Hecke Algebras

Daniel Bump

August 22, 2018

By a *Hecke Algebra* we will usually mean an *Iwahori Hecke algebra*. We will now explain what these are. A *Coxeter group* consist of data (W, I) where W is a group and $I = \{s_1, \cdots, s_r\}$ of elements of order 2 which generate W, subject to a certain condition, which we will now explain. If $1 \leqslant i, j \leqslant r$ and $i \neq j$ let $m(i, j)$ be the order of $s_i s_j$. Since s_i and s_j have order 2, we have

$$s_i s_j s_i s_j \cdots = s_j s_i s_j s_i \cdots \tag{1}$$

where there are $m(i, j)$ factors on both sides. For example, if $m(i, j) = 2$, this means $s_i s_j = s_j s_i$, so that s_i and s_j commute. If $m(s, s') = 3$, then

$$s_i s_j s_i = s_j s_i s_j$$

which is *Artin's braid relation*. In general we will refer to (1) as the *braid relation* satisfied by s_i and s_j. In order for W to be a *Coxeter group* it is required that the given set of relations between elements of I give a presentation of W.

Informally, this means that any relation between generators in I can be deduced from the fact that the $s \in \Sigma$ have order 2 and the braid relations. Formally, it means the following. More formally, it means that W is isomorphic to the free group on r generators $\sigma_1, \cdots, \sigma_r$ modulo the smallest normal subgroup containing σ_i^2 and $(\sigma_i \sigma_j)^{m(i,j)}$.

For example, the symmetric group S_{r+1} is a Coxeter group with generators $s_i = (i, i+1)$. If $r = 2$, we have a presentation in generators and relations:

$$S_3 = \langle s_1, s_2 | s_1^2 = s_2^2 = 1, s_1 s_2 s_1 = s_2 s_1 s_2 \rangle$$

Weyl groups (both finite and affine) are important examples of Coxeter groups. Finite Weyl groups arise in the theory of Lie groups; there is one for every Cartan type. There is also an *affine Weyl group* which is infinite.

Given a Coxeter group W as above, there is an algebra called the *Iwahori Hecke algebra* which we now describe. The ground field F is assumed to contain a quantity q which might be an indeterminate or (for some purposes) an integer prime power or (for other purposes) a root of unity. So we will denote the algebra $\mathcal{H}_q(W)$. It has generators $T_1, \cdots, T_r$ subject to relations which we now state. First, it must satisfy the braid relations:

$$T_i T_j T_i \cdots = T_j T_i T_j \cdots , \tag{2}$$

where there are $m(i,j)$ factors on both sides. Second, instead of the relation $s_i^2 = 1$, it satisfies a quadratic relation

$$T_i^2 = (q-1)T_i + q.$$

Note that if $q = 1$, this becomes $T_i^2 = 1$, so $\mathcal{H}_1(W)$ is isomorphic to the group algebra $\mathbb{C}[W]$. In general, $\mathcal{H}_q(W)$ may be thought of as a *deformation* of $\mathbb{C}[W]$.

How do Iwahori Hecke algebras arise in nature? As it turns out, they are quite important.

- If G is a group of Lie type over a finite field, and W is its Weyl group, then $\mathcal{H}_q(W)$ can be embedded in $\mathbb{C}[G(\mathbb{F}_q)]$, and this helps us understand the representation theory of $G(\mathbb{F}_q)$. For example, if $G = \mathrm{GL}_n$ then we gain insight into the representation theory of $\mathrm{GL}_n(\mathbb{F}_q)$.

- Let F be a nonarchimedean local field such as $\mathbb{Q}_p$, and let $\mathbb{F}_q$ be the residue field. Let W_{aff} be the *affine Weyl group*. It is an infinite Coxeter group containing W as a finite subgroup. Then Iwahori and Matsumoto showed that $\mathcal{H}_q(W_{\mathrm{aff}})$ can be realized as a convolution ring of functions on $G(F)$. This turns out to be very important, and we will spend quite a bit of time explaining it, in the process getting a good start on the representation theory of $G(F)$, needed for the theory of automorphic forms.

But Iwahori Hecke algebras appear in other ways, too, seemingly unrelated to the representation theory of p-adic groups.

- Kazhdan and Lusztig used them to define Kazhdan-Lusztig polynomials. These appear in different seemingly unrelated contexts, such as the theory of singularities of Schubert varieties, and in the decomposition of Verma modules of Lie algebras.

- Jimbo showed that Iwahori Hecke algebras appear in a duality theory for quantum groups. This is a deformation of Frobenius-Schur duality, which is an important relationship between representations of symmetric groups and of $\mathrm{GL}_n(\mathbb{C})$.
- The Iwahori Hecke algebra is closely related to the Temperly-Lieb algebras which arise in both statistical physics and quantum physics. The related examples were key in the discovery of quantum groups.
- Iwahori Hecke algebras were used in Vaughn Jones' first paper defining the Jones polynomial.
- They appear in Dipper and James' important papers on modular representations of finite groups of Lie type.

Thus Iwahori Hecke algebras are involved in many diverse problems.

1 Hecke Algebras reduce infinite dimensional problems to finite-dimensional ones

In this section, we will not give proofs, but explain some "facts of life" about representations of p-adic groups to orient the reader. We will come back to these matters more rigorously later. In the next sections, we will give analogs of these facts of life for finite groups, with proofs. Later we will return to the p-adic case giving proofs.

Let F be a nonarchimedean local field, and let $\mathfrak{o}$ be its ring of integers. Thus we could take $F = \mathbb{Q}_p$ and $\mathfrak{o} = \mathbb{Z}_p$. Let $\mathfrak{p}$ be the maximal ideal of the discrete valuation ring $\mathfrak{o}$. Then $\mathfrak{o}/\mathfrak{p}$ is a finite field $\mathbb{F}_q$.

Let $G = \mathrm{GL}(n, F)$. This group is totally disconnected: its topology has a neighborhood basis at the identity consisting of open subgroups. Thus let $K^\circ = \mathrm{GL}(n, \mathfrak{o})$. This is a maximal compact subgroup. If N is any positive integer, let $K(N) = \{g \in K^\circ | g \equiv 1 \bmod \mathfrak{p}^N\}$. Then $K(N)$ are a family of open subgroups forming a basis of neighborhoods of the identity.

A representation $\pi : G \longrightarrow \mathrm{GL}(V)$, where V is a complex vector space is called *smooth* if when $0 \neq v \in V$ the stabilizer $\{k \in G | \pi(k)v = v\}$ is open. It is called *admissible* if furthermore given any open subgroup K the vector subspace V^K is finite-dimensional. The admissible representations contain the ones that are needed in the theory of automorphic forms. For example,

if $\pi : G \longrightarrow \mathrm{GL}(H)$ is any unitary representation on a Hilbert space, then H contains a dense subspace V on which G acts, and $\pi : G \longrightarrow \mathrm{GL}(V)$ is admissible. In the theory of automorphic forms one often works mainly with admissible representations.

The space V is usually infinite-dimensional. It is very useful to know that we may capture the representation in a finite-dimensional subspace V as follows. Let K be an open subgroup, and let $\mathcal{H}_K$ be the vector space of all compactly supported functions ϕ on G such that $\phi(kgk') = \phi(g)$ when $k, k' \in K$. We make K into a ring as follows:

$$(\phi * \psi)(g) = \int_G \phi(gx^{-1})\psi(x)\, dx.$$

Now if $\phi \in \mathcal{H}_K$ and $v \in V$, where (π, V) is any smooth representation, we may define $\pi(\phi) \in \mathrm{End}(V)$ by

$$\pi(\phi)v = \int_G \phi(g)\pi(g)v\, dv. \tag{3}$$

It is easy to check that

$$\pi(\phi * \psi) = \pi(\phi) \circ \pi(\psi).$$

The *spherical Hecke algebra* $\mathcal{H}_{K^\circ}$ is commutative.

On the other hand, let J be the subgroup of $k \in K^\circ = \mathrm{GL}(n, \mathfrak{o})$ such that $\bar{k}$ is upper triangular, where $\bar{k} \in \mathrm{GL}(n, \mathbb{F}_q)$ is the image under the homomorphism $\mathrm{GL}(n, \mathfrak{o}) \longrightarrow \mathrm{GL}(n, \mathbb{F}_q)$. This subgroup J is the *Iwahori subgroup*. The algebra $\mathcal{H}_J$ is nonabelian, but it has a beautiful structure. It has generators $T_0, \cdots, T_{n-1}$ and t such that T_i and T_j commute unless $i \equiv j \pm 1 \bmod n$, with the braid relations

$$T_i T_{i+1} T_i = T_{i+1} T_i T_{i+1},$$

where we interpret $i + 1$ as 0 if $i = n - 1$. Moreover

$$T_i^2 = (q-1)T_i + q.$$

Thus $T_0, \cdots, T_n$ generate an Iwahori Hecke algebra. The Coxeter group is the (infinite) affine Weyl group of type $A_{n-1}^{(1)}$. The extra element t has the effect $tT_it^{-1} = T_{i+1}$, where we again interpret things mod n, so $tT_{n-1}t^{-1} = T_0$.

Returning to the general case of an arbitrary open subgroup K, if $\phi \in \mathcal{H}_K$ then $\pi(\phi)$ projects V onto the finite-dimensional subspace V^K. We make V^K into an $\mathcal{H}_K$-module with the multiplication $\phi \cdot v = \pi(\phi)v$ for $\phi \in \mathcal{H}_K$, $v \in V^K$. We assume that V is admissible and that K is chosen to be small enough that V^K is nonzero.

Theorem 1 *(i) If (π, V) is an irreducible admissible representation and V^K is nonzero, then V^K is an irreducible (i.e. simple) $\mathcal{H}_K$-module.*

(ii) If (π, V) and (σ, W) are irreducible admissible representations, and if $V^K \cong W^K$ as $\mathcal{H}_K$-modules, then π and σ are equivalent representations.

The proof will be given later in Section 3.

Thus the representation theory finite-dimensional of $\mathcal{H}_K$ faithfully captures the representation theory of G, provided we limit ourselves to the representations of G that have a nonzero subspace of K-fixed vectors.

We will be mainly interested in Iwahori Hecke algebras, so we will mainly be interested in representations that have Iwahori fixed vectors. This excludes, for example, supercuspidal representations. Nevertheless, this class of representations is large enough for many purposes. It includes the spherical representations, that is, those that have K°-fixed vectors. If $\pi = \otimes \pi_v$ is an automorphic cuspidal representation of the adele group $\mathbb{A}$ of a number field F, written as a restricted tensor product over the places of F, then π_v is spherical for all but finitely many places v.

Then why not just restrict to the spherical Hecke algebra $\mathcal{H}_{K^\circ}$ instead of the larger, nonabelian Iwahori Hecke algebra? The answer is that even if one is only concerned with spherical representations, their theory naturally leads to the Iwahori subgroup and the Iwahori Hecke algebra. We will see why later.

2 Hecke Algebras of Finite Groups

Even for finite groups, the theory of Hecke algebras has nontrivial important content, which we turn to now.

Let G be a finite group.

If (π, V) is a representation, let $(\hat{\pi}, \hat{V})$ be the contragredient representation. Thus $\hat{V} = V^*$ is the dual space of V. If $\hat{v} \in \hat{V}$ then $\hat{v}$ is a linear functional on V. We will use the notation $\langle v, \hat{v} \rangle$ instead of $\hat{v}(v)$. The repre-

sentation $\hat{\pi}(g)$ is defined by the condition

$$\langle \pi(g)v, \hat{v} \rangle = \langle v, \hat{\pi}(g^{-1})\hat{v} \rangle.$$

If ϕ, ψ are functions on G, the *convolution* $\phi * \psi$ is defined by

$$(\phi * \psi)(g) = \frac{1}{|G|} \sum_{x \in G} \phi(x)\psi(x^{-1}g) = \frac{1}{|G|} \sum_{x \in G} \phi(gx)\psi(x^{-1}).$$

The space $\mathcal{H}$ of all functions on G with convolution as multiplication is a ring isomorphic to the group algebra. Namely, if $\phi \in \mathcal{H}$ let $\phi' = \frac{1}{|G|} \sum_{g \in G} \phi(g)\, g$.

Lemma 1 *$\phi \mapsto \phi'$ is a ring isomorphism $\mathcal{H} \longrightarrow \mathbb{C}[G]$.*

Proof The coefficient of g in $\phi'\psi' = \frac{1}{|G|^2} \sum \phi(x)\psi(y)xy$ is $\frac{1}{|G|}(\phi * \psi)(g)$. □

Suppose that $\pi : G \longrightarrow \mathrm{GL}(V)$ is a representation of G on a complex vector space and that $\phi \in \mathcal{H}$. Define $\pi(\phi) \in \mathrm{End}(V)$ by

$$\pi(\phi)v = \frac{1}{|G|} \sum_{g \in G} \phi(g)\pi(g)v.$$

Lemma 2 *If $\phi, \psi \in \mathcal{H}$ then $\pi(\phi * \psi) = \pi(\phi) \circ \pi(\psi)$.*

Proof We leave the proof of this to the reader. □

Let K be a subgroup of G. We define the Hecke algebra $\mathcal{H}_K$ to be the vector space of K-biinvariant functions on G, that is, functions $\phi : G \longrightarrow \mathbb{C}$ such that $\phi(kgk') = \phi(g)$ for $k, k' \in K$. It too is a ring under convolution.

Suppose that (π, V) is a representation of G. Let

$$V^K = \{v \in V | \pi(k)v = v \text{ for all } k \in K\}$$

be the space of K-fixed vectors. Then if $\phi \in \mathcal{H}_K$, $\pi(\phi)$ maps V into V^K. We then make V^K into an $\mathcal{H}_K$-module with the multiplication $\phi \cdot v = \pi(\phi)v$ for $\phi \in \mathcal{H}_K$ and $v \in V$.

Lemma 3 *Let $l : V^K \longrightarrow \mathbb{C}$ be any linear functional. Then there exists a vector $\hat{v} \in \hat{V}^K$ such that $l(v) = \langle v, \hat{v} \rangle$.*

Proof We extend l to a linear functional $\widehat{v_0}$ on V. Let $\hat{v} = \frac{1}{|K|}\sum_{k\in K}\hat{\pi}(k)v_0$. Then $\hat{v}$ agrees with $\hat{v}_0$ on V^K since if $v \in V^K$ we have

$$\langle v, \hat{v}\rangle = \frac{1}{|K|}\sum_{k\in K}\langle v, \hat{\pi}(k)\hat{v}_0\rangle = \langle v, \hat{v}\rangle = \frac{1}{|K|}\sum_{k\in K}\langle \pi(k^{-1})v, \hat{v}_0\rangle = \frac{1}{|K|}\sum_{k\in K}\langle v, \hat{v}_0\rangle$$

because $v \in V^K$. □

Proposition 1 *If $V^K \neq 0$ then $\hat{V}^K \neq 0$.*

Proof This is immediate from the Lemma. □

Proposition 2 *Let R be an algebra over a field F and let M_1, M_2 be simple R-modules which are finite-dimensional vector spaces over F. Assume there exist linear functionals $L_i : M_i \longrightarrow F$ and $m_i \in M_i$ such that $L_i(m_i) \neq 0$ and $L_1(rm_1) = L_2(rm_2)$ for all $r \in R$. Then $M_1 \cong M_2$ as R-modules.*

In the next Proposition, we will apply this when R is a group algebra. In that case, we could equally well use Schur orthogonality of matrix coefficients for irreducible representations of finite groups. However the statement at hand will be useful later.

Proof Let M be a simple R-module. If $m \in M$ and L is in the dual space M^* let us define $\phi_{m,L} \in \mathrm{End}_F(M)$ and $f_{m,L} : R \longrightarrow F$ by

$$\phi_{m,L}(x) = L(x)m, \qquad f_{m,L}(r) = L(rm).$$

Let $\mathcal{R}_M$ be the ring of functions on R which are finite linear combinations of the functions $f_{m,L}$. Then the maps $(m, L) \longrightarrow \phi_{m,L}$ and $(m, L) \longrightarrow f_{m,L}$ are bilinear, hence there are linear maps $M \otimes M^* \longrightarrow \mathrm{End}_F(M)$ and $M \otimes M^* \longrightarrow \mathcal{R}_M$ sending $m \otimes L$ to $\phi_{m,L}$ and $f_{m,L}$ respectively. The first map is a vector space isomorphism and so there exists a linear $\Lambda : \mathrm{End}_F(M) \longrightarrow \mathcal{R}_M$ such that $\Lambda\phi_{m,L} = f_{m,L}$.

We define left R-module structures on $\mathrm{End}_F(M)$ and on $\mathcal{R}_M$ as follows. If $\phi \in \mathrm{End}_F(M)$ and $r \in R$ then $r\phi$ is the endomorphism $(r\phi)(m) = r\phi(m)$. On the other hand, if $f \in \mathcal{R}_M$ and $r \in R$ we define $rf : R \longrightarrow F$ by $rf(s) = f(sr)$ for $s \in R$. To see that $rf \in \mathcal{R}_M$ we may assume that $f = f_{m,L}$, in which case we easily check that $rf_{m,L} = f_{rm,L}$. We also have $r\phi_{m,L} = \phi_{rm,L}$, and it follows that the map Λ is an R-module homomorphism with these structures.

Now as an R-module $\mathrm{End}_F(M)$ decomposes as a direct sum of d copies of M, where $d = \dim_F(M)$. Since this R-module contains only copies of this one isomorphism class of simple modules, and since $\Lambda : \mathrm{End}_F(M) \longrightarrow \mathcal{R}_M$ is a surjection, it follows that any simple R-submodule of $\mathcal{R}_F$ is isomorphic to M.

Because $\mathcal{R}_{M_1}$ and $\mathcal{R}_{M_2}$ have a nonzero element in common, it follows that M_1 and M_2 are isomorphic. □

If (π, V) is an irreducible representation of G we call any function of the form $\langle \pi(g)v, \hat{v} \rangle$ a *matrix coefficient of* V. Applying Proposition 2 to the group algebra, we see that two irreducible representations are equivalent if they have a matrix coefficient in common. The next result shows that the $\mathcal{H}_K$-module V^K contains complete information about V, even though it may be much smaller, provided $V^K \neq 0$. This is the analog of Theorem 1, which we have not yet proved.

Theorem 2 *(i) Suppose that (π, V) is an irreducible representation of G such that V^K is nonzero. Then V^K is an irreducible $\mathcal{H}_K$ submodule.*

(ii) If (σ, W) is another irreducible representation of G such that V^K and W^K are both nonzero, and $V^K \cong W^K$ as $\mathcal{H}_K$-modules. Then π and σ are equivalent representations.

Proof Let us prove (i). Suppose that $U \subset V^K$ is a nonzero submodule. We wish to show that $U = V^K$. Let $0 \neq u \in U$. It is sufficient to show that $\mathcal{H}_K u = V^K$. Therefore let $v \in V^K$. We will show that there is $\phi \in \mathcal{H}_K$ such that $\pi(\phi)u = v$.

Since V is irreducible, and since $\mathcal{H}u$ is a G-submodule of V, we have $\mathcal{H}u = V$. Therefore let $\psi \in \mathcal{H}$ such that $\pi(\psi)u = v$. Let

$$\phi(g) = \frac{1}{|K|^2} \sum_{k,k' \in K} \psi(kgk').$$

Clearly $\phi \in \mathcal{H}_K$. Now we have

$$\pi(\phi)u = \frac{1}{|K|^2} \sum_{k,k' \in K} \frac{1}{|G|} \sum_{g \in G} \psi(kgk')\pi(g)u.$$

Make the variable change $g \to k^{-1}g(k')^{-1}$ to obtain

$$\pi(\phi)u = \frac{1}{|K|^2} \sum_{k,k' \in K} \frac{1}{|G|} \sum_{g \in G} \psi(g)\pi(k)^{-1}\pi(g)\pi(k')^{-1}u.$$

Now we may drop the summation over k' since $u \in V^K$, and interchanging the summation write this as

$$\frac{1}{|K|}\sum_{k\in K}\frac{1}{|G|}\sum_{g\in G}\psi(g)\pi(k)^{-1}\pi(g)u = \frac{1}{|K|}\sum_{k\in K}\pi(k)^{-1}\pi(\psi)u.$$

Since $\pi(\psi)u = v$, this equals $\frac{1}{|K|}\sum_{k\in K}\pi(k^{-1})v$ and since $v \in V^K$, this equals v. Thus $v \in \mathcal{H}u$ and $\mathcal{H}u = V$. This proves (i).

To prove (ii), suppose that V^K and W^K are isomorphic as $\mathcal{H}_K$-modules, with V and W irreducible G-modules. Let $\lambda : V^K \longrightarrow W^K$ be an isomorphism. Pick a nonzero linear functional $l : W^K \longrightarrow \mathbb{C}$. By the Lemma there exist $\hat{v} \in \hat{V}^K$ and $\hat{w} \in \hat{W}^K$ such that $l(\lambda(v)) = \langle v, \hat{v}\rangle$ for $v \in V^K$ and $\langle w, \hat{w}\rangle = l(w)$ for $w \in W^K$.

Since λ is an $\mathcal{H}_K$-module homomorphism, if $\phi \in \mathcal{H}_K$ we have, for $v \in V^K$

$$\langle\sigma(\phi)\lambda(v), \hat{w}\rangle = \langle\lambda(\pi(\phi)v), \hat{w}\rangle = l(\lambda(\pi(\phi)v)) = \langle\pi(\phi)v, \hat{v}\rangle. \tag{4}$$

Since l is nonzero we may pick $w_0 \in W^K$ such that $\langle w_0, \hat{w}\rangle = l(w_0) \neq 0$. Since λ is an isomorphism, there exists $v_0 \in V^K$ such that $\lambda(v_0) = w_0$. Then (4) implies that

$$\langle\sigma(\phi)w_0, \hat{w}\rangle = \langle\pi(\phi)v_0, \hat{v}\rangle \tag{5}$$

for $\phi \in \mathcal{H}_K$. Now we claim that (5) is true for all $\phi \in \mathcal{H}$. Indeed, if $\phi \in \mathcal{H}$, we project it into $\mathcal{H}$ by defining

$$\phi_K(g) = \frac{1}{|K|^2}\sum_{k,k'\in K}\phi(kgk').$$

Clearly $\phi_K \in \mathcal{H}_K$. On the other hand

$$\begin{aligned}\langle\sigma(\phi_K)w_0, \hat{w}\rangle = \frac{1}{|K|^2}\left\langle\sum_{k,k'\in K}\sigma(k)\sigma(\phi)\sigma(k')w_0, \hat{w}\right\rangle &= \\ \frac{1}{|K|^2}\sum_{k,k'\in K}\langle\sigma(\phi)\sigma(k')w_0, \hat{\sigma}(k^{-1})\hat{w}\rangle &= \langle\sigma(\phi)w_0, \hat{w}\rangle\end{aligned}$$

since $w_0 \in W^K$ and $\hat{w} \in \hat{W}^K$. Similarly $\langle\pi(\phi_K)v_0, \hat{v}\rangle = \langle\pi(\phi)v_0, \hat{v}\rangle$, and so (5) for $\phi_K \in \mathcal{H}_K$ implies (5) for $\phi \in \mathcal{H}$.

Now let $g \in G$. Take $\phi = \phi_g$ where

$$\phi_g(x) = \begin{cases} |G| & \text{if } x = g, \\ 0 & \text{otherwise.}\end{cases}$$

Then $\pi(\phi_g) = \pi(g)$, and so (5) implies that

$$\langle \sigma(g)w_0, \hat{w}\rangle = \langle \pi(g)v_0, \hat{v}\rangle.$$

We see that the representations π and σ have a matrix coefficient in common, and it follows from Proposition 2 that the two representations are isomorphic. □

Let G be a finite group, H a subgroup and (π, V) a representation of H. We will define V^G to be the vector space of all functions $f : G \longrightarrow V$ such that $f(hx) = \pi(h)f(x)$ when $h \in H$ and $x \in G$. Define, for $g \in G$

$$(\pi^G(g)f)(x) = f(xg).$$

Thus g acts on V^G by *right translation*. The representation (π^G, V^G) is the *induced representation*.

Exercise 1 Check that if $f \in V^G$ and $g \in G$ then $\pi^G(g)f \in V^G$. Also check that

$$\pi^G(g_1g_2) = \pi^G(g_1)\pi^G(g_2),$$

so that (π^G, V^G) is a representation of G.

Theorem 3 (Frobenius reciprocity) *Let (π, V) be a representation of H and let (σ, W) be a representation of G. We have a vector space isomorphism*

$$\mathrm{Hom}_G(W, V^G) \cong \mathrm{Hom}_H(W, V).$$

In this isomorphism the G-module homomorphism $\Phi : W \longrightarrow V^G$ corresponds to the H-module homomorphism $\phi : W \longrightarrow V$, where we may express Φ in terms of ϕ and ϕ in terms of Φ by the following formulae.

$$\phi(w) = \Phi(w)(1), \qquad \Phi(w)(g) = \phi(\sigma(g)w).$$

Proof We first check that if $\Phi : W \longrightarrow V^G$ is a G-module homomorphism, then $\phi(w) = \Phi(w)(1)$ defines an H-module homomorphism. Indeed, we have, for $h \in H$

$$\phi(\sigma(h)w) = \Phi(\sigma(h)w)(1) = (\pi^G(h)\Phi(w))(1) = \Phi(w)(1\cdot h) = \Phi(w)(h\cdot 1) = \pi(h)\Phi(w)(1),$$

where we have used the definition of ϕ, the assumption that Φ is a G-module homomorphism, the definition of Φ^G, the identity $1 \cdot h = h \cdot 1$, and the assumption that $\Phi(w) \in V^G$. This equals $\pi(h)\phi(w)$, so ϕ is an H-module homomorphism.

We leave the reader to complete the proof (Exercise 2). □

Exercise 2 Complete the above proof as follows.

(a) Show that if $\phi : W \longrightarrow V$ is an H-module homomorphism then $\Phi(w)(g) = \phi(\sigma(g)w)$ defines an element of V^G, and that $\Phi : W \longrightarrow V^G$ is a G-module homomorphism.

(b) Show that the two constructions $\phi \longmapsto \Phi$ and $\Phi \longmapsto \phi$ are inverse maps between $\mathrm{Hom}_G(W, V^G)$ and $\mathrm{Hom}_H(W, V)$.

Let us explain why this Theorem 3 is called Frobenius reciprocity. Frobenius considered characters before representation theory was properly understood. For him, induction was an operation on characters that was adjoint to restriction. If H is a subgroup of G and χ is a character of H then the induced character χ^G of G is characterized by the adjointness property

$$\langle \chi^G, \theta \rangle_G = \langle \chi, \theta \rangle_H$$

where $\langle\ ,\ \rangle_G$ is the inner product on $L^2(G)$. It follows from the following statement that the induced character χ^G is the character of V^G.

Proposition 3 *Let G be a finite group, (π, V) and (σ, W) two representations. Let χ_π and χ_σ be their characters. Then*

$$\langle \chi_\pi, \chi_\sigma \rangle_G = \dim\ \mathrm{Hom}_{\mathbb{C}[G]}(V, W).$$

Proof Both sides are bilinear in the sense that if $\pi = \pi_1 \oplus \pi_2$ for representations (π_i, V_i) then $\langle \chi_\pi, \chi_\sigma \rangle = \langle \chi_{\pi_1}, \chi_\sigma \rangle + \langle \chi_{\pi_2}, \chi_\sigma \rangle$ and $\mathrm{Hom}(V, W) \cong \mathrm{Hom}(V_1, W) \oplus \mathrm{Hom}(V_2, W)$, and similarly for W. Hence we are reduced to the case where π and σ are irreducible. Then

$$\langle \chi_\pi, \chi_\sigma \rangle = \left\{ \begin{array}{ll} 1 & \text{if } V \cong W \\ 0 & \text{if } V \ncong W \end{array} \right\} = \dim\ \mathrm{Hom}_{\mathbb{C}[G]}(V, W)$$

by Schur orthogonality of characters and Schur's Lemma. □

Mackey theory asks the following question: if H_1 and H_2 are subgroups of G and V_1 and V_2 are modules for H_1 and H_2 respectively, then what is $\mathrm{Hom}_G(V_1^G, V_2^G)$?

Mackey theory answers this and related questions. For simplicity, we will limit ourselves to the special case where V_1 and V_2 are one-dimensional, which makes for a minor simplification, and is already enough for some important examples.

We recall that $\mathcal{H}$ is the space of all functions on G. As we explained earlier, it is a ring under convolution, isomorphic to the group algebra.

We recall the right regular representation $\rho : G \longrightarrow \mathrm{End}(\mathcal{H})$ is the action $(\rho(g)f)(x) = f(xg)$.

Lemma 4 *Let $T : \mathcal{H} \longrightarrow \mathcal{H}$ be a linear transformation that commutes with $\rho(g)$; that is, $T(\rho(g)f) = \rho(g)T(f)$. Then there exists a unique $\lambda \in \mathcal{H}$ such that $T(f) = \lambda * f$.*

Proof Define $\delta_0(g) = |G|$ if $g = 1$, and 0 if $g \neq 1$. Then δ_0 is the unit in the convolution ring $\mathcal{H}$, that is, $\delta_0 * f = f * \delta_0 = f$ for all $f \in \mathcal{H}$. If λ exists such that $T(f) = \lambda * f$ for all f, then $\lambda = \lambda * \delta_0 = T(\delta_0)$. Hence it is unique, and it remains to be shown that $\lambda = T(\delta_0)$ works. We claim that if $f \in \mathcal{H}$ then

$$f = \frac{1}{|G|} \sum_{g \in G} f(g)\rho(g^{-1})\delta_0. \tag{6}$$

Indeed, applying the right-hand side to $x \in G$ gives

$$\frac{1}{|G|} \sum_{g \in G} f(g)(\rho(g^{-1})\delta_0)(x) = \frac{1}{|G|} \sum_{g \in G} f(g)\delta_0(xg^{-1}).$$

Only one term contributes, which is $g = x$, and that term equals $f(x)$. This proves (6).

Now applying T to (6) gives

$$Tf = \frac{1}{|G|} \sum_{g \in G} f(g)T(\rho(g^{-1})\delta_0) = \frac{1}{|G|} \sum_{g \in G} f(g)\rho(g^{-1})T(\delta_0) = \frac{1}{|G|} \sum_{g \in G} f(g)\rho(g^{-1})\lambda.$$

Thus

$$Tf(x) = \frac{1}{|G|} \sum_{g} (\rho(g^{-1})\lambda)(x)f(g) = \frac{1}{|G|} \sum_{g} \lambda(xg^{-1})f(g) = (\lambda * f)(x).$$

□

If H is a group, a one-dimensional representation is basically the same thing as a *linear character*, that is, a homomorphism $\psi : H \longrightarrow \mathbb{C}^\times$. That is, if (π, V) is a representation of H and $\dim(V) = 1$ then there is a linear character ψ such that $\pi(g)v = \psi(g)v$ for all $g \in G$. We will sometimes write ψ^G instead of V^G for the induced representation. Identifying $V = \mathbb{C}$ this is the representation of G on the space of functions $f : G \longrightarrow \mathbb{C}$ such that $f(hg) = \psi(h)f(g)$ for $h \in H$. The action of G is by right translation, that is, from the right regular representation ρ acting on functions by $\rho(g)f(x) = f(xg)$.

Theorem 4 (Geometric form of Mackey's Theorem) *Let H_1, H_2 be subgroups of the finite group G, and let ψ_i be a linear character of H_i. Let $\Lambda \in \mathrm{Hom}_G(\psi_1^G, \psi_2^G)$. Then there exists a function $\Delta : G \longrightarrow \mathbb{C}$ such that*

$$\Delta(h_2 g h_1) = \psi_2(h_2)\Delta(g)\psi_1(h_1), \qquad h_i \in H_i, \tag{7}$$

and $\Lambda f = \Delta * f$ for all $f \in \psi_1^G$. The map $\Lambda \longmapsto \Delta$ is a vector space isomorphism of $\mathrm{Hom}_G(\psi_1^G, \psi_2^G)$ with the space of all functions satisfying (7).

Proof Given Δ satisfying (7), it is straightforward to check that $\Delta * f \in \psi_2^G$ for any $f \in \mathcal{H}$. In particular, this is true if $f \in \psi_1^G$. Moreover, left convolution commutes with right translation, so $\rho(g)(\Delta * f) = \Delta * \rho(g)f$. This means that the map $\Lambda f = \Delta * f$ is an intertwining operator in $\mathrm{Hom}_G(\psi_1^G, \psi_2^G)$.

Let us consider, conversely, how to start with Λ and produce Δ. Let $\dot{\psi_1} : G \longrightarrow \mathbb{C}$ be the function

$$\dot{\psi_1}(g) = \begin{cases} \frac{|G|}{|H_1|}\psi_1(g) & \text{if } g \in H_1, \\ 0 & \text{otherwise.} \end{cases}$$

Thus for any function f we have

$$(\dot{\psi_1} * f)(g) = \frac{1}{|H_1|} \sum_{h \in H_1} \psi_1(h) f(h^{-1}g).$$

It is easy to check that the map $p : \mathcal{H} \longrightarrow \mathcal{H}$ defined by $p(f) = \dot{\psi_1} * f$ is a projection with image ψ_1^G. This means that $p^2 = p$, for any $f \in \mathcal{H}$ we have $p(f) \in \psi_1^G$ and that $p(f) = f$ if $f \in \psi_1^G$. We define $T : \mathcal{H} \longrightarrow \mathcal{H}$ to be $\Lambda \circ p$.

Then since Λ is a G-module homomorphism, we have $\Lambda \circ \rho(g) = \rho(g) \circ \Lambda$. It is also true that $\rho(g) \circ p = p \circ \rho(g)$ since p is left convolution with ψ_1, and left convolution commutes with right translation. Therefore T satisfies $T \circ \rho(g) = \rho(g) \circ T$. By Lemma 4 we have $Tf = \Delta * f$ for some unique Δ. Let us check that Δ has the property (7). This can be separated into two statements,

$$\Delta(gh_1) = \Delta(g)\psi_1(h_1), \qquad h_1 \in H_1, \tag{8}$$

and

$$\Delta(h_2 g) = \psi_2(h_2)\Delta(g), \qquad h_2 \in H_2. \tag{9}$$

For (8) we note that if $f \in \mathcal{H}$ we have

$$\Delta * \dot{\psi}_1 * f = T(p(f)) = \Lambda(p^2(f)) = \Lambda(p(f)) = \Delta * f.$$

Since this is true for every f, we have $\Delta = \Delta * \dot{\psi}_1$. Since $\dot{\psi}_1(gh_1) = \dot{\psi}_1(g)\psi_1(h_1)$ for $g \in G$ and $h_1 \in H_1$, we obtain (8). We leave (9) to the reader, with the hint that it follows from the fact that the image of T is contained in ψ_2^G.

We leave the reader to check that the two maps $\Delta \mapsto \Lambda$ and $\Lambda \mapsto \Delta$ described above are inverses of each other. □

Exercise 3 Fill out the details in the proof of Theorem 4.

Exercise 4 Let G be a finite group and V, W vector spaces. Let $C(G, V)$ be the space of maps $G \longrightarrow V$. There is a representation $\rho_V : G \longrightarrow \mathrm{End}(C(G, V))$ by right translation:

$$(\rho_V(g)f)(x) = f(xg), \qquad g, x \in G,\ f \in C(G, V).$$

Let $T : C(G, V) \longrightarrow C(G, W)$ be a linear map that commutes with this action, i.e.

$$T(\rho_V(g)f) = \rho_W(g)T(f), \qquad g \in G, f \in C(G, V).$$

Prove that there is a map $\lambda : G \longrightarrow \mathrm{Hom}(V, W)$ such that $T(f) = \lambda * f$, where the convolution is

$$(\lambda * f)(x) = \frac{1}{|G|} \sum_{g \in G} \lambda(g) f(g^{-1}x). \tag{10}$$

Exercise 5 In Theorem 4 we assumed that the two modules were one-dimensional. This exercise removes that restriction. Let G be a finite group, H_1 and H_2 subgroups and (π_i, V_i) an H_i-module for $i = 1, 2$. Let $\Lambda \in \mathrm{Hom}_G(V_1^G, V_2^G)$. Prove that there exists a function $\Delta : G \longrightarrow \mathrm{Hom}_{\mathbb{C}}(V_1, V_2)$ such that

$$\Delta(h_2 g h_1) = \pi_2(h_2) \circ \Delta(g) \circ \pi_1(h_1), \qquad h_i \in H_i, \tag{11}$$

and $\Lambda f = \Delta * f$ for all $f \in V_1^G$, with the convolution defined by (10). The map $\Lambda \longmapsto \Delta$ is a vector space isomorphism of $\mathrm{Hom}_G(V_1^G, V_2^G)$ with the space of all functions satisfying (11). **Hint:** Use Exercise 4 in place of Lemma 4.

A G-module homomorphism is sometimes called an *intertwining operator*. We see that intertwining operators between induced representations are obtained by convolution with functions Δ such as in the geometric form of Mackey's theorem. This geometric interpretation of intertwining operators is one reason for the remarkable usefulness of Mackey's theorem.

Now let H_1, H_2, H_3 three subgroups, with linear characters ψ_i of H_i. Let $\Lambda \in \mathrm{Hom}_G(\psi_1^G, \psi_2^G)$ and $\Lambda' \in \mathrm{Hom}_G(\psi_2^G, \psi_3^G)$. Let Δ and Δ' be the functions

on G corresponding to these two intertwining operators by Mackey theory. Since Λ is convolution with Δ and Λ' is convolution with Δ' we see that $\Lambda' \circ \Lambda \in \mathrm{Hom}_G(\psi_1^G, \psi_3^G)$ is convolution with $\Delta' * \Delta$.

A special case is when $H_1 = H_2 = H_3 = H$. If ψ is a linear character of H we will write ψ^G for the corresponding induced representation, suppressing the underlying one-dimensional vector space.

Proposition 4 *Let H be a subgroup of G and let ψ be a linear character of H. Then the ring $\mathrm{End}_G(\psi^G)$ is isomorphic as a ring to the convolution ring $\mathcal{H}_\psi$, which is the space of functions $\Delta : G \longrightarrow \mathbb{C}$ such that $\Delta(hgh') = \psi(h)\Delta(g)\psi(h')$ when $h, h' \in H$.*

This is a Hecke algebra in the sense that we have already considered when $\psi = 1$.

Proof This is clear from the above discussion. □

A representation of G is called *multiplicity free* if it is a direct sum of nonisomorphic irreducible representations, each appearing at most once.

Proposition 5 *Let H be a subgroup of G and let ψ be a linear character of H. The following conditions are equivalent:*

(i) The induced representation ψ^G is multiplicity free;

(ii) For every irreducible representation π of G, $\pi|_H$ contains at most one invariant subspace isomorphic to ψ;

(iii) The Hecke algebra $\mathcal{H}_\psi$ is commutative.

Proof The equivalence if (ii) and (iii) is clear from Frobenius reciprocity. We show that (i) is equivalent to (iii). Indeed, $\mathcal{H}_\psi \cong \mathrm{End}_G(\psi^G)$, so we consider when this is commutative. Write $\psi^G = \bigoplus d_i \pi_i$ as a direct sum of distinct irreducibles with multiplicities. Then $\mathrm{End}_G(\psi^G) = \bigoplus \mathrm{Mat}(d_i, \mathbb{C})$. This is commutative if and only if all $d_i \leqslant 1$. □

If $H \subset G$ is such that 1_H^G is multiplity-free then H is called a *Gelfand subgroup*. We see that a necessary and sufficient condition is that the Hecke algebra $\mathcal{H}_H$ be commutative. We now discuss Gelfand's method for proving such commutativity.

By *involution* of a group G we will mean a map $\iota : G \to G$ of order 2 that is anticommutative:

$$\iota(g_1 g_2) = \iota g_2 \, \iota g_1.$$

Similarly an *involution* of a ring R is an additive map of order 2 that is anticommutative for the ring multiplication.

Theorem 5 *Let H be a subgroup of the finite group G, and suppose that G admits an involution fixing H, such that every double coset of H is invariant: $HgH = H{}^{\iota}gH$. Then H is a Gelfand subgroup.*

Proof The ring $\mathcal{H}_H$ is just the convolution ring of H-bi-invariant functions on G. We have an involution on this ring:

$$ {}^{\iota}\Delta(g) = \Delta({}^{\iota}g). $$

It is easy to check that

$$ {}^{\iota}(\Delta_1 * \Delta_2) =^{\iota} \Delta_2 *^{\iota} \Delta_1. $$

On the other hand, each Δ is constant on each double coset, and these are invariant under ι by hypothesis. So ι is the identity map. This proves that $\mathcal{H}$ is commutative, so (G, H) is a Gelfand pair. □

Here is an example of Gelfand's method. Let S_n denote the symmetric group. We can embed $S_n \times S_m \to S_{n+m}$ by letting S_n act on the first n elements of the set $\{1, 2, 3, \cdots, n+m\}$, and letting S_m act on the last m elements.

Proposition 6 *The subgroup $S_n \times S_m$ is a Gelfand subgroup of S_{n+m}.*

Proof Let $H = S_n \times S_m$ and $G = S_{n+m}$. We take the involution ι in Theorem 5 to be the inverse map $g \longrightarrow g^{-1}$. We must check that each double coset is ι-stable.

It will be convenient to represent elements of S_{n+m} by permutation matrices. We will show that each double coset HgH has a representative of the form

$$ \begin{pmatrix} I_r & 0 & 0 & 0 \\ 0 & 0_{n-r} & 0 & I_{n-r} \\ 0 & 0 & I_{m-n+r} & 0 \\ 0 & I_{n-r} & 0 & 0_{n-r} \end{pmatrix}. \tag{12} $$

Here I_n and 0_n are the $n \times n$ identity and zero matrices, and the remaining 0 matrices are rectangular blocks.

We write g in block form:

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

where A, B, C and D are matrices with only 1's and 0's, and with at most one nonzero entry in each row and column. Here A is $n \times n$ and D is $m \times m$. Let r be the rank of A. Then clearly B and C both must have rank $n - r$, and so D has rank $m - n + r$.

Multiplying A on the left by an element of S_n we may arrange its rows so that its nonzero entries lie in the first r rows, then multiplying on the right by an element of S_n we may put these in the upper left corner. Similarly we may arrange it so that D has its nonzero entries in the upper left corner. Now the form of the matrix is

$$\begin{pmatrix} T_r & 0 & 0 & 0 \\ 0 & 0_{n-r} & 0 & U_{n-r} \\ 0 & 0 & V_{m-n+r} & 0 \\ 0 & W_{n-r} & 0 & 0_{n-r} \end{pmatrix}.$$

where the sizes of the square blocks are indicated by subscripts. The matrices T, U, V and W are permutation matrices. Left multiplication by element of $S_r \times S_{n-r} \times S_{m-n+r} \times S_{n-r}$ can now replace these four matrices by identity matrices. This proves that (12) is a complete set of double coset representatives.

Since these double coset representatives are all invariant under the involution, by Theorem 5 it follows that $S_n \times S_m$ is a Gelfand subgroup. □

3 Proof of Theorem 1

If G is totally disconnected and locally compact, then its topology has a basis of neighborhoods of the identity consisting of open and compact subgroups.

Proposition 7 *Let K be a compact totally disconnected group. Then K has a neighborhood basis at the identity consisting of open and compact subgroups which are normal in K.*

Proof If K' is an open subgroup of K then K' has an open subgroup K'' that is normal in K. Indeed, K' has only finitely many conjugates since it

is of finite index, and we may take K'' to be the intersection of these. Now given any neighborhood base consisting of open subgroups, we may replace each by a smaller open subgroup which is normal in K, and obtain another neighborhood base. □

Proposition 8 *Let K be a totally disconnected compact group and $\rho : K \longrightarrow \mathrm{GL}(V)$ a finite-dimensional complex representation. Then K has a normal subgroup K' of finite index such that $K' \subset \ker(\rho)$. Therefore ρ is actually a representation of the finite group K/K'.*

Proof Let Ω be an open neighborhood of the identity in $\mathrm{GL}(V)$ that does not contain any subgroup of $\mathrm{GL}(V)$. Then $\rho^{-1}(\Omega)$ is an open neighborhood of the identity in K. Since K is totally disconnected and compact, it has a neighborhood base at the identity consisting of compact open normal subgroups. Therefore there is some compact open normal subgroup K' of K contained in $\rho^{-1}(\Omega)$. Since $\rho(K') \subset \Omega$ we have $K' \subset \ker(\rho)$. The quotient K/K' is finite since K is compact and K' open. □

Let G be a totally disconnected locally compact group and K° a compact open subgroup, which we may take to be maximal. Let (π, V) be a smooth representation. We have already defined V to be admissible if V^K is finite-dimensional for every compact open subgroup K, but there is another way of thinking of this. If ρ is any irreducible representation of K, then the Peter-Weyl theorem guarantees that ρ is finite-dimensional, that is, one of the representations in Proposition 8. Let V_ρ be the ρ-isotypic subspace, that is, the direct sum of all K°-invariant subspaces of V that are isomorphic to ρ as K°-modules.

Proposition 9 *Let (π, V) be a smooth representation of G. Then*

$$V = \bigoplus_\rho V_\rho \qquad \textit{(algebraic direct sum)}$$

where ρ runs through the finite-dimensional irreducible representations of K°. The representation V is admissible if and only if every V_ρ is finite-dimensional.

