A Satake isomorphism for representations modulo p of reductive groups over local fields

Guy Henniart, Marie–France Vignéras

Abstract

Let F be a local field with finite residue field of characteristic p. Let G be a connected reductive group over F and B a minimal parabolic subgroup of G with Levi decomposition $B = ZU$. Let K be a special parabolic subgroup of G, in good position relative to (Z, U).

Fix an absolutely irreducible smooth representation of K on a vector space V over some field C of characteristic p. Writing $\mathcal{H}(G, K, V)$ for the intertwining Hecke algebra of V in G, we define a natural algebra homomorphism from $\mathcal{H}(G, K, V)$ to $\mathcal{H}(Z, Z \cap K, V^{U \cap K})$, we show it is injective and identify its image. We thus generalize work of F. Herzig, who assumed F of characteristic 0, G unramified and K hyperspecial, and took for C an algebraic closure of the prime field $\mathbb{F}_p$. We show that in the general case $\mathcal{H}(G, K, V)$ need not be commutative; that is in contrast with the cases Herzig considers and with the more classical situation where V is trivial and the field of coefficients is the field of complex numbers.

MS Class : 22E50

Key words : Local fields, Hecke algebra, Satake isomorphism

Adresses : Guy Henniart

Univ. Paris–Sud, Laboratoire de Mathématiques d'Orsay

Orsay Cedex F–91405 ; CNRS, UMR 8628, Orsay Cedex F–91405

Courriel : Guy.Henniart@math.u-psud.fr

Adresses : M.–F. Vignéras
Institut de Mathématiques de Jussieu
UMR 7586
175 Rue du Chevalet
75013 Paris
Courriel : vigneras@math.jussieu.fr

Contents

1 Introduction **4**

2 Abstract Satake homomorphism **11**

3 Parahoric subgroups **23**

4 The case where G is compact mod. centre **29**

5 Irreducible mod. p representations of parahoric subgroups **33**

6 Double coset decompositions **39**

7 Satake isomorphisms **49**

1 Introduction

1.1

Throughout the paper, F is a locally compact non–Archimedean field with finite residue field k of characteristic p.

In this introduction, C is a field, we fix a connected reductive group $\underline{G}$ over F, and we consider the locally pro–p–group $G = \underline{G}(F)$.

A representation of G on a C–vector space W is <u>smooth</u> if every vector in W has an open stabilizer in G. Classically one is interested in complex irreducible smooth representations of G, because they occur as local components of automorphic representations of adelic reductive groups.

In the recent decades, the study of congruences between modular forms has had tremendous impact in Number Theory, leading in particular to a proof of Fermat's Last Theorem. This inexorably leads to the study of congruences between automorphic forms or automorphic representations. As a local counterpart, one has to explore smooth irreducible representations of G on C–vector spaces, where C is a field of positive characteristic, for example a finite field.

In this paper, our main interest lies in the case where C has the same characteristic p as k.

1.2

Let K be an open compact subgroup of G. If π is a smooth representation of G on a C–vector space W, then the subspace W^K of fixed points under K is endowed with an action of the convolution algebra $\mathcal{H}(G, K, C)$ of double cosets in $K\backslash G/K$, usually called a Hecke algebra.

If C is the field of complex numbers and π is irreducible, then it is known that W^K is finite dimensional and, if non–zero, is a simple module over $\mathcal{H}(G, K, \mathbb{C})$. More precisely, the assignment $W \mapsto W^K$ yields a bijection between isomorphism classes of smooth irreducible complex representations of G with non–zero fixed points under K, and isomorphism classes of simple modules over $\mathcal{H}(G, K, \mathbb{C})$. The same is true, more generally, when the pro–order of K is prime to the characteristic exponent of C [V1]. When C has characteristic p however, the functor $W \mapsto W^K$ reveals less about smooth representations of G [O2]. Still it is important to understand the algebra $\mathcal{H}(G, K, C)$ and its category of modules. In the classical setting, such an understanding is provided by the Satake isomorphism when K is a special maximal compact subgroup of G (see below), and we want to generalize it to the present setting.

1.3

The general framework for "Satake morphisms" is the following. We fix a minimal parabolic subgroup B of G and a Levi decomposition $B = ZU$ where U is the unipotent radical of B. We assume $G = KB$ and $B \cap K = (Z \cap K)(U \cap K)$. In § 2 we define a natural algebra homomorphism

$$S : \mathcal{H}(G, K, C) \longrightarrow \mathcal{H}(Z, Z \cap K, C)\,.$$

We speak of a "Satake isomorphism" when S is injective and we can identify its image.

The prototype of Satake isomorphism is indeed due to Satake. In [Sa], where C is the field of complex numbers, Satake established a Satake isomorphism for maximal open compact subgroups K satisfying some axiomatic conditions, which he verified when G is a classical group, for natural maximal compact subgroups K.

Remark.— For arithmetic purposes, it is more interesting to describe the algebra $\mathcal{H}(G, K, \mathbb{Z})$ with integer coefficients. In his setting, Satake does get such a description. For example, when $\underline{G}$ is a classical simple group with trivial centre, $\mathcal{H}(G, K, \mathbb{Z})$ is a polynomial ring in m variables over $\mathbb{Z}$, where m is the rank of a maximal split torus in $\underline{G}$.

Bruhat and Tits subsequently verified that Satake's axioms are verified, for any G, when K is a maximal compact subgroup which is **special with respect to** Z, by which we mean that it corresponds to a special point of the building of the adjoint group of G, belonging to an apartment attached to a maximal split torus in Z (see § 3).

More recently, Haines and Rostami [Ha-Ro], motivated by applications to Shimura varieties, established a similar Satake isomorphism with complex coefficients, when K is a parahoric subgroup of G which is special with respect to Z (with the same meaning as above). The classical proofs in [Sa] and [Cartier] have to be modified then.

1.4

For the previous Satake isomorphisms (in [Sa, Cartier, Ha-Ro]), the map S is defined by the following formula, where we interpret $\mathcal{H}(G, K, \mathbb{C})$ as an algebra of functions on G, and $\mathcal{H}(Z, Z\cap K, \mathbb{C})$ as an algebra of functions on Z:

$$S(\Phi)(x) = \delta^{1/2}(x) \int_U \Phi(xu)du \qquad (\Phi \text{ in } \mathcal{H}(G, K, \mathbb{C}), x \text{ in } Z)\,.$$

In the formula, du is a Haar measure on U and δ is the modulus character of B, whose values are powers of p. Without the factor $\delta^{1/2}$, we already have an algebra homomorphism (see § 2), but because of the factor $\delta^{1/2}$ the image of S is invariant under the natural action of the Weyl group W of G; indeed the image of S is the algebra of W–invariants in $\mathcal{H}(Z, Z\cap K, \mathbb{C})$. The algebra $\mathcal{H}(Z, Z\cap K, \mathbb{C})$ is isomorphic to the group algebra over $\mathbb{C}$ of $Z/Z\cap K$ – which is a finitely generated abelian group – so $\mathcal{H}(Z, Z\cap K, \mathbb{C})$ is commutative and finitely generated over $\mathbb{C}$, as is the image of S, hence also $\mathcal{H}(G, K, \mathbb{C})$.

An all–important special case was singled out by Langlands [Ll]: that is the so–called "unramified" case, where $\underline{G}$ is unramified, i.e. quasi–split over F and split over some unramified extension of F, and where K is a hyperspecial maximal compact subgroup of G. Langlands in that case interpreted the Satake isomorphism above as giving a parametrization of the characters of the algebra $\mathcal{H}(G, K, \mathbb{C})$ — hence of the isomorphism classes of complex smooth irreducible representations of G with non–zero K–fixed vectors — by certain semisimple conjugacy classes in a complex group ${}^LG$ "dual" to G. He used the parametrization to define (partial) L–functions for automorphic representations of adelic reductive groups, and with the dual group he formulated a conjectural classification of all complex smooth irreducible representations of G — this is now proved for GL_n [HT, H] and a lot is known for split classical groups [Ar].

1.5

In our main case where C has characteristic p, the combinatorial arguments remain, but we cannot use the modulus character of B, and all invariance under W is lost. In analogy with the classical case nonetheless F. Herzig [He1] introduced a map $\mathcal{S} : \mathcal{H}(G, K, C) \to \mathcal{H}(Z, Z\cap K, C)$ simply defined by

$$\mathcal{S}(\Phi)(x) = \sum_{u\in U/U\cap K} \Phi(xu) \;\text{ for }\; \Phi \;\text{ in }\; \mathcal{H}(G, K, C) \;\text{ and }\; x \;\text{ in }\; Z\,.$$

We prove:

THEOREM.— *Let K be a parahoric subgroup of G, special with respect to Z. Let C be a field of characteristic p. Then*

(i) *$\mathcal{S}$ injective.*

(ii) *Its image is the space of functions supported on antidominant elements of Z.*

(iii) *$\mathcal{H}(Z, Z \cap K, C)$ and the image of $\mathcal{S}$ are commutative algebras of finite type over C.*

(We say that an element x of Z is antidominant if $x^{-r}(U \cap K)x^r$ does not blow up as the integer r goes to $+\infty$).

Remarks.— 1) The results in the theorem remain true if we replace the group K by the maximal compact subgroup of G containing K.

2) When C is $\mathbb{Z}$ we get an integral version of the results of [Ha-Ro], thus generalizing [Sa, §9] and [ST]; see § 7.10.

In fact the previous theorem is the special case $V = C$ of more general results describing the (intertwining) Hecke algebra $\mathcal{H}(G, K, V)$ for a smooth absolutely irreducible representation of K on a C–vector space V. We now turn to those more general results, which are inspired by the work of Herzig [He1] in the unramified case.

1.6

We return for a moment to a general field C. We keep the first assumptions of 1.3 but assume given in addition a smooth representation ρ of K on a finite dimensional C–vector space V.

The (intertwining) Hecke algebra $\mathcal{H}(G, K, V)$ is the convolution algebra consisting of functions Φ from G to $\mathrm{End}_C(V)$ which vanish outside finitely many cosets KgK and satisfy $\Phi(kg) = \rho(k)\Phi(g)$ and $\Phi(gk) = \Phi(g)\rho(k)$ for k and g in G. It is isomorphic to the endomorphism algebra of the smooth representation of G compactly induced from ρ, and for any smooth representation of G on a G–vector space W, the space $W(\rho) := \mathrm{Hom}_K(V, W)$ is a right–module over $\mathcal{H}(G, K, V)$. When V is the trivial representation of K on C, $W(\rho)$ identifies with W^K and we recover the algebra $\mathcal{H}(G, K, C)$. When C is the field of complex numbers and ρ is irreducible, the assignment

$W \mapsto W(\rho)$ again yields a bijection between isomorphism classes of complex smooth irreducible representations W of G such that $W(\rho) \neq 0$ and isomorphism classes of simple right–modules over $\mathcal{H}(G, K, C)$ – again this extends to any field C where the pro-order of K is invertible. For some complex representations ρ, called types, we even have stronger statements.

A very important special case is the so–called **level–zero** case. In that case K is a parahoric subgroup of G; writing K_+ for its pro–p radical, i.e. its maximal normal pro–p subgroup, we know that K/K_+ is the group of points over k of some connected reductive group $\underline{G}$; the level–zero case occurs when ρ is trivial on K_+. When moreover ρ comes from a complex irreducible **cuspidal** representation of the finite reductive group $\underline{G}(k)$, L. Morris determined the structure of $\mathcal{H}(G, K, V)$ in [Mo].

1.7

By contrast, when the field C has characteristic p, the assignment $W \mapsto W(\rho)$ does not usually yield a bijection as above : this problem already arose for trivial ρ. However Herzig [He1, He2] showed that one can use $W(\rho)$ to reveal properties of W, even giving, for $\underline{G} = GL_{n/F}$, a complete classification of smooth irreducible representations of $GL_n(F)$ over an algebraic closure of $\mathbb{F}_p$ [He2], in terms of supercuspidal representations of $GL_r(F)$, $p < r \leq n$, thus yielding the equivalent of Zelevinsky's classification for complex representations[1].

Our main interest here is in the following situation:

- K is a parahoric subgroup of G, special with respect to Z;
- C is a field of characteristic p;
- ρ is an absolutely irreducible representation of K on a C–vector space V, trivial on the pro–p–radical K_+.

[1] A smooth irreducible C–representation of G is <u>cuspidal</u> if it is not a subrepresentation of a representation obtained by parabolic induction from a smooth irreducible C–representation of a proper Levi subgroup of G; it is <u>supercuspidal</u> if it is not a subquotient of a such a parabolically induced representation. When C has characteristic 0 there is no difference between the two notions. When C has positive characteristic, there is a big difference; for example the Steinberg representation of $GL_2(F)$, in characteristic p, is cuspidal but not supercuspidal. Supercuspidal representations of G in characteristic p are still a mystery in general, even for $\underline{G} = GL_2$; the only exception is $GL_2(\mathbb{Q}_p)$.

As recalled above K/K_+ is naturally a finite reductive group over k, and we have at our disposal the theory of irreducible representations of such groups on C–vector spaces, for which our reference is [CE]. When V is absolutely irreducible, $V^{U\cap K}$ has dimension 1 over C (see § 6), so that $Z\cap K$ acts on it via a character $\chi_V : Z\cap K \to C^\times$.

In the unramified case (G unramified, K hyperspecial), Herzig identified $\mathcal{H}(G,K,V)$, via a morphism defined as in 1.5, with the subalgebra of the algebra $\mathcal{H}(Z, Z\cap K, V^{U\cap K})$ — which in his case is commutative — consisting of functions supported on antidominant elements.

Remark.— The first investigations of such algebras when C has characteristic p were done by Barthel and Livné [BL1,2] in the case where G is $GL_2(F)$ and C is an algebraic closure of $\mathbb{F}_p$. With the same field C, the algebras $\mathcal{H}(G,K,V)$ have been described by Vignéras [V2] for split groups G, and K a pro–p–Iwahori subgroup of G; applications to smooth irreducible representations of $GL_n(F)$ over C were given by Vignéras [V2] and Ollivier [O1, O2].

1.8

Here we generalize [He1] to our situation. We use the same formula 1.5 of Herzig for a map

$$\mathcal{S} : \mathcal{H}(G,K,V) \longrightarrow \mathcal{H}(Z, Z\cap K, V^{U\cap K})$$

As in 1.7 we assume that ρ is absolutely irreducible, and we write Z_V for the subgroup of elements in Z normalizing the character χ_V; we write Z_- for the monoid of antidominant elements in Z.

Theorem.— *In the situation of* 1.7*, the map S is an injective algebra homomorphism and its image consists of functions with support in $Z_V \cap Z_-$.*

In Herzig's case, as mentioned above, the target algebra is commutative. In our more general case however, we give an example where $\mathcal{H}(G,K,V)$ is not commutative in 4.4: in our example $G = Z$ and V is one–dimensional.

