Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 32 (1986)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SOME CHARACTERIZATIONS OF COXETER GROUPS
Autor: Deodhar, Vinay V.
Kapitel: §2. Main Theorem
DOI: https://doi.org/10.5169/seals-55081

properties characterize Coxeter groups. It therefore seems worthwhile to compile together various characterizations of Coxeter groups. This is done in § 2. A part of it is of expository nature though our proofs for the well-known characterizations are somewhat more direct.

The author wishes to thank J. Tits and J. E. Humphreys for encouragement for writing this note up. Thanks are also due to T. Springer for his comments on a preliminary version of this note.

§ 2. Main Theorem

Let W be a group generated by a set S of involutary generators (i.e. order $s = 2\ \forall s \in S$). One then has the notion of the length $l(w)$ of an element $w \in W$ viz. the least integer k such that $w = s_1 \dots s_k$ with $s_i \in S$. Further, such an expression is called a reduced expression. We then have the following:

Main Theorem. Let W, S be as above. Then the following conditions are equivalent:

1) *Coxeter condition:* If $\tilde{W}$ is the free group generated by a copy $\tilde{S}$ of S subject to relations $(\tilde{s})^2 = \mathrm{id}\ \forall s \in S$ and $\eta : \tilde{W} \to W$ is the canonical map, then Ker η is generated as a normal subgroup by elements of the type:

$\{(\tilde{s}_1\tilde{s}_2)^{m_{s_1,s_2}}, s_1 \neq s_2 \in S, m_{s_1,s_2} \geqslant 2\}$ i.e. $<S \mid s^2 = \mathrm{id}\ \forall s \in S, (s_1 s_2)^{m_{s_1,s_2}} = \mathrm{id}$

for some pairs $s_1 \neq s_2$ in $S>$ is a presentation of W. (Note that the above relations *may not* involve *all* pairs $s_1 \neq s_2$).

2) *Root-system condition:* There exists a representation V of W over $\mathbf{R}$, a W-invariant set Φ of non-zero vectors in V which is symmetric (i.e. $\Phi = -\Phi$) and a subset $\{e_s \mid s \in S\}$ of Φ such that the following conditions are satisfied.

(i) Every $\phi \in \Phi$ can be written as $\sum_{s \in S} a_s e_s$ with either all $a_s \geqslant 0$ or all $a_s \leqslant 0$, but not in both ways.

(Accordingly, we write $\phi > 0$ or $\phi < 0$.)

(ii) $e_s \in \Phi$, $s(e_s) < 0$ and $s(\phi) > 0$ for all $\phi > 0$, $\phi \neq e_s$.

(iii) If $w \in W$, $s, s' \in S$ are such that $w(e_{s'}) = e_s$. Then $ws'w^{-1} = s$.

3) *Strong exchange condition:* If $t \in T = \bigcup_{x \in W} xSx^{-1}$ and $w \in W$ are such that $l(tw) \leqslant l(w)$ then for any expression (not necessarily reduced) $w = s_1 \dots s_p$, one has $tw = s_1 \dots \hat{s}_i \dots s_p$ for some i.

4) *Bruhat condition:* For $w \in W$ one can associate a subset $\mathrm{Br}(w)$ of W such that the following conditions are satisfied:

(i) If $w = s_1 \dots s_k$ is any reduced expression then

$$\mathrm{Br}(w) = \{x \in W \mid x = s_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_m} \dots s_k \text{ for some } m \geqslant 0 \text{ and } 1 < i_1 < \dots < i_m \leqslant k\}.$$

(ii) For $w \in W$ and $t \in T$, we have the dichotomy: either $w \in \mathrm{Br}(tw)$ or $tw \in \mathrm{Br}(w)$.

5) *Hyperplane condition.* For $s \in S$ one can associate a subset P_s of W such that the following conditions are satisfied:

(i) $\mathrm{id} \in P_s \ \forall s \in S$,

(ii) $P_s \cap sP_s = \emptyset \ \forall s \in S$,

(iii) If $w \in W$, $s, s' \in S$ are such that $w \in P_s$ and $ws' \notin P_s$ then $ws'w^{-1} = s$.

