LIFTING INVOLUTIONS IN A WEYL GROUP
TO THE TORUS NORMALIZER

G. LUSZTIG

ABSTRACT. Let N be the normalizer of a maximal torus T in a split reductive group over F_q, and let w be an involution in the Weyl group N/T. We explicitly construct a lifting n of w in N such that the image of n under the Frobenius map is equal to the inverse of n.

INTRODUCTION

0.1. Let $\mathbf{k}$ be an algebraically closed field. Let G be a connected reductive algebraic group over $\mathbf{k}$. Let T be a maximal torus of G, and let U be the unipotent radical of a Borel subgroup of G containing T. Let N be the normalizer of T in G, let $W = N/T$ be the Weyl group, and let $\kappa : W \to N$ be the obvious map. Let $w \mapsto |w|$ be the length function on W and let $S = \{w \in W; |w| = 1\}$. Let $Y = \operatorname{Hom}(\mathbf{k}^*, T)$. We write the group operation on Y as addition. For each $s \in S$ we denote by $\check{\alpha}_s \in Y$ the corresponding simple coroot; let L be the subgroup of Y generated by $\{\check{\alpha}_s; s \in S\}$. Now W acts on T by $w : t \mapsto w(t) = ntn^{-1}$, where $n \in \kappa^{-1}(w)$; this induces an action of W on Y and L by $w : y \mapsto y'$, where $y'(z) = w(y(z))$ for $z \in \mathbf{k}^*$. We fix a pinning $\{x_s : \mathbf{k} \to G, y_s : \mathbf{k} \to G; s \in S\}$ associated to T, U and we denote by $w \mapsto \dot{w}$ be the corresponding Tits cross-section [T] of $\kappa : N \to W$. A *halving* of S is a subset S' of S such that $s_1 s_2 = s_2 s_1$ whenever s_1, s_2 in S are both in S' or both in $S - S'$. Clearly a halving of S exists. Let $W_2 = \{w \in W; w^2 = 1\}$. Let $\epsilon = -1 \in \mathbf{k}^*$. It turns out that, when $w \in W_2$, one can define representatives for w in $\kappa^{-1}(w)$ other than $\dot{w}$, which in a certain sense are better behaved than $\dot{w}$ (see 0.5). Namely, for $w \in W_2$, $c \in \mathbf{k}^*$ and for a halving S' of S we will consider the element

$$n_{w,c,S'} = \dot{w} r_w(c) b_w^{S'}(\epsilon) \in \kappa^{-1}(w),$$

where $r_w \in L$, $b_w \in L/2L$ are given by Theorems 0.2 and 0.3 below. (We then have $r_w(c) \in T$ and $b_w^{S'}(\epsilon) \in T$: if $y \in L$, then $y(\epsilon) \in T$ depends only on the image of y in $L/2L$; hence $y(\epsilon) \in T$ is defined for any $y \in L/2L$.)

Theorem 0.2. *There is a unique map $W_2 \to L$, $w \mapsto r_w$ such that* (i)–(iii) *below hold:*

(i) $r_1 = 0$, $r_s = \check{\alpha}_s$ *for any* $s \in S$;

(ii) *for any* $w \in W_2, s \in S$ *such that* $sw \neq ws$, *we have* $s(r_w) = r_{sws}$;

(iii) *for any* $w \in W_2, s \in S$ *such that* $sw = ws$, *we have* $r_{sw} = r_w + \mathcal{N}\check{\alpha}_s$ *where* $\mathcal{N} \in \mathbf{Z}$.

Moreover, in (iii) *we necessarily have* $\mathcal{N} \in \{-1, 0, 1\}$; *if in addition* G *is simply laced we have* $\mathcal{N} \in \{-1, 1\}$. *We have:*
   (iv) *if* w, s *are as in* (iii) *and* $|sw| > |w|$, *then* $s(r_w) = r_w$;
   (v) *if* $w \in W_2$, *then* $w(r_w) = -r_w$.

A part of the proof of the existence part of the theorem is based on constructing a basis consisting of certain positive roots (including the highest root) for the reflection representation of W assuming that the longest element is central. After I found this basis, I realized that this basis is the "cascade of roots" that B. Kostant has talked about on several occasions. In 2012 he wrote a paper [Kos12] about the cascade. (I thank D. Vogan for supplying this reference.) The proof of property (iii) is based on a case-by-case verification.

Theorem 0.3. *Let* S' *be a halving of* S. *There is a unique map* $b = b^{S'} : W_2 \to L/2L, w \mapsto b_w = b_w^{S'}$ *such that* (i)–(iii) *below hold:*
   (i) $b_1 = 0$, $b_s = \check{\alpha}_s$ *for any* $s \in S'$, *and* $b_s = 0$ *for any* $s \in S - S'$;
   (ii) *for any* $w \in W_2, s \in S$ *such that* $sw \neq ws$, *we have* $s(b_w) = b_{sws} + \check{\alpha}_s$;
   (iii) *for any* $w \in W_2, s \in S$ *such that* $sw = ws$, *we have* $b_{sw} = b_w + l\check{\alpha}_s$, *where* $l \in \{0, 1\}$;
   Moreover,
   (iv) *for any* $w \in W_2, s \in S$ *such that* $sw = ws$, *we have* $s(b_w) = b_w + (\mathcal{N} + 1)\check{\alpha}_s$, *where* $r_{sw} = r_w + \mathcal{N}\check{\alpha}_s, \mathcal{N} \in \mathbf{Z}$;
   (v) $b_w(\epsilon)w(b_w(\epsilon)) = r_w(\epsilon)\dot{w}^2$, *or equivalently* $(\dot{w}b_w(\epsilon))^2 = r_w(\epsilon)$.

A part of the proof of this theorem is based on computer calculation.

0.4. In this subsection we assume that (i) or (ii) below holds:
   (i) $\mathbf{k}$ is an algebraic closure of a finite field F_q with q elements;
   (ii) $\mathbf{k} = \mathbf{C}$.
   We define $\phi : \mathbf{k} \to \mathbf{k}$ by $\phi(c) = c^q$ in case (i) and $\phi(c) = \bar{c}$ (complex conjugation) in case (ii). In case (i) we assume that G has a fixed F_q-rational structure with Frobenius map $\phi : H \to H$ such that $\phi(t) = t^q$ for all $t \in T$.
   In case (ii) we assume that G has a fixed $\mathbf{R}$-rational structure so that $G(\mathbf{R})$ is the fixed point set of an antiholomorphic involution $\phi : G \to G$ such that $\phi(y(c)) = y(\phi(c))$ for any $y \in Y, c \in \mathbf{k}^*$.
   In both cases we assume that ϕ is compatible with the fixed pinning of G attached to T, U so that $\phi(\dot{w}) = \dot{w}$ for any $w \in W$. In both cases we define $\phi' : G \to G$ by $\phi'(g) = \phi(g)^{-1}$. In case (i), ϕ' is a Frobenius map for an F_q-rational structure on G which is not in general compatible with the group structure. In case (ii), ϕ' is an antiholomorphic involution of G not in general compatible with the group structure. Hence $G^{\phi'} = \{g \in G; \phi(g)g = 1\}$ is not in general a subgroup of G.
   In both cases we set

$$N^{\phi'} = \{g \in N; \phi(g)g = 1\} = N \cap G^{\phi'}.$$

Since $\phi(\dot{w}) = \dot{w}$, we see that for $w \in W$, $\kappa^{-1}(w) \cap N^{\phi'} = \emptyset$ if $w \in W - W_2$.
   We define $\phi' : \mathbf{k} \to \mathbf{k}$ by $\phi'(c) = -\phi(c)$. In case (i) we have $\mathbf{k}^{\phi'} = \{x \in \mathbf{k}; x^q = -x\}$, and in case (ii) we have $\mathbf{k}^{\phi'} = \{x \in \mathbf{C}; \bar{x} + x = 0\}$, the set of purely imaginary complex numbers.
   Note that for $w \in W_2$, $\dot{w}$ is not necessarily in $N^{\phi'}$. The following result provides some explicit elements in $\kappa^{-1}(w)$ which do belong to $N^{\phi'}$.

Theorem 0.5. *We assume that we are in the setup of subsection 0.4. Let $w \in W_2$, let $c \in \mathbf{k}^*$, and let S' be a halving of S. We have $\phi'(n_{w,c,S'}) = n_{w,\phi'(c),S'}$. Hence if $c \in \kappa^{\phi'}$ we have $n_{w,c,S'} \in N^{\phi'}$.*

0.6. If $X \subset X'$ are sets and $\iota : X' \to X'$ satisfies $\iota(X) \subset X$, we write $X^{\iota} = \{x \in X ; \iota(x) = x\}$.

1. The one parameter group r_w attached to an involution w in W

1.1. Let R' be a root system in an $\mathbf{R}$-vector space $\mathbf{X}'$ of finite dimension; we assume that R' generates $\mathbf{X}$ and that multiplication by -1 (viewed as a linear map $\mathbf{X}' \to \mathbf{X}'$) is contained in the Weyl group W' of R'. We assume that we are given a set of positive roots R'^+ for R'. Let $\mathbf{Y}' = \operatorname{Hom}(\mathbf{X}', \mathbf{R})$. Let $\langle , \rangle : \mathbf{Y}' \times \mathbf{X}' \to \mathbf{R}$ be the obvious pairing. Let $\check{R}' \subset \mathbf{Y}'$ be the set of coroots; let $\alpha \leftrightarrow \check{\alpha}$ be the usual bijection $R' \leftrightarrow \check{R}'$. Let $\check{R}'^+ = \{\check{\alpha}; \alpha \in R'^+\}$. For $\alpha \in R'$ let $s_\alpha : \mathbf{X}' \to \mathbf{X}'$ and $s_\alpha : \mathbf{Y}' \to \mathbf{Y}'$ be the reflections defined by α.

For α, α' in R'^+ we write $\alpha \leq \alpha'$ if $\alpha' - \alpha \in \sum_{\beta \in R'^+} \mathbf{R}_{\geq 0}\beta$. This is a partial order on R'^+.

Let $\mathcal{E}_1$ be the set of maximal elements of R'^+. For $i \geq 2$, let $\mathcal{E}_i$ be the set of maximal elements of

$$\{\alpha \in R'^+ ; \langle \check{\alpha}', \alpha \rangle = 0 \text{ for any } \alpha' \in \mathcal{E}_1 \cup \mathcal{E}_2 \cup \cdots \cup \mathcal{E}_{i-1}\}.$$

Note that $\mathcal{E}_1, \mathcal{E}_2, \ldots$ are mutually disjoint. Let

$$\check{\mathcal{E}}_i = \{\check{\alpha}; \alpha \in \mathcal{E}_i\}, \quad \mathcal{E} = \bigcup_{i \geq 1} \mathcal{E}_i, \quad \check{\mathcal{E}} = \bigcup_{i \geq 1} \check{\mathcal{E}}_i.$$

The definition of $\mathcal{E}, \check{\mathcal{E}}$ given above is due to B. Kostant [Kos12] who called them *cascades*.

From the definition we see that:

(a) *if $\alpha \in \mathcal{E}, \alpha' \in \mathcal{E}, \alpha \neq \alpha'$, then $\langle \check{\alpha}', \alpha \rangle = 0$.*

We note the following property:

(b) *$\check{\mathcal{E}}$ is basis of $\mathbf{Y}'$.*

For a proof see [Kos12]. Alternatively, we can assume that our root system is irreducible and we can verify (b) by listing the elements of $\check{\mathcal{E}}$ in each case. (We denote the simple roots by $\{\alpha_i; i \in [1, l]\}$ as in [Bou68].)

Type A_1: $\check{\alpha}_1$.

Type $B_l, l = 2n + 1 \geq 3$: $\check{\alpha}_1 + 2\check{\alpha}_2 + \cdots + 2\check{\alpha}_{2n} + \check{\alpha}_{2n+1}, \check{\alpha}_3 + 2\check{\alpha}_4 + \cdots + 2\check{\alpha}_{2n} + \check{\alpha}_{2n+1}, \ldots, \check{\alpha}_{2n-1} + 2\check{\alpha}_{2n} + \check{\alpha}_{2n+1}, \check{\alpha}_1, \check{\alpha}_3, \ldots, \check{\alpha}_{2n+1}$.

Type $B_l, l = 2n \geq 3$: $\check{\alpha}_1 + 2\check{\alpha}_2 + \cdots + 2\check{\alpha}_{2n-1} + \check{\alpha}_{2n}, \check{\alpha}_3 + 2\check{\alpha}_4 + \cdots + 2\check{\alpha}_{2n-1} + \check{\alpha}_{2n}, \ldots, \check{\alpha}_{2n-1} + \check{\alpha}_{2n}, \check{\alpha}_1, \check{\alpha}_3, \ldots, \check{\alpha}_{2n-1}$.

Type $C_l, l \geq 2$: $\check{\alpha}_1 + \check{\alpha}_2 + \cdots + \check{\alpha}_{l-1} + \check{\alpha}_l, \check{\alpha}_2 + \cdots + \check{\alpha}_{l-1} + \check{\alpha}_l, \ldots, \check{\alpha}_l$.

