1)

Coxeter groups.

Let S be a finite set and let $(m_{ss'})_{(s,s')\in S\times S}$ be a matrix with entries in $\mathbb{N}\cup\infty$ such that $m_{ss}=1$ $\forall s$ and $m_{ss'}=m_{s's}\geq 2$ for $s\neq s'$. (A Coxeter matrix). Let W be the group defined by the generators s $(s\in S)$ and relations $(ss')^{m_{ss'}}=1$ for any s s' in S such that $m_{ss'}<\infty$. We say that W,S is a Coxeter group. In W we have $s^2=1$ for $s\in S$. There is a unique homomorphism $sgn: W\to\{\pm1\}$ such that $sgn(s)=-1$ for $s\in S$.

For $w\in W$ let $|w|$ be the smallest integer $q\geq 0$ such that $w=s_1\cdots s_q$ with $s_1,\dots,s_q$ in S. We then say that $w=s_1\cdots s_q$ is a reduced expression and $|w|$ is the length of w. Now $|1|=0$, $|s|=1$. (We have $s\neq 1$ since $sgn(s)=-1$.)

Let $w\in W$, $s\in S$. We have either $|sw|=|w|+1$ or $|sw|=|w|-1$. (Use $|sw|\neq|w|$ since $sgn\, sw\neq sgn\, w$ and $|w|-1\leq|sw|\leq|w|+1$). We have either $|ws|=|w|+1$ or $|ws|=|w|-1$.

1A)

The exchange condition in a Coxeter group: Let $w \in W$, $s \in S$ be such that $|sw| = |w| - 1$. Let $w = s_1 \dots s_q$ be a reduced expr. Then there exists $j \in \{1, \dots, q\}$ such that $s s_1 \dots s_{j-1} = s_1 s_2 \dots s_j$.
(See Bourbaki, Ch. IV).

__Lemma__ Let $w \in W$, let s, t in S be such that $|swt| = |w|$, $|sw| = |wt|$. Then $sw = wt$.

__Proof.__ Let $w = s_1 \dots s_q$ be a reduced expr. Assume first that $|wt| = q+1$. Then $s_1 \dots s_q t$ is a red. exp. for wt. Now $|swt| = |wt| - 1$ hence by the exch. cond. there exists $i \in \{1, \dots q\}$ with $s s_1 s_2 \dots s_{i-1} = s_1 s_2 \dots s_i$ or else $s s_1 \dots s_q = s_1 \dots s_q t$. In the last case we are done. In the first case, $sw = s_1 \dots s_{i-1} s_{i+1} \dots s_q$ hence $|sw| \leq q-1$, contradicting $|sw| = |wt|$. Next assume $|wt| = q-1$. Let $w' = wt$. Then $|sw't| = |w'|$, $|sw'| = |w't|$. We have $|w't| = |w'| + 1$ hence the first part of the proof applies and $sw' = w't$ so that $sw = wt$. Δ

2) The reflection representation. Let E be $\mathbb{R}$-vector space with basis $\{e_s;\ s\in S\}$. For $s\in S$ define a linear map $\sigma_s : E\to E$ by

$$\sigma_s(e_{s'}) = e_{s'} + 2\cos\left(\frac{\pi}{m_{s,s'}}\right) e_s \qquad \forall\, s'\in S.$$

There is a unique homomorphism $\sigma : W\to GL(E)$ such that $\sigma(s)=\sigma_s$ for any $s\in S$.

(Easy to prove.)

Theorem (Tits). σ is injective.

Examples of Coxeter groups.

1) W = group of permutations of $\{1,2,\dots,n\}$
$S=\{\sigma_i \mid i=1,\dots,n-1\}$, σ_i = transposition $(i,i+1)$.
We have $\sigma_i^2=1$, $(\sigma_i\sigma_j)^3=1$ if $|i-j|=1$, $(\sigma_i\sigma_j)^2=1$ if $|i-j|\geq 2$. Let W' be the Coxeter group with generators S and relations above. One can check that the image of W' in $GL(E)$ (refl. rep.) is W. Using Tits theorem, we deduce $W'\cong W$.