6) *Exchange condition:* If $w \in W$, $s \in S$ are such that $l(sw) \leqslant l(w)$ then for any reduced expression $w = s_1 \dots s_k$, one has $sw = s_1 \dots \hat{s}_j \dots s_k$ for some j.

Remarks:

1) (W, S) is called a Coxeter group if it satisfies the equivalent conditions of the theorem.

2) Equivalence of conditions (1), (5) and (6) is well-known. ([B, Thm. 1, Prop. 6].) The name "hyperplane condition" is derived from the applicability of the condition (5) to groups generated by reflections in hyperplanes (e.g. Weyl groups).

3) The condition (3) is known in literature.

4) Condition (4) allows one to define a partial order on W viz. $x \leqslant w$ iff $x \in \mathrm{Br}(w)$; this is the Bruhat ordering on W.

5) In condition (2), one does not assume the faithfulness of V; it follows as a consequence of properties (i)-(iii). The set Φ can be called *a* root system associated to W. It should be noted that neither of V and Φ is

unique e.g. keeping V fixed, the set $\Phi_R = \bigcup_{\substack{s\in S\\ w\in W}} w(e_s)$ can be seen to satisfy properties (i)-(iii).

6) The relevance of conditions (2) and (4) is discussed in the introduction. Note that in condition (2), the set $\{e_s \mid s \in S\}$ need not be linearly independent.

7) Since W is generated by a set S of involutions and $\mathrm{id} \notin S$, it is clear that $l(s) = 1\ \forall s \in S$. Also, for $w \in W$ and $s \in S$, $| l(sw) - l(w) | \leqslant 1$ and $| l(ws) - l(w) | \leqslant 1$. However, we do not assume, to begin with, that equality holds. In other words, we do not assume the existence of a sign character σ on W such that $\sigma(s) = -1\ \forall s \in S$. This condition is obviously built in conditions (1), (3) and (6). It is not so obvious in conditions (2) and (5) although it follows as a consequence. In condition (4), it is not true if one leaves out part (ii) of the condition. (The group $\mathbf{Z}_2 \times \mathbf{Z}_2$ provides an easy counter-example.)

Proof of Main Theorem:

(1) $\Rightarrow$ (2). The construction of the representation V and the set Φ is along the same lines as in ([D]) with suitable modifications to fit into our present set-up.

We quickly recall the construction of V. For a pair $s_1 \neq s_2 \in S$, define m_{s_1,s_2} to be the least integer such that $(\tilde{s}_1\tilde{s}_2)^{m_{s_1,s_2}} \in \operatorname{Ker} \eta$. (Here, we use the convention viz. $m_{s_1,s_2} = \infty$ if no non-zero power of $\tilde{s}_1\tilde{s}_2$ belongs to $\operatorname{Ker} \eta$.) Let V be a vector-space over $\mathbf{R}$ with $\{e_s \mid s \in S\}$ as a basis. Define a bilinear form (,) on V by setting

$$(e_s, e_s) = 1\ \forall s \in S, (e_{s_1}, e_{s_2}) = (e_{s_2}, e_{s_1}) = -\cos\left(\frac{\pi}{m_{s_1,s_2}}\right)$$

for $s_1 \neq s_2 \in S$ and then extending bilinearly to $V \times V$.

For $\tilde{s} \in \tilde{S}$, $v \in V$, define $\tilde{s}(v) = v - 2(v, e_s)e_s$. It can be easily checked that $(\tilde{s})^2(v) = v\ \forall v \in V$ and that $(\tilde{s}_1\tilde{s}_2)^{m_{s_1 s_2}}(v) = v\ \forall v \in V$ if $s_1 \neq s_2$ and $m_{s_1,s_2} < \infty$. Since $\operatorname{Ker} \eta$ is generated as a normal subgroup by these elements, it is clear that one has an action of W on V such that $s(v) = v - 2(v, e_s)e_s\ \forall v \in V, s \in S$. Note also that $\big(s(v), s(v')\big) = (v, v')\ \forall v, v' \in V$ and hence $\big(w(v), w(v')\big) = (v, v')\ \forall v, v' \in V$, $w \in W$. Let $\Phi = \bigcup_{s\in S} W(e_s)$. Then Φ is obviously W-invariant. Note that $s(e_s) = -e_s$ and so $\Phi = -\Phi$ and $(\phi, \phi) = 1\ \forall \phi \in \Phi$.

