Clay Mathematics Proceedings
Volume 4, 2005

A Statement of the Fundamental Lemma

Thomas C. Hales

ABSTRACT. These notes give a statement of the fundamental lemma, which is a conjectural identity between p-adic integrals.

1. Introduction

Notation. Let F be a p-adic field, given either as a finite field extension of $\mathbb{Q}_p$, or as the field $F = \mathbb{F}_q((t))$. Let $\mathbb{F}_q$ (a finite field with q elements and characteristic p) be the residue field of F. Let $\bar{F}$ be a fixed algebraic closure of F. Let F^{un} be the maximal unramified extension of F in $\bar{F}$. For simplicity, we also assume that the characteristic of F is not 2.

The fundamental lemma pertains to groups that satisfy a series of hypotheses. Here is the first.

ASSUMPTION 1.1. *G is a connected reductive linear algebraic group that is defined over F.*

The following examples give the F-points of three different families of connected reductive linear algebraic groups: orthogonal, symplectic, and unitary groups.

EXAMPLE 1.2. Let $M(n, F)$ be the algebra of n by n matrices with coefficients in F. Let $J \in M(n, F)$ be a symmetric matrix with nonzero determinant. The special orthogonal group with respect to the matrix J is

$$\mathrm{SO}(n, J, F) = \{X \in M(n, F) \mid {}^tXJX = J, \quad \det(X) = 1\}.$$

EXAMPLE 1.3. Let $J \in M(n, F)$, with $n = 2k$, be a skew-symmetric matrix ${}^tJ = -J$ with nonzero determinant. The symplectic group with respect to J is defined in a similar manner:

$$\mathrm{Sp}(2k, J, F) = \{X \in M(2k, F) \mid {}^tXJX = J\}.$$

EXAMPLE 1.4. Let E/F be a separable quadratic extension. Let $\bar{x}$ be the Galois conjugate of $x \in E$ with respect to the nontrivial automorphism of E fixing F. For any $A \in M(n, E)$, let $\bar{A}$ be the matrix obtained by taking the Galois

I thank R. Kottwitz and S. DeBacker for many helpful comments.
This work was supported in part by the NSF.

conjugate of each coefficient of A. Let $J \in M(n,E)$ satisfy ${}^t\bar{J} = J$ and have a nonzero determinant. The unitary group with respect to J and E/F is

$$U(n,J,F) = \{X \in M(n,E) \mid {}^t\bar{X}JX = J\}.$$

The algebraic groups $SO(n,J)$, $Sp(2k,J)$, and $U(n,J)$ satisfy Assumption 1.1.

Assumption 1.5. *G splits over an unramified field extension.*

That is, there is an unramified extension F_1/F such that $G \times_F F_1$ is split.

Example 1.6. In the first two examples above (orthogonal and symplectic), if we take J to have the special form

$$J = \begin{pmatrix} 0 & 0 & * \\ 0 & * & 0 \\ * & 0 & 0 \end{pmatrix} \tag{1.6.1}$$

(that is, nonzero entries from F along the cross-diagonal and zeros elsewhere), then G splits over F. In the third example (unitary), if J has this same form and if E/F is unramified, then the unitary group splits over the unramified extension E of F.

Assumption 1.7. *G is quasi-split.*

This means that there is an F-subgroup $B \subset G$ such that $B \times_F \bar{F}$ is a Borel subgroup of $G \times_F \bar{F}$.

Example 1.8. In all three cases (orthogonal, symplectic, and unitary), if J has the cross-diagonal form 1.6.1, then G is quasi-split. In fact, we can take the points of B to be the set of upper triangular matrices in $G(F)$.

Assumption 1.9. *K is a hyperspecial maximal compact subgroup of $G(F)$, in the sense of Definition 1.11.*

Example 1.10. Let O_F be the ring of integers of F and let $K = GL(n, O_F)$. This is a hyperspecial maximal compact subgroup of $GL(n,F)$.

Definition 1.11. K is *hyperspecial* if there exists $\mathcal{G}$ such that the following conditions are satisfied.

- $\mathcal{G}$ is a smooth group scheme over O_F,
- $G = \mathcal{G} \times_{O_F} F$,
- $\mathcal{G} \times_{O_F} \mathbb{F}_q$ is reductive,
- $K = \mathcal{G}(O_F)$.

