Astérisque

R. B. HOWLETT
G. I. LEHRER

On the integral group algebra of a finite algebraic group

Astérisque, tome 168 (1988), p. 141-155
<http://www.numdam.org/item?id=AST_1988__168__141_0>

© Société mathématique de France, 1988, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques
http://www.numdam.org/

Société Mathématique de France
Astérisque 168 (1988), p.141-155.

On the integral group algebra of a finite algebraic group

R. B. HOWLETT and G. I. LEHRER

§1 Introduction and notation

Let G be the group of $\mathbf{F}_q$-rational points of a connected reductive algebraic group defined over $\mathbf{F}_q$ and let U be a maximal unipotent subgroup of G. In this note we give three explicit embeddings of the ring of endomorphisms $E = \mathrm{End}_{\mathbf{Z}G}(\mathrm{Ind}_U^G(1))$ into the integral group ring $\mathbf{Z}G$. The embeddings have properties related to certain $\mathbf{Z}G$ modules, and all have the same image. Thus they imply the existence of certain automorphisms of E.

There is a canonical surjection $\sigma: E \to \overline{E} = \mathrm{End}_{\mathbf{Z}G}(\mathrm{Ind}_B^G(1))$, and $\sigma \otimes 1: E \otimes_{\mathbf{Z}} \mathbf{Z}[|H|^{-1}] \to \overline{E} \otimes_{\mathbf{Z}} \mathbf{Z}[|H|^{-1}]$ has a left inverse τ. (Here B is a Borel subgroup and H a maximal split torus in G such that $B = HU$.) One of our embeddings composed with τ gives the embedding of $\overline{E} \otimes_{\mathbf{Z}} \mathbf{Z}[|H|^{-1}]$ which we constructed in [3]. Thus the present work may be thought of as an extension of the results of that paper.

Another direction for applications of this work is the construction of idempotents (analogous to Steinberg's idempotent for St_G) in FG (F a field) which are not in the Hecke algebra $H(G, B)$ (or even $H(G, U)$). This could provide explicit constructions of representations of G in characteristic p (where $p|q$).

We begin here with some generalities which will establish our notation. Let R be a commutative (unital) ring, A an R-algebra and $a \in A$. Then aA is a (right) A-module, and we write $E = \mathrm{End}_A(aA)$. We have

(1.1) *There is an algebra homomorphism* $\lambda: \widetilde{A} = \{\, x \in A \mid xaA \subseteq aA \,\} \to E$ *defined by* $x \mapsto (\lambda_x: y \mapsto xy) \qquad (x,\, y \in aA)$.

If a is an idempotent and $\phi \in E$ then $\phi(y) = \phi(ay) = \phi(a)y$ for any $y \in aA$; hence $\phi = \lambda_{\phi(a)}$, and $\phi(a) = \phi(a)a \in aAa$. Thus we have

(1.2) *If a is an idempotent then*

(i) λ is surjective

(ii) There is an algebra homomorphism $\mu: E \to aAa \subseteq aA \subseteq A$ such that $\lambda\mu = \mathrm{id}_E$.

(1.3) DEFINITION If there is an algebra homomorphism $\mu: E \to A$ such that $\lambda\mu = \mathrm{id}_E$, we say that E is *embedded* in A, and that μ is an *embedding of E into A*.

Let G be a finite group and take $A = RG$, the group ring over R. For any subset $S \subseteq G$ denote by $[S]$ the sum $[S] = \sum_{s \in S} s \in RG$, and consider the case $a = [K]$, where K is a subgroup of G. If $G = \coprod_i Kx_iK$ is the double coset decomposition of G with respect to K, the map $T_i: [K] \mapsto [Kx_iK]$ defines an element of E, and it is well known that

(1.4) *E is the free R-module with basis $\{T_i\}$.*

Moreover, in this case we have

(1.5) *$\lambda: aA \to E$ is surjective.*

For here $T_i = \lambda_y$, where $y = \sum_j k_j x_j$ and $Kx_iK = \coprod_j k_j x_i K$. However, in general there is no embedding μ in the sense of (1.3).

Here we shall be concerned with the case $R = \mathbf{Z}$, G the group of $\mathbf{F}_q$-rational points of a connected reductive $\mathbf{F}_q$-group and $K = U$, its maximal unipotent subgroup. We shall show that there is an embedding of $E = \mathrm{End}_{\mathbf{Z}G}[U]\mathbf{Z}G$ into $\mathbf{Z}G$, and in the course of its study some automorphisms of E will play a role. Our embedding has properties connected with those of the Steinberg representation of $\mathbf{Z}G$ (see §3 below). For this observation we are indebted to Okuyama.

We remark finally that the nature of our formulae are strongly suggestive that there is an underlying geometric explanation for the facts we present here, related to the geometric structure of the Bruhat cells and Schubert varieties of the underlying algebraic group.