2) For $k\in\mathbb{Z}$ define $\gamma_k : \mathbb{Z}\to\mathbb{Z}$ by $z\to z+k$.
Let $n\geq 2$. Let $\widetilde{W}$ be the group of all permutations $\sigma:\mathbb{Z}\to\mathbb{Z}$ such that $\sigma\rho_n=\rho_n\sigma$.

3) Define $\chi : \tilde{W} \to \mathbb{Z}$ by $\chi(\sigma) = \sum_{k \in X} (\sigma(k) - k)$ where X is a set of representatives for the residue classes mod n in $\mathbb{Z}$. Note that $\chi(\sigma)$ does not depend on the choice of X and is a group homomorphism with image $n\mathbb{Z}$. Let $\tilde{W}' = \ker \chi$. Then $\tilde{W}'$ is generated by $\{s_m ; m \in \mathbb{Z}/n\mathbb{Z}\}$ where $s_m : \mathbb{Z} \to \mathbb{Z}$ is defined by

$$s_m(z) = \begin{cases} z+1 & \text{if } z = m \bmod n \\ z-1 & \text{if } z = m+1 \bmod n \\ z & \text{otherwise} \end{cases}$$

We have $s_m^2 = 1$, $(s_m s_{m'})^3 = 1$ if $\begin{cases} m - m' \equiv \pm 1 \ (n) \\ n \geq 3 \end{cases}$

$(s_m s_{m'})^2 = 1$ if $\begin{cases} m - m' \not\equiv \pm 1 \ (n) \\ n \geq 3 \end{cases}$

$\tilde{W}'$ is a Coxeter group defined by $\{s_m\}$ and these relations. (Same proof as for symmetric group, using reflection representation and Tits theorem.)

We call $\tilde{W}'$ the <u>affine symmetric group</u>

Let (W, S) be a Coxeter group

Let X be the set of all sequences $(s_1, \dots, s_q)$ in S such that $|s_1 \cdots s_q| = q$.

We regard X as the vertices of a graph in which

4) $(s_1, \dots s_q)$, $(s'_1, \dots s'_{q'})$ are joined if one is obtained from the other by replacing m consecutive entries of form $s, s', s, s', \dots$ by the m entries $s', s, s', s, \dots$ where $s \neq s'$ in S are such that $m = m_{s,s'} < \infty$. (Then $q = q'$ and $s_1 \dots s_q = s'_1 \dots s'_q$)

<u>Theorem</u> (Matsumoto, Tits) Let $(s_1, \dots s_q) \in X$, $(s'_1 \dots s'_q) \in X$. Assume $s_1 s_2 \dots s_q = s'_1 \dots s'_q$. Then $(s_1, \dots s_q)$, $(s'_1, \dots, s'_q)$ are in the same connected component of the graph above.

<u>Proof</u> see: Bourbaki, Ch IV

Let $A = \mathbb{Z}[v, v^{-1}]$, v an indeterminate.

Let $\mathcal{H}$ be the A-algebra defined by the generators $\{T_s, s \in S\}$ and the relations

$(T_s - v)(T_s + v^{-1}) = 0$ for $s \in S$

$T_s T_{s'} T_s \dots = T_{s'} T_s T_{s'} \dots$

(both products with $m_{s,s'}$ factors) for any $s \neq s'$ in S such that $m_{s,s'} < \infty$

$\mathcal{H}$ is called the <u>Iwahori-Hecke</u> algebra

5)

For $w \in W$ we define $T_w \in \mathcal{H}$ by $T_w = T_{s_1} T_{s_2} \cdots T_{s_q}$ where $w = s_1 \cdots s_q$ is a reduced expression. This is independent of the choice of reduced expression, by Matsumoto-Tits. We have for $s \in S$, $w \in W$:

$$T_s T_w = \begin{cases} T_{sw} & \text{if } |sw| = |w|+1 \\ T_{sw} + (v - v^{-1}) T_w & \text{if } |sw| = |w| - 1. \end{cases}$$

In particular the A-submodule of $\mathcal{H}$ generated by $\{T_w;\, w \in W\}$ is a left ideal. It contains $1 = T_1$ hence it is $= \mathcal{H}$. Thus $\{T_w;\, w \in W\}$ generate $\mathcal{H}$ as A-module.