We next prove by induction on $l(w)$ that for $s' \in S$,

$$\text{(I)} \qquad l(ws') \geqslant l(w) \Rightarrow w(e_{s'}) = \sum_{s\in S} a_s e_s \quad \text{with} \quad a_s \geqslant 0,\ s \in S\,.$$

If $l(w) = 0$ then $w = \mathrm{id}$ and there is nothing to prove. So let $l(w) \geqslant 1$. Choose $s'' \in S$ such that $l(ws'') = l(w) - 1$. Since $l(ws') \geqslant l(w)$, $s' \neq s''$. Let $J = \{s', s''\}$ and W_J be the subgroup of W generated by J. Let l_J denote the length function in $W_J (l \leqslant l_J$ on $W_J)$. Consider the set $A = \{z \in W \mid z^{-1}w \in W_J$ and $l(z) + l_J(z^{-1}w) = l(w)\}$. Clearly $w \in A$. Choose $x \in A$ such that $l(x)$ is minimum. Now $ws'' \in A$ as can be checked and so $l(x) \leqslant l(ws'') = l(w) - 1$. Next, if possible, let $l(xs') < l(x)$. Then $l(xs') = l(x) - 1$ and we have,

$$l(w) \leqslant l(xs') + l(s'x^{-1}w) \leqslant l(xs') + l_J(s'x^{-1}w) = l(x) - 1 + l_J(s'x^{-1}w)$$
$$\leqslant l(x) - 1 + l_J(x^{-1}w) + 1 = l(x) + l_J(x^{-1}w) = l(w)\,.$$

Thus equality must hold at all places and so $l(w) = l(xs') + l_J(s'x^{-1}w)$. This means $xs' \in A$ which is a contradiction since $l(xs') < l(x)$. Hence $l(xs') \geqslant l(x)$. Similarly we can prove that $l(xs'') \geqslant l(x)$. Since $l(x) < l(w)$, we can apply induction to pairs (x, s') and (x, s'') to get: $x(e_{s'}) = \sum_{s\in S} c_s e_s$ and $x(e_{s''}) = \sum_{s\in S} d_s e_s$ with $c_s, d_s \geqslant 0\ \forall s \in S$.

Let $y = x^{-1}w$. If possible, let $l_J(ys') < l_J(y)$. Then

$$l_J(ys') = l_J(y) - 1 \quad \text{and} \quad l(ws') = l(x\,x^{-1}ws') \leqslant l(x) + l(x^{-1}ws')$$
$$\leqslant l(x) + l_J(ys') = l(x) + l_J(y) - 1 = l(w) - 1$$

which is a contradiction since $l(ws') \geqslant l(w)$. Thus $l_J(ys') \geqslant l(y)$. Write down a reduced expression for y in terms of generators s' and s''. It is clear that it ends with s''. Now either $m_{s',s''} = \infty$, in which case a direct computation shows that $y(e_{s'}) = pe_{s'} + qe_{s''}$ with $p, q \geqslant 0$ (also, $|p-q| = 1$) or $m_{s',s''} < \infty$, in which case $l_J(y) < m_{s',s''}$. (Note that $(s's'')^{m_{s',s''}} = \mathrm{id}$). Again a direct computation shows that $y(e_{s'}) = pe_{s'} + qe_{s''}$ with $p, q \geqslant 0$. In either case, $y(e_{s'}) = pe_{s'} + qe_{s''}$ with $p, q \geqslant 0$. Hence $w(e_{s'}) = x \cdot y(e_{s'}) = x(pe_{s'} + qe_{s''}) = \sum_{s\in S} (pc_s + qd_s)e_s$ with $a_s = pc_s + qd_s \geqslant 0\ \forall s \in S$. This verifies the induction hypothesis for w and so (I) is true.

