LOUIS SOLOMON

THE BRUHAT DECOMPOSITION, TITS SYSTEM AND IWAHORI RING FOR THE MONOID OF MATRICES OVER A FINITE FIELD

For Jacques Tits on his sixtieth birthday

ABSTRACT. Let $G = \mathrm{GL}_n(\mathbf{F}_q)$ be the finite general linear group and let $M = \mathrm{M}_n(\mathbf{F}_q)$ be the monoid of all $n \times n$ matrices over $\mathbf{F}_q$. Let B be a Borel subgroup of G, let W be the subgroup of permutation matrices, and let $\mathscr{R} \supset W$ be the monoid of all zero-one matrices which have at most one non-zero entry in each row and each column. The monoid $\mathscr{R}$ plays the same role for M that the Weyl group W does for G. In particular there is a length function on $\mathscr{R}$ which extends the length function on W and a C-algebra $H_{\mathbf{C}}(M, B)$ which includes Iwahori's 'Hecke algebra' $H_{\mathbf{C}}(G, B)$ and shares many of its properties.

1. INTRODUCTION

This paper has its roots in the combinatorics of inversion of permutations. Let W be the symmetric group on $\{1, \ldots, n\}$. If $w \in W$ let $n(w)$ be the number of its inversions; an inversion is a pair (wi, wj) for which $i < j$ and $wi > wj$. Let q be an indeterminate. Rodrigues [21] found the generating function

$$(1.1) \qquad \sum_{w \in W} q^{n(w)} = \prod_{i=1}^{n-1} (1 + q + \cdots + q^i)$$

for the numbers $n(w)$. The set of transpositions $S = \{(12), (23), \ldots, (n-1, n)\}$ generates W and (W, S) is a Coxeter system. If $w \in W$ let $l(w)$ be the length of w, the least integer l such that w may be written as a word of length l in the elements of S. Then

$$(1.2) \qquad l(w) = n(w)$$

for all $w \in W$ so we may replace $n(w)$ by $l(w)$ in (1.1). Now let q be a prime power. Formula (1.1) may be interpreted in terms of the group $G = \mathrm{GL}_n(\mathbf{F}_q)$. The order of G is the number of frames (ordered bases) for $\mathbf{F}_q^n$ which, by direct count, is $(q^n - 1)(q^n - q) \ldots (q^n - q^{n-1})$. Thus

$$(1.3) \qquad |G| = (q-1)^n q^{n(n-1)/2} \prod_{i=1}^{n-1} (1 + q + \cdots + q^i).$$

In view of (1.1) and (1.2), we have

$$(1.4) \qquad |G| = (q-1)^n q^{n(n-1)/2} \sum_{w \in W} q^{l(w)}.$$

Geometriae Dedicata **36**: 15–49, 1990.

Now consider singular matrices. Let $M = \mathrm{M}_n(\mathbf{F}_q)$ be the monoid of all $n \times n$ matrices over $\mathbf{F}_q$. Let $M^r \subseteq M$ be the set of matrices of rank r. The group $G \times G$ acts transitively on M^r using left and right multiplication. We compute the order of the stabilizer of the idempotent $e_r = \mathrm{diag}(1, \ldots, 1, 0, \ldots, 0) \in M^r$ using the formula (1.3) for $|G|$ and find

$$(1.5) \qquad |M^r| = (q-1)^r q^{r(r-1)/2} \begin{bmatrix} n \\ r \end{bmatrix}^2 [r]!$$

where

$$[r]! = \prod_{i=1}^{r-1} (1 + q + \cdots + q^i)$$

and

$$\begin{bmatrix} n \\ r \end{bmatrix} = \frac{[n]!}{[r]![n-r]!}.$$

Since (1.5) is the same as (1.3) when $r = n$, we may ask for an analogue of (1.4) when $r < n$. The question is: can we find a length function $\sigma \mapsto l(\sigma)$ on some finite algebraic object such that (1.5) may be written as

$$(1.6) \qquad |M^r| = (q-1)^r q^{r(r-1)/2} \sum q^{l(\sigma)} \quad ?$$

The proper understanding of (1.4) lies in the Bruhat decomposition of G. We will see in this paper that the proper formulation and understanding of (1.6) lies in the 'Bruhat decomposition' of M. The Bruhat decomposition of G is

$$(1.7) \qquad G = \bigcup_{w \in W} BwB,$$

where $B \subseteq G$ is the Borel subgroup of upper triangular matrices. The union is disjoint and

$$(1.8) \qquad BwB = Bw'B \Rightarrow w = w'.$$

One can give an elementary argument for (1.7) using a variation on Gaussian elimination. The same argument works for the monoid M. Here is the result [20]. Let $\mathcal{R} \subseteq M$ be the set of all matrices σ such that (i) the entries of σ lie in $\{0, 1\}$ and (ii) σ has at most one non-zero entry in each row and column. Then

$$(1.9) \qquad M = \bigcup_{\sigma \in \mathcal{R}} B\sigma B.$$

The union is disjoint and

$$(1.10) \qquad B\sigma B = B\sigma' B \Rightarrow \sigma = \sigma'.$$

Note that

$$(1.11) \qquad |\mathscr{R}| = \sum_{r=0}^{n} \binom{n}{r}^2 r!$$

is the number of ways to place r non-attacking rooks on an $n \times n$ chessboard. The binomial coefficient gives the number of ways to choose the rows and columns which contain the rooks, and $r!$ is the number of ways to place r non-attacking rooks on an $r \times r$ chessboard. If we divide the right-hand side of (1.5) by $(q-1)^r$ and set $q = 1$ we get the right-hand side of (1.11). This suggests that the sum in our desired formula (1.6) should be taken over the set $\mathscr{R}^r$ of elements of rank r in $\mathscr{R}$. Note that $\mathscr{R}$ is a monoid. Since the elements of $\mathscr{R}$ are in one to one correspondence with placements of rooks we call $\mathscr{R}$ the *rook monoid*. The rook monoid plays the same role for M that the symmetric group does for G. It is an example of a *Renner monoid*, to be defined later in this Introduction, just as the symmetric group is an example of a Weyl group. The monoid $\mathscr{R}$ has been studied in semigroup theory under the name symmetric inverse semigroup ([7], [16]) but it has not been studied in the spirit of the combinatorics of Coxeter groups.

The preceding remarks about matrices may be put in a more general setting. In 1954, Bruhat [3] showed that a classical semisimple Lie group G has a double coset decomposition as in (1.7) where B is a maximal solvable subgroup of G and W is the Weyl group of G. Shortly thereafter, Chevalley [6] defined for each complex semisimple Lie algebra and field F a linear group G over F. The Chevalley groups have a double coset decomposition of the form (1.7). Chevalley proved a refinement of (1.7) which allowed him to show, in the case where the ground field F is $\mathbf{F}_q$, that the order of G is

$$(1.12) \qquad |G| = |B| \sum_{w \in W} q^{n(w)},$$

where B is a Borel subgroup, W is the Weyl group and $n(w)$ is the number of positive roots of the Lie algebra which are carried into negative roots by $w \in W$. We know from work of Iwahori [10] that the analogue of (1.2) is true in this context: $n(w) = l(w)$ where $l(w)$ is the length of w as a word in the Coxeter generating set S of reflections corresponding to simple roots. Thus $n(w)$ may be replaced by $l(w)$ in Chevalley's formula. If $G = \mathrm{PSL}_n(\mathbf{F}_q)$ then W is the symmetric group, Chevalley's $n(w)$ is the number of inversions of w and $|B| = (q-1)^n q^{n(n-1)/2}$. Thus (1.12) is essentially (1.4).

In 1962 Jacques Tits introduced the notion of a group G with (B, N)-pair [26]. He was inspired in part by Chevalley's paper: 'On étudie, d'un point de vue axiomatique, quelques propriétés d'un groupe algébrique. Pour l'explication des hypothèses et l'origine de certains raisonnements, cf. C.

Chevalley....' Tits immediately applied this idea to abstract simple groups in [27] and to reductive algebraic groups in [1]. Since its introduction in 1962, the notion of a group with a (B, N)-pair or Tits system (G, B, N) has had extraordinary influence on group theory, geometry and other parts of mathematics. The axioms are few. Their consequences are many. The key axiom is one for the multiplication of double cosets:

$$(1.13)\quad BsB \cdot BwB \subseteq BwB \cup BswB \qquad \text{for all } s \in S \text{ and } w \in W.$$

Here W is the Weyl group of G and S is a distinguished set of involutory generators for W. It follows from the axioms that (W, S) is a Coxeter system and that (1.13) may be written in stronger form as

$$(1.14)\qquad BsB \cdot BwB = \begin{cases} BswB & \text{if } l(sw) > l(w) \\ BswB \cup BwB & \text{if } l(sw) < l(w), \end{cases}$$

where $l(w)$ is the length of w as a word in the generating set S.

In 1981, Grigor'ev [9] considered an analogue of the Bruhat decomposition for certain submonoids M of $\mathrm{M}_n(F)$ determined by classical groups G in their natural representation over a field F. If $G = \mathrm{SL}_n(F)$ his monoid M is $\mathrm{M}_n(F)$, but his work did not lead him to the monoid $\mathscr{R}$.

In 1986, Renner [20] found the correct general setting for (1.13) in the theory of reductive algebraic monoids. The theory of algebraic monoids over an algebraically closed field F is the combined work of Renner and Putcha; see Putcha's monograph [17] for a complete set of references. An affine algebraic monoid is a Zariski closed submonoid M of $\mathrm{M}_n(F)$. Waterhouse [28] has shown that every connected algebraic group G with a non-trivial homomorphism into the multiplicative group $F^\times$ occurs as the group of units of an algebraic monoid M which properly includes G. An algebraic monoid M is reductive if its group G of units is a connected reductive algebraic group. For example, $M = \mathrm{M}_n(F)$ is a reductive algebraic monoid with unit group $G = \mathrm{GL}_n(F)$. Renner [19] has classified the reductive algebraic monoids. The implications of this work for algebraic combinatorics have not been explored at all.

Renner [20] developed a theory of 'Bruhat decomposition' in a reductive algebraic monoid M with unit group G. Let T be a maximal torus of G and let $B \supset T$ be a Borel subgroup of G. Let R be the Zariski closure of the normalizer $N_G(T)$ in M and let $\mathscr{R} = R/T$ be the orbit monoid, which is well defined because $\sigma T = T\sigma$ for all $\sigma \in \mathscr{R}$. The Renner monoid $\mathscr{R}$ is finite and has the Weyl group W of G as its group of units. Renner's Bruhat decomposition for M asserts that (1.9) and (1.10) are true in this context. Thus $\mathscr{R}$ plays the

By [21, Theorem – or, more precisely, (4.1)], $|L| \leqslant k := q^{3n}$ for L in $\mathbf{C}_9$. On the other hand, in [1, §1] there is a thorough discussion of the conjugacy classes of subgroups L of types $\mathbf{C}_1$–$\mathbf{C}_8$, from which it follows that the numbers of conjugacy classes are bounded above as follows:

$\mathbf{C}_1$: $2n$
$\mathbf{C}_2$, $\mathbf{C}_3$, $\mathbf{C}_4$: n (an upper bound on the number of divisors of n)
$\mathbf{C}_5$: $\log q$ (where, throughout this paper, logarithms are always to the base 2)
$\mathbf{C}_6$: 1
$\mathbf{C}_7$: $\log n$
$\mathbf{C}_8$: 4.

In each case, $|G:L| \geqslant \frac{1}{2}q^{n-1}$. Since $|G| > \frac{1}{2}q^{n^2-1}/n$, (*) becomes (with Σ' denoting the sum over $\mathbf{C}_1$–$\mathbf{C}_8$ and Σ_9 denoting the sum over $\mathbf{C}_9$)

$$(**) \qquad P(G) \leqslant \sum \frac{|L|}{|G|} = \sum{}' \frac{|L|}{|G|} + \sum_9 \frac{|L|}{|G|}$$
$$\leqslant \frac{\{5n + \log q + 1 + \log n + 4\}}{\frac{1}{2}q^{n-1}} + \frac{2n(\Sigma_9 |L|)}{q^{n^2-1}}.$$

The first term is negligible, so consider the second one. Recall that $|L| \leqslant k$ for L in $\mathbf{C}_9$.

The number of possible simple groups S of a given order $s \leqslant k$ is itself $\leqslant 2$ (by the classification of finite simple groups). Fix such a simple group S. The number of (equivalence classes of) absolutely irreducible projective representations of S in characteristic p is at most $|\tilde{S}|$, where $|\tilde{S}| \leqslant |S| \log |S|$. For each such representation, maximality forces L to be the normalizer of (the image of) S; and L is isomorphic to a subgroup of $\mathrm{Aut}(S)$ containing S, so that $|L| \leqslant |S| \log |S|$. (All of these estimates are very crude: slightly less crude ones are used in Lemmas 1 and 3 below.) Thus,

$$\sum_9 |L| \leqslant \sum_{s \leqslant k} \sum_{|S| = s} \sum_{\text{representations of } S} |L|$$
$$\leqslant k \cdot 2 \cdot k \log k \cdot k \log k \leqslant 2(q^{3n})^3 (\log q^{3n})^2,$$

so that, if $n \geqslant 10$, then

$$\frac{2n(\Sigma_9 |L|)}{q^{n^2-1}} \leqslant \frac{4n \cdot q^{9n}(3n \log q)^2}{q^{n^2-1}} \leqslant \frac{36n^3(\log q)^2}{q^{n-1}} \to 0$$

as $|G| \to \infty$.

This proves the Theorem for $n \geqslant 10$. The remaining cases can be handled by slightly sharpening some of the above estimates in order to handle same role for M that the Weyl group W does for G. Renner has also shown that M admits a 'Tits system' in the sense that there are formulas

(1.15) $BsB \cdot B\sigma B \subseteq Bs\sigma B \cup B\sigma B$ for all $s \in S$ and $\sigma \in \mathcal{R}$,

where S is a set of Coxeter generators for the Weyl group W of the algebraic group G. Putcha [18] has studied Renner's analogue of the Bruhat decomposition in a more axiomatic way: the setting is a monoid in which the group of units admits a Tits system.

If we can find a suitable length function $\sigma \mapsto l(\sigma)$ on $\mathcal{R}$, we may be able to make (1.15) as precise as (1.14) and proceed further, for example in the direction of (1.6). Renner defined a length function in [20] but it does not satisfy the conditions (1.14) with w replaced by σ and it does not satisfy (1.6) with summation over $\sigma \in \mathcal{R}$. If, in addition, we can interpret $l(\sigma)$ in terms of the underlying root system by proving an analogue of the formula $l(w) = n(w)$ then we may re-examine, for *any* ground field F, the various aspects of combinatorics and/or representation theory of G which involve the function $n(w)$ and see what results if the group G is replaced by the monoid M.