In general we can describe the centre of $\mathcal{H}(G,K,V)$ via the Satake homomorphism $\mathcal{S}$. Let Z'_V be the set of elements x in Z_V such that χ_V is trivial on $xyx^{-1}y^{-1}$ for all y in Z_V; it is a subgroup of Z_V with finite index.

Proposition.— *In the situation of* 1.7*, the algebra $\mathcal{H}(G,K,V)$ is a finitely generated module over its centre and this centre, consisting of elements Φ in*

$\mathcal{H}(G,K,V)$ *such that* $\mathcal{S}(\Phi)$ *has support in* Z'_V, *is an algebra of finite type over* C.

On the positive side, we can show that $\mathcal{H}(Z, Z \cap K, V^{U \cap K})$ is commutative when Z is semi–simple simply connected, or semi–simple adjoint, or split over an unramified extension of F — the only difficult case is the last one; it will be given in a companion paper. As for $\mathcal{H}(G,K,V)$ it is clear that it is commutative if G is quasi–split, as then Z is a torus. In the mentioned companion paper, we shall prove that $\mathcal{H}(G,K,V)$ is commutative when G is a classical group of isometries or similitudes, and when it is semi–simple adjoint, semi–simple simply connected, or split over an unramified extension of F.

1.9

Let us now give the plan of the paper. In § 2, we explain the mechanism giving rise to Satake homomorphisms. We proceed in an abstract manner, dealing with a general locally profinite group G. From § 3 on, however, G is a $\underline{G}(F)$ where $\underline{G}$ is a connected reductive group over F. In § 4, we investigate the case where $\underline{G}$ is anisotropic modulo its centre, so is its own minimal parabolic subgroup. We determine in this case the centre of $\mathcal{H}(G,K,V)$, we give an example where $\mathcal{H}(G,K,V)$ is not commutative, but show that it is commutative in a few easy cases.

In § 5, we recall the classification of irreducible representations of groups $\underline{H}(k)$, where $\underline{H}$ is a connected reductive group over k, on vector spaces over fields of characteristic p.

The technical heart of the paper is in § 6. We state the Cartan and Iwasawa decomposition for our special parahoric subgroup K and describe the intersection of a "Cartan" double coset KgK with an "Iwasawa" double coset KhU: one can take g, h in Z and we show that if KgK intersects KhU, then the class of $g \mod Z \cap K$ is in some sense "smaller" than $h \mod Z \cap K$. Also in § 6, for an element x in Z, we investigate the intersection of K with the parabolic subgroup of G contracted by x.

In § 7 finally, we show that Herzig's methods in [He1] extend to our case, given the technical results of § 6.

It is a pleasure to thank F. Herzig for communicating his results to us in a preprint form.

2 Abstract Satake homomorphisms

2.1

The goal of this section is to unravel the basic mechanism behind the existence of Satake homomorphisms. For that reason we proceed in a rather abstract manner.

Throughout the section, C is any commutative ring, and for any group H we write $C[H]$ for the group algebra of H over C. If H is a locally profinite group, a $C[H]$–module is **smooth** if every element in it has an open stabilizer in H.

We fix a locally profinite group G and an open subgroup K of G. We also fix a smooth $C[K]$–module V; we sometimes write $\rho(k)$ for the endomorphism $v \mapsto kv$ of V.

We consider the smooth $C[G]$–module $\mathrm{ind}_K^G V$ made out of the functions f from G to V which verify $f(kg) = kf(g)$ for g in G and k in K, and vanish outside a finite number of cosets Kg; the action of G is via right translations. If W is any smooth $C[G]$–module, Frobenius reciprocity yields a canonical isomorphism of $\mathrm{Hom}_{C[K]}(V, W)$ onto $\mathrm{Hom}_{C[G]}$ $(\mathrm{ind}_K^G V, W)$: if ψ is a $C[K]$–morphism from V to W, the corresponding $C[G]$–morphism from $\mathrm{ind}_k^G V$ to W is given by $f \mapsto \sum\limits_{h \in G/K} h\psi(f(h^{-1}))$.

2.2

Of central interest to us is the endomorphism algebra $\mathrm{End}_{C[G]}$ $(\mathrm{ind}_K^G(V))$, which by Frobenius reciprocity is canonically isomorphic as a vector space to $\mathrm{Hom}_{C[K]}(V, \mathrm{ind}_K^G V)$.

We want a model of that algebra as an algebra $\mathcal{H}(G, K, V)$ on double cosets in $K\backslash G/K$. More generally, it is of interest to consider the space $\mathrm{Hom}_{C[G]}$ $(\mathrm{ind}_K^G V,\ \mathrm{ind}_K^G V')$ where V' is another smooth $C[K]$–module; by Frobenius reciprocity it is isomorphic to $\mathrm{Hom}_{C[K]}(V, \mathrm{ind}_K^G V')$, and again we seek a description of it as a space of functions on G. We write ρ' for the action of K on V'.

To work well (compare [V1, I.8], it is useful to make two further assumptions, in force from now on.

A1) Any double coset KgK in G is the union of finitely many cosets Kg', and also the union of finitely many cosets $g''K$. (That is the case, for example, when K is compact modulo a closed subgroup central in G).

A2) V and V' are finitely generated over $C[K]$.

With assumptions A1) and A2), if we associate to a $C[K]$–morphism φ from V to $\mathrm{ind}_K^G V'$ the function $\Phi_\varphi : G \to \mathrm{Hom}_C(V, V')$ given by $\Phi_\varphi(g)(v) = \varphi(v)g$ (for g in G and v in V), we get an isomorphism of $\mathrm{Hom}_{C[K]}(V, \mathrm{ind}_K^G V')$ with the C–module $\mathcal{H}(G, K, V, V')$ of functions $\Phi : G \to \mathrm{Hom}_C(V, V')$ which satisfy

(i) $\Phi(kg) = \rho'(k)\Phi(g)$ and $\Phi(gk) = \Phi(g)\rho(k)$ for g in G, k in K.

(ii) Φ vanishes outside finitely many cosets KgK.

If f is a function in $\mathrm{ind}_K^G V$, its image under the $C[G]$–morphism corresponding to φ above is given by a convolution product with $\Phi = \Phi_\varphi$:

$$\Phi * f(g) = \sum_{h \in G/K} \Phi(h)(f(h^{-1}g)) \text{ for } g \text{ in } G\,.$$

Note that the summand depends only on hK by (i), and that the sum is finite by (ii) and assumption A1.

If V'' is another finitely generated smooth $C[K]$–module, the composition map from $\mathrm{Hom}_{C[G]}(\mathrm{ind}_K^G V, \mathrm{ind}_K^G V') \times \mathrm{Hom}_{C[G]}(\mathrm{ind}_K^G V', \mathrm{ind}_K^G V'')$ to $\mathrm{Hom}_{C[G]}(\mathrm{ind}_K^G V, \mathrm{ind}_K^G V'')$ is reflected in a convolution operation $\mathcal{H}(G, K, V', V'') \times \mathcal{H}(G, K, V, V') \to \mathcal{H}(G, K, V, V'')$ $(\Psi, \Phi) \mapsto \Psi * \Phi$ given by

$$\Psi * \Phi(g) = \sum_{h \in G/K} \Psi(h)\Phi(h^{-1}g) \quad \text{for } g \text{ in } G\,.$$

Again the summand depends only on hK and the sum is finite. This convolution operation is C–bilinear, and there is an obvious "associativity" property if we consider a further finitely generated smooth $C[K]$–module V'''.

Taking $V = V' = V''$, we get an (associative) algebra structure on $\mathcal{H}(G, K, V, V)$, which we rather write $\mathcal{H}(G, K, V)$, and which we call the **Hecke algebra** of V in G, or sometimes the **intertwining algebra** of V in G.

2.3

We want to extend somewhat the previous constructions. Consider the C–module $F(G,K,V)$ of all functions $f : G \to V$ such that $f(kg) = kf(g)$ for k in K and g in G. It contains $\mathrm{ind}_K^G V$ as the submodule of functions supported on finitely many cosets Kg. Consider also the analogous module $F(G,K,V')$ for V'.

Let f be in $F(G,K,V)$ and Φ in $\mathcal{H}(G,K,V,V')$. We want to define a function $\Phi * f$ in $F(G,K,V')$ by the above convolution formula

$$(\Phi * f)(g) = \sum_{h \in G/K} \Phi(h)(f(h^{-1}g)) \quad \text{for } g \text{ in } G\,.$$

To make sense of the formula, we first remark that the summand, by (i) again, depends only on the coset hK; also the sum is finite because Φ vanishes outside finitely many cosets KxK and, by assumption A2), each KxK consists of finitely many cosets hK. By (i), the resulting function $\Phi * f$ belongs to $F(G,K,V')$, and we recover the previous definition of $\Phi * f$ if f is in $\mathrm{ind}_K^G V$.

Remark.— If the support of Φ is the disjoint union of cosets h_iK, $i \in I$, then $\Phi * f(g) = \sum_{i \in I} \Phi(h_i)(f(h_i^{-1}g))$ for any g in G.

If V'' is another finitely generated smooth $C[K]$–module, and Ψ an element in $\mathcal{H}(G,K,V',V'')$ we have the associativity formula

$$(\Psi * \Phi) * f = \Psi * (\Phi * f)\,,$$

which can be proved directly but also follows from topological considerations. Indeed put on V the discrete topology and on $F(G,K,V)$, $F(G,K,V')$ and $F(G,K,V'')$ the topology of pointwise convergence; by the remark above the map $f \mapsto \Phi * f$, for fixed Φ, is a continuous map from $F(G,K,V)$ to $F(G,K,V')$. Since $\mathrm{ind}_K^G V$ is clearly dense in $F(G,K,V)$ the associativity formula holds for f in $F(G,K,V)$ because it already holds for f in $\mathrm{ind}_K^G V$.

2.4

The action of $\mathcal{H}(G,K,V,V')$ sends $F(G,K,V)$ to $F(G,K,V')$ and this obviously commutes with the action of G on the latter spaces via right translations.

Let N be a closed subgroup of G; we write $F(G/N, K, V)$ for the set of functions in $F(G, K, V)$ which are constant on cosets gN, and $F_c(G, K, V)$ for the set of functions in $F(G/N, K, V)$ which vanish outside finitely many cosets KgN. They are clearly submodules of $F(G, K, V)$ and the operation of $\mathcal{H}(G, K, V, V')$ sends $F(G/N, K, V)$ into the analogous module $F(G/N,K,V')$ and $F_c(G/N, K, V)$ into $F_c(G/N, K, V')$. In particular $F_c(G/N, K, V)$ is a module over the Hecke algebra $\mathcal{H}(G, K, V)$.

If P is any closed subgroup of G normalizing N, its action on $F(G, K, V)$ by right translations stabilizes $F(G/N, K, V)$ and $F_c(G/N, K, V)$ and this action of P commutes with the operation of $\mathcal{H}(G, K, V, V')$. The subgroup $P \cap N$ acts trivially so that the action of P factors through $P/P \cap N$.

Remark.— The action of P on $F_c(G/N, K, V)$ is smooth: indeed if f in $F_c(G/N, K, V)$ vanishes outside finitely many cosets Kg_iN, $i \in I$, and takes value v_i at g_i, then $P \cap \bigcap_{i \in I} g_i^{-1} K_i g_i$ acts trivially on f, where K_i is the stabilizer of v_i in K.

2.5

To put ourselves in the context of a Satake morphism, we specialize to the following situation where:

(i) K is compact modulo a closed subgroup J central in G

(ii) P is a closed subgroup of G, which is the semi–direct product of an invariant closed subgroup N with a closed subgroup M containing J.

We **assume** that K, M, N satisfy the following conditions:

C1) $G = KP$ (Iwasawa decomposition)

C2) $P \cap K$ is the semi–direct product of $N \cap K$ by $M \cap K$

This is clearly inspired by the situation of reductive groups, treated from § 3 on, but it can also be applied in other situations, even trivial ones, where G would be discrete and K, M trivial!

Remark.— By (i) and (ii), $M \cap K$ is compact modulo its subgroup J; the group $N \cap K$ is compact since $N \cap J$, contained in $N \cap M$, is trivial. Also notice that (i) implies that condition (A1) of 2.2 is satisfied.

In this context, the existence of a Satake morphism, proved in 2.7, will derive from the following proposition, proved in 2.6.

PROPOSITION.— *Restricting to M the functions in $F(G/N,K,V)$ yields a bijection of $F(G/N,K,V)$ onto $F(M,M\cap K,V^{N\cap K})$ which sends $F_c(G/N,K,V)$ onto $F_c(M,M\cap K,V^{N\cap K})$.*

Remark.— Because $M\cap K$ normalizes $N\cap K$, the set $V^{N\cap K}$ of elements of V fixed by $N\cap K$ is a module over $C[M\cap K]$. We have used the notation relative to $(M,M\cap K)$ as we did relative to (G,K). Note also that the space $F_c(M,M\cap K,V^{N\cap K})$ is nothing but $\mathrm{ind}_{M\cap K}^{M} V^{N\cap K}$. Finally the restriction map in the proposition is obviously C–linear and compatible with the action of M via right translations, which is smooth.

2.6

The proof of the proposition is rather straightforward. For f in $F(G/N,K,V)$ we write f_M for its restriction to M.

a) We first verify that for f in $F(G/N,K,V)$, f_M indeed belongs to $F(M,M\cap K,V^{N\cap K})$. The property $f_M(km)=kf_M(m)$ for k in $M\cap K$ and m in M being obvious, the point is to show that $f(m)$ is fixed by $N\cap K$ for m in M; but for n in $N\cap K$ we have $nf(m)=f(nm)=f(mm^{-1}nm)=f(m)$ because $m^{-1}nm$ belongs to N.

b) The map $f\mapsto f_M$ is injective; indeed if $f_M=0$ then $f(kmn)=0$ for all m in M, n in N and k in K, so that $f=0$ by the Iwasawa decomposition $C1$).

c) The following lemma implies that the image of $F_c(G/N,K,V)$ is contained in $F_c(M,M\cap K,V^{N\cap K})$.

LEMMA.— *For g in G, $KgN\cap M$ is a single coset $(K\cap M)m$.*

Proof. Since $KgN\cap M$ is non–empty by the Iwasawa decomposition $C1$) we may assume g in M. If k in K and n in N are such that $m=kgn$ belongs to M then $k=mn^{-1}g^{-1}$ belongs to P; projecting to M we get by $C2$) that mg^{-1} belongs to $M\cap K$ hence $m\in(M\cap K)g$ □

d) It remains to prove the surjectivity statements.