Now given $\phi \in \Phi$, $\phi = w(e_{s'})$ for some $w \in W$, $s' \in S$. If $l(ws') \geqslant l(w)$ then $\phi > 0$ by (I). If $l(ws') < l(w)$ then $ws'(e_{s'}) > 0$ by (I) (Note; $l(ws' \cdot s') \geqslant l(ws')$). Hence $\phi < 0$ in this case. This proves (i). Note that we have proved a more precise statement than (i) viz.

$$(*) \qquad l(ws') \geqslant l(w) \Rightarrow w(e_{s'}) > 0\,.$$

We now come to the proof of (ii). Obviously $e_s \in \Phi$ and $s(e_s) = -e_s < 0$. Next, let $\phi > 0$ and $\phi \neq e_s$. Since $(\phi, \phi) = 1$, it is clear that ϕ can't be a multiple of e_s. Since $s(\phi) - \phi$ is a multiple of e_s, it is easy to see that $s(\phi) > 0$. (This is the "standard" argument with any "root-system".)

Next, let $w(e_{s'}) = e_s$. Consider $y = ws'w^{-1}s$. Then for any

$$v \in V,\ y(v) = ws'w^{-1}(v - 2(v, e_s)e_s) = ws'(w^{-1}(v) - 2(v, e_s)w^{-1}(e_s))$$
$$= w(w^{-1}(v) - 2(w^{-1}(v), e_{s'})e_{s'} + 2(v, e_s)e_{s'})$$

(This is because $w^{-1}(e_s) = e_{s'}) = w(w^{-1}(v) - 2(v, w(e_{s'}))\, e_{s'} + 2(v, e_s)e_{s'}) = w(w^{-1}(v)) = v$. In other words, $y(v) = v \ . \ v \in V$. Now, if possible, let $y \neq \mathrm{id}$. Then $\exists s'' \in S$ such that $l(ys'') < l(y)$. By applying (*) to ys'', we get $ys''(e_{s''}) > 0$ i.e. $y(-e_{s''}) > 0$ i.e. $-e_{s''} > 0$. This is a contradiction. Hence $y = \mathrm{id}$ and so $ws'w^{-1} = s$. This proves (iii).

We note at this stage that the special representation constructed above is the so-called geometric realization of W as given in ([B]). The fact that this is faithful as well as some other properties of it are consequences of conditions (i)-(iii). We will prove these things for any representation with conditions (i)-(iii); this is done in the next implication.

(2) $\Rightarrow$ (3). We first observe that $s(e_s) = -e_s$. (For: $-s(e_s) > 0$ and $s(-s(e_s)) = -e_s < 0$ and so $-s(e_s) = e_s$ by (ii).)

Next, we establish a one-one correspondence between T and the set $\{\phi > 0 \mid \phi = w(e_s) \text{ for some } s \in S,\ w \in W\}$. For $\phi > 0$ such that $\phi = w(e_s)$, define $t_\phi = wsw^{-1}$. Condition (iii) then ensures that t_ϕ is independent of the choice of w and s. Conversely, let $t \in T$ such that $t = wsw^{-1}$. Define $\phi_t = w(e_s)$ or $-w(e_s)$ whichever is > 0. We want to claim that ϕ_t is independent of the choice of w and s. So let $t = wsw^{-1} = w_1 s_1 w_1^{-1}$. Then $w^{-1}w_1 s_1 w_1^{-1} w = s$. Consider $\psi = w^{-1}w_1(e_{s_1})$. Now

$$s(\psi) = w^{-1}w_1 s_1 w_1^{-1} w w^{-1} w_1(e_{s_1}) = w^{-1}w_1 s_1(e_{s_1}) = -w^{-1}w_1(e_{s_1}) = -\psi\,.$$

It is now clear from (ii) that $e_s = \psi$ or $-\psi$ whichever is positive. Our claim is now clear. It is easy to see that these two maps are inverses of each other. It is also easy to see that $t(\phi_t) = -\phi_t$.

We now prove the following:

(**) Let $w = s_1 \dots s_p$ be any expression (not necessarily reduced) and $t \in T$ such that $w^{-1}(\phi_t) < 0$ then $tw = s_1 \dots \hat{s}_i \dots s_p$ for some $1 \leqslant i \leqslant p$.

