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 2021

THE UNIVERSITY OF QUEENSLAND
SCHOOL OF MATHEMATICS AND PHYSICS

Contents

ACKNOWLEDGEMENTS

<center>INTRODUCTION</center>

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.
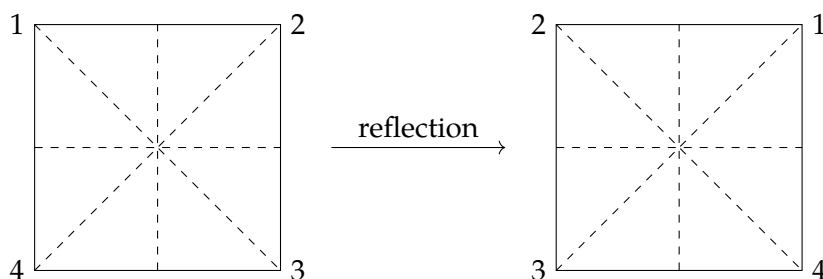

FIGURE 1. The symmetries of a square and a reflection about the vertical line of symmetry.

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*

$$\underbrace{T_i T_j T_i \ldots}_{m_{ij} \text{ terms}} = \underbrace{T_j T_i T_j \ldots}_{m_{ij} \text{ terms}}.$$

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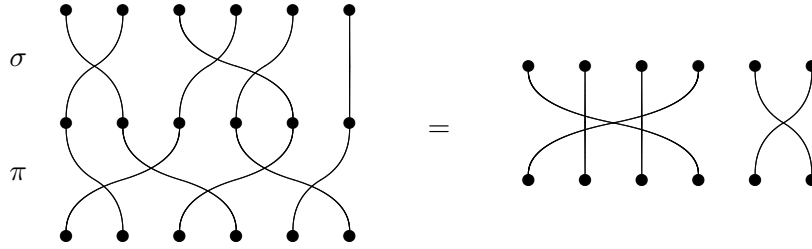
FIGURE 2. A braid diagram visualising the multiplication $\pi\sigma = (1\ 4)(5\ 6)$.

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

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

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 3, 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 4, 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 5, 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-archimedian 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.

$$
\begin{array}{ccccccc}
& \overset{\text{Ch. } 2}{\mathcal{H}(G,K,\sigma)} & \xrightarrow{\ \sigma=\mathbf{1}\ } & \overset{\text{Ch. } 1}{\mathcal{H}(G,K)} & \xleftarrow{\ G \text{ finite}\ } & \overset{\text{Ch. } 4}{C_c(K\backslash G/K)} & \xrightarrow{\ K=I\ } & \overset{\text{Ch. } 5}{C_c(I\backslash G/I)} \\
& & & \Big\downarrow{\scriptstyle G \text{ Lie type}} & & \Big\downarrow{\scriptstyle K=K^\circ} & & \\
& & & {\scriptstyle \text{over } \mathbb{F}_q} & & & & \\
& & & \mathcal{H}_q(W,S) & & C_c(K^\circ\backslash G/K^\circ) & & \\
& & & {\text{Ch. } 3} & & {\text{Ch. } 5} & &
\end{array}
$$

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-archimedian 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-archimedian 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 5.

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 $\mathbb{C}[\Lambda^\vee]$.

1. Hecke Algebras of Finite Groups

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

$$(f \star w)(gk) = \sum_{xy=gk} f(x)w(y) = \sum_{x \in G} f(x)w(x^{-1}gk)$$

$$= \sum_{x \in G} f(x)w(x^{-1}g) = \sum_{xy=g} f(x)w(y) = (f \star w)(g). \quad \square$$

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 $\Phi \colon \mathrm{Fun}(G) \to \mathbb{C}[G]$ 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 $\delta_{gh}(x)$. $\qquad\square$

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

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

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

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

$$= \frac{1}{|K|}\sum_{\substack{g\in G\\k\in K}}a_ge_g = \frac{1}{|K|}\sum_{k\in K}\sum_{g\in G}a_ge_g = \frac{1}{|K|}\sum_{k\in K}\Phi(f) = \Phi(f).$$

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*). $\qquad\square$

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

$$(\Psi(\alpha)(g\cdot w))(h) = ((g\cdot w)\star\alpha)(h) = \sum_{xy=h}w(g^{-1}x)\alpha(y) = \sum_{x\in G}w(g^{-1}x)\alpha(x^{-1}h)$$

$$= \sum_{ab=g^{-1}h}w(a)\alpha(b) = (g\cdot(w\star\alpha))(h) = (g\cdot\Psi(\alpha)(w))(h).$$

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. $\qquad\square$

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

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

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

$$\mathrm{Hom}_G(U_i, U_j) \cong \begin{cases} \mathbb{C}, & \text{if } U_i \cong U_j, \\ \{0\}, & \text{if } U_i \not\cong U_j. \end{cases}$$

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. $\qquad \square$

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. $\qquad \square$

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. $\qquad \square$

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

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

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 $\operatorname{Ind}_K^G \mathbf{1}$ 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

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

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:* $(O_{n+1}(\mathbb{F}_q), O_n(\mathbb{F}_q))$ *with* $q \neq 2^k$. We can embed the group $O_n(\mathbb{F}_q)$ inside $O_{n+1}(\mathbb{F}_q)$ by the injection

$$O_n(\mathbb{F}_q) \hookrightarrow O_{n+1}(\mathbb{F}_q), \quad A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}.$$

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 $(g_1 H, g_2 H) \mapsto Hg_1 g_2^{-1} H$.

Notice that $G/H := O_{n+1}(\mathbb{F}_q)/O_n(\mathbb{F}_q)$ 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 $g \in O_n(\mathbb{F}_q)$ 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 orthogonal 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 $\mathrm{Ind}_K^G\sigma$. 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** $\mathrm{Ind}_K^G\sigma$. Suppose that $\sigma\colon K\to\mathbb{C}^\times$ is a character, i.e. a group homomorphism. Consider the space

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

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

Lemma 14. 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

$$(f\star w)(gk)=\sum_{xy=gk}f(x)w(y)=\sum_{x\in G}f(x)w(x^{-1}gk)=\sum_{x\in G}f(x)w(x^{-1}g)\sigma(k)$$

$$=\left[\sum_{x\in G}f(x)w(x^{-1}g)\right]\sigma(k)=\left[\sum_{xy=g}f(x)w(y)\right]\sigma(k)=(f\star w)(g)\sigma(k).\quad\square$$

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

$$\mathcal{H}:=\{f\colon G\to\mathbb{C}\mid f(k_1gk_2)=\sigma(k_1)f(g)\sigma(k_2),\ \forall g\in G,\ \forall k_1,k_2\in K\}\subseteq\mathrm{Fun}(G).$$

The proof of Lemma 14 can be adapted to show that $\mathcal{H}$ is a two-sided ideal in $(\mathrm{Fun}(G),\star)$. As before, 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^σ, which we define below.

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

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. $\qquad\square$

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

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

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 $1 \le i \le j \le n$ and E_{ij} is the matrix of 0's except for a 1 in the ith row and j^{th} column. Notice that $x_{ij}(t) \in B$ since $i \le j$. 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: $g_{n,1} \ne 0$ 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 $g_{i1} \ne 0$ and $g_{nj} \ne 0$ 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. $\qquad\square$

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

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

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

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

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. $\qquad\square$

3. Hecke Algebras Generated by a Coxeter Group

The purpose of this section is to investigate the Hecke algebra obtained when we choose $G = \mathrm{SL}_n(\mathbb{F}_q)$ and $K = B(\mathbb{F}_q)$, the Borel subgroup of G, i.e. the subgroup of upper-triangular matrices in G. For this chapter, our convolution product associated to $\mathcal{H}$ is modified with a normalising factor $\frac{1}{|B|}$. We begin in Section 3.1 by investigating the Weyl group of G. We give its general definition and show that it reduces to the symmetric group S_n for our purposes. Next, in Section 3.2, we thoroughly describe the algebra $\mathcal{H}(G, B)$ in the simple case of $G = \mathrm{SL}_2(\mathbb{F}_q)$. We move to the more difficult cases of $G = \mathrm{SL}_3(\mathbb{F}_q)$ and $G = \mathrm{SL}_4(\mathbb{F}_q)$ in Sections 3.3 and 3.4 respectively. These examples lead us to the definition of a Coxeter group, given in Section 3.5. This chapter is concluded with the definition of a Hecke algebra of a finite Coxeter group and a complete description of $\mathcal{H}(G, B)$ in the general case. This is done so in Section 3.6.

3.1. **The Weyl group** W**.** Fix the group $G = \mathrm{GL}_n(\mathbb{F}_q)$. Consider the subgroup of diagonal matrices

$$T := \{\mathrm{diag}(a_1, \ldots, a_n) \mid a_i \in \mathbb{F}_q^\times\} \subseteq G.$$

This is a *maximal torus* of G. The *Weyl group* of G is defined as the quotient group $W := N_G(T)/T$, where $N_G(T) := \{t \in T \mid gTg^{-1} = T\}$ is the *normaliser* of T in G. The Weyl group may be understood as the reflection group of the *root system* associated to a Lie group G. It is a useful fact in [BD85] that all maximal tori are conjugate to each other over the algebraic closure of $\mathbb{F}_q$. As a result, W is independent of the choice of maximal tori, so we only need to consider the one we have chosen.

Our goal in this section is to show that $W \cong S_n$. To do this, we need a lemma.

Lemma 19. $N_G(T)$ *is the set of monomial matrices in* G.

Before we prove the lemma, we need a definition and a small fact about matrices. The *spectrum* of a matrix is the multiset of its eigenvalues. The fact we need is that conjugation preserves the spectrum of a matrix. More specifically, for any $A, B \in G$, the spectrums of A and BAB^{-1} coincide. To see this, notice

$$\det(BAB^{-1} - \lambda I) = \det(BAB^{-1} - \lambda BB^{-1}) = \det(B)\det(A - \lambda I)\det(B^{-1}) = \det(A - \lambda I).$$

We see that A and BAB^{-1} have the same characteristic polynomial which proves the fact.

Proof of Lemma 19. First, we show that the monomial matrices lie in $N_G(T)$. To see this, fix a monomial matrix $p = \sum_{i=1}^n a_i E_{i,\sigma(i)}$ for some $\sigma \in S_n$. It is not difficult to see that $p^{-1} = \sum_{i=1}^n a_i^{-1} E_{i,\sigma^{-1}(i)}$. To verify this, one can compute $(pp^{-1})_{ij} = \delta_{ij}$, so $pp^{-1} = I$. Now, take an arbitrary element $t = \sum_{i=1}^n b_i E_{ii} \in T$. We compute

$$(ptp^{-1})_{ij} = \sum_{k=1}^n (pt)_{ik}(p^{-1})_{kj} = \sum_{k=1}^n \left(\sum_{l=1}^n p_{il}t_{lk} \right)(p^{-1})_{kj} = \sum_{k=1}^n \sum_{l=1}^n p_{il}t_{lk}(p^{-1})_{kj}.$$

Notice p_{il} is non-zero if and only if $l = \sigma(i)$, t_{lk} is non-zero if and only if $l = k$ and $(p^{-1})_{kj}$ is non-zero if and only if $j = \sigma^{-1}(k)$. Then $(ptp^{-1})_{ij}$ is non-zero if and only if $\sigma(i) = \sigma(j)$, i.e. $i = j$. Thus, $ptp^{-1} = t'$ and $pt = t'p$ for some diagonal matrix $t' \in T$. This means p normalizes T in G.

Conversely, we show that a normaliser of T in G must be a monomial matrix. Let $s \in N_G(T)$. By definition of the normaliser, we know sts^{-1} is a diagonal matrix for each $t \in T$. Choose $t = \sum_{i=1}^n i E_{ii}$.