<u>Proposition</u>. $\{T_w;\, w \in W\}$ is an A-basis of $\mathcal{H}$

Proof. Let $\mathcal{E}$ be the free A-module with basis $\{e_w;\, w \in W\}$. For $s \in S$ we define A-linear maps $P_s, Q_s : \mathcal{E} \to \mathcal{E}$ by

$$P_s(e_w) = \begin{cases} e_{sw} & \text{if } |sw| = |w|+1 \\ e_{sw} + (v - v^{-1}) e_w & \text{if } |sw| = |w| - 1 \end{cases}$$

$$Q_s(e_w) = \begin{cases} e_{ws} & \text{if } |ws| = |w|+1 \\ e_{ws} + (v - v^{-1}) e_w & \text{if } |ws| = |w| - 1. \end{cases}$$

6) We shall continue the proof assuming that

(*) $P_s Q_t = Q_t P_s$ for s,t in S.

Let $\mathcal{U}$ be the A-subalgebra with 1 of $\mathrm{End}(\mathcal{E})$ generated by $\{P_s, s\in S\}$. The map $\mathcal{U} \to \mathcal{E}$ given by $\pi \to \pi(e_1)$ is surjective. Indeed if $w = s_1 \cdots s_q$ is a reduced expression in W then $e_w = P_{s_1} \cdots P_{s_q} e_1$. Assume now that $\pi \in \mathcal{U}$ satisfies $\pi(e_1) = 0$. Let $\pi' = Q_{s_q} \cdots Q_{s_1}$. By (*) we have $\pi\pi' = \pi'\pi$ hence $0 = \pi'\pi(e_1) = \pi\pi'(e_1) = \pi(Q_{s_q} \cdots Q_{s_1}(e_1))$ $= \pi(e_w)$. Since w is arbitrary, it follows that $\pi = 0$. Thus, $\mathcal{U} \to \mathcal{E}$ is injective, hence an isomorphism of A-modules. Using this isomorphism, we transport the algebra structure of $\mathcal{U}$ to an algebra structure on $\mathcal{E}$ with unit element e_1. For this algebra structure we have

$P_s(e_1)\pi(e_1) = P_s(\pi(e_1))$ for $s \in S$, $\pi \in \mathcal{U}$.

Hence $e_s e_w = P_s(e_w)$ for $s \in S$, $w \in W$.

7) It follows that

$$e_s e_w = \begin{cases} e_{sw} & \text{if } |sw| = |w| + 1 \\ e_{sw} + (v - v^{-1}) e_w & \text{if } |sw| = |w| - 1 \end{cases}$$

In particular, if $w = s_1 \cdots s_q$ is a red.-expr. then $e_w = e_{s_1} \cdots e_{s_q}$. Thus if $s \neq s'$ in S are such that $m = m_{s,s'} < \infty$ then $e_s e_{s'} e_s \cdots = e_{s'} e_s e_{s'} \cdots$ (both products have m factors), i.e. $e_{ss's\cdots} = e_{s's\cdots}$ (we use that $ss's' \cdots$, $s'ss' \cdots$ with m factors are reduced expressions, see (**) below.) We have $e_s^2 = 1 + (v - v^{-1}) e_s$ for $s \in S$. Thus there is a unique algebra homomorphism $\mathcal{H} \to \mathcal{E}$ preserving 1 such that $T_s \mapsto e_s$, $\forall s \in S$. It takes T_w to e_w for any $w \in W$. It follows that $\{T_w\}$ is an $\mathcal{A}$-basis.

We now prove (*). Let $w \in W$. We have six cases

1) swt, sw, wt, w have length $q+2, q+1, q+1, q$. Then $P_s Q_t (e_w) = Q_t P_s (e_w) = e_{swt}$.

2) w, sw, wt, swt have length $q+2, q+1, q+1, q$.

