THE UNIVERSITY OF QUEENSLAND

AUSTRALIA

Optimizing performance in Gaussian Processes

Michael Ciccotosto-Camp

Supervisor: Fred (Farbod) Roosta
Co-Supervisors: Andries Potgieter
Yan Zhao

Bachelor of Mathematics (Honours)
June 2022

The University of Queensland
School of Mathematics and Physics

Contents

Acknowledgements

I would like to deeply thank my supervisor Dr. Masoud Kamgarpour for his advice and all of his time spent with me. I consider myself lucky and am glad to have been his student for my honours year. I would also like to thank my co-supervisor Dr. Anna Puskás for the same reasons. A special thanks to Dr. Valentin Buciumas for his time spent teaching me while he was at The University of Queensland.

Introduction

Origins of group theory. The mathematical field of group theory has its origins in the early 19th century. At the time, mathematicians were investigating the solutions to polynomial equations. That is, solutions to equations of the form

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0.$$

Full solutions to polynomial equations of low degrees (i.e. $n \leq 4$) had already been formulated [Rig96]. These include the familiar *quadratic formula*, which has been known since antiquity. The formula tells us that the solutions to a general quadratic equation $ax^2 + bx + c = 0$ are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The full solutions to any cubic $(n = 3)$ or quartic $(n = 4)$ polynomial equation were also known. These are given by the lesser-known Cardano's formula and Ferrari's method, respectively. We say that a polynomial is *solvable by radicals* if one can write all of its solutions in terms of its coefficients combined with the algebraic operations; addition, subtraction, multiplication, division, powers and radicals (i.e. k^{th} roots).

In the 1830s, the mathematician Évariste Galois provided an elegant method to prove that a general polynomial of degree $n \geq 5$ is not solvable by radicals. Galois understood that to every polynomial one could associate a *Galois group*, a new mathematical object at the time. The Galois group was the first object in a class of mathematical objects that we call *groups* today. We say that the pair $(G, \circ)$ is a group, where G is a set and $\circ\colon G \times G \to G$ is a binary operation on G, when three conditions are satisfied:

- Associativity: $g \circ (h \circ k) = (g \circ h) \circ k$ for all $g, h, k \in G$.
- Existence of an identity: there exists some $1_G \in G$ such that $1_G \circ g = g \circ 1_G = g$ for all $g \in G$.
- Existence of inverses: for every $g \in G$, there exists some $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = 1_G$.

Examples of groups that are likely familiar to the reader include $(\mathbb{Z}, +)$, the integers under addition, $(\mathbb{R}^+, \times)$, the positive real numbers under multiplication, and $(\mathbb{Z}/n\mathbb{Z}, +)$, the integers modulo n under addition. Some geometric examples of groups are the *dihedral groups*. These groups are generated by the m symmetries associated to the regular m-sided polygon (i.e. a polygon with all interior angles and all side lengths the same). Then each dihedral group contains $2m$ elements (m reflections and m rotations) with the group operation of composition of reflections and rotations.

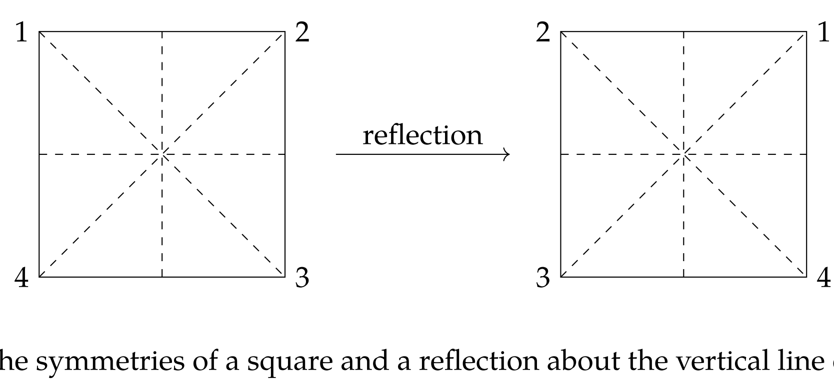

Figure 1. The symmetries of a square and a reflection about the vertical line of symmetry.

This gives us an intuitive understanding of groups: they encode the symmetries of mathematical objects.

What is representation theory? The study of groups yields insight into geometric objects. The action of the dihedral group on the m-gon serves as example of a group acting on a geometric object. More generally, we can consider the action of a group on some object. Specifically, we say that a group G *acts* on a set X if, for each $g \in G$, there is a map $\cdot\colon G \times X \to X$ satisfying $1_G \cdot x = x$ and $g \cdot (h \cdot x) = (gh) \cdot x$ for all $x \in X$. Alternatively, one can view this as a group homomorphism $\rho\colon G \to \mathrm{Sym}(X)$, where $\mathrm{Sym}(X)$ is the symmetric group associated to X, i.e. the group of permutations of elements of X.

Now we linearise the setting above by requiring that $X = V$ is a *vector space*. Then we say that G acts *linearly* on V if there exists a group homomorphism $\rho\colon G \to \mathrm{GL}(V)$. We call (V, ρ) a *representation* of G, and ρ is often suppresed from notation. We see that G acts on V in the sense that $\rho(g)\colon V \to V$ is a linear invertible map on V. We may denote $\rho(g)(v)$ by $g \cdot v$ as before.

Representation theory is concerned with understanding and classifying linear actions of groups. The general situation of representation theory is as follows. If the group G acts on a vector space V, then we say that a vector subspace $W \subseteq V$ is a *subrepresentation* of V if it is invariant under the action of G. A representation is called *irreducible* if its only proper subrepresentation is the trivial representation $W = \{0\}$. The primary goals of representation theory are finding all irreducible representations of G, and to decompose a given representation into its irreducible components.

We can think of irreducible representations as the building blocks of all other representations. This is a common idea in mathematics, seen in other areas. For instance, in number theory, the building blocks of integers are primes and, in group theory, the building blocks of groups are simple groups.

Writing a general representation in terms of irreducible components is not always possible. We call a representation *decomposable* if we can write it as the direct sum of irreducible representations. A lot can be said about the case where the representation of a finite group is over a field whose characteristic not dividing the order of the group. In this case, *Maschke's theorem* tells us that these representations are always decomposable [Lan02]. In particular, complex representations of a finite group are always decomposable.

Gelfand Pairs. Henceforth, we assume some knowledge of abstract algebra from the reader. Let G be a finite group and $K \leq G$ a subgroup. The pair (G, K) is called a *Gelfand pair* if the induced representation $\mathrm{Ind}_K^G \mathbf{1}$ is multiplicity-free. Here $\mathbf{1}$ denotes the trivial (1-dimensional) complex representation of K, and multiplicity-free means that any irreducible representation appears in the decomposition of $\mathrm{Ind}_K^G \mathbf{1}$ at most once (up to isomorphism).

Gelfand pairs play an important role in representation theory [Mus93], analysis [Kor80, Mor18], combinatorics [BI84], number theory [Gro91, Ter99] and probability [CSST20, Dia88]. One of our objectives is to give a detailed study of Gelfand pairs of finite groups. A main theorem of this thesis is the following:

Theorem 1. (*Gelfand's Trick*) *Let G be a finite group and K a subgroup of G. Suppose $\varphi\colon G \to G$ is an involutive anti-automorphism (i.e. a bijective anti-homomorphism) such that $K\varphi(x)K = KxK$ for all $x \in G$. Then (G, K) is a Gelfand pair.*

The theorem above is proved using the *Hecke algebra*. There are multiple constructions of Hecke algebras in the literature [CMHL03, CSST20].

Types of Hecke algebras. Another objective of this thesis is to present these a priori different Hecke algebras and resolve their apparent discrepancies. For instance, one way to define the Hecke algebra is as a convolution algebra of K-bi-invariant complex-valued functions $f\colon G \to \mathbb{C}$ on a group. Another way to define the Hecke algebra is as the algebra generated by $n-1$ variables $T_1, \ldots T_{n-1}$ subject to a *quadratic relation* $T_i^2 = (q-1)T_i + q$ and a *braid relation*

$$\underbrace{T_iT_jT_i\ldots}_{m_{ij}\text{ terms}} = \underbrace{T_jT_iT_j\ldots}_{m_{ij}\text{ terms}}.$$

Here m_{ij} is the ij^{th} entry in the *Coxeter matrix* associated to the *Weyl group* of G. The name 'braid relation' is due to a method of visualising the *symmetric group S_n*. If n is a positive integer then the group S_n is the collection of bijections on the set $\{1, 2, \ldots, n\}$ to itself, with the group operation of composing functions. A natural method of visualising elements and multiplication in this group is via *braid diagrams*. For instance, if $\sigma = (1\ 2)(3\ 5\ 4)$ and $\pi = (1\ 2\ 4\ 6\ 5\ 3)$ are permutations in S_6 (written in cycle notation), then we may visualise these elements and their product $\pi\sigma = (1\ 4)(5\ 6)$ in the following manner:

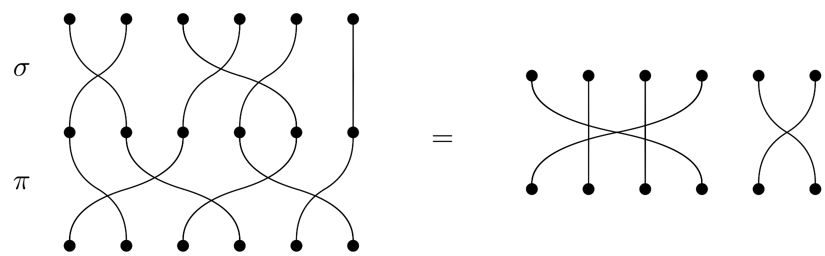

FIGURE 2. A braid diagram visualising the multiplication $\pi\sigma = (1\ 4)(5\ 6)$.

Why study Hecke algebras? The Hecke algebra arises naturally when one wishes to compute certain irreducible representations of a group [RW21, CMHL03]. Consider a finite group G and a normal subgroup $N \triangleleft G$. If G acts linearly on a vector space V (i.e. V is a representation of G), then there is a natural action of G on the subrepresentation V^N, the space of vectors in V that are fixed by N. Under this action, N will clearly act trivially on V^N. This yields a representation of the quotient group G/N. After some representation theoretic arguments, one arrives at the conclusion that

$$\left\{\begin{array}{c}\text{Irreducible representations}\\ \text{of } G \text{ with } N\text{-fixed vectors}\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c}\text{Irreducible representations}\\ \text{of } G/N\end{array}\right\}.$$

It is a straightforward exercise that a complex representation of the group G/N is the same as a representation of the algebra $\mathbb{C}[G/N]$, the *group algebra* of G/N.