Type $D_l, l = 2n \geq 4$: $\check{\alpha}_1 + 2\check{\alpha}_2 + 2\check{\alpha}_3 + \cdots + 2\check{\alpha}_{2n-2} + \check{\alpha}_{2n-1} + \check{\alpha}_{2n}, \check{\alpha}_3 + 2\check{\alpha}_4 + 2\check{\alpha}_5 + \cdots + 2\check{\alpha}_{2n-2} + \check{\alpha}_{2n-1} + \check{\alpha}_{2n}, \ldots, \check{\alpha}_{2n-3} + 2\check{\alpha}_{2n-2} + \check{\alpha}_{2n-1} + \check{\alpha}_{2n}, \check{\alpha}_1, \check{\alpha}_3, \ldots, \check{\alpha}_{2n-3}, \check{\alpha}_{2n-1}, \check{\alpha}_{2n}$.

Type E_7: $2\check{\alpha}_1 + 2\check{\alpha}_2 + 3\check{\alpha}_3 + 4\check{\alpha}_4 + 3\check{\alpha}_5 + 2\check{\alpha}_6 + \check{\alpha}_7, \check{\alpha}_2 + \check{\alpha}_3 + 2\check{\alpha}_4 + 2\check{\alpha}_5 + 2\check{\alpha}_6 + \check{\alpha}_7, \check{\alpha}_2 + \check{\alpha}_3 + 2\check{\alpha}_4 + \check{\alpha}_5, \check{\alpha}_7, \check{\alpha}_2, \check{\alpha}_3, \check{\alpha}_5$.

Type E_8: $2\check{\alpha}_1 + 3\check{\alpha}_2 + 4\check{\alpha}_3 + 6\check{\alpha}_4 + 5\check{\alpha}_5 + 4\check{\alpha}_6 + 3\check{\alpha}_7 + 2\check{\alpha}_8, 2\check{\alpha}_1 + 2\check{\alpha}_2 + 3\check{\alpha}_3 + 4\check{\alpha}_4 + 3\check{\alpha}_5 + 2\check{\alpha}_6 + \check{\alpha}_7, \check{\alpha}_2 + \check{\alpha}_3 + 2\check{\alpha}_4 + 2\check{\alpha}_5 + 2\check{\alpha}_6 + \check{\alpha}_7, \check{\alpha}_2 + \check{\alpha}_3 + 2\check{\alpha}_4 + \check{\alpha}_5, \check{\alpha}_7, \check{\alpha}_2, \check{\alpha}_3, \check{\alpha}_5$.

Type F_4: $2\check{\alpha}_1 + 3\check{\alpha}_2 + 2\check{\alpha}_3 + \check{\alpha}_4, \check{\alpha}_2 + \check{\alpha}_3 + \check{\alpha}_4, \check{\alpha}_2 + \check{\alpha}_3, \check{\alpha}_2$.

Type G_2: $\check{\alpha}_1 + 2\check{\alpha}_2, \check{\alpha}_1$.

We note the following result (see [Kos12]):

(c) *The reflections* $\{s_\beta : \mathbf{Y}' \to \mathbf{Y}'; \beta \in \mathcal{E}\}$ *commute with each other and their product (in any order) is equal to* -1.

Let α, α' in $\mathcal{E}$ be such that $\alpha \neq \alpha'$. Using (a) we see that $s_\alpha(\alpha') = \alpha'$. We also have $s_\alpha(\alpha) = -\alpha$. Now the result follows from (b).

1.2. Let $R', \check{R}', W'$ be as in subsection 1.1. Let L' be the subgroup of $\mathbf{Y}'$ generated by $\check{R}'$. We set
$$r = \sum_{\beta \in \check{\mathcal{E}}} \beta \in L'.$$
We list the values of r for various types (assumimg that R' is irreducible):

Type A_1: $r = \check{\alpha}_1$.

Type $B_l, l = 2n + 1 \geq 3$: $r = 2\check{\alpha}_1 + 2\check{\alpha}_2 + 4\check{\alpha}_3 + 4\check{\alpha}_4 + \cdots + 2n\check{\alpha}_{2n-1} + 2n\check{\alpha}_{2n} + (n+1)\check{\alpha}_{2n+1}$.

Type $B_l, l = 2n \geq 4$: $r = 2\check{\alpha}_1 + 2\check{\alpha}_2 + 4\check{\alpha}_3 + 4\check{\alpha}_4 + \cdots + 2(n-1)\check{\alpha}_{2n-3} + 2(n-1)\check{\alpha}_{2n-2} + 2n\check{\alpha}_{2n-1} + n\check{\alpha}_{2n}$.

Type $C_l, l \geq 2$: $r = \check{\alpha}_1 + 2\check{\alpha}_2 + \cdots + l\check{\alpha}_l$.

Type $D_l, l = 2n \geq 4$: $r = 2\check{\alpha}_1 + 2\check{\alpha}_2 + 4\check{\alpha}_3 + 4\check{\alpha}_4 + \cdots + (2n-2)\check{\alpha}_{2n-3} + (2n-2)\check{\alpha}_{2n-2} + n\check{\alpha}_{2n-1} + n\check{\alpha}_{2n}$.

Type E_7: $r = 2\check{\alpha}_1 + 5\check{\alpha}_2 + 6\check{\alpha}_3 + 8\check{\alpha}_4 + 7\check{\alpha}_5 + 4\check{\alpha}_6 + 3\check{\alpha}_7$.

Type E_8: $r = 4\check{\alpha}_1 + 8\check{\alpha}_2 + 10\check{\alpha}_3 + 14\check{\alpha}_4 + 12\check{\alpha}_5 + 8\check{\alpha}_6 + 6\check{\alpha}_7 + 2\check{\alpha}_8$.

Type F_4: $r = 2\check{\alpha}_1 + 6\check{\alpha}_2 + 4\check{\alpha}_3 + 2\check{\alpha}_4$.

Type G_2: $r = 2\check{\alpha}_1 + 2\check{\alpha}_2$.

Note that in each case the sum of coefficients of r is equal to $(\sharp(R'^+) + \mathrm{rank}(R'))/2$.

If R' is irreducible and simply laced, we have $r/2 = \sum_{i \in [1,l]} \delta_i \omega_i$, where $\omega_i \in \mathbf{Y}'$ are the fundamental coweights (that is $\langle \omega_i, \alpha_j \rangle = \delta_{ij}$) and $\delta_i = \pm 1$ are such that $\delta_i + \delta_j = 0$ when i, j are joined in the Coxeter graph; moreover, we have $\delta_i = -1$ if in the extended (affine) Coxeter graph i is joined with the vertex outside the unextended Coxeter graph. Another way to state this is that the coefficient of $\check{\alpha}_i$ in r is equal to half the sum of the coefficients of the neighbouring $\check{\alpha}_j$ (that is, with j joined with i in the Coxeter graph) plus or minus 1. For example in type E_8 we have:
$$4 = \frac{10}{2} - 1, 10 = \frac{4+14}{2} + 1, 8 = \frac{14}{2} + 1, 14 = \frac{8+10+12}{2} - 1, 12 = \frac{8+14}{2} + 1,$$
$$8 = \frac{6+12}{2} - 1, 6 = \frac{2+8}{2} + 1, 2 = \frac{6}{2} - 1.$$
Note that the sign of ± 1 in this formula changes when one moves from one $\check{\alpha}_i$ to a neighbouring one.

1.3. In the remainder of this section we place ourselves in the setup of subsection 0.1. Let $X = \mathrm{Hom}(T, \mathbf{k}^*)$. We write the group operation in X as addition. Let $\mathbf{X} = \mathbf{R} \otimes X, \mathbf{Y} = \mathbf{R} \otimes Y$. Let $\langle, \rangle : \mathbf{Y} \times \mathbf{X} \to \mathbf{R}$ be the obvious nondegenerate bilinear pairing. The W-action on Y in subsection 0.1 induces a linear W-action on $\mathbf{Y}$. We define an action of W on X by $w : x \mapsto x'$, where $x'(t) = x(w^{-1}(t))$ for $t \in T$. This induces a linear W-action on $\mathbf{X}$. Let $R \subset X$ be the set of roots; let $\check{R} \subset Y$ be the set of coroots. The canonical bijection $R \leftrightarrow \check{R}$ is denoted by $\alpha \leftrightarrow \check{\alpha}$. For any $\alpha \in R$ we define $s_\alpha = s_{\check{\alpha}} : \mathbf{X} \to \mathbf{X}$ by $x \mapsto x - \langle \check{\alpha}, x \rangle \alpha$ and $s_\alpha = s_{\check{\alpha}} : \mathbf{Y} \to \mathbf{Y}$ by $\chi \mapsto \chi - \langle \chi, \alpha \rangle \check{\alpha}$. Then $s_\alpha = s_{\check{\alpha}}$ represents the action of an element of W on $\mathbf{X}$ and $\mathbf{Y}$ denoted again by s_α or $s_{\check{\alpha}}$. Let $R^+ \subset R$ (resp., $\check{R}^+ \subset \check{R}$)

be the set of positive roots (resp., corroots) determined by U. Let $R^- = R - R^+$, $\check{R}^- = \check{R} - \check{R}^+$. For $s \in S$ let $\alpha_s \in R^+$ be the corresponding simple root; for any $t \in T$ we have $s(t) = t\check{\alpha}_s(\alpha_s(t^{-1}))$; $\check{\alpha}_s$ has also been considered in subsection 0.1. Recall that L is the subgroup of Y generated by $\{\check{\alpha}_s; s \in S\}$. For any $c \in \mathbf{k}^*$ we set $c_s = \check{\alpha}_s(c) \in T$. We have $\dot{s}^2 = \epsilon_s$ for $s \in S$. Recall that $W_2 = \{w \in W; w^2 = 1\}$. Note that $\dot{w}^2 \in T$ for any $w \in W_2$.

Lemma 1.4. *Let $w \in W_2$. Then either* (i) *or* (ii) *below holds:*
(i) *There exists $s \in S$ such that $|sw| < |w|$ and $sw \neq ws$.*
(ii) *There exists a (necessarily unique) subset $J \subset S$ such that w is the longest element in the subgroup W_J of W generated by J; moreover, w is in the centre of W_J. For $s \in J$ we have $w(\alpha_s) = -\alpha_s$.*

We can assume that $w \neq 1$ and that (i) does not hold for w. Let $s_1, s_2, \cdots, s_k$ in S be such that $w = s_1 s_2 \ldots s_k$, $|w| = k$. We have $k \geq 1$ and $|s_1 w| < |w|$. Since (i) does not hold we have $s_1 w = w s_1$; hence $w = s_2 s_3 \cdots s_k s_1$. Thus $|s_2 w| < |w|$. Since (i) does not hold we have $s_2 w = w s_2$; hence $w = s_3 \cdots s_{k-1} s_k s_1$. Continuing in this way we see that $|s_i w| < |w|$ and $s_i w = w s_i$ for $i = 1, \ldots, k$. We see that the first sentence in (ii) holds with $J = \{s \in S; s = s_i \text{ for some } i \in [1, k]\}$.

Now let $s \in J$. We have $s = s_\alpha$, where $\alpha = \alpha_s$ and $wsw = s_{w(\alpha)}$. Since $wsw = s$ we have $s_{w(\alpha)} = s_\alpha$; hence $w(\alpha) = \pm\alpha$. Since $|sw| < |w|$ we must have $w(\alpha) \in R^-$; hence $w(\alpha) = -\alpha$. We see that the second sentence in (ii) holds. The lemma is proved.

1.5. For $w \in W_2$ we set $\mathbf{Y}_w = \{y \in \mathbf{Y}; w(y) = -y\}$, $\mathbf{X}_w = \{x \in \mathbf{X}; w(x) = -x\}$, $R_w = R \cap \mathbf{X}_w$, $\check{R}_w = \check{R} \cap \mathbf{Y}_w$, $R_w^+ = R^+ \cap R_w$, and $\check{R}_w^+ = \check{R}^+ \cap \check{R}_w$. Note that $\langle, \rangle$ restricts to a nondegenerate bilinear pairing $\mathbf{Y}_w \times \mathbf{X}_w \to \mathbf{R}$, denoted again by $\langle, \rangle$, and $\alpha \leftrightarrow \check{\alpha}$ restricts to a bijection $R_w \leftrightarrow \check{R}_w$.