In this paper we consider the case $G = \mathrm{GL}_n(F)$ and $M = \mathrm{M}_n(F)$. Our aim is to describe an analogue $H(M, B)$ in case $M = \mathrm{M}_n(\mathrm{F}_q)$ and $G = \mathrm{GL}_n(\mathrm{F}_q)$ of the ring $H(G, B)$ which was studied by Iwahori [10] in case G is a finite Chevalley group and B is a Borel subgroup. This paper is patterned after Iwahori's. In Section 2 we define the length function $l(\sigma)$ and give a formula for $l(\sigma)$, in terms of the root system, analogous to the formula $l(w) = n(w)$. We prove that

$$(1.16) \qquad \sum_{\sigma \in \mathcal{R}^r} q^{l(\sigma)} = \begin{bmatrix} n \\ r \end{bmatrix}^2 [r]!.$$

This is the desired formula (1.6) given without any reference to M. For $r = n$ it is (1.1) with $n(w)$ replaced by $l(w)$. In Section 3 we study the multiplication of $B \times B$ orbits on M and prove the desired analogue of (1.14). It may happen that $l(s\sigma) = l(\sigma)$. This happens precisely when $Bs\sigma B = B\sigma B$. The results in Section 3 allow us to interpret (1.16) in terms of M. In Section 4 we construct the ring $H(M, B)$, a $\mathbf{Z}$-order which contains $H(G, B)$ as a subring with the same identity element. The ring $H(G, B)$ has a $\mathbf{Z}$-basis of elements T_w for $w \in W$. Iwahori [10] showed that $H(G, B)$ is generated by the T_s for $s \in S$ and that the multiplication in $H(G, B)$ is determined by the formulas

$$(1.17) \qquad T_s T_w = \begin{cases} T_{sw} & \text{if } l(sw) = l(w) + 1 \\ qT_{sw} + (q-1)T_w & \text{if } l(sw) = l(w) - 1. \end{cases}$$

The ring $H(M, B)$ has a $\mathbf{Z}$-basis of elements T_σ for $\sigma \in \mathcal{R}$. It is generated by the

T_s for $s \in S$ together with one additional element T_ν where $\nu \in \mathscr{R}$ is nilpotent element

$$(1.18) \qquad \nu = E_{12} + \cdots + E_{n-1,n}$$

and the E_{ij} denote matrix units. The multiplication in $H(M, B)$ is determi by the formulas

$$(1.19) \qquad T_s T_\sigma = \begin{cases} qT_\sigma & \text{if } l(s\sigma) = l(\sigma) \\ T_{s\sigma} & \text{if } l(s\sigma) = l(\sigma) + 1 \\ qT_{s\sigma} + (q-1)T_\sigma & \text{if } l(s\sigma) = l(\sigma) - 1 \end{cases}$$

and

$$(1.20) \qquad T_\nu T_\sigma = q^{l(\sigma) - l(\nu\sigma)} T_{\nu\sigma}.$$

There are similar formulas for right multiplication of T_σ by T_s and T_ν. If l any commutative ring, define K-algebras $H_K(G, B) = K \otimes H(G, B)$ ε $H_K(M, B) = K \otimes H(M, B)$. The isomorphism

$$(1.21) \qquad H_{\mathbf{C}}(G, B) \simeq \mathbf{C}[W]$$

of the Iwahori algebra over $\mathbf{C}$ with the group algebra of the Weyl group i central fact in the representation theory of finite groups G with (B, N)-p This is a theorem of Tits which shows another facet of his extraordin influence on the recent history of Lie theory. The main tool in the prooi (1.21) is a construction of an algebra $A(W)$, called the generic algebra ([5], [[11], [12]) which has both the $\mathbf{C}$-algebras $H_{\mathbf{C}}(G, B)$ and $\mathbf{C}[W]$ as sp ializations. We construct an analogous algebra $A(\mathscr{R})$ for $H(M, B)$ in c $M = \mathrm{M}_n(\mathbf{F}_q)$ and prove that there is an isomorphism

$$(1.22) \qquad H_{\mathbf{C}}(M, B) \simeq \mathbf{C}[\mathscr{R}].$$

In a sequel to this paper we intend to complete the analogy with Iwaho paper [10] by giving a presentation for $H(M, B)$ in terms of the generators and T_ν analogous to Iwahori's presentation

$$(1.23) \qquad \begin{array}{ll} T_s^2 = q \cdot 1 + (q-1)T_s & \text{if } s \in S \\ T_s T_{s'} = T_{s'} T_s & \text{if } ss' = s's \\ T_s T_{s'} T_s = T_{s'} T_s T_{s'} & \text{if } ss's = s'ss' \end{array}$$

for $H(G, B)$. The defining relations involving T_ν and the T_s are complicat

NOTATION AND TERMINOLOGY. Let $\mathbf{N}$ denote the set of no negative integers. If n is a positive integer let $\mathbf{n} = \{1, \ldots, n\}$. If $a \in \mathrm{M}_n(F)$, rk(a) denote the rank of a and let a^* denote the transpose of a. The symbol is used for emphasis and means disjoint union; some unions which are clearly disjoint are written $\cup$.

Some explanation of my use of the name 'Iwahori ring' for $H(G, B)$ or $H(M, B)$ seems in order because current usage is 'Hecke ring'. In 1933, I. Schur [*Collected Works*, Vol. III, p. 266] introduced the ring $A = eRe$ in the case where R is the group ring of a finite group G and e is the idempotent corresponding to a subgroup B. At that time the passage from R to eRe was already a familiar construct in ring theory. Schur had in fact used the same ring A in 1908 [*Collected Works*, Vol I, p. 266] with a definition in terms of bilinear forms. There are related analytic constructions, with a long history, in the theory of spherical functions.

The name 'Hecke ring' and the notation $H(G, B)$ were introduced around 1962. One can follow the evolution of this notation and terminology in papers of G. Shimura and T. Tamagawa. I have made some changes in their notation for consistency here. Let G be any group and let B be a subgroup of G commensurable with all its conjugates. In 1959 [*J. Math. Soc. Japan*, **11**, 309] Shimura wrote: 'Nous nous proposons maintenant de construire, d'après une idée de A. Weil une algèbre A a partir des elements de G... On appelle A l'anneau de transformations de B par rapport à G.' If G is finite then A is the ring defined by Schur. Shimura considered the case where B is a suitable discrete subgroup of $SL_2(\mathbf{R})$ and used certain representations of A to construct Hecke operators. In 1961 [*J. Math. Soc. Japan*, **13**, 277] A was still called the 'ring of transformations of B with respect to G'. In 1962 [*Ann. of Math.* **72**, 248] A was called the Hecke ring: 'We call, after Tamagawa, the ring A the Hecke-ring...' The first section of Tamagawa's 1963 paper on the zeta function of a division algebra [*Ann. of Math.* **77**, 387] is titled 'Hecke algebras'. This fixed the terminology. Iwahori followed this usage when he studied the ring $H(G, B)$ for G a group of Lie type and B a Borel subgroup. He did this in [10] when G is a finite Chevalley group, in [11] for the analogous situation in p-adic groups, and in [12] for finite groups with (B, N)-pair. Iwahori was the first to discover that there are marvelous facts about $H(G, B)$ which are peculiar to this special but extremely important case. Thus, contrary to popular usage, with all proper homage to Hecke (who did not study the ring), and with some small hope that the terminology may survive in the (B, N)-setting, I have called $H(G, B)$ and the analogous ring $H(M, B)$ the Iwahori ring in this paper.

2. The length function on the rook monoid

Let F be a field. As in the Introduction let $\mathscr{R} \subseteq \mathrm{M}_n(F)$ be the rook monoid. Let $W \subseteq GL_n(F)$ be the group of permutation matrices and let $S = \{(12), (23), \ldots, (n-1, n)\}$ be its set of distinguished generators where $(k, k+1) \in GL_n(F)$ interchanges the standard basis vectors for F^n which are indexed by k and $k+1$. We do not identify W with the symmetric group on $\mathbf{n}$ because W will have both left and right actions on $\mathbf{n}$. For $0 \leqslant r \leqslant n$ let $\mathscr{R}^r$ denote the set of elements of rank r in $\mathscr{R}$. Note that $\mathscr{R}^0$ consists of the zero matrix. To avoid vacuous remarks assume when necessary that $r \geqslant 1$. An element $\sigma \in \mathscr{R}^r$ has the form

$$\sigma = \sum_{\nu=1}^{r} E_{i_\nu j_\nu}$$

where $I(\sigma) := \{i_1, \ldots, i_r\}$ and $J(\sigma) := \{j_1, \ldots, j_r\}$ are subsets of $\mathbf{n}$ of size r and the E_{ij} are matrix units with 1 in position (i, j) and 0 elsewhere. Write $i_\nu \sigma = j_\nu$ and $\sigma j_\nu = i_\nu$. Thus

$$(2.1) \qquad \sum_{i \in I(\sigma)} E_{i, i\sigma} = \sigma = \sum_{j \in J(\sigma)} E_{\sigma j, j}.$$

The maps $i \mapsto i\sigma$ from $I(\sigma)$ to $J(\sigma)$ and $j \mapsto \sigma j$ from $J(\sigma)$ to $I(\sigma)$ are bijective. If $w \in W$ then $I(w) = \mathbf{n} = J(w)$ and $wi = iw^{-1}$ for all $i \in \mathbf{n}$. Since $E_{ij}^* = E_{ji}$ we have $I(\sigma) = J(\sigma^*)$ and $J(\sigma) = I(\sigma^*)$. Also $(i\sigma)\sigma^* = i$ for $i \in I(\sigma)$ and $\sigma^*(\sigma j) = j$ for $j \in J(\sigma)$. The group $W \times W$ acts on $\mathscr{R}$ by

$$(2.2) \qquad (w, w')\sigma = w\sigma w'^{-1} \quad \text{for } \sigma \in \mathscr{R} \text{ and } w, w' \in W.$$

Since left (right) multiplication by $w \in W$ permutes the rows (columns) of a matrix, two elements of $\mathscr{R}$ lie in the same $W \times W$ orbit if and only if they have the same rank. Thus the $W \times W$ orbits on $\mathscr{R}$ are the sets $\mathscr{R}^r$ for $0 \leqslant r \leqslant n$. Fix such an integer r. We will define the length $l(\sigma)$ for $\sigma \in \mathscr{R}^r$ in such a way that (1.16) holds. Define a graph with vertex set $\mathscr{R}^r$ as follows. Say that two vertices σ, τ are adjacent if either there exists $s \in S$ with $\tau = s\sigma$ or there exists $s \in S$ with $\tau = \sigma s$. The graph is connected because S generates W and $\mathscr{R}^r$ is a $W \times W$ orbit. For $\tau, \sigma \in \mathscr{R}^r$ let $d(\tau, \sigma)$ be the graph distance from τ to σ. This is given by

$$(2.3) \qquad d(\tau, \sigma) = \min\{l(w) + l(w') \mid w, w' \in W \text{ and } \sigma = w\tau w'\}.$$

It is natural to define $l(\sigma) = d(\tau, \sigma)$ for some suitably chosen τ which will then be the unique element in $\mathscr{R}^r$ of length zero. The correct choice of τ is suggested by the demand that (1.16) be true. Let

$$(2.4) \qquad \nu = E_{12} + E_{23} + \cdots + E_{n-1,n}.$$

If $0 \leqslant r \leqslant n$, then

$$(2.5) \qquad \nu_r = \nu^{n-r} = E_{1,n-r+1} + E_{2,n-r+2} + \cdots + E_{r,n}$$

has rank r. We choose v_r as our element of length zero and thus define

$$(2.6) \qquad l(\sigma) = \min\{l(w) + l(w') \mid w, w' \in W \text{ and } \sigma = wv_r w'\}$$

for $\sigma \in \mathscr{R}^r$. It follows from the definition that $|l(s\sigma) - l(\sigma)| \leqslant 1$ and $|l(\sigma s) - l(\sigma)| \leqslant 1$ for $\sigma \in \mathscr{R}$ and $s \in S$. In [20] Renner defined $l(\sigma) = \min\{l(w) \mid \sigma \in wI(\mathscr{R})\}$ where $I(\mathscr{R})$ is the set of idempotents of $\mathscr{R}$. This is not the same as (2.6) since it gives $|I(\mathscr{R})| = n!/r!(n-r)!$ elements of length zero in $\mathscr{R}^r$.

Our aim in this section is to give a combinatorial description of $l(\sigma)$ for $\sigma \in \mathscr{R}$ and a proof of the formula (1.16). We will define two functions $n: \mathscr{R} \to \mathbf{N}$ and $m: \mathscr{R} \to \mathbf{N}$, in terms of the cardinalities of certain sets of roots in a root system of type A_{n-1} and prove that $l(\sigma) = m(\sigma) + n(\sigma)$ for all $\sigma \in \mathscr{R}$. If one is interested only in the analogue of Rodrigues' formula (1.1) for $r < n$, stated as Theorem 2.45, one can define the functions m and n without the roots and shorten the argument. But the lemmas we prove about the roots are used in Section 3 to find the multiplication formulas for the sets $B\sigma B$ and to find their cardinalities when the ground field F is finite. The argument in this section is patterned after Iwahori's proof in [10] that $l(w) = n(w)$ but the combinatorics is more complicated. To begin, we recall some of the facts from [10], with minor changes in notation. Let

$$(2.7) \qquad \Delta = \{(i, j) \in \mathbf{n} \times \mathbf{n} \mid 1 \leqslant i \neq j \leqslant n\}$$

and let

$$(2.8) \qquad \Delta^+ = \{(i, j) \in \Delta \mid i < j\}, \qquad \Delta^- = \{(i, j) \in \Delta \mid i > j\}.$$

We may think of Δ as a root system of type A_{n-1} and think of Δ^+ and Δ^- as the sets of positive and negative roots. Let W act on Δ by $w(i, j) = (wi, wj)$ for $w \in W$. If $s \in S$ is the transposition of k and $k+1$ let $\alpha_s = (k, k+1) \in \Delta^+$ denote the corresponding simple root. Then

$$(2.9) \qquad s(\Delta^+ - \{\alpha_s\}) = \Delta^+ - \{\alpha_s\}.$$

Chevalley [6] introduced for each $w \in W$ a partition of the set of positive roots into two disjoint subsets: if $w \in W$ let

$$(2.10) \qquad \Psi'(w) = \{\alpha \in \Delta^+ \mid w^{-1}\alpha \in \Delta^+\}$$

$$\Psi''(w) = \{\alpha \in \Delta^+ \mid w^{-1}\alpha \in \Delta^-\}.$$

Thus

$$(2.11) \qquad \Delta^+ = \Psi'(w) \sqcup \Psi''(w).$$

Note that $(i, j) \in \Psi''(w)$ if and only if (j, i) is an inversion of the permutation

$k \mapsto wk$ of $\mathfrak{n}$. Thus $n(w) = |\Psi''(w)|$. It follows from (2.9) that the function $w \mapsto \Psi''(w)$ satisfies the 'cocycle condition'

$$(2.12) \qquad \begin{aligned} \Psi''(sw) &= s\Psi''(w) \cup \{\alpha_s\} \quad \text{if } \alpha_s \in \Psi'(w) \\ \Psi''(w) &= s\Psi''(sw) \cup \{\alpha_s\} \quad \text{if } \alpha_s \in \Psi''(w) \end{aligned}$$

where the unions are disjoint and thus

$$(2.13) \qquad n(sw) = \begin{cases} n(w) + 1 & \text{if } \alpha_s \in \Psi'(w) \\ n(w) - 1 & \text{if } \alpha_s \in \Psi''(w). \end{cases}$$

We will prove several formulas analogous to (2.13) with W replaced by $\mathscr{R}$ and use them to get our formula for $l(\sigma)$ in terms of the root system. The underlying idea is simple but the formalism is not, so we begin with some informal remarks which may help the reader. If $\sigma = \Sigma_{\nu=1}^{r} E_{i_\nu j_\nu}$ let $d(\sigma) = \Sigma_{\nu=1}^{r} (i_\nu - 1) + (n - j_\nu)$. Note that $(i - 1) + (n - j)$ is the distance, in a colloquial sense, from position ij to position $1n$ in an $n \times n$ matrix, where $i - 1$ is the vertical distance and $n - j$ is the horizontal distance. Since $d(\sigma)$ is the sum of these distances over all positions in which σ has a non-zero entry we have $d(\sigma) \geqslant d(v_r) = r(r - 1)$ with equality if and only if $\sigma = v_r$. Let $\sigma^\star$ be the permutation matrix of size r obtained from σ by deleting the rows and columns which consist of zeros. To pass from σ to v_r by a sequence of transpositions s of adjacent rows and columns we may proceed as follows. First, by a sequence of transpositions $\tau \mapsto s\tau$ of adjacent rows, we may arrange to get all the non-zero entries in rows $1, \dots, r$ in such a way that $(s\tau)^\star$ and $\tau^\star$ have the same set of inversions and $d(s\tau) = d(\tau) - 1$. Next, by a sequence of tranpositions $\tau \mapsto \tau s$ of adjacent columns, we may arrange to get all the non-zero entries in rows $1, \dots, r$ and columns $n - r + 1, \dots, n$ in such a way that $\tau^\star$ and $(\tau s)^\star$ have the same set of inversions and $d(\tau s) = d(\tau) - 1$. Now we have an $r \times r$ permutation matrix in the northeast corner of our $n \times n$ matrix. Finally by a sequence of transpositions $\tau \mapsto s\tau$ of adjacent rows in the set $\{1, \dots, r\}$ we may arrange to arrive at the matrix v_r in such a way that $n((s\tau)^\star) = n(\tau^\star) - 1$ and $d(s\tau) = d(\tau)$. This shows that $l(\sigma) \leqslant d(\sigma) - r(r - 1) + n(\sigma^\star)$. In fact equality holds. In the formal argument we define certain sets of positive roots with cardinalities $m_{01}(\sigma)$, $m_{10}(\sigma)$, and $n(\sigma)$. These sets satisfy cocycle conditions like (2.12). The translation from informal to formal is given by $n(\sigma) = n(\sigma^\star)$ and $m(\sigma) = m_{01}(\sigma) + m_{10}(\sigma) = d(\sigma) - r(r - 1)$. The splitting $m(\sigma) = m_{01}(\sigma) + m_{10}(\sigma)$ corresponds to the splitting of $d(\sigma)$ into its vertical and horizontal components.