Let F belong to $C(M, M \cap K, V^{N\cap K})$. If m in M, k in K and n in N verify $m = kmn$ then $k = mn^{-1}m^{-1}$ belongs to $N \cap K$ and $kF(m) = F(m)$. This shows that we can unambiguously define a function $f : G \to V$ by the formula $f(kmn) = kF(m)$ for k in K, m in M, n in N; that function belongs to $F(G/N, K, V)$ and f_M is equal to F. If F is supported on finitely many cosets $(M \cap K)m_i$ then f is supported on the cosets Km_iN.

The proposition is proved.

2.7

Let us stay in the context of 2.3–2.5. The operation of $\mathcal{H}(G, K, V, V')$ sending $F_c(G/N, K, V)$ to $F_c(G/N, K, V')$ commutes with the action of M via right translations, and the isomorphisms $f \mapsto f_M$ in Prop. 2.5 are M–equivariant. It follows then from Prop. 2.5 that there is a unique map $S = S_G^M(V, V')$ from $\mathcal{H}(G, K, V, V')$ to $\mathcal{H}(M, M \cap K, V^{N\cap K}, V'^{N\cap K})$ such that

$$(\Phi * f)_M = S(\Phi) * f_M \text{ for } f \text{ in } F_C(G/N, K, V) \text{ and } \Phi \text{ in } \mathcal{H}(G, K, V, V')\,.$$

(Here of course the convolution operation on the right hand side is taken with respect to M and $M \cap K$; also, by continuity, as in 2.3, the same formula holds for f in $F(G/N, K, V)$.

If V'' is another finitely generated smooth $C[K]$–module, the composite $S_G^M(V', V'') \circ S_G^M(V, V')$ is equal to $S_G^M(V, V'')$ so that when $V = V'$, then $S = S_G^M(V, V)$ is an algebra morphism, which we call a **Satake morphism**.

Remark.— In the cases we look at in § 7, S will be injective. We have no abstract general criterion for injectivity. It is not enough that V be generated as $C[K]$–module by $V^{N\cap K}$: indeed take for G a finite non–trivial abelian group and $N = G$, $M = K = 1$, and take for V the trivial module C. Then $\mathrm{ind}_K^G V$ is the regular representation $C[G]$ of G and the map $S : C[G] \to C$ is given by

$$\sum_{g\in G} \alpha_g g \longmapsto \sum_{g\in G} \alpha_g\,.$$

Proposition.— *For Φ in $\mathcal{H}(G, K, V, V')$, $S(\Phi)$ is given by $S(\Phi)(m)(v) = \sum_{n\in N/N\cap K} \Phi(mn)(v)$ for m in M and v in $V^{N\cap K}$.*

The proof will be given in 2.8, but we first give a few comments.

(i) The proposition is reminiscent of the classical definition of the Satake morphism via integration on mN (cf. 1.4).

(ii) As v is fixed by $N \cap K$, the summand depends only on $n(N \cap K)$.

(iii) The sum itself is finite. Indeed the support of Φ consists of finitely many cosets gK and if we have equalities $mn = gk$ and $mn' = gk'$ for some k, k' in K and n, n' in N, then $n'^{-1}n = k'^{-1}k$ belongs to $N \cap K$ so that n belongs to $n'(N \cap K)$.

2.8

Let us prove the formula in Proposition 2.7. Fix Φ in $\mathcal{H}(G, K, V, V')$. By (ii) and (iii) above, the right hand side defines a function φ on M, with values in $\mathrm{Hom}_C(V^{N\cap K}, V')$. By the lemma in 2.6, φ is supported on finitely many cosets $(M \cap K)m$. Let us first verify that φ belongs to $\mathcal{H}(M, M \cap K, V^{N\cap K}, V'^{N\cap K})$. We have $\Phi(kg) = \rho'(k)\Phi(g)$ for k in K and g in G. Taking k in $N \cap K$ gives that $\varphi(m)(v)$ belongs to $V'^{N\cap K}$ for v in $V^{N\cap K}$: indeed

$$\begin{aligned} \rho'(k)(\varphi(m)(v)) &= \sum_{n\in N/N\cap K} \Phi(kmn)(v) \\ &= \sum_{n\in N/N\cap K} \Phi(mm^{-1}kmn)(v) \end{aligned}$$

and we can use the change of summation $n \mapsto m^{-1}kmn$, since $m^{-1}km$ belongs to N. Taking rather k in $M \cap K$ then yields

$$\varphi(km) = \rho'_M(k)\varphi(m)$$

where we have written $\rho'_M(k)$ for the endomorphism $v \mapsto kv$ of $V'^{N\cap K}$.

We also have $\Phi(kg) = \Phi(g)\rho(k)$ for k in K and g in G. Taking k in $M \cap K$ gives $\varphi(mk) = \varphi(m)\rho_M(k)$ where $\rho_M(k)$ is the endomorphism $v \mapsto kv$ of $V^{N\cap K}$: indeed we compute, for v in $V^{N\cap K}$,

$$\begin{aligned} \varphi(mk)(v) &= \sum_{n\in N/N\cap K} \Phi(mkn)(v) \\ &= \sum_{n\in N/N\cap K} \Phi(mknk^{-1}k)(v) \\ &= \sum_{n\in N/N\cap K} \Phi(mknk^{-1})(\rho_M(k)v) \end{aligned}$$

and as k in $M \cap K$ normalizes $N \cap K$ we can use the change of summation $n \mapsto knk^{-1}$.

We have proved that φ belongs to $\mathcal{H}(M, M \cap K, V^{N \cap K}, V'^{N \cap K})$.

We now want to prove that $(\Phi * f)_M = \varphi * f_M$ for any f in $F_c(G/N, K, V)$.

For m in M we have $(\Phi * f)(m) = \sum_{h \in G/K} \Phi(h)(f(h^{-1}m))$. As $G = PK$ we may replace the sum over G/K with a sum over $P/P \cap K$. The resulting sum over $P/P \cap K$ can be obtained by summing first over $N/N \cap K$ then summing the result — which is right invariant under N — over $M/M \cap K$. We obtain

$$(\Phi * f)(m) = \sum_{j \in M/M \cap K} \sum_{n \in N/N \cap K} \Phi(jn)(f(j^{-1}m))$$

since $f(n^{-1}j^{-1}m) = f(j^{-1}mm^{-1}jn^{-1}j^{-1}m)$ which is $f(j^{-1}m)$ because $m^{-1}jn^{-1}j^{-1}m$ belongs to N. But the right hand side is exactly $\varphi * f_M$.

This proves the proposition.

For future use, it is worth noting a transitivity property of the Satake morphism constructed above.

In addition to the setting of 2.5 we assume given a closed subgroup B of G, which is the semi–direct product of an invariant closed subgroup U by a closed subgroup Z. We assume in addition that P contains B, M contains Z, N is contained in U and the central subgroup J is contained in Z. Concerning K we assume

(i) $G = KB$ (Iwasawa decomposition)

(ii) $(B \cap K)$ is the semi–direct product of $B \cap U$ by $B \cap Z$.

Those assumptions are of course inspired by the case of two parabolic subgroups P, B, with P containing B, in a reductive group G over F, with their Levi decompositions.

The assumptions in 2.5 and above have the following easy consequences:

a) $M \cap B$ is the semi–direct product of $M \cap U$ and Z.

b) U is the semi–direct product of N and $M \cap U$.

c) $M \cap B \cap K$ is the semi–direct product of $M \cap U \cap K$ and $Z \cap K$.

d) $U \cap K$ is the semi–direct product of $N \cap K$ and $M \cap U \cap K$.

We can apply Proposition 2.7 in three different situations.
Going from (G, K) to $(Z, Z \cap K)$ yields a map

$$S_G^M : \mathcal{H}(G, K, V, V') \longrightarrow \mathcal{H}(M, M \cap K, V^{N\cap K}, V'^{N\cap K})$$

Going from $(M, M \cap K)$ to $(Z, Z \cap K)$ yields a map

$$S_M^Z : \mathcal{H}(M, M \cap K, V^{N\cap K}, V'^{N\cap K}) \longrightarrow \mathcal{H}(Z, Z \cap K, V^{U\cap K}, V'^{U\cap K})$$

(note that $M \cap U \cap K$ acts on $V^{N\cap K}$ and by d) the set of fixed points is $V^{U\cap K}$).
Finally going directly from (G, K) to $(Z, Z \cap K)$ yields a map

$$S_G^Z : \mathcal{H}(G, K, V, V') \longrightarrow \mathcal{H}(Z, Z \cap K, V^{U\cap K}, V'^{U\cap K})$$

(as mentioned in 2.7, when $V = V'$ all three maps S are algebra homomorphisms).

Proposition.— $S_G^Z = S_M^Z \circ S_G^M$.

The proposition is of course no surprise. It can be given an abstract non–sense proof using the comment before Prop. 2.7 but for us it is quicker to use Prop. 2.7 itself. Let Φ in $\mathcal{H}(G, K, V)$ and x in Z. Then

$$S_G^M(\Phi)(x)(v) = \sum_{n\in N/N\cap K} \Phi(xn)(v) \qquad \text{for } v \text{ in } V^{N\cap K},$$

and consequently

$$S_M^Z \circ S_G^M(\Phi)(x)(v) = \sum_{\nu\in M\cap U/M\cap U\cap K} \sum_{n\in N/N\cap K} \Phi(x\nu n)(v)$$

for v in $V^{U\cap K}$.

On the other hand

$$S_G^Z(x)(v) = \sum_{u\in U/U\cap K} \Phi(xu)(v) \qquad \text{for } v \text{ in } V^{U\cap K}.$$

By properties b) and d) above this last summation on $U/U \cap K$ can be done first by summing over $N/N \cap K$ then over $M \cap U/M \cap U \cap K$. The result follows.

2.9

For use in § 4, we now investigate a situation where K, in addition to verifying the assumptions in 2.1 and 2.2, is **normal** in G.

We consider $\mathcal{H}(G,K,V,V')$ when V is given by a smooth character $\chi : K \to C^\times$ — so that the C–module V is C itself — and V' is a given by a smooth character $\chi' : K \to C^\times$. We write $\mathcal{H}(G,K,\chi,\chi')$, $\mathcal{H}(G,K,\chi)$ and $\mathcal{H}(G,K,\chi')$ instead of $\mathcal{H}(G,K,V,V')$, $\mathcal{H}(G,K,V)$ and $\mathcal{H}(G,K,V')$.

Let g be an element of G. It is immediate that the coset $gK = Kg$ supports a function in $\mathcal{H}(G,K,\chi,\chi')$ if and only if $\chi(x) = \chi'(gxg^{-1})$ for x in K, and that then there exists a unique such function τ_g with value 1_C at g. In particular, $\mathcal{H}(G,K,\chi,\chi')$ is non–zero if and only if χ and χ' are conjugate in G.

With g as above conjugating χ' into χ, we write τ'_{g-1} for the function in $\mathcal{H}(G,K,\chi',\chi)$ with support $g^{-1}K$ and value 1_C at g^{-1}. Then $\tau_g * \tau'_{g-1}$, is the unit of the algebra $\mathcal{H}(G,K,\chi)$ and $\tau'_{g-1} * \tau_g$ the unit of $\mathcal{H}(G,K,\chi')$, so that $\Phi \mapsto \tau_g * \Phi$ is an isomorphism – in fact an isomorphism of right modules over $\mathcal{H}(G,K,\chi)$ — of $\mathcal{H}(G,K,\chi)$ onto $\mathcal{H}(G,K,\chi,\chi')$, with inverse given by $\Psi \mapsto \tau'_{g-1} * \Psi$. Also there is an algebra isomorphism ι_g of $\mathcal{H}(G,K,\chi)$ onto $\mathcal{H}(G,K,\chi')$ given by $\Phi \mapsto \tau_g * \Phi * \tau'_{g-1}$.

Given the above remarks, we assume **from now on** $\chi' = \chi$. The coset gK, for g in G, supports a function in $\mathcal{H}(G,K,\chi)$ if and only if g belongs to the stabilizer G_χ of χ in G, which is a subgroup of G containing K, and there is a unique such function τ_g with value 1_C at g. If R is a set of representatives for G_χ/K in G, then $\mathcal{H}(G,K,\chi)$ is a free C–module with basis $(\tau_r)_{r\in R}$. We have the obvious multiplication formula

$$(*) \qquad\qquad \tau_g * \tau_{g'} = \tau_{gg'} \quad \text{for } g,\ g' \text{ in } G_\chi\,.$$

If G_χ/K is **abelian**, we get $\tau_{gg'} = \chi(gg'g^{-1}g'^{-1})\tau_{g'g}$ for g, g' in G_χ, and we define G'_χ as the set of g in G_χ such that $\chi(gxg^{-1}x^{-1}) = 1$ for all x in G_χ; clearly G'_χ contains K.

Assume G_χ/K abelian. For h, g, x in G_χ we have

$$\begin{aligned}\chi(ghx(gh)^{-1}x^{-1}) &= \chi(g(hxh^{-1}x^{-1})g^{-1})\chi(gxg^{-1}x^{-1})\\ &= \chi(hxh^{-1}x^{-1})\chi(gxg^{-1}x^{-1})\,,\end{aligned}$$

so that G'_χ is a subgroup of G_χ: take g, h in G'_χ or g in G'_χ and $h = g^{-1}$. Moreover we obtain $\chi(g^rxg^{-r}x^{-1}) = \chi(gxg^{-1}x^{-1})^r$ for any integer r and g, x

in G_χ. If χ has finite order, which is automatic if K is compact, then G_χ/G'_χ has exponent dividing that order and if moreover G_χ/K is finitely generated, then G'_χ has finite index in G_χ.

Proposition.— *Assume that K is normal in G and that G_χ/K is abelian. Then the centre of $\mathcal{H}(G,K,\chi)$ is the subalgebra $\mathcal{H}(G'_\chi,K,\chi)$ and $\mathcal{H}(G,K,\chi)$ is a free module over its centre of rank the cardinality of G'_χ/G_χ. If G_χ/K is finitely generated, $\mathcal{H}(G'_\chi,K,\chi)$ is a C–algebra of finite type; if moreover χ has finite order, G'_χ/G_χ is finite.*

Remark.— Assume that the character χ of K into $C^\times$ extends to a character $\tilde\chi$ of G'_χ into $C^\times$: this happens if C is an algebraically closed field since then $C^\times$ is divisible. Then the map $\Phi \mapsto \Phi\tilde\chi^{-1}$ induces an algebra isomorphism of $\mathcal{H}(G'_\chi,K,\chi)$ onto $\mathcal{H}(G'_\chi,K,C)$, and the latter is nothing but the group algebra $C[G'_\chi/K]$.