Lemma 1.6. *Let $w \in W_2, s \in S$. Then:*
(i) $s(\mathbf{Y}_w) = \mathbf{Y}_{sws}$, $s(\mathbf{X}_w) = \mathbf{X}_{sws}$, $s(R_w) = R_{sws}$, *and* $s(\check{R}_w) = \check{R}_{sws}$;
(ii) *if $sw \neq ws$, then $s(R_w^+) = R_{sws}^+$ and $s(\check{R}_w^+) = \check{R}_{sws}^+$;*
(iii) *if $sw = ws$ and $|sw| > |w|$, then $s(R_w^+) = R_w^+$ and $s(\check{R}_w^+) = \check{R}_w^+$;*
(iv) *if $sw = ws$ and $|sw| < |w|$, then $R_{sw} = \{\alpha \in R_w; \langle\check{\alpha}_s, \alpha\rangle = 0\}$, $\check{R}_{sw} = \{\check{\alpha} \in \check{R}_w; \langle\check{\alpha}, \alpha_s\rangle = 0\}$, $R_{sw}^+ = R_{sw} \cap R_w^+$, and $\check{R}_{sw}^+ = \check{R}_{sw} \cap \check{R}_w^+$.*

(i) is immediate. We prove (ii). Let $\alpha \in R_w^+$; assume that $s(\alpha) \in R^-$. This implies that $\alpha = \alpha_s$ so that $\alpha_s \in R_w$; that is, $w(\alpha_s) = -\alpha_s$ and $w(\check{\alpha}_s) = -\check{\alpha}_s$. For $x \in \mathbf{X}$ we have

$$ws(x) - sw(x) = w(x - \langle\check{\alpha}_s, x\rangle\alpha_s) - (w(x) - \langle\check{\alpha}_s, w(x)\rangle\alpha_s)$$
$$= \langle\check{\alpha}_s, x\rangle\alpha_s + \langle w^{-1}\check{\alpha}_s, x\rangle\alpha_s$$
$$= \langle\check{\alpha}_s, x\rangle\alpha_s - \langle\check{\alpha}_s, x\rangle\alpha_s = 0.$$

Thus $ws(x) = sw(x)$ for any $x \in \mathbf{X}$ so that $sw = ws$, which contradicts our assumption. We see that $\alpha \in R_w^+$ implies $s(\alpha) \in R^+$; hence $s(\alpha) \in R_{sws}^+$. Thus $s(R_w^+) \subset R_{sws}^+$. The same argument shows with w, sws interchanged that $s(R_{sws}^+) \subset R_w^+$. It follows that $s(R_w^+) = R_{sws}^+$. Now (ii) follows.

We prove (iii). Let $\alpha \in R_w^+$; assume that $s(\alpha) \in R^-$. This implies that $\alpha = \alpha_s$ so that $\alpha_s \in R_w$; that is, $w(\alpha_s) = -\alpha_s$. Since $w(\alpha_s) \in R^-$ we have $|sw| < |w|$, which contradicts our assumption. We see that $\alpha \in R_w^+$ implies $s(\alpha) \in R^+$; hence

$s(\alpha) \in R_{sws}^+ = R_w^+$. Thus $s(R_w^+) \subset R_w^+$. Since R_w^+ is finite it follows that $s(R_w^+) = R_w^+$. Now (iii) follows.

We prove (iv). We choose a W-invariant positive definite form $(,) : \mathbf{X} \times \mathbf{X} \to \mathbf{R}$. Our assumption implies $w(\alpha_s) = -\alpha_s$; that is, $\alpha_s \in \mathbf{X}_w$. Then $\mathbf{X}_w = \mathbf{R}\alpha_s \oplus \mathbf{X}'_w$, where $\mathbf{X}'_w = \{x \in \mathbf{X}; (x, \alpha_s) = 0\} = \{x \in \mathbf{X}; \langle \check{\alpha}_s, x \rangle = 0\}$ and s acts as identity on $\mathbf{X}'_w$. Since w acts as -1 on $\mathbf{X}_w$, sw must act as -1 on $\mathbf{X}'_w$; hence $\mathbf{X}_{sw} \subset \mathbf{X}'_w$. Since $\dim(\mathbf{X}_{sw}) = \dim(\mathbf{X}_w) - 1 = \dim \mathbf{X}'_w$, it follows that $\mathbf{X}_{sw} = \mathbf{X}'_w$. We have $R_{sw} = R \cap \mathbf{X}_{sw} = R \cap \mathbf{X}'_w$, $R_{sw}^+ = R^+ \cap R_{sw} = R^+ \cap (R \cap \mathbf{X}'_w) = R^+ \cap \mathbf{X}'_w$, and $R_{sw} \cap R_w^+ = (R \cap \mathbf{X}_{sw}) \cap (R^+ \cap \mathbf{X}_w) = R^+ \cap \mathbf{X}'_w$; hence $R_{sw}^+ = R_{sw} \cap R_w^+$. Similarly we have $\check{R}_{sw} = \{\check{\alpha} \in \check{R}_w; \langle \check{\alpha}, \alpha_s \rangle = 0\}$, $\check{R}_{sw}^+ = \check{R}_{sw} \cap \check{R}_w^+$. This proves (iv).

Lemma 1.7. *Let $w \in W_2$.*

(a) *R_w generates the vector space $\mathbf{X}_w$ and $\check{R}_w$ generates the vector space $\mathbf{Y}_w$.*

(b) *The system $(\mathbf{Y}_w, \mathbf{X}_w, \langle, \rangle, \check{R}_w, R_w)$ is a root system and R_w^+ (resp., $\check{R}_w^+$) is a set of positive roots (resp., positive coroots) for it.*

(c) *The longest element of the Weyl group of the root system in* (b) *acts on $\mathbf{Y}_w$ and on $\mathbf{X}_w$ as multiplication by -1.*

We argue by induction on $|w|$. If $|w| = 0$ we have $w = 1$ and the lemma is obvious. Assume now that $|w| > 0$. If we can find $s \in S$ such that $|sw| < |w|$, $sw \neq ws$, then by the induction hypothesis, the lemma is true when w is replaced by sws, since $|sws| = |w| - 2$. Using Lemma 1.6 we deduce that the lemma is true for w. Now using Lemma 1.4 we see that we can assume that w is as in Lemma 1.4(ii). Let $J \subset S$ be as in Lemma 1.4(ii). Let $\mathbf{X}'_w$ be the subspace of $\mathbf{X}_w$ generated by $\{a_s; s \in J\}$. By Lemma 1.4(ii) we have $\mathbf{X}'_w \subset \mathbf{X}_w$. As in the proof of Lemma 1.4 we can write $w = s_1 s_2 \cdots s_k$ with $s_1, s_2, \ldots, s_k$ in J. Then for any $x \in \mathbf{X}$ we have

$$wx = s_1 s_2 \cdots s_k x = s_2 s_3 \cdots s_k x + c_1 \alpha_{s_1} = s_3 \cdots s_k x + c_2 \alpha_{s_2} + c_1 \alpha_{s_1}$$
$$= \cdots = x + c_k \alpha_{s_k} + \cdots + c_2 \alpha_{s_2} + c_1 \alpha_{s_1}$$

with $c_1, c_2, \ldots, c_k$ in $\mathbf{R}$. Thus we have $(w - 1)\mathbf{X} \subset \mathbf{X}'_w$. Since $w^2 = 1$ we have $(w - 1)\mathbf{X} = \mathbf{X}_w$. Thus $\mathbf{X}_w \subset \mathbf{X}'_w$. This proves the first part of (a); the second part of (a) is proved in an entirely similar way. If $\alpha \in R_w$ (so that $\check{\alpha} \in \check{R}_w$) and if $\alpha' \in R$, then $s_\alpha(\alpha')$ is a linear combination of α and hence α' is in $\mathbf{X}_w$. Since $s_\alpha(\alpha') \in R$ we have $s_\alpha(\alpha') \in R \cap \mathbf{X}_w$; that is, $s_\alpha(\alpha') \in R_w$. We see that (b) holds. We prove (c). We write again $w = s_1 s_2 \cdots s_k$ with $s_1, s_2, \ldots, s_k$ in J. We can wiew this as an equality of endomorphisms of $\mathbf{X}$ and we restrict it to an equality of endomorphisms of $\mathbf{X}_w$. Each s_i restricts to an endomorphism of $\mathbf{X}_w$ which is in the Weyl group of the root system in (b). It follows that w acts on $\mathbf{X}_w$ as an element of the Weyl group of the root system in (b) with simple roots $\{\alpha_s; s \in J\}$. By Lemma 1.4(ii), we have $w(\alpha_s) = -\alpha_s$ for any $s \in J$. Thus some element in the Weyl group of the root system in (b) maps each simple root to its negative. This proves (c). The lemma is proved.

Let Π_w be the set of simple roots of R_w such that $\Pi_w \subset R_w^+$. Let $\check{\Pi}_w$ be the set of simple coroots of $\check{R}_w$ such that $\check{\Pi}_w \subset \check{R}_w^+$.

1.8. Let $w \in W_2$. Let $\check{\mathcal{E}}_w$ be the subset of $\check{R}_w^+$ defined as $\check{\mathcal{E}}$ in subsection 1.1 in terms of the root system R_w in $\mathbf{X}_w$ (instead of R' in $\mathbf{X}'$). The definition is applicable in

view of Lemma 1.7(c). Recall that $\check{\mathcal{E}}_w$ is a basis of $\mathbf{Y}_w$. We define $r_w \in L$ by

$$r_w = \sum_{\beta \in \check{\mathcal{E}}_w} \beta.$$

Note that r_w is a special case of the elements r defined as in subsection 1.2 in terms of R_w instead of R'. We show:

(a) *The reflections $\{s_\beta : \mathbf{Y} \to \mathbf{Y}; \beta \in \check{\mathcal{E}}_w\}$ commute with each other, and their product (in any order) is equal to w.*

From subsection 1.1(c) we see that this holds after restriction to $\mathbf{Y}_w$. Since each s_β and w induces identity on $\mathbf{Y}/\mathbf{Y}_w$, they must act as 1 on the orthogonal complement to $\mathbf{Y}_w$ for a W-invariant positive definite inner product on $\mathbf{Y}$. Hence the statements of (a) must hold on $\mathbf{Y}$.

We now describe the set $\check{\mathcal{E}}_w$ and the elements r_w in the case where G is almost simple and w is the longest element in W in the case where w is not central in W. (The cases where w is central in W were already described in subsections 1.1 and 1.2.) We again denote the simple roots by $\{\alpha_i; i \in [1,l]\}$ as in [Bou68].

Type $A_l, l = 2n \geq 2$: $\check{\alpha}_1 + \check{\alpha}_2 + \cdots + \check{\alpha}_{2n-1} + \check{\alpha}_{2n}, \check{\alpha}_2 + \check{\alpha}_3 + \cdots + \check{\alpha}_{2n-1}$, $\check{\alpha}_3 + \cdots + \check{\alpha}_{2n-2}, \ldots, \check{\alpha}_n + \check{\alpha}_{n+1}$;

$r_w = \check{\alpha}_1 + 2\check{\alpha}_2 + \cdots + n\check{\alpha}_n + n\check{\alpha}_{n+1} + \cdots + 2\check{\alpha}_{2n-1} + \check{\alpha}_{2n}$.

Type $A_l, l = 2n + 1 \geq 3$: $\check{\alpha}_1 + \check{\alpha}_2 + \cdots + \check{\alpha}_{2n} + \check{\alpha}_{2n+1}, \check{\alpha}_2 + \check{\alpha}_3 + \cdots + \check{\alpha}_{2n}$, $\check{\alpha}_3 + \cdots + \check{\alpha}_{2n-1}, \ldots, \check{\alpha}_{n+1}$;

$r_w = \check{\alpha}_1 + 2\check{\alpha}_2 + \cdots + (n+1)\check{\alpha}_{n+1} + \cdots + 2\check{\alpha}_{2n} + \check{\alpha}_{2n+1}$.

Type $D_l, l = 2n+1 \geq 5$: $\check{\alpha}_1 + 2\check{\alpha}_2 + 2\check{\alpha}_3 + \cdots + 2\check{\alpha}_{2n-1} + \check{\alpha}_{2n} + \check{\alpha}_{2n+1}, \check{\alpha}_3 + 2\check{\alpha}_4 + 2\check{\alpha}_5 + \cdots + 2\check{\alpha}_{2n-1} + \check{\alpha}_{2n} + \check{\alpha}_{2n+1}, \ldots, \check{\alpha}_{2n-3} + 2\check{\alpha}_{2n-2} + 2\check{\alpha}_{2n-1} + \check{\alpha}_{2n} + \check{\alpha}_{2n+1}$, $\check{\alpha}_{2n-1} + \check{\alpha}_{2n} + \check{\alpha}_{2n+1}, \check{\alpha}_1, \check{\alpha}_3, \ldots, \check{\alpha}_{2n-3}, \check{\alpha}_{2n-1}$;

$r_w = 2\check{\alpha}_1 + 2\check{\alpha}_2 + 4\check{\alpha}_3 + 4\check{\alpha}_4 + \cdots + (2n-2)\check{\alpha}_{2n-3} + (2n-2)\check{\alpha}_{2n-2} + 2n\check{\alpha}_{2n-1} + n\check{\alpha}_{2n} + n\check{\alpha}_{2n+1}$.

Type E_6: $\check{\alpha}_1 + 2\check{\alpha}_2 + 2\check{\alpha}_3 + 3\check{\alpha}_4 + 2\check{\alpha}_5 + \check{\alpha}_6, \check{\alpha}_1 + \check{\alpha}_3 + \check{\alpha}_4 + \check{\alpha}_5 + \check{\alpha}_6, \check{\alpha}_3 + \check{\alpha}_4 + \check{\alpha}_5$, $\check{\alpha}_4$;

$r_w = 2\check{\alpha}_1 + 2\check{\alpha}_2 + 4\check{\alpha}_3 + 6\check{\alpha}_4 + 4\check{\alpha}_5 + 2\check{\alpha}_6$.