What happens when we do not require a normal subgroup of G? Consider an arbitrary subgroup K of a finite group G. Now G/K is no longer necessarily a group, so G/K and $\mathbb{C}[G/K]$ no longer necessarily make sense. We ask ourselves: what acts on V^K? The action of G on V is not well-defined on V^K since K is no longer normal. It is not obvious how we could study irreducible G-representations with K-fixed vectors. We are able to salvage the situation with the help of the Hecke algebra.

For $g \in G$, define the Hecke operator $[KgK] := \frac{1}{|K|}\sum_{x\in KgK} x \in \mathbb{C}[G]$, which acts on V^K by

$$[KgK]\cdot v := \frac{1}{|K|}\sum_{x\in KgK} x\cdot v.$$

Now define the Hecke algebra $\mathcal{H}(G,K)$ to be the space of functions $f\colon G\to\mathbb{C}$ that are constant on K-double cosets. The indicator functions χ_{KgK} form a basis of this space and we can uniquely associate the indicator functions χ_{KgK} to the Hecke operators $[KgK]$. We see that, through the Hecke operators, we have defined an action of $\mathcal{H}(G,K)$ on V^K. This answers our question of what acts on V^K. Through another representation-theoretic exercise, one can conclude that

$$\left\{\begin{array}{c}\text{Irreducible representations}\\ \text{of } G \text{ with } K\text{-fixed vectors}\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c}\text{Irreducible representations}\\ \text{of } \mathcal{H}(G,K)\end{array}\right\}.$$

An immediate example of the utility of this result is as follows. It is easy to show that if $\mathcal{H}(G,K)$ is commutative, then all of its irreducible finite-dimensional representations are one-dimensional [EGH+11]. The commutativity of the Hecke algebra turns out to be an important property which will be investigated throughout this thesis.

Contents of this thesis. In Chapter 1, we begin our study of the Hecke algebra. First, we investigate the convolution algebra of all complex-valued functions on G and its ideal of K-right-invariant complex-valued functions. This is followed by results describing the relationship between the induced representation and its associated Hecke algebra. We use these results to prove Theorem 1. This allows us to write down simple proofs that $\mathrm{Ind}_K^G \mathbf{1}$ is multiplicity-free for certain choices of G and K. Namely, (G,K) with G commutative, (G,K) with $[G\colon K]=2$, $(S_{n+m}, S_n\times S_m)$, and $(O_{n+1}(\mathbb{F}_q), O_n(\mathbb{F}_q))$ for q odd.

In Chapter 2, we generalise the discussion of Chapter 1 to the case of a non-trivial *character* $\sigma\colon K\to\mathbb{C}^\times$. Here our goal is to obtain a twisted analogue of Theorem 1. To this end, we describe the basis of the Hecke algebra using the idea of *relevant orbits*. We state and prove the generalisation of Theorem 1. We apply the new theorem to a particular representation, the *Gelfand–Graev representation* of $\mathrm{GL}_n(\mathbb{F}_q)$, to show that it is multiplicity-free.

In Chapter **??**, we investigate the Hecke algebra of Chapter 1 under the particular choice of $G=\mathrm{SL}_n(\mathbb{F}_q)$ and $K=B(\mathbb{F}_q)$, the *Borel subgroup* of G, i.e. the subgroup of upper-triangular matrices. The *Weyl group* associated to G is introduced and shown to be isomorphic to S_n. Next, we perform some elementary matrix calculations which yields the surprising result above: the Hecke algebra may be written in terms of $n-1$ generators subject to the quadratic relation and the braid relations associated to W. This leads to a concluding discussion of Hecke algebras generated by any finite *Coxeter group*.

In Chapter **??**, we generalise the results of earlier chapters to the case where G is no longer finite, but instead a locally compact topological group. This allows for an extension of the theory we have developed to more general groups and their Hecke algebras. To do this, we discuss how one can impose a topological structure on a group and supply examples to give some intuition for these types of groups. To define Hecke algebras of these groups, we require some measure theory. In particular, the convolution product on the Hecke algebra is defined in terms of an integral with respect to the *Haar measure*. We spend some time developing the theory of Haar measures for this purpose. We conclude with a discussion of how to recover the Hecke algebra of a finite group from this new definition. In this chapter, we shall denote the Hecke algebra by $C_c(K\backslash G/K)$ to emphasise the non-finiteness of G.

In Chapter **??**, we take a look at some specific Hecke algebras of locally compact topological groups. In particular, we restrict our attention to the general linear group over a non-archimedean local field k and its ring of integers $\mathcal{O}$. We look at the *Spherical Hecke algebra*, formed when one considers $G = \mathrm{GL}_n(k)$ and $K = K^\circ := \mathrm{GL}_n(\mathcal{O})$, and the *Iwahori–Hecke algebra*, formed when one considers $G = \mathrm{GL}_n(\mathcal{O})$ and $K = I$, the *Iwahori subgroup*. In order to investigate these algebras, we must develop an understanding of these fields. We detail their definition, classification and structure.

The contents of this thesis may be visualised with the following diagram.

$$\begin{tikzcd}
\underset{}{\overset{\text{Ch. 2}}{\mathcal{H}(G,K,\sigma)}} \arrow[r, "\sigma=\mathbf{1}"] & \overset{\text{Ch. 1}}{\mathcal{H}(G,K)} \arrow[d, "\substack{G \text{ Lie type} \\ \text{over } \mathbb{F}_q}"] & \overset{\text{Ch. ??}}{C_c(K\backslash G/K)} \arrow[l, "G \text{ finite}"'] \arrow[r, "K=I"] \arrow[d, "K=K^\circ"] & \overset{\text{Ch. ??}}{C_c(I\backslash G/I)} \\
& \underset{\text{Ch. ??}}{\mathcal{H}_q(W,S)} & \underset{\text{Ch. ??}}{C_c(K^\circ\backslash G/K^\circ)} &
\end{tikzcd}$$

FIGURE 3. The relationship diagram of this thesis.

Directions for future research. We assume the reader is familiar with the contents of this thesis. The modern study of Hecke algebras is largely focused on the *Iwahori–Hecke algebra*, which is also known as the *affine Hecke algebra*. This algebra is central to the study of representations of *reductive groups* over non-archimedean local fields (e.g. groups such as GL_n, SL_n, Sp_{2n} over fields such as $\mathbb{Q}_p$ or $\mathbb{F}_q(\!(t)\!)$).

Some topics relevant to the Iwahori–Hecke algebra include *Bernstein's presentation*, the *Iwahori–Matsumoto presentation* and the *Satake isomorphism* [HKP09]. Properties of the Iwahori–Hecke algebra such as these presentations may be viewed as a consequence of the *universal unramified principal series module*, which we now describe.

Fix a "nice" (i.e. split and connected) reductive group G (e.g. SL_n) over a non-archimedean local field k with ring of integers $\mathcal{O}$. Then write A to mean a *split maximal torus* of G and write N to mean the *unipotent radical* of a Borel subgroup of G that contains A. Also recall I is the Iwahori subgroup of G given in Chapter **??**.

The universal unramified principal series module M is given by $C_c(A(\mathcal{O})N\backslash G/I)$. It is a right module over the Iwahori–Hecke algebra under convolution. Furthermore, a basis of the Iwahori–Hecke algebra is parameterised by the *affine Weyl group* $\widetilde{W}$. We may write $\widetilde{W} \cong W \ltimes \Lambda^\vee$, where $\Lambda^\vee$ is the *coroot lattice* of G. Then $\mathbb{C}[\Lambda^\vee]$ is the corresponding group algebra over $\mathbb{C}$. Then M is also a left module over $\mathbb{C}[\Lambda^\vee]$.

The aim of this chapter is to study the structure of the Hecke algebra and elucidate its significance in the representation theory of G.

In Section 1.1, we introduce $(\mathrm{Fun}(G), \star)$, the convolution algebra of functions from G to $\mathbb{C}$. In Section 1.2, we present and discuss the induced representation $\mathrm{Ind}_K^G \mathbf{1}$ and its underlying vector space, W. In Section 1.3, we introduce the Hecke algebra, $\mathcal{H}(G, K)$. This is the space of functions that are constant on K-double cosets. In Section 1.4, we present the group algebra $\mathbb{C}[G]$, which is isomorphic to $\mathrm{Fun}(G)$, and describe the copies of W and $\mathcal{H}(G, K)$ that lie inside of $\mathbb{C}[G]$. In Section 1.5, we make the fundamental observation that $\mathcal{H}(G, K) \cong \mathrm{End}_G(W)$, the endomorphism algebra of G-intertwiners on W. This is crucial for the final section, Section 1.6, where we prove that a representation V is multiplicity-free if and only if $\mathrm{End}_G(V)$ is commutative. This lets us conclude that the induced representation W is multiplicity-free if and only if its associated Hecke algebra is commutative.

The purpose of Section 1.7 is to develop a tool to expedite the process of proving $\mathcal{H}(G, K)$ is commutative. This tool comes in the form of Gelfand's Trick, which transforms the task of proving commutativity into the task of writing down an involutive anti-automorphism of G that preserves K-double cosets. We will see that this is a much easier task to perform. To prove Gelfand's Trick, we investigate the behavior of anti-automorphisms on G and $\mathrm{Fun}(G)$. As we do this, the required conditions for Gelfand's Trick reveal themselves, leading to a natural statement and proof. We conclude with some examples of applications of the main theorem in Section 1.8.

1.1. **The convolution algebra of functions** $\mathrm{Fun}(G)$**.** Let X be a finite set. Denote the vector space of complex-valued maps on X by $\mathrm{Fun}(X) := \{f \colon X \to \mathbb{C}\}$. It has a basis of delta functions $\{\delta_x\}_{x \in X}$ defined by $\delta_x(x) = 1$ and $\delta_x(y) = 0$ for $y \neq x$. Note that $\mathrm{Fun}(X)$ is a commutative unital associative algebra under pointwise multiplication of functions. Also note that if a group G acts on X, then G also acts on $\mathrm{Fun}(X)$ by $(g \cdot f)(x) := f(g^{-1} \cdot x)$. Thus, $\mathrm{Fun}(X)$ is a representation of G.