For $K \subseteq \mathbf{n}$ define

$$(2.14)\qquad \begin{aligned} \Delta_{00}(K) &= \{(i,j)\in\Delta \mid i\notin K \text{ and } j\notin K\} \\ \Delta_{01}(K) &= \{(i,j)\in\Delta \mid i\notin K \text{ and } j\in K\} \\ \Delta_{10}(K) &= \{(i,j)\in\Delta \mid i\in K \text{ and } j\notin K\} \\ \Delta_{11}(K) &= \{(i,j)\in\Delta \mid i\in K \text{ and } j\in K\}. \end{aligned}$$

Thus

$$(2.15)\qquad \Delta = \Delta_{00}(K) \sqcup \Delta_{10}(K) \sqcup \Delta_{01}(K) \sqcup \Delta_{11}(K).$$

If $a, b\in\{0,1\}$ and $\sigma\in\mathscr{R}$, define subsets $\Psi_{ab}(\sigma)$ and $\Phi_{ab}(\sigma)$ of Δ by

$$(2.16)\qquad \Psi_{ab}(\sigma) = \Delta_{ab}(I(\sigma)) \quad\text{and}\quad \Phi_{ab}(\sigma) = \Delta_{ab}(J(\sigma)).$$

We make a *convention* concerning subsets of Δ which will be in force throughout the paper. If Γ is a subset of Δ we write $\Gamma^+ = \Gamma\cap\Delta^+$. Define

$$(2.17)\qquad \begin{aligned} \Psi'(\sigma) &= \{(i,j)\in\Psi_{11}^+(\sigma) \mid (i\sigma, j\sigma)\in\Delta^+\} \\ \Psi''(\sigma) &= \{(i,j)\in\Psi_{11}^+(\sigma) \mid (i\sigma, j\sigma)\in\Delta^-\} \\ \Phi'(\sigma) &= \{(i,j)\in\Phi_{11}^+(\sigma) \mid (\sigma i, \sigma j)\in\Delta^+\} \\ \Phi''(\sigma) &= \{(i,j)\in\Phi_{11}^+(\sigma) \mid (\sigma i, \sigma j)\in\Delta^-\}. \end{aligned}$$

If $\sigma = w\in W$ then all the sets $\Psi_{00}(w)$, $\Psi_{01}(w)$, $\Psi_{10}(w)$, $\Phi_{00}(w)$, $\Phi_{01}(w)$, $\Phi_{10}(w)$ are empty and the sets $\Psi'(w)$, $\Psi''(w)$ are as in (2.10). Since $J(\sigma) = I(\sigma^*)$ we have

$$(2.18)\qquad \Phi_{ab}(\sigma) = \Psi_{ab}(\sigma^*) \quad\text{and}\quad \Phi_{ab}^+(\sigma) = \Psi_{ab}^+(\sigma^*)$$

for $a, b\in\{0,1\}$. Also

$$(2.19)\qquad \Phi'(\sigma) = \Psi'(\sigma^*) \quad\text{and}\quad \Phi''(\sigma) = \Psi''(\sigma^*).$$

To each 'Ψ-statement' concerning left multiplication $\sigma\mapsto s\sigma$ there corresponds a dual 'Φ-statement' concerning right multiplication $\sigma\mapsto\sigma s$ which may be deduced from it if we replace σ by σ^* and use $(s\sigma)^* = \sigma^* s$. For example (2.12) yields

$$(2.20)\qquad \begin{aligned} \Phi''(ws) &= s\Phi''(w)\cup\{\alpha_s\} \quad \text{if } \alpha_s\in\Phi'(w) \\ \Phi''(w) &= s\Phi''(ws)\cup\{\alpha_s\} \quad \text{if } \alpha_s\in\Phi''(w). \end{aligned}$$

To avoid superfluous statements we usually suppress the duality between (J,Ψ) and (I,Φ). Our choice of Ψ or Φ is a matter of convenience.

LEMMA 2.21. *The map $(i,j)\mapsto(j\sigma, i\sigma)$ is bijective from $\Psi''(\sigma)$ to $\Psi''(\sigma^*)$.*

Proof. Suppose $(i, j) \in \Psi''(\sigma)$. Then $i \in I(\sigma)$, $j \in I(\sigma)$, $i < j$ and $i\sigma > j\sigma$. Thus $j\sigma \in J(\sigma)$, $i\sigma \in J(\sigma)$, $j\sigma < i\sigma$ and $(j\sigma)\sigma^* = j > i = (i\sigma)\sigma^*$ so that $(j\sigma, i\sigma) \in \Psi''(\sigma^*)$. Replacing σ by σ^* we see that if $(i', j') \in \Psi''(\sigma^*)$ then $(j'\sigma^*, i'\sigma^*) \in \Psi''(\sigma^{**}) = \Psi''(\sigma)$. □

DEFINITION 2.22. Define $n: \mathscr{R} \mapsto \mathbf{N}$ by $n(\sigma) = |\Psi''(\sigma)|$.

If $\sigma = w \in W$ this agrees with $n(w)$ defined in the Introduction. It follows from Lemma 2.21 that

$$n(\sigma^*) = n(\sigma). \tag{2.23}$$

If $\sigma = v_r$ then $I(\sigma) = \{1, \ldots, r\}$ and $i\sigma = i + n - r$ for $i \in I(\sigma)$ so $\Psi''(\sigma)$ is empty and thus $n(\sigma) = 0$. If $w \in W$ and $n(w) = 0$ then $w = 1$. It is not true that if $\sigma \in \mathscr{R}^r$ and $n(\sigma) = 0$ then $\sigma = v_r$. To overcome this difficulty we introduce a second function $m: \mathscr{R} \to \mathbf{N}$.

DEFINITION 2.24. If $K \subseteq \mathbf{n}$ define

$$m_{01}(K) = |\Delta_{01}^+(K)| \quad \text{and} \quad m_{10}(K) = |\Delta_{10}^+(K)|.$$

LEMMA 2.25. *If K is an r-subset of* $\mathbf{n}$ *then*

$$m_{01}(K) = \sum_{k \in K} (k - 1) - \frac{r(r-1)}{2}$$

$$m_{10}(K) = \sum_{k \in K} (n - k) - \frac{r(r-1)}{2}.$$

Proof. We must prove that

$$|\Delta_{01}^+(K)| = \sum_{k \in K} (k - 1) - \frac{r(r-1)}{2} \tag{2.26}$$

$$|\Delta_{10}^+(K)| = \sum_{k \in K} (n - k) - \frac{r(r-1)}{2}.$$

Write $K = \{k_1, \ldots, k_r\}$ where $k_1 < \cdots < k_r$. For $1 \leqslant v \leqslant r$ let

$$\Delta_{01}^v(K) = \{(i, j) \in \Delta_{01}^+(K) \mid j = k_v\}.$$

Since

$$\Delta_{01}^v(K) = \{(1, k_v), (2, k_v), \ldots, (k_v - 1, k_v)\} - \{(k_1, k_v), (k_2, k_v), \ldots, (k_{v-1}, k_v)\}$$

we have $|\Delta_{01}^v(K)| = (k_v - 1) - (v - 1)$. Since $\Delta_{01}(K) = \bigsqcup_{v=1}^r \Delta_{01}^v(K)$ this proves the first formula. The second formula is proved in the same way. □

DEFINITION 2.27. If $\sigma \in \mathscr{R}$ let

$$m_{01}(\sigma) = m_{01}(I(\sigma)) = |\Psi^+_{01}(\sigma)|, \qquad m_{10}(\sigma) = m_{10}(J(\sigma)) = |\Phi^+_{10}(\sigma)|$$

and let

$$m(\sigma) = m_{01}(\sigma) + m_{10}(\sigma).$$

It follows from the definition and (2.25) that if $\sigma \in \mathscr{R}^r$ then

$$(2.28) \qquad m(\sigma) = \sum_{i \in I(\sigma)} (i-1) + \sum_{j \in J(\sigma)} (n-j) - r(r-1).$$

Since $J(\sigma) = I(\sigma^*)$ it follows from (2.27) and (2.25) that $m_{01}(\sigma) + m_{10}(\sigma^*) = r(n-r)$. Similarly, since $I(\sigma) = J(\sigma^*)$ we have $m_{10}(\sigma) + m_{01}(\sigma^*) = r(n-r)$. Thus if $\sigma \in \mathscr{R}^r$ then

$$(2.29) \qquad m(\sigma) + m(\sigma^*) = 2r(n-r).$$

Define $p\colon \mathscr{R} \mapsto \mathbf{N}$ by $p(\sigma) = m(\sigma) + n(\sigma)$. We will prove in Proposition 2.43 that $p(\sigma) = l(\sigma)$.

LEMMA 2.30. *If $\sigma \in \mathscr{R}^r$ then $p(\sigma) = 0$ with equality if and only if $\sigma = v_r$.*

Proof. We have already remarked that both $\Psi^+_{01}(v_r)$ and $\Phi^+_{10}(v_r)$ are empty. So is $\Psi''(v_r)$. Thus $p(v_r) = 0$. Suppose conversely that $\sigma \in \mathscr{R}^r$ and that $p(\sigma) = 0$. Then $m(\sigma) = 0$ and $n(\sigma) = 0$. Since $m(\sigma) = 0$ we have $|\Psi^+_{01}(\sigma)| = 0 = |\Phi^+_{10}(\sigma)|$. Since $I(\sigma)$ and $J(\sigma)$ are r-subsets of $\mathbf{n}$, it follows from Lemma 2.25 that $I(\sigma) = \{1, \ldots, r\}$ and $J(\sigma) = \{n-r+1, \ldots, n\}$. Since $|\Psi''(\sigma)| = n(\sigma) = 0$ we have $i\sigma < j\sigma$ for all $1 \leqslant i < j \leqslant r$. Since $i\sigma \in J(\sigma) = \{n-r+1, \ldots, n\}$ and the map $i \mapsto i\sigma$ is bijective from $I(\sigma)$ to $J(\sigma)$ we must have $i\sigma = n-r+i$ for $1 \leqslant i \leqslant r$. Thus $\sigma = v_r$. □

In view of (2.15), (2.16), and (2.17) each $\sigma \in \mathscr{R}$ determines a partition of Δ^+ into five parts:

$$(2.31) \qquad \Delta^+ = \Psi^+_{00}(\sigma) \sqcup \Psi^+_{01}(\sigma) \sqcup \Psi^+_{10}(\sigma) \sqcup \Psi'(\sigma) \sqcup \Psi''(\sigma).$$

This replaces the two part partition (2.11) corresponding to an element $w \in W$. We need analogues of (2.13) for the sets in this partition. These will be proved in Lemma 2.36. If $w \in W$ then $I(w\sigma) = wI(\sigma)$ and $I(\sigma w) = I(\sigma)$. It follows that if $w \in W$ and $a, b \in \{0, 1\}$ then

$$(2.32) \qquad \Psi_{ab}(w\sigma) = w\Psi_{ab}(\sigma) \quad \text{and} \quad \Psi_{ab}(\sigma w) = \Psi_{ab}(\sigma).$$

LEMMA 2.33. *Suppose $a, b \in \{0, 1\}$, $\sigma \in \mathscr{R}$, and $s \in S$. Then*

$$s(\Psi^+_{ab}(\sigma) - \{\alpha_s\}) = \Psi^+_{ab}(s\sigma) - \{\alpha_s\} \quad \textit{and} \quad s(\Psi''(\sigma) - \{\alpha_s\}) = \Psi''(s\sigma) - \{\alpha_s\}.$$

Proof. Since $\Psi^+_{ab}(\sigma) - \{\alpha_s\} = (\Delta^+ - \{\alpha_s\}) \cap \Psi_{ab}(\sigma)$, the first assertion follows from (2.9) and (2.32). Suppose $(i, j) \in \Psi''(\sigma) - \{\alpha_s\}$. Then $i \in I(\sigma)$, $j \in I(\sigma)$, $i < j$ and $i\sigma > j\sigma$. Thus $si \in I(s\sigma)$, $sj \in I(s\sigma)$ and $si < sj$ because $(i, j) \neq \{\alpha_s\}$. Since $(si)(s\sigma) = (is)(s\sigma) = i\sigma > j\sigma = (js)(s\sigma) = (sj)(s\sigma)$ it follows that $(si, sj) \in \Psi''(s\sigma)$. Thus $s(\Psi''(\sigma) - \{\alpha_s\}) \subseteq \Psi''(s\sigma)$ and thus $s(\Psi''(\sigma) - \{\alpha_s\}) \subseteq \Psi''(s\sigma) - \{\alpha_s\}$. Now replace σ by $s\sigma$ to get the reverse inclusion. □

LEMMA 2.34. *Suppose $a, b \in \{0, 1\}$, $\sigma \in \mathscr{R}$, and $s \in S$. Then*

$$\alpha_s \in \Psi_{ab}(\sigma) \Leftrightarrow \alpha_s \in \Psi_{ba}(s\sigma) \quad \textit{and} \quad \alpha_s \in \Psi'(\sigma) \Leftrightarrow \alpha_s \in \Psi''(s\sigma).$$

Proof. To prove the first assertion suppose, for example, that $a = 0$ and $b = 1$. Write $\alpha_s = (k, k+1)$ where $1 \leqslant k \leqslant n - 1$. It follows from (2.32) that $\alpha_s \in \Psi_{01}(\sigma) \Leftrightarrow k \notin I(\sigma)$ and $k + 1 \in I(\sigma) \Leftrightarrow sk \in I(\sigma)$ and $s(k+1) \notin I(\sigma) \Leftrightarrow k \in I(s\sigma)$ and $k + 1 \notin I(s\sigma) \Leftrightarrow \alpha_s \in \Psi_{10}(s\sigma)$. The proof of the second assertion is similar. □

LEMMA 2.35. *Suppose $\sigma \in \mathscr{R}$ and $s \in S$.*

(1) *If $\alpha_s \in \Psi_{00}(\sigma)$ then $s\sigma = \sigma$.*
(2) *If $\alpha_s \in \Psi_{01}(\sigma)$ then*
  (2a) $\Psi^+_{01}(\sigma) = s\Psi^+_{01}(s\sigma) \sqcup \{\alpha_s\}$
  (2b) $\Psi^+_{10}(s\sigma) = s\Psi^+_{10}(\sigma) \sqcup \{\alpha_s\}$
  (2c) $\Psi''(s\sigma) = s\Psi''(\sigma)$.
(3) *If $\alpha_s \in \Psi_{10}(\sigma)$ then*
  (3a) $\Psi^+_{10}(\sigma) = s\Psi^+_{10}(s\sigma) \sqcup \{\alpha_s\}$
  (3b) $\Psi^+_{01}(s\sigma) = s\Psi^+_{01}(\sigma) \sqcup \{\alpha_s\}$
  (3c) $\Psi''(s\sigma) = s\Psi''(\sigma)$.
(4) *If $\alpha_s \in \Psi_{11}(\sigma)$ then*
  (4a) $\Psi^+_{01}(s\sigma) = s\Psi^+_{01}(\sigma)$
  (4b) $\Psi^+_{10}(s\sigma) = s\Psi^+_{10}(\sigma)$
  (4c) $\Psi''(s\sigma) = s\Psi''(\sigma) \sqcup \{\alpha_s\}$ *if* $\alpha_s \in \Psi'(\sigma)$
  (4d) $\Psi''(\sigma) = s\Psi''(s\sigma) \sqcup \{\alpha_s\}$ *if* $\alpha_s \in \Psi''(\sigma)$.