Then $sts^{-1} = w$ for some $w \in T$. The matrix t clearly has the spectrum $\{1, \dots, n\}$ and we know that conjugation preserves the spectrum, so $sts^{-1} = w$ has the same spectrum, up to permutation. We write $w = \sum_{i=1}^{n} \sigma(i)E_{ii}$ for some $\sigma \in S_n$ permuting the spectrum of t. The equation $sts^{-1} = w$ tells us that $st - ws = 0$. We compute

$$(st)_{ij} = \sum_{k=1}^{n} s_{ik}t_{kj} = js_{ij}, \quad (ws)_{ij} = \sum_{k=1}^{n} w_{ik}s_{kj} = \sigma(i)s_{ij}.$$

We put this together and see that

$$0 = (st - ws)_{ij} = (st)_{ij} - (ws)_{ij} = js_{ij} - \sigma(i)s_{ij} = s_{ij}(j - \sigma(i)).$$

This tells us that s_{ij} must be 0 if $j \neq \sigma(i)$ and s_{ij} can be arbitrary when $j = \sigma(i)$. This is exactly what it means for s to be a monomial matrix associated to σ. □

Proposition 20. $N_G(T)/T \cong S_n$.

Proof. Consider the map $f \colon N_G(T) \to G$ defined on matrix entries by

$$(f(g))_{ij} := \begin{cases} 1, & \text{if } g_{ij} \neq 0, \\ 0, & \text{if } g_{ij} = 0. \end{cases}$$

This sends the non-zero entries of $g \in N_G(T)$ to 1. Notice this is a group homomorphism with $\ker f = T$ and $\operatorname{im} f = \{\text{permutation matrices}\} \subseteq G$. Here a permutation matrix is a monomial matrix with its non-zero entries all equal to 1. The group of permutation matrices is isomorphic to S_n. Thus, the first isomorphism theorem tells us that $N_G(T)/T \cong S_n$. □

The above proof can be followed for the choice $G = \mathrm{SL}_n(\mathbb{F}_q)$ to see that its Weyl group is also S_n. Then, similarly to Lemma 18, we see that $\mathrm{SL}_n(\mathbb{F}_q)$ has its own Bruhat decomposition in terms of S_n. This is explicitly proven in [Bum13].

3.2. **A simple case,** $G = \mathrm{SL}_2(\mathbb{F}_q)$. We investigate the structure of the Hecke algebra $\mathcal{H}(G, K)$ when $G = \mathrm{SL}_2(\mathbb{F}_q)$ and $K = B(\mathbb{F}_q)$. Recall the Hecke algebra $\mathcal{H}(G, B) = \{f \colon G \to \mathbb{C} \mid f(bgb') = f(g)\}$. However, instead of the convolution product used throughout Chapter 1, we define the *normalised convolution product*

$$(f \star g)(x) := \frac{1}{|B|} \sum_{yz=x} f(y)g(z).$$

Notice that this normalising factor only affects the identity in $\mathcal{H}$. Specifically, it rescales the identity. In Section 1.3, we saw that $\mathcal{H}(G, K)$ has the identity ι_K. Under the normalised convolution product, it is easy to see that $\mathcal{H}(G, B)$ has identity χ_B, the characteristic function of B.

Consider the symmetric group $S_2 = \{1, s\}$. Note that s may be represented by the permutation matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. However, this has determinant -1 so it is not an element of $\mathrm{SL}_2(\mathbb{F}_q)$. However, we can swap a non-zero element from 1 to -1 so that s has the permutation matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ with determinant 1. In general, given the natural map $n \colon N_G(T) \to N_G(T)/T \cong S_n$, we say that $g \in N_G(T)$ is a *lift* of $w \in S_n$ if $n(g) = w$. We see that $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ is a lift of $s \in S_2$, but $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is not.

We have the Bruhat decomposition

$$\mathrm{SL}_2(\mathbb{F}_q) = \bigsqcup_{w \in S_2} BwB = B \sqcup BsB = \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q \end{pmatrix}}_{B} \sqcup \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{BsB}.$$

The Bruhat decomposition above and Section 1.3 tell us that $\mathcal{H}(G, B)$ has a basis $\{\chi_B, \chi_{BsB}\}$. For brevity, we write $I := \chi_B$ and $T := \chi_{BsB}$. We are interested in the products of these basis elements. The objective of this section is to show that

$$\mathcal{H}(G, B) = \langle T \mid T^2 = (q-1)T + qI \rangle.$$

To do this, we compute all possible convolution products: $I \star I$, $I \star T$, $T \star I$ and $T \star T$. The first three computations are clear, since I is the identity. The fourth computation requires more work. The basis of $\mathcal{H}(G, B)$ tells us that $T \star T = \alpha I + \beta T$ for some $\alpha, \beta \in \mathbb{C}$. Notice that

$$\alpha = (\alpha I + \beta T)(1) = (T \star T)(1), \quad \beta = (\alpha I + \beta T)(s) = (T \star T)(s).$$

Thus, it suffices to evaluate $T \star T$ at 1 and s. We compute

$$(T \star T)(1) = \frac{1}{|B|} \sum_{x \in G} \chi_{BsB}(x) \chi_{BsB}(x^{-1}) = \frac{1}{|B|} \sum_{x \in G} \chi_{BsB}(x) = \frac{1}{|B|} \sum_{x \in BsB} 1 = \frac{|BsB|}{|B|},$$

where the second equality comes from the observation that $G = B \sqcup BsB$ so $x \in BsB$ if and only if $x^{-1} \in BsB$. Notice that $B = \{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \neq 0 \}$. Thus, we have $q - 1$ choices for a and q choices for b, so $|B| = (q-1)q$. To compute $|BsB|$, notice that

$$BsB = \mathrm{SL}_2(\mathbb{F}_q) - B = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \, \middle| \, c \neq 0, \ ad - bc = 1 \right\} = \left\{ \begin{pmatrix} a & \frac{ad-1}{c} \\ c & d \end{pmatrix} \, \middle| \, c \neq 0 \right\}.$$

Thus, we have $q - 1$ choices for c and q choices for both a and d, so $|BsB| = (q-1)q^2$. Then $\alpha = |BsB|/|B| = q$. Next, we compute

$$(T \star T)(s) = \frac{1}{|B|} \sum_{x \in G} \chi_{BsB}(sx) \chi_{BsB}(x^{-1}) = \frac{1}{|B|} \sum_{x \in BsB} \chi_{BsB}(sx) \chi_{BsB}(x^{-1})$$

$$= \frac{|\{x \in BsB \mid sx \in BsB\}|}{|B|} = \frac{|\{x \in BsB \mid x \in s^{-1}BsB\}|}{|B|} = \frac{|BsB \cap s^{-1}BsB|}{|B|}.$$

Notice that, for arbitrary $g = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in B$, we have $s^{-1}gs = \begin{pmatrix} a^{-1} & 0 \\ -b & a \end{pmatrix}$ which is the general form of a lower-triangular matrix in $\mathrm{SL}_2(\mathbb{F}_q)$. Thus, $s^{-1}Bs =: B^-$, the subgroup of lower-triangular matrices in $\mathrm{SL}_2(\mathbb{F}_q)$. Then $s^{-1}BsB = B^-B$.

We wish to characterise B^-B. Consider the product

$$\underbrace{\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}}_{B^-} \underbrace{\begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix}}_{B} = \begin{pmatrix} ac & ad \\ bc & bd + a^{-1}c^{-1} \end{pmatrix}.$$

The entry ac is invertible and the entries bc, ad and $bd + a^{-1}c^{-1}$ are not necessarily invertible. Thus

$$B^-B = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q) \, \middle| \, a \neq 0 \right\}$$

and

$$BsB \cap B^-B = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q) \,\middle|\, a \neq 0, c \neq 0 \right\} = \left\{ \begin{pmatrix} a & b \\ c & \frac{1+bc}{a} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q) \,\middle|\, a \neq 0, c \neq 0 \right\}.$$

Thus, we have $q - 1$ choices for both a and c, and q choices for b, so $|BsB \cap B^-B| = (q-1)^2 q$. Then $\beta = |BsB \cap B^-B|/|B| = q - 1$.

We conclude that $T^2 = (q-1)T + qI$ and we may write

$$\mathcal{H}(G, B) = \langle T \mid T^2 = (q-1)T + qI \rangle.$$

This is known as the *quadratic relation*. The relation lets us prove the existence of the inverse of T. Define the function $X := q^{-1}T + (q^{-1} - 1)I \in \mathcal{H}(G, B)$. Observe that

$$T \star X = T \star (q^{-1}T + (q^{-1} - 1)I) = q^{-1}T^2 + (q^{-1} - 1)T$$
$$= q^{-1}((q-1)T + qI) + (q^{-1} - 1)T = (1 - q^{-1})T + I + (q^{-1} - 1)T = I.$$

Similarly, $X \star T = I$. Thus, X is the inverse of T and we may write $T^{-1} = q^{-1}T + (q^{-1} - 1)I$.

3.3. **A less simple case, $G = \mathrm{SL}_3(\mathbb{F}_q)$.** Consider the symmetric group

$$S_3 = \{1, s_1, s_2, s_1 s_2, s_2 s_1, s_1 s_2 s_1\} = \left\langle s_1, s_2 \,\middle|\, \begin{array}{l} s_1^2 = s_2^2 = 1, \\ s_1 s_2 s_1 = s_2 s_1 s_2 \end{array} \right\rangle.$$

The elements of S_3 have multiple permutation matrix representations in $\mathrm{SL}_3(\mathbb{F}_q)$, i.e. there are multiple lifts of each permutation. We fix the following representations

$$1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad s_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad s_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$s_1 s_2 = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \quad s_2 s_1 = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \quad s_1 s_2 s_1 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}.$$

Note that our choice of lifts of s_1 and s_2 do not matter, but these choices affect the matrix representations of $s_1 s_2$, $s_2 s_1$ and $s_1 s_2 s_1$. As in Section 3.2, we have the Bruhat decomposition

$$SL_3(\mathbb{F}_q) = \bigsqcup_{w \in S_3} BwB = B \sqcup Bs_1B \sqcup Bs_2B \sqcup Bs_1s_2B \sqcup Bs_2s_1B \sqcup Bs_1s_2s_1B.$$

The Bruhat decomposition tells us that $\mathcal{H}(G, K)$ has a basis $\{\chi_{BwB}\}_{w \in S_3}$. For brevity, we write $I := \chi_B$, $T := \chi_{Bs_1B}$ and $S := \chi_{Bs_2B}$. We are interested in the products of these elements. The objective of this section is to show that

$$\mathcal{H}(G, B) = \left\langle T, S \,\middle|\, \begin{array}{l} T^2 = (q-1)T + qI, \\ S^2 = (q-1)S + qI, \end{array} \ TST = STS \right\rangle.$$

To do this, we compute the convolution products $T \star T$, $S \star S$, $T \star S \star T$ and $S \star T \star S$. Recall that $\star$ is associative so the last two products are unambiguous. The basis of $\mathcal{H}(G, B)$ tells us that

$$(T \star T)(x) = (\alpha_1 \chi_B + \alpha_2 \chi_{Bs_1B} + \alpha_3 \chi_{Bs_2B} + \alpha_4 \chi_{Bs_1s_2B} + \alpha_5 \chi_{Bs_2s_1B} + \alpha_6 \chi_{Bs_1s_2s_1B})(x),$$

$$(S \star S)(x) = (\beta_1\chi_B + \beta_2\chi_{Bs_1B} + \beta_3\chi_{Bs_2B} + \beta_4\chi_{Bs_1s_2B} + \beta_5\chi_{Bs_2s_1B} + \beta_6\chi_{Bs_1s_2s_1B})(x),$$

$$(T \star S \star T)(x) = (\gamma_1\chi_B + \gamma_2\chi_{Bs_1B} + \gamma_3\chi_{Bs_2B} + \gamma_4\chi_{Bs_1s_2B} + \gamma_5\chi_{Bs_2s_1B} + \gamma_6\chi_{Bs_1s_2s_1B})(x),$$

$$(S \star T \star S)(x) = (\delta_1\chi_B + \delta_2\chi_{Bs_1B} + \delta_3\chi_{Bs_2B} + \delta_4\chi_{Bs_1s_2B} + \delta_5\chi_{Bs_2s_1B} + \delta_6\chi_{Bs_1s_2s_1B})(x),$$

for some $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{C}$. Notice that

$$\alpha_1 = (T \star T)(1), \ \alpha_2 = (T \star T)(s_1), \ \alpha_3 = (T \star T)(s_2),$$
$$\alpha_4 = (T \star T)(s_1s_2), \ \alpha_5 = (T \star T)(s_2s_1), \ \alpha_6 = (T \star T)(s_1s_2s_1).$$

The analogous statements are true for the other convolution products and their coefficients.

