Character Rings and Hecke Algebras

Yichao Zhang 993894461

December 8, 2005

1 Introduction

In this project, we are going to study some results concerning the character rings and Heche Algebras in S_k and $GL(k, F)$.

In next section, we will introduce some notation system in S_k and $GL(k, F)$ first, and with that, we will deduce some interesting and important results in this field, such as the results about the length function on W and the double $B - B$ cosets, where W is the Weyl group of $GL(k, F)$.

In Section 3, we will show a basic result concerning the W_I-W_J double cosets in W and the P_I-P_J double cosets in $GL(k, F)$. After this a beautiful connection between $\mathcal{R}_k$ and $\mathcal{R}_k(q)$ follows, where $\mathcal{R}_k$ is the character ring of S_k and $\mathcal{R}_k(q)$ is the character ring of $GL(k, \mathbb{F}_q)$.

In Section 4, we move to the Hecke algebras $\mathcal{H}$ and $\mathcal{H}_k(q)$, where $\mathcal{H}$ is the convolution ring of B-bi-invariant functions on $GL(k, \mathbb{F}_q)$. Based on the properties of $\mathcal{H}$, we will present the more general definition of $\mathcal{H}_k(q)$, with q any complex number and as we will see, if q is prime power, then $\mathcal{H}$ and $\mathcal{H}_k(q)$ coincide, which reaches the end of this project.

Statement: All of the materials in this project come from Bump's book, [1]; concretely, it occupies the whole Chapter 48, main part of Chapter 30, half of Chapter 28 and 21, and the main theorem in Chapter 37. Except the *Jacobi-Trudi Identity*, we deduce all of the results from the beginning to the end. Besides, all of these chapters in Bump's are based on the concept *root system*, however, in this specific case, we do not need its general definition and I successfully avoid the discussion about it throughout this project.

2 Some results in S_k and $GL(k, F)$

Let F be a field. Let G=GL(k,F), B be the Borel subgroup of upper triangular matrices in G, T the maximal torus of diagonal elements in G, N the normalizer of T, and W=N/T the Weyl group. As we know, N consists of the monomial matrices, that is, matrices having exactly one nonzero entry in each row and column.

Identifying W with S_k. Let $\Phi = \{(i, j) : i \neq j\}$,$\Phi^+ = \{(i, j) : i < j\}$, $\Phi^- = \{(i, j) : i > j\}$ and $\Sigma = \{(1, 2), (2, 3), \cdots, (k-1, k)\}$. Hence $\Sigma \subset \Phi^+ \subset \Phi$. We will say $(i, j) = -(j, i)$ for convenience. For any $w \in W$, we consider it as a map: $\Phi \to \Phi$ by $w(i, j) = (w(i), w(j))$(here $w(i), w(j)$ make sense since $W = S_k$ has a natural action on $\{1, 2, \cdots, k\}$). Hence the map w is a bijection. And it is trivial that $w(-\alpha) = -w(\alpha)$ for all $\alpha \in \Phi$. For each $\alpha = (i, j) \in \Phi$, we can associate it with a matrix $s_\alpha \in W$, which is the transposition matrix corresponding to the transposition (i, j). It is easy to see that $s_\alpha = s_{-\alpha}$ and we will call s_α a *simple reflection* if $\alpha \in \Sigma$. As a nearly trivial result, we have

$$w s_\alpha w^{-1} = s_{w(\alpha)} \tag{1}$$

It is trivial that the set of simple reflections can generate S_k, so it makes sense when we define

$$l(w) = \begin{cases} min\{r \in \mathbb{N} : w = s_{\alpha_1} \cdots s_{\alpha_r} \text{ for } \alpha_i \in \Sigma, 1 \le i \le r\} & \text{if } \ w \neq 1, \\ 1 & \text{if } \ w = 1. \end{cases}$$

Also, we define another function $l^{'}(w) = |\Phi^+ \cap w^{-1}\Phi^-|$, i.e., the number of $\alpha \in \Phi^+$ such that $w(\alpha) \in \Phi^-$.

We should add a word here that Φ above is essentially a root system associated to G; but actually, we do not need this concept here, and we can successfully avoid the discussion of root systems here.

Let us see a proposition, which will play a basic role in this project, since it reveals some essential properties of the length function l on W.

Proposition 1. *(i) If $\alpha \in \Sigma$ and $\beta \in \Phi^+$, then either $\beta = \alpha$ or $s_\alpha(\beta) \in \Phi^+$.*

(ii) Let $s = s_\alpha (\alpha \in \Sigma)$ be a simple reflection, and let $w \in W$. We have

$$l^{'}(sw) = \begin{cases} l^{'}(w) + 1 & \textit{if} \ \ w^{-1}(\alpha) \in \Phi^+, \\ l^{'}(w) - 1 & \textit{if} \ \ w^{-1}(\alpha) \in \Phi^-, \end{cases} \tag{2}$$

and

$$l^{'}(ws) = \begin{cases} l^{'}(w) + 1 & \textit{if} \ \ w(\alpha) \in \Phi^+, \\ l^{'}(w) - 1 & \textit{if} \ \ w(\alpha) \in \Phi^-. \end{cases} \tag{3}$$

(iii) Suppose that $\alpha_1, \cdots, \alpha_r$ and α are elements of Σ, and let $s_i = s_{\alpha_i}$. Suppose that $s_1 \cdots s_r(\alpha) \in \Phi^-$. Then

$$s_1 \cdots s_r = s_1 \cdots \hat{s_j} \cdots s_r s_\alpha, \tag{4}$$

where $\hat{s_j}$ means the omission of the single element s_j.

(iv) Suppose that $\alpha_1, \cdots, \alpha_r$ are elements of Σ, and let $s_i = s_{\alpha_i}$. Suppose that $l^{'}(s_1 \cdots s_r) < r$. Then there exist $1 \le i < j \le r$ such that

$$s_1 \cdots s_r = s_1 \cdots \hat{s_i} \cdots \hat{s_j} \cdots s_r. \tag{5}$$

(v) If $w \in W$, then $l(w) = l^{'}(w)$.

Proof. For (i), assume $\beta = (i, j)$ with $i < j$. Hence $s_\alpha(\beta) = (s_\alpha(i), s_\alpha(j))$. Since

$$s_\alpha(i) \le i + 1 \le j \le s_\alpha(j) + 1,$$

either $s_\alpha(i) = s_\alpha(j) + 1$ or $s_\alpha(i) < s_\alpha(j)$. But

$$s_\alpha(i) = s_\alpha(j) + 1 \Longleftrightarrow s_\alpha(i) = i + 1 \ , \ s_\alpha(j) = j - 1 \ \text{ and } \ j = i + 1,$$

so either $\beta = \alpha$ or $s_\alpha(\beta) \in \Phi^+$.