Proof. Write $\alpha_s = (k, k+1)$ where $1 \leqslant k \leqslant n - 1$. To prove (1) suppose $\alpha_s \in \Psi_{00}(\sigma)$. Then $k \notin I(\sigma)$ and $k + 1 \notin I(\sigma)$. Thus $si = i$ for all $i \in I(\sigma)$. Since $sE_{ij} = E_{si,j}$ for all $i, j \in \mathbf{n}$ we have $s\sigma = \sigma$. This proves (1). We will deduce (2)–(4) from (2.33), (2.34) and the fact that the union (2.31) is disjoint. Note that the unions in (2)–(4) are disjoint because $s\alpha_s \in \Delta^-$. To prove (2) suppose $\alpha_s \in \Psi_{01}(\sigma)$. Then $\alpha_s \in \Psi_{10}(s\sigma)$ by (2.34). Thus $\alpha_s \notin \Psi_{10}(\sigma)$ and thus $\alpha_s \notin \Psi_{01}(s\sigma)$. It follows from (2.33) that $s(\Psi^+_{01}(\sigma) - \{\alpha_s\}) = \Psi^+_{01}(s\sigma) - \{\alpha_s\} = \Psi^+_{01}(s\sigma)$ and $\Psi^+_{10}(s\sigma) - \{\alpha_s\} = s(\Psi^+_{10}(s\sigma) - \{\alpha_s\}) = s\Psi^+_{10}(s\sigma)$. This proves (2a) and (2b). Since $\alpha_s \in \Psi_{01}(\sigma)$ we have $\alpha_s \notin \Psi_{11}(\sigma)$ and thus $\alpha_s \notin \Psi_{11}(s\sigma)$. *A fortiori* $\alpha_s \notin \Psi''(\sigma)$

and $\alpha_s \notin \Psi''(s\sigma)$. Now (2c) follows from (2.33). To prove (3) suppose $\alpha_s \in \Psi_{10}(\sigma)$. Then $\alpha_s \in \Psi_{01}(s\sigma)$ by (2.34). Thus we may apply (2) with $s\sigma$ in place of s. This proves (3). To prove (4) suppose $\alpha_s \in \Psi_{11}(\sigma)$. Then $\alpha_s \notin \Psi_{01}(\sigma)$ and $\alpha_s \notin \Psi_{10}(\sigma)$ so $\alpha_s \notin \Psi_{01}(s\sigma)$ and $\alpha_s \notin \Psi_{10}(s\sigma)$ by (2.34). Now (4a) and (4b) follow from (2.33). If $\alpha_s \in \Psi'(\sigma)$ then $\alpha_s \notin \Psi''(\sigma)$ and also $\alpha_s \in \Psi''(s\sigma)$ by (2.34). Now (4c) follows from (2.33). If $\alpha_s \in \Psi''(\sigma)$ then $\alpha_s \in \Psi'(s\sigma)$ so (4d) follows from (4c) by replacing σ by $s\sigma$. □

LEMMA 2.36. *Suppose $\sigma \in \mathscr{R}$ and $s \in S$.*

(1) *If $\alpha_s \in \Psi_{00}(\sigma)$ then $s\sigma = \sigma$.*
(2) *If $\alpha_s \in \Psi_{01}(\sigma)$ then $m(s\sigma) = m(\sigma) - 1$ and $n(s\sigma) = n(\sigma)$.*
(3) *If $\alpha_s \in \Psi_{10}(\sigma)$ then $m(s\sigma) = m(\sigma) + 1$ and $n(s\sigma) = n(\sigma)$.*
(4) *If $\alpha_s \in \Psi_{11}(\sigma)$ then $m(s\sigma) = m(\sigma)$ and*

$$n(s\sigma) = \begin{cases} n(\sigma) + 1 & \text{if } \alpha_s \in \Psi'(\sigma) \\ n(\sigma) - 1 & \text{if } \alpha_s \in \Psi''(\sigma). \end{cases}$$

Proof. It follows from (2.32) that $m_{10}(s\sigma) = |\Psi_{10}^{+}(\sigma^* s)| = |\Psi_{10}^{+}(\sigma^*)| = m_{10}(\sigma)$. Thus we may replace m by m_{01} in each of (2)–(4). Now the assertions follow at once from Lemma 2.35. Note that the assertions (2b), (3b) and (4b) of Lemma 2.35 are not used in the proof. □

COROLLARY 2.37. *If $\sigma \in \mathscr{R}$ and $s \in S$ then $s\sigma = \sigma$ or $p(s\sigma) = p(\sigma) \pm 1$.*

Note that the assertions in Lemma 2.36 which compare $m(s\sigma)$ with $m(\sigma)$ may be expressed in a single formula: if $a, b \in \{0, 1\}$ then

(2.38) $\qquad \alpha_s \in \Psi_{ab}(\sigma) \Rightarrow m(s\sigma) - m(\sigma) = a - b.$

Recall that $\Phi_{ab}(\sigma) = \Psi_{ab}(\sigma^*)$. Since $s\sigma^* = (\sigma s)^*$ and $\mathrm{rk}(\sigma) = \mathrm{rk}(\sigma s)$ it follows from Lemma 2.36 that if $a, b \in \{0, 1\}$ then

(2.39) $\qquad \alpha_s \in \Phi_{ab}(\sigma) \Rightarrow m(\sigma s) - m(\sigma) = b - a.$

Note $n(\sigma^*) = n(\sigma)$ by (2.23). Also $\Phi'(\sigma) = \Psi'(\sigma^*)$ and $\Phi''(\sigma) = \Psi''(\sigma^*)$ by (2.19). Thus the analogue of Lemma 2.36 for right multiplication is:

LEMMA 2.40. *Suppose $\sigma \in \mathscr{R}$ and $s \in S$.*

(1) *If $\alpha_s \in \Phi_{00}(\sigma)$ then $\sigma s = \sigma$.*
(2) *If $\alpha_s \in \Phi_{01}(\sigma)$ then $m(\sigma s) = m(\sigma) - 1$ and $n(\sigma s) = n(\sigma)$.*
(3) *If $\alpha_s \in \Phi_{10}(\sigma)$ then $m(\sigma s) = m(\sigma) + 1$ and $n(\sigma s) = n(\sigma)$.*
(4) *If $\alpha_s \in \Phi_{11}(\sigma)$ then $m(\sigma s) = m(\sigma)$ and*

$$n(\sigma s) = \begin{cases} n(\sigma) + 1 & \text{if } \alpha_s \in \Phi'(\sigma) \\ n(\sigma) - 1 & \text{if } \alpha_s \in \Phi''(\sigma). \end{cases}$$

COROLLARY 2.41. *If $\sigma \in \mathscr{R}$ and $s \in S$ then $\sigma s = \sigma$ or $p(\sigma s) = p(\sigma) \pm 1$.*

If $w \in W$ and $w \neq 1$ then there exists $s \in S$ such that $n(sw) = n(w) - 1$ and there exists (a possibly different) $s \in S$ such that $n(ws) = n(w) - 1$. This means that we may decrease $l(w) = n(w)$ by *our* choice of left multiplication or right multiplication by an element of S. We have seen in the informal remarks at the beginning of this section that the situation in $\mathscr{R}$ is more restricted: we may not have our choice of left or right multiplication.

LEMMA 2.42. *If $\sigma \in \mathscr{R}^r$ and $\sigma \neq v_r$ then there exists $s \in S$ such that $p(s\sigma) = p(\sigma) - 1$ or $p(\sigma s) = p(\sigma) - 1$.*

Proof. Suppose first that $I(\sigma) \neq \{1,\dots,r\}$. Write $I(\sigma) = \{i_1,\dots,i_r\}$ where $i_1 < \cdots < i_r$. Then either (i) $i_1 > 1$ or (ii) there exists $v \in \{2,\dots,r\}$ such that $i_v - i_{v-1} > 1$. If (i) occurs let $k = i_1 - 1$. If (ii) occurs let $k = i_v - 1$. Then $k \notin I(\sigma)$ and $k + 1 \in I(\sigma)$ so $(k, k+1) \in \Psi_{01}(\sigma)$. Define $s \in S$ by $\alpha_s = (k, k+1)$. It follows from Lemma 2.36(2) that $m(s\sigma) = m(\sigma) - 1$ and $n(s\sigma) = n(\sigma)$ so $p(s\sigma) = p(\sigma) - 1$. Thus we may assume that $I(\sigma) = \{1,\dots,r\}$. If $J(\sigma) \neq \{n-r+1,\dots,n\}$, it follows by a similar argument using Lemma 2.40(3) that there exists $s \in S$ with $p(\sigma s) = p(\sigma) - 1$. Thus we may assume that $I(\sigma) = \{1,\dots,r\}$ and that $J(\sigma) = \{n-r+1,\dots,n\}$. Then $\sigma = \Sigma_{i=1}^r E_{i,i\sigma}$ where $\{1\sigma,\dots,r\sigma\} = \{n-r+1,\dots,n\}$. Since $\sigma \neq v_r$ there exists $k \in \{1,\dots,r-1\}$ such that $k\sigma > (k+1)\sigma$. Thus $(k, k+1) \in \Psi''(\sigma)$. Define $s \in S$ by $\alpha_s = (k, k+1)$. It follows from Lemma 2.36(4) that $p(s\sigma) = p(\sigma) - 1$. □

PROPOSITION 2.43. *If $\sigma \in \mathscr{R}^r$ then $l(\sigma) = m(\sigma) + n(\sigma)$.*

Proof. First argue $p(\sigma) \leqslant l(\sigma)$ by induction on $l(\sigma)$. Write $\sigma = wv_rw'$ where $l(w) + l(w') = l(\sigma)$. If $l(\sigma) = 0$ then $w = 1 = w'$ so $\sigma = v_r$ and thus $p(\sigma) = 0$ by Lemma 2.30. Suppose $l(\sigma) > 0$. Then $l(w) > 0$ or $l(w') > 0$. Without loss of generality we may assume that $l(w) > 0$. Write $w = sw''$ where $s \in S$, $w'' \in W$ and $l(w'') = l(w) - 1$. Let $\tau = s\sigma = w''v_rw'$. Then $l(\tau) < l(\sigma)$. By Corollary 2.37 and the induction hypothesis we have $p(\sigma) \leqslant p(\tau) + 1 \leqslant l(\tau) + 1 \leqslant l(\sigma)$.

Now argue the reverse inequality $l(\sigma) \leqslant p(\sigma)$ by induction on $p(\sigma)$. If $p(\sigma) = 0$ then $\sigma = v_r$ by Lemma 2.30 so $l(\sigma) = 0$. If $p(\sigma) > 0$ then $\sigma \neq v_r$ so by Lemma 2.42 there exists $s \in S$ such that $p(s\sigma) < p(\sigma)$ or $p(\sigma s) < p(\sigma)$. Without loss of generality assume that $p(s\sigma) < p(\sigma)$. Then, by induction, $l(\sigma) \leqslant l(s\sigma) + 1 \leqslant p(s\sigma) + 1 \leqslant p(\sigma)$. □

COROLLARY 2.44. *Suppose $\sigma \in \mathscr{R}$ and $s \in S$. If $l(s\sigma) = l(\sigma)$ then $\sigma s = \sigma$. If $l(\sigma s) = l(\sigma)$ then $\sigma s = \sigma$.*

In view of Proposition 2.43 the precise circumstances in which $l(s\sigma) = l(\sigma) + 1$ and $l(s\sigma) = l(\sigma) - 1$ are given by Lemma 2.36. Similarly the precise circumstances in which $l(\sigma s) = l(\sigma) + 1$ and $l(\sigma s) = l(\sigma) - 1$ are given by Lemma 2.40. Note that although $l(w) = l(w^{-1})$ for all $w \in W$ the analogous assertion $l(\sigma^*) = l(\sigma)$ for all $\sigma \in \mathscr{R}$ is false. In fact, since $n(\sigma^*) = n(\sigma)$ Lemma 2.29 shows that we rarely have $l(\sigma^*) = l(\sigma)$.

THEOREM 2.45. *Let $\mathscr{R}$ be the rook monoid, let l be the length function on $\mathscr{R}$ and let q be an indeterminate. If $0 \leqslant r \leqslant n$ then*

$$\sum_{\sigma \in \mathscr{R}^r} q^{l(\sigma)} = [r]! \begin{bmatrix} n \\ r \end{bmatrix}^2.$$

Proof. Let $W_r \subseteq \mathrm{GL}_r(F)$ be the group of $r \times r$ permutation matrices. Define a map $h\colon \mathscr{R}^r \to W_r$ by $h(\sigma) = \sigma^\star$ where, as in the informal remarks at the beginning of this section, $\sigma^\star$ is obtained from σ by deleting the rows and columns consisting of zeros. Then $n(\sigma)$ is the number $n(\sigma^\star)$ of inversions of the permutation matrix $\sigma^\star$. For $z \in W_r$ define $\mathscr{R}(z) \subseteq \mathscr{R}^r$ by $\mathscr{R}(z) = \{\sigma \in \mathscr{R} \mid h(\sigma) = z\}$. It follows from Proposition 2.43 that

$$\text{(2.46)} \qquad \sum_{\sigma \in \mathscr{R}^r} q^{l(\sigma)} = \sum_{z \in W_r} q^{n(z)} \sum_{\sigma \in \mathscr{R}(z)} q^{m(\sigma)}.$$

Let $\mathscr{A}$ be the set of r-subsets of $\mathbf{n}$. For fixed z the map $\sigma \to (I(\sigma), J(\sigma))$ is bijective from $\mathscr{R}(z)$ to $\mathscr{A} \times \mathscr{A}$. Since $m(\sigma) = m_{01}(\sigma) + m_{10}(\sigma) = m_{01}(I(\sigma)) + m_{10}(J(\sigma))$ we have

$$\text{(2.47)} \qquad \sum_{\sigma \in \mathscr{R}(z)} q^{m(\sigma)} = \left(\sum_{K \in \mathscr{A}} q^{m_{01}(K)}\right) \cdot \left(\sum_{K \in \mathscr{A}} q^{m_{10}(K)}\right).$$

Thus

$$\text{(2.48)} \qquad \sum_{\sigma \in \mathscr{R}^r} q^{l(\sigma)} = \left(\sum_{z \in W_r} q^{n(z)}\right) \cdot \left(\sum_{K \in \mathscr{A}} q^{m_{01}(K)}\right) \cdot \left(\sum_{K \in \mathscr{A}} q^{m_{10}(K)}\right).$$

The first factor on the right is $[r]!$ by (1.1) with r in place of n. The second and third factors on the right are equal. Let $e_r(x_1, \ldots, x_n)$ be the rth elementary symmetric function of indeterminates $x_1, \ldots, x_n$. Then

$$\text{(2.49)} \qquad \sum_{K \in \mathscr{A}} q^{m_{01}(K)} = q^{-r(r-1)/2} e_r(1, q, \ldots, q^{n-1}) = \begin{bmatrix} n \\ r \end{bmatrix}$$

where the second equality is an identity of Euler [14, p. 18]. □

The inequality in the following lemma will be used in Section 4 in the proof of the existence of the ring $H(M, B)$.

LEMMA 2.50. *If $\sigma \in \mathscr{R}$ then $l(v\sigma) \leqslant l(\sigma)$.*

Proof. Note that we get $v\sigma$ from σ by replacing row i by row $i + 1$ for $i = 1, \ldots, n - 1$ and replacing row n by a row of zeros. Thus, if $i \in I(v\sigma)$ then $i + 1 \in I(\sigma)$. Also $J(v\sigma) \subseteq J(\sigma)$. It follows from (2.28) that $m(v\sigma) \leqslant m(\sigma)$. Note that $I(v\sigma) \subseteq I(v) = \{1, \ldots, n-1\}$. If $(i,j) \in \Psi''(v\sigma)$ then (2.17) implies $i, j \in I(v\sigma)$ and $i < j$ and $iv\sigma > jv\sigma$. Then $i + 1 < j + 1$ and $(i+1)\sigma > (j+1)\sigma$ so $(i+1, j+1) \in \Psi''(\sigma)$. Thus from (2.22) we have $n(v\sigma) = |\Psi''(v\sigma)| \leqslant |\Psi''(\sigma)| = n(\sigma)$. Now the assertion follows from Proposition 2.43. $\square$

3. THE TITS SYSTEM IN $\mathrm{M}_n(F)$

Let F be a field. Let $G = \mathrm{GL}_n(F)$. Let $T \subset G$ be the group of diagonal matrices, let $U \subset G$ be the group of upper unitriangular matrices and let $B = TU$ be the group of upper triangular matrices. Let $M = \mathrm{M}_n(F)$. Since M is a reductive monoid it follows from Renner's general results [20], in case F is algebraically closed, that M has a Bruhat decomposition in which $\mathscr{R}$ plays the role of the Weyl group. In case $M = \mathrm{M}_n(F)$ this decomposition may be done over any field F.