We begin by showing that $\alpha_i = 0$ for all $i \neq 1, 2$. For α_3, we compute

$$(T \star T)(s_2) = \frac{1}{|B|} \sum_{xy=s_2} \chi_{Bs_1B}(x)\chi_{Bs_1B}(y) = \frac{|\{(x,y) \in Bs_1B \times Bs_1B \mid xy = s_2\}|}{|B|}.$$

To compute the numerator, notice that

$$\underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{s_1} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix},$$

which tells us that Bs_1B is a subset of all matrices in $\mathrm{SL}_3(\mathbb{F}_q)$ with 0's in the bottom left and bottom middle entries. In fact, this is exactly Bs_1B. To see this, we compute:

$$\left| \left\{ \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix} \right\} \right| = q^4 \cdot (q-1)^2, \qquad \left| \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix} \right\} \right| = q^3 \cdot (q-1)^2.$$

It is a proposition of Bump in [Bum10] that $|Bs_1B|/|B| = q$, so $|Bs_1B| = q|B|$. This tells us that Bs_1B consists of all matrices of the form above.

We multiply two of these matrices together to see that

$$\underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{Bs_1B} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{Bs_1B} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}.$$

Then the product of two elements in Bs_1B will always have a 0 in the bottom left entry. However, s_2 has a 1 in the bottom left entry. Then $|\{(x,y) \in Bs_1B \times Bs_1B \mid xy = s_2\}| = 0$ and $\alpha_3 = 0$. Similarly, notice that s_1s_2, s_2s_1 and $s_1s_2s_1$ all have non-zero entries in the bottom left or bottom middle entry. This shows that $\alpha_4 = \alpha_5 = \alpha_6 = 0$ as well. Thus, $T^2 = \alpha_1 I + \alpha_2 T$.

Similarly, we show that $\beta_i = 0$ for all $i \neq 1, 3$. For β_2, we compute

$$(S \star S)(s_1) = \frac{1}{|B|} \sum_{xy=s_1} \chi_{Bs_2B}(x)\chi_{Bs_2B}(y) = \frac{|\{(x,y) \in Bs_2B \times Bs_2B \mid xy = s_1\}|}{|B|}.$$

To compute the numerator, notice that

$$\underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{s_2} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} = \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix},$$

which tells us that Bs_2B is a subset of all matrices in $\mathrm{SL}_3(\mathbb{F}_q)$ with 0's in the bottom left and middle left entries. As before, Bs_2B consists of all matrices of the form above. We multiply two of these matrices together to see that

$$\underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{Bs_2B} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{Bs_2B} = \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}.$$

Then the product of two elements in Bs_2B will always have a 0 in the middle left entry. However, s_1 has a 1 in the middle left entry. Then $|\{(x,y) \in Bs_2B \times Bs_2B \mid xy = s_1\}| = 0$ and $\beta_2 = 0$. Similarly, notice that s_1s_2, s_2s_1 and $s_1s_2s_1$ all have non-zero entries in the middle left or bottom left entry. This shows that $\beta_4 = \beta_5 = \beta_6 = 0$ as well. Thus, $S^2 = \beta_1 I + \beta_3 S$.

All that is left is to determine $\alpha_1, \alpha_2, \beta_1$ and β_3. Notice that if $x \in BwB$ for some $w \in W$, then $x = b_1wb_2$ and $x^{-1} = b_2^{-1}w^{-1}b_1^{-1} \in Bw^{-1}B$. If w is a simple reflection then $w^{-1} = w$. Thus $x \in Bs_iB$ if and only if $x^{-1} \in Bs_iB$ for $i = 1, 2$. We compute

$$\alpha_1 = (T \star T)(1) = \frac{1}{|B|} \sum_{x \in G} \chi_{Bs_1B}(x)\chi_{Bs_1B}(x^{-1}) = \frac{1}{|B|} \sum_{x \in G} \chi_{Bs_1B}(x) = \frac{|Bs_1B|}{|B|}.$$

To count $|Bs_1B|$, notice that the bottom rows and right columns of Bs_1B and B are the same (highlighted in red below):

$$\underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} \quad \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{Bs_1B}$$

This tells us that, when computing $|Bs_1B|/|B|$, the terms resulting from these columns and rows will cancel out. Thus, we only need to consider the submatrices obtained by deleting the bottom row and right column. Explicitly, we have

$$\frac{|Bs_1B|}{|B|} = \frac{\left|\left\{ \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix} \right\}\right|}{\left|\left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times \end{pmatrix} \right\}\right|}.$$

However, we have already performed this calculation in Section 3.2. We evaluated this to be q, so $\alpha_1 = q$. Similarly, for β_1, we compute

$$\beta_1 = (S \star S)(1) = \frac{1}{|B|} \sum_{x \in G} \chi_{Bs_2B}(x)\chi_{Bs_2B}(x^{-1}) = \frac{|\{x \in Bs_2B \mid x^{-1} \in Bs_2B\}|}{|B|}.$$

As before, s_2 is a simple reflection so $\beta_1 = |Bs_2B|/|B|$. To count $|Bs_2B|$, again, notice that the top rows and left columns of Bs_2B and B are the same (highlighted in red below):

$$\underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} \quad \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{Bs_2B}$$

This tells us that we only need to consider the submatrices obtained by deleting the top row and left column. Explicitly, we have

$$\frac{|Bs_2B|}{|B|} = \frac{\left| \left\{ \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix} \right\} \right|}{\left| \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times \end{pmatrix} \right\} \right|}.$$

We've already evaluated this to be q, so $\beta_1 = q$. Now we compute α_2. Notice

$$\alpha_2 = (T \star T)(s_1) = \frac{|\{x \in G \mid s_1 x \in Bs_1B,\ x^{-1} \in Bs_1B\}|}{|B|} = \frac{|\{x \in s_1^{-1}Bs_1B \mid x \in Bs_1B\}|}{|B|}.$$

We want to describe $s_1^{-1}Bs_1$. Notice $s_1^{-1} = s_1$. Then

$$\underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{s_1^{-1}} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{s_1} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} = \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}$$

We see that

$$s_1^{-1}Bs_1B \cap Bs_1B = \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix} \right\} \cap \left\{ \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix} \right\} = \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix} \right\}.$$

Notice that the bottom rows and right columns of $s_1^{-1}Bs_1B \cap Bs_1B$ and B are the same. This tells us that, when computing $|s_1^{-1}Bs_1B \cap Bs_1B|/|B|$, the terms resulting from this column and row will cancel out. Thus, we only need to consider the submatrices obtained by deleting the bottom row and right column. More specifically, we have

$$\frac{|s_1^{-1}Bs_1B \cap Bs_1B|}{|B|} = \frac{\left| \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix} \right\} \right|}{\left| \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times \end{pmatrix} \right\} \right|}.$$

However, we have already performed this calculation in Section 3.3. We evaluated this to be $q - 1$. Thus, $\alpha_2 = q - 1$. Similarly, notice

$$\beta_3 = (S \star S)(s_2) = \frac{|\{x \in G \mid s_2 x \in Bs_2B,\ x^{-1} \in Bs_2B\}|}{|B|} = \frac{|\{x \in s_2^{-1}Bs_2B \mid x \in Bs_2B\}|}{|B|}.$$

We want to describe $s_2^{-1} B s_2$. Notice $s_2^{-1} = s_2$. Then

$$\underbrace{\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{s_2^{-1}} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{s_2} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} = \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \end{pmatrix}.$$

We see that

$$s_2^{-1} B s_2 B \cap B s_2 B = \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \end{pmatrix} \right\} \cap \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix} \right\} = \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix} \right\}.$$

Again, notice that the top rows and left columns of $s_2^{-1} B s_2 B \cap B s_2 B$ and B are the same. We only need to consider the submatrices obtained by deleting the top row and left column. More specifically, we have

$$\frac{|s_2^{-1} B s_2 B \cap B s_2 B|}{|B|} = \frac{\left| \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix} \right\} \right|}{\left| \left\{ \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times \end{pmatrix} \right\} \right|}.$$

We've already evaluated this to be $q - 1$. Thus, $\beta_3 = q - 1$. This lets us conclude that

$$T^2 = (q-1)T + qI, \quad S^2 = (q-1)S + qI.$$

Lastly, we wish to show that $TST = STS$. To do this, we show that $\gamma_i = \delta_i$ for each i. Notice that

$$\begin{aligned}
\gamma_i - \delta_i &= ((T \star S) \star T)(w) - ((S \star T) \star S)(w) \\
&= \frac{1}{|B|^2} \sum_{x,y \in G} T(wxy)S(y^{-1})T(x^{-1}) - \frac{1}{|B|^2} \sum_{x,y \in G} S(wyx)T(x^{-1})S(y^{-1}) \\
&= \frac{1}{|B|^2} \sum_{x,y \in G} T(x^{-1})S(y^{-1})[T(wxy) - S(wyx)],
\end{aligned}$$

where $w \in S_3$ is chosen appropriately. For instance, to compute $\gamma_4 - \delta_4$, we choose $w = s_1 s_2$.

For $\gamma_1 - \delta_1$, we want to compute

$$\gamma_1 - \delta_1 = \frac{1}{|B|^2} \sum_{x,y \in G} T(x^{-1})S(y^{-1})[T(xy) - S(yx)].$$

For the summand to be non-zero, we require that $x \in B s_1 B$ and $y \in B s_2 B$. We look at the products xy and yx:

$$\underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{x} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{y} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix} \notin B s_1 B,$$

$$\underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{y} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{x} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \end{pmatrix} \notin Bs_2B.$$

We see that $T(xy) - S(yx)$ is always zero whenever $T(x^{-1})$ and $S(y^{-1})$ are non-zero, so this sum is always 0. Thus, $\gamma_1 = \delta_1$.

For $\gamma_2 - \delta_2$, we want to compute

$$\gamma_2 - \delta_2 = \frac{1}{|B|^2} \sum_{x,y \in G} T(x^{-1})S(y^{-1})[T(s_1 xy) - S(s_1 yx)].$$

For the summand to be non-zero, we require that $x \in Bs_1B$ and $y \in Bs_2B$. We look at the products $s_1 xy$ and $s_1 yx$:

$$\underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{s_1} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{x} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{y} = \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix} \notin Bs_1B,$$

$$\underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{s_1} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{y} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{x} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \end{pmatrix} \notin Bs_2B.$$

We see that $T(s_1 xy) - S(s_1 yx)$ is always zero whenever $T(x^{-1})$ and $S(y^{-1})$ are non-zero, so this sum is always 0. Thus, $\gamma_2 = \delta_2$.

For $\gamma_3 - \delta_3$, we want to compute

$$\gamma_3 - \delta_3 = \frac{1}{|B|^2} \sum_{x,y \in G} T(x^{-1})S(y^{-1})[T(s_2 xy) - S(s_2 yx)].$$

For the summand to be non-zero, we require that $x \in Bs_1B$ and $y \in Bs_2B$. We look at the products $s_2 xy$ and $s_2 yx$:

$$\underbrace{\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{s_2} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{x} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{y} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \end{pmatrix} \notin Bs_1B,$$

$$\underbrace{\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{s_2} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{y} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{x} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \end{pmatrix} \notin Bs_2B.$$

We see that $T(s_2 xy) - S(s_2 yx)$ is always zero whenever $T(x^{-1})$ and $S(y^{-1})$ are non-zero, so this sum is always 0. Thus, $\gamma_3 = \delta_3$.