§2 The case of a finite algebraic group

For the rest of this note, G, U, $B = HU$ and E will be as in the last section (G the group of rational points of a connected reductive group defined over $\mathbf{F}_q$, and so on). If $N = N_G(H)$ then $N/H = W$ is the Weyl group of G, with simple reflection set S, length function $l(w)$ ($w \in W$) and longest element w_0. Denote by Φ and Π the corresponding root system and set of simple roots (respectively). For elementary facts concerning the structure of G the reader is referred to [2], [1] or [3]. We assume that the representatives $\dot{w} \in N$ ($w \in W$) have been chosen so that if $w = w_1 w_2$ with $l(w) = l(w_1) + l(w_2)$ then $\dot{w} = \dot{w}_1 \dot{w}_2$. (See [9] for the proof that this is possible.) We shall require the following well known fact (see, for example, [3] Lemma 2.8):

(2.1) LEMMA *Let $a \in \Phi$ with $U_a \subseteq U$ the corresponding root subgroup of G, and suppose that $n \in N$ maps onto r_a, the reflection in W corresponding to a. Then each element x of $U_a^\#$ ($= U_a - \{1\}$) has a unique expression $x = h_n(x) f_n(x) n g_n(x)$, where h_n is a map $U_a^\# \to H$ and f_n, g_n are bijections $U_a^\# \to U_{-a}^\#$.*

An easy computation proves

(2.2) LEMMA *Use the notation of (2.1) and let $t \in H$. Then for $u \in U_a^\#$,*
(i) $h_{tn}(u) = h_n(u) t^{-1}$
(ii) $f_{tn}(u) = t f_n(u) t^{-1}$ and $g_{tn}(u) = g_n(u)$.

If $r \in W$ is a reflection then we will write h, f and g for $h_{\dot{r}}$, $f_{\dot{r}}$ and $g_{\dot{r}}$ if there is no danger of ambiguity. We also adopt the notation $V = \dot{w}_0^{-1} U \dot{w}_0$ and $V_a = U_{-a}$.

(2.3) PROPOSITION *(i) In the above the notation, if a is a simple root and $r = r_a$ then we have (in $\mathbf{Z}G$)*

$$[B \cap V\dot{r}V] = \sum_{u \in U_a^\#} k(u) u = \sum_{v \in V_a^\#} v \dot{r} f(g^{-1}(v)),$$

where $k(u) = h(u)^{-1}$.
(ii) We have $\dot{r}^2 \sum_{u \in U_a^\#} h(u) = \sum_{u \in U_a^\#} k(u)$.

Proof. Part (i) follows easily from [3,§2] and (2.1).

(ii) Inverting $k(u) = f(u)\dot{r}g(u)$ gives $u^{-1}k(u)^{-1} = g(u)^{-1}\dot{r}^{-1}f(u)^{-1}$. Multiplying both sides on the left by $k(u)$ and conjugating by $\dot{r}^2$ we obtain

$$h(\dot{r}^{-2}k(u)u^{-1}k(u)^{-1}\dot{r}^2) = \dot{r}^{-2}k(u) \qquad (u \in U_a^{\#}). \tag{2.3.1}$$

Since $k(u)uk(u)^{-1} = f(u)\dot{r}g(u)k(u)^{-1}$ with uniqueness of expression on the right, it follows that $k(u)uk(u)^{-1}$ determines $f(u)$ and hence u; thus as u runs over $U_a^{\#}$ so does $k(u)uk(u)^{-1}$. Now sum (2.3.1) over $u \in U_a^{\#}$ to obtain (ii). □

Since the sum in (2.3) (ii) will recur later we give it a name: with the notation as in (2.3) write

$$\eta_{\dot{r}} = \sum_{u \in U_a^{\#}} k(u) = \dot{r}^2 \sum_{u \in U_a^{\#}} h(u) \in \mathbf{Z}G. \tag{2.3.2}$$

(2.4) LEMMA *With the notation as in (2.1), let $u \in U_a^{\#}$. Then we have $g\big(g(u)^{\dot{r}}\big) = u^{\dot{r}}$ (where $x^y = y^{-1}xy$).*

Proof. We have $u = h(u)f(u)\dot{r}g(u)$. Make $g(u)$ the subject of this formula, conjugate by $\dot{r}$ and collect terms as follows:

$$g(u)^{\dot{r}} = \big(\dot{r}^{-2}h(u)^{-1}\big)\big(h(u)f(u)^{-1}h(u)^{-1}\big)\dot{r}\big(\dot{r}^{-1}u\dot{r}\big).$$

The result follows. □

The double coset decomposition of G with respect to U is well-known; we have $G = \coprod_{n \in N} UnU$. Hence it follows from the generalities in §1 above that $E = \mathrm{End}_{\mathbf{Z}G}([U]\mathbf{Z}G)$ has a $\mathbf{Z}$-module basis $\{\, T_n \mid n \in N \,\}$ defined as in (1.3). The rules for multiplying these T_n were determined by Yokonuma [10], and may be expressed as follows. (In writing the relations we regard the length function of W as lifted to N—that is, for $n \in N$ we define $l(n) = l(\bar{n})$ where $\bar{n}$ is the image of n in W.)

(2.5) PROPOSITION (Yokonuma [10]) *The algebra* $E = \mathrm{End}_{\mathbf{Z}G}([U]\mathbf{Z}G)$ *has a* $\mathbf{Z}$*-basis* $\{T_n \mid n \in N\}$ *satisfying*

(i) *If* $l(n_1n_2) = l(n_1) + l(n_2)$ *then* $T_{n_1}T_{n_2} = T_{n_1n_2}$.