Proof of the Proposition. Choose a set R of representatives for G_χ/K in G. Let $\varphi = \sum\limits_{r\in R} \alpha_r\tau_r$ be an element of $\mathcal{H}(G,K,\chi)$ with the coefficients α_r taken in C. Then for s in R we have

$$\begin{aligned} \tau_s * \varphi &= \sum \alpha_r\tau_{sr} \text{ and} \\ \varphi * \tau_s &= \sum \alpha_r\chi(rsr^{-1}s^{-1})\tau_{sr}\,. \end{aligned}$$

Hence φ is in the centre of $\mathcal{H}(G,K,\chi)$ if and only if its support is in G'_χ. This proves the first assertion. If S is a set of representatives for G_χ/G'_χ in G_χ then by formula (*) above $(\tau_s)_{s\in S}$ is a basis of $\mathcal{H}(G,K,\chi)$ as a module over its centre $\mathcal{H}(G'_\chi,K,\chi)$. If G_χ/K is finitely generated, we have already seen before the proposition that G'_χ has finite index in G_χ provided χ has finite order; finally if $g_1,\ldots,g_r$ are elements of G'_χ whose images in G'_χ/K generate G'_χ/K, formula (*) implies that $\tau_{g_1},\ldots,\tau_{g_r}$ generate the C–algebra $\mathcal{H}(G'_\chi,K,\chi)$.

2.10

Keep the situation of 2.9, still assuming that G_χ/K is abelian (which is the case, of course, if G/K is abelian). It is interesting to know when $\mathcal{H}(G,K,\chi)$ is commutative, i.e. when $G'_\chi = G_\chi$. Clearly $G'_\chi = G_\chi$ means that $G_\chi/\mathrm{Ker}\chi$ is abelian.

Proposition.— *If G_χ/K is cyclic, $\mathcal{H}(G,K,\chi)$ is commutative.*

Indeed by construction $K/\mathrm{Ker}\chi$ is central in $G_\chi/\mathrm{Ker}\chi$. If G_χ/K is cyclic, then $G_\chi/\mathrm{Ker}\chi$ is necessarily abelian.

The following example shows that we can hardly expect to improve on the proposition, without further assumptions.

Example. Let G be a non–abelian group of order 8, and K its centre. Then K has order 2 and is also the commutator subgroup of G; the quotient G/K is abelian of exponent 2. If $\chi : K \to C^\times$ is a faithful character, $\mathcal{H}(G, K, \chi)$ is not commutative.

PROPOSITION.— *If G is a semi–direct product of K with a commutative subgroup S, then $\mathcal{H}(G, K, \chi)$ is commutative.*

Indeed each g in G can be written as ks with k in K and s in S, and g is in G_χ if and only if s is. Take now g and h in G_χ and decompose them as $g = ks$, $h = \ell t$. Then

$$ghg^{-1}h^{-1} = k(s\ell s^{-1})(sts^{-1}t^{-1})(tk^{-1}t^{-1})\ell^{-1}\,.$$

Since S is abelian and s, t are in G_χ we get

$$\chi(ghg^{-1}h^{-1}) = \chi(k\ell k^{-1}\ell^{-1}) = 1$$

and consequently $G'_\chi = G_\chi$. □

2.11

Let us stay in the context of 2.9, assuming further that $\Lambda = G/K$ is **abelian**. In § 7 we shall encounter a situation where we are given a submonoid Λ_- of Λ.

Let G_- be the inverse image of Λ_- in G. The submodule $\mathcal{H}(G_-, K, \chi)$ consisting of functions with support in G_- (or, equivalently, $G_- \cap G_\chi$) clearly forms a subalgebra of $\mathcal{H}(G, K, \chi)$. If $G_- \cap G_\chi$ generates G_χ as a group, the centre of $\mathcal{H}(G_-, K, \chi)$ is the submodule $\mathcal{H}(G'^{-}_\chi, K, \chi)$ of functions supported on $G'^{-}_\chi = G_- \cap G'_\chi$: indeed for each g in G_χ there are x, y in $G_- \cap G_\chi$ such that $g = x^{-1}y$, so that $\tau_g = (\tau_x)^{-1} * \tau_y$, and if φ in $\mathcal{H}(G_-, K, \chi)$ commutes with τ_x and τ_y, it also commutes with τ_g.

In § 3, Λ will be a finitely generated abelian group, and Λ_- a finitely generated submonoid of Λ. Then $G_- \cap G_\chi/K$ and $G_- \cap G'_\chi/K$ are submonoids of Λ_-, but it is not automatic that they are also finitely generated. Indeed if θ is a positive real number we can consider the submonoid $\{(x, y) \in \mathbb{N}^2 \mid y \leq \theta x\}$ of the additive monoid $\mathbb{N}^2$, but it is finitely generated if and only if

θ is rational. We shall use the well–known Gordan's lemma from the theory of convex polytopes [Fu, Prop. 1 p. 12].

LEMMA.— *Let $\mathcal{L}$ be a finitely generated free abelian group, and $\mathcal{C}$ a convex rational polyhedral closed cone in $\mathcal{L} \otimes \mathbb{R}$. Then $\mathcal{L} \cap \mathcal{C}$ is a finitely generated monoid.*

2.12

Finally, still in the context of 2.9, we mention a situation occuring in § 4.

We assume given a closed central subgroup J of G; we write $\bar{G}$ for the quotient G/J, $g \mapsto \bar{g}$ for the quotient map, and $\bar{K}$ for the image of K in $\bar{G}$. We assume that the character χ of K is trivial on $J \cap K$, i.e. comes via inflation from a character $\bar{\chi}$ of $\bar{K}$. Finally we assume that G/K is abelian, so that $\bar{G}/\bar{K}$, isomorphic to G/JK, is also abelian. For g, x in G we have $\chi(gxg^{-1}x^{-1}) = \bar{\chi}(\bar{g}\bar{x}\bar{g}^{-1}\bar{x}^{-1})$; it follows that G_χ is the inverse image of $\bar{G}_{\bar{\chi}}$ and similarly G'_χ is the inverse image of $\bar{G}'_{\bar{\chi}}$ (with obvious notation). Consequently $\mathcal{H}(\bar{G}, \bar{K}, \bar{\chi})$ is commutative if and only if $\mathcal{H}(G, K, \chi)$ is.

Remarks.— 1) Let Φ be in $\mathcal{H}(G, K, \chi)$. For g in G, the sum $\sum_{x \in J/J \cap K} \Phi(xg)$ is finite and clearly depends only on $\bar{g}$; writing it $\Phi(\bar{g})$ we get a function $\bar{\Phi}$ in $\mathcal{H}(\bar{G}, \bar{K}, \bar{\chi})$. Since $g \mapsto \bar{g}$ gives an isomorphism of G/JK onto $\bar{G}/\bar{K}$, we obtain that $\Phi \mapsto \bar{\Phi}$ is an algebra homomorphism, and $\mathcal{H}(\bar{G}, \bar{K}, \bar{\chi})$ appears as the quotient of $\mathcal{H}(G, K, \chi)$ by the two–sided ideal generated by the central elements $\tau_x - \tau_1$ for x in J.

2) In a slightly different situation, assume given a closed central subgroup J of G, and an extension $\tilde{\chi}$ of χ to a smooth character of JK. Then $\mathcal{H}(G, JK, \tilde{\chi})$ appears as the quotient of $\mathcal{H}(G, K, \chi)$ by the two–sided ideal generated by the central elements $\tau_x - \chi(x)\tau_1$ for x in J.

3 Parahoric subgroups

3.1

This section is mainly for reference. The field F is a locally compact non–Archimedean field with finite residue field k of characteristic p, and $\underline{G}$ is a connected reductive group over F. We put $G = \underline{G}(F)$ — we shall use similar notation for all algebraic groups over F. On G we put the natural topology, for which G is a locally pro–p topological group.

Following Haines and Rapoport [Ha–Ra], we recall one possible definition of parahoric subgroups of G — of course it is compatible with the one given by Bruhat and Tits [BT,II, 5.2.6 et 5.2.8] – and some of their properties. The parahoric subgroups of G are some particular open compact subgroups of G.

We fix a separable algebraic closure F_{sep} of F and write $\mathcal{G}$ for the Galois group of F_{sep}/F. We write F_u for the maximal unramified extension of F in F_{sep} and $\mathcal{I}$ for the inertia subgroup of $\mathcal{G}$, $\mathcal{I} = \mathrm{Gal}(F_{sep}/F_u)$; we put $\Gamma = \mathrm{Gal}(F_u/F)$ and write σ for the arithmetic Frobenius automorphism of F_u/F, which is a topological generator of Γ. We put $G_u = \underline{G}(F_u)$, and similarly for other algebraic groups over F_u.

3.2

To $\underline{G}$ is functorially associated a finitely generated abelian group $X^*(Z(\hat{\underline{G}})^{\mathcal{I}})$; when the derived group $\underline{G}_{der}$ of $\underline{G}$ is simply connected, it is the group of coinvariants $X_*(\underline{D})_{\mathcal{I}}$ where $\underline{D}$ is the torus $\underline{G}/\underline{G}_{der}$, for the natural action of $\mathcal{I}$ on the group $X_*(\underline{D})$ of cocharacters of $\underline{D}$.

We shall also need the canonical surjective homomorphism

$$q_G : X^*(Z(\hat{\underline{G}})^{\mathcal{I}}) \longrightarrow \mathrm{Hom}(X^*(\underline{G})^{\mathcal{I}}, \mathbb{Z})$$

whose kernel is the torsion subgroup of $X^*(Z(\hat{\underline{G}})^{\mathcal{I}})$ [K, 7.4.4]; when $\underline{G}_{der}$ is simply connected, it is simply given by the duality between $X_*(\underline{D})$ and $X^*(\underline{D})$ for $\underline{D} = \underline{G}/\underline{G}_{der}$.

We have a natural homomorphism $v_{G_u} : G_u \to \mathrm{Hom}(X^*(\underline{G})^{\mathcal{I}}, \mathbb{Z})$ given by $v_{G_u}(h)(\lambda) = val_{F_u}(\lambda(h))$ for λ in $X^*(\underline{G})^{\mathcal{I}}$, where val_{F_u} is the normalized valuation on F_u.

Kottwitz [K, 7.1 to 7.4] has defined a functorial surjective homomorphism $w_G : G_u \to X^*(Z(\hat{\underline{G}})^{\mathcal{I}})$ such that [K, 7.4.5]

$$v_{G_u} = q_G \circ w_G \, .$$

Consider the analogously defined homomorphism $v_G : G \to \mathrm{Hom}(X^*(\underline{G})^{\mathcal{G}}, \mathbb{Z})$, and the natural restriction map $\iota : \mathrm{Hom}(X^*(\underline{G})^{\mathcal{I}}, \mathbb{Z}) \to \mathrm{Hom}(X^*(\underline{G})^{\mathcal{G}}, \mathbb{Z})$. Clearly $v_G(g) = \iota v_{G_u}(g)$ for g in G.

LEMMA

(i) Ker $v_G = G \cap$ Ker v_{G_u}

(ii) Ker v_G *is the set of* g *in* G *such that* $w_G(g)$ *is torsion.*

Proof. Let $g \in G$. For χ in $X^*(\underline{G})^{\mathcal{I}}$ we have $\chi^\sigma(g) = \chi(g)$ since $g^\sigma = g$, so that $v_{G_u}(g)$ factors through the coinvariants of σ in $X^*(\underline{G})^{\mathcal{I}}$. But the natural map

$$X^*(\underline{G})^{\mathcal{G}} \longrightarrow (X^*(\underline{G})^{\mathcal{I}})_\sigma$$

has finite cokernel, as is easily seen by tensoring with $\mathbb{Q}$, so that $v_{G_u}(g)$ vanishes if and only if $v_G(g)$ vanishes. This gives (i), and (ii) follows since Kerq_G is the torsion subgroup of $X^*(Z(\hat{\underline{G}})^{\mathcal{I}})$.

Remark.— There is another useful way to look at the map v_G. Let $\underline{S}$ be the maximal F–split torus in the centre of $\underline{G}$. Then $X^*(\underline{G})^{\mathcal{G}} \to X^*(\underline{S})$ is injective with finite cokernel [cf. BT II, 4.2.6], which gives an injective map

$$\mathrm{Hom}(X^*(\underline{S}), \mathbb{Z}) \longrightarrow \mathrm{Hom}(X^*(\underline{G})^{\mathcal{G}}, \mathbb{Z})$$

with finite cokernel.

This results in an identification of $X_*(\underline{S}) \otimes_{\mathbb{Z}} \mathbb{R}$ with $\mathrm{Hom}(X^*(\underline{G})^{\mathcal{G}}, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R}$, and we may as well see v_G as a map to $X_*(\underline{S}) \otimes_{\mathbb{Z}} \mathbb{R}$, with image a lattice in that real vector space, and even in the rational vector space $X_*(\underline{S}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

3.3

We write $\mathcal{B}$ for the building of the adjoint group $\underline{G}_{ad}$ of $\underline{G}$ over F_u; it is a polysimplicial complex on which G_u acts by simplicial automorphisms. The set $\mathcal{B}^\sigma$ of fixed points under σ is the building of $\underline{G}_{ad}$ over F; it is also a polysimplicial complex and G acts on $\mathcal{B}^\sigma$ by simplicial automorphisms.

Each facet in $\mathcal{B}^\sigma$ is contained in a unique σ–invariant facet of $\mathcal{B}$ and in this way we get a bijection between facets of $\mathcal{B}^\sigma$ and σ–invariant facets of $\mathcal{B}$: the inverse map is obtained by intersecting a σ–invariant facet of $\mathcal{B}$ with $\mathcal{B}^\sigma$. Besides alcoves in $\mathcal{B}^\sigma$ correspond to σ–invariant alcoves in $\mathcal{B}$.

Let $\mathcal{F}$ be a facet in $\mathcal{B}$. The corresponding parahoric subgroup $K_{G_u}(\mathcal{F})$ of G_u is the set of g in Kerw_G which act trivially on $\mathcal{F}$. It is an open bounded subgroup of G_u. A **parahoric** subgroup of G_u is a subgroup of the form $K_{G_u}(\mathcal{F})$ for some facet $\mathcal{F}$ in $\mathcal{B}$. [BT II, 5.2.6]

If $\mathcal{F}$ is a σ–invariant facet of $\mathcal{B}$, we put $K_G(\mathcal{F}) = K_{G_u}(\mathcal{F})^\sigma$; it is an open compact subgroup of G. A **parahoric** subgroup of G is a subgroup of the form $K_G(\mathcal{F})$ for some σ–invariant facet $\mathcal{F}$ in $\mathcal{B}$. If $\mathcal{F}'$ is the facet $\mathcal{F} \cap \mathcal{B}^\sigma$ of $\mathcal{B}^\sigma$ we also put $K_G(\mathcal{F}') = K_G(\mathcal{F})$ [BT II, 5.2.6 and 5.2.8].