For $\gamma_4 - \delta_4$, we want to compute

$$\gamma_4 - \delta_4 = \frac{1}{|B|^2} \sum_{x,y \in G} T(x^{-1})S(y^{-1})[T(s_1 s_2 xy) - S(s_1 s_2 yx)].$$

For the summand to be non-zero, we require that $x \in Bs_1 B$ and $y \in Bs_2 B$. We look at the products $s_1 s_2 xy$ and $s_1 s_2 yx$:

$$\underbrace{\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}}_{s_1 s_2} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{x} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{y} = \begin{pmatrix} 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \end{pmatrix} \notin Bs_1 B.$$

$$\underbrace{\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}}_{s_1 s_2} \underbrace{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & f & g \end{pmatrix}}_{y} \underbrace{\begin{pmatrix} h & i & j \\ k & l & m \\ 0 & 0 & n \end{pmatrix}}_{x} = \begin{pmatrix} fk & fl & fm + gn \\ -ah - bk & -ai - bl & -aj - bm - cn \\ -dk & -dl & -dm - en \end{pmatrix}.$$

For x to lie in $Bs_1 B$ and $y \in Bs_2 B$, we must have $afkn \neq 0$. For the product $s_1 s_2 yx$ to lie in $Bs_2 B$, we require $-dk = 0$. Since $k \neq 0$, we must have $d = 0$. However, this means $-dl = 0$, but we also require $-dl \neq 0$ for this product to lie in $Bs_2 B$. Then this product can never lie in $Bs_2 B$. We see that $T(s_2 xy) - S(s_2 yx)$ is always zero whenever $T(x^{-1})$ and $S(y^{-1})$ are non-zero, so this sum is always 0. Thus, $\gamma_4 = \delta_4$.

For $\gamma_5 - \delta_5$, we want to compute

$$\gamma_5 - \delta_5 = \frac{1}{|B|^2} \sum_{x,y \in G} T(x^{-1})S(y^{-1})[T(s_2 s_1 xy) - S(s_2 s_1 yx)].$$

For the summand to be non-zero, we require that $x \in Bs_1 B$ and $y \in Bs_2 B$. We look at the products $s_2 s_1 xy$ and $s_2 s_1 yx$:

$$\underbrace{\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}}_{s_2 s_1} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{x} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{y} = \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \end{pmatrix} \notin Bs_1 B,$$

$$\underbrace{\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}}_{s_2 s_1} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}}_{y} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{x} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \end{pmatrix} \notin Bs_2 B.$$

We see that $T(s_2 s_1 xy) - S(s_2 s_1 yx)$ is always zero whenever $T(x^{-1})$ and $S(y^{-1})$ are non-zero, so this sum is always 0. Thus, $\gamma_5 = \delta_5$.

For $\gamma_6 - \delta_6$, we will compute γ_6 and δ_6 seperately and show that they are equal. We want to compute

$$\gamma_6 = \frac{1}{|B|^2} \sum_{x,y \in G} T(x^{-1})S(y^{-1})T(s_1 s_2 s_1 xy).$$

We look at the product $s_1 s_2 s_1 xy$:

$$\underbrace{\begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}}_{s_1 s_2 s_1} \underbrace{\begin{pmatrix} h & i & j \\ k & l & m \\ 0 & 0 & \frac{1}{hl-ik} \end{pmatrix}}_{x} \underbrace{\begin{pmatrix} \frac{1}{dg-ef} & b & c \\ 0 & d & e \\ 0 & f & g \end{pmatrix}}_{y} = \begin{pmatrix} 0 & \frac{-f}{hl-ik} & \frac{-g}{hl-ik} \\ \frac{-k}{dg-ef} & -bk-dl-fm & -ck-el-gm \\ \frac{-h}{dg-ef} & -bh-di-fj & -ch-ei-gj \end{pmatrix}.$$

For x to lie in $Bs_1 B$, we require that $k \neq 0$ and $hl - ik \neq 0$ which can be restated at $i \neq \frac{hl}{k}$. Similarly, for y to lie in $Bs_2 B$, we require that $f \neq 0$ and $e \neq \frac{dg}{f}$.

We now investigate when the product $s_1 s_2 s_1 xy$ lies in $Bs_1 B$ which will lead to an easy evaluation of γ_6. First, we require that $\frac{-k}{dg-ef} \neq 0$ which is already true since $k \neq 0$. Secondly, we require that $\frac{-h}{dg-ef} = 0$ which tells us that $h = 0$. Next, we require that $-bh - di - fj = -di - fj = 0$. We arrange to rewrite this condition as $j = \frac{-di}{f}$. Lastly, we require that $-ch - ei - gj = -ei - gj \neq 0$. In other words, we require that $-ei - g(\frac{-di}{f}) = i(-e + \frac{dg}{f}) \neq 0$. This tell us that $i \neq 0$ and $-e + \frac{dg}{f} \neq 0$, which is already true since $y \in Bs_2 B$.

We see that $s_1 s_2 s_1 xy$ lies in $Bs_1 B$ when $f, i, k \neq 0$, $h = 0$, $j = \frac{-di}{f}$ and $b, c, d, e, g, l, m \in \mathbb{F}_q$ are arbitrary. Thus,

$$|B|\gamma_6 = \underbrace{q^7}_{b,c,d,e,g,l,m \in \mathbb{F}_q} \cdot \underbrace{(q-1)^3}_{f,i,k \neq 0} \cdot \underbrace{1}_{h=0} \cdot \underbrace{1}_{j=\frac{-di}{f}} = q^7(q-1)^3.$$

Now we want to compute

$$\delta_6 = \frac{1}{|B|^2} \sum_{x,y \in G} S(y^{-1})T(x^{-1})S(s_1 s_2 s_1 yx).$$

We look at the product $s_1 s_2 s_1 yx$:

$$\underbrace{\begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}}_{s_1 s_2 s_1} \underbrace{\begin{pmatrix} \frac{1}{dg-ef} & b & c \\ 0 & d & e \\ 0 & f & g \end{pmatrix}}_{y} \underbrace{\begin{pmatrix} h & i & j \\ k & l & m \\ 0 & 0 & \frac{1}{hl-ik} \end{pmatrix}}_{x} = \begin{pmatrix} -fk & -fl & -fm - \frac{g}{hl-ik} \\ -dk & -dl & -dm - \frac{e}{hl-ik} \\ \frac{-h}{dg-ef} - bk & \frac{-i}{dg-ef} - bl & \frac{-j}{dg-ef} - bm - \frac{c}{hl-ik} \end{pmatrix}.$$

Now we investigate when the product $s_1 s_2 s_1 yx$ lies in $Bs_2 B$ which will lead to an easy evaluation of δ_6. First, we require that $-fk \neq 0$ which is already true since $f, k \neq 0$. Secondly, we require that $-dk = 0$ which tells us that $d = 0$. Next, we require that $\frac{-h}{dg-ef} - bk = \frac{h}{ef} = 0$ which tells us that $e \neq 0$ and we can rearrange to see that $b = \frac{h}{efk}$. Lastly, we require that $\frac{-i}{dg-ef} - bl \neq 0$ which we can rearrange to see that $i \neq befl = (\frac{h}{efk})efl = \frac{hl}{k}$, which is already true since $x \in Bs_1 B$.

We see that $s_1 s_2 s_1 yx$ lies in $Bs_2 B$ when $e, f, k \neq 0$, $d = 0$, $b = \frac{h}{efk}$ and $c, g, h, i, j, l, m \in \mathbb{F}_q$ are arbitrary. Thus,

$$|B|\delta_6 = \underbrace{q^7}_{c,g,h,i,j,l,m \in \mathbb{F}_q} \cdot \underbrace{(q-1)^3}_{e,f,k \neq 0} \cdot \underbrace{1}_{d=0} \cdot \underbrace{1}_{b=\frac{h}{efk}} = q^7(q-1)^3.$$

Then $|B|(\gamma_6 - \delta_6) = 0$ and $\gamma_6 = \delta_6$. Thus, $TST = STS$. This completes our example of $G = \mathrm{SL}_3(\mathbb{F}_q)$ and we conclude that

$$\mathcal{H}(G, B) = \left\langle T, S \ \middle| \ \begin{array}{l} T^2 = (q-1)T + qI, \\ S^2 = (q-1)S + qI, \end{array} TST = STS \right\rangle.$$

As in Section 3.2, we can write down the inverses of T and S:

$$T^{-1} = q^{-1}T + (q^{-1} - 1)I, \quad S^{-1} = q^{-1}S + (q^{-1} - 1)I.$$

3.4. **An even less simple case,** $G = \mathrm{SL}_4(\mathbb{F}_q)$**.** Consider the symmetric group

$$S_4 = \left\langle s_1, s_2, s_3 \;\middle|\; \begin{array}{c} s_i^2 = 1, \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, \\ s_1 s_3 = s_3 s_1 \end{array} \right\rangle.$$

We fix a choice of permutation matrices in $\mathrm{SL}_4(\mathbb{F}_q)$ that generate S_4:

$$s_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; s_2 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; s_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

As before, $\mathcal{H}(G, K)$ has a basis $\{\chi_{BwB}\}_{w \in S_4}$. For brevity, we write $I := \chi_B$ and $T_i := \chi_{Bs_iB}$. The objective of this section is to show that

$$\mathcal{H}(G, B) = \left\langle T_1, T_2, T_3 \;\middle|\; \begin{array}{c} T_i^2 = (q-1)T_i + qI, \\ T_i T_{i+1} T_i = T_{i+1} T_i T_{i+1}, \\ T_1 T_3 = T_3 T_1 \end{array} \right\rangle.$$

We begin by investigating the structure of the double cosets Bs_1B, Bs_2B and Bs_3B. Observe that

$$\underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{s_1} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix},$$

$$\underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{s_2} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} = \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix},$$

$$\underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}}_{s_3} \underbrace{\begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{B} = \begin{pmatrix} \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \end{pmatrix}.$$

Notice that copies of $Bs_1B \subseteq \mathrm{SL}_3(\mathbb{F}_q)$ and $Bs_2B \subseteq \mathrm{SL}_3(\mathbb{F}_q)$ from the previous example (highlighted in blue and red with their common entries in purple) lie in these three double cosets in $\mathrm{SL}_4(\mathbb{F}_q)$. We

multiply two matrices belonging to Bs_1B together to see that

$$\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix} \underbrace{\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}}_{Bs_1B} = \begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}.$$

Then the product of two elements in Bs_1B lies in Bs_1B. The same is true for Bs_2B and Bs_3B.

After making these observations, it is clear that the $\mathrm{SL}_4(\mathbb{F}_q)$ case will reduce to the $\mathrm{SL}_3(\mathbb{F}_q)$ case when verifying the relations $T_i^2 = (q-1)T_i + qI$ and $T_iT_{i+1}T_i = T_{i+1}T_iT_{i+1}$, just as verifying these conditions reduced to the $\mathrm{SL}_2(\mathbb{F}_q)$ case. However, we must still manually verify the relation $T_1T_3 = T_3T_1$. First, we write

$$T_1T_3 = \sum_{w \in S_4} \alpha_w \chi_{BwB}, \quad T_3T_1 = \sum_{w \in S_4} \beta_w \chi_{BwB}.$$

Then we may write

$$\alpha_w - \beta_w = \frac{1}{|B|} \sum_{x \in G} T_3(x^{-1})[T_1(wx) - T_1(xw)].$$

For the summand to be non-zero, we require that $x \in Bs_3B$. Fix $x \in Bs_3B$, so it has the form

$$x = \begin{pmatrix} \frac{1}{e(hk-ij)} & b & c & d \\ 0 & e & f & g \\ 0 & 0 & h & i \\ 0 & 0 & j & k \end{pmatrix},$$

with $ej \neq 0$ and $i \neq \frac{hk}{j}$. Notice that if $wx \notin Bs_1B$ and $xw \notin Bs_1B$ then $T_1(wx) - T_1(xw) = 0$. We show that if $w \neq s_1s_3$ then $wx \notin Bs_1B$ and $xw \notin Bs_1B$ (hence, $\alpha_w - \beta_w = 0$ for all $w \in S_4 - \{s_1s_3\}$). The contrapositive of this statement is that if $wx \in Bs_1B$ or $xw \in Bs_1B$ then $w = s_1s_3$, which we now prove.