Proof Since V is smooth, every vector $v \in V$ is invariant under some open subgroup K, which may be assumed normal by Proposition 7. Now there are a finite number of irreducible representations that factor through the finite

group K°/K, and one of these, say ρ, has finite multiplicity in V if and only if V_ρ is finite-dimensional. □

Now let us consider the contragredient of an admissible representation. A linear functional L on V is called *smooth* if there exists an open subgroup K of G such that $L(\pi(k)v) = L(v)$ for all $v \in V$ and $k \in K$. Let $\hat{V}$ be the space of smooth linear functionals. Also, let $\hat{V}_\rho$ be the dual space of the finite dimensional vector space V_ρ.

Proposition 10 *Assume that V is admissible. Then*

$$\hat{V} = \bigoplus_\rho \hat{V}_\rho \qquad \textit{(algebraic direct sum).}$$

Proof If $\hat{v}$ is a smooth linear functional, then $\hat{v}$ is invariant under an open subgroup K that is normal in K°. This means that $\hat{v}$ annihilates V_ρ for all ρ that do not factor through K°/K. Therefore $\hat{v}$ lies in the finite direct sum of those $\hat{V}_\rho$ that do factor through K°/K, and so lies in the algebraic direct sum $\bigoplus_\rho \hat{V}_\rho$. □

If $v \in V$ and $\hat{v} \in \hat{V}$, we will write $\langle v, \hat{v}\rangle$ instead of $\hat{v}(v)$. We have a representation $\hat{\pi}$ on $\hat{V}$ defined by $\langle v, \hat{\pi}(g)\rangle = \langle \pi(g^{-1})v, \hat{v}\rangle$. Then $(\hat{\pi}, \hat{V})$ is the *contragredient representation*.

Proposition 11 *If (π, V) is an admissible representation then so is $(\hat{\pi}, \hat{V})$, and π is isomorphic to the contragredient of $\hat{\pi}$.*

Proof This follows immediately from Propositions 9 and 10, because each V_ρ is finite dimensional, and so therefore is $\hat{V}_\rho$, and V_ρ is the dual space of $\hat{V}_\rho$. □

Let $\mathcal{H}$ be the space of all locally constant compactly supported functions on G. It is easy to see that a compactly supported function is locally constant if and only if it is constant on the cosets some open subgroup K. Therefore

$$\mathcal{H} = \bigcup \mathcal{H}_K$$

where K runs through the open compact subgroups of G; we may choose any cofinal family of subsets, for example the normal open subgroups of K° for some fixed maximal compact subgroup K°.

Although $\mathcal{H}$ is a ring under convolution, it does not have a unit. Rather it is an *idempotented algebra*, which is a ring with a family of idempotents that substitutes for the unit. Let us explain this point.

If R is a ring and e an idempotent, then eRe is a 2-sided ideal in which e serves as a unit. Let R be a ring and let E be a set of idempotents on R. We may define a partial order on E by writing $e \geqslant f$ if $f \in eRe$. We assume that E is a directed set with this order and that

$$R = \bigcup_{e \in E} eRe.$$

Then we call R an *idempotented ring*. It is clear that $\mathcal{H}$ is an idempotented algebra, and we give another example in the following exercises.

Exercise 6 Let G be a compact group, and let (π, V) be a finite-dimensional irreducible representation. Recall that a *matrix coefficient* of π is a function of the form $g \mapsto \langle \pi(g)v, \hat{v} \rangle$ with $v \in V$ and $\hat{v} \in \hat{V}$. Prove Schur orthogonality for matrix coefficients in the form

$$\int_G \langle \pi(g)v, \hat{v} \rangle \langle \pi(g^{-1})w, \hat{w} \rangle \, dg = \frac{1}{\dim(V)} \langle v, \hat{w} \rangle \langle w, \hat{v} \rangle,$$

where Haar measure is normalized so that G has total volume 1.

Hint: With $\hat{v}, w$ fixed define a map $T : V \longrightarrow V$ by

$$T(x) = \int_G \langle \pi(g)x, \hat{v} \rangle \pi(g^{-1})w \, dg.$$

Show that $T(\pi(g)x) = \pi(g)T(x)$ and deduce that there is some scalar c such that

$$\int_G \langle \pi(g)x, \hat{v} \rangle \pi(g^{-1})w \, dg = c(w, \hat{v})x$$

for all $v \in V$. The integral is $c(w, \hat{v})\langle v, \hat{w} \rangle$. But it is also $c(v, \hat{w})\langle w, \hat{v} \rangle$. Thus $c(w, \hat{v}) = c\langle w, \hat{v} \rangle$ for some constant c. To evaluate c, let $v_1, \cdots, v_d$ be a basis of V and let $\widehat{v_1}, \cdots, \hat{v}_d$ be the dual basis of $\hat{V}$. Note that the trace of $\pi(g)$ is $\sum_i \langle \pi(g)v_i, \widehat{v_i} \rangle$, and compute $\int_G \operatorname{tr}(g) \operatorname{tr}(g^{-1}) \, dg$ in two different ways.

Exercise 7 Let $\mathcal{R}_\pi$ be the space of matrix coefficients of an irreducible representation (π, V) of the compact group G and let $d = \dim(V)$. We have a bilinear maps $V \times \hat{V} \longrightarrow \operatorname{End}_{\mathbb{C}}(V)$ and $V \times \hat{V} \longrightarrow \mathcal{R}_\pi$ as follows. The first map sends

$v \otimes \hat{v}$ to the rank one linear transformation $f_{v,\hat{v}} \in \mathrm{End}(V)$ and the second maps $v \otimes \hat{v}$ to the matrix coefficient $\phi_{v,\hat{v}}(g)$, where

$$f_{v,\hat{v}}(x) = \frac{1}{d}\langle x, \hat{v}\rangle v, \qquad \phi_{v,\hat{v}}(g) = \langle \pi(g)v, \hat{v}\rangle.$$

Show that

$$f_{v,\hat{v}} \circ f_{w,\hat{w}} = \frac{1}{d}\langle w, \hat{v}\rangle f_{v,\hat{w}}, \qquad \phi_{w,\hat{w}} * \phi_{v,\hat{v}} = \frac{1}{d}\langle w, \hat{v}\rangle \phi_{v,\hat{w}}.$$

Conclude that $\mathcal{R}_\pi$ is isomorphic to the opposite ring of $\mathrm{End}(V)$.

Exercise 8 Let G be any compact group. Let $f \in C(G)$. Show that the following are equivalent:

(i) The space of left translates of f spans a finite-dimensional vector space.

(ii) The space of right translates of f spans a finite-dimensional vector space.

(iii) There exists a finite-dimensional representation (π, V) of G with a vector $v_0 \in V$ and a linear functional L on V such that $f(g) = L(\pi(g)v_0)$.

Hint: To prove (i) $\Rightarrow$ (iii), we may take V to be the space of functions spanned by left-translates of f with the action $\pi(g)v(x) = v(g^{-1}x)$ with $v_0 = f$ and $L(v) = v(1)$.

Now let $\mathcal{R}$ be the space of functions that satisfy (i),(ii) and (iii). It is an algebra under convolution. Show that

$$\mathcal{R} = \bigoplus \mathcal{R}_\pi \qquad (\text{algebraic direct sum}),$$

where π runs through the irreducible representations of G. Show that $\mathcal{R}$ is an idempotented algebra.

If K is a compact open subgroup, let ε_K be $\frac{1}{\mathrm{vol}(K)}$ times the characteristic function of K. Then the set of such $\{\varepsilon_K\}$ forms a directed set of idempotents and $\mathcal{R}$ is an idempotented ring.

Recall that if (π, V) is a smooth representation of G and $\phi \in \mathcal{H}$ then

$$\pi(g)v = \int_G \phi(g)\pi(g)v \; dg.$$

This integral reduces to a finite sum for the following reason. We may find an open subgroup $K \in V^K$, and we may choose K such that ϕ is constant on the cosets γK. Choosing representatives $\gamma_1, \cdots, \gamma_N$ for the finite number of cosets such that $\phi(\gamma K) \neq 0$, the integral equals

$$\mathrm{vol}(K) \sum_{i=1}^{N} \phi(\gamma_i)\pi(\gamma_i)v.$$

We now may give the proof of Theorem 1, whose statement we recall.

Theorem 1. *(i) If (π, V) is an irreducible representation and $V^K \neq 0$, then V^K is a simple $\mathcal{H}_K$-module.*

(ii) If (π, V) and (σ, W) are irreducible admissible representations and $V^K \cong W^K$ as $\mathcal{H}_K$-modules, and $V^K \neq 0$, then π and σ are equivalent representations.

Proof The proof is the same as that of Theorem 2.

We prove (i). If V is irreducible and $0 \neq U \subset V^K$ is a nonzero submodule, we claim $U = V^K$. It is sufficient to show $\mathcal{H}_K u = V^K$ for a given nonzero $u \in \mathcal{H}_K$. Let $v \in V^K$. Since V is irreducible, we may find $\psi \in \mathcal{H}$ such that $\pi(\psi)u = v$; indeed, $\{\pi(\psi)u | \psi \in \mathcal{H}\}$ is a nonzero invariant subspace, hence all of V. Now consider $\phi = \varepsilon_K * \psi * \varepsilon_K \in \mathcal{H}_K$. We have $\pi(\varepsilon_K)u = u$ and $\pi(\varepsilon_K)v = v$ since $u, v \in V^K$. Now

$$\pi(\phi)u = \pi(\varepsilon_K)\pi(\psi)\pi(\varepsilon_K)u = \pi(\varepsilon_K)\pi(\psi)u = \pi(\varepsilon_K)v = v,$$

proving that $v \in \mathcal{H}_K u$.

We prove (ii). Suppose that V^K and W^K are isomorphic as $\mathcal{H}_K$-modules, with V and W irreducible G-modules.

Let $\lambda : V^K \longrightarrow W^K$ denote an isomorphism. Let $l : W^K \longrightarrow \mathbb{C}$ be a nonzero linear functional and let $w \in W^K$ be a vector such that $l(w) \neq 0$. We claim that there exists $\hat{w} \in \hat{W}^K$ such that $l(x) = \langle x, \hat{w} \rangle$ when $x \in W^K$. Indeed, we extend the functional l to an arbitrary smooth functional $\hat{w}_1$, then take $\hat{w} = \hat{\sigma}(\varepsilon_K)$, and if $x \in W^K$ then

$$\langle x, \hat{w} \rangle = \frac{1}{\mathrm{vol}(K)} \int_K \langle x, \hat{\sigma}(k) w_1 \rangle \, dk = \frac{1}{\mathrm{vol}(K)} \int_K \langle \sigma(k)x, w_1 \rangle \, dk = l(x).$$

Similarly we may find $\hat{v} \in \hat{V}^K$ such that $l(\lambda(x)) = \langle x, \hat{v} \rangle$ for $x \in V^K$. Let $v \in V^K$ be the unique vector such that $\lambda(v) = w$. We will show that if $\phi \in \mathcal{H}$ then

$$\langle \pi(\phi)v, \hat{v} \rangle = \langle \sigma(\phi)w, \hat{w} \rangle. \tag{13}$$

If $\phi \in \mathcal{H}_K$, then we have

$$\langle \pi(\phi)v, \hat{v} \rangle = l(\lambda(\pi(\phi)v)) = l(\sigma(\phi)\lambda(v)) = l(\sigma(\phi)w) = \langle \sigma(\phi)w, \hat{w} \rangle.$$

The general case follows from the following consideration. Let $\phi \in \mathcal{H}$ and let $\phi' = \varepsilon_K * \phi * \varepsilon_K$. Then

$$\langle \pi(\phi')v, \hat{v} \rangle = \langle \pi(\varepsilon_K)\pi(\phi)\pi(\varepsilon_K)v, \hat{v} \rangle = \langle \pi(\phi)\pi(\varepsilon_K)v, \hat{\pi}(\varepsilon_K)\hat{v} \rangle = \langle \pi(\phi)v, \hat{v} \rangle,$$

and similarly $\langle \sigma(\phi')w, \hat{w}\rangle = \langle \sigma(\phi)w, \hat{w}\rangle$. Thus the general case of (13) follows from the special case that is already proved.

Now let $L \subset K$ be a smaller compact open subgroup. Since V^L and W^L are finite-dimensional simple $\mathcal{H}_L$-modules we may apply Proposition 2 and conclude that, then $V^L \cong W^L$ as $\mathcal{H}_L$-modules. This isomorphism λ_L is uniquely determined up; it is determined up to scalar by Schur's Lemma, and the scalar is determined if we require that the isomorphism agree with λ on $V^K \subset V^L$. Now if L' is another compact open subgroup of K, then the isomorphism λ_L and $\lambda_{L'}$ must agree on $V^L \cap V^{L'}$ because they agree with $\lambda_{L\cap L'}$ on $V^{L\cap L'} \supset V^L \cap V^{L'}$. Therefore these isomorphisms may be patched together to get an $\mathcal{H}$-module isomorphism $V \longrightarrow W$. It is a G-module isomorphism since $\pi(g)v = \pi(\phi)v$ agrees with $\pi(\phi)v$ if ϕ is any function supported on a sufficiently small neighborhood of v such that $\int_G \phi = 1$, so the action of $\mathcal{H}$ determines the action of G on any admissible module. $\square$

4 Root Systems and Weyl Groups

Before we can discuss more interesting Hecke algebras, we need a portion of the theory of roots systems, and the theory of Coxeter groups. A root system and its Weyl group may be found in any group of Lie type. In this section, we will study the Weyl group by its action on the roots, and finally prove that the Weyl group is a Coxeter group. Many of the facts that we prove along the way are standard, useful properties of Weyl groups and root systems.

Let V be a Euclidean space, that is, a real vector space with an inner product $\langle\ ,\ \rangle$ that is symmetric and positive definite. If $0 \neq \alpha \in V$ is a nonzero vector, then the reflection in the hyperplane perpendicular to α is the map $r_\alpha : V \longrightarrow V$ given by

$$r_\alpha(x) = x - \frac{2\langle \alpha, x\rangle}{\langle \alpha, \alpha\rangle}\alpha. \tag{14}$$

By a *root system* we mean a nonempty finite set $\Phi \subset V$ of nonzero vectors such that if $\alpha \in \Phi$ then $r_\alpha(\Phi) = \Phi$, and such that if $\alpha, \beta \in \Phi$ then $\frac{2\langle \alpha,\beta\rangle}{\langle \alpha,\alpha\rangle} \in \mathbb{Z}$. Note that if $\alpha \in \Phi$ then $-\alpha = r_\alpha(\alpha)$, so the axioms imply that $-\alpha \in \Phi$.

If $\alpha, \beta \in \Phi$ and $\alpha = \lambda\beta$ for $\lambda \in \mathbb{R}$ implies that $\lambda = \pm 1$, then Φ is called *reduced*. We will mainly deal with reduced root systems.

We do not assume that V is spanned by the roots. Let V_0 be the vector subspace spanned by Φ. Then $\dim(V_0)$ is called the *rank* of Φ.

The root system is called *reducible* if we can write $V = V_1 \oplus V_2$, an orthogonal direct sum, such that $\Phi = \Phi_1 \cup \Phi_2$, with Φ_1 and Φ_2 root systems in V_i. The irreducible root systems were classified by Cartan, and lie in four infinite families A_r, B_r, C_r, D_r with five *exceptional* root systems G_2, F_4, E_6, E_7, E_8. The subscript in every case is the rank.

If the vectors are all of the same length, then Φ is called *simply-laced*. The simply-laced Cartan types are A_r, D_r and E_r. A reduced irreducible root system that is not simply-laced always has roots of exactly two different lengths.

If $V = \mathbb{R}^k$ and $1 \leqslant i \leqslant k$ let $\boldsymbol{e}_i$ denote the i-th standard basis vector $(0, \cdots, 1, \cdots, 0)$ with the 1 in the i-th position.

Example 1 Let $V = \mathbb{R}^{r+1}$, and let Φ consist of the $r(r+1)$ vectors $\alpha_{i,j} = \boldsymbol{e}_i - \boldsymbol{e}_j$ with $i \neq j$. For example if $r = 2$ then

$$\Phi = \{(1,-1,0), (0,1,-1), (1,0,-1), (-1,1,0), (0,-1,1), (-1,0,1)\}.$$

This is the root system of Cartan type A_r. As a variant, we may take V to be the hyperplane consisting of all $x \in \mathbb{R}^{r+1}$ such that $x = (x_1, \cdots, x_{r+1})$ and $\sum x_i = 0$, with the same root system Φ.

Example 2 Let $V = \mathbb{R}^r$, and let Φ consist of $2r^2$ vectors to be described. The long roots are the vectors

$$\pm\boldsymbol{e}_i \pm \boldsymbol{e}_j, \qquad i \neq j.$$

The short roots are the vectors

$$\pm e_i.$$

This Cartan type is called B_r. In this example it is assumed that $r \geqslant 2$.

Example 3 Let $V = \mathbb{R}^r$, and let Φ consist of $2r^2$ vectors to be described. The short roots are the vectors

$$\pm\boldsymbol{e}_i \pm \boldsymbol{e}_j, \qquad i \neq j.$$

The long roots are the vectors

$$\pm 2\boldsymbol{e}_i.$$

This Cartan type is called C_r. In this example it is assumed that $r \geqslant 2$.

Example 4 Let $V = \mathbb{R}^r$ and let Φ consist of the $2r(r-1)$ vectors

$$\pm \boldsymbol{e}_i \pm \boldsymbol{e}_j, \qquad i \neq j.$$

This is the Cartan type D_r.

We will not describe the exceptional Cartan types, but you may get access to any information you want about them if you are running Sage.

Let V be a Euclidean space, $\Phi \subset V$ a reduced root system. Since Φ is a finite set of nonzero vectors, we may choose $\rho_0 \in V$ such that $\langle \alpha, \rho_0 \rangle \neq 0$ for all $\alpha \in \Phi$. Let Φ^+ be the set of roots α such that $\langle \alpha, \rho_0 \rangle > 0$. This consists of exactly half the roots, since evidently a root $\alpha \in \Phi^+$ if and only if $-\alpha \notin \Phi^+$. Elements of Φ^+ are called *positive roots*. Elements of set $\Phi^- = \Phi - \Phi^+$ are called *negative roots*.

If α, $\beta \in \Phi^+$ and $\alpha + \beta \in \Phi$, then evidently $\alpha + \beta \in \Phi^+$. Let Σ be the set of elements in Φ^+ that cannot be expressed as a sum of other elements of Φ^+. If $\alpha \in \Sigma$, then we call α a *simple positive root*, and we will denote r_α as s_α in this case. We will reserve the notation s_α for the case where α is a simple positive root. If $\alpha \in \Sigma$ we call s_α a *simple reflection*.

Proposition 12 *(i) The elements of Σ are linearly independent.*

(ii) If $\alpha \in \Sigma$ and $\beta \in \Phi^+$ then either $\beta = \alpha$ or $s_\alpha(\beta) \in \Phi^+$.

(iii) If α and β are distinct elements of Σ then $\langle \alpha, \beta \rangle \leqslant 0$.

(iv) Every element $\alpha \in \Phi$ can be expressed uniquely as a linear combination

$$\alpha = \sum_{\beta \in \Sigma} n_\beta \cdot \beta$$

in which each $n_\beta \in \mathbb{Z}$, and either all $n_\beta \geqslant 0$ (if $\beta \in \Phi^+$) or all $n_\beta \leqslant 0$ (if $\beta \in \Phi^-$).

Proof Let Σ' be a subset of Φ^+ that is minimal with respect to the property that every element of Φ^+ is a linear combination with nonnegative coefficients of elements of Σ'. (Subsets with this property clearly exists, for example Σ' itself.) We will eventually show that $\Sigma' = \Sigma$.

First we show that if $\alpha \in \Sigma'$ and $\beta \in \Phi^+$, then either $\beta = \alpha$ or $r_\alpha(\beta) \in \Phi^+$. If not, then $-r_\alpha(\beta) \in \Phi^+$, and

$$2\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\alpha = \beta + (-r_\alpha(\beta))$$

is a sum of two positive roots β and $-r_\alpha(\beta)$. Both β and $-r_\alpha(\beta)$ can be expressed as linear combinations of the elements of Σ' with nonnegative coefficients, and therefore

$$2\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\alpha = \sum_{\gamma\in\Sigma'} n_\gamma\cdot\gamma, \qquad n_\gamma \geqslant 0.$$

Write

$$\left(2\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle} - n_\alpha\right)\alpha = \sum_{\substack{\gamma\,\in\,\Sigma'\\ \gamma\,\neq\,\alpha}} n_\gamma\cdot\gamma.$$

Because $\beta \neq \alpha$, and because Φ is assumed to be reduced, β is not a multiple of α. Therefore at least one of the coefficients n_γ with $\gamma \neq \alpha$ is positive. Taking the inner product with ρ_0 shows that the coefficient on the left is strictly positive; dividing by this positive constant, we see that α may be expressed as a linear combination of the elements $\gamma \in \Sigma'$ distinct from α, and so α may be omitted from Σ', contradicting its assumed minimality. This contradiction shows that $r_\alpha(\beta) \in \Phi^+$.

Next we show that if α and β are distinct elements of Σ' then $\langle\alpha,\beta\rangle \leqslant 0$. We have already shown that $r_\alpha(\beta) \in \Phi^+$. If $\langle\alpha,\beta\rangle > 0$, then write

$$\beta = r_\alpha(\beta) + 2\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\alpha. \tag{15}$$

Writing $r_\alpha(\beta)$ as a linear combination with nonnegative coefficients of the elements of Σ', and noting that the coefficient of α on the right side of (15) is strictly positive, we may write

$$\beta = \sum_{\gamma\in\Sigma'} n_\gamma\cdot\gamma$$

where $n_\alpha > 0$. We rewrite this

$$(1-n_\beta)\cdot\beta = \sum_{\substack{\gamma\,\in\,\Sigma'\\ \gamma\,\neq\,\beta}} n_\gamma\cdot\gamma.$$

At least one coefficient, $n_\alpha > 0$ on the right, so taking the take the inner product with ρ_0 we see that $1 - n_\beta > 0$. Thus β is a linear combination with nonnegative coefficients of other elements of Σ', hence may be omitted, contradicting the minimality of Σ'.

Now let us show that the elements of Σ' are $\mathbb{R}$-linearly independent. In a relation of algebraic dependence we move all the negative coefficients to the other side of the identity, and obtain a relation of the form

$$\sum_{\alpha \in \Sigma_1} c_\alpha \cdot \alpha = \sum_{\beta \in \Sigma_2} d_\beta \cdot \beta, \tag{16}$$

where Σ_1 and Σ_2 are disjoint subsets of Σ', and the coefficients $c_\alpha,\ d_\beta$ are all positive. Call this vector v. We have

$$\langle v, v \rangle = \sum_{\substack{\alpha \in \Sigma_1 \\ \beta \in \Sigma_2}} c_\alpha d_\beta \langle \alpha, \beta \rangle \leqslant 0.$$

since we have already shown that the inner products $\langle \alpha, \beta \rangle \leqslant 0$. Therefore $v = 0$. Now taking the inner product of the left side in (16) with ρ_0 gives

$$0 = \sum_{\alpha \in \Sigma_1} c_\alpha \langle \alpha, \rho_0 \rangle,$$

and since $\langle \alpha, \rho_0 \rangle > 0$, $c_\alpha > 0$, this is a contradiction. This proves the linear independence of the elements of Σ'.

Next let us show that every element of Φ^+ may be expressed as a linear combination of elements of Σ' with *integer* coefficients. We define a function h from Φ^+ to the positive real numbers as follows. If $\alpha \in \Phi^+$ we may write

$$\alpha = \sum_{\beta \in \Sigma'} n_\beta \cdot \beta, \qquad n_\beta \geqslant 0.$$

The coefficients n_β are uniquely determined since the elements of Σ' are linearly independent. We define

$$h(\alpha) = \sum n_\beta. \tag{17}$$

Evidently $h(\alpha) > 0$. We want to show that the coefficients n_β are integers. Assume a counterexample with $h(\alpha)$ minimal. Evidently $\alpha \notin \Sigma'$, since if

$\alpha \in \Sigma'$, then $n_\alpha = 1$ while all other $n_\beta = 0$, so such an α has all $n_\beta \in \mathbb{Z}$. Since

$$0 < \langle \alpha, \alpha \rangle = \sum_{\beta \in \Sigma'} n_\beta \langle \alpha, \beta \rangle \tag{18}$$

it is impossible that $\langle \alpha, \beta \rangle \leqslant 0$ for all $\beta \in \Sigma'$. Thus there exists $\gamma \in \Sigma'$ such that $\langle \alpha, \gamma \rangle > 0$. Then by what we have already proved, $\alpha' = r_\gamma(\alpha) \in \Phi^+$, and by (14) we see that

$$\alpha' = \sum_{\beta \in \Sigma'} n'_\beta \cdot \beta,$$

where

$$n'_\beta = \begin{cases} n_\beta & \text{if } \beta \neq \gamma; \\ n_\gamma - 2\frac{\langle \gamma, \alpha \rangle}{\langle \gamma, \gamma \rangle} & \text{if } \beta = \gamma. \end{cases}$$

Since $\langle \gamma, \alpha \rangle > 0$, we have

$$h(\alpha') < h(\alpha)$$

so by induction we have $n'_\beta \in \mathbb{Z}$. Since Φ is a root system, $2\langle \gamma, \alpha \rangle / \langle \alpha, \alpha \rangle \in \mathbb{Z}$, so $n_\beta \in \mathbb{Z}$ for all $\beta \in \Sigma'$. This is a contradiction.

Finally, let us show that $\Sigma = \Sigma'$.

If $\alpha \in \Sigma$, then by definition of Σ, α cannot be expressed as a linear combination with integer coefficients of other elements of Φ^+. Hence α cannot be omitted from Σ'. Thus $\Sigma \subset \Sigma'$.

On the other hand if $\alpha \in \Sigma'$, then we claim that $\alpha \in \Sigma$. If not, then we may write $\alpha = \beta + \gamma$ with β, $\gamma \in \Phi^+$, and β and γ may both be written as linear combinations of elements of Σ' with positive integer coefficients, and thus $h(\beta)$, $h(\gamma) \geqslant 1$; so $h(\alpha) = h(\beta) + h(\gamma) > 1$. But evidently $h(\alpha) = 1$ since $\alpha \in \Sigma'$. This contradiction shows that $\Sigma' \subset \Sigma$. □

Let W be the *Weyl group* generated by the simple reflections s_α with $\alpha \in \Sigma$. Our goal is to show that W and the set of simple reflections form a Coxeter group. We will show that the r_α with $\alpha \in \Phi$ are all conjugates of the s_α with $\alpha \in \Sigma$.

We now introduce the important *length function* on W. We will give two definitions, and eventually show they are the same.

If $w \in W$, let the length $l(w)$ be defined to be the smallest k such that w admits a factorization $w = s_1 \cdots s_k$ into simple reflections, or $l(w) = 0$ if $w = 1$. Let $l'(w)$ be the number of $\alpha \in \Phi^+$ such that $w(\alpha) \in \Phi^-$. We will eventually show that the functions l and l' are the same.

Proposition 13 *Let $s = s_\alpha$ ($\alpha \in \Sigma$) be a simple reflection and let $w \in W$. Then*

$$l'(sw) = \begin{cases} l'(w) + 1 & \text{if } w^{-1}(\alpha) \in \Phi^+; \\ l'(w) - 1 & \text{if } w^{-1}(\alpha) \in \Phi^-, \end{cases} \tag{19}$$

and

$$l'(ws) = \begin{cases} l'(w) + 1 & \text{if } w(\alpha) \in \Phi^+; \\ l'(w) - 1 & \text{if } w(\alpha) \in \Phi^-. \end{cases} \tag{20}$$

Proof By Proposition 12, $s(\Phi^-)$ is obtained from Φ^- by deleting $-\alpha$ and adding α. So $(sw)^{-1}\Phi^- = w^{-1}(s\Phi^-)$ is obtained from $w^{-1}\Phi^-$ by deleting $-w^{-1}(\alpha)$ and adding $w^{-1}(\alpha)$. Since $l'(w)$ is the cardinality of $\Phi^+ \cap w^{-1}\Phi^-$, we obtain (19). To prove (20), we note that $l'(ws)$ is the cardinality of $\Phi^+ \cap (ws)^{-1}\Phi^-$, which equals the cardinality of $s(\Phi^+ \cap (ws)^{-1}\Phi^-) = s\Phi^+ \cap w^{-1}\Phi^-$, and since $s\Phi^+$ is obtained from Φ^+ by deleting the element α and adjoining $-\alpha$, (20) is evident. □

If w is any orthogonal linear endomorphism of V, then evidently $wr_\alpha w^{-1}$ is the reflection in the hyperplane perpendicular to $w(\alpha)$:

$$wr_\alpha w^{-1} = r_{w(\alpha)}. \tag{21}$$

We now come to the famous *exchange property*, which is a fundamental property of Coxeter groups.

Proposition 14 (Exchange Property) *Suppose that $s_1, \cdots, s_k$ and s are simple reflections. Let $w = s_1 \cdots s_k$ and suppose that $l(ws) < l(w)$. Then there exists a $1 \leqslant j \leqslant k$ such that*

$$s_1 s_2 \cdots s_k = s_1 s_2 \cdots \hat{s}_j \cdots s_k s_\alpha, \tag{22}$$

where the "hat" on the right signifies the omission of s_j.

Although we only prove this for Weyl groups, see Humphreys, *Reflection Groups and Coxeter Groups*, Section 5.8 for general Coxeter groups.

Proof Let $s = s_\alpha$ where $\alpha \in \Sigma$. By Proposition 13 $s_1 \cdots s_k(\alpha) \in \Phi^-$. Thus there is a minimal $1 \leqslant j \leqslant k$ such that $s_{j+1} \cdots s_k(\alpha) \in \Phi^+$. Therefore $s_j s_{j+1} \cdots s_k(\alpha) \in \Phi^-$. Since α_j is the unique element of Φ^+ mapped into Φ^- by s_j, we have

$$s_{j+1} \cdots s_k(\alpha) = \alpha_j,$$

and by (21) we have

$$(s_{j+1}\cdots s_k)s_\alpha(s_{j+1}\cdots s_k)^{-1} = s_j,$$

or

$$s_{j+1}\cdots s_k s = s_j s_{j+1}\cdots s_k.$$

This implies (22). □

Proposition 15 *Suppose that $\alpha_1, \cdots, \alpha_k$ are elements of Σ and let $s_i = s_{\alpha_i}$. Suppose that $l'(s_1 s_2 \cdots s_k) < k$. Then there exist $1 \leqslant i < j \leqslant k$ such that*

$$s_1 s_2 \cdots s_k = s_1 s_2 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_k, \tag{23}$$

where the "hats" on the right signify omission of the elements s_i and s_j.

Proof Evidently there is a first j such that $l'(s_1 s_2 \cdots s_j) < j$, and (since $l'(s_1) = 1$) we have $j > 1$. Then $l'(s_1 s_2 \cdots s_{j-1}) = j - 1$, and by Proposition 13, we have $s_1 s_2 \cdots s_{j-1}(\alpha_j) \in \Phi^-$. The existence of i satisfying $s_1 \cdots s_{j-1} = s_1 \cdots \hat{s}_i \cdots s_{j-1} s_j$ now follows from Proposition 14, which implies (23). □

We can now prove that the two definitions of the length function agree.

Proposition 16 *If $w \in W$ then $l(w) = l'(w)$.*

Proof The inequality

$$l'(w) \leqslant l(w)$$

follows from Proposition 14 because we may write $w = sw_1$ where s is a simple reflection and $l(w_1) = l(w) - 1$, and by induction on $l(w_1)$ we may assume that $l'(w_1) \leqslant l(w_1)$, so $l'(w) \leqslant l'(w_1) + 1 \leqslant l(w_1) + 1 = l(w)$.

Let us show that

$$l'(w) \geqslant l(w).$$

Indeed, let $w = s_1 \cdots s_k$ be a counterexample with $l(w) = k$, where each $s_i = s_{\alpha_i}$ with $\alpha_i \in \Sigma$. Thus $l'(s_1 \cdots s_k) < k$. Then by Proposition 15 there exist i and j such that

$$w = s_1 s_2 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_k.$$

This expression for w as a product of $k-2$ simple reflections contradicts our assumption that $l(w) = k$. □

Proposition 17 *The function $w \longmapsto (-1)^{l(w)}$ is a character of W.*

Proof A reflection, as an endomorphism of V, has eigenvalue -1 with multiplicity 1 and eigenvalue 1 with multiplicity $\dim(V) - 1$. Therefore $\det(r_\alpha) = -1$ for every reflection. In particular, $\det(s_\alpha) = -1$ for every simple reflection. Writing $w \in W$ as a product of $l(w)$ simple reflections, we see that $\det(w) = (-1)^{l(w)}$, and so this is a character. □

Proposition 18 *If $w(\Phi^+) = \Phi^+$ then $w = 1$.*

Proof If $w(\Phi^+) = \Phi^+$, then $l'(w) = 0$, so $l(w) = 0$, that is, $w = 1$. □

Proposition 19 *If $\alpha \in \Phi$, there exists an element $w \in W$ such that $w(\alpha) \in \Sigma$.*

Proof First assume that $\alpha \in \Phi^+$. We will argue by induction on $h(\alpha)$, which is defined by (17). In view of Proposition 12 (iv), we know that $h(\alpha)$ is a positive integer, and if $\alpha \notin \Sigma$ (which we may as well assume) then $h(\alpha) > 1$. As in the proof of Proposition 12, (18) implies that $\langle \alpha, \beta \rangle > 0$ for some $\beta \in \Sigma$, and then with $\alpha' = s_\beta(\alpha)$ we have $h(\alpha') < h(\alpha)$. On the other hand $\alpha' \in \Phi^+$ since $\alpha \neq \beta$, by Proposition 12 (ii). By our inductive hypothesis, $w'(\alpha') \in \Sigma$ for some $w' \in W$. Then $w(\alpha) = w'(\alpha')$ with $w = w's_\beta \in W$. This shows that if $\alpha \in \Phi^+$ then there exists $w \in W$ such that $w(\alpha) \in \Sigma$.

If on the other hand $\alpha \in \Phi^-$, then $-\alpha \in \Phi^+$ so we may find $w_1 \in W$ such that $w_1(-\alpha) \in \Sigma$, so if $w_1(-\alpha) = \beta$, then $w(\alpha) = \beta$ with $w = s_\beta w_1$.

In both cases $w(\alpha) \in \Sigma$ for some $w \in W$. □

Proposition 20 *The group W contains r_α for every $\alpha \in \Phi$.*

Proof Indeed, $w(\alpha) \in \Sigma$ for some $w \in W$, so $r_{w(\alpha)} \in W$, and r_α is conjugate in W to $s_{w(\alpha)}$ by (21). Therefore $r_\alpha \in W$. □

Proposition 21 *The group W is finite.*

Proof By Proposition 18, $w \in W$ is determined by $w(\Phi^+) \subset \Phi$. Since Φ is finite, W is finite. □

Proposition 22 *Suppose that $w \in W$ such that $l(w) = k$. Write $w = s_1 \cdots s_k$, where $s_i = s_{\alpha_i}$, $\alpha_1, \cdots, \alpha_k \in \Sigma$. Then*

$$\{\alpha \in \Phi^+ | w(\alpha) \in \Phi^-\} = \{\alpha_k, s_k(\alpha_{k-1}), s_k s_{k-1}(\alpha_{k-2}), \cdots, s_k s_{k-1} \cdots s_2(\alpha_1)\}.$$

Proof By Proposition 16, the cardinality of $\{\alpha \in \Phi^+ | w(\alpha) \in \Phi^-\}$ is k, so the result will be established if we show that the described elements are distinct and in the set. Let $w = s_1 w_1$ where $w_1 = s_2 \cdots s_k$, so that $l(w_1) = l(w) - 1$. By induction we have

$$\{\alpha \in \Phi^+ | w_1(\alpha) \in \Phi^-\} = \{\alpha_k, s_k(\alpha_{k-1}), s_k s_{k-1}(\alpha_{k-2}), \cdots, s_k s_{k-1} \cdots s_3(\alpha_2)\},$$

and the elements on the right are distinct. We claim that

$$\{\alpha \in \Phi^+ | w_1(\alpha) \in \Phi^-\} \subset \{\alpha \in \Phi^+ | s_1 w_1(\alpha) \in \Phi^-\}. \tag{24}$$

If not, let $\alpha \in \Phi^+$ such that $w_1(\alpha) \in \Phi^-$ while $s_1 w_1(\alpha) \in \Phi^+$. Let $\beta = -w_1(\alpha)$. Then $\beta \in \Phi^+$ while $s_1(\beta) \in \Phi^-$. By Proposition 12 (ii), this implies that $\beta = \alpha_1$. Therefore $\alpha = -w_1^{-1}(\alpha_1)$. By Proposition 13, since $l(s_1 w_1) = k = l(w_1) + 1$, we have $-\alpha = w_1^{-1}(\alpha_1) \in \Phi^+$. This contradiction proves (24).

We will be done if we show that the last remaining element $s_k \cdots s_2(\alpha_1)$ is in $\{\alpha \in \Phi^+ | s_1 w_1(\alpha) \in \Phi^-\}$ but not $\{\alpha \in \Phi^+ | w_1(\alpha) \in \Phi^-\}$, since that will guarantee that it is distinct from the other elements listed. This is clear since if $\alpha = s_k \cdots s_2(\alpha_1)$, we have $w_1(\alpha) = \alpha_1 \notin \Phi^-$, while $s_1 w_1(\alpha) = -\alpha_1 \in \Phi^-$. □

Our goal is to show that W is a Coxeter group with $I = \{s_\alpha | \alpha \in \Sigma\}$. We will work with a larger (usually infinite) group B, the *braid group*. If $\alpha, \beta \in \Sigma$, let $n(\alpha, \beta)$ be the order of $s_\alpha s_\beta$. Then B is the group with generators u_α and *braid relations*

$$u_\alpha u_\beta u_\alpha u_\beta \cdots = u_\beta u_\alpha u_\beta u_\alpha \cdots$$

where there are $m(\alpha, \beta)$ factors on each side. (This differs from W since it is *not* true that $u_\alpha^2 = 1$.)

The braid relations are satisfied in W so there exists a homomorphism $B \longrightarrow W$ in which $u_\alpha \mapsto s_\alpha$. Let G be the group generated by elements t_α subject to the braid relations

$$t_\alpha t_\beta t_\alpha t_\beta \cdots = t_\beta t_\alpha t_\beta t_\alpha \cdots$$

and also the relations $t_\alpha^2 = 1$. Thus we have homomorphisms $B \longrightarrow G \longrightarrow W$ such that $u_\alpha \longrightarrow t_\alpha \longrightarrow s_\alpha$. We want to show that the last homomorphism $G \longrightarrow W$ is an isomorphism, which will show that W satisfies the definition of a Coxeter group.

Proposition 23 (Tits) *Let $w \in W$ such that $l(w) = k$. Let $s_1 \cdots s_k = s'_1 \cdots s'_k$ be two decompositions of w into products of simple reflections, where $s_i = s_{\alpha_i}$ and $s'_i = s_{\beta_i}$, for simple roots α_i and β_j. Let $u_i = u_{\alpha_i}$ and $u'_i = u_{\beta_i}$ be the corresponding elements of B, and let $t_i = t_\alpha$ and $t'_i = t_{\beta_i}$ be the corresponding elements of G. Then $u_1 \cdots u_k = u'_1 \cdots u'_k$ and $t_1 \cdots t_k = t'_1 \cdots t'_k$.*

Proof The proof is identical for the braid group and the Coxeter group. We prove this for the braid group.

Let us assume that we have a counterexample of shortest length. Thus $l(s_1 \cdots s_k) = k$ and

$$s_1 \cdots s_k = s'_1 \cdots s'_k \quad \text{but} \quad u_1 \cdots u_k \neq u'_1 \cdots u'_k. \tag{25}$$

We will show that

$$s_2 s_3 \cdots s_k s'_k = s_1 \cdots s_k \quad \text{but} \quad u_2 u_3 \cdots u_k u'_k \neq u_1 \cdots u_k. \tag{26}$$

Before we prove this let us explain how it implies the Proposition. The W element in (26) is w and thus has length k, so we may repeat the process, obtaining

$$s_3 s_4 \cdots s_k s'_k s_k = s_2 s_3 \cdots s_k s'_k \quad \text{but} \quad u_3 u_4 \cdots u_k u'_k u_k \neq u_2 u_3 \cdots u_k u'_k.$$

Repeating the process, we eventually obtain

$$\cdots s'_k s_k s'_k s_k = \cdots s_k s'_k s_k s'_k \quad \text{but} \quad \cdots u'_k u_k u'_k u_k \neq \cdots u_k u'_k u_k u'_k \tag{27}$$

Moving all the s's on the left together $(s'_k s_k)^k = 1$, so k is a multiple of $n(s_k, s'_k)$. Now (27) contradicts the braid relation.

It remains to prove (26). Note that $w s'_k = s'_1 \cdots s'_{k-1}$ has length $k-1$, so by Proposition 13 we have $w(\beta_k) \in \Phi^-$. Now by Proposition 14, we have

$$s_1 \cdots s_k = s_1 \cdots \hat{s}_i \cdots s_k s'_k \tag{28}$$

for some $1 \leqslant i \leqslant k$, where the hat denotes an omitted element. Using (25)

$$s_1 \cdots \hat{s}_i \cdots s_k = s'_1 \cdots s'_{k-1},$$

and this element of W has length $k-1$. (If it had shorter length, multiplying on the right by s'_k would contradict the assumption that $l(w) = k$). By the minimality of the counterexample, we have

$$u_1 \cdots \hat{u}_i \cdots u_k = u'_1 \cdots u'_{k-1}. \tag{29}$$

We now claim that $i = 1$. Suppose $i > 1$. Cancel $s_1 \cdots s_{i-1}$ in (28) to obtain

$$s_i \cdots s_k = s_{i+1} \cdots s_k s'_k$$

and since $i > 1$, this has length $k - i + 1 < k$. By the minimality of the counterexample (25) we have

$$u_i \cdots u_k = u_{i+1} \cdots u_k u'_k.$$

We can multiply this identity on the left by $u_1 \cdots u_{i-1}$, then use (29) to obtain a contradiction to (25). This proves that $i = 1$.

Now (28) proves the first part of (26). As for the second part, suppose $u_2 \cdots u_{k-1} u'_k = u_1 \cdots u_k$. Then multiplying (29) on the right by u'_k gives a contradiction to (25) and (26) is proved. □

Theorem 6 *Let W be the Weyl group of the root system Φ, and let I be the set of simple reflections in W. Then (W, I) is a Coxeter group.*

Proof We have to show that the homomorphism $G \longrightarrow W$ is injective. Suppose that $t_1 \cdots t_n$ is in the kernel, where $t_i = t_{\alpha_i}$ for simple roots α_i. We will denote $s_i = s_{\alpha_i}$. We have $s_1 \cdots s_n = 1$, and we will show that $t_1 \cdots t_n = 1$.

It follows from Proposition 17 that n is even. Let $n = 2r$. Letting $s'_1 = s_n$, $s'_2 = s_{n-1}$, etc. and similarly $t'_i = t^{-1}_{n+1-i}$ when $1 \leqslant i \leqslant r$ we have

$$s_1 \cdots s_r = s'_1 \cdots s'_r$$

and we want to show that $t_1 \cdots t_r = t'_1 \cdots t'_r$. Suppose not; then

$$t_1 \cdots t_r \neq t'_1 \cdots t'_r. \tag{30}$$

We assume this counterexample minimizes r. By Proposition 23, we already have a contradiction unless $l(s_1 \cdots s_r) < r$. It follows from Proposition 15 that

$$s_1 \cdots \widehat{s_i} \cdots \widehat{s_j} \cdots s_r = s_1 \cdots s_r = s'_1 \cdots s'_r \tag{31}$$

for some i and j. Moving s'_r to the other side,

$$s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_r s'_r = s'_1 \cdots s'_{r-1},$$

and by the minimality of r we therefore have

$$t_1 \cdots \hat{t}_i \cdots \hat{t}_j \cdots t_r t'_r = t'_1 \cdots t'_{r-1}, \qquad \text{so} \qquad t_1 \cdots \hat{t}_i \cdots \hat{t}_j \cdots t_r = t'_1 \cdots t'_{r-1} t'_r.$$

It follows from (30) that

$$t_1 \cdots \hat{t}_i \cdots \hat{t}_j \cdots t_r \neq t_1 \cdots t_r. \tag{32}$$

Now comparing (31) and (32) we have

$$s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_r s_r = s_1 \cdots s_{r-1} \qquad \text{but} \qquad t_1 \cdots \hat{t}_i \cdots \hat{t}_j \cdots t_r t_r \neq t_1 \cdots t_{r-1},$$

where there are $r-1$ terms on both sides, again contradicting the minimality of r. □

A connected component of the complement of the union of the hyperplanes

$$\{x \in V | \langle x, \alpha \rangle = 0 \text{ for all } \alpha \in \Phi\}.$$

is called an *open Weyl chamber*. The closure of an open Weyl chamber is called a *Weyl chamber*. For example $\mathcal{C}_+ = \{x \in V | \langle x, \alpha \rangle \geqslant 0 \text{ for all } \alpha \in \Sigma\}$ is called the *positive Weyl chamber*. Since every element of Φ^+ is a linear combination of elements of $\mathcal{C}$ with positive coefficients, $\mathcal{C}_+ = \{x \in V | \langle x, \alpha \rangle \geqslant 0 \text{ for all } \alpha \in \Phi^+\}$. The interior

$$\mathcal{C}_+^\circ = \{x \in V | \langle x, \alpha \rangle > 0 \text{ for all } \alpha \in \Sigma\} = \{x \in V | \langle x, \alpha \rangle > 0 \text{ for all } \alpha \in \Phi^+\}$$

is an open Weyl chamber.