To prove this, observe that $\phi_t > 0$ and $w^{-1}(\phi_t) = s_p \dots s_1(\phi_t) < 0$. Hence $\exists\, 1 \leqslant i \leqslant p$ such that

$$s_{i-1} \dots s_1(\phi_t) > 0 \quad \text{and} \quad s_i \dots s_1(\phi_t) < 0\,.$$

By (ii), $s_{1-i} \dots s_1(\phi_t) = e_{s_i}$ i.e. $\phi_t = s_1 \dots s_{i-1}(e_{s_i})$. Now from the correspondence mentioned earlier, it is clear that $t = s_1 \dots s_{i-1} s_i s_{i-1} \dots s_1$. Thus $tw = s_1 \dots \hat{s}_i \dots s_p$.

As a consequence of (**), we get: For

$$w \in W,\ t \in T\ w^{-1}(\phi_t) < 0 \Rightarrow l(tw) < l(w) \Rightarrow l(tw) \leqslant l(w) \Rightarrow w^{-1}(\phi_t) < 0$$

(i.e. $w^{-1}(\phi_t) < 0$ iff $l(tw) < l(w)$ iff $l(tw) \leqslant l(w)$). Indeed, the first implication follows by applying (**) to a reduced expression of w and the last implication follows by applying the first implication to the pair tw, t. (Note that $t = t^{-1}$.)

The strong exchange condition is now clear. Hence (3) is proved.

Before proceeding further with the proof of the main Theorem, we observe the following consequences of (**):

(***) For $y \in W$, let $\Phi_y^+ = \{\phi > 0 \mid y^{-1}(\phi) < 0\}$ then $|\Phi_y^+| = l(y)$. In particular, the representation V is faithful.

Proof of (***). Let $y = s_1 \dots s_k$ be a reduced expression. Consider $\phi_i = s_1 \dots s_{i-1}(e_{s_i})$, $1 \leqslant i \leqslant k$. We then claim that $\phi_j > 0\ \forall j$, $\phi_j \neq \phi_r$ for $j \neq r$ and $\Phi_y^+ = \{\phi_1, \dots, \phi_k\}$: If $\phi_j < 0$ for some j then by (**) applied to $w = s_{j-1} \dots s_1$ and $t = s_j$ gives $s_j \dots s_1 = s_{j-1} \dots \hat{s}_i \dots s_1$ which then contradicts the fact that $y = s_1 \dots s_k$ is a reduced expression. The remaining claims can be proved in a similar manner.

(3) $\Rightarrow$ (4). For $w \in W$, define the subset Br (w) as follows:

$$\text{Br}\,(w) = \{x \in W \mid \exists m \geqslant 0 \quad \text{and} \quad t_1, \dots, t_m \in T$$

such that

$$\text{(a)}\quad x = t_m \dots t_1 w \quad \text{and (b)} \quad l(t_i \dots t_1 w) \leqslant l(t_{i-1} \dots t_1 w)\ \forall 1 \leqslant i \leqslant m\}$$

(Note that $w \in$ Br (w) vacuously).

Proof of (i). Let $w = s_1 \dots s_k$ be a reduced expression. Let $x \in$ Br (w). Then $\exists\, t_1, \dots, t_m \in T$ such that conditions (a) and (b) (given above) are satisfied. A repeated application of (3) and (b) implies that

$$x = s_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_m} \dots s_k\,.$$

(Note that eventhough $w = s_1 \dots s_k$ is a reduced expression, $t_1 w = s_1 \dots \hat{s}_{i_p} \dots s_k$ need not be. In order to continue, we need the full strength of (3) and not just the exchange condition (6)).

Conversely, let $z = s_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_m} \dots s_k$ for some $m \geqslant 0$ and $1 \leqslant i_1 < i_2 < \dots < i_m \leqslant k$. We prove by induction on $(k+1)m - (i_1 + \dots + i_m)$ $(\geqslant 0)$ that $z \in \mathrm{Br}\,(w)$.

If the above number is zero then $m = 0$ and $z = w \in \mathrm{Br}\,(w)$. In other cases, $m > 0$. Let $t = s_1 \dots s_{i_1} \dots s_1$. Then $z' = tz = s_1 \dots \hat{s}_{i_2} \dots \hat{s}_{i_m} \dots s_k$.