Suppose that $wx \in Bs_1B$. Note that left-multiplication by w permutes the rows of x according to w. Recall that elements of Bs_1B have the form

$$\begin{pmatrix} \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ \mathbb{F}_q^\times & \mathbb{F}_q & \mathbb{F}_q & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^\times & \mathbb{F}_q \\ 0 & 0 & 0 & \mathbb{F}_q^\times \end{pmatrix}.$$

We see that, for wx to lie in Bs_1B, w must perform the row operation $R_1 \mapsto R_2$. We also see that w must not perform the row operations $R_2 \mapsto R_3$ or $R_2 \mapsto R_4$ since $e \neq 0$. This means w must perform the row operation $R_2 \mapsto R_1$. Lastly, w cannot perform the row operation $R_4 \mapsto R_4$ since $j \neq 0$. This means w must be the permutation matrix $s_1s_3 = (1\ 2)(3\ 4) \in S_4$.

Similarly, suppose that $xw \in Bs_1B$. Note that right-multiplication by w permutes the columns of x according to w. We see that w cannot perform the column operation $C_1 \mapsto C_1, C_1 \mapsto C_3$ or $C_1 \mapsto C_4$ since the bottom three entries of C_1 are 0. Then w must perform the column operation $C_1 \mapsto C_2$. We also see that w cannot perform the column operation $C_2 \mapsto C_3$ or $C_2 \mapsto C_4$ since the bottom two entries of C_2 are

0. Then w must perform the column operation $C_2 \mapsto C_1$. Lastly, w cannot perform the column operation $C_3 \mapsto C_3$ since $j \neq 0$. This means w must be the permutation matrix $s_1 s_3 = (1\ 2)(3\ 4) \in S_4$.

We have shown that $\alpha_w = \beta_w$ for all $w \in S_4 - \{s_1 s_3\}$. Now we show that $\alpha_{s_1 s_3} = \beta_{s_1 s_3}$ by manually computing both coefficients. Observe that

$$\alpha_{s_1 s_3} = (T_1 \star T_3)(s_1 s_3) = \frac{1}{|B|} \sum_{x \in G} T_1(s_1 s_3 x) T_3(x^{-1}),$$

$$\beta_{s_1 s_3} = (T_3 \star T_1)(s_1 s_3) = \frac{1}{|B|} \sum_{x \in G} T_3(x^{-1}) T_1(x s_1 s_3).$$

To count $\alpha_{s_1 s_3}$, we count how many ways $s_1 s_3 x$ can lie in $B s_1 B$. We compute

$$
\underbrace{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{s_1}
\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}}_{s_3}
\underbrace{\begin{pmatrix} \frac{1}{e(hk-ij)} & b & c & d \\ 0 & e & f & g \\ 0 & 0 & h & i \\ 0 & 0 & j & k \end{pmatrix}}_{x}
= \begin{pmatrix} 0 & -e & -f & -g \\ \frac{1}{e(hk-ij)} & b & c & d \\ 0 & 0 & -j & -k \\ 0 & 0 & h & i \end{pmatrix}.
$$

For $s_1 s_3 x$ to lie in $B s_1 B$, we require that $h = 0$. We also require that $i \neq 0$ but this is already true since we require that $i \neq \frac{hk}{j} = 0$. We also require that $j \neq 0$ and $\frac{1}{e(hk-ij)} \neq 0$ but these are already true since $x \in B s_3 B$. Overall, we require that $e, i, j \neq 0$, $h = 0$ and $b, c, d, f, g, k \in \mathbb{F}_q$. Thus,

$$|B| \alpha_{s_1 s_3} = \underbrace{q^6}_{b,c,d,f,g,k \in \mathbb{F}_q} \cdot \underbrace{(q-1)^3}_{e,i,j \neq 0} \cdot \underbrace{1}_{h=0} = q^6 (q-1)^3.$$

To count $\beta_{s_1 s_3}$, we count how many ways $x s_1 s_3$ can lie in $B s_1 B$. We compute

$$
\underbrace{\begin{pmatrix} \frac{1}{e(hk-ij)} & b & c & d \\ 0 & e & f & g \\ 0 & 0 & h & i \\ 0 & 0 & j & k \end{pmatrix}}_{x}
\underbrace{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{s_1}
\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}}_{s_3}
= \begin{pmatrix} b & \frac{-1}{e(hk-ij)} & d & -c \\ e & 0 & g & -f \\ 0 & 0 & i & -h \\ 0 & 0 & k & -j \end{pmatrix}.
$$

For $x s_1 s_3$ to lie in $B s_1 B$, we require that $k = 0$. We also require that $i \neq 0$ but this is already true since we require that $i \neq \frac{hk}{j} = 0$. We also require that $j \neq 0$ and $\frac{1}{e(hk-ij)} \neq 0$ but these are already true since $x \in B s_3 B$. Overall, we require that $e, i, j \neq 0$, $k = 0$ and $b, c, d, f, g, h \in \mathbb{F}_q$. Thus,

$$|B| \beta_{s_1 s_3} = \underbrace{q^6}_{b,c,d,f,g,h \in \mathbb{F}_q} \cdot \underbrace{(q-1)^3}_{e,i,j \neq 0} \cdot \underbrace{1}_{k=0} = q^6 (q-1)^3.$$

Then $|B|(\alpha_{s_1 s_3} - \beta_{s_1 s_3}) = 0$ and $\alpha_{s_1 s_3} = \beta_{s_1 s_3}$. Thus $T_1 T_3 = T_3 T_1$. This completes our example of $G = \mathrm{SL}_4(\mathbb{F}_q)$ and we conclude that

$$\mathcal{H}(G, B) = \left\langle T_1, T_2, T_3 \ \middle| \ \begin{array}{c} T_i^2 = (q-1)T_i + qI, \\ T_i T_{i+1} T_i = T_{i+1} T_i T_{i+1}, \\ T_1 T_3 = T_3 T_1 \end{array} \right\rangle.$$

As in the previous cases, we can write down the inverse of T_i:

$$T_i^{-1} = q^{-1} T_i + (q^{-1} - 1)I.$$

3.5. **Coxeter groups.** The previous sections illustrate a relationship between the Weyl group $W \cong S_n$ and the relations generating $\mathcal{H}(G, B)$. In particular, generators of S_n are subject to the braid relation $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$, whereas generators of $\mathcal{H}(G, B)$ are subject to the relation $T_i T_{i+1} T_i = T_{i+1} T_i T_{i+1}$. Similarly, generators of S_n are subject to the commuting relation $s_i s_j = s_j s_i$ for $|i - j| > 1$, whereas the generators of $\mathcal{H}(G, B)$ are subject to a similiar relation $T_i T_j = T_j T_i$ for $|i - j| > 1$.

We make some observations about S_n. Firstly, note that S_n may be generated by a finite set of elements $\{s_1, s_2, \ldots, s_{n-1}\}$, where each element is the simple transposition $s_i = (i \ i + 1)$. Next, notice that each generating element satisfies $s_i^2 = 1$, so they are involutions. The braid relation may be rewritten as $(s_i s_{i+1})^3 = 1$ since s_i and s_{i+1} are involutions. Similarly, the commuting relation may be rewritten as $(s_i s_j)^2 = 1$. Notice that each of these three properties may be expressed as $(s_i s_j)^{m_{ij}} = 1$ for some sequence $(m_{ij})_{i,j=1,\ldots,n-1}$. Here $m_{ii} = 1$, $m_{i,i+1} = 3$ and $m_{ij} = 2$ for $|i - j| > 1$. This information can be encoded in the matrix

$$M = \begin{pmatrix} 1 & 3 & 2 & \cdots & 2 \\ 3 & 1 & 3 & \ddots & \vdots \\ 2 & 3 & 1 & \ddots & 2 \\ \vdots & \ddots & \ddots & \ddots & 3 \\ 2 & \cdots & 2 & 3 & 1 \end{pmatrix}.$$

Generally we say that W is a *Coxeter group*, and (W, S) is a *Coxeter system* with *Coxeter matrix* $M = (m_{ij})$ if W is generated by the finite set $S = \{s_1, \ldots, s_n\}$ subject to the relations $(s_i s_j)^{m_{ij}} = 1$, where $m_{ii} = 1$ and $m_{ij} \in \{2, 3, 4, \ldots, \infty\}$ with the convention that $m_{ij} = \infty$ means no relation is imposed [Hum90].

A few important consequences are immediate from this definition. It is easy to see that s_i and s_j commute if and only if $m_{ij} = 2$. Furthermore, M must always be a symmetric matrix. To see this, notice $(s_j s_i)^{m_{ij}} = (s_j s_i)^{m_{ij}} s_j s_j = s_j (s_i s_j)^{m_{ij}} s_j = s_j s_j = 1$. Thus, $m_{ji} = m_{ij}$.

We will restrict our attention to finite Coxeter groups. Note that all finite Weyl groups are examples of finite Coxeter groups.

3.6. **The Hecke algebra $\mathcal{H}_q(W, S)$.** Fix the field $\mathbb{F}_q$. The Hecke algebra generated by the finite Coxeter group (W, S) over $\mathbb{F}_q$ is denoted $\mathcal{H}_q(W, S)$, and is the algebra generated by an identity I and $\{T_s\}_{s \in S}$ subject to the quadratic relation $T_s^2 = (q - 1)T_s + qI$ and the braid relations

$$\underbrace{T_s T_t T_s \cdots}_{m_{st} \text{ terms}} = \underbrace{T_t T_s T_t \cdots}_{m_{st} \text{ terms}}.$$

Let $G = \mathrm{SL}_n(\mathbb{F}_q)$ and $B = B(\mathbb{F}_q)$. Sections 3.2, 3.3 and 3.4 illustrate that $\mathcal{H}(G, B)$ is actually a Hecke algebra generated by the Coxeter group S_n. Then we may write

$$\mathcal{H}(G, B) = \left\langle T_1, T_2, \ldots, T_3 \ \middle| \ \begin{array}{c} T_i^2 = (q - 1)T_i + qI, \\ \underbrace{T_i T_j T_i \cdots}_{m_{ij} \text{ terms}} = \underbrace{T_j T_i T_j \cdots}_{m_{ij} \text{ terms}} \end{array} \right\rangle.$$

More generally, if G is a group of Lie type over a finite field, B is its Borel subgroup, and (W, S) is the Coxeter system of its Weyl group, then $\mathcal{H}(G, B) = \mathcal{H}_q(W, S)$.

In [Cox35], Coxeter presented a classification of the finite Coxeter groups. This contains four infinite families of groups, and eight other groups. One of these infinite families are the dihedral groups, D_{2n}. Recall that the dihedral group has the familiar presentation $\langle r, f \mid r^m = f^2 = (rf)^2 = 1 \rangle$, where r represents a rotation of the n-gon by $\frac{2\pi}{n}$ radians and f represents a flip of the n-gon. Notice that there is another presentation $\langle s, t \mid s^2 = t^2 = (st)^n = 1 \rangle$. Then D_{2n} has the Coxeter matrix $\left(\begin{smallmatrix} 1 & n \\ n & 1 \end{smallmatrix} \right)$. We conclude that the Hecke algebra generated by D_{2n} over $\mathbb{F}_q$ is given by

$$\mathcal{H}_q(D_{2n}, \{s, t\}) = \left\langle T_s, T_t \;\middle|\; \begin{array}{c} T_s^2 = (q-1)T_s + qI, \\ T_t^2 = (q-1)T_t + qI, \end{array} \; \underbrace{T_s T_t T_s \ldots}_{n \text{ terms}} = \underbrace{T_t T_s T_t \ldots}_{n \text{ terms}} \right\rangle.$$

4. Hecke Algebras of Locally Compact Groups

This chapter is devoted to generalising the notion of the Hecke algebra of a finite group. In particular, we weaken the condition that G and K must be finite to the condition that G must be a locally compact topological group and K must be a compact subgroup. We add the additional assumption that the functions in the Hecke algebra must have compact support. This is done for technical purposes, namely so that the functions of the Hecke algebra may be expressed as finite sums of basis elements. Since our groups are not longer finite, the convolution product on $\mathrm{Fun}(G)$ defined in Section 1.1 no longer results in a finite sum of $\mathbb{C}$-valued functions, so it cannot be used. To deal with this, we must introduce the notion of the Haar measure. This allows us to define the convolution product in terms of an integral with respect to the Haar measure. We see that this new Hecke algebra reduces to the Hecke algebra of Chapter 1 when G is finite.