From Lemma 1.6 and the definitions we deduce the following result.

Lemma 1.9. *Let $w \in W_2, s \in S$.*

(a) *If $sw \neq ws$, then $s(\mathcal{E}_w) = \mathcal{E}_{sws}$ and $s(r_w) = r_{sws}$.*

(b) *If $sw = ws$ and $|sw| > |w|$, then $s(\mathcal{E}_w) = \mathcal{E}_w$ and $s(r_w) = r_w$.*

1.10. In this subsection we assume that G is almost simple of type $D_l, l \geq 4$. Let $\mathcal{Z} = [1,l]$. We can find a basis $\{e_i; i \in \mathcal{Z}\}$ of $\mathbf{Y}$ with the following properties:

W consists of all automorphisms $w : \mathbf{Y} \to \mathbf{Y}$ such that for any $i \in \mathcal{Z}$ we have $w(e_i) = \delta_i e_j$ for some $j \in \mathcal{Z}$ and some $\delta_i \in \{1, -1\}$ and such that $\prod_i \delta_i = 1$:

$$\check{R}^+ = \{e_i - e_j; (i,j) \in \mathcal{Z} \times \mathcal{Z}, i < j\} \sqcup \{e_i + e_j; (i,j) \in \mathcal{Z} \times \mathcal{Z}, i < j\}.$$

Let $w \in W_2$. Let P'_w be the set of two element subsets $\{i,j\}$ of $\mathcal{Z}$ such that $w(i) = j$ and $w(j) = i$. Let P''_w be the set of two element subsets $\{i,j\}$ of $\mathcal{Z}$ such that $w(i) = -j$ and $w(j) = -i$. Let $\mathcal{Z}_w^+ = \{i \in \mathcal{Z}; w(i) = i\}$ and $\mathcal{Z}_w^- = \{i \in \mathcal{Z}; w(i) = -i\}$. We have

$$\mathcal{Z} = \bigsqcup_{\{i,j\} \in P'_w} \{i,j\} \sqcup \bigsqcup_{\{i,j\} \in P''_w} \{i,j\} \sqcup \mathcal{Z}_w^+ \sqcup \mathcal{Z}_w^-.$$

Note that $\sharp(\mathcal{Z}_w^-)$ is even. For $w \in W_2$ we have

$$\check{\mathcal{E}}_w = \{e_i - e_j; \{i,j\} \in P_w', i < j\} \sqcup \{e_i + e_j; \{i,j\} \in P_w'', i < j\}$$

$$\sqcup \{e_{i_1} - e_{i_2}, e_{i_1} + e_{i_2}, e_{i_3} - e_{i_4}, e_{i_3} + e_{i_4}, \ldots, e_{i_{2u-1}} - e_{i_{2u}}, e_{i_{2u-1}} + e_{i_{2u}}\},$$

where $\mathcal{Z}_w^-$ consists of $i_1 < i_2 < i_3 < \cdots < i_{2u}$. Now let $s \in S$. There are two possibilities:

(i) There exist a, b in $\mathcal{Z}$ such that $b = a+1$, $s(e_a) = e_b$, $s(e_b) = e_a$, and $s(e_z) = e_z$ for $z \in \mathcal{Z} - \{a,b\}$; moreover, $\check{\alpha}_s = e_a - e_b$.

(ii) Taking $a = l-1$ and $b = l$ we have $s(e_a) = -e_b$, $s(e_b) = -e_a$, and $s(e_z) = e_z$ for $z \in \mathcal{Z} - \{a,b\}$; moreover, $\check{\alpha}_s = e_a + e_b$.

We show:

(a) *Assume that $w \in W_2$ and $s \in S$ are such that $sw = ws$, and $|sw| > |w|$. We have $r_{sw} = r_w \pm \check{\alpha}_s$.*

Assume first that s is as in (i). Let $i_1 < i_2 < i_3 < \cdots < i_{2u}$ be the numbers in $\mathcal{Z}_w^-$. We have either $\{a,b\} \in P_w''$ or $\{a,b\} \subset \mathcal{Z}_w^+$. (If $\{a,b\} \in P_w'$ or $\{a,b\} \subset \mathcal{Z}_w^-$, then $|sw| < |w|$.) If $\{a,b\} \subset \mathcal{Z}_w^+$, then $\check{\mathcal{E}}_{sw} = \check{\mathcal{E}}_w \sqcup \{e_a - e_b\}$. Hence $r_{sw} - r_w = \check{\alpha}_s$. If $\{a,b\} \in P_w''$ and $i_h < a < b < i_{h+1}$ for some odd $h \in [1, k-1]$, then $\check{\mathcal{E}}_{sw}$ is obtained from $\check{\mathcal{E}}_w$ by removing $e_{i_k} - e_{i_{k+1}}$, $e_{i_k} + e_{i_{k+1}}$, $e_a + e_b$ and by including instead $e_{i_k} - e_a, e_{i_k} + e_a, e_b - e_{i_{k+1}}, e_b + e_{i_{k+1}}$. Hence

$$r_{sw} - r_w = (e_{i_k} - e_a) + (e_{i_k} + e_a) + (e_b - e_{i_{k+1}}) + (e_b + e_{i_{k+1}})$$

$$- (e_{i_k} - e_{i_{k+1}}) - (e_{i_k} + e_{i_{k+1}}) - (e_a + e_b) = e_b - e_a = -\check{\alpha}_s.$$

If $\{a,b\} \in P_w''$ and there is no odd $h \in [1, k-1]$ such that $i_h < a < b < i_{h+1}$, then $\check{\mathcal{E}}_{sw} = \check{\mathcal{E}}_w \sqcup \{e_a - e_b\}$. Hence $r_{sw} - r_w = \check{\alpha}_s$. Next we assume that s is as in (ii). We have $\check{\mathcal{E}}_{sw} = \check{\mathcal{E}}_w \sqcup \{e_a + e_b\}$. Hence $r_{sw} - r_w = \check{\alpha}_s$. This completes the proof of (a).

1.11. In this subsection we assume that G is simple of type E_8. Let w be the longest element of W. We denote the simple roots by $\{\alpha_i; i \in [1,8]\}$ as in [Bou68] and write s_i instead of s_{α_i}. For $i \in [1,8]$ we have $s_i w \in W_2$ and $R_{s_i w} = \{\alpha \in R; \langle \check{\alpha}_i, \alpha \rangle = 0\}$. From this $\check{\Pi}_{s_i w}$ is easily determined in each case:

$$\check{\Pi}_{s_1 w} = \{\check{\alpha}_1 + 2\check{\alpha}_2 + 2\check{\alpha}_4 + \check{\alpha}_3 + \check{\alpha}_5, \check{\alpha}_2, \check{\alpha}_4, \check{\alpha}_5, \check{\alpha}_6, \check{\alpha}_7, \check{\alpha}_8\}.$$

$$\check{\Pi}_{s_2 w} = \{\check{\alpha}_1, \check{\alpha}_2 + 2\check{\alpha}_4 + \check{\alpha}_3 + \check{\alpha}_5, \check{\alpha}_3, \check{\alpha}_5, \check{\alpha}_6, \check{\alpha}_7, \check{\alpha}_8\}.$$

$$\check{\Pi}_{s_3 w} = \{\check{\alpha}_1 + \check{\alpha}_3 + \check{\alpha}_4, \check{\alpha}_2, \check{\alpha}_3 + 2\check{\alpha}_4 + \check{\alpha}_2 + \check{\alpha}_5, \check{\alpha}_5, \check{\alpha}_6, \check{\alpha}_7, \check{\alpha}_8\}.$$

$$\check{\Pi}_{s_4 w} = \{\check{\alpha}_1, \check{\alpha}_2 + \check{\alpha}_4 + \check{\alpha}_3, \check{\alpha}_3 + \check{\alpha}_4 + \check{\alpha}_5, \check{\alpha}_6, \check{\alpha}_2 + \check{\alpha}_4 + \check{\alpha}_5, \check{\alpha}_7, \check{\alpha}_8\}.$$

$$\check{\Pi}_{s_6 w} = \{\check{\alpha}_1, \check{\alpha}_2, \check{\alpha}_3, \check{\alpha}_4, \check{\alpha}_5 + \check{\alpha}_6 + \check{\alpha}_7, \check{\alpha}_2 + \check{\alpha}_3 + 2\check{\alpha}_4 + 2\check{\alpha}_5 + \check{\alpha}_6, \check{\alpha}_8\}.$$

$$\check{\Pi}_{s_7 w} = \{\check{\alpha}_1, \check{\alpha}_2, \check{\alpha}_3, \check{\alpha}_4, \check{\alpha}_5, \check{\alpha}_6 + \check{\alpha}_7 + \check{\alpha}_8, \check{\alpha}_2 + \check{\alpha}_3 + 2\check{\alpha}_4 + 2\check{\alpha}_5 + 2\check{\alpha}_6 + \check{\alpha}_7\}.$$

$$\check{\Pi}_{s_8 w} = \{\check{\alpha}_1, \check{\alpha}_2, \check{\alpha}_3, \check{\alpha}_4, \check{\alpha}_5, \check{\alpha}_6, \check{\alpha}_2 + \check{\alpha}_3 + 2\check{\alpha}_4 + 2\check{\alpha}_5 + 2\check{\alpha}_6 + 2\check{\alpha}_7 + \check{\alpha}_8\}.$$

This is the set of simple roots of a root system of type E_7. Hence $r_{s_i w}$ is given by substituting the simple roots in the formula for r in type E_7 given in subsection 1.2 by the roots in $\check{\Pi}_{s_1 w}$. We find the same result as for r_w (given by r in type E_8 in subsection 1.2) plus a multiple of $\check{\alpha}_i$. More precisely:

$$r_{s_1 w} = r_w - \check{\alpha}_1, \quad r_{s_2 w} = r_w + \check{\alpha}_2, \quad r_{s_3 w} = r_w + \check{\alpha}_3,$$

$$r_{s_4 w} = r_w - \check{\alpha}_4, \quad r_{s_5 w} = r_w + \check{\alpha}_5, \quad r_{s_6 w} = r_w - \check{\alpha}_6,$$

$$r_{s_7 w} = r_w + \check{\alpha}_7, \quad r_{s_8 w} = r_w - \check{\alpha}_8.$$

1.12. In this subsection we preserve the setup and notation of subsection 1.11. Let w' be the longest element in the standard parabolic subgroup of type E_7 of W. For $i \in [1, 7]$ we have $s_i w' \in W_2$ and $R_{s_i w'} = \{\alpha \in R_{w'}; \langle \check{\alpha}_i, \alpha \rangle = 0\}$. From this $\check{\Pi}_{s_i w'}$ is easily determined in each case:

$$\check{\Pi}_{s_1 w'} = \{\check{\alpha}_1 + 2\check{\alpha}_3 + 2\check{\alpha}_4 + \check{\alpha}_2 + \check{\alpha}_5, \check{\alpha}_2, \check{\alpha}_4, \check{\alpha}_5, \check{\alpha}_6, \check{\alpha}_7\},$$
$$\check{\Pi}_{s_2 w'} = \{\check{\alpha}_1, \check{\alpha}_3, \check{\alpha}_3 + 2\check{\alpha}_4 + \check{\alpha}_2 + \check{\alpha}_5, \check{\alpha}_5, \check{\alpha}_6, \check{\alpha}_7\},$$
$$\check{\Pi}_{s_3 w'} = \{\check{\alpha}_1 + \check{\alpha}_3 + \check{\alpha}_4, \check{\alpha}_2, \check{\alpha}_3 + 2\check{\alpha}_4 + \check{\alpha}_2 + \check{\alpha}_5, \check{\alpha}_5, \check{\alpha}_6, \check{\alpha}_7\},$$
$$\check{\Pi}_{s_4 w'} = \{\check{\alpha}_1, \check{\alpha}_3 + \check{\alpha}_4 + \check{\alpha}_5, \check{\alpha}_4 + \check{\alpha}_2 + \check{\alpha}_3, \check{\alpha}_4 + \check{\alpha}_2 + \check{\alpha}_5, \check{\alpha}_6, \check{\alpha}_7\},$$
$$\check{\Pi}_{s_5 w'} = \{\check{\alpha}_1, \check{\alpha}_2, \check{\alpha}_3, \check{\alpha}_4 + \check{\alpha}_5 + \check{\alpha}_6, \check{\alpha}_5 + 2\check{\alpha}_4 + \check{\alpha}_2 + \check{\alpha}_3, \check{\alpha}_7\},$$
$$\check{\Pi}_{s_6 w'} = \{\check{\alpha}_1, \check{\alpha}_2, \check{\alpha}_3, \check{\alpha}_4, \check{\alpha}_5 + \check{\alpha}_6 + \check{\alpha}_7, \check{\alpha}_6 + 2\check{\alpha}_5 + 2\check{\alpha}_4 + \check{\alpha}_2 + \check{\alpha}_3\},$$
$$\check{\Pi}_{s_7 w'} = \{\check{\alpha}_1, \check{\alpha}_2, \check{\alpha}_3, \check{\alpha}_4, \check{\alpha}_5, \check{\alpha}_7 + 2\check{\alpha}_6 + 2\check{\alpha}_5 + 2\check{\alpha}_4 + \check{\alpha}_2 + \check{\alpha}_3\}.$$