Remarks.— 1) If $\mathcal{F}$ is a σ–invariant facet of $\mathcal{B}$, then $H^1(\sigma, K_{G_u}(\mathcal{F})) = 1$ [Ha–Ra, Remark 9].

2) If $\mathcal{F}$ is a σ–invariant facet of $\mathcal{B}$, we shall also consider a slightly larger group $\tilde{K}_G(\mathcal{F})$: it is the group of elements h of G fixing $\mathcal{F}$ such that $w_G(h)$ is torsion. By the lemma in 3.2 it is the group of elements in $\mathrm{Ker} v_G$ fixing $\mathcal{F}$. Clearly $K_G(\mathcal{F})$ has finite index in $\tilde{K}_G(\mathcal{F})$ so that $\tilde{K}_G(\mathcal{F})$ is open and compact in G.

3.4

When $\underline{G}$ is a torus, $\mathcal{B}$ has only one point, G_u is abelian and has only one parahoric subgroup K_{G_u}. The quotient G_u/K_{G_u}, isomorphic to $X_*(\underline{G})_\mathcal{I}$ via w_G, is a finitely generated abelian group. The inverse image in G_u of the torsion subgroup of G_u/K_{G_u} is the unique maximal bounded subgroup $\tilde{K}_{G_u}$ of G_u; it contains K_{G_u} as an open invariant subgroup of finite index. If $X_*(\underline{G})_\mathcal{I}$ has no torsion, then $\tilde{K}_{G_u} = K_{G_u}$; this happens for example when $\underline{G}$, over F_u, is a product of induced tori.

In a similar manner, when $\underline{G}$ is anisotropic mod.centre, $\mathcal{B}^\sigma$ has only one point, G has only one parahoric subgroup K_G, and G/K_G is a finitely generated abelian group. The inverse image in G of the torsion subgroup of G/K_G is the unique maximal compact subgroup $\tilde{K}_G$ of G; it contains K_G as an open invariant subgroup of finite index. Note also that if $\underline{S}$ is the maximal split central torus in $\underline{G}$, then $K_G \cap S$ and $\tilde{K}_G \cap S$ are equal to the maximal compact subgroup of S: indeed $\tilde{K}_G \cap S$ is compact hence contained in $\tilde{K}_S$, and on the other hand $K_G \cap S$ contains K_S by functoriality of the Kottwitz morphism; but $K_S = \tilde{K}_S$ because $\underline{S}$ is a split torus. Note also that S/K_S has finite index in G/K_G.

3.5

Some exact sequences of groups are useful.

(i) Assume that $\underline{G}_{der}$ is simply connected, and write $\underline{D} = \underline{G}/\underline{G}_{der}$. If $\mathcal{F}$ is a facet of $\mathcal{B}$, then the natural exact sequence

$$1 \longrightarrow K_{G_{der,u}}(\mathcal{F}) \longrightarrow K_{G_u}(\mathcal{F}) \longrightarrow K_{D,u} \longrightarrow 1$$

is exact (assertion c) in the proof of Prop. 3 in [Ha–Ra]).

If $\mathcal{F}$ is σ–invariant, then taking fixed points under σ gives (3.3 Remark 1) an induced exact sequence

$$1 \longrightarrow K_{G_{der}}(\mathcal{F}) \longrightarrow K_G(\mathcal{F}) \longrightarrow K_D \longrightarrow 1\,.$$

(ii) Assume we are given a z–extension $\underline{G}'$ of $\underline{G}$ with kernel $\underline{Z}'$. Then the exact sequence

$$1 \longrightarrow Z'_u \longrightarrow G'_u \longrightarrow G_u \longrightarrow 1$$

gives rise to an exact sequence

$$1 \longrightarrow K_{Z'_u} \longrightarrow K_{G'_u}(\mathcal{F}) \longrightarrow K_{G_u}(\mathcal{F}) \longrightarrow 1$$

for any facet $\mathcal{F}$ of $\mathcal{B}$. If $\mathcal{F}$ is σ–invariant we get another exact sequence

$$1 \longrightarrow K_{Z'} \longrightarrow K_{G'}(\mathcal{F}) \longrightarrow K_G(\mathcal{F}) \longrightarrow 1$$

(assertion a) in the proof of Prop. 3 in [Ha–Ra]).

3.6

A parahoric subgroup K of G has a characteristic subgroup, its pro–p radical, the properties of which we now recall.

Lemma.— *Let H be a profinite group, with an open pro–p subgroup J. Then H has a largest open normal pro–p subgroup.*

Proof. The subgroup $J' = \bigcap_{g\in H/J} gJg^{-1}$ is an open subgroup of H, as an intersection of finitely many open subgroups; by construction it is normal in H, and is a pro–p group. In the finite discrete group H/J', take the intersection of the p–Sylow subgroups; its inverse image H_+ in H is clearly an open normal pro–p subgroup. If H' is another open normal pro–p subgroup of H, its image in H/J' is a normal p–subgroup, hence is included in the intersection of the p–Sylow subgroups of H/S'; consequently H' is contained in H_+, which proves the lemma.

Definition.— *If H is a profinite group with an open pro–p subgroup, we write H_+ for its largest open normal pro–p subgroup, and we call it the pro–p radical of H.*

3.7

Fix a parahoric subgroup K of G. Its pro–p radical K_+ has another description using Bruhat–Tits theory, which we now recall. As usual we write $\mathcal{O}_F$ for the ring of integers of F, P_F for its maximal ideal, and k_F for the residue field $\mathcal{O}_F/P_F$.

Indeed K is canonically the group of points over $\mathcal{O}_F$ of a smooth connected affine group scheme $\mathcal{G}_K$ over $\mathcal{O}_F$, with generic fibre $\underline{G}$; that group is written $\mathfrak{G}_x^0$ in [BT II 5.1, 30] if K fixes the point x in the building of G_{ad}. Writing $\bar{\mathcal{G}}_K$ for its special fibre, the map from $\mathcal{G}_K(\mathcal{O}_F)$ to $\bar{\mathcal{G}}_K(k_F)$ obtained by reduction mod P_F is surjective (by smoothness and Hensel's lemma, see also [BTII, 5.1.32 (ii)]), and its kernel is an open pro–p subgroup of K.

Let $\mathcal{R}$ be the unipotent radical of $\bar{\mathcal{G}}_K$, so that the quotient $\bar{\mathcal{G}}_K^{red} = \bar{\mathcal{G}}_K/\mathcal{R}$ is the maximal reductive quotient of $\bar{\mathcal{G}}_K$. If $\bar{k}$ is an algebraic closure of k_F then we get an exact sequence of finite groups

$$1 \longrightarrow \mathcal{R}(\bar{k}) \longrightarrow \bar{\mathcal{G}}_K(\bar{k}) \longrightarrow \bar{\mathcal{G}}_K^{red}(\bar{k}) \longrightarrow 1\,.$$

But the finite field k_F is perfect, so $\mathcal{R}$ is a split unipotent group over k_F. Therefore $H^1(k_F, \mathcal{R}(\bar{k}))$ is trivial, and taking fixed points under the Galois group of $\bar{k}$ over k_F we get another exact sequence of groups

$$1 \longrightarrow \mathcal{R}(k_F) \longrightarrow \bar{\mathcal{G}}_K(k_F) \longrightarrow \bar{\mathcal{G}}_K^{red}(k_F) \longrightarrow 1$$

where $\mathcal{R}(k_F)$ is a p–group.

Proposition.— *Fix a parahoric subgroup K of G. The pro–p radical K_+ of K is the kernel of the composite map from $K = \mathcal{G}_K(\mathcal{O}_F)$ to $\bar{\mathcal{G}}_K^{red}(k_F)$.*

Proof. Indeed from the construction that kernel is an open pro–p subgroup of K, hence is included in K_+. The reverse inclusion comes from the following lemma, applied to the reductive group $H = \bar{\mathcal{G}}_K^{red}$ over k_F.

Lemma.— *Let $\underline{H}$ be a connected reductive group over a finite field k of characteristic p, and H the finite group $\underline{H}(k)$. Then any normal p–subgroup of H is trivial.*

The argument is well–known to experts and has been indicated to us by F. Digne. Let $\underline{B}$ be a Borel subgroup of $\underline{H}$ and $\underline{U}$ its unipotent radical. Looking at cardinals one sees that $U = \underline{U}(k)$ is a p–Sylow subgroup of H; as all p–Sylow subgroups of H are conjugate, a normal p–subgroup J of H is contained in U. But if $\underline{B}^-$ is a Borel subgroup of $\underline{G}$ opposite to $\underline{B}$, J is also contained in $U^- = \underline{U}^-(k)$ where $\underline{U}^-$ is the unipotent radical of $\underline{B}^-$, so that J is contained in $U \cap U^-$ which is trivial. $\square$

4 The case where G is compact mod. centre

4.1

In this section, C is any commutative ring, the field F is the same as in § 3, and the connected reductive group $\underline{G}$ over F is assumed to be anisotropic mod.centre — equivalently, the topological group $G = \underline{G}(F)$ is compact mod.centre.

As recalled in 3.4, G has a unique parahoric subgroup K, which is thus invariant in G, and the quotient G/K is a finitely generated abelian group. Also, G has a unique maximal compact subgroup $\tilde{K}$ and $\tilde{K}/K$ is the torsion subgroup of G/K. The pro–p radical K_+ of K is invariant in G too, and the quotient K/K_+ is a finite abelian group of order prime to p. Indeed the group $\bar{\mathcal{G}}_K^{red}$ of 3.7 is a torus; examples in 4.2 will show that in general G/K_+ is not abelian.

We fix a character $\chi : K \to C^\times$ trivial on K_+ and we investigate the Hecke algebra $\mathcal{H}(G, K, \chi)$, in particular its commutativity. As in 2.9 we introduce the subgroups G_χ and G'_χ of G; as K/K_+ is finite, χ has only finitely many conjugates under G, and G_χ has finite index in G. As G_χ/K is finitely generated, G'_χ has finite index in G_χ (2.9).

The algebra $\mathcal{H}(G, K, \chi)$ is commutative exactly when $G'_\chi = G_\chi$. That is clearly the case when χ is trivial; in that case from 2.9 Proposition we deduce:

Proposition.— *($\underline{G}$ anisotropic mod.centre) The Hecke algebra $\mathcal{H}(G, K, C)$ is a commutative algebra of finite type over C.*

Remarks.— 1) If G is semi–simple and simply connected, Kottwitz's application w_G is trivial, and G is equal to K so that $\mathcal{H}(G, K, \chi)$ is isomorphic to C for any χ. This is of course a rare and trivial case.

2) As we shall see in 4.4, $\mathcal{H}(G, K, \chi)$ is not always commutative. But from 2.9 Proposition, we know that its centre is $\mathcal{H}(G'_\chi, K, \chi)$, a finitely generated C–algebra; moreover $\mathcal{H}(G, K, \chi)$ is a free module over $\mathcal{H}(G'_\chi, K, \chi)$ of finite rank $|G_\chi/G'_\chi|$.

3) Similarly, for any subgroup K' between K and the maximal compact subgroup $\tilde{K}$ we have that $\mathcal{H}(G, K', C)$ is commutative.

4.2

Let us first give a few more examples where $\mathcal{H}(G, K, \chi)$ is commutative.

Let E be a finite separable extension of F, and D a central division algebra over E, of finite degree. The multiplicative group $D^\times$ is compact modulo its centre $E^\times$. We can take $\underline{G}$ such that $G = \underline{G}(F) = D^\times$. The derived group $\underline{G}_{der}$ of $\underline{G}$ is simply connected, and $\underline{G}_{der}(F)$ is the group D^1 of elements in D with reduced norm to E equal to 1; the quotient $\underline{G}/\underline{G}_{der}$ is the induced torus $\underline{T}$ such that $\underline{T}(F) = E^\times$.

We have the exact sequence of groups

$$1 \longrightarrow D^1 \longrightarrow D^\times \xrightarrow{N} E^\times \longrightarrow 1$$

given by the reduced norm N, and K is the inverse image of the unique parahoric subgroup U_E of $E^\times$ (3.3 and 3.4). This implies that K, equal to $\tilde{K}$, is the group of units U_D in D, and that K_+ is the group of principal units U_D^1; in particular $G/K = D^\times/U_D$ is isomorphic to $\mathbb{Z}$, and unless $D = E$, G/K_+ is not abelian. From the first proposition in 2.10, we deduce:

Proposition.—*With $G = D^\times$ as above, the Hecke algebra $\mathcal{H}(D^\times, U_D, \chi)$ is commutative for any character $\chi : U_D \to C^\times$ trivial on U_D^1.*

Remark.— Clearly we can also take for G a product of groups $D_i^\times$, where D_i is a division algebra as above, and the corresponding Hecke algebras $\mathcal{H}(G, K, \chi)$ are always commutative. We can also take the product of such a group with any torus, and commutativity still holds.

4.3

Keep the situation of 4.2. The torus $\underline{T}$ also appears as the centre of $\underline{G}$ and taking F–rational points gives an exact sequence of groups

$$1 \longrightarrow E^\times \longrightarrow D^\times \longrightarrow G_{ad} \longrightarrow 1\,,$$

where $\underline{G}_{ad}$ is the adjoint group of G.

Writing K_{ad} for the unique parahoric subgroup of G_{ad}, we get an exact sequence of groups $1 \to U_E \to U_D \to K_{ad} \to 1$, and K_{ad}/K_{ad^+} gets identified with $k_D^\times/k_E^\times$, where k_E is the residue field of E, and k_D that of D. Note that G_{ad} is compact so that K_{ad} is **not** a maximal compact subgroup of G_{ad}.

From 2.12 and 4.2 Proposition we get

PROPOSITION.— *In the situation above, let χ be a character $K_{ad} \to C^\times$ trivial on K_{ad_+}. Then the algebra $\mathcal{H}(G_{ad}, K_{ad}, \chi)$ is commutative.*

That can also be obtained from 2.9 since G_{ad}/K_{ad} is cyclic.

As in 4.2 Remark, we can take products, which by [BTIII] yield all semi–simple groups which are anisotropic mod. centre and of adjoint type.

COROLLARY.— *Assume that the group $\underline{G}$ of* 4.1 *is (anisotropic and) semi–simple of adjoint type. Then $\mathcal{H}(G, K, \chi)$ is commutative for any character $\chi : K \to C^\times$ trivial on K_+.*

4.4

We now give an example where $\mathcal{H}(G, K, \chi)$ is **not** commutative. In that example $\underline{G}_{der}$ is simply connected, but $\underline{G}$ is not semisimple. At this moment we do not know whether there is such an example with $\underline{G}$ semisimple (but of course not simply connected cf. 4.1 Remark).