4.1. **Locally compact groups and Haar measures.** We say that a group G is a *topological group* if it is equipped with a topology such that the group multiplication map $\mu\colon G \times G \to G$ and the group inversion map $\iota\colon G \to G$ are continuous. Here the product space $G \times G$ is equipped with the product topology.

We can equip any group with the discrete topology (i.e. the topology where all sets are open) to form a topological group. Some more interesting examples to keep in mind are:

  (*i*) $(\mathbb{R}^n, +)$ equipped with the Euclidean topology.
 (*ii*) $(\mathbb{Q}, +)$ equipped with the subspace topology from $\mathbb{R}^n$.
(*iii*) $\mathrm{GL}_n(\mathbb{R})$. This may be viewed as a subspace of $\mathbb{R}^{n^2}$ via an 'obvious' injection (see below).
 (*iv*) $\mathrm{O}_n(\mathbb{R})$. This is a subgroup of $\mathrm{GL}_n(\mathbb{R})$ and is equipped with the subspace topology.
  (*v*) $\mathrm{GL}_n(\mathbb{F}_q[\![t]\!])$ and $\mathrm{GL}_n(\mathbb{F}_q(\!(t)\!))$. Here $\mathbb{F}_q[\![t]\!]$ is the field of formal power series over $\mathbb{F}_q$ in the variable t and $\mathbb{F}_q(\!(t)\!)$ is the field of formal Laurent series over $\mathbb{F}_q$ in variable t. More generally, we may take GL_n over any non-archimedian local field k or its ring of integers $\mathcal{O}$ (see Chapter 5).

Recall that a topological space is *compact* if every open cover contains a finite subcover. Furthermore, a topological space is *locally compact* if every point has a compact neighbourhood. We say that a topological group G is (locally) compact if its associated topological space is (locally) compact. Some examples are $\mathrm{O}_n(\mathbb{R})$ (compact), $\mathrm{GL}_n(\mathbb{F}_q[\![t]\!])$ (compact) and $\mathrm{GL}_n(\mathbb{F}_q(\!(t)\!))$ (locally compact).

In order to define the Hecke algebra of a locally compact group, we want to define a notion of integration over topological groups. Those familiar with measure theory should already know that this requires the notion of measurable sets, measurable functions and measures. To this end, we present some concepts from measure theory. See [Fol84] for details.

The topology of G can be used to generate a *σ-algebra* on G. Here a σ-algebra on G means a collection of subsets of G that includes G, is closed under set-complements in G, and is closed under countable unions. De Morgan's laws tell us that this implies closure under countable intersections as well. The σ-algebra induced by the topology of G is called the *Borel σ-algebra* is the σ-algebra generated by the open sets of G. That is, every open set is contained in the Borel σ-algebra, along with every complement, countable union and countable intersection as well.

We call the elements of a σ-algebra *measurable sets*. Given a σ-algebra, we can define a notion of length on the measurable sets. Suppose that Σ is a σ-algebra. The function $\mu\colon \Sigma \to [0,\infty]$ is a *measure* if $\mu(\varnothing) = 0$, and whenever the sets $E_1, E_2, \ldots \in \Sigma$ are disjoint, there holds the countable additivity property

$$\mu\left(\bigcup_{i=1}^{\infty} E_i\right) = \sum_{i=1}^{n} \mu(E_i).$$

A consequence of the above property is the countable sub-additivity property: if $E_1, E_2, \ldots \in \Sigma$ is any sequence (not necessarily disjoint), then there holds

$$\mu\left(\bigcup_{i=1}^{\infty} E_i\right) \leq \sum_{i=1}^{n} \mu(E_i).$$

Now fix a locally compact topological group G and fix Σ to be the Borel σ-algebra of G. A *left Haar measure* on G is a non-zero measure $\mu_l\colon \Sigma \to [0,\infty]$ such that, for all $g \in G$ and $S \in \Sigma$, there holds $\mu_l(gS) = \mu_l(S)$, $\mu_l(K) < \infty$ for all compact $K \subseteq G$, and

$$\mu_l(S) = \inf\{\mu_l(U) \mid \text{open } U \supseteq S\} = \sup\{\mu_l(K) \mid \text{compact } K \subseteq S\}.$$

This last condition is called *regularity* of μ_l. Here the set gS is the *left-translation* of S by g. A *right Haar measure* μ_r is defined similarly, instead with the right-translation invariance property that $\mu_r(Sg) = \mu_r(S)$.

In [Fol84], it is shown that all locally compact topological groups possess a left/right Haar measure. Furthermore, this Haar measure is unique up to a positive scalar multiple. Then we do not need to concern ourselves with the question of existence and uniqueness of Haar measures.

A familiar example of a left Haar measure is the Lebesgue measure on $\mathbb{R}^n$. This is an abelian group, so the left Haar measure is also clearly a right Haar measure. We investigate the relationship between left and right Haar measures now.

Let μ be a left Haar measure on G. Take $x \in G$ and some measurable subset $E \subseteq G$. Then the measure μ_x defined by $\mu_x(E) := \mu(Ex)$ is also a left Haar measure by the associativity of G. Then, since all left Haar measures are a scalar multiple of each other, there exists a scalar $\Delta(x)$ such that $\mu_x = \Delta(x)\mu$. This defined a function $\Delta\colon G \to (0,\infty)$ called the *modular function* of G. This is a continuous group homomorphism from G to $(0,\infty)$.

The modular function describes the relationship between left and right Haar measures. Specifically, left and right Haar measures coincide when $\Delta \equiv 1$. A locally compact group for which every left Haar measure is also a right Haar measure is called *unimodular*.

We present some propositions in [Fol84].

Proposition 21. *If $G/[G,G]$ is finite the G is unimodular.*

Proof. The modular function is a continuous group homomorphism from G to $(0,\infty)$, the latter of which is abelian. Then this map Δ must annihilate the commutators $[x,y]$ for all x and y, so it must factor through $G/[G,G]$. Since $G/[G,G]$ is finite, we know $\Delta(G)$ is a finite subgroup of $(0,\infty)$. However, the only finite subgroup of $(0,\infty)$ is the trivial subgroup. $\qquad\square$

Proposition 22. *If G is compact then G is unimodular.*

Proof. It's clear that $G = Gx$, for any $x \in G$. Now let μ be a left Haar measure and notice

$$\mu(G) = \mu(Gx) = \Delta(x)\mu(G).$$

Since G is compact, we have $0 < \mu(G) < \infty$. Then we must have $\Delta(x) = 1$ for any choice of x. $\qquad\square$

We sketch an example of a Haar measure for the case $G = \mathrm{GL}_2(\mathbb{R})^+$, the subgroup of $\mathrm{GL}_2(\mathbb{R})$ of matrices with positive determinants. We may identify $\mathrm{GL}_2(\mathbb{R})^+$ with an open subset of $\mathbb{R}^4$. Specifically, we make the identification

$$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \longleftrightarrow (x_1, x_2, x_3, x_4).$$

Now take a measurable set $E \subseteq \mathrm{GL}_2(\mathbb{R})^+$. To define the measure of E, we employ the Lebesgue measure on $\mathbb{R}^4$. Specifically, define the measure of E by

$$\mu(E) := \int_E \frac{1}{(x_1 x_4 - x_2 x_3)^2} \, dx_1 dx_2 dx_3 dx_4 = \int_E \frac{1}{(\det x)^2} \, dx,$$

where the left integral is easily understood as the Lebesgue integral of a real-valued function on $\mathbb{R}^4$. To show that μ is a Haar measure, we note that the Lebesgue integral endows μ with many properties. It is clear that μ will be non-negative, positive definite, countably additive, finite on compact sets and regular. The only property left to check is left-translation invariance. To check this, fix $g \in \mathrm{GL}_2(\mathbb{R})^+$ and we consider the translation map $T_g \colon \mathbb{R}^4 \to \mathbb{R}^4$ given by $T_g(x) := gx$. Then we have

$$\mu(gE) = \int_{T(E)} \frac{1}{(\det x)^2} \, dx_1 dx_2 dx_3 dx_4.$$

We make the change of variables $x = T_g(y) = gy$ which yields

$$\mu(gE) = \int_E \frac{1}{(\det gy)^2} \, \mathrm{Jac}\, T_g \, dy_1 dy_2 dy_3 dy_4,$$

where $\mathrm{Jac}\, T_g$ is the Jacobian of the transformation T_g. One can compute $\mathrm{Jac}\, T_g = (\det g)^2$ which allows us to compute

$$\mu(gE) = \int_E \frac{1}{(\det gy)^2} \, \mathrm{Jac}\, T_g \, dy_1 dy_2 dy_3 dy_4 = \int_E \frac{1}{(\det y)^2} \, dy_1 dy_2 dy_3 dy_4 = \mu(E).$$

We see that μ is left-translation invariant and μ is indeed a left Haar measure.

4.2. **The Hecke algebra of a locally compact group** $C_c(K\backslash G/K)$**.** Consider a unimodular locally compact topological group G and some open and compact subgroup K. Note that a non-trivial K might not exist for some choices of G. However, we will see in Chapter 5 that non-trivial choices for K exist when G is a matrix group over a non-archimedian local field.

Then the Hecke algebra $C_c(K\backslash G/K)$ is defined as

$$C_c(K\backslash G/K) := \{f \colon G \to \mathbb{C} \mid \mathrm{supp}\, f \text{ is compact, and } f(k_1 g k_2) = f(g), \ \forall g \in G, \ \forall k_1, k_2 \in K\}.$$

Notice that, since K is open and compact, the topological space $K\backslash G/K$ is discrete. This means that a function on $K\backslash G/K$ having compact support is equivalent to it having finite support.

Clearly $C_c(K\backslash G/K)$ has the structure of a complex vector space. We wish to endow it with the structure of an algebra. To this end, we equip the space with the convolution product defined by

$$(f \star f')(x) = \int_G f(xg)f'(g^{-1})\, d\mu(g),$$

where $d\mu(g)$ denotes integration with respect to the Haar measure μ in the variable g. Recall that μ is unique up to a scalar multiple. It is common to choose this scalar so that $\mu(K) = 1$, which uniquely fixes μ. As in Chapter 1, the Hecke algebra here is an associative algebra.

It is natural to ask whether or not this construction of the Hecke algebra is a true generalisation of the Hecke algebra throughout Chapter 1. In other words, we want to recover the usual definitions of $\star$ and $\mathcal{H}$ is the case that G is a finite group.

To this end, let G be finite and equipped with the discrete topology (i.e. every subset is open). In this topology, every subset is compact. Then it is easy to see that G is locally compact. Furthermore, the Borel σ-algebra will contain every subset of G.

Define the function $\mu\colon \Sigma \to [0, \infty]$ by $\mu(A) := |A|$, the cardinality of A. It is easy to verify that this is a measure and it is known as the *counting measure*. To see that it is a Haar measure, we can see that μ is left-invariant since $|S| = |gS|$ for any $g \in G$ and $S \subseteq G$. Secondly, notice that $\mu(K) < \infty$ for all compact K since every subset of G is finite. Lastly, since every subset of G is open and compact, sub-additivity of measures tells us that the condition $\mu(S) = \inf\{\mu(U) \mid \text{open } U \supseteq S\} = \sup\{\mu(K) \mid \text{compact } K \subseteq S\}$ is satisfied by picking $U = K = S$.

Next, notice that in this setting, all functions $G \to \mathbb{C}$ have compact support. Then pick two functions $f, f'\colon G \to \mathbb{C}$ and any $x \in G$. Observe that

$$(f \star f')(x) = \int_G f(xg)f'(g^{-1})\, d\mu(g) = \sum_{x \in G} f(xg)f'(g^{-1}) = \sum_{yz=x} f(y)f'(z),$$

since μ is the counting measure. We see that we truly recover the previous results of Chapter 1 when we choose G to be a finite group.

5. Spherical Hecke Algebras and Iwahori–Hecke Algebras

In this chapter, we investigate two Hecke algebras: the spherical Hecke algebra and the Iwahori–Hecke algebra. In order to define these algebras, we require an understanding of local fields and their structure. In Section 5.1, we present the notions of a field extension, finite extension, absolute values and the p-adic numbers. This allows us to succinctly classify all local fields. Next, we describe the structure of local fields in Section 5.2 and explicitly compute some of these objects to aid in our understanding of these fields. We define the spherical Hecke algebra and give a proof that it is commutative. We conclude with the definition of the Iwahori subgroup and an investigation of the Iwahori–Hecke algebra.