Case (α). $l(tz) \geqslant l(z)$.

In this case, the induction hypothesis holds for $z' = tz$ and so $z' \in \mathrm{Br}\,(w)$. Since $l(tz) \geqslant l(z)$, it is clear that $z \in \mathrm{Br}\,(w)$ as well.

Case (β). $l(tz) < l(z)$.

We use (3) for the expression

$$z = s_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_m} \dots s_k \quad \text{and} \quad t \cdot \exists j (j \neq i_r \forall 1 \leqslant r \leqslant m)$$

such that tz has an expression obtained by deleting s_j from the above expression of z. We claim that $j > i_1$. If not, $tz = s_1 \dots \hat{s}_j \dots \hat{s}_{i_1} \dots \hat{s}_{i_m} \dots s_k$. It then follows that $t = s_1 \dots s_{i_1} \dots s_1 = s_1 \dots s_j \dots s_1$. This gives a contradiction to the fact that $w = s_1 \dots s_k$ is a reduced expression. Hence $j > i_1$. Let $i_r < j < i_{r+1} (r \geqslant 1)$. Then we have, $tz = s_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_r} \dots \hat{s}_j \dots \hat{s}_{i_{r+1}} \dots \hat{s}_{i_m} \dots s_k$. Hence, $z = t \cdot tz = s_1 \dots \hat{s}_{i_2} \dots \hat{s}_{i_r} \dots \hat{s}_j \dots \hat{s}_{i_{r+1}} \dots \hat{s}_{i_m} \dots s_k$. Now the "number" associated with this expression is $(k+1)m - (i_2 + \dots + i_r + j + i_{r+1} + \dots + i_m)$. Since $i_1 < j$, it is clear that this number is smaller than $(k+1)m - (i_1 + \dots + i_m)$. Hence the induction hypothesis applies and so $z \in \mathrm{Br}\,(w)$. This proves (i).

To prove (ii), we need to observe that for $t \in T$, $w \in W$, either $l(tw) < l(w)$ on $l(tw) > l(w)$. For: if $l(tw) = l(w)$ then $l(tw) \leqslant l(w)$ and so by (3) starting with a reduced expression $w = s_1 \dots s_k$, we get $tw = s_1 \dots \hat{s}_i \dots s_k$ i.e. $l(tw) \leqslant k - 1$, a contradiction. Now by definition of Br ( ), it is clear that either $tw \in \mathrm{Br}\,(w)$ or $w \in \mathrm{Br}\,(tw)$ *but* not *both*. The dichotomy in (ii) is now clear.

This proves (4).

(4) $\Rightarrow$ (5). We first observe the following two consequences of (4):

(α) If $x \in \mathrm{Br}\,(w)$ then $l(x) \leqslant l(w)$ with equality holding precisely when $x = w$.

(β) For $w \in W$, $s \in S$ $l(w) < l(sw)$ iff $w \in \mathrm{Br}\,(sw)$.

Define $P_s = \{w \in W \mid w \in \mathrm{Br}\,(sw)\}$ $(s \in S)$. It is clear that $\mathrm{id} \in P_s$ and $P_s \cap sP_s = \emptyset$. Next, let $w \in W$, $s' \in S$ be such that $w \in P_s$ and $ws' \notin P_s$. Hence $l(w) < l(sw)$ and $l(sws') < l(ws')$.

(Note that $ws' \notin P_s \Rightarrow ws' \notin \mathrm{Br}\,(sws') \Rightarrow sws' \in \mathrm{Br}\,(ws') \Rightarrow l(sws') < l(ws')$). Now $l(ws') = l(sws') + 1 \geqslant (l(sw) - 1) + 1 = l(sw) > l(w)$. Start with a reduced expression $w = s_1 \dots s_k$ then $ws' = s_1 \dots s_k s'$ is a reduced expression. Since $l(sws') < l(ws')$, $sws' \in \mathrm{Br}(ws')$ and so sws' is a subexpression of $s_1 \dots s_k \cdot s'$ (property (a) of (4)). However, $l(sws') = l(ws') - 1$ and so either $sws' = s_1 \dots s_k$ or $sws' = s_1 \dots \hat{s}_j \dots s_k \cdot s'$. However, the second case is not possible since it means $sw = s_1 \dots \hat{s}_j \dots s_k$ which is not true since $l(sw) > l(w) = k$. Hence $sws' = s_1 \dots s_k = w$. Thus $ws'w^{-1} = s$. This proves (5).