Now suppose that $X = G$ is a finite group. The group structure on G yields a second algebra structure on $\mathrm{Fun}(G)$. Specifically, it has the convolution product defined by

$$(f \star f')(x) := \sum_{yz = x} f(y) f'(z) = \sum_{g \in G} f(xg) f'(g^{-1}).$$

One can show that $\star$ is associative with identity δ_{1_G}, so $(\mathrm{Fun}(G), \star)$ is a unital associative algebra. It is easy to see that this algebra is commutative if and only if G is commutative.

1.2. **The induced representation** $\mathrm{Ind}_K^G \mathbf{1}$**.** Consider the space of functions in $\mathrm{Fun}(G)$ that are invariant under right-multiplication by elements of K. Explicitly, this space is defined by

$$W := \{f \colon G \to \mathbb{C} \mid f(gk) = f(g),\ \forall g \in G, \forall k \in K\} \subseteq \mathrm{Fun}(G).$$

Note that the action of G on $\mathrm{Fun}(G)$ leaves W invariant. The resulting action of G on W is called the *induced representation* and denoted $\mathrm{Ind}_K^G \mathbf{1}$. When $K = \{1\}$, the representation $\mathrm{Ind}_{\{1\}}^G \mathbf{1} = \mathrm{Fun}(G)$ is the *left regular* representation of G. For future use, we prove the following lemma.

Lemma 2. *The space W is a left ideal of* $(\mathrm{Fun}(G), \star)$.

Proof. We verify that $f \star w \in W$ whenever $w \in W$ and $f \in \mathrm{Fun}(G)$. Let $g \in G$ and $k \in K$. Then

$$\begin{aligned}(f \star w)(gk) &= \sum_{xy=gk} f(x)w(y) = \sum_{x \in G} f(x)w(x^{-1}gk) \\ &= \sum_{x\in G} f(x)w(x^{-1}g) = \sum_{xy=g} f(x)w(y) = (f \star w)(g). \qquad \square\end{aligned}$$

1.3. **The Hecke algebra of a finite group $\mathcal{H}(G, K)$.** Consider the space of functions in $\mathrm{Fun}(G)$ that are invariant under right- and left-multiplication by elements of K. Explicitly, this space is defined by

$$\mathcal{H}(G,K) := \{f \colon G \to \mathbb{C} \mid f(k_1 g k_2) = f(g),\ \forall g \in G,\ \forall k_1, k_2 \in K\} \subseteq \mathrm{Fun}(G).$$

This is the *Hecke algebra* associated to G and K and we will write $\mathcal{H}$ to mean $\mathcal{H}(G,K)$ when there is no ambiguity. The proof of Lemma 2 can be adapted to show that $\mathcal{H}$ is a two-sided ideal in $(\mathrm{Fun}(G), \star)$. Notice that the identity of $(\mathrm{Fun}(G), \star)$ does not lie in $\mathcal{H}$. Nevertheless, $\mathcal{H}$ does have an identity of its own. It is easy to verify that the identity is ι_K, which we define below.

$$\iota_K : G \to \mathbb{C}, \quad \iota_K(g) := \begin{cases} \frac{1}{|K|}, & \text{if } g \in K, \\ 0, & \text{else.} \end{cases}$$

We see that ι_K is an idempotent element, since $(\iota_K \star \iota_K)(g) = 0$ for $g \notin K$, and

$$(\iota_K \star \iota_K)(k) = \sum_{x \in G} \iota_K(kx)\iota_K(x^{-1}) = \sum_{x \in K} \frac{1}{|K|^2} = \frac{1}{|K|}$$

for $k \in K$.

This is a special case of a more general situation: if R is a ring and e is an idempotent, then eRe will be a ring in which e serves as a unit. This is clear since $eree = ere = eere$ for all $ere \in eRe$. The ring eRe is sometimes called an *idempotented ring* or a *Pierce corner* [Bum10, Lam03].

We present a basis for $\mathcal{H}$. For $KxK \in K\backslash G/K$, the K-double cosets in G, we define

$$\chi_{KxK}(y) := \begin{cases} 1, & \text{if } y \in KxK, \\ 0, & \text{else.} \end{cases}$$

Recall that double cosets partition G so there is no ambiguity in this definition. We call χ_{KxK} the *characteristic function* of the K-double coset KxK. As an abuse of notation for the sake of brevity, we will denote this family by $\{\chi_x\}_{x \in G}$, where x ranges over the K-double coset representatives as written above.

It is not hard to see that the characteristic functions form a basis of $\mathcal{H}$. By the definition of $\mathcal{H}$, we see characteristic functions span the space. To see that they're linearly independent, assume that

$$\alpha_1 \chi_{x_1} + \cdots + \alpha_n \chi_{x_n} = 0,$$

for some complete collection of K-double coset representatives $x_i \in G$ and scalars $\alpha_i \in \mathbb{C}$. Here 0 denotes the zero function $g \mapsto 0$ for all $g \in G$. Evaluating both sides at x_i tells us that $\alpha_i = 0$, so the only solution is the trivial solution and we have linear independence.

1.4. **The group algebra** $\mathbb{C}[G]$**.** We can associate to G another algebra, $\mathbb{C}[G]$, called the *group algebra* of G over $\mathbb{C}$. This algebra is defined by

$$\mathbb{C}[G] := \left\{ \sum_{g\in G} a_g e_g \;\middle|\; a_g \in \mathbb{C} \right\}.$$

Clearly, the set $\{e_g\}_{g\in G}$ serves as a basis of this space. We endow the space with a multiplication defined on basis elements by $e_g e_h := e_{gh}$. The following lemma illustrates the relevance of the group algebra.

Lemma 3. *The map $\Phi\colon \operatorname{Fun}(G) \to \mathbb{C}[G]$ defined on basis elements by $\delta_g \mapsto e_g$ and extended linearly is an algebra isomorphism.*

Proof. By construction, Φ is a linear map of vector spaces. It is also clear that this map is bijective since it is a bijection on basis elements. Thus Φ is a vector space isomorphism.

We need to check that Φ respects the algebra multiplication. This amounts to verifying that $\delta_g \star \delta_h = \delta_{gh}$. Notice that $(\delta_g \star \delta_h)(x) = \sum_{ab=x} \delta_g(a)\delta_h(b)$ is equal to 1 when $g = a$ and $h = b$, and 0 otherwise. This is exactly $\delta_{gh}(x)$. $\square$

We may ask ourselves: what is the image of the induced representation and the Hecke algebra inside of the group algebra? To answer this, we define the group algebra element

$$e := \frac{1}{|K|} \sum_{k\in K} e_k.$$

Note that e is an idempotent element. Then the following proposition answers our question.

Proposition 4. *(i) $\Phi(W) = \mathbb{C}[G]e$.*
(ii) $\Phi(\mathcal{H}) = e\mathbb{C}[G]e$.

Proof. (*i*) We begin by showing that $\mathbb{C}[G]e \subseteq \Phi(W)$. To see this, take an arbitrary element $(\sum_{g\in G} a_g e_g)e$ in $\mathbb{C}[G]e$. Then notice

$$\Big(\sum_{g\in G} a_g e_g\Big)e = \frac{1}{|K|}\Big(\sum_{g\in G} a_g e_g\Big)\Big(\sum_{k\in K} e_k\Big) = \frac{1}{|K|}\sum_{\substack{g\in G\\ k\in K}} a_g e_g e_k = \frac{1}{|K|}\sum_{\substack{g\in G\\ k\in K}} a_g e_{gk}.$$

Then we apply Φ^{-1} to see that

$$\frac{1}{|K|}\sum_{\substack{g\in G\\ k\in K}} a_g e_{gk} \mapsto \frac{1}{|K|}\sum_{\substack{g\in G\\ k\in K}} a_g \delta_{gk}.$$

We wish to show that this lies in W, so we wish to check that this map is invariant under right-multiplication by an element of K. To this end, let $g' \in G$, $k' \in K$ and apply $\frac{1}{|K|}\sum_{\substack{g\in G\\ k\in K}} a_g\delta_{gk}$ to $g'k'$. Note that $\delta_{gk}(g'k') = 1$ if and only if $gk = g'k'$ (and 0 otherwise). This is equivalent to $g = g'k'k^{-1}$. Thus

$$\frac{1}{|K|}\sum_{\substack{g\in G\\ k\in K}} a_g \delta_{gk}(g'k') = \frac{1}{|K|}\sum_{k\in K} a_{g'k'k^{-1}}\delta_{g'k'}(g'k') = \frac{1}{|K|}\sum_{k\in K} a_{g'k'k^{-1}}.$$

Similarly, we apply the map $\frac{1}{|K|}\sum_{\substack{g\in G\\k\in K}} a_g\delta_{gk}$ to g'. This yields

$$\frac{1}{|K|}\sum_{\substack{g\in G\\k\in K}} a_g\delta_{gk}(g') = \frac{1}{|K|}\sum_{k\in K} a_{g'k^{-1}}$$

Since right-multiplication by any element of K is an automorphism of G, we see that

$$\frac{1}{|K|}\sum_{k\in K} a_{g'k'k^{-1}} = \frac{1}{|K|}\sum_{k\in K} a_{g'k^{-1}},$$

which shows that $\mathbb{C}[G]e \subseteq \Phi(W)$. Conversely, take $f = \sum_{g\in G} a_g\delta_g \in W$. Let $g' \in G$, $k' \in K$ and notice that

$$a_{g'k'} = \sum_{g\in G} a_g\delta_g(g'k') = f(g'k') = f(g') = \sum_{g\in G} a_g\delta_g(g') = a_{g'}.$$

Then $a_{g'k'} = a_{g'}$ for any $g' \in G$ and $k' \in K$. Then observe

$$\begin{aligned}\Phi(f)e = \left(\sum_{g\in G} a_g\delta_g\right)\left(\frac{1}{|K|}\sum_{k\in K} e_k\right) &= \frac{1}{|K|}\sum_{\substack{g\in G\\k\in K}} a_g e_{gk} = \frac{1}{|K|}\sum_{\substack{g\in G\\k\in K}} a_{gk^{-1}} e_g \\ &= \frac{1}{|K|}\sum_{\substack{g\in G\\k\in K}} a_g e_g = \frac{1}{|K|}\sum_{k\in K}\sum_{g\in G} a_g e_g = \frac{1}{|K|}\sum_{k\in K}\Phi(f) = \Phi(f).\end{aligned}$$

Then $\varphi(f) = \varphi(f)e \in \mathbb{C}[G]e$, so $\Phi(W) \subseteq \mathbb{C}[G]e$ as required.