We assume p odd, and we choose a ramified quadratic extension E of F; we write $y \mapsto \bar{y}$ for the non–trivial automorphism of E/F. We also choose a division algebra D with centre E and reduced degree 4, such that a uniformizer of D acts on its residue field k_D via the Frobenius automorphism of k_D over the residue field k_E of E. We write N for the reduced norm from D to E; on residue fields, it induces the norm from k_D to k_E, which we write n.

Let $G = \{d, x, y) \in D^\times \times E^\times \times E^\times \mid N(d)x^2y/\bar{y} = 1\}$. This is clearly the group of F–points of a linear algebraic group $\underline{G}$ over F. As N is surjective, we have a surjective homomorphism $(d, x, y) \mapsto (x, y)$ from G to $E^\times \times E^\times$ with kernel $D^1 = \mathrm{Ker} N$. The exact sequence

$$1 \longrightarrow D^1 \longrightarrow G \longrightarrow E^\times \times E^\times \longrightarrow 1$$

comes from an exact sequence of algebraic groups

$$1 \longrightarrow \underline{G}^1 \longrightarrow \underline{G} \longrightarrow \underline{T} \longrightarrow 1\,.$$

As $\underline{G}^1$ is connected reductive and $\underline{T}$ is a torus, $\underline{G}$ is connected reductive, and it follows that $\underline{G}^1$ is the derived group of G.

Because $\underline{T}$ is an induced torus, the unique parahoric subgroup of $E^\times \times E^\times$ is $U_E \times U_E$ and from 3.5 (i) we get an exact sequence of groups

$$1 \longrightarrow D^1 \longrightarrow K \longrightarrow U_E \times U_E \longrightarrow 1$$

for the unique parahoric subgroup K of G. We deduce that

$$\begin{aligned} \tilde{K} = \quad K \quad &= \{(d,x,y) \in U_D \times U_E \times U_E \mid N(d)x^2y/\bar{y} = 1\} \quad \text{and} \\ K_+ \quad &= \{(d,x,y) \in U_D^1 \times U_E^1 \times U_E^1 \mid N(d)x^2y/\bar{y} = 1\}\,, \quad \text{so} \end{aligned}$$

that K/K_+ appears as $\{(z,t,u) \in k_D^\times \times k_E^\times \times k_E^\times \mid n(z)t^2 = 1\}$.

Proposition.— *Assume that k has 3 elements. Let ε be a character $k_D^\times \to C^\times$ of order 16, and let χ be the character $(z,x,y) \mapsto \varepsilon(z \mod U_D)$ of K. Then $\mathcal{H}(G,K,\chi)$ is **not** commutative.*

Remark.— The group $k_D^\times$ has order $80 = 3^4 - 1$, so we have $\varepsilon(-1) = -1$. We can take $C = k_D$ and $\varepsilon(z) = z^5$. We can also choose for C the field of complex numbers: that gives an example of intertwining algebra, over $\mathbb{C}$, for level zero [cf. Mo], which is not commutative; we believe this is the first example of such.

Proof. We compute the subgroups G_χ and G'_χ of 2.11. Let $g = (d,x,y)$ be in G; its action on K/K_+ depends only on the valuation v of d and is given by $(z,t,u) \mapsto (z^{3^v}, t, u)$. By the condition $N(d)x^2y/\bar{y} = 1$, v is even. On the other hand, the condition $n(z)t^2 = 1$ imposes $n(z) = 1$ i.e. $z^{40} = 1$ so that z is a square in $k_D^\times$. As ε has order 16, we get

$$\varepsilon(z^{3^v - 1}) = 1 \text{ for even } v, \quad \text{so that } G_\chi = G\,.$$

On the other hand, let $\tilde{\omega}$ be a uniformizer of D; then $g = (\tilde{\omega}^2, N(\tilde{\omega})^{-1}, 1)$ belongs to G. Let ξ be an element of U_D with reduced norm -1 to E; its image z in $k_D^\times$ satisfies $n(z) = z^{40} = -1$. If $\tilde{\omega}_E$ is a uniformizer of E with $\tilde{\omega}_E^2$ in F, then $h = (\xi, 1, \tilde{\omega}_E)$ also belongs to G. We compute

$$ghg^{-1}h^{-1} \mod K_+ = (z^8, 1, 1)$$

and $\chi(ghg^{-1}h^{-1}) = \varepsilon(z^8)$. Since $\varepsilon(z^{40}) = \varepsilon(-1) = -1$, we see that G'_χ is distinct from G_χ (equal to G) and $\mathcal{H}(G,K,\chi)$ is not commutative indeed.

4.5

We have presented our simplest example, but the same principle can be used to provide other examples, in any residue characteristic. We only indicate the modifications.

If p is odd, and the cardinality q of k is congruent to 1 modulo 4, then we can take the same construction as above: E/F is quadratic ramified, D/E is a central division algebra of degree 16, and $\underline{G}$ is given by the equation $N(x)y^2z/\bar{z} = 1$ in $D^\times \times E^\times \times E^\times$, K being given by the same equation in $U_D \times U_E \times U_E$, and K/K_+ by the equation $n(\bar{x})\bar{y}^2 = 1$ in $k_D^\times \times k_E^\times \times k_E^\times$. We take a character ε from $k_D^\times$ to $C^\times$ with order 2^{r+1} where r is the 2–adic valuation of $q^2 - 1$, and we put $\chi(x, y, z) = \varepsilon(x \mod U_D)$ for (x, y, z) in G. If p is odd and q is congruent to 3 modulo 4, we use the previous example over a quadratic unramified extension F' of F — where the cardinality of the residue field is q^2, congruent to 1 modulo 8 — and take the Weil restriction from F' to F to get an example over F.

If p is 2 and q is congruent to 1 modulo 3, we take E/F cubic cyclic ramified, D/E a central division algebra of degree 81, $\underline{G}$ being given by the equation $N(x)y^3z/z^\tau = 1$ in $D^\times \times E^\times \times E^\times$, where τ is one of the non–trivial automorphisms of E/F. Then K is given by the same equation in $U_D \times U_E \times U_E$, and K/K_+ by the equation $n(\bar{x})y^3 = 1$ in $k_D^\times \times k_E^\times \times k_E^\times$. We then take for ε a character from $k_D^\times$ to $C^\times$ of order 3^{t+1} where t is the 3–adic valuation of $q^3 - 1$ and we put $\chi(x, y, z) = \varepsilon(x \mod U_D)$ for (x, y, z) in G, as above. If p is 2 and q is congruent to $-1 \mod 3$, we use a quadratic unramified extension as in the case where p is odd.

5 Irreducible mod.p representations of parahoric subgroups

5.1

This section is also for reference, to be used in the final § 7. In this section, C is a field of characteristic p, and k is a finite field of the same characteristic. There is no other relation between C and k (cf. Remark 5.5).

We are interested in irreducible smooth representations of a parahoric group K as in 3.3, on a C–vector space V. As V is not zero and the pro–p–radical K_+ of K is a pro–p group, K_+ has a non–zero fixed point in V;

because V is irreducible and K_+ is invariant in K, K_+ acts trivially on V, so that K acts on V via its quotient K/K_+.

As recalled in 3.4, that quotient is the group of points of a connected reductive group over k. We thus recall the representation theory of such groups in the natural characteristic p. Our main reference is the book of Cabanes and Enguehard [CE, Chapter 1].

Linear algebraic groups over k will be denoted by underlined capital letters like $\underline{G}$, and the group of k–rational points by the corresponding ordinary capital letter, like G.

We fix a connected reductive group $\underline{G}$ over k, a maximal k–split torus $\underline{S}$ in $\underline{G}$, and we write $\underline{T}$ for the centralizer of $\underline{S}$ in $\underline{G}$; it is a torus since $\underline{G}$ is quasi–split over k. We fix a Borel subgroup $\underline{B}$ of $\underline{G}$ containing $\underline{T}$, and write $\underline{U}$ for the unipotent radical of $\underline{B}$.

We let Φ be the set of roots of $\underline{G}$ relative to $\underline{S}$, and Δ the set of simple roots determined by the choice of $\underline{B}$. For each root a in Φ, we let $\underline{U}_a$ be the corresponding root subgroup of $\underline{G}$ (written $\underline{U}_{(a)}$ in [Bo, 21.9]).

Writing $\underline{N}$ for the normalizer of $\underline{S}$ in $\underline{G}$, we have the relative Weyl group $W = \underline{N}/\underline{T}$; it is known that $W = \underline{N}(k)/\underline{T}(k) = N/T$. [Bo, 21.2 Theorem]. For each a in Δ there is a corresponding element s_a in W with $s_a^2 = 1$ [Bo] loc. cit. and those element generate W. We write $\mathcal{S}$ for the set of such reflections.

5.2

The results of Cabanes and Enguehard apply to strongly split BN–pairs of characteristic p [CE, Déf. 2.20]. Although that notion is clearly inspired by the case of reductive groups over finite fields, they do not seem to state the following, which is certainly well–known, possibly obvious to the experts.

LEMMA.— $(G, B, N, \mathcal{S})$, *together with the decomposition* $B = TU$, *form a strongly split* BN*–pair of characteristic* p.

Remark.— We insist that the lemma is true whether or not G is split over k.

Proof. We review the different parts of the definition of loc. cit. First $(G, B, N, \mathcal{S})$ has to be a BN–pair, which is true by [Bo, Prop. 21.15]. Second B has to the semi–direct product of an invariant p–group U and a commutative group T of order prime to p, which is indeed true in our case.

Third, we need $B \cap B^{w_0} = T$, where w_0 is the longest element of W (with respect to $\mathcal{S}$).

Those first three conditions mean that we have a split BN–pair of characteristic p in the sense of loc. cit. But Carter [Carter, Chapter 2] has a stricter notion of split BN–pair in that he imposes the condition $\bigcap_{n\in N} nBn^{-1} = T$, which he shows is true in our case. Moreover that condition indeed implies $B \cap B^{w_0} = T$ [Carter, Prop. 2.5.5 (ii)].

To have a **strongly** split BN–pair of characteristic p, Cabanes and Enguehard impose a further condition which is a consequence of condition (C) in [CE, § 2 exer. 5(a), p. 39] — in fact it is equivalent to (C) by the end of the exercise. Condition (C) is imposed on some "root subgroups" X_α of G attached to the non–divisible roots α in Φ — it is known by [B, Lie VI § 1, Prop. 15] that those roots are the images of the simple roots in Δ by the action of W.

Condition (C) says:

(C) If α and β are non–divisible roots in Φ, $\alpha \neq \pm\beta$, then the commutators (x, y), for x in X_α and y in X_β, are contained in the subgroup generated by the X_γ's, where γ runs through roots which can be written as $\gamma = a\alpha + b\beta$ for positive integers a and b.

Again that is stated by Carter [Carter, p. 57], but for subgroups Y_α which are, at least formally, defined in a different manner.

In [CE], X_α is the set of p–elements in a group B_α which is defined as follows: write $\alpha = w\delta$ for an element w of W and δ in Δ, and then $B_\alpha = {}^w(B \cap B^{w_0 s_\delta})$. On the other hand [Carter, p. 57 line -1] Y_α is ${}^wY_\delta$ where $Y_\delta = U \cap U^{w_0 s_\delta}$ [Carter, p. 50]. Now $B = TU$ gives $B^{w_0 s_\delta} = TU^{w_0 s_\delta}$ as W normalizes T, and by [Carter Prop. 2.5.9] $B \cap B^{w_0 s_\delta} = T(U \cap U^{w_0 s_\delta})$ so that finally $Y_\alpha = X_\alpha$ indeed.

This ends the proof of the lemma!

5.3

[CE, Theorem 6.10] provides, under some condition (*) on C, a precise relationship between irreducible C–representations of G, and characters of the Hecke algebra $\mathcal{H}(G, U, C)$.

By [CE, Prop. 6.6], G is the disjoint union of the double cosets UnU where n runs through N. It follows that $\mathcal{H}(G, U, C)$ has a basis T_n where, for n in N, T_n corresponds to the double coset UnU; moreover the structure constants giving the multiplication in $\mathcal{H}(G,U,C)$ in that basis are in the prime field of C.

In general, $\mathcal{H}(G,U,C)$ is not commutative. However, writing $g_{p'}$ for the prime–to–p part of the cardinality of G, assume

$$(*) \qquad C \text{ contains all } g_{p'}\text{-th roots of unity}.$$

Then [CE, Thm. 6.10] gives:

(i) If V is an irreducible C–representation of G, V^U is a simple module over $\mathcal{H}(G,U,C)$.

(ii) The assignment $V \to V^U$ gives a bijection between isomorphism classes of irreducible C–representations of G and isomorphism classes of simple modules over $\mathcal{H}(G,U,C)$.

(iii) Every simple module over $\mathcal{H}(G,U,C)$ has dimension 1.

In particular isomorphism classes of irreducible C–representations of G correspond bijectively to characters $\mathcal{H}(G,U,C) \to C$. In turn those characters are parametrized bijectively by pairs (χ, I) where χ is a character $T \to C^\times$ and I is any subset of a set of simple roots Δ_χ determined by χ: for any root a in Δ, we let T_a be the intersection of T with the subgroup generated by U_a and U_{-a}, and Δ_χ is the set of roots a such that χ is trivial on T_a. To such a pair (χ, I) corresponds the character $\psi(\chi, I)$ of $\mathcal{H}(G,U,C)$ defined as follows: for n in N with image w in W, take a reduced decomposition $w = s_{a_j} \cdot \ldots \cdot s_{a_r}$, lift it to a decomposition of $n = n_1 \cdot \ldots \cdot n_r t$ (with $n_i \in s_{a_i}$ for $i = 1, \ldots, r$, and t in T) and put $\psi(\chi, I)(T_n) = (-1)^r \chi(t)$ if $a_1, \ldots, a_r$ all belong to I and otherwise $\psi(\chi, I)(T_n) = 0$; in particular $\psi(\chi, I)(t) = \chi(t)$ for all t in T.

5.4

Still under condition (*), let us derive a few consequences of the previous results.

(a) Every irreducible C–representation of G is defined over the finite field generated by the $g_{p'}$–th roots of unity. Indeed all characters $\psi(\chi, I)$ are clearly defined over such a field.

(b) All irreducible C–representations V of G are absolutely irreducible: the commutant of V is reduced to scalars, and the same remains true over any extension C' of C.

(c) Let V be an irreducible C–representation of G, with associated character $\psi = \psi(\chi, I)$. Let σ be an automorphism of C. Then the character associated to $C \otimes_\sigma V$ is $\psi(\sigma \circ \chi, I)$. In particular V and $C \otimes_\sigma V$ are isomorphic if and only if $\sigma \circ \chi = \chi$. Waldspurger's proof [W, lemme 1.1] adapts to give that V is in fact defined over the field of values of ψ.

5.5

We now deduce some results without condition (*), i.e. for a general field C of characteristic p.

Proposition (*i*) *If V is an absolutely irreducible C–representation of G, V^U has dimension* 1.

