

# THE STEINBERG MODULE AND THE HECKE ALGEBRA

N. P. STRICKLAND

## 1. INTRODUCTION

This note aims to give a self-contained exposition of the Steinberg module and the Hecke algebra for  $GL_n(\mathbb{F}_p)$ , aiming towards the applications in algebraic topology. We have tried to use methods that are elementary, or failing that, familiar to topologists.

I have not tried to investigate the history of these ideas but it seems likely that it goes something like this.

- (a) People worked out how to solve problems by matrix calculations, including row-reduction.
- (b) Thinking more abstractly, other people worked out the ideas presented here.
- (c) Generalising further, people developed a still more abstract theory of Coxeter groups,  $BN$  pairs and so on.

There is plenty of current literature written at levels (a) and (c), but not so much at level (b). Everything that we say is well-known to those who have digested the more general theory, so our purpose is purely expository.

To avoid trivialities, we assume  $n > 1$  unless otherwise stated.

## 2. LENGTH OF PERMUTATIONS

For any permutation  $\sigma \in \Sigma_n$ , we put

$$\begin{aligned} L(\sigma) &= \{(i, j) \mid 0 < i < j \leq n \text{ and } \sigma(i) > \sigma(j)\} \\ L^+(\sigma) &= L(\sigma) \amalg \{(i, i) \mid 0 < i \leq n\} \\ &= \{(i, j) \mid 0 < i \leq j \leq n \text{ and } \sigma(i) \geq \sigma(j)\} \\ l(\sigma) &= |L(\sigma)|. \end{aligned}$$

The integer  $l(\sigma)$  is called the *length* of  $\sigma$ .

**Example 2.1.** For  $\sigma = (1\ 3\ 5)(2\ 4)$  we have

$$L(\sigma) = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\},$$

so  $l(\sigma) = 7$ .

It is sometimes convenient to reformulate this slightly. We put

$$\bar{L}(\sigma) = \{\{i, j\} \mid (i, j) \in L(\sigma)\}.$$

Equivalently,  $\bar{L}(\sigma)$  is the set of subsets  $T \subseteq \{1, \dots, n\}$  such that  $|T| = 2$  and  $\sigma: T \rightarrow \sigma T$  is order-reversing. As  $i < j$  for all  $(i, j) \in L(\sigma)$  we see that  $\bar{L}(\sigma)$  bijects with  $L(\sigma)$ , so  $|\bar{L}(\sigma)| = l(\sigma)$ .

**Remark 2.2.** Put  $\Delta = \prod_{i < j} (x_j - x_i) \in \mathbb{Z}[x_1, \dots, x_n]$ . One can then see that for  $\sigma \in \Sigma_n$  we have  $\sigma \cdot \Delta = (-1)^{l(\sigma)} \Delta$ . Using this, we find that the map  $\sigma \mapsto (-1)^{l(\sigma)}$  is a nontrivial homomorphism  $\Sigma_n \rightarrow \{\pm 1\}$ , which must therefore be the same as the signature.

**Lemma 2.3.**  $l(\sigma^{-1}) = l(\sigma)$ .

*Proof.*  $\sigma$  induces a bijection  $L(\sigma) \rightarrow L(\sigma^{-1})$ . □

**Definition 2.4.** For  $i = 1, \dots, n - 1$  we let  $s_i$  denote the transposition that exchanges  $i$  and  $i + 1$ .

**Proposition 2.5.**  $l(\sigma)$  is the least  $r$  such that  $\sigma$  can be written in the form  $s_{i_1} s_{i_2} \dots s_{i_r}$ .

**Lemma 2.6.** For permutations  $\sigma, \tau \in \Sigma$  we have

$$\overline{L}(\sigma\tau) = \overline{L}(\tau)\Delta\tau_*^{-1}\overline{L}(\sigma)$$

(where  $A\Delta B$  is the symmetric difference,  $(A \cup B) \setminus (A \cap B)$ .)

*Proof.* Consider a pair of permutations  $\sigma, \tau$ . The composite

$$\{i, j\} \xrightarrow{\tau} \tau_*\{i, j\} = \{\tau(i), \tau(j)\} \xrightarrow{\sigma} \sigma_*\tau_*\{i, j\}$$

is order-reversing iff precisely one of the two composed maps is order-reversing.  $\square$

**Lemma 2.7.** If  $\sigma(k) < \sigma(k+1)$  then  $l(\sigma s_k) = l(\sigma) + 1$ , otherwise  $l(\sigma s_k) = l(\sigma) - 1$ .

*Proof.* Now take  $\tau = s_k$  in the previous lemma, so  $\overline{L}(\tau) = \{\{k, k+1\}\}$ . It follows that  $l(\sigma s_k)$  is  $l(\sigma) - 1$  if  $\{k, k+1\} \in s_{k*}^{-1}\overline{L}(\sigma)$ , and  $l(\sigma) + 1$  otherwise. As  $s_{k*}\{k, k+1\} = \{k, k+1\}$  we have  $\{k, k+1\} \in s_{k*}^{-1}\overline{L}(\sigma)$  iff  $\{k, k+1\} \in \overline{L}(\sigma)$  iff  $\sigma(k) > \sigma(k+1)$ , as required.  $\square$

*Proof of Proposition 2.5.* If  $\sigma = s_{i_1}s_{i_2}\dots s_{i_r}$ , then it is immediate from the lemma that  $l(\sigma) \leq r$ . Conversely, suppose we have  $l(\sigma) = r$ . If  $r = 0$  then  $\sigma$  is order-preserving and so must be the identity, which is compatible with the claim in the proposition. If  $r > 0$  then  $\sigma$  is not order-preserving, so there must exist  $k$  with  $\sigma(k+1) < \sigma(k)$ . The lemma tells us that  $l(\sigma s_k) = r - 1$ . We may thus assume inductively that  $\sigma s_k = s_{i_1}s_{i_2}\dots s_{i_{r-1}}$  for some  $i_1, \dots, i_{r-1}$ . It follows that  $\sigma = s_{i_1}\dots s_{i_{r-1}}s_k$ , which is an expression of the required form.  $\square$

**Definition 2.8.** Consider a word  $w = s_{i_1}s_{i_2}\dots s_{i_r}$  in the variables  $s_1, \dots, s_{n-1}$ . The corresponding permutation then has length at most  $r$ . If the length is precisely  $r$ , we say that  $w$  is *reduced*.

**Definition 2.9.** We write  $\rho$  for the permutation  $\rho(i) = n+1-i$ , which satisfies  $\rho^2 = 1$ . Note that  $\rho(i) > \rho(j)$  iff  $i < j$ , so  $l(\rho) = n(n-1)/2$ .

**Definition 2.10.** For  $m \leq k$  we put  $t_m^k = s_m s_{m+1} \dots s_{k-1}$  (to be interpreted as the identity when  $m = k$ ). In cycle notation, this is

$$t_m^k = (m, m+1, \dots, k-1, k).$$

**Proposition 2.11.** For any  $\sigma \in \Sigma_n$  there is a unique sequence  $m_1, \dots, m_n$  with  $1 \leq m_k \leq k$  and

$$\sigma = t_{m_n}^n t_{m_{n-1}}^{n-1} \dots t_{m_2}^2 t_{m_1}^1.$$

Moreover, we have  $l(\sigma) = \sum_{k=1}^n (k - m_k)$ .

*Proof.* Put  $m_n = \sigma(n)$  and  $\tau = (t_{m_n}^n)^{-1}\sigma$ . Then  $\tau(n) = n$ , so  $\tau$  can be regarded as an element of  $\Sigma_{n-1}$ , so by induction we have

$$\tau = t_{m_{n-1}}^{n-1} t_{m_{n-2}}^{n-2} \dots t_{m_2}^2 t_{m_1}^1$$

for some  $m_{n-1}, \dots, m_1$ , and  $l(\tau) = \sum_{k=1}^{n-1} (k - m_k)$ . It follows that

$$\sigma = t_{m_n}^n \tau = t_{m_n}^n t_{m_{n-1}}^{n-1} \dots t_{m_2}^2 t_{m_1}^1.$$

We also have

$$\overline{L}(t_{m_n}^n) = \{\{i, n\} \mid m_n \leq i < n\},$$

so

$$\tau_*^{-1}\overline{L}(t_{m_n}^n) = \{\{\tau^{-1}(i), n\} \mid m_n \leq i < n\},$$

whereas  $\overline{L}(\tau)$  contains no pairs of the form  $\{i, n\}$ . Thus  $\overline{L}(\tau)$  and  $\tau_*^{-1}\overline{L}(t_{m_n}^n)$  are disjoint, and

$$l(\sigma) = |\overline{L}(\tau)| + |\tau_*^{-1}\overline{L}(t_{m_n}^n)| = l(\tau) + (n - m_n) = \sum_{k=1}^n (k - m_k).$$

$\square$

**Definition 2.12.** Let  $\widetilde{\Sigma}_n$  be the group freely generated by symbols  $s_1, \dots, s_{n-1}$  subject to the relations  $s_i^2 = 1$  and  $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$  and  $s_i s_j = s_j s_i$  whenever  $|i - j| > 1$ . It is straightforward to check that the corresponding relations hold in  $\Sigma_n$ , so there is a canonical map  $\epsilon: \widetilde{\Sigma}_n \rightarrow \Sigma_n$  sending  $s_i$  to  $s_i$ . We will use the notation  $t_m^k$  for the element  $s_m s_{m+1} \dots s_{k-1}$  in  $\widetilde{\Sigma}_n$  as well as the corresponding element in  $\Sigma_n$ .

**Proposition 2.13.** *The map  $\epsilon: \tilde{\Sigma}_n \rightarrow \Sigma_n$  is an isomorphism.*

*Proof.* Let  $X_n \subseteq \tilde{\Sigma}_n$  be the set of elements of the form  $t_{m_n}^n t_{m_{n-1}}^{n-1} \dots t_{m_1}^1$  with  $1 \leq m_k \leq k$ , so  $|X_n| \leq n!$ . We see from Proposition 2.11 that  $\epsilon: X_n \rightarrow \Sigma_n$  is surjective, and hence bijective by a counting argument. It will therefore suffice to show that  $X_n = \tilde{\Sigma}_n$ . Note that  $X_n = \bigcup_{m=1}^n t_m^n X_{n-1}$ , and we may assume by induction that  $X_{n-1} = \tilde{\Sigma}_{n-1}$ , so  $X_n$  is closed under right multiplication by  $\tilde{\Sigma}_{n-1}$ . As  $\tilde{\Sigma}_n$  is generated by  $\tilde{\Sigma}_{n-1}$  and  $s_{n-1}$ , it will suffice to show that  $X_n$  is closed under right multiplication by  $s_{n-1}$ . This can be deduced from Lemma 2.14 below, after noting that  $s_{n-1}$  commutes with  $t_m^k$  for all  $k < n-1$ .  $\square$

**Lemma 2.14.** *If  $k \leq n$  and  $l < n$  then in  $\tilde{\Sigma}_n$  we have*

$$t_k^n t_l^{n-1} s_{n-1} = t_k^n t_l^n = \begin{cases} t_{l+1}^n t_k^{n-1} & \text{for } k \leq l \\ t_l^n t_{k-1}^{n-1} & \text{for } k > l. \end{cases}$$

*Proof.* (a) It is immediate from the definitions that  $t_k^n t_l^{n-1} s_{n-1} = t_k^n t_l^n$ .

