Essays on the Fundamental Lemma

Langlands' Fundamental Lemma for SL_2

Bill Casselman
University of British Columbia
cass@math.ubc.ca

In this note I hope to give an elementary and self-contained introduction to what Langlands calls **endoscopy**, by explaining what happens in the simplest case, in which one considers the embedding of an unramified torus in the group $\mathrm{SL}_2(\mathfrak{k})$, where $\mathfrak{k}$ is a $\mathfrak{p}$-adic field. The main result amounts to Langlands' Fundamental Lemma for $\mathrm{SL}_2(\mathfrak{k})$.

In the first section, however, I'll begin the paper with a little known but intriguing observation of Hecke dating to around 1930. In this example the groups involved are finite and all the difficulties of analysis vanish, but at the same time many of the important phenomena involved in endoscopy already appear, somewhat more transparently than for $\mathrm{SL}_2(F)$.

Next I'll recall the structure of unramified representations of SL_2 over $\mathfrak{p}$-adic groups. Then I'll prove the Fundamental Lemma following an elementary and elegant method found in [Kottwitz:1981]. He applied it to the group SL_3, but it works nicely for the group SL_2 as well. Oddly enough this proof has not appeared before in the literature. Kottwitz' method, which works directly with the geometry of the Bruhat-Tits building. turned out to be a dead end, but is nonetheless interesting and suggestive.

In a subsequent paper I hope to sketch the more promising approach of Goresky, Kottwitz, and MacPherson and relate it to the geometry of the building, and perhaps relate both to Ngo's recent proof.

I wish to thank audiences at the Tata Institute in Mumbai and the universities of Minnesota and McGill, as well as Mark Goresky, for helping me work things out.

Contents

Part I. Introduction

1. Hecke's precursor

The group $\mathrm{PSL}_2(\mathbb{Z}/N) = \mathrm{SL}_2(\mathbb{Z}/N)/\{\pm I\}$ acts on the holomorphic cusp forms of weight 2 on $\mathcal{H}$ with respect to the principal congruence group $\Gamma(N)$ of level N:

$$\pi(\gamma)f = f \,\big|\, [\gamma^{-1}]_2$$

where (using Shimura's notation)

$$\big(f \,\big|\, [g]_k\big)(z) = f\big(g(z)\big)(cz+d)^{-k} \text{ if } g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} .$$

The group $\Gamma(N)$ itself acts trivially by definition, and so does $\pm I$, so the action passes to the quotient $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N)\cdot\{\pm I\}$, which is canonically isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/N)$. A natural question apparently first investigated by Hecke is: *what is the irreducible decomposition of this representation?* At the time he asked this, the classification of the irreducible representations of $\mathrm{PSL}_2(\mathbb{Z}/N)$ had been worked out by Frobenius in the case $N = p$, a prime, and this was the case Hecke looked at.

Incidentally, Hecke works with the *right* action $f \mapsto f \,\big|\, [\gamma]_k$ instead of the one I do.

Let $\overline{X}_p$ be the compactification of X_p by cusps. The forms of weight two with respect to $\Gamma(p)$ may be identified with the space of holomorphic differential forms on $\overline{X}_p$. Let π be the representation of $\mathrm{PSL}_2(\mathbb{Z}/p)$ on this space. It was known to Hecke, as it is to us, that the representation $\pi \oplus \overline{\pi}$ is that of $\mathrm{PSL}_2(\mathbb{Z}/p)$ on the rational cohomology of $\overline{X}_p$. Therefore the sum of π and its complex conjugate has to be rational. But the representation π itself is not necessarily even real, and so it makes sense to ask, *what can one say about the difference between π and $\overline{\pi}$?* This is the question that most intrigued Hecke.

The case $p = 2$ is not interesting. Nor is the case $p \equiv 1 \bmod 4$, since it follows from Frobenius' character tables that in this case π is always isomorphic to its conjugate. What is interesting is the remaining case in which $p \equiv 3 \bmod 4$. Understanding what happens for these primes leads to an instructive prototype of later results of Labesse and Langlands. Since $\mathrm{PSL}_2(\mathbb{Z}/p)$ is a finite group, phenomena are more transparent than they are for $\mathrm{SL}_2(F)$, and it is remarkable that many of the features explored by Labesse and Langlands occur already here. Among other things, much like the later results, Hecke's observation has ties to quadratic reciprocity.

The case $p = 3$ is exceptional, and also uninteresting. So from now on I assume that $p > 3$, $p \equiv 3 \bmod 4$. One immediate consequence of this assumption is that -1 is not a square in $\mathbb{Z}/p$. I'll first discuss the representations of $\mathrm{SL}_2(\mathbb{Z}/p)$, then explain how this relates to the representation on holomorphic forms on $\overline{X}_p$.

Representations Let $F = \mathbb{Z}/p$, $E = F(\sqrt{-1})$, Let $G = \mathrm{PSL}_2(F)$. I'll recall here the classification of conjugacy classes and irreducible representations of G.

Representatives of conjugacy classes are

$$\begin{aligned} &\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &\pm \begin{bmatrix} t & 0 \\ 0 & 1/t \end{bmatrix} \sim \pm \begin{bmatrix} 1/t & 0 \\ 0 & t \end{bmatrix} \quad (t \neq 1) \\ &\pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \\ &\pm \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \sim \pm \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \quad (a^2 + b^2 = 1, a \neq 0) \\ &\pm \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ &\pm \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} . \end{aligned}$$

The classification of semi-simple conjugacy classes will be dealt with in detail later on, but I point out here that the map

$$a + b\sqrt{-1} \longmapsto \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

is an embedding of the group $N^1_{E/F}$ into $\mathrm{SL}_2(F)$, inducing a map from $N^1_{E/F}/\{\pm 1\}$ into G. The group $N^1_{E/F}/\{\pm 1\}$ is of order $(p+1)/2$. Since $p \equiv 3 \bmod 4$, it has a unique non-trivial element ε_0 of order two, as well as a unique non-trivial character ρ_0 of order two. As for the unipotent classes, the important fact is that

$$\begin{bmatrix} t & 0 \\ 0 & 1/t \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} t & 0 \\ 0 & 1/t \end{bmatrix}^{-1} = \begin{bmatrix} 1 & t^2 x \\ 0 & 1 \end{bmatrix} ,$$

so that since -1 is not a square in F the two classes are distinct. Among all classes, they have the unique property that although distinct in $\mathrm{PSL}_2(F)$ they fuse in $\mathrm{PSL}_2(E)$. This is the simplest example of the distinction between ordinary conjugacy and what Langlands calls **stable conjugacy** in reductive groups—two elements are said to be stably conjugate if they are conjugate over the algebraic closure.

The matrix

$$\iota = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

in $\mathrm{GL}_2(F)$ acts by conjugation on G. All except the two unipotent classes in G are fixed by this conjugation, but the unipotent classes are swapped by it.

As for representations, the group G has

- one representation of dimension 1 (the trivial representation)
- one representation of dimension p (called the **Steinberg** representation)
- representations $\pi(\chi)$ of dimension $p+1$ parametrized by characters χ of $F^\times$ (the principal series)
- representations $\pi(\rho)$ of dimension $p-1$ parametrized by characters $\rho \neq \rho_0$ of $N^1_{E/F}$ (cuspidal representations)
- two representations of dimension $(p-1)/2$, which I'll call $\pi_\pm$, corresponding to the unique character ρ_0 of order two of $N^1_{E/F}$

The trivial and Steinberg representations together decompose the representation of G on the space $\mathbb{C}\big(\mathbb{P}^1(F)\big)$. It is only the last two we are really interested in. In general, there is a representation $\pi(\rho)$ of G associated to every ρ of $N^1_{E/F}/\{\pm 1\}$, and there exists a G-ismorphism T of $\pi(\rho)$ with $\pi(1/\rho)$. For $\rho = \rho_0$ this is a non-trivial G-automorphism of $\pi(\rho_0)$ of order two, and the representations $\pi_\pm$ are its eigenspaces.

The representations $\pi_\pm$ have the unique feature that neither is isomorphic to its complex conjugate. Instead, complex conjugation interchanges them. What is especially important for us is that *their characters differ only on the two unipotent classes of G*. In other words, the unusual representations $\pi_\pm$ are in some way matched with the unusual unipotent conjugacy classes. Details of this matching appear in the following character table:

CONJUGACY CLASS \ REPRESENTATION	I	STEINBERG	$\pi(\chi)$	$\pi(\rho)$	$\pi_+(\rho_0)$	$\pi_-(\rho_0)$
$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$	1	p	$p+1$	$p-1$	$(p-1)/2$	$(p-1)/2$
$\begin{bmatrix}t & 0\\ 0 & 1/t\end{bmatrix}$	1	1	$\chi(t)+\chi(1/t)$	0	0	0
$\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$	1	1	0	$-2\rho(\varepsilon_0)$	$-\rho_0(\varepsilon_0)$	$-\rho_0(\varepsilon_0)$
$\begin{bmatrix}a & -b\\ b & a\end{bmatrix}$	1	-1	0	$-\rho(\varepsilon)-\rho(1/\varepsilon)$	$-\rho_0(\varepsilon)$	$-\rho_0(\varepsilon)$
$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$	1	0	1	-1	$\overline{\mathfrak{G}}$	$\mathfrak{G}$
$\begin{bmatrix}1 & -1\\ 0 & 1\end{bmatrix}$	1	0	1	-1	$\mathfrak{G}$	$\overline{\mathfrak{G}}$

Here

$$\mathfrak{G} = \sum_{(x/p)=1} e^{2\pi i x/p}, \quad \overline{\mathfrak{G}} = \sum_{(x/p)=-1} e^{2\pi i x/p}$$

are partial Gauss sums, $\varepsilon = a + b\sqrt{-1}$, and $\varepsilon_0 = \sqrt{-1}$. There is a slight difference between my notation and Hecke's. Because his representations are right actions, his characters are the conjugates of the ones in this table.

The representations $\pi_\pm$ are to be thought of as twins, distinguished only by which of $\mathfrak{G}$ and $\overline{\mathfrak{G}}$ they correspond to. One thing that can be read from this table is that π^ι is isomorphic to $\overline{\pi}$ for all π, and isomorphic to π itself for all but $\pi_\pm$, for which

$$\pi^\iota_\pm \cong \overline{\pi}_\pm \cong \pi_\mp \,.$$

One consequence of these observations is a very close analogue of the Fundamental Lemma. The space of conjugation-invariant 'distributions' D on G such that $D = -D^\iota$ has dimension one. It includes

$$f \longmapsto \text{trace}\ \pi_+(f) - \text{trace}\ \pi_-(f)$$

as well as the difference of 'orbital integrals'

$$f \longmapsto \sum_{x\sim\nu} \big(f(x) - f(x^\iota)\big)\,,$$

where

$$\nu = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \bmod p\,.$$

These two are therefore proportional to each other. This is exactly what the Fundamental Lemma is all about, but for p-adic groups.

For our purposes another direct consequence is more relevant.

Proposition 1.1.1. *Suppose π to be any finite-dimensional representation of G. Let $m_\pm$ be the multiplicity of $\pi_\pm$ in its irreducible decomposition. Then*

$$m_+ - m_- = \frac{\operatorname{trace} \pi(\nu) - \operatorname{trace} \overline{\pi}(\nu)}{\overline{\mathfrak{G}} - \mathfrak{G}}\,.$$

Proof. Say

$$\pi = \sum_k m_k \pi_k$$

is the decomposition of π into irreducibles. Then for g in G

$$\begin{aligned} \operatorname{trace} \pi(g) &= \sum m_k \operatorname{trace} \pi_k(g) \\ \operatorname{trace} \overline{\pi}(g) &= \sum m_k \operatorname{trace} \overline{\pi}_k(g) \\ \operatorname{trace} \pi(g) - \operatorname{trace} \overline{\pi}(g) &= \sum m_k \big(\operatorname{trace} \pi_k(g) - \operatorname{trace} \overline{\pi}_k(g)\big)\,. \end{aligned}$$

All terms in this last sum vanish unless g lies in the 'stable conjugacy class' of unipotents, and in that case the only terms that don't vanish are those for the pair $\pi_\pm$. Then

$$\begin{aligned} \operatorname{trace} \pi(\nu) - \operatorname{trace} \overline{\pi}(\nu) &= m_+\big(\operatorname{trace} \pi_+(\nu) - \operatorname{trace} \overline{\pi}_-(\nu)\big) + m_-\big(\operatorname{trace} \pi_-(\nu) - \operatorname{trace} \overline{\pi}_+(\nu)\big) \\ &= (m_+ - m_-)\big(\operatorname{trace} \pi_+(\nu) - \operatorname{trace} \overline{\pi}_-(\nu)\big) \\ &= (m_+ - m_-)\big(\overline{\mathfrak{G}} - \mathfrak{G}\big) \\ m_+ - m_- &= \frac{\operatorname{trace} \pi(\nu) - \operatorname{trace} \overline{\pi}(\nu)}{\overline{\mathfrak{G}} - \mathfrak{G}}\,. \end{aligned}$$

The modular curves We are going to apply Proposition 1.1.1 to the representation of $\mathrm{SL}_2(\mathbb{Z}/p)$ on the space of holomorphic differential forms on $\overline{X}_p$. The first if well known step is to understand the transition from $\mathrm{SL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z}/p)$.

The group $\Gamma(p)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$. The action of $\mathrm{SL}_2(\mathbb{Z})$ passes through its quotient by $\Gamma(p)$.

Lemma 1.2.1. *The sequence*

$$1 \to \Gamma(p) \longrightarrow \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p) \longrightarrow 1$$

is exact.