5.1. **Local fields.** Fix a field F. We call $K \subset F$ a *subfield* of F if K is a field with respect to the addition and multiplication operations equipped to F. There are many immediate examples. For instance, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$, $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, and so on.

If $K \subset F$ is a subfield then we call F a *field extension* of K and denote this extension by F/K. The *degree* of the extension F/K is the dimension of F when considered as a K-vector space. The degree of F/K is written $[F : K]$ and we say F/K is a *finite extension* when $[F : K] < \infty$.

For instance, there holds $[\mathbb{C} : \mathbb{R}] = 2$. To see this, we consider $\mathbb{C}$ as a real vector space. We convince ourselves that $\{1, i\}$ is an appropriate basis that demonstrates $\mathbb{C}/\mathbb{R}$ is a field extension of degree 2.

As another example, consider $[\mathbb{R} : \mathbb{Q}]$. We can think of infinitely many irrational numbers that are not rational scalar multiples of each other. For example, $\sqrt{2}, \log 3, \pi$, and so on. This tells us that we can't find a finite basis for $\mathbb{R}$ as a $\mathbb{Q}$-vector space. Then $[\mathbb{R} : \mathbb{Q}]$ is not finite and $\mathbb{R}/\mathbb{Q}$ is not a finite field extension.

Our fields of interest are $\mathbb{Q}_p$, the *p-adic numbers*, and $\mathbb{F}_q((t))$, the *formal Laurent series*. We remind the reader that the latter field is given by

$$\mathbb{F}_q((t)) := \left\{ \sum_{i=N}^{\infty} a_i t^i \ \middle| \ a_i \in \mathbb{F}_q, \ N \in \mathbb{Z}, \ a_N \neq 0 \right\}.$$

To describe $\mathbb{Q}_p$, we require a definition that equips fields with a notion of norm.

A *norm* or an *absolute value* on a ring R is a function $|\cdot| \colon R \to [0, \infty)$ such that, for all $r, s \in R$, there holds $|r \cdot s| = |r| \cdot |s|$, $|r + s| \leq |r| + |s|$, and $|r| = 0$ if and only if $r = 0$. If the second condition is replaced with the *strong triangle inequality* $|r + s| \leq \max\{|x|, |y|\}$ then we say that $|\cdot|$ is *non-archimedian*. Otherwise, we say that $|\cdot|$ is *archimedian*.

All fields have a trivial absolute value, given by $|r|_{\text{triv}} = 1$ for $r \neq 0$ and $|0|_{\text{triv}} = 0$. An example of a non-trivial absolute value is the one defined on $\mathbb{F}_q((t))$. Consider an arbitrary element $\sum_{i=N}^{\infty} a_i t^i$ in $\mathbb{F}_q((t))$ written so that $a_N \neq 0$ if the chosen element of $\mathbb{F}_q((t))$ is non-zero. Then

$$\left| \sum_{i=N}^{\infty} a_i t^i \right| := \begin{cases} 0, & \text{if } a_i = 0 \text{ for all } i, \\ q^{-N}, & \text{else.} \end{cases}$$

Another example of an absolute value is found in the construction of $\mathbb{Q}_p$.

Fix a prime $p \geq 2$. Given any $\frac{a}{b} \in \mathbb{Q}^{\times}$, we can uniquely write $\frac{a}{b} = p^n \cdot \frac{x}{y}$ where $\gcd(x, y) = 1$ and p does not divide x any further. This is a simple consequence of the fundamental theorem of arithmetic. Then

the *p-adic absolute value* $|\cdot|_p \colon \mathbb{Q} \to [0, \infty)$ is defined by

$$\left| \frac{a}{b} \right|_p := \begin{cases} 0 & \text{if } \frac{a}{b} = 0, \\ p^{-n} & \text{if } \frac{a}{b} = p^n \cdot \frac{x}{y} \text{ as above.} \end{cases}$$

The *p-adic numbers*, denoted $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ with respect to the *p*-adic absolute value. This is analogous to the usual completion of a normed vector space. More precisely, we can explicitly write out the elements of $\mathbb{Q}_p$ as

$$\mathbb{Q}_p = \left\{ \sum_{i=N}^{\infty} a_i p^i \;\middle|\; a_i = 0, 1, 2, \ldots, p-1, \; N \in \mathbb{Z}, \; a_N \neq 0 \right\}.$$

Then the absolute value defined on $\mathbb{Q}_p$ is given by

$$\left| \sum_{i=N}^{\infty} a_i p^i \right| = p^{-N}.$$

We are almost ready to define local fields. We say that a ring R is a *topological ring* if it is equipped with a topology such that the addition and multiplication maps $+, \cdot \colon R \times R \to R$ are continuous. Here the product space $R \times R$ is equipped with the product topology. We say that a topological ring is (locally) compact if its associated topological space is (locally) compact. A locally compact topological field is a field equipped with a topological space whose underlying ring is a locally compact topological ring. Now we are ready to define local fields.

A *local field* is a locally compact topological field k with respect to a non-trivial absolute value. In fact, as remarked in [Mil20], all fields satisfying such a property are isomorphic to a small family of fields. We summarise the possibilities for k:

(*i*) If $|\cdot|$ is archimedian, then k is $\mathbb{R}$ or $\mathbb{C}$.

(*ii*) If $|\cdot|$ is non-archimedian and $\operatorname{char} k = 0$, then k is a finite extension of $\mathbb{Q}_p$, where p is prime.

(*iii*) If $|\cdot|$ is non-archimedian and $\operatorname{char} k = p$, then k is $\mathbb{F}_q((t))$, where $q = p^m$ and $m \geq 1$.

We present an example of a finite extension of $\mathbb{Q}_p$. Take $\mathbb{Q}_p((t^{1/m}))$ for some prime $p > 2$ and $m \in \mathbb{Z}$ with $p \nmid m$. This field has the elements

$$\mathbb{Q}_p((t^{1/m})) = \left\{ \sum_{i=N}^{\infty} a_i t^i \;\middle|\; a_i \in \mathbb{Q}_p, \; N \in \mathbb{Z}, \; a_N \neq 0 \right\}.$$

Inside $\mathbb{Q}_p((t^{1/m}))$ lies a subfield of constant functions, K. That is,

$$K = \{ f \in \mathbb{Q}_p((t^{1/m})) \mid f(t) = c, \text{ for some } c \in \mathbb{Q}_p \}.$$

Then K is isomorphic to $\mathbb{Q}_p$ and we can think of $\mathbb{Q}_p$ as a subfield of $\mathbb{Q}_p((t^{1/m}))$ via this subfield K. We see that $B = \{t^{1/m}, t^{2/m}, \ldots, t\}$ is a basis demonstrating $\mathbb{Q}_p((t^{1/m}))$ is a $\mathbb{Q}_p$-vector space of dimension m. Thus, $\mathbb{Q}_p((t^{1/m}))$ is a finite extension of $\mathbb{Q}_p$ with degree m.

5.2. **The structure of non-archimedian local fields.** Let k be a non-archimedian local field. We require some understanding of the structure of these fields. To this end, we define the following important objects:

(i) $\mathcal{O} := \{x \in k : |x| \leq 1\}$, the *ring of integers* of k.
(ii) $\mathcal{O}^\times := \{x \in k : |x| = 1\}$, the group of units in the ring of integers.
(iii) $\mathcal{P} := \mathcal{O} - \mathcal{O}^\times = \{x \in k : |x| < 1\}$, the unique maximal ideal of $\mathcal{O}$.
(iv) $\mathcal{K} := \mathcal{O}/\mathcal{P}$, the *residue field* of k.
(v) $\varpi :=$ a generator of $\mathcal{P}$ called a *uniformiser* of k. Then we may write $\mathcal{K} = \mathcal{O}/\varpi\mathcal{O}$.

We compute some of these objects in some cases.

Suppose that $k = \mathbb{F}_q((t))$. Then $\mathcal{O} = \{\sum_{i=N}^\infty a_i t^i \in k \mid q^{-N} \leq 1\}$. Note that $q^{-N} \leq 1$ if and only if $N \geq 0$. Then $\mathcal{O} = \mathbb{F}_q[\![t]\!]$, the ring of formal power series over $\mathbb{F}_q$. Furthermore, $\mathcal{O}^\times = \{\sum_{i=N}^\infty a_i t^i \in k \mid q^{-N} = 1\}$. Note that $q^{-N} = 1$ if and only if $N = 0$. Then $\mathcal{O}^\times = \{f \in k \mid f(0) \neq 0\}$. Next, $\mathcal{P} = \{x \in k \mid |x| < 1\}$. Note that $q^{-N} < 1$ if and only if $N \geq 1$. Then $\mathcal{P} = t\mathbb{F}_q[\![t]\!]$. Lastly, $\mathcal{K} = \mathbb{F}_q[\![t]\!]/t\mathbb{F}_q[\![t]\!] \cong \mathbb{F}_q$. This can be seen by the surjective ring homomorphism $\mathbb{F}_q[\![t]\!] \to \mathbb{F}_q$ given by $f \mapsto f(0)$. It is easily seen that this map has kernel $t\mathbb{F}_q[\![t]\!]$, so the first isomorphism theorem for rings yields the result.

Suppose that $k = \mathbb{Q}_p$. Then $\mathcal{O} = \{\sum_{i=N}^\infty a_i p^i \in k \mid p^{-N} \leq 1\}$. Note that $p^{-N} \leq 1$ if and only if $N \geq 0$. Then $\mathcal{O} = \mathbb{Z}_p$, the ring of p-adic integers. Furthermore, $\mathcal{O}^\times = \{\sum_{i=N}^\infty a_i p^i \in k \mid p^{-N} = 1\}$. Note that $p^{-N} = 1$ if and only if $N = 0$. Then $\mathcal{O}^\times = \{\sum_{i=N}^\infty a_i p^i \in k \mid a_0 \neq 0\}$. Next, $\mathcal{P} = \{x \in k \mid |x| < 1\}$. Note that $p^{-N} < 1$ if and only if $N \geq 1$. Then $\mathcal{P} = \{\sum_{i=N}^\infty a_i p^i \in k \mid N \geq 1\} = \{p\sum_{i=N}^\infty a_i p^i \in k \mid N \geq 0\} = p\mathbb{Z}_p$. Lastly, $\mathcal{K} = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. This can be seen by the surjective ring homomorphism $\mathbb{Z}_p \to \mathbb{F}_p$ given by $\sum_{i=N}^\infty a_i p^i \mapsto a_0$. It is easily seen that this map has kernel $p\mathbb{Z}_p$, so the first isomorphism theorem for rings yields the result.

We make the observation that $\mathcal{K} \cong \mathbb{F}_q$ for all non-archmedian local fields. We have not yet shown this for the case when k is a finite extension of $\mathbb{Q}_p$. In this case, $\mathcal{O}$ will be a finite extension of $\mathbb{Z}_p$ and the above procedure can be followed to see that $\mathcal{K}$ is a finite extension of $\mathcal{K}_{\mathbb{Q}_p} \cong \mathbb{F}_q$, so $\mathcal{K}$ is also a finite field.

5.3. **The spherical Hecke algebra** $C_c(K^\circ \backslash G / K^\circ)$**.** Choose a non-archimedian local field k. Then consider $G := \mathrm{GL}_n(k)$ and $K^\circ := \mathrm{GL}_n(\mathcal{O})$. To see that G is locally compact, we recall that it is a subspace of k^{n^2}, and every open subset of k^{n^2} is locally compact in the subspace topology. The ring of integers $\mathcal{O}$ is open and compact in k, so K° is open and compact in G. The *spherical Hecke algebra* is the Hecke algebra $C_c(K^\circ \backslash G / K^\circ)$, following the notation of Section 4.2.

We conclude this section with the result that the spherical Hecke algebra is commutative. To this end, we present a preparatory lemma of Bump which is stated and proved in [Bum10].