(ii) *If* $l(n) = 1$ *then* $T_n^2 = q_aT_{n^2} + T_n \sum_{u \in U_a^\#} T_{h_n(u)n^2}$, *where* $a \in \Pi$ *is the root corresponding to* $\bar{n} \in S$ *and* $q_a = |U_a|$. *(Note that* $n^2 \in H$*.)*

Proof. (i) follows easily from the definition of T_n (namely, $T_n[U] = [UnU]$) and Chevalley's refinement of the Bruhat decomposition for G, by induction on $l(n_2)$. Note that the case $l(n_2) = 0$ reads $T_nT_h = T_{nh}$ $(h \in H, n \in N)$. For (ii) one uses the Chevalley decomposition together with (2.1) above. We leave the details to the reader. □

(2.6) DEFINITION For $n \in N$ define the element $\gamma_n \in \mathbf{Z}G$ by

$$\gamma_n = \sum_{t \in W} (-1)^{l(t)}[Bt \cap VnV].$$

Note that from (2.3) of [3] it follows that $Bt \cap VnV = \emptyset$ unless $t \leq \bar{n}$ (in the Bruhat order on W). Hence (2.6) may be written

$$\gamma_n = \sum_{\substack{t \leq \bar{n} \\ t \in W}} (-1)^{l(t)}[Bt \cap VnV]. \tag{2.6$'$}$$

(2.7) THEOREM *The elements* γ_n *form a* $\mathbf{Z}$*-basis of a subalgebra* Γ *of* $\mathbf{Z}G$, *and the map* $\phi: T_n \to \gamma_n$ *is an isomorphism of* $\mathbf{Z}$*-algebras.*

Proof. Since the support of γ_n is contained in VnV and G is the disjoint union of $\{VnV \mid n \in N\}$, the γ_n are clearly $\mathbf{Z}$-linearly independent. In view of (2.5) it therefore suffices to prove

(2.7.1) $\gamma_{n_1}\gamma_{n_2} = \gamma_{n_1n_2}$ *if* $n_1, n_2 \in N$ *with* $l(n_1n_2) = l(n_1) + l(n_2)$,

and

(2.7.2) $\gamma_n^2 = q_a\gamma_{n^2} + \gamma_n \sum_{u \in U_a^\#} \gamma_{h(u)n^2}$ *if* $a \in \Pi$ *and* $n = \dot{r}_a$, *where* $h = h_n$ *is the function defined in (2.1).*

We first prove (2.7.1). If $l(n_2) = 0$ then $n_2 \in H$ and it follows that $\gamma_{n_2} = [B \cap Vn_2V] = [B \cap n_2V] = n_2$; thus $\gamma_{n_1}\gamma_{n_2} = \gamma_{n_1}n_2 = \gamma_{n_1n_2}$, since

$[Bt \cap Vn_1V]n_2 = [Bt \cap Vn_1n_2V]$ for all $t \in W$. Observe now that if we can prove (2.7.1) for $n_2 = \dot{r}_a$ with $a \in \Pi$ then we will be finished; for in general we may write $n_2 = h\dot{r}_1\dot{r}_2 \ldots \dot{r}_l$ with $h \in H$, $r_i \in S$ for each i and $l = l(n_2)$, and then induction on l will give $\gamma_{n_2} = \gamma_h \gamma_{\dot{r}_1} \gamma_{\dot{r}_2} \ldots \gamma_{\dot{r}_l}$ and $\gamma_{n_1}\gamma_{n_2} = \gamma_{n_1}\gamma_h\gamma_{\dot{r}_1} \ldots \gamma_{\dot{r}_l} = \gamma_{n_1 h\dot{r}_1 \ldots r_l} = \gamma_{n_1 n_2}$ as required.

Thus we turn to the proof of (2.7.1) in the case where $n_2 = \dot{r}$ with $r = r_a \in S$ and $n_1 = n \in N$ with $l(n\dot{r}) = l(n) + 1$. First observe that $\gamma_{\dot{r}} = [B \cap V\dot{r}V] - [Br \cap V\dot{r}V]$ (by (2.6)$'$), and from (2.3) we have $[B \cap V\dot{r}V] = \sum_{u \in U_a^{\#}} k(u)u$. Moreover, by a slight extension of Lemma 2.4 of [3], $[Br \cap V\dot{r}V] = [U_a\dot{r}] = [\dot{r}V_a]$. Hence

$$\text{(2.7.3)} \qquad \gamma_n\gamma_{\dot{r}} = \sum_{l(tr)>l(t)} (-1)^{l(t)}\big([Bt\cap VnV]-[Btr\cap VnV]\big)\Big(\sum_{u\in U_a^{\#}} k(u)u-[U_a\dot{r}]\Big).$$

Now writing $B_a = HU_a$, we have $BtB_a = Bt$ since $l(tr_a) > l(t)$. Hence

$$\begin{aligned}
[Bt \cap VnV]\Big(\sum_{u\in U_a^{\#}} k(u)u\Big) &= \sum_{u\in U_a^{\#}} [Bt \cap VnVk(u)u] \\
&= \sum_{v\in V_a^{\#}} [Bt \cap VnVv\dot{r}f(g^{-1}(v))] \qquad \text{(by (2.3))} \\
&= [Bt \cap VnV\dot{r}V_a^{\#}]
\end{aligned}$$

since the sets $VnV\dot{r}v$ are disjoint for distinct v. Hence we have

$$\text{(2.7.4)} \qquad [Bt \cap VnV]\Big(\sum_{u\in U_a^{\#}} k(u)u\Big) = [Bt \cap Vn\dot{r}V] - [Bt \cap VnV\dot{r}].$$

Similarly,

$$\begin{aligned}
[Bt \cap VnV][U_a]\dot{r} &= \sum_{u\in U_a} [Bt \cap VnVu]\dot{r} \\
&= \sum_{u\in U_a} [Btr \cap VnVu\dot{r}] \\
&= \sum_{v\in V_a} [Btr \cap VnV\dot{r}v] \\
&= [Btr \cap VnV\dot{r}V_a].
\end{aligned}$$