For (ii), since $s(\Phi^-)$ is obtained from Φ^- by deleting $-\alpha$ and adding α, we see that $(sw)^{-1}(\Phi^-) = w^{-1}(s\Phi^-)$ is obtained from $w^{-1}\Phi^-$ by deleting $-w^{-1}(\alpha)$ and adding $w^{-1}(\alpha)$. Since $l^{'}(w) = |\Phi^+ \cap w^{-1}\Phi^-|$, we have identity (2). To prove (3), we note that

$$l^{'}(ws) = |\Phi^+ \cap (ws)^{-1}\Phi^-| = |s(\Phi^+ \cap (ws)^{-1}\Phi^-)| = |s\Phi^+ \cap (w)^{-1}\Phi^-|,$$

and since $s\Phi^+$ is obtained from Φ^+ by deleting α and adding $-\alpha$, (3) follows.

For (iii), Let $1 \leq j \leq r$ be minimal such that $s_{j+1} \cdots s_r(\alpha) \in \Phi^+$. j exists since $\alpha \in \Phi^+$. Then $s_j \cdots s_r(\alpha) \in \Phi^-$. Since α_j is the unique element of Φ^+ mapped into Φ^- by $s_j = s_{\alpha_j}$ by part (i), we have

$$s_{j+1} \cdots s_r(\alpha) = \alpha_j,$$

and by (1) we have

$$(s_{j+1} \cdots s_r)s_\alpha(s_{j+1} \cdots s_r)^{-1} = s_j$$

or

$$s_{j+1} \cdots s_r s_\alpha = s_j s_{j+1} \cdots s_r,$$

which implies (4).

For (iv), evidently there is a first j such that $l^{'}(s_1 \cdots s_j) < j$, and we have $j > 1$ since $l^{'}(s_1) = 1$. Then $l^{'}(s_1 \cdots s_{j-1}) = j-1$, and by (ii), we have $s_1 \cdots s_{j-1}(\alpha_j) \in \Phi^-$. The existence of i satisfying $s_1 \cdots s_{j-1} = s_1 \cdots \hat{s}_i \cdots s_{j-1}s_j$ now follows from (iii), which implies (5).

For (v), first we are to show $l^{'}(w) \leq l(w)$ by induction on $l(w)$. Choose a simple reflection s such that $l^{'}(sw) = l^{'}(w) - 1$. So

$$l^{'}(w) \leq l^{'}(sw) + 1 \leq l(w) + 1 = l(w).$$

For the opposite inequality, let $w = s_1 \cdots s_r$ be a counterexample with $l(w) = k$, where each $s_i = s_{\alpha_i}$ with $\alpha_i \in \Sigma$. Thus $l^{'}(s_1 \cdots s_r) < r$. Then by (iv), there exist i and j such that

$$w = s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_r,$$

which contradicts our assumption that $l(w) = k$. QED

Let us introduce a notation system as follows.

Let $\lambda = (k_1, \cdots, k_r)$ be a partition of k, i.e. k_i's are positive integers and $\sum_i k_i = k$. A *Ferrers diagram* represents a partition as patterns of dots, with the i-th row having the same number of dots as the i-th term in the partition. Two partitions are called *conjugate* if their Ferrers diagrams transform into each other when reflected about the line $y = -x$. S_k has a subgroup isomorphic to $S_{k_1} \times \cdots \times S_{k_r}$ in which S_{k_1} acts on $\{1, \cdots, k_1\}$, S_{k_2} acts on $\{k_1 + 1, \cdots, k_2\}$, and so forth. In this project, we let I or J denote subsets of Σ. we have the following lemma:

Lemma 1. *For any subset J of Σ, there exist integers $k_1, \cdots, k_r$ such that the subgroup of S_k generated by J is $S_{k_1} \times \cdots \times S_{k_r}$.*

Proof. If J contains $(1,2),(2,3),\cdots,(k_1-1,k_1)$, then the subgroup they generate is the symmetric group S_{k_1} acting on $\{1,\cdots,k_1\}$. Taking k_1 as large as possible, assume J omits (k_1,k_1+1). Taking k_2 as large as possible such that J contains $(k_1+1,k_1+2),\cdots,(k_1+k_2-1,k_1+k_2)$, the subgroup they generate is the symmetric group S_{k_2} acting on $\{k_1+1,\cdots,k_1+k_2\}$, and so forth. Thus J contains generators of each factor in $S_{k_1}\times\cdots\times S_{k_r}$ and does not contain any element that is not in this product, so this is the group it generates. QED.

Let W_J be the subgroup of W generated by $\{s_\alpha : \alpha\in J\}$. Hence, by the lemma above, we have (for suitable k_i)

$$W_J \cong S_{k_1}\times\cdots\times S_{k_r}. \tag{6}$$

Let N_J be the preimage of W_J in N under the canonical projection to W. Let P_J be the group generated by B and N_J. Then

$$P_J = \left\{ \begin{pmatrix} G_{11} & G_{12} & \cdots & G_{1r} \\ 0 & G_{22} & \cdots & G_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & G_{rr} \end{pmatrix} \right\},$$

where each G_{ij} is a $k_i\times k_j$ block. The group P_J is a semidirect product $P_J = M_JU_J = U_JM_J$, where M_J is characterized by the condition that $G_{ij}=0$ unless $i=j$, and the normal subgroup U_J is characterized by the condition that each G_{ii} is the identity matrix in $GL(k_i)$. Evidently,

$$M_J \cong GL(k_1,F)\times\cdots\times GL(k_r,F). \tag{7}$$

Let $B_J = M_J\cap B$.

As we know, a double coset $B\omega B$, or more generally $P_I\omega P_J$, does not depend on the choice $\omega\in N$ of representative for an element $w\in W$ and we usually use the notation $BwB=\mathcal{C}(w)$ or P_IwP_J for this double coset, respectively.

For $\alpha=(i,j)\in\Phi$ and $a\in F$, let $x_\alpha(a)=I+aE_{ij}$, where E_{ij} is the matrix with $(i,j)-$entry 1 and 0 else.

The following proposition investigates some properties of B-double cosets.

Proposition 2. *(i) If $\omega\in N$ represents the Weyl group element $w\in W$ and $\alpha\in\Phi$, then*

$$\omega x_\alpha(a)\omega^{-1}\in x_{w(\alpha)}(F). \tag{8}$$

(ii) Assume $\alpha\in\Sigma$ and $J=\{\alpha\}$. Then $B=Tx_\alpha(F)U_J$ and $\mathcal{C}(s_\alpha)\cup B$ is a subgroup of G.

(iii) Assume $\alpha\in\Sigma$ and $w\in W$ such that $w(\alpha)\in\Phi^+$. Let $s=s_\alpha$. Then $wBs\subset BwsB$ and equivalently, $\mathcal{C}(w)\mathcal{C}(s)=\mathcal{C}(ws)$.