This is the set of simple roots of a root system of type D_6. Hence $r_{s_i w'}$ is given by substituting the simple roots in the formula for r in type D_6 given in subsection 1.2 by the roots in $\check{\Pi}_{s_1 w'}$. We find the same result as for $r_{w'}$ (given by r in type E_7 in subsection 1.2) plus a multiple of $\check{\alpha}_i$. More precisely:

$$r_{s_1 w'} = r_{w'} - \check{\alpha}_1, \quad r_{s_2 w'} = r_{w'} + \check{\alpha}_2, \quad r_{s_3 w'} = r_{w'} + \check{\alpha}_3, \quad r_{s_4 w'} = r_{w'} - \check{\alpha}_4,$$
$$r_{s_5 w'} = r_{w'} + \check{\alpha}_5, \quad r_{s_6 w'} = r_{w'} - \check{\alpha}_6, \quad r_{s_7 w'} = r_{w'} + \check{\alpha}_7.$$

1.13. In this subsection we preserve the setup and notation of subsection 1.11. We show:

(a) *Let $z \in W_2, s \in S$ be such that $sz = zs$. We have $r_{sz} = r_z + \mathcal{N}\check{\alpha}_s$, where $\mathcal{N} \in \{-1, 1\}$.*

By interchanging if necessary z, sz, we can assume that $|z| > |sz|$. By Lemma 1.4 we can find a sequence $s_1, s_2, \ldots, s_k$ in S (with $k \geq 0$) such that $|z| > |s_1 z s_1| > |s_2 s_1 z s s_1 s_2| > \cdots > |s_k \cdots s_2 s_1 z s_1 s_2 \cdots s_k|$ and $z' := s_k \cdots s_2 s_1 z s_1 s_2 \cdots s_k$ is the longest element of a standard parabolic subgroup W_J of W such that z' is in the centre of W_J. Let $\sigma = s_k \cdots s_2 s_1 \in W$. Applying Lemma 1.6(ii) repeatedly we see that $\check{R}^+_{s_k \cdots s_2 s_1 z s_1 s_2 \cdots s_k} = s_k(\check{R}^+_{s_{k-1} \cdots s_2 s_1 z s_1 s_2 \cdots s_{k-1}}), \ldots, \check{R}^+_{s_2 s_1 z s_1 s_2} = s_2(\check{R}^+_{s_1 z s_1})$, $\check{R}^+_{s_1 z s_1} = s_1(\check{R}^+_z)$. It follows that $\check{R}^+_{s_k \cdots s_2 s_1 z s_1 s_2 \cdots s_k} = s_k \cdots s_2 s_1(\check{R}^+_z)$; that is, $\check{R}^+_{z'} = s_k \cdots s_2 s_1(\check{R}^+_z) = \sigma(\check{R}^+_z)$. This implies that:

(b) $\check{\Pi}_{z'} = \sigma(\check{\Pi}_z)$.

From our assumption we have $z(\check{\alpha}_s) = -\check{\alpha}_s$. Thus $\check{\alpha}_s \in \check{R}^+_z$. Since $\check{\alpha}_s$ is a simple coroot in $\check{R}$, we necessarily have $\check{\alpha}_s \in \check{\Pi}_z$. Using (b) we deduce that $\sigma(\check{\alpha}_s) \in \check{\Pi}_{z'}$. From the definition of z' we see that $\check{\Pi}_{z'}$ consists of the simple coroots of $\check{R}$ such that the corresponding simple reflections are in W_J. Thus we have $\sigma(\check{\alpha}_s) = \check{\alpha}_{s'}$, where $s' \in S \cap W_J$. It follows that $\sigma s \sigma^{-1} = s'$, $\sigma(\alpha_s) = \alpha_{s'}$. Note that $s' z' = z' s'$ (since z' is in the centre of W_J) and $|s' z'| < |z'|$ (since z' is the longest element of W_J). From Lemma 1.6(iv) we see that $\check{R}^+_{sz} = \{\check{\alpha} \in R^+_z; \langle \check{\alpha}, \alpha_s \rangle = 0\}$, $\check{R}^+_{s' z';} = \{\check{\alpha} \in R^+_{z'}; \langle \check{\alpha}, \alpha_{s'} \rangle = 0\}$. If $\langle \check{\alpha}, \alpha_s \rangle = 0$, then $\langle \sigma(\check{\alpha}), \sigma(\alpha_s) \rangle = 0$; hence $\langle \sigma(\check{\alpha}), \alpha_{s'} \rangle = 0$. Since $\sigma(R^+_z) = R^+_{z'}$ it follows that $\sigma(\{\check{\alpha} \in R^+_z; \langle \check{\alpha}, \alpha_s \rangle = 0\}) = \{\check{\alpha} \in R^+_{z'}; \langle \check{\alpha}, \alpha_{s'} \rangle = 0\}$; that is, $\sigma(\check{R}^+_{sz}) = \check{R}^+_{s' z'}$. This implies $\sigma(\check{\Pi}_{sz}) = \check{\Pi}_{s' z'}$. Using the definitions we deduce that $\sigma(\mathcal{E}_{sz}) = \mathcal{E}_{s' z'}$; hence $\sigma(r_{sz}) = r_{s' z'}$. Similarly we have $\sigma(r_z) = r_{z'}$. Hence if (a) holds for z', s', that is, $r_{s' z'} = r_{z'} + \mathcal{N}\check{\alpha}_{s'}$ where $\mathcal{N} \in \{-1, 1\}$, then $r_{sz} - r_z = \sigma^{-1}(\mathcal{N}\check{\alpha}_{s'}) = \mathcal{N}\check{\alpha}_s$ so that (a) holds for z, s. Thus it is enough to prove (a) assuming in addition that z is the longest element of a standard parabolic subgroup W_J of W such that z is in the centre of W_J. If

$W_J = W$, (a) follows from subsection 1.11. If W_J is of type E_7, (a) follows from 1.12. If W_J is of type other than $E_8 and E_7$, then it is of type $A_1 \times A_1 \times \cdots$ or of type $D_l \times A_1 \times A_1 \times \cdots$ (with $l \in \{4, 6\}$). If s belongs to the $A_1 \times A_1 \times \cdots$-factor, the result is trivial. If s belongs to the D_l-factor, the result follows from subsection 1.10. This completes the proof of (a).

1.14. In this subsection we assume that G is almost simple, simply connected, simply laced, and that we are given an automorphism $\iota : G \to G$ such that $\iota(T) = T$, $\iota(U) = U$, and that for any $s \in S, c \in \mathbf{k}^*$ we have $x_{\iota(s)}(c) = \iota(x_s(c))$, $y_{\iota(s)}(c) = \iota(y_s(c))$. Then ι induces an automorphism of W and automorphisms of X and Y, leaving $R, \check{R}, S$ stable; these are denoted again by ι. We also assume that if s, s' in S are in the same ι-orbit, then $ss' = s's$. Let $\tilde{G} = G^\iota$ be a connected simply connected algebraic group. Now $\tilde{T} = T^\iota$ is a maximal torus of $\tilde{G}$ and $\tilde{U} = U^\iota$ is the unipotent radical of a Borel subgroup of $\tilde{G}$. Let $\tilde{W}$ be the Weyl group of $\tilde{G}$ with respect to $\tilde{T}$. We can identify $\tilde{W} = W^\iota$. Let $w \mapsto |w|_\iota$ be the length function on $\tilde{W}$. Let $\tilde{S} = \{w \in \tilde{W}; |w|_\iota = 1\}$. Now $\tilde{S}$ consists of the elements $\sigma = \prod_s s$, where s runs over an ι-orbit in S. Let $\tilde{X} = \mathrm{Hom}(\tilde{T}, \mathbf{k}^*)$ (a quotient of X), and let $\tilde{Y} = \mathrm{Hom}(\mathbf{k}^*, \tilde{T})$ (a subgroup of Y); we have $\tilde{Y} = Y^\iota$. Let $\tilde{R}$ (resp., $\check{\tilde{R}}$) be the set of roots (resp., coroots) of $\tilde{G}$ with respect to $\tilde{T}$. Now $\tilde{R}$ consists of the images of roots of G under $X \to \tilde{X}$ and $\check{\tilde{R}}$ consists of the elements of Y which are sums of coroots in an ι-orbit on $\check{R}$. If $\sigma \in \tilde{S}$ corresponds to an ι-orbit $\mathcal{O}$ in S, then the simple root α_σ of $\tilde{G}$ corresponding to σ is the restriction to $\tilde{X}$ of α_s for any $s \in \mathcal{O}$; the simple coroot of $\tilde{G}$ corresponding to σ is $\check{\alpha}_\sigma = \sum_{s \in \mathcal{O}} \check{\alpha}_s \in \tilde{Y}$. Let $\tilde{W}_2 = W_2 \cap \tilde{W}$. Let $\{\tilde{r}_w; w \in \tilde{W}_2\}$ be the elements of $\tilde{Y}$ defined like $\{r_w; w \in W_2\}$ (see subsection 1.8) in terms of $\tilde{G}$ instead of G. We show:

(a) *For $w \in \tilde{W}_2$ we have $\tilde{r}_w = r_w$.*

We argue by induction on $|w|_\iota$. If $|w|_\iota = 0$ we have $w = 1$ and the result is obvious. Assume now that $|w|_\iota \geq 1$. Assume also that we can find $\sigma \in \tilde{S}$ such that $|\sigma w|_\iota < |w|_\iota$ and $\sigma w \neq w\sigma$. We write $\mathcal{O} = \{s_1, \ldots, s_k\} \subset S$, $\sigma = s_1 \cdots s_k$. Then for some $i \in [1, k]$ we have $s_i w \neq w s_i$. Hence for all $i \in [1, k]$ we have $s_i w \neq w s_i$. Hence we have $s_1 w \neq w s_1, s_2 s_1 w \neq w s_1 s_2, \ldots, s_k \cdots s_1 w \neq w s_1 \cdots s_k$. By Lemma 1.9(a) for G and $\tilde{G}$ we have $\tilde{r}_w = \sigma \tilde{t}_{sws} \sigma$ and $r_w = s_1(r_{s_1 w s_1}) = s_1 s_2(r_{s_2 s_1 w s_1 s_2}) = \cdots = s_1 \cdots s_k(r_{s_k \cdots s_1 w s_1 \cdots s_k})$ so that $r_w = \sigma r_{\sigma w \sigma} s$. By the induction hypothesis we have $\tilde{r}_{\sigma w \sigma} = r_{\sigma w \sigma}$; hence $\tilde{r}_w = r_w$. Next we assume that there is no $\sigma \in \tilde{S}$ such that $|\sigma w|_\iota < |w|_\iota$ and $\sigma w \neq w\sigma$. Then, by Lemma 1.4 for $\tilde{G}$ we can find a standard parabolic subgroup $\tilde{W}'$ of $\tilde{W}$ such that w is the longest element of $\tilde{W}'$ and w is central in $\tilde{W}'$. In this case the equality $\tilde{r}_w = r_w$ follows by comparing the formulas in subsection 1.2 with those in subsection 1.10. This completes the proof of (a).

We return to the general case.

Lemma 1.15. *Let $w \in W_2, s \in S$ be such that $sw = ws$. We have:*
(a) *$r_{sw} = r_w + \mathcal{N}\check{\alpha}_s$, where $\mathcal{N} \in \{-1, 0, 1\}$.*
If in addition G is simply laced, then $\mathcal{N} \in \{-1, 1\}$.

If the result holds when $|w| > |sw|$, then it also holds when $|w| < |sw|$ (by interchanging w, sw); thus we can assume that $|w| > |sw|$. We can assume that G is almost simple. If G is of type D_l, $l \geq 4$, the result follows from subsection 1.10. If G is of type A_l, the result follows from the corresponding result for a group of type $D_{l'}$ with $l < l' \geq 4$. If G is of type E_8, the result follows from subsection

1.13(a). If G is of type E_7 or E_6 the result follows from the corresponding result for a group of type E_8. Thus (a) holds when G is simply laced.

Let $G, \iota, \tilde{G}, \tilde{T}, \tilde{W}, \tilde{S}, \tilde{Y}, ||_\iota, \tilde{W}_2$ be as in the proof of subsection 1.14(a). To complete the proof it is enough to show that (a) holds when G is replaced by $\tilde{G}$. Let $\{\tilde{r}_w; w \in \tilde{W}_2\}$ be the elements of $\tilde{Y}$ defined like $\{r_w; w \in W_2\}$ in terms of $\tilde{G}$ instead of G. We must show that $\{\tilde{r}_w; w \in \tilde{W}_2\}$ satisfy conditions like (a). By subsection 1.14(a) we have $\tilde{r}_w = r_w$ for $w \in \tilde{W}_2$.