In this section we give a formula for multiplication of the sets $B\sigma B$ in terms of the length function $l(\sigma)$ introduced in Section 2. We also give a refinement of the Bruhat decomposition for M analogous to Chevalley's refinement $BwB = BwU''_w$ of the Bruhat decomposition for G. This depends on the sets of roots introduced in Section 2. In case the ground field $F = \mathbf{F}_q$ is finite we get a formula for $|B\sigma B|$ analogous to Chevalley's formula $|BwB| = |B|q^{l(w)}$. This formula is used in Section 4 to describe the multiplication in the ring $H(M, B)$. As a by-product of the results in this section we get a second proof of Proposition (2.45). To keep this paper self-contained we begin with a short elementary proof of the Bruhat decomposition in case $M = \mathrm{M}_n(F)$.

PROPOSITION 3.1. *$M = \bigsqcup_{\sigma \in \mathscr{R}} B\sigma B$. If σ, $\sigma' \in \mathscr{R}$ and $B\sigma B = B\sigma' B$ then $\sigma = \sigma'$.*

Proof. For $(i,j) \in \Delta$ and $t \in F$ let $x_{ij}(t) = 1 + tE_{ij}$ where 1 denotes the identity matrix. If $a \in M$ then $a \mapsto x_{ij}(t)a$ adds t times row j to row i and $a \mapsto ax_{ij}(t)$ adds t times column i to column j. We want to keep the $x_{ij}(t)$ in B so we allow only $i < j$. This means that addition of rows may be done only from below to above and addition of columns may be done only from left to right. If all the entries in the first column are zero then move to the second column. If the first column has a non-zero entry let j_1 be the largest integer such that $a_{j_1 1} \neq 0$. Pivot on the $(j_1, 1)$ entry of a to conclude that there exist u, $v \in U \subseteq B$ such that $a' = uav$ has zero entries in column 1 and row j_1 except for the entry $(j_1, 1)$. If we multiply by an element of T we may arrange to make this entry equal to 1. Now work on the second column. If all entries in the second column are zero then move to the third column. Otherwise let j_2 be the largest integer such that $a'_{j_2 2} \neq 0$. Note that $j_2 \neq j_1$. Pivot on the $(j_2, 2)$

entry of a' to conclude that there exist $u', v' \in B$ such that $u'a'v'$ has zero entries in rows j_1, j_2 and columns 1, 2 except perhaps for the entries $(j_1, 1)$ and $(j_2, 2)$ which, if not 0 may be chosen to be 1. Continue in this way and arrive at an element of $\mathscr{R}$. The proof of uniqueness is similar. Suppose σ, $\sigma' \in \mathscr{R}$ and $\sigma' \in B\sigma B$. Then σ' may be obtained from σ by a sequence of elementary row operations in which addition of rows is done from below to above and addition of columns is done from left to right. Thus if the first column of σ consists of zeros, the same is true for σ'. If the first column of σ contains a 1 in position $(j_1, 1)$ then σ' has a non-zero entry in position $(j_1, 1)$ and hence σ' has the same first column as σ. Now show in similar fashion, that σ' and σ agree in columns $2, \ldots, n$. □

If $(i, j) \in \Delta$ let $X_{ij} = \{x_{ij}(t) \mid t \in F\}$ be the corresponding root subgroup. We recall some facts about these subgroups which may be traced to Chevalley [6]. The formulation here is taken from [4] and [25]. A subset Γ of Δ is *closed* if it has the property: $(i, j) \in \Gamma$, $(j, k) \in \Gamma$ and $i \neq k \Rightarrow (i, k) \in \Gamma$. This condition is equivalent, with our definition of Δ as a set of pairs, to the usual condition 'α, $\beta \in \Gamma$ and $\alpha + \beta \in \Delta \Rightarrow \alpha + \beta \in \Gamma$'. If $\Gamma \subseteq \Delta^+$ let U_Γ be the subgroup of U generated by the X_{ij} with $(i, j) \in \Gamma$. If Γ is a closed subset of Δ^* then every $u \in U_\Gamma$ may be written uniquely in the form

$$(3.2) \qquad u = \prod_{(i,j)\in\Gamma} x_{ij}(t_{ij})$$

where $t_{ij} \in F$ and the product is taken in *any* fixed order. If $\Delta^+ = \Gamma' \sqcup \Gamma''$ where Γ', Γ'' are closed subsets of Δ^+ then

$$(3.3) \qquad U = U_{\Gamma'} U_{\Gamma''} \quad \text{and} \quad U_{\Gamma'} \cap U_{\Gamma''} = 1.$$

Suppose $w \in W$. Then $\Phi'(w)$, $\Phi''(w)$ are closed subsets of Δ^+. Define subgroups U'_w U''_w of U by $U'_w = U_{\Phi'(w)}$ and $U''_w = U_{\Phi''(w)}$. Since $\Delta^+ = \Phi'(w) \sqcup \Phi''(w)$ we have

$$(3.4) \qquad U'_w U''_w = U = U''_w U'_w \quad \text{and} \quad U'_w \cap U''_w = 1.$$

Every element in BwB may be written in the form bwu'' where $b \in B$ and $u'' \in U''_w$ are uniquely determined. We will use the partition (2.31) to define subgroups U'_σ and U''_σ for $\sigma \in \mathscr{R}$ and show that they have analogous properties.

DEFINITION 3.5. If $\sigma \in \mathscr{R}$ define

$$\Theta'(\sigma) = \Phi^+_{00}(\sigma) \sqcup \Phi^+_{01}(\sigma) \sqcup \Phi'(\sigma)$$

$$\Theta''(\sigma) = \Phi^+_{10}(\sigma) \sqcup \Phi''(\sigma).$$

Note that if $\sigma = w \in W$ then $\Theta'(\sigma) = \Phi'(w)$ and $\Theta''(\sigma) = \Phi''(w)$.

LEMMA 3.6. *If $\sigma \in \mathscr{R}$ then $\Theta'(\sigma)$ and $\Theta''(\sigma)$ are closed subsets of Δ^+ and $\Delta^+ = \Theta'(\sigma) \bigsqcup \Theta''(\sigma)$.*

Proof. Suppose $(i,j) \in \Theta'(\sigma)$ and $(j,k) \in \Theta'(\sigma)$ and $i \neq k$. If $(i,j) \in \Phi^+_{00}(\sigma) \bigsqcup \Phi^+_{01}(\sigma)$ then $i \notin J(\sigma)$ so $(i,k) \in \Phi^+_{00}(\sigma) \bigsqcup \Phi^+_{01}(\sigma) \subseteq \Theta'(\sigma)$ because $i \neq k$. Suppose $(i,j) \in \Phi'(\sigma)$. Then $i \in J(\sigma)$, $j \in J(\sigma)$ and $\sigma i < \sigma j$. Since $j \in J(\sigma)$ and $(j,k) \notin \Theta'(\sigma)$ we must have $(j,k) \in \Phi'(\sigma)$. Thus $k \in J(\sigma)$ and $\sigma j < \sigma k$. Thus $i \in J(\sigma)$, $k \in J(\sigma)$ and $\sigma i < \sigma k$ so $(i,k) \in \Phi'(\sigma) \subseteq \Theta'(\sigma)$. Thus $\Theta'(\sigma)$ is closed. Suppose $(i,j) \in \Theta''(\sigma)$ and $(j,k) \in \Theta''(\sigma)$ and $i \neq k$. Then $i \in J(\sigma)$ and $j \in J(\sigma)$. Since $j \in J(\sigma)$ we have $(i,j) \notin \Phi^+_{01}(\sigma)$. Thus $(i,j) \in \Phi''(\sigma)$. If $k \notin J(\sigma)$ then, since $i \neq k$, we have $(i,k) \in \Phi^+_{10}(\sigma) \subseteq \Theta'(\sigma)$. If $k \in J(\sigma)$ then $(j,k) \in \Phi''(\sigma)$ so $\sigma j > \sigma k$. Thus $\sigma i > \sigma k$ so $(i,k) \in \Phi''(\sigma) \subseteq \Theta''(\sigma)$. Thus $\Theta''(\sigma)$ is closed. The assertion $\Delta^+ = \Theta'(\sigma) \bigsqcup \Theta''(\sigma)$ follows from (2.31) with σ^* in place of σ. □

Define subgroups U'_σ, U''_σ of U by

(3.7) $$U'_\sigma = U_{\Theta'(\sigma)} \quad \text{and} \quad U''_\sigma = U_{\Theta''(\sigma)}.$$

It follows from (3.3) that

(3.8) $$U'_\sigma U''_\sigma = U = U''_\sigma U'_\sigma \quad \text{and} \quad U'_\sigma \cap U''_\sigma = 1.$$

If $\sigma = w \in W$ then U'_σ and U''_σ have their earlier meaning and (3.8) agrees with (3.4). We need the following elementary formulas in $\mathrm{M}_n(F)$. If $i, j \in \mathbf{n}$ then

(3.9) $$E_{ij}\sigma = \begin{cases} E_{i,j\sigma} & \text{if } j \in I(\sigma) \\ 0 & \text{otherwise} \end{cases} \qquad \sigma E_{ij} = \begin{cases} E_{\sigma i,j} & \text{if } i \in J(\sigma) \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

(3.10) $$x_{ij}(t)\sigma = \sigma \quad \text{if } j \notin I(\sigma)$$
$$\sigma x_{ij}(t) = \sigma \quad \text{if } i \notin J(\sigma)$$

and

(3.11) $$x_{ij}(t)\sigma = \sigma x_{i\sigma,j\sigma}(t) \quad \text{if } i, j \in I(\sigma)$$
$$\sigma x_{ij}(t) = x_{\sigma i,\sigma j}(t)\sigma \quad \text{if } i, j \in J(\sigma).$$

PROPOSITION 3.12. *Suppose $\sigma \in \mathscr{R}$ and $s \in S$. Then*

$$BsB \cdot B\sigma B = \begin{cases} B\sigma B & \text{if } \alpha_s \in \Psi_{00}(\sigma) \\ Bs\sigma B & \text{if } \alpha_s \in \Psi_{10}(\sigma) \bigsqcup \Psi'(\sigma) \\ Bs\sigma B \bigsqcup B\sigma B & \text{if } \alpha_s \in \Psi_{01}(\sigma) \bigsqcup \Psi''(\sigma). \end{cases}$$

Proof. If $Bs\sigma B = B\sigma B$ then $s\sigma = \sigma$ by Proposition 3.1. It follows from

(2.36) or direct computation that $\alpha_s \in \Psi_{00}(\sigma)$. Thus $\alpha_s \in \Psi_{01}(\sigma) \sqcup \Psi''(\sigma) \Rightarrow BsB \neq Bs\sigma B$. We argue the Lemma as in [6]. We may replace the left-hand side by $sB\sigma$ and replace equality by inclusion provided we show for $\alpha_s \in \Psi_{01}(\sigma) \sqcup \Psi''(\sigma)$ that $s\beta\sigma$ meets both orbits. Write $U = U_s' U_s''$. We have $\Psi''(s) = \{\alpha_s\}$ and $\Psi'(s) = \Delta^+ - \{\alpha_s\}$. It follows from (2.9) that $s\Psi'(s) = \Psi'(s)$ so $sU_s's = U_s'$. Define k by $\alpha_s = (k, k+1)$. Then $U_s'' = X_{k,k+1}$. Thus $sB = sTU = TsU_s'U_s'' = T \cdot sU_s's \cdot sX_{k,k+1} \subseteq BsX_{k,k+1}$. If $\alpha_s \in \Psi_{00}(\sigma) \sqcup \Psi_{10}(\sigma)$ then $k+1 \notin I(\sigma)$ so $X_{k,k+1}\sigma = \sigma$ by (3.10). Thus $sB\sigma \subseteq Bs\sigma \subseteq Bs\sigma B$. If $\alpha_s \in \Psi_{00}(\sigma)$ then $s\sigma = \sigma$ by (2.35) so $sB\sigma \subseteq B\sigma B$. Suppose $\alpha_s \in \Psi_{01}(\sigma)$. We must show that $sx_{k,k+1}(t)\sigma \in BsB \cup Bs\sigma B$. This is clear for $t = 0$. Suppose $t \neq 0$. Let $h \in \mathrm{GL}_n(F)$ be the diagonal matrix with entries $-t^{-1}, t$ in positions $k, k+1$ and the other diagonal entries equal to 1. Then

$$(3.13) \qquad sx_{k,k+1}(t) = hx_{k,k+1}(-t)x_{k+1,k}(t^{-1}).$$

This identity may be checked in $\mathrm{GL}_2(F) \hookrightarrow \mathrm{GL}_n(F)$. Since $\alpha_s \in \Psi_{01}(\sigma)$ we have $k \notin I(\sigma)$ so $x_{k+1,k}(t^{-1})\sigma = \sigma$ by (3.10). Thus $sx_{k,k+1}(t)\sigma = hx_{k,k+1}(-t)\sigma \in B\sigma B$ as desired. Suppose $\alpha_s \in \Psi_{11}(\sigma)$. Then k, $k+1 \in I(\sigma)$ so by (3.11) we have $x_{k,k+1}(t)\sigma = \sigma x_{k\sigma,(k+1)\sigma}(t)$. If $\alpha_s \in \Psi'(\sigma)$ then $k\sigma < (k+1)\sigma$ so $sx_{k,k+1}(t)\sigma \in Bs\sigma B$. If $\alpha_s \in \Psi''(\sigma)$ then $\alpha_s \in \Psi'(s\sigma)$ by (2.34) so, arguing with $s\sigma$ in place of σ we have $sBs\sigma \subseteq B\sigma B$. Since $sBs \subseteq B \cup BsB$ by (1.14), we have $sB\sigma = sBs \cdot s\sigma \subseteq (B \cup BsB)s\sigma \subseteq Bs\sigma B \cup B\sigma B$. □

We may reformulate this result in terms of the length function defined in Section 2 as follows.

PROPOSITION 3.14. *Suppose $\sigma \in \mathscr{R}$ and $s \in S$. Then*

$$BsB \cdot B\sigma B = \begin{cases} B\sigma B & \text{if } l(s\sigma) = l(\sigma) \\ Bs\sigma B & \text{if } l(s\sigma) = l(\sigma) + 1 \\ Bs\sigma B \cup B\sigma B & \text{if } l(s\sigma) = l(\sigma) - 1. \end{cases}$$

Proof. This follows from Proposition 3.12, the behavior of the functions $m(\sigma)$ and $n(\sigma)$ under left multiplication $\sigma \mapsto s\sigma$ determined in Lemma 2.36, and Proposition 2.43 which asserts that $l(\sigma) = m(\sigma) + n(\sigma)$. □

LEMMA 3.15. *If $\sigma \in \mathscr{R}$ then $B\sigma B = B\sigma U_\sigma''$. Furthermore, if $b_1\sigma u_1 = b_2\sigma u_2$ where b_1, $b_2 \in B$ and u_1, $u_2 \in U_\sigma''$ then $u_1 = u_2$ and $b_1\sigma = b_2\sigma$.*

Proof. We show first that if $\sigma \in \mathscr{R}$ and $u \in U$ then

$$(3.16) \qquad \sigma u \in U\sigma \Leftrightarrow u \in U_\sigma'.$$

This is the main part of the argument. Suppose $u \in U_\sigma'$. Take $\Gamma = \Theta'(\sigma)$ in (3.2) and write $u = \Pi x_{ij}(t_{ij})$ where the order of the factors is chosen so that the terms with $(i,j) \in \Phi_{00}^+(\sigma) \sqcup \Phi_{01}^+(\sigma)$ appear on the left. By (3.10) we have $\sigma x_{ij}(t) = x_{ij}(t)$ for $(i,j) \in \Phi_{00}^+(\sigma) \sqcup \Phi_{01}^+(\sigma)$. Thus $\sigma u = \sigma \Pi x_{ij}(t_{ij})$ where the product is over $(i,j) \in \Phi'(\sigma)$. If $(i,j) \in \Phi'(\sigma)$ then $i \in J(\sigma)$, $j \in J(\sigma)$ and $\sigma i < \sigma j$. Then $\sigma j \in I(\sigma)$ and $(\sigma j)\sigma = j$. It follows from (3.4) that if $t \in F$ then $\sigma x_{ij}(t) = x_{\sigma i, j}(t) = x_{\sigma i, \sigma j}(t)\sigma \in U\sigma$. Thus $\sigma u \in U'_\sigma$.