(iv) If $w,w^{'}\in W$ are such that $l(ww^{'})=l(w)+l(w^{'})$, then

$$\mathcal{C}(ww^{'})=\mathcal{C}(w)\mathcal{C}(w^{'}). \tag{9}$$

(v) Let $w\in W$ and $\alpha\in\Sigma$. Then

$$wBs_\alpha\subset Bws_\alpha B\cup BwB. \tag{10}$$

Proof. For (i), we know for some $\{a_l\} \subset F^\times$,

$$\omega = \sum_{l=1}^{n} a_l E_{l,w^{-1}(l)} \text{ and } \omega^{-1} = \sum_{r=1}^{n} a_r^{-1} E_{w^{-1}(r),r}.$$

So

$$\omega x_\alpha(a)\omega^{-1} = I + \sum_{l,r} a_l a_r^{-1} E_{l,w^{-1}(l)} E_{ij} E_{w^{-1}(r),r} = I + a_{w(i)} a_{w(j)}^{-1} E_{w(i),w(j)} \in x_{w(\alpha)}(F).$$

For (ii), the partition corresponding to J is $\lambda = (1, \cdots, 1, 2, 1, \cdots 1)$ where there are $(i-1)$ 1's before 2 and $(k-i-1)$ 1's after 2 in λ. it is trivial that $B \supset Tx_\alpha(F)U_J$ since each component of the right-hand side is contained in B. For the opposite inclusion, $\forall b \in B$, of course we can choose $t \in T$ such that $tb \in B$ with its diagonal entries all 1's. Hence we pick out its diagonal block matrices, say, $diag\{1, \cdots, 1, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, 1, \cdots, 1\}$ for some $a \in F$. Then we choose $x_\alpha(-a)$ and we have the diagonal block matrices of $x_\alpha(-a)tb$ is $diag\{1, \cdots, 1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1, \cdots, 1\}$, which implies $x_\alpha(-a)tb \in U_J$. Hence $b \in t^{-1}x_\alpha(a)U_J$.

Since $s_\alpha \in N_J$, we have both $\mathcal{C}(s_\alpha)$ and B are subsets of P_J and it suffices to show their union is P_J. Let us first see the case $k = 2$ and α has to be $(1, 2)$. Then the conclusion follows from the Bruhat decomposition. For general k, we have $M_J \cong P_J/U_J \cong GL(2, F) \times (F^\times)^{k-2}$. So by the results of the case $k = 2$, we have $M_J \subset \mathcal{C}(s_\alpha) \cup B$. Since $U_J \subset B$, we have $P_J = M_J U_J \subset \mathcal{C}(s_\alpha) \cup B$. We are done.

For (iii), we will show

$$wBs \subset BwsB. \tag{11}$$

For any $b \in B$ and any representatives ω and σ of w and s, respectively, where w and s are considered as cosets in $N/T = W$, we may write $b = tx_\alpha(a)u$ by (ii), where $t \in T$, $a \in F$ and $u \in U_J$. Then

$$\omega b\sigma = \omega t\omega^{-1} \cdot \omega x_\alpha(a)\omega^{-1} \cdot \omega\sigma \cdot \sigma^{-1}u\sigma.$$

We have $\omega t\omega^{-1} \in\subset B$ since $\omega \in N = N(T)$, and $\omega x_\alpha(a)\omega^{-1} \in x_{w(\alpha)}(F) \subset B$ by (i) since $w(\alpha) \in \Phi^+$. Also, we have $\sigma^{-1}u\sigma \in U_J \subset B$ since M_J normalizes U_J and $\sigma \in M_J$. Hence $\omega B\sigma \in BwsB$ and $wBs \subset BwsB$. It follows that $\mathcal{C}(w)\mathcal{C}(s) \subset \mathcal{C}(ws)$ by multiplying both left and right of both RHS and LHS of (11). The opposite inclusion is obvious. Done.

For (iv), first we show that if $l(w) = r$ and $w = s_1 \cdots s_r$ with s_i's simple reflections, then

$$\mathcal{C}(w) = \mathcal{C}(s_1) \cdots \mathcal{C}(s_r).$$

Indeed, let $w_1 = s_1 \cdots s_{r-1}$, hence $l(w_1 s_r) = l(w_1) + 1$, by Proposition 1(ii)and(v), which means $w_1(\alpha) \in \Phi^+$ where $\alpha \in \Sigma$ is such that $s_r = s_\alpha$. By (iii) and induction on r, we know

$$\mathcal{C}(w) = \mathcal{C}(w_1)\mathcal{C}(s_r) = \mathcal{C}(s_1) \cdots \mathcal{C}(s_r).$$

Let $w' = s_1' \cdots s_{r'}'$ and $l(w') = r'$. Then $s_1 \cdots s_r s_1' \cdots s_{r'}'$ is a decomposition of ww' into simple reflections with $l(ww') = r + r'$. And

$$\mathcal{C}(ww') = \mathcal{C}(s_1) \cdots \mathcal{C}(s_r)\mathcal{C}(s_1') \cdots \mathcal{C}(s_{r'}') = \mathcal{C}(w)\mathcal{C}(w'),$$

so we are done.

For (v), if $w(\alpha) \in \Phi^+$, then by (iii), $wBs_\alpha \subset Bws_\alpha B$. If $w(\alpha) \notin \Phi^+$, then $ws_\alpha(\alpha) = w(-\alpha) = -w(\alpha) \in \Phi^+$. So by (iii), we have

$$ws_\alpha Bs_\alpha \subset Bws_\alpha^2 B = BwB.$$

By (ii), $B \cup \mathcal{C}(s_\alpha)$ is a subgroup, hence $B \cup \mathcal{C}(s_\alpha) = s_\alpha B \cup s_\alpha \mathcal{C}(s_\alpha)$, and thus

$$Bs_\alpha \subset s_\alpha B \cup s_\alpha \mathcal{C}(s_\alpha).$$

So

$$wBs_\alpha \subset w(s_\alpha B \cup s_\alpha \mathcal{C}(s_\alpha)) = ws_\alpha B \cup ws_\alpha Bs_\alpha B \subset Bws_\alpha B \cup BwB.$$

Done. QED

Also, we are interested in the size of the double coset $\mathcal{C}(w)$ with $w \in W$. Before we study this, let us present a notation: for any subset $S \subset \Phi$, let U_S be the subset of G which consists of $g = (g_{ij})$ such that $g_{ii} = 1$, and if $i \neq j$, then $g_{ij} = 0$ unless $(i, j) \in S$.

Proposition 3. *(i) Assume $S \subset \Phi^+$ is such that if $(i, j), (j, k) \in S$, then $i \neq k$ and $(i, k) \in S$. Then U_S is subgroup. Consequently, $U_w^- = U_{\Phi^+ \cap w\Phi^-}$ and $U_w^+ = U_{\Phi^+ \cap w\Phi^+}$ are both subgroups, for any $w \in W$.*

(ii) Let $F = \mathbb{F}_q$ and $w \in W$. Then the multiplication map $U_w^- \times U_w^+ \to U$ is bijective, where U is the group of all upper triangular unipotent matrices in G. Consequently, any $b \in B$ has a unique representation of the form $u^- u^+ t$, with $u^\pm \in U_w^\pm$ and $t \in T$.