8) Then

$$P_s Q_t e_w = Q_t P_s e_w = e_{swt} + (v-v^{-1}) e_{sw} +$$
$$+ (v-v^{-1}) e_{wt} + (v-1)^2 e_w.$$

3) wt, swt, w, sw have length $q+2, q+1, q+1, q$

Then

$$P_s Q_t e_w = Q_t P_s e_w = e_{swt} + (v-v^{-1}) e_{wt}$$

4) sw, swt, w, wt have lengths $q+2, q+1, q+1, q$

Then

$$P_s Q_t e_w = Q_t P_s e_w = e_{swt} + (v-v^{-1}) e_{sw}$$

5) swt, w, wt, sw have length $q+1, q+1, q, q$.

Then

$$P_s Q_t (e_w) = e_{swt} + (v-v^{-1}) e_{sw} + (v-v^{-1})^2 e_w$$
$$Q_t P_s (e_w) = e_{swt} + (v-v^{-1}) e_{wt} + (v-v^{-1})^2 e_w$$

6) sw, wt, w, swt have length $q+1, q+1, q, q$.

Then

$$P_s Q_t (e_w) = e_{swt} + (v-v^{-1}) e_{wt}$$
$$Q_t P_s (e_w) = e_{swt} + (v-v^{-1}) e_{sw}.$$

In cases 5), 6) we have $sw = wt$, by an earlier lemma. $\square$

9)

Let $s \neq s'$ in S be such that $m = m_{ss'} < \infty$. Then ss' has order m. (This follows by showing that the image of ss' in the reflection repres. has order m.) We show

(**) $ss's\ldots$ (m factors) is a reduced expression.

Let $s_k = ss's\ldots$ (k factors) $s'_k = s'ss'\ldots$ (k factors)

Since ss' has order m, the elements $s_0, s_1, \ldots, s_m, s'_0, \ldots, s'_m$ are distinct except for $s_0 = s'_0$, $s_m = s'_m$. Assume that $s_k = ss's\ldots$ is a red. exp but $s'_{k+1} = s's\ldots$ is not (for some $k < m$). By the exchange condition we have $s'_{k+1} = \underbrace{ss'\ldots\downarrow\downarrow\ldots}_{k-1}$ with two factors omitted.

But the s'_{k+1} is equal to some s_ℓ or s'_ℓ with $\ell \leq k-1$. This is absurd. We see that s_k red. exp. $\Rightarrow s'_{k+1}$ red. exp. (for $k < m$). Similarly, s'_k red exp. $\Rightarrow s_{k+1}$ red. exp. (for $k < m$).

From this we see by induction that each s_k, s'_k is a red exp. for $k \leq m$.

This proves (**).

10)

Let $\bar{\ }: \mathcal{A} \to \mathcal{A}$ be the ring involution such that $\overline{v^n} = v^{-n}$ for $n \in \mathbb{Z}$.

For $s \in S$, $T_s \in \mathcal{H}$ is invertible: $T_s^{-1} = T_s - (v - v^{-1})$. It follows that for any $w \in W$, $T_w \in \mathcal{H}$ is invertible: if $w = s_1 \cdots s_q$ is a reduced exp. then $T_w^{-1} = T_{s_q}^{-1} \cdots T_{s_1}^{-1}$.

<u>Lemma</u>. There is a unique ring homomorphism $\bar{\ }: \mathcal{H} \to \mathcal{H}$ such that $\overline{aT_s} = \bar{a} T_s^{-1}$ for any $a \in \mathcal{A}$, $s \in S$. This is an involution. It takes T_w to $T_{w^{-1}}^{-1}$ for any $w \in W$.

<u>Proof</u>. We have
$(T_s^{-1} - v^{-1})(T_s^{-1} + v) = 0$ for $s \in S$
$T_s^{-1} T_t^{-1} T_s^{-1} \cdots = T_t^{-1} T_s^{-1} T_t^{-1} \cdots$ (both products have m factors) for any $s \neq t$ in S such that $m = m_{s,t} < \infty$. This implies the first sentence. Let $s \in S$. Applying $\bar{\ }$ to $T_s \widehat{T_s} = 1$ we obtain $\overline{T_s}\, \overline{\overline{T_s}} = 1$. We have also $\widehat{T_s}\, T_s = 1$ hence $\overline{\overline{T_s}} = T_s$. Hence the square of $\bar{\ }$ is 1. If $w = s_1 \cdots s_q$ is a red exp. then $\overline{T_w} = \overline{T_{s_1}} \cdots \overline{T_{s_q}} = T_{s_1}^{-1} \cdots T_{s_q}^{-1} = (T_{s_q} \cdots T_{s_1})^{-1} = T_{w^{-1}}^{-1}$. $\square$

11) For any $w \in W$ we write uniquely
$\overline{T_w} = \sum_y \overline{r_{yw}} T_y$, finite sum; $r_{yw} \in A$.