(*ii*) *The assignment $V \to V^U$ yields a bijection between isomorphism classes of absolutely irreducible C–representations of G and characters $\mathcal{H}(G, U, C) \to C$.*

(*iii*) *The characters $\mathcal{H}(G, U, C) \to C$ are parametrized bijectively by pairs (χ, I) with χ a character $T \to C^\times$ and I a subset of Δ_χ, with the same formulas as above.*

Remark. We can take for example the trivial representation of G on $C = \mathbb{Z}/p\mathbb{Z}$, whatever k is.

Proof. The theorem is certainly true when C satisfies (*). In general adjoin to C all $g_{p'}$–th roots of unity. We obtain a finite Galois extension C'/C and C' satisfies (*).

(a) If V is an absolutely irreducible C–representation of G, then $C' \otimes_C V$ is an irreducible C'–representation of G, so $(C' \otimes_C V)^U$ has dimension 1 over C'. But $(C' \otimes_C V)^U = C' \otimes_C V^U$, so that V^U has dimension 1 over C. This proves (i).

(b) Let V_1, V_2 be absolutely irreducible C–representations of G, and ψ_1, ψ_2 the corresponding characters $\mathcal{H}(G, U, C) \to C$. If V_1, V_2 are isomorphic clearly $\psi_1 = \psi_2$. Conversely assume $\psi_1 = \psi_2$. Consider $C' \otimes_C V_i$ for $i = 1, 2$; the corresponding character of $\mathcal{H}(G, U, C') = C' \otimes_C \mathcal{H}(G, U, C)$

is simply given by $1_{C'} \otimes \psi_i$. As $1_{C'} \otimes \psi_1 = 1_{C'} \otimes \psi_2$ we see that $C' \otimes_C V_1$ and $C' \otimes_C V_2$ are isomorphic C'–representations of G. Consequently V_1^d and V_2^d, where d is the degree of C'/C, are isomorphic, and so are V_1 and V_2. This proves the injectivity assertion in (ii).

(c) If ψ is a character $\mathcal{H}(G, U, C) \to C$, its restriction to elements T_t for t in T clearly gives a character $\chi : T \to C^\times$. Moreover $1_{C'} \otimes \psi$ is a character of $\mathcal{H}(G, U, C')$ so it is of the form $\psi(\iota \circ \chi, I)$ for some $I \subset \Delta_\chi$, where we have written ι the inclusion of C into C'. But then obviously ψ is given by the formulas in 5.3 for $\psi(\chi, I)$, and ψ determines both χ and I. In the other direction, if a parameter (χ, I) is given where χ is a character $T \to C^\times$ and I a subset of Δ_χ, then $\psi(\iota \circ \chi, I)$ is a character $\mathcal{H}(G, U, C') \to C'$; its restriction to $\mathcal{H}(G, U, C)$ is a character taking values in C so the formulas in 5.3 indeed define a character $\psi(\chi, I)$ from $\mathcal{H}(G, U, C)$ to C. This proves (iii).

(d) Let $\psi = \psi(\chi, I)$ be a character $\mathcal{H}(G, U, C) \to C$. Let V' be an irreducible C'–representation of G corresponding to the character $1_{C'} \otimes \psi$ of $\mathcal{H}(G, U, C')$. By 5.4 c) there is an irreducible C–representation V of G with $C' \otimes_C V$ isomorphic to V'. The action of $\mathcal{H}(G, U, C)$ on V^U is then obtained by restricting to $\mathcal{H}(G, U, C)$ the action of $\mathcal{H}(G, U, C')$ on V'^U, so indeed it is given by $\psi(\chi, I)$. Moreover V is absolutely irreducible since V' is. This proves the surjectivity statement in (ii). $\square$

5.6

We need a couple of properties, to be used in section 7. First we look at automorphisms of the situation.

Let σ be an automorphism of $\underline{G}$, preserving $\underline{T}$ and $\underline{U}$. If π is a representation of G on a C–vector space V, $\pi \circ \sigma$ is a representation of G on the same vector space V. The action of $\mathcal{H}(G, U, C)$ on $(\pi \circ \sigma)^U$ is also obtained by composing with σ — which induces an automorphism of $\mathcal{H}(G, U, C)$ — the action on π^U. If π is absolutely irreducible, corresponding to the character $\psi(\chi, I)$ of $\mathcal{H}(G, U, C)$, then $\pi \circ \sigma$ is also absolutely irreducible, and corresponds to $\psi(\chi \circ \sigma_T, I \circ \sigma)$ where we have written σ_T for the automorphism of T induced by σ, and $I \circ \sigma$ is the set $\{\alpha \circ \sigma_T \mid \alpha \in I\}$.

5.7

More important is some information on the action of parabolic subgroups — we always assume them to be defined over k. Let $\underline{P}$ be a parabolic subgroup of $\underline{G}$ containing $\underline{B}$. Let $\underline{N}$ be its unipotent radical, and $\underline{M}$ its Levi subgroup containing $\underline{T}$. Then $\underline{M}\cap\underline{B}$ is a Borel subgroup of $\underline{M}$ with Levi decomposition $\underline{M}\cap\underline{B} = \underline{T}(\underline{M}\cap\underline{U})$. The set of roots of $\underline{M}$ with respect to $\underline{M}\cap\underline{U}$ is a subset $\Delta_{\underline{M}}$ of $\underline{\Delta}$. We let $\underline{P}^- = \underline{M}\underline{N}^-$ be the parabolic subgroup opposite to $\underline{P}$.

Let V be an absolutely irreducible C–representation of G, with associated character $\psi = \psi(\chi, I)$.

(i) The representation of M on V^N is absolutely irreducible with associated character $\psi(\chi, \Delta_{\underline{M}} \cap I)$.

(ii) We have $V = C[N^-]V^N$, and in particular the projection of V onto the coinvariants V_{N^-} induces an isomorphism of V^N onto V_{N^-}, which is M–equivariant.

When C satisfies condition (*) of 5.3, the first assertion is given by [Cab, 3.6] and the second by [Cab, 3.2]; the general case is a consequence, using the reasoning of 5.5.

Remark. Applying (ii) to the contragredient representation of V (or, more simply, replacing $\underline{B}$, $\underline{P}$ by the opposites with respect to $\underline{T}$), we get that the projection of V onto V_N induces an isomorphism of V^{N^-} onto V_N.

6 Double coset decompositions

6.1

This section, although a bit technical, is at the heart of our reasoning. We prove a number of facts of combinatorial or geometric nature, which will be crucial for the proof of our main results in the next section.

The context is the same as in [Ha-Ro] and [Ha-Ra], which we often refer to. Our main notation, though, is close to that of [BT II].

In this section the coefficient ring C does not play a role, F is the same field as in sections 3 and 4, $\underline{G}$ is a general connected reductive group over F. As before we put $G = \underline{G}(F)$ and similarly for other (underlined) algebraic groups over F. All parabolic subgroups of $\underline{G}$ will be assumed to be defined over F, and a Levi subgroup of $\underline{G}$ will be a Levi subgroup defined over F of a parabolic subgroup. We shall also have to consider algebraic groups $\underline{H}$ over k_F, and we write, as in section 5, H for $\underline{H}(k_F)$.

We fix a maximal F–split torus $\underline{S}$ in $\underline{G}$, and we let $\underline{Z}$ be its centralizer in $\underline{G}$; then $\underline{Z}$ is a minimal Levi subgroup of $\underline{G}$, and is anisotropic mod. centre. To avoid any confusion with unipotent radicals, we write $\mathcal{N}$ — instead of N as in [BT II] — for the normalizer of $\underline{S}$ in $\underline{G}$. We let Φ be the set of roots of $\underline{S}$ in $\underline{G}$, Φ_{red} for the set of reduced roots. In the building $\mathcal{B}$ of $\underline{G}_{ad}$ over F, we have the apartment A corresponding to $\underline{S}$, and we choose a special vertex v_0 in A [T, 1.9][BTI, 1.3.7]; we think of A as a vector space with origin v_0.

We write K for the special parahoric subgroup $K_G(\{v_0\})$, in the notation of section 3, and $\tilde{K}$ for the group $\tilde{K}_G(\{v_0\})$.

6.2

We shall need the Cartan decomposition of G with respect to K. We let $W_0 = W(\underline{G}, \underline{S})$ be the Weyl group of $\underline{G}$ with respect to $\underline{S}$, that is the quotient $\underline{\mathcal{N}}/\underline{Z}$; it is equal to $\mathcal{N}/Z$ [Bo, 21.2 Theorem] and acts naturally on S. Because v_0 is special, W_0 has representatives in K and also appears as $\mathcal{N} \cap K/Z \cap K$ [Ha-Ro, lemma 5.0.1]. The group $\mathcal{N} \cap K$ acts via conjugation on Z and $Z \cap K$, and since $\Lambda = Z/Z \cap K$ is abelian, W_0 acts naturally on Λ. Recall also that Λ is a finitely generated abelian group.

The **Cartan decomposition** [Ha-Ro, Theorem 1.0.3] says that the map $Z \to K\backslash G/K$ sending z in Z to the double coset KzK induces a bijection between the set of orbits of W_0 in Λ and $K\backslash G/K$. Using a couple of lemmas, we want to express it in a way more convenient to us.

It is worth noting first the following facts.

Lemma (*i*) *$Z \cap K$ is the unique parahoric subgroup K_Z of Z.*

(*ii*) *$Z \cap \tilde{K}$ is the maximal compact subgroup $\tilde{K}_Z$ of Z.*

(*iii*) *The inclusion of $Z \cap \tilde{K}$ in $\tilde{K}$ induces an isomorphism of $Z \cap \tilde{K}/Z \cap K$ onto $\tilde{K}/K$.*

Proof. (*i*) is given by [Ha-Ro, 4.1.1]. We have $\tilde{K} = (Z \cap \tilde{K})K$ by the proof of Proposition 9.1.1 in [Ha-Ro], which gives (*iii*). On the other hand, the maximal compact subgroup $\tilde{K}_Z$ of Z is the inverse image in Z of the torsion subgroup Λ_{tor} of Λ (§ 3.4), and therefore the equality $\tilde{K}_Z = Z \cap \tilde{K}$ comes from [Ha-Ro, Proposition 11.1.4 and its proof].

6.3

Recall from § 3.2 Remark that the map $v_Z : Z \to X_*(\underline{S}) \otimes_{\mathbb{Z}} \mathbb{R}$ identifies Λ/Λ_{tor} with a lattice $\bar{\Lambda}$ in $X_*(\underline{S}) \otimes_{\mathbb{Z}} \mathbb{R}$. By construction, v_Z is W_0–equivariant.

Remark. 1) The apartment A can be identified with the quotient of $X_*(S) \otimes_{\mathbb{Z}} \mathbb{R}$ by the subspace orthogonal to all roots of $\underline{S}$ in $\underline{G}$. On that quotient A an element z of Z acts by the translation corresponding to $-v_Z(z)$. In particular z acts trivially on A if and only if $v_Z(z)$ is orthogonal to all roots of $\underline{S}$ in $\underline{G}$.

We let $\mathcal{C}$ be a Weyl chamber in $X_*(\underline{S}) \otimes_{\mathbb{Z}} \mathbb{R}$, we put $\bar{\Lambda}_+ = \mathcal{C} \cap \bar{\Lambda}$ and write Λ_+ for the inverse image of $\bar{\Lambda}_+$ in Λ, Z_+ for the inverse image in Z; we call elements of Z_+ dominant (with respect to $\mathcal{C}$). We put subscripts $-$ for the analogous objects corresponding to the opposite Weyl chamber, so that for example $\Lambda_- = \{\lambda^{-1} \mid \lambda \in \Lambda\}$, and we call elements of Z_- **antidominant**.

Remark. 2) It is well known [B, Lie V, § 4. Proposition 6 (ii)] that $\bar{\Lambda}_+$ is a set of representatives for the orbits of W_0 in $\bar{\Lambda}$.

Lemma.— Λ_+ *is a set of representatives for the orbits of* W_0 *in* Λ.

We give the proof in 6.4. Of course we can replace Λ_+ with Λ_- in that lemma. Given that lemma, we can restate the Cartan decomposition.

Proposition.— (Cartan decomposition for K) *The map* $Z \to K\backslash G/K$, $z \mapsto KzK$, *induces a bijection between* Λ_+ (*or* Λ_-) *and* $K\backslash G/K$.

6.4

Proof of lemma 6.3. Let λ, μ in Λ_+ and w in W_0 satisfy $\lambda = w(\mu)$. Projecting to $\bar{\Lambda}$ we get by 6.3 Remark 2 that $\lambda = \mu\nu$ for some ν in Λ_{tor}, so that $w(\mu) = \mu\nu$. Choose a representative z for μ in Z and a representative n for w in $\mathcal{N} \cap K$; then we have

$$nzn^{-1} = zt$$

for some t in $\tilde{K}_Z$ hence in $Z \cap \tilde{K}$ by 6.2 Lemma (ii). Consider now the Kottwitz homomorphism w_G of § 3.2. As w_G takes values in an abelian group, we get $w_G(t) = 1$. But t belongs to $\tilde{K}$, and w_G induces an injection on $\tilde{K}/K$, so that t belongs to $Z \cap K$ and $w(\mu) = \mu$, which proves the lemma.

6.5

We also need the Iwasawa decomposition for K.

PROPOSITION.— (Iwasawa decomposition) *Let $\underline{P}$ be a parabolic subgroup of $\underline{G}$. Then $G = PK$.*

Proof. It suffices to prove this when $\underline{P}$ is minimal. If $\underline{P}$ has $\underline{Z}$ as Levi component, the result is given by Corollary 9.1 2(i) in [Ha-Ro]. Any minimal parabolic subgroup $\underline{P}$ in $\underline{G}$ is conjugate to some minimal parabolic subgroup $\underline{B}$ with Levi component $\underline{Z}$, by an element g which we can write $g = kb$ with k in K and b in B. From $G = BK$ we get $G = kBk^{-1}K = PK$.

The next result we need is not true for a general parabolic subgroup of $\underline{G}$, only for semi–standard ones. Recall that a parabolic subgroup of $\underline{G}$ is called **semi–standard** if it contains $\underline{S}$, and that a Levi subgroup of $\underline{G}$ is called **semi–standard** if the maximal split torus in its centre is contained in $\underline{S}$. A semi–standard parabolic subgroup of $\underline{G}$ has a unique semi–standard Levi component, and conversely a semi–standard Levi subgroup of $\underline{G}$ is a Levi component for some, possibly several, semi–standard parabolic subgroups of $\underline{G}$.