(b) We claim that for  $l < n$  we have  $(t_{l+1}^n)^{-1} t_l^n = t_l^{n-1} (t_l^n)^{-1}$ . We first give a proof for the case  $l = 5$  and  $n = 10$ , writing  $k$  instead of  $s_k$  for brevity, and  $e$  for the identity permutation.

$$\begin{aligned} (t_6^{10})^{-1} t_5^{10} &= 987656789 \\ &= 987565789 && (656 = 565) \\ &= 598767895 && ([5, 7] = [5, 8] = [5, 9] = e) \\ &= 598676895 && (767 = 676) \\ &= 569878965 && ([6, 8] = [6, 9] = e) \\ &= 569787965 && (878 = 787) \\ &= 567989765 && ([7, 9] = e) \\ &= 567898765 && (989 = 898) \\ &= t_5^9 (t_5^{10})^{-1} \end{aligned}$$

This pattern can be converted to a formal proof as follows. The claim is clear when  $l = n-1$ , so we can work by downwards induction on  $l$ . Consider the relation  $s_{l+1} s_l s_{l+1} = s_l s_{l+1} s_l$ . We multiply on the right by  $t_{l+2}^n$  and on the left by  $(t_{l+2}^n)^{-1}$ , noting that  $(t_{l+2}^n)^{-1} s_{l+1} = (t_{l+1}^n)^{-1}$  and  $s_l s_{l+1} t_{l+2}^n = t_l^n$  and that  $s_l$  commutes with  $t_{l+2}^n$ . This gives

$$(t_{l+1}^n)^{-1} t_l^n = s_l (t_{l+2}^n)^{-1} s_{l+1} t_{l+2}^n s_l.$$

We can use the relation  $s_{l+1} t_{l+2}^n = t_{l+1}^n$  and the induction hypothesis to convert the right hand side to  $s_l t_{l+1}^{n-1} (t_{l+1}^n)^{-1} s_l$ , and from the definitions, this is the same as  $t_l^{n-1} (t_l^n)^{-1}$ .

- (c) Now suppose that  $k \leq l$ . Note that  $t_k^m = t_k^l t_l^m$  and that  $t_k^l$  commutes with  $t_{l+1}^m$ . We can therefore multiply the identity in (b) on the left by  $t_k^l$  to get  $(t_{l+1}^n)^{-1} t_k^n = t_k^{n-1} (t_l^n)^{-1}$ . This can be rearranged to give the case  $k \leq l$  of the lemma.
- (d) Now suppose we have  $n \geq i > j$ . Take  $k = j$  and  $l = i-1$  in (c) to get  $(t_i^n)^{-1} t_j^n = t_j^{n-1} (t_{i-1}^n)^{-1}$ . From the definitions, the right hand side can be rewritten as  $t_j^n (t_{i-1}^{n-1})^{-1}$ , and the equation can then be rearranged to give  $t_i^n t_j^n = t_j^n t_{i-1}^{n-1}$ . Up to a change of notation, this is the same as the second case of the lemma.  $\square$

**Definition 2.15.** Let  $W_r$  be the set of words of length  $r$  in letters  $s_1, \dots, s_n$ , and put  $W = \coprod_r W_r$ , which is the free monoid generated by  $s_1, \dots, s_n$ . Let  $\sim_r$  be the equivalence relation on  $W_r$  generated by the following rules:

- $u s_i s_j v \sim u s_j s_i v$  if  $|i - j| > 1$
- $u s_i s_j s_i v = u s_j s_i s_j v$  if  $|i - j| = 1$ .

Put  $M_r = W_r / \sim_r$  and  $M = \coprod_r M_r$ , so  $M$  is the quotient monoid of  $W$  by the relations  $s_i s_j = s_j s_i$  (for  $|i - j| > 1$ ) and  $s_i s_j s_i = s_j s_i s_j$  (for  $|i - j| = 1$ ). We then have

$$\Sigma = M / \langle s_i^2 = 1 \mid i = 1, \dots, n-1 \rangle$$

Let

$$\begin{array}{ccc} W & \xrightarrow{\pi'} & M \\ & \searrow \pi & \swarrow \pi'' \\ & \Sigma & \end{array}$$

be the obvious projection maps. Recall that a word  $w = s_{p_1} \cdots s_{p_r} \in W$  is *reduced* iff  $l(\pi(w)) = r$ . We write  $R_r$  for the set of reduced words of length  $r$ , and put  $R = \coprod_r R_r$ . Note that if  $u \in R_r$  and  $v \in W_r$  and  $u \sim_r v$  then  $v \in R_r$ .

**Theorem 2.16.** *Let  $u, v \in R_r$  be such that  $\pi(u) = \pi(v)$ ; then  $u \sim_r v$  (or equivalently  $\pi'(u) = \pi'(v)$ ).*

The proof will be given after some preliminaries.

**Definition 2.17.** Given  $\sigma, \tau \in \Sigma$ , we say that  $\sigma$  *could end with*  $\tau$  if the following equivalent conditions are satisfied:

- (a) There exists  $\rho \in \Sigma$  such that  $\sigma = \rho\tau$  and  $l(\sigma) = l(\rho) + l(\tau)$ .
- (b)  $l(\sigma\tau^{-1}) = l(\sigma) - l(\tau)$ .
- (c) There are reduced words  $u, v$  such that  $\pi(v) = \tau$  and  $\pi(uv) = \sigma$ .
- (d)  $\overline{L}(\tau) \subseteq \overline{L}(\sigma)$ .

(It is straightforward to check that (a) to (c) are equivalent, and it follows from Lemma 2.6 that (a) is equivalent to (d).)

**Lemma 2.18.** *Suppose that  $\sigma \in \Sigma$  and that  $\sigma$  could end with  $s_i$ , and also  $\sigma$  could end with  $s_j$ , where  $j \neq i$ .*

- (a) *If  $|i - j| > 1$  then  $\sigma$  could end with  $s_i s_j = s_j s_i$ .*
- (b) *If  $|i - j| = 1$  then  $\sigma$  could end with  $s_i s_j s_i = s_j s_i s_j$ .*

*Proof.* As  $\sigma$  could end with  $s_i$  we have  $\overline{L}(s_i) = \{\{i, i+1\}\} \subseteq \overline{L}(\sigma)$ , so  $\sigma(i) > \sigma(i+1)$ . Similarly  $\sigma(j) > \sigma(j+1)$ . If  $|i - j| > 1$  one checks that  $\overline{L}(s_i s_j) = \{\{i, i+1\}, \{j, j+1\}\}$ , so  $\sigma$  could end with  $s_i s_j$ . Suppose instead that  $|i - j| = 1$ ; we may assume without loss that  $j = i + 1$ . We have  $\sigma(i) > \sigma(i+1) = \sigma(j) > \sigma(j+1)$ , so

$$\{\{i, i+1\}, \{i+1, i+2\}, \{i, i+2\}\} \subseteq \overline{L}(\sigma).$$

The permutation  $\tau = s_i s_j s_i = s_j s_i s_j$  is then the 3-cycle  $(i, i+1, i+2)$ , so  $\overline{L}(\tau) = \{\{i, i+1\}, \{i+1, i+2\}, \{i, i+2\}\}$ , so  $\sigma$  could end with  $\tau$ , as claimed.  $\square$

*Proof.* Proof of Theorem 2.16 We work by induction on  $r$ , noting that the cases  $r = 0$  and  $r = 1$  are easy. We may thus suppose that  $r > 1$  and that  $u = x s_i$ ,  $v = y s_j$  for some  $x, y \in R_{r-1}$  and  $i, j \in \{1, \dots, n-1\}$ . Put

$$\sigma = \pi(u) = \pi(v) = \pi(x) s_i = \pi(y) s_j.$$

If  $i = j$  we see that  $\pi(x) = \pi(y)$ , so  $x \sim y$  by the induction hypothesis, so  $u = x s_i \sim y s_i = y s_j = v$  as required. If  $|i - j| = 1$  we see from Lemma 2.18 that there exists  $z \in R_{r-3}$  with  $\sigma = \pi(z s_i s_j s_i) = \pi(z s_j s_i s_j)$ . The  $i = j$  case now tells us that  $u = x s_i \sim z s_i s_j s_i$  and  $z s_j s_i s_j \sim y s_j = v$ , and from the definitions we have  $z s_i s_j s_i \sim z s_j s_i s_j$  so  $u = v$ . A very similar argument works when  $|i - j| > 1$ .  $\square$

### 3. STANDARD NOTATION

In some parts of our exposition, it will be convenient to work with an arbitrary finite-dimensional vector space  $W$  over  $\mathbb{F}_p$ . In others, it will be convenient to take  $W = \mathbb{F}_p^n$ . In that context, we let  $e_1, \dots, e_n$  be the

standard basis, and put  $E_i = \mathbb{F}_p\{e_1, \dots, e_i\}$ . We let  $G = GL_n(\mathbb{F}_p)$  be the automorphism group of  $\mathbb{F}_p^n$ , and put

$$\begin{aligned} T &= \{g \in G \mid ge_i \in \mathbb{F}_p e_i \text{ for all } i\} \\ &= \{\text{invertible diagonal matrices}\} \\ B &= \{g \in G \mid gE_i = E_i \text{ for all } i\} \\ &= \{\text{invertible upper triangular matrices}\} \\ U &= \{g \in B \mid ge_i = e_i \pmod{E_{i-1}}\} \\ &= \{\text{upper unitriangular matrices}\}. \end{aligned}$$

Given  $g \in G$  we let  $g_{ij}$  denote the element in the  $i$ 'th row and  $j$ 'th column of the corresponding matrix. If  $n = 3$ , a typical element of  $G$  then has the form

$$\begin{bmatrix} g_{11} & g_{12} & g_{13} \\ g_{21} & g_{22} & g_{23} \\ g_{31} & g_{32} & g_{33} \end{bmatrix}$$

With this convention, we have  $(gh)_{ik} = \sum_j g_{ij}h_{jk}$  and  $g.e_j = \sum_i g_{ij}e_i$  and  $(g.x)_i = \sum_j g_{ij}x_j$ . Moreover, we have

$$\begin{aligned} T &= \{g \in G \mid g_{ij} = 0 \text{ whenever } i \neq j\} \\ B &= \{g \in G \mid g_{ij} = 0 \text{ whenever } i > j\} \\ U &= \{g \in B \mid g_{ii} = 1 \text{ for all } i\}. \end{aligned}$$

We regard  $\Sigma_n$  as a subgroup of  $G$  in the usual way, so  $\sigma.e_i = e_{\sigma(i)}$  and  $(\sigma.x)_i = x_{\sigma^{-1}(i)}$ . The corresponding matrix elements are  $\sigma_{ij} = \delta_{i, \sigma(j)}$ . Note that  $B$  fits in a split extension  $U \rightarrow B \rightarrow T$ , and we have

$$\begin{aligned} |T| &= (p-1)^n \\ |U| &= p^{n(n-1)/2} \\ |B| &= (p-1)^n p^{n(n-1)/2}. \end{aligned}$$

#### 4. JORDAN PERMUTATIONS

Let  $W$  be a vector space of dimension  $n$  over  $\mathbb{F}_p$ . We write  $\text{Flag}(W)$  for the set of complete flags  $\underline{U} = (U_0 < U_1 < \dots < U_n = W)$  (where necessarily  $\dim(U_i) = i$  for all  $i$ ). Now suppose we have two flags  $\underline{U}, \underline{V} \in \text{Flag}(W)$ . For  $0 < i, j \leq n$  we put

$$Q_{ij} = \frac{U_i \cap V_j}{(U_{i-1} \cap V_j) + (U_i \cap V_{j-1})}.$$

One checks that the natural map from this to

$$\frac{U_{i-1} + (U_i \cap V_j)}{U_{i-1} + (U_i \cap V_{j-1})}$$

is an isomorphism. Thus, the groups  $Q_{i,1}, \dots, Q_{i,n}$  are the quotients in the filtration of the one-dimensional space  $U_i/U_{i-1}$  by the groups  $(U_{i-1} + (U_i \cap V_j))/U_{i-1}$ . It follows that for each  $i$  there is a unique index  $j = \sigma(i)$  such that  $Q_{i, \sigma(i)} \neq 0$ . Similarly, for each  $j$ , there is a unique  $i = \tau(j)$  such that  $Q_{\tau(j), j} \neq 0$ . It follows that  $\sigma$  and  $\tau$  are inverse to each other, so both lie in  $\Sigma_n$ . We write  $\delta(\underline{U}, \underline{V})$  for  $\sigma$ , and note that  $\delta(\underline{V}, \underline{U}) = \delta(\underline{U}, \underline{V})^{-1}$ .