(5) $\Rightarrow$ (6). Let $z \in W$. We prove that $l(z) \leqslant l(sz) \Rightarrow z \in P_s$. Let $z = s_1 \dots s_k$ be a reduced expression. If possible, let $z \notin P_s$. Since $\mathrm{id} \in P_s$ and $s_1 \dots s_k \notin P_s$, $\exists\, j$ such that $s_1 \dots s_{j-1} \in P_s$ but $s_1 \dots s_j \notin P_s$. So by (iii) of condition (5), $s_1 \dots s_{j-1} s_j s_{j-1} \dots s_1 = s$. Hence $sz = s_1 \dots \hat{s}_j \dots s_k$ which is a contradiction since $l(sz) \geqslant l(z) = k$. This proves that $z \in P_s$. Next, we claim that $z \in P_s \Rightarrow l(z) < l(sz)$. If not, then $l(sz) \leqslant l(z)$ and so by the earlier argument, $sz \in P_s$. This means $z \in P_s \cap sP_s$ which is a contradiction. Thus, $z \in P_s$ iff $l(z) < l(sz)$ iff $l(z) \leqslant l(sz)$.

Now consider a reduced expression $w = s_1 \dots s_k$ and $s \in S$ such that $l(sw) \leqslant l(w)$. From above, $w \notin P_s$. It is now clear that $\exists\, j$ such that $s_1 \dots s_{j-1} \in P_s$ but $s_1 \dots s_j \notin P_s$. So by (iii), $sw = s_1 \dots \hat{s}_j \dots s_k$.

(6) $\Rightarrow$ (1). Consider the canonical map $\eta : \tilde{W} \to W$. For $s \in S$, let $\tilde{s}$ be the "canonical" preimage of s. For $s_1 \neq s_2 \in S$, let m_{s_1, s_2} denote the order of $s_1 s_2$ if it is finite. Let $\tilde{N}$ denote the normal subgroup of $\tilde{W}$ generated by $\{(\tilde{s}_1 \cdot \tilde{s}_2)^{m_{s_1, s_2}} \mid m_{s_1, s_2} < \infty\}$. It is then clear that $\tilde{N} \subseteq \mathrm{Ker}\, \eta$. We claim that $\tilde{N} = \mathrm{Ker}\, \eta$ which proves (I).

If the claim is not true, choose $\tilde{z} = \tilde{s}_1 \dots \tilde{s}_k \in \mathrm{Ker}\, \eta$ such that $\tilde{z} \notin \tilde{N}$ and $\tilde{l}(\tilde{z}) = k$ is minimal with respect to this property ($\tilde{l}$ is the length function in $\tilde{W}$). Now $\mathrm{id} = \eta(\tilde{z}) = s_1 \dots s_k$. Since $l(s_k) = 1$ and $l(s_1 \dots s_k) = 0$, it is clear that $\exists\, i \leqslant k - 1$ such that $l(s_i \dots s_k) < l(s_{i+1} \dots s_k)$. In fact, i can be so chosen that $i \geqslant \dfrac{k}{2}$ (or else there is no hope of acheiving $l(s_1 \dots s_k) = 0$.

Thus by exchange condition, $\exists i + 1 \leqslant j \leqslant k$ such that $s_i \dots s_k = s_{i+1} \dots \hat{s}_j \dots s_k$. i.e. $s_i \dots s_j = s_{i+1} \dots s_{j-1}$. Now $\tilde{s}_i \dots \tilde{s}_j \tilde{s}_{j-1} \dots \tilde{s}_{i+1} \in \mathrm{Ker}\, \eta$ and

$$\tilde{l}(\tilde{s}_i \dots \tilde{s}_j \tilde{s}_{j-1} \dots \tilde{s}_{i+1}) \leqslant j - i + 1 + j - 1 - i = 2j - 2i \leqslant 2k - k = k$$