If $y \in V$ let $W(y)$ be the stabilizer $\{w \in W | w(y) = y\}$.

Proposition 24 *Suppose that $w \in W$ such that $l(w) = k$. Write $w = s_1 \cdots s_k$, where $s_i = s_{\alpha_i}$, $\alpha_1, \cdots, \alpha_k \in \Sigma$. Assume that $x \in \mathcal{C}_+$ such that $wx \in \mathcal{C}_+$ also.*

(i) We have $\langle x, \alpha_i \rangle = 0$ for $1 \leqslant i \leqslant k$.

(ii) Each $s_i \in W(x)$.

(iii) We have $w(x) = x$.

Proof If $\alpha \in \Phi^+$ and $w\alpha \in \Phi^-$ then we have $\langle x, \alpha \rangle = 0$. Indeed, $\langle x, \alpha \rangle \geqslant 0$ since $\alpha \in \Phi^+$ and $x \in \mathcal{C}_+$, and $\langle x, \alpha \rangle = \langle wx, w\alpha \rangle \leqslant 0$ since $wx \in \mathcal{C}_+$ and $w\alpha \in \Phi^-$.

The elements of $\{\alpha \in \Phi^+ | w\alpha \in \Phi^-\}$ are listed in Proposition 22. Since α_k is in this set, we have $s_k(x) = x - (2\langle x, \alpha_k\rangle/\langle \alpha_k, \alpha_k\rangle)\alpha_k = x$. Thus $s_k \in W(x)$. Now since $s_k(\alpha_{k-1}) \in \{\alpha \in \Phi^+ | w\alpha \in \Phi^-\}$, we have $0 = \langle x, s_k(\alpha_{k-1})\rangle = \langle s_k(x), \alpha_{k-1}\rangle = \langle x, \alpha_{k-1}\rangle$, which implies $s_{k-1}(x) = x - 2\langle x, \alpha_{k-1}\rangle/\langle \alpha_{k-1}, \alpha_{k-1}\rangle = x$. Proceeding in this way we prove (i) and (ii) simultaneously. Of course (ii) implies (iii). □

Theorem 7 *The set $\mathcal{C}_+$ is a fundamental domain for the action of W on V. More precisely, let $x \in V$.*

(i) There exists $w \in W$ such that $w(x) \in \mathcal{C}_+$.

(ii) If $w, w' \in W$ and $w(x) \in \mathcal{C}_+, w'(x) \in \mathcal{C}_+^\circ$ then $w = w'$.

(iii) If $w, w' \in W$ and $w(x) \in \mathcal{C}_+, w'(x) \in \mathcal{C}_+$ then $w(x) = w'(x)$.

Proof Let $w \in W$ be chosen so that the cardinality of $S = \{\alpha \in \Phi^+ | \langle w(x), \alpha\rangle < 0\}$ is as small as possible. We claim that S is empty. If not, then there exists an element of $\beta \in \Sigma \cap S$. We have $\langle w(x), -\beta\rangle > 0$, and since s_β preserves Φ^+ except for β, which it maps to $-\beta$, the set $S' = \{\alpha \in \Phi^+ | \langle w(x), s_\beta(\alpha)\rangle < 0\}$ is smaller than S by one. Since $S' = \{\alpha \in \Phi^+ | \langle s_\beta w(x), \alpha\rangle < 0\}$ this contradicts the minimality of $|S|$. Clearly $w(x) \in \mathcal{C}_+$. This proves (i).

We prove (ii). We may assume that $w' = 1$, so $x \in \mathcal{C}_+^\circ$. Since $\langle x, \alpha\rangle > 0$ for all $\alpha \in \Phi^+$ we have $\Phi^+ = \{\alpha \in \Phi | \langle x, \alpha\rangle > 0\} = \{\alpha \in \Phi | \langle x, \alpha\rangle \geqslant 0\}$. Since $w'(x) \in \mathcal{C}_+$, if $\alpha \in \Phi^+$ we have $\langle w^{-1}(\alpha), x\rangle = \langle \alpha, w(x)\rangle \geqslant 0$ so $w^{-1}(\alpha) \in \Phi^+$. By Proposition 18 this implies that $w^{-1} = 1$, whence (ii).

Part (iii) follows from Proposition 24 (iii). □

5 Dynkin Diagrams and Coxeter Groups

It is worth knowing that we can read off the Coxeter group presentation of the Weyl group from the Dynkin diagram.

The Dynkin diagram has vertices in bijection with the simple roots. The following labeling convention is used: two vertices i and j are linked with an edge if the corresponding simple roots α_i and α_j are not orthogonal. If these make an angle of $2\pi/3$, then i and j are linked with an edge, which is drawn

as a single bond. In this case the roots α_i and α_j have the same length. If they make an angle of $3\pi/4$, the edge is drawn with a double bond and an arrow from the long root to the short root. This arises with the Cartan types B_r, C_r and F_4. Finally (for G_2) if they make an angle of $5\pi/6$, the edge is drawn with a triple bond and an arrow from the long root to the short root.

As to the labeling of the nodes, there are two conventions, Dynkin's and Bourbaki's. The Bourbaki conventions are used by most authors, an important exception being Kac' book *Infinite-dimensional Lie algebras*, which follows Dynkin. The Appendices at the end of Bourbaki's *Groupes et AlgÃbres de Lie* Ch 4,5,6 give the conventions. Sage follows Bourbaki's convention.

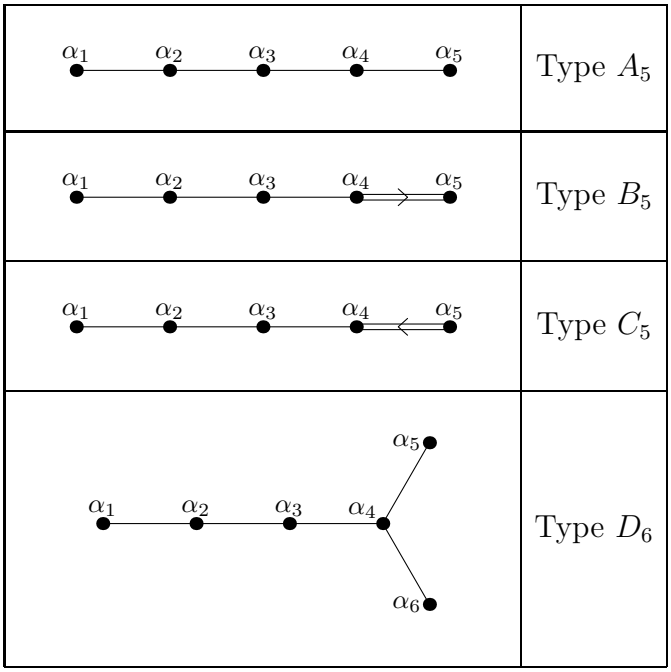


Table 1: The Dynkin diagrams of the classical Cartan types.

From the Dynkin diagram we can view the braid relations for the Coxeter group presentation of the Weyl group. If i and j are not joined by an edge, then s_i and s_j commute. If i and j are joined by a single edge, then $(s_i s_j)^3 = 1$, or $s_i s_j s_i = s_j s_i s_j$, which is Artin's braid relation. If they are joined by an

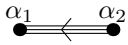
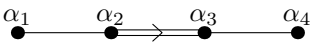
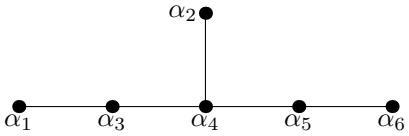
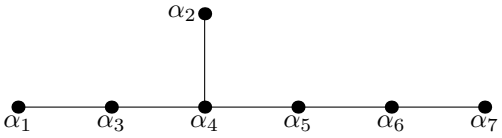
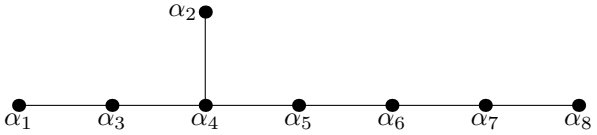
	Type G_2
	Type F_4
	Type E_6
	Type E_7
	Type E_8

Table 2: The Dynkin diagrams of the exceptional Cartan types.

double edge, then $(s_i s_j)^4 = 1$, and if they are joined by a triple edge, then $(s_i s_j)^6 = 1$.

6 Root Systems in GL_{r+1} and other algebraic groups

We wish to show how root systems arise in practice. Let us start with the case of $G = \mathrm{GL}_{r+1}$.

A *Lie algebra* $\mathfrak{g}$ is a vector space over a field F with a bracket operation $X, Y \longmapsto [X, Y]$ that is bilinear, skew-symmetric and satisfies the *Jacobi identity*

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0.$$

As an example, if A is any associative algebra then A has a Lie group structure with the bracket operation $[x, y] = xy - yx$ for $x, y \in A$. We will denote this Lie algebra as $\mathrm{Lie}(A)$. In particular, if $A = \mathrm{End}(V)$ where V is a finite-dimensional vector space, then we will denote this Lie algebra as $\mathfrak{gl}(V)$. Equivalently, if $A = \mathrm{Mat}_{r+1}(F)$ for F any field, we will use the notation $\mathfrak{gl}_{r+1}(F)$ for $\mathrm{Lie}(A)$. These notations will be justified when we show that $\mathfrak{gl}_{r+1}$ is Lie algebra is the Lie algebra of GL_{r+1}.

A *representation* of $\mathfrak{g}$ is a linear map $\rho : \mathfrak{g} \longrightarrow \mathrm{End}(V)$ where V is a vector space is a map that satisfies $\rho([X, Y]) = \rho(X)\rho(Y) - \rho(Y)\rho(X)$. In other words,

$$\rho([X, Y]) = [\rho(X), \rho(Y)] \tag{33}$$

where the second bracket operation is in $\mathfrak{gl}(V)$.

As an example, we have a representation $\mathrm{ad} : \mathfrak{g} \longrightarrow \mathfrak{gl}(\mathfrak{g})$, the so-called *adjoint representation*, defined by

$$\mathrm{ad}(X)Y = [X, Y].$$

Then (33) follows from the Jacobi identity.

The adjoint representation of GL_{r+1} which we have described is a special case of a more general situation. In general, if G is an algebraic group over a field F and if $\mathfrak{g}$ is the tangent space at the identity, then $\mathfrak{g}$ has a Lie algebra structure. As a particular case, suppose that $G = \mathrm{GL}(V)$. Then G is a Zariski-open subset of the vector space $\mathrm{End}(V)$, so the tangent space to G at the identity may be identified with the ambient space $\mathrm{End}(V)$. It may be shown that Lie algebra structure we obtain on $\mathrm{End}(V)$ this way is the same as that described above, so $\mathfrak{gl}(V)$ is indeed the Lie algebra of $\mathrm{GL}(V)$.

Suppose that $\rho : G \longrightarrow \mathrm{GL}(V)$ is a homomorphism. Then there is induced a map of tangent spaces at the identity, which is a Lie algebra homomorphism $d\rho : \mathfrak{g} \longrightarrow \mathfrak{gl}(V)$.

As a special case, G acts on itself by conjugation, fixing the identity, and so there is a representation $\mathrm{Ad} : G(F) \longrightarrow \mathrm{GL}(\mathfrak{g})$. If $\rho = \mathrm{Ad}$ then $d\rho = \mathrm{ad}$.

Restricting ourselves to GL_{r+1} has the advantage that we may see features of the general situation without developing very much machinery. So we will look at this example first.

Let T be the *diagonal torus* consisting of diagonal entries in G. Let B be the *Borel subgroup* of upper triangular elements. We write $B = TU$ where U is the group of upper triangular unipotent matrices. These are algebraic groups. We will write $B(E)$, $T(E)$ or $U(E)$ for the group of elements with entries in E, when E is any field (or commutative algebra) containing F. We have

$$T = \left\{ \begin{pmatrix} * & & \\ & \ddots & \\ & & * \end{pmatrix} \right\}, \qquad B = \left\{ \begin{pmatrix} * & * & \cdots & * \\ & * & & * \\ & & \ddots & \vdots \\ & & & * \end{pmatrix} \right\}, \qquad U = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ & 1 & & * \\ & & \ddots & \vdots \\ & & & 1 \end{pmatrix} \right\}.$$

Now if $1 \leqslant i, j \leqslant r+1$ let $E_{i,j}$ be the matrix having 1 in the i, j position and 0's elsewhere. The $E_{i,j}$ form a basis of $\mathfrak{g}$.

Let $X^*(T)$ be the group of *rational characters* of T. These are the homomorphisms

$$\boldsymbol{z} = \begin{pmatrix} z_1 & & \\ & \ddots & \\ & & z_{r+1} \end{pmatrix} \longmapsto \boldsymbol{z}^\lambda = \prod_{i=1}^{r+1} z_i^{\lambda_i}, \qquad \lambda = (\lambda_1, \cdots, \lambda_{r+1}) \in \mathbb{Z}^{r+1}.$$

We will *identify* $X^*(T)$ with $\mathbb{Z}^{r+1}$ by this parametrization. Elements of $X^*(T)$ will be called *weights*, and we will also denote $X^*(T) = \Lambda$, the *weight lattice*. We will embed Λ in $V = \mathbb{R}^{r+1} = \mathbb{R} \otimes \mathbb{Z}^{r+1} = \mathbb{R} \otimes X^*(T)$. We make $\mathbb{R}^{r+1}$ into a Euclidean space with the usual inner product.

Let $T(F)$ act on $\mathfrak{g}$ by the adjoint representation as above. Then we can decompose $\mathfrak{g}$ into invariant subspaces that are eigenspaces of weights:

$$\mathfrak{g} = \bigoplus_\lambda \mathfrak{g}_\lambda, \qquad \mathfrak{g}_\lambda = \left\{ X \in \mathfrak{g} \,|\, \mathrm{Ad}(\boldsymbol{z})X = \boldsymbol{z}^\lambda X \text{ for } \boldsymbol{z} \in T(F) \right\}.$$

If $\lambda = 0$, then $\mathfrak{g}_0$ is the span of the $E_{i,i}$, which is the Lie algebra of T. On the other hand if $\lambda \neq 0$ then each $\mathfrak{g}_\lambda$ that appears is one-dimensional, and is the span of the $E_{i,j}$ with $i \neq j$. The corresponding characters $\alpha_{i,j}$ are exactly the roots of the root system Φ of Type A_r listed in Example 1.

Let $N(T)$ be the normalizer of T. It consists of monomial matrices, that is, matrices with exactly one nonzero entry in every row and column. The quotient $N(T)/T$ is isomorphic to the symmetric group S_{r+1}. It acts on T and hence on $X^*(T)$ by conjugation.

We note that this is the Weyl group associated with the root system Φ as developed in the previous section. The simple roots Σ are $\alpha_i = \alpha_{i,i+1}$. The simple reflection s_{α_i} is realized as in $N(T)/T$ as the coset with representative

$$s_{\alpha_i} = \begin{pmatrix} I_{i-1} & & \\ & \boxed{\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}} & \\ & & I_{r-i} \end{pmatrix}.$$

All of this generalizes to other root systems. The classical Cartan types B_r, C_r and D_r can be realized in algebraic groups $\mathrm{SO}(2r+1)$, $\mathrm{Sp}(2r)$ and $\mathrm{SO}(2r)$ respectively, where $\mathrm{SO}(n)$ and $\mathrm{Sp}(2n)$ are the special orthogonal and symplectic groups. The exceptional groups give rise to the exceptional root systems.

$\star$ $\star$ $\star$

We will next summarize (without proof) how root systems arise in algebraic groups in general. We will not give proofs, for which see Borel, *Linear Algebraic Groups*, especially Chapter 4 Section 14. For each of the classical Cartan types the existence of a root system and Weyl group structure on N/T may be verified independent of the general theory, as we have done for GL_{r+1} above.

An *algebraic group* is an algebraic variety G defined over some field F with morphisms $m : G \times G \longrightarrow G$ and $\mathrm{inv} : G \longrightarrow G$ which become the multiplication and inverse maps on $G(E)$ making the group $G(E)$ of E-rational points into a group when E is any commutative F-algebra. We will only consider affine algebraic groups, that is, G will be an affine variety. An example is the *multiplicative group* G_{m}, with $G(E) = E^\times$, or more generally $G = \mathrm{GL}_{r+1}$.

A *torus* is a group T that is isomorphic to G_{m}^k for some k. If the isomorphism is defined over F we say T is *split* (over F). For example, the group

$$K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a^2 + b^2 = 1 \right\}$$

over $\mathbb{R}$ is not split since $K(\mathbb{R})$ is compact. But $K(\mathbb{C}) \cong \mathbb{C}^\times$ and indeed $K \cong G_{\mathrm{m}}$ via the isomorphism $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto a + bi$. The isomorphism is defined over $\mathbb{C}$ but not over $\mathbb{R}$.

Let G be an affine algebraic group over F. By a *representation* we mean a morphism $\rho : G \longrightarrow \mathrm{GL}_n$ for some n such that $\rho : G(E) \longrightarrow \mathrm{GL}_n(E)$ is a group homomorphism for any commutative F-algebra E. Suppose that ρ is a faithful representation and $g \in G(F)$. Then the condition that $\rho(g) \in \mathrm{GL}_n(F)$ is semisimple (diagonalizable over $\bar{F}$) or unipotent (having only eigenvalue 1) is independent of ρ. Therefore elements of $G(F)$ may be classified as semisimple or unipotent. The group G is called *unipotent* if every element is unipotent. The group G has a maximal normal unipotent subgroup U, called the *unipotent* radical. If the unipotent radical is trivial, then G is called *reductive*. If it is reductive and has no nontrivial normal tori, it is called *semisimple*. The group

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right\}$$

is not reductive since $\left\{ \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \right\}$ is a normal unipotent subgroup. The group SL_n is semisimple. The group GL_n is reductive but not semisimple.

If G is any smooth variety of dimension d defined over a field F, and if x is a point in $G(F)$, then there is defined at x the Zariski tangent space $T_x G$, which is a vector space of dimension d. If G is an algebraic group, then G is smooth and so the tangent space $\mathfrak{g} = T_1(G)$ at the identity has dimension equal d. It may be given the structure of a Lie algebra. Since G acts on itself by conjugation, with the identity as a fixed point, it acts on $\mathfrak{g}$, and this is the *adjoint representation* $\mathrm{Ad} : G(F) \longrightarrow \mathrm{End}(\mathfrak{g})$.

Let G be a reductive group. If G has a maximal torus that is split over F, then G is called *F-split*.

All maximal tori in $G(F)$ are conjugate if F is algebraically closed. Let G be an semisimple algebraic group, and let T be a maximal torus, that is, a subgroup as large as possible such that T is a product of multiplicative groups. We assume that T is split over F. If such a T exists, then G is called *F-split*.

We assume that G is an F-split reductive group and that T is an F-split maximal torus. Let N be the normalizer of T. Then N/T is a Weyl group W.

To realize W as a Weyl group, we must introduce a vector space V and a root system Φ in V. Let $\Lambda = X^*(T)$ be the group of rational characters of T, that is, algebraic homomorphisms from T to the multiplicative group

$G_{\rm m}$, and let $V = \mathbb{R} \otimes X^*(T)$. The elements of Λ are called *weights*, and are thus embedded as a lattice in the ambient real vector space V. We may give V a Euclidean structure (real inner product) that is W invariant.

We write

$$\mathfrak{g} = \bigoplus_{\lambda} \mathfrak{g}_\lambda$$

where for a weight λ, the space $\mathfrak{g}_\lambda$ is $\{X \in \mathfrak{g} \mid \mathrm{Ad}(t)X = \lambda(t)X \text{ for } t \in T(F)\}$. If $\lambda = 0$ then $\mathfrak{g}_0$ is the Lie algebra of T. If $\alpha \neq 0$ and $\mathfrak{g}_\alpha \neq 0$ then $\mathfrak{g}_\alpha$ is one-dimensional, and in this case α is called a *root*.

Theorem 8 *The roots in a split reductive algebraic group form a root system.*

Proof See Borel, *Linear Algebraic Groups*, Chapter 4, Section 14. □

Let Φ be this root system. We may partition the roots Φ into positive and negative ones. If Φ^+ are the positive roots then

$$\bigoplus_{\alpha \in \Phi^+} \mathfrak{g}_\alpha$$

is the root system of a unipotent subgroup U that is normalized by T, and $B = TU$ is the *positive Borel subgroup*. It is a maximal subgroup of G and G/B is a projective algebraic variety, the *flag variety*.

7 The Bruhat Decomposition

The Bruhat decomposition is a basic fact about Lie groups. Remarkably for something so basic, it went undiscovered for a long time. It originated in Ehresmann's study of flag manifolds, but was not really articulated until Bruhat's work in the 1950s.

Tits found axioms, which were slightly generalized later by Iwahori and Matsumoto. Let G be a group and B, N subgroups. It is assumed that $T = N \cap B$ is normal in N. The group $W = N/T$ will be a Weyl group. If $w \in W$, then w is actually a coset ωT, but we will write wB, Bw and BwB to denote the cosets and double coset ωB, $B\omega$ and $B\omega B$. These do not depend on the representative ω since $T \subseteq B$.

Axiom TS1. *The group $T = B \cap N$ is normal in N;*

Axiom TS2. *There is specified a set I of generators of the group $W = N/T$ such that if $s \in I$ then $s^2 = 1$;*

Axiom TS3. *Let $w \in W$ and $s \in I$. Then*

$$wBs \subset BwsB \cup BwB; \tag{34}$$

Axiom TS4. *Let $s \in I$. Then $sBs^{-1} \neq B$;*

Axiom TS5. *The group G is generated by N and B.*

Then we say that (B, N, I) is a *Tits' system*.

We will be particularly concerned with the double cosets $\mathcal{C}(w) = BwB$ with $w \in W$. Then Axiom TS3 can be rewritten

$$\mathcal{C}(w)\,\mathcal{C}(s) \subset \mathcal{C}(w) \cup \mathcal{C}(ws),$$

which is obviously equivalent to (34). Taking inverses, this is equivalent to

$$\mathcal{C}(s)\,\mathcal{C}(w) \subset \mathcal{C}(w) \cup \mathcal{C}(sw). \tag{35}$$

Theorem 9 *Let (B, N, I) be a Tits' system within a group G, and let W be the corresponding Weyl group. Then*

$$G = \bigcup_{w \in W} BwB, \tag{36}$$

and this union is disjoint.

Proof Let us show that $\bigcup_{w \in W} \mathcal{C}(w)$ is a group. It is clearly closed under inverses. We must show that it is closed under multiplication.

So let us consider $\mathcal{C}(w_1) \cdot \mathcal{C}(w_2)$, where $w_1,\ w_2 \in W$. We will denote by $l(w)$ the length of a shortest decomposition of $w \in W$ into a product of elements of I. We show by induction on $l(w_2)$ that this is contained in a union of double cosets. If $l(w_2) = 0$, then $w_2 = 1$ and the assertion is obvious. If $l(w_2) > 0$, write $w_2 = sw_2'$ where $s \in I$ and $l(w_2') < l(w_2)$. Then by Axiom TS3, we have

$$\mathcal{C}(w_1) \cdot \mathcal{C}(w_2) = Bw_1Bsw_2'B \subset Bw_1Bw_2'B \cup Bw_1sBw_2'B,$$

and by induction, this is contained in a union of double cosets.

We have shown that the right side of (36) is a group, and since it clearly contains B and N, it must be all of G by Axiom TS5.

It remains to be shown that the union (36) is disjoint. Of course two double cosets are either disjoint or equal. So assume that $\mathcal{C}(w) = \mathcal{C}(w')$ where $w,\ w' \in W$. We will show that $w = w'$.

Without loss of generality, we may assume that $l(w) \leqslant l(w')$, and we proceed by induction on $l(w)$. If $l(w) = 0$, then $w = 1$, and so $B = \mathcal{C}(w')$. Thus in N/T a representative for w' will lie in B. Since $B \cap N = T$, this means that $w' = 1$, and we are done in this case. Assume therefore that $l(w) > 0$, and that whenever $\mathcal{C}(w_1) = \mathcal{C}(w_1')$ with $l(w_1) < l(w)$ we have $w_1 = w_1'$.

Write $w = w''s$ where $s \in I$ and $l(w'') < l(w)$. Thus $w''s \in \mathcal{C}(w')$, and since s has order 2, we have

$$w'' \in \mathcal{C}(w')s \subset \mathcal{C}(w') \cup \mathcal{C}(w's)$$

by Axiom TS3. Since two double cosets are either disjoint or equal, this means that either

$$\mathcal{C}(w'') = \mathcal{C}(w') \qquad \text{or} \qquad \mathcal{C}(w'') = \mathcal{C}(w's).$$

Our induction hypothesis implies that either $w'' = w'$ or $w'' = w's$. The first case is impossible since $l(w'') < l(w) \leqslant l(w')$. Therefore so $w'' = w's$. Hence $w = w''s = w'$, as required. □

As a first example, let $G = \mathrm{GL}(r+1, F)$, where F is any field. As in the last section, let B be the Borel subgroup of upper triangular matrices in G, let T be the standard maximal torus of all diagonal elements, and let N be the normalizer in G of T. The group N consists of the monomial matrices, that is, matrices having exactly one nonzero entry in each row and column.

Our goal is to show that N and B form a Tits system.

If $\alpha = \alpha_{i,j}$ with $i \neq j$ is a root, let $x_\alpha : F \longrightarrow G(F)$ be the homomorphism $x_\alpha(a) = 1 + aE_{i,j}$ where $E_{i,j}$ is (as in the last section) the matrix with 1 in the i, j position and 0 elsewhere.

The positive roots are $\alpha_{i,j}$ with $i < j$, and the simple roots are $\alpha_i = \alpha_{i,i+1}$ with $1 \leqslant i \leqslant r$. Suppose that $\alpha = \alpha_i$ is a simple root. The corresponding simple reflection is

$$s_i = \begin{pmatrix} I_{i-1} & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & I_{n-1-i} \end{pmatrix}.$$

More precisely, the coset of this matrix in N/T is s_i. Let $T_\alpha \subset T$ be the kernel of α. Let M_α be the centralizer of T_α, and let P_α be the "parabolic subgroup" generated by B and M_α. We have a semidirect product decomposition $P_\alpha = M_\alpha U_\alpha$, where U_α is the group generated by the $x_\beta(\lambda)$ with $\beta \in \Phi^+ - \{\alpha\}$. For example if $n = 4$ and $\alpha = \alpha_2 = \alpha_{23}$ then

$$T_\alpha = \left\{ \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & t_2 & \\ & & & t_4 \end{pmatrix} \right\}, \quad M_\alpha = \left\{ \begin{pmatrix} * & & & \\ & * & * & \\ & * & * & \\ & & & * \end{pmatrix} \right\}$$

$$P_\alpha = \left\{ \begin{pmatrix} * & * & * & * \\ & * & * & * \\ & * & * & * \\ & & & * \end{pmatrix} \right\}, \quad U_\alpha = \left\{ \begin{pmatrix} 1 & * & * & * \\ & 1 & & * \\ & & 1 & * \\ & & & 1 \end{pmatrix} \right\},$$

where $*$ indicates an arbitrary value.

Lemma 5 *Let $G = \mathrm{GL}(n, F)$ for any field F, and let other notations be as above. If s is a simple reflection then $B \cup \mathcal{C}(s)$ is a subgroup of G.*

Proof First let us check this when $n = 2$. In this case there is only one simple root s_α where $\alpha = \alpha_{12}$. We check easily that

$$\mathcal{C}(s_\alpha) = B s_\alpha B = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, F) \,|\, c \neq 0 \right\},$$

so $\mathcal{C}(s_\alpha) \cup B = G$.

In the general case, both $\mathcal{C}(s_\alpha)$ and B are subsets of P_α. We claim that their union is all of P_α. Both double cosets are right-invariant by U_α, since $U_\alpha \subset B$. So it is sufficient to show that $\mathcal{C}(s_\alpha) \cup B \supset M_\alpha$. Passing to the quotient in $P_\alpha / U_\alpha \cong M_\alpha \cong \mathrm{GL}(2) \times (F^\times)^{n-2}$, this reduces to the case $n = 2$ just considered. □

The action of W on T by conjugation induces the action of W on Φ. This action is such that if $\omega \in N$ represents the Weyl group element $w \in W$, we have

$$\omega x_\alpha(\lambda) \omega^{-1} \in x_{w(\alpha)}(F). \tag{37}$$

Lemma 6 *Let $G = \mathrm{GL}(n, F)$ for any field F, and let other notations be as above. If α is a simple root and $w \in W$ such that $w(\alpha) \in \Phi^+$ then $\mathcal{C}(w)\mathcal{C}(s) = \mathcal{C}(ws)$.*

Proof We will show that

$$wBs \subseteq BwsB.$$

If this is known, then multiplying right and left by B gives $\mathcal{C}(w)\mathcal{C}(s) = BwBsB \subseteq BwsB = \mathcal{C}(ws)$. The other inclusion is obvious, so this is sufficient. Let ω and σ be representatives of w and s as cosets in $N/T = W$, and let $b \in B$. We may write $b = tx_\alpha(\lambda)u$ where $t \in T$, $\lambda \in F$ and $u \in U_\alpha$. Then

$$\omega b\sigma = \omega t\omega^{-1}.\omega x_\alpha(\lambda)\omega^{-1}.\omega\sigma.\sigma^{-1}u\sigma.$$

We have $\omega t\omega^{-1} \in T \subset B$ since $\omega \in N = N(T)$. We have $\omega x_\alpha(\lambda)\omega^{-1} \in x_{w(\alpha)}(F) \subset B$, using (37) and the fact that $w(\alpha) \in \Phi^+$. We have $\sigma^{-1}u\sigma \in U_\alpha \subset B$ since M_α normalizes U_α and $\sigma \in M_\alpha$. We see that $\omega b\sigma \in BwsB$ as required. □

Proposition 25 *Let $G = \mathrm{GL}(n, F)$ for any field F, and let other notations be as above. If $w, w' \in W$ are such that $l(ww') = l(w) + l(w')$, then*

$$\mathcal{C}(ww') = \mathcal{C}(w) \cdot \mathcal{C}(w').$$

Proof It is sufficient to show that if $l(w) = r$, and if $w = s_1 \cdots s_r$ be a decomposition into simple reflections, then

$$\mathcal{C}(w) = \mathcal{C}(s_1) \cdots \mathcal{C}(s_r). \tag{38}$$

Indeed, assuming we know this fact, let $w' = s'_1 \cdots s'_{r'}$ be a decomposition into simple reflections with $r' = l(r')$. Then $s_1 \cdots s_r s'_1 \cdots s'_{r'}$ is a decomposition of ww' into simple reflections with $l(ww') = r + r'$, so

$$C(ww') = \mathcal{C}(s_1) \cdots \mathcal{C}(s_r)\mathcal{C}(s'_1) \cdots \mathcal{C}(s'_{r'}) = \mathcal{C}(w)\mathcal{C}(w').$$

To prove (38), let $s_r = s_\alpha$, and let $w_1 = s_1 \cdots s_{r-1}$. Then $l(w_1 s_\alpha) = l(w_1) + 1$, so by Proposition 13 we have $w'(\alpha) \in \Phi^+$. Thus Lemma 6 is applicable and $\mathcal{C}(w) = \mathcal{C}(w_1)\mathcal{C}(s_r)$. By induction on r, we have $\mathcal{C}(w_1) = \mathcal{C}(s_1) \cdots \mathcal{C}(s_{r-1})$ and so we are done. □

Theorem 10 *With $G = \mathrm{GL}(n, F)$ and B, N, I as above, (B, N, I) is a Tits' system in G.*

Proof Only Axiom TS3 requires proof; the others can be safely left to the reader. Let $\alpha \in \Sigma$ such that $s = s_\alpha$.

First, suppose that $w(\alpha) \in \Phi^+$. In this case, it follows from Lemma 6 that $wBs \subset BwsB$.

Next suppose that $w(\alpha) \notin \Phi^+$. Then $ws_\alpha(\alpha) = w(-\alpha) = -w(\alpha) \in \Phi^+$, so we may apply the case just considered, with ws_α replacing w, to see that

$$wsBs \subset Bws^2B = BwB. \tag{39}$$

By Lemma 5, $B \cup BsB$ is a group containing a representative of the coset of $s \in N/T$, so $B \cup BsB = sB \cup sBsB$ and thus

$$Bs \subset sB \cup sBsB.$$

Using (39),

$$wBs \subset wsB \cup wsBsB \subset BwsB \cup BwB.$$

This proves Axiom TS3. □

Similarly, if G is any split reductive group, T a maximal split torus, B a Borel subgroup containing G and N the normalizer of T, then $B(F)$ and $N(F)$ are a Tits system and so we have a Bruhat decomposition. For proofs, see Borel's book *Linear Algebraic Groups*.

8 Finite Field Iwahori Hecke algebras

Let W be a Coxeter group and let F be a field containing an element q. Let $I = \{s_1, \cdots, s_r\}$ be the set of simple reflections. We recall that we defined the *Iwahori Hecke algebra* $\mathcal{H}_q(W)$ has basis $T_1, \cdots, T_r$ subject to the braid relations

$$T_iT_jT_iT_j \cdots = T_jT_iT_jT_i \cdots$$

where the number of terms is the order of s_is_j, and

$$T_i^2 = (q-1)T_i + q.$$

Proposition 26 *For any Coxeter group W, if $q = 1$ then $\mathcal{H}_q(W)$ is isomorphic to the group algebra $\mathbb{C}[W]$.*

Proof This is because the relations between the T_i become exactly the braid relations and $T_i^2 = 1$, which are a presentation of W. □

We will assume that W is the Weyl group of a root system Φ. In this case, we defined a braid group B with generators u_i subject to the braid relations

$$u_i u_j u_i u_j \cdots = u_j u_i u_j u_i \cdots$$

Clearly there is a homomorphism $B \longrightarrow \mathcal{H}_q(W)^\times$ such that $u_i \mapsto T_i$.

We recall that if $w \in W$ then the length $l(w)$ is the smallest k such that we may write w as a product of k simple reflections. An such representation $w = s_{i_1} \cdots s_{i_k}$ into a minimal number of simple reflections will be called a *reduced decomposition*.

Proposition 27 *Assume that W is the Weyl group of a root system Φ. Then for every $w \in W$ there exists an element T_w of $\mathcal{H}_q(W)$ such that if $w = s_i$ is a simple reflection then $T_w = T_i$, and if $l(ww') = l(w) + l(w')$ then $T_{ww'} = T_w T_{w'}$. If s is a simple reflection then*

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

The T_w span $\mathcal{H}_q(W)$ as a vector space, so dim $\mathcal{H}_q(W) \leqslant |W|$.

Proof Let $w = s_{i_1} \cdots s_{i_k}$ be a reduced decomposition of w into a product of simple reflections, where $k = l(w)$. Then we will define $T_w = T_{i_1} \cdots T_{i_k}$. We must show this is well-defined.

If $w = s_{j_1} \cdots s_{j_k}$ is another reduced decomposition, then by Proposition 23 we have $u_{i_1} \cdots u_{i_k} = u_{j_1} \cdots u_{j_k}$ in the braid group. Therefore applying the homomorphism $u_i \mapsto T_i$ we have $T_{i_1} \cdots T_{i_k} = T_{j_1} \cdots T_{j_k}$, and so T_w is well-defined.

It is clear that $T_{s_i} = T_i$. Moreover if $l(ww') = l(w) + l(w')$ then $T_{ww'} = T_w T_{w'}$ since we may obtain a reduced decomposition of ww' by concatenating reduced decompositions of w and w'.

If $l(sw) > l(w)$ we have $l(sw) = l(w)+1 = l(s)+l(w)$ and $T_s T_w = T_{sw}$. On the other hand if $l(sw) < l(w)$ we may write $w = sw'$ and $l(w) = l(s) + l(w')$ so $T_w = T_s T_{w'}$. Now using $T_s^2 = (q-1)T_s + q$ we obtain $T_s T_w = T_s^2 T_{w'} = (q-1)T_s T_{w'} + qT_{w'} = (q-1)T_w + qT_{sw}$.

Now it follows that the linear span of the T_w is closed under multiplication by the generators T_i, and so this linear span is all of $\mathcal{H}_q(W)$. □

Let F be a field. We will denote by U the group of upper triangular unipotent matrices in $\mathrm{GL}(r+1, F)$.

Proposition 28 *Suppose that S is any subset of Φ such that if $\alpha \in S$ then $-\alpha \notin S$, and if $\alpha, \beta \in S$ and $\alpha + \beta \in \Phi$, then $\alpha + \beta \in S$. Let U_S be the set of $g = (g_{ij})$ in $\mathrm{GL}(r+1, F)$ such that $g_{ii} = 1$, and if $i \neq j$ then $g_{ij} = 0$ unless $\alpha_{ij} \in S$. Then U_S is a group.*

Proof Let $\tilde{S}$ be the set of (i, j) such that the root $\alpha_{ij} \in S$. Translating the hypothesis on S into a statement about $\tilde{S}$, if $(i, j) \in \tilde{S}$ we have $i < j$, and

$$\text{if both } (i,j) \text{ and } (j,k) \text{ are in } \tilde{S} \text{ then } i \neq k \text{ and } (i,k) \in \tilde{S}. \tag{40}$$

From this it is easy to see that if g and h are in U_S then so are g^{-1} and gh. □

As a particular case, if $w \in W$ then $S = \Phi^+ \cap w\Phi^-$ satisfies the hypothesis of Proposition 28, and we denote

$$U_{\Phi^+ \cap w\Phi^-} = U_w^-.$$

Similarly $S = \Phi^+ \cap w\Phi^+$ meets this hypothesis, and we denote

$$U_{\Phi^+ \cap w\Phi^+} = U_w^+.$$

Lemma 7 *We have $|\Phi^+ \cap w\Phi^-| = l(w)$.*

Proof We gave two definitions of the length function l, which were proved equivalent by Proposition 16. One of them was the number of positive roots α such that $w(\alpha) \in \Phi^{-1}$, in other words, the cardinality of $S = \Phi^+ \cap w^{-1}\Phi^-$. From the other definition as the length of a reduced decomposition, it is clear that $l(w) = l(w^{-1})$ and so $|\Phi^+ \cap w\Phi^-| = l(w)$. □

Proposition 29 *Let $F = \mathbb{F}_q$ be finite, and let $w \in W$. Then and*

$$|U_w^-| = q^{l(w)}.$$

Proof This follows from the Lemma. □

Proposition 30 *Let $w \in W$. The multiplication map $U_w^+ \times U_w^- \longrightarrow U$ is bijective.*

Proof We will prove this if F is finite, the only case we need. In this case $U_w^+ \cap U_w^- = \{1\}$ by definition, since the sets $\Phi^+ \cap w\Phi^-$ and $\Phi^+ \cap w\Phi^+$ are disjoint. Thus if $u_1^+ u_1^- = u_2^+ u_2^-$ with $u_i^\pm \in U_w^\pm$, then $(u_2^+)^{-1}u_1^+ = u_2^-(u_1^-)^{-1} \in U_w^+ \cap U_w^-$ so $u_1^\pm = u_2^\pm$. Therefore the multiplication map $U_w^+ \times U_w^- \longrightarrow U$ is injective. To see that it is surjective, note that

$$|U_w^-| = q^{|\Phi^+ \cap w\Phi^-|}, \qquad |U_w^+| = q^{|\Phi^+ \cap w\Phi^+|},$$

so the order of $U_w^+ \times U_w^-$ is $q^{|\Phi^+|} = |U|$, and the surjectivity is now clear. □

We are interested in the size of the double coset BwB. In geometric terms, G/B can be identified with the space of F-rational points of a projective algebraic variety, and the closure of BwB/B is an algebraic subvariety in which BwB/B is an open subset; the dimension of this "Schubert cell" turns out to be $l(w)$.

If $F = \mathbb{F}_q$ an equally good measure of the size of BwB is its cardinality. It can of course be decomposed into right cosets of B, and its cardinality will be the order of B times the cardinality of the quotient BwB/B.

Proposition 31 *Let $F = \mathbb{F}_q$ be finite, and let $w \in W$. The order of BwB/B is $q^{l(w)}$.*

Proof We will show that $u^- \longmapsto u^- wB$ is a bijection $U_w^- \longrightarrow BwB/B$. The result then follows from Proposition 29.

Note that every right coset in BwB/B is of the form bwB for some $b \in B$. Using Proposition 30 we may write $b \in B$ uniquely in the form $u^- u^+ t$ with $u^\pm \in U_w^\pm$ and $t \in T$. Now $w^{-1}u^+ tw = w^{-1}u^+ w.w^{-1}tw \in B$, because $w^{-1}u^+ w \in U$ and $w^{-1}tw \in T$. Therefore $bwB = u^- wB$.

It is now clear that the map $u^- \longmapsto u^- wB$ is surjective. We must show that it is injective, in other words if $u_1^- wB = u_2^- wB$ for $u_i^- \in U_w^-$ then $u_1^- = u_2^-$. Indeed, if $u^- = (u_1^-)^{-1}u_2^-$ then $w^{-1}u^- w \in B$ from the equality of the double cosets. On the other hand $w^{-1}u^- w$ is lower triangular by definition of U_w^-. It is both upper triangular and lower triangular, and unipotent, so $u^- = 1$. □

With r and q fixed, let $\mathcal{H}$ be the convolution ring of B-bi-invariant functions on G. The dimension of $\mathcal{H}$ equals the cardinality of $B\backslash G/B$, which is $|W| = (r+1)!$ by the Bruhat decomposition. A basis of $\mathcal{H}$ consists of the functions ϕ_w ($w \in W$), where ϕ_w is the characteristic function of the double

coset $\mathcal{C}(w) = BwB$. We normalize the convolution as follows:

$$(f_1 * f_2)(g) = \frac{1}{|B|} \sum_{x \in G} f_1(x) f_2(x^{-1}g) = \frac{1}{|B|} \sum_{x \in G} f_1(gx) f_2(x^{-1}).$$

With this normalization, the characteristic function f_1 of B serves as a unit in the ring.

The ring $\mathcal{H}$ is a normed ring with the L^1 norm. That is, we have

$$|f_1 * f_2| \leqslant |f_1| \cdot |f_2|,$$

where

$$|f| = \frac{1}{|B|} \sum_{x \in G} |f(x)|.$$

There is also an *augmentation map*, that is, a $\mathbb{C}$-algebra homomorphism $\epsilon : \mathcal{H} \longrightarrow \mathbb{C}$ given by

$$\epsilon(f) = \frac{1}{|B|} \sum_{x \in G} f(x).$$

By Proposition 31 we have

$$\epsilon(\phi_w) = q^{l(w)}. \tag{41}$$

Proposition 32 *Let $w, w' \in W$ such that $l(ww') = l(w) + l(w')$. Then*

$$\phi_{ww'} = \phi_w * \phi_{w'}.$$

Proof By Proposition 25, we have $\mathcal{C}(ww') = \mathcal{C}(w)\mathcal{C}(w')$. Therefore $\phi_w * \phi_{w'}$ is supported in $\mathcal{C}(ww')$ is a constant multiple of $\phi_{ww'}$. Writing $\phi_w * \phi_{w'} = c\phi_{ww'}$ and applying the augmentation ϵ and using (41), we see that $c = 1$. □

Proposition 33 *Let $s \in W$ be a simple reflection. Then*

$$\phi_s * \phi_s = q\phi_1 + (q-1)\phi_s.$$

Proof By (34) we have $\mathcal{C}(s)\mathcal{C}(s) \subseteq \mathcal{C}(1) \cup \mathcal{C}(s)$. Therefore there exist constants λ and μ such that $\phi_s * \phi_s = \lambda\phi_1 + \mu\phi_s$. Evaluating both sides at the identity gives $\lambda = q$. Now applying the augmentation and using the special cases $\epsilon(\phi_s) = q$, $\epsilon(f_1) = 1$ of (41) we have $q^2 = \lambda \cdot 1 + \mu \cdot q = q + \mu q$, so $\mu = q - 1$. □

Theorem 11 (Iwahori) *The algebra $\mathcal{H}$ is isomorphic to $\mathcal{H}_q(W)$ under a homomorphism such that $\phi_w \longmapsto T_w$.*

Proof By Propositions 32 and 33 the ϕ_w satisfy the defining relations of T_i and so there is a homomorphism $\mathcal{H}_q(W) \longrightarrow \mathcal{H}$ such that $T_{s_i} \longmapsto \phi_{s_i}$. The homomorphism is surjective since the ϕ_{s_i} generate $\mathcal{H}$. We have dim $\mathcal{H}_q(W) \leqslant |W| =$ dim $\mathcal{H}$ so this homomorphism is an isomorphism. □

9 The Spherical Hecke algebra for $\mathrm{GL}(n)$

This section is **optional**. Omitting it will not cause any problems of continuity.