<u>Lemma</u> For any x, z in W we have
$\sum_y \overline{r_{xy}} r_{yz} = \delta_{xz}$

<u>Proof</u> $T_z = \overline{\overline{T_z}} = \overline{\sum_y \overline{r_{yz}} T_y} = \sum_y r_{yz} \overline{T_y}$
$= \sum_{y,x} r_{yz} \overline{r_{xy}} T_x$. $\square$

We define a partial order $\leq$ on W by
$y \leq w$ if either $y = w$ or $|y| < |w|$.

<u>Lemma</u> (a) If $r_{yw} \neq 0$ then $y \leq w$.
(b) $r_{w,w} = 1$.

<u>Proof</u> We prove (a) by induction on $|w|$.
If $|w| = 0$ then $\overline{T_w} = \overline{T_1} = T_1$ and the result is clear. Now assume that $|w| \geq 1$.
We can write $w = w' w''$ where
$|w| = |w'| + |w''|$, $|w'| < |w|$, $|w''| < |w|$.

12) We have

$$\overline{T_w} = \overline{T_{w'}}\,\overline{T_{w''}} = \sum_{y' \le w'} \overline{r_{y'w'}}\, T_{y'} \sum_{y'' \le w''} \overline{r_{y''w''}}\, T_{y''}.$$

We have

$$T_{y'} T_{y''} = \text{lin comb. of } T_y \,, \ |y| \le |y'| + |y''|.$$

If $y' \ne w'$, or $y'' \ne w''$ then $|y'| < |w'|$ or $|y''| < |w''|$ and $|y| < |w'| + |w''| = |w|$.

If $y' = w'$ and $y'' = w''$ then $T_{y'} T_{y''} = T_w$

Thus $\overline{T_w}$ is a lin. comb. of T_w and of T_y with $|y| < |w|$. This proves (a).

The same argument shows that $\overline{r_{w,w}} = \overline{r_{w'w'}}\, r_{w''w''}$ which by induction is 1. This proves (b).

13) Let $\mathcal{A}_{\leq 0} = \mathbb{Z}[v^{-1}] \subset \mathcal{A}$, $\mathcal{A}_{<0} = v^{-1}\mathbb{Z}[v^{-1}]$.

Let $\mathcal{H}_{\leq 0} = \bigoplus_w \mathcal{A}_{\leq 0} T_w$, $\mathcal{H}_{<0} = \bigoplus_w \mathcal{A}_{<0} T_w$.

<u>Theorem</u> (a) Let $w \in W$. There is a unique element $c_w \in \mathcal{H}_{\leq 0}$ such that $\overline{c_w} = c_w$ and $c_w = T_w \mod \mathcal{H}_{<0}$.

(b) $\{c_w \mid w \in W\}$ is an $\mathcal{A}_{\leq 0}$-basis of $\mathcal{H}_{\leq 0}$ and an $\mathcal{A}$-basis of $\mathcal{H}$.

We construct for any x such that $x \leq w$ an element $u_x \in \mathcal{A}_{\leq 0}$ such that

(c) $u_w = 1$

(d) $u_x \in \mathcal{A}_{<0}$, $\overline{u_x} - u_x = \sum_{\substack{y \\ x<y\leq w}} r_{x,y} u_y$ for $x < w$

We argue by induction on $|w|-|x|$. If $|w|-|x| = 0$ then $x = w$ and we set $u_w = 1$. Assume now that $|w|-|x| > 0$. Then the right hand side of the equality in (d) is defined. We denote by $a_x \in \mathcal{A}$. We have

$$a_x + \overline{a_x} = \sum_{\substack{y \\ x<y\leq w}} r_{xy} u_y + \sum_{\substack{y \\ x<y\leq w}} \overline{r_{xy}}\, \overline{u_y}$$