**Example 4.1.** We claim that  $\delta(\sigma \underline{E}, \underline{E}) = \sigma$ . This is more or less clear except perhaps for the fact that it is  $\sigma$  and not  $\sigma^{-1}$ . To check this we put

$$U_i = \sigma E_i = \text{span}\{e_{\sigma(1)}, \dots, e_{\sigma(i)}\} = \text{span}\{e_k \mid \sigma^{-1}(k) \leq i\}$$

and  $V_j = E_j = \text{span}\{e_1, \dots, e_j\}$ , and we consider the quotients

$$Q_{ij} = \frac{U_i \cap V_j}{(U_{i-1} \cap V_j) + (U_i \cap V_{j-1})}$$

Put  $A_i = \{e_k \mid \sigma^{-1}(k) \leq i\}$  and  $B_j = \{e_k \mid k \leq j\}$ . Then  $A_i \cap B_j$  is a basis for  $U_i \cap V_j$ , so the set

$$C_{ij} = (A_i \cap B_j) \setminus ((A_{i-1} \cap B_j) \cup (A_i \cap B_{j-1}))$$

is a basis for  $Q_{ij}$ . However, we have

$$C_{ij} = (A_i \setminus A_{i-1}) \cap (B_j \setminus B_{j-1}) = \{e_{\sigma(i)}\} \cap \{e_j\},$$

so  $Q_{ij} = 0$  unless  $j = \sigma(i)$ .

**Example 4.2.** Take  $W = \mathbb{F}_p^5$ . Given elements  $a, \dots, g \in \mathbb{F}_p$ , put

$$u_1 = \begin{bmatrix} a \\ b \\ c \\ d \\ 1 \end{bmatrix} \quad u_2 = \begin{bmatrix} e \\ f \\ g \\ 1 \\ 0 \end{bmatrix} \quad u_3 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad u_4 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad u_5 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

Then  $Q_{15}$  is spanned by  $u_1$ ,  $Q_{24}$  is spanned by  $u_2$ ,  $Q_{31}$  is spanned by  $u_3$ ,  $Q_{42}$  is spanned by  $u_4$ ,  $Q_{53}$  is spanned by  $u_5$ , and all other  $Q_{ij}$ 's are zero. It follows that  $\delta(\underline{U}, \underline{E}) = (1 \ 5 \ 3)(2 \ 4)$ .

**Remark 4.3.** As the definition of  $\delta(\underline{U}, \underline{V})$  is completely natural, we have  $\delta(g\underline{U}, g\underline{V}) = \delta(\underline{U}, \underline{V})$  for all  $\underline{U}, \underline{V} \in \text{Flag}(W)$  and  $g \in \text{Aut}(W)$ .

**Remark 4.4.** It is not true in general that

$$\delta(\underline{T}, \underline{V}) = \delta(\underline{T}, \underline{U})\delta(\underline{U}, \underline{V}).$$

Indeed, if  $n = 2$  then  $\text{Flag}(V)$  is naturally identified with the set  $PV$  of one-dimensional subspaces of  $V$ . If we let  $\rho$  be the nontrivial element of  $\Sigma_2$ , then  $\delta(L, L) = 1$ , and  $\delta(L, M) = \rho$  whenever  $L \neq M$ . It follows that if  $L, M$  and  $N$  are all distinct, then

$$\delta(L, N) \neq \delta(L, M)\delta(M, N).$$

We now consider the cases where  $\delta(\underline{U}, \underline{V})$  is the identity or one of the adjacent transpositions  $s_i$ . These could also be extracted from the more general theory in the next section but it is instructive to treat them directly.

**Lemma 4.5.** *Suppose we have flags  $\underline{U}, \underline{V}$  with  $\delta(\underline{U}, \underline{V}) = \sigma$ . If  $U_{i-1} = V_{i-1}$  then  $\sigma(i) = i$  iff  $U_i = V_i$ .*

*Proof.* Put  $A = U_{i-1} = V_{i-1}$ , so  $\dim(A) = i - 1$ . We have  $U_{i-1} \cap V_i = V_{i-1} \cap V_i = V_{i-1} = A$  and similarly  $U_i \cap V_{i-1} = A$  so  $Q_{ii} = (U_i \cap V_i)/A$ . Thus  $\sigma(i) = i$  iff  $Q_{ii} \neq 0$  iff  $U_i \cap V_i > A$ . As  $U_i$  and  $V_i$  have dimension  $i$  and  $A$  has dimension  $i - 1$ , we have  $U_i \cap V_i > A$  iff  $U_i = V_i$ .  $\square$

**Corollary 4.6.** *If  $\delta(\underline{U}, \underline{V}) = 1$  then  $\underline{U} = \underline{V}$ .*  $\square$

**Proposition 4.7.** *We have  $\delta(\underline{U}, \underline{V}) = s_i$  iff  $U_j = V_j$  for all  $j \neq i$  but  $U_i \neq V_i$ .*

*Proof.* Suppose that  $\delta(\underline{U}, \underline{V}) = s_i$ . Lemma 4.5 tells us that  $U_j = V_j$  for  $j < i$ , but  $U_i \neq V_i$ . Put  $A = U_{i-1} = V_{i-1}$ . As  $U_i \neq V_i$  we see that  $U_i \cap V_i$  must be strictly smaller than  $U_i$ , but it contains  $A$ , which has codimension one in  $U_i$ , so  $U_i \cap V_i = A$ . Using this we find that  $Q_{i,i+1} = (U_i \cap V_{i+1})/A$ . As  $\delta(\underline{U}, \underline{V}) = s_i$  we have  $Q_{i,i+1} \neq 0$ , so  $\dim(U_i \cap V_{i+1}) \geq \dim(A) + 1 = i$ , but  $\dim(U_i) = i$  so  $U_i \cap V_{i+1} = U_i$ , so  $U_i < V_{i+1}$ . Of course we also  $V_i < V_{i+1}$  and

$$\dim(U_i + V_i) = \dim(U_i) + \dim(V_i) - \dim(U_i \cap V_i) = i + i - (i - 1) = i + 1 = \dim(V_{i+1}),$$

so  $V_{i+1} = U_i + V_i$ . Symmetrically, we have  $U_{i+1} = U_i + V_i$ . For  $j > i + 1$  we have  $s_i(j) = j$ , so we can use Lemma 4.5 to show that  $U_j = V_j$  for all such  $j$ .

We leave the converse to the reader.  $\square$

## 5. SCHUBERT CELLS

Given a flag  $\underline{V} \in \text{Flag}(W)$  and a permutation  $\sigma \in \Sigma_n$  we put

$$Y = Y(\sigma, \underline{V}) = \{\underline{U} \mid \delta(\underline{U}, \underline{V}) = \sigma\} \subset \text{Flag}(W).$$

We write  $Y(\sigma)$  for  $Y(\sigma, \underline{E}) \subset \text{Flag}(\mathbb{F}_p^n)$ . We also put

$$X = X(\sigma) = U \cap U^{(\sigma\rho)^{-1}},$$

where  $\rho(i) = n + 1 - i$  as in Definition 2.9.

**Lemma 5.1.** A matrix  $g = (g_{ij})_{i,j=1}^n \in M_n(\mathbb{F}_p)$  lies in  $X(\sigma)$  iff we have

$$g_{ij} = \begin{cases} 1 & \text{if } i = j \\ \text{arbitrary} & \text{if } (i, j) \in L(\sigma^{-1}) \\ 0 & \text{otherwise.} \end{cases}$$

In particular, we have  $|X(\sigma)| = p^{l(\sigma)}$ .

*Proof.* We have  $g \in U$  iff  $g_{ii} = 1$ , and  $g_{ij} = 0$  whenever  $i > j$ . Next, we have  $g \in U^\tau$  iff  $\tau g \tau^{-1} \in U$  iff  $a_{ij} = 0$  whenever  $\tau(i) > \tau(j)$ . In particular, we have  $g \in U^{(\sigma\rho)^{-1}} = U^{\rho\sigma^{-1}}$  iff  $g_{ij} = 0$  whenever  $\rho\sigma^{-1}(i) > \rho\sigma^{-1}(j)$ , or equivalently  $\sigma^{-1}(i) < \sigma^{-1}(j)$ . The claim follows.  $\square$

**Proposition 5.2.** The map  $\phi: g \mapsto g\sigma\underline{E}$  gives a bijection  $X(\sigma) \rightarrow Y(\sigma)$ . In particular, we have  $|Y(\sigma)| = p^{l(\sigma)}$ , and thus  $|Y(\sigma, \underline{V})| = p^{l(\sigma)}$  for any  $\underline{V}$ .

*Proof.* First note that  $X(\sigma) \subseteq U \subseteq B$ , so for  $g \in X(\sigma)$  we have  $g^{-1}\underline{E} = \underline{E}$ , so

$$\delta(g\sigma\underline{E}, \underline{E}) = \delta(\sigma\underline{E}, g^{-1}\underline{E}) = \delta(\sigma\underline{E}, \underline{E}) = \sigma,$$

so the flag  $\phi(g) = g\sigma\underline{E}$  lies in  $Y(\sigma)$  as claimed.

Next, observe that the stabiliser of  $\sigma\underline{E}$  in  $G$  is  $B^{\sigma^{-1}}$ , so the stabiliser in  $X(\sigma) = U \cap U^{\rho\sigma^{-1}}$  is contained in the group

$$H = B^{\sigma^{-1}} \cap U^{\rho\sigma^{-1}} = (B \cap U^\rho)^{\sigma^{-1}}.$$

Now  $B$  consists of upper triangular matrices, and  $U^\rho$  consists of lower unitriangular matrices, so  $B \cap U^\rho = 1$ , so  $H = 1$ . It follows that  $X(\sigma)$  acts freely on  $\sigma\underline{E}$ , so  $\phi: X(\sigma) \rightarrow Y(\sigma)$  is injective.

Now put

$$T_i = \mathbb{F}_p\{e_m \mid m \leq \sigma(i), \sigma^{-1}(m) \geq i\} \leq E_{\sigma(i)}.$$

Let  $\epsilon_i: \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be the  $i$ 'th coordinate projection.