Let $G = \mathrm{GL}_n(F)$ where F is a nonarchimedean local field, and let $K^\circ = \mathrm{GL}_{r+1}(\mathfrak{o})$ be its maximal compact subgroup. There is a homomorphism $K^\circ \longrightarrow \mathrm{GL}_{r+1}(\mathbb{F}_q)$, where $\mathbb{F}_q = \mathfrak{o}/\mathfrak{p}$ is the residue field. The preimage J of the Borel subgroup $B(\mathbb{F}_q)$ is the *Iwahori subgroup*.

The Iwahori Hecke algebra $\mathcal{H}_J$ is our main object of study. However the spherical Hecke algebra $\mathcal{H}^\circ = \mathcal{H}_{K^\circ}$ is worth first considering. It is commutative, hence a Gelfand subgroup. It is not a subring of $\mathcal{H}_J$ (since it does not contain the unit of $\mathcal{H}_J$). It is an ideal. Moreover $\mathcal{H}^\circ$ does not play an important role in the theory of $\mathcal{H}_J$, which contains other commutative subrings that take its place – the center, and a larger commutative subring.

We now describe a method of distinguishing the double cosets $K^\circ \backslash G / K^\circ$. If $g \in G$, let $\gcd(g)$ be the fractional ideal of $\mathfrak{o}$ generated by the entries in g. Evidently $\gcd(g)$ is invariant under both left and right multiplication by K°. We may refine this invariant of the double coset $K^\circ g K^\circ$ as follows: if $1 \leqslant k \leqslant n$, let

$$\wedge^k : GL(n, F) \longrightarrow GL\left(\binom{n}{k}, F\right)$$

be the k-th exterior power representation; the matrix entries $\wedge^k g$ are the $k \times k$ minors of g. Then $\gcd(\wedge^k g)$ is the fractional ideal generated by these minors. Clearly $\wedge^k(K^\circ) \subset GL\left(\binom{n}{k}, \mathfrak{o}\right)$, so $\gcd(\wedge^k g)$ is also invariant under left and right multiplication by K°.

Proposition 34 (The Elementary Divisor Theorem) *Let R be a principal ideal domain, let M be a free R-module of rank n, and let N be a submodule of M which is also free of rank n. Then there exists an R-basis*

$\xi_1, \cdots, \xi_n$ of M and nonzero elements $D_1, \cdots, D_n$ of R such that each D_{i+1} divides D_i $(i = 1, \cdots, n-1)$ and $D_1\xi_1, \cdots, D_n\xi_n$ is a R-basis of N.

Proof See Theorem III.7.8 of Lang's *Algebra*. □

Proposition 35 (The p-adic Cartan Decomposition) *Every double coset in $K^\circ \backslash G / K^\circ$ has a unique representative of the form*

$$\begin{pmatrix} \varpi^{\lambda_1} & & \\ & \ddots & \\ & & \varpi^{\lambda_n} \end{pmatrix}, \qquad \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n. \tag{42}$$

Proof We show first that if $g \in G$, then there exist elements $\kappa_1, \kappa_2 \in K^\circ$ such that $\kappa_1 g \kappa_2$ is diagonal. If we know this for elements $g \in \mathrm{Mat}_n(\mathfrak{o})$, then we can deduce it for all g, since we can multiply g by a scalar to put it in $\mathrm{Mat}_n(\mathfrak{o})$. Hence there is no loss of generality in assuming $g \in \mathrm{Mat}_n(\mathfrak{o})$. We apply the Elementary Divisor Theorem with $R = \mathfrak{o}$, $M = \mathfrak{o}^n$, and N the submodule generated by the columns of g. Let $\xi_1, \cdots, \xi_n$ and D_i be such that $\xi_1, \cdots, \xi_n$ generate $\mathfrak{o}^n$ and $D_1\xi_1, \cdots, D_n\xi_n$ generate the same $\mathfrak{o}$-module as the columns of g, there exists $\kappa_2 \in K^\circ$ such that

$$(D_1\xi_1, \cdots, D_n\xi_n) = g\kappa_2.$$

We may rewrite this

$$(\xi_1, \cdots, \xi_n) \begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_n \end{pmatrix} = g\kappa_2,$$

and the first matrix on the left is an element of K°, so we have shown that

$$\begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_n \end{pmatrix} \in K^\circ g K^\circ.$$

We may clearly adjust the D_i's by units, proving that every coset has a representative of the form (42).

It remains to be shown the matrices (42) lie in distinct double cosets. Indeed, the invariants $\gcd(\wedge^k g)$ determine $\lambda_1, \cdots, \lambda_n$, since clearly if g equals the matrix (42) we have $\gcd(g) = \lambda_n$, $\gcd(\wedge^2 g) = \lambda_{n-1}\lambda_n$, and so forth. □

Theorem 12 *(i) The spherical Hecke algebra $\mathcal{H}^\circ$ is commutative.*

(ii) If (π, V) is an irreducible admissible representation of $\mathrm{GL}(n, F)$, then the space V^{K° of K°-fixed vectors in V is at most one-dimensional.

Proposition 5 shows that it is expected that commutativity of the Hecke algebra will have $\dim(V^{K^\circ}) \leqslant 1$ as a consequence. The following "involution" method of proof is due to Gelfand. The second assertion is sometimes expressed by the statement that K° is a *Gelfand subgroup* of $\mathrm{GL}(n, F)$.

Proof Define a map $\iota : \mathcal{H}^\circ \to \mathcal{H}^\circ$ by $(\iota f)(g) = f({}^t g)$. Since K° is stable under transposition, this is a well-defined transformation of $\mathcal{H}^\circ$, and because transposition is an anti-automorphism of G, it is easy to see that ι is an anti-automorphism of $\mathcal{H}^\circ$:

$$\iota(f_1 * f_2) = \iota(f_2) * \iota(f_1).$$

On the other hand, ι is just the identity map, since every double coset has a representative which is diagonal, hence stable under transposition, by Proposition 35. We see that the identity map is an anti-automorphism of $\mathcal{H}^\circ$. This means that $\mathcal{H}^\circ$ is commutative.

For the second statement, V^{K°, if nonzero, is a finite-dimensional simple module over the commutative $\mathbb{C}$-algebra $\mathcal{H}^\circ$. It is therefore one-dimensional. □

We call an irreducible admissible representation (π, V) *spherical* if it has a K°-fixed vector. The commutative Hecke algebra $\mathcal{H}^\circ$ is called the *spherical Hecke algebra*. We recall the partial order on partitions, in which $\mu \preccurlyeq \nu$ means that

$$\mu_1 + \ldots + \mu_r \leqslant \nu_1 + \ldots + \nu_r$$

for each r. Now let us study the product of two double cosets.

Proposition 36 *Suppose that λ and μ are partitions of k and l, respectively, of length $\leqslant n$. for each $1 \leqslant r \leqslant n$. We will denote by $\lambda + \mu$ the partition $\{\lambda_1 + \mu_1, \cdots, \lambda_n + \mu_n\}$ of $k + l$. Let*

$$g = \begin{pmatrix} \varpi^{\lambda_1} & & \\ & \ddots & \\ & & \varpi^{\lambda_n} \end{pmatrix}, \qquad h = \begin{pmatrix} \varpi^{\mu_1} & & \\ & \ddots & \\ & & \varpi^{\mu_n} \end{pmatrix},$$

where $\lambda_1 \geqslant \cdots \geqslant \lambda_n$ *and* $\mu_1 \geqslant \cdots \geqslant \mu_n$. *Suppose that* $(K^\circ g K^\circ)(K^\circ h K^\circ)$ *contains a double coset*

$$K^\circ \begin{pmatrix} \varpi^{\nu_1} & & \\ & \ddots & \\ & & \varpi^{\nu_n} \end{pmatrix} K^\circ, \qquad \nu_1 \geqslant \cdots \geqslant \nu_n. \tag{43}$$

Then ν *is a partition of* $k+l$, *and* $\nu \preccurlyeq \lambda + \mu$.

Proof Since g and $h \in \mathrm{Mat}_n(\mathfrak{o})$, we have $K^\circ g K^\circ h K^\circ \subset \mathrm{Mat}_n(\mathfrak{o})$ and so the ν_i are nonnegative integers. Comparing determinants, ν is a partition of $k+l$. To prove that $\nu \preccurlyeq \lambda + \mu$, it is sufficient to check the inequalities

$$\nu_n \geqslant \lambda_n + \mu_n, \tag{44}$$

$$\nu_{n-1} + \nu_n \geqslant \lambda_{n-1} + \mu_{n-1} + \lambda_n + \mu_n, \tag{45}$$

etc. since subtracting these inequalities from the equality

$$\nu_1 + \ldots + \nu_n = k + l = \lambda_1 + \mu_1 \cdots + \lambda_n + \mu_n$$

will give $\nu \leqslant \lambda + \mu$. The matrix entries of an element of $K^\circ g K^\circ$ have greatest common divisor equal to $\mathfrak{p}^{\lambda_n}$, and the matrix entries of an element of $K^\circ h K^\circ$ have greatest common divisor $\mathfrak{p}^{\mu_n}$; it is evident that the matrix entries of an element of $(K^\circ g K^\circ)(K^\circ h K^\circ)$ lie in the ideal $\mathfrak{p}^{\lambda_n + \mu_n}$, and therefore we have (44). Repeating this argument with $\wedge^2 g$ and $\wedge^2 h$ replacing g and h gives (45), and so forth. □

For $1 \leqslant r \leqslant n$, let θ_r be $q^{-r(n-r)/2}$ times the characteristic function of the double coset

$$K^\circ \tau_r K^\circ, \qquad \tau_r = \begin{pmatrix} \varpi I_r & \\ & I_{n-r} \end{pmatrix}. \tag{46}$$

Of these "Hecke operators" the last one, θ_n is invertible, having as its inverse the characteristic function of the double coset $K^\circ \tau_r^{-1} K^\circ$. Also, if $\lambda = \{\lambda_1, \cdots, \lambda_n\}$ is a sequence of integers satisfying $\lambda_1 \geqslant \ldots \geqslant \lambda_n$, let θ_λ equal

$$q^{\frac{1}{2}((1-n)\lambda_1 + (3-n)\lambda_2 + \ldots + (n-1)\lambda_n)}$$

times the characteristic function of the double coset (42). By the p-adic Cartan decomposition, these form a $\mathbb{Z}$-basis of $\mathcal{H}^\circ$.

Proposition 37 (Tamagawa, Satake) *The ring $\mathcal{H}^\circ$ is a polynomial ring over in $\theta_1, \cdots, \theta_n$ and θ_n^{-1}:*

$$\mathcal{H}^\circ \cong \mathbb{C}[\theta_1, \cdots, \theta_{n-1}, \theta_n, \theta_n^{-1}].$$

This structure theorem is a special case of the *Satake isomorphism* describing the structure of the spherical Hecke algebra of a reductive p-adic group.

Proof Let us show that θ_λ lies in the $\mathbb{C}$-algebra generated by $\theta_1, \cdots, \theta_n, \theta_n^{-1}$, where $\lambda = \{\lambda_1, \cdots, \lambda_n\}$ is a sequence of integers satisfying $\lambda_1 \geqslant \ldots \geqslant \lambda_n$. Clearly $\theta_n^{-r} * \theta_\lambda = \theta_{\lambda'}$, where

$$\lambda' = \{\lambda_1 - r, \cdots, \lambda_n - r\},$$

and so we may assume that $\lambda_n = 0$. Then the $\lambda_i \geqslant 0$, and λ is a partition, so (42) lies in $\mathrm{Mat}_n(\mathfrak{o})$. With this assumption, we will prove that θ_λ is a polynomial in $\theta_1, \cdots, \theta_n$. ($\theta_n^{-1}$ is not needed if the $\lambda_i \geqslant 0$.)

If the λ_i are all equal zero, then $\theta_\lambda = 1$ and there is nothing to prove, so assume that $\lambda_1 > 0$. Let $1 \leqslant k \leqslant n-1$ be the largest integer such that $\lambda_k \neq 0$, and let

$$\mu = \{\lambda_1 - 1, \cdots, \lambda_k - 1, 0, \cdots, 0\}.$$

By induction, θ_μ lies in the $\mathbb{C}$-algebra generated by $\theta_1, \cdots, \theta_n$. We ask which double cosets occur in the support of $\theta_k * \theta_\mu$. Evidently the double coset of (42) occurs, and every other double coset is of the form (43) with ν a partition of $|\lambda|$, which strictly preceeds λ in the partial order. By induction, the characteristic of each such double coset is a polynomial in $\theta_1, \cdots, \theta_n$. We see that $\theta_k * \theta_\mu$ lies in the $\mathbb{C}$-algebra generated by $\theta_1, \cdots, \theta_n$, and it differs from a nonzero multiple of θ_λ by a sum of elements θ_ν which lie in this ring; hence θ_λ is a polynomial in $\theta_1, \cdots, \theta_n$.

We must also show that the θ_i are algebraically independent. We note that θ_i is the characteristic function of a set supported on the matrices of determinant equal to ϖ^i times a unit, so we may grade the ring $\mathcal{H}^\circ$ by degree, θ_i having degree i. Given relation of algebraic dependence, we may clearly separate out the part which is homogeneous of given degree and obtain a homogeneous relation

$$\sum_{|\lambda|=k} a(\lambda)\, \theta_1^{\lambda_1 - \lambda_2} \cdots \theta_{n-1}^{\lambda_{n-1} - \lambda_n} \theta_n^{\lambda_n} = 0. \tag{47}$$

The point is that the homogeneous degree of the monomial

$$\theta_1^{\lambda_1-\lambda_2}\cdots\theta_{n-1}^{\lambda_{n-1}-\lambda_n}\theta_n^{\lambda_n} \tag{48}$$

is

$$(\lambda_1-\lambda_2)+2(\lambda_2-\lambda_3)+\cdots+n\lambda_n=\lambda_1+\ldots+\lambda_n=|\lambda|.$$

Now let us expand this out in terms of the θ_λ, which are a $\mathbb{Z}$-basis of $\mathcal{H}^\circ$. It is a consequence of Proposition 36 that when (48) is expanded out, θ_λ will occur, together with terms of the form θ_ν, where ν runs through partitions of k strictly preceeding λ in the partial order. Thus if λ is minimal in the partial ordering subject to the condition that $a(\lambda)\neq 0$, it is clear that the coefficient of θ_λ in the expansion of (47) is nonzero. Thus (47) does not vanish. This contradiction shows that the θ_i are algebraically independent, and we have proved that $\mathcal{H}^\circ$ is a polynomial ring $\mathbb{C}[\theta_1,\cdots,\theta_{n-1},\theta_n,\theta_n^{-1}]$. □

Proposition 38 (Iwasawa decomposition) *Let $B(F)$ be the Borel subgroup of upper triangular matrices in $G=\mathrm{GL}(n,F)$, and let $K^\circ=\mathrm{GL}(n,\mathfrak{o})$. Then $G=B(F)\,K^\circ$.*

Proof See Bump, *Automorphic Forms and Representations*, Proposition 4.5.2. □

Now let us construct representations of $G=\mathrm{GL}(n,F)$ which have a K°-fixed vector. These are the *spherical principal series* representations. We recall that a *quasicharacter* of a locally compact group is a continuous homomorphism into $\mathbb{C}^\times$; a quasicharacter of $F^\times$ is called *nonramified* if it is trivial on $\mathfrak{o}^\times$.

The *modular quasicharacter* a topological group H is the quasicharacter $\delta_H: H\to\mathbb{C}$ such that if d_Lh and d_Rh denote left and right Haar measures, respectively, on H, then $d_Rh=\delta_H(h)\,d_Lh$. The the modular quasicharacter of $B(F)$ is

$$\delta\begin{pmatrix} y_1 & * & \cdots & * \\ & y_2 & & * \\ & & \ddots & \vdots \\ & & & y_n \end{pmatrix} = |y_1|^{n-1}|y_2|^{n-3}\cdots|y_n|^{1-n}.$$

Fix quasicharacters $\chi_1, \cdots, \chi_n$ of $F^\times$. Then we have a quasicharacter $\chi : B(F) \longrightarrow \mathbb{C}^\times$ given by

$$\chi \begin{pmatrix} y_1 & * & \cdots & * \\ & y_2 & & * \\ & & \ddots & \vdots \\ & & & y_n \end{pmatrix} = \chi_1(y_1) \cdots \chi_n(y_n).$$

Let $V = V(\chi_1, \cdots, \chi_n)$ be the space of locally constant functions $f : G \to \mathbb{C}$ such that

$$f(bg) = \chi(b)\, \delta^{1/2}(b)\, f(g). \tag{49}$$

We define an action $\pi = \pi(\chi_1, \cdots, \chi_n)$ of G on V by right translation:

$$(\pi(h)f)(g) = f(gh).$$

It is easily verified that $\pi(h)f \in V$ with this definition, and since the functions f are locally constant, the stabilizer of any particular f is open, so this is a smooth representation. We may see that it is admissible as follows: If K is any open subgroup, we want to show that V^K is finite. This is a subspace of $V^{K \cap K^\circ}$, so without loss of generality $K \subset K^\circ$. The index of K in K° is finite, and if $x_1, \cdots, x_N$ are a complete set of coset representatives, so $K^\circ = \bigcup x_i K$, then we claim that $f \in V^K$ is completely determined by the values $f(x_i)$. Indeed, since f is right K-invariant, knowledge of these values determines f on K° and by (49) and the Iwasawa decomposition, f is therefore completely known. We see that V^K is finite-dimensional, so this representation is admissible.

Proposition 39 *Assume that the quasicharacters χ_i are nonramified. The space of K°-fixed vectors in the representation $\pi(\chi_1, \cdots, \chi_n)$ is one-dimensional.*

Proof We will show that the space of K°-fixed vectors is spanned by the function f° defined by

$$f^\circ(bk) = \chi(b)\, \delta^{1/2}(b), \qquad b \in B(F),\ k \in K^\circ. \tag{50}$$

It is called the *standard spherical vector*. It is a consequence of the Iwasawa decomposition that every element of G can be written as bk as in (50), so the definition (50) makes sense provided the right-hand side is well-defined, independent of the decomposition of g as bk. This is true on our assumption

that $\chi_1, \cdots, \chi_n$ are nonramified, since if $bk = b'k'$ where b, $b' \in B(F)$ and k, $k' \in K^\circ$, then $b^{-1}b' \in B(F) \cap K^\circ$ is upper triangular with units on the diagonal, and so $\chi(b^{-1}b') = \delta(b^{-1}b') = 1$. Thus f° is well defined. It is clear from the Iwasawa decomposition that a K°-fixed vector is a constant multiple of this f°, so V^{K° is exactly one-dimensional. $\square$

Proposition 40 *Assume that the quasicharacters χ_i are nonramified, and let f° be the K°-fixed vector (50). Then*

$$\theta_r f^\circ = e_r(t_1, \cdots, t_n)\, f^\circ, \tag{51}$$

where e_r is the r-th elementary symmetric polynomial, and $t_i = \chi_i(\varpi)$.

Proof It is clear that $\theta_r * f \in V^{K^\circ}$ for any f since θ_r is K°-bi-invariant, and so $\theta_r * f^\circ = cf^\circ$ for some constant c. Evidently $c = (\theta_r * f^\circ)(1)$, so we must show that

$$(\theta_r * f^\circ)(1) = e_r(t_1, \cdots, t_n).$$

Since $K^\circ \tau_r K^\circ$ is the continuous image of $K^\circ \times K^\circ$ under the map $(k_1, k_2) \mapsto k_1 \tau_r k_2$, it is compact; and since K° is open, there are a finite number of right cosets in $K^\circ \tau_r K^\circ / K^\circ$. Let Λ be a complete set of coset representatives for these, so that

$$K^\circ \tau_r K^\circ = \bigcup_{\beta \in \Lambda} \beta K^\circ, \tag{52}$$

Since $K^\circ \tau_r K^\circ \subset \mathrm{Mat}_n(\mathfrak{o})$, the matrix entries in β are all integers. It follows from the Iwasawa decomposition that we may chose the representatives β to be upper triangular, and we have the freedom to change them by an element of $K^\circ \cap B(F)$ on the right. We may then arrange that the diagonal entries of β are all powers of π. In order to lie in the same double coset as τ_r, it is necessary that $\gcd(\wedge^k \tau_r)$ and $\gcd(\wedge^k \beta)$ agree. The implications of this are as follows: of the diagonal entries of β, there are exactly r ϖ's and exactly $n - r$ 1's. Moreover, if S is the set (of cardinality r) of $1 \leqslant i \leqslant n$ such that $\beta_{ii} = \varpi$, and if i, j are distinct elements of S, then β_{ij} must lie in $\mathfrak{p}$. If these conditions are not satisfied, then β will not lie in the same double coset as τ_r. Given that we have the freedom to change β on the right by an upper triangular unipotent element of K, we may change each β_{ij} $(i < j)$ by any multiple of β_{ii}. If $i, j \in S$ then $\mathfrak{p} | \beta_{ij}$ while $\beta_{ii} = \varpi$, and so we may assume that $\beta_{ij} = 0$. On the other hand if $i \notin S$, then $\beta_{ii} \in \mathfrak{o}^\times$ while $\beta_{ij} \in \mathfrak{o}$, and so

again we may assume that $\beta_{ij} = 0$. On the other hand, if $i \in S$ and $j \notin S$, then β_{ij} may be any element of $\mathfrak{o}$ modulo $\mathfrak{p}$.

With this in mind, let us fix $S = \{\lambda_1, \cdots, \lambda_r\}$, where $\lambda_1 < \lambda_2 < \cdots < \lambda_r$. We ask how many β there are in the decomposition (52) whose diagonal entries equal to ϖ are β_{ii} with $i \in S$. We have just shown that if $i < j$ with $i \in S$ and $j \notin S$, then β_{ij} can be chosen to be an arbitrary element of $\mathfrak{o}/\mathfrak{p}$; and all other entries above the diagonal can be assumed to be zero. If $i = \lambda_1$, there are $n - r - \lambda_1 + 1$ values of j such that $j > i$ and $j \notin S$, so there are $n - r - \lambda_1 + 1$ elements to be chosen inthe λ_1 row, and similarly, there are $n - r - \lambda_2 + 2$ entries to be chosen in the λ_2 row, and so forth; the total number of elements to be chosen is

$$\sum_{i=1}^{r} (n - r - \lambda_i + i) = r\left(n - r - \frac{1}{2}\right) - \sum_{i=1}^{r} \lambda_i,$$

and so the total number of β for this choice of S is

$$q^{r\left(n-r-\frac{1}{2}\right) - \sum_{i=1}^{r} \lambda_i}.$$

For such a β, we have

$$f^\circ(\beta) = \delta^{1/2}(\beta)\, \chi(\beta) = q^{-(n+1)\frac{r}{2} + \sum \lambda_i}\, t_{\lambda_1} \cdots t_{\lambda_r}.$$

Recalling that θ_r is $q^{-r(n-r)/2}$ times the characteristic function of the double coset $K^\circ \tau_r K^\circ$, we see that $(\theta_r f^\circ)(1)$ equals

$$\begin{aligned} & q^{-\frac{r(n-r)}{2}} \sum_{\lambda_1 < \cdots < \lambda_r} q^{r\left(n - \frac{r-1}{2}\right) - \sum_{i=1}^{r} \lambda_i}\; q^{-\frac{(n+1)r}{2} + \sum \lambda_i}\, t_{\lambda_1} \cdots t_{\lambda_r} \\ & = e_r(t_1, \cdots, t_r), \end{aligned}$$

as required. □

10 The Affine Weyl Group

We may extend the Weyl group by a group of translations, and obtain the so-called *affine Weyl group*.

Let Φ be a root system in the vector space V, and let $W = W(\Phi)$ be the Weyl group. We give V a W-invariant inner product $\langle\ ,\ \rangle$. If $\alpha \in \Phi$ and

$k \in \mathbb{Z}$ let $P_{\alpha,k}$ be the hyperplane $P_{\alpha,k} = \{v \in V | \langle \alpha, v \rangle = k\}$. A connected component of

$$V - \bigcup_{\substack{\alpha \in \Phi \\ k \in \mathbb{Z}}} P_{\alpha,k}$$

is called an *open alcove*. They are relatively compact open subsets of V. The closure of an open alcove is called an *alcove*.

Let $\mathcal{C}^+$ be the positive Weyl chamber, so that

$$\mathcal{C}^+ = \{v \in V | \langle \alpha_i, v \rangle \geqslant 0 \ (1 \leqslant i \leqslant r)\}$$

where $\{\alpha_1, \cdots, \alpha_r\}$ are the simple roots. There is a unique alcove in $\mathcal{C}^+$ which contains the origin. This is the *fundamental alcove* $\mathfrak{F}$. Our immediate goal is to describe it more explicitly.

There is a partial order on V in which $v \geqslant 0$ if $v = \sum c_i \alpha_i$ with $c_i \geqslant 0$. We call a root α *highest* if $\alpha' \geqslant \alpha$ for $\alpha' \in \Phi$ implies that $\alpha' = \alpha$. We will see that if Φ is irreducible, this implies more: that actually $\alpha \geqslant \alpha'$ for every root $\alpha' \in \Phi$.

Exercise 9 Let $\alpha, \beta \in \Phi$ be linearly independent. and let U be the two-dimensional space spanned by α and β. Show that $U \cap \Phi$ is a root system in U.

Exercise 10 Assume that Φ is reduced and that α, β are distinct elements of Φ. Show that if $\langle \alpha, \beta \rangle \geqslant 0$ then $\alpha - \beta \in \Phi$. (One way: you may use the previous exercise to reduce to the rank two case, and check this for the four rank two root systems $A_1 \times A_1$, A_2, B_2 and G_2.)

Proposition 41 *Suppose that Φ is irreducible. Then there is a unique root $-\alpha_0$ that is highest with respect to the partial order. If α is any positive root, then $\alpha \leqslant -\alpha_0$ and $\langle \alpha, -\alpha_0 \rangle \geqslant 0$. If α is any root then $\langle \alpha, -\alpha_0 \rangle \leqslant \langle \alpha_0, \alpha_0 \rangle$ with equality if and only if $\alpha = -\alpha_0$.*

It is most useful to use the notation α_0 for the *negative* of the highest root, since then it will play a role exactly analogous to the simple roots $\{\alpha_1, \cdots, \alpha_r\}$ in certain situations.

Proof Suppose that β is a highest root. Since $\beta \geqslant -\beta$, β is positive.

We claim that $\langle \beta, \alpha_i \rangle \geqslant 0$. If not, then $s_i(\beta) = \beta - \frac{2\langle \alpha_i, \beta \rangle}{\langle \alpha_i, \alpha_i \rangle} \alpha_i \geqslant \beta$, contradicting the assumption that β is a highest root.

Write $\beta = \sum k_i \alpha_i$. Clearly any highest root is positive, so $k_i \geqslant 0$. We will show that $k_i > 0$. Otherwise, let $\Sigma = \Sigma_1 \cup \Sigma_2$, where $\Sigma_1 = \{\alpha_i | k_i > 0\}$

and $\Sigma_2 = \{\alpha_i | k_i = 0\}$. Because Φ is irreducible, the simple roots may not be partitioned into two disjoint mutually orthogonal sets. Therefore there is $\alpha_l \in \Sigma_1$ and $\alpha_j \in \Sigma_2$ such that $\langle \alpha_l, \alpha_j \rangle < 0$. Now

$$\langle \beta, \alpha_j \rangle = \left\langle \sum_{\alpha_i \in \Sigma_1} k_i \alpha_i, \alpha_j \right\rangle = \sum_{\alpha_i \in \Sigma_1} k_i \langle \alpha_i, \alpha_j \rangle.$$

All terms on the right are non-positive since $k_l > 0$, and one term ($i = l$) is negative. This contradicts the fact that $\langle \beta, \alpha_i \rangle \geqslant 0$, proving that all $k_i > 0$.

Now let γ be another highest weight. Consider $\langle \beta, \gamma \rangle = \sum k_i \langle \alpha_i, \gamma \rangle$. We have $\langle \alpha_i, \gamma \rangle \geqslant 0$ with strict inequality for some i, and $k_i > 0$, so $\langle \beta, \gamma \rangle > 0$. It follows from Exercise 10 that $\beta - \gamma$ is a root. Either $\beta - \gamma \in \Phi^+$, in which case $\beta = \gamma + (\beta - \gamma)$, contradicting the maximality of γ, or $\beta - \gamma \in \Phi^-$, in which case $\gamma = \beta + (\gamma - \beta)$, contradicting the maximality of β. This contradiction shows that the highest root is unique. (We are therefore justified in naming it, and we call it $-\alpha_0$.)

Now suppose that α is any positive root. We can write $\alpha = \sum n_i \alpha_i$ with $n_i \geqslant 0$, and $\langle \beta, \alpha \rangle = \sum n_i \langle \beta, \alpha_i \rangle \geqslant 0$. By Exercise 10, $\beta - \alpha$ is a root. It cannot be a negative root, since then $\alpha = \beta + (\alpha - \beta)$ would contradict the maximality of β. Since $\beta - \alpha$ is a positive root, we have $\beta \geqslant \alpha$.

Next we show that if γ is any root then $\langle \gamma, \beta \rangle \leqslant \langle \beta, \beta \rangle$ with equality only in the case $\gamma = \beta$. We embed γ and β in a rank two root system $\Phi_0 = \Phi \cap V_0$ where V_0 is the vector space they span. Then Φ_0 is one of $A_1 \times A_1$ or A_2, B_2 or G_2. Except in the first case β is the unique highest weight vector, and in every case, the assertion may be checked by inspection. We leave the verification to the reader. □

Let α_0 be the negative of the highest root. We see that

$$\langle \alpha_i, \alpha_j \rangle \geqslant 0 \qquad \text{if } \alpha_i, \alpha_j \in \{\alpha_0, \alpha_1, \cdots, \alpha_r\},\ i \neq j.$$

Indeed, this is part of Proposition 12 if $\alpha_i, \alpha_j \in \Sigma$ and Proposition 41 if one of α_i is α_0.

Proposition 42 *The fundamental alcove $\mathfrak{F}$ is defined by the inequalities*

$$\langle \alpha_i, v \rangle \geqslant 0 \quad (1 \leqslant i \leqslant r), \qquad \langle \alpha_0, v \rangle \geqslant -1. \tag{53}$$

Proof It is clear that the fundamental alcove is determined by the inequalities $\langle \alpha_i, v \rangle \geqslant 0$ and $\langle \alpha, v \rangle \leqslant 1$ as α runs through the positive roots. We

have to show that the inequalities $\langle \alpha, v\rangle \leqslant 1$ all follow from the inequality $\langle -\alpha_0, v\rangle \leqslant 1$, which is equivalent to the assumed inequality $\langle \alpha_0, v\rangle \geqslant -1$. Indeed, if α is any positive root, then $\alpha \leqslant -\alpha_0$, so we may write $\alpha = -\alpha_0 - \sum k_i\alpha_i$ with $k_i \geqslant 0$. Then $\langle \alpha, v\rangle = \langle -\alpha_0, v\rangle - \sum k_i\langle \alpha_i, v\rangle$. However if α is already assumed to satisfy he first inequalities in (53), then $\langle \alpha_i, v\rangle \geqslant 0$, so $\langle \alpha, v\rangle \leqslant \langle -\alpha_0, v\rangle$. Hence the inequality $\langle -\alpha_0, v\rangle \leqslant 1$ is sufficient to imply $\langle \alpha, v\rangle \leqslant 1$ for all positive roots α, and thus the fundamental alcove is indeed determined by the given inequalities. □

If $\alpha \in \Phi$ and $k \in \mathbb{Z}$ we consider the reflection $r_{\alpha,k}$ in the hyperplane $P_{\alpha,k}$. This is the map

$$r_{\alpha,-k} = v - \langle \alpha^\vee, v\rangle\alpha + k\alpha^\vee = v - \langle \alpha, v\rangle\alpha^\vee + k\alpha^\vee.$$

We have $P_{\alpha,k} = P_{-\alpha,-k}$ and $r_{-\alpha,-k} = r_{\alpha,k}$. Let $s_i = r_{\alpha_i,0}$ $(1 \leqslant i \leqslant r)$ and $s_0 = r_{\alpha_0,-1}$. These are the reflections in the hyperplanes bounding the fundamental alcove.

Proposition 43 *The group W_{aff} is generated by the s_i.*

Proof Let $w \in W_{\text{aff}}$. Then $w\mathfrak{F}$ is an alcove. We consider a path p from an interior vertex of $\mathfrak{F}$ to an interior vertex of $w\mathfrak{F}$. Let $\mathfrak{F}_0 = \mathfrak{F}, \mathfrak{F}_1, \cdots, \mathfrak{F}_k = w\mathfrak{F}$ be the series of alcoves through which p passes. Each pair $\mathfrak{F}_i, \mathfrak{F}_{i+1}$ is separated by a $P_{\alpha,k}$.

Since $\mathfrak{F}_1$ is adjacent to $\mathfrak{F}_0 = \mathfrak{F}$, by Proposition 42 we have $\mathfrak{F}_1 = s_{i_1}\mathfrak{F}$ for some $0 \leqslant i_1 \leqslant r$. Now $\mathfrak{F}_2$ is adjacent to $\mathfrak{F}_1$, so $s_{i_1}^{-1}\mathfrak{F}_2$ is adjacent to $s_{i_1}^{-1}\mathfrak{F}_1 = \mathfrak{F}$. Thus $s_{i_1}^{-1}\mathfrak{F}_2 = s_{i_2}\mathfrak{F}$ for some $0 \leqslant i_2 \leqslant r$, and so $\mathfrak{F}_2 = s_{i_1}s_{i_2}\mathfrak{F}$. Continuing this way we obtain a sequence $i_1, i_2, \cdots$ such that $\mathfrak{F}_l = s_{i_1}\cdots s_{i_l}\mathfrak{F}$. Now $w\mathfrak{F} = s_{i_1}\cdots s_{i_k}\mathfrak{F}$ implies that $w = s_{i_1}\cdots s_{i_k}$, proving that W_{aff} is generated by the s_i. □

Theorem 13 *W_{aff} is a Coxeter group with generators $\{s_0, s_1, \cdots, s_r\}$.*

Proof Let us suppose that

$$s_{i_1}\cdots s_{i_k} = s_{j_1}\cdots s_{j_l}$$

are two words representing the same element $w \in W_{\text{aff}}$. Let G be the group with generators $\sigma_0, \cdots \sigma_r$ and relations $\sigma_i^2 = 1$ and $(\sigma_i\sigma_j)^{m(i,j)} = 1$, where $m(i,j)$ is the order of s_is_j. We want to show that $\sigma_{i_1}\cdots\sigma_{i_k} = \sigma_{j_1}\cdots\sigma_{j_l}$.

If $t = 1, 2, 3, \cdots$ let S_t be the set of all affine subspaces M of V that are the interesection of t or more hyperplanes $P_{\alpha,k}$ ($\alpha \in \Phi$, $k \in \mathbb{Z}$) such that $\dim(M) = \dim(V) - t$. Thus S_1 consists of the set of hyperplanes $P_{\alpha,k}$ themselves. Observe that $\Omega = V - \bigcup S_3$ is simply-connected since the removed sets consists of closed affine spaces of codimenion 3 with no accumulation point.

The alcove $s_{i_1}\mathfrak{F}$ is adjacent to $\mathfrak{F}$, separated by a hyperplane. Also, $s_{i_2}\mathfrak{F}$ is adjacent to $\mathfrak{F}$ so $s_{i_1}s_{i_2}\mathfrak{F}$ is adjacent to $s_{i_1}\mathfrak{F}$. We therefore get a sequence of alcoves:

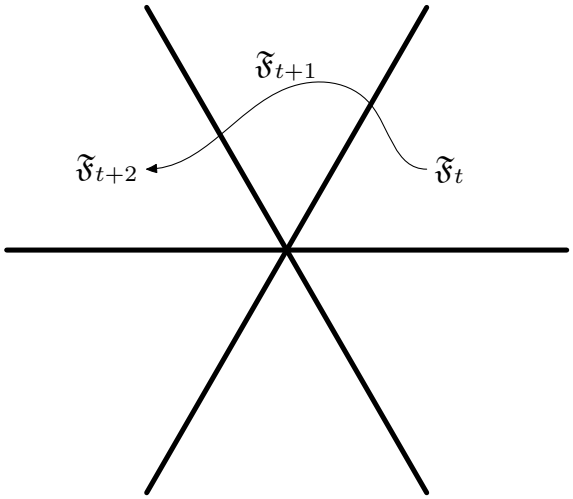
$$\mathfrak{F}, s_{i_1}\mathfrak{F}, s_{i_1}s_{i_2}\mathfrak{F}, \cdots, s_{i_1}s_{i_2}\cdots s_{i_k}\mathfrak{F} = \mathfrak{F}_0, \mathfrak{F}_1, \cdots, \mathfrak{F}_k.$$

We take a path p from a point u in the interior of $\mathfrak{F}$ to a point v in the interior of $\mathfrak{F}_k = w\mathfrak{F}$, passing through these alcoves in order. Similarly we have another path p' from u to v passing through the alcoves $\mathfrak{F}'_0, \mathfrak{F}'_1, \cdots, \mathfrak{F}'_l$, where $\mathfrak{F}'_t = s_{j_1}\cdots s_{j_t}\mathfrak{F}$, with $\mathfrak{F}'_0 = \mathfrak{F}_0$ and $\mathfrak{F}'_l = \mathfrak{F}_k = w\mathfrak{F}$. The paths p and p' both lie in the simply connected space Ω.

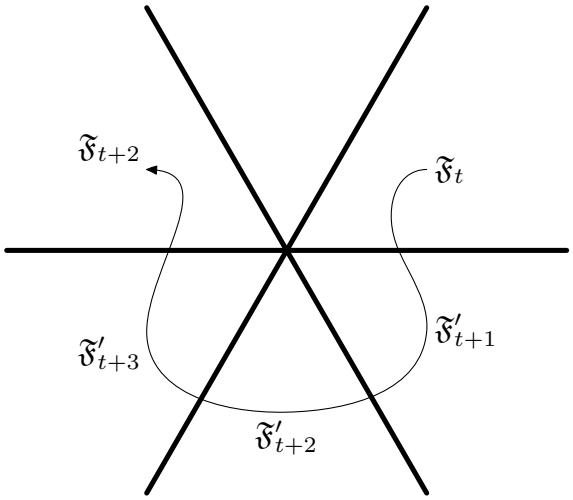
We deform p into p' and observe how the set of alcoves changes as we make this deformation. We stay within Ω at every stage. We are allowed to cross elements of S_2 but not S_3. We arrange so that we cross elements of S_2 one at a time and observe how the word $s_{i_1}\cdots s_{i_k}$ representing w changes when we do. We will see that each such change corresponds to a use of the braid relation.

Since we may never pass through a space M in S, the only types of transitions that can occur have the path move across a subset M in S_2. We may visualize this by taking a cross section in a 2-dimensional affine space perpendicular to M, and projecting the path onto that path. The homotopy

thus moves $p_0 = p$, one segment of which might look like this:



to an equivalent path p_1, whose corresponding segment looks like this:



Now if we have $\mathfrak{F}_t = s_{i_1} \cdots s_{i_t} \mathfrak{F}$, $\mathfrak{F}_{t+1} = s_{i_1} \cdots s_{i_{t+1}} \mathfrak{F}$, $\mathfrak{F}_{t+2} = s_{i_1} \cdots s_{i_{t+2}} \mathfrak{F}$. On the other hand (in this example)

$$\begin{aligned}
\mathfrak{F}'_{t+1} &= s_{i_1} \cdots s_{i_t} s_{i_{t+2}} \mathfrak{F}, \\
\mathfrak{F}'_{t+2} &= s_{i_1} \cdots s_{i_t} s_{i_{t+2}} s_{i_{t+1}} \mathfrak{F}, \\
\mathfrak{F}'_{t+3} &= s_{i_1} \cdots s_{i_t} s_{i_{t+2}} s_{i_{t+1}} s_{i_{t+2}} \mathfrak{F}, \\
\mathfrak{F}'_{t+3} &= s_{i_1} \cdots s_{i_t} s_{i_{t+2}} s_{i_{t+1}} s_{i_{t+2}} s_{i_{t+1}} \mathfrak{F} = \mathfrak{F}_{t+2}.
\end{aligned}$$

So this homotopy replaces the word $s_{i_1} \cdots s_{i_k}$ by

$$s_{i_1} s_{i_1} \cdots s_{i_t} s_{i_{t+2}} s_{i_{t+1}} s_{i_{t+2}} s_{i_{t+1}} s_{i_{t+3}} \cdots s_{i_k}.$$

In this example, the order of $s_{i_t} s_{i_{t+1}}$ is 3, so $(\sigma_{i_t} \sigma_{i_{t+1}})^3 = 1$ and

$$\sigma_{i_{t+1}} \sigma_{i_t} = \sigma_{i_{t+1}} \sigma_{i_t} \sigma_{i_{t+1}} \sigma_{i_t},$$

Thus this homotopy crossing the affine subspace M of codimension 2 replaces $\sigma_{i_1} \cdots \sigma_{i_t}$ by

$$\sigma_{i_1} \sigma_{i_1} \cdots \sigma_{i_{t-1}} \sigma_{i_{t+1}} \sigma_{i_t} \sigma_{i_{t+1}} \sigma_{i_t} \sigma_{i_{t+1}} \cdots \sigma_{i_k},$$

but these are equal in the group G. Continuing in this way, we eventually get $\sigma_{i_1} \cdots \sigma_{i_k} = \sigma_{j_1} \cdots \sigma_{j_l}$.

We have done just one example of crossing an element M of S_2 but clearly any such crossing amounts to an application of a braid relation. We see thus that W_{aff} is a Coxeter group. □

We wish to have analogs of the roots. These will be the *affine roots*, which in our interpretation are affine-linear functions on V that vanish on the hyperplanes $P_{\alpha,k}$.

Remark 1 Our definition of the affine roots is that given by Macdonald. However in view of the work of Kac and of Moody on infinite-dimensional Lie algebras, the affine roots of Macdonald should be supplemented by other "imaginary" roots. We will ignore the imaginary roots since they play no role for us.

If $\alpha \in \Phi$ let

$$\alpha^\vee = \frac{2\alpha}{\langle \alpha, \alpha \rangle}.$$

The $\alpha^\vee$ are called *coroots*, and the set $\hat{\Phi}$ of coroots is called the *dual root system*. If $\alpha \in \Phi$ and $k \in \mathbb{Z}$ let $L_{\alpha,k} : V \longrightarrow \mathbb{R}$ be the linear functional

$$L_{\alpha,k}(v) = \langle \alpha, v \rangle - k.$$

Then $L_{\alpha,k}$ vanishes on $P_{\alpha,k}$, as does $L_{-\alpha,-k} = -L_{\alpha,k}$.

The Weyl group acts on the roots by $wL(v) = L(w^{-1}v)$.

We note that a root L never vanishes on an alcove. Let us say that an affine root L is *positive* (resp. *negative*) if its values are positive (negative) on the fundamental alcove $\mathfrak{F}$. Let Φ^+_{aff} be the positive affine roots and Φ^-_{aff} be the negative ones. If $1 \leqslant i \leqslant r$ let $L_i = L_{\alpha_i,0}$ and $P_i = P_{\alpha_i,0}$. Let $L_0 = L_{\alpha_0,-1}$ and $P_0 = P_{\alpha_0,-1}$.

Proposition 44 *Let $0 \leqslant i \leqslant r$ and let L be a positive root. Then $s_i(L) \in \Phi^-$ if and only if $L = L_i$.*

Proof If $L = L_{\alpha,k}$, then $s_i(L)$ is a negative root if and only if $L(s_i v) < 0$, where $v \in \mathfrak{F}$. Since $L(v) > 0$, v and $s_i(v)$ must lie on opposite sides of the hyperplane $L_{\alpha,k}$. But the only hyperplane among the $P_{\alpha,k}$ that separates v and $s_i(v)$ is P_i, and so $P_{\alpha,k} = P_i$. Since L is a positive root, $L = L_i$. □

Let $Q^\vee$ be the lattice generated by the coroots. If $\lambda \in Q^\vee$ let $\tau(\lambda) : V \longrightarrow V$ be the map $\tau(\lambda)v = v + \lambda$. We may identify $Q^\vee$ with its image under τ as a group of translations.

Proposition 45 *The subgroup $Q^\vee$ is normal in W_{aff} and W_{aff} is the semidirect product $Q^\vee \rtimes W$.*

Proof Translation by $\alpha_i^\vee$ moves $P_{\alpha,k}$ to $P_{\alpha,l}$ where $l = k + \langle \alpha_i^\vee, \alpha \rangle$ so $l \in \mathbb{Z}$ if $k \in \mathbb{Z}$. Thus translation by an element of the coroot lattice permutes the alcoves, and corresponds to an element of W_{aff}.