Thus

$$[Bt \cap VnV][U_a]\dot{r} = [Btr \cap Vn\dot{r}V]. \tag{2.7.5}$$

The next term arising in the expansion of (2.7.3) is

$$\begin{aligned}
[Btr \cap VnV]\Big(\sum_{v \in V_a^\#} v\dot{r}f(g^{-1}(v))\Big) &= \sum_{v \in V_a^\#} [Btrv \cap VnVv]\dot{r}f(g^{-1}(v)) \\
&= \sum_{v \in V_a^\#} [Btr \cap VnV]\dot{r}f(g^{-1}(v)) \\
&= [Btr \cap VnV]\dot{r}[V_a^\#].
\end{aligned} \tag{2.7.6}$$

The last term is

$$[Btr \cap VnV][U_a\dot{r}] = [Btr \cap VnV]\dot{r}[V_a]. \tag{2.7.7}$$

Adding the right hand sides of (2.7.4)–(2.7.7) with appropriate signs gives $[Bt \cap Vn\dot{r}V] - [Btr \cap Vn\dot{r}V]$, and substituting into (2.7.3) completes the proof of (2.7.1).

To complete the proof of Theorem (2.7) we now have to prove the formula (2.7.2). For this, we have

$$\gamma_{\dot{r}}^2 = [B\cap V\dot{r}V]^2 - [B\cap V\dot{r}V][Br\cap V\dot{r}V] - [Br\cap V\dot{r}V][B\cap V\dot{r}V] + [Br\cap V\dot{r}V]^2,$$

and we proceed to compute the four terms on the right.

$$\begin{aligned}
[B \cap V\dot{r}V]^2 &= [B \cap V\dot{r}V_a] \sum_{u \in U_a^\#} k(u)u \\
&= \sum_{u \in U_a^\#} [B \cap V\dot{r}V_a k(u)u] \\
&= \sum_{u \in U_a^\#} [B \cap V\dot{r}V_a f(u)\dot{r}g(u)] \qquad \text{(by (2.1))} \\
&= \sum_{v \in V_a^\#} [B \cap V\dot{r}V_a\dot{r}v] \quad \text{(since } g \text{ is a bijection from } U_a^\# \text{ to } V_a^\#\text{)} \\
&= \sum_{v \in V_a^\#} [B \cap V\dot{r}^2 v] + \sum_{v', v \in V_a^\#} [B \cap V\dot{r}v'\dot{r}v]
\end{aligned}$$

$$
\begin{aligned}
&= (q_a - 1)\dot r^2 + \sum_{\substack{u \in U_a^{\#} \\ v \in V_a^{\#}}} \dot r^2 [B \cap Vuv] \\
&= (q_a - 1)\dot r^2 + \sum_{\substack{u \in U_a^{\#} \\ v \in V_a}} \dot r^2 [B \cap Vh(u)f(u)\dot r g(u)v] - \sum_{u \in U_a^{\#}} \dot r^2 [B \cap Vu] \\
&= (q_a - 1)\dot r^2 + \dot r^2 \sum_{u \in U_a^{\#}} h(u)[B \cap V\dot r V] - \dot r^2 [U_a^{\#}] \\
&= (q_a - 1)\dot r^2 + \sum_{u \in U_a^{\#}} k(u)[B \cap V\dot r V] - \dot r^2 [U_a^{\#}] \qquad \text{(by (2.3) (ii)).} \qquad (2.7.8)
\end{aligned}
$$

Next we have

$$
[B \cap V\dot r V][Br \cap V\dot r V] = \sum_{u \in U_a^{\#}} k(u)u[U_a \dot r] = \sum_{u \in U_a^{\#}} k(u)[U_a]\dot r \qquad (2.7.9)
$$

and

$$
\begin{aligned}
[Br \cap V\dot r V][B \cap V\dot r V] &= [\dot r V_a] \sum_{u \in U_a^{\#}} f(u)\dot r g(u) \\
&= [\dot r V_a][\dot r V_a^{\#}], \qquad (2.7.10)
\end{aligned}
$$

while finally

$$
[Br \cap V\dot r V]^2 = [\dot r V_a][\dot r V_a]. \qquad (2.7.11)
$$

Now add the terms (2.7.8)–(2.7.11) with appropriate signs, obtaining

$$
\begin{aligned}
\gamma_{\dot r}^2 &= q_a \dot r^2 + \sum_{u \in U_a^{\#}} k(u)\gamma_{\dot r} \\
&= q_a \dot r^2 + \eta_{\dot r}\gamma_{\dot r}
\end{aligned}
$$

in the notation of (2.3.2). But $\gamma_{\dot r}$ trivially commutes with $\dot r^2$ and with $\gamma_{\dot r}^2$. It follows (since $\gamma_{\dot r}$ is invertible in $\mathbf{Q}G$) that $\gamma_{\dot r}$ commutes with $\eta_{\dot r}$. Hence again using (2.3) (ii), we have

$$
\gamma_{\dot r}^2 = q_a \gamma_{\dot r^2} + \gamma_{\dot r} \sum_{u \in U_a^{\#}} \gamma_{h(u)\dot r^2},
$$

which is (2.7.2). This completes the proof of Theorem (2.7). □

The map ϕ of (2.7) is not an embedding in the sense of (1.3). This follows easily from the next proposition, which deals with the effect of left multiplication by γ_n on the module $[U]\mathbf{Z}G$.