Consider a flag  $\underline{V} \in Y(\sigma)$ . We claim that there is a unique element  $v_i \in V_i \cap T_i$  such that  $\epsilon_{\sigma(i)}(v_i) = 1$ , and moreover that  $v_1, \dots, v_i$  is a basis for  $V_i$  over  $\mathbb{F}_p$ . We will prove this by induction on  $i$ , so we assume that the corresponding fact holds for all  $j < i$ . Put

$$S_i = \mathbb{F}_p\{v_j \mid j < i \text{ and } \sigma(j) < \sigma(i)\} \leq V_i \cap E_{\sigma(i)}$$

The leading terms of the vectors  $v_j$  in  $S_i$  are precisely the vectors  $e_m$  with  $m < \sigma(i)$  but  $i > \sigma^{-1}(m)$ . Using this, we see that  $E_{\sigma(i)} = S_i \oplus T_i$ , and thus that  $V_i \cap E_{\sigma(i)} = S_i \oplus L_i$  for some (unique) subspace  $L_i \leq T_i$ . We next claim that  $S_i = V_{i-1} \cap E_{\sigma(i)}$ . This is straightforward, given that  $\{v_1, \dots, v_{i-1}\}$  is a basis for  $V_{i-1}$  and the leading term in  $v_j$  is  $e_{\sigma(j)}$ . It follows that the space

$$L_i \simeq (V_i \cap E_{\sigma(i)}) / (V_{i-1} \cap E_{\sigma(i)})$$

has dimension at most one. On the other hand, because  $\delta(\underline{V}, \underline{E}) = \sigma$  we see that  $\epsilon_{\sigma(i)}: L_i \rightarrow \mathbb{F}_p$  must be surjective, so there is a unique element  $v_i$  as described.

Now define  $g: \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$  by  $g(e_i) = v_{\sigma^{-1}(i)}$ , so  $g\sigma(e_i) = v_i$ , so  $g\sigma(\underline{E}) = \underline{V}$ . As the leading term of  $v_{\sigma^{-1}(i)}$  is  $e_i$ , we have  $g \in U$ . We also have

$$g\sigma(e_k) = v_k \in T_k \leq \mathbb{F}_p\{e_m \mid \sigma^{-1}(m) \geq k\} = \mathbb{F}_p\{e_{\sigma(k)}, e_{\sigma(k+1)}, \dots, e_{\sigma(m)}\},$$

so  $\sigma^{-1}g\sigma$  is a lower-triangular matrix, so  $\rho\sigma^{-1}g\sigma\rho$  is upper-triangular, so  $g \in B^{\rho\sigma^{-1}}$ . We also know that the diagonal entries in  $g$  are all equal to 1, so the same is true of the diagonal entries in  $\rho\sigma^{-1}g\sigma\rho$ , so  $g \in U^{\rho\sigma^{-1}}$ . This means that  $g \in X(\sigma)$ , and  $\phi(g) = \underline{V}$ . We conclude that  $\phi$  is surjective as well as injective.  $\square$

**Example 5.3.** Consider the permutation  $\sigma = (1\ 5\ 3)(2\ 4) \in \Sigma_5$ , corresponding to the matrix

$$\sigma = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Then

$$L(\sigma^{-1}) = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\},$$

so  $X(\sigma)$  is the set of matrices of the form

$$g = \begin{bmatrix} 1 & 0 & 0 & b & a \\ 0 & 1 & 0 & d & c \\ 0 & 0 & 1 & f & e \\ 0 & 0 & 0 & 1 & g \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

For such  $g$ , we have

$$g\sigma = \begin{bmatrix} a & e & 1 & 0 & 0 \\ b & f & 0 & 1 & 0 \\ c & g & 0 & 0 & 1 \\ d & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The columns of this are the vectors  $u_i$  as in Example 4.2, so  $\phi(g)$  is the flag  $\underline{U}$  considered in Example 4.2.

**Corollary 5.4.** *Consider triples  $(V, \underline{U}, \underline{W})$  where  $V$  is an  $n$ -dimensional vector space over  $\mathbb{F}_p$  and  $\underline{U}$  and  $\underline{W}$  are complete flags in  $V$ . Then such triples are classified up to isomorphism by the invariant  $\delta(\underline{U}, \underline{W}) \in \Sigma$ . In particular, if  $\underline{U}, \underline{W}, \underline{W}' \in \text{Flag}(V)$  then there is an automorphism  $g \in \text{Aut}(V)$  with  $g\underline{U} = \underline{U}$  and  $g\underline{W} = \underline{W}'$  if and only iff  $\delta(\underline{U}, \underline{W}) = \delta(\underline{U}, \underline{W}')$ .*

*Proof.* Let  $(V, \underline{U}, \underline{W})$  be a pair as above, and put  $\sigma = \delta(\underline{U}, \underline{W})$ . It will suffice to show that  $(V, \underline{U}, \underline{W}) \simeq (\mathbb{F}_p^n, \sigma\underline{E}, \underline{E})$ . Choose elements  $w_i \in W_i \setminus W_{i-1}$  and define  $f: \mathbb{F}_p^n \rightarrow V$  by  $f(a) = \sum_i a_i w_i$ . This gives an isomorphism  $\mathbb{F}_p^n \rightarrow V$  sending  $\underline{E}$  to  $\underline{W}$ . This must send some other flag  $\underline{F}$  to  $\underline{U}$ . By naturality we have  $\delta(\underline{F}, \underline{E}) = \delta(\underline{U}, \underline{W}) = \sigma$ , so  $\underline{F} \in Y(\sigma)$ , so  $\underline{F} = x\sigma\underline{E}$  for some  $x \in X(\sigma) \leq B$ . The map  $x^{-1}$  now gives an isomorphism  $(\mathbb{F}_p^n, \underline{F}, \underline{E}) \rightarrow (\mathbb{F}_p^n, \sigma\underline{E}, \underline{E})$ .  $\square$

**Corollary 5.5.** *For a triple  $(V, \underline{U}, \underline{W})$  as above, we have  $\delta(\underline{U}, \underline{W}) = \sigma$  iff there exists a basis  $v_1, \dots, v_n$  such that for all  $i$  we have*

$$\begin{aligned} U_i &= \text{span}\{v_{\sigma(1)}, \dots, v_{\sigma(i)}\} \\ W_i &= \text{span}\{v_1, \dots, v_i\}. \end{aligned}$$

If so, then the number of such bases is  $(p-1)^n p^{l(\sigma^{-1}\rho)}$ .

*Proof.* A basis is the same thing as an isomorphism  $\mathbb{F}_p^n \rightarrow V$ ; a basis with properties as above is the same as an isomorphism  $(\mathbb{F}_p^n, \sigma\underline{E}, \underline{E}) \rightarrow (V, \underline{U}, \underline{W})$ . Thus, such bases exist iff  $\delta(\underline{U}, \underline{W}) = \sigma$ , and if so, the number of such bases is  $|\text{Aut}(\mathbb{F}_p^n, \sigma\underline{E}, \underline{E})|$ . This automorphism group is just  $B \cap B^{\sigma^{-1}}$ , which is conjugate to  $B^\sigma \cap B$ . This fits into a short exact sequence

$$X(\sigma^{-1}\rho) = U^\sigma \cap U \rightarrow B^\sigma \cap B \rightarrow T,$$

so  $|B^\sigma \cap B| = |T||X(\sigma^{-1}\rho)| = (p-1)^n p^{l(\sigma^{-1}\rho)}$  as claimed.  $\square$

## 6. THE BRUHAT DECOMPOSITION

**Proposition 6.1.** *We have  $G = \coprod_{\sigma \in \Sigma_n} B\sigma B$ . Moreover, for each  $\sigma \in \Sigma_n$  we have a bijection*

$$X(\sigma) \times B = (U \cap U^{\rho\sigma^{-1}}) \times B \rightarrow B\sigma B$$

given by  $(g, b) \mapsto g\sigma b$ . We thus have

$$|B\sigma B| = p^{l(\sigma)}|B| = p^{l(\sigma) + n(n-1)/2} (p-1)^n.$$

*Proof.* Given  $g \in G$ , put  $\pi(g) = \delta(g\underline{E}, \underline{E}) \in \Sigma_n$ . If  $b, b' \in B$  then  $b\underline{E} = \underline{E} = b'\underline{E}$ , so

$$\pi(b^{-1}gb') = \delta(b^{-1}gb'\underline{E}, \underline{E}) = \delta(gb'\underline{E}, b\underline{E}) = \delta(g\underline{E}, \underline{E}) = \pi(g).$$

Moreover, if  $\sigma \in \Sigma_n \leq G$  then  $\sigma E_i = \mathbb{F}_p\{e_{\sigma(j)} \mid j \leq i\}$ , from which it follows directly that  $\pi(\sigma) = \sigma$ . This means that  $\pi(B\sigma B) = \{\sigma\}$ .

Conversely, suppose that  $\pi(h) = \sigma$ . Proposition 5.2 tells us that there is a unique element  $g \in X(\sigma)$  such that  $g\sigma\underline{E} = h\underline{E}$ . If we put  $b = (g\sigma)^{-1}h$  we find that  $b \in B$  and  $h = g\sigma b$ . In particular, this shows that  $h \in B\sigma B$ , so  $\pi^{-1}\{\sigma\} = B\sigma B$ , so  $G = \coprod_{\sigma \in \Sigma_n} B\sigma B$ . We also see that our map  $X(\sigma) \times B \rightarrow B\sigma B$  is surjective. To see that it is also injective, suppose we have  $h = g'\sigma b'$  for some other  $g' \in X(\sigma)$  and  $b' \in B$ . As  $b\underline{E} = \underline{E} = b'\underline{E}$  we see that  $g\sigma\underline{E} = g'\sigma\underline{E}$ . Proposition 5.2 now tells us that  $g = g'$ , and as  $g\sigma b = g'\sigma b'$  we also have  $b = b'$ .  $\square$

**Corollary 6.2.**  $|B \cap B^{\rho\sigma^{-1}}| = |B\sigma B|/|U|$ .

*Proof.* We have  $B = T \times U$  and  $T^\tau = T$  for all  $\tau \in \Sigma_n$ , so

$$|B \cap B^{\rho\sigma^{-1}}| = |T| \cdot |U \cap U^{\rho\sigma^{-1}}| = |T| \cdot p^{l(\sigma)}.$$

On the other hand,

$$|B\sigma B| = p^{l(\sigma)}|B| = |U||T|p^{l(\sigma)},$$

and the claim follows easily.  $\square$

**Corollary 6.3.** For each  $\sigma \in \Sigma_n$  we have a bijection

$$B \times X(\sigma^{-1}) = B \times (U \cap U^{\rho\sigma}) \rightarrow B\sigma B$$

given by  $(b, g) \mapsto b\sigma g$ .