The coroot lattice $Q^\vee$ is invariant under W_{aff}, since the reflection in $P_{\alpha,k}$ moves any vector v to $v + (k - \langle \alpha, v \rangle)\alpha^\vee$; it sends a coroot $\beta^\vee$ to $\beta^\vee + (k - \langle \alpha, \beta^\vee \rangle)\alpha^\vee$ which is also in the coroot lattice. If $\mathfrak{G}$ is any alcove, then $\mathfrak{G} = w\mathfrak{F}$ for some $w \in W_{\text{aff}}$, so $\mathfrak{G}$ contains $\lambda = w(0)$ which we see is an element of $Q^\vee$. Therefore $\tau(-\lambda)w$ is an element of W_{aff} that fixes 0, hence is an element of W. This shows that $W_{\text{aff}} = Q^\vee W$. □

We will prove results about the *length function* that are analogous to those for the ordinary Weyl group in Section 4. As in that section, there are two definitions that are eventually shown to be equivalent.

As with the ordinary Weyl group the first definition makes $l : W_{\text{aff}} \longrightarrow \mathbb{Z}$ the minimal length of a decomposition $w = s_{i_1} \cdots s_{i_k}$. The second definition, temporarily denoted l' until we prove that they are the same, is the number of $L \in \Phi^+$ such that $w(L) \in \Phi^-$.

Lemma 8 *$l'(w)$ is the number of hyperplanes $P_{\alpha,k}$ that lie between $\mathfrak{F}$ and $w^{-1}\mathfrak{F}$.*

Proof If $L = L_{\alpha,k} \in \Phi^+$, then $w(L) \in \Phi^-$ if and only if $L(w^{-1}v) < 0$ for $v \in \mathfrak{F}$. This means that $P_{\alpha,k}$ is a hyperplane between $\mathfrak{F}$ and $w^{-1}\mathfrak{F}$. □

From the Lemma, $l'(w) < \infty$.

Proposition 46 *Let $w \in W_{\text{aff}}$ and let $s = s_i$, $L = L_i$ for $0 \leqslant i \leqslant r$. Then*

$$l'(ws) = \begin{cases} l'(w) + 1 & \text{if } w(L) \in \Phi^+, \\ l'(w) - 1 & \text{if } w(L) \in \Phi^-. \end{cases}$$

Proof We have $l'(w) = |\Phi^+ \cap w^{-1}\Phi^-|$. Therefore $l'(ws) = |\Phi^+ \cap s^{-1}w^{-1}\Phi^-|$. Applying s replaces this set with one of equal cardinality, so $l'(ws) = |s\Phi^+ \cap w^{-1}\Phi^-|$. Now by Proposition 44, $s\Phi^+$ is obtained from Φ^+ by removing $L = L_i$ and replacing it by its negative. From this it is clear that $l'(ws) = l'(w)+1$ if $L \in w^{-1}\Phi^+$, that is, if $wL \in \Phi^+$, and $l'(w) - 1$ otherwise. □

Theorem 14 *The Exchange property (Propositions 14 and 15) is true for the affine Weyl group. The two definitions of the length function are the same: $l = l'$. Tits' Theorem 23 remains true.*

Tits' Theorem, in this context, says the following. Let B be the braid group with generators $u_0, u_1, \cdots, u_r$ subject to the same braid relations satisfied by the s_i. Then if $w \in W_{\text{aff}}$ has two reduced representations $w = s_{i_1} \cdots s_{i_k} = s_{j_1} \cdots s_{j_k}$ as products of simple reflections with $k = l(w)$, then $u_{i_1} \cdots u_{i_k} = u_{j_1} \cdots u_{j_k}$.

Proof The proofs of Section 4 go through without much change. We leave the details to the reader. (One also gets another proof that W_{aff} is a Coxeter group.) □

Proposition 47 (Iwahori and Matsumoto) *Let $d \in Q^\vee$ and $w \in W$. Let $L = L_i$ where $1 \leqslant i \leqslant r$. Then*

$$l(\tau(d)ws_i) = \begin{cases} l(\tau(d)w) + 1 & \text{if } w(\alpha_i) \in \Phi^+ \text{ and } \langle w(\alpha_i), d\rangle \leqslant 0, \\ & \text{or } w(\alpha_i) \in \Phi^- \text{ and } \langle w(\alpha_i), d\rangle < 0. \\ l(\tau(d)w) - 1 & \text{if } w(\alpha_i) \in \Phi^+ \text{ and } \langle w(\alpha_i), d\rangle > 0, \\ & \text{or } w(\alpha_i) \in \Phi^- \text{ and } \langle w(\alpha_i), d\rangle \geqslant 0. \end{cases}$$

Moreover

$$l(\tau(d)ws_0) = \begin{cases} l(\tau(d)w) + 1 & \text{if } w(\alpha_0) \in \Phi^+ \text{ and } \langle w(\alpha_0), d\rangle \leqslant 1, \\ & \text{or } w(\alpha_0) \in \Phi^- \text{ and } \langle w(\alpha_0), d\rangle < 1, \\ l(\tau(d)w) - 1 & \text{if } w(\alpha_0) \in \Phi^+ \text{ and } \langle w(\alpha_0), d\rangle > 1, \\ & \text{or } w(\alpha_0) \in \Phi^- \text{ and } \langle w(\alpha_0), d\rangle \geqslant 1. \end{cases}$$

Proof Let $1 \leqslant i \leqslant r$. By Proposition 46, a necessary and sufficient condition for $l(\tau(d)ws_i) = l(\tau(d)w) + 1$ is that $\tau(d)w(L_i) \in \Phi^+$. This means that for $v \in \mathfrak{F}$ we need $\langle (\tau(d)w)^{-1}(v), \alpha_i \rangle > 0$, that is, $\langle v - d, w(\alpha_i) \rangle > 0$. We may take v near the origin. Then $\langle v, w(\alpha_i) \rangle$ will be small, while $\langle -d, w(\alpha_i) \rangle \in \mathbb{Z}$. If $\langle w(\alpha_i), d \rangle$ is nonzero, then $\langle v - d, w(\alpha_i) \rangle > 0$ depending on whether $\langle w(\alpha_i), d \rangle < 0$ or > 0. On the other hand, if $\langle w(\alpha_i), d \rangle = 0$, then $\langle v - d, w(\alpha_i) \rangle > 0$ or < 0 depending on whether $w(\alpha_i)$ is a positive or negative root, because v is in the positive Weyl chamber. This proves the first case. We leave the second one (with $i = 0$) to the reader, but similar considerations suffice. □

Let us say that $w \in W_{\text{aff}}$ is *dominant* if $w(\mathfrak{F})$ is contained in the positive Weyl chamber. If $d \in Q^\vee$ then clearly d is dominant in this sense if and only if it is dominant in the usual sense: $\langle \alpha, d \rangle \geqslant 0$ for all $\alpha \in \Phi$.

Proposition 48 *Suppose $d \in Q^\vee$ and that d is dominant. Then*

$$l(d) = \sum_{\alpha \in \Phi^+} \langle \alpha, d \rangle = \langle 2\rho, d \rangle.$$

Here $\rho = \frac{1}{2} \sum_{\alpha \in \Phi} \alpha$ is the Weyl vector.

Proof The length $l(d)$ is equal to the number of hyperplanes $H_{\alpha,k}$ between $\mathfrak{F}$ and $\tau(d)\mathfrak{F}$. The hyperplane $H_{\alpha,k}$ lies between $\mathfrak{F}$ and $\tau(d)\mathfrak{F}$ if and only if $0 < k \leqslant \langle \alpha, d \rangle$. There are $\langle \alpha, d \rangle$ of this, and summing over α, the statement follows. □

11 Extended Dynkin Diagrams and Coxeter Groups

Beyond the Dynkin diagram, there is also an *extended Dynkin diagram* for each Cartan type. These too are tabulated by Bourbaki. The weights have a partial order in which $\lambda \geqslant \mu$ if $\lambda - \mu = \sum k_i \alpha_i$ where α_i are the simple roots and $k_i \geqslant 0$. There is a unique highest root with respect to this order. Let α_0 be the negative root such that $-\alpha_0$ is this highest root. Then we adjoin α_0 to the set $\{\alpha_1, \cdots, \alpha_r\}$ of simple positive roots, and draw the extended Dynkin diagram by the same recipe as before based on the angle between two (extended) roots: no edge between i and j if α_i and α_j are orthogonal,

double edge if they make an angle of $2\pi/3$, and so forth. This results in the *extended Dynkin diagram*.

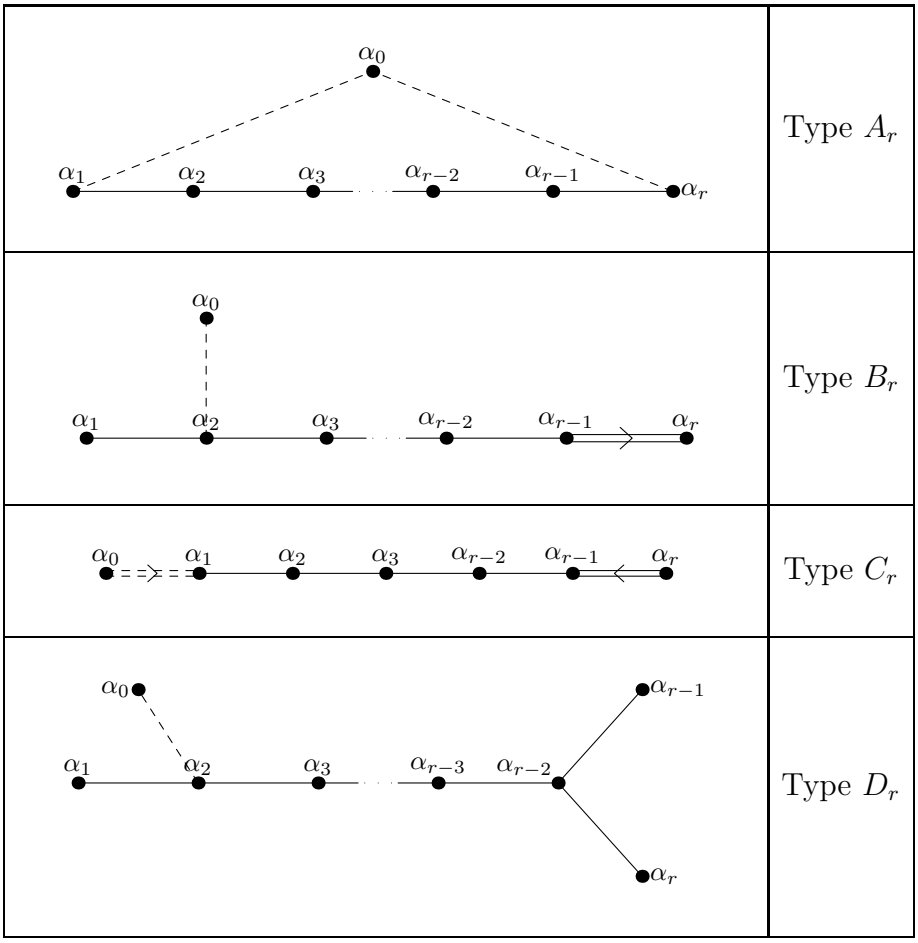


Table 3: Extended Dynkin diagrams of the classical Cartan types.

Given the extended Dynkin diagram, we may make a Coxeter group using the same recipe that we used for the ordinary Weyl group. That is, it has

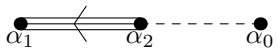
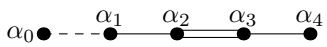
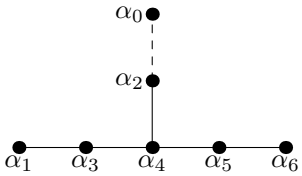
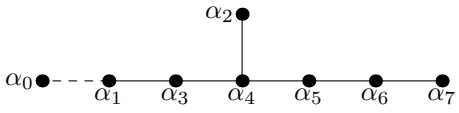
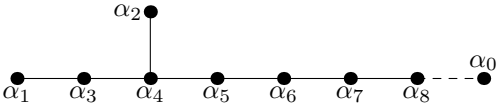
	Type G_2
	Type F_4
	Type E_6
	Type E_7
	Type E_8

Table 4: Extended Dynkin diagrams of the exceptional Cartan types.

one generator s_i for each node i in the diagram, with the braid relations:

$$\begin{cases} s_i s_j = s_j s_i & \text{if } i \text{ and } j \text{ are not joined by an edge,} \\ s_i s_j s_i = s_j s_i s_i & \text{if } i, j \text{ are joined by a single edge,} \\ s_i s_j s_i s_j = s_j s_i s_j s_i & \text{if } i, j \text{ are joined by a double edge,} \\ s_i s_j s_i s_j s_i s_j = s_j s_i s_j s_i s_j s_i & \text{if } i, j \text{ are joined by a triple edge.} \end{cases}$$

We have already seen that this is the affine Weyl group, and it is denoted $A_r^{(1)}, B_r^{(1)}, C_r^{(1)}, \cdots$ in the notation of Kac, *Infinite-dimensional Lie algebras*.

12 Roots and Coroots

If G is a semisimple algebraic group, there are two root systems Φ and $\hat{\Phi}$ associated with G, which are in duality: there is a bijection $\alpha \longrightarrow \hat{\alpha}$ from the roots in Φ to the coroots in $\hat{\Phi}$. The Weyl groups W are isomorphic, but long roots in Φ correspond to short roots in $\hat{\Phi}$.

For many purposes it is useful to put the roots and coroots in the same vector space V, so that we can write (as we have been writing)

$$\alpha^\vee = \frac{2\alpha}{\langle \alpha, \alpha \rangle}. \tag{54}$$

However Φ and $\hat{\Phi}$ arise differently, and in this section we will describe them as living in different vector spaces, V and its dual space V^*. The reason we may put them together is that the ambient space V of Φ has a W-invariant inner product, so we may identify it with V^*. But let us keep them separated for the moment.

Let T be a maximal torus of G, which we will assume to be defined and split over F. Thus $T \cong G_{\mathrm{m}}^r$ for some r, the *rank* of G. We will denote by $X_*(T) \cong \mathbb{Z}^r$ the group of one-parameter subgroups, that is, algebraic homomorphisms $G_{\mathrm{m}} \longrightarrow T$, and by $X^*(T) \cong \mathbb{Z}^r$ the group of rational characters, that is, algebraic homomorphisms $T \longrightarrow G_{\mathrm{m}}$. There is a dual pairing between these groups, since given a one parameter subgroup $i : G_{\mathrm{m}} \longrightarrow T$ and a character $\lambda : T \longrightarrow G_{\mathrm{m}}$, the composition is an endomorphism of G_{m} of the form $x \mapsto x^k$, so $(i, \lambda) \longrightarrow k$ gives a pairing $X_*(T) \times X^*(T) \longrightarrow \mathbb{Z}$. We will denote this by $\langle\ ,\ \rangle$.

Let $V = \mathbb{R} \otimes X^*(T)$ and $V^* = \mathbb{R} \otimes X_*(T)$. The roots Φ will live in V, and the coroots $\hat{\Phi}$ will live in V^*. The roots, as we have mentioned, are the nonzero elements of $X^*(T)$ that occur in the adjoint representation $\mathrm{Ad} : G \longrightarrow \mathrm{End}(\mathfrak{g})$, where $\mathfrak{g}$ is the Lie algebra of G. The *coroots* are elements of the dual module of $X^*(T)$ that implement the simple reflections. That is, we have for every root α a simple reflection $s_\alpha : X^*(T) \longrightarrow X^*(T)$, and there is a unique element $\alpha^\vee$ of the dual module $X_*(T)$ of $X^*(T)$ such that for $\lambda \subset X^*(T)$ we have

$$s_\alpha(\lambda) = \lambda - \langle \lambda, \alpha^\vee \rangle \alpha.$$

Then $\alpha^\vee$ is a *coroot*.

If G and G' are connected algebraic groups, an *isogeny* is a morphism $f : G \longrightarrow G'$ that is a finite covering map. The map f will be surjective in

the sense of algebraic groups. However the induced map $G(F) \longrightarrow G'(F)$ may not be surjective if the ground field F is not algebraically closed. For example if F is a finite field, $G(F)$ and $G'(F)$ will have the same number of elements. Given $g' \in G'(F)$ there exists $g \in G(\bar{F})$ such that $f(g) = g'$, but g may not be rational over F. For semisimple algebraic groups, the kernel of an isogeny f will always be a subgroup of the finite center.

The semisimple group G is *simply-connected* if there are no nontrivial isogenies $G' \longrightarrow G$. If the ground field is $\mathbb{C}$, this is equivalent to $G(\mathbb{C})$ being simply-connected in the topological sense. We say G is *adjoint-type* if there are no nontrivial isogenies $G \longrightarrow G'$. This means that the center of G is trivial.

Given a Cartan type, there is a unique simply connected group in the corresponding isogeny class, which we will denote G_{sc}. It has a finite center, and we will denote $G_{\mathrm{sc}}/Z(G_{\mathrm{sc}})$ as G_{ad}, the *adjoint form*. The group $\pi_1(G_{\mathrm{ad}}) \cong Z(G_{\mathrm{sc}})$ is a finite abelian group. It may be shown that it is isomorphic to P/Q where Q is the root lattice (spanned by the roots in V) and P is the weight lattice (consisting of $\lambda \in V$ such that $\langle \lambda, \alpha^\vee \rangle \in \mathbb{Z}$ for all coroots $\alpha^\vee$). It is given in the following table for the simple Cartan types.

Cartan Type	$\pi_1(G_{\mathrm{ad}})$
A_r	Z_{r+1}
B_r	Z_2
C_r	Z_2
D_r	$\begin{cases} Z_4 & r \text{ odd} \\ Z_2 \times Z_2 & r \text{ even} \end{cases}$
E_6	Z_3
E_7	Z_2
E_8	1
F_4	1
G_2	1

$(Z_n = \mathbb{Z}/n\mathbb{Z})$

Table 5: Fundamental groups of simple groups of Lie type.

Let T_{sc} and T_{ad} be split maximal tori in G_{sc} and G_{ad}, arranged so the isogeny $G_{\mathrm{sc}} \longrightarrow G_{\mathrm{ad}}$ maps $T_{\mathrm{sc}} \longrightarrow T_{\mathrm{ad}}$. The fundamental group of G_{ad} is the

center of $G_{\rm sc}$. We have maps:

$$\begin{array}{cc} X_*(T_{\rm sc}) & X^*(T_{\rm sc}) \\ \downarrow & \uparrow \\ X_*(T_{\rm ad}) & X^*(T_{\rm ad}) \end{array} \tag{55}$$

They are of course all injective. It is useful to bear in mind that the roots span $X^*(T_{\rm ad})$ and that the coroots span $X_*(T_{\rm sc})$.

It is useful to have embeddings $\mathrm{SL}_2 \longrightarrow G$ which have good integrality properties. One way to do this is to realize the Lie algebra $\mathfrak{g}_F = F \otimes_{\mathbb{Z}} \mathfrak{g}_{\mathbb{Z}}$ where $\mathfrak{g}_{\mathbb{Z}}$ is a Lie algebra defined over $\mathbb{Z}$. It was proved by Chevalley, Sur certains groupes simples, *TÃĭhoku Math. J. (2)*, 7:14–66, 1955, that every semisimple complex Lie algebra $\mathfrak{g}_{\mathbb{C}}$ had such a basis. By tensoring this with an arbitrary field F, one obtains a Lie algebra $\mathfrak{g}_F$, and the Lie algebras of semisimple split reductive groups can all be obtained this way.

To give a bit more detail, the semisimple Lie algebra $\mathfrak{g} = \mathfrak{g}_F$ decomposes via the adjoint representation as

$$\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha,$$

where $\mathfrak{t}$ is the Lie algebra of T and $\mathfrak{g}_\alpha$ is the root eigenspace. Chevalley showed that we may choose elements X_α of $\mathfrak{g}_\alpha$ such that $[X_\alpha, X_\beta] = \pm(p+1)X_{\alpha+\beta}$ when $\alpha, \beta \in \Phi$ are such that $\alpha + \beta$ is a root, where p is the greatest integer such that $\beta - p\alpha \in \Phi$. Moreover, if $H_\alpha = [X_\alpha, X_{-\alpha}]$ then $H_\alpha \in \mathfrak{t}$, and $[H_\alpha, X_\beta] = \langle \beta, \alpha^\vee \rangle X_\beta$. Thus the $H_\alpha \in \mathfrak{t}$ themselves form a root system isomorphic to $\hat{\Phi}$, and sometimes the H_α are called coroots, though we will use that term differently.

The group $G_{\rm ad}$ may then be taken to be the group of inner automorphisms of $\mathfrak{g}$. The group $G_{\rm sc}$ may be taken to be the universal covering group of $G_{\rm ad}$.

For every $\alpha \in \Phi$, the elements $X_\alpha, X_{-\alpha}$ and H_α satisfy

$$[H_\alpha, X_\alpha] = 2X_\alpha, \qquad [H_\alpha, X_{-\alpha}] = -2X_{-\alpha}, \qquad [X_\alpha, X_{-\alpha}] = H_\alpha.$$

These are the defining relations of the SL_2 Lie algebra. Since SL_2 is simply connected, it follows that there is a homomorphism $i_\alpha : \mathrm{SL}_2 \longrightarrow G$ such that the induced map di_α on Lie algebras that satisfies

$$di_\alpha \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} = H_\alpha, \qquad di_\alpha \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = X_\alpha, \qquad di_\alpha \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = X_{-\alpha}.$$

As elements of $X_*(T)$, the coroots are the homomorphisms $\alpha^\vee : G_{\rm m} \longrightarrow T$ defined by

$$t \longmapsto i_\alpha \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix}.$$

It would be correct but potentially confusing to write this as $\alpha^\vee(t)$ so we will write instead

$$h_{\alpha^\vee}(t) = i_\alpha \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix}. \tag{56}$$

We will also make use of homomorphism $x_\alpha : F \longrightarrow G(F)$ defined for $\alpha \in \Phi$ by

$$x_\alpha(u) = i_\alpha \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}. \tag{57}$$

Then

$$x_{-\alpha}(u) = i_\alpha \begin{pmatrix} 1 & \\ x & 1 \end{pmatrix}.$$

Proposition 49 *If $t, u \in F$ and $t \neq 0$ then for $\alpha, \beta \in \Phi$ we have*

$$h_{\alpha^\vee}(t) x_\beta(u) h_{\alpha^\vee}(t)^{-1} = x_\beta(t^{\langle \alpha^\vee, \beta \rangle} u). \tag{58}$$

If $w \in W$ then

$$w h_{\alpha^\vee}(t) w^{-1} = h_{w(\alpha)^\vee}(\pm t). \tag{59}$$

Proof Equation (58) is an exponentiated version of the formula

$$\mathrm{Ad}(h_{\alpha^\vee}(t)) X_\beta = t^{\langle \alpha^\vee, \beta \rangle} X_\beta,$$

which is what we will verify. Since X_β spans a root eigenspace and $i_\alpha \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix}$ there is some integer k such that $\mathrm{Ad}\left(i_\alpha \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix} \right) X_\beta = t^k X_\beta$. To determine k, we remember how to pass from an action of the Lie group to the Lie algebra: we differentiate and set $t = 0$. In other words, if $\rho : G \longrightarrow \mathrm{GL}(V)$ is a representation and $X \in \mathfrak{g}$, $v \in V$ then

$$d\rho(X) v = \frac{d}{dt} \exp(tX) v|_{t=0}.$$

If $\rho = \mathrm{Ad}$ then $d\rho = \mathrm{ad}$. Thus

$$\mathrm{ad}(H_\alpha) X_\beta = \frac{d}{dt} \mathrm{Ad}(tH_\alpha) X_\beta|_{t=0} = \frac{d}{dt} \mathrm{Ad}\left(i_\alpha \begin{pmatrix} e^t & \\ & e^{-1} \end{pmatrix} X_\beta \right)|_{t=0} = \frac{d}{dt} e^{kt} X_\beta|_{t=0} = k X_\beta.$$

On the other hand, $\mathrm{ad}(H_\alpha)X_\beta = [H_\alpha, X_\beta] = \langle \beta, \alpha^\vee \rangle X_\beta$. Therefore $k = \langle \beta, \alpha^\vee \rangle$.

The action of W on $T(F)$ and hence on $X_*(T(F))$ is by conjugation, and so (59) is also true. $\square$

Let us consider an example. Let $G = \mathrm{Sp}_4$. This group is simply-connected. It is the group of $g \in \mathrm{SL}_4$ such that

$$gJ^t g = J, \qquad J = \begin{pmatrix} & & & -1 \\ & & -1 & \\ & 1 & & \\ 1 & & & \end{pmatrix}.$$

Then $\mathfrak{g}$ is the Lie algebra of matrices of trace 0 satisfying $XJ + J^t X = 0$. Let T be the diagonal torus

$$T = \left\{ \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & t_2^{-1} & \\ & & & t_1^{-1} \end{pmatrix} \right\}.$$

The simple roots α_1 and α_2 are the characters $t_1 t_2^{-1}$ and t_2^2. The Chevalley generators include

$$X_{\alpha_1} = \begin{pmatrix} 0 & 1 & & \\ & 0 & & \\ & & 0 & -1 \\ & & & 0 \end{pmatrix}, \quad X_{-\alpha_1} = \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & & 0 & \\ & & -1 & 0 \end{pmatrix}, \qquad H_{\alpha_1} = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix},$$

$$X_{\alpha_2} = \begin{pmatrix} 0 & & & \\ & 0 & 1 & \\ & & 0 & \\ & & & 0 \end{pmatrix}, \qquad X_{\alpha_2} = \begin{pmatrix} 0 & & & \\ & 0 & & \\ & 1 & 0 & \\ & & & 0 \end{pmatrix}, \qquad H_{\alpha_2} = \begin{pmatrix} 0 & & & \\ & 1 & & \\ & & -1 & \\ & & & 0 \end{pmatrix}.$$

We have

$$i_{\alpha_1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b & & \\ c & d & & \\ & & a & -b \\ & & -c & d \end{pmatrix}, \qquad i_{\alpha_2} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & & & \\ & a & b & \\ & c & d & \\ & & & 1 \end{pmatrix}.$$

So the the coroots, as elements of $X_*(T)$, are the homomorphisms $G_{\mathrm{m}} \longrightarrow T$ given by

$$h_{\alpha_1^\vee}(t) = \begin{pmatrix} t & & & \\ & t^{-1} & & \\ & & t & \\ & & & t^{-1} \end{pmatrix}, \qquad h_{\alpha_2^\vee}(t) = \begin{pmatrix} 1 & & & \\ & t & & \\ & & t^{-1} & \\ & & & 1 \end{pmatrix}.$$

The differentials of these maps send the unit vector to H_{α_1} and H_{α_2}, respectively. We have

$$x_{\alpha_1}(u) = \begin{pmatrix} 1 & u & & \\ & 1 & & \\ & & 1 & -u \\ & & & 1 \end{pmatrix}, \qquad x_{\alpha_2}(u) = \begin{pmatrix} 1 & & & \\ & 1 & u & \\ & & 1 & \\ & & & 1 \end{pmatrix},$$

$$x_{\alpha_1+\alpha_2}(u) = \begin{pmatrix} 1 & & u & \\ & 1 & & u \\ & & 1 & \\ & & & 1 \end{pmatrix}, \qquad x_{2\alpha_1+\alpha_2}(u) = \begin{pmatrix} 1 & & & u \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

The $x_{-\alpha}(u)$ with $\alpha \in \Phi^+$ are the transposes of these matrices.

Exercise 11 Check (58) for various $\alpha^\vee$ and β.

To get started on the exercise, suppose $\alpha^\vee = \alpha_1^\vee$ and $\beta = \alpha_1 + \alpha_2$. To calculate the inner product $\langle \alpha^\vee, \beta \rangle$, we embed the root system in Euclidean space by the usual type C embedding (Example 3). In this embedding

$$\alpha_1 = \boldsymbol{e}_1 - \boldsymbol{e}_2 = (1, -1), \qquad \alpha_2 = 2\boldsymbol{e}_2 = (0, 2).$$

Although we have been avoiding using (54) we use it now for the purpose of computing inner products, and find that

$$\alpha_1^\vee = (1, -1), \qquad \alpha_2^\vee = (0, 1).$$

Therefore $\beta = \alpha_1 + \alpha_2 = (1, 1)$ and $\langle \alpha_1^\vee, \beta \rangle = 0$. Indeed, $h_{\alpha_1^\vee}(t)$ and $x_{\alpha_1+\alpha_2}(u)$ commute, confirming (58).

13 The Affine Weyl group in a p-adic group

Let G be a split, simply-connected, semisimple affine algebraic group over a nonarchimedean local field F. Let other notations be as in the last section. We have already seen that $N(T(F))/T(F)$ is isomorphic to the ordinary Weyl group. In this section we will show that $N(T(F))/T(\mathfrak{o})$ is isomorphic to the affine Weyl group.

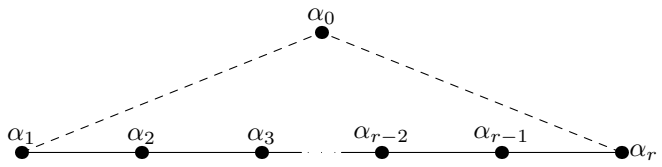
The Lie algebra $\mathfrak{g} = \mathfrak{g}_F$ is a finite-dimensional vector space over F. The Lie subring $\mathfrak{g}_\mathfrak{o} = \mathfrak{o} \otimes \mathfrak{g}_\mathbb{Z}$ is a lattice, that is, a compact open $\mathfrak{o}$-submodule of this F-vector space. The stabilizer of $\mathfrak{g}_\mathfrak{o}$ in $\mathrm{GL}(\mathfrak{g})$ is a compact open subgroup of $\mathrm{GL}(\mathfrak{g})$, and so the stabilizer of $\mathfrak{g}_\mathfrak{o}$ in the adjoint representation of $G(F)$ on $\mathfrak{g}$ is a compact open subgroup of $G(F)$, which we will denote by $G(\mathfrak{o})$. It contains, and is generated by, the groups $x_\alpha(\mathfrak{o})$ as α runs through the roots of G.

With x_α as in (57), let

$$U(F) = \langle x_\alpha(F) | \alpha \in \Phi^+ \rangle, \qquad U_-(F) = \langle x_\alpha(F) | \alpha \in \Phi^- \rangle, \qquad B(F) = T(F)U(F).$$

We will denote by $T(\mathfrak{o})$ the intersection of $G(\mathfrak{o})$ and $T(F)$, and similarly for the groups U, U_- and B.

Before we consider the general case let us consider the case $G = \mathrm{SL}_{r+1}$. In this case, we recall the affine Dynkin diagram is as follows:



So what we are claiming is that $N(T(F))/T(\mathfrak{o})$ has generators $s_1, \cdots, s_r$ and s_0 subject to the relations

$$\begin{aligned} s_i^2 &= 1 \\ s_i s_{i+1} s_i &= s_{i+1} s_i s_{i+1} \\ s_i s_j &= s_j s_i \qquad \text{if } j \equiv \pm i + 1 \bmod r \end{aligned}$$

where the indices are taken modulo r, so that in the second relation $(i, i+1)$ can be $(0, 1)$ or $(r, 0)$. Due to the cyclic symmetry of the diagram, there is an automorphism τ such that $\tau(s_i) = s_{i+1}$.

Representatives for the s_i may be taken as follows:

$$s_i = \begin{pmatrix} I_{i-1} & & \\ & \boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}} & \\ & & I_{r-i} \end{pmatrix}, \qquad (1 \leqslant i \leqslant r) \tag{60}$$

and

$$s_0 = \begin{pmatrix} & & \varpi^{-1} \\ & I_{r-1} & \\ (-1)^{r+1}\varpi & & \end{pmatrix}, \tag{61}$$

where ϖ is a prime element. It is understood that these are actually cosets of $T(\mathfrak{o})$ in $N(T(F))/T(\mathfrak{o})$. It is straightforward to see that these generators satisfy the given relations.

Exercise 12 Check this.

To obtain an explicit isomorphism of $N(T(F))/T(\mathfrak{o})$ with the group generated by $\langle s_0, s_1, s_2\rangle$ let us consider the action of G on F^{r+1} by matrix multiplication. This induces a map of $N(T(F))$ on $F^{r+1}/\mathfrak{o}^{r+1} \cong \mathbb{Z}^{r+1}$. It preserves the subgroup M_0 of $v = (v_i)$ such that $\sum v_i = 0$. We extend this to a vector space $V = \mathbb{R} \otimes M_0$. Then s_i $(1 \leqslant i \leqslant r)$ acts by the usual Weyl group action. On the other hand s_0 is the affine transformation that sends

$$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_{r+1} \end{pmatrix} \longrightarrow \begin{pmatrix} v_{r+1} + 1 \\ v_2 \\ \vdots \\ v_1 - 1 \end{pmatrix}.$$

Since $\alpha_0 = (-1, 0, \cdots, 0, 1)$, this is the reflection in the hyperplane $\langle \alpha_0, v\rangle = -1$, as required.

Turning next to the general case, we have already explained how the coroot lattice $Q^\vee$ is isomorphic to $X_*(T)$. In the case where F is an nonarchimedean local field, this gives an isomorphism $Q^\vee \cong T(F)/T(\mathfrak{o})$. Indeed, if $\alpha \in \Phi$ we map $\alpha^\vee$ to $h_{\alpha^\vee}(\varpi^{-1})$. Since we are dividing by $T(\mathfrak{o})$ this does not depend on the choice of prime element ϖ. We extend this map to $Q^\vee \longrightarrow T(F)/T(\mathfrak{o})$ by linearity, and denote the image of $d \in Q^\vee$ by ϖ^{-d}.

Theorem 15 *Assuming that G is semisimple, split and simply-connected, there exists an isomorphism $W_{\text{aff}} \longrightarrow N(T(F))/T(\mathfrak{o})$. In this isomorphism,*

the image of $Q^\vee$ is $T(F)/T(\mathfrak{o})$ More precisely, the translation $\tau(d) \in W_{\text{aff}}$ for $d \in Q^\vee$ is mapped to ϖ^{-d}, and the reflections s_i are mapped to elements with the representatives

$$s_i = i_{\alpha_i}\begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \quad (i = 1, \cdots, r), \qquad s_0 = i_{-\alpha_0}\begin{pmatrix} & \varpi^{-1} \\ -\varpi & \end{pmatrix}.$$

By abuse of notation we will use the same notation for these elements of $N(T(F))/T(\mathfrak{o})$ as for the corresponding elements of the affine Weyl group.

Proof We must check that these embeddings are compatible, that is, that $\varpi^{-w(d)} = w\varpi^{-d}w^{-1}$ for $d \in Q^\vee$ and $w \in W$. This follows from (59). We conclude that the advertised isomorphism exists.

Now we need to check that s_i corresponds to the right reflection in the affine Weyl group. This is clear for $s_1, \cdots, s_r$. As for s_0, we write

$$i_{-\alpha_0}\begin{pmatrix} & \varpi^{-1} \\ -\varpi & \end{pmatrix} = i_{-\alpha_0}\begin{pmatrix} \varpi^{-1} & \\ & \varpi \end{pmatrix} i_{-\alpha_0}\begin{pmatrix} & 1 \\ -1 & \end{pmatrix} = \varpi^{\alpha_0^\vee} i_{-\alpha_0}\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}.$$

This corresponds to $\tau(-\alpha_0^\vee)r_{\alpha_0}$ in W_{aff}, which is the reflection in the hyperplane $\langle \alpha_0, v\rangle = -1$, as required. (We are using the notation r_{α_0} to denote the reflection determined by r_{α_0} in W.) □

Proposition . *If $d \in Q^\vee$ we have*

$$\varpi^{-d} x_\alpha(u)\varpi^d = x_\alpha(\varpi^{-\langle d,\alpha\rangle}u). \tag{62}$$

Proof This follows from (58). □

Exercise 13 Suppose that $G = \mathrm{SL}_2$. Show that with this identification of $N(T(F))/T(\mathfrak{o})$ with the affine Weyl group, the length function is

$$l\begin{pmatrix} p^a & \\ & p^{-a} \end{pmatrix} = |2a|, \qquad l\begin{pmatrix} & p^{-a} \\ p^a & \end{pmatrix} = |2a-1|.$$

This concludes our discussion of the case where G is semisimple and simply-connected. Let us indicate what happens if these conditions are relaxed.

Without the assumption that G is semisimple and simply connected, we may construct a homomorphism of $Q^\vee$ into $T(F)/T(\mathfrak{o})$ as above. However in general the map is not surjective.

First consider the case where $G = \mathrm{GL}_{r+1}$. In this case, the affine Weyl group must be enlarged. The generators $s_0, s_1, \cdots, s_r$ defined by (60) and (61) must be supplemented with another one:

$$t = \begin{pmatrix} & & & \varpi^{-1} \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}.$$

Since the determinant is not in $\mathfrak{o}^\times$, the coset of t in $N(T(F))/T(\mathfrak{o})$ has infinite order. It may be checked that

$$ts_it^{-1} = s_{i+1},$$

where the elements are taken to be periodic, i.e. $s_{r+1} = s_0$. Therefore $N(T(F))/T(\mathfrak{o})$ is a semidirect product of the Coxeter group W_{aff} generated by the s_i by an infinite cyclic group: $N(T(F))/T(\mathfrak{o}) = W_{\mathrm{aff}} \rtimes \mathbb{Z}$.

If we are working over PGL_{r+1}, which is semisimple, the story will be the same, but t^{r+1} is a scalar matrix, and is in the center, so t has finite order $r+1$. In this case, $N(T(F))/T(\mathfrak{o}) \cong W_{\mathrm{aff}} \rtimes \Omega$, where Ω is the cyclic group $\langle t \rangle$ of order $r+1$.

This is typical of the general semisimple case. If G is a split semisimple group that is not simply-connected, then the fundamental group $\pi_1(G)$ is a finite abelian group which acts on the extended Dynkin diagram. It therefore has an action on the affine Weyl group, and $N(T(F))/T(\mathfrak{o})$ is the semidirect product $W_{\mathrm{aff}} \rtimes \pi_1(G)$.

14 The Iwahori-Bruhat Decomposition

After the Bruhat decomposition was found in the 1950's, it was extended in generality by Chevalley and Borel. Tits gave a fully axiomatic approach (1962). A completely unexpected instance of Bruhat's axioms was found by Iwahori and Matsumoto, in a p-adic group. The (noncompact) Borel subgroup B is replaced by the (compact) Iwahori subgroup, and the (finite) Weyl group W is replaced by the (infinite) affine Weyl group W_{aff}.

Let G be a split, simply-connected semisimple affine algebraic group over the nonarchimedean local field F. Notations will be as in the preceding section. The Iwahori subgroup J, we have noted, consists of $k \in G(\mathfrak{o})$ such

that the image of k in $G(\mathbb{F}_q)$ lies in the Borel subgroup $B(\mathbb{F}_q)$. Let $I_0 = \{s_0, s_1, \cdots, s_r\}$ be the set of simple reflections, together with the "affine" reflection s_0.

Theorem 16 (Iwahori and Matsumoto) *Let G be a split, simply-connected semisimple affine algebraic group over the nonarchimedean local field F. The data $(J, N(T(F), I_0)$ are a Tits' system. Therefore*

$$G(F) = \bigcup_{w \in W_{\text{aff}}} JwJ \qquad \text{(disjoint)}.$$

The proof will occupy the present section. The main thing to be verified is Axiom TS3 (Section 7).

Let us consider how this will change if G is not simply-connected. In this case, we have already explained, there is still a homomorphism from the coroot lattice $Q^\vee$ to $T(F)/T(\mathfrak{o})$, but this homomorphism is no longer surjective. It must be supplemented by another subgroup Ω of $N(T(F))$, as at the end of the last section. If G is semisimple, then Ω is isomorphic to the fundamental group $\pi_1(G)$, which can be viewed as a group of automorphisms of the extended Dynkin diagram.

The general case where G is reductive was considered by Bruhat and Tits.

For the rest of the section we will assume that G is split, semisimple and simply-connected.

Let U be the unipotent algebraic subgroup generated by the $x_\alpha(u)$ with $\alpha \in \Phi^+$. Let U_- be the unipotent subgroup generated by the $x_\alpha(u)$ with $\alpha \in \Phi^-$. If $\mathfrak{a}$ is any fractional ideal let $U(\mathfrak{a})$ be the group generated by $x_\alpha(u)$ with $u \in \Phi^+$ and $\alpha \in \mathfrak{a}$, and similarly for $U_-(\mathfrak{a})$.

The following fact is very important.

Proposition 50 (Iwahori Factorization) *We have*

$$J = U_-(\mathfrak{p})U(\mathfrak{o})T(\mathfrak{o}).$$

That is, the multiplication map $U_-(\mathfrak{p}) \times U(\mathfrak{o}) \times T(\mathfrak{o}) \longrightarrow J$ is bijective. The three factors can be written in any order.

Proof Rather than prove this in general we prove it for SL_3 in order to make the ideas clear. Let

$$g = \begin{pmatrix} t_1 & u_1 & u_2 \\ v_1 & t_2 & u_3 \\ v_2 & v_3 & t_3 \end{pmatrix} \in J.$$

We will show that $g \in U_-(\mathfrak{p})B(\mathfrak{o})$. The $u_i \in \mathfrak{o}$, $v_i \in \mathfrak{p}$ and since g is invertible, the t_i are units. Now we may multiply on the left by

$$x_{-\alpha_1-\alpha_2}(-v_2t_1^{-1}) = \begin{pmatrix} 1 & & \\ & 1 & \\ -\frac{v_2}{t_1} & & 1 \end{pmatrix}$$

which is in $U_-(\mathfrak{p})$; this annihilates v_2. For the purpose of showing that $g \in U_-(\mathfrak{p})B(\mathfrak{o})$, we see that we may assume $v_2 = 0$. Next we may multiply on the left by $x_{-\alpha_1}(-v_1t_1^{-1})$ and arrange that $v_1 = 0$. Finally, we use $x_{-\alpha_2}(-v_3t_2^{-1})$ to arrange that $v_3 = 0$.

Now we know that $J = U_-(\mathfrak{p})B(\mathfrak{o})$, we may use the fact that $B(\mathfrak{o}) = T(\mathfrak{o})U(\mathfrak{o}) = U(\mathfrak{o})T(\mathfrak{o})$ to see that $J = U_-(\mathfrak{p})T(\mathfrak{o})U(\mathfrak{o}) = U_-(\mathfrak{p})U(\mathfrak{o})T(\mathfrak{o})$. We also have $U_-(\mathfrak{p})T(\mathfrak{o}) = T(\mathfrak{o})U_-(\mathfrak{p})$, a semidirect product with $U_-(\mathfrak{p})$ normal. This allows us to put the $U_-(\mathfrak{p})$ in the middle if we want. We see that the factors may be in any order.

This same proof works for general G, and we leave this to the reader. See Lemma 11 for a similar situation. □

Lemma 9 *If $u \in U_-(\mathfrak{p})$ and $w \in W$ then $wuw^{-1} \in J$. If $t \in T(\mathfrak{o})$ then $wtw^{-1} \in J$.*

There is an abuse of notation here, since w is actually a coset of $N(T(F))/T(\mathfrak{o})$. The truth of $wtw^{-1} \in J$ is independent of the choice of w.

Proof We may assume that $u = x_\alpha(v)$ with $v \in \mathfrak{p}$. Then $wuw^{-1} = x_{w(\alpha)}(\varepsilon v)$ where ε is a unit. If $w(\alpha) \in \Phi^+$ then this is in $U(\mathfrak{o})$. If $w(\alpha) \in \Phi^-$ it is in $U_-(\mathfrak{p})$. Either way it is in J. Also $wT(\mathfrak{o})w^{-1} = T(\mathfrak{o})$ since we chose the representatives w of W to be in the normalizer of $T(\mathfrak{o})$ in $G(\mathfrak{o})$. □

Lemma 10 *Suppose that $\alpha \in \Phi$, $\alpha \neq \alpha_0$. Suppose that $u = x_\alpha(v)$ where either $\alpha \in \Phi^+$ and $v \in \mathfrak{o}$ or $\alpha \in \Phi^-$ and $v \in \mathfrak{p}$. Then $s_0^{-1}us_0 \in J$.*

Proof We write

$$s_0 = \varpi^{\alpha_0^\vee} i_{-\alpha_0} \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} = \varpi^{\alpha_0^\vee} r_{\alpha_0}.$$

Then

$$s_0^{-1}us_0 = r_{\alpha_0}^{-1} x_\alpha(\varpi^{-\langle\alpha_0^\vee,\alpha\rangle}v) r_{\alpha_0} = x_{r_{\alpha_0}(\alpha)}(\varpi^{-\langle\alpha_0^\vee,\alpha\rangle}v).$$

By abuse of notation we are using the notation r_{α_0} to denote both the reflection r_{α_0} in W and its representative $i_{-\alpha_0}\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ in $T(F)/T(\mathfrak{o})$.

First assume that $\alpha \in \Phi^+$ and $v \in \mathfrak{o}$. Since $-\alpha_0$ is the highest root, $\langle \alpha_0^\vee, \alpha \rangle \leqslant 0$ by Proposition 41. If $\langle \alpha_0^\vee, \alpha \rangle < 0$ then this is in J by Lemma 9. On the other hand if $\langle \alpha_0^\vee, \alpha \rangle = 0$ then $r_{\alpha_0}^{-1}(\alpha) = \alpha$ since α_0 and α are orthogonal roots, and so $s_0^{-1} u s_0 = u \in J$.