Conversely, suppose $u \in U$ and $\sigma u \in U\sigma$. Write $u = u'u''$ where $u' \in U'_\sigma$ and $u'' \in U''_\sigma$. Then $\sigma u' \in U\sigma$ by the first part of the argument. Thus $\sigma u'' \in U\sigma$. If $(i,j) \in \Phi_{10}^+(\sigma)$ then $x_{ij}(t)\sigma^* = \sigma^*$ by (3.10). Write $u'' = yz$ where $y \in U_{\Phi''(\sigma)}$ and z is a product of factors $x_{ij}(t)$ with $(i,j) \in \Phi_{10}^+(\sigma)$. Then $z\sigma^* = \sigma^*$ so $\sigma y \sigma^* = \sigma u \sigma^* \in U\sigma\sigma^*$. Since $\sigma\sigma^*$ is an idempotent diagonal matrix it follows that $\sigma y \sigma^*$ is upper triangular. If Γ is a closed subset of Δ^+ and $v \in U_\Gamma$, then it follows by induction on the number of factors $x_{ij}(t)$ of v which are different from 1 that we may write

$$v = 1 + \sum_{(i,j)\in\Gamma} t_{ij}E_{ij} \tag{3.17}$$

for suitable $t_{ij} \in F$. Apply (3.17) with $\Gamma = \Phi''(\sigma)$ and $v = y$. Since $j\sigma^* = \sigma j$ for $j \in J(\sigma)$ we have

$$\sigma y \sigma^* = \sigma\sigma^* + \sum_{(i,j)\in\Phi''(\sigma)} t_{ij}E_{\sigma i, \sigma j}.$$

Since $\sigma y \sigma^* - \sigma\sigma^*$ is upper triangular and $\sigma i > \sigma j$ for $(i,j) \in \Phi''(\sigma)$ it follows that $t_{ij} = 0$ for all $(i,j) \in \Phi''(\sigma)$. Thus $y = 1$ and $z = u'' \in U''_\sigma$. Now apply (3.17) with $\Gamma = \Phi_{10}^+(\sigma)$ and $v = z$. Write

$$z = 1 + \sum_{(i,j)\in\Phi_{10}^+(\sigma)} t_{ij}E_{ij}.$$

The indices j which occur here are not in $J(\sigma)$. On the other hand, the elements of $U\sigma$ are F-linear combinations of elements E_{ij} with $j \in J(\sigma)$. Thus $t_{ij} = 0$ for all $(i,j) \in \Phi_{10}^+(\sigma)$ so $z = 1$. Thus $u'' = yz = 1$ and $u = u' \in U'_\sigma$. This completes the proof of (3.16). Since $\sigma T = T\sigma$ it follows from (3.8) and the $\Leftarrow$ part of (3.16) that

$$B\sigma B = B\sigma TU = B\sigma U'_\sigma U''_\sigma \subseteq B\sigma U''_\sigma \subseteq B\sigma B.$$

Thus $B\sigma B = B\sigma U''_\sigma$. It remains to prove the uniqueness. Suppose $b_1\sigma u_1 = b_2\sigma u_2$ where $b_1, b_2 \in B$ and $u_1, u_2 \in U''_\sigma$. Then $\sigma u_2 u_1^{-1} \in B\sigma$. It follows from the $\Rightarrow$ part of (3.16) that $u_2u_1^{-1} \in U'_\sigma$. Since $U'_\sigma \cap U''_\sigma = 1$ we have $u_1 = u_2$ and thus $b_1\sigma = b_2\sigma$. □

If $\sigma \in \mathscr{R}$ then $b\sigma = \sigma$ need not imply $b = 1$. Thus the uniqueness statement in the preceding lemma is, of necessity, weaker than the corresponding statement for $w \in W$. In the rest of this section we assume that the field $F = \mathbf{F}_q$ is finite.

LEMMA 3.18. *Suppose $F = \mathbf{F}_q$ and $\sigma \in \mathcal{R}^r$. Then*

$$|B\sigma B| = (q-1)^r q^{r(r-1)/2} q^{l(\sigma)}.$$

Proof. Write $\sigma = \Sigma_{v=1}^r E_{i_v j_v}$. Let $b \in B$ and write $b = \Sigma_{1 \leqslant i \leqslant j \leqslant n} t_{ij} E_{ij}$ where $t_{ii} \in \mathbf{F}_q^\times$ and $t_{ij} \in \mathbf{F}_q$ for $i < j$. Then

$$(3.19) \qquad b\sigma = \sum_{v=1}^{r} \sum_{1 \leqslant i \leqslant i_v} t_{i i_v} E_{i j_v}.$$

Thus

$$(3.20) \qquad |B\sigma| = (q-1)^r q^{\sum_{i \in I(\sigma)} (i-1)}.$$

It follows from Lemma 2.25 that

$$(3.21) \qquad |B\sigma| = (q-1)^r q^{r(r-1)/2} q^{m_{01}(\sigma)}.$$

Choose $\Gamma = \Theta''(\sigma) = \Phi_{10}^+(\sigma) \sqcup \Phi''(\sigma)$ in (3.2). From (2.27) we have $|\Phi_{10}^+(\sigma)| = m_{10}(\sigma)$. From (2.19) and (2.23) we have $|\Phi''(\sigma)| = |\Psi''(\sigma^*)| = n(\sigma^*) = n(\sigma)$. Now the uniqueness in (3.2) gives

$$(3.22) \qquad |U_\sigma''| = q^{m_{10}(\sigma) + n(\sigma)}.$$

It follows from (3.15) that

$$(3.23) \qquad |B\sigma B| = |B\sigma|\,|U_\sigma''| = (q-1)^r q^{r(r-1)/2} q^{m_{01}(\sigma) + m_{10}(\sigma) + n(\sigma)}.$$

Now the desired assertion follows from Proposition 2.43. □

It follows from the Bruhat decomposition (3.1) that

$$(3.24) \qquad |M^r| = \sum_{\sigma \in \mathcal{R}^r} |B\sigma B|.$$

Thus (3.18) and (1.5) give a proof of the formula (2.45) in case q is a prime power. Since the formula holds for all prime powers q this gives a second proof of the polynomial identity (2.45).

4. THE IWAHORI RING $H(M, B)$ AND THE GENERIC ALGEBRA $A(\mathcal{R})$

Let M be a finite monoid. Let G be the group of units of M. Let K be a field of characteristic zero. Let $K[M]$ denote the monoid algebra of M with coefficients in K. Let B be a subgroup of G. Let

$$(4.1) \qquad \varepsilon = \varepsilon_B = \frac{1}{|B|} \sum_{b \in B} b$$

be the corresponding idempotent in the group algebra $K[G] \subseteq K[M]$. Then $\varepsilon K[G]\varepsilon \subseteq \varepsilon K[M]\varepsilon$ are K-algebras with the same identity element ε. The algebra $\varepsilon K[G]\varepsilon$ controls the decomposition of the permutation representation of G on G/B ([8], [10]). The group $B \times B$ acts on M by $(b, b')x = bxb'^{-1}$. Let $B\backslash M/B$ denote the set of orbits for this action. Thus

(4.2) $$M = \bigsqcup_{D \in B\backslash M/B} D.$$

Any orbit which meets G is included in G. These orbits are the $(B:B)$-double cosets. For $D \in B\backslash M/B$ define $[D] \in K[M]$ by

(4.3) $$[D] = \sum_{x \in D} x.$$

If $b \in B$ then $bD = D = Db$. Thus $\varepsilon[D] = [D] = [D]\varepsilon$ so that $[D] \in \varepsilon K[M]\varepsilon$. The set $\{[D]: D \in B\backslash M/B\}$ is a K-basis for $\varepsilon K[M]\varepsilon$. The structure constants in the multiplication table for the subalgebra $\varepsilon K[G]\varepsilon$ with respect to the basis $\{[D]: D \in B\backslash G/B\}$ are multiples of $|B|$. Thus there is a distinguished $\mathbf{Z}$-order

(4.4) $$H(G, B) = \sum_{D \in B\backslash G/B} \mathbf{Z}T_D$$

where

(4.5) $$T_D = |B|^{-1}[D].$$

The structure constants in the multiplication table with respect to the basis $\{T_D \mid D \in B\backslash G/B\}$ are in $\mathbf{N}$. If we replace G by M and try to define an analogous $\mathbf{Z}$-order in $\varepsilon K[M]\varepsilon$ we are faced with the problem of suitably normalizing the basis elements $[D]$ as in (4.5). Although there exist integers $m(D, D'; D'')$ with

(4.6) $$[D][D'] = \sum_{D'' \in B\backslash M/B} m(D, D'; D'')[D'']$$

the structure constants $m(D, D'; D'')$ need not be integer multiples of $|B|$. Nevertheless we can make progress in the special case $M = \mathrm{M}_n(\mathbf{F}_q)$. Henceforth let $M = \mathrm{M}_n(\mathbf{F}_q)$ and let $G = \mathrm{GL}_n(\mathbf{F}_q)$. Proposition 3.1 asserts that the orbits have the form $D = B\sigma B$ with $\sigma \in \mathscr{R}$. Let $\pi: K[M] \to K$ be the one-dimensional representation defined by $\pi(\sigma) = 1$ for all $\sigma \in M$. Let

(4.7) $$\mathrm{ind}: \varepsilon K[M]\varepsilon \to K$$

be the representation of $\varepsilon K[M]\varepsilon$ obtained by restricting π. Thus $\mathrm{ind}[D] = |D|$. If $D = BwB$ is a $(B:B)$-double coset, with $w \in W$ write $T_w = T_D$. Since $|BwB| = |BwU''_w| = q^{l(w)}$ we have

(4.8) $$\mathrm{ind}(T_w) = q^{l(w)}.$$

Suppose now that $D = B\sigma B$ is a $B \times B$ orbit on M, with $\sigma \in \mathscr{R}$. Formula (4.8) suggests that we define a **Q**-multiple T_σ of $[D]$ in such a way that $\operatorname{ind}(T_\sigma) = q^{l(\sigma)}$. If $\sigma \in \mathscr{R}^r$ we define

$$(4.9) \qquad T_\sigma = (q-1)^{-r} q^{-r(r-1)/2}[B\sigma B].$$

In the case $r = n$ this agrees with the earlier normalization (4.8). It follows from (3.18) that if $\sigma \in \mathscr{R}^r$ then

$$\operatorname{ind}(T_\sigma) = (q-1)^{-r} q^{-r(r-1)/2} |B\sigma B| = q^{l(\sigma)}.$$

Thus

$$(4.10) \qquad \operatorname{ind}(T_\sigma) = q^{l(\sigma)}$$

for all $\sigma \in \mathscr{R}$. Define a free **Z**-module $H(M, B)$ by

DEFINITION 4.11. $H(M,B) = \bigoplus_{\sigma \in \mathscr{R}} \mathbf{Z} T_\sigma$.

THEOREM 4.12. *The* **Z**-*module* $H(M,B)$ *is a ring generated by the* T_s *for* $s \in S$ *and* T_ν, *where* $\nu = E_{12} + E_{23} + \cdots + E_{n-1,n}$. *Furthermore, we have*

$$T_s T_\sigma = \begin{cases} qT_\sigma & \text{if } l(s\sigma) = l(\sigma) \\ T_{s\sigma} & \text{if } l(s\sigma) = l(\sigma) + 1 \\ qT_{s\sigma} + (q-1)T_\sigma & \text{if } l(s\sigma) = l(\sigma) - 1 \end{cases}$$

$$T_\sigma T_s = \begin{cases} qT_\sigma & \text{if } l(\sigma s) = l(\sigma) \\ T_{\sigma s} & \text{if } l(\sigma s) = l(\sigma) + 1 \\ qT_{\sigma s} + (q-1)T_\sigma & \text{if } l(\sigma s) = l(\sigma) - 1 \end{cases}$$

$$T_\nu T_\sigma = q^{l(\sigma) - l(\nu\sigma)} T_{\nu\sigma}$$

$$T_\sigma T_\nu = q^{l(\sigma) - l(\sigma\nu)} T_{\sigma\nu}$$

for all $\sigma \in \mathscr{R}$ *and* $s \in S$.

Proof. We begin by proving the formulas for left multiplication by T_s and T_ν. First note that if $\rho, \sigma, \tau \in \mathscr{R}$ and $B\rho B \cdot B\sigma B = B\tau B$ then

$$(4.13) \qquad T_\rho T_\sigma = q^{l(\rho) + l(\sigma) - l(\tau)} T_\tau.$$

This is so because (4.9) implies $T_\rho T_\sigma = cT_\tau$ for some $c \in \mathbf{Q}$, and we may apply the homomorphism ind to find $c = q^{l(\rho) + l(\sigma) - l(\tau)}$. At this point we do not know that $l(\rho) + l(\sigma) \geqslant l(\tau)$, so we cannot assert that c is an integer. It follows from (3.14) that

$$(4.14) \qquad T_s T_\sigma = \begin{cases} qT_\sigma & \text{if } l(s\sigma) = l(\sigma) \\ T_{s\sigma} & \text{if } l(s\sigma) = l(\sigma) + 1. \end{cases}$$

Suppose $l(s\sigma) = l(\sigma) - 1$. Let $\rho = s\sigma$. Then $\sigma = s\rho$ and $l(\sigma) = l(\rho) + 1$ so, by (4.14) $T_\sigma = T_s T_\rho$. Now Iwahori's formula (1.17) with $w = s$ gives

$$(4.15) \qquad T_s T_\sigma = qT_\rho + (q-1)T_s T_\rho = qT_{s\sigma} + (q-1)T_\sigma.$$

Since $Bv = vB$ we have $BvB \cdot B\sigma B = Bv\sigma B$ for all $\sigma \in \mathscr{R}$. Since $l(v) = 0$ it follows from (4.13) that

$$(4.16) \qquad T_v T_\sigma = q^{l(\sigma) - l(v\sigma)} T_{v\sigma}.$$

This proves the formulas for left multiplication. The formulas for right multiplication are proved in the same way, using the analogues of (3.14) for right multiplication by s. $\square$

Since $l(v^i) = 0$ for all $i \geqslant 0$ it follows from (4.16) by induction that

$$(4.17) \qquad T_v^i T_\sigma = q^{l(\sigma) - l(v^i\sigma)} T_{v^i\sigma}.$$

In particular with $\sigma = 1$ this gives

$$(4.18) \qquad T_v^i = T_{v^i}.$$

Lemma (2.50) insures that the power of q in (4.16) is an integer. Thus

$$(4.19) \qquad T_s \cdot H(M,B) \subseteq H(M,B) \quad \text{and} \quad T_v \cdot H(M,B) \subseteq H(M,B).$$

If $\sigma \in \mathscr{R}$ write $\sigma = wv^iw'$ where $i = n - \operatorname{rk}(\sigma)$ and w, $w' \in W$ satisfy $l(w) + l(w') = l(\sigma)$. Then

$$(4.20) \qquad T_\sigma = T_w T_v^i T_{w'}.$$

To see this argue by induction on $l(\sigma)$. If $l(\sigma) = 0$ then $\sigma = v^i$ and the assertion amounts to (4.18). If $l(\sigma) > 0$ then either $l(w) > 0$ or $l(w') > 0$. Suppose $l(w) > 0$. Choose $s \in S$ with $l(sw) < l(w)$. Then $s\sigma = swv^iw'$ so $l(s\sigma) \leqslant l(sw) + l(w') < l(w) + l(w') = l(\sigma)$ and thus $l(\sigma) = l(s\sigma) + 1$. Now (4.14) and induction imply $T_\sigma = T_s T_{s\sigma} = T_s T_{sw} T_v^i T_{w'} = T_w T_v^i T_{w'}$. If $l(w') > 0$ the argument is the same, using the analogue of (4.14) for right multiplication by T_s. This proves (4.20). It follows from Iwahori's formula (1.17) that T_w and $T_{w'}$ may be written as products of elements T_s with $s \in S$. Now it follows from (4.19) and (4.20) that $H(M,B)$ is a ring and that the elements T_s with $s \in S$ and T_v generate $H(M,B)$. $\square$

Note that in proving $H(M,B)$ is a ring generated by the T_s and T_v, we used all the formulas for left multiplication by the generators T_s and T_v but only the formula $T_\sigma T_s = T_{\sigma s}$ when $l(\sigma s) = l(\sigma) + 1$ for right multiplication. Since $v^n = 0$ it follows from (4.17) or direct calculation that

$$(4.21) \qquad T_0 T_\sigma = q^{l(\sigma)} T_0.$$

If K is any commutative ring we define the K-algebra $H_K(M, B)$ by

$$(4.22) \qquad H_K(M, B) = K \otimes H(M, B)$$

where $\otimes = \otimes_{\mathbf{Z}}$. In particular, if K is the ground field used to define the monoid ring $K[M]$ we have $H_K(M, B) \simeq \varepsilon K[M]\varepsilon$.

