the singleton orbit $X_1 = \{\mathbf{o}\}$ and the orbit $X_2 = X - \{\mathbf{o}\}$ or, what is the same, all of X except the origin.

Recall from elementary group theory that the *group of permutations on a set*, $X = \{1, 2, \cdots, n\}$, *of n letters* is the collection, S_n, of bijections from X to X. Furthermore, the natural action of S_n on X we will describe as follows. If σ is a member of S_n such that

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix},$$

then define $\Psi : S_n \times X \mapsto X$ by $\Psi(\sigma, x) = \sigma(x)$, for all x in X and σ in S_n, or, as we will write the action Ψ henceforth, $\sigma x = \sigma(x)$.

4.2. The Radon Transform on $X = \{1, \cdots, n\}$

Now set $G = S_n$ and $X = \{1, 2, \cdots, n\}$; then X is a doubly transitive G-space under the natural action of $G = S_n$ on X described in the previous paragraph. Next, let $Y = \{S \subseteq X : |S| = k\}$. Then G acts on Y in the obvious way, a natural extension of the action of G on X—that is, if g is in G, then $gS = \{gs : s \in S\}$. Set, finally, $\mathbf{o} = 1$ as our origin in X. Thus,

$$\begin{aligned} G_{\mathbf{o}} &= \{g \in G : g1 = 1\} \\ &= \{\sigma \in S_n : \sigma(1) = 1\} \\ &= \{\sigma \in S_n : \sigma(\{2, \cdots, n\}) = \{2, \cdots, n\}\}, \end{aligned}$$

The last equality, with some renaming, evinces that $G_{\mathbf{o}} = S_{n-1}$.

Next, define $R : \ell^2(X) \mapsto \ell^2(Y)$ by the natural Radon transform,

$$(R\phi)(S) = \sum_{x \in S} \phi(x).$$

Now let

$$\phi_1(x) = \begin{cases} 1 & x = 1 \\ 0 & x \neq 1 \end{cases}$$

and

$$\phi_2(x) = \begin{cases} 0 & x = 1 \\ 1 & x \neq 1 \end{cases}$$

Then $\{\phi_1, \phi_2\}$ is a basis of $\ell^2(X)^{G_{\mathbf{o}}}$. The image of the basis vectors, ϕ_1 and ϕ_2, is

$$(R\phi_1)(S) = \sum_{x \in S} \phi_1(x) = \begin{cases} 1 & 1 \in S \\ 0 & 1 \notin S \end{cases}$$

and

$$(R\phi_2)(S) = \sum_{x \in S} \phi_2(x) = \begin{cases} k-1 & 1 \in S \\ k & 1 \notin S \end{cases}.$$

If we suppose that $\phi_0 = c_1\phi_1 + c_2\phi_2$ and that $\phi_0 \in \operatorname{Ker}\left(R\big|_{\ell^2(X)^{G_{\mathbf{o}}}}\right)$, then

$$R\phi_0 = c_1 R\phi_1 + c_2 R\phi_2 = 0.$$

Let $S_1 = \{1, \cdots, k\}$ and $S_2 = \{2, \cdots, k+1\}$. Now if we evaluate $R\phi_0$ at S_1 and S_2, we get the following pair of homogeneous equations.

$$R\phi_0(S_1) = c_1 R\phi_1(S_1) + c_2 R\phi_2(S_1) = 0$$

$$R\phi_0(S_2) = c_1 R\phi_1(S_2) + c_2 R\phi_2(S_2) = 0,$$

which, by our results above, show that $c_1 = c_2 = 0$, which, in turn, reveals that $\{R\phi_1, R\phi_2\}$ is linearly independent. Therefore,

$$\operatorname{Ker}\left(R\big|_{\ell^2(X)^{G_{\mathbf{o}}}}\right) = \{0\}$$

and, because $\dim \ell^2(X) < \infty$, we know, by a famous theorem from elementary linear algebra, that $R\big|_{\ell^2(X)^{G_{\mathbf{o}}}}$ is injective.

By Theorem 3.4.2, then, R is injective.