(ii) The proof is similar to that of (i). $\square$

1.5. **Identifying $\mathcal{H}(G,K)$ with the endomorphism algebra $\mathrm{End}_G(W)$.** For any representation V of G, define the space of *G-intertwining endomorphisms on V* by

$$\mathrm{End}_G(V) := \{f \in \mathrm{End}(V) \mid g\cdot f(v) = f(g\cdot v),\ \forall\, v\in V,\ g\in G\} \subseteq \mathrm{End}(V).$$

These are the endomorphisms of V that respect the action of G on V. It is easy to see that this is a vector space. It has the additional structure of a unital associative algebra when endowed with the product of endomorphism composition.

Now set V to be W, the induced representation of the trivial character from K to G, and define the linear map

$$\Psi\colon \mathcal{H} \to \mathrm{End}(W), \quad \alpha \mapsto (w \mapsto w\star\alpha).$$

Lemma 2 tells us that $w\star\alpha$ is indeed an element of W so the image of Ψ is indeed $\mathrm{End}(W)$. The following proposition highlights the significance of this map.

Proposition 5. *The map Ψ defines an algebra isomorphism $\mathcal{H} \cong \mathrm{End}_G(W)$.*

Proof. First we observe that $\Psi(\alpha)$ is indeed a G-intertwiner. Given $g,h\in G$ and $w\in W$, we have

$$\begin{aligned}(\Psi(\alpha)(g\cdot w))(h) = ((g\cdot w)\star\alpha)(h) &= \sum_{xy=h} w(g^{-1}x)\alpha(y) = \sum_{x\in G} w(g^{-1}x)\alpha(x^{-1}h) \\ &= \sum_{ab=g^{-1}h} w(a)\alpha(b) = (g\cdot(w\star\alpha))(h) = (g\cdot\Psi(\alpha)(w))(h).\end{aligned}$$

Thus, the image of Ψ lies in $\mathrm{End}_G(W)$. Next, we check that Ψ is an algebra isomorphism. Let $\alpha_1, \alpha_2 \in \mathcal{H}$ and observe

$$\Psi(\alpha_1 \star \alpha_2)(w) = w \star (\alpha_1 \star \alpha_2) = (w \star \alpha_1) \star \alpha_2 = \Psi(\alpha_1)(w) \star \alpha_2 = (\Psi(\alpha_1) \circ \Psi(\alpha_2))(w).$$

Thus Ψ is an algebra homomorphism. To see that Ψ is injective, we compute

$$\ker \Psi = \{\alpha \in \mathcal{H} \mid \Psi(\alpha)(w) = w\} = \{\alpha \in \mathcal{H} \mid w \star \alpha = w\} = \{\delta_{1_G}\}.$$

We see that Ψ has trivial kernel so it is injective. It is easy to see that surjectivity is a consequence of Theorem 13 in [Mur05] which also contains its proof. □

1.6. **Consequences for representation theory.** We prove a general property of representations. Namely, the decomposition of a representation is linked to its corresponding algebra of G-intertwining endomorphisms. We apply this to the induced representation W and Proposition 5 lets us conclude that W is multiplicity-free if and only if $\mathcal{H}$ is commutative.

First, suppose that V is a complex representation of G. Write $V = \bigoplus_{i=1}^n V_i$ as the decomposition of V into irreducible constituents, using Maschke's theorem. Notice that some of these V_i may be isomorphic to each other as G-representations. We group these mutually isomorphic irreducible representations together by writing

$$V = \bigoplus_{i=1}^n V_i = \bigoplus_{i=1}^n U_i^{\oplus m_i},$$

where m_i is the number of times U_i appears in the decomposition of V, henceforth referred to as the *multiplicity* of U_i in V. We say V is *multiplicity-free* if $m_i = 1$ for all i. The $U_i^{\oplus m_i}$ are called the *isotypical components* of V. We now prove the main proposition of this section.

Proposition 6. (*i*) *If V is a representation of G with the decomposition into isotypical components as above, then* $\mathrm{End}_G(V) \cong \bigoplus_{i=1}^n \mathrm{Mat}_{m_i}(\mathbb{C})$.

(*ii*) *V is multiplicity-free if and only if* $\mathrm{End}_G(V)$ *is commutative.*

Proof. (*i*) Observe that

$$\mathrm{End}_G(V) = \mathrm{Hom}_G(V_1 \oplus \cdots \oplus V_n, V_1 \oplus \cdots \oplus V_n) \cong \bigoplus_{i,j=1,\dots,n} \mathrm{Hom}_G(V_i, V_j).$$

Then we compute

$$\mathrm{Hom}_G(V_i, V_j) = \mathrm{Hom}_G(U_i^{\oplus m_i}, U_j^{\oplus m_j}) \cong \mathrm{Hom}_G(U_i, U_j)^{\oplus m_i m_j}.$$

Schur's lemma tells us that

$$\mathrm{Hom}_G(U_i, U_j) \cong \begin{cases} \mathbb{C}, & \text{if } U_i \cong U_j, \\ \{0\}, & \text{if } U_i \ncong U_j. \end{cases}$$

Then $\mathrm{Hom}_G(U_i, U_j)^{\oplus m_i m_j} = \{0\}$ if $i \neq j$ and

$$\mathrm{Hom}_G(U_i, U_i)^{\oplus m_i^2} \cong \mathbb{C}^{m_i^2} \cong \mathrm{Mat}_{m_i}(\mathbb{C}).$$

Thus $\mathrm{End}_G(V) \cong \bigoplus_{i=1}^n \mathrm{Mat}_{n_i}(\mathbb{C})$.

(*ii*) We know from (i) that we can identify $\mathrm{End}_G(V)$ with an algebra of block-diagonal matrices over $\mathbb{C}$. The sizes of the blocks correspond to m_i, the multiplicity of U_i in V. Composing two $f, g \in \mathrm{End}_G(V)$ corresponds to multiplying their associated matrices. Then $\mathrm{End}_G(V)$ is commutative if and only if the block sizes are all 1. That is, if $m_i = 1$ for all i. ☐

Corollary 7. (*i*) *The induced representation W is multiplicity-free if and only if its associated Hecke algebra $\mathcal{H}$ is commutative.*

(*ii*) *W is irreducible if and only if $\mathcal{H} \cong \mathbb{C}$.*

Proof. (*i*) Apply Proposition 6 with $V = W$. Then W is multiplicity-free if and only if $\mathrm{End}_G(W)$ is commutative. Proposition 5 tells us that $\mathrm{End}_G(W) \cong \mathcal{H}$. Thus W is multiplicity-free if and only if $\mathcal{H}$ is commutative.

(*ii*) Suppose that W is irreducible. Schur's Lemma tells us that $\mathrm{End}_G(W) \cong \mathbb{C}$, so $\mathcal{H} \cong \mathbb{C}$. Conversely, suppose that $\mathcal{H} \cong \mathbb{C}$. Write the decomposition of W into irreducible constituents

$$W = \bigoplus_{i=1}^{n} W_i.$$

Schur's lemma tells us that $\mathrm{End}_G(W_i) \cong \mathbb{C}$ for each i. Then

$$\mathrm{End}_G(W) = \mathrm{End}_G\left(\bigoplus_{i=1}^{n} W_i\right) \cong \bigoplus_{i=1}^{n} \mathrm{End}_G(W_i) \cong \bigoplus_{i=1}^{n} \mathbb{C} = \mathbb{C}^n.$$

However $\mathbb{C} \cong \mathcal{H} \cong \mathrm{End}_G(W) \cong \mathbb{C}^n$. Thus $n = 1$ and W is irreducible. ☐

1.7. **Gelfand's Trick.** Our goal in this section is to prove the following theorem.

Theorem 8 (Gelfand's Trick)**.** *Suppose that G is a finite group and $K \leq G$ is a subgroup. Let $\varphi\colon G \to G$ be an anti-automorphism with*

(*i*) *$\varphi^2 = 1$, and*

(*ii*) *$K\varphi(x)K = KxK$ for all $x \in G$.*

Then $\mathcal{H}(G, K)$ is commutative.

The key idea of this theorem is the following lemma.

Lemma 9. *Let A be an algebra and $B \subseteq A$ be a subalgebra with basis $\{b_i\}_{i \in I}$. Suppose $F\colon A \to A$ is an anti-homomorphism (i.e. $F(a_1 a_2) = F(a_2)F(a_1)$) and $F(b_i) = b_i$. Then B is commutative.*

Proof. Since F is the identity on basis elements of B, there holds $F|_B = \mathrm{Id}_B$. Let $b_i, b_j \in B$ be basis elements and notice

$$b_i b_j = F(b_i b_j) = F(b_j)F(b_i) = b_j b_i.$$

Then basis elements of B commute as desired. ☐

We employ Lemma 9 by applying it to the case where $A = \mathrm{Fun}(G)$ and $B = \mathcal{H}(G, K)$. Recall from Section 1.3 that the characteristic functions $\{\chi_x\}_{x \in G}$ form a basis of $\mathcal{H}(G, K)$.

Corollary 10. *Suppose $F\colon \operatorname{Fun}(G) \to \operatorname{Fun}(G)$ is an anti-homomorphism such that $F(\chi_x) = \chi_x$ for all $x \in X$. Then $\mathcal{H}(G, K)$ is commutative.*

This gives us a clear direction going forward: we want to find such a map F.

Given an anti-homomorphism of groups $\varphi\colon G \to G$, we can consider the map $\varphi^*\colon \operatorname{Fun}(G) \to \operatorname{Fun}(G)$ defined by $\varphi^* f := f \circ \varphi$. This is the *pullback* of f by φ. In general, φ^* is not an anti-homomorphism of convolution algebras. For instance, consider $G = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ and the map $\varphi(x) = x + x = 0$. Clearly φ is an anti-homomorphism. However, consider the maps $f, g \in \operatorname{Fun}(G)$ given by $f(x) = g(x) = 0$ if $x = 0$ and $f(x) = g(x) = 1$ if $x = 1$. Then

$$(\varphi^*(f \star g))(0) = \sum_{x+y=\varphi(0)} f(x)g(y) = \sum_{x+y=0} f(x)g(y) = f(0)g(0) + f(1)g(1) = 1,$$

$$((\varphi^* g) \star (\varphi^* f))(0) = \sum_{x+y=0} g(\varphi(x))f(\varphi(y)) = \sum_{x+y=0} g(0)f(0) = 2g(0)f(0) = 0.$$

Thus φ^* is not an anti-homomorphism. However, when φ has the stronger anti-automorphism property, we can say the same for φ^*. More precisely, we have the following lemma.