Let K be a commutative ring. We will construct a K-algebra $A(\mathscr{R})$ which is the analogue for the monoid $\mathscr{R}$ of the generic algebra $A(W)$ of a Coxeter group W ([5], [8], [11]). We call $A(\mathscr{R})$ the generic algebra of $\mathscr{R}$. The construction of $A(W)$ is due to Tits. We follow his idea as written in [11]. Tits used the existence of $A(W)$ to prove that $H_{\mathbf{C}}(G, B) \simeq \mathbf{C}[W]$. We will argue in a similar way and prove that $H_{\mathbf{C}}(M, B) \simeq \mathbf{C}[\mathscr{R}]$.

THEOREM 4.23. *Let K be a commutative ring and let x be a fixed element of K. Let*

$$A(\mathscr{R}) = \bigoplus_{\sigma \in \mathscr{R}} K a_\sigma$$

be a free K-module with basis elements a_σ indexed by $\mathscr{R}$. Then $A(\mathscr{R})$ has the structure of a K-algebra such that

$$a_s a_\sigma = \begin{cases} x a_\sigma & \text{if } l(s\sigma) = l(\sigma) \\ a_{s\sigma} & \text{if } l(s\sigma) = l(\sigma) + 1 \\ x a_{s\sigma} + (x-1) a_\sigma & \text{if } l(s\sigma) = l(\sigma) - 1 \end{cases}$$

$$a_\sigma a_s = \begin{cases} x a_\sigma & \text{if } l(\sigma s) = l(\sigma) \\ a_{\sigma s} & \text{if } l(\sigma s) = l(\sigma) + 1 \\ x a_{\sigma s} + (x-1) a_\sigma & \text{if } l(\sigma s) = l(\sigma) - 1 \end{cases}$$

$$a_v a_\sigma = x^{l(\sigma) - l(v\sigma)} a_{v\sigma}$$

$$a_\sigma a_v = x^{l(\sigma) - l(\sigma v)} a_{\sigma v}$$

for all $\sigma \in \mathscr{R}$ and $s \in S$.

Note that the relations in Theorem 4.23 are just the relations in Theorem 4.12 with q replaced by x. The K-algebra $A(\mathscr{R})$ depends on the ground ring K as well as the chosen element $x \in K$ but we suppress this dependence in our notation. Suppose for the moment that $A(\mathscr{R})$ exists. For s, $t \in S$ let $P_s \in \operatorname{End}_K A(\mathscr{R})$ be left multiplication by a_s and let $Q_t \in \operatorname{End}_K A(\mathscr{R})$ be right multiplication by a_t. Similarly, let P_v and Q_v be left and right multiplication by a_v. The associative law implies

$$\begin{aligned} (4.24) \qquad P_sQ_t &= Q_tP_s \\ P_sQ_v &= Q_vP_s \\ Q_sP_v &= P_vQ_s \\ Q_vP_v &= P_vQ_v. \end{aligned}$$

Tits' idea was to reverse the procedure. Define a ring of K-endomorphisms of the free K-module $A(\mathscr{R})$ in which the above commutation relations hold, and use this ring to define multiplication in $A(\mathscr{R})$. The proof of the analogous theorem for W uses the following lemma on Coxeter groups [2, p. 18, Property C]:

LEMMA 4.25. *If $w \in W$ and $s, s' \in S$ satisfy $l(sw) = l(ws')$ and $l(sws') = l(w)$ then $sw = ws'$.*

In the case of $\mathscr{R}$ we need an analogue of Lemma 4.25, stated as Lemma 4.26 below. In addition we need a strange property of the length function in $\mathscr{R}$, stated as Lemma 4.27 below, which is introduced by the presence of the nilpotent $v \in \mathscr{R}$ and has no analogue in the symmetric group. Although the details of the proof that these lemmas imply Theorem 4.23 are a bit onerous, we include many of them.

Our proofs of Lemma 4.26 and Lemma 4.27 are indirect and use the existence of the ring $H(M, B)$. It would surely contribute to our understanding of the combinatorics in the monoid $\mathscr{R}$ if we had direct proofs of Lemma 4.26 and Lemma 4.27 without the intervention of the ring $H(M, B)$.

LEMMA 4.26. *Suppose $\sigma \in \mathscr{R}$ and $s, t \in S$. Suppose* (i) *$s\sigma \neq \sigma$ and $\sigma t \neq \sigma$ and suppose* (ii) *that $l(s\sigma) = l(\sigma t)$ and $l(s\sigma t) = l(\sigma)$. Then $s\sigma = \sigma t$.*

Proof. Note that if $\sigma = w \in W$ then (i) cannot occur and we are back to Lemma 4.25. Fix a prime power q and let $T_\sigma \in H(M, B)$ be as in (4.9). We shall see that the lemma is implied by the associative law in $H(M, B)$. Note that (i) implies $l(s\sigma) \neq l(\sigma)$ and $l(\sigma t) \neq l(\sigma)$ by Corollary 2.44. Thus either (a) $l(s\sigma) = l(\sigma) + 1 = l(\sigma t)$ or (b) $l(s\sigma) = l(\sigma) - 1 = l(\sigma t)$. Suppose we are in case (a). Then $l(s\sigma t) = l(\sigma) = l(\sigma t) - 1$. It follows from Theorem 4.12 that

$$\begin{aligned} T_s(T_\sigma T_t) &= T_s T_{\sigma t} = qT_{s\sigma t} + (q-1)T_{\sigma t} \\ (T_s T_\sigma)T_t &= T_{s\sigma}T_t = qT_{s\sigma t} + (q-1)T_{s\sigma}. \end{aligned}$$

Since $q > 1$ and the T_τ for $\tau \in \mathscr{R}$ are linearly independent over $\mathbf{Z}$ we have $s\sigma = \sigma t$. In case (b) we have $l(s\sigma t) = l(\sigma t) + 1$. Here

$$T_s(T_\sigma T_t) = qT_{s\sigma t} + q(q-1)T_{s\sigma} + (q-1)^2 T_\sigma$$

$$(T_s T_\sigma)T_t = qT_{s\sigma t} + q(q-1)T_{\sigma t} + (q-1)^2 T_\sigma$$

so again $s\sigma = \sigma t$. □

LEMMA 4.27. *Suppose $\sigma \in \mathscr{R}$ and $s \in S$. Then $l(s\sigma) - l(\sigma)$ and $l(s\sigma v) - l(\sigma v)$ cannot have opposite signs. To be precise, if $\delta \in \{\pm 1\}$ and $l(s\sigma) - l(\sigma) = \delta$ then $l(s\sigma v) - l(\sigma v) \neq -\delta$.*

Proof. Choose a prime power q and argue by way of contradiction, using the associative law in $H(M, B)$. Suppose there exist $\sigma \in \mathscr{R}$, $s \in S$ and $\delta \in \{\pm 1\}$ such that $l(s\sigma) - l(\sigma) = \delta$ and $l(s\sigma v) - l(\sigma v) = -\delta$. Let $a = l(\sigma)$ and let $b = l(\sigma v)$. Compare $T_s(T_\sigma T_v)$ with $(T_s T_\sigma)T_v$. The results are:

$l(s\sigma) - l(\sigma)$	$l(s\sigma v) - l(\sigma v)$	$T_s(T_\sigma T_v)$	$(T_s T_\sigma)T_v$
$+1$	-1	$q^{a-b+1}T_{s\sigma v} + q^{a-b}(q-1)T_{\sigma v}$	$q^{a-b+2}T_{s\sigma v}$
-1	$+1$	$q^{a-b}T_{s\sigma v}$	$q^{a-b-1}T_{s\sigma v} + q^{a-b}(q-1)T_{\sigma v}$

where the first row applies if $\delta = +1$ and the second row applies if $\delta = -1$. In either case we have a contradiction since $q > 1$ and the T_τ for $\tau \in \mathscr{R}$ are linearly independent over $\mathbf{Z}$. □

DEFINITION 4.28. Suppose $s, t \in S$. Define K-endomorphisms P_s, Q_t of the free K-module $A(\mathscr{R})$ by

$$P_s a_\sigma = \begin{cases} xa_\sigma & \text{if } l(s\sigma) = l(\sigma) \\ a_{s\sigma} & \text{if } l(s\sigma) = l(\sigma) + 1 \\ xa_{s\sigma} + (x-1)a_\sigma & \text{if } l(s\sigma) = l(\sigma) - 1 \end{cases}$$

$$Q_t a_\sigma = \begin{cases} xa_\sigma & \text{if } l(\sigma t) = l(\sigma) \\ a_{\sigma t} & \text{if } l(\sigma t) = l(\sigma) + 1 \\ xa_{\sigma t} + (x-1)a_\sigma & \text{if } l(\sigma t) = l(\sigma) - 1 \end{cases}$$

for all $\sigma \in \mathscr{R}$. Define K-endomorphisms P_v, Q_v of $A(\mathscr{R})$ by

$$P_v a_\sigma = x^{l(\sigma) - l(v\sigma)} a_{v\sigma}$$

$$Q_v a_\sigma = x^{l(\sigma) - l(\sigma v)} a_{\sigma v}$$

for all $\sigma \in \mathscr{R}$.

LEMMA 4.29. *If $s, t \in S$ then $P_s Q_t = Q_t P_s$.*

Proof. Let $\sigma \in \mathscr{R}$. We must prove that $P_s Q_t a_\sigma = Q_t P_s a_\sigma$. Since $l(s\sigma) -$

$l(\sigma) \in \{0, \pm 1\}$ and $l(\sigma t) - l(\sigma) \in \{0, \pm 1\}$ the defining formulas (4.28) show that there are $3 \times 3 = 9$ cases to consider. First consider the five cases where either $l(s\sigma) = l(\sigma)$ in which case $s\sigma = \sigma$, or $l(\sigma t) = l(\sigma)$ in which case $\sigma t = \sigma$. Thus $(l(s\sigma) - l(\sigma), l(\sigma t) - l(\sigma))$ is one of the pairs $(0,0)$, $(0, +1)$, $(0, -1)$, $(+1,0)$, $(-1,0)$. Compute $P_sQ_ta_\sigma$ and $Q_tP_sa_\sigma$ in each case and find equality $P_sQ_ta_\sigma = Q_tP_sa_\sigma$. The results of the computation are given in Table I.

TABLE I

$l(s\sigma) - l(\sigma)$	$l(\sigma t) - l(\sigma)$	$P_sQ_ta_\sigma = Q_tP_sa_\sigma$
0	0	x^2a_σ
0	+1	$xa_{\sigma t}$
0	−1	$x^2a_{\sigma t} + x(x-1)a_\sigma$
+1	0	$xa_{s\sigma}$
−1	0	$x^2a_{s\sigma} + x(x-1)a_\sigma$

In the remaining four cases we have $l(s\sigma) - l(\sigma) \in \{\pm 1\}$ and $l(\sigma t) - l(\sigma) \in \{\pm 1\}$. Here there is still some work to be done. However Lemma 4.26 settles these cases in the same way (verbatim) that Lemma 4.25 settles the corresponding cases for $A(W)$. Since the details for $A(W)$ are given in [5] we omit the analogous computations for $A(\mathscr{R})$. □

LEMMA 4.30. *If* $s, t \in S$ *then* $P_sQ_v = Q_vP_s$ *and* $Q_sP_v = P_vQ_s$.

Proof. It will suffice to prove the first equality. Since $l(s\sigma) - l(\sigma) \in \{0, \pm 1\}$ and $l(s\sigma v) - l(\sigma v) \in \{0, \pm 1\}$ we separate $3 \times 3 = 9$ cases. Note that $l(s\sigma) = l(\sigma)$ implies $s\sigma = \sigma$ and thus $l(s\sigma v) = l(\sigma v)$. This eliminates two cases. Lemma 4.27 eliminates two more cases. Thus $(l(s\sigma) - l(\sigma), l(s\sigma v) - l(\sigma v))$ is one of the pairs $(0,0)$, $(+1,0)$, $(+1,+1)$, $(-1,0)$, $(-1,-1)$. Compute $P_sQ_va_\sigma$ and $Q_vP_sa_\sigma$ in each case and find equality $P_sQ_va_\sigma = Q_vP_sa_\sigma$. The results of the computation are given in Table II, where $a = l(\sigma)$ and $b = l(\sigma v)$.

TABLE II

$l(s\sigma) - l(\sigma)$	$l(s\sigma v) - l(\sigma v)$	$P_sQ_va_\sigma = Q_vP_sa_\sigma$
0	0	$x^{a-b+1}a_{\sigma v}$
+1	0	$x^{a-b+1}a_{\sigma v}$
+1	+1	$x^{a-b}a_{s\sigma v}$
−1	0	$x^{a-b+1}a_{\sigma v}$
−1	−1	$x^{a-b+1}a_{s\sigma v} + x^{a-b}(x-1)a_{\sigma v}$

This completes the proof. □

Since

$$(4.31)\quad P_v Q_v a_\sigma = x^{l(\sigma)-l(v\sigma v)} a_{v\sigma v} = Q_v P_v a_\sigma$$

we have $P_v Q_v = Q_v P_v$. This completes the proof that P_s, Q_t, P_v, Q_v satisfy the commutation formulas (4.24).

Now we may prove Theorem 4.23. Let $\mathscr{P}$ be the K-algebra of K-endomorphisms of $A(\mathscr{R})$ generated by the P_s for $s \in S$, P_v and the identity. Let $\mathscr{Q}$ be the K-algebra of K-endomorphisms of $A(\mathscr{R})$ generated by the Q_s for $s \in S$, Q_v, and the identity. It follows from the commutation formulas that $\mathscr{P}$ and $\mathscr{Q}$ centralize each other.