(iii) Let $F = \mathbb{F}_q$ is finite and $w \in W$, then

$$|BwB| = q^{l(w)}|B|, \quad i.e., \quad |BwB/B| = q^{l(w)}.$$

Proof. For (i), let $g = (a_{ij}), g^{-1} = (b_{ij})$. Of course g^{-1} is upper triangular and has all diagonal entries 1. Assume $g^{-1} \notin U_S$, and we have the set $\{(i, j) \in \Phi^+ - S : b_{ij} \neq 0\}$ is nonempty. Choose one of its elements (i, j) with i maximal. And we have

$$0 = (gg^{-1})(i, j) = \sum_{l=i}^{k} a_{il} b_{lj} = b_{ij} + \sum_{l=i+1}^{j} a_{il} b_{lj}.$$

If $(i, l) \notin S$, then $a_{il} = 0$ and if $(i, l) \in S$, then $(l, j) \notin S$(otherwise, $(i, j) \in S$ by assumption on S), hence $b_{lj} = 0$ since i is the maximal one. In any case, $b_{lj} = 0$, so we have $\sum_{l=i+1}^{j} a_{il} b_{lj} = 0$ and $0 = b_{ij}$. A contradiction. So $g^{-1} \in U_S$. For $g = I + \sum_{(i,j) \in S} a_{ij} E_{ij}$ and $h = I + \sum_{(i,j) \in S} b_{ij} E_{ij}$ in U_S, it is easy to see that gh has the same form, by the assumption on S and $E_{ij} E_{kl} = \delta_{jk} E_{il}$ where $\delta_{jk} = 1$ if $j = k$ and 0 if $j \neq k$. So U_S is a subgroup.

Let $S = \Phi^+ \cap w\Phi^+$. If $(i, j), (j, k) \in S$, that is, $i < j < k$ and $w^{-1}(i) < w^{-1}(j) < w^{-1}(k)$, then $(i, k) \in S$. So U_w^+ is a subgroup. Similarly, we can show U_w^- is also a subgroup. Done.

For (ii), the map is well-defined, since both the two components are in U and U is a group. First we note that $U_w^+ \cap U_w^- = \{1\}$ by definition since the sets $\Phi^+ \cap w\Phi^-$ and $\Phi^+ \cap w\Phi^+$ are disjoint. Thus, if $u_1^- u_1^+ = u_2^- u_2^+$ with $u_i^\pm \in U_w^\pm$, then

$(u_2^-)^{-1}u_1^- = u_2^+(u_1^+)^{-1} \in U_w^+ \cap U_w^- = \{1\}$ by (i), which implies $u_1^\pm = u_2^\pm$, i.e., the map is injective. To see that it is also surjective, note that

$$|U_w^-| = q^{|\Phi^+ \cap w\Phi^-|}, \qquad |U_w^+| = q^{|\Phi^+ \cap w\Phi^+|},$$

so the order of $U_w^- \times U_w^+$ is $q^{\Phi^+} = |U|$ and the surjectivity is now clear.

Of course we can choose suitable $t \in T$ such that $bt \in U$. Since the above map is bijective, we have there exist $u^\pm \in U_w^\pm$ such that $bt = u^-u^+$. So $b = u^-u^+t^{-1}$ and b has a such representation. If $b = u_1^-u_1^+t_1 = u_2^-u_2^+t_2$ with $u_i^\pm \in U_w^\pm$ and $t_i \in T$, then by comparing the diagonal entries of these two representation, we have $t_1 = t_2$. Hence $u_1^-u_1^+ = u_2^-u_2^+$ and we have $u_1^\pm = u_2^\pm$ since again the above map is bijective. Done.

For (iii), we are going to show the map $u^- \mapsto u^-wB$ is a bijection $U_w^- \to BwB/B$. Hence the result follows since we know $|U_w^-| = q^{|\Phi^+ \cap w\Phi^-|} = q^{l'(w)} = q^{l(w)}$ by the definition of $l'(w)$ and Proposition 1.

First, the map is surjective. Indeed, every right coset in BwB/B is of the form bwB for some $b \in B$. Then by (ii), we may write $b = u^-u^+t$ uniquely with $u^\pm \in U_w^\pm$ and $t \in T$. In the proof of Proposition 2(i), we have already shown that $w^{-1}E_{ij}w \in E_{w^{-1}(i),w^{-1}(j)}(F)$. For any $(i,j) \in \Phi^+ \cap w\Phi^+$, we have $(i,j) \in w\Phi^+$ which means $(w^{-1}(i), w^{-1}(j)) \in \Phi^+$, i.e., $w^{-1}E_{ij}w \in U$, hence $w^{-1}u^+w \in U$. Now $w^{-1}u^+tw = w^{-1}u^+w \cdot w^{-1}tw \in B$, because $w^{-1}u^+w \in U$ and $w^{-1}tw \in T$. Therefore $bwB = u^-wB$.

Next, if $u_1^-wB = u_2^-wB$ for $u_i^- \in U_w^-$, then let $u^- = (u_1^-)^{-1}u_2^-$ and we have $w^{-1}u^-w \in B$, hence upper triangular. But using the same way above, we can show that $w^{-1}u^-w$ is lower triangular. As a result $w^{-1}u^-w = 1$, i.e. $u^- = 1$. QED

3 $\mathcal{R}_k$ and $\mathcal{R}_k(q)$

We denote $\mathcal{R}_k$ the free Abelian group generated by the isomorphism classes of irreducible representations of symmetric group S_k or equivalently the additive group of generalized characters. Similarly, let $\mathcal{R}_k(q)$ be the free Abelian group generated by the isomorphism classes of irreducible representations of $GL(k, \mathbb{F}_q)$ or equivalently the additive group of generalized characters.

Before we begin to give the theorem concerning the connection between $\mathcal{R}_k$ and $\mathcal{R}_k(q)$, first let us see one more proposition in $GL(k, F)$ and S_k for general F.

Proposition 4. *(i)*

$$M_J = \coprod_{w \in W_J} B_J w B_J.$$

(ii) If $w \in W$, we have

$$BW_I w W_J B = P_I w P_J.$$

(iii) The canonical map $w \mapsto P_I w P_J$ from $W \to P_I \backslash G / P_J$ induces a bijection

$$W_I \backslash W / W_J \cong P_I \backslash G / P_J.$$

Proof. For (i), we have identity (7) for suitable k_i. Now B_J is the direct product of the Borel subgroup of these $GL(k_i, F)$, and W_J is the direct product(6). Part(i) follows directly from the Bruhat decomposition for $GL(k, F)$.

As for (ii), since $BW_I \subset P_I$ and $W_J B \subset P_I$, we have $BW_I w W_J B \subset P_I w P_J$.