Because X is a doubly transitive G-space, we know from our remarks above that the orbits of X under $G_{\mathbf{o}}$ must be $X_1 = \{\mathbf{o}\} = \{1\}$ and $X_2 = X - \{\mathbf{o}\} = \{2, 3, \cdots, n\}$. By the results, then, of Theorem 3.3.1, $\ell^2(X) = E_1 \oplus E_2$, as $r = 2$, in the notation of that theorem. Because these two subspaces of $\ell^2(X)$ are both G-invariant, the weight space E_1 comprises the set of all constant functions and E_2, the set of all functions that sum to zero, or, in symbols,

$$E_2 = \{\phi \in \ell^2(X) : \sum_{x \in X} \phi(x) = 0\}.$$

Because $\ell^2(X)$ is the orthogonal sum $E_1 \oplus E_2$, to see that E_2 is as we have described, we must simply show that E_2 is orthogonal to E_1. To that end, let ϕ_0 be in E_2 and consider

$$0 = \langle \phi_0, 1 \rangle = \sum_{x \in X} \phi_0(x),$$

which implies that E_2 is, indeed, the set of functions that sum to zero.

Certainly, as E_1 is the set of constant functions on X, we have that $p_1(x) \equiv 1$ is the spherical function corresponding to E_1. Furthermore, the spherical function of E_2 will be of the form

$$p_2(x) = \begin{cases} 1 & x = 1 \\ C_2 & x \neq 1 \end{cases}, \quad \text{where } C_2 = \frac{-1}{|X| - 1}.$$

That $p_2(x)$ is the spherical function of E_2 follows easily from

$$\begin{aligned} 0 &= p(1) + p(2) + \cdots + p(|X|) \\ &= 1 + (|X| - 1)C_2, \end{aligned}$$

which gives us the value for C_2. The orthogonal projections of $\ell^2(X)$ onto E_1 and E_2 we claim, respectively, are

$$\pi_1\phi(x) = \frac{1}{|X|}\sum_{y\in X}\phi(y)$$

and

$$\pi_2\phi(x) = \phi(x) - \frac{1}{|X|}\sum_{y\in X}\phi(y),$$

the latter projection following because, as π_1 and π_2 are orthogonal projections, we can decompose ϕ into $\pi_1\phi + \pi_2\phi$; thence, $\phi = \pi_1\phi + \pi_2\phi$. Solving for $\pi_2\phi$ gives us

$$\pi_2\phi(x) = \phi(x) - \pi_1\phi(x) = \phi(x) - \frac{1}{|X|}\sum_{y\in X}\phi(y),$$

with substitution of π_1 from above justifying the latter equality. We next give the image of the spherical functions, $p_1(x)$ and $p_2(x)$, under the Radon transform R : namely,

$$(Rp_1)(S) = \sum_{x\in S} p_1(x) = |S| = k$$

and

$$(Rp_2)(S) = \sum_{x\in S} p_2(x) = \begin{cases} 1 + (k-1)C_2 & 1 \in S \\ kC_2 & 1 \notin S \end{cases}.$$

There exists, as well, a natural adjoint of the Radon transform R. Define $R^* : \ell^2(Y) \mapsto \ell^2(X)$ by

$$(R^*F)(x) = \sum_{S\ni x} F(S),$$

if ϕ is in $\ell^2(X)$ and F is in $\ell^2(Y)$, for

$$\begin{aligned}\langle \phi, R^*F\rangle &= \sum_{x\in X}\phi(x)\overline{(R^*F)(x)} \\ &= \sum_{x\in X}\phi(x)\overline{\sum_{S\ni x}F(S)}\end{aligned}$$

$$
\begin{aligned}
&= \sum_{S \ni x} \sum_{x \in X} \phi(x) \overline{F(S)} \\
&= \sum_{S \ni x} (R\phi) \overline{F(S)} = \langle R\phi, F \rangle.
\end{aligned}
$$

Finally, we claim that the image of p_1 and p_2 under the adjoint, R^*, evaluated at 1 are

$$
\begin{aligned}
(R^* Rp_1)(1) &= \sum_{S \ni 1} (Rp_1)(S) \\
&= \sum_{S \ni 1} k, \quad \text{from our work above,} \\
&= \binom{|X| - 1}{k - 1} k
\end{aligned}
$$

and

$$
\begin{aligned}
(R^* Rp_2)(1) &= \sum_{S \ni 1} (Rp_2)(S) \\
&= \binom{|X| - 1}{k - 1} \left[1 + (k-1) C_2 \right].
\end{aligned}
$$

4.3. The Radon Transform for Doubly Transitive Actions

Notice that in the example above of the Radon transform on the space $X = \{1, \cdots, n\}$, we used no special characteristics of S_n or X other than that X is doubly transitive under the action of S_n. Therefore, the resulting decomposition of $\ell^2(X)$ into weight spaces, the spherical functions, and the adjoint of the Radon transform all generalize nicely as follows. We will omit some of the details, inasmuch as many of these specifics are directly analogous to those in the special case outlined above.