Lemma 23 (The p-adic Cartan Decomposition). *Every double coset in $K^\circ \backslash G / K^\circ$ has a unique representative of the form*

$$\begin{pmatrix} \varpi^{\lambda_1} & & & \\ & \varpi^{\lambda_2} & & \\ & & \ddots & \\ & & & \varpi^{\lambda_n} \end{pmatrix},$$

where ϖ is the uniformiser of $\mathcal{P}$ and $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ are integers.

Theorem 24. *The spherical Hecke algebra $C_c(K^\circ \backslash G / K^\circ)$ is commutative.*

The following proof follows the idea of Gelfand's Trick from Section 1.7. One can follow the proof of Gelfand's Trick in the finite case in order to produce a proof of the Trick in the locally compact case. This is because the requirement that functions are compactly supported reduces the convolution product of the Hecke algebra to a finite sum when performing the proof. Then the proof in the locally compact case will reduce to the computation we have already performed in the finite case.

Proof of Theorem 24. The anti-automorphism $\varphi \colon G \to G$ given by $\varphi(g) := g^t$ is an involution. It can be pulled back to the map $\varphi^* \colon \mathrm{Fun}(G) \to \mathrm{Fun}(G)$ given by $(\varphi^* f)(g) = f(\varphi(g)) = f(g^t)$. This map φ preserves K° (i.e. the image of K° lies in K°). The previous lemma tells us that each double coset contains a diagonal representative, on which φ is clearly the identity. Then φ^* is an involutive anti-automorphism acting as the identity on a basis of the Hecke algebra, so it is commutative. $\qquad\square$

We generalise the notion of a Geland pairs from Chapter 1. See [Bum10] and [AGS08]. A complex representation $G \to \mathrm{GL}(V)$ is said to be *smooth* if the stabiliser $\{k \in G \mid k \cdot v = v\}$ is open for every non-zero $v \in V$. Furthermore, a smooth representation is *admissible* if, given any open subgroup K, the vector subspace of K-fixed vectors V^K is finite-dimensional.

Then the pair (G, K) is said to be a Gelfand pair if, for every admissible irreducible representation V of G, the subspace of K-fixed vectors V^K is at most one-dimensional. This is equivalent to saying that $C_c(K \backslash G / K)$ is commutative. In the case that G is a finite group, this is equivalent to saying that $\mathrm{Ind}_K^G \mathbf{1}$ is multiplicity-free (c.f. Section 1.8). Theorem 24 tells us that (G, K°) is a Gelfand pair.

5.4. **The Iwahori subgroup I.** Fix a non-archimedian local field k. Recall its ring of integers $\mathcal{O}$ and its residue field $\mathcal{O}/\mathcal{P} \cong \mathbb{F}_q$. Now suppose that G is a "nice" reductive group. In particular, suppose that G is a connected, split reductive group over k. For example, $G(k) = \mathrm{SL}_n(k)$ for $n \geq 2$.

Consider the group homomorphism $\phi \colon G(\mathcal{O}) \to G(\mathcal{O}/\mathcal{P}) \cong G(\mathbb{F}_q)$ given by

$$\phi((g_{ij})_{i,j=1,\ldots,n}) \mapsto (n(g_{ij}))_{i,j=1,\ldots,n},$$

where $n \colon \mathcal{O} \to \mathcal{O}/\mathcal{P}$ is the natural map $x \mapsto x + \mathcal{P}$. The map ϕ amounts to applying the natural map to each entry of the matrix. Then the *Iwahori subgroup* of $G(\mathcal{O})$ is $I := \phi^{-1}(B(\mathbb{F}_q))$.

As an example, if $k = \mathbb{F}_q((t))$, the natural map n is the evaluation map $t \mapsto 0$, and the map ϕ will evaluate the entries at $t = 0$. For a matrix to lie in the preimage of $B(\mathbb{F}_q)$, its entries below the diagonal must have a constant term of 0, the entries on the diagonal must have a non-zero constant term, and the entries above the diagonal may be chosen freely. Then

$$I = \phi^{-1}(B(\mathbb{F}_q)) = \begin{pmatrix} \mathcal{O}^\times & \mathcal{O} & \cdots & \mathcal{O} \\ \mathcal{P} & \mathcal{O}^\times & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathcal{O} \\ \mathcal{P} & \cdots & \mathcal{P} & \mathcal{O}^\times \end{pmatrix}$$

In fact, this characterises the Iwahori subgroup for any non-archimedian local field. We require that the elements below the diagonal vanish under ϕ, so they must lie in $\mathcal{P}$. The diagonal elements must map to a non-zero element under ϕ, so they must lie in $\mathcal{O}^\times$. We have no restriction on the elements above the diagonal, so they lie in $\mathcal{O}$.

5.5. **The Iwahori–Hecke algebra** $C_c(I\backslash G/I)$. Take $G = G(k)$ and I as defined above. Then the *Iwahori–Hecke algebra* is given by $C_c(I\backslash G/I)$ in the notation of Section 4.2.

We will see that the Iwahori–Hecke algebra contains a subalgebra we are already familiar with. Namely, consider the Hecke algebra $C_c(I\backslash G(\mathcal{O})/I)$. This is clearly a subalgebra of the Iwahori–Hecke algebra; these are the functions in $C_c(I\backslash G/I)$ that are supported on $G(\mathcal{O})$.

Recall the Hecke algebra $\mathcal{H}(G, B)$ of Chapter 3. These are the complex-valued functions on $G(\mathbb{F}_q) = \mathrm{SL}_n(\mathbb{F}_q)$ that are constant on B-double cosets. In the notation of Chapter 4, this algebra may also be written as $C_c(B(\mathbb{F}_q)\backslash G(\mathbb{F}_q)/B(\mathbb{F}_q))$.

Recall the map $\phi\colon G(\mathcal{O}) \to G(\mathbb{F}_q)$ given in Section 5.4. Take f in $C_c(B(\mathbb{F}_q)\backslash G(\mathbb{F}_q)/B(\mathbb{F}_q))$ and consider the pullback of f by ϕ, given by $\phi^* f := f \circ \phi$. This is now a function $G(\mathcal{O}) \to \mathbb{C}$. Then we have the following proposition:

Proposition 25. *The map*

$$\phi^*\colon C_c(B(\mathbb{F}_q)\backslash G(\mathbb{F}_q)/B(\mathbb{F}_q)) \to C_c(I\backslash G(\mathcal{O})/I), \quad \phi^* f := f \circ \phi$$

is an algebra isomorphism.

Proof (*Sketch*). We must check that the image of ϕ^* lies in $C_c(I\backslash G(\mathcal{O})/I)$. To this end, let $i, i' \in I$ and $g \in G(\mathcal{O})$. Then

$$(\phi^* f)(igi') = f(\phi(igi')) = f(\phi(i)\phi(g)\phi(i')) = f(\phi(g)) = (\phi^* f)(g),$$

since $\phi(i) \in B(\mathbb{F}_q)$ by the definition of I, and f is invariant on $B(\mathbb{F}_q)$-double cosets. It is an exercise to show that $\phi^* f$ has compact support.

Next, the map ϕ^* is clearly linear. Furthermore, it is easy to see that $\ker \phi^*$ is trivial since $f \circ \phi = 0$ is only satisfied by the constant map $f \equiv 0$. The spaces $C_c(B(\mathbb{F}_q)\backslash G(\mathbb{F}_q)/B(\mathbb{F}_q))$ and $C_c(I\backslash G(\mathcal{O})/I)$ have the same dimension because they both have a basis parameterised by the Weyl group. Then ϕ^* is an isomorphism of vector spaces.

Lastly, we must check that ϕ^* preserves the algebra multiplication. To see this, take two maps $f, f' \in C_c(B(\mathbb{F}_q)\backslash G(\mathbb{F}_q)/B(\mathbb{F}_q))$ and an element $x \in G(\mathcal{O})$. Then

$$(\phi^* f \star \phi^* f')(x) = \int_G f(\phi(xg))f'(\phi(g^{-1})) \, d\mu(g) = \sum_{g \in G(\mathbb{F}_q)} f(\phi(xg))f'(\phi(g^{-1}))$$

$$= \sum_{yz=\phi(x)} f(y)f'(z) = (f \star f')(\phi(x)) = \phi^*(f \star f')(x). \quad \square$$

5.6. **The Iwahori–Matsumoto presentation.** We conclude this thesis with a presentation of the Iwahori–Hecke algebra called the *Iwahori–Matsumoto presentation* [HP02, MS21, Pra05, Bum10].

Recall that $G(k)$ is a "nice" reductive group, e.g. $G(k) = \mathrm{SL}_n(k)$ where $n \geq 2$. Fix a maximal split torus A in G. If $G(k) = \mathrm{SL}_n(k)$, then we may choose A to be the subgroup of diagonal matrices. Let $X^*(A) := \mathrm{Hom}_{\mathrm{alg}}(A, \mathbb{G}_m)$ denote the *rational characters* of A, and let $X_*(A) := \mathrm{Hom}_{\mathrm{alg}}(\mathbb{G}_m, A)$ denote the *rational cocharacters* of A, where $\mathrm{Hom}_{\mathrm{alg}}$ denotes the space of *algebraic homomorphisms*. Here $\mathbb{G}_m$ is the *one-dimensional torus* over k. Specifically, $\mathbb{G}_m$ is isomorphic to the group scheme $\mathrm{Spec}(k[t, t^{-1}])$. If one is not familiar with these notions, one can think of $\mathbb{G}_m$ as the multiplicative group $k^\times$.

Given a rational character $\lambda \in X^*(A)$ and a rational cocharacter $\mu \in X_*(A)$, their composition is an endomorphism of $\mathbb{G}_m$ of the form $x \mapsto x^k$. This yields a bilinear map

$$\langle \cdot, \cdot \rangle \colon X^*(A) \times X_*(A) \to \mathbb{Z}$$

defined by $\langle \lambda, \mu \rangle := k$, where k is given above.

The *affine Weyl group* of G is the quotient group $\widetilde{W} = N_{G(k)}(A)/A(\mathcal{O})$. One may show that $\widetilde{W}$ may be written as $\widetilde{W} = \frac{A}{A(\mathcal{O})} \rtimes W$, where W is the Weyl group of G [Hum90]. Recall from Section 3.1 that if $G = \mathrm{SL}_{r+1}$ then $W \cong S_{r+1}$. The Weyl group is a Coxeter group with simple reflections $S = \{s_i = (i\ i+1) \mid i = 1, \ldots, r\}$. We can consider these simple reflections as elements of SL_{r+1} by writing

$$s_i = \begin{pmatrix} I_{i-1} & & & \\ & 0 & 1 & \\ & -1 & 0 & \\ & & & I_{r-i} \end{pmatrix}.$$

Similarly, the affine Weyl group has the generators $\widetilde{S} := \{s_0, s_1, \ldots, s_r\}$, where $s_1, \ldots, s_r$ are as before, and s_0 is given by

$$s_0 = \begin{pmatrix} & & \varpi^{-1} \\ & I_{r-1} & \\ (-1)^{r+1}\varpi & & \end{pmatrix}.$$

This generator is understood as an element of $N_{G(k)}(A)/A(\mathcal{O})$. Then we have

$$\widetilde{W} = \left\langle s_0, \ldots, s_r \;\middle|\; \begin{array}{c} s_i^2 = 1, \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, \\ s_i s_j = s_j s_i \end{array} \right\rangle.$$

We can define the *length function* on the Weyl group W with associated generators S. This is the map $l \colon W \to \mathbb{Z}_{\geq 0}$ given by $l(w) = k$, where k is the smallest integer such that $w = s_1 s_2 \cdots s_k$, where $s_i \in S$. It is seen in [Bum10] that this map is well-defined and unique. The definition of l clearly extends to the affine Weyl group $\widetilde{W}$ and its generators $\widetilde{S}$.

Now we may present the Iwahori–Matsumoto presentation of the Iwahori–Hecke algebra. The Iwahori–Hecke algebra has the basis $\{T_w \mid w \in \widetilde{W}\}$ subject to the multiplication relations

$$T_s^2 = (q-1)T_s + q, \quad \text{if } s \in \widetilde{S},$$
$$T_w T_{w'} = T_{ww'}, \quad \text{if } l(ww') = l(w) + l(w').$$

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* $R_i^2 = (R_i R_j)^{k_{ij}} = 1$ **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.