To prove the opposite inclusion, we first note that

$$wBW_J \subset BwW_J B. \tag{12}$$

Indeed, any element of W_J can be written as $s_1 s_2 \cdots s_l$, where $s_i = s_{\alpha_i}$ with $\alpha_i \in J$. Using Proposition 2(v), we have

$$wBs_1 \cdots s_l \subset Bws_1 Bs_2 \cdots s_l \cup BwBs_2 \cdots s_l.$$

By induction on l, we have $ws_1 Bs_2 \cdots s_l \subset Bws_1 W_J B$ (since here $ws_1 \in W$), hence $Bws_1 Bs_2 \cdots s_l \subset Bws_1 W_J B = BwW_J B$. Similarly, $BwBs_2 \cdots s_l \subset BwW_J B$ and we've proved (12).

Next we are going to show that

$$W_I BwW_J \subset BW_I wW_J B, \tag{13}$$

and it suffices to show

$$W_I Bw \subset BW_I wB. \tag{14}$$

For any $w \in W$ and $s = s_\alpha \in W_I$, we have two possibilities: if $l(sw) = l(w) + 1$, by Proposition 1(ii), $\mathcal{C}(sw) = \mathcal{C}(s)\mathcal{C}(w)$, whence $sBw \subset BswB \subset BW_I wB$; if $l(sw) = l(w) - 1$, let $w' = sw$ and we have

$$sBw = sBsw' \subset (BsB \cup B)w' = BsBw' \cup Bw' \subset BW_I w' B \cup Bw' B \subset BW_I wB,$$

where in the first inclusion we use Proposition 1(i) and the second inclusion is due to the induction on $l(w)$ and $l(w') < l(w)$. Here we finish the proof of (13).

Now using (i),

$$P_I w P_J = U_I M_I w M_J U_J = U_I B_I W_I B_I w B_J W_J B_J U_J \subset BW_I BwBW_J B.$$

Applying (12) and (13), we have $BW_I wW_J B \supset P_I w P_J$, whence the part (ii) ends.

As for (iii), the map $W_I w W_J \mapsto P_I w P_J$ is well-defined, since if $W_I w W_J = W_I w' W_J$, then $BW_I wW_J B = BW_I w' W_J B$, by part (ii), which is exactly $P_I w P_J = P_I w' P_J$. Of course it is onto. Indeed, for any $P_I \omega P_J$ with $\omega \in G$, there exists $w \in W$ s.t. $BwB = B\omega B$, because of the Bruhat decomposition. So $BwB \subset P_I w P_J \cap P_I \omega P_J$, whence $P_I w P_J = P_I \omega P_J$. It suffices to show this map is also 1-1. Actually, if $P_I w P_J \cap P_I w' P_J$, we must have $W_I w W_J = W_I w' W_J$ by part (ii) and the Bruhat decomposition. QED

Next, we will assume that $F = \mathbb{F}_q$ is a finite field.

Proposition 5. *Let H be a group, and let M_1 and M_2 be subgroups of H. Then in the character ring of H, the inner product of the characters induced from the trivial characters of M_1 and M_2, respectively, is equal to the number of double cosets in $M_1 \backslash H / M_2$.*

Proof. By Mackey' Theorem, the space of intertwining maps from $Ind_{M_1}^{H}(1)$ to $Ind_{M_2}^{H}(1)$ is isomorphic to the space of functions $\Delta : H \to Hom(\mathbb{C}, \mathbb{C}) \cong \mathbb{C}$ that satisfy $\Delta(m_1 h m_2) = \Delta(h)$ for $m_i \in M_i$ and $h \in H$. Of course, a function has this property if and only if it is constant on double cosets, so the dimension of this function space is just the number of different double cosets. On the other hand, as a well known result in representation theory, the dimension of the space of intertwining operators equals the inner product in the character ring. QED.

Let $\mathbf{h}_k$ and $\mathbf{e}_k \in \mathcal{R}_k$ be the trivial representation and the alternating representation of S_k, respectively. With the convention that $\mathbf{h}_r = \mathbf{e}_r = 0$ for $r < 0$ and $\mathbf{h}_0 = \mathbf{e}_0 = 1$, we have the following theorem(for the proof, see Bump's book, Theorem 37.1):

Theorem 1. ($\mathbf{Jacobi-Trudi\ \ Identity}$)*Let $\lambda = (\lambda_1, \cdots, \lambda_r)$ and $\mu = (\mu_1, \cdots, \mu_s)$ be conjugate partitions of k. We have the identity*

$$det(\mathbf{h}_{\lambda_i - i + j})_{1 \le i,j \le r} = det(\mathbf{e}_{\mu_i - i + j})_{1 \le i,j \le s} \tag{15}$$

in $\mathcal{R}_k$. We denote this element (15) as $\mathbf{s}_\lambda$. It is an irreducible character of S_k and may be characterized as the unique irreducible character that occurs with positive multiplicity in both $Ind_{S_\mu}^{S_k}(\varepsilon)$ and $Ind_{S_\lambda}^{S_k}(1)$; it occurs with multiplicity one in each of them. The p(k) characters $\mathbf{s}_\lambda$ are all distinct, and are all the irreducible characters of S_k.

Remark: In the theorem, ε denotes the alternating character of S_λ and p(k) is the number of all partitions of k.

Now we are ready to present the following theorem concerning the relationship between $\mathcal{R}_k$ and $\mathcal{R}_k(q)$:

Theorem 2. *There is a unique isometry of $\mathcal{R}_k$ into $\mathcal{R}_k(q)$ in which for each subset I of Σ the representation $Ind_{W_I}^{W}(1)$ maps to the representation $Ind_{P_I}^{G}(1)$. This mapping takes irreducible representations to irreducible representations.*

Proof. If $I \subset \Sigma$, let χ_I denote the character of S_k induced from the trivial character of W_I, and let $\chi_I(q)$ denote the character of G induced from the trivial character of P_I.

First, we note that the representations χ_I of $\mathcal{R}_k$ span $\mathcal{R}_k$. Indeed, by the definition of the multiplication in $\mathcal{R}_k$, inducing the trivial representation from $S_{k_1} \times \cdots \times S_{k_r}$ to S_k, where $\Sigma k_i = k$, gives the representation denoted by

$$\mathbf{h}_{k_1} \mathbf{h}_{k_2} \cdots \mathbf{h}_{k_r},$$

which is χ_I. Expanding the left-hand side of (15) expresses each $\mathbf{s}_\lambda$ as a linear combination of such representations, and by Theorem 1 the $\mathbf{s}_\lambda$ span $\mathcal{R}_k$; hence so do the χ_I.

We would like to define a map $\mathcal{R}_k \to \mathcal{R}_k(q)$ by

$$\sum_{I \in \Sigma} n_I \chi_I \mapsto \sum_{I \in \Sigma} n_I \chi_I(q). \tag{16}$$

We need to show this map is well-defined and an isometry.