Proof. It must be shown that for each γ in $\mathrm{SL}_2(\mathbb{Z}/p)$ there exists g in $\mathrm{SL}_2(\mathbb{Z})$ with image γ modulo p. The Bruhat decomposition of $\mathrm{SL}_2(\mathbb{Z}/p)$ reduces this to three cases:

$$\gamma = \begin{cases} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \\ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} & (ab \equiv 1 \bmod p) \\ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \end{cases}$$

Only the second is non-trivial. But if $ab = 1$ in $\mathbb{Z}/p$, choose $\alpha \equiv a$ modulo p. Since α is invertible modulo p, it is also invertible modulo p^2, so we may choose β such that $\beta \equiv b$ and $\alpha\beta \equiv 1$ modulo p^2, If $\alpha\beta = 1 + kp^2$ then

$$\begin{bmatrix} \alpha & kp \\ p & \beta \end{bmatrix} \longmapsto \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} . \quad \square$$

The usual proof of this is somewhat more elementary. This one has the advantage that it generalises well to $\mathrm{SL}_2(\mathfrak{o}_K)$ where K is an arbitrary number field. This theorem is the simplest case of the strong approximation theorem, valid for arbitrary simply connected, semi-simple groups over number fields.

Corollary 1.2.2. *The action of* $\mathrm{SL}_2(\mathbb{Z})$ *on* $\overline{X}_p$ *induces one of* $\mathrm{SL}_2(\mathbb{Z}/p)$*.*

The next step is to recall how to interpret the points of $\overline{X}_p$ as parameters of certain structures. This is quite different for interior points and cusps.

Interior points On $\mathbb{C}$ define the symplectic form

$$u \wedge v = \mathrm{IM}(u \cdot \overline{v}), \quad (x_1 + iy_1) \wedge (x_2 + iy_2) = x_2y_1 - x_1y_2 .$$

We have

$$cu \wedge cv = |c|^2 \, (u \wedge v) ,$$

so that if (u, v) is a pair with $u \wedge v > 0$ so is (cu, cv). Hence it makes sense to define the space $\mathfrak{H}$ to be that of all pairs (u, v) of points of $\mathbb{C}$ with $u \wedge v > 0$ modulo scalar multiplication by $c \in \mathbb{C}^\times$. Similarly, if (u, v) is a pair with $u \wedge v = 1$ and $|c| = 1$ then also $cu \wedge cv = 1$, and it makes sense to define $\mathfrak{H}_1$ to be the space of all pairs (u, v) with $u \wedge v = 1$ modulo multiplication by c in the unit group

$$\mathbb{S} = \left\{ c \in \mathbb{C} \,\middle|\, |c| = 1 \right\} .$$

The map $z \mapsto (z, 1)$ induces a bijection of the upper half plane $\mathcal{H}$ with $\mathfrak{H}$, and similarly the inclusion of $\mathfrak{H}_1$ into $\mathfrak{H}$ is a bijection. The group $\mathrm{SL}_2(\mathbb{R})$ acts on the left on $\mathfrak{H}$ and $\mathfrak{H}_1$:

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \, (u, v) \longmapsto (au + bv, cu + dv) .$$

The scalar matrices $\pm I$ act trivially in both cases, since $\pm 1 \in \mathbb{S}$. The identifications of $\mathfrak{H}$ and $\mathfrak{H}_1$ with $\mathcal{H}$ are compatible with the classical action on $\mathcal{H}$ by fractional linear transformations.

Each pair (u, v) with $u \wedge v > 0$ determines a lattice $L_{u,v} = \mathbb{Z}u + \mathbb{Z}v$. If g lies in $\mathrm{SL}_2(\mathbb{Z})$ then (gu, gv) determines the same lattice. If $u \wedge v = 1$ then the volume of $\mathbb{C}/L$ is 1—it is a **unit lattice**.

Lemma 1.3.1. *If* L *is a unit lattice in* $\mathbb{C}$ *there exists a basis* (u, v) *for* L *such that* $u \wedge v = 1$*, which is unique modulo* $\mathrm{SL}_2(\mathbb{Z})$*.*

Proof. If u, v make up a basis, then the familiar volume formula tells us that $|u \wedge v| = 1$, so if necessary we can swap u and v to obtain $u \wedge v = 1$. The last claim follows from the equation $g(u) \wedge g(v) = \det(g) \, (u \wedge v)$. $\square$

Corollary 1.3.2. *The map* $(u, v) \mapsto L_{u,v}$ *induces a bijection of the quotient* $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}_1$ *with the space of unit lattices modulo* $\mathbb{S}$*.*

I want now to describe X_p similarly. It parametrizes **level structures**. If L is a unit lattice in $\mathbb{C}$ then the symplectic form on $\mathbb{C}$ induces an integral symplectic form on L, hence also a symplectic form on L/pL with values in $\mathbb{Z}/p$. Given (u, v) in $\mathfrak{H}_1$, let $\overline{u}$, $\overline{v}$ be the images of u, v in L/pL.

Proposition 1.3.3. *The map*

$$(u, v) \longmapsto L_{u,v}, \quad (\overline{u}, \overline{v})$$

induces a bijection of $\Gamma(p)\backslash\mathfrak{H}_1$ *with the set of unit lattices* L *together with a symplectic basis of* L/pL *modulo scalar multiplication by* ± 1*, all modulo* $\mathbb{S}$*.*

Cusps If Γ is an arbitrary arithmetic subgroup of $\mathrm{SL}_2(\mathbb{Q})$, the cusps of $\Gamma\backslash\mathcal{H}$ are in bijection with the Γ-orbits on $\mathbb{P}^1(\mathbb{Q})$. A point of $\mathbb{P}^1(\mathbb{Q})$ is either ∞ or a fraction a/c. The expression a/c for a reduced fraction is unique up to multiplication of numerator and denominator by ± 1, so the map from relatively prime pairs (a, c)—called **primitive points**—in $\mathbb{Z}^2$ to $\mathbb{P}^1(\mathbb{Q})$ is a double covering. (Primitive points of any free module over a ring can be characterized as part of a babis.) For example, if $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ there is just one cusp since this Γ acts transitively on primitive points (a, c). The Euclidean algorithm shows this explicitly—given a, c with a, c relatively prime, we can find b, d with $ad - bc = 1$, and hence

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} : (1, 0) \sim \infty \longmapsto (a, c) \sim a/c\,.$$

Reduction modulo p maps primitive points of $(\mathbb{Z})^2$ to primitive poinst of $(\mathbb{Z}/p)^2$.

Proposition 1.4.1. *Reduction modulo p induces a bijection of the orbits of $\Gamma(p)$ among primitive points (a, c) with primitive points of $(\mathbb{Z}/p)^2$.*

Proof. Let $\Gamma = \Gamma(p)$. I first ask, what is the Γ-orbit of $(1, 0)$? If γ lies in Γ and γ takes $(1, 0)$ to (a, c) then of course $a \equiv 1$, $c \equiv 0$ modulo p. Conversely, suppose $a \equiv 1$, $c \equiv 0$ modulo p with a relatively prime to c. Then a is also prime to c^2, so we can find k, m with $ka - mc^2 = 1$. If

$$\gamma = \begin{bmatrix} a & lc \\ c & k \end{bmatrix}$$

then $\gamma \equiv I$ modulo p and $\gamma(1, 0) = (a, c)$. Thus the orbit of $(1, 0)$ with respect to Γ is the set of all primitive (a, c) with $a \equiv 1$ and $c \equiv 0$ modulo p.

I next ask, what are the other Γ-orbits? If $p_1 = (a_1, c_1)$ and $p_2 = (a_2, c_2)$ are in the same Γ-orbit then clearly $(a_2, c_2) \equiv \pm(a_1, c_1)$ modulo p. Conversely, suppose this condition to hold. Say $(a_1, c_1) = \alpha(1, 0)$. Because of the congruence conditions on p_1 and p_2, the first part of our argument implies that $\alpha^{-1}(p_2)$ will be in the orbit of $(1, 0)$, say $\alpha^{-1}(p_2) = \gamma(\infty)$ with $\gamma \equiv I$ modulo p. Then $\alpha\gamma\alpha^{-1}(p_1) = p_2$. ▯

Corollary 1.4.2. *The map*

$$a/c \longmapsto (a, c)$$

induces a bijection of the cusps of $\Gamma(p)$ with the primitive points of $(\mathbb{Z}/p)^2$ modulo ± 1.

Hecke's theorem Hecke's really interesting observation was that the difference between the representations $\pi_\pm$ has global arithmetic significance. They do not occur with the same multiplicity in the representation of $\mathrm{SL}_2(\mathbb{Z}/p)$ on differential forms on $\overline{X}_p$. Instead, the difference in multiplicities is accounted for by the cusp forms contributed by Grössencharaktere associated (through binary θ-functions) to $\mathbb{Q}(\sqrt{-p})$. These had been constructed in [Hecke:1928]. Hecke proved this by a clever application of Riemann-Roch, but it can be more cleanly proved by applying the Atiyah-Bott trace formula (which was in fact motivated by an earlier result of Eichler about algebraic curves, brought to the attention of Atiyah and Bott by Shimura at the Woods Hole conference of 1965).

Let π be the representation of $G = \mathrm{PSL}_2(\mathbb{Z}/p)$ at hand. Let $h(-p)$ be the ideal class number of the quadratic imaginary quadratic extension $\mathbb{Q}(\sqrt{-p})$. Suppose that as a representation of G

$$\pi = \sum m_{\pi_k}\, \pi_k\,.$$

Proposition 1.5.1. (Hecke) *The difference $m_{\pi_+} - m_{\pi_-}$ is equal to $h(-p)$.*

The class number will arise through Dirichlet's formula

$$h(-p) = -\frac{1}{p} \sum_{1}^{p-1} m \left(\frac{m}{p} \right) .$$

Recall that

$$\nu = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} .$$

According to Proposition 1.1.1

$$m_+ - m_- = \frac{\text{trace}\, \pi(\nu) - \text{trace}\, \overline{\pi}(\nu)}{\overline{\mathfrak{G}} - \mathfrak{G}} .$$

So we must calculate

$$\tau = \text{trace}\, \pi(\nu) - \text{trace}\, \overline{\pi}(\nu) ,$$

for which I'll use the formula of Eichler-Atiyah-Bott. More precisely, I use the formulation on p. 12 of [Atiyah-Bott:1964]: *If X is a compact Riemann surface and $f \colon X \to X$ a holomorphic map, let α be the trace of f^* on $H^0(X, \Omega)$. If the fixed points of f are isolated, then*

$$1 - \overline{\alpha} = \sum_{f(x)=x} \frac{1}{1 - f'(x)} ,$$

where $f'(x)$ is the map of the holomorphic tangent space induced by f at x. In our situation the group has been made to act by the inverse of f^* and f is of finite order, so $\overline{\alpha}$ itself will be the trace we are looking at. In other words

$$\tau - \overline{\tau} = - \sum_{\nu(x)=x} \left(\frac{1}{1 - \zeta_x} - \frac{1}{1 - \overline{\zeta}_x} \right) ,$$

where ν acts as multiplication by ζ_x around the fixed point x.

Thus we must classify the points of $\overline{X}_p$ fixed by ν. *What points are fixed by ν? How does ν act on the tangent space of those points?*

Proposition 1.5.2. *The fixed points of ν acting on $\overline{X}_p$ are the cusps associated to the points $(x, 0)$ for x in $(\mathbb{Z}/p)^\times$.*

Since $(\pm x, 0)$ give rise to the same cusp, there are $(p-1)/2$ of them.

Proof. It is fairly straightforward to see that if γ in $\mathrm{SL}_2(\mathbb{Z}/p)$ fixes an interior point of $\overline{X}_p$ then the point is the transform of i or of a sixth root of unity, and γ has order divisible by 2 or 3. Since ν has order $p > 3$ this possibility is excluded. Any fixed point must therefore be a cusp. There is one simple possibility, the cusp at infinity, where ν acts locally by multiplication by $\zeta = e^{2\pi i/p}$. Which of the other cusps are fixed by ν?

Any cusp fixed by ν has to correspond to a non-zero point of $(\mathbb{Z}/p)^2$ fixed by the image of ν modulo p, so must be of the form a/c with $c \equiv 0$ modulo p. Conversely, consider $(x, 0)$ for x in $\mathbb{Z}$ with $x \not\equiv 0$ modulo p. Then (x, p) is a primitive point of $(\mathbb{Z})^2$ with image $(x, 0)$ modulo p.

I am going to show that ν fixes the image of (x, p) in $\overline{X}_p$. For this, it suffices to find γ in $\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(x, p) = (x, p)$, $\gamma \equiv \nu$ modulo p.

Choose y, k such that $xy - kp^2 = 1$, so now

$$\alpha = \begin{bmatrix} x & kp \\ p & y \end{bmatrix}$$

takes $(1,0)$ to (x,p). Let

$$\mu = \begin{bmatrix} 1 & y^2 \\ 0 & 1 \end{bmatrix}.$$

Since

$$\alpha \equiv \begin{bmatrix} x & 0 \\ 0 & 1/x \end{bmatrix}$$

modulo p, $y \equiv 1/x$ modulo p, and

$$\begin{bmatrix} x & 0 \\ 0 & 1/x \end{bmatrix} \begin{bmatrix} 1 & y^2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1/x & 0 \\ 0 & x \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

I set $\gamma = \alpha\mu\alpha^{-1}$. ∎

Proposition 1.5.3. *The action of ν on the tangent space associated to $(x,0)$ is multiplication by $e^{2\pi i y^2/p}$, where $xy \equiv 1$ modulo p.*

Proof. Follows immediately from the definition of γ in the proof of the preceding Proposition. ∎

The fixed point formula tells us what $1 - \operatorname{trace} \pi(\nu)$ is, and then also $1 - \operatorname{trace} \overline{\pi}(\nu)$. Taking the difference, we get

$$\operatorname{trace} \pi(\nu) - \operatorname{trace} \overline{\pi}(\nu) = \sum_{m \bmod p} \left(\frac{m}{p}\right) \frac{1}{\zeta^m - 1}$$

where $\zeta = e^{2\pi i/p}$.