Example 1.12. In all three examples (orthogonal, symplectic, and unitary), take G to have the form of Example 1.6. Assume that each cross-diagonal entry is a *unit* in the ring of integers. Assume further that the residual characteristic is not 2. Then the equations

$${}^tXJX = J \quad \text{(or in the unitary case } {}^t\bar{X}JX = J\text{)}$$

define a group scheme $\mathcal{G}$ over O_F, and $\mathcal{G}(O_F)$ is hyperspecial.

2. Classification of Unramified Reductive Groups

DEFINITION 2.1. If G is quasi-split and splits over an unramified extension (that is, if G satisfies Assumptions 1.5 and 1.7), then G is said to be an *unramified reductive group*.

Let G be an unramified reductive group. It is classified by data (called root data)

$$(X^*, X_*, \Phi, \Phi^\vee, \sigma).$$

The data are as follows:

- X^* is the character group of a Cartan subgroup of G.
- X_* is the cocharacter group of the Cartan subgroup.
- $\Phi \subset X^*$ is the set of roots.
- $\Phi^\vee \subset X_*$ is the set of coroots.
- σ is an automorphism of finite order of X^* sending a set of simple roots in Φ to itself.

  σ is obtained from the action on the character group induced from the Frobenius automorphism of $\mathrm{Gal}(F^{un}/F)$ on the maximally split Cartan subgroup in G.

The first four elements $(X^*, X_*, \Phi, \Phi^\vee)$ classify split reductive groups G over F. For such groups $\sigma = 1$.

3. Endoscopic Groups

H is an unramified endoscopic group of G if it is an unramified reductive group over F whose classifying data has the form

$$(X^*, X_*, \Phi_H, \Phi_H^\vee, \sigma_H).$$

The first two entries are the same for G as for H. To distinguish the data for H from that for G, we add subscripts H or G, as needed. The data for H are subject to the constraints that there exists an element $s \in \mathrm{Hom}(X_*, \mathbb{C}^\times)$ and a Weyl group element $w \in W(\Phi_G)$ such that

- $\Phi_H^\vee = \{\alpha \in \Phi_G^\vee \mid s(\alpha) = 1\}$,
- $\sigma_H = w \circ \sigma_G$, and
- $\sigma_H(s) = s$.

3.1. Endoscopic groups for $SL(2)$. As an example, we determine the unramified endoscopic groups of $G = SL(2)$. The character group X^* can be identified with $\mathbb{Z}$, where $n \in \mathbb{Z}$ is identified with the character on the diagonal torus given by

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \mapsto t^n.$$

The set Φ can be identified with the subset $\{\pm 2\}$ of $\mathbb{Z}$:

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \mapsto t^{\pm 2}.$$

The cocharacter group X_* is also identified with $\mathbb{Z}$, where $n \in \mathbb{Z}$ is identified with

$$t \mapsto \begin{pmatrix} t^n & 0 \\ 0 & t^{-n} \end{pmatrix}.$$

Under this identification $\Phi^\vee = \{\pm 1\}$. Since the group is split, $\sigma = 1$.

We get an unramified endoscopic group by selecting $s \in \mathrm{Hom}(X_*, \mathbb{C}^\times) \cong \mathbb{C}^\times$ and $w \in W(\Phi)$.

$$\begin{aligned} \Phi_H^\vee = \{\alpha \mid s(\alpha) = 1\} \quad &= \{n \in \{\pm 1\} \mid s^n = 1\} \\ &= \text{if } (s = 1) \text{ then } \Phi_G^\vee, \text{ else } \emptyset. \end{aligned} \tag{3.0.1}$$

We consider two cases, according as w is nontrivial or trivial. If w is the nontrivial reflection, then $\sigma_H = w$ acts by negation on $\mathbb{Z}$. Thus,

$$(\sigma_H(s) = s) \implies (s^{-1} = s) \implies (s = \pm 1).$$

If $s = 1$, then σ_H does not fix a set of simple roots as required. So $s = -1$ and $\Phi_H^\vee = \emptyset$. Thus, H has root data

$$(\mathbb{Z}, \mathbb{Z}, \emptyset, \emptyset, w)$$

This determines H up to isomorphism as $H = U_E(1)$, a 1-dimensional torus split by an unramified quadratic extension E/F.