By Proposition 4, the cardinality of $W_I\backslash W/W_J$ equals the cardinality of $P_I\backslash G/P_J$. Then by Proposition 5, it follows that

$$\langle\chi_I,\chi_J\rangle_{S_k}=|W_I\backslash W/W_J|=|P_I\backslash G/P_J|=\langle\chi_I(q),\chi_J(q)\rangle_G. \tag{17}$$

Now, if $\sum_{I\in\Sigma} n_I\chi_I=0$, then we have

$$\begin{aligned}\langle\sum_I n_I\chi_I(q),\sum_I n_I\chi_I(q)\rangle_G &= \sum_{I,J} n_I n_J\langle\chi_I(q),\chi_J(q)\rangle_G\\ &= \sum_{I,J} n_I n_J\langle\chi_I,\chi_J\rangle_{S_k}\\ &= \langle\sum_I n_I\chi_I,\sum_I n_I\chi_I\rangle_{S_k}=0,\end{aligned}$$

hence $\sum_{I\in\Sigma} n_I\chi_I(q)=0$. Therefore, (16) is well-defined. And by (17) we know it is an isometry.

It remains to be shown that irreducible characters go to irreducible characters. By Theorem 1, we know $\mathbf{s}_\lambda$ are all the irreducible characters of S_k. For any partition λ, it suffices to show the corresponding character $\widehat{\mathbf{s}_\lambda}$ of $\mathbf{s}_\lambda$ in G is irreducible. We already know that $\langle\widehat{\mathbf{s}_\lambda},\widehat{\mathbf{s}_\lambda}\rangle=\langle\mathbf{s}_\lambda,\mathbf{s}_\lambda\rangle=1$, hence either $\widehat{\mathbf{s}_\lambda}$ or $-\widehat{\mathbf{s}_\lambda}$ is irreducible and it suffices to show that $\widehat{\mathbf{s}_\lambda}$ occurs with positive multiplicity in some proper character of G. Indeed, by Theorem 1, $\mathbf{s}_\lambda$ appears with multiplicity one in the character induced from the trivial character of S_λ. Consequently, $\widehat{\mathbf{s}_\lambda}$ occurs with multiplicity one in $\chi_I(q)$, where I is any subset of Σ such that $W_I\cong S_\lambda$. This completes the proof. QED

Let $\mathbf{s}_\lambda(q)$,$\mathbf{h}_k(q)$ and $\mathbf{e}_k(q)$ denote the images of the characters $\mathbf{s}_\lambda$,$\mathbf{h}_k$ and $\mathbf{e}_k$, respectively, of S_k under the isomorphism of Theorem 2.

Proposition 6. *As a virtual representation, the alternating character* $\mathbf{e}_k$ *of* S_k *admits the following expression:*

$$\mathbf{e}_k=\sum_{J\subset\Sigma}(-1)^{|J|}Ind_{W_J}^W(1).$$

Proof. We know that $\mathbf{e}_k=\mathbf{s}_\lambda$, where $\lambda=(1,\cdots,1)$. The right-hand side of (15) gives

$$\mathbf{e}_k=\begin{vmatrix}\mathbf{h}_1 & \mathbf{h}_2 & \mathbf{h}_3 & \cdots & \mathbf{h}_k\\ 1 & \mathbf{h}_1 & \mathbf{h}_2 & \cdots & \mathbf{h}_{k-1}\\ 0 & 1 & \mathbf{h}_1 & \cdots & \mathbf{h}_{k-2}\\ \vdots & \vdots & \vdots & & \vdots\\ 0 & 0 & 0 & \cdots & \mathbf{h}_1\end{vmatrix}.$$

Expanding this gives a sum of exactly 2^{k-1} monomials in the $\mathbf{h}_i$, which are in one-to-one correspondence with the subsets J of Σ. Indeed, let J be given, and let k_1, k_2, $\cdots$ be as in Lemma 1. Then there is a monomial that has $|J|$ 1's taken from below the diagonal; namely, if $(i,i+1)\in J$, then there is a 1 taken from the $(i+1,i)$ position, and as a result there is an $\mathbf{h}_{k_1}$ taken from the $(1,k_1)$ position, and $\mathbf{h}_{k_2}$ taken from the (k_1+1,k_2+1) position, and so forth. This monomial equals $(-1)^{|J|}\mathbf{h}_{k_1}\mathbf{h}_{k_1}\cdots$, which is $(-1)^{|J|}$ times the character induced from the trivial representation of $W_J=S_{k_1}\times S_{k_2\times\ldots}$, i.e., $Ind_{W_J}^W(1)$. QED

Theorem 3. *As a virtual representation,* $\mathbf{e}_k(q)$ *of* $GL(k, \mathbb{F}_q)$ *admits the following expression:*

$$\mathbf{e}_k(q) = \sum_{J \subset \Sigma} (-1)^{|J|} Ind_{P_J}^{P}(1).$$

Proof. This follows immediately from Proposition 6 on applying the mapping of Theorem 2. QED

4 Hecke Algebras $\mathcal{H}$ and $\mathcal{H}_k(q)$

With k and q fixed, let $\mathcal{H}$ be the convolution ring of B-bi-invariant functions on G. The dimension of $\mathcal{H}$ equals the cardinality of $B\backslash G/B$, which is $|W| = k!$ by Bruhat decomposition. A basis of $\mathcal{H}$ consists of the functions $\phi_w (w \in W)$, where ϕ_w is the characteristic function of the double coset $\mathcal{C}(w) = BwB$. We normalize the convolution as follows:

$$(f_1 * f_2)(g) = \frac{1}{|B|} \sum_{x \in G} f_1(x) f_2(x^{-1}g) = \frac{1}{|B|} \sum_{x \in G} f_1(gx) f_2(x^{-1}).$$

With this normalization, the characteristic function f_1 of B serves as a unit in the ring. Here $\mathcal{H}$ is just the *Hecke algebra* $\mathcal{H}(G, \pi)$ with π the trivial representation of B. Define the L^1 norm:

$$|f| = \frac{1}{|B|} \sum_{x \in G} |f(x)|$$

and an *augmentation map* ϵ in $\mathcal{H}$

$$\epsilon(f) = \frac{1}{|B|} \sum_{x \in G} f(x).$$

Proposition 7. *(i)* $\forall f_1, f_2 \in \mathcal{H}$,

$$|f_1 * f_2| \leq |f_1||f_2|.$$

(ii) ϵ *is a* $\mathbb{C}$*-algebra homomorphism and*

$$\epsilon(\phi_w) = q^{l(w)}. \tag{18}$$

Proof. As for (i),

$$\begin{aligned} |f_1 * f_2| &= \frac{1}{|B|} \sum_{x \in G} |(f_1 * f_2)(x)| \\ &\leq \frac{1}{|B|^2} \sum_{x \in G} \sum_{y \in G} |f_1(y)||f_2(y^{-1}x) \\ &= |f_2| \frac{1}{|B|} \sum_{y \in G} |f_1(x)| \\ &= |f_1||f_2|. \end{aligned}$$