We want to rewrite this expression. Start with the algebraic formula:

$$\begin{aligned} z^p - 1 &= (z-1)(z^{p-1} + z^{p-2} + \cdots + z + 1) \\ \frac{1}{z-1} &= \frac{z^{p-1} + z^{p-2} + \cdots + z + 1}{z^p - 1} \end{aligned}$$

If we set z equal to a p-th root of unity, the right hand side must be evaluated by l'Hôpital's rule:

$$\frac{1}{z-1} = \frac{\sum_1^{p-1} k z^{k-1}}{p z^{p-1}} = \frac{1}{p} \sum k z^k .$$

The trace on $\pi - \overline{\pi}$ is therefore

$$\begin{aligned} \frac{1}{p} \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \left(\sum_{k=1}^{p-1} k \zeta^{km}\right) &= \frac{1}{p} \sum_k k \left(\sum \left(\frac{m}{p}\right) \zeta^{km}\right) \\ &= \frac{1}{p} \sum_k k \left(\frac{k}{p}\right) \left(\sum \left(\frac{n}{p}\right) \zeta^n\right) \\ &= \frac{\mathfrak{G} - \overline{\mathfrak{G}}}{p} \sum_k k \left(\frac{k}{p}\right) \end{aligned}$$

To get the difference $m_+ - m_-$, we divide by $\overline{\mathfrak{G}} - \mathfrak{G}$ to give us $h(-p)$. ∎

Which of the two representations $\pi_\pm$ occurs more often than the other is implicitly related, as Hecke himself observed, to the sign of Gauss sums. This sort of problem—i.e. relations with class field theory—is ubiquitous in this business. Hecke didn't tie all these facts together systematically, but this was done by Labesse and Langlands around 1971, who generalized Hecke's observation to all representations on all quotients $\mathrm{SL}_2(F)\backslash SL_2(\mathbb{A}_F)$.

2. Setting up

I now start in on the principal part of this paper. From now on:

$$\begin{aligned} \mathfrak{k} &= \text{a field with a discrete valuation, assumed to be locally compact} \\ \overline{\mathfrak{k}} &= \text{a separable closure of } \mathfrak{k} \\ \mathfrak{o} &= \text{the associated discrete valuation ring} \\ \mathfrak{p} &= \text{the unique maximal ideal of } \mathfrak{o} \\ \varpi &= \text{a generator of } \mathfrak{p} \\ q &= \text{cardinality of the residue field } \mathfrak{o}/\mathfrak{p} \\ \mathfrak{F} &= \text{the Frobenius automorphism of the maximal unramified extension of } \mathfrak{k} \\ \langle\mathfrak{F}\rangle &= \text{the group generated by } \mathfrak{F} \end{aligned}$$

I assume that the characteristic of $\mathfrak{k}$ itself is not 2, to avoid some inconvenience caused by inseoarability. Every element x of $\mathfrak{k}$ can be factored as $x = u\varpi^k$, with $|x| = q^{-k}$.

I'll begin by recalling in a very general context what Langlands calls **functoriality**. Suppose here in the introduction that

$$\begin{aligned} G &= \text{an arbitrary unramified reductive group over } \mathfrak{k} \\ C^\infty(G) &= \text{locally constant functions on } G \text{ with values in } \mathbb{C} \\ B &= TN \\ &= \text{a Borel subgroup of } G \text{ with unipotent radical } N, \text{ maximal torus } T \\ A &= \text{a maximal split torus in } T \\ \delta_B &= \big|\det \mathrm{Ad}_{\mathfrak{n}}\big|, \text{ the modulus character of } B \\ K &= G(\mathfrak{o}) \\ W &= N_G(T)/T \text{ (the Weyl group)}\,. \end{aligned}$$

These make sense because G is obtained by base extension from a smooth reductive group over $\mathfrak{o}$. Representatives of elements of W may be chosen in K. Assign G a Haar measure with K of measure 1. It is a consequence of a theorem of Serge Lang, that asserts that the map $g \mapsto g/g^{\mathfrak{F}}$ is surjective on groups over finite fields, that the embedding of $A/A(\mathfrak{o})$ into $T/T(\mathfrak{o})$ is a bijection.

An irreducible representation (π, V) of G is **unramified** if $V^K \neq 0$. These are important in the theory of automorphic forms because a representation appearing among automorphic forms will be a restricted tensor product $\widehat{\bigotimes}\,\pi_v$ where all but a finite number of π_v are unramified.

There is a simple classification of unramified representations. Suppose χ to be an unramified character of T, which is to say a homomorphism $T \to \mathbb{C}^\times$ that is trivial on $T(\mathfrak{o})$. Since T is a quotient of B, it gives rise to a character of B. The corresponding **principal series representation** of G is the right regular representation on the space

$$I(\chi) = \mathrm{Ind}(\chi \,|\, B, G) = \big\{ f \in C^\infty(G) \,\big|\, f(bg) = \chi(b)\delta^{1/2}(b) f(g) \text{ for all } b \in B,\ g \in G \big\}\,.$$

Because $G = BK$, the subspace of vectors fixed by K may be identified by restriction to K with the constant functions on K. Therefore each $I(\chi)$ has as consitituent a unique unramified representation $V(\chi)$ of G, and it turns out that every unramified representation of G is isomorphic to one of these. The space $I(\delta_B^{-1/2})$ may be identified with $C^\infty(B\backslash G)$, whereas $I(\delta_B^{1/2})$ may be identified with its smooth dual, the space of smooth one-densities on $P\backslash G$. If χ is unitary, so is $I(\chi)$.

There are meromorphically defined, normalized intertwining operators

$$T_w \colon I(\chi) \longrightarrow I(w\chi)$$

that are equal to 1 on V^K, and generically isomorphisms. Therefore $V(\chi) \cong V(w\chi)$, and the unramified representations of G are parametrized by the characters of $T/T(\mathfrak{o}) \cong A/A(\mathfrak{o})$ modulo W.

There is an important observation of Langlands to be explained here. Let

$$X_*(T) = \mathrm{Hom}(\mathbb{G}_m, T)$$

be the **cocharacter group** of T, the lattice of algebraic homomorphisms from $\mathbb{G}_m$ to T defined over $\overline{gk}$. Similarly define $X_*(A)$. The group $\langle \mathfrak{F} \rangle$ acts on $X_*(T)$, and $X_*(A)$ is the subgroup of invariants. The map

$$\lambda^\vee \longmapsto \lambda^\vee(\varpi)$$

allows us to identify $X_*(A)$ with $A/A(\mathfrak{o})$. Define $\widehat{T}$ to be the complex torus $\mathrm{Hom}(X_*(T), \mathbb{C}^\times)$, and similarly $\widehat{A}$. The embedding of A into T makes $\widehat{A}$ a quotient of $\widehat{T}$. The torus $\widehat{T}$ is a maximal torus in a reductive group $\widehat{G}$ whose root datum is the dual of the root datum defining G. If we fix a Borel group $\widehat{B} \supseteq \widehat{T}$ of $\widehat{G}$, then $\mathfrak{F}$ acts on $\widehat{G}$ by permuting positive roots in accordance with the twist defining the quasi-split group G. This gives rise to the semi-direct product $\widehat{G} \rtimes \langle \mathfrak{F} \rangle$, which is the unramified L-group ${}^LG$ of G.

Langlands' basic observation is that

> *the set $\widehat{A}/W$, which parametrizes the W-orbits in the set of unramified characters of A and hence also the unramified representations of G, may be identified with semi-simple conjugacy classes in the Frobenius coset $\widehat{G} \rtimes \mathfrak{F}$.*

For all this, refer to [Borel:1979].

The conjugacy class associated to the unramified representation π is its **Frobenius** $\mathfrak{F}_\pi$. Its principal role is in defining the family of L-functions

$$L(s, \pi) = \det\left(I - \frac{\rho(\mathfrak{F}_\pi)}{q^s}\right)^{-1}$$

associated to finite-dimensional representations ρ of ${}^LG$. These are the local factors in L-functions associated globally to automorphic forms.

If $R = \mathbb{C}$ or $\mathbb{Z}$, the Hecke algebra $\mathcal{H}_R(G/\!/K)$ is the $\mathbb{Z}$-module of compactly supported R-valued functions on G invariant on left and right by K. If (π, V) is an unramified representation of G and $v \in V^K$ then

$$\int_G f(g)\pi(g)v\, dg = \varphi(f)\, v$$

for some constant $c_\pi(f)$, and the map $f \mapsto c(_\pi(f)$ is a ring homomorphism from $\mathcal{H}_\mathbb{C}(G/\!/K)$ to $\mathbb{C}$. Let φ_χ be the homomorphism associated to the unramified character χ. Since these characters are parametrized by elements of the complex torus $\widehat{T}$, this defines for every f a conjugation-invariant complex-valued function on $\widehat{G} \rtimes \mathfrak{F}$. The **Satake isomorphism** is identifies $\mathcal{H}_\mathbb{C}(G/\!/K)$ with the affine ring of such functions.

If G is split, the integral Hecke ring is naturally ismorphic to the representation ring of $\widehat{G}$. Making this completely explicit, and extending the assertion to all unramified groups, is an interesting exercise that does not seem to be completely laid out in the literature.

Since conjugacy classes in ${}^LG$ parametrize unramified representations of G, a homomorphism $\eta\colon {}^LH \to {}^LG$ compatible with the projection onto $\langle \mathfrak{F} \rangle$ by definition associates to every unramified representation of H one of G. This is the simplest example of what Langlands calls **functoriality**. Since Hecke algebras may be identifies with functions on ${}^LG$, we also get a map η^* backwards from the complex Hecke algebra of G to that of H. (Examples are just around the corner.)

A very special case of functoriality arises from unramified **endoscopic subgroups** of G (which are not necessarily in fact subgroups of G). Suppose as above that $\widehat{T} \subset \widehat{B}$ is a Borel pair in $\widehat{G}$. Roughly, an endoscopic subgroup amounts to a choice of a conjugacy class s in $\widehat{T}$ and an extra datum. From s we recover the group $\widehat{H}$, which is the connected component of the centralizer of s in $\widehat{G}$. The extra datum is an automorphism of the intersection $\widehat{B} \cap H$ of the form $\mathfrak{F}_H = w\mathfrak{F}_G$ defining an unramified group H, where w is in the normalizer of $\widehat{T}$. From these data one can find an embedding of ${}^L H$ into ${}^L G$ compatible with the Frobenius elements. The motivation for introducing these is that harmonic analysis on G is unavoidably related to harmonic analysis on its endoscopic subgroups. We have already seen something like this in Hecke's observation. This paper will be concerned with a special case of this, which I now look at briefly.

Let $G = \mathrm{SL}_2(\mathfrak{k})$. Let $\mathfrak{l}/\mathfrak{k}$ be the unramified quadratic extension, and let H be the algebraic group $N^1_{\mathfrak{l}/\mathfrak{k}}$ defined as the kernel of the norm map from $\mathfrak{l}^\times$ to $\mathfrak{k}^\times$. Its character lattice is just $\mathbb{Z}$, on which conjugation in $\mathfrak{l}/\mathfrak{k}$ acts as multiplication by -1. The group ${}^L G$ is the direct product $\mathrm{PGL}_2 \times \langle \mathfrak{F} \rangle$, that of H is the semi-direct product

$$\mathbb{C}^\times \rtimes \langle \mathfrak{F} \rangle$$

with $\mathfrak{F}$ taking z to z^{-1}. The map

$$\eta\colon \quad \begin{aligned} z \rtimes 1 &\mapsto z \times 1 \\ 1 \rtimes \mathfrak{F} &\mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times 1 \end{aligned}$$

is an identification of ${}^L H$ with the centralizer of

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

in ${}^L G$. There is exactly one unramified character of H, and the embedding η associates to it the unique unramified unitary principal series representation of G that decomposes into two pieces. The simplest manifestation of the relationship between harmonic analysis and endoscopy is that the difference between the characters of the two pieces has support on the semi-simple elements of G associated to the quadratic extension $\mathfrak{l}/\mathfrak{k}$. The Fundamental Lemma is concerned with a similar fact about another family of conjugation-invariant distributions on G, the orbital integrals.

In the next part I'll recall the construction of the unramified principal series of $\mathrm{SL}_2(\mathfrak{k})$ and its relationship with the Hecke algebra. In the part after that I'll look at conjugacy classes in SL_2, and finally in the last part introduce orbital integrals and prove the Fundamental Lemma.

Part II. Unramified representations and the Hecke algebra

3. The tree of SL(2)

A smooth representation (π, V) of $G = \mathrm{SL}_2(\mathfrak{k})$ is one in which every vector is fixed by some open subgroup. An admissible representation is one such that V^K has finite dimension for every compact open subgroup K. Its admissible dual is the space $\widetilde{V}$ of all linear functions on V fixed by some open subgroup of G, which is also an admissible representation of G since $\widetilde{V}^K$ is the linear dual of V^K.

Now fix $K = \mathrm{SL}_2(\mathfrak{o})$. I call an irreducible admissible (π, V) representation **unramified** if $V^K \neq 0$. In that situation, let $\widetilde{v} \neq 0$ be a vector in $\widetilde{V}^K$. The map $v \mapsto \langle \pi(g)\widetilde{v}, v\rangle$ is then a G-equivariant embedding of V into the space of functions on the discrete set G/K. It is useful to embed this set into the Bruhat-Tits tree of $\mathrm{SL}_2(\mathfrak{k})$, which will in fact play a major role throughout this paper. The rest of this section will introduce this tree. For this material, the standard reference is Chapitre II of [Serre:1977].