Now let $w \in \tilde{W}_2$, $\sigma \in \tilde{S}$ be such that $\sigma w = w\sigma$. We write $\mathcal{O} = \{s_1, \ldots, s_k\} \subset S$ and $\sigma = s_1 \cdots s_k$, where ι permutes $s_1, s_2, \ldots, s_k$ cyclically: $s_1 \mapsto s_2 \mapsto \cdots s_k \mapsto s_1$. (Note that $k \leq 3$.) We have $w(\check{\alpha}_\sigma) = \check{\alpha}_\sigma$; hence $w(\check{\alpha}_{s_1} + \cdots + \check{\alpha}_{s_k}) = \check{\alpha}_{s_1} + \cdots + \check{\alpha}_{s_k}$. If $w(\check{\alpha}_{s_i}) \in -\check{R}^+$ for some $i \in [1, k]$, then the same is true for any $i \in [1, k]$. Hence $w(\check{\alpha}_{s_1} + \cdots + \check{\alpha}_{s_k})$ is an $\mathbf{N}$-linear combination of elements in $\check{R}^+$ and is also equal to $\check{\alpha}_{s_1} + \cdots + \check{\alpha}_{s_k}$, a contradiction. Thus $w(\check{\alpha}_{s_i}) \in \check{R}^+$ for any $i \in [1, k]$. This, combined with $w(\check{\alpha}_{s_1}) + \cdots + w(\check{\alpha}_{s_k}) = \check{\alpha}_{s_1} + \cdots + \check{\alpha}_{s_k}$, forces the equality $w(\check{\alpha}_{s_i}) = \check{\alpha}_{s_{h(i)}}$ for all $i \in [1, k]$, where $h : [1, k] \to [1, k]$ is a permutation. Note that h necessarily commutes with the cyclic permutation of $[1, k]$ induced by ι; hence it is a power of this cyclic permutation. Moreover, we have $h^2 = 1$; hence $h = 1$ unless $k = 2$.

Assume first that $h = 1$. We have

$$w(\check{\alpha}_{s_1}) = \check{\alpha}_{s_1}, (s_1 w)(\check{\alpha}_{s_2}) = \check{\alpha}_{s_2}, (s_{k-1} \cdots s_1 w)(\check{\alpha}_{s_k}) = \check{\alpha}_{s_k};$$

hence $s_1 w = w s_1$, $s_2 s_1 w = s_1 w s_2, \ldots, s_k \cdots s_1 w = s_{k-1} \cdots s_1 w s_k$. By (a) for G we have $r_{s_1 w} - r_w = \pm \check{\alpha}_{s_1}$, $r_{s_2 s_1 w} - r_{s_1 w} = \pm \check{\alpha}_{s_2}$, and $r_{s_k \cdots s_1 w} - r_{s_{k-1} \cdots s_1 w} = \pm \check{\alpha}_{s_k}$. Taking the sum we obtain $r_{\sigma w} - r_w = r_{s_k \cdots s_2 s_1 w} - r_w = c_1 \check{\alpha}_{s_1} + \cdots + c_k \check{\alpha}_{s_k}$ with $c_1, \ldots, c_k$ in $\{-1, 1\}$. Since $r_{\sigma w} - r_w$ is fixed by ι, so must be $c_1 \check{\alpha}_{s_1} + \cdots + c_k \check{\alpha}_{s_k}$. It follows that $c_1 = \cdots = c_k$ so that $r_{\sigma w} - r_w = \pm(\check{\alpha}_1 + \cdots + \check{\alpha}_k)$. We see that (a) holds for $\tilde{G}$.

Next we assume that $h \neq 1$; then $k = 2$ and $w(\check{\alpha}_{s_1}) = \check{\alpha}_{s_2}$ and $w(\check{\alpha}_{s_2}) = \check{\alpha}_{s_1}$. It follows that $w s_1 w = s_2$. We have $s_1 s_2 w = s_1 w s_1 \neq w$ and $s_1 s_2 w = s_2 w s_2 \neq w$. By Lemma 1.9 for G we have $r_{s_1 s_2 w} = r_{s_1 w s_1} = s_1(r_w)$ and $r_{s_1 s_2 w} = r_{s_2 w s_2} = s_2(r_w)$. In particular, we have $s_1(r_w) = s_2(r_w)$; hence $(s_1 s_2) r_w = r_w$. We have $s_1(r_w) - r_w \in \mathbf{Z}\check{\alpha}_{s_1}$ and $s_2(r_w) - r_w \in \mathbf{Z}\check{\alpha}_{s_2}$. Hence $r_{s_1 s_2 w} - r_w \in (\mathbf{Z}\check{\alpha}_{s_1}) \cap (\mathbf{Z}\check{\alpha}_{s_2})$. We have $(\mathbf{Z}\check{\alpha}_{s_1}) \cap (\mathbf{Z}\check{\alpha}_{s_2}) = 0$; hence $r_{s_1 s_2 w} = r'_w$, that is, $r_{\sigma w} = r_w$. We see that (a) holds for $\tilde{G}$. This completes the proof of (a).

1.16. **Proof of Theorem 0.2.** The map $W_2 \to L$, $w \mapsto r_w$ in subsection 1.8 satisfies Theorem 0.2(i) by definition, satisfies Theorems 0.2(ii) and (iv) by Lemma 1.9, and satisfies Theorem 0.2(iii) by Lemma 1.15. It satisfies Theorem 0.2(v) since $r_w \in \mathbf{Y}_w$ and w acts as multiplication by -1 on $\mathbf{Y}_w$. This proves the existence part of Theorem 0.2.

Assume now that $w \mapsto r'_w$ is a map $W_2 \to L$ satisfying conditions like Theorem 0.2(i)–(iii). We show that $r'_w = r_w$ for $w \in W_2$ by induction on $|w|$. When $|w| \leq 1$ this follows from Theorem 0.2(i). Now assume that $|w| \geq 2$. Assume first that there exists $s \in S$ such that $|sw| < |w|$ and $sw \neq ws$. By the induction hypothesis we have $r'_{sws} = r_{sws}$; hence, by Theorem 0.2(ii), $s(r'_w) = s(r_w)$ so that $r'_w = r_w$. Assume next that no such s exists. Then by Lemma 1.4, w is the longest element in a standard parabolic subgroup W_J of W whose center contains w. Since $|w| \geq 2$ we can find two distinct elements s_1, s_2 of S which are contained in W_J. Then $s_1 w \in W_2, s_2 w \in W_2$ and $|s_1 w| < |w|, |s_2 w| < |w|$, so that by the induction hypothesis we have $r'_{s_1 w} = r_{s_1 w}$ and $r'_{s_2 w} = r_{s_2 w}$. Now let $s \in S$. If $s \neq s_1$, the

coefficient of $\check{\alpha}_s$ in r'_w is equal to the coefficient of $\check{\alpha}_s$ in r_w (they are both equal to the coefficient of $\check{\alpha}_s$ in $r'_{s_1 w} = r_{s_1 w}$; see Theorem 0.2(iii)). If $s = s_1$, then $s \neq s_2$ and the coefficient of $\check{\alpha}_s$ in r'_w is equal to the coefficient of $\check{\alpha}_s$ in r_w (they are both equal to the coefficient of $\check{\alpha}_s$ in $r'_{s_2 w} = r_{s_2 w}$; see Theorem 0.2(iii)). Thus $r'_w = r_w$. This completes the induction. Theorem 0.2 is proved.

1.17. For $w \in W_2$ and $s \in S$ such that $sw = ws$. we define a number $(w : s) \in \{-1, 0, 1\}$ as follows. Assume first that G is almost simple and simply laced. The root system $\check{R}_w, R_w$ is simply laced and has no component of type $A_l, l > 1$. Moreover, we have $\check{\alpha}_s \in \check{\Pi}_w$.

If the component containing $\check{\alpha}_s$ is not of type A_1, there is a unique sequence $\check{\alpha}_1, \check{\alpha}_2, \ldots, \check{\alpha}_m$ in $\check{\Pi}_w$ such that $\check{\alpha}_i, \check{\alpha}_{i+1}$ are joined in the Dynkin diagram of $\check{R}_w$ for $i = 1, 2, \ldots, m-1$, $\check{\alpha}_1 = \check{\alpha}_s$, and $\check{\alpha}_m$ corresponds to a branch point of the Dynkin diagram of $\check{R}_w$; if the component containing $\check{\alpha}_s$ is of type A_1, we define $\check{\alpha}_1, \check{\alpha}_2, \ldots, \check{\alpha}_m$ as the sequence with one term $\check{\alpha}_s$ (so that $m = 1$). We define $(w : s) = (-1)^m$ if $|sw| < |w|$ and $(w : s) = (-1)^{m+1}$ if $|sw| > |w|$. Next we assume that G is almost simple but not simply laced. Then G can be regarded as a fixed point set of an automorphism of a simply connected almost simple, simply laced group G' (as in subsection 1.14) with Weyl group W', a Coxeter group with a length preserving automorphism $W' \to W'$ with fixed point set W. When s is regarded as an element of W', it is a product of k commuting simple reflections $s'_1, s'_2, \ldots, s'_k$ of W'; here $k \in \{1, 2, 3\}$. If $k \in \{0, 3\}$, then we define $(w : s)$ for W to be $(w : s_i)$ for G', where i is any element of $\{1, 2, 3\}$. If $k = 2$ we have either $ws_1 = s_1 w$, $ws_2 = s_2 w$ (and $(w : s)$ for G is defined to be $(w : s_1) = (w : s_2)$ for G'), or $ws_1 = s_2 w$, $ws_2 = s_1 w$ (and $(w : s)$ for G is defined to be 0). We now drop the assumption that G is almost simple. Let G'' be the almost simple factor of G_{der} with Weyl group $W'' \subset W$ such that $s \in W''$, and let w'' be the W'-component of w. Then $(w : s)$ for G is defined to be $(w'' : s)$ for G'' (which is is defined as above).

The proof of Lemma 1.15(a) yields the following refinement of Lemma 1.15(a).

Lemma 1.18. *Let $w \in W_2$ and $s \in S$ be such that $sw = ws$. We have*
(a) $r_{sw} = r_w + (w : s)\check{\alpha}_s$.

2. The elements b_w

Assume that we are in the setup of subsection 0.1. We have the following result.

Lemma 2.1.
(a) *Let W_J be the parabolic subgroup of W generated by $J \subset S$; we assume that W_J is an irreducible Weyl group and that the centre of W_J contains the longest element w_J of W_J. Let $\alpha = \alpha_J \in R$ be the unique root such that $\alpha = \sum_{s \in J} u_s \alpha_s$ with $u_s \in \mathbf{N}$ and $\sum_s u_s$ as large as possible. We have $\dot{s}_\alpha^2 = r_{s_\alpha}(\epsilon)$.*
(b) *We have $\dot{w}_J^2 = r_{w_J}(\epsilon)$.*

We can assume that W is irreducible. We denote the simple roots by $\{\alpha_i; i \in [1, l]\}$ as in [Bou68] and the corresponding simple reflections as $\{s_i; i \in [1, l]\}$. We write ϵ_i instead of ϵ_{s_i}. We write $i_1 i_2 \cdots i_k$ instead of $\dot{s}_{i_1} \dot{s}_{i_2} \cdots \dot{s}_{i_k}$.

We note that (a) does not hold in general if w_J is not central in W_J. For example, if $W = W_J$ is of type A_2 we have $(121)^2 = 121121 = 12\epsilon_1 21 = 1\epsilon_1 1 = \epsilon_1 =$ unit element and $r_{121}(\epsilon) = \epsilon_1 \epsilon_2$.

We prove (a). By an argument in the proof of subsection 1.14(a), we can reduce the general case to the case where G is simply laced. Moreover, we can assume that $J = S$; hence $W_J = W$. In this case the proof of (a) is case by case.

Type A_1. We have $\dot{s}_\alpha^2 = \dot{s}_1^2 = \epsilon_1 = r_\alpha(\epsilon)$.

Type D_l, $l = 2n \geq 4$. We have

$$\dot{s}_\alpha = 234\cdots(l-2)(l-1)(l)(l-2)\cdots 212\cdots(l-2)(l)(l-1)(l-2)\cdots 432.$$

A direct computation shows that $\dot{s}_\alpha^2 = \epsilon_{l-1}^n \epsilon_l^n$, and this is also equal to $r_{s_\alpha}(\epsilon)$ (see subsection 1.2). For example, if $l = 4$ we have

$$234212342234212342 = 23421234\epsilon_2 34212342 = 2342123\epsilon_2\epsilon_4 3212342$$

$$= 234212\epsilon_2\epsilon_3\epsilon_4 212342 = 23421\epsilon_3\epsilon_4 12342 = 2342\epsilon_3\epsilon_4 2342$$

$$= 234\epsilon_2\epsilon_3\epsilon_4 342 = 23\epsilon_2\epsilon_3 32 = 2\epsilon_2 2 = \text{unit element}.$$

Type E_7. We have

$$\dot{s}_\alpha = 134567243156432545234651342765431.$$

(See [Lus83].) A direct computation (as for D_4 above) shows that $\dot{s}_\alpha^2 = \epsilon_3\epsilon_5\epsilon_7 = r_{\dot{s}_\alpha}(\epsilon)$. (See subsection 1.2.)