Lemma 11. *Suppose $\varphi\colon G \to G$ is a group anti-automorphism. Then $\varphi^*\colon \operatorname{Fun}(G) \to \operatorname{Fun}(G)$ is an algebra anti-automorphism.*

Proof. Let φ be a group anti-automorphism. Thus φ is a bijection and an anti-homomorphism. This lets us write $yz = x \iff \varphi(yz) = \varphi(x)$ since φ is a bijection. We can also write $\varphi(yz) = \varphi(x) \iff \varphi(z)\varphi(y) = \varphi(x)$ since φ is an anti-homomorphism. Then we compute

$$((\varphi^* f) \star (\varphi^* g))(x) = \sum_{yz=x} (\varphi^* f)(y)(\varphi^* g)(z) = \sum_{yz=x} f(\varphi(y))g(\varphi(z)) =$$
$$\sum_{\varphi(z)\varphi(y)=\varphi(x)} g(\varphi(z))f(\varphi(y)) = \sum_{z'y'=\varphi(x)} g(z')f(y') = (\varphi^*(g \star f))(x).$$

Thus $\varphi^*(g \star f) = (\varphi^* f) \star (\varphi^* g)$. We also need to check that φ^* is a bijection. We check this on the basis elements $\{\delta_g\}_{g \in G}$ of $\operatorname{Fun}(G)$. Let $g, h \in G$ and we compute

$$(\varphi^* \delta_g)(h) = \begin{cases} 1, & \text{if } g = \varphi(h), \\ 0, & \text{else.} \end{cases} = \begin{cases} 1, & \text{if } h = \varphi^{-1}(g), \\ 0, & \text{else.} \end{cases} = \delta_{\varphi^{-1}(g)}(h).$$

We see that φ^* sends δ_g to $\delta_{\varphi^{-1}(g)}$. We know φ and φ^{-1} are bijections on G, so φ^* acts bijectively on the basis of $\operatorname{Fun}(G)$. $\square$

Now we know that an anti-automorphism φ of G induces an anti-automorphism φ^* of $\operatorname{Fun}(G)$. We ask ourselves: when does this anti-automorphism restrict to an anti-automorphism of $\mathcal{H}(G, K)$? That is, when is φ^* also an anti-automorphism of $\mathcal{H}(G, K)$? The following lemma provides an answer.

Lemma 12. *Suppose that $\varphi\colon G \to G$ is an anti-automorphism. If $\varphi(K) = K$ then φ^* restricts to an anti-automorphism of $\mathcal{H}(G, K)$.*

Proof. Suppose $f \in \mathcal{H}$. Then notice

$$(\varphi^* f)(k_1 g k_2) = f(\varphi(k_1 g k_2)) = f(\varphi(k_2)\varphi(g)\varphi(k_1)) = f(k_2'\varphi(g)k_1') = f(\varphi(g)) = (\varphi^* f)(g).$$

Thus $\varphi^* f \in \mathcal{H}$ since it's constant on K-double cosets. $\square$

Now we explore the effect of φ^* on the basis elements $\{\chi_x\}_{x\in G}$ of $\mathcal{H}(G, K)$.

Lemma 13. *Suppose $\varphi\colon G \to G$ is an anti-automorphism. If $\varphi^2 = 1$ and $K\varphi(x)K = KxK$ for all $x \in G$, then $\varphi^*\chi_x = \chi_x$.*

Before we present the proof, notice that $\varphi(K) = K$ is a consequence of the assumption that $K\varphi(x)K = KxK$ for all $x \in G$. This assumption implies that $K\varphi(x)K = KxK$ for all $x \in K$, which in turn implies that $\varphi(K) = K$.

Proof. First, if $g \in KxK$, then

$$\varphi(g) \in \varphi(KxK) = \varphi(K)\varphi(x)\varphi(K) = K\varphi(x)K = KxK.$$

On the other hand, if $\varphi(g) \in KxK$, then

$$g = \varphi(\varphi(g)) \in \varphi(KxK) = \varphi(K)\varphi(x)\varphi(K) = K\varphi(x)K = KxK.$$

We see that $g \in KxK$ if and only if $\varphi(g) \in KxK$. Then we compute

$$(\varphi^*\chi_x)(g) = \chi_x(\varphi(g)) = \begin{cases} 1, & \text{if } \varphi(g) \in KxK, \\ 0, & \text{else.} \end{cases} = \begin{cases} 1, & \text{if } g \in KxK, \\ 0, & \text{else.} \end{cases} = \chi_x(g). \qquad \square$$

We are now ready to prove Theorem 8.

Proof of Theorem 8. Lemma 13 tells us that φ^* is the identity on the characteristic functions χ_x. These are the basis elements of $\mathcal{H}(G, K)$. Since φ is an anti-automorphism, φ^* will be too. We apply Corollary 10 with $F = \varphi^*$ to see that the basis elements commute. Thus $\mathcal{H}(G, K)$ is commutative. $\square$

When applying Gelfand's Trick, we will often consider $\varphi(x) = x^{-1}$ or $\varphi(x) = x^t$ (the latter of which is understood as the transpose map when G is a matrix group). It is easy to see that they are both involutive anti-automorphisms, so the condition $K\varphi(x)K = KxK$ for all $x \in G$ will be the only condition left to verify.

1.8. **Gelfand pairs.** We say that a pair of groups (G, K) with $K \leq G$ is a *Gelfand pair* if $\mathrm{Ind}_K^G \mathbf{1}$ is multiplicity-free. To be a Gelfand pair, it is sufficient to find an anti-automorphism satisfying the conditions of Theorem 8. We present some examples of applications of this technique.

1.8.1. *Example: (G, K) with G abelian.* For any abelian group G, the identity map $\varphi(g) = g$ is an anti-automorphism. This map clearly satisfies $\varphi^2 = 1$ and $K\varphi(x)K = KxK$ for all $x \in G$.

1.8.2. *Example:* (G, K) *with* $[G : K] = 2$. The condition $[G : K] = 2$ tells us that K is a normal subgroup of G. Thus, the quotient group G/K is defined and contains two cosets, K and $G - K$. Consider the involutive anti-automorphism $\varphi(g) = g^{-1}$. We verify that double cosets are preserved. If $x \in K$, then $K\varphi(x)K = Kx^{-1}K = K = KxK$. On the other hand, if $x \in G - K$, then $K\varphi(x)K = Kx^{-1}K = G \setminus K = KxK$. We see that $K\varphi(x)K = KxK$ in all cases.

1.8.3. *Example:* $(G \times G, G)$. We can embed the group G inside $G \times G$ by the injective map $g \mapsto (g, g)$. Then it makes sense to consider G as a subgroup of $G \times G$. We apply Gelfand's Trick with the involutive anti-automorphism $\varphi(g_1, g_2) = (g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$. There holds

$$\begin{aligned} G\varphi(g_1, g_2)G &= \{(hg_1^{-1}k, hg_2^{-1}k) \mid h, k \in G\} \\ &= \{(k^{-1}g_1h^{-1}, k^{-1}g_2h^{-1})^{-1} \mid h, k \in G\} = \{(xg_1y, xg_2y) \mid x, y \in G\} = G(g_1, g_2)G. \end{aligned}$$

We see that φ preserves double cosets and we have a Gelfand pair.

1.8.4. *Example:* $(S_{n+m}, S_n \times S_m)$. We present an original proof, but one may also see [Bum13] for an alternate proof. The group $S_n \times S_m$ can be embedded inside S_{n+m} by taking $w = (w_1, w_2) \in S_n \times S_m$ and forming an element of S_{n+m} by having w_1 act on the first n elements of $\{1, 2, \ldots, n+m\}$ and having w_2 act on the last m elements of $\{1, 2, \ldots, n+m\}$.

Consider the involutive anti-automorphism $\varphi(w) = w^{-1}$. We must verify that $K\varphi(w)K = KwK$ for each double coset. If $w \in K$, then $K\varphi(w)K = Kw^{-1}K = K = KwK$ so all that is left is to verify double cosets are preserved for $w \in G - K$.

We wish to show that $Kw^{-1}K \subseteq KwK$ and $KwK \subseteq Kw^{-1}K$. Note that it suffices to show only one of these. We will show that $Kw^{-1}K \subseteq KwK$. Again, note that it suffices to show that $w^{-1} \in KwK$. This is equivalent to showing that $w^{-1} = k_1wk_2$ for some $k_1, k_2 \in K$. This equation is equivalent to $k_2^{-1} = wk_1w$. Then it suffices to show that $wkw \in K$ for some $k \in K$.

We call $i \in \{1, \ldots, n+m\}$ a *crossing point* of w if one of two mutually exclusive conditions hold: $i \in \{1, \ldots, n\}$ and $w(i) \in \{n+1, \ldots, n+m\}$, or $i \in \{n+1, \ldots, n+m\}$ and $w(i) \in \{1, \ldots, n\}$. Notice that the number of crossing points in $\{1, \ldots, n\}$ must equal the number of crossing points in $\{n+1, \ldots, n+m\}$ since w is a bijection. Then there is a bijection $f\colon \{\text{crossing points} \leq n\} \to \{\text{crossing points} > n\}$. This yields two other bijections $g\colon \{1, \ldots, n\} - \{\text{crossing points} \leq n\} \to \{1, \ldots, n\} - w(\{\text{crossing points} > n\})$ and $h\colon \{n+1, \ldots, n+m\} - \{\text{crossing points} > n\} \to \{n+1, \ldots, n+m\} - w(\{\text{crossing points} \leq n\})$. Define $k \in S_{n+m}$ by

$$k(w(i)) := \begin{cases} f(i), & \text{if } i \leq n \text{ is a crossing point,} \\ f^{-1}(i), & \text{if } i > n \text{ is a crossing point,} \\ g(i), & \text{if } i \leq n \text{ is not a crossing point,} \\ h(i), & \text{if } i > n \text{ is not a crossing point.} \end{cases}$$

It is easy to check that k and wkw lie in K as desired.