The tree of $G = \mathrm{SL}_2(\mathfrak{k})$ is a graph $\mathfrak{X}$ on which it acts, and the geometry of this graph encodes much of the structure of G. Its nodes are the $\mathfrak{o}$-lattices in $\mathfrak{k}^2$ modulo similarity. For each lattice L let $\langle\!\langle L\rangle\!\rangle$ be its equivalence class. There is an edge between two nodes if they possess representatives L and M with

$$\varpi L \subset M \subset L \,,$$

in which case $L/M \cong \mathfrak{o}/\mathfrak{p}$. The nodes to which a node is linked by an edge thus correspond to points of $\mathbb{P}^1(\mathbb{F}_q)$, and there are $q+1$ of them.

If u and v are a basis of $\mathfrak{k}$, let $[u, v]$ be the lattice they span. Let $u_0 = (1, 0)$, $v_0 = (0, 1)$, so $[u_0, v_0] = \mathfrak{o}^2$.

The group $\mathrm{GL}_2(\mathfrak{k})$ transforms lattices, preserving equivalence. It also transforms links to links, so it therefore acts on the graph $\mathfrak{X}$, and since by definition scalar matrices act trivially this action factors through $\mathrm{PGL}_2(\mathfrak{k})$. The group $\mathrm{GL}_2(\mathfrak{k})$ acts transitively on lattices so $\mathrm{PGL}_2(\mathfrak{k})$ acts transitively on nodes of the tree. The stabilizer in $\mathrm{PGL}_2(\mathfrak{k})$ of the node ν_0 corresponding to $\mathfrak{o}^2$ is the maximal compact subgroup $\mathrm{PGL}_2(\mathfrak{o})$.

According to the principal divisor theorem we can express any matrix g in $\mathrm{GL}_2(\mathfrak{k})$ as

$$g = k_1 a k_2 \quad \text{with} \quad k_i \in \mathrm{GL}_2(\mathfrak{o}), \quad a = \begin{bmatrix} \varpi^k & 0 \\ 0 & \varpi^\ell \end{bmatrix} \; (k \leq \ell) \,.$$

If g is in $\mathrm{SL}_2(\mathfrak{k})$ then we can choose the k_i in $\mathrm{SL}_2(\mathfrak{o})$ and in this case $k = -\ell$. Thus we have the **Cartan decompositions**

$$\mathrm{GL}_2(\mathfrak{k}) = \mathrm{GL}_2(\mathfrak{o}) A^{++} \,\mathrm{GL}_2(\mathfrak{o}), \quad A^{++} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & \varpi^m \end{bmatrix} \;\middle|\; m \geq 0 \right\}$$

and

$$\mathrm{SL}_2(\mathfrak{k}) = \mathrm{SL}_2(\mathfrak{o}) A^{++} \,\mathrm{SL}_2(\mathfrak{o}), \quad A^{++} = \left\{ \begin{bmatrix} 1/\varpi^m & 0 \\ 0 & \varpi^m \end{bmatrix} \;\middle|\; m \geq 0 \right\}.$$

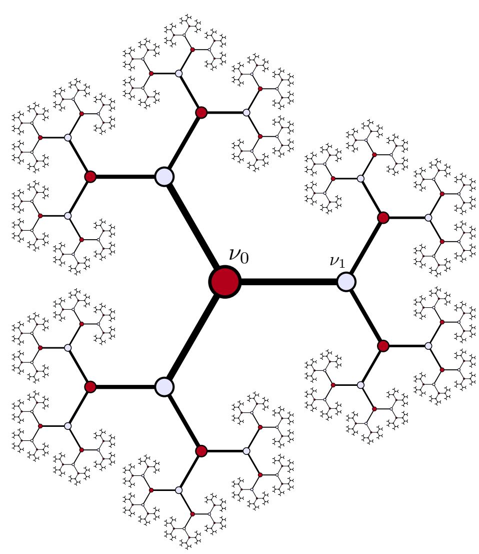
This implies that if L and M are any two lattices in $\mathfrak{k}^2$ then we can find a basis (u, v) of L such that some $(\varpi^k u, \varpi^\ell v)$ is a basis of M with $k \leq \ell$. If $L = \mathfrak{o}^2$, then the difference $\ell - k$ is an invariant of the equivalence class of M. I call the class $\langle\!\langle M\rangle\!\rangle$ **even** if this number is even and **odd** if it is odd. There are two orbits of the group $\mathrm{SL}_2(\mathfrak{k})$, each one corresponding to lattices of a given parity. If we replace M by some multiple of itself, then we may assume $k = 0$, $\ell \geq 0$. That means that there exists a chain of edges from $\langle\!\langle L\rangle\!\rangle$ to $\langle\!\langle M\rangle\!\rangle$, hence:

Proposition 3.1. *The graph $\mathfrak{X}$ is connected.*

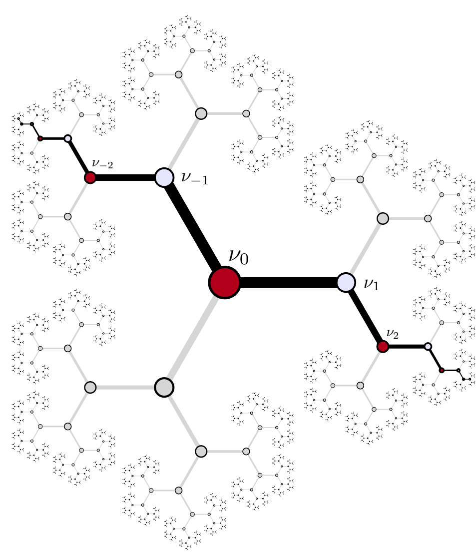
A **chain** in $\mathfrak{X}$ is a path that doesn't back-track. It can be doubly infinite, in which case it is called an **apartment**; or semi-infinite, in which case it is called a **branch** from its first node; or finite. A chain is called **standard** if it is assembled from links between nodes of the form $\nu_m = \langle\!\langle\, [u_0, \varpi^m v_0]\,\rangle\!\rangle$ and $\nu_{m+1} = \langle\!\langle\, [u_0, \varpi^{m+1} v_0]\,\rangle\!\rangle$. Every chain may be transformed by an element of $\mathrm{GL}_2(\mathfrak{k})$ to a standard chain. Since a standard chain has no loops, and $\mathfrak{X}$ is connected:

Proposition 3.2. *The graph $\mathfrak{X}$ is a tree.*

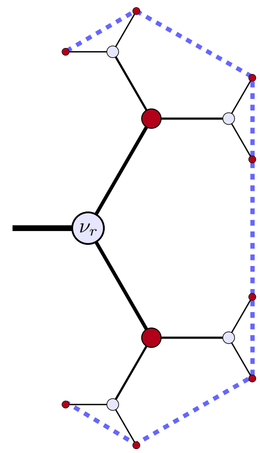
The node ν_0 may be chosen as root. The structure of $\mathfrak{X}$ is completely determined by the properties: (a) it is connected; (b) it is a tree; (c) every node has $q+1$ neighbours. For example, when $q = 2$ it looks like this:



and an apartment in the tree looks like this:



The number of edges between two nodes is called the distance between them. The distance between ν_0 and ν_m is $|m|$. The Cartan decompositions imply that both $\mathrm{PGL}_2(\mathfrak{o})$ and $\mathrm{SL}_2(\mathfrak{o})$ act transitively on the $q^{m-1}(q+1)$ nodes at distance m from ν_0.



The nodes at distance 1 from ν_0 may be identified with the points of $\mathbb{P}^1(\mathfrak{o}/\mathfrak{p})$. Similarly, those at distance r may be identified with $\mathbb{P}^1(\mathfrak{o}/\mathfrak{p}^r)$. The fixed points of the congruence group

$$K_r = \left\{ k \in \mathrm{SL}_2(\mathfrak{o}) \,\middle|\, k \equiv I \ (\mathrm{mod}\ \mathfrak{p}^r) \right\}.$$

are those at distance $\le r$ from ν_0. Any other node may be transformed by k in K_0 to some ν_n with $n > r$. The path from ν_n to ν_0 intersects the fixed points at node ν_r. The K_r-orbit of ν_n is the set of all nodes at distance n from ν_0 and $n-r$ from ν_r (that is to say, at distance $n-r$ from ν_r and on the outside of the disk fixed by K_r). The picture at right shows what happens in the tree of $\mathrm{SL}_2(\mathbb{Q}_2)$ for $n = r+3$.

4. The Hecke algebra

Assign $G = \mathrm{SL}_2(\mathfrak{k})$ a Haar measure, according to which the measure of K is 1. The integral Hecke algebra $\mathcal{H}_\mathbb{Z} = \mathcal{H}_\mathbb{Z}(G/\!/K)$ is that of all $\mathbb{Z}$-valued functions of compact support on G invariant on left and right by K. Multiplication is by convolution. Because of the Cartan decomposition it has as basis the characteristic functions of the double cosets $\tau_m = K\omega^m K$ $(m \ge 0)$ where

$$\omega = \begin{bmatrix} 1/\varpi & 0 \\ 0 & \varpi \end{bmatrix}.$$

We can define Hecke operators on the tree as correspondances, reminiscent of the definition of Hecke operators as algebraic correspondances on the upper half plane, that commute with G. Define a **cycle** to be an integral linear combination of nodes on $\mathfrak{X}$. The definition is determined by G-equivariance tother with the specification of what happens to ν_0. If T_h is the characteristic function of $KhK = \bigsqcup h_i K$ then

$$T_h \nu_0 = \sum h_i(\nu_0),$$

so if $\nu = g(\nu_0)$ then

$$T_h \nu = T_h g \nu_0 = \sum g h_i(\nu_0).$$

This is independent of the choice of g, since the union $\bigsqcup h_i K$ is left stable with respect to K. For example, *the characteristic function T_m of $K\omega^m K$ takes a node to the sum of all of its neighbours at distance $2m$.*

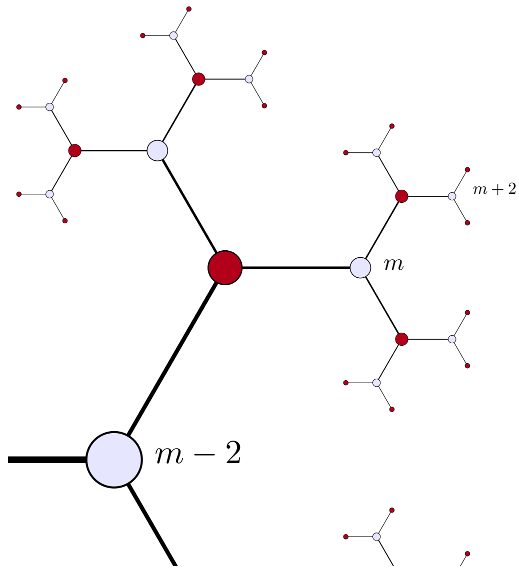
The principal result about the Hecke algebra is:

Proposition 4.1. *The Hecke algebra is generated by T_1.*

In particular, it is a commutative ring.

Proof. The T_m are a basis of the algebra, so it suffices to show that they are in the ring generated by $T = T_1$.

Lemma 4.2. *Among the nodes at distance two from ν_m for $n > 0$ are q^2 at distance $m+2$ from ν_0, $(q-1)$ at distance m, and 1 at distance $m-2$.*



Proof of the Lemma. From the picture. ∎

Therefore

$$T \circ T_m = q^2 T_{m+1} + (q-1) T_m + T_{m-1}, \quad ,$$

from which an induction argument concludes. ∎

These operators commute with the geometric action of G on the orbit. There is a dual action on functions on the nodes. If F takes ν to $\sum c_i \nu_i$ then

$$F^* f(\nu) = \sum c_i f(\nu_i) .$$

I have already mentioned unramified principal series as a source of unramified representations of reductive groups. We shall see later what happens more specifically for $G = \mathrm{SL}_2(\mathfrak{k})$. But there is another simple way to obtain unramified representations in this case. The group G acts on the nodes in the orbit of ν_0 in the tree $\mathfrak{X}$. It also acts on functions on $\mathfrak{X}$ by the left regular representation:

$$L_g f(\nu) = f\big(g^{-1}(\nu)\big) .$$

Let $T = T_1$. Since G commutes with T, if λ is any complex number then the space V_λ of eigenfunctions f on the orbit with eigenvalue λ—that of f with $T^* f = \lambda f$—is stable under G.

Proposition 4.3. *The representation of G on V_λ is admissible, and V^K has dimension* 1.

Proof. I'll start with the proof that the dimension of V^K is one, because the basic idea is the same as that involved in proving admissibility, but avoids technical complications.

Suppose that φ is fixed by K. Because of the Cartan decomposition $G = KA^{++}K$ the function φ takes a common value φ_m on all the nodes at distance $2m$ from ν_0.