Type E_8. We have

$$\dot{s}_\alpha = 876542314563457624587634524313425436785426754365413245678.$$

(See [Lus83].) A direct computation (as for D_4 above) shows that $\dot{s}_\alpha^2 = \epsilon_2\epsilon_5\epsilon_7 = r_{\dot{s}_\alpha}(\epsilon)$. (See subsection 1.2.) This proves (a).

We prove (b). Let w be the longest element of W. By subsection 1.8(a) we have $w = \prod_{\beta \in \check{\mathcal{E}}} s_\beta$ with s_β commuting with each other; moreover, each s_β is of the form $s_{\alpha_{J'}}$, where J' is like J in the lemma, and hence (a) is applicable to it. Thus $\dot{s}_{\check{\mathcal{E}}}^2 = r_{s_\beta}(\epsilon)$. From the description of $\check{\mathcal{E}}$ in subsection 1.1 we see that $|w| = \sum_{\beta \in \check{\mathcal{E}}} |s_\beta|$; hence $\dot{w} = \prod_{\beta \in \check{\mathcal{E}}} \dot{s}_\beta$ and $\dot{w}^2 = \prod_{\beta \in \check{\mathcal{E}}} \dot{s}_\beta^2$ (using the fact the s_β commute). Using (a) for s_β we obtain $\dot{w}^2 = \prod_{\beta \in \check{\mathcal{E}}} r_{\dot{s}_\beta}(\epsilon)$; hence $\dot{w}^2 = r_w(\epsilon)$. The lemma is proved.

2.2. In this subsection we prove the following weak version of Theorem 0.3.

(a) *For any $w \in W_2$ one can find $b_w \in L/2L$ such that $b_w(\epsilon)w(b_w(\epsilon)) = r_w(\epsilon)\dot{w}^2$ or equivalently $(\dot{w}b_w(\epsilon))^2 = r_w(\epsilon)$.*

We argue by induction on $|w|$. If $|w| = 0$ we can take $b_w = 0$. Now assume that $|w| \geq 1$. Assume first that there exists $s \in S$ such that $|sw| < |w|$ and $sw \neq ws$. Then $|sws| = |w| - 2$. Using the induction hypothesis applied to $w' := sws$ and Theorem 0.2(ii), we see that we can find $b \in L/2L$ such that $b(\epsilon)w'(b(\epsilon)) = (s(r_w))(\epsilon)\dot{w}'^2$. Let $b' = s(b) + \check{\alpha}_s \in L/2L$ so that $b(\epsilon) = s(b'(\epsilon))\epsilon_s$. We have $s(b'(\epsilon)\epsilon_s)s(w(b'(\epsilon)\epsilon_s)) = s(r_w(\epsilon))\dot{w}'^2$; hence $b'(\epsilon)\epsilon_s w(b'(\epsilon))w(\epsilon_s) = r_w(\epsilon)s(\dot{w}'^2)$. We show that $b'(\epsilon)w(b'(\epsilon)) = r_w(\epsilon)\dot{w}^2$. It is enough to show that $\epsilon_s w(\epsilon_s)\dot{w}^2 = s(\dot{w}'^2)$ or that $\epsilon_s w(\epsilon_s)\dot{s}\dot{w}'\dot{s}\dot{s}\dot{w}'\dot{s} = \dot{s}^{-1}\dot{w}'^2\dot{s}$ or that $\epsilon_s w(\epsilon_s)\dot{s}\dot{w}'\epsilon_s = \dot{s}^{-1}\dot{w}'$ or that $\epsilon_s w(\epsilon_s)\dot{s}w'(\epsilon_s) = \epsilon_s\dot{s}$. This is immediate. Thus we can take $b_w = b'$ and (a) holds for w.

Next we assume that no $s \in S$ as above can be found. Then, by Lemma 1.4, w is the longest element in a standard parabolic subgroup of W whose centre contains w. By Lemma 2.1 we have $\dot{w}^2 r_w(\epsilon) = 1$. Thus we can take $b_w = 0$. This completes the proof of (a).

Note that the elements b_w do not necessarily satisfy conditions Theorem0.3(ii), (iii). The interest in proving the weaker result (a) is that unlike the proof of Theorem 0.3, it does not rely on computer calculations.

2.3. We prove the uniqueness statement in Theorem 0.3. The argument is similar to that in the proof of uniqueness in Theorem 0.2. Assume that b' and b'' are two functions of $W_2 \to L/2L$ satisfying conditions like (i), (ii), (iii) in Theorem 0.3. We show that $b'(w) = b''(w)$ for $w \in W_2$ by induction on $|w|$. When $|w| \le 1$ this follows from Theorem 0.3(i). Now assume that $|w| \ge 2$. Assume first that there exists $s \in S$ such that $|sw| < |w|$ and $sw \ne ws$. By the induction hypothesis we have $b'_{sws} = b''_{sws}$; hence, by Theorem 0.3(ii), $s(b'_w) + \check{\alpha}_s = s(b''_w) + \check{\alpha}_s$ so that $b'_w = b''_w$. Assume next that no such s exists. Then by Lemma 1.4, w is the longest element in a standard parabolic subgroup W_J of W whose center contains w. Since $|w| \ge 2$ we can find two distinct elements s_1, s_2 of S which are contained in W_J. Then $s_1 w \in W_2, s_2 w \in W_2$ and $|s_1 w| < |w|, |s_2 w| < |w|$, so that by the induction hypothesis we have $b'_{s_1 w} = b''_{s_1 w}$, $b'_{s_2 w} = b''_{s_2 w}$. Now let $s \in S$. If $s \ne s_1$, the coefficient of $\check{\alpha}_s$ in b'_w is equal to the coefficient of $\check{\alpha}_s$ in b''_w (they are both equal to the coefficient of $\check{\alpha}_s$ in $b'_{s_1 w} = b''_{s_1 w}$ (see Theorem 0.3(iii)). If $s = s_1$, then $s \ne s_2$ and the coefficient of $\check{\alpha}_s$ in b'_w is equal to the coefficient of $\check{\alpha}_s$ in b''_w (they are both equal to the coefficient of $\check{\alpha}_s$ in $b'_{s_2 w} = b''_{s_2 w}$; see Theorem 0.3(iii)). Thus $b'_w = b''_w$. This completes the inductive proof of uniqueness.

2.4. We sketch a proof of the existence part of Theorem 0.3 in the setup of subsection 1.10. In this case the set Σ of simple coroots consists of

$$e_1 - e_2, e_2 - e_3, \ldots, e_{l-1} - e_l, e_{l-1} + e_l.$$

Let $w \in W_2$. For any two element subset $\{\beta, \beta'\}$ of $\check{\mathcal{E}}_w$ we define a subset $\mathcal{M}_{\beta, \beta'} \subset \Sigma$ as follows:

(a) Assume that $\{\beta, \beta'\} = \{e_i - e_j, e_k - e_h\}$, where $i < j, k < h, i \ne k, i \ne h, j \ne k, j \ne h$. Then $\mathcal{M}_{\beta, \beta'}$ consists of all $e_a - e_{a+1} \in \Sigma$ such that $i \le a < a + 1 \le j$, $k \le a < a + 1 \le h$.

(b) Assume that $\{\beta, \beta'\} = \{e_i - e_j, e_k + e_h\}$, where $i < j, k < h, i \ne k, i \ne h, j \ne k, j \ne h$. Then $\mathcal{M}_{\beta, \beta'}$ consists of all $e_a - e_{a+1} \in \Sigma$ such that $i \le a < a + 1 \le j$, $k \le a < a + 1 \le h$.

(c) Assume that $\{\beta, \beta'\} = \{e_i + e_j, e_k + e_h\}$, where $i < j, k < h, i \ne k, i \ne h, j \ne k, j \ne h$. Then $\mathcal{M}_{\beta, \beta'}$ consists of all $e_a - e_{a+1} \in \Sigma$ such that $a = n - 2 \mod 2$, $i \le a < a + 1 \le j, k \le a < a + 1 \le h$.

(d) Assume that $\{\beta, \beta'\} = \{e_i - e_j, e_i + e_j\}$, where $i < j$. Then $\mathcal{M}_{\beta, \beta'}$ consists of all $e_a - e_{a+1} \in \Sigma$ such that $a = n - 2 \mod 2, i \le a < a + 1 \le j$.

Let S' be a halving of S. We have $r_w = \sum_{s \in S} c_s \check{\alpha}_s$, where $c_s \in \mathbf{N}$. We set $r_w^{S'} = \sum_{s \in S} c'_s \check{\alpha}_s \in L/2L$, where $c'_s = c_s$ if $s \in S'$ and $c'_s = 0$ if $s \in S - S'$. We define

$$b_w = r_w^{S'} + \sum_{\beta, \beta'} \sum_{s \in S; \check{\alpha}_s \in \mathcal{M}_{\beta, b'}} \check{\alpha}_s,$$

where $\{\beta, \beta'\}$ runs through all 2 element subsets of $\check{\mathcal{E}}_w$. One can verify that the elements $b_w, w \in W_2$, satisfy conditions (i)-(iv) in Theorem 0.3. This, together with subsection 2.3 proves Theorem 0.3 when G is almost simple of type D_l (except for condition Theorem 0.3(v)).

Now if G is adjoint of type A_l, $l \geq 1$, then G can be regarded as the adjoint group of a Levi subgroup of a parabolic subgroup in a group of type $D_{l'}$ for some l' such that $l < l' \geq 4$, and Theorem 0.3 for G can be deduced from the results above (for type $D_{l'}$) (except for condition Theorem 0.3(v)).

Next, the argument in the proof of uniqueness in subsection 2.3 can be viewed as an inductive method to compute b_w in Theorem 0.3 for any $w \in W_2$ by induction on $|w|$. This can be used to prove the existence statement in Theorem 0.3(i)–(iv) in any given case with a powerful enough computer. We have used this method to prove the existence statement in Theorem 0.3(i)–(iv) for G of type E_8. (I thank Gongqin Li for carrying out the programming in GAP using the CHEVIE package.) Then Theorem 0.3(i)–(iv) automatically holds for G of type E_7 and E_6. We see that Theorem 0.3 holds for any simply laced G (except for condition Theorem 0.3(v)).

2.5. We show:

(a) *If Theorem 0.3(i)–(iv) is assumed to hold for G, then Theorem 0.3(v) holds for G.*

We prove the equality in Theorem 0.3(v) for $w \in W_2$ by induction on $|w|$. If $|w| = 0$ the result is obvious. Assume first that there exists $s \in S$ such that $sw \neq ws$, $|sw| < |w|$. We have $|sws| = |w| - 2$. By the induction hypothesis we have $w'(b_{w'}(\epsilon))b_{w'}(\epsilon) = r_{w'}(\epsilon)\dot{w}'^2$ where $w' = sws$. As in the proof in subsection 2.2 we deduce that $b' := s(b_{w'}) + \check{\alpha}_s$ satisfies $w(b'(\epsilon))b'(\epsilon) = r_w(\epsilon)\dot{w}^2$. By Theorem 0.3(ii) we have $b' = b_w$. Thus Theorem 0.3(v) holds for w. Next we assume that no s as above can be found. Then, by Lemma 1.4, w is the longest element of a standard parabolic subgroup W_J of W and w is in the centre of W_J. In this case, using Lemma 2.1, we see that it is enough to show that $w(b_w(\epsilon)) = b_w(\epsilon)$. From the definition we see that $b_w = \sum_{s \in J} a_s \check{\alpha}_s$, where $a_s \in \{0, 1\}$. Hence to show that $w(b_w(\epsilon)) = b_w(\epsilon)$ it is enough to show that for any $s \in J$ we have $w(\check{\alpha}_s) = \check{\alpha}_s$ in $L/2L$. This is clear since $w(\check{\alpha}_s) = -\check{\alpha}_s$ in L. This completes the proof of (a).

We see that Theorem 0.3 holds for any simply laced G.

2.6. In this subsection we assume that $G, \iota, \tilde{G}, \tilde{T}, \tilde{W}, \tilde{S}, \tilde{Y}, ||_\iota, \tilde{W}_2$ are as in the proof of subsection 1.14(a). Assume that S' is a halving of S such that $\iota(S') = S'$. (Such a halving exists.) Assume also that $w \mapsto b_w$ is a function $W_2 \to L/2L$ satisfying Theorem 0.3(i)–(iv) for G. Let $\tilde{S}'$ be the subset of $\tilde{S}$ consisting of the elements $\sigma = \prod_s s$, where s runs over an ι-orbit in S'. Clearly, $\tilde{S}'$ is a halving of $\tilde{S}$ (and any halving of $\tilde{S}$ is of this form). Let $\tilde{L}$ be the subgroup of L generated by the coroots of $\tilde{G}$. We have canonically $\tilde{L}/2\tilde{L} = (L/2L)^\iota$. We define a function $\tilde{b} : \tilde{W}_2 \to \tilde{L}/2\tilde{L}$ by $w \mapsto \tilde{b}_w = b_w$. (Note that if $w \in \tilde{W}_2$, then $\iota(b_w) = b_w$, by the uniqueness statement in Theorem 0.3.) We show:

(a) *The function $\tilde{W}_2 \to \tilde{L}/2\tilde{L}$, $w \mapsto \tilde{b}_w$ satisfies Theorem 0.3(i)–(iv) for $\tilde{G}$.*

We have $\tilde{b}_1 = 0$. Let $\sigma \in \tilde{S}$. Now σ corresponds to an ι-orbit $\mathcal{O}$ in S. We can view σ as an element of W_2 and we have $\tilde{b}_\sigma = b_\sigma = \sum_{s \in \mathcal{O}} \check{\alpha}_s$ if $\mathcal{O} \subset S'$ and $\tilde{b}_\sigma = 0$ if $\mathcal{O} \subset S - S'$ (this follows from Theorem 0.3(i) for b applied to each $s \in \mathcal{O}$ and from Theorem 0.3(iii) for G applied to $\sigma \in W_2$). Thus Theorem 0.3(i) holds for $\tilde{b}$.