1.8.5. *Example:* $(\mathrm{O}_{n+1}(\mathbb{F}_q), \mathrm{O}_n(\mathbb{F}_q))$ *with* $q \neq 2^k$. We can embed the group $\mathrm{O}_n(\mathbb{F}_q)$ inside $\mathrm{O}_{n+1}(\mathbb{F}_q)$ by the injection

$$\mathrm{O}_n(\mathbb{F}_q) \hookrightarrow \mathrm{O}_{n+1}(\mathbb{F}_q), \quad A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}.$$

Consider the involutive anti-automorphism $\varphi(x) = x^t = x^{-1}$. We verify that φ preserves double cosets. First note, for any group G and subgroup H, the action of G on G/H by left translation gives rise to an action of G on $G/H \times G/H$. The orbits of this action are the double cosets $H\backslash G/H$. This yields an identification of $H\backslash G/H$ with $G\backslash(G/H \times G/H)$. Explicitly, the identification is given by $(g_1H, g_2H) \mapsto Hg_1g_2^{-1}H$.

Notice that $G/H := \mathrm{O}_{n+1}(\mathbb{F}_q)/\mathrm{O}_n(\mathbb{F}_q)$ is isomorphic to the unit sphere. Given the previous discussion, it suffices to show that, given two unit vectors $u, v \in \mathbb{R}^n$, there exists $g \in \mathrm{O}_n(\mathbb{F}_q)$ with $g(u) = v$ and $g(v) = u$, since the transpose map sends (u, v) to (v, u). If $u - v$ is not orthogonal to itself, take g to be the reflection relative to the hyperplane orthogonal to $u - v$. More specifically, set $g(x) := x - \frac{2\langle u-v,x\rangle}{\langle u-v,u-v\rangle}(u-v)$. Then

$$g(u) = u - \frac{2\langle u - v, u\rangle}{\langle u - v, u - v\rangle}(u - v) = u - \frac{2\|u\|^2 - 2\langle u, v\rangle}{\|u\|^2 + \|v\|^2 - 2\langle u, v\rangle}(u - v) = u - (u - v) = v,$$

$$g(v) = v - \frac{2\langle u - v, v\rangle}{\langle u - v, u - v\rangle}(u - v) = v - \frac{2\langle u, v\rangle - 2\|v\|^2}{\|u\|^2 + \|v\|^2 - 2\langle u, v\rangle}(u - v) = v + (u - v) = u.$$

If $u - v$ is orthogonal to itself, this tells us that $0 = \langle u - v, u - v\rangle = \|u\|^2 + \|v\|^2 - \langle u, v\rangle = 2 - 2\langle u, v\rangle$ so $\langle u, v\rangle = 1$. Then $\langle u + v, u + v\rangle = 4$ so $u + v$ is not orthgonal to itself, and we take g to be the reflection relative to $u + v$. That is, $g(x) := \frac{2\langle u+v,x\rangle}{\langle u+v,u+v\rangle}(u + v) - x$. Then

$$g(u) = \frac{2\langle u + v, u\rangle}{\langle u + v, u + v\rangle}(u + v) - u = \frac{2\langle u, v\rangle + 2\|u\|^2}{4}(u + v) - u = (u + v) - u = v,$$

$$g(v) = \frac{2\langle u + v, v\rangle}{\langle u + v, u + v\rangle}(u + v) - v = \frac{2\langle u, v\rangle + 2\|v\|^2}{4}(u + v) - v = (u + v) - v = u.$$

2. Twisted Hecke Algebras of Finite Groups

We have now completed our investigation of the Hecke algebra $\mathcal{H}(G, K)$. The aim of this section is to generalise the results of Chapter 1 to the case of a non-trivial character $\sigma\colon K \to \mathbb{C}^\times$. Here the Hecke algebra $\mathcal{H} = \mathcal{H}(G, K, \sigma)$ is the convolution algebra of (K, σ)-bi-invariant functions on G. In Section 2.1, we discuss the theory of the induced representation $\operatorname{Ind}_K^G \sigma$. In Section 2.2, we revisit the Hecke algebra, identify its identity and describe its basis. Notice that the results of Section 1.4 and Section 1.5 were independent of the choice $\sigma = \mathbf{1}$, so they still apply now that we are considering a non-trivial character.

In Section 2.3, we generalise Gelfand's Trick from Section 1.7 to the case of a non-trivial character σ. Naturally, we will need to reconsider the conditions that the anti-automorphism $\varphi\colon G \to G$ must satisfy. As in Section 1.7, we will investigate these conditions and conclude with a natural statement and proof of Gelfand's Trick in the twisted case. We conclude with Section 2.4, in which we investigate the Gelfand–Graev representation and use the results of this chapter to prove that it is multiplicity-free.

2.1. The induced representation $\operatorname{Ind}_K^G \sigma$.

Suppose that $\sigma\colon K \to \mathbb{C}^\times$ is a character, i.e. a group homomorphism. Consider the space

$$W := \{f\colon G \to \mathbb{C} \mid f(gk) = f(g)\sigma(k),\ \forall g \in G, \forall k \in K\} \subseteq \operatorname{Fun}(G).$$

As in the previous section, W is called the induced representation and denoted $\operatorname{Ind}_K^G \sigma$. We state and prove a lemma analogous to Lemma 2.

Lemma 14. *W is a left ideal of $(\operatorname{Fun}(G), \star)$.*

Proof. We verify that $f \star w \in W$ whenever $w \in W$ and $f \in \operatorname{Fun}(G)$. Let $g \in G$ and $k \in K$. Then

$$\begin{aligned}(f \star w)(gk) &= \sum_{xy=gk} f(x)w(y) = \sum_{x\in G} f(x)w(x^{-1}gk) = \sum_{x\in G} f(x)w(x^{-1}g)\sigma(k)\\ &= \Big[\sum_{x\in G} f(x)w(x^{-1}g)\Big]\sigma(k) = \Big[\sum_{xy=g} f(x)w(y)\Big]\sigma(k) = (f\star w)(g)\sigma(k). \qquad \square\end{aligned}$$

2.2. The twisted Hecke algebra of a finite group $\mathcal{H}(G, K, \sigma)$.

The Hecke algebra $\mathcal{H} = \mathcal{H}(G, K, \sigma)$ is the space

$$\mathcal{H} := \{f\colon G \to \mathbb{C} \mid f(k_1 g k_2) = \sigma(k_1)f(g)\sigma(k_2),\ \forall g \in G,\ \forall k_1, k_2 \in K\} \subseteq \operatorname{Fun}(G).$$

The proof of Lemma 14 can be adapted to show that $\mathcal{H}$ is a two-sided ideal in $(\operatorname{Fun}(G), \star)$. As before, the identity of $(\operatorname{Fun}(G), \star)$ does not lie in $\mathcal{H}$. Nevertheless, $\mathcal{H}$ does have an identity of its own. It is easy to verify that the identity is ι_K^σ, which we define below.

$$\iota_K^\sigma : G \to \mathbb{C}, \quad \iota_K^\sigma(g) := \begin{cases} \frac{1}{|K|}\sigma(g), & \text{if } g \in K,\\ 0, & \text{else.}\end{cases}$$

Thus, $(\mathcal{H}, \star)$ is a unital associative algebra in its own right.

We now construct a basis for $\mathcal{H}$. Recall that when $\sigma = \mathbf{1}$, the basis of $\mathcal{H}$ was described by the characteristic functions of K-double cosets. To treat the case when $\sigma \neq \mathbf{1}$, we need a lemma about group actions.

Consider the finite group K acting on a set X. For each $x \in X$, let $\mathcal{O}_x := \{g \cdot x \mid g \in G\}$ be the orbit containing x and let $K_x := \{k \in K \mid k \cdot x = x\}$ be the stabiliser subgroup of x in K (also denoted as $\mathrm{stab}_K(x)$). Consider the vector space

$$V := \{f \colon X \to \mathbb{C} \mid f(k \cdot x) = \sigma(k) f(x),\ \forall k \in K,\ \forall x \in X\} \subseteq \mathrm{Fun}(X).$$

An orbit $\mathcal{O}_x$ is called (K, σ)-*relevant* if there exists $f \in V$ such that $f|_{\mathcal{O}_x}$ is non-zero. Otherwise, we say $\mathcal{O}_x$ is (K, σ)-*irrelevant*. We omit mention of (K, σ) if it is clear from the context.

Lemma 15. *An orbit $\mathcal{O}_x$ is (K, σ)-relevant if and only if $\sigma(K_x) = \{1\}$.*

Proof. Assume that $\sigma(K_x) \neq \{1\}$. Then there exists $k \in K_x$ such that $\sigma(k) \neq 1$. Now recall that for $f \in V$ we have $f(x) = f(k \cdot x) = \sigma(k) f(x)$. However $\sigma(k) \neq 1$, so $f(x) = 0$. Then f must be zero on $\mathcal{O}_x$ and $\mathcal{O}_x$ is irrelevant.

Conversely, the fact that σ is trivial on K_x implies that it factors through a well-defined function $\sigma_x \colon \mathcal{O}_x \simeq K/K_x \to \mathbb{C}$ given by $\sigma_x(kK_x) := \sigma(k)$. To see that this function is well-defined, suppose that $k_1 K_x = k_2 K_x$. Then $k_1 k_2^{-1} \in K_x$. Since σ is trivial on K_x, we know $1 = \sigma(k_1 k_2^{-1}) = \sigma(k_1)\sigma(k_2)^{-1}$. Then $\sigma(k_1) = \sigma(k_2)$ so $\sigma_x(k_1 K_x) = \sigma_x(k_2 K_x)$. It is easy to check that $\sigma_x \in V$. Thus, $\mathcal{O}_x$ is relevant. $\square$

Now suppose K is a subgroup of G acting on $X = G$ from the left and right by translation. Then the orbit $\mathcal{O}_x$ is nothing but the double coset KxK and V becomes the Hecke algebra $\mathcal{H}$. Explicitly, we have

$$\mathcal{H} = \{f \colon X \to \mathbb{C} \mid f(k_1 \cdot x \cdot k_2) = \sigma(k_1) f(x) \sigma(k_2),\ \forall k_1, k_2 \in K,\ \forall x \in X\} \subseteq \mathrm{Fun}(X).$$

We can re-write this data by considering the left action of $K \times K^{\mathrm{op}}$ on X, where K^{op} is the group opposite to K. Then

$$\mathcal{H} = \{f \colon X \to \mathbb{C} \mid f((k_1, k_2) \cdot x) = \sigma(k_1)\sigma(k_2) f(x),\ \forall k_1, k_2 \in K,\ \forall x \in X\} \subseteq \mathrm{Fun}(X).$$

A double coset KxK is relevant if it supports a non-zero function from $\mathcal{H}$. Let X_{rel} be a family of relevant coset representatives. Define the family of functions $\{\chi_x\}_{x \in X_{\mathrm{rel}}}$ by

$$\chi_x(y) := \begin{cases} \sigma(k)\sigma(k'), & \text{if } y \in KxK \text{ with } y = kxk', \\ 0, & \text{if } y \notin KxK. \end{cases}$$

One easily checks that χ_x is well-defined. We call χ_x a *twisted characteristic function* associated to the relevant orbit KxK. When $\sigma = \mathbf{1}$, every orbit is relevant and $\sigma(k)\sigma(k') = 1$, so we obtain the original characteristic functions described in Section 1.3. Define the map

$$\sigma \boxtimes \sigma \colon K \times K \to \mathbb{C}^\times \times \mathbb{C}^\times, \quad (\sigma \boxtimes \sigma)(k_1, k_2) := (\sigma(k_1), \sigma(k_2)).$$

As a result of Lemma 15, we see that an orbit under the left action of $K \times K^{\mathrm{op}}$ is relevant if and only if $(\sigma \boxtimes \sigma)(\mathrm{stab}_{K \times K}(x)) = \{1\}$. As in Section 1.3, it is not difficult to see that the twisted characteristic functions of relevant orbits form a basis of $\mathcal{H}(G, K, \sigma)$.