(2.8) PROPOSITION *Let a be a simple root and $r = r_a$. Then left multiplication by $\gamma_{\dot{r}}$ is the endomorphism $\sum_{u\in U_a^\#} T_{k(u)} - T_{\dot{r}}$ of $[U]\mathbf{Z}G$.*

Proof. We have

$$\gamma_{\dot{r}}[U] = \Big(\sum_{u\in U_a^\#} k(u)u - [U_a\dot{r}]\Big)[U] = \sum_{u\in U_a^\#} k(u)[U] - [U\dot{r}U]$$
$$= \Big(\sum_{u\in U_a^\#} T_{k(u)} - T_{\dot{r}}\Big)[U].$$

Since left multiplication obviously commutes with the $\mathbf{Z}G$ action on $[U]\mathbf{Z}G$, the result follows. □

(2.8)′ COROLLARY *The endomorphism $T_{\dot{r}}$ of $[U]\mathbf{Z}G$ is given by left multiplication by $\sum_{u\in U_a^\#} k(u) - \gamma_{\dot{r}} \in \Gamma$.*

The results of this section may be summarized in

(2.9) THEOREM *Let $E = \mathrm{End}_{\mathbf{Z}G}[U]\mathbf{Z}G$ where U is a maximal unipotent subgroup of the finite algebraic group G. (For a more precise definition of G see the beginning of this section.) Then*

(i) There is a map $\mu\colon E \to \mathbf{Z}G$ satisfying $T_h \mapsto \gamma_h$ (for $h \in H$) and $T_{\dot{r}} \mapsto \eta_{\dot{r}} - \gamma_{\dot{r}}$ (for $r = r_a \in S$, with $\eta_{\dot{r}}$ and $\gamma_{\dot{r}}$ as defined in (2.3.2) and (2.6) respectively), such that μ is an embedding of E in $\mathbf{Z}G$ in the sense of (1.3) (that is, $T \in E$ is given by left multiplication by $\mu(T)$), and $\mu(E) = \Gamma$, the $\mathbf{Z}$-linear span of the elements γ_n ($n \in N$).

(ii) There is an (involutory) automorphism α of E defined by $\alpha(T_h) = T_h$ for $h \in H$ and $\alpha(T_{\dot{r}}) = \sum_{u\in U_a^\#} T_{k(u)} - T_{\dot{r}}$ for $r = r_a \in S$.

Proof. (i) By Proposition (2.8) we see that the elements γ_h and $\gamma_{\dot{r}}$ induce endomorphisms of $[U]\mathbf{Z}G$ by left multiplication, and since these elements generate Γ the same holds for all $\gamma \in \Gamma$. Thus there is a map $\lambda\colon \Gamma \to E$ such that $\lambda(\gamma)$ is left multiplication by γ. It follows from (2.8) and (2.8)′ that T_h, $T_{\dot{r}} \in E$ are respectively given by left multiplication by $\mu(T_h)$, $\mu(T_{\dot{r}}) \in \Gamma$

as defined in the statement. Now since the T_h and the $T_{\dot{r}}$ generate E, it follows that every element of E is realized by left multiplication by some element of Γ; that is, λ is surjective. Since Γ and E both have $\mathbf{Z}$-rank $|N|$ it follows that λ is injective too, whence $\mu(T) = \lambda^{-1}(T)$ defines our embedding μ.

(ii) The map $\phi: T_n \mapsto \gamma_n$ is an isomorphism $E \to \Gamma$ (Theorem (2.7)) and the automorphism α is simply $\phi^{-1}\mu$. It is trivially an involution. □

REMARK. Notice that in the proof of (2.9) (i) we have only used the fact that Γ is a *subalgebra* of $\mathbf{Z}G$. This is the thrust of Theorem (2.7).

§3 Connection with Steinberg's representation

Maintaining the notation of §2, let $B = HU$ and write $\mathrm{St} = \sum_{w \in W} \varepsilon_w [Bw]$ where $\varepsilon_w = (-1)^{l(w)}$. The elements $\{ (\mathrm{St})u \mid u \in U \}$ are linearly independent since the coefficient of $\dot{w}_0 u_1$ in $\sum_{u \in U} \lambda_u (\mathrm{St})u$ is $\lambda_{u_1} \varepsilon_{w_0}$ (where w_0 is the longest element of W). Moreover, Steinberg's method (see Theorem 1 of [8]) may be applied to show

(3.1) PROPOSITION *The set* $\{ (\mathrm{St})u \mid u \in U \}$ *is a* $\mathbf{Z}$*-basis for the right* $\mathbf{Z}G$*-module* $(\mathrm{St})\mathbf{Z}G$.

We shall begin by proving

(3.2) LEMMA *Let* $V = \dot{w}_0^{-1} U \dot{w}_0$ *as in §2. Then the right* $\mathbf{Z}G$*-module* $[V]\mathbf{Z}G \otimes_{\mathbf{Z}} (\mathrm{St})\mathbf{Z}G$ *is cyclic, generated by* $[V] \otimes \mathrm{St}$.

Proof. Consider the submodule M generated by $[V] \otimes \mathrm{St}$. Applying $\dot{w}_0$ we obtain $\varepsilon_{w_0}[V]\dot{w}_0 \otimes \mathrm{St}$, and since for $u \in U$ we have $[V]\dot{w}_0 u = [V]\dot{w}_0$ we may apply elements of U and obtain that $[V]\dot{w}_0 \otimes (\mathrm{St})\mathbf{Z}G \subseteq M$ (by (3.1)). The result now follows trivially. □

(3.2)′ COROLLARY *There is a* $\mathbf{Z}G$*-isomorphism* $\mathbf{Z}G \to [V]\mathbf{Z}G \otimes_{\mathbf{Z}} (\mathrm{St})\mathbf{Z}G$ *defined by* $1 \mapsto [V] \otimes \mathrm{St}$.