Next assume that $\alpha \in \Phi^-$ and that $\alpha \neq \alpha_0$. In this case we are also assuming that $v \in \mathfrak{p}$. Then $\langle \alpha_0^\vee, \alpha \rangle \geqslant 0$ by Proposition 41. Indeed, by Proposition 41 and our assumption that $\alpha \neq \alpha_0$ we have $\langle \alpha_0^\vee, \alpha \rangle < \langle \alpha_0^\vee, \alpha_0 \rangle = 2$. Since $\langle \alpha_0^\vee, \alpha \rangle$ is an integer, $\langle \alpha_0^\vee, \alpha \rangle \leqslant 1$. if $\langle \alpha_0^\vee, \alpha \rangle \leqslant 0$ then $\varpi^{-\langle \alpha_0^\vee, \alpha \rangle} v \in \mathfrak{p}$ and $s_0 u s_0 = x_{r_{\alpha_0}(\alpha)}(\varpi^{-\langle \alpha_0^\vee, \alpha \rangle} v) \in J$ by Lemma 9. We are left with the case $\langle \alpha_0^\vee, \alpha \rangle = 1$. In this case $\varpi^{-\langle \alpha_0^\vee, \alpha \rangle} v \in \mathfrak{o}$. Moreover $r_{\alpha_0}(\alpha) = \alpha - \langle \alpha_0^\vee, \alpha \rangle \alpha_0 = \alpha - \alpha_0$. This cannot be a negative root since $-\alpha_0$ is the highest root, and so $x_{\alpha_0(\alpha)}(\varpi^{-\langle \alpha_0^\vee, \alpha \rangle} v) \in U(\mathfrak{o}) \subset J$. □

Iwahori and Matsumoto showed that the Iwahori subgroup satisfies Bruhat's axioms, giving rise to a Bruhat decomposition based on the affine Weyl group. The next result is a first step towards this goal.

Proposition 51 *If $w \in W_{\text{aff}}$ and $l(ws_i) = l(w) + 1$ then $wJs_i \subseteq Jws_iJ$.*

Proof First assume that $1 \leqslant i \leqslant r$.

Using the Iwahori factorization, we may write an element of wJs_i as $wu_+u_-ts_i$ where $u_- \in U_-(\mathfrak{p})$, $t \in T(\mathfrak{o})$ and $u_+ \in U(\mathfrak{o})$. By Lemma 9 $u_-ts_i \in s_iJ$, so we may assume that the element is of the form wu_+s_i. Now we write u_+ as a product of elements of the form $x_\alpha(v)$ with $v \in \mathfrak{o}$. If $\alpha \neq \alpha_i$ we have $s_i^{-1} x_\alpha(v) s_i = x_{s_i(\alpha)}(v)$ and $s_i(\alpha) \in \Phi^+$, so this is in J. Therefore we may handle all the $x_\alpha(v)$ this way except only one root $\alpha = \alpha_i$. It is thus sufficient to show that $wx_{\alpha_i}(v)w^{-1} \in Jw$.

We may write $w = \varpi^{-d} w'$ where $w' \in W$ and $d \in Q^\vee$. By (62) we have $wx_{\alpha_i}(v)w^{-1} = \varpi^{-d} x_{w'(\alpha_i)}(v) \varpi^d = x_{w'(\alpha_i)}(\varpi^{\langle -d, w'(\alpha_i) \rangle} v)$. By Proposition 47 we have either $\langle w'(\alpha_i), d \rangle < 0$ or $\langle w'(\alpha_i), d \rangle = 0$ and $w'(\alpha_i) \in \Phi^+$. Assume first that $\langle w(\alpha_i), d \rangle < 0$. Then $\varpi^{\langle -d, w'(\alpha_i) \rangle} v \in \mathfrak{p}$ and $x_{w'(\alpha_i)}(\varpi^{\langle -d, w'(\alpha_i) \rangle} v) \in J$ regardless of whether $w'(\alpha_i)$ is a positive or negative root. On the other hand if $\langle w'(\alpha_i), d \rangle = 0$, we are guaranteed that $w'(\alpha) \in \Phi^+$. In the second case we also have $x_{w'(\alpha_i)}(\varpi^{\langle -d, w'(\alpha_i) \rangle} v) = x_{w'(\alpha_i)}(v) \in J$.

It remains for us to treat the case $i = 0$. We may use the Iwahori factorization again to write an element of wJs_0 as $wu_-u_+ts_0$ where $u_- \in$

$U_-(\mathfrak{p})$, $t \in T(\mathfrak{o})$ and $u_+ \in U_+(\mathfrak{o})$. We have, as before $ts_0 \in s_0 J$, and we may write u_- and u_+ as products of factors $x_\alpha(v)$ where either $\alpha \in \Phi^+$ and $v \in \mathfrak{o}$ or $\alpha \in \Phi^-$ and $v \in \mathfrak{p}$. In every case except $\alpha = \alpha_0$ we have $u_\alpha s_0 \in s_0 J$ by Lemma 10.

We are therefore left to show that $w x_{\alpha_0}(v) w^{-1} \in J$. We write $w = \varpi^{-d} w'$ where $w' \in W$ and $d \in Q^\vee$. By Proposition 47 we have either $\langle w'(\alpha_0), d\rangle < 1$ or $\langle w'(\alpha_0), d\rangle = 1$ and $w(\alpha_0) \in \Phi^+$. Now consider $w x_{\alpha_0}(v) w^{-1} = x_{w'(\alpha_0)}(\varpi^{\langle -d, w'(\alpha_0)\rangle} v)$. Since $v \in \mathfrak{p}$ if $\langle w'(\alpha_0), d\rangle \leqslant 0$, then $\varpi^{\langle -d, w'(\alpha_0)\rangle} v \in \mathfrak{p}$ and so $w x_{\alpha_0}(v) w^{-1} \in J$ by Lemma 9. On the other hand if $\langle w'(\alpha_0), d\rangle = 1$ and $w'(\alpha_0) \in \Phi^+$ then $\varpi^{\langle -d, w'(\alpha_0)\rangle} v \in \mathfrak{o}$, and in this case $w x_{\alpha_0}(v) w^{-1} \in U(\mathfrak{o}) \subset J$. □

Proposition 52 *If $0 \leqslant s_i \leqslant r$ then $s_i J s_i \in J \cup J s_i J$.*

Proof First assume that $1 \leqslant i \leqslant r$. We may write an arbitrary element of J as a product of factors of the form $t \in T$ and $x_\alpha(v)$ where either $v \in \mathfrak{o}$ and $\alpha \in \Phi^+$ or $v \in \mathfrak{p}$ and $\alpha \in \Phi^-$. Except in the case $\alpha = \alpha_i$ we have $s_i^{-1} x_\alpha(v) s_i = x_{s_i(\alpha)}(v) \in J$, because if $\alpha \in \Phi^+$ and $\alpha \neq \alpha_i$ then $s_i(\alpha) \in \Phi^+$, while if $\alpha \in \Phi^-$ then $v \in \mathfrak{p}$ and so $s_i^{-1} x_\alpha(v) s_i \in J$ by Lemma 9. Also $s_i^{-1} t s_i \in T(\mathfrak{o}) \in J$. In conclusion, every one of the factors except one may be moved across s_i. We are left with showing that $s_i x_{\alpha_i}(v) s_i \in J \cup J s_i J$. We have $v \in \mathfrak{o}$. If $v \in \mathfrak{p}$ then we may use Lemma 9. Therefore we assume that $v \in \mathfrak{o}^\times$. We make use of the identity

$$\begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \begin{pmatrix} 1 & v \\ & 1 \end{pmatrix} \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} = \begin{pmatrix} 1 & \\ -v & 1 \end{pmatrix} = \begin{pmatrix} 1 & -v^{-1} \\ & 1 \end{pmatrix} \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \begin{pmatrix} v & -1 \\ & v^{-1} \end{pmatrix}.$$

Applying i_{α_i}, this leads to

$$s_{\alpha_i}^{-1} x_{\alpha_i}(v) s_{\alpha_i} = x_{\alpha_i}(-v^{-1}) s_{\alpha_i} i_{\alpha_i} \begin{pmatrix} v & -1 \\ & v^{-1} \end{pmatrix} \in J s_{\alpha_i} J.$$

This concludes the proof when $1 \leqslant i \leqslant r$.

Next assume that $i = 0$. We leave it to the reader to check that if $\alpha \neq \alpha_0$ and either $v \in \mathfrak{o}$ and $\alpha \in \Phi^+$ or $v \in \mathfrak{p}$ and $\alpha \in \Phi^-$, then $s_0^{-1} x_\alpha(v) s_0 \in J$. This leaves us to consider the case where $\alpha = \alpha_0$ and $v \in \mathfrak{p}$. It may also be checked that if $v \in \mathfrak{p}^2$ then $s_0^{-1} x_{\alpha_0}(v) s_0 \in J$. Therefore we may assume that

$v = \varpi\varepsilon$ where ε is a unit. Now we use the identity

$$\begin{pmatrix} & -\varpi^{-1} \\ \varpi & \end{pmatrix}\begin{pmatrix} 1 & \\ \varpi\varepsilon & 1 \end{pmatrix}\begin{pmatrix} & \varpi^{-1} \\ -\varpi & \end{pmatrix} = \begin{pmatrix} 1 & \\ -\varepsilon^{-1}\varpi & 1 \end{pmatrix}\begin{pmatrix} & \varpi^{-1} \\ -\varpi & \end{pmatrix}\begin{pmatrix} -\varepsilon^{-1} & \\ \varpi & -\varepsilon \end{pmatrix}$$

Applying $i_{-\alpha_0}$ shows that $s_0^{-1}x_{\alpha_0}(\varpi\varepsilon)s_0 \in C(s_0)$. □

Exercise 14 Verify the claim in the above proof that if $i = 0$ and $\alpha \neq \alpha_0$ and either $v \in \mathfrak{o}$ and $\alpha \in \Phi^+$ or $v \in \mathfrak{p}$ and $\alpha \in \Phi^-$, then $s_0^{-1}x_\alpha(v)s_0 \in J$.

We will use the notation $JwJ = C(w)$ as in Section 7. Then the content of Proposition 51 may be written $C(w)C(s_i) = C(ws_i)$ if $l(ws_i) = l(w) + 1$, and Proposition 52 may be written $C(s_i)C(s_i) \subset C(1) \cup C(s_i)$.

Theorem 17 *If $w \in W_{\text{aff}}$ and $0 \leqslant i \leqslant r$ then*

$$wJs_i \subseteq Jws_iJ \cup JwJ.$$

Proof This may be written $C(w)C(s_i) \subseteq C(ws_i) \cup C(w)$. If $l(ws_i) = l(w) + 1$, this follows from Proposition 51.

Therefore we assume that $l(ws_i) = l(w)-1$. Let $w' = ws_i$. Then $l(w's_i) = l(w') + 1$ and so by Proposition 51 we have $C(w')C(s_i) = C(w's_i) = C(w)$. Therefore

$$C(w)C(s_i) = C(w')C(s_i)C(s_i).$$

By Proposition 52 this is contained in

$$C(w')C(s_i) \cup C(w')C(1) = C(w) \cup C(w') = C(w) \cup C(ws_i),$$

as required. □

This gives us Axiom TS3. The other axioms we leave to the reader.

Exercise 15 Verify the remaining axioms of a Tits System. **Hint:** For Axiom TS5, you must show that G is generated by J and $N(T(F))$. Show that conjugates of $U(\mathfrak{o})$ by elements of $T(F)$ contain all of $U(F)$, and so the group generated by J and $N(T(F))$ contains $B(F)$.

This concludes the proof of Theorem 16.

Lemma 11 *If $u \in U_-(F)$ then $u \in G(\mathfrak{o})B(F)$.*

Proof We write

$$u = \prod_{\alpha \in \Phi^-} x_\alpha(u_\alpha), \qquad u_\alpha \in F.$$

We order the roots so that if β comes after α in the product, then either $\beta - \alpha$ is not a root or $\beta - \alpha \in \Phi^+$. We may accomplish this by taking the negative roots α such that the inner products $\langle -\rho, \alpha \rangle$ are in nonincreasing order.

Now we modify u by left multiplications by elements of $G(\mathfrak{o})$ and right multiplication by elements of $B(F)$ so that until all u_α are 0. Let α be the first root such that $x_\alpha(u_\alpha) \neq 0$. If $u_\alpha \in \mathfrak{o}$, we left multiply by $x_\alpha(-u_\alpha)$. If $u_\alpha \in \mathfrak{o}$ then we left multiply by $i_{-\alpha} \begin{pmatrix} & 1 \\ -1 & u_\alpha \end{pmatrix}$. We have

$$i_{-\alpha} \begin{pmatrix} & 1 \\ -1 & u_\alpha \end{pmatrix} x_\alpha(u) = i_{-\alpha} \begin{pmatrix} u & 1 \\ & u^{-1} \end{pmatrix} \in B(F).$$

Conjugating the remaining $x_\beta(u_\beta)$ by this element of $B(F)$ produces commutators that are in $B(F)$ by the way we have ordered the roots. In either case, we are able to replace u_α by 0. Continuing, eventually all u_α are zero. □

Theorem 18 (Iwasawa Decomposition) *We have $G(F) = G(\mathfrak{o})B(F) = B(F)G(\mathfrak{o})$.*

Proof Using the Iwahori-Bruhat decomposition, it is sufficient to show that $JwJ \subseteq G(\mathfrak{o})B(F)$, where $w \in W_{\text{aff}}$ may be written $w = w't$ with $w' \in W$ and $t \in T$. Now $Jw' \in G(\mathfrak{o})$ so what we must show is that $tJ \subseteq G(\mathfrak{o})B(F)$. Using the Iwahori factorization, we write a typical element of J as u_-b with $u_- \in U_-(\mathfrak{p})$ and $b \in B(\mathfrak{o})$. Now $tu_-t^{-1} \in G(\mathfrak{o})B(F)$ by the Lemma, so $tu_-b = (tu_-t^{-1})tb \in G(\mathfrak{o})B(F)$. □

The following decomposition is called the Cartan decomposition by analogy with the corresponding decomposition in Lie groups. However in this p-adic context the result is actually due to Bruhat.

We will say that an element of $d \in Q^\vee$ or its ambient vector space is *dominant* if $\langle d, \alpha \rangle \geqslant 0$ for all $\alpha \in \Phi^+$. Then (because we are assuming G to be simply-connected) the ϖ^d with $d \in Q^\vee$ dominant form a fundamental domain for the action of W on $T(F)/T(\mathfrak{o})$.

Theorem 19 (Cartan Decomposition) *We have*

$$G(F) = \bigcup_{\substack{d \in Q^\vee \\ d \text{ dominant}}} G(\mathfrak{o})\, \varpi^d\, G(\mathfrak{o}) \qquad \text{(disjoint)}.$$

Proof We have

$$G(F) = \bigcup_{w \in W_{\text{aff}}} JwJ = \bigcup_{\substack{d \in Q^\vee \\ w \in W}} Jw\varpi^d J,$$

where $\varpi^{-d} \in T(F)$ and $w \in G(\mathfrak{o})$. This shows that $G(F) = \bigcup_{d \in Q^\vee} G(\mathfrak{o})\varpi^d G(\mathfrak{o})$. Since $G(\mathfrak{o})$ contains representatives for W, we may conjugate ϖ^d by W and assume that d is dominant.

We will omit the proof that these double cosets are disjoint. For GL_n, we proved it in Proposition 35. For the general case, see Bruhat, Sur une classe du sous-groupes compacts maximaux des groupes de Chevalley sur un corps p–adique. (French) Inst. Hautes ÃĽtudes Sci. Publ. Math. No. 23 1964 45–74, ThÃĭorÃĺm 12.2. □

15 The Iwahori Hecke algebra

We continue to assume that G is semisimple, split and simply connected and following Iwahori and Matsumoto we consider the structure of the Iwahori Hecke algebra.

It will be convenient to normalize the Haar measure so that J has volume 1. Then $\mathcal{H}_J$ is the ring of J-bi-invariant functions. The convolution is then normalized thus:

$$(\phi_1 * \phi_2)(g) = \int_G \phi_1(gh^{-1})\phi_2(h)\, dg.$$

Since we have a set of J double cosets in the affine, let ϕ_w be the characteristic function of BwB for $w \in W_{\text{aff}}$.

We have an *augmentation map* $\varepsilon : \mathcal{H} \longrightarrow \mathbb{C}$ defined by

$$\varepsilon(\phi) = \int_G \phi(g)\, dg.$$

Lemma 12 *We have* $\varepsilon(\phi_1 * \phi_2) = \varepsilon(\phi_1)\varepsilon(\phi_2)$.

Proof Indeed $\varepsilon(\phi_1 * \phi_2) = \int_G \int_G \phi_1(gh^{-1})\, \phi_2(h)\, dh\, dg$. Interchanging the order of integration and substituting $g \longrightarrow gh$, the integral factors as required. □

Lemma 13 *Let G be a group, H a subgroup, and $x \in G$. Then the cardinality of the coset space HxH/H is $[H : H \cap xHx^{-1}]$.*

Proof Now if K and H are arbitrary subgroups of G then the inclusion of K into KH induces a bijection $K/(H \cap K) \longrightarrow KH/H$. (The coset spaces here are not groups since we are not assuming that H is normal.) Indeed, the composition $K \longrightarrow KH \longrightarrow KH/H$ is certainly surjective, and two cosets $kH = k'H$ with $k, k' \in K$ are equal if and only if $k^{-1}k' \in H$; since $k^{-1}k' \in K$, this is equivalent to k and k' having the same image in $K/(H \cap K)$.

Left multiplication by x^{-1} commutes with right multiplication by elements of H, hence induces a bijection $HxH/H \longrightarrow x^{-1}HxH/H = KH/K$, where $K = x^{-1}Hx$. Therefore HxH/H is in bijection with $x^{-1}Hx/(H \cap x^{-1}Hx)$. Now conjugating by x, this is equivalently in bijection with $H/(xHx^{-1} \cap H)$. □

Proposition 53 *Let $w \in W$. Then*

$$\varepsilon(\phi_w) = |JwJ/J| = [J \cap wJw^{-1}].$$

Proof Since ϕ_w is the characteristic function of JwJ, it is clear that $\varepsilon(\phi_w)$ is the volume of this double coset. This equals the number of right cosets in JwJ/J since each of those cosets has volume 1. □

We will say that an element of $d \in Q^\vee$ or its ambient vector space is *dominant* if $\langle d, \alpha \rangle \geqslant 0$ for all $\alpha \in \Phi^+$, and *antidominant* if $-d$ is dominant. More generally, if $w \in W_{\text{aff}}$, we say that w is *dominant* if $w\mathfrak{F}$ is contained in the positive Weyl chamber $\mathcal{C}$, and antidominant if $w\mathfrak{F}$ is contained in $-\mathcal{C}$.

Lemma 14 *Suppose that $d \in Q^\vee$ is dominant, and let $w = \varpi^d$. Then $\varepsilon(\phi_w) = q^{l(w)}$.*

Note that ϖ^d is antidominant, since the embedding of Theorem 15 sends $\tau(d)$ to ϖ^{-d}. Thus w actually corresponds to $-d$.

Proof We note that $wU(\mathfrak{o})w^{-1} \subseteq U(\mathfrak{o})$ while $wU_-(\mathfrak{p})w^{-1} \supseteq U_-(\mathfrak{p})$. Indeed, by (62) and our assumption that d is dominant, we have $wx_\alpha(\mathfrak{o})w^{-1} \subseteq x_\alpha(\mathfrak{o})$ if $\alpha \in \Phi^+$, while $wx_\alpha(\mathfrak{p})w^{-1} \supseteq x_\alpha(\mathfrak{p})$ if $\alpha \in \Phi^-$.

Both groups J and wJw^{-1} have Iwahori factorizations, $J = U_-(\mathfrak{p})T(\mathfrak{o})U(\mathfrak{o})$ and

$$wJw^{-1} = (wU_-(\mathfrak{p})w^{-1})T(\mathfrak{o})(wU(\mathfrak{o})w^{-1}).$$

It follows that

$$J \cap wJw^{-1} = U_-(\mathfrak{p})T(\mathfrak{o})wU(\mathfrak{o})w^{-1}$$

Indeed, it is clear that the right-hand side is contained in the left-hand side. For the other inclusion, if we have an element g of J and write it as $g = u_-tu$ with $u_- \in U_-(\mathfrak{p})$, $t \in T(\mathfrak{o})$ and $u \in U(\mathfrak{o})$, and if it also equals $u'_-t'u'$ with $u'_- \in wU_-(\mathfrak{p})^{-1}$, $t' \in T(\mathfrak{o})$ and $u' \in wU(\mathfrak{o})w^{-1}$, then $u_-^{-1}u'_- = tu(t'u')^{-1} \in U_-(F) \cap B(F)$. The intersection of these two groups is trivial, so $u_- = u'_-$, and so $g = u'_-tu$ is in $U_-(\mathfrak{p})T(\mathfrak{o})wU(\mathfrak{o})w^{-1}$.

We see that $[J : J \cap wJw^{-1}] = [U(\mathfrak{o}) : wU(\mathfrak{o})w^{-1}]$. This index is, again by (62)

$$\prod_{\alpha\in\Phi^+} [x_\alpha(\mathfrak{o}) : wx_\alpha(\mathfrak{o})w^{-1}] = \prod_{\alpha\in\Phi^+} [x_\alpha(\mathfrak{o}) : wx_\alpha(\mathfrak{p}^{\langle d,\alpha\rangle})w^{-1}] = \prod_{\alpha\in\Phi^+} q^{\langle d,\alpha\rangle}.$$

By Proposition 48, this equals $q^{l(d)}$. □

Proposition 54 *Let $0 \leqslant i \leqslant r$. Then $\varepsilon(\phi_{s_i}) = q$.*

Proof We leave it to the reader to check that if $1 \leqslant i \leqslant r$ then $s_iJs_i^{-1} = U_-(\mathfrak{p})T(\mathfrak{o})U_i(\mathfrak{o})$ where

$$U_i(\mathfrak{o}) = \prod_{\alpha\in\Phi^+} \begin{cases} x_\alpha(\mathfrak{p}) & \text{if } \alpha = \alpha_i, \\ x_\alpha(\mathfrak{o}) & \text{otherwise.} \end{cases}$$

The index in J equals $[U(\mathfrak{o}) : U_i(\mathfrak{o})] = q$. Similarly if $i = 0$ then $s_iJs_i^{-1} = U'_-(\mathfrak{p})T(\mathfrak{o})U(\mathfrak{o})$ where

$$U'_-(\mathfrak{p}) = \prod_{\alpha\in\Phi^-} \begin{cases} x_\alpha(\mathfrak{p}^2) & \text{if } \alpha = \alpha_0, \\ x_\alpha(\mathfrak{p}) & \text{otherwise,} \end{cases}$$

and again the index is q. □

Now let G be a group and H a subgroup. We will assume for all $x \in G$ that $i(x) < \infty$, where $i(x) = |HxH/H| = [H : H \cap xHx^{-1}]$.

Lemma 15 *Let G be a group and H a subgroup. Define $i(x) = H \cap xHx^{-1}$ for $x \in G$. Suppose that $x, y \in G$. Then $i(xy) \leqslant i(x)i(y)$.*

Proof We have $i(y) = [H : H \cap yHy^{-1}]$ and conjugating by x, $i(y) = [xHx^{-1} : xHx^{-1} \cap (xy)H(xy)^{-1}]$. Intersecting with H can only decrease the index, so

$$[H \cap xHx^{-1} : H \cap xHx^{-1} \cap (xy)H(xy)^{-1}] \leqslant i(y).$$

Now

$$\begin{aligned} i(xy) = [H : H \cap (xy)H(xy)^{-1}] &\leqslant \\ [H : H \cap xHx^{-1} \cap (xy)H(xy)^{-1}] &= \\ [H : H \cap xHx^{-1}][H \cap xHx^{-1} : H \cap xHx^{-1} \cap (xy)H(xy)^{-1}] &\leqslant i(x)i(y). \end{aligned}$$

□

Theorem 20 *Let $w \in W_{\text{aff}}$. Then $\varepsilon(\phi_w) = q^{l(w)}$.*

Iwahori and Matsumoto deduce this quickly from Proposition 54. It seems to me that there is a gap in their proof, which I fill using Lemma 14.

Proof By Proposition 53 and Lemma 15 we have $\varepsilon(\phi_{ww'}) \leqslant \varepsilon(\phi_w)\varepsilon(\phi_{w'})$. Using this fact and Proposition 54 it follows that $\varepsilon(\phi_w) \leqslant q^{l(w)}$, after factoring w into a product of simple reflections.

We claim that for every $w \in W_{\text{aff}}$ there exists a $w' \in W_{\text{aff}}$ such that $l(w'w) = l(w) + l(w')$ and $\varepsilon(\phi_{w'w}) = q^{l(w)+l(w')}$. By Lemma 14 it is sufficient to find w' such that $w'w \in Q^\vee$, with $w'w$ an antidominant element of $Q^\vee$. It is easy to see geometrically that we may find a path from $w\mathfrak{F}$ to the negative Weyl chamber that does not cross any of the hyperplanes $H_{\alpha,k}$between $\mathfrak{F}$ and $w\mathfrak{F}$, and we may arrange that the path ends in an alcove $w'w\mathfrak{F}$ that is a $Q^\vee$-translate of $\mathfrak{F}$. Since the path does not recross any hyperplane that it has already crossed, $l(w'w) = l(w') + l(w)$.

Now we have

$$q^{l(w)+l(w')} = \varepsilon(\phi_{w'w}) \leqslant \varepsilon(\phi_{w'})\varepsilon(\phi_w) \leqslant q^{l(w')}\varepsilon(\phi_w),$$

so $\varepsilon(\phi_w) \geqslant q^{l(w)}$. We have proved both inequalities and the statement follows.

□

Corollary 1 *If $l(ww') = l(w) + l(w')$ then $\phi_{ww'} = \phi_w * \phi_{w'}$.*

Proof In the integral

$$(\phi_w * \phi_{w'})(g) = \int_G \phi_w(gh^{-1})\phi_{w'}(h)\, dg,$$

the integrand vanishes unless $gh^{-1} \in JwJ$ and $h \in Jw'J$, which implies that $g = gh^{-1} \cdot h$ is in $JwJ' \cdot Jw'J$. But by Proposition 51 we have $JwJ \cdot Jw'J = Jww'J$. Thus the convolution is supported on a single double coset and so $\phi_w * \phi_{w'} = c\phi_{ww'}$ for some constant c. We apply ε and apply the Theorem to get $q^{l(w)+l(w')} = cq^{l(w)+l(w')}$, so $c = 1$. □

Now we need to know the quadratic relations. We will leave some of the work to the reader.

Exercise 16 Show that if $0 \leqslant i \leqslant r$ then $J \cup Js_iJ$ is a group. **Hint:** if $i \neq 0$ then this is

$$U^i_-(\mathfrak{p})\; i_{\alpha_i}(\mathrm{SL}(2, \mathfrak{o}))U^i(\mathfrak{o})$$

where

$$U^i_-(\mathfrak{p}) = \prod_{\substack{\alpha \in \Phi^- \\ \alpha \neq -\alpha_i}} x_\alpha(\mathfrak{p}), \qquad U^i(\mathfrak{o}) = \prod_{\substack{\alpha \in \Phi^+ \\ \alpha \neq \alpha_i}} x_\alpha(\mathfrak{o}).$$

Show that this is closed under multiplication because $i_{\alpha_i}(\mathrm{SL}(2, \mathfrak{o}))$ normalizes the two unipotent groups.

Proposition 55 *Let $0 \leqslant i \leqslant r$. Then*

$$\phi^2_{s_i} = (q-1)\phi_{s_i} + q.$$

Proof Since the support of ϕ_i is contained in $J \cup Js_iJ$, which is a group, $\phi^2_{s_i}$ is a linear combination of ϕ_1 (the identity element in $\mathcal{H}_J$) and ϕ_{s_i}. Thus $\phi^2_{s_i} = a\phi_{s_i} + b\phi_1$ for some a and b. To compute b, evaluate at the identity. We have $\phi_1(1) = 1$ and $\phi_{s_i}(1) = 0$, while

$$(\phi_{s_i} * \phi_{s_i})(1) = \int_G \phi_{s_i}(h)\, \phi_{s_i}(h^{-1})\, dh = \int_{Js_iJ} 1\, dh = |Js_iJ/J| = q$$

by Proposition 54. Therefore $b = q$. We apply the homomorphism $\varepsilon : \mathcal{H}_J \longrightarrow \mathbb{C}$ such that $\varepsilon(\phi_{s_i}) = 1$ and obtain the relation $q^2 = aq + b$ and since $b = q$ we get $a = q - 1$. □

Taking W to be the Coxeter group W_{aff}, we have an Iwahori Hecke algebra $\mathcal{H}_q(W_{\mathrm{aff}})$, with generators T_i in bijection with the s_i, subject to the quadratic

relations and the braid relations. Using Tits' Theorem (see Theorem 14) we may define elements T_w for $w \in W_{\text{aff}}$ by $T_w = T_{i_1} \cdots T_{i_k}$ where $s_{i_1} \cdots s_{i_k} = w$ is a reduced decomposition for any $w \in W_{\text{aff}}$ with $l(w) = k$. It is easy to see that the T_w span $\mathcal{H}_q(W_{\text{aff}})$.

Theorem 21 *We have an isomorphism $\mathcal{H}_J \longrightarrow \mathcal{H}_q(W_{\text{aff}})$ in which $\phi_{s_i} \longmapsto T_i$.*

Proof We have checked that the ϕ_i satisfy the quadratic relations in Proposition 55. The braid relations follow from Corollary 1. For example, suppose that the order $n(i,j)$ of $s_i s_j$ is 3; then $s_i s_j s_i = s_j s_i s_j$. Let w denote $s_i s_j s_i$. Then $l(w) = l(s_i) + l(s_j) + l(s_i)$ and so $\phi_w = \phi_{s_i} * \phi_{s_j} * \phi_{s_i}$. Similarly $\phi_w = \phi_{s_j} * \phi_{s_i} * \phi_{s_j}$, and so the braid relation is satisfied. Hence there is a homomorphism $\mathcal{H}_q(W_{\text{aff}}) \longrightarrow \mathcal{H}_J$ in which $T_i \longrightarrow \phi_{s_i}$.

Since the T_w span $\mathcal{H}_q(W_{\text{aff}})$, and their images ϕ_w are a basis of $\mathcal{H}_J$, it follows that this homomorphism is a vector space isomorphism. □

16 Bernstein-Zelevinsky Presentation

An important presentation was described by Bernstein in lectures but never published by him. He proved it in collaboration with Zelevinsky, but they did not publish the proof. The first proof was published in

- Lusztig, Affine Hecke algebras and their graded version. J. Amer. Math. Soc. 2 (1989), no. 3, 599–635.

Another proof, for GL_n only, is found in:

- Howe, Affine-like Hecke algebras and p-adic representation theory. Iwahori-Hecke algebras and their representation theory (Martina-Franca, 1999), 27–69, Lecture Notes in Math., 1804, Springer, Berlin, 2002.

Another proof is found in:

- Thomas J. Haines, Robert E. Kottwitz, and Amritanshu Prasad. Iwahori-Hecke algebras. *http://arxiv.org/abs/math/0309168*, 2003.

The latter proof is less difficult than Lusztig's but starts with different premises since it does not begin with the abstract Hecke algebra given by the Iwahori-Matsumoto presentation.

We start with a root system Φ in a vector space V. Assume that Φ spans V. We recall that $Q^\vee$ is the coweight lattice, and $P^\vee$ be the coweight lattice. This is the set of $\lambda^\vee \in V^\vee = \mathbb{R} \otimes Q^\vee$ such that $\langle \lambda^\vee, \alpha \rangle \in \mathbb{Z}$ for all $\alpha \in \Phi$.

We recall that the affine Weyl group $W_{\rm aff}$ is the group generated by the simple reflections $\{s_0, s_1, \cdots, s_r\}$ in the walls of the fundamental alcove $\mathfrak{F}$. If $d \in Q^\vee$ we denote by $\tau(d)$ the translation $v \longmapsto v + d$. If we identify $Q^\vee$ with its image under τ, then $W_{\rm aff}$ is the semidirect product $W_{\rm aff} \ltimes Q^\vee$.

It is easy to see that translations by elements of $P^\vee$ also permute the alcoves, though these are generally not contained in $W_{\rm aff}$. The *extended affine Weyl* group $\tilde{W}_{\rm aff}$ is group generated by $\tau(P^\vee)$ and $W_{\rm aff}$. The whole group $\tilde{W}_{\rm aff}$ then acts on $V^\vee$, permuting the alcoves, extending the action of $W_{\rm aff}$ in which $Q^\vee$ acts by translations.

Remark 2 The extended affine Weyl group arises as follows. As we have seen, if G is a split semisimple group over a local field F that is simply connected then $N(T(F))/T(\mathfrak{o}) \cong W_{\rm aff}$. If G is *not* simply-connected the group $N(T(F))/T(\mathfrak{o})$ is larger than $W_{\rm aff}$. In the extreme case where G is of adjoint type, then $N(T(F))/T(\mathfrak{o}) \cong \tilde{W}_{\rm aff}$.

There is a difference between the actions of $Q^\vee$ and $P^\vee$ on the alcoves. If $\lambda^\vee \in P^\vee$ but $\lambda^\vee \notin Q^\vee$, the translate $\mathfrak{F} + \lambda^\vee$ is an alcove, so it agrees with $w\mathfrak{F}$ for some $w \in W_{\rm aff}$. However since $\lambda^\vee \notin Q^\vee$, $\tau(\lambda^\vee) \notin W_{\rm aff}$. Thus the transformations $v \longmapsto v + \lambda^\vee$ and $v \longmapsto wv$ are not the same. Both transformations take $\mathfrak{F}$ to the same alcove, but in a different spatial orientation. This leads to the following Proposition.

Proposition 56 *The finite abelian group $P^\vee/Q^\vee$ is isomorphic to the finite group Ω of affine linear maps in $\tilde{W}_{\rm aff}$ that stabilize $\mathfrak{F}$. Since $\{s_0, \cdots, s_r\}$ are the reflections in the walls of $\mathfrak{F}$, this means that if $t \in \Omega$ then $s_i \longmapsto t s_i t^{-1}$ is a permutation of $\{s_0, \cdots, s_r\}$. The group $\tilde{W}_{\rm aff}$ is the semidirect product $W_{\rm aff} \ltimes (P^\vee/Q^\vee)$ by this finite group of automorphisms.*

Any automorphism of the Coxeter group $W_{\rm aff}$ that permutes the generators must preserve the braid relations, which are encoded in the extended Dynkin diagram. The group $P^\vee/Q^\vee$ can therefore be interpreted as a subgroup of the group of automorphisms of the extended Dynkin diagram.

Proof Conjugation by an element of the subgroup Ω of $\tilde{W}_{\rm aff}$ that stabilizes $\mathfrak{F}$ permutes the reflections $\{s_0, \cdots, s_r\}$ in the walls of $\mathfrak{F}$, and so it normalizes the group $W_{\rm aff}$ that they generate. If $\lambda^\vee \in P^\vee$ then $\tau(\lambda^\vee)\mathfrak{F} = \mathfrak{F} + \lambda^\vee$ is

an alcove, so there exists a unique $w \in W_{\text{aff}}$ such that $w\tau(\lambda^\vee)\mathfrak{F} = \mathfrak{F}$. Now $w\tau(\lambda^\vee) \in \Omega$. Hence $W_{\text{aff}} \cdot \Omega$ contains W_{aff} and $P^\vee$ with W_{aff} as a normal subgroup, and since these generate $\tilde{W}_{\text{aff}}$, we have $\tilde{W}_{\text{aff}} = W_{\text{aff}} \rtimes \Omega$. □

We extend the length function on W_{aff} by writing $l(wt) = l(w)$ when $t \in \Omega$. Therefore elements of Ω have length zero.

Proposition 57 *If $w \in \tilde{W}_{\text{aff}}$ then $l(w)$ is the number of hyperplanes $H_{\alpha,k}$ between $\mathfrak{F}$ and $w\mathfrak{F}$.*

Proof If $w \in W_{\text{aff}}$ then this follows from Lemma 8 and Theorem 14. For general $w \in \tilde{W}_{\text{aff}}$, there is $w' \in W_{\text{aff}}$ and $t \in \Omega$ such that $w = w't$. Now $w\mathfrak{F} = w'\mathfrak{F}$ and $l(w) = l(w')$, and the statement follows. □

We say that $\lambda^\vee \in P^\vee$ is *dominant* if $\langle \alpha_i, \lambda^\vee \rangle \geqslant 0$ for $i = 1, \cdots, r$.

Proposition 58 *Let $\lambda^\vee$ is a dominant element of $P^\vee$. Then with $1 \leqslant i \leqslant r$ we have*

$$l(\tau(\lambda^\vee)s_i) = \begin{cases} l(\tau(\lambda^\vee)) + 1 & \text{if } \langle \alpha_i, \lambda^\vee \rangle = 0, \\ l(\tau(\lambda^\vee)) - 1 & \text{if } \langle \alpha_i, \lambda^\vee \rangle > 0. \end{cases}$$

Proof Let $w = \tau(\lambda^\vee)s_i$. Suppose that $\langle \alpha_i, \lambda^\vee \rangle = 0$. Then every hyperplane $H_{\alpha,k}$ that separates $\mathfrak{F}$ from $\mathfrak{F} + \lambda^\vee$ also separates $\mathfrak{F}$ from $s_i\mathfrak{F} + \lambda^\vee$, and there is one more that lies between $\mathfrak{F}$ and $s_i\mathfrak{F} + \lambda^\vee$, namely the hyperplane $H_{\alpha_i,0}$, which is a wall of the positive Weyl chamber. Thus $l(\tau(\lambda^\vee)s_i) = l(\tau(\lambda^\vee)) + 1$.

On the other hand, suppose that $\langle \alpha_i, \lambda^\vee \rangle > 0$. Let us count the hyperplanes between $\mathfrak{F}$ and $s_i\mathfrak{F}$ as follows. Let $v \in \mathfrak{F}$ be very close to the wall $L_i = H_{\alpha_i,0}$. Then $s_iv + \lambda^\vee$ lies in $s_i\mathfrak{F} + \lambda^\vee$ and is close to v and we follow a straight line from an interior point of $\mathfrak{F}$ to the two points v and $s_iv + \lambda^\vee$. These intersect the same hyperplanes except that the path to $s_i\mathfrak{F} + \lambda^\vee$ does not intersect $H_{\alpha_i,0} + \lambda^\vee$. Therefore $l(\tau(\lambda^\vee)s_i) = l(\tau(\lambda^\vee)) - 1$. □

Let $\mathcal{H}_q(W_{\text{aff}})$ be an Iwahori Hecke algebra associated with W_{aff}. That is, it has generators $T_0, T_1, \cdots, T_r$ with the usual relations, determined by the extended Dynkin diagram of an irreducible root system Φ. The parameter q can be an indeterminate, for the ring is described in terms of generators and relations. We will eventually need both q and $\sqrt{q}$ to be in the ground field.

The relations satisfied by the T_i are the braid relations, and the quadratic relations $T_i^2 = (q-1)T_i + q$. The ring $\mathcal{H}_q(W_{\text{aff}})$ has a basis consisting of elements T_w ($w \in W_{\text{aff}}$) where $T_w = T_{i_1} \cdots T_{i_k}$ when $w = s_{i_1} \cdots s_{i_k}$ is a

reduced decomposition of w into a product of simple reflections. This is well-defined by Tits' theorem (Theorem 14).

Let $\mathcal{H}_q(\tilde{W}_{\text{aff}})$ be the algebra with basis T_w where $w \in \tilde{W}_{\text{aff}}$, with the following description. It has generators T_i with $i \in \{0, 1, \cdots, r\}$ subject to the braid and quadratic relations, with additional generators T_t ($t \in \Omega$), subject to the conditions that $T_t T_u = T_{tu}$ when $t, u \in \Omega$, and the additional relations $T_t T_w = T_{twt^{-1}} T_t$ when $t \in \Omega$ and $w \in W_{\text{aff}}$.

Proposition 59 *If $w, w' \in \tilde{W}_{\text{aff}}$ and $l(ww') = l(w) + l(w')$ then $T_w T_{w'} = T_{ww'}$.*

Proof First consider the case where $w, w' \in W_{\text{aff}}$. Let $w = s_{i_1} \cdots s_{i_k}$ and $w' = s_{j_1} \cdots s_{j_l}$ be reduced decompositions, so $k = l(w)$ and $l = l(w')$. Then $ww' = s_{i_1} \cdots s_{i_k} s_{j_1} \cdots s_{j_l}$ is a reduced decomposition, and $T_{ww'} = T_{i_1} \cdots T_{i_k} T_{j_1} \cdots T_{j_l} = T_w T_{w'}$.

Now we turn to the general case. Write $w = w_1 t$ and $w' = w_1' t'$ where $t, t' \in \Omega$. Let $w_2' = t w_1' t^{-1} \in W_{\text{aff}}$. It has the same length as w_1', since conjugation by t simply permutes the generators. Now $ww' = w_1 w_2' t t'$ and $l(w_1 w_2') = l(w_1) + l(w_2')$. Thus $T_{w_1 w_2'} = T_{w_1} T_{w_2'}$. We have

$$T_w = T_{w_1} T_t, \qquad T_{w'} = T_{w_1'} T_{t'},$$

so

$$T_{ww'} = T_{w_1 w_2' t t'} = T_{w_1 w_2'} T_{tt'} = T_{w_1} T_{w_2'} T_t T_{t'} = T_{w_1} T_t T_{w_1'} T_{t'} = T_w T_{w'}.$$

□

Lemma 16 *T_w is invertible. Indeed, if $w = s_{i_1} \cdots s_{i_k}$ then*

$$T_w^{-1} = T_{s_{i_k}}^{-1} \cdots T_{s_{i_1}}^{-1}, \qquad T_i^{-1} = q^{-1} T_i + (1 - q^{-1}). \tag{63}$$

Proof It follows from the quadratic relation $T_i^2 + (q-1)T_i + q = 0$ that $q^{-1} T_i + (1 - q^{-1})$ is an inverse to T_i. The rest is immediate. □

The Bernstein-Zelevinsky presentation is related to the realization of the affine Weyl group as a semidirect product $\tilde{W}_{\text{aff}} = W \ltimes P^\vee$. It realizes the algebra $\mathcal{H}_q(W_{\text{aff}})$ as the amalgamation of two subalgebras, namely $\mathcal{H}_q(W)$ and an abelian subalgebra isomorphic to the group algebra of $P^\vee$.

We have a map $P^\vee \to \mathcal{H}_q(\tilde{W}_{\rm aff})^\times$ defined by $d \mapsto T_d$. But this map is not a homomorphism. Indeed, by Proposition 59 $T_w T_{w'} = T_{ww'}$ if $l(ww') = l(w) + l(w')$ though not generally otherwise. Therefore

However we may obtain a proper homomorphism $P^\vee \longrightarrow \mathcal{H}_q(W_{\rm aff})^\times$ as follows. Let $P^\vee_{\rm dom}$ be the set of dominant weights in the coroot lattice. Thus $d \in P^\vee_{\rm dom}$ if $d \in P^\vee$ and $\langle d, \alpha\rangle \geqslant 0$ for every root α.

Lemma 17 *If $d, d' \in P^\vee_{\rm dom}$ then $l(dd') = l(d) + l(d')$ and so $T_{dd'} = T_d T_{d'}$.*

Proof We use the characterization that $l(d)$ is the number of hyperplanes $H_{\alpha,k}$ that lie between the fundamental alcove $\mathfrak{F}$ and $\mathfrak{F} + d$. Let $H_1, \cdots, H_k$ be the hyperplanes between $\mathfrak{F}$ and $\mathfrak{F} + d$, and $H'_1, \cdots, H'_l$ be the hyperplanes between $\mathfrak{F}$ and $\mathfrak{F} + d'$. The $k+l$ hyperplanes $H_1, \cdots, H_k, H'_1 + d, \cdots, H'_l + d$ lie between $\mathfrak{F}$ and $\mathfrak{F} + d + d'$. Indeed, Each of the hyperplanes H_i is perpendicular to α for some positive root α. Since $\langle d, \alpha\rangle \geqslant 0$, we may take a straight-line path from $v \in \mathfrak{F}$ to $v + d$, and follow that by a straight-line path from $v + d$ to $v + d + d'$ and it will cross each of the advertised hyperplanes exactly once.

The last statement follows by Proposition 59. □

Now we have a monoid homomorphism $\theta : P^\vee_{\rm dom} \to \mathcal{H}_q(\tilde{W}_{\rm aff})^\times$ defined by $\theta(d) = q^{-l(d)/2} T_d$. The group $P^\vee$ is the Grothendieck group of this monoid. That is, it is universal for homomorphisms of the monoid $P^\vee_{\rm dom}$ into groups. Therefore we obtain a homomorphism $\theta : P^\vee \to \mathcal{H}_q^\times(\tilde{W}_{\rm aff})$ such that $\theta(d) = q^{-l(d)/2} T_d$ when d is dominant. In general, if we have $d \in P^\vee$ we may write $d = d_1 - d_2$ with d_1 and d_2 dominant, and $\theta(d) = q^{(l(d_2) - l(d_1))/2} T_{d_1} T_{d_2}^{-1}$.