*Proof.* We have a bijection  $\phi: X(\sigma^{-1}) \times B \rightarrow B\sigma^{-1}B$  given by  $\phi(g, b) = g\sigma b$ . Define  $\chi: G \rightarrow G$  by  $\chi(g) = g^{-1}$ . As  $B$  and  $X(\sigma^{-1})$  are groups, they are preserved by  $\chi$ . We also have  $\chi(B\sigma^{-1}B) = B\sigma B$ . We therefore have a bijection  $B \times X(\sigma^{-1}) \rightarrow B\sigma B$  given by

$$(b, g) \mapsto \chi(\phi(\chi(g), \chi(b))) = (g^{-1}\sigma^{-1}b^{-1})^{-1} = b\sigma g.$$

$\square$

**Proposition 6.4.** If  $l(\sigma\tau) = l(\sigma) + l(\tau)$  then there is a bijection  $\phi: X(\sigma) \times X(\tau) \rightarrow X(\sigma\tau)$  given by  $\phi(g, h) = g h^{\sigma^{-1}} = g\sigma h\sigma^{-1}$ .

*Proof.* Recall first that the condition  $l(\sigma\tau) = l(\sigma) + l(\tau)$  is equivalent to the following: for any  $T \subseteq \{1, \dots, n\}$  with  $|T| = 2$ , at most one of the two maps

$$T \xrightarrow{\tau} \tau(T) \xrightarrow{\sigma} \sigma\tau(T)$$

is order-reversing.

We now show that  $\phi(g, h) \in X(\sigma\tau)$ , or equivalently that  $g h^{\sigma^{-1}} \in U \cap U^{\rho\tau^{-1}\sigma^{-1}}$ . We are given that  $g \in U$  and  $h \in U^{\rho\tau^{-1}}$ , so it will suffice to show that  $h^{\sigma^{-1}} \in U$  and  $g \in U^{\rho\tau^{-1}\sigma^{-1}}$ . For the first of these, recall that the  $(i, j)$ 'th matrix element in  $h^{\sigma^{-1}}$  is  $h_{\sigma^{-1}(i), \sigma^{-1}(j)}$ . Thus, if  $h^{\sigma^{-1}} \notin U$ , we have some  $i > j$  with  $h_{\sigma^{-1}(i), \sigma^{-1}(j)} \neq 0$ . As  $h \in X(\tau)$  we must have  $\sigma^{-1}(i) < \sigma^{-1}(j)$  and  $\tau^{-1}\sigma^{-1}(i) > \tau^{-1}\sigma^{-1}(j)$ . This means that both the maps

$$\{\tau^{-1}\sigma^{-1}(i), \tau^{-1}\sigma^{-1}(j)\} \xrightarrow{\tau} \{\sigma^{-1}(i), \sigma^{-1}(j)\} \xrightarrow{\sigma} \{i, j\}$$

are order-reversing, contrary to our hypothesis; so  $h^{\sigma^{-1}} \in U$  after all. For the second claim, suppose that  $g \notin U^{\rho\tau^{-1}\sigma^{-1}}$ , so  $g^{\sigma\tau} \notin U^\rho$ . Then there must exist  $i < j$  with  $g_{\sigma\tau(i), \sigma\tau(j)} \neq 0$ . As  $g \in X(\sigma)$ , this means that  $\sigma\tau(i) < \sigma\tau(j)$  and  $\sigma^{-1}\sigma\tau(i) > \sigma^{-1}\sigma\tau(j)$ , or equivalently  $\tau(i) > \tau(j)$ . This means that both the maps

$$\{i, j\} \xrightarrow{\tau} \{\tau(i), \tau(j)\} \xrightarrow{\sigma} \{\sigma\tau(i), \sigma\tau(j)\}$$

are order-reversing, which again gives a contradiction. This completes the proof that  $\phi(g, h) \in X(\sigma\tau)$ .

We now show that  $\phi$  is surjective. Consider an arbitrary element  $k \in X(\sigma\tau)$ . Then  $k \in B$ , so  $k\sigma \in B\sigma B$ . Corollary 6.1 tells us that there is a unique pair  $(g, b) \in X(\sigma) \times B$  with  $g\sigma b = k\sigma$ . Similarly, we have  $b\tau \in B\tau B$ , so there is a unique  $(h, c) \in X(\tau) \times B$  with  $b\tau = h\tau c$ . It follows that

$$k\sigma\tau = g\sigma b\tau = g\sigma h\tau c = \phi(g, h)\sigma\tau c$$

We can now apply Corollary 6.1 to the permutation  $\sigma\tau$  to deduce that  $k = \phi(g, h)$  and  $c = 1$ . This shows that  $\phi$  is surjective, but

$$|X(\sigma\tau)| = p^{l(\sigma\tau)} = p^{l(\sigma)+l(\tau)} = |X(\sigma) \times X(\tau)|,$$

so  $\phi$  is actually a bijection.  $\square$

**Proposition 6.5.** If  $l(\sigma\tau) = l(\sigma) + l(\tau)$  then  $B\sigma B\tau B = B\sigma\tau B$ .

*Proof.* It is clear that  $B\sigma\tau B \subseteq B\sigma B\tau B$ , so it will suffice to show that

$$|B\sigma B\tau B| \leq |B\sigma\tau B| = |B|p^{l(\sigma\tau)} = |B|p^{l(\sigma)}p^{l(\tau)}.$$

For this we note that  $B\sigma B = X(\sigma)\sigma B$  and  $B\tau B = B\tau X(\tau^{-1})$  so

$$B\sigma B\tau B = X(\sigma)\sigma B\tau X(\tau^{-1}).$$

As  $|X(\sigma)| = p^{l(\sigma)}$  and  $|X(\tau^{-1})| = p^{l(\tau^{-1})} = p^{l(\tau)}$ , this gives the required inequality.  $\square$

## 7. PARABOLIC SUBGROUPS

**Definition 7.1.** For any set  $I \subseteq \{1, \dots, n-1\}$ , we put  $\Sigma_I = \langle s_i \mid i \in I \rangle \leq \Sigma_n$ . Suppose that  $\{0, \dots, n\} \setminus I = \{i_0, i_1, \dots, i_r\}$  with  $0 = i_0 < i_1 < \dots < i_r = n$ . Then  $\Sigma_I$  preserves the sets,

$$(0, i_1], (i_1, i_2], \dots, (i_{r-1}, i_r].$$

In fact, it is the largest subgroup of  $\Sigma_n$  that preserves these sets, so

$$\Sigma_I \simeq \Sigma_{i_1} \times \Sigma_{i_2 - i_1} \times \dots \times \Sigma_{i_r - i_{r-1}}.$$

**Definition 7.2.** Next, for any  $n$ -dimensional vector space  $V$  over  $\mathbb{F}_p$  we let  $\text{Flag}_I(V)$  be the set of flags

$$\underline{W} = (0 = W_{i_0} < W_{i_1} < W_{i_2} < \dots < W_{i_r} = V)$$

with  $\dim(W_j) = j$  for all  $j \in I^c$ . This gives a functor from  $n$ -dimensional vector spaces to sets.

In the case  $V = \mathbb{F}_p^n$  we have an obvious flag  $\underline{E} \in \text{Flag}_I(\mathbb{F}_p^n)$  given by  $E_j = \text{span}\{e_1, \dots, e_j\}$  for all  $j \in I^c$ . We let  $P_I$  denote the stabiliser of this flag. We also write  $P_i$  for  $P_{\{i\}}$  and  $P_{ij}$  for  $P_{\{i, j\}}$ , and so on. The subgroups  $P_I$  are called *standard parabolic subgroups* of  $G$ . More generally a subgroup  $P \leq G$  is *parabolic* if it contains a conjugate of  $B$ .

For example, we have  $P_\emptyset = B$  and  $P_{\{1, \dots, n-1\}} = G$ . In the case  $n = 7$  and  $I = \{1, 3, 4, 6\}$ , the group  $P_I$  consists of invertible matrices of the following shape:

$$\begin{bmatrix} * & * & * & * & * & * & * \\ * & * & * & * & * & * & * \\ \hline 0 & 0 & * & * & * & * & * \\ 0 & 0 & * & * & * & * & * \\ 0 & 0 & * & * & * & * & * \\ \hline 0 & 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & * & * \end{bmatrix}$$

Here  $I^c = \{0, 2, 5, 7\}$ , and the sizes of the diagonal blocks are  $2 - 0$ ,  $5 - 2$  and  $7 - 5$ .

**Proposition 7.3.**  $P_I = B\Sigma_I B$ .

*Proof.* Firstly, it is clear from the definitions that  $\Sigma_I \leq P_I$  and  $B \leq P_I$  so  $B\Sigma_I B \subseteq P_I$ . Conversely, suppose that  $g \in P_I$  and put  $U_j = gE_j$ , so for  $a \in I^c$  we have  $U_a = E_a$ . Let  $\sigma$  be the permutation such that  $g \in B\sigma B$ . Recall from Section 6 that this is characterised by characterised by  $Q_{i, \sigma(i)} \neq 0$ , where

$$Q_{ij} = (U_i \cap E_j) / ((U_{i-1} \cap E_j) + (U_i \cap E_{j-1})).$$

Suppose we have  $a < i \leq b$ , with  $a, b \in I^c$ . We claim that  $a < \sigma(i) \leq b$ , or in other words that  $Q_{ij} = 0$  for  $j \leq a$  or  $j > b$ . Indeed, if  $j \leq a$  then  $E_j \leq E_a = U_a \leq U_{i-1}$ , so  $(U_i \cap E_j) \leq (U_{i-1} \cap E_j)$ , so  $Q_{ij} = 0$ . Similarly, if  $j > b$  then  $E_{j-1} \geq E_b = U_b \geq U_i$ , so  $(U_i \cap E_j) \leq (U_i \cap E_{j-1})$ , so  $Q_{ij} = 0$ . This shows that  $\sigma$  preserves the interval  $(a, b]$  as claimed, for all  $a, b \in I^c$ . It follows that  $\sigma \in \Sigma_I$ .  $\square$

**Lemma 7.4.** If  $\sigma(k) > \sigma(k+1)$  then  $\sigma \in B\sigma B s_k B$ .

*Proof.* Define  $g \in G$  by  $g(e_k) = e_k + e_{k+1}$  and  $g(e_i) = e_i$  for  $i \neq k$ . We claim that  $g \in B s_k B$ . In the case  $n = 2$  and  $k = 1$  this follows from the equation

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The general case follows by taking block sums with suitable identity matrices. Next, we claim that the element  $g = \sigma g \sigma^{-1}$  lies in  $B$ . Indeed, we have  $b(e_{\sigma(k)}) = e_{\sigma(k+1)}$  and  $b(e_i) = e_i$  for all other  $i$ , so the claim follows from the fact that  $\sigma(k+1) < \sigma(k)$ . We now have  $\sigma = b^{-1} \sigma g$  and  $g \in B s_k B$  so  $\sigma \in B\sigma B s_k B$  as claimed.  $\square$

**Proposition 7.5.** *Let  $P$  be a subgroup of  $G$  such that  $P \geq B$ . Then  $P = P_I$  for some  $I$  (so  $P$  is a standard parabolic subgroup).*

*Proof.* Put  $I = \{i \mid s_i \in P\}$ , so  $P_I \leq P$ . Suppose that  $g \in P$ , and put  $\sigma = \pi(g)$ . As  $BgB = B\sigma B$  and  $B \leq P_I \leq P$  we have  $\sigma \in P$ , and  $g \in P_I$  iff  $\sigma \in P_I$ . If  $l(\sigma) = 0$  then  $\sigma = 1 \in P$ . If  $l(\sigma) = 1$  then  $\sigma = s_i$  for some  $i$  and  $\sigma \in P$  so  $i \in I$  so  $\sigma \in P_I$ . Now suppose that  $l(\sigma) > 1$ , so we have  $\sigma(k) > \sigma(k+1)$  for some  $k$ . Lemma 7.4 tells us that  $\sigma = b\sigma c s_k d$  for some  $b, c, d \in B$ . As  $\sigma, b, c, d \in P$  we conclude that  $s_k \in P$ , so  $k \in I$ , so  $s_k \in P_I$ . It also follows that the element  $\tau = \sigma s_k$  lies in  $P$ . As  $\sigma(k+1) < \sigma(k)$  we have  $l(\tau) = l(\sigma) - 1$ , so we can assume by induction that  $\tau \in P_I$ . It follows that  $\sigma = \tau s_k \in P_I$  and thus that  $g \in P_I$ .  $\square$