If w is trivial, then there are two further cases, according as Φ_H is empty or not:

- The endoscopic group $\mathbb{G}_m$ has root data
$$(\mathbb{Z}, \mathbb{Z}, \emptyset, \emptyset, 1).$$
- The endoscopic group $H = SL(2)$ has root data
$$(\mathbb{Z}, \mathbb{Z}, \{\pm 2\}, \{\pm 1\}, 1).$$

In summary, the three unramified endoscopic groups of $SL(2)$ are $U_E(1)$, $\mathbb{G}_m$, and $SL(2)$ itself.

3.2. Endoscopic groups for $PGL(2)$**.** As a second complete example, we determine the endoscopic groups of $PGL(2)$. The group $PGL(2)$ is dual to $SL(2)$ in the sense that the coroots of one group can be identified with the roots of the other group. $PGL(2)$ has root data

$$(\mathbb{Z}, \mathbb{Z}, \{\pm 1\}, \{\pm 2\}, 1).$$

When the Weyl group element is trivial, then the calculation is almost identical to the calculation for $SL(2)$. We find that there are again two cases, according as Φ_H is empty or not:

- The endoscopic group $\mathbb{G}_m$ has root data
$$(\mathbb{Z}, \mathbb{Z}, \emptyset, \emptyset, 1).$$
- The endoscopic group $H = PGL(2)$ has root data
$$(\mathbb{Z}, \mathbb{Z}, \{\pm 1\}, \{\pm 2\}, 1).$$

When the Weyl group element w is nontrivial, then $s \in \{\pm 1\}$, as in the $SL(2)$ calculation.

$$\Phi_H^\vee = \{\alpha \mid s(\alpha) = 1\} = \{n \in \{\pm 2\} \mid s^n = 1\} = \Phi_G^\vee. \tag{3.0.2}$$

From this, we see that picking w to be nontrivial is incompatible with the requirement that $\sigma_H = w$ must fix a set of simple roots. Thus, there are no endoscopic groups with w nontrivial.

In summary, the two endoscopic groups of $PGL(2)$ are $\mathbb{G}_m$ and $PGL(2)$ itself.

3.3. Elliptic Endoscopic groups.

DEFINITION 3.1. An unramified endoscopic group H is said to be *elliptic* if

$$(\mathbb{R}\Phi_G)^{W(\Phi_H)\rtimes\langle\sigma_H\rangle} = (0).$$

That is, the span of the set of roots of G has no invariant vectors under the Weyl group of H and the automorphism σ_H.

The origin of the term *elliptic* is the following. We will see below that each Cartan subgroup of H is isomorphic to a Cartan subgroup of G. (Here and elsewhere, when we speak of an isomorphism between algebraic groups defined over F, we mean an isomorphism over F.) The condition on H for it to be elliptic is precisely the condition that is needed for some Cartan subgroup of H to be isomorphic to an *elliptic* Cartan subgroup of G.

EXAMPLE 3.2. We calculate the elliptic unramified endoscopic subgroups of $SL(2)$. We may identify $\mathbb{R}\Phi$ with $\mathbb{R}\{\pm 2\}$ and hence with $\mathbb{R}$. An unramified endoscopic group is elliptic precisely when $W(\Phi_H)$ or $\langle\sigma_H\rangle$ contains the nontrivial reflection $x \mapsto -x$. When $H = SL(2)$, the Weyl group contains the nontrivial reflection. When $H = U_E(1)$, the element σ_H is the nontrivial reflection. But when $H = \mathbb{G}_m$, both $W(\Phi_H)$ and $\langle\sigma_H\rangle$ are trivial. Thus, $H = SL(2)$ and $H = U_E(1)$ are elliptic, but $H = \mathbb{G}_m$ is not.

3.4. An exercise: elliptic endoscopic groups of unitary groups. This exercise is a calculation of the elliptic unramified endoscopic groups of $U(n, J)$. We assume that J is a cross-diagonal matrix with units along the cross-diagonal as in Section 1.6.1. We give a few facts about the endoscopic groups of $U(n, J)$ and leave it as an exercise to fill in the details.

Let $T = \{\mathrm{diag}(t_1, \ldots, t_n)\}$ be the group of diagonal n by n matrices. The character group X^* can be identified with $\mathbb{Z}^n$ in such a way that the character

$$\mathrm{diag}(t_1, \ldots, t_n) \mapsto t_1^{k_1} \cdots t_n^{k_n}$$

is identified with $(k_1, \ldots, k_n)$.