14)

$$= \sum_{\substack{y \\ x<y\leq w}} r_{xy} u_y + \sum_{\substack{y \\ x<y\leq w}} \bar{r}_{xy}\Big(u_y + \sum_{\substack{z \\ y<z\leq w}} r_{yz} u_z\Big)$$

$$= \sum_{\substack{z \\ x<z\leq w}} r_{xz} u_z + \sum_{\substack{z \\ x<z\leq w}} \bar{r}_{xz} u_z + \sum_{\substack{z;\ x<z\leq w \\ y;\ x<y<z}} \bar{r}_{xy} r_{yz} u_z$$

$$= \sum_{\substack{z;\ x<z\leq w \\ y;\ x\leq y\leq z}} \bar{r}_{xy} r_{yz} u_z \qquad (\text{using } r_{yy}=1)$$

$$= \sum_{z;\ x<z\leq w} \delta_{xz} u_z = 0 . \qquad (\text{using an earlier lemma})$$

Since $a_x + \bar{a}_x = 0$ we have $a_x = \sum_{n\in\mathbb{Z}} \gamma_n v^n$ (finite sum) where $\gamma_n \in \mathbb{Z}$ satisfy $\gamma_n + \gamma_{-n} = 0$ and in particular $\gamma_0 = 0$. We set $u_x = \sum_{n<0} \gamma_n v^n \in \mathcal{A}_{<0}$ so that $\bar{u}_x - u_x = a_x$. This completes the inductive definition of u_x.

We set $c_w = \sum_{\substack{y \\ y\leq w}} u_y T_y \in \mathcal{H}_{\leq 0}$. Clearly $c_w = T_w \bmod \mathcal{H}_{<0}$. We have

$$\bar{c}_w = \sum_{\substack{y \\ y\leq w}} \bar{u}_y \bar{T}_y = \sum_{\substack{y \\ y\leq w}} \bar{u}_y \sum_{\substack{x \\ x\leq y}} \bar{r}_{xy} T_x = \sum_{\substack{x \\ x\leq w}} \Big(\sum_{\substack{y \\ x\leq y\leq w}} \bar{r}_{xy} \bar{u}_y\Big) T_x$$

$$= \sum_{\substack{x \\ x\leq w}} u_x T_x = c_w .$$ The existence of c_w is proved.

15) To prove uniqueness it is enough to verify:

(e) If $h \in \mathcal{H}_{<0}$ satisfies $\bar{h} = h$, then $h = 0$.

We can write uniquely $h = \sum_y f_y T_y$, $f_y \in \mathcal{A}_{<0}$.
Assume that not all f_y are 0. We can find $l_0 \in \mathbb{N}$ such that

$$Y_0 = \{ y \in W ; f_y \neq 0, |y| = l_0 \} \neq \phi$$
$$\{ y \in W ; f_y \neq 0, |y| > l_0 \} = \phi$$

Now $\sum_y f_y T_y = \sum_y \bar{f}_y \bar{T}_y$ implies

$$\sum_{y \in Y_0} f_y T_y = \sum_{y \in Y_0} \bar{f}_y T_y \mod \sum_{\substack{y \\ |y| < l_0}} \mathcal{A} T_y$$

hence $\bar{f}_y = f_y$ for $y \in Y_0$. Since $f_y \in \mathcal{A}_{<0}$ it follows that $f_y = 0$ for $y \in Y_0$, contradiction.. Thus (e) holds.

Thus part (a) of the Theorem holds.
Now the elements c_w are related to T_w by a triangular matrix with 1 on diagonal.
Hence the c_w form an $\mathcal{A}$-basis. $\square$.

For any $w \in W$ we set $c_w = \sum_{y \leq w} p_{y,w} T_y$ where $p_{y,w} \in \mathcal{A}_{\leq 0}$. We have
$p_{y,y} = 1$, $p_{y,w} \in \mathcal{A}_{<0}$ if $y < w$.

16)

one can show that for $y \leq w$:

$$P_{y,w} = v^{|w|-|y|} p_{y,w} \in \mathbb{Z}[v^2].$$