2.3. **Twisted Gelfand's Trick.** Our goal in this section is to prove the twisted analogue of Gelfand's Trick.

Theorem 16 (Twisted Gelfand's Trick). *Suppose that G is a finite group with $K \leq G$ as a subgroup and character $\sigma\colon K \to \mathbb{C}^\times$. Let $\varphi\colon G \to G$ be an anti-automorphism such that*

(i) $\varphi^2 = 1$,
(ii) $\varphi(K) = K$,
(iii) $\sigma(\varphi(k)) = \sigma(k)$ *for all* $k \in K$, *and*
(iv) $\varphi(x) = x$ *for all* $x \in X_{\mathrm{rel}}$, *a family of representatives for the* (K,σ)*-relevant* K*-double cosets.*

Then $\mathcal{H}(G, K, \sigma)$ *is commutative.*

This is a true generalisation of Theorem 8. Indeed, if we consider the trivial representation $\sigma = \mathbf{1}$, condition (*iii*) is trivially satisfied, condition (*iv*) corresponds to the requirement that $K\varphi(x)K = KxK$ in Theorem 8, and condition (*ii*) is contained in the requirement that $K\varphi(x)K = KxK$.

As in Section 2.1, the proof of Theorem 16 relies on the observation that an anti-homomorphism of an algebra that acts as the identity on basis elements of the subalgebra is sufficient to conclude that the subalgebra is commutative (c.f. Lemma 9 and Corollary 7). This leaves us with a question: can we rewrite the condition $\varphi^*\chi_x = \chi_x$?

Recall that X_{rel} denotes a family of representatives for the relevant double cosets. Recall the twisted characteristic functions $\{\chi_x\}_{x\in X_{\mathrm{rel}}}$ defined in Section 2.2 given by

$$\chi_x(y) = \begin{cases} \sigma(k)\sigma(k'), & \text{if } y \in KxK \text{ with } y = kxk', \\ 0, & \text{if } y \notin KxK. \end{cases}$$

Thus,

$$(\varphi^*\chi_x)(g) = \begin{cases} \sigma(k)\sigma(k'), & \text{if } \varphi(g) \in KxK \text{ with } \varphi(g) = kxk', \\ 0, & \text{else.} \end{cases}$$

If $\varphi\colon G \to G$ is an involutive homomorphism, then $\varphi(g) = kxk'$ is equivalent to $g = \varphi(k')\varphi(x)\varphi(k)$. If we further suppose that $\varphi(x) = x$ for all $x \in X_{\mathrm{rel}}$ and $\varphi(K) = K$, then $g = \varphi(k')\varphi(x)\varphi(k)$ is equivalent to $g = \varphi(k')x\varphi(k)$. Thus,

$$(\varphi^*\chi_x)(g) = \begin{cases} \sigma(\varphi(k'))\sigma(\varphi(k)), & \text{if } g \in KxK \text{ with } g = \varphi(k')x\varphi(k), \\ 0, & \text{else.} \end{cases}$$

This tells us that $\varphi^*\chi_x$ is also supported (i.e. non-zero) on KxK. Now let's also assume that $\sigma(\varphi(k)) = \sigma(k)$ for all $k \in K$. Then we can easily verify that $\varphi^*\chi_x \in \mathcal{H}(G, K, \sigma)$. So $\varphi^*\chi_x$ must be a multiple of χ_x. In fact, this multiple is 1, since

$$(\varphi^*\chi_x)(x) = \chi_x(\varphi(x)) = \chi_x(x) = 1.$$

We are now ready to prove Theorem 16.

Proof of Theorem 16. Suppose that $\varphi\colon G \to G$ is an anti-automorphism. Also suppose that $\varphi^2 = 1$, $\varphi(K) = K$, $\sigma(\varphi(k)) = \sigma(k)$ for all $k \in K$, and $\varphi(x) = x$ for all $x \in X_{\mathrm{rel}}$. The above discussion tells us that $\varphi^*\chi_x =$

χ_x. These are the basis elements of $\mathcal{H}(G, K, \sigma)$. We apply Corollary 10 to conclude that $\mathcal{H}(G, K, \sigma)$ is commutative. $\square$

2.4. **The Gelfand–Graev representation.** We construct the *Gelfand–Graev representation* of $G = \mathrm{GL}_n(\mathbb{F}_q)$. First, consider the *unipotent radical* of G, given by

$$U(\mathbb{F}_q) := \begin{pmatrix} 1 & \mathbb{F}_q & \dots & \mathbb{F}_q \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & 1 & \mathbb{F}_q \\ 0 & \dots & 0 & 1 \end{pmatrix}.$$

Next, fix a non-trivial additive character $\psi\colon \mathbb{F}_q \to \mathbb{C}^\times$ (i.e. $\psi(a+b) = \psi(a)\psi(b)$). Then define a character $\pi\colon U(\mathbb{F}_q) \to \mathbb{C}^\times$ by

$$\pi(x) := \psi(x_{12} + x_{23} + \cdots + x_{n-1,n}).$$

To see that π is a character, observe

$$\begin{aligned} \pi(xy) &= \psi((xy)_{12} + (xy)_{23} + \cdots + (xy)_{n-1,n}) \\ &= \psi\left(\sum_{k=1}^{n-1} x_{1k}y_{k2} + \sum_{k=1}^{n-1} x_{2k}y_{k3} + \cdots + \sum_{k=1}^{n-1} x_{n-1,k}y_{kn}\right) \\ &= \psi\left(\sum_{k=1}^{n-1} x_{1k}y_{k2}\right)\psi\left(\sum_{k=1}^{n-1} x_{2k}y_{k3}\right)\cdots\left(\sum_{k=1}^{n-1} x_{n-1,k}y_{kn}\right) \\ &= \psi(x_{12} + y_{12})\psi(x_{23} + y_{23})\cdots\psi(x_{n-1,n} + y_{n-1,n}) \\ &= \psi(x_{12})\psi(y_{12})\psi(x_{23})\psi(y_{23})\cdots\psi(x_{n-1,n})\psi(y_{n-1,n}) \\ &= \psi(x_{12})\psi(x_{23})\cdots\psi(x_{n-1,n})\psi(y_{12})\psi(y_{23})\cdots\psi(y_{n-1,n}) \\ &= \psi(x_{12} + \cdots + x_{n-1,n})\psi(y_{12} + \cdots + y_{n-1,n}) \\ &= \pi(x)\pi(y). \end{aligned}$$

The *Gelfand–Graev representation* of G is $\mathrm{Ind}_U^G \pi$. In [Bum13], Bump explains, "this Gelfand–Graev representation is important because it contains *most* irreducible representations of the group; those it contains are therefore called *generic*." Furthermore, we have the following theorem.

Theorem 17. *The Gelfand–Graev representation is multiplicity-free. That is,* $(\mathrm{GL}_n(\mathbb{F}_q), U(\mathbb{F}_q), \pi)$ *is a twisted Gelfand pair.*

This theorem will be proven in two parts. We begin with a lemma.

Lemma 18. (*i*) *We have the Bruhat decomposition*

$$\mathrm{GL}_n(\mathbb{F}_q) = \bigsqcup_{w \in W} BwB,$$

where W is the group of all $n \times n$ permutation matrices and B is the subgroup of all $n \times n$ upper-triangular matrices.

(*ii*) *We can modify the Bruhat decomposition and write*

$$\mathrm{GL}_n(\mathbb{F}_q) = \bigsqcup_{m \in M} UmU,$$

where M is the group of all $n \times n$ monomial matrices. A monomial matrix is a matrix with exactly one non-zero element in each row and column.

Before we prove Lemma 18, we recall a simple fact about matrices. Define $x_{ij}(t) := I_{n\times n} + tE_{ij}$, where $1 \leq i \leq j \leq n$ and E_{ij} is the matrix of 0's except for a 1 in the i^{th} row and j^{th} column. Notice that $x_{ij}(t) \in B$ since $i \leq j$. We can achieve the usual row and column operations on a matrix A by multiplying on the left or the right by some $x_{ij}(t)$. The following makes this statement precise.

Right-multiplying A by $x_{ij}(t)$ corresponds to the column operation of $C_j \mapsto C_j + tC_i$, where C_k is column k of A. Similarly, left-multiplying A by $x_{ij}(t)$ corresponds to the row operation of $R_i \mapsto R_i + tR_j$, where R_k is row k of A. Right-multiplying A by $x_{ii}(\lambda - 1)$ corresponds to the column operation $C_i \mapsto \lambda C_i$, for some scalar λ. Similarly, left-multiplying A by $x_{ii}(\lambda - 1)$ corresponds to the row operation $R_i \mapsto \lambda R_i$. We see that we can perform the usual row and column operations by right- and left-multiplying by elements of B.

Proof of Lemma 18. We begin by proving that $\mathrm{GL}_n(\mathbb{F}_q) = \bigcup_{w \in W} BwB$ and will prove disjointness of the union later. We proceed by induction. The $n = 1$ case is clearly true since all matrices in $\mathrm{GL}_1(\mathbb{F}_q)$ are upper-triangular. Now let $n > 1$ and $g \in \mathrm{GL}_n(\mathbb{F}_q)$. We wish to find a permutation matrix w in BgB. We have two cases: $g_{n,1} \neq 0$ and $g_{n,1} = 0$.