Let X be any doubly transitive G-space and let $G_{\mathbf{o}}$ be as before for a fixed origin, $\mathbf{o}$. Then, again, $G_{\mathbf{o}}$ has two orbits, $X_1 = \{\mathbf{o}\}$ and $X_2 = X - \{\mathbf{o}\}$, and from the

Cartan-Gel′fand Theorem, that is Theorem 3.3.1, $\ell^2(X) = E_1 \oplus E_2$, and, once more,

$$E_1 = \{\phi \in \ell^2(X) : \phi(x) = c_0 \text{ for all } x \in X\},$$

where c_0 is a constant—that is, E_1 is the set of all constant functions—and

$$E_2 = \{\phi \in \ell^2(X) : \sum_{x \in X} \phi(x) = 0\}.$$

Then the spherical functions are, as above,

$$p_1(x) \equiv 1$$

and

$$p_2(x) = \begin{cases} 1 & x = \mathbf{o} \\ C_2 & x \neq \mathbf{o} \end{cases}, \quad \text{where } C_2 = \frac{-1}{|X| - 1}.$$

Furthermore, the orthogonal projections of $\ell^2(X)$ onto E_1 and E_2 are given exactly as above by, respectively,

$$\pi_1\phi(x) = \frac{1}{|X|} \sum_{y \in X} \phi(y)$$

and

$$\pi_2\phi(x) = \phi(x) - \frac{1}{|X|} \sum_{y \in X} \phi(y).$$

Let L_0 be a nonempty subset of X other than X itself, and let $\overline{X} = \{gL_0 : g \in G\}$ be the set of G-translates of L_0. If $\overline{K} = \{g \in G : gL_0 = L_0\}$, then $|\overline{X}| = |G||\overline{K}|$, as $G/\overline{K} \cong \overline{X}$.

There exists, then, a natural Radon transform $\boldsymbol{R} : \ell^2(X) \mapsto \ell^2(\overline{X})$ given by

$$(\boldsymbol{R}\phi)(L) = \sum_{x \in L} \phi(x).$$

Furthermore, $\boldsymbol{R}$ has a dual transformation $\boldsymbol{R}^* : \ell^2(\overline{X}) \mapsto \ell^2(X)$ defined by

$$(\boldsymbol{R}^*F)(x) = \sum_{L \ni x} F(L).$$

In this case, we remark that $\boldsymbol{R}^*$ is the adjoint of $\boldsymbol{R}$ in the following sense:

$$\langle \boldsymbol{R}\phi, F\rangle_{\ell^2(\overline{X})} = \sum_{x \in L} \phi(x)\overline{F(L)} = \langle \phi, \boldsymbol{R}^*F\rangle_{\ell^2(X)}.$$

Therefore, $\boldsymbol{R}$ is injective if and only if $\boldsymbol{R}^*$ is surjective.

The image of the spherical functions, p_1 and p_2, under $\boldsymbol{R}$ is

$$(\boldsymbol{R}p_1)(L) = \sum_{x \in L} p_1(x) = |L| = |L_0|$$

and

$$(\boldsymbol{R}p_2)(L) = \sum_{x \in L} p_2(x) = \begin{cases} \dfrac{|X| - |L_0|}{|X| - 1} & \mathbf{o} \in L \\ \\ \dfrac{-|L_0|}{|X| - 1} & \mathbf{o} \notin L \end{cases}$$

If x is in X, let $m = |\{L \in \overline{X} : x \in L\}|$ be the number of elements of $\overline{X}$ that contain x. Then by counting the pairs (x, L) with x in L in two ways—that is, first summing on x and then L, or *vice versa*, we have

$$m = \frac{|L_0||\overline{X}|}{|X|}.$$

Then the images of $\boldsymbol{R}p_1$ and $\boldsymbol{R}p_2$ under $\boldsymbol{R}^*$ are

$$\boldsymbol{R}^*\boldsymbol{R}p_1(\mathbf{o}) = m|L_0|$$

and

$$\boldsymbol{R}^*\boldsymbol{R}p_2(\mathbf{o}) = m\frac{|X| - |L_0|}{|X|}.$$

As the operator $\boldsymbol{R}^*\boldsymbol{R}$ is G-invariant, if we apply the results of Theorem 3.4.2, we establish

THEOREM 4.3.1. let X be a doubly transitive G-space. Then the Radon transform $\boldsymbol{R} : \ell^2(X) \mapsto \ell^2(\overline{X})$ is injective and any ϕ in $\ell^2(X)$ we can recover from $\boldsymbol{R}\phi$ by

$$\phi = \frac{1}{m}\left(\frac{1}{|L_0|}\pi_1\boldsymbol{R}^* + \frac{|X|}{|X| - |L_0|}\pi_2\boldsymbol{R}^*\right)\boldsymbol{R}\phi,$$

where

$$m = \frac{|L_0||\overline{X}|}{|X|}$$

and $\pi_1 : \ell^2(X) \mapsto E_1$ and $\pi_2 \mapsto E_2$ are orthogonal projections. By duality, the transform $\boldsymbol{R}^* : \ell^2(\overline{X}) \mapsto \ell^2(X)$ is surjective.