$\left(\text{since } j \leqslant k \text{ and } i \geqslant \dfrac{k}{2}\right)$. If the length is strictly smaller than k, then $\tilde{n} = \tilde{s}_i \dots \tilde{s}_j \cdot \tilde{s}_{j-1} \dots \tilde{s}_{i+1} \in \tilde{N}$ by minimality of k and in that case

$$\tilde{z} = \tilde{s}_1 \dots \tilde{s}_k = \tilde{s}_1 \dots \tilde{s}_{i-1} \cdot \tilde{n} \tilde{s}_{i+1} \dots \tilde{s}_{j-1} \cdot \tilde{s}_{j+1} \dots \tilde{s}_k .$$

So $\tilde{z} \in \tilde{N}$ as well since $\tilde{s}_1 \dots \hat{\tilde{s}}_i \dots \hat{\tilde{s}}_j \dots \tilde{s}_k \in \operatorname{Ker} \eta$, of length $\leqslant k-2$ and $so \in \tilde{N}$. This gives a contradiction. Hence $\tilde{l}(\tilde{s}_i \dots \tilde{s}_j \cdot \tilde{s}_{j-1} \dots \tilde{s}_{i+1}) = k$ and $j = k = 2i$. Also, $s_1 \dots s_k = \mathrm{id} = s_1 \dots \hat{s}_i \dots \hat{s}_k$ and so $\tilde{s}_1 \dots \hat{\tilde{s}}_i \dots \hat{\tilde{s}}_k \in \tilde{N}$. Thus,

$$\tilde{z} \in \tilde{s}_1 \dots \tilde{s}_{i-1}\tilde{s}_i \dots \tilde{s}_1 \cdot \tilde{s}_k \cdot \tilde{N} .$$

Let $\tilde{z}_1 = \tilde{s}_k \cdot \tilde{s}_1 \dots \tilde{s}_{i-1} \cdot \tilde{s}_i \cdot \tilde{s}_{i-1} \dots \tilde{s}_1$ then $\tilde{z}_1 \in \tilde{z} \cdot \tilde{N}$ (Note that $\tilde{N}$ is normal).

Now argue with $\tilde{z}_1$ instead of $\tilde{z}$ (Note that $\tilde{l}(\tilde{z}_1) = k$ again!) Thus we get $\tilde{z}_2 = \tilde{s}_1\tilde{s}_k\tilde{s}_1 \dots \tilde{s}_{i-2}\tilde{s}_{i-1} \dots \tilde{s}_1 \cdot \tilde{s}_k \in \tilde{z}_1\tilde{N} = \tilde{z}\tilde{N}$ and so on. Finally, we get an element $\tilde{z}_r$ (for a suitable r) which is of the form $\tilde{s}_1\tilde{s}_k \dots \tilde{s}_1 \cdot \tilde{s}_k$ (total number of terms $= 2i$) and such that $\tilde{z}_r \in \tilde{z} \cdot \tilde{N}$. Since $\tilde{z}_r \in \operatorname{Ker} \eta$, it is clear that $m_{s_1, s_k} < \infty$ and it divides i and so $\tilde{z}_r \in \tilde{N}$ by definition. Thus $\tilde{z} \in \tilde{N}$ which is a contradiction. This finally proves that $\tilde{N} = \operatorname{Ker} \eta$ and so (1) holds.

This completes the proof of the main theorem.

REFERENCES

The references given here form a very small subset of a large literature available on Coxeter groups and related topics. Some of the references given are standard and some are included because of their need in the proof of main theorem.

[B] Bourbaki, N. *Groupes et algèbres de Lie, ch. 4, 5 et 6.* Hermann, Paris (1968).

[D] Deodhar, V. On the root system of a Coxeter group. *Commu. in alg. 10 (6)*, 611-630 (1982).

[K-L] Kazhdan, D. and G. Lusztig. Representations of Coxeter groups and Hecke algebras. *Inventiones Math. 53* (1979), 165-184.

[S] Steinberg, R. *Lectures on Chevalley groups.* Mimeo. notes, Yale University (1967).

(Reçu le 6 février 1985)

Vinay V. Deodhar

Indiana University
Bloomington
IN 47405, USA