Proof. Since $\mathbf{Z}G$ is free $1 \mapsto [V] \otimes \mathrm{St}$ defines a map. It is surjective by (3.2), and an isomorphism since the two modules have the same $\mathbf{Z}$-rank and are $\mathbf{Z}$-free. □

Now $\mathrm{End}_{\mathbf{Z}G}\,\mathbf{Z}G = \{\,\lambda_\beta \mid \beta \in \mathbf{Z}G\,\}$, where $\lambda_\beta(\xi) = \beta\xi$ for $\xi \in \mathbf{Z}G$, and $\beta \mapsto \lambda_\beta$ is an isomorphism $\mathbf{Z}G \to \mathrm{End}_{\mathbf{Z}G}\,\mathbf{Z}G$. Hence from (3.2)$'$ we deduce

(3.3) *There is an isomorphism* $\mathbf{Z}G \to \mathrm{End}_{\mathbf{Z}G}([V]\mathbf{Z}G \otimes_{\mathbf{Z}} (\mathrm{St})\mathbf{Z}G)$ *given by* $\beta \mapsto \nu(\beta)$, *where* $\nu(\beta)\colon ([V] \otimes (\mathrm{St}))\xi \mapsto ([V] \otimes (\mathrm{St}))\beta\xi$ *for all* ξ, $\beta \in \mathbf{Z}G$.

Let $E' = \mathrm{End}_{\mathbf{Z}G}[V]\mathbf{Z}G$. This has $\mathbf{Z}$-basis $\{\,T'_n \mid n \in N\,\}$, where $T'_n([V]) = [VnV]$ for each $n \in N$. Since $\dot{w}_0[V] = [U]\dot{w}_0$ there is an isomorphism $\omega\colon [V]\mathbf{Z}G \to [U]\mathbf{Z}G$ given by $\omega(x) = \dot{w}_0 x$ for all $x \in [V]\mathbf{Z}G$, and therefore

(3.4) *There is an isomorphism* $\widetilde{\omega}\colon E \to E'$ *given by*

$$\widetilde{\omega}(\zeta) = \omega^{-1}\zeta\omega \qquad (\zeta \in \mathrm{End}_{\mathbf{Z}G}[U]\mathbf{Z}G)$$

where (as above) ω *is left multiplication by* $\dot{w}_0$.

A simple calculation shows that

$$\widetilde{\omega}(T_n) = T'_{\dot{w}_0^{-1} n \dot{w}_0}. \tag{3.4.1}$$

Now there is a natural embedding $E' \to \mathrm{End}_{\mathbf{Z}G}([V]\mathbf{Z}g \otimes_{\mathbf{Z}} (\mathrm{St})\mathbf{Z}G)$ given by $\theta \mapsto \theta \otimes \mathrm{id}_{(\mathrm{St})\mathbf{Z}G}$. So by (3.3) there is an algebra monomorphism $E' \to \mathbf{Z}G$ such that $\theta \mapsto \beta$, where $\theta \otimes \mathrm{id}_{(\mathrm{St})\mathbf{Z}G} = \nu(\beta)$. Pulling back via $\widetilde{\omega}$ gives the following statement.

(3.5) THEOREM *We maintain the above notation. Then*

(i) *We have* $T'_{\dot{r}} \otimes \mathrm{id}_{(\mathrm{St})\mathbf{Z}G} = \nu(\gamma_{\dot{r}})$; *that is,*

$$(T'_{\dot{r}}[V] \otimes \mathrm{St})\xi = ([V] \otimes \mathrm{St})\gamma_{\dot{r}}\xi$$

for $\xi \in \mathbf{Z}G$, $a \in \Pi$ *and* $r = r_a \in S$.

(ii) *The map* $T'_n \mapsto \gamma_n$ *defines an isomorphism* $E' = \mathrm{End}_{\mathbf{Z}G}[V]\mathbf{Z}G \to \Gamma$ *which pulls back via* $\widetilde{\omega}$ *(see (3.4)) to the isomorphism* $\eta\colon E \to \Gamma$, *where* $\eta(T_n) = \gamma_{\dot{w}_0 n \dot{w}_0}$.

Proof. (i) It suffices to show that $([V] \otimes \mathrm{St})\gamma_{\dot{r}} = [V\dot{r}V] \otimes \mathrm{St}$. Now

$$([V] \otimes \mathrm{St})\gamma_{\dot{r}} = \sum_{u \in U_a^{\#}} ([V] \otimes \mathrm{St})k(u)u - \sum_{u \in U_a} ([V] \otimes \mathrm{St})u\dot{r}. \tag{3.5.1}$$

Using (2.1)we have

$$\sum_{u\in U_a^{\#}} ([V]\otimes \mathrm{St})k(u)u = \sum_{u\in U_a^{\#}} [V]\dot r g(u)\otimes(\mathrm{St})u. \tag{3.5.2}$$

The second term on the right side of (3.5.1) is

$$-([V]\dot r\otimes \mathrm{St}) + \sum_{u\in U_a^{\#}} [V]u\dot r\otimes(\mathrm{St})u\dot r. \tag{3.5.3}$$