Bibliography

1. E. D. Bolker, *The finite radon transform*, Integral Geometry (R. L. Bryant *et al.,* eds., ed.), Contemporary Mathematics, vol. 63, Amer. Math. Soc., Providence, Rhode Island, 1987, pp. 27–49.
2. E. D. Bolker, E. Grinberg, and J. P. S. Kung, *Admissible complexes for the combinatorial Radon transform. A progress report*, Integral geometry and tomography (Arcata, CA, 1989), Contemp. Math., vol. 113, Amer. Math. Soc., Providence, RI, 1990, pp. 1–3.
3. Jan Boman, Ethan D. Bolker, and Patrick O'Neil, *The combinatorial Radon transform modulo the symmetric group*, Adv. in Appl. Math. **12** (1991), no. 4, 400–411. MR **92m:**05014
4. John B. Conway, *A course in functional analysis*, second ed., Springer-Verlag, New York, 1990. MR **91e:**46001
5. A. M. Cormack, *Computed tomography: some history and recent developments*, Computed tomography (Cincinnati, Ohio, 1982), Amer. Math. Soc., Providence, R.I., 1982, pp. 35–42. MR **84g:**92006
6. Richard A. DeMillo, George I. Davida, David P. Dobkin, Michael A. Harrison, and Richard J. Lipton, *Applied cryptology, cryptographic protocols, and computer security models*, American Mathematical Society, Providence, RI, 1983, Lecture notes prepared for the American Mathematical Society short course held in San Francisco, Calif., Jan. 5–6, 1981, AMS Short Course Lecture Notes. MR **86g:**68002
7. P. Diaconis and R. L. Graham, *The radon transform on* ${\mathbf{Z}_2}^k$, Pacific Jour. Math. **118** (1985), 323–345.
8. William Fulton and Joe Harris, *Representation theory*, Springer-Verlag, New York, 1991, A first course, Readings in Mathematics. MR **93a:**20069
9. I. M. Gel′fand and S. G. Gindikin (eds.), *Mathematical problems of tomography*, American Mathematical Society, Providence, RI, 1990, Translated from the Russian by S.Gel′fand fand, Translation edited by A. Sossinsky [A. B. Sosinskiĭ]. MR **91k:**44001

10. E. Grinberg, *The admissibility theorem for the hyperplane transform over a finite field*, Jour. Combin. Theory Ser. A **53** (1990), 316–320.

11. Paul R. Halmos, *Finite-dimensional vector spaces*, second ed., Springer-Verlag, New York, 1974, Undergraduate Texts in Mathematics. MR 53 #13258

12. Kenneth Hoffman and Ray Kunze, *Linear algebra*, Prentice-Hall Inc., Englewood Cliffs, N.J., 1971. MR 43 #1998

13. R. Howard, *Radon transforms and spherical functions on finite homogeneous and symmetric spaces*, Unpublished set of notes.

14. J. P. S. Kung, *The radon transformations of a combinatorial geometry*, Jour. Combin. Theory Ser. A **26** (1979), 97–102.

15. ______, *Radon transforms in combinatorics and lattice theory*, Combinatorics and ordered sets (Arcata, Calif., 1985), Contemp. Math., vol. 57, Amer. Math. Soc., Providence, R.I., 1986, pp. 33–74.

16. Serge Lang, *Linear algebra*, third ed., Springer-Verlag, New York, 1989. MR **90b:**15001

17. ______, *Real and functional analysis*, third ed., Springer-Verlag, New York, 1993. MR **94b:**00005

18. Johann Radon, *Über die bestimmung von funktionen durch ihre integralwerte längs gewisser mannigfaltigkeiten*, Computed tomography (Cincinnati, Ohio, 1982), Amer. Math. Soc., Providence, R.I., 1982, pp. 71–86. MR **84g:**92006

19. Joseph J. Rotman, *An introduction to the theory of groups*, fourth ed., Springer-Verlag, New York, 1995. MR **95m:**20001

20. Lawrence A. Shepp (ed.), *Computed tomography*, American Mathematical Society, Providence, R.I., 1982, Lecture notes prepared for the American Mathematical Society Short Course held in Cincinnati, Ohio, January 11–12, 1982. MR **84b:**92012