Now let $w \in \tilde{W}_2$ and $\sigma \in \tilde{S}$ be such that $\sigma w \neq w \sigma$. We write $\sigma = \{s_1, \ldots, s_k\} \subset S$. Then for some $i \in [1, k]$ we have $s_i w \neq w s_i$. Hence for all $i \in [1, k]$ we have $s_i w \neq w s_i$. Hence we have $s_1 w \neq w s_1, s_2 s_1 w \neq w s_1 s_2, \ldots, s_k \cdots s_1 w \neq w s_1 \cdots s_k$. By Theorem 0.3(ii) for b we have $b_w = s_1(b_{s_1 w s_1}) + \check{\alpha}_{s_1}$, $s_1(b_{s_1 w s_1}) = s_1 s_2(b_{s_2 s_1 w s_1 s_2}) + \check{\alpha}_{s_2}$, and $s_1 \cdots s_k(b_{s_k \cdots s_1 w s_1 \cdots s_k}) = s_1 \cdots s_{k-1}(b_{s_{k-1} \cdots s_1 w s_1 \cdots s_{k-1}}) +$

$\check{\alpha}_{s_k}$ so that $b_{\sigma w\sigma} = \sigma(b_w) + \check{\alpha}_{s_1} + \cdots + \check{\alpha}s_k$; that is, $\tilde{b}_{\sigma w\sigma} + \sigma(\tilde{b}_w) + \check{\alpha}_{s_1} + \cdots + \check{\alpha}s_k$. We see that 0.3(ii) holds for $\tilde{b}$.

Next, let $w \in \tilde{W}_2 \cap \tilde{W}$ and $\sigma \in \tilde{S}$ be such that $\sigma w = w\sigma$. We write $\mathcal{O} = \{s_1, \ldots, s_k\} \subset S$, $\sigma = s_1 \cdots s_k$, where ι permutes $s_1, s_2, \ldots, s_k$ cyclically: $s_1 \mapsto s_2 \mapsto \cdots \mapsto s_k \mapsto s_1$. (Note that $k \leq 3$.) As in the proof of subsection 1.15 we have $w(\check{\alpha}_{s_i}) = \check{\alpha}_{s_{h(i)}}$ for all $i \in [1, k]$, where h is a permutation of $[1, k]$ such that $h = 1$ unless $k = 2$.

Assume first that $h = 1$. We have:

$$w(\check{\alpha}_{s_1}) = \check{\alpha}_{s_1}, (s_1 w)(\check{\alpha}_{s_2}) = \check{\alpha}_{s_2}, \ldots, (s_{k-1} \cdots s_1 w)(\check{\alpha}_{s_k}) = \check{\alpha}_{s_k};$$

hence $s_1 w = w s_1$, $s_2 s_1 w = s_1 w s_2, \ldots, s_k \cdots s_1 w = s_{k-1} \cdots s_1 w s_k$, $|s_1 w| > |w|$, and $|s_2 s_1 w| > |s_1 w|, \ldots, |s_k \cdots s_1 w| > |s_{k-1} \cdots s_1 w|$. By Theorem 0.3(iii) for b we have $b_{s_1 w} - b_w = l_1 \check{\alpha}_{s_1}$, $b_{s_2 s_1 w} - b_{s_1 w} = l_2 \check{\alpha}_{s_2}$, and $b_{s_k \cdots s_2 s_1 w} - b_{s_{k-1} \cdots s_1 w} = l_k \check{\alpha}_{s_k}$ with $l_1, \ldots, l_l$ in $\{0, 1\}$. Taking the sum we obtain $b_{\sigma w} - b_w = b_{s_k \cdots s_2 s_1 w} - b_w = l_1 \check{\alpha}_{s_1} + \cdots + l_k \check{\alpha}_{s_k}$. Since $b_{\sigma w} - b_w$ is fixed by ι, so must $l_1 \check{\alpha}_{s_1} + \cdots + l_k \check{\alpha}_{s_k}$. It follows that $l_1 = \cdots = l_k$ so that $b_{\sigma w} - b_w = l_1(\check{\alpha}_1 + \cdots + \check{\alpha}_k)$. We see that Theorem 0.3(iii) holds for $\tilde{b}$. Repeatedly using Theorem 0.3(iv) for b we have $\sigma(b_w) = s_1 s_2 \cdots s_k(b_w) = b_w$ (here we use the fact that G is simply laced). We see that Theorem 0.3(iv) holds for $\tilde{b}$ (in this case we have $r_{\sigma w} - r_w = \pm(\check{\alpha}_1 + \cdots + \check{\alpha}_k)$ by the proof of Lemma 1.15).

Next we assume that $h \neq 1$; then $k = 2$ and $w(\check{\alpha}_{s_1}) = \check{\alpha}_{s_2}$, $w(\check{\alpha}_{s_2}) = \check{\alpha}_{s_1}$. It follows that $w s_1 w = s_2$. We have $s_1 s_2 w = s_1 w s_1 \neq w$ and $s_1 s_2 w = s_2 w s_2 \neq w$. By Theorem 0.3(ii) for b we have

$$b_{s_1 s_2 w} = b_{s_1 w s_1} = s_1(b_w) + \check{\alpha}_{s_1} = b_w + c_1 \check{\alpha}_1,$$
$$b_{s_1 s_2 w} = b_{s_2 w s_2} = s_2(b_w) + \check{\alpha}_{s_2} = b_w + \chi_2 \check{\alpha}_2 \text{ where } c_1, c_2 \in \{0, 1\}.$$

It follows that $c_1 \check{\alpha}_1 = c_2 \check{\alpha}_2$ in $L/2L$. Hence $c_1 = c_2 = 0$ and $b_{s_1 s_2 w} = b_w$; that is, $b_{\sigma w} = b_w$. We see that Theorem 0.3(iii) holds for $\tilde{b}$. By Theorem 0.3(ii) for b we have $b_{w s_1 s_2} = b_{s_1 w s_1} = s_1(b_w) + \check{\alpha}_1$ and $b_{w s_1 s_2} = b_{s_2 w s_2} = s_2(b_w) + \check{\alpha}_2$; hence $s_1(b_w) + \check{\alpha}_1 = s_2(b_w) + \check{\alpha}_2$. Applying s_1 we obtain $s_1 s_2(b_w) + \check{\alpha}_2 = b_w + \check{\alpha}_1$; hence $\sigma(b_w) = b_w + \check{\alpha}_1 + \check{\alpha}_2$. We see that Theorem 0.3(iv) holds for $\tilde{b}$ (in this case we have $r_{\sigma w} - r_w = 0$ by the proof of Lemma 1.15). This completes the proof of (a).

2.7. From subsection 2.6 we see that Theorem 0.3(i)–(iv) can be reduced to the case where G is simply laced. Using this and the results in subsection 2.5 we see that Theorem 0.3 holds in the general case.

2.8. Let S' be a halving of S. Then clearly $S - S'$ is a halving of S. We define $W_2 \to L/2L$ by $w \mapsto b_w^* = b_w + r_w$, where $b_w = b_w^{S'}$. We have:

(a) $b_w^{S-S'} = b_w^*$.

The fact that b^* satisfies Theorem 0.3(i) for $S - S'$ is immediate; that it satisfies Theorem 0.3(ii) for $S - S'$ follows from Lemma 1.9(a); that it satisfies Theorem 0.3(iii) for $S - S'$ follows from subsection 1.13(a). Then (a) follows from the uniqueness in Theorem 0.3.

2.9. **Proof of Theorem 0.5.** In this subsection we assume that we are in the setup of subsection 0.4. Let w, c, S' be as in Theorem 0.5. We must show that

$$\phi(n_{w,c,S'})n_{w,-\phi(c),S'} = 1.$$

We write b_w instead of $b_w^{S'}$. We have $\phi(\dot{w}) = \dot{w}$, $\phi(r_w(c)) = r_w(\phi(c))$, and $\phi(b_w(\epsilon)) = b_w(\epsilon)$; hence

$$\phi(n_{w,c,S'})n_{w,-\phi(c),S'} = \phi(\dot{w}r_w(c)b_w(\epsilon))\dot{w}r_w(-\phi(c))b_w(\epsilon)$$
$$= \dot{w}r_w(\phi(c))b_w(\epsilon)\dot{w}r_w(-\phi(c))b_w(\epsilon) = \dot{w}^2w(r_w(\phi(c)))w(b_w(\epsilon))r_w(-\phi(c))b_w(\epsilon)$$
$$= w(r_w(\phi(c)))r_w(-\phi(c))r_w(\epsilon) = w(r_w(\phi(c)))r_w(\phi(c)).$$

This equals 1 since $w(r_w(\phi(c))) = r_w(\phi(c)^{-1})$ by Theorem 0.2(v). Theorem 0.5 is proved.

2.10. Assume now that G is almost simple. Then there are exactly two halvings S', $S - S'$ for S. Let $w \in W_2$. We note that the family of elements $\{n_{w,c,S'}; c \in \mathbf{k}^*\}$ coincides with the family of elements $\{n_{w,c,S-S'}; c \in \mathbf{k}^*\}$. Indeed, by subsection 2.8(a) we have

$$n_{w,c,S-S'} = \dot{w}r_w(c)b_w^{S'}(\epsilon)r_w(\epsilon) = n_{w,\epsilon c,S'}.$$

2.11. In this subsection we assume that $\mathbf{k}, G, \phi, \phi', F_q$ are as in subsection 0.4 (in case subsection 0.4(i)). Now:

(a) $g_1 : g \mapsto g_1 g\phi(g_1)^{-1}$

defines an action of $G^{\phi^2} = G(F_{q^2})$ on $G^{\phi'}$. Indeed for $g_1 \in G^{\phi^2}$, $g \in G^{\phi'}$. We have

$$\phi(g_1 g\phi(g_1)^{-1})g_1 g\phi(g_1)^{-1} = \phi(g_1)\phi(g)g_1^{-1}g_1 g\phi(g_1)^{-1}$$
$$= \phi(g_1)\phi(g)g\phi(g_1)^{-1} = \phi(g_1)\phi(g_1)^{-1} = 1,$$

and our claim follows. We have $1 \in G^{\phi'}$ and the stabilizer of 1 for the action above is G^{ϕ}. Thus we have an injective map $G^{\phi^2}/G^{\phi} \to G^{\phi'}$. We show that this is a bijection. Let $g \in G^{\phi'}$. By Lang's theorem we have $g = g_1\phi(g_1)^{-1}$ for some $g_1 \in G$. We have $g\phi(g) = 1$; hence $g_1\phi(g_1)^{-1}\phi(g_1)\phi^2(g_1)^{-1} = 1$. That is, $g_1\phi^2(g_1)^{-1} = 1$ so that $g_1 \in G^{\phi^2}$. We see that g is in the G^{ϕ^2}-orbit of 1. Thus we have the following result.

(b) *The action* (a) *of* $G^{\phi^2} = G(F_{q^2})$ *on* $G^{\phi'}$ *is transitive; the stabilizer of 1 for this action is* G^{ϕ}. *Hence* $\sharp(G^{\phi'}) = \sharp(G^{\phi^2})/\sharp(G^{\phi})$.

References

[Bou68] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines* (French), Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968. MR0240238

[GHL+96] Meinolf Geck, Gerhard Hiss, Frank Lübeck, Gunter Malle, and Götz Pfeiffer, *CHEVIE—a system for computing and processing generic character tables*, Computational methods in Lie theory (Essen, 1994), Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 3, 175–210. MR1486215

[Kos12] Bertram Kostant, *The cascade of orthogonal roots and the coadjoint structure of the nilradical of a Borel subgroup of a semisimple Lie group* (English, with English and Russian summaries), Mosc. Math. J. **12** (2012), no. 3, 605–620, 669. MR3024825

[Lus83]   George Lusztig, *Some examples of square integrable representations of semisimple p-adic groups*, Trans. Amer. Math. Soc. **277** (1983), no. 2, 623–653. MR694380

[L2]   G.Lusztig, *Hecke modules based on involutions in extended Weyl groups*, arxiv:1710.03670.

[T]   J. Tits, *Normalisateurs de tores. I. Groupes de Coxeter étendus* (French), J. Algebra **4** (1966), 96–116. MR0206117

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASSACHUSETTS 02139

Email address: gyuri@math.mit.edu