As for (ii), $\forall f_1, f_2, f \in \mathcal{H}, k \in \mathbb{C}$, it is trivial that

$$\epsilon(f_1 + f_2) = \epsilon(f_1) + \epsilon(f_2), \epsilon(kf) = k\epsilon(f).$$

And also

$$\begin{aligned}\epsilon(f_1 * f_2) &= \frac{1}{|B|}\sum_{x\in G}(f_1 * f_2)(x) \\ &= \frac{1}{|B|^2}\sum_{x\in G}\sum_{y\in G} f_1(y)f_2(y^{-1}x) \\ &= \frac{1}{|B|}\epsilon(f_2)\sum_{x\in G} f_1(x) \\ &= \epsilon(f_1)\epsilon(f_2).\end{aligned}$$

The identity (18)is trivial since

$$\epsilon(\phi_w) = \frac{1}{|B|}\sum_{x\in G}\phi_w(x) = \frac{1}{|B|}\sum_{x\in BwB} 1 = q^{l(w)}$$

by Proposition 3(iii). QED

Proposition 8. *Let* $w, w^{'} \in W$ *such that* $l(ww^{'}) = l(w)l(w^{'})$*. Then*

$$\phi_{ww'} = \phi_w * \phi_{w'}.$$

Proof. By Proposition 2(iv), we have $\mathcal{C}(ww^{'}) = \mathcal{C}(w)\mathcal{C}(w^{'})$.

If for $g \in G$, $\phi_w * \phi_{w'}(g) \neq 0$, then $\exists x \in G$ such that $gx \in BwB$ and $x^{-1} \in Bw^{'}B$, by the definition of convolution. So $g = gxx^{-1} \in \mathcal{C}(w)\mathcal{C}(w^{'}) = \mathcal{C}(ww^{'})$. Therefore $\phi_w * \phi_{w'}$ is supported in $\phi_{ww'}$ and is hence a constant multiple of $\phi_{ww'}$. Writing $\phi_{ww'} = c\phi_w * \phi_{w'}$, applying the augmentation ϵ and using identity (18), we have c=1. Done. QED.

Proposition 9. *Let* $s \in W$ *be a simple reflection. Then*

$$\phi_s * \phi_s = q\phi_1 + (q-1)\phi_s.$$

Proof. By Proposition 2(v), we have $\mathcal{C}(s)\mathcal{C}(s) \subset \mathcal{C}(1)\cup\mathcal{C}(s)$, so $\phi_s * \phi_s$ is supported in $\mathcal{C}(1) \cup \mathcal{C}(s)$, hence there exist constants a and b, such that $\phi_s * \phi_s = a\phi_1 + b\phi_s$. Evaluating both sides at 1 gives $a = q$. Now applying the augmentation and using the special case $\epsilon(\phi_s) = q$ and $\epsilon(\phi_1) = 1$ of (18), we have $q^2 = a\cdot 1 + b\cdot q$, so $b = q-1$. Done. QED

Inspired by those properties of $\mathcal{H}$, we are going to give a general definition of a certain kind of Hecke algebra. From now on, let q be a nonzero element of a field containing $\mathbb{C}$ and let $R = \mathbb{C}[q, q^{-1}]$. Thus q might be a complex number, in which case $R = \mathbb{C}$ or it might be transcendental over $\mathbb{C}$, in which case the ring R will be the Laurent polynomials over $\mathbb{C}$.

Definition 1. We define $\mathcal{H}_k(q)$ to be the free R-algebra on generators $f_{s_{\alpha_i}}(i = 1, \cdots, k-1)$ subject to the following relations:

$$f_{s_{\alpha_i}}^2 = q + (q-1)f_{s_{\alpha_i}}, \tag{19}$$
$$f_{s_{\alpha_i}} * f_{s_{\alpha_{i+1}}} * f_{s_{\alpha_i}} = f_{s_{\alpha_{i+1}}} * f_{s_{\alpha_i}} * f_{s_{\alpha_{i+1}}}, \tag{20}$$
$$f_{s_{\alpha_i}} * f_{s_{\alpha_j}} = f_{s_{\alpha_j}} * f_{s_{\alpha_i}} \quad \text{if } |i-j| > 1 \tag{21}$$

We note that each $f_{s_{\alpha_i}}$ is invertible, with inverse $q^{-1}f_{s_{\alpha_i}} + q^{-1} - 1$ by (19).

If $w \in W$ is arbitrary, we want to associate an element f_w of $\mathcal{H}_k(q)$ extending the definition of the generators. (Of course, f_w is already defined if w is a simple reflection or the identity.) The next proposition will make it possible.

Proposition 10. *Suppose that $w \in W$ with $l(w) = r$, and suppose that $w = s_1 \cdots s_r = s_1^{'} \cdots s_r^{'}$ are distinct decompositions of minimal length into simple reflections. Then*

$$f_{s_1} * \cdots * f_{s_r} = f_{s_1^{'}} * \cdots * f_{s_r^{'}}.$$

Proof. Let us assume that we have a courterexample of shortest length, say r. Of course $r > 1$. Thus, $l(s_1 \cdots s_r) = r$ and

$$s_1 \cdots s_r = s_1^{'} \cdots s_r^{'} \quad \text{but} \quad f_1 * \cdots * f_r \neq f_1^{'} * \cdots * f_r^{'}, \tag{22}$$

where we write $f_i, f_i^{'}$ for f_{s_i} and $f_{s_i^{'}}$, respectively. Obviously, $s_r \neq s_r^{'}$, since r is the smallest. We will show that

$$s_2 s_3 \cdots s_r s_r^{'} = s_1 s_2 \cdots s_r \quad \text{but} \quad f_2 f_3 * \cdots * f_r f_r^{'} \neq f_1 f_2 * \cdots * f_r \tag{23}$$

Before we prove this, let us explain how it implies the proposition. The W element above is w and thus has length r, so we may repeat the process, obtaining

$$s_3 s_4 \cdots s_r s_r^{'} s_r = s_2 s_3 \cdots s_r s_r^{'} \quad \text{but} \quad f_3 f_4 * \cdots * f_r f_r^{'} f_r \neq f_2 f_3 * \cdots * f_r f_r^{'}.$$

Repeating the process, we eventually obtain

$$s_r^{'} s_r s_r^{'} s_r \cdots = s_r s_r^{'} s_r s_r^{'} \cdots \quad \text{but} \quad f_r^{'} * f_r * f_r^{'} * f_r * \cdots \neq f_r * f_r^{'} * f_r * f_r^{'} * \cdots .$$

Hence moving all the s's on the left together and f's together we have

$$(s_r^{'} s_r)^r = 1 \quad \text{but} \quad (f_r^{'} f_r)^r \neq 1.$$

But from $s_r^{'} s_r)^r = 1$, if we assume $s_r = s_{\alpha_i}$ and $s_r^{'} = s_{\alpha_j}$, then we have $3|r$ if $|i-j| > 1$ and $2|r$, if $|i-j| = 1$. And by the relations in the definition of $\mathcal{H}_k(q)$, we must have $(f_r^{'} * f_r)^r = 1$. Contradiction.