In the first case, the previous discussion tells us that we can multiply g on the left and the right by appropriate elements of B so that the resulting matrix has zeros in the left column and bottom row, except for the bottom left entry, which is $g_{n,1}$. This is non-zero so we can normalise this resulting matrix by $g_{n,1}$ to yield $\left(\begin{smallmatrix} 0 & g' \\ 1 & 0 \end{smallmatrix}\right)$. Here g' lies in $\mathrm{GL}_{n-1}(\mathbb{F}_q)$. The inductive hypothesis that the $n-1$ is true tells us that g' lies in a double coset $Bw'B$ for some $(n-1) \times (n-1)$ permutation matrix w'. Then the desired w is obtained by setting $w = \left(\begin{smallmatrix} 0 & w' \\ 1 & 0 \end{smallmatrix}\right)$.

In the second case, choose $g_{i1} \neq 0$ and $g_{nj} \neq 0$ so that i is as large as possible and j is as small as possible. This amounts to choosing the two non-zero entries in the left column and bottom row that are closest to the bottom left entry. Left- and right-multiplication by appropriate elements of B yields a matrix whose first and jth columns and ith and last rows are empty, except the entries g_{i1} and g_{nj}. Since these entries are non-zero, we can normalise these to 1 as well. Now we apply the inductive hypothesis to the matrix obtained by removing these two rows and two columns. We are left with a permutation matrix and this completes the induction.

We verify that the union is disjoint. Let $w_1, w_2 \in W$ be representatives for the same double coset. Then $Bw_1B = Bw_2B$ and, given any $b \in B$, there exists $b' \in B$ with $w_1 b w_2^{-1} = b'$. In particular, $w_1 w_2^{-1} \in B \cap W = \{1\}$. Thus $w_1 = w_2$.

We now prove the modified decomposition. Consider the subgroup T of diagonal matrices in $\mathrm{GL}_n(\mathbb{F}_q)$. Notice that $B = TU = UT$ and $M = TW = WT$ so the result follows from the regular Bruhat decomposition. Disjointness is proven as before. $\square$

Proof of Theorem 17. Consider the involutive anti-automorphism $\varphi\colon G \to G$ defined by

$$\varphi(g) := w_0 g^t w_0, \quad \text{where } w_0 = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}.$$

We verify that $U\varphi(g)U = UgU$ for all $g \in G$. For each double coset UgU, we will show that UgU has a certain coset representative g' with $\varphi(g') = g'$, or $f(g) = 0$ for all $f \in \mathcal{H}$.

The modification of the Bruhat decomposition in Lemma 18 tells us that $UgU = UmU$ for some monomial matrix m. Let $f \in \mathcal{H}$ be non-vanishing on UmU. That is, $f(m) \neq 0$. We show that m has the form

$$m = \begin{pmatrix} & & & D_1 \\ & & D_2 & \\ & \iddots & & \\ D_r & & & \end{pmatrix},$$

for some diagonal matrices $D_1,\ldots,D_r$. Equivalently, we show that if m_{ij} and $m_{i+1,k}$ are non-zero, then we must have $k \leq j+1$.

To see this, assume that $m_{ij}, m_{i+1,k} \neq 0$ and $k > j+1$. Then define $x := I_n + m_{ij}E_{i,i+1} \in U$ and $y := I_n + m_{i+1,k}E_{jk} \in U$. Simple computations tell us that $xm = m + m_{ij}m_{i+1,k}e_{ik} = my$, $\pi(x) = \psi(m_{ij}) \neq 1$ and $\pi(y) = \pi(0) = 1$. Then, since $f \in \mathcal{H}$, there holds $\pi(x)f(m) = f(xm) = f(my) = f(m)\pi(y)$. Thus $(\pi(x) - \pi(y))f(m) = 0$, so $f(m) = 0$ since $\pi(x) \neq \pi(y)$.

Now we show that each diagonal matrix D_i is actually a matrix of scalars. In particular, we show that if $m_{i,j}$ and $m_{i+1,j+1}$ are non-zero then they are equal. Consider x and y as given above, with $k = j+1$. Then $xm = my$, $\pi(x) = \psi(m_{ij})$, $\pi(y) = \psi(m_{i+1,j+1})$ and $(\pi(x) - \pi(y))f(m) = 0$. Recall that f doesn't vanish on UmU so $f(m) \neq 0$. Thus $\pi(x) = \pi(y)$, which tells us that $\psi(m_{ij}) = \psi(m_{i+1,j+1})$ and $m_{ij} = m_{i+1,j+1}$ by injectivity of ψ.

Finally, notice $\varphi(m) = m$. This is easy to see, since m^t is simply m with the elements on the opposite diagonal reversed, and left- and right-multiplying by w_0 also reverses the opposite diagonal. This completes the proof. $\square$

References

[AGS08] A. Aizenbud, D. Gourevitch, and E. Sayag, $(\mathrm{GL}_{n+1}(F), \mathrm{GL}_n(F))$ *is a Gelfand pair for any local field* F, Compositio Mathematica, Volume 144, Issue 6, 2008, pp. 1504–1524.

[BD85] T. Brocker and T. Dieck, *Representations of Compact Lie Groups*, Springer-Verlag, Berlin, 1985.

[BI84] E. Bannai and T. Ito, *Algebraic Combinatorics I : Association Schemes*, Benjamin Cummings Publishing Company, San Francisco, 1984.

[Bum10] D. Bump, *Hecke Algebras* (2010), http://sporadic.stanford.edu/bump/math263/hecke.pdf. Accessed 12/03/2021.

[Bum13] D. Bump, *Lie Groups*, Second Edition, Springer-Verlag, New York, 2013.

[Car85] R. W. Carter, *Finite Groups of Lie Type*, John Wiley & Sons Ltd, 1985.

[CSST20] T. Ceccherini-Silberstein, F. Scarabotti, and F. Tolli, *Gelfand Triples and Their Hecke Algebras: Harmonic Analysis for Multiplicity-Free Induced Representations of Finite Groups*, Lecture Notes in Mathematics, Springer International Publishing, 2020.

[CMHL03] I. Cherednik, Y. Markov, R. Howe, and G. Lusztig, *Iwahori-Hecke Algebras and Their Representation Theory*, Springer, Berlin, Heidelberg, 2003.

[Cox35] H. S. M. Coxeter, *The Complete Enumeration of Finite Groups of the Form* $R_i^2 = (R_iR_j)^{k_{ij}} = 1$ **s1-10** (1935), 21–25.

[CR87a] C. W. Curtis and I. Reiner, *Methods of Representation Theory - with applications to finite groups and orders*, Vol. 1, John Wiley & Sons, 1987.

[CR87b] C. W. Curtis and I. Reiner, *Methods of Representation Theory - with applications to finite groups and orders*, Vol. 2, John Wiley & Sons, 1987.

[Dia88] P. Diaconis, *Group representations in probability and statistics*, Institute of Mathematical Statistics, Hayward, California, 1988.

[EGH$^+$11] P. I. Etingof, O. Golberg, S. Hensel, T. Liu, A. Schwendner, D. Vaintrob, and E. Yudovina, *Introduction to Representation Theory*, American Mathematical Society, 2011.

[Fol84] G. B. Folland, *Real Analysis*, John Wiley & Sons Inc., 1984.

[Gro91] B. H. Gross, *Some applications of Gelfand pairs to number theory*, Bulletin (New Series) of the American Mathematical Society **24** (1991), 277–301.

[Hen20] Y. I. Hendel, *On Twisted Gelfand Pairs Through Commutativity of a Hecke Algebra* (2020), https://arxiv.org/pdf/1807.02843.pdf. Accessed 20/01/21.

[HKP09] T. J. Haines, R. E. Kottwitz, and A. Prasad, *Iwahori–Hecke Algebras* (2009), https://arxiv.org/abs/math/0309168. Accessed 29/04/2021.

[HP02] T. J. Haines and A. Pettet, *Formulae relating the Bernstein and Iwahori–Matsumoto presentations of an affine Hecke algebra*, Journal of Algebra **252** (2002), 127–149.

[Hum90] J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge University Press, New York, 1990.

[Kor80] A. Koranyi, *Some Applications of Gelfand Pairs in Classical Analysis*, Harmonic Analysis and Group Representation, 1980, pp. 334–348.

[Lam03] T. Y. Lam, *Corner Ring Theory: A Generalization of Peirce Decompositions, I*, Algebras, Rings and Their Representations: Proceedings of the International Conference on Algebras, Modules and Rings, 2003, pp. 153–182.

[Lan02] S. Lang, *Algebra*, revised 3rd edition, Springer-Verlag, New York, 2002.

[Mac95] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd ed., Oxford University Press Inc., New York, 1995.

[Mil20] J. S. Milne, *Algebraic Number Theory (v3.08)* (2020), www.jmilne.org/. Accessed 15/04/2021.

[Mor18] S. Morel, *MAT 449 : Representation theory* (2018), https://web.math.princeton.edu/~smorel/449/notes_449.pdf. Accessed 14/02/2021.

[MS21] Maarten Solleveld, *Affine Hecke Algebras and their Representations* (2021), https://arxiv.org/pdf/2009.03007.pdf. Accessed 31/05/21.

[Mur05] F. Murnaghan, *MAT445/1196F - Representation Theory Course Notes* (2005), http://www.math.toronto.edu/murnaghan/courses/mat445/notes.pdf. Accessed 15/02/2021.

[Mus93] C. Musili, *Representations of Finite Groups*, Texts and Readings in Mathematics, vol. 8, 1993, pp. 115–140.

[Pra05] A. Prasad, *On Bernstein's Presentation of Iwahori–Hecke Algebras and Representations of Split Reductive Groups over Non-Archimedian Local Fields* (2005), https://arxiv.org/pdf/math/0504417.pdf. Accessed 27/05/21.

[Rig96] L. J. Riggs, *Polynomial equations and solvability: A historical perspective*, California State University, San Bernardino, 1996.

[RW21] A. Romanov and G. Williamson, *Langlands correspondence and Bezrukavnikov's equivalence* (2021), https://arxiv.org/abs/2103.02329. Accessed 2/05/2021.

[Ter99] A. Terras, *Fourier Analysis on Finite Groups and Applications*, Cambridge University Press, London Mathematical Society, 1999.