Suppose $\sigma \in \mathscr{R}$. Write $\sigma = wv^i w'$ where $i = n - \mathrm{rk}(\sigma)$ and $w, w' \in W$ satisfy $l(w) + l(w') = l(\sigma)$. Write $w = s_1 \ldots s_j$ and write $w' = t_1 \ldots t_k$ where the $s_1, \ldots, s_j$ and $t_1, \ldots, t_k$ are in S, where $j = l(w)$ and $k = l(w')$. Then, as in the proof of (4.20), we have

$$(4.32)\qquad a_\sigma = P_{s_1} \ldots P_{s_j} P_v^i P_{t_1} \ldots P_{t_k} a_1$$

and

$$(4.33)\qquad a_\sigma = Q_{t_k} \ldots Q_{t_1} Q_v^i Q_{s_j} \ldots Q_{s_1} a_1.$$

Define a K-linear map $\varphi: \mathscr{P} \to A(\mathscr{R})$ by $\varphi(P) = Pa_1$ for $P \in \mathscr{P}$. Then φ is surjective by (4.32). Let $P \in \ker(\varphi)$. If $\sigma \in \mathscr{R}$ then by (4.33) there exists $Q \in \mathscr{Q}$ with $Q_{a_1} = a_\sigma$. Then $0 = QPa_1 = PQa_1 = Pa_\sigma$. Thus $P = 0$. Thus φ is an isomorphism of K-modules. By (4.32) we have

$$(4.34)\qquad \varphi^{-1} a_s = P_s \quad \text{and} \quad \varphi^{-1} a_v = P_v.$$

Also

$$(4.35)\qquad \varphi^{-1}(a_\sigma) a_1 = a_\sigma.$$

Now define the multiplication in $A(\mathscr{R})$ by transport of structure: if $\sigma, \tau \in \mathscr{R}$ let

$$(4.36)\qquad a_\sigma a_\tau = \varphi(\varphi^{-1}(a_\sigma)\varphi^{-1}(a_\tau)).$$

This makes $A(\mathscr{R})$ an associative ring. The formulas (4.34) and (4.35) show that it has the desired properties $a_s a_\sigma = P_s a_\sigma$ and $a_v a_\sigma = P_v a_\sigma$. The formulas for left multiplication by a_s and a_v determine, in principle, all products $a_\sigma a_\tau$ for $\sigma, \tau \in \mathscr{R}$. In practice, a proof that the products $a_\sigma a_s$ and $a_\sigma a_v$ are as stated in the theorem involves a rather long induction on $l(\sigma)$. Consider, for example, a product $a_\sigma a_s$. If $\sigma \in \mathscr{R}^r$ write $\sigma = wv^i w'$ where $i = n - \mathrm{rk}(\sigma)$ and $l(w) + l(w') = l(\sigma)$. If $l(\sigma) = 0$ then use $a_{v^i} = a_v^i$. Suppose $l(\sigma) > 0$. If $l(w) > 0$ choose $t \in S$ so that $l(tw) < l(w)$. Let $\tau = t\sigma$. Then $a_\sigma = a_t a_\tau$ by the formula for left multiplication, so $a_\sigma a_s = a_t(a_\tau a_s)$. Since $l(\tau) < l(\sigma)$ we may apply induction.

One must separate cases and use Lemma 4.26. Now we are reduced to the case $\sigma = v^i w'$ where $l(\sigma) = l(w')$ and thus, by the formula for left multiplication $a_\sigma = a_v^i a_{w'}$. Again, one must separate cases to complete the induction. We omit the details. This completes the proof of the existence of the K-algebra $A(\mathscr{R})$. □

Note that $A(\mathscr{R})$ has a K-subalgebra

$$(4.37) \qquad A(W) = \bigoplus_{w \in W} K a_w$$

which is the generic algebra of the Coxeter group W. Henceforth let X be an indeterminate over $\mathbf{C}$, let $K = \mathbf{C}[X]$ be the ring of polynomials over $\mathbf{C}$ and let $x = X \in \mathbf{C}[X]$. Let A be any associative algebra over $\mathbf{C}[X]$ which is a free $\mathbf{C}[X]$-module of finite rank and let $\alpha \in \mathbf{C}$. Let $\mathbf{C}_\alpha$ be the $\mathbf{C}[X]$-module which has $\mathbf{C}$ as its underlying vector space and module structure defined by $f \cdot 1 = f(\alpha)$ for $f \in \mathbf{C}[X]$. Define a $\mathbf{C}$-algebra $A(\alpha)$ by

$$(4.38) \qquad A(\alpha) = A \otimes_{\mathbf{C}[X]} \mathbf{C}_\alpha .$$

If $\{a_k\}$ is a $\mathbf{C}[X]$-basis for A then $\{a_k \otimes 1\}$ is a $\mathbf{C}$-basis for $A(\alpha)$. We have formulas

$$a_i a_j = \sum_k p_{ijk} a_k$$

with structure constants $p_{ijk} = p_{ijk}(X) \in \mathbf{C}[X]$. The structure constants of $A(\alpha)$ with respect to the basis $\{a_k \otimes 1\}$ are obtained by evaluating the polynomials p_{ijk} at α.

If Ω is an algebraically closed field and Λ is a semisimple algebra of finite dimension over Ω, then there exist integers $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_r > 0$ such that $\Lambda \simeq \mathrm{M}_{n_1}(\Omega) \oplus \cdots \oplus \mathrm{M}_{n_r}(\Omega)$. Call the sequence $(n_1, \ldots, n_r)$ the numerical invariant of Λ. We will use the following theorem of Tits ([5], [8], [11]):

THEOREM 4.39. *Let A be an associative algebra over $\mathbf{C}[X]$ which is a free $\mathbf{C}[X]$-module of finite rank. Let Ω be the algebraic closure of $\mathbf{C}(X)$. If $\alpha \in \mathbf{C}$ and $A(\alpha)$ is semisimple then $A \otimes_{\mathbf{C}[X]} \Omega$ is semisimple and has the same numerical invariant as $A(\alpha)$.*

This theorem shows, in particular, that if α, $\beta \in \mathbf{C}$ and $A(\alpha)$, $A(\beta)$ are semisimple then $A(\alpha) \simeq A(\beta)$. Tits applied this theorem ([5], [8], [11]) with $A = A(W)$ to conclude that

$$(4.40) \qquad H_{\mathbf{C}}(G, B) \simeq \mathbf{C}[W].$$

We may apply it in similar fashion with $A = A(\mathscr{R})$. Note that $A(1) \simeq \mathbf{C}[\mathscr{R}]$

and that if q is a prime power then $A(q) \simeq H_{\mathbf{C}}(M, B)$ where $M = \mathbf{M}_n(\mathbf{F}_q)$. The isomorphisms are defined by $a_\sigma \otimes 1 \mapsto \sigma$ in the first case and $a_\sigma \otimes 1 \mapsto T_\sigma$ in the second. Munn [15, Th. 4.4] has shown that if $\mathscr{S}$ is an *inverse semigroup* then the algebra $\mathbf{C}[\mathscr{S}]$ is semisimple. In particular, $\mathbf{C}[\mathscr{R}]$ is semisimple. Let $\Delta(X)$ be the discriminant of the basis $\{a_\sigma \mid \sigma \in \mathscr{R}\}$ for the $\mathbf{C}[X]$-algebra A. It follows from the multiplication formulas in Theorem 4.23 that $\Delta(X)$ is a polynomial in X with integer coefficients. Since $\Delta(1)$ is the discriminant of the basis $\mathscr{R}$ for the semisimple algebra $A(1)$ we have $\Delta(1) \neq 0$ and thus $\Delta(X) \neq 0$. Thus $\Delta(q)$ can be 0 for at most a finite number of q, depending on n. Since $\Delta(q)$ is the discriminant of the basis $\{T_\sigma \mid \sigma \in \mathscr{R}\}$ for the algebra $A(q)$, it follows that $A(q)$ is semisimple except, perhaps, for a finite number of q.

I know no general theorem on semigroup algebras which will ensure that $\mathbf{C}[M]$ is semisimple. However the ideas in Munn's papers [15], [16] can be used to prove that $\mathbf{C}[M]$ is semisimple when $M = \mathbf{M}_n(\mathbf{F}_q)$; this will be done in a sequel to the present paper.[1] It follows that $H_{\mathbf{C}}(M, B) \simeq \varepsilon\mathbf{C}[M]\varepsilon$ is semisimple for all q. This proves

THEOREM 4.41. *Let* $M = \mathbf{M}_n(\mathbf{F}_q)$ *and let* B *be a Borel subgroup of* $\mathrm{GL}_n(\mathbf{F}_q)$. *Let* $\mathscr{R} \subseteq M$ *be the rook monoid. Then*

$$H_{\mathbf{C}}(M, B) \simeq \mathbf{C}[\mathscr{R}].$$

It seems likely, as in the case of the symmetric group, that $\mathbf{C}$ may be replaced by $\mathbf{Q}$ in Theorem 4.41. To replace $\mathbf{C}$ by $\mathbf{Q}$ it would suffice to show that $\mathbf{Q}$ is a splitting field for both $H_{\mathbf{Q}}(M, B)$ and $\mathbf{Q}[\mathscr{R}]$. Munn [16] has shown this for $\mathbf{Q}[\mathscr{R}]$.

The algebra $H_{\mathbf{C}}(M, B)$ also occurs, remarkably, in a different context. Let $G = \mathrm{GL}_n(\mathbf{F}_q)$ and let $\tilde{G} = \mathrm{AGL}_n(\mathbf{F}_q) \supset G$ be the group of affine transformations of $\mathbf{F}_q^n$. Let B and ε be as before. It was remarked in [24] that the dimension of $H_{\mathbf{C}}(\tilde{G}, B) = \varepsilon\mathbf{C}[\tilde{G}]\varepsilon$ is the number (1.11) of rook placements. Siegel [22] has found the irreducible representations of $H_{\mathbf{C}}(\tilde{G}, B)$. Their degrees are the same as the degrees of the irreducible representations of $\mathbf{C}[\mathscr{R}]$ found by Munn [16]. Thus, in view of (4.40) we have $H_{\mathbf{C}}(\tilde{G}, B) \simeq H_{\mathbf{C}}(M, B)$, a non-explicit isomorphism of two algebras which, on the face of it, have nothing to do with one another. The role (if any) of the rooks in connection with $H_{\mathbf{C}}(\tilde{G}, B)$ is still mysterious.

I hope to do the representation theory of $H_{\mathbf{C}}(M, B)$ in a sequel to this paper.

[1] After this paper was submitted, the author learned from M. S. Putcha that he and J. Okniński have proved the complete reducibility of complex representations of finite monoids M of Lie type. Their work shows in particular that $\mathbf{C}[M_n(\mathbf{F}_q)]$ is semisimple. Their paper titled 'Complex representations of matrix semigroups' will appear in the *Transactions of the American Mathematical Society*.

Here is one fact, stated in terms of the generic algebra $A(\mathscr{R})$ which suggests that it will be interesting. Let $K = \mathbf{C}[X]$, let

$$(4.42)\qquad J_r = \bigoplus_{\sigma \in \mathscr{R}^r} K a_\sigma$$

and let

$$(4.43)\qquad I_r = J_0 \oplus \cdots \oplus J_r.$$

Then J_r is an $A(W)$-module and I_r is a two-sided ideal of $A(\mathscr{R})$. Consider the representation of $A(\mathscr{R})$ on I_1/I_0. In the specialization $X \to 1$ this quotient is naturally isomorphic to $\mathrm{M}_n(\mathbf{C})$ because there is a distinguished basis $\{E_{ij} + I_0 \mid 1 \leqslant i, j \leqslant n\}$ consisting of the cosets of the matrix units modulo I_0. For each j with $1 \leqslant j \leqslant n$, the 'column space' spanned by the cosets $E_{1j} + I_0, \ldots, E_{nj} + I_0$ is a $\mathbf{C}[\mathscr{R}]$-module which affords the defining representation of $\mathscr{R}$ by $n \times n$ matrices; although we began with $\mathscr{R} \subseteq \mathrm{M}_n(\mathbf{F}_q)$ we may equally well view $\mathscr{R} \subseteq \mathrm{M}_n(\mathbf{C})$ because the matrix entries of $\sigma \in \mathscr{R}$ are 0 or 1. Write the matrix units in the form $E_{ij} = w v_1 w'$, where $v_1 = E_{1n}$ is our distinguished nilpotent of rank 1 as in (2.5) and $w, w' \in W$ are chosen so that $l(E_{ij}) = l(w) + l(w')$. If we replace v by a_v and s by a_s for $s \in S$ in these formulas, we are led to a direct sum decomposition of I_1/I_0 into n isomorphic $A(\mathscr{R})$-submodules. Each of these, when viewed as a module for the subring $A(W)$, affords the reflection representation of $A(W)$ of degree n. In particular, each of these modules affords the Burau representation of the braid group [13]. Thus the Burau representation is as natural as the representation of a matrix algebra on the space of column vectors.

REFERENCES

1. Borel, A. and Tits, J., 'Groupes réductifs', *Publ. Math. I.H.E.S.* **27** (1965), 55–151.
2. Bourbaki, N., *Groupes et Algèbres de Lie*, Chapitres IV, V, VI, Hermann, Paris, 1968.
3. Bruhat, F., 'Représentations Induites des Groupes de Lie Semi-Simples Connexes', *C.R. Acad. Sci. Paris* **238** (1954), 437–439.
4. Carter, R. W., *Simple Groups of Lie Type*, Wiley, Interscience, 1972.
5. Carter, R. W., *Finite Groups of Lie Type – Conjugacy Classes and Complex Characters*, Wiley, Interscience, 1985.
6. Chevalley, C., 'Sur certains groupes simples', *Tôhoku Math. J.* **7** (1955), 14–66.
7. Clifford, A. H. and Preston, G. B., *The Algebraic Theory of Semigroups*, Vol. I, Math. Surveys 7, American Math. Soc., 1961.
8. Curtis, C. W. and Reiner, I., *Methods of Representation Theory, with Applications to Finite Groups and Orders*, Vol. II, Wiley, 1987.
9. Grigor'ev, D. Ju., 'An analogue of the Bruhat decomposition for the closure of the cone of a Chevalley group of the classical series', *Soviet Math. Dokl.* **23** (1981), 393–397.
10. Iwahori, N., 'On the structure of a Hecke ring of a Chevalley group over a finite field', *J. Fac. Sci. Univ. Tokyo*, Sec. I, **10** (1964), 215–236.

11. Iwahori, N., 'Generalized Tits system (Bruhat decomposition) on p-adic semisimple groups', in *Proc. Symp. Pure Math.* 9 (1966), *Algebraic Groups and Discontinuous Subgroups*, pp. 71–83.
12. Iwahori, N., 'On some properties of groups with BN-pairs', in *Theory of Finite Groups, a Symposium* (eds R. Brauer and C.-H. Sah), W. A. Benjamin, 1969, pp. 203–212.
13. Lehrer, G. I., 'A survey of Hecke algebras and the Artin braid groups', *Contemp. Math.* **74** (1988), 365–385.
14. Macdonald, I. G., *Symmetric Functions and Hall Polynomials*, Clarendon Press, Oxford, 1979.
15. Munn, W. D., 'Matrix representations of semigroups', *Proc. Camb. Phil. Soc.* **53** (1957), 5–12.
16. Munn, W. D., 'The characters of the symmetric inverse semigroup', *Proc. Camb. Phil. Soc.* **53** (1957), 13–18.
17. Putcha, M. S., 'Linear algebraic monoids', *London Math. Soc. Lecture Notes* **133**, Cambridge Univ. Press, 1988.
18. Putcha, M. S., 'Monoids on groups with BN-pairs', *J. Algebra* **120** (1989), 139–169.
19. Renner, L., 'Classification of semisimple algebraic monoids', *Trans. Amer. Math. Soc.* **292** (1985), 193–223.
20. Renner, L., 'Analogue of the Bruhat decomposition for algebraic monoids', *J. Algebra* **101** (1986), 303–338.
21. Rodrigues, O., 'Note sur les inversions, ou dérangements produits dans les permutations', *J. de Math.*, 1 Série, **4** (1839), 236–239.
22. Siegel, E., 'On the representations of a Hecke ring of the affine group over a finite field', thesis, Univ. of Wisconsin, Madison, 1990.
23. Solomon, L., 'The orders of the finite Chevalley groups', *J. Algebra* **3** (1966), 376–393.
24. Solomon, L., 'The affine group I. Bruhat decomposition', *J. Algebra* **20** (1972), 512–539.
25. Steinberg, R., 'Lectures on Chevalley groups', Yale University, 1967, mimeographed notes.
26. Tits, J., 'Théorème de Bruhat et sous-groupes paraboliques', *C.R. Acad. Sci. Paris* **254** (1962), 2910–2912.
27. Tits, J., 'Algebraic and abstract simple groups', *Ann. of Math.* **80** (1964), 313–329.
28. Waterhouse, W. C., 'The unit groups of affine algebraic monoids', *Proc. Amer. Math. Soc.* **85** (1982), 506–508.

Author's address:

Louis Solomon,
University of Wisconsin,
Madison, WI 53706,
U.S.A

(Received, November 2, 1989)

Added in proof. Concerning the remarks which precede Theorem 4.41 and the related footnote: About a week ago Putcha informed me that there is a gap in my argument for the semisimplicity of $\mathbf{C}[M]$. Thus, at this writing, the only proof of semisimplicity is the one by Okniński and Putcha.