So it remains to show (23). Note that $w_1 = ws_r^{'} = s_1^{'} \cdots s_{r-1}^{'}$ has length $r-1$, so by Proposition 1(ii), assuming $s_r^{'} = s_\alpha$, $\alpha \in \Sigma$, we have $w(\alpha) \in \Phi^-$. Now by Proposition 1(iii), we have

$$s_1 \cdots s_r = s_1 \cdots \widehat{s_i} \cdots s_r s_r^{'} \tag{24}$$

for some $1 \le i \le r$. Then $s_1' \cdots s_{r-1}' = s_1 \cdots \widehat{s_i} \cdots s_r$ and this element has length $r-1$.(If it has a short length, then multiplying on the right by s_r' would contradict the assumption that $l(w) = r$.) By the minimality of the courterexample, we have

$$f_1 * \cdots * \widehat{f_i} * \cdots * f_r = f_1' * \cdots * f_{r-1}'. \tag{25}$$

We claim that $i = 1$. Suppose $i > 1$. Cancel $s_1 \cdots s_{i-1}$ in (24) and we have

$$s_i \cdots s_r = s_{i+1} \cdots \widehat{s_i} \cdots s_r s_r',$$

and since $i > 1$, this has length $r - i + 1 < r$. By the minimality of the courterexample, we have

$$f_i * \cdots * f_r = f_{i+1} * \cdots * f_r f_r'.$$

Now we can multiply this identity on the left by $f_1 * \cdots * f_{i-1}$ and then use (25), we get a contradiction to (22). Hence the first part of (23) follows. As for the second part, if $f_2 f_3 * \cdots * f_r f_r' \neq f_1 f_2 * \cdots * f_r$, then multiplying (25) on the right by f_r' gives a contradiction to (22). So (23) is proved and so is the proposition. QED

If $w \in W$, let $w = s_1 \cdots s_r$ be a decomposition of w into $r = l(w)$ simple reflections, and define

$$f_w = f_{s_1} * \cdots * f_{s_r}.$$

According to the above proposition, this f_w is well-defined.

Theorem 4. ***(IWahori)*** *The f_w form a basis of $\mathcal{H}_k(q)$ as a free R-module. Thus the rank of $\mathcal{H}_k(q)$ is $|W|$.*

Proof. First, assume that q is transcendental, so that R is the ring of Laurent polynomials in q. We will deduce the corresponding statement when $q \in \mathbb{C} - \{0\}$ at the end.

Let us check that

$$\sum_{w \in W} R f_w = \mathcal{H}_k(q). \tag{26}$$

It is sufficient to show that this R-submodule(on the left side of (26)) is closed under right multiplication by generators f_s of W with s a simple reflection. If $l(ws) = l(w) + 1$, then $f_w * f_s = f_{ws}$ which is of course in this module; on the other hand, if $l(ws) = l(w) - 1$, then writing $w\prime = ws$ we have

$$f_w * f_s = f_{w's} * f_s = f_{w'} * f_s^2 = f_{w'} * (q + (q-1) f_s) = q f_{w'} + (q-1) f_{w'} * f_s = q f_{w'} + (q-1) f_w.$$

It remains to show that the sum in (26) is direct. If not, there will be some Laurent polynomials $c_w(q)$, not all zero, such that $\sum_w c_w(q) f_w = 0$. Then there exists a rational prime p such that $c_w(p)$ is not all zero(since as a rational function c_w has only finitely many roots). As before, let $\mathcal{H}$ be the convolution ring of B-bi-invariant functions on $GL(k, \mathbb{F}_p)$. It follows from the Proposition 7 and 8 that (19),(20) and (21) are all satisfied by the standard generators of $\mathcal{H}$, so we have a homomorphism $\mathcal{H}_k(q) \to \mathcal{H}$ mapping each f_w to the corresponding generator ϕ_w and mapping q to p. The images of f_w are linearly independent in $\mathcal{H}$, yet since the $c_w(p)$ are not all zero, we obtain a relation of linear dependence. This is a contradiction.

The result is proved if q is transcendental. It remains to show the same result follows for $\mathcal{H}_k(q_0)$ if $0 \neq q_0 \in \mathbb{C}$. There is a homomorphism $R \to \mathbb{C}$, and a compatible homomorphism $\mathcal{H}_k(q) \to \mathcal{H}_k(q_0)$, in which $q \mapsto q_0$. Similarly, we can show the identity (26), and what we must show is that the R-basis elements f_w remain linearly independent when projected to $\mathcal{H}_k(q_0)$. To prove this, we note that in $\mathcal{H}_k(q)$ we have

$$f_w * f_{w'} = \sum_{w'' \in W} a_{w,w',w''}(q, q^{-1}) f_{w''},$$

where $a_{w,w',w''}$ is a polynomial in q and q^{-1}. Here we construct a new ring $\widetilde{\mathcal{H}}_k(q_0)$ over $\mathbb{C}$ with basis elements $\widetilde{f}_w$ indexed by W and specialized ring structure constants $a_{w,w',w''}(q_0, q_0^{-1})$. The associative law in $\mathcal{H}_k(q)$ boils down to a polynomial identity that remains true in this new ring, so this ring exists. Clearly, the identities (19),(20) and (21) are true in this new ring. So there exists a homomorphism $\mathcal{H}_k(q_0) \to \widetilde{\mathcal{H}}_k(q_0)$ mapping the f_w to the $\widetilde{f}_w$. Since the $\widetilde{f}_w$ are linearly independent, so are the f_w in $\mathcal{H}_k(q_0)$. QED

Let us return to the case where q is a prime power.

Theorem 5. *Let q be a prime power. Then the Hecke algebra $\mathcal{H}_k(q)$ is isomorphic to the convolution ring $\mathcal{H}$ of B-bi-invariant functions on $GL(k, \mathbb{F}_q)$, where B is the Borel subgroup of upper triangular matrices in $GL(k, \mathbb{F}_q)$. In this isomorphism, the standard basis element $f_w (w \in W)$ corresponds to the characteristic function of the double coset BwB.*

Proof. It follows from Proposition 8 and 9 that those identities (19),(20) and (21) are all satisfied by the elements ϕ_w in the ring $\mathcal{H}$ of B-bi-invariant functions on $GL(k, \mathbb{F}_q)$, so there exists a homomorphism $\mathcal{H}_k(q) \to \mathcal{H}$ such that $f_w \mapsto \phi_w$. Since the $\{f_w\}$ are a basis of $\mathcal{H}_k(q)$ and the $\{\phi_w\}$ is a basis of $\mathcal{H}$, this ring homomorphism is an isomorphism. QED

References

[1] Daniel Bump, Lie Groups, Chapter 48, 30, 28, 21 and 37 (2004)