(1) Because ν_0 has $q(q+1)$ neighbours at distance 2, and $T\varphi = \lambda\varphi$

$$\lambda \varphi_0 = q(q+1)\varphi_1 .$$

(2) For $m > 1$, by Lemma 4.2,

$$\lambda \varphi_m = \varphi_{m-1} + (q-1)\varphi_m + q^2 \varphi_{m+1} .$$

In other words, φ_m satisfies the difference equation

$$q^2\varphi_{m+1} - (\lambda - q + 1)\varphi_m + \varphi_{m-1} = 0$$

for $m > 0$ together with the initial condition

$$\varphi_1 = \frac{\lambda}{q(q+1)}\,\varphi_0\,.$$

If for convenience I set

$$q\mu = \lambda - q + 1, \quad \lambda = q\mu + q - 1\,,$$

then the difference equation reads

$$\varphi_{m+1} - \frac{\mu\varphi_m}{q} + \frac{\varphi_{m-1}}{q^2} = 0\,.$$

There is a well known formula for the solution of a difference equation, setting $\varphi_m = \alpha^m$. Plugging into the equation, we see that α must be a root of

$$x^2 - \frac{\mu}{q}x + \frac{1}{q^2} = 0\,.$$

• If this equation has distinct roots α, β, then the general solution is of the form $c\alpha^m + d\beta^m$. Set $\alpha = z/q$, $\beta = z^{-1}/q$ where $z + z^{-1} = \mu$, so now

$$\lambda = q(z + z^{-1} + 1) - 1\,.$$

This makes the solution

$$\varphi_m = c\left(\frac{z}{q}\right)^m + d\left(\frac{z^{-1}}{q}\right)^m$$

for constants c, d satisfying the initial conditions (1).

• The roots are equal when $\mu = \pm 2$, in which case $\alpha = \pm 1/q$ is a root. The solutions are linear combinations of α^m and $m\alpha^m$.

In all cases, there is a unique function φ_m satisfying the difference equation with a given value of φ_0, and proportional to φ_0. Therefore the representation V_λ is unramified and V_λ^K has dimension one.

If $\varphi_0 = 1$, then after a little bit of work we get for all m

$$\varphi_m = \frac{q^{-m}}{1+1/q}\left(\left(\frac{1-q^{-1}z^{-1}}{1-z^{-1}}\right)z^m + \left(\frac{1-q^{-1}z}{1-z}\right)z^{-m}\right)$$

as long as $z \neq 1$, and some non-trivial linear combination of $1/q^m$ and m/q^m when $z = 1$. So not only is the space of functions fixed by K of dimension 1, but we know exactly what the functions in the space are. This can be checked. If $z = q$ the representation is on the space of functions φ such that $q(q+1)\varphi(\nu)$ is the sum of the values of φ at the nodes at distance 2 from ν. This contains the constants, and we get $\varphi_m \equiv 1$.

The proof of admissibility is a variation on this. Functions fixed by K_r are determined by their restriction to the ball of fixed points of K_r. Beyond that ball they satisfy difference conditions with initial conditions determined by the values on that ball. ▯

The operator T acts by λ on V_λ. From the induction relationship between T and the T_m on can deduce that it has to act by a constant λ_m. It is immediate that $\lambda_0 = 1$ and $\lambda_m = q^{2m-1}(q+1)\,\varphi_m$ for $m > 0$. This leads to:

Corollary 4.4. *For $m > 0$ we have*

$$\lambda_m = q^m(z^m + z^{m-1} + \cdots + z^m) = q^{m-1}(z^{m-1} + z^{m-2} + \cdots +_m z^{-(m-1)}\,.$$

Proof. Set $x = \sqrt{z}$. Then

$$\begin{aligned}
&\left(\frac{1-q^{-1}z^{-1}}{1-z^{-1}}\right)z^m + \left(\frac{1-q^{-1}z}{1-z}\right)z^{-m} \\
&\qquad = \left(\frac{1-q^{-1}x^{-2}}{1-x^{-2}}\right)x^{2m} + \left(\frac{1-q^{-1}x^{2}}{1-x^{2}}\right)x^{-2m} \\
&\qquad = \left(\frac{x-q^{-1}x^{-1}}{x-x^{-1}}\right)x^{2m} + \left(\frac{x^{-1}-q^{-1}x}{x^{-1}-x}\right)x^{-2m} \\
&\qquad = \frac{\big(x^{2m+1}-x^{-(2m+1)}\big) - q^{-1}\big(x^{2m-1}-x^{-(2m-1)}\big)}{x-x^{-1}} \\
&\qquad = (x^{2m} + x^{(2m-2)} + \cdots + x^{-2m}) - q^{-1}(x^{2m-2} + \cdots + x^{-(2m-2)}) \\
&\qquad = (z^m + z^{m-1} + \cdots + z^{-m}) - q^{-1}(z^{m-1} + \cdots + z^{-(m-1)})\,,
\end{aligned}$$

from which the claim follows immediately. ∎

The apparent relationship with the character formula for finite-dimensional representations of the complex group $\mathrm{PGL}_2(\mathbb{C})$ is not an accident (see [Kato:1985]).

There is another way to understand the Hecke operators I have introduced here. First of all, the Hecke algebra acts on the K-fixed vectors in any admissible representation:

$$\pi(f)v = \int_G f(g)\pi(g)v\,dg\,.$$

Let (π, V) be an irreducible unramified admissible representation of G, $\widetilde{V}$ its dual. Since the Hecke algebra is commutative, we may choose in $\widetilde{V}$ a non-zero eigenvector for it. Say $\widetilde{\pi}(T)\widetilde{v} = \lambda\widetilde{v}$. The map taking v in V to

$$\big\langle \widetilde{\pi}(g)\widetilde{v}, v\big\rangle$$

is then a G-covariant embedding of V into V_λ.

5. The principal series

As I have already mentioned earlier, there is a second construction of unramified representations that relates more directly to Langlands' introduction of the L-group.

Let

$$\begin{aligned}
G &= \mathrm{SL}_2(\mathfrak{k}) \\
K &= \mathrm{SL}_2(\mathfrak{o}) \\
P &= \text{group of upper triangular matrices in } G\,.
\end{aligned}$$

If

$$\chi\colon P \longrightarrow \mathbb{C}^\times, \quad \begin{bmatrix} a & x \\ 0 & 1/a \end{bmatrix} \longmapsto |a|^s$$

is an unramified character of P then the corresponding principal series representation is by right multiplication on the space

$$I_\chi = \left\{ f \in C^\infty(G) \,|\, \big| f(pg) = \chi(p)\delta_P^{1/2}(p)f(g) \text{ for all } p \in P, g \in G \right\}.$$

Here

$$\delta_P \colon P \longrightarrow \mathbb{R}^\times, \quad p \longmapsto \big|\det \mathrm{Ad}_{\mathfrak{n}}(p)\big|$$

is the modulus character of the non-unimodular group P. This normalization factor is chosen so that I_χ is unitary if χ is.

Since $G = PK$, the space I_χ^K has dimension one, and may be identified with the space of scalars on K. The admissible dual of I_χ is $I_{\chi^{-1}}$. The relationship with the construction of unramified representations in the last section is that if $\widetilde{v}$ is the function in $I_{\chi^{-1}}^K$ whose value at 1 is 1, the function $\langle \pi(g)\widetilde{v}, v\rangle$ gives a map from I_χ to the space of functions on G/K, which may be identified with functions on even nodes of the tree. The relationship associates the unramified character χ to the with point $z = |\varpi|^s = q^{-s}$ in $\mathbb{C}^\times$.

By the principal divisor theorem, the Hecke algebra has as basis the characteristic functions $\tau_m = f_{K\omega^m K}$ of the double cosets

$$K \begin{bmatrix} 1/\varpi^m & 0 \\ 0 & \varpi^m \end{bmatrix} K \quad (m \geq 0).$$

The Hecke algebra acts on I_χ^K by scalars. The main result of the previous section is that if $z = q^{-s}$ then τ_m for $m > 0$ acts as multiplication by

$$\tau_m^\vee(\chi) = q^m(z^m + z^{m-1} + \cdots + z^{-m}) - q^{m-1}(z^{m-1} + \cdots + z^{m-1}).$$

This is the simplest example of Macdonald's formula for the spherical function, since the Satake transform and the spherical function are almost the same thing. It could been easily predicted that this would be invariant under $z \mapsto 1/z$, since I_χ and $I_{\chi^{-1}}$ are isomorphic. Since ${}^L G$ is the direct product of $\mathrm{PGL}_2(\mathbb{C})$ and $\langle \mathfrak{F} \rangle$ when $G = \mathrm{SL}_2(\mathfrak{k})$, this is one of the simplest cases of Langlands' observation that unramified representations of G are parametrized by certain conjugacy classes in the L-group of G. Here, z corresponds to the image of

$$\begin{bmatrix} z & 0 \\ 0 & 1 \end{bmatrix}$$

Now suppose that $\mathfrak{l}/\mathfrak{k}$ is the unramified quadratic extension of $\mathfrak{k}$. Let $\mathrm{sgn} = \mathrm{sgn}_{\mathfrak{l}/\mathfrak{k}}$ be the non-trivial character of $\mathfrak{k}^\times / N\mathfrak{l}^\times$. As a special case of the results above, if $\chi = \mathrm{sgn}$ then $z = -1$ and we get

$$\tau_m^\vee(\mathrm{sgn}) = \begin{cases} 1 & \text{if } m = 0 \\ (-1)^m(q+1)q^{m-1} & \text{otherwise.} \end{cases}$$

If we choose a basis of $\mathfrak{l}$ as a vector space over $\mathfrak{k}$, we get an embedding of $\mathfrak{l}^\times$ into $\mathrm{GL}_2(\mathfrak{k})$, and in particular of $\mathfrak{o}_\mathfrak{l}^\times$ into the maximal compact subgroup $\mathrm{GL}_2(\mathfrak{o})$ and of the compact group $N_{\mathfrak{l}/\mathfrak{k}}^1$ into $\mathrm{SL}_2(\mathfrak{o})$. As we'll see later in detail, if we conjugate by an element of g whose determinant is not in $N\mathfrak{l}^\times$ we get a conjugate copy of $N_{\mathfrak{l}/\mathfrak{k}}^1$ in another maximal compact subgroup of $\mathrm{SL}_2(\mathfrak{k})$, one not conjugate to it inside $\mathrm{SL}_2(\mathfrak{k})$ but only conjugate by an element of the automorphism group $\mathrm{PGL}_2(\mathfrak{k})$, or inside $\mathrm{SL}_2(\overline{\mathfrak{k}})$. Corresponding elements of the two copies of $N_{\mathfrak{l}/\mathfrak{k}}^1$ are stably conjugate.

To fix things, I choose

$$\iota = \begin{bmatrix} 1 & 0 \\ 0 & \varpi \end{bmatrix}$$

and let ι be also the map taking x to $x^\iota = \iota x \iota^{-1}$.

Let H be the algebraic group whose $\mathfrak{k}$-rational points are $N^1_{\mathfrak{l}/\mathfrak{k}}$. This is a torus that splits, and becomes isomorphic to $\mathbb{G}_m$, over $\mathfrak{l}$. The Galois action on the character group $\mathbb{Z}$ is multiplication by -1, and we have an exact sequence of Galois modules

$$1 \longrightarrow H(\mathfrak{l}) = \mathfrak{l}^\times \longrightarrow R(\mathfrak{l}) = \mathfrak{l}^\times \times \mathfrak{l}^\times \longrightarrow \mathbb{G}_m(\mathfrak{l}) = \mathfrak{l}^\times \longrightarrow 1$$

where R is the group obtained from $\mathbb{G}_m$ by **restriction of scalars** from $\mathfrak{l}$ to $\mathfrak{k}$. The first map takes x to $(x, 1/x)$, the second takes (x, y) to xy. The Frobenius automorphism acts by -1 on the first term, by swap on the second, and trivially on the third. This short exact sequence gives rise to a long exact sequence of cohomology

$$1 \longrightarrow N^1_{\mathfrak{l}/\mathfrak{k}} \longrightarrow \mathfrak{l}^\times \longrightarrow \mathfrak{k}^\times \longrightarrow H^1\big(\mathcal{G}, H(\mathfrak{l})\big) \longrightarrow H^1\big(\mathcal{G}, R(\mathfrak{l})\big) = 1 \longrightarrow \dots$$

that identifies $H^1\big(\mathcal{G}, H(\mathfrak{l})\big)$ with $\mathfrak{k}^\times / N\mathfrak{l}^\times$.

The L-group ${}^LH$ of H is the semi-direct product of $\widehat{H} = \mathbb{C}^\times$ with the quadratic Galois group $\mathcal{G}$ of order two, with the Frobenius acting by $z \mapsto z^{-1}$ on $\widehat{H}$. The L-group ${}^LG$ of SL_2 is the direct product of $\mathrm{PGL}_2(\mathbb{C})$ and $\langle \mathfrak{F} \rangle$. The maximal torus of $\widehat{G}$ is the group of diagonal matrices in $\mathrm{GL}_2(\mathbb{C})$ modulo scalars. There is an embedding of ${}^LH$ into ${}^LG$, taking

$$z \times 1 \longmapsto \iota(z) = \begin{bmatrix} z & 0 \\ 0 & 1 \end{bmatrix}, \quad 1 \times \sigma \longmapsto w \times \sigma$$

where

$$w = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

This identifies H with an endoscopic group for G, because ${}^LH$ is the centralizer in $\mathrm{PGL}_2(\mathbb{C})$ of

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

A map of L-groups, in terms of Langlands' functoriality, gives rise to a map of conjugacy classes in the Frobenius coset, from $\widehat{H} \times \mathfrak{F}$ to $\widehat{G} \rtimes \mathfrak{F}$, and thence to an association of unramified representations.

The matrix w is conjugate in $\mathrm{PGL}_2(\mathbb{C})$ to the diagonal matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Therefore, in terms of Langlands' functoriality, the trivial character of H, which is its only unramified character, gives rise to the unitary principal series representation of $\mathrm{SL}_2(\mathfrak{k})$ corresponding to the quadratic character $\mathrm{sgn}_{\mathfrak{l}/\mathfrak{k}}$ of $\mathfrak{k}^\times / N\mathfrak{l}^\times$. As we'll see in the next section, this representation splits into a direct sum of two pieces, one with a one-dimensional subspace of vectors fixed by K, the other with vectors fixed by the 'twin' maximal compact subgroup K^ι. In fact, ι takes one component of the reducible representation into the other. This decomposition relates more interestingly to what Langlands calls endoscopy of which the Fundamental Lemma is a part. What happens is that the difference between the characters of the two summands has support on the conjugates of the embedded torus $H(\mathfrak{k})$, while the sum has support on the split torus.