Now to compute $(\mathrm{St})u\dot r$ for $u\in U_a$, take $w\in W$ with $l(wr) > l(w)$. Then $BwB_a = Bw$, and so $[Bw] = [X][B_a]$ for some transversal X. Thus

$$\begin{aligned}([Bw]-[Bwr])u\dot r &= [X]([B_ar]-[B_a])u\dot r\\ &= [X]([B_ar]-[B_arf(u)\dot r g(u)\dot r])\\ &= [X][B_ar](1-g(u)^{\dot r})\\ &= [X]([B_ar]-[B_a])(1-g(u)^{\dot r})\\ &= ([Bw]-[Bwr])(g(u)^{\dot r}-1).\end{aligned}$$

Therefore

$$(\mathrm{St})u\dot r = (\mathrm{St})(g(u)^{\dot r}-1). \tag{3.5.4}$$

Thus, using Lemma (2.4), we obtain

$$\sum_{u\in U_a^{\#}} [V]u\dot r\otimes(\mathrm{St})(g(u)^{\dot r}-1) = \sum_{u\in U_a^{\#}} [V]\dot r g(u)\otimes(\mathrm{St})(u-1).$$

Hence the expression (3.5.3) becomes

$$\begin{aligned}&-([V]\dot r\otimes \mathrm{St}) - \sum_{u\in U_a^{\#}} [V]\dot r g(u)\otimes \mathrm{St} + \sum_{u\in U_a^{\#}} [V]\dot r g(u)\otimes(\mathrm{St})u\\ &= -[V\dot rV]\otimes \mathrm{St} + \sum_{u\in U_a^{\#}} [V]\dot r g(u)\otimes(\mathrm{St})u. \qquad (3.5.5)\end{aligned}$$

Now substitute into (3.5.1) using (3.5.2), obtaining

$$\begin{aligned}([V]\otimes \mathrm{St}\gamma_{\dot r} &= \sum_{u\in U_a^{\#}} [V]\dot r g(u)\otimes(\mathrm{St})u + [V\dot rV]\otimes \mathrm{St} - \sum_{u\in U_a^{\#}} [V]\dot r g(u)\otimes(\mathrm{St})u\\ &= [V\dot rV]\otimes \mathrm{St}\\ &= (T'_{\dot r}\otimes \mathrm{id})([V]\otimes \mathrm{St})\end{aligned}$$

which completes the proof of (i).

(ii) Since $T'_h = \nu(h) = \nu(\gamma_h)$ (for $h\in H$) and E' is generated by the T'_h together with the $T'_{\dot r}$ for $r\in S$, the result follows from (i) and the discussion immediately preceding (3.5) (and Theorem (2.7)). □

(3.6) COROLLARY *The algebra E has another automorphism, namely, the map β defined by $\beta(T_n) = T_{\dot{w}_0^{-1} n \dot{w}_0}$. Moreover, if the transversal $\{ \dot{w} \mid w \in W \}$ is chosen so that $\dot{w} = \dot{w}_1 \dot{w}_2$ whenever $w = w_1 w_2$ with $l(w) = l(w_1) + l(w_2)$ then β is involutory.*

Proof. The automorphism β is given by $\beta = \phi^{-1}\eta$ where ϕ is the isomorphism $E \to \Gamma$ of (2.7). The involutory nature of β follows from the fact that the stated assumptions on the $\dot{w}$ imply that $\dot{w}_0^2$ is in the centre of N. This is proved as follows. Let $r \in S$ and write $r' = w_0 r w_0^{-1} \in S$. Then $w_0 = w'r' = rw'$ where $w' = rw_0$ has length $l(w_0) - 1$. By assumption $\dot{w}_0 = \dot{w}'\dot{r}' = \dot{r}\dot{w}'$, whence $\dot{w}_0(\dot{r}')^{-1} = (\dot{r})^{-1}\dot{w}_0$ and $\dot{w}_0^{-1}\dot{r}\dot{w}_0 = \dot{r}'$. By symmetry $\dot{w}_0^{-1}\dot{r}'\dot{w}_0 = \dot{r}$, and hence $\dot{w}_0^2$ commutes with $\dot{r}$. Since $\dot{w}_0^2$ lies in H (which is abelian) it also commutes with all elements of H, and hence with all elements of N, since N is generated by H and the elements $\dot{r}$ for $r \in S$. □

REMARK. The algebra $\Gamma \subseteq \mathbf{Z}G$ appears in yet a third way, since another computation (different from the one above) shows that in the *left* $\mathbf{Z}G$-module $\mathbf{Z}G[V] \otimes \mathbf{Z}G(\mathrm{St}) = \mathbf{Z}G([V] \otimes \mathrm{St}) \cong \mathbf{Z}G$ we have

(3.7) $$\gamma_{\dot{r}}([V] \otimes \mathrm{St}) = [V\dot{r}V] \otimes \mathrm{St}.$$

§4 Connection with principal series

The principal series of G is realized by the module $[B]\mathbf{Z}G$, which is a submodule of $[U]\mathbf{Z}G$ and is fixed by each of the endomorphisms in E (since $T_n[B] = [UnU][H] = [BnB]$); moreover, each endomorphism in the algebra $\overline{E} = \mathrm{End}_{\mathbf{Z}G}[B]\mathbf{Z}G$ is the restriction of an endomorphism in E. Thus

(4.1) *There is an epimorphism $\rho\colon E \to \overline{E}$ given by $\rho(T_n) = \overline{T}_n = T_n|_{[B]\mathbf{Z}G}$.*

Clearly $\overline{T}_n = \overline{T}_{n'}$ if and only if $\bar{n} = \overline{n'} \in W$, and $\overline{E}$ has $\mathbf{Z}$-basis consisting of $\{ T_w \mid w \in W \}$, where $T_w = \overline{T}_n$ for any $n \in N$ such that $\bar{n} = w$.