The cocharacter group can be identified with $\mathbb{Z}^n$ in such a way that the cocharacter

$$t \mapsto \mathrm{diag}(t^{k_1}, \ldots, t^{k_n})$$

is identified with $(k_1, \ldots, k_n)$.

Let e_i be the basis vector of $\mathbb{Z}^n$ whose j-th entry is Kronecker δ_{ij}. The set of roots can be identified with

$$\Phi = \{e_i - e_j \mid i \neq j\}.$$

The set of coroots $\Phi^\vee$ can be identified with the set of roots Φ under the isomorphism $X_* \cong \mathbb{Z}^n \cong X^*$.

We may identify $\mathrm{Hom}(X_*, \mathbb{C}^\times)$ with $\mathrm{Hom}(\mathbb{Z}^n, \mathbb{C}^\times) = (\mathbb{C}^\times)^n$. Thus, we take the element s in the definition of endoscopic group to have the form $s = (s_1, \ldots, s_n) \in (\mathbb{C}^\times)^n$. The element $\sigma = \sigma_G$ acts on characters and cocharacters by

$$\sigma(k_1, \ldots, k_n) = (-k_n, \ldots, -k_1).$$

Let $I = \{1, \ldots, n\}$. Show that if H is an elliptic unramified endoscopic group, then there is a partition

$$I = I_1 \coprod I_2$$

with $s_i = 1$ for $i \in I_1$ and $s_i = -1$ otherwise. The elliptic endoscopic group is a product of two smaller unitary groups $H = U(n_1) \times U(n_2)$, where $n_i = \#I_i$, for $i = 1, 2$.

4. Cartan subgroups

All unramified reductive groups are classified by their root data. This includes the classification of unramified tori T as a special case (in this case, the set of roots and the set of coroots are empty):

$$(X^*(T), X_*(T), \emptyset, \emptyset, \sigma).$$

We can extend this classification to ramified tori. If T is any torus over F, it is classified by

$$(X^*(T), X_*(T), \rho),$$

where ρ is now allowed to be any homomorphism

$$\rho : \mathrm{Gal}(\bar{F}/F) \to \mathrm{Aut}(X^*(T))$$

with finite image.

A basic fact is that T embeds over F as a Cartan subgroup in a given unramified reductive group G if and only if the following two conditions hold.

- The image of ρ in $\mathrm{Aut}(X^*(T))$ is contained in $W(\Phi_G) \rtimes \langle \sigma_G \rangle$.
- There is a commutative diagram:

$$\begin{array}{ccc}
\mathrm{Gal}(\bar{F}/F) & \longrightarrow & \mathrm{Gal}(F^{un}/F) \\
{\scriptstyle\rho}\big\downarrow & & \big\downarrow{\scriptstyle \mathrm{Frob} \mapsto \sigma_G} \\
W(\Phi_G) \rtimes \langle \sigma_G \rangle & \xrightarrow[w \rtimes \tau \mapsto \tau]{} & \langle \sigma_G \rangle.
\end{array}$$

It follows that every Cartan subgroup T_H of H is isomorphic over F to a Cartan subgroup T_G of G. (To check this, simply observe that these two conditions are more restrictive for H than the corresponding conditions for G.) The isomorphism can be chosen to induce an isomorphism of Galois modules between the character group (and cocharacter group) of T_H and that of T_G.

We say that a semisimple element in a reductive group is *strongly regular*, if its centralizer is a Cartan subgroup. If $\gamma \in H(F)$ is strongly regular semisimple, then its centralizer T_H is isomorphic to some $T_G \subset G$. Let $\gamma_0 \in T_G(F) \subset G(F)$ be the element in $G(F)$ corresponding to $\gamma \in T_H(F) \subset H(F)$, under this isomorphism.

Remark 4.1. The element γ_0 is not uniquely determined by γ. The Cartan subgroup T_G can always be replaced with a conjugate $g^{-1}\, T_G\, g$, $g \in G(F)$, without altering the root data. However, the non-uniqueness runs deeper than this. An example will be worked in Section 8.1 to show how to deal with the problem of non-uniqueness. Non-uniqueness of γ_0 is related to stable conjugacy, which is our next topic.

5. Stable Conjugacy

Definition 5.1. Let δ and δ' be strongly regular semisimple elements in $G(F)$. They are *conjugate* if $g^{-1}\delta g = \delta'$ for some $g \in G(F)$. They are *stably conjugate* if $g^{-1}\delta g = \delta'$ for some $g \in G(\bar{F})$.