The Hecke algebra of H has dimension 1, with generator f_H, since $N^1_{\mathfrak{l}/\mathfrak{k}}$ is compact. The embedding of ${}^LH$ into ${}^LG$ gives rise to a map back from the Hecke algebra of G to multiples of f_H, taking

$$f \longmapsto f^\vee(\mathrm{sgn})\, f_H .$$

6. Intertwining operators

Let

$$w = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Formally, we can define intertwining operators from I_χ to I_χ as

$$T_\chi f(g) = \int_N f(wng)\, dn\,.$$

It can be checked easily that if the integral converges, then T is a G-equivariant map from $I(\chi)$ to $I(\chi^{-1})$.

Proposition 6.1. *The integral for T_χ converges for* $\mathrm{RE}(s) > 0$, *and extends meromorphically to all of* $\mathbb{C}$.

Proof. It is not difficult, but the most intelligible approach breaks it up into small steps. Replacing f by $R_g f$, we have to examine only at the integral

$$\langle \Lambda_\chi, f\rangle = \int_N f(wn)\, dn\,.$$

Lemma 6.2. (Bruhat decomposition) *The group G is the disjoint union of P and PwN.*

Proof. Explicitly, if $c \neq 0$ then we have a unique factorization

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1/c & a \\ 0 & c \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & d/c \\ 0 & 1 \end{bmatrix}.$$

Of course one can prove the Lemma by verifying this equation, but it is probably worthwhile pointing out how it can be derived. The group G acts on the right on row vectors, and P is the stabilizer of the line $[0, z]$. Thus it suffices to find for every vector $[x, y]$ a matrix in wN taking some $[0, z]$ to $[x, y]$. ∎

The following is the special case of this that we shall need often.

Corollary 6.3. *For $x \neq 0$*

$$\begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix} = \begin{bmatrix} 1/x & 1 \\ 0 & x \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1/x \\ 0 & 1 \end{bmatrix}.$$

This can be rewritten as

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1/x & -1 \\ 0 & x \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1/x & 1 \end{bmatrix}.$$

I can now prove Proposition 6.1. Any function in $\mathrm{Ind}(\chi)$ must be locally constant on K in the neighbourhood of 1. From the second version of the formula in Corollary 6.3, the integral $\langle \Lambda_\chi, f\rangle$ is therefore a finite sum plus some infinite sum

$$\int_{|x|\ge q^n} |x|^{-s-1}\, dx = \sum_{m\ge n} (q^m - q^{m-1}) q^{-ms-m} = (1-1/q)z^n(1+z+z^2+\cdots) = \frac{(1-1/q)z^n}{1-z}$$

as long as $|z| < 1$, where $z = q^{-s}$. ∎

Proposition 6.4. *We have*

$$T_w \varphi_{\chi,K} = \left(\frac{1 - z/q}{1 - z} \right) \varphi_{\chi^{-1},K}$$

$$T_w \varphi_{\chi,K_*} = z \left(\frac{1 - z/q}{1 - z} \right) \varphi_{\chi^{-1},K_*} \,.$$

Proof. The operator T_w takes $\varphi_{\chi,K}$ into a multiple of itself, so it suffices to evaluate

$$T_w \varphi_{\chi,K}(1) = \langle \Lambda_\chi, \varphi_{\chi,K} \rangle = \int_{|x| \le 1} \varphi_{\chi,K}(w n_x)\, dx + \int_{|x| \ge q} \varphi_{\chi,K}(w n_x)\, dx \,,$$

where

$$n_x = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} .$$

But by the calculation just made this is

$$1 + \left(\frac{(1 - 1/q) z}{1 - z} \right) = \frac{1 - z/q}{1 - z} \,.$$

The second formula can be derived directly from the first. Express

$$\varphi_*(g) = \varphi(\omega^{-1} g \omega) \;.$$

where $K_* = \omega K \omega^{-1}$. Then

$$\langle \Lambda_w, K_* \rangle = \int_N \varphi(\omega^{-1} w \omega^{-1} \cdot \omega n \omega)\, dn \,.$$

But

$$\omega w \omega^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & \varpi \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1/\varpi \end{bmatrix} = \begin{bmatrix} 0 & -\varpi \\ 1/\varpi & 0 \end{bmatrix} = \begin{bmatrix} \varpi & 0 \\ 0 & 1/\varpi \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

so this becomes

$$z q^{-1} \int_N \varphi(w n)\, d\, \omega n \omega^{-1} = z q^{-1} \cdot q \langle \Lambda_w, \varphi \rangle \,. \quad \square$$

This calculation has the great advantage that it works for other unramified groups.

Part III. Conjugacy and stable conjugacy

7. Conjugation in SL(2)

Let $\overline{\mathfrak{k}}$ be the separable closure of $\mathfrak{k}$. Two semi-simple (diagonalizable) elements of $\mathrm{SL}_2(\overline{\mathfrak{k}})$ are conjugate if and only if they have the same characteristic polynomial $x^2 - \tau x + 1$, where τ is the trace. A conjugacy class is called **$\mathfrak{k}$-rational** if its trace lies in $\mathfrak{k}$. This is equivalent to the condition that the class be Galois-invariant.

The following is elementary in the case at hand, but is a special case of a much more difficult result of [Steinberg:1965] about simply connected semi-simple groups.

Lemma 7.1. *Every rational semi-simple conjugacy class in* $\mathrm{SL}_2(\mathfrak{k})$ *contains a rational element.*

Proof. Suppose τ in $\mathfrak{k}$, and let α be a root of the equation $x^2 - \tau x + 1 = 0$. If α is rational, the conjugacy class we want is the diagonal matrix with entries $\alpha^{\pm 1}$. Otherwise α generates a quadratic extension $\mathfrak{l}$ of $\mathfrak{k}$ with basis 1, α. Elements of $\mathfrak{l}$ act by multiplication on $\mathfrak{l} = \mathfrak{k}^2$, and since

$$\begin{aligned} \alpha \cdot 1 &= \alpha \\ \alpha \cdot \alpha &= -1 + \tau\alpha \end{aligned}$$

the element α corresponds to the matrix

$$\begin{bmatrix} 0 & -1 \\ 1 & \tau \end{bmatrix}$$

with trace τ. ∎

Any rational conjugacy class is stable under conjugation by $\mathrm{SL}_2(\mathfrak{k})$. If the conjugacy class contains elements which are diagonal matrices with entries in $\mathfrak{k}$—if the conjugacy class is **split**—it is easy to see that the class is in fact a single orbit of $\mathrm{SL}_2(\mathfrak{k})$. A semi-simple element of $\mathrm{SL}_2(\mathfrak{k})$ coming from the quadratic extension $\mathfrak{l}/\mathfrak{k}$ will be diagonalizable in $\mathrm{SL}_2(\mathfrak{l})$. This reasoning applied to $\mathfrak{l}$ implies:

Lemma 7.2. *If α is a rational element of* $\mathrm{SL}_2(\mathfrak{k})$ *diagonalizable over the quadratic extension $\mathfrak{l}$, then two elements of its conjugacy class are conjugate in* $\mathrm{SL}_2(\overline{\mathfrak{k}})$ *if and only if they are conjugate in* $\mathrm{SL}_2(\mathfrak{l})$.

Two elements of $\mathrm{SL}_2(\mathfrak{k})$ are said to be **stably conjugate** if they are conjugate in $\mathrm{SL}_2(\overline{\mathfrak{k}})$. The Lemma says that questions of stable conjugacy for SL_2 reduce to questions of conjugacy in quadratic extensions.

Proposition 7.3. *Any non-split, semi-simple, stable conjugacy class of* $\mathrm{SL}_2(\mathfrak{k})$ *consists of exactly two* $\mathrm{SL}_2(\mathfrak{k})$*-orbits.*

Proof. I am going to examine the question by techniques that generalize well to other groups. I shall therefore take up from scratch the question

> *Suppose*
>
> $$\alpha = \begin{bmatrix} a & 0 \\ 0 & 1/a \end{bmatrix} \quad (a \in \mathfrak{l}^\times).$$
>
> *Under what circumstances does the conjugacy class of α in* $\mathrm{SL}_2(\mathfrak{l})$ *contain elements of* $\mathrm{SL}_2(\mathfrak{k})$*, and if it does, into how many orbits of* $\mathrm{SL}_2(\mathfrak{k})$ *does it break up into?*

Let $\mathcal{G}$ be the Galois group of $\mathfrak{l}/\mathfrak{k}$. We may assume that $a \neq \pm 1$, since otherwise the questions are trivial. For g in $\mathrm{SL}_2(\mathfrak{l})$ the matrix $\gamma = g^{-1}\alpha g$ will be in $\mathrm{SL}_2(\mathfrak{k})$ if and only if $\overline{\gamma} = \gamma$, or more precisely

$$\overline{g}^{-1}\overline{\alpha}\,\overline{g} = g^{-1}\alpha g, \quad (\overline{g}/g)\,\alpha(\overline{g}/g)^{-1} = \overline{\alpha}\,.$$

Since $a \neq \pm 1$, this happens if and only if $\overline{g}/g$ lies in the normalizer of the diagonal matrices in $\mathrm{SL}_2(\mathfrak{l})$. If it is itself diagonal then α must be in $\mathfrak{k}$. This is a very simple case to deal with, as I have already said—the split conjugacy classes are the same as the stable conjugacy classes, and each contains among the diagonal matrices precisely α and α^{-1}, which are conjugate by any non-trivial element

$$w_y = \begin{bmatrix} 0 & -y \\ 1/y & 0 \end{bmatrix}$$

of the normalizer.

So we are primarily interested in the case when $h = \overline{g}/g$ represents the non-trivial element of the Weyl group. In this case, we deduce $\overline{\alpha} = \alpha^{-1}$, or $a\overline{a} = 1$. (Which of course we knew anyway. Just checking.) So

$$h = \overline{g}/g = \begin{bmatrix} 0 & x \\ -1/x & 0 \end{bmatrix}$$

for some $x \neq 0$. Since

$$\overline{h}h = (g/\overline{g})(\overline{g}/g) = 1\,.$$

and also

$$\overline{h}h = \begin{bmatrix} 0 & \overline{x} \\ -1/\overline{x} & 0 \end{bmatrix} \begin{bmatrix} 0 & x \\ -1/x & 0 \end{bmatrix} = \begin{bmatrix} -\overline{x}/x & 0 \\ 0 & -\overline{x}/x \end{bmatrix},$$

we must have $\overline{x}/x = -1$. There always are such x, since all elements of $N^1_{\mathfrak{l}/\mathfrak{k}}$, and in particular -1, are Galois cocycles of $\mathfrak{l}^\times$, and the $\overline{x}/x$ are the coboundaries, and Hilbert's Theorem 90 says $H^1(\mathcal{G}, \mathfrak{l}^\times) = 1$.

Furthermore, the short exact sequence defining $\mathrm{SL}_2(\mathfrak{l})$ as the kernel of the determinant map gives us a long exact sequence, which since $H^1\big(\mathcal{G}, \mathrm{GL}_2(\mathfrak{l})\big) = 1$ tells us that $H^1\big(\mathcal{G}, \mathrm{SL}_2(\mathfrak{l})\big) = 1$, too. (This is the simplest case of a result proved by Kneser through a case-by-case argument and by Bruhat and Tits more elegantly—that $H^1\big(\mathcal{G}(\overline{\mathfrak{k}}/\mathfrak{k}), G(\overline{\mathfrak{k}})\big) = 1$ for every semi-simple, simply connected G.) So for every acceptable x there exists an acceptable g. We conclude that for every a with $a\overline{a} = 1$ the conjugacy class of α is rational over F and contains a rational element in $\mathrm{SL}_2(\mathfrak{k})$.

So far, we have only recovered a result we already knew from more elementary considerations. But now we ask, how do these elements partition according to conjugacy in $\mathrm{SL}_2(\mathfrak{k})$?

For x with $\overline{x}/x = -1$, let Γ_x be the set of g in $\mathrm{SL}_2(\mathfrak{l})$ such that

$$\overline{g}g^{-1} = \begin{bmatrix} 0 & x \\ -1/x & 0 \end{bmatrix}.$$

Under right multiplication, this is a principal homogeneous space for $\mathrm{SL}_2(\mathfrak{k})$. Let Γ be the union of all the Γ_x, on which $\mathrm{SL}_2(\mathfrak{k})$ acts by right multiplication.

Now suppose we are given a conjugate γ of α in $\mathrm{SL}_2(\mathfrak{k})$. Choose g in Γ such that $g^{-1}\alpha g = \gamma$, and let x correspond to $\overline{g}/g$. The element g is determined only up to a factor β for some diagonal matrix

$$\beta = \begin{bmatrix} b & 0 \\ 0 & 1/b \end{bmatrix},$$

and an easy calculation shows that βg corresponds to $\overline{b}bx$. In this way we get a well defined map from those elements of $\mathrm{SL}(\mathfrak{k})$ conjugate to α onto the quotient of $\{x \,|\, \overline{x}/x = -1\}$ by $N\mathfrak{l}^\times$, which is non-canonically in bijection with $\mathfrak{k}^\times/N\mathfrak{l}^\times$, a group of order two (in accord with local class field theory). ▯

In the rest of this section, fix a quadratic extension $\mathfrak{l}/\mathfrak{k}$. Assume given an embedding of $N^1_{\mathfrak{l}/\mathfrak{k}}$ into $\mathrm{SL}_2(\mathfrak{k})$, and let $T_\mathfrak{l}$ be its image.