**Corollary 7.6.** *Every parabolic subgroup is conjugate to a standard parabolic subgroup.*

**Proposition 7.7.** *If  $I \subseteq J$  then  $\text{Map}_G(\text{Flag}_I(V), \text{Flag}_J(V))$  is a singleton; otherwise, it is empty.*

*Proof.* We first observe that the orbits of  $B$  in  $V$  are precisely the sets  $E_k \setminus E_{k-1}$ , and thus that the spaces  $E_k$  are the only  $B$ -invariant subspace of  $V$ . This means that the point  $\underline{E}_I \in \text{Flag}_I(V)$  (which we call the *basepoint*) is the unique  $B$ -fixed point in  $\text{Flag}_I(V)$ . Thus, any map from  $\text{Flag}_I(V)$  to  $\text{Flag}_J(V)$  must send the basepoint to the basepoint, and this determines it uniquely because  $G$  acts transitively on  $\text{Flag}_I(V)$ . As the stabilisers of the basepoints are  $P_I$  and  $P_J$ , there is a unique map when  $P_I \leq P_J$ , and no maps otherwise. It is also clear that  $P_I \leq P_J$  iff  $I \subseteq J$ .  $\square$

**Definition 7.8.** We say that a finite  $G$ -set  $X$  is *parabolic* if every point has parabolic isotropy group. We write  $\mathcal{P}$  for the category of parabolic finite  $G$ -sets and equivariant maps. We also write  $\mathcal{P}'$  for the category of finite sets  $Y$  equipped with a list  $(Y_1, \dots, Y_{n-1})$  of subsets. We define a functor  $F: \mathcal{P} \rightarrow \mathcal{P}'$  by  $FX = X^B$ , equipped with the subsets  $F_i X = X^{P_i}$  for  $i = 1, \dots, n-1$ .

$$FX = (X^B; X^{P_1}, \dots, X^{P_{n-1}}).$$

**Proposition 7.9.**  *$F: \mathcal{P} \rightarrow \mathcal{P}'$  is an equivalence of categories.*

*Proof.* Consider an object  $Y \in \mathcal{P}'$ . For  $y \in Y$  we put  $I_y = \{i \mid y \in Y_i\}$ . We then put  $F'Y = \coprod_{y \in Y} G/P_{I_y} \in \mathcal{P}$ . Now consider a morphism  $f: Y \rightarrow Z$  in  $\mathcal{P}'$ . As  $f(Y_i) \subseteq Z_i$  we have  $I_y \subseteq I_{f(y)}$ , so there is a unique  $G$ -map  $G/P_{I_y} \rightarrow G/P_{I_{f(y)}} \subseteq F'Z$ . Putting these together, we get a map  $F'f: F'Y \rightarrow F'Z$ , and this gives us a functor  $\mathcal{P}' \rightarrow \mathcal{P}$ . Note that

$$(G/P_I)^{P_i} = \text{Map}_G(\text{Flag}_i(V), \text{Flag}_I(V)) = \begin{cases} 1 & \text{if } i \in I \\ \emptyset & \text{otherwise.} \end{cases}$$

Using this we see that  $FF' = 1_{\mathcal{P}'}$ . Next, consider an object  $X \in \mathcal{P}$ . This can be written as a disjoint union of orbits, each of which is isomorphic to  $G/P$  for some parabolic  $P$ . We then note that  $P$  is conjugate to  $P_I$  for some  $I$ , so  $G/P$  is isomorphic to  $G/P_I$ . The only  $B$ -fixed point in  $G/P_I$  is the basepoint, and the basepoint is fixed by  $P_i$  iff  $i \in I$ . It now follows that  $X = F'FX$ , and thus that  $F$  is an equivalence as claimed.  $\square$

## 8. THE HECKE ALGEBRA

Let  $\mathcal{V}$  be the category of  $n$ -dimensional vector spaces over  $\mathbb{F}_p$ , with linear isomorphisms as the morphisms. Let  $\mathcal{F}$  be the category of finite sets, and let  $\mathcal{A}$  be the category of finitely generated free  $\mathbb{Z}_{(p)}$ -modules. We write  $\mathcal{V}\mathcal{F}$  and  $\mathcal{V}\mathcal{A}$  for the functor categories  $[\mathcal{V}, \mathcal{F}]$  and  $[\mathcal{V}, \mathcal{A}]$ .

We will be interested in various functors  $X \in \mathcal{V}\mathcal{F}$  such as

$$\begin{aligned} \text{Flag}(V) &= \{ \text{complete flags in } V \} \\ \text{Base}(V) &= \{ \text{bases for } V \}. \end{aligned}$$

Given  $X \in \mathcal{V}\mathcal{F}$  we define  $\mathbb{Z}_{(p)}[X] \in \mathcal{V}\mathcal{A}$  by  $\mathbb{Z}_{(p)}[X](V) = \mathbb{Z}_{(p)}[X(V)]$ , the free  $\mathbb{Z}_{(p)}$ -module generated by the finite set  $X(V)$ .

**Definition 8.1.** The *Hecke algebra* is the ring  $\mathcal{H} = \text{End}(\mathbb{Z}[\text{Flag}])$ .

This formulation is convenient for conceptual purposes, but for calculations a more explicit version is useful. If  $X$  is a functor from  $\mathcal{V}$  to sets then  $X(\mathbb{F}_p^n)$  is a  $G$ -set (where  $G = GL_n(\mathbb{F}_p)$ ), and this construction gives an equivalence  $[\mathcal{V}, \{\text{sets}\}] = \{G\text{-sets}\}$ . This identifies  $\mathbb{Z}_{(p)}[\text{Flag}]$  with the  $\mathbb{Z}_{(p)}[G]$ -module  $\mathbb{Z}_{(p)}[G/B]$ , and so identifies  $\mathcal{H}$  with  $\text{End}_{\mathbb{Z}_{(p)}[G]}(\mathbb{Z}_{(p)}[G/B])$ . We will analyse this in more detail later.

First, however, we discuss some general constructions giving maps between functors. Note that  $\mathbb{Z}_{(p)}[X]$  has an obvious inner product, given by  $\langle [x], [x'] \rangle = \delta_{xx'}$ . Given  $f: \mathbb{Z}_{(p)}[X] \rightarrow \mathbb{Z}_{(p)}[Y]$  we let  $f^t: \mathbb{Z}_{(p)}[Y] \rightarrow \mathbb{Z}_{(p)}[X]$  be the adjoint with respect to this inner product. In particular, if  $f$  comes from a map  $f: X \rightarrow Y$  then  $f^t[y] = \sum_{f(x)=y} [x]$ .

**Definition 8.2.** Define  $Z(\sigma) \in \mathcal{VF}$  by

$$Z(\sigma)(V) = \{(U, W) \in \text{Flag}(V)^2 \mid \delta(U, W) = \sigma\}$$

(where  $\delta(\underline{U}, \underline{V})$  is the Jordan permutation, as in Section 4). This has projection maps

$$\text{Flag} \xleftarrow{\pi_0} Z(\sigma) \xrightarrow{\pi_1} \text{Flag}$$

and we put  $T_\sigma = \pi_1 \pi_0^t: \mathbb{Z}_{(p)}[\text{Flag}] \rightarrow \mathbb{Z}_{(p)}[\text{Flag}]$ , so  $T_\sigma \in \mathcal{H}$  and

$$T_\sigma[\underline{U}] = \sum_{\delta(\underline{U}, \underline{W})=\sigma} [\underline{W}].$$

It is clear from this that  $T_\sigma^t = T_{\sigma^{-1}}$ . We will write  $T_i$  for  $T_{s_i}$ .

**Proposition 8.3.** *The maps  $T_\sigma$  give a basis for  $\mathcal{H}$  over  $\mathbb{Z}_{(p)}$ .*

*Proof.* Consider an element  $f: \mathbb{Z}_{(p)}[\text{Flag}] \rightarrow \mathbb{Z}_{(p)}[\text{Flag}]$ . For any  $V \in \mathcal{V}$  and any  $\underline{U}, \underline{W} \in \text{Flag}(V)$  we let  $n(V, \underline{U}, \underline{W})$  be the coefficient of  $[\underline{W}]$  in  $f([\underline{U}])$ . As  $f$  is natural, this coefficient depends only on the isomorphism class of the triple  $(V, \underline{U}, \underline{W})$ . Thus, by Corollary 5.4, there are well-defined numbers  $n_\sigma$  for  $\sigma \in \Sigma$  such that  $n(V, \underline{U}, \underline{W}) = n_{\delta(\underline{U}, \underline{W})}$ . It follows that  $f = \sum_\sigma n_\sigma T_\sigma$ .  $\square$

**Proposition 8.4.** *Fix  $i \in \{1, \dots, n-1\}$ . Let  $\underline{U}$  be a flag, let  $F$  be the set of flags  $\underline{W}$  such that  $W_j = U_j$  for all  $j \neq i$ , and put  $a = \sum_{\underline{W} \in F} [\underline{W}]$ . Then  $T_i[\underline{U}] = a - [\underline{U}]$  and*

$$(T_i - p)(T_i + 1)[\underline{U}] = (T_i^2 - (p-1)T_i - p)[\underline{U}] = 0.$$

*Proof.* The formula  $T_i[\underline{U}] = a - [\underline{U}]$  is immediate from Proposition 4.7. Note also that the definition of  $a$  depends only on the spaces  $U_j$  for  $j \neq i$ , so for  $\underline{W} \in F$  we have  $T_i[\underline{W}] = a - [\underline{W}]$ . It follows that

$$T_i(a) = \sum_{\underline{W} \in F} T_i[\underline{W}] = \sum_{\underline{W} \in F} (a - [\underline{W}]) = |F|a - \sum_{\underline{W} \in F} [\underline{W}] = (|F| - 1)a.$$

Moreover,  $F$  bijects with the set of one-dimensional subspaces of  $U_{i+1}/U_{i-1} \simeq \mathbb{F}_p^2$ , so  $|F| = p + 1$ , so  $T_i(a) = pa$ . It follows that  $(T_i - p)(T_i + 1)[\underline{W}] = (T_i - p)(a) = 0$  as claimed.  $\square$

**Definition 8.5.** We define  $\hat{e}: \mathbb{Z}_{(p)}[\text{Flag}(V)] \rightarrow \mathbb{Z}_{(p)}[\text{Flag}(V)]$  by

$$\hat{e}[\underline{U}] = |\text{Flag}(V)|^{-1} \sum_{\underline{W} \in \text{Flag}(V)} [\underline{W}]$$

(so  $\hat{e}[\underline{U}]$  is independent of  $\underline{U}$ ). This is natural, and so defines an element of  $\mathcal{H}$ . We also define a map  $\hat{\xi}: \mathcal{H} \rightarrow \mathbb{Z}_{(p)}$  by  $\hat{\xi}(\sum_\sigma n_\sigma T_\sigma) = \sum_\sigma p^{l(\sigma)}$ .