The group homomorphism $\theta : P^\vee \longrightarrow \mathcal{H}_q^\times(\tilde{W}_{\rm aff})^\vee$ extends to a ring homomorphism from the group algebra $\mathbb{C}[P^\vee] \longrightarrow \mathcal{H}^\times(\tilde{W}_{\rm aff})$. The image Θ of this map is the vector space spanned by the elements $\theta(d)$ with $d \in P^\vee$. This is an abelian subalgebra Θ isomorphic to the group algebra of $P^\vee$. We wish to consider $\mathcal{H}_q(\tilde{W}_{\rm aff})$ as an amalgam of this commutative ring Θ and $\mathcal{H}_q(W)$.

Let $\omega_1^\vee, \cdots, \omega_k^\vee$ be the fundamental coweights, defined by the formula

$$\langle \alpha_i, \omega_j^\vee \rangle = \delta_{ij}, \qquad (i = 1, \cdots, r). \tag{64}$$

Lemma 18 *Let $\lambda^\vee \in P^\vee_{\rm dom}$. Then $l(\tau(\lambda^\vee)) = \langle 2\rho, \lambda^\vee\rangle$ where*

$$\rho = \frac{1}{2} \sum_{\alpha \in \Phi^+} \alpha.$$

Proof The proof of Proposition 48 goes through without much change. Let $w \in W_{\text{aff}}$ such that $w\mathfrak{F} = \tau(\lambda^\vee)\mathfrak{F}$. Then $\tau(\lambda^\vee) = wt$ for some $t \in \Omega$, so $l(\tau(\lambda^\vee)) = l(w)$. This is the number of hyperplanes $H_{\alpha,k}$ between $\mathfrak{F}$ and $\mathfrak{F} + \lambda^\vee$, and the number of these is counted as in Proposition 48. □

Lemma 19 *We have*

$$\omega_k^\vee + s_k(\omega_k^\vee) = \sum_{j \neq k} (-\langle \alpha_j, \alpha_k^\vee \rangle) \omega_j^\vee.$$

This is an element of $P_{\text{dom}}^\vee$. *Moreover*

$$\sum_{j \neq k} (-\langle \alpha_j, \alpha_k^\vee \rangle) l(\tau(\omega_j^\vee)) = l\left(\tau\left(\sum_{j \neq k}\left(-\langle \alpha_j, \alpha_k^\vee \rangle\right)\omega_j^\vee\right) s_k\right) - 1 = 2l(\tau(\omega_k^\vee)) - 2. \tag{65}$$

Proof We have

$$s_k(\omega_k^\vee) = \omega_k^\vee - \langle \alpha_k, \omega_k^\vee \rangle \alpha_k^\vee = \omega_k^\vee - \alpha_k^\vee.$$

Now expanding $\alpha_k^\vee = \sum c_j \varepsilon_j^\vee$, using (64) we have $c_j = \langle \alpha_j, \alpha_k^\vee \rangle$.

$$\omega_k^\vee + s_k(\omega_k^\vee) = 2\omega_k^\vee - \alpha_k^\vee = 2\omega_k^\vee - \sum_{j=1}^{r} \langle \alpha_j, \alpha_k^\vee \rangle \omega_j^\vee = -\sum_{j \neq k} \langle \alpha_j, \alpha_k^\vee \rangle \omega_j^\vee, \tag{66}$$

since $\langle \alpha_k, \alpha_k^\vee \rangle = 2$. The coefficients $-\langle \alpha_j, \alpha_k^\vee \rangle$ are all nonnegative, so this is in $P_{\text{dom}}^\vee$. By Lemma 17

$$\sum_{j \neq k} (-\langle \alpha_j, \alpha_k^\vee \rangle) l(\tau(\omega_j^\vee)) = l\left(\sum_{j \neq k} -\langle \alpha_j, \alpha_k^\vee \rangle \tau(\omega_j^\vee)\right).$$

Now α_k is orthogonal to $\omega_j^\vee$ when $k \neq j$, and it follows from Proposition 58 that

$$l\left(\tau\left(\sum_{j \neq k}\left(-\langle \alpha_j, \alpha_k^\vee \rangle\right)\omega_j^\vee\right) s_k\right) = l\left(\sum_{j \neq k} -\langle \alpha_j, \alpha_k^\vee \rangle \tau(\omega_j^\vee)\right) + 1.$$

It is well-known that ρ is the sum of the fundamental weights ω_i defined by $\langle \alpha_i^\vee, \omega_j \rangle = \delta_{ij}$, so $\langle \rho, \alpha_k^\vee \rangle = 1$. (Bump, *Lie Groups*, Proposition 21.16.) Using Lemma 18,

$$\left(\sum_{j \neq k} -\langle \alpha_j, \alpha_k^\vee \rangle \tau(\omega_j^\vee) \right) = \langle 2\rho, \omega_k^\vee + s_k(\omega_k^\vee) \rangle = \langle 2\rho, 2\omega_k^\vee - \alpha_k \rangle \quad =$$

$$2\langle 2\rho, \omega_k^\vee \rangle - 2\langle \rho, \alpha_k^\vee \rangle \quad = \quad 2l(\tau(\omega_k^\vee)) - 2.$$

□

Lemma 20 *If $\lambda^\vee \in P^\vee$ is orthogonal to α_k, then T_k and $T_{\tau(\lambda^\vee)}$ commute.*

Proof We may write $\lambda^\vee$ as the difference of two dominant coweights that are orthogonal to α_k and hence reduce to the case where $\lambda^\vee$ is dominant. By Proposition 58 we have $l(\tau(\lambda^\vee)s_k) = l(\tau(\lambda^\vee)) + 1$. Since $s_k(\lambda^\vee) = \lambda^\vee - \langle \alpha, \lambda^\vee \rangle \alpha_k^\vee = \lambda^\vee$ we have

$$s_k \tau(\lambda^\vee) s_k^{-1} = \tau(s_k(\lambda^\vee)) = \tau(\lambda^\vee)$$

so $\tau(\lambda^\vee)s_k = s_k\tau(\lambda^\vee)$, and $l(s_k\tau(\lambda^\vee)) = l(\tau(\lambda^\vee)s_k) = \lambda(\tau(\lambda^\vee)) + 1$ also. Therefore by Proposition 59 we have

$$T_k T_{\tau(\lambda^\vee)} = T_{s_k} T_{\tau(\lambda^\vee)} = T_{s_k \tau(\lambda^\vee)} = T_{\tau(\lambda^\vee)} T_{s_k} = T_{\tau(\lambda^\vee)} T_k.$$

□

Lemma 21 *We have*

$$T_{\tau(\omega_k^\vee) s_k} T_{\tau(\omega_k^\vee)} = T_k \left(\prod_{j \neq k} T_{\tau(\omega_j^\vee)}^{-\langle \alpha_j, \alpha_k^\vee \rangle} \right). \tag{67}$$

Proof By Lemma 19

$$\tau(\omega_k^\vee) s_k \tau(\omega_k^\vee) s_k^{-1} = \tau(\omega_k^\vee)\tau(s_k(\omega_k^\vee)) = \tau\left(\sum_{j \neq k} \Big(- \langle \alpha_j, \alpha_k^\vee \rangle \Big) \omega_j^\vee \right)$$

so

$$\tau(\omega_k^\vee) s_k \tau(\omega_k^\vee) = \tau\left(\sum_{j \neq k} \Big(- \langle \alpha_j, \alpha_k^\vee \rangle \Big) \omega_j^\vee \right) s_k. \tag{68}$$

By Lemma 19

$$l\left(\tau\left(\sum_{j\neq k}\left(-\langle\alpha_j,\alpha_k^\vee\rangle\right)\omega_j^\vee\right)s_k\right)=2l(\tau(\omega_k^\vee))-1. \tag{69}$$

Furthermore by Proposition 59 we have

$$T_{\tau\left(\sum_{j\neq k}\left(-\langle\alpha_j,\alpha_k^\vee\rangle\right)\omega_j^\vee\right)s_k}=T_{\tau\left(\sum_{j\neq k}\left(-\langle\alpha_j,\alpha_k^\vee\rangle\right)\omega_j^\vee\right)}T_{s_k}=T_k\left(\prod_{j\neq k}T_{\tau(\omega_j^\vee)}^{-\langle\alpha_j,\alpha_k^\vee\rangle}\right).$$

We have used the fact that $T_{\tau(\omega_j^\vee)}T_k=T_kT_{\tau(\omega_j^\vee)}$ when $j\neq k$ by Lemma 20 to move the T_k across the product.

On the other hand by Proposition 58 we have

$$l(\tau(\omega_k^\vee)s_k)=l(\tau(\omega_k))-1.$$

By (69) the length of (68) is $2l(\tau(\omega_k))-1$, so Proposition 59 implies that

$$T_{\tau(\omega_k^\vee)s_k\tau(\omega_k^\vee)}=T_{\tau(\omega_k)s_k}T_{\tau(\omega_k^\vee)}.$$

Invoking (68) one more time gives (67). □

Theorem 22 *Let $d\in P^\vee$ and let $1\leqslant k\leqslant r$. Then $\theta(d)-\theta(s_kd)$ is divisible by $1-\theta(-\alpha_k^\vee)$ in the ring Θ and*

$$\theta(d)T_k-T_k\theta(s_k(d))=T_k\theta(d)-\theta(s_k(d))T_k=(q-1)\frac{\theta(d)-\theta(s_k(d))}{1-\theta(-\alpha_k^\vee)}. \tag{70}$$

Proof It is enough to show

$$\theta(d)T_k-T_k\theta(s_k(d))=(q-1)\frac{\theta(d)-\theta(s_k(d))}{1-\theta(-\alpha_k^\vee)}. \tag{71}$$

Indeed, if this is known, then replacing d by $s_k(d)$ and multiplying both sides by -1 gives another expression for the right-hand side, namely $T_k\theta(d)-\theta(s_k(d))T_k$.

First suppose that (71) is true for d and d'. Then since θ is a homomorphism from $P^\vee$ to $\mathcal{H}(\tilde{W}_{\text{aff}})^\times$ we have

$$\begin{aligned}\theta(d+d')T_k-T_k\theta(s_k(d+d')) \;&=\\ \theta(d)[\theta(d')T_k-T_k\theta(s_k(d')]+[\theta(d)T_k-T_k\theta(s_k(d))]\theta(s_k(d')).&\end{aligned}$$

Substituting (71) and simplifying we see that it is true for $\theta(d+d')$. A similar argument shows that (71) for d implies the same formula for $-d$. Therefore we are reduced to the case where d is chosen from a basis of $P^\vee$.

We have

$$s_k\omega_i^\vee = \omega_i^\vee - \langle \alpha_k, \omega_i^\vee\rangle \alpha_k^\vee = \begin{cases} \omega_k^\vee - \alpha_k^\vee & \text{if } i = k, \\ 0 & \text{if } i \neq k. \end{cases}$$

Therefore

$$\frac{\theta(\omega_i^\vee) - \theta(s_k\omega_i^\vee)}{1 - \theta(-\alpha_k^\vee)} = \begin{cases} \theta(\omega_k^\vee) & \text{if } i = k, \\ 0 & \text{if } i \neq k. \end{cases}$$

We must therefore show that

$$\theta(\omega_i^\vee)T_k - T_k\theta(s_k(\omega_i^\vee)) = \begin{cases} \theta(\omega_k^\vee) & \text{if } i = k, \\ 0 & \text{if } i \neq k. \end{cases} \tag{72}$$

Let us first consider the case where $i \neq k$. In this case $s_k(\omega_i^\vee) = \omega_i^\vee$, by Lemma 20 T_k and $\theta(\omega_i^\vee)$ commute, so (72) is satisfied.

Next let us consider the case where $i = k$. We will prove

$$T_k\theta(s_k(\omega_k^\vee)) = q^{1-l(\omega_k^\vee)/2}T_{\tau(\omega_k^\vee)s_k}. \tag{73}$$

By Lemma 19 $s_k(\omega_k^\vee) = \left(-\sum_{j\neq k}\langle \alpha_j, \alpha_k^\vee\rangle\omega_k^\vee\right) - \omega_k^\vee$ is expressed as a difference between two dominant elements of $P^\vee$. Therefore

$$\theta(s_k(\omega_k^\vee)) = \prod_{j\neq k}(q^{-l(\omega_j^\vee)/2}T_{\tau(\omega_j^\vee)})^{-\langle \alpha_j, \alpha_k^\vee\rangle}q^{l(\omega_k)/2}T^{-1}_{\tau(\omega_k^\vee)}.$$

The factors on the right-hand side commute with each other since the image of $\tau(P^\vee)$ is commutative. (See Lemma 17.) Using Lemma 19 we may rewrite this

$$\theta(s_k(\omega_k^\vee)) = q^{1-l(\omega_k^\vee)/2}\prod_{j\neq k}T^{-\langle \alpha_j, \alpha_k^\vee\rangle}_{\tau(\omega_j^\vee)}T^{-1}_{\tau(\omega_k^\vee)}.$$

Using (67) we obtain (73).

Now by Proposition 58 we have $l(\tau(\omega_k^\vee)s_k) = l(\tau(\omega_k^\vee)) - 1$ and so by Proposition 59 we have $T_{\omega_k^\vee s_k}T_k = T_{\omega_k^\vee}$. Therefore (using

$$T_k\theta(s_k(\omega_k^\vee)) = q^{1-l(\omega_k^\vee)/2}T_{\tau(\omega_k^\vee)}T_k^{-1} = q^{1-l(\omega_k^\vee)/2}T_{\tau(\omega_k^\vee)}(q^{-1}T_k + (1-q^{-1})).$$

Thus

$$T_k\theta(s_k(\omega_k^\vee)) - \theta(\omega_k^\vee)T_k = (q-1)\theta(\omega_k^\vee),$$

proving (72) when $i = k$. □

Now we may describe the Bernstein-Zelevinsky presentation as follows: it is generated by the finite Hecke algebra $\mathcal{H}_q(W)$, which is a $|W|$-dimensional algebra over $\mathbb{C}$, and by an algebra Θ which is isomorphic to the group algebra of $P^\vee$ under a homomorphism $\theta : P^\vee \longrightarrow \Theta$. These two algebras are subject to the relation (70).

This is a very convenient presentation of $\mathcal{H}_q(\tilde{W}_{\text{aff}})$. Of course it gives rise to a presentation of $\mathcal{H}_q(W_{\text{aff}})$ in which we restrict ourselves to the subalgebra of Θ generated by the image of $Q^\vee$.

17 The Center of $\mathcal{H}_J$

The *Bruhat order* is an order on a Coxeter group. We will explain it for the Weyl group W with simple reflections $\{s_1, \cdots, s_r\}$. We recall that if $\alpha \in \Phi^+$ is a positive root then there is a reflection r_α in the hyperplane perpendicular to α.

Lemma 22 *Let $v = s_{i_1} \cdots s_{i_k}$ be a reduced decomposition of $v \in W$, so $k = l(v)$. Then there exists a j such that*

$$u = s_{i_1} \cdots \widehat{s_{i_j}} \cdots s_{i_k} \tag{74}$$

if and only if there exists $\alpha \in \Phi^+$ such that $v(\alpha) \in \Phi^-$ and $u = v.r_\alpha$.

The "hat" denotes the omission of the factor s_{i_j}. We note that (74) may not be a reduced decomposition.

Proof The $\alpha \in \Phi^+$ such that $v(\alpha) \in \Phi^-$ are listed in Proposition 22. Such a α is one of $s_{i_k} s_{i_{k-1}} \cdots s_{i_{j+1}}(\alpha_{i_j})$. Then $r_\alpha = s_{i_k} s_{i_{k-1}} \cdots s_{i_{j+1}} s_{i_j} (s_{i_k} s_{i_{k-1}} \cdots s_{i_{j+1}})^{-1}$ and so (74) is valid. □

Lemma 23 *Suppose that $v = s_{i_1} \cdots s_{i_k}$ is a reduced decomposition of $v \in W$, so $k = l(v)$. Suppose there exists a subsequence $\{j_1, \cdots, j_l\}$ of $\{i_1, \cdots, i_k\}$ such that*

$$u = s_{i_1} \cdots \widehat{s_{j_1}} \cdots \widehat{s_{j_2}} \cdots\cdots s_{i_k}.$$

Then there exists another subsequence $\{j_1', j_2', \cdots\}$ such that

$$u = s_{i_1} \cdots \widehat{s_{j_1'}} \cdots \widehat{s_{j_2'}} \cdots\cdots s_{i_k},$$

and such that the latter decomposition is reduced.

Proof Using repeated applications of Proposition 15 we may further discard pairs of elements of the sequence of simple reflections until we obtain a reduced word. □

Let us say that $u \leqslant v$ in the Bruhat partial order if the following condition is satisfied. There must be a sequence $r_1, \cdots, r_l$ of reflections such that

$$l(v) > l(vr_1) > l(vr_1r_2) > \cdots > l(vr_1 \cdots r_l)$$

and $u = vr_1 \cdots r_l$.

Proposition 60 *Let $u, v \in W$ and let $v = s_{i_1} \cdots s_{i_k}$ be a reduced decomposition. Then $u \leqslant v$ if and only if there exists a subsequence $\{j_1, \cdots, j_l\}$ of $\{i_1, \cdots, i_k\}$ such that*

$$u = s_{i_1} \cdots \widehat{s_{j_1}} \cdots \widehat{s_{j_2}} \cdots \cdots s_{i_k}.$$

If so, we may assume that this decomposition is reduced.

It is a remarkable fact that this criterion does not depend on the choice of a reduced decomposition of v.

Proof This follows Lemmas 22 and 23. □

Using affine roots, the Bruhat order may defined for affine Weyl groups, and Proposition 60 remains valid.

If $w \in W$ and

Lemma 24 *Let $w \in W$ and let $d \in P^\vee$. Then $\theta(d)T_w - T_w\theta(w^{-1}(d))$ lies in the Θ-submodule of $\mathcal{H}_q(\tilde{W}_{\text{aff}})$ spanned by $u \in W$ with $u < w$ in the Bruhat order.*

Proof Write $w = s_{i_1} \cdots s_{i_k}$, a reduced decomposition. Then writing $w_l = s_{i_1} \cdots s_{i_l}$ we may write

$$\theta(d)T_w - T_w\theta(w^{-1}d) = \sum_{l=1}^{k} T_{w_{l-1}}\theta(w_{l-1}^{-1}d)T_{i_l} \cdots T_{i_k} - T_{w_{l-1}}\theta(T_{i_l}w_{l-1}d)T_{i_{l+1}} \cdots T_{i_k}.$$

Using the Bernstein relation (70) the l-th term is in

$$T_{i_1} \cdots T_{i_{l-1}} \Theta T_{i_{l+1}} \cdots T_{i_k}.$$

This is contained in the Θ-submodule of $\mathcal{H}_q(\tilde{W}_{\text{aff}})$ spanned by $u \in W$ with $u < w$. □

Theorem 23 *The center $\mathcal{Z}$ of $\mathcal{H}_q(\tilde{W}_{\text{aff}})$ equals Θ^W, the space of elements of Θ that are invariant under conjugation by W.*

Proof First let us show that the center $\mathcal{Z}$ is contained in Θ. Let us write an element as

$$\sum_{\substack{w \in W \\ d \in P^\vee}} c(w,d)\, w\theta(d).$$

Let w be maximal with respect to the Bruhat order such that some coefficient $c(w,d) \neq 0$. If $\lambda^\vee \in P^\vee$ then

$$\theta(\lambda^\vee) w\theta(d)\theta(\lambda^\vee)^{-1} \equiv w\theta(d - w^{-1}(\lambda^\vee) + \lambda^\vee)$$

module the Θ-submodule of $\mathcal{H}_q(\tilde{W}_{\text{aff}})$ spanned by $u \in W$ with $u < w$. Since $\lambda^\vee$ is arbitrary, $d - w^{-1}(\lambda^\vee) + \lambda^\vee$ can take on an infinite number of values, which is a contradiction since only finitely many $c(w,d)$ can be nonzero.

Therefore $\mathcal{Z} \subseteq \Theta$. We must show that an elemen

$$\zeta = \sum_{d \in P^\vee} c(d)\theta(d)$$

of Θ is central if and only if $c(d)$ is constant on W-orbits. We have

$$T_k \left(\sum_{d \in P^\vee} c(d)\theta(d) \right) - \left(\sum_{d \in P^\vee} c(s_k(d))\theta(d) \right) T_k = \frac{q-1}{1-\theta(-\alpha_k^\vee)} \sum [c(d) - c(s_k d)]\theta(d).$$

From this, it is clear that if $c(d)$ is constant on W-orbits then ζ is central. Conversely, suppose that ζ is central. Then with $\eta = \sum_{d \in P^\vee} [c(d) - c(s_k(d))]\theta(d)$ we have

$$T_k \eta = \frac{q-1}{1-\theta(-\alpha_k^\vee)} \eta.$$

Since $\Theta \cap T_k \Theta = 0$ we get $\eta = 0$. Therefore ζ is invariant under s_k. Since this is true for every simple reflection, $\zeta \in \Theta^W$. □

18 Principal Series Representations: Finite Field

Let G be a split reductive group over $F = \mathbb{F}_q$. Let B be a Borel subgroup. Write $B = TU$ where T is a split maximal torus, and U its unipotent radical.

We have functors:

$$\begin{array}{ccc} \text{Representations} & \longrightarrow & \text{Representations} \\ \text{of } T(F) & \longleftarrow & \text{of } G(F) \end{array}$$

These are *parabolic induction* and its adjoint, the *Jacquet functor*. Since F is finite, we may restrict ourselves to finite-dimensional representations of these finite groups.

To define parabolic induction, begin with a module V of $T(F)$. Extend it to a character of $B(F)$ by letting $U(F)$ be in the kernel, and induce this module to $G(F)$. We will denote this induced module $\mathrm{Ind}_B^G(V)$

Let W be a module of $G(F)$. The Jacquet module in this case may be defined to be $W^{U(F)}$, the space of $U(F)$-invariants. Since T normalizes U, this is a U-submodule. We will denote the Jacquet module by $J(T)$.

The Jacquet module will have to be defined differently when F is a local. We could alternatively have defined it to be the quotient W/W_U where W_U is the vector subspace of V generated by elements of the form $v - \pi(u)v$ with $v \in V$ and $u \in U(F)$. This definition is correct for local fields F. But if F is finite, then W splits as a direct sum $W_U \oplus W^{U(F)}$, so the two definitions are equivalent.

Proposition 61 *Let W be a $G(F)$-module and V a $T(F)$-module. Then*

$$\mathrm{Hom}_{G(F)}(W, \mathrm{Ind}_B^G(V)) \cong \mathrm{Hom}_{T(F)}(J(W), V).$$

Proof By ordinary Frobenius reciprocity, we have

$$\mathrm{Hom}_{G(F)}(W, \mathrm{Ind}_B^G(V)) \cong \mathrm{Hom}_{B(F)}(W, V).$$

Since $U(F)$ acts trivially on W, any $B(F)$-equivariant map $W \longrightarrow V$ annihilates an element of the form $v - \pi(u)v$, hence factors through the canonical map $W \to J(W)$. □

Since $T(F)$ is abelian, its irreducible modules are one-dimensional. Let χ be a character of $T(F)$. An important question is when $\mathrm{Ind}_B^G(\chi)$ is irreducible. They Weyl group $W = N(T(F))/T(F)$ acts on $T(F)$ and hence on its characters by conjugation. Let us say that χ is *regular* if its stabilizer in W is trivial.

For example, if $G = \mathrm{GL}_n$ then T may be taken to be the diagonal torus, and there exist characters $\chi_1, \cdots, \chi_n$ such that

$$\chi \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix} = \prod_{i=1}^{n} \chi_i(t_i).$$

Then χ is regular if the χ_i are distinct.

Proposition 62 *Let χ and θ be characters of $T(F)$. Then the dimension of*

$$\mathrm{Hom}_{G(F)}(\mathrm{Ind}_B^G(\chi), \mathrm{Ind}_B^G(\theta))$$

is the number of $w \in W$ such that $\theta = {}^w\chi$.

Proof By Mackey theory, the dimension is the dimension of the space of Δ such that

$$\Delta(bgb') = \theta(b)\Delta(g)\chi(b'), \qquad b, b' \in B(F).$$

Such a function is determined on its values on the $B(F)$-double cosets, which have representatives in $N(F)$, one for each Weyl group element $w \in W$. Chosing a representative ω in $N(T(F))$ of W, we must have

$$\Delta(\omega) = \Delta(t\omega(\omega^{-1}t\omega)^{-1}) = \theta(t) \cdot \Delta(\omega) \cdot {}^w\chi(t)^{-1}, \qquad t \in T(F).$$

Thus we must have $\theta = {}^w\chi$, or else Δ vanishes identically on the double coset. Conversely if this is true, then it is easy to see that the double coset $B(F)\omega B(F)$ does support such a function Δ. □

Theorem 24 *A necessary and sufficient condition for $\mathrm{Ind}_B^G(\chi)$ to be irreducible is that χ be regular.*

This is *not* correct if F is a local field. For $G = \mathrm{GL}_n$, if F is local, the condition that $\mathrm{Ind}_B^G(\chi)$ be irreducible is that no $\chi_i(t) = \chi_j(t)|t|^{\pm 1}$. This is a major difference between the finite and nonarchimedean local cases.

Proof A necessary and sufficient condition is that $\mathrm{End}_{G(F)}(\mathrm{Ind}_B^G(\chi))$ is one-dimensional, and by Proposition 62 this is true if and only if χ has trivial stabilizer in W, that is, is regular. □

Theorem 25 *If χ is regular, then $\mathrm{Ind}_B^G(\chi)$ is isomorphic to $\mathrm{Ind}_B^G({}^w\chi)$ for any $w \in W$.*

Proof This follows from the existence of an intertwining operator, a consequence of Proposition 62. □

We may construct an explicit intertwining operator $M(w) : \mathrm{Ind}_B^G(\chi) \longrightarrow \mathrm{Ind}_B^G({}^w\chi)$ as follows. Interpret $\mathrm{Ind}_B^G(\chi)$ as the space of functions $G(F) \longrightarrow \mathbb{C}$ such that

$$f(bg) = \chi(b)f(g).$$

Let

$$M(w)f(g) = \sum_{u \in U(F) \cap wU_-(F)w^{-1}} f(w^{-1}ug). \tag{75}$$

Theorem 26 *If $f \in \mathrm{Ind}_B^G(\chi)$ then $M(w)f \in \mathrm{Ind}_B^G({}^w\chi)$. The map $M(w)$ commutes with the action of $G(F)$.*

Proof To check that $M(w)f \in \mathrm{Ind}_B^G({}^w\chi)$, note that if $t \in T(F)$ then since t normalizes $U \cap wU_-w^{-1}$ we have

$$M(w)f(tg) = \sum_{u \in U \cap wU_-w^{-1}} f(w^{-1}tw \cdot w^{-1}ug) = {}^w\chi(t)M(w)f(g).$$

We need to check that $M(w)f(ug) = M(w)f(g)$ for $u \in U(F)$. To this end, we note that $U(F) = (U(F) \cap wU_-(F)w)(U(F) \cap wU(F)w^{-1})$ by Proposition 30. The value of $f(w^{-1}ug)$ is unchanged if we alter u on the left by an element of $U(F) \cap wU(F)w^{-1}$. Thus we could also write

$$M(w)f(g) = \sum_{u \in (U(F) \cap wU(F)w^{-1}) \backslash U(F)} f(w^{-1}ug). \tag{76}$$

From this it is clear that $M(w)f$ is left $U(F)$-invariant. □

Lemma 25 *Assume $l(w_1w_2) = l(w_1) + l(w_2)$. We have*

$$\{\alpha \in \Phi^+ | (w_1w_2)^{-1}\alpha \in \Phi^-\} = \{\alpha \in \Phi^+ | w_1^{-1}\alpha \in \Phi^-\} \cup \{w_1(\alpha) \in \Phi^+ | w_2^{-1}\alpha \in \Phi^-\}.$$

The union is disjoint. Multiplication induces a bijection

$$w_1(U \cap w_2U_-w_2^{-1})w_1^{-1} \times (U \cap w_1U_-w_1^{-1}) \longrightarrow U \cap (w_1w_2)U_-(w_1w_2)^{-1}.$$

Proof The first part we leave to the reader. The first assertion in (ii) follows from (i) since

$$U \cap wU_-w^{-1} = \prod_{\{\alpha\in\Phi^+ | w^{-1}(\alpha)\in\Phi^-\}} x_\alpha(F).$$

That is, the multiplication map from the Cartesian product on the right to $U \cap wU_-w^{-1}$ is bijection, and the product may be taken in any fixed order.

$$\begin{aligned}
M_{w_1w_2}f(g) = \sum_{u\in U\cap(w_1w_2)U_-(w_1w_2)^{-1}} f((w_1w_2)^{-1}ug) &= \\
\sum_{u_1\in U\cap w_1U_-w_1^{-1}} \sum_{u_2\in w_1(U\cap w_2U_-w_2^{-1})w_1^{-1}} f(w_2^{-1}w_1^{-1}u_2u_1g) &= \\
\sum_{u_1\in U\cap w_1U_-w_1^{-1}} \sum_{u_2\in U\cap w_2U_-w_2^{-1}} f(w_2^{-1}w_1^{-1}w_1u_2w_1^{-1}u_1g) &= \\
\sum_{u_1\in U\cap w_1U_-w_1^{-1}} \sum_{u_2\in U\cap w_2U_-w_2^{-1}} f(w_2^{-1}u_2w_1^{-1}u_1g) &= M_{w_1}\circ M_{w_2}f(g).
\end{aligned}$$

□

Theorem 27 *If $l(ww') = l(w) + l(w')$ then $M(w_1)\circ M(w_2) = M(w_1w_2)$.*

Proof Using the Lemma,

$$\begin{aligned}
M_{w_1w_2}f(g) = \sum_{u\in U\cap(w_1w_2)U_-(w_1w_2)^{-1}} f((w_1w_2)^{-1}ug) &= \\
\sum_{u_1\in U\cap w_1U_-w_1^{-1}} \sum_{u_2\in w_1(U\cap w_2U_-w_2^{-1})w_1^{-1}} f(w_2^{-1}w_1^{-1}u_2u_1g) &= \\
\sum_{u_1\in U\cap w_1U_-w_1^{-1}} \sum_{u_2\in U\cap w_2U_-w_2^{-1}} f(w_2^{-1}w_1^{-1}w_1u_2w_1^{-1}u_1g) &= \\
\sum_{u_1\in U\cap w_1U_-w_1^{-1}} \sum_{u_2\in U\cap w_2U_-w_2^{-1}} f(w_2^{-1}u_2w_1^{-1}u_1g) &= M_{w_1}\circ M_{w_2}f(g).
\end{aligned}$$

□

Exercise 17 Suppose that χ is regular. Show that

$$J(\mathrm{Ind}_B^G(\chi)) = \bigoplus_{w\in W} {}^w\chi.$$

19 The L-group

References for the notion of the L-group:

- Langlands, *Problems in the theory of automorphic forms* and related papers, available at `http://publications.ias.edu/rpl/series.php?series=51`
- Borel, A. Automorphic L-functions. Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 27–61, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.

References for root data and reductive groups:

- Springer, T. A. Reductive groups. Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1, pp. 3–27, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.
- Demazure, Groupes Réductifs : Déploiements, Sous-Groupes, Groupes-Quotients, Springer Lecture Notes in Mathematics vol. 153 (1970).
- Borel, and Tits, Groupes rÃĬductifs. Inst. Hautes ÃĽtudes Sci. Publ. Math. No. 27 1965 55–150.

What data are needed to describe a reductive group?

Let us first ignore rationality issues and consider a reductive group G over an algebraically closed field. Then if T is a maximal torus, the root system Φ lives in $L = X^*(T)$, which is a lattice in the vector space $V = \mathbb{R} \otimes X^*(T)$.

Discarding the lattice and just considering the root system in V loses some information. For example, if G is semisimple, then knowledge of Φ in L determines the fundamental group, which is isomorphic to P/L, where P is the weight lattice, and the center of G, which is isomorphic to L/Q, where Q is the root lattice. If we simply regard Φ as living in the ambient Euclidean space $V = \mathbb{R} \otimes L$, this information is lost.

These considerations lead to the following definition of *root data*, due to Demazure and Grothendieck. Let L be a lattice, that is, a free $\mathbb{Z}$-module of finite rank, and let $L^\vee$ be its dual module, defined by a dual pairing $\langle\ ,\ \rangle : L \times L^\vee \longrightarrow \mathbb{Z}$ that identifies $L^\vee$ with $\mathrm{Hom}(L, \mathbb{Z})$. Let there be given in L and $L^\vee$ finite sets Φ and $\Phi^\vee$ of vectors with a bijection $\alpha \to \alpha^\vee$ of Φ to $\Phi^\vee$

subject to conditions that we now describe. If $\alpha \in \Phi$ then $s_\alpha : L^\vee \longrightarrow L^\vee$ is the reflection $s_\alpha(v) = v - \langle \alpha, v \rangle \alpha^\vee$ and $s_\alpha : L \longrightarrow L$ is defined by $s_\alpha(v) = v - \langle v, \alpha^\vee \rangle \alpha$. It is assumed that $\langle \alpha, \beta^\vee \rangle \in \mathbb{Z}$ and that $\langle \alpha, \alpha^\vee \rangle = 2$.

If these conditions are satisfied, then $(L, \Phi, L^\vee, \Phi^\vee)$ are called *root data*. For example, taking $L = X^*(T)$ and $L = X_*(T)$ the roots and coroots give root data, and this is exactly the information needed to reconstruct the group G. More data would be needed to construct G over a field F that is not algebraically closed, but since we are restricting ourselves to split groups, this is sufficient.

The definition of root data is symmetric, so $(L^\vee, \Phi^\vee, L, \Phi)$ are also root data, and correspond to a reductive group $\hat{G}$.

If the ground field is not algebraically closed, then further data is needed to describe G. Since the scope of this course is only split groups, we will ignore these issues. The group $\hat{G}(\mathbb{C})$ is only the connected component of the identity in the L-group ${}^L G$, but when G is F-split, it is sufficient for many purposes.

If G is F-split, the group $\hat{G}(\mathbb{C})$ is defined as above, and it controls the representation theory of $G(F)$. The strongest statement in this direction is the local Langlands correspondence, and this is outside the scope of this notes. An important special case is that the spherical representations of $G(F)$ are parametrized by the semisimple conjugacy classes of $\hat{G}(\mathbb{C})$, a statement closely related to the Satake isomorphism computing the structure of the spherical Hecke algebra. We will come to this later. At the moment, we will content ourselves with showing that the unramified quasicharacters of $T(F)$ are parametrized by elements of $\hat{T}(\mathbb{C})$.

If T is a group, a *quasicharacter* of T is a homomorphism $\chi : T \longrightarrow \mathbb{C}^\times$. If χ is unitary, then χ is called a *character*. If T is an abelian locally compact group, it has a unique maximal compact subgroup K, and it is normal. If T is furthermore totally disconnected, then K is open. In this case we will call χ *unramified* if it is trivial on that subgroup. Thus an unramified quasicharacter of $F^\times$ is a character that factors through $F^\times / \mathfrak{o}^\times \cong \mathbb{Z}$.

Given a torus T over a nonarchimedean local field F, there is a torus $\hat{T}$ over $\mathbb{C}$ such that the unramified characters of $T(F)$ are parametrized by the elements or $\hat{T}(\mathbb{C})$. For example if

$$T = \left\{ \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_{r+1} \end{pmatrix} \right\}$$

is the diagonal torus in GL_{r+1}, then we may take $\hat{T}$ also to be the diagonal torus in GL_{r+1}. If $t \in T$ and $\boldsymbol{z} \in \hat{T}$ we may write $t = (t_1, \cdots, t_n)$ and $\boldsymbol{z} = (z_1, \cdots, z_n)$ instead of

$$t = \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix}, \qquad \boldsymbol{z} = \begin{pmatrix} z_1 & & \\ & \ddots & \\ & & z_n \end{pmatrix},$$

for notational convenience. If $\boldsymbol{z} \in \hat{T}$ then we have a quasicharacter $\chi_{\boldsymbol{z}}$ of $T(F)$ defined by $\chi_{\boldsymbol{z}}(t) = \prod z_i^{\mathrm{ord}(t_i)}$. Every unramified quasicharacter is of this sort.

In general, let $X^*(T)$ be the group of rational characters of T, and $X_*(T)$ the group of one-parameter subgroups. As we explained in Section 12, both groups are isomorphic to $\mathbb{Z}^r$ and come equipped with a dual pairing $X^*(T) \times X_*(T) \longrightarrow \mathbb{Z}$ that makes $V = \mathbb{R} \otimes X^*(T)$ and $V^* = \mathbb{R} \otimes X_*(T)$ into dual spaces.

The exercises below will show that the torus $\hat{T}$ may be chosen so that $X_*(\hat{T}) \cong X^*(T)$ and $X^*(\hat{T}) \cong X_*(T)$. Let $X^{\mathrm{nr}}(T(F))$ denote the group of unramified characters of $T(F)$.

Exercise 18 Show that there is a natural isomorphism $\mathrm{Hom}(X_*(T), \mathbb{C}^\times) \cong X^{\mathrm{nr}}(T(F))$. Indeed, given $\chi \in X^{\mathrm{nr}}(T(F))$ associate with χ the homomorphism $X_*(T) \longrightarrow \mathbb{C}^\times$ be the map that sends the one-parameter subgroup $i : G_{\mathrm{m}} \longrightarrow T$ to $\chi(i(\varpi))$ for prime element ϖ.

Exercise 19 Show that there is a natural isomorphism $\mathrm{Hom}(X^*(\hat{T}), \mathbb{C}^\times) \cong \hat{T}(\mathbb{C})$. Indeed, give $\boldsymbol{z} \in \hat{T}(\mathbb{C})$, associate with $\boldsymbol{z}$ the homomorphism $X^*(\hat{T}) \longrightarrow \mathbb{C}^\times$ be the map that sends the rational character $\eta \in X^*(\hat{T})$ to $\eta(\boldsymbol{z}) \in \mathbb{C}^\times$.

Since $X_*(T)$ and $X^*(\hat{T})$ are identified, it is clear that the unramified characters of $T(F)$ are parametrized by the elements of $\hat{T}(\mathbb{C})$.

20 Intertwining integrals: nonarchimedean fields

The intertwining integrals appear very naturally in the theory of Eisenstein series. They were introduced into the theory of induced representations of Lie and p-adic groups by Bruhat around 1956.

Some results, particularly on analytic continuation of the integrals will be stated without proof. References:

- Casselman, *Introduction to Admissible Representations of p-adic Groups*, linked from the class web page. Section 6.4 contains the fundamental results about the intertwining operators.

- Casselman, The unramified principal series of p-adic groups. I. The spherical function. Compositio Mathematica, 40 no. 3 (1980), p. 387-406.

- Bump, *Automorphic Forms and Representations* only treats GL_2 completely, but many of the important ideas can be understood from that special case.

Let F be a nonarchimedean local field. Let G be a F-split reductive group. Let T be a maximal F-split torus, and let B be a Borel subgroup containing T. The derived group G' is semisimple, and we may let $x_\alpha : G_{\mathrm{m}} \longrightarrow G'$ be as in Section 16. We will denote by $K^\circ = G'(\mathfrak{o})$ the group generated by the $x_\alpha(\mathfrak{o})$. It is a maximal compact subgroup of $G(F)$. We have the Iwasawa decomposition

$$G(F) = B(F)\, G(\mathfrak{o}).$$

We still have functors of parabolic induction and the Jacquet module. However parabolic induction requires a "shift" by $\delta^{1/2}$, where δ is the modular quasicharacter of $B(F)$. Thus $\delta : B(F) \longrightarrow \mathbb{C}$ is defined so that if $d\mu_L(b)$ is a left Haar-measure then $\delta(b)\, d\mu_L(b)$ is a right Haar-measure. We have

$$\delta(tu) = \prod_{\alpha \in \Phi^+} |t^\alpha|, \qquad t \in T(F),\, u \in U(F).$$

For example, for $G = \mathrm{GL}(3)$,

$$\delta \begin{pmatrix} t_1 & * & * \\ & t_2 & * \\ & & t_3 \end{pmatrix} = |t^{\alpha_1}| \cdot |t^{\alpha_2}| \cdot |t^{\alpha_1+\alpha_2}| = \left|\frac{t_1}{t_2}\right| \left|\frac{t_2}{t_3}\right| \left|\frac{t_1}{t_3}\right| = |t_1^2 t_3^{-2}|.$$

Now let χ be an unramified quasicharacter of $T(F)$. We define $V(\chi)$ to be the space of smooth (locally constant) functions $f : G(F) \longrightarrow \mathbb{C}$ that satisfy

$$f(bg) = (\delta^{1/2}\chi)(b) f(g), \qquad b \in B(F). \tag{77}$$

The group G acts on $V(\chi)$ by right translation:

$$\pi(g) f(x) = f(xg). \tag{78}$$

The condition that f is smooth is equivalent to assuming that $\pi(k)f = f$ for k in some open subgroup of $G(F)$. Thus

$$V(\chi) = \bigcup_K V(\chi)^K$$

as K runs through the open subgroups of $G(F)$. We recall that $V(\chi)^K$ is a $\mathcal{H}_K$-module, where $\mathcal{H}_K$ is the convolution ring of K-biinvariant functions.

In view of (3) and (78), if $\phi \in \mathcal{H}_J$ and $f \in V(\chi)^K$ then

$$(\phi \cdot f)(x) = \pi(\phi)f(x) = \int_G \phi(g)f(xg)\,dg. \tag{79}$$

We will be particularly interested in $V(\chi)^J$ where J is the Iwahori subgroup.

One reason for including the factor $\delta^{1/2}$ in the definition of the induced representation is that if χ is unitary, then $\pi(\chi)$ is a unitary representation. Indeed if $\mathrm{Ind}_{B(F)}^{G(F)}(\delta)$ is the space of functions that satisfy

$$f(bg) = \delta(b)f(g)$$

then by Lemma 2.6.1 of Bump, *Automorphic Forms and Representations* we may define a linear functional I on $\mathrm{Ind}_{B(F)}^{G(F)}(\delta)$ that is invariant under right-translation by

$$I(f) = \int_{K^\circ} f(k)\,dk.$$

Thus if $f_1, f_2 \in V(\chi)$, and if χ is unitary, then $f_1\overline{f_2}$ is in the space $\mathrm{Ind}_{B(F)}^{G(F)}(\delta)$ and so

$$\langle f_1, f_2\rangle = \int_{K^\circ} f_1(k)\overline{f_2(k)}\,dk$$

is an inner product, making the representation $V(\chi)$ unitary. It is possible for $V(\chi)$ to be unitary even if χ is not, owing to the existence of complementary series.

Another reason for the normalization factor is so that the intertwining integrals map $V(\chi) \longrightarrow V({}^w\chi)$. The intertwining integrals may be defined by the analogs of either (75) or (76). That is:

$$M(w)f(g) = \int_{U(F)\cap wU_-(F)w^{-1}} f(w^{-1}ug)\,du \;=\; \int_{(U(F)\cap wU(F)w^{-1})\backslash U(F)} f(w^{-1}ug)\,du. \tag{80}$$

The two formulas are equivalent due to the fact that

$$U(F) = (U(F) \cap wU_-(F)w)(U(F) \cap wU(F)w^{-1})$$

by Proposition 30.

Proposition 63 *The integral (80) is convergent if*

$$\left|\chi\left(i_\alpha\begin{pmatrix} \varpi & \\ & \varpi^{-1}\end{pmatrix}\right)\right| < 1 \tag{81}$$

for all positive roots α such that $w^{-1}\alpha \in \Phi^-$. If $l(ww') = l(w) + l(w')$ then $M(ww') = M(w) \circ M(w')$.