There happen to be two ways to think of stable conjugacy in $\mathrm{SL}_2(\mathfrak{k})$. The group $\mathrm{PGL}_2(\mathfrak{k})$ conjugates semi-simple elements and it can be used to analyze the same phenomena.

Proposition 7.4. *Suppose $\gamma \neq \pm I$ to be in $T_{\mathfrak{l}}$. If g is in $\mathrm{GL}_2(\mathfrak{k})$, then $g^{-1}\gamma g$ is conjugate in $\mathrm{SL}_2(\mathfrak{k})$ to γ if and only if $\det g$ lies in $N\mathfrak{l}^\times$.*

In the next result, let

$$\iota = \begin{bmatrix} 1 & 0 \\ 0 & \varpi \end{bmatrix}.$$

Corollary 7.5. *If $\mathfrak{l}$ is unramified, the torus $\iota\, T_{\mathfrak{l}}\, \iota^{-1}$ is not conjugate to $T_{\mathfrak{l}}$ in $\mathrm{SL}_2(\mathfrak{k})$.*

I leave this as an exercise. Note that $\det(\iota)$ is not in $N\mathfrak{l}^\times$.

How $\mathrm{PGL}_2(\mathfrak{k})$ acts on conjugacy classes of unramified tori is a special case of a result of [Debacker:2006] about unramified tori and the Bruhat-Tits building.

I finish this section with a natural question. If α is semi-simple, then α^{-1} is in its stable conjugacy class. When is it actually in the same conjugacy class?

Proposition 7.6. *Suppose $\gamma \neq \pm I$ to be in $T_{\mathfrak{l}}$. It is conjugate in $\mathrm{SL}_2(\mathfrak{k})$ to γ^{-1} if and only if -1 lies in $N\mathfrak{l}^\times$.*

There is a trivial way to see this, since we are in odd characteristic and may assume $\mathfrak{l} = \mathfrak{k}(\sqrt{D})$. The element

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

conjugates $a + b\sqrt{D}$ to $a - b\sqrt{D}$, using the explicit embedding of $T_{\mathfrak{l}}$ into $\mathrm{GL}_2(\mathfrak{k})$. Presumably something as simple can be made to work always, but as I have said, I prefer again a technique not restricted to SL_2.

Proof. Suppose

$$h\gamma h^{-1} = \gamma^{-1}$$

where h lies in $\mathrm{SL}_2(\mathfrak{k})$ and γ in $T_{\mathfrak{l}}$. Since γ is $\mathfrak{k}$-rational, we have

$$\gamma = g^{-1}\alpha g$$

for some g with

$$\overline{g}/g = \begin{bmatrix} 0 & x \\ -1/x & 0 \end{bmatrix}, \quad \overline{x}/x = -1\,.$$

But now

$$\begin{aligned} hg^{-1}\alpha g h^{-1} &= g^{-1}\alpha^{-1} g \\ (ghg^{-1})\alpha(ghg^{-1})^{-1} &= \alpha^{-1} \\ ghg^{-1} &= \begin{bmatrix} 0 & y \\ -1/y & 0 \end{bmatrix} \\ h &= g^{-1}\begin{bmatrix} 0 & y \\ -1/y & 0 \end{bmatrix} g \end{aligned}$$

for some $y \neq 0$. Hence, since h is $\mathfrak{k}$-rational,

$$\begin{aligned} g^{-1}\begin{bmatrix} 0 & y \\ -1/y & 0 \end{bmatrix} g &= \overline{g}^{-1}\begin{bmatrix} 0 & \overline{y} \\ -1/\overline{y} & 0 \end{bmatrix}\overline{g} \\ (\overline{g}g^{-1})\begin{bmatrix} 0 & y \\ -1/y & 0 \end{bmatrix}(\overline{g}g^{-1})^{-1} &= \begin{bmatrix} 0 & \overline{y} \\ -1/\overline{y} & 0 \end{bmatrix}. \end{aligned}$$

But we have an explicit expression for $\overline{g}g^{-1}$, so we get

$$\begin{bmatrix} 0 & x \\ -1/x & 0 \end{bmatrix} \begin{bmatrix} 0 & y \\ -1/y & 0 \end{bmatrix} \begin{bmatrix} 0 & -x \\ 1/x & 0 \end{bmatrix} = \begin{bmatrix} 0 & \overline{y} \\ -1/\overline{y} & 0 \end{bmatrix}$$

and then $-(\overline{x}x/\overline{y}y) = 1$. The reasoning can also be reversed. ▯

Part IV. Orbital integrals and the Fundamental Lemma

8. Orbital integrals

I have already mentioned that there is a relation between harmonic analysis on a $\mathfrak{p}$-adic reductive group G and on certain smaller groups, and I have mentioned the example of the characters of admissible representations. There is also a second kind of conjugation-invariant distribution on G, the **orbital integrals** associated to conjugacy classes. I'll look just at the simplest case. Suppose γ to be a regular semi-simple element of G whose centralizer G_γ in G is a compact torus. Assign G_γ to have total Haar measure 1. If f is a smooth function of compact support on G then the function $F(g) = f(g^{-1}\gamma g)$ has compact support on the orbit of γ under conjugation in G, because that orbit is closed. The associated orbital integral over the conjugation class is the distribution (linear function on $C_c^\infty(G)$) taking f to

$$\langle O_{\gamma,G}, f\rangle = \int_{G_\gamma\backslash G} f(g^{-1}\gamma g)\, dg\,,$$

which is manifestly conjugation-invariant. As γ approaches the identity in G, or in fact approaches any conjugation class for which the centralizer is not a torus, this orbital integral blows up but, as we'll see in some examples later on, it turns out that multiplying it by a suitable factor tames it.

Orbital integrals have a simple interpretation. Suppose K to be any compact open subgroup of G, x_0 the coset K of the discrete set G/K. I want to define a function on G/K which generalizes the notion of distance on the tree of $\mathrm{SL}_2(\mathfrak{k})$.

Lemma 8.1. *There exists a unique function $[y\colon x]$ from $G/K \times G/K$ to $K\backslash G/K = G/\!/K$ such that*

(a) $[g(y)\colon g(x)] = [y\colon x]$;
(b) $[y\colon x_0] = KhK$ *if* $y \in KhK$.

Proof. If x and y are two points of G/K, let g be such that $x = gx_0$ or, equivalently, $g^{-1}x = x_0$. Define $[y\colon x] = KhK$ if $g^{-1}y \in Khx_0$. ▯

Because I think notation should reflect meaning closely, I'll usually write $[y\colon x] = [KhK\colon K]$ instead of KhK. Also, I'll continue to write $[y : x] = m$ if x and y are nodes of the tree of SL_2 at distance m.

Lemma 8.2. *If f is the characteristic function of KhK and K is assigned measure 1 then*

$$\int_{G_\gamma\backslash G} f(g^{-1}\gamma g)\, dg$$

is equal to the number of points x in G/K with $[\gamma(x)\colon x] = [KhK\colon K]$.

One special case of this result is when $h = 1$, in which case the orbital integral is the number of points on G/K fixed by γ.

Proof. With this normalization of measures, for F on $G_\gamma\backslash G/K$, and in particular for $F(g) = f(g^{-1}\gamma g)$, we have

$$\int_{G_\gamma\backslash G} F(g)\, dg = \sum_{G/K} F(g)\,.$$

Furthermore, $g^{-1}\gamma g \in KhK$ if and only if $[\gamma\, gx_0\colon gx_0] = [KhK\colon K]$. ▯

The particular case we'll be interested in is that in which $G = \mathrm{SL}_2(\mathfrak{k})$, $h = \omega^m$, $K = \mathrm{SL}_2(\mathfrak{o})$. In this case G/K may be identified with the orbit of ν_0 in the tree of G, and I'll almost always write $[y\colon x] = 2m$ instead of $[y\colon x] = [\tau_m\colon \tau_0]$.

9. The Fundamental Lemma

The Fundamental Lemma is concerned with a very particular aspect of orbital integrals—how they behave with respect to the automorphism ι.

Recall that $H = N^1_{\mathfrak{l}/\mathfrak{k}}$ where $\mathfrak{l}$ is the unramified quadratic extension of $\mathfrak{k}$. I have mentioned that the embedding $\eta\colon {}^LH \hookrightarrow {}^LG$ is related to an identity of characters of representations. The Fundamental Lemma is about orbital integrals, which are dual, in a sense, to characters. For γ in $\mathfrak{l}^\times$, let

$$D(\gamma) = 1 - (\gamma/\overline{\gamma})\,.$$

Thus $D(\gamma) = 0$ if and only if γ lies in $\mathfrak{k}^\times$. In other words $D(\gamma) \neq 0$ if and only if $\mathrm{Ad}_{\mathfrak{g}}(\gamma)$ is not trivial, and in this case the element γ is said to be **regular**. In general $D(\gamma)$ measures how close $\mathrm{Ad}_{\mathfrak{g}}(\gamma)$ is to being trivial. There is another function of γ depending on this closeness:

$$\Delta(\gamma) = (-1)^n \ \text{ if } \ \big|D(\gamma)\big| = q^{-2n}\,.$$

In Langlands' papers, for example §I.4 of [Langlands:1979], this is usually written in the form

$$\mathrm{sgn}_{\mathfrak{l}/\mathfrak{k}}\left(\frac{\gamma - \overline{\gamma}}{\gamma_0 - \overline{\gamma}_0}\right)\,,$$

where γ_0 is a fixed element of $\mathfrak{o}_{\mathfrak{l}}^\times$ not congruent to 1 modulo $\mathfrak{p}$. The formula makes sense because the ratio lies in $\mathfrak{k}^\times$. Identify elements of $N^1_{\mathfrak{l}/\mathfrak{k}}$ with their images in $\mathrm{SL}_2(\mathfrak{o})$.

Proposition 9.1. (Fundamental Lemma) *For f in $\mathcal{H}(G/\!/K)$ and γ regular in $N^1_{\mathfrak{l}/\mathfrak{k}}$*

$$\Delta(\gamma)\,\big|D(\gamma)\big|^{1/2}\big\langle O_{\gamma,G} - O_{\gamma^\iota,G}, f\big\rangle = \big\langle O_{\gamma,H}, \eta^*_{G|H}(f)\big\rangle = f^\vee(\mathrm{sgn})\,.$$

I recall that $\eta^*_{G|H}(f)$ is the image of f in the Hecke algebra of H, and also that measures are normalized so that the measures of H and K are 1.

This result has much in common with observations made in the earlier discussion about Hecke's result. Something like this could have been predicted here because all unramified representations π of G except one have the property that $\pi^\iota \cong \pi$. The exception is the component π_+ of I_{sgn} containing I^K_{sgn}. In this case, the conjugate representation is the other component, the one with vectors fixed by K^ι. Thus it is to be expected that the left hand side be expressible in terms of $f^\vee(\mathrm{sgn})$.

This is only one of many similar results involving other quadratic extensions and other functions f. But it is the most important, since unramified representations and the Hecke algebra $\mathcal{H}(G/\!/K)$ play an important global role.

From now on, let the left hand side of this be $\Phi_\gamma(f)$. The Proposition can be broken usefully into two parts:

$$\begin{array}{lll} \mathrm{FL(a)} & \Phi_\gamma(f_K) & = \Delta(\gamma)\big|D(\gamma)\big|^{-1/2} \\ \mathrm{FL(b)} & \Phi_\gamma(f_{K\omega^m K}) & = \varphi_{\mathrm{sgn}}(f_{K\omega^m K})\cdot\Phi_\gamma(f_K)\,. \end{array}$$

A similar dichotomy also occurs in dealing with the Fundamental Lemma in the most general situation. One of the relatively early developments in the history of the Fundamental Lemma was the reduction by Hales to the apparently simpler case concerning only the identity elements of Hecke algebras (although his proof has nothing in common with what we shall see here, and is quite technical). But then this proved to be extremely difficult, although as we shall see that is not the case here.

The first step is to reformulate the Fundamental Lemma by making a change of variables in the second orbital integral. I may assume $f = f_{K\varpi^m K}$. So this integral is

$$\int_{H^\iota\backslash G} f_{K\varpi^m K}(g\gamma^\iota g)\, dg\,.$$

We may replace ι by ι^{-1}, since ι^2 amounts to conjugation by an element of $\mathrm{SL}_2(\mathfrak{k})$. But then we change variables by $z = x^\iota$ to make that second integral equal to

$$\int_{H\backslash G} f_{K^\iota\varpi^m K^\iota}(g^{-1}\gamma g)\, dg$$

According to Lemma 8.2, this is the number of points on the odd nodes x of the tree of SL_2 with $[\gamma(x)\colon x] = 2m$.

10. Counting fixed points

There are two orbits of the group $\mathrm{SL}_2(\mathfrak{k})$ among the nodes of the tree, that of ν_0, fixed by K, and that of ν_1, fixed by K^ι. Let ε be the function equal to 1 on the first group and -1 on the second, and let $\mathfrak{X}_\pm$ be those where $\varepsilon = \pm 1$. According to Lemma 8.2 and the expression at the edn of the last section for the second orbital integral in the Fundamental Lemma, the first claim now becomes the equation

$$\mathrm{FL(a')}\qquad \#\{x \in \mathfrak{X}_+ \mid \gamma(x) = x\} - \#\{x \in \mathfrak{X}_- \mid \gamma(x) = x\} = \#\mathfrak{X}_+^\gamma - \#\mathfrak{X}_-^\gamma = (-1)^n q^n$$

if $D(\gamma) = q^{-2n}$. The second claim reduces $\Phi_\gamma(f_{K\varpi^m K})$ to $\Phi_\gamma(f_K)$, becomes

$$\mathrm{FL(b')}\qquad \#\big\{x \in \mathfrak{X}_+ \,\big|\, [\gamma x\colon x] = 2m\big\} - \#\big\{x \in \mathfrak{X}_- \,\big|\, [\gamma x\colon x] = 2m\big\} = \tau_m^\vee(\mathrm{sgn})\big(\#\mathfrak{X}_+^\gamma - \#\mathfrak{X}_-^\gamma\big)\,.$$

I'll prove FL(a) first. I start with an observation about how the copy of $\mathfrak{o}_\mathfrak{l}^\times$ in K acts on the tree.