**Proposition 8.6.**  *$\hat{e}$  is a central idempotent in  $\mathcal{H}$ , with  $\hat{e}^t = \hat{e}$ . Moreover,  $\hat{\xi}$  is a ring map, with  $\hat{\xi}(a^t) = \hat{\xi}(a)$  and  $a\hat{e} = \hat{e}a = \hat{\xi}(a)\hat{e}$  for all  $a \in \mathcal{H}$ .*

*Proof.* Consider an object  $V \in \mathcal{V}$ , and put  $x = |\text{Flag}(V)|^{-1} \sum_{\underline{W} \in \text{Flag}(V)} [\underline{W}]$ , so  $\hat{e}[\underline{U}] = x$  for all  $\underline{W}$ . It is easy to see that  $\hat{e}(x) = x$  also, and thus that  $\hat{e}^2 = \hat{e}$ . We have  $\langle \hat{e}[\underline{U}], [\underline{W}] \rangle = |\text{Flag}(V)|^{-1} = \langle [\underline{U}], \hat{e}[\underline{W}] \rangle$  for all  $\underline{U}$  and  $\underline{W}$ , so  $\hat{e}$  is self-adjoint, so  $\hat{e}^t = \hat{e}$ .

Next, we have

$$\hat{e}T_\sigma[\underline{U}] = \sum_{\delta(\underline{U}, \underline{W})=\sigma} \hat{e}[\underline{W}] = |\{\underline{W} \mid \delta(\underline{W}, \underline{U}) = \sigma^{-1}\}|x = p^{l(\sigma^{-1})}x = p^{l(\sigma)}\hat{e}[\underline{W}].$$

(using Proposition 5.2 and the fact that  $l(\sigma^{-1}) = l(\sigma)$ ). It follows that  $\hat{e}T_\sigma = p^{l(\sigma)}\hat{e}$ , and thus that  $\hat{e}a = \widehat{\xi}(a)\hat{e}$  for all  $a \in \mathcal{H}$ . By expanding  $\hat{e}ab$  in two ways we deduce that  $\widehat{\xi}$  is a ring map.

Now take the transpose of  $\hat{e}a = \widehat{\xi}(a)\hat{e}$  to get  $a^t\hat{e} = \widehat{\xi}(a)\hat{e}$ . Replacing  $a$  by  $a^t$  gives  $a\hat{e} = \xi(a^t)\hat{e}$ . We also have  $T_\sigma^t = T_{\sigma^{-1}}$  and  $l(\sigma^{-1}) = l(\sigma)$  so  $\widehat{\xi}(a^t) = \widehat{\xi}(a)$ . Our equation now reads  $a\hat{e} = \widehat{\xi}(a)\hat{e}$ , so  $a\hat{e} = \hat{e}a$ , so  $\hat{e}$  is central.  $\square$

**Lemma 8.7.** *Under the identification  $\mathcal{H} = \text{End}_{\mathbb{Z}_{(p)}[G]}(\mathbb{Z}_{(p)}[G/B])$ , we have*

$$T_{\sigma^{-1}}[gB] = T_\sigma^t[gB] = \sum_{x \in X(\sigma)} [gx\sigma B].$$

*Proof.* As  $T_{\sigma^{-1}}$  is a  $G$ -map it will suffice to prove this for  $g = 1$ . Using the identification  $G/B = \text{Flag}(\mathbb{F}_p^n)$  (given by  $hB \mapsto h\underline{E}$ ) it will suffice to check that  $T_{\sigma^{-1}}[\underline{E}] = \sum_{x \in X(\sigma)} [x\sigma\underline{E}]$ . By definition we have  $T_{\sigma^{-1}}[\underline{E}] = \sum_{\delta(\underline{E}, \underline{U}) = \sigma^{-1}} [\underline{U}]$ . Note that  $\delta(\underline{E}, \underline{U}) = \sigma^{-1}$  if and only if  $\delta(\underline{U}, \underline{E}) = \sigma$ , and the Bruhat decomposition tells us that any flag  $\underline{U}$  with  $\delta(\underline{U}, \underline{E}) = \sigma$  can be expressed uniquely as  $x\sigma\underline{E}$  with  $x \in X(\sigma)$ , as required.  $\square$

To give another reformulation of this, note that  $\text{Base}(V)$  is canonically the same as  $\text{Iso}(\mathbb{F}_p^n, V)$ , so an element  $g \in G = \text{Aut}(\mathbb{F}_p^n)$  gives a map  $g^*: \text{Base} \rightarrow \text{Base}$ , with  $(gh)^* = h^*g^*$ .

**Corollary 8.8.** *The following diagram commutes:*

$$\begin{array}{ccc} \mathbb{Z}_{(p)}[\text{Base}] & \xrightarrow{\pi} & \mathbb{Z}_{(p)}[\text{Flag}] \\ \sum_{x \in X(\sigma)} (x\sigma)^* \downarrow & & \downarrow T_\sigma^t \\ \mathbb{Z}_{(p)}[\text{Base}] & \xrightarrow{\pi} & \mathbb{Z}_{(p)}[\text{Flag}]. \end{array}$$

*Proof.* The main point to note is that all the maps make sense so that the claim is meaningful. It then reduces to the lemma using the equivalence  $\mathcal{VA} = \{\mathbb{Z}_{(p)}[G] - \text{modules}\}$ .  $\square$

**Corollary 8.9.** *If  $l(\sigma\tau) = l(\sigma) + l(\tau)$  then  $T_\sigma T_\tau = T_{\sigma\tau}$ .*

*Proof.* It will suffice to prove that  $T_\tau^t T_\sigma^t [gB] = T_{\sigma\tau}^t [gB]$ . The right hand side is  $\sum_{z \in X(\sigma\tau)} [gz\sigma\tau B]$ . Proposition 6.4 converts this to

$$\sum_{x \in X(\sigma)} \sum_{y \in X(\tau)} [gx\sigma y\sigma^{-1}\sigma\tau B] = \sum_{x,y} [gx\sigma y\tau B] = \sum_x T_\tau^t [gx\sigma B] = T_\tau^t T_\sigma^t [gB],$$

as required.  $\square$

**Corollary 8.10.** *If  $s_{i_1} \dots s_{i_r}$  is a reduced word for  $\sigma$  then  $T_{i_1} \dots T_{i_r} = T_\sigma$*   $\square$

**Proposition 8.11.** *The ring  $\mathcal{H}$  is generated over  $\mathbb{Z}_{(p)}$  by the elements  $T_i$ , subject only to the relations*

$$\begin{aligned} T_i^2 &= p + (p-1)T_i \\ T_i T_{i+1} T_i &= T_{i+1} T_i T_{i+1} \\ T_i T_j &= T_j T_i \quad \text{if } |i-j| > 1. \end{aligned}$$

(The first relation can also be written as  $(T_i + 1)(T_i - p) = 0$ .)

*Proof.* For any  $\sigma \in \Sigma$  of length  $r$  we can choose a reduced word  $s_{i_1} \dots s_{i_r}$  representing  $\sigma$ , and we find from Corollary 8.10 that  $T_\sigma = T_{i_1} \dots T_{i_r}$ . This shows that the elements  $T_i$  generate  $\mathcal{H}$ . Moreover, if  $s_{j_1} \dots s_{j_r}$  is another reduced word representing  $\sigma$  then  $T_{j_1} \dots T_{j_r} = T_\sigma = T_{i_1} \dots T_{i_r}$ . The second and third relations above are instances of this. Now consider  $T_i^2$ . Fix a flag  $\underline{U} \in \text{Flag}(V)$  and put  $A = \{W \mid U_{i-1} < W < U_{i+1}\}$ , so  $|A| = p+1$ . Put

$$\phi(W) = (0 = U_0 < \dots < U_{i-1} < W < U_{i+1} < \dots < U_n = V),$$

so  $\phi(U_i) = \underline{U}$ . One checks that the flags with  $\delta(W, \underline{U}) = s_i$  are precisely those of the form  $\phi(W)$  for some  $W \in A \setminus \{U_i\}$ . It follows that  $T_i[\underline{U}] = \sum_{W \neq U_i} [\phi(W)]$  and thus that

$$\begin{aligned} T_i^2[\underline{U}] &= \sum_{W \neq U_i} T_i[\phi(W)] = \sum_{W \neq U_i} \sum_{W' \neq W} [\phi(W')] \\ &= \sum_{W'} [\phi(W')] \cdot |\{W \mid U_i \neq W \neq W'\}| = p[\underline{U}] + (p-1) \sum_{W' \neq U_i} [\phi(W')] \\ &= (p + (p-1)T_i)[\underline{U}] \end{aligned}$$

as claimed.

Now let  $\mathcal{H}'$  be generated by symbols  $T'_1, \dots, T'_{n-1}$  subject only to the relations in the statement of the proposition. As these relations are satisfied in  $\mathcal{H}$  and the  $T_i$  generate, there is a well-defined and surjective ring map  $\theta: \mathcal{H}' \rightarrow \mathcal{H}$  given by  $\theta(T'_i) = T_i$ .

Now consider an arbitrary element  $\sigma \in \Sigma$ . Choose any reduced word  $u = s_{i_1} \cdots s_{i_r}$  such that  $\pi(u) = \sigma$ , and put  $T'_\sigma = T'_{i_1} \cdots T'_{i_r} \in \mathcal{H}'$ . This is well-defined by Theorem 2.16, and we have  $\theta(T'_\sigma) = T_\sigma$  by Corollary 8.10. Define a map  $\phi: \mathcal{H} \rightarrow \mathcal{H}'$  by  $\phi(T_\sigma) = T'_\sigma$ , so  $\theta\phi = 1_{\mathcal{H}}$ , so  $\phi$  is injective.