For any integer a and any $\mathbf{Z}$-module M denote by M_a the $\mathbf{Z}[a^{-1}]$-module $M \otimes_{\mathbf{Z}} \mathbf{Z}[a^{-1}]$.

(4.2) THEOREM *(i) The map* $\tau: \overline{T}_n \mapsto |H|^{-1} \sum_{h \in H} T_h T_n$ *defines a monomorphism* $\overline{E}_{|H|} \to E_{|H|}$.

(ii) For $w \in W$ *let* $\gamma_w = |H|^{-1}[H]\gamma_n$, *where* n *is any element of* N *such that* $\bar{n} = w$. *Then* $\gamma_w = |H|^{-1} \sum_{t \in W} \varepsilon_w [Bt \cap DwD]$, *where* $D = HV$, *and* $\gamma_w = h_w$ *in the notation of [3], (1.8).*

(iii) The map $(\phi \otimes \mathrm{id})\tau: \overline{E}_{|H|} \to \Gamma_{|H|}$ *is the isomorphism of [3], Theorem (1.7).*

(iv) The map $(\mu \otimes \mathrm{id})\tau: \overline{E}_{|H|} \to \mathbf{Z}G_{|H|}$ *is an embedding in the sense of (1.3), and coincides with the embedding of (1.11′) of [3].*

(v) The involution $T_w \mapsto \widehat{T}_w$ *of [3] is realized as the restriction of* $\alpha \otimes \mathrm{id}$ *(see (2.7) above) to* $\tau(\overline{E})$.

All the above statements are straightforward consequences of the results of §2 above.

This puts the results of [3] into a natural setting, and shows why the stipulation that one should be able to divide by $|H|$ in the case of $\mathrm{Ind}_B^G(1)$ is a natural one. It also makes explicit that the obstruction to carrying out the embeddings of [3] in arbitrary characteristic are cohomological (cf. Tits [9]).

§5 Concluding remarks

(5.1) In §4 of [3] certain almost-idempotents $e_J \in \overline{E} \otimes_{\mathbf{Z}} \mathbf{Z}(|H|^{-1})$ were constructed (for each $J \subseteq \Pi$), which, over a field k of characteristic p (where $p|q$), were used to give an algorithmic decomposition of $\mathrm{Ind}_B^G(1)$ into indecomposables, each of which has irreducible socle. We hope in a later work to produce idempotents $e_J(\lambda) \in E \otimes_{\mathbf{Z}} k$, one for each character $\lambda: H \to k^*$, which will play an analogous role for the representation $\mathrm{Ind}_U^G(1)$. Since the socle of this representation is the direct sum of all the irreducible representations of G, each occurring with multiplicity one, this would be a significant construction.

(5.2) The sets $\boldsymbol{B}t \cap \boldsymbol{V}n\boldsymbol{V}$ in the overlying algebraic group $\boldsymbol{G}$ are locally closed in $\boldsymbol{G}$, and one might ask whether our multiplication formulae for the alternating sums of their "characteristic functions" reflect some geometric facts concerning composition of sheaves on "Schubert-like varieties", in analogy with the case (cf. [7]) of the ordinary Hecke algebra (cf. [4]).

(5.3) The indecomposable summands of $\mathrm{Ind}_B^G(\lambda)$ (or $\mathrm{Ind}_U^G(1)$) in characteristic p can be constructed homologically from coefficient systems on the

Tits building (see [5] and [6]). A knowledge of the $e_J(\lambda)$ ((5.1) above) would assist in the analysis of these direct summands.

References

1. N. Bourbaki, *Groupes et algèbres de Lie, Chap. IV, V et VI* Hermann, Paris (1968).
2. C. Chevalley, *Séminaire sur le classification des groupes de Lie algébriques* Paris (1956–58).
3. R. B. Howlett and G. I. Lehrer, 'Embeddings of Hecke Algebras in group algebras', *J. Alg.* **105** (1987) 159–174.
4. N. Iwahori, 'On the structure of the Hecke ring of a Chevalley group over a finite field', *J. Fac. Sci. Univ. Tokyo* **10** (1964) 214–236.
5. G. I. Lehrer, 'The spherical building and regular semisimple elements', *Bull. Austral. Math. Soc.* **27** (1983) 361–379.
6. M-T. Schmidt, 'Beziehungen zwischen Homologie-Darstellungen und der Hauptserie endlicher Chevalley-Gruppen', *Bonner Math. Schr.* Bonn (1986).
7. T. A. Springer, 'Quelques applications de la cohomologie d'intersection', *Astérisque* **92–93** (Sém. Bourbaki 589) (1982) 249–273.
8. R. Steinberg, 'Prime power representations of finite linear groups II', *Can. J. Math.* **9** (1957) 347–351.
9. J. Tits, 'Normalisateurs de tores I. Groupes de Coxeter étendus', *J. Alg.* **4** (1966) 96–116.
10. T. Yokonuma, 'Sur le commutant d'une représentation d'un groupe de Chevalley finis', *J. Fac. Sci. Univ. Tokyo* **15** (1968) 115–129; II ibid. **16** (1969), 65–82.

Department of Pure Mathematics
University of Sydney
N.S.W. 2006
Australie