Proof The statement that $l(ww') = l(w) + l(w')$ then $M(ww') = M(w) \circ M(w')$ is formally similar to the finite field case: one simply replaces the summations by integrations. Using this, the convergence statement reduces to the case where $w = s_\alpha$ for a simple root α. In that case, $U(F) \cap wU(F)w^{-1} = i_\alpha(F)$, and the integral is

$$\int_F f\left(s_\alpha i_\alpha\begin{pmatrix} 1 & v \\ & 1\end{pmatrix} g\right)\, dv, \qquad s_\alpha = i_\alpha\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$$

If $v \neq 0$, then

$$\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\begin{pmatrix} 1 & v \\ & 1\end{pmatrix} = \begin{pmatrix} 1 & -v^{-1} \\ & 1\end{pmatrix}\begin{pmatrix} v^{-1} & \\ & v\end{pmatrix}\begin{pmatrix} 1 & \\ v^{-1} & 1\end{pmatrix}.$$

Thus the integral equals

$$\int_F f\left(i_\alpha\begin{pmatrix} 1 & -v^{-1} \\ & 1\end{pmatrix} i_\alpha\begin{pmatrix} v^{-1} & \\ & v\end{pmatrix} i_\alpha\begin{pmatrix} 1 & \\ v^{-1} & 1\end{pmatrix} g\right)\, dv \;=$$
$$\int_F |v|^{-1}\chi\left(i_\alpha\begin{pmatrix} v^{-1} & \\ & v\end{pmatrix}\right) f\left(i_\alpha\begin{pmatrix} 1 & \\ v^{-1} & 1\end{pmatrix} g\right)\, dv.$$

The factor $|v|^{-1}$ is from $\delta^{1/2}$. If v is sufficiently large, the value of f is constant since f is locally constant. Therefore absolute convergence depends on the convergence of

$$\int_{|v|>C} |v|^{-1}\left|\chi\left(i_\alpha\begin{pmatrix} v^{-1} & \\ & v\end{pmatrix}\right)\right| dv,$$

where C is a nonzero constant. The absolute value of χ is constant on the sets $\varpi^{-k}\mathfrak{o}^\times$, which have volume $q^k(1-q^{-1})$. The factor $|v|^{-1} = q^{-k}$ on this set, so we need the convergence of

$$\sum_{|q^k|>C} \left| \chi\left(i_\alpha \begin{pmatrix} \varpi^k & \\ & \varpi^{-k} \end{pmatrix} \right) \right|^k.$$

The convergence of this geometric series follows from (81). □

Lemma 26 *If $t \in T(F)$ and $w \in W$ then the Jacobian of the transformation*

$$u \mapsto tut^{-1}$$

of $U(F) \cap wU_-(F)w^{-1}$ is

$$\frac{\delta^{1/2}(t)}{\delta^{1/2}(w^{-1}tw)}.$$

Proof We have

$$U(F) \cap wU_-(F)w^{-1} = \prod_{\substack{\alpha \in \Phi^+ \\ w^{-1}(\alpha) \in \Phi^-}} x_\alpha(F).$$

We have $tx_\alpha(v)t^{-1} = x_\alpha(t^\alpha v)$, so the Jacobian in question is

$$\prod_{\substack{\alpha \in \Phi^+ \\ w^{-1}(\alpha) \in \Phi^-}} |t^\alpha|. \tag{82}$$

Now

$$\delta^{1/2}(w^{-1}tw) = \prod_{\alpha\in\Phi^+} |(w^{-1}tw)^\alpha| = \prod_{\alpha\in\Phi^+} |t^{w(\alpha)}| = \prod_{\substack{\alpha \in \Phi^+ \\ w^{-1}\alpha \in \Phi^+}} |t^\alpha| \prod_{\substack{\alpha \in \Phi^- \\ w^{-1}\alpha \in \Phi^+}} |t^\alpha|.$$

Thus

$$\delta^{1/2}(w^{-1}tw) = \sqrt{\frac{\prod_{\substack{\alpha \in \Phi^+ \\ w^{-1}\alpha \in \Phi^+}} |t^\alpha|}{\prod_{\substack{\alpha \in \Phi^+ \\ w^{-1}\alpha \in \Phi^-}} |t^\alpha|}},$$

while $\delta^{1/2}(t) = \sqrt{\left[\prod_{\substack{\alpha\in\Phi^+\\ w^{-1}\alpha\in\Phi^+}} |t^\alpha|\right]\cdot\left[\prod_{\substack{\alpha\in\Phi^+\\ w^{-1}\alpha\in\Phi^-}} |t^\alpha|\right]}$ and it follows that $\frac{\delta^{1/2}(t)}{\delta^{1/2}(w^{-1}tw)}$ equals (82). □

Proposition 64 *If $M(w)f$ is convergent, then $M(w)f \in V({}^w\chi)$.*

Proof In order to show that one proceeds as follows. If $t \in T(F)$ we can write

$$M(w)f(tg) = \int_{U(F)\cap wU_-(F)w^{-1}} f(w^{-1}utg)\,du \;=$$
$$\int_{U(F)\cap wU_-(F)w^{-1}} f(w^{-1}tw\cdot w^{-1}(t^{-1}ut)g)\,du \;=$$
$$\delta^{1/2}(w^{-1}tw)\cdot {}^w\chi(t)\int_{U(F)\cap wU_-(F)w^{-1}} f(w^{-1}(t^{-1}ut)g)\,du.$$

We make a variable change $u \mapsto tut^{-1}$ and by the Lemma the Jacobian of this map is $\delta^{1/2}(t)/\delta^{1/2}(w^{-1}tw)$. Therefore we obtain $(\delta^{1/2}\cdot {}^w\chi)(t)M(w)f(g)$, as required. □

Although the intertwining integrals are not convergent for all χ, even when they are not convergent we may make sense of the integrals more generally as follows. Let us organize the quasicharacters of $T(F)$ into a complex analytic manifold $\mathfrak{X}$ as follows. First, the unramified characters, we have seen, are, by Exercise 18, $X^{\rm nr}(T(F)) \cong \mathrm{Hom}(X^*(T), \mathbb{C}^\times)$ which is a product of copies of $\mathbb{C}^\times$. This is thus a connected complex manifold $\mathfrak{X}^{\rm ur}$. If we fix a (not necessarily unramified) character χ_0, then we may consider $\chi\chi_0$ with $\chi \in X^{\rm nr}(T(F))$ to vary though a copy of $\mathfrak{X}^{\rm ur}$. Thus $\mathfrak{X}$ is a union (over cosets of the unramified characters) of copies of $\mathfrak{X}^{\rm ur}$, and is therefore a complex analytic manifold.

Let $\mathfrak{X}_{\rm reg}$ be the set of regular characters in $\mathfrak{X}$. It is an open set, the *regular set*. The complement $\mathfrak{X}_{\rm sing}$ is the *singular set*.

Now we may consider the disjoint union

$$\mathfrak{V} = \bigcup_{\chi\in\mathfrak{X}} V(\chi).$$

By a *section* we mean a function $\mathfrak{X} \longrightarrow \mathfrak{V}$, to be denoted $\chi \mapsto f_\chi$ such that if $\chi \in \mathfrak{X}$ then $f_\chi \in V(\chi)$. We would like to define the notion of an *analytic*

section. First, let us say that the section is *flat* if $f_\chi|K^\circ$ is constant on each connected component of $\mathfrak{X}$. The flat sections are analytic. Moreover since $\mathfrak{X}$ is a complex analytic manifold, we have a notion of analytic and meromorphic functions on $\mathfrak{X}$. We say that a section is *analytic* (resp. *meromorphic*) if it is a linear combination of flat sections with analytic coefficients.

The intertwining operators do not necessarily take flat sections to flat sections, but they do take analytic sections to meromorphic sections. The poles in the complement of the regular set: that is, if f_χ is an analytic section, then $M(w)f_\chi$ is meromorphic, and analytic on $\mathfrak{X}_{\mathrm{reg}}$.

We now come to a major difference between the finite field case and the local field case. Whereas in the finite field case, the reducible places of the principal series were when χ was not regular, regularity in the local field case happens at shifts of the singular set. Nevertheless something interesting does happen where regularity fails.

Let us see this at work when $G = \mathrm{GL}_2$. Let

$$\chi \begin{pmatrix} y_1 & \\ & y_2 \end{pmatrix} = \chi_1(y_1)\chi_2(y_2)$$

and consider the intertwining integral $M(w_0) : V(\chi) \longrightarrow V({}^w\chi)$, where $w_0 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ is the long Weyl group element. If $\chi_1 = \chi_2$, then $M(w_0)$ has a pole. In this case, $V(\chi) = V({}^w\chi)$, and this module is irreducible. There is only one intertwining operator $V(\chi) \longrightarrow V({}^w\chi) = V(\chi)$, and this is $M(1)$. If both $M(w_0)$ and $M(1)$ were analytic, there would be two, and one is "not needed" so it has a pole.

However the Jacquet module at this special value shows some interesting behavior. The Jacquet module $J(V)$ of a smooth $G(F)$-module V is

$$J(V) = V/V_U, \qquad V_U = \langle v - \pi(u)v | v \in V, u \in U(F) \rangle.$$

It is an $T(F)$-module, and if $V = V(\chi)$ where χ is regular, then

$$J(V(\chi)) = \bigoplus_{w \in W} \delta^{1/2} \cdot {}^w\chi.$$

The Jacquet module is an exact functor and is an important tool in the representation theory of p-adic groups. We refer to the references of Casselman and Bump for further information.

In the GL_2 case, if χ is regular, the last formula reduces to

$$J(V(\chi)) = \delta^{1/2}\chi \oplus \delta^{1/2} \cdot {}^{w_0}\chi.$$

When $\chi = {}^{w_0}\chi$, the Jacquet module $V(\chi)$ becomes indecomposable. It has two isomorphic composition factors, both $\delta^{1/2}\chi$, and sits in a short exact sequence:

$$0 \longrightarrow \delta^{1/2}\chi \longrightarrow J(V(\chi)) \longrightarrow \delta^{1/2}\chi \longrightarrow 0.$$

However the irreducible submodule is not a direct summand, and this exact sequence does not split.

The reducibility of the principal series is when $\chi_1\chi_2^{-1}(t) = |t|$ or $\chi_1\chi_2^{-1}(t) = |t|^{-1}$.

In the general case, $V(\chi)$ will be reducible if $\chi(h_{\alpha^\vee}(\varpi)) = q^{\pm 1}$ for some coroot $\alpha^\vee$, and will be maximally reducible if χ is in the W-orbit of $\delta^{1/2}$.

21 The Formula of Gindikin and Karpelevich

The original formula of Gindikin and Karpelevich was for the archimedean case. The nonarchimedean case (which is our concern here) is actually due to Langlands. A convenient reference is the paper of Casselman cited below.

- S. Gindikin and F. Karpelevich, Plancherel measure for symmetric Riemannian spaces of non-positive curvature. (Russian) Dokl. Akad. Nauk SSSR 145 1962 252–255.
- R. Langlands, Euler products. A James K. Whittemore Lecture in Mathematics given at Yale University, 1967. Yale University (1971).
- Casselman, The unramified principal series of p-adic groups. I. The spherical function. Compositio Math. 40 (1980), no. 3, 387–406.

With notations as in the previous section, we assume that χ is an unramified regular character of $T(F)$. Let $\boldsymbol{z} \in \hat{T}(\mathbb{C})$ such that $\chi = \chi_{\boldsymbol{z}}$.

Let $\phi^\circ = {}^{\chi}\phi^\circ$ be the standard spherical vector in $V(\chi)$. Thus

$$\phi^\circ(bk) = (\delta^{1/2}\chi)(bk), \qquad b \in B(F),\ k \in G(\mathfrak{o}).$$

Theorem 28 *We have*

$$M(w)^{\chi}\phi^\circ = c_w(\chi)\,{}^{w\chi}\phi^\circ$$

where

$$c_w(\chi) = \prod_{\substack{\alpha \in \Phi^+ \\ w(\alpha) \in \Phi^-}} \frac{1 - q^{-1}\boldsymbol{z}^\alpha}{1 - \boldsymbol{z}^\alpha}.$$

Proof [Sketch] We know that $M(w)\phi^\circ$ is a spherical vector in $V({}^w\chi)$. It is thus a constant multiple of ${}^{w\chi}\phi^\circ$. To determine the constant it is sufficient to evaluate at the identity. Therefore it is sufficient to prove

$$M(w)^\chi\phi^\circ(1) = c_w(\chi).$$

Using the fact that $M(w)M(w') = M(ww')$ when $l(ww') = l(w) + l(w')$, we reduce to the case where $w = s_\alpha$ is a simple reflection. Thus we must show

$$\int_F \phi^\circ \left(i_\alpha \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} i_\alpha \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \right) dx = \frac{1 - q^{-1}\boldsymbol{z}^\alpha}{1 - \boldsymbol{z}^\alpha}$$

when α is a simple reflection. This computation takes place entirely in the subgroup $i_\alpha \operatorname{SL}_2(F)$, and so we reduce to the rank one case.

If $x \in \mathfrak{o}$ then $i_\alpha \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} i_\alpha \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \in G(\mathfrak{o})$ and the integrand equals 1. Thus we have a contribution of 1.

If $x \notin \mathfrak{o}$ let $x \in \varpi^{-k}\mathfrak{o}^\times$. Then

$$\begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ -x^{-1} & 1 \end{pmatrix} = \begin{pmatrix} x^{-1} & -1 \\ & x \end{pmatrix}.$$

Since $i_\alpha \begin{pmatrix} 1 & \\ -x^{-1} & 1 \end{pmatrix} \in G(\mathfrak{o})$ we have

$$\phi^\circ \left(i_\alpha \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} i_\alpha \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \right) = \phi^\circ \begin{pmatrix} x^{-1} & -1 \\ & x \end{pmatrix} = |x|^{-1}\boldsymbol{z}^{-k\alpha} = q^{-k}\boldsymbol{z}^{-k\alpha}$$

Thus we obtain a contribution of

$$\sum_{k=1}^{\infty} q^{-k}\boldsymbol{z}^{-k\alpha} \operatorname{vol}(\varpi^{-k}\mathfrak{o}^\times) = (1 - q^{-1}) \sum_{k=1}^{\infty} \boldsymbol{z}^{k\alpha} = (1 - q^{-1}) \frac{\boldsymbol{z}^\alpha}{1 - \boldsymbol{z}^\alpha}.$$

Hence the integral is

$$1 + (1 - q^{-1}) \frac{\boldsymbol{z}^\alpha}{1 - \boldsymbol{z}^\alpha} = \frac{1 - q^{-1}\boldsymbol{z}^\alpha}{1 - \boldsymbol{z}^\alpha}.$$

□

22 Casselman's proof of the Macdonald formula

Two fundamental papers are

- Casselman, The unramified principal series of p-adic groups. I. The spherical function. Compositio Math. 40 (1980), no. 3, 387–406.
- Casselman and Shalika, The unramified principal series of p-adic groups. II. The Whittaker function. Compositio Math. 41 (1980), no. 2, 207–231.

These make use of the intertwining operators and Iwahori fixed vectors to prove two fundamental formulas in the representation theory of p-adic groups: the Macdonald formula for the spherical function, and the Shintani-Casselman-Shalika formula for the spherical Whittaker function.

We will sketch the proof of the Macdonald formula. Some statements such as the linear independence of the linear functionals built from the intertwining integrals will not be verified. For these, see Casselman's original paper.

We let G be as in the last section. In this section we will denote by K° the maximal compact subgroup $G(\mathfrak{o})$.

Suppose that (π, V) is an irreducible admissible representation that has a K°-fixed vector. Using the Bruhat-Cartan decomposition (Theorem 19) and an involution based on the Chevalley basis, the argument in Theorem 12 may be generalized to show that the spherical Hecke $\mathcal{H}_{K^\circ}$ is commutative. Alternatively, this may be deduced from the structure of the Iwahori-Hecke algebra $\mathcal{H}_J$. The commutativity of $\mathcal{H}_{K^\circ}$ implies that that $V^\circ = V^{K^\circ}$ is at most one-dimensional. If this is true, then we say that V is *spherical*.

Proposition 65 *If (π, V) is spherical so is $(\hat{\pi}, \hat{V})$.*

Proof If V^{K° is one-dimensional, then so is $\hat{V}^\circ = \hat{V}^{K^\circ}$, since we may construct a K°-invariant linear functional on V by taking a linear functional that is nonzero on V^{K° but which vanishes on every other K°-isotypic part. (See Proposition 9.) □

If (π, V) is any irreducible admissible representation, and if $v \in V$, $\hat{v} \in \hat{V}$ then the function $\sigma(g) = \langle \pi(g)v, \hat{v} \rangle$ is called a *matrix coefficient*. If v° and $\hat{v}^\circ$ are spherical vectors (that is, elements of V° and $\hat{V}^\circ$) then

$$\Gamma_\pi(g) = \langle \pi(g)v^\circ, \hat{v}^\circ \rangle$$

is called the *spherical function*. It is determined up to constant multiple, and we want to normalize it so that $\Gamma_\pi(1) = 1$.

It may be shown that every spherical representation is a subquotient of $V(\chi)$ for some unramfied quasicharacter χ of $T(F)$. If $V(\chi)$ is irreducible, then it is spherical, for it contains the vector

$$\phi^\circ(bk) = (\delta^{1/2}\chi)(b), \qquad b \in B(F), k \in K^\circ.$$

Proposition 66 *Suppose that $\pi = V(\chi)$ where χ is unramified, and that $V(\chi)$ is irreducible. Then*

$$\Gamma_\pi(g) = \frac{1}{\mathrm{vol}(K^\circ)} \int_{K^\circ} \phi^\circ(kg)\, dk. \tag{83}$$

With this normalization, $\Gamma_\pi(1) = 1$.

Proof Define a linear functional on $V(\chi)$ by

$$L(\phi) = \frac{1}{\mathrm{vol}(K^\circ)} \int_{K^\circ} \phi(k)\, dk.$$

This functional is clearly K°-invariant, and $L(\pi(g)\phi^\circ)$ is the described function. □

For the rest of this section, we will assume that χ is unramified and regular, and that $V(\chi)$ is irreducible.

We call $t \in T(F)$ *dominant* if for every positive root α we have $t^\alpha \in \mathfrak{p}$. It is sufficient to check this when α is a simple root. For example, suppose that $G = \mathrm{GL}_n$ and that

$$t = \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix}.$$

Then the condition is that $t_i/t_{i+1} \in \mathfrak{o}$.

The dimension of $V(\chi)^J$ is $|W|$. We may exhibit a basis as follows.

Lemma 27 *Choose a set of representatives for w for $W = N(T(F))/T(F)$ that are in K°. Then*

$$G(F) = \bigcup_w B(F) w J \qquad \text{(disjoint)}.$$

Proof We have $K^\circ = \bigcup JwJ$ (disjoint). Using the Iwahori factorization $U = B(\mathfrak{o})U_-(\mathfrak{p})$. The statement follows since $B(\mathfrak{o}) \subseteq B(F)$ while $U_-(\mathfrak{p})w \subseteq wJ$. □

Proposition 67 *The dimension of $V(\chi)^J$ is $|W|$. A basis consists of the functions*

$$\phi_w(bk) = \begin{cases} \delta^{1/2}\chi(w) & \text{if } k \in Jw^{-1}J \\ 0 & \text{otherwise,} \end{cases}$$

when $b \in B(F)$, $k \in K^\circ$.

Proof This is clear from the previous Lemma. □

If $w \in W$, define a linear functional on $V(\chi)^J$ by $\Lambda_w(\phi) = M(w)\phi(1)$.

Proposition 68 (Casselman) *The linear functionals Λ_w are linearly independent.*

Proof We will not prove this, but refer to the first of Casselman's papers cited above (discussion before Proposition 3.7). □

By the last two propositions we may find a basis f_w of $V(\chi)$ indexed by $w \in W$ such that $\Lambda_w f_{w'} = \delta_{w,w'}$ (Kronecker δ). This is the *Casselman basis*. The Casselman basis is generally difficult to compute; that is, if we write f_w as a linear combination of the ϕ_w, the transition matrix will be upper triangular in the Bruhat order, and but some of the coefficients will be very complicated. However Casselman observed that one element of the basis is computable, and remarkably, this gives enough information for applications.

We will denote by w_0 the long element of W.

Lemma 28 (Casselman) *We have $f_{w_0} = \phi_{w_0}$.*

Proof Using the Iwahori factorization, the support $B(F)w_0J$ of ϕ_{w_0} is contained in the big Bruhat cell $B(F)w_0B(F)$. If $v \in W$ then

$$\Lambda_v\phi_{w_0} = \int_{U(F)\cap vU_-(F)v^{-1}} \phi_{w_0}(v^{-1}u)\,du.$$

If $v \neq w_0$ then $v^{-1}u \in B(F)v^{-1}B(F)$ is never in the big cell $B(F)w_0B(F)$. Therefore $\Lambda_v\phi_{w_0} = 0$. On the other hand if $u = w_0$, then $v^{-1}u = w_0u \in B(F)w_0J$ if and only if $u \in U(\mathfrak{o})$. We are normalizing the Haar measure on $U(F)$ so that the volume of $U(\mathfrak{o})$ is 1, and therefore $\Lambda_{w_0}\phi_{w_0} = 1$. We see that $\Lambda_v\phi_{w_0} = \delta_{v,w_0}$ and so $\phi_{w_0} = f_{w_0}$. □

Proposition 69 *Let t be dominant, and define*

$$F_t(g) = \int_{U(\mathfrak{o})} \phi^\circ(gut)\, du.$$

Then $F_t \in V(\chi)^J$.

Proof Since the function $g \longmapsto \phi^\circ(gut)$ is in $V(\chi)$ for every u, t it is sufficient to show that this function is fixed by J. We show that

$$F_t(g) = \int_J \phi^\circ(gkt)\, dk. \tag{84}$$

Indeed, we may use the Iwahori factorization and write

$$\int_J \phi^\circ(gkt)\, dk = \int_{U(\mathfrak{o})} \int_{T(\mathfrak{o})} \int_{U_-(\mathfrak{p})} \phi^\circ(guu_-at)\, du_-\, da\, du.$$

Since t is dominant, if $a \in T(\mathfrak{o})$ and $u_- \in U_-(\mathfrak{p})$ we have $t^{-1}au_-t \in T(\mathfrak{o})U_-(\mathfrak{p}) \subseteq K^\circ$ and so we may discard the integrals over $u_-(\mathfrak{p})$ and $T(\mathfrak{o})$. This proves (84), and the statement follows. □

Proposition 70 *We have*

$$F_t = \sum_{w \in W} c_w(t)\, (\delta^{1/2} \cdot {}^w\chi)(t) f_w. \tag{85}$$

Proof Since F_t is an Iwahori-fixed vector, there exist constants $R(w,t)$ such that

$$F_t = \sum_w R(w,t)\, f_w.$$

By definition of the f_w we may compute $R(w,t)$ by applying $M(w)$ and evaluating at 1. Thus

$$R(w,t) = M(w)F_t(1) = \int_{U(F)\cap w^{-1}U_-(F)w} \int_{U(\mathfrak{o})} \phi^\circ(w^{-1}uu_1t)\, du_1\, du.$$

Interchanging the order of integration and making a variable change, we may eliminate the u_1 integration and we find that

$$R(w,t) = \int_{U(F)\cap w^{-1}U_-(F)w} \phi^\circ(w^{-1}ut)\, du = M(w)\phi^\circ(t) = c_w(t)\, (\delta^{1/2} \cdot {}^w\chi)(t)$$

by the formula of Gindikin and Karpelevich. □

Theorem 29 (Macdonald) *Let $Q = \sum_{w\in W} q^{-l(w)}$, and let $\pi = V(\chi)$. If $t \in T(F)$ is dominant, we have*

$$\Gamma_\pi(t) = \frac{1}{Q}\sum_{w\in W} w\left(\prod_{\alpha\in\Phi^+}\frac{1-q^{-1}\boldsymbol{z}^\alpha}{1-\boldsymbol{z}^\alpha}(\delta^{1/2}\cdot {}^{w_0}\chi)(t)\right). \tag{86}$$

Proof We have

$$\int_{K^\circ} F_t(k)\,dk = \int_{K^\circ}\int_{U(\mathfrak{o})} \phi^\circ(kut)\,du\,dk.$$

Interchanging he order of integration and making a variable change eliminates the u integration, so by (83) we have

$$\Gamma_\pi(t) = \int_{K^\circ} F_t(k)\,dk = \sum_{w\in W} a_w(\chi)\,(\delta^{1/2}\cdot {}^w\chi)(t) \tag{87}$$

where the constants

$$a_w(\chi) = \frac{c_w(\chi)}{\mathrm{vol}(K^\circ)}\int_{K^\circ} f_w(k)\,dk.$$

In general these are not directly computable due to the complexity of f_w, but if $w = w_0$ then $f_{w_0} = \phi_{w_0}$ by Lemma 28

$$a_{w_0}(\chi) = \frac{c_{w_0}(\chi)}{\mathrm{vol}(K^\circ)}\int_{K^\circ}\phi_{w_0}(k)\,dk = \left(\prod_{\alpha\in\Phi^+}\frac{1-q^{-1}\boldsymbol{z}^\alpha}{1-\boldsymbol{z}^\alpha}\right)\frac{\mathrm{vol}(Jw_0J)}{\mathrm{vol}(K^\circ)}.$$

We recall that the volume of JwJ is $q^{l(w)}$. Since K° is the disjoint union of the JwJ, we have

$$\mathrm{vol}(Jw_0J) = q^{l(w_0)}, \qquad \mathrm{vol}(K^\circ) = \sum_{w\in W} q^{l(w)}, \qquad \frac{\mathrm{vol}(K^\circ)}{\mathrm{vol}(Jw_0J)} = \sum_{w\in W} q^{l(w)-l(w_0)}.$$

If $w' = w_0w^{-1}$ then $l(w) - l(w_0) = -l(w')$, so $\frac{\mathrm{vol}(K^\circ)}{\mathrm{vol}(Jw_0J)} = Q$. We have proved that

$$a_w(\chi) = \frac{1}{Q}\prod_{\alpha\in\Phi^+}\frac{1-q^{-1}\boldsymbol{z}^\alpha}{1-\boldsymbol{z}^\alpha}.$$

In order to conclude the proof, we note that as a rational function in $\boldsymbol{z}$, $\Gamma_w(t)$ must be invariant under the action of W. This is because if $\boldsymbol{z}$ is in

general position, then $\pi = V(\chi)$ is irreducible and isomorphic to $\pi' = V({}^w\chi)$. Therefore π and π' have the same spherical function.

This means that $a_w(\chi)(\delta^{1/2} \cdot {}^w\chi)(t)$ is invariant under the action of W, and since we know one of these factors, we know them all. Now (86) follows. □

23 Intertwining Operators and $\mathcal{H}_q(\tilde{W}_{\text{aff}})$

We consider now the case where G is semisimple and F-split. Let χ denote an unramified quasicharacter of $T(F)$, and let other notations be as in the last section. We will always assume that χ is regular, so that $M(w)$ is defined on $V(\chi)$.

If $w \in W$, we will also denote by w an element of $N(T(F)) \cap G(\mathfrak{o})$ representing the coset of w in $W = N(T(F))/T(F)$, and by abuse of notation, we will also denote that representative as w.

Because we will be working with $V(\chi)$ where the character χ of $T(F)$ is unramified, none of our formulas will depend on the choice of representative. This is because the representative is determined by an element of $T(\mathfrak{o})$, where χ is trivial. We will denote by $B(\mathfrak{o})$, $U(\mathfrak{o})$, $T(\mathfrak{o})$, etc. the intersections of $B(F)$, $U(\mathfrak{o})$, $T(\mathfrak{o})$ with $G(\mathfrak{o})$.

Proposition 71 *The dimension $V(\chi)^J$ is equal to $|W|$. It has a basis consisting of the vectors ϕ_w defined by*

$$\phi_w(bk) = \begin{cases} (\delta^{1/2}\chi)(b) & \text{if } k \in B(F)w^{-1}J, \\ 0 & \text{otherwise} \end{cases} \tag{88}$$

for $w \in W$, when $k \in G(\mathfrak{o})$ and $b \in B(F)$.

Proof An element of $V(\chi)^J$ is an element of $V(\chi)$ that is right invariant by J. By (77) an element of $V(\chi)^J$ is determined by its restriction to a set of representatives for $B(F)\backslash G(F)/J$. Using the Iwasawa decomposition, the representatives may be chosen $G(\mathfrak{o})$, so we want representatives for $B(\mathfrak{o})\backslash G(\mathfrak{o})/J$. We recall that a set of representatives for $J\backslash G(\mathfrak{o})/J$ may be chosen from W, that is, from $T(\mathfrak{o})\backslash(N(T(F)) \cap G(\mathfrak{o}))$; this fact follows by pulling the Bruhat decomposition for $G(\mathbb{F}_q)$ back to $G(\mathfrak{o})$ under the canonical map $G(\mathfrak{o}) \longrightarrow G(\mathbb{F}_q)$.

Let w^{-1} be such a representative. Using the Iwahori factorization, $J = B(\mathfrak{o})U_-(\mathfrak{p})$, and by Lemma 9 we have $wU_-(\mathfrak{p})w^{-1} \in J$, so

$$Jw^{-1}J = B(\mathfrak{o})w^{-1}J.$$

There is therefore a unique element of $V(\chi)^J$ supported on $B(F)w^{-1}J$. $\square$

It was shown in

- J. D. Rogawski. On modules over the Hecke algebra of a p-adic group. *Invent. Math.*, 79(3):443–465, 1985.

that one may use the Iwahori Hecke algebra to work with the intertwining integrals. From Rogawski's remarks, I believe this idea is due to Bernstein. As we will see, the Bernstein presentation is particularly useful for this. The same idea is used elsewhere in the literature, for example:

- Mark Reeder. On certain Iwahori invariants in the unramified principal series. *Pacific J. Math.*, 153(2):313–342, 1992.
- Thomas J. Haines, Robert E. Kottwitz, and Amritanshu Prasad. Iwahori-Hecke algebras. *http://arxiv.org/abs/math/0309168*, 2003.
- Bump and Nakasuji, Casselman's Basis of Iwahori Vectors and the Bruhat Order, `http://arxiv.org/abs/1002.2996`, 2010.

If G is simply-connected, we have seen that $N(T(F))/T(\mathfrak{o}) \cong W_{\text{aff}}$. In general, $N(T(F))/T(\mathfrak{o})$ may be slightly larger. If G is of adjoint type, it is $\tilde{W}_{\text{aff}}$. In general, there is a lattice L such that $Q^\vee \subseteq L \subseteq P^\vee$ and $N(T(F))/T(\mathfrak{o})$ is the semidirect product of L by W. Then $L/Q^\vee$ is the fundamental group $\pi_1(G)$. We will write W_{aff}^L for $N(T(F))/T(\mathfrak{o})$. We will denote by Θ^L the image of L in $\tilde{W}_{\text{aff}}$

The algebra $\mathcal{H}_J$ is the convolution ring of compactly supported J-biinvariant functions. Then $V(\chi)^J$ is a module for $\mathcal{H}_J$. We will denote by $\mathcal{H}(W)$ the subring of functions with support in $G(\mathfrak{o})$. These are supported on the double cosets JwJ with $w \in W$, so this may be identified with the finite-field Hecke algebra with generators $\{s_1, \cdots, s_r\}$.

Proposition 72 *Let $\alpha : V(\chi)^J \longrightarrow \mathcal{H}(W)$ be the map that sends $f \in V(\chi)^J$ to the function $\alpha(f) \in \mathcal{H}(W)$ where*

$$\alpha(f)(g) = \begin{cases} F(g^{-1}) & \text{if } g \in G(\mathfrak{o}), \\ 0 & \text{otherwise.} \end{cases}$$

Then α is an isomorphism of left $\mathcal{H}(W)$-modules.

Proof By Proposition 71 the map α is a vector space isomorphism. The action of $\mathcal{H}(W)$ on itself is by left multiplication (convolution). The action on $V(\chi)^J$ is by (79). We have, for $f \in V(\chi)^J$ and $\phi \in \mathcal{H}(W)$

$$\alpha(\phi \cdot f)(g) = (\phi \cdot f)(g^{-1}) = \int_G \phi(h) f(g^{-1}h)\, dh = \int_G \phi(gh) f(h)\, dh$$

if $g \in G(\mathfrak{o})$. Since $g \in G(\mathfrak{o})$ and ϕ is supported on $G(\mathfrak{o})$ we may restrict the domain of integration to $G(\mathfrak{o})$ and make the variable change $h \mapsto h^{-1}$. The integral is

$$\int_K \phi(gh^{-1}) f(h^{-1})\, dg = \int_K \phi(gh^{-1}) \alpha(f)(h)\, dh = \int_G \phi(gh^{-1}) \alpha(f)(h)\, dh$$

using the fact that $\alpha(f)$ is supported on $G(\mathfrak{o})$. This is $\phi \cdot \alpha(f)(g)$ where now the $\cdot$ is left convolution. Thus $\alpha(\phi \cdot f)$ and $\phi \cdot \alpha(f)$ agree on $G(\mathfrak{o})$. It is easy to check that both vanish off $G(\mathfrak{o})$. □

Now let $w \in W$ and define a map $\mathcal{M}_w = \mathcal{M}_{w,\boldsymbol{z}} : \mathcal{H}(W) \longrightarrow \mathcal{H}(W)$ by requiring the diagram:

$$\begin{array}{ccc} V(\chi)^J & \stackrel{M(w)}{\longrightarrow} & V({}^w\chi)^J \\ \downarrow \alpha(\chi) & & \downarrow \alpha({}^w\chi) \\ \mathcal{H}(W) & \stackrel{\mathcal{M}_w}{\longrightarrow} & \mathcal{H}(W) \end{array}$$

to be commutative.

If $w \in W$ let us define $\mu(\chi, w) = \mathcal{M}_w(1_{\mathcal{H}_J}) \in \mathcal{H}(W)$, where $1_{\mathcal{H}_J}$ is the unit element in $\mathcal{H}_J$, that is, the characteristic function of J. We note that under the map α, $1_{\mathcal{H}_J}$ corresponds to the

Proposition 73 *We have*

$$\mathcal{M}_w(h) = h \cdot \mu(\chi, w)$$

for all $h \in \mathcal{H}(W)$.

Proof $\mathcal{M}_w$ is a homomorphism of left $\mathcal{H}(W)$-modules. Therefore

$$\mathcal{M}_w(h) = \mathcal{M}_w(h \cdot 1) = h\mathcal{M}_w(1) = h \cdot \mu(\chi, w).$$

□

Lemma 29 *If* $l(w_1w_2) = l(w_1) + l(w_2)$ *then*

$$\mu(\chi, w_1w_2) = \mu(\chi, w_2)\mu({}^{w_2}\chi, w_1).$$

Proof By Proposition 63 we have $M(w_1w_2) = M(w_1) \circ M(w_2)$. Therefore this follows from the commutativity of the diagram:

$$\begin{array}{ccccc} V(\chi)^J & \stackrel{M(w_2)}{\longrightarrow} & V({}^{w_2}\chi)^J & \stackrel{M(w_1)}{\longrightarrow} & V({}^{w_1w_2}\chi)^J \\ \downarrow\alpha(\chi) & & \downarrow\alpha({}^{w_2}\chi) & & \downarrow\alpha({}^{w_1w_2}\chi) \\ \mathcal{H}(W) & \stackrel{\mathcal{M}_{w_2}}{\longrightarrow} & \mathcal{H}(W) & \stackrel{\mathcal{M}_{w_1}}{\longrightarrow} & \mathcal{H}(W) \end{array}$$

□

Lemma 30 *Let* $w \in W$ *and* $\alpha = \alpha_k$ *where* $1 \leqslant k \leqslant r$. *Then for* $u \in F$ *let us write*

$$s_k x_\alpha(u) w = \beta w' k$$

with $\beta \in B(F)$, $w' \in W$ *and* $k \in J$. *Then if* $u \in \mathfrak{o}^\times$ *and* $w^{-1}(\alpha) \in \Phi^+$ *or if* $u \in \mathfrak{p}$ *we have*

$$w' = s_k w, \qquad \delta^{1/2}\chi(\beta) = 1,$$

while if $u \in \mathfrak{o}^\times$ *and* $w^{-1}(\alpha) \in \Phi^-$ *or if* $u \notin \mathfrak{o}$ *we have*

$$w' = w, \qquad \delta^{1/2}\chi(\beta) = |u|^{-1}\boldsymbol{z}^{\mathrm{ord}(u^{-1})\alpha}.$$

Here $\chi = \chi_{\boldsymbol{z}}$ is an unramified quasicharacter of $T(F)$, with $\boldsymbol{z} \in \hat{T}(\mathbb{C})$. There is an abuse of notation in writing $w' \in W$. When we write $\beta w' k$ we are chosing a representative in $N(T(F)) \cap G(\mathfrak{o})$ of the Weyl group element w'. This choice is unimportant because the character χ is unramified, so the value of $\delta^{1/2}\chi(\beta)$ is independent of this choice of representative.

Proof First suppose that $u \in \mathfrak{p}$ or $u \in \mathfrak{o}^\times$ and $w^{-1}(\alpha) \in \Phi^+$. Then

$$w^{-1}x_\alpha(-u)w \in J$$

and $s_k x_\alpha(u)w$ is in the same double coset as $s_k x_\alpha(u)w \cdot w^{-1}x_\alpha(-u)w = s_k w$. We may take $\beta = 1$ in this case.

On the other hand suppose that $u \notin \mathfrak{o}$ or $u \in \mathfrak{o}^\times$ and $w^{-1}(\alpha) \in \Phi^-$. Then

$$w^{-1}x_{-\alpha}(-u^{-1})w \in J.$$

and $s_k x_\alpha(u)w$ is in the same double coset as

$$s_k x_\alpha(u)w \cdot w^{-1} x_{-\alpha}(-u^{-1})w.$$

We have the matrix identity

$$\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\begin{pmatrix} 1 & u \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ -u^{-1} & 1 \end{pmatrix} = \begin{pmatrix} u^{-1} & -1 \\ & u \end{pmatrix}.$$

Applying i_α we see that $s_k x_\alpha(u) x_{-\alpha}(-u^-) \in B$, so the double coset is $B(F)wJ$ in this case. In this case we may take $\beta = i_\alpha \begin{pmatrix} u^{-1} & 1 \\ & u \end{pmatrix}$. □

Proposition 74 (Casselman) *If $w = s_k$ is a simple reflection, then $\mu(\chi, w) = \frac{1}{q}T_k + (1 - \frac{1}{q})\frac{\boldsymbol{z}^{\alpha_i}}{1-\boldsymbol{z}^{\alpha_i}}$, where $\boldsymbol{z} \in \hat{T}(\mathbb{C})$ corresponds to χ as in Section 19.*

Proof Since $1_{\mathcal{H}_W}$ and $T_k \in \mathcal{H}(W)$ correspond to ϕ_1 and ϕ_{s_k} defined by (88) under the map α, this is equivalent to the formula

$$M(s_k)\phi_1 = \frac{1}{q}\phi_{s_k} + \left(1 - \frac{1}{q}\right)\frac{\boldsymbol{z}^{\alpha_k}}{1 - \boldsymbol{z}^{\alpha_k}}\phi_1,$$

which we will prove. It is sufficient to compare the values of both sides at $w \in W$, so what we need to prove is that

$$(M(s_k)\phi_1)(w) = \begin{cases} \left(1 - \frac{1}{q}\right)\frac{\boldsymbol{z}^{\alpha_k}}{1-\boldsymbol{z}^{\alpha_k}} & \text{if } w = 1 \\ \frac{1}{q} & \text{if } w = s_k \\ 0 & \text{otherwise.} \end{cases}$$

We may assume that (81) is satisfied so that the integral is convergent; otherwise, the result is still true by analytic continuation. Therefore $|\boldsymbol{z}_{\alpha_k}| < 1$. Note that

$$M(s_k)\phi_1(w) = \int_F \phi_1(s_k x_{\alpha_k}(u)w)\, du. \tag{89}$$

The integrand is evaluated in Lemma 30. If $w \notin \{1, s_k\}$ then $s_k x_{\alpha_k}(u)w$ is never in $B(F)J$, so $M(s_k)\phi_1(w) = 0$. If $w = 1$, then by the Lemma (since $w^{-1}(\alpha) \in \Phi^-$ cannot occur)

$$\phi_1(s_k x_{\alpha_k}(u)) = \begin{cases} |u|^{-1}\boldsymbol{z}^{\mathrm{ord}(u^{-1})} & \text{if } u \notin \mathfrak{o}^\times, \\ 0 & \text{otherwise.} \end{cases}$$

The contribution from the region where $\mathrm{ord}(u) = -n$ with $n > 0$ is $q^n(1-q^{-1})$ (the volume of the domain) times q^{-n} times $\boldsymbol{z}^{n\alpha}$. Thus we obtain

$$(M(s_k)\phi_1)(1) = (1-q^{-1})\sum_{n=1}^{\infty} \boldsymbol{z}^{n\alpha} = (1-q^{-1})\frac{\boldsymbol{z}^{\alpha}}{1-\boldsymbol{z}^{\alpha}}.$$

If $w = s_k$ then by the Lemma (since $w^{-1}(\alpha) \in \Phi^+$ cannot occur)

$$\phi_1(s_k x_{\alpha_k}(u)) = \begin{cases} 1 & \text{if } u \in \mathfrak{p} \\ 0 & \text{otherwise,} \end{cases}$$

and in this case the contribution is

$$(M(s_k)\phi_1)(s_k) = \mathrm{vol}(\mathfrak{p}) = q^{-1}.$$

□

24 Whittaker functions and Whittaker models

Let F be a field that may be finite or nonarchimedean. The case where $F = \mathbb{R}$ or $\mathbb{C}$ is similar, but some statements must be more carefully formulated.

Let G be a split reductive group over F, and let $U(F)$, $T(F)$, etc. be as in previous sections.

If $\alpha, \beta \in \Phi^+$ then the commutator of two one-parameter unipotent subgroups is computed as follows:

$$[x_\alpha(F), x_\beta(F)] = \begin{cases} x_{\alpha+\beta}(F) & \text{if } \alpha+\beta \in \Phi, \\ 1 & \text{if } \alpha+\beta \text{ is not a root.} \end{cases}$$

Therefore the commutator subgroup $U(F)'$ of $U(F)$ is the subgroup generated by the one parameter subgroups $x_\alpha(F)$ for the roots $\alpha \in \Phi^+$ that are not simple, and the abelianization $U(F)^{\mathrm{ab}} = U(F)/U(F)'$ is isomorphic to the abelian group

$$\prod_{\alpha\in\Sigma} F, \qquad (u_\alpha | \alpha \in \Sigma) \longmapsto \left[\prod_{\alpha\in\Sigma} x_\alpha(u_\alpha)\right] U(F)'.$$

Here Σ is the set of simple roots.

The characters of $U(F)$ factor through this abelianization. Therefore each character ψ is determined by its restriction to the groups $x_\alpha(F)$ with α simple, and these restrictions can be arbitrary characters. The character ψ is called *nondegenerate* if these restrictions are nontrivial.

Theorem 30 (Gelfand-Graev) *Let F be a finite field, and let ψ be a nondegenerate character of $U(F)$. Then $\mathrm{Ind}_U^G(\psi)$ is multiplicity-free.*

We will prove this for $G = \mathrm{GL}(n)$ only. In general, it depends on an involution that was constructed by Steinberg.

Proof [GL(n) only] The group $T(F)$ acts transitively on the nondegenerate characters of $U(F)$ by conjugation so the representations $\mathrm{Ind}_U^G(\psi)$ are the same for every nondegenerate character. Therefore we may assume

$$\psi\begin{pmatrix} 1 & u_{12} & \cdots & u_{n-1,n} \\ & 1 & & \vdots \\ & & \ddots & u_{n-1,n} \\ & & & 1 \end{pmatrix} = \psi_0(x_{12} + x_{23} + \ldots + x_{n-1,n})$$

where ψ_0 is any fixed nontrivial character of F. To show that $\mathcal{W} = \mathrm{Ind}_U^G(\psi)$ is multiplicity-free, we note that Proposition 5 it is sufficient to show that $\mathcal{H}_\psi$ is abelian, where $\mathcal{H}_\psi$ is the convolution ring of functions f on $G(F)$ that satisfy $f(ugu') = \psi(u)f(g)\psi(u')$.

Let $\theta : G(F) \longrightarrow G(F)$ be the involution

$$\theta(g) = J \cdot {}^t g \cdot J, \qquad J = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}.$$

The map θ sends $U(F)$ to itself and stabilizes the character ψ. But it is an anti-automorphism: $\theta(gg') = \theta(g')\theta(g)$. Therefore $\Theta(f) = f \circ \theta$ defines an anti-automorphism Θ of $\mathcal{H}_\psi$, namely $\Theta(f * f') = \Theta(f') * \Theta(f)$. If we can show that this map is the identity, then it will follow that $\mathcal{H}_\psi$ is commutative.

Lemma 31 *Let $m \in N(T(F))$. Then either $\theta(m) = m$ or there exists an element $v \in U(F)$ such that $\psi(v) \neq \psi(mvm^{-1})$.*

Proof Let w be the Weyl group element corresponding to m. We may consider the action of w on roots. First we show that if $\alpha \in \Sigma$ and if

$w(\alpha) \in \Phi^+$ then $w(\alpha) \in \Sigma$. If not, then let $v \in X_\alpha$ such that $\psi(v) \neq 1$. Then $mvm^{-1} \in x_{w(\alpha)}(F) \subseteq U(F)$ but $\psi(mvm^{-1}) = 1$ since $w(\alpha)$ is not a simple root.

Let Φ be the set

Now consider $m^{-1}\theta(m)$. □

Now suppose that $f \in \mathcal{H}_\psi$. We will show that $\Theta(f) = f$; as we have already noted, this will prove the theorem. Suppose that $f(g) \neq 0$. Then we will show $f(g) = f(\theta(g))$. By the Bruhat decomposition we may write $g = umu'$ for $u, u' \in U(F)$ and $m \in N(T(F))$. It is sufficient to show that $\theta(m) = m$ because then

$$f(g) = \psi(u)f(m)\psi(u') = \psi(u')f(\theta(m))\psi(u) = f(u'\theta(m)u) = f(\theta(g)).$$

If $\theta(m) \neq m$ then by the Lemma there exists $v \in U(f)$ such that $\psi(v) \neq \psi(mvm^{-1})$. Now

$$f(m) = f(mvm^{-1} \cdot m \cdot v^{-1}) = \psi(mvm^{-1})f(m)\psi(v)^{-1}.$$

This is a contradiction since $f(m) = \psi(u)^{-1}f(g)\psi(u')^{-1} \neq 0$. □

Let (π, V) be an irreducible admissible representation

25 The Casselman-Shalika formula

The lattice $P^\vee$ is the coweight lattice of G but it is also the weight lattice of $\hat{G}$. Let $\lambda^\vee \in P^\vee$ be dominant. Then $\lambda^\vee$ is