Now put  $A = \phi(\mathcal{H}) \leq \mathcal{H}'$ . We claim that  $A$  is closed under right multiplication by  $T'_i$  for all  $i$ . To see this, consider an element  $T'_\sigma \in A$ . If  $\sigma(i) > \sigma(i+1)$  then  $l(\sigma s_i) = l(\sigma) + 1$ . We choose any reduced word  $w$  for  $\sigma$  and note that  $ws_i$  is a reduced word for  $\sigma s_i$ , so  $T'_\sigma T'_i = T'_{\sigma s_i} \in A$ . Otherwise we choose a reduced word  $w$  for the permutation  $\tau = \sigma s_i$  and note that  $ws_i$  is a reduced word for  $\sigma$ . It follows that

$$T'_\sigma T'_i = T'_\tau (T'_i)^2 = T'_\tau (p + (p-1)T'_i) = pT'_\tau + (p-1)T'_{\tau s_i} \in A.$$

As  $1 \in A$  and  $A$  is closed under multiplication by the generators of  $\mathcal{H}'$  we see that  $A = \mathcal{H}'$ , so  $\phi$  is surjective as well as injective, so  $\phi$  is an isomorphism. As  $\theta\phi = 1$  is an isomorphism it follows that  $\theta$  is also an isomorphism.  $\square$

## 9. THE STEINBERG MODULE

**Definition 9.1.** We define  $\pi: \text{Base} \rightarrow \text{Flag}$  by

$$\pi(v_1, \dots, v_n) = (0 < \text{span}\{v_1\} < \text{span}\{v_1, v_2\} < \cdots < \text{span}\{v_1, \dots, v_n\}).$$

This induces  $\pi: \mathbb{Z}_{(p)}[\text{Base}] \rightarrow \mathbb{Z}_{(p)}[\text{Flag}]$  and  $\pi^t: \mathbb{Z}_{(p)}[\text{Flag}] \rightarrow \mathbb{Z}_{(p)}[\text{Base}]$ . Next, we define

$$\omega = |G/U|^{-1} \sum_{\sigma \in \Sigma} \text{sgn}(\sigma) \sigma^*: \mathbb{Z}_{(p)}[\text{Base}] \rightarrow \mathbb{Z}_{(p)}[\text{Base}].$$

We note that  $(\sigma^*)^t = (\sigma^{-1})^*$  and so  $\omega^t = \omega$ . We put  $\mu = \pi\omega: \mathbb{Z}_{(p)}[\text{Base}] \rightarrow \mathbb{Z}_{(p)}[\text{Flag}]$ , and let  $M_{\text{St}}$  denote the image of  $\mu$ . Note that  $M_{\text{St}}(\mathbb{F}_p^n)$  is a module over  $\mathbb{Z}_{(p)}[G]$ ; we call this the *Steinberg module*. We also put

$$\begin{aligned} e &= \mu\pi^t = \pi\omega\pi^t = e^t: \mathbb{Z}_{(p)}[\text{Flag}] \rightarrow \mathbb{Z}_{(p)}[\text{Flag}] \\ e_{\text{St}} &= \pi^t\mu = \pi^t\pi\omega: \mathbb{Z}_{(p)}[\text{Base}] \rightarrow \mathbb{Z}_{(p)}[\text{Base}] \end{aligned}$$

so  $e \in \mathcal{H}$  and  $e_{\text{St}} \in \text{End}(\mathbb{Z}_{(p)}[\text{Base}]) = \mathbb{Z}_{(p)}[G]^{\text{op}}$ . We call  $e_{\text{St}}$  the *Steinberg idempotent*. (We will show later that both  $e_{\text{St}}$  and  $e$  are indeed idempotent.)

**Proposition 9.2.** *The map  $\xi: \mathcal{H} \rightarrow \mathbb{Z}_{(p)}$  given by  $\xi(T_\sigma) = \text{sgn}(\sigma)$  is a ring map, with  $\xi(a^t) = \xi(a)$  for all  $a$ . Moreover, for all  $a \in \mathcal{H}$  we have  $a\mu = \xi(a)\mu$  and  $ae = ea = \xi(a)e$  (so  $e$  is central in  $\mathcal{H}$ ).*

*Proof.* We see from Proposition 8.4 that  $(1 + T_i)[\underline{U}]$  depends only on the spaces  $U_j$  for  $j \neq i$ . On the other hand, we see from the definitions that  $\pi s_i^*(v)$  only differs from  $\pi(v)$  in the  $i$ 'th space, so  $(1 + T_i)\pi = (1 + T_i)\pi s_i^*$ , so  $(1 + T_i)\mu = (1 + T_i)\pi s_i^*\omega$ . However, we have  $s_i^*\omega = -\omega$ , so  $(1 + T_i)\pi s_i^*\omega = -(1 + T_i)\mu$ . It follows that  $(1 + T_i)\mu = 0$ , or in other words  $T_i\mu = -\mu$ . Given any  $\sigma \in \Sigma$  we can find a reduced word  $s_{i_1} \cdots s_{i_r}$  for  $\Sigma$ . We then have

$$T_\sigma\mu = T_{i_1} \cdots T_{i_r}\mu = (-1)^r\mu = \widehat{\xi}(T_\sigma)\mu.$$

As the  $T_\sigma$  span  $\mathcal{H}$  this gives  $a\mu = \widehat{\xi}(a)\mu$  for all  $a$ . It follows that  $\xi(ab)\mu = \xi(a)\xi(b)\mu$  and one sees directly that  $\mu \neq 0$  so  $\xi$  is a ring map. (This could also have been deduced from Proposition 8.11.) We also have  $T_\sigma^t = T_{\sigma^{-1}}$  and  $\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma)$  so  $\xi(a^t) = \xi(a)$ .

Next, as  $e = \mu\pi^t$  and  $a\mu = \widehat{\xi}(a)\mu$  we have  $ae = \xi(a)e$ . We observed in Definition 9.1 that  $e^t = e$ , so we can transpose the above equation to get  $ea^t = \xi(a)e$ , and replace  $a$  by  $a^t$  to get  $ea = \xi(a^t)e$ . As  $\xi(a^t) = \xi(a)$  this gives  $ea = \xi(a)e$ , showing that  $e$  is central.  $\square$

**Proposition 9.3.**  $e = |G/B|^{-1} \sum_{\sigma} \text{sgn}(\sigma) p^{l(\sigma^{-1}\rho)} T_{\sigma}$ .

*Proof.* Corollary 5.5 tells us that

$$\langle \pi\sigma^* \pi^t [\underline{U}], [\underline{W}] \rangle = \langle \sigma^* \pi^t [\underline{U}], [\underline{W}] \rangle = \begin{cases} |B/U| p^{l(\sigma^{-1}\rho)} & \text{if } \delta(\underline{U}, \underline{W}) = \sigma \\ 0 & \text{otherwise.} \end{cases}$$

It follows that  $\pi\sigma^* \pi^t = |B/U| p^{l(\sigma^{-1}\rho)} T_{\sigma}$ , and thus that

$$e = |G/U|^{-1} \sum_{\sigma} \text{sgn}(\sigma) \pi\sigma^* \pi^t = |G/B|^{-1} \sum_{\sigma} \text{sgn}(\sigma) p^{l(\sigma^{-1}\rho)} T_{\sigma}$$

as claimed.  $\square$

**Proposition 9.4.** *We have  $\mu\pi^t\mu = \mu$ . The maps  $e$  and  $e_{\text{St}}$  are idempotent, and  $\text{image}(e) = M_{\text{St}}$ . The map  $\mu: \mathbb{Z}_{(p)}[\text{Base}] \rightarrow M_{\text{St}}$  restricts to give an isomorphism  $\text{image}(e_{\text{St}}) \rightarrow M_{\text{St}}$ , with inverse given by the restriction of  $\pi^t$ .*

*Proof.* First, we have

$$\xi(e) = |G/B|^{-1} \sum_{\sigma} p^{l(\sigma^{-1}\rho)} = |G/B|^{-1} |\coprod_{\sigma} X(\sigma^{-1}\rho)| = |G/B|^{-1} |\coprod_{\tau} X(\tau)| = 1.$$

It follows that  $\mu\pi^t\mu = e\mu = \widehat{\xi}(e)\mu = \mu$ , and thus that

$$\begin{aligned} e^2 &= \mu\pi^t\mu\pi^t = \mu\pi^t = e \\ e_{\text{St}}^2 &= \pi^t\mu\pi^t\mu = \pi^t\mu = e_{\text{St}}, \end{aligned}$$

so  $e$  and  $e_{\text{St}}$  are idempotent. As  $e = \mu\pi^t$  we have  $\text{image}(e) \leq \text{image}(\mu)$ , and as  $\mu = e\mu$  we have  $\text{image}(\mu) \leq \text{image}(e)$ , so  $\text{image}(e) = \text{image}(\mu) = M_{\text{St}}$ . Now put  $M'_{\text{St}} = \text{image}(e_{\text{St}})$ , and let  $\alpha: M'_{\text{St}} \rightarrow M_{\text{St}}$  be the restriction of  $\mu$ . As  $e_{\text{St}} = \pi^t\mu$  we see that  $\pi^t(M_{\text{St}}) = \text{image}(\pi^t\mu) = M'_{\text{St}}$ . Thus, if we let  $\beta$  be the restriction of  $\pi^t$  to  $M_{\text{St}}$ , we see that  $\beta$  gives an epimorphism  $M_{\text{St}} \rightarrow M'_{\text{St}}$ . As the map  $\mu\pi^t = e$  restricts to 1 on  $M_{\text{St}}$  we see that  $\alpha\beta = 1$ , and as  $\beta$  is an epimorphism this tells us that  $\alpha$  and  $\beta$  are mutually inverse isomorphisms.  $\square$

**Proposition 9.5.**  *$M_{\text{St}}$  is projective and self dual in  $\mathcal{V}\mathcal{A}$ , and has rank  $p^{n(n-1)/2}$ . The natural map  $\mathbb{Z}_{(p)} \rightarrow \text{End}_{\mathcal{V}\mathcal{A}}(M_{\text{St}})$  is an isomorphism. If we put  $N = \text{image}(1 - e)$  then  $\text{Hom}_{\mathcal{V}\mathcal{A}}(M_{\text{St}}, N) = 0$  and  $\text{Hom}_{\mathcal{V}\mathcal{A}}(N, M_{\text{St}}) = 0$ .*

*Proof.* There is a Yoneda isomorphism  $\text{Hom}_{\mathcal{V}\mathcal{A}}(\mathbb{Z}_{(p)}[\text{Base}], A) = A(\mathbb{F}_p^n)$ , so  $\mathbb{Z}_{(p)}[\text{Base}]$  is projective. We have seen that  $M_{\text{St}}$  is isomorphic to the image of  $e_{\text{St}}$ , which is a summand in  $\mathbb{Z}_{(p)}[\text{Base}]$ , so  $M_{\text{St}}$  is projective. On the other hand,  $M_{\text{St}}$  is also the image of a self-adjoint idempotent on  $\mathbb{Z}_{(p)}[\text{Flag}]$ , so the standard perfect pairing on  $\mathbb{Z}_{(p)}[\text{Flag}]$  restricts to give one on  $M_{\text{St}}$ , so  $M_{\text{St}}$  is self dual. We also see that the rank of  $M_{\text{St}}$  is the trace of  $e$ . If  $\sigma \neq 1$  then  $\delta(\underline{U}, \underline{U}) \neq \sigma$  so one sees from the definitions that  $T_{\sigma}$  has trace zero. For  $\sigma = 1$  the map  $T_{\sigma}$  is the identity, with trace  $|\text{Flag}| = |G/B|$ . We therefore see from Proposition 9.3 that  $\text{trace}(e) = p^{l(\rho)} = p^{n(n-1)/2}$ .

Next, note that  $\mathbb{Z}_{(p)}[\text{Flag}] = M_{\text{St}} \oplus N$ , so any map from  $M_{\text{St}}$  to itself (or from  $M_{\text{St}}$  to  $N$ , or from  $N$  to  $M_{\text{St}}$ ) can be extended to an endomorphism of  $\mathbb{Z}_{(p)}[\text{Flag}]$ , or in other words an element  $a \in \mathcal{H}$ . Any such element satisfies  $ae = \xi(a)e = ea$ , which means that  $a$  preserves  $M_{\text{St}} = \text{image}(e)$  and  $N = \ker(e)$ , and acts as a scalar on  $M_{\text{St}}$ . Thus  $\text{End}_{\mathcal{V}\mathcal{A}}(M_{\text{St}}) = \mathbb{Z}_{(p)}$  and  $\text{Hom}_{\mathcal{V}\mathcal{A}}(M_{\text{St}}, N) = 0$  and  $\text{Hom}_{\mathcal{V}\mathcal{A}}(N, M_{\text{St}}) = 0$ .  $\square$