Proposition 10.1. *Suppose γ to be in $\mathfrak{o}_L^\times$, with $|\gamma - \overline{\gamma}|_\mathfrak{l} = q^{-2n}$. The nodes of the tree fixed by γ are precisely those at distance at most n from the root node.*

Proof. The points at distance n from the root node can be identified with the points of $\mathbb{P}^1(\mathfrak{o}_\mathfrak{k}/\mathfrak{p}_\mathfrak{k}^n)$, or the lines in $(\mathfrak{o}_\mathfrak{k}/\mathfrak{p}_\mathfrak{k}^n)^2 = \mathfrak{o}_\mathfrak{l}/\mathfrak{p}_\mathfrak{l}^n$. But this in turn may be identified with primitive points modulo scalar multiplication by units in $\mathfrak{o}_\mathfrak{k}$. Thus also as $\mathfrak{o}_\mathfrak{l}^\times/(1+\mathfrak{p}_\mathfrak{l}^n)\mathfrak{o}_\mathfrak{k}^\times$. The following concludes the proof:

Lemma 10.2. *For $\gamma \in \mathfrak{o}_\mathfrak{l}$, the following are equivalent:*

(a) $\gamma/\overline{\gamma} \equiv 1 \bmod \mathfrak{p}^n$;
(b) $\gamma \in \big(1 + \mathfrak{p}_\mathfrak{l}^n\big)\mathfrak{o}_\mathfrak{k}^\times$.

Proof. According to Hilbert's Theorem 90, the sequence

$$1 \to \mathfrak{k}_\mathfrak{k}^\times \to \mathfrak{l}_\mathfrak{k}^\times \to N_{\mathfrak{l}/\mathfrak{k}}^1 \to 1$$

in which the last map takes x to $x/\overline{x}$, is exact. Because $\mathfrak{l}/\mathfrak{k}$ in unramified the image of ϖ is 1, so this sequence is also exact:

$$1 \to \mathfrak{o}_\mathfrak{k}^\times \to \mathfrak{o}_\mathfrak{k}^\times \to N_{\mathfrak{l}/\mathfrak{k}}^1 \to 1\,.$$

It is then easy to show that so is each sequence of congruence subgroups

$$1 \to 1 + \mathfrak{p}_\mathfrak{k}^n \to 1 + \mathfrak{p}_\mathfrak{l}^n \to (1 + \mathfrak{p}_\mathfrak{l}^n) \cap N_{\mathfrak{l}/\mathfrak{k}}^1 \to 1\,. \;\square$$

The sum we are calculating in FL(a') is therefore

$$1 - (q+1) + (q+1)q - (q+1)q^2 + \cdots \pm (q+1)q^{n-1} = (-1)^n q^n ,$$

which proves FL(a').

One consequence of the Proposition is that $\mathfrak{X}^{\gamma}$ is convex. If x is any node of the tree, the path from x to ν_0 will enter $\mathfrak{X}^{\gamma}$ at some unique point $\rho(x)$, and it will never again exit $\mathfrak{X}^{\gamma}$. Thus $\rho(x) = x$ for x in $\mathfrak{X}^{\gamma}$. The map ρ is a retraction of the entire tree onto $\mathfrak{X}^{\gamma}$.

Another consequence is that we know very explicitly the possible local environments of points in $\mathfrak{X}^{\gamma}$. Before I summarize what these are, let me consider *a priori* what the possibilities are. It's a matter of linear algebra in the finite group $\mathrm{GL}_2(\mathbb{F}_q)$. If $\gamma \in \mathrm{GL}_2(\mathfrak{k})$ fixes a node ν, then it belongs to the maximal compact subgroup GL_ν fixing that node. If $g\nu_0 = \nu$, then $\gamma_0 = g^{-1}\gamma g \in \mathrm{GL}_2(\mathfrak{o})$. The neighbours of ν_0 fixed by γ_0 are in bijection with the lines in $\mathbb{P}^1(\mathbb{F}_q)$ fixed by it, which in turn correspond to $\mathbb{F}_q$-rational eigenvalues. There are *a priori* four possibilities: (a) γ_0 has no rational eigenvalues; (b) it is a scalar matrix, and fixes all of $\mathbb{P}^1(\mathbb{F}_q)$; (c) it is unipotent with one eigenline; and (d) it is diagonalizable and has two distinct eigenlines. In our case, with γ in the image of an unramified extension, Proposition 10.1 tells us that case (d) cannot occur, but all the others do.

We can specify the environment of y in $\mathfrak{X}^{\gamma}$ by a function $d(\gamma, y)$, the number of edges connecting to y that are fixed by γ. The Lemma implies that it takes three different possible values.

(a) The first is that in which $y = \nu_0$ and $\big|D(\gamma)\big| = 1$. Then γ fixes y, but none of its neighbours. Thus $d(\gamma, y) = 0$.
(b) Or y could be in the interior of $\mathfrak{X}^{\gamma}$. In this case, $d(\gamma, y) = q + 1$.
(c) The last possibility is that y lies on a true boundary of $\mathfrak{X}^{\gamma}$. In this case the only edge fixed by γ runs towards the root node, $d(\gamma, y) = 1$.

I now move on to prove FL(b). It would be possible to do this by explicit calculation, but there is a more elegant method to be found in [Kottwitz:1980] and [Kottwitz:1990]. We have

$$\begin{aligned} \#\big\{x \in \mathfrak{X}_+ \,\big|\, [\gamma x\colon x] = m\big\} - \#\big\{x \in \mathfrak{X}_- \,\big|\, [\gamma x\colon x] = m\big\} &= \sum_{[\gamma x: x] = 2m} \varepsilon(x) \\ &= \sum_{\gamma y = y} \varepsilon(y)\cdot\varepsilon(y) \sum_{\substack{\rho(x)=y \\ [\gamma x:x]=2m}} \varepsilon(x) \\ &= \sum_{\gamma y = y} \varepsilon(y)\langle L_{\gamma,y}, \tau_m\rangle \end{aligned}$$

if for every y in $\mathfrak{X}^{\gamma}$ I define

$$\langle L_{\gamma,y}, \tau_m\rangle = \varepsilon^{-1}(y) \sum_{\substack{\rho(x)=y \\ [\gamma(x):x]=2m}} \varepsilon(x) \,.$$

Lemma 10.3. *For y in $\mathfrak{X}^{\gamma}$ and $m > 0$*

$$\langle L_{\gamma,y}, \tau_m\rangle = (-1)^m\big((q+1) - d(\gamma, y)\big)q^{m-1} \,.$$

I'll postpone the proof, but show right now how it allows us to prove FL(b). We have

$$\begin{aligned}\sum_{\gamma y=y} \varepsilon(y)\langle L_{\gamma,y}, \tau_m\rangle &= \sum_{\gamma y=y} \varepsilon(y)(-1)^m\big((q+1)q^{m-1} - d(\gamma,y)\big)q^{m-1} \\ &= (-1)^m(q+1)q^{m-1}\,\Phi_\gamma(f_K) \\ &= \tau_m^\vee(sgn)\,\Phi_\gamma(f_K)\,.\end{aligned}$$

The reason we can ignore the terms $d(\gamma, y)$ is that in the sum they cancel, since every value occurs twice, once for each end of an edge, with opposite sign. ∎

So now it remains to prove Lemma 10.3.

First, a basic property of the retraction ρ:

Lemma 10.4. *If $\rho(x) = y$, then $[\gamma(x){:}\, x] = 2m$ if and only if $[y{:}\, x] = m$.*

Proof. For $m = 0$ this is immediate. So suppose the distance from x to y to be $m > 0$. Since x is not fixed by γ, $[x{:}\,\nu_0] > 0$. Let $x_0 = y$, x_1, … , $x_m = x$ be the geodesic from y to x. Since $\rho(x) = y$, no x_i is fixed by γ. Therefore the path (γx_i) must also have length m, and the path from x to y and back to γx does not backtrack, and is also a geodesic. It has length $2m$, so $\gamma(x){:}\, x] = 2m$. ∎

The map taking x to the geodesic from x to y is therefore a bijection between the set of x with $[\gamma x{:}\, x] = m$, $\rho(x) = y$ and the sets of geodesics running out from y of length m that start with a point not fixed by γ.

To prove Lemma 10.3, we look in turn at each of the three possibilities for y.

(a) $d(\gamma, y) = 0$. Here $y = \nu_0$, and there are $q + 1$ edges running out from y. Each contributes q^{m-1} points x with $[\gamma x{:}\, x] = m$ retracting to y. So $L_{\gamma,y}(f_{K\omega^m K}) = (q + 1)q^{m-1}$.

(b) $d(\gamma, y) = q + 1$. The number of x with $[\gamma x{:}\, x] = m$ retracting to y is 0.

(c) $d(\gamma, y) = 1$. There are q relevant edges,a nd each contributes q^{m-1}.

In each case, the number of paths leading to x with $[\gamma(x){:}\, x] = 2m$ is $\big((q + 1) - d(\gamma, y)\big)q^{m-1}$. ∎

The underlying principle of the proof is that all configurations of geodesics (x_i) with $x_0 = y$ and $\gamma x_1 \neq x_1$ are congruent, and that every point with $\gamma x \neq x$ and $\rho(x) = y$ occurs as the endpoint of one of these.

Kottwitz' proof of the Fundamental Lemma for SL_3 uses the same reduction to a functional $L_{\gamma,y}$, but the analysis of possible local configurations for y in $\mathfrak{X}^\gamma$ is much more complicated. In particular, it is not easy to specify the fixed points of unramified cubic elements γ. There are more terms analogous to $d(\gamma, y)$, for example, recording the different types of facettes in the building neighbouring y. It has not been feasible to prove the Fundamental Lemma for general groups by calculations on the building, but the proofs for $SL_2(\mathfrak{k})$ and $SL_3(\mathfrak{k})$ suggest much about how the eventual proof of Ngo at al., complicated though it may be, proceeds.

As pointed out very clearly in [Hales:1994] there is little or even no hope that the Fundamental Lemma will ever be proved by elementary means, but one might hope for a proof more direct than the one found by Ngo and predecessors. Even if a direct proof of most cases of the Fundamental Lemma is not feasible, it would be nice to be able to bypass for SL_2 and SL_3 the explicit form of Macdonald's formula and arrive at a more conceptual proof.

11. References

1. M. Atiyah and R. Bott, **Notes on the Lefschetz fixed point theorem for elliptic complexes**, notes from the Harvard University Mathematics Department, 1964.

2. A. Borel, 'Automorphic L-functions', in volume 2 of **Automorphic forms, representations, and L-functions**, proceedings of a conference in Corvallis, *Proc. Symp. Pure Math.* **33**, A.M.S., 1979.

3. S. Debacker, 'Parametrizing conjugacy classes of maximal unramified tori via Bruhat-Tits theory', *Mich. Math. Jour.* **56** (2006), 157–178.

4. Mark Goresky, Robert Kottwitz, and Robert MacPherson, 'Homology of affine Springer fibres in the unramified case', *Duke Mathematical Journal* **121** (2004), 509–561.

5. T. Hales, 'Hyperelliptic curves and harmonic analysis', in **Representation theory and analysis on homogeneous spaces**, *Contemp. Math.*, 1994.

6. —–, 'On the fundamental lemma for standard endoscopy: reduction to unit elements', *Can. Jour. Math.* **47** (1995), 974–994.

7. —–, 'A statement of the Fundamental Lemma', in **Harmonic analysis, the trace formula, and Shimura varieties**, A.M.S., 2005.

8. E. Hecke, 'Bestimmungen der Perioden gewisser Integrale durch die Theorie der Klassenkörper', *Mathematisches Zeitschrift* **28** (1928), 708–727.

9. —–, 'Über das verhalten der Integrale 1. Gattung bei Abbildungen, insbesondere in der Theorie der elliptischen Modulfunktionen', *Abhandlungen aus einem Seminar der Hamburgische Universität* **8** (1930), 271–281.

10. S.-I. Kato, 'On the Kazhdan-Lusztig polynomials for affine Weyl groups', *Advances in Mathematics* **55** (1985), 103–130.

11. R. E. Kottwitz, 'Orbital integrals on GL(3)', *Amer. Jour. Math.* **102** (1980), 327–384.

12. —– , 'Unstable orbital integrals on SL_3', *Duke Math. Jour.* **48** (1981), 649–664.

13. —– , 'Rational conjugacy classes in reductive groups', *Duke Math. Jour.* **49** (1982), 785–806.

14. —– , 'Harmonic analysis on p-adic groups and Lie algebras', 393–522 in **Harmonic analysis, the trace formula, and Shimura varieties**, *Clay Mathematics Proceedings* **4**, AMS, 2005.

15. J.-P.Labesse and R. P. Langlands, 'L-indistinguishability for SL(2)', *Can. Jour. of Math.* **XXXI** (1979), 726–785.

16. R. P. Langlands, **Base change for GL(2)**, *Annals of Mathematics Studies* **96**, Princeton, 1980.

17. J-P. Serre, **Arbres, amalgames, et SL(2)**, *Astérisque* **46** (1977). Translated into English as **Trees**, Springer-Verlag, 1980.

18. R. Steinberg, 'Regular elements of semisimple algebraic groups', *Publ. Math. IHES* **25** (1965), 49–80.