THEOREM.— *Let $\underline{P}$ be a semi–standard parabolic subgroup of $\underline{G}$, $\underline{M}$ its semi–standard Levi component, $\underline{N}$ its unipotent radical. Then we have $P \cap \tilde{K} = (M \cap \tilde{K})(N \cap \tilde{K})$, $N \cap \tilde{K} = N \cap K$ and $P \cap K = (M \cap K)(N \cap K)$.*

Of course, this will be used to construct Satake homomorphisms in § 7. In fact we shall need only the case where $M = Z$, in which case the assertion for $P \cap K$ is in [Ha-Ro, Corollary 9.1.2 (ii)] but we do not understand the proof there. In any case, the added generality will be useful.

6.6

To prove the theorem, we progressively have to go deeper into the construction of K [BT II Chapter 4.25].

Let $\underline{B}$ be a minimal parabolic subgroup of $\underline{G}$ with Levi component $\underline{Z}$, contained in $\underline{P}$, and let $\underline{U}$ be its unipotent radical. To $\underline{U}$ corresponds a set of positive roots Φ_+ of $\underline{G}$, and the opposite unipotent radical $\underline{U}^-$ corresponds to $\Phi_- = -\Phi_+$

By [BTII, 5.2.4] we have an equality

$$K = U_0 U_0^- \mathcal{N}_0$$

where U_0 is an open compact subgroup of $\underline{U}$, U_0^- an open compact subgroup of U^-, and $\mathcal{N}_0$ an open compact subgroup of $\mathcal{N}$ containing $Z \cap K$: we have put $\Omega = \{v_0\}$ in loc. cit. and taken into account the definition of parahoric subgroups in [BTII, 5.2.6 and 5.2.8]. Using $\underline{B}^- = \underline{Z}\,\underline{U}^-$ instead of $\underline{B}$ we also have

$$K = U_0^- U_0 \mathcal{N}_0 .$$

Remark.— 1) As was pointed out by T. Haines [Ha, erratum] there are typographical errors in [BT II, 5.2.4], hats should be removed in lines 8 and 10. But we use only the equalities in line 9.

In the following, it will be convenient to put $Z_0 = Z \cap K$, $\tilde{Z}_0 = Z \cap \tilde{K}$, $\tilde{\mathcal{N}}_0 = \mathcal{N}_0 \tilde{Z}_0$.

Lemma.— *We have* $U \cap \tilde{K} = U \cap K = U_0$, $U^- \cap \tilde{K} = U^- \cap K = U_0^-$, $\mathcal{N} \cap \tilde{K} = \tilde{\mathcal{N}}_0$, $\mathcal{N} \cap K = \mathcal{N}_0$.

As in [Lv, Corollary 12.6 (iii)], this is a consequence of the Bruhat decomposition in $\underline{G}$.

By 6.2 lemma (iii) we have $\tilde{K} = K\tilde{Z}_0$ so that

$$\tilde{K} = U_0^- U_0 \tilde{\mathcal{N}}_0 = U_0 U_0^- \tilde{\mathcal{N}}_0 .$$

Let u in $U \cap \tilde{K}$ be written as $u = vv_-\nu$ with v in U_0, v_- in U_0^- and ν in $\tilde{\mathcal{N}}_0$. Then $\nu = v_-^{-1} v^{-1} u$ belongs to $U^- U$. The Bruhat decomposition [BTII, 5.15, see also Lv 0.18 (iii)] gives $\mathcal{N} \cap U^- U = \{1\}$ so that $\nu = 1$, $v_- = 1$, $u = v$ which shows that $U \cap \tilde{K} = U_0$ and a fortiori $U \cap K = U_0$. Using rather $\tilde{K} = U_0^- U_0 \tilde{\mathcal{N}}_0$ we get $U^- \cap \tilde{K} = U^- \cap K = U_0^-$. Finally let u in $\mathcal{N} \cap \tilde{K}$ be written as $\mu = vv_-\nu$ as above; then $\mu\nu^{-1}$ belongs to UU^-, hence $\nu = \mu$, so that $\mathcal{N} \cap \tilde{K} = \tilde{\mathcal{N}}_0$, and similarly $\mathcal{N} \cap K = \mathcal{N}_0$.

Remark.— 2) For each a in Φ_{red}, there is a corresponding root subgroup $\underline{U}_a$ in $\underline{G}$ ($\underline{U}_a$ is written $\underline{U}_{(a)}$ in [Bo 21.9]). By construction U_0 is the product of groups $U_{a,0}$ for a in $\Phi_+ \cap \Phi_{red}$, the product being taken for any ordering on $\Phi_+ \cap \Phi_{red}$; here $U_{a,0}$ is some open compact subgroup of U_a. It follows that $U_{a,0} = U_a \cap U_0$ and the lemma implies $U_a \cap \tilde{K} = U_a \cap K = U_{a,0}$. We have the analogous statement for a in Φ_-. If ψ is any closed subset of roots in $\Phi_+ \cap \Phi_{red}$ and $\underline{U}_\psi$ the corresponding unipotent subgroup of $\underline{U}$, [loc. cit.] then $U_\psi \cap \tilde{K} = U_\psi \cap K$ is the product of the groups $U_{a,0}$ for a in ψ.

6.7

We have $\underline{U} = \underline{N}(\underline{U} \cap \underline{M})$ and accordingly, by Remark 2) above, we get a decomposition $U_0 = N_0(U \cap M)_0$. Using the opposite parabolic subgroup

$\underline{P} = \underline{MN}^-$, we have a similar decomposition $U_0^- = N_0^-(U^- \cap M)_0$.

We now proceed to the proof of 6.5 Theorem. That $N \cap \tilde{K} = N \cap K$ comes from Remark 2 above.

Let p in $P \cap \tilde{K}$; write it as $p = vv_-\nu$ with v in U_0, v_- in U_0^- and ν in $\tilde{\mathcal{N}_0}$. Decompose $v = nu$ with n in N_0, u in $(U \cap M)_0$ and similarly $v_- = u_-n_-$ with n_- in N_0^- and u_- in $(U^- \cap M)_0$. Then

$$p = nuu_-n_-\nu \quad \text{so that} \quad n_-\nu \quad \text{belongs to} \quad P\,.$$

The lemma below gives that ν belongs to $\mathcal{N} \cap M$ so that n_- belongs to P so $n_- = 1$ and $p = nuu_-\nu$ with n in $N_0 = N \cap \tilde{K}$ and $uu_-\nu$ obviously in $M \cap \tilde{K}$. If moreover p belongs to $P \cap K$, then $uu_-\nu$ is in $M \cap K$. This proves 6.5 Theorem.

Remark.— Starting with p in $M \cap K$ yields $n = 1$ and $p = uu_-\nu$, so that

$$M \cap K = (U \cap M \cap K)(U_- \cap M \cap K)(\mathcal{N} \cap M \cap K)\,.$$

Lemma.— $N^-\mathcal{N} \cap P = \mathcal{N} \cap M$.

Assume $n_-\nu = mn$ for n_- in N^-, ν in $\mathcal{N}$, m in M, n in N. By the Bruhat decomposition for M we can write

$$m = u_-\mu u \quad \text{for} \quad u_- \text{ in } U^- \cap M,\ \mu \text{ in } \mathcal{N} \cap M,\ u \text{ in } U \cap M\,,$$

so that $n_-\nu = u_-\mu\ un$ and $U^-\nu U = U^-\mu U$. This implies $\nu = \mu$ by the Bruhat decomposition for $\underline{G}$. Then n_- is in P, so n_- is trivial. $\square$

6.8

The preceding proof may be applied more generally. Indeed let Ω be a bounded non–empty subset of A, and K_Ω the group of elements in Kerw_G fixing Ω. By [Ha-Ra, Remark 4] and unramified descent, K_Ω is the group of points over the ring of integers $\mathcal{O}_F$ of F of the group scheme $\mathfrak{G}_\Omega^0$ in [BT II 5.1.24]. By [BT II 5.2.4] again we get decompositions $K_\Omega = U_\Omega U_\Omega^- \mathcal{N}_\Omega = U_\Omega^- U_\Omega \mathcal{N}_\Omega$ and each of U_Ω, U_Ω^- is a product of root subgroups $U_{a,\Omega}$. By the same reasoning as above, we deduce:

(i) $U_\Omega = K_\Omega \cap U$, $U_\Omega^- = K_\Omega \cap U^-$, $\mathcal{N}_\Omega = \mathcal{N} \cap K_\Omega$, $U_{a,\Omega} = K_\Omega \cap U_a$ for $a \in \Phi$.

(ii) $P \cap K_\Omega = (M \cap K_\Omega)(N \cap K_\Omega)$.

(iii) $M \cap K_\Omega = (U \cap M \cap K_\Omega)(U^- \cap M \cap K_\Omega)(\mathcal{N} \cap M \cap K_\Omega)$.

We can even complement (iii). It is known [BT II, last line of 5.2.4 and 4.6.6 Corollary] that $K_\Omega = U_\Omega U_\Omega^- U_\Omega Z_0$. Using the Bruhat decomposition as above we get

(iv) $M \cap K_\Omega = (U \cap M \cap K_\Omega)(U^- \cap M \cap K_\Omega)(U \cap M \cap K_\Omega)Z_0$; this is consistent with [Ha-Ro, lemma 4.1.1] which shows, at least when Ω is a facet of A, that $M \cap K_\Omega$ is the group of elements in $M \cap \mathrm{Ker} w_M$ fixing the projection of Ω onto the apartment of the building of $\underline{M}_{ad}$ corresponding to $\underline{S}$.

6.9

We now **fix** a minimal parabolic subgroup $\underline{B}$ with Levi component $\underline{Z}$ and unipotent radical $\underline{U}$ and we investigate the intersection of a double coset KzK with a double coset KtU for z, t in Z.

Fixing $\underline{B}$ determines a set of positive roots Φ_+, a positive Weyl chamber $\mathcal{C}$ in A made out of the points on which positive roots take nonnegative values. In $\mathcal{C}$ there is a unique alcove a_0 in A with vertex v_0, and we let I be the corresponding parahoric subgroup: it is a (connected) Iwahori subgroup of G (see the discussion of Iwahori subgroups in [Ha]). We use the notations Z_+, Z_- etc. introduced in 6.3.

Proposition.— *Let z in Z_-. Then $KzK \cap zU = z(U \cap K)$.*

By [BT I, 4.4.4 (ii)][2] we have

$$\tilde{K} z \tilde{K} \cap U z \tilde{K} = z\tilde{K}$$

so $\tilde{K} z \tilde{K} \cap zU = z\tilde{K} \cap zU = z(\tilde{K} \cap U)$. But $\tilde{K} \cap U = K \cap U$ by 6.6 lemma. □

[2]The reader has to realize that we can indeed apply the results of [BI I 4.4.4] to our situation; one way to see that goes as follows: their group $\hat{G}$ is our group G, their group G is the group G' of [BT II 5.2.11] generated by the parahoric subgroups of G and the inclusion $\varphi : G' \to G$ is of connected type. Their group K is our group $\tilde{K}$ which, being special, is a good maximal compact subgroup [BT I, 4.4.1] Finally their $\widehat{\mathcal{B}_0}$ is just U and their $\hat{V}_D^0$ is $\mathcal{C}$. Also take into account 6.3 Remark 1.

6.10

We now investigate the intersection $KzK \cap KtU$ for z in Z_- and t in Z.

Recall the map $v_Z : Z \to X_*(\underline{S}) \otimes \mathbb{R}$ of 3.2; for a root a in Φ and z in Z, we put $< a, z >= a(v_Z(z))$, seeing a as a linear form on $X_*(\underline{S}) \otimes \mathbb{R}$. As this only depends on the image λ of z in $\Lambda = Z/Z \cap K$, we also write it as $< a, \lambda >$.

Write Δ for the set of simple roots in Φ_+. The image of Λ in $\mathbb{R}^\Delta$ by the map $A : \lambda \mapsto (< a, \lambda >)_{a\in\Delta}$ is a lattice; by 6.3 Remark 1 the kernel Λ_0 of A is the set of elements in Λ acting trivially on the building of $\underline{G}_{ad}$ over F.

The closed cone $\mathbb{R}_+^\Delta$ gives an ordering $\leq$ on $\mathbb{R}^\Delta$, and Λ_- is the inverse image of the set of negative elements. It is clear that for λ in Λ_- there are only finitely many elements x of $A(\Lambda)$ with $A(\lambda) \leq x \leq 0$.

Proposition.— *Let z in Z_-, t in Z, and write λ, μ for their images in Λ. If $\tilde{K}z\tilde{K} \cap \tilde{K}tU$ is non empty, then $A(\mu) \geq A(\lambda)$. If $KzK \cap KtU$ is non empty and $A(\mu) = A(\lambda)$ then $\mu = \lambda$.*

The first assertion is [BTI, 4.4.4 (i)]. Let us assume $KzK \cap KtU$ non empty and $A(\mu) = A(\lambda)$. Then we have $z = tx$ with $A(x) = 0$ and also $zk = k'tu$ for some k and k' in K, u in U. Applying the Kottwitz homomorphism w_G, which is trivial on K and U, we get $w_G(x) = 0$, and in particular $v_G(x) = 0$. This implies $\mathrm{val}_F(\chi(x)) = 0$ for all F–rational characters χ of $\underline{G}$; but on the other hand $A(x) = 0$ so finally $v_Z(x) = 0$, and x belongs to $Z \cap \tilde{K}$. Then $w_G(x) = 0$ implies that x in fact belongs to $Z \cap K$, so that $\mu = \lambda$. □

Remark. Clearly the Weyl group W_0 stabilizes Λ_0. Taking λ in Λ_0 and $\mu = w\lambda$ for some w in W_0 we get $A(\lambda) = A(\mu) = 0$; on the other hand $KzK = KtK$ has non-empty intersection with KtU so that the proposition gives $\mu = \lambda$. We thus see that W_0 acts trivially on Λ_0.

6.11

For the end of this section, we **fix** an element z in Z. We let $\Phi_{>0}$, Φ_0, $\Phi_{<0}$ be the sets of roots a such that $< a, z >$ is > 0, 0 or < 0 respectively.

We let $\underline{M}$ be the (semi–standard) Levi subgroup of $\underline{G}$ generated by $\underline{Z}$ and the root subgroups $\underline{U}_a$ of $\underline{G}$, for a in Φ_0; we let $\underline{N}$ be the unipotent subgroup generated by the $\underline{U}_a$ for a in $\Phi_{>0}$, $\underline{N}^-$ the one generated by the $\underline{U}_a$ for a in

$\Phi_{<0}$. Then $\underline{M}$ is the intersection of the parabolic subgroups $\underline{P} = \underline{MN}$ and $\underline{P}^- = \underline{MN}$, and is their common Levi component.

If $\underline{H}$ is any of those algebraic groups over F, we indicate with a subscript 0 the intersection $\underline{H}(F) \cap K$.

We have to describe how the groups $U_{a,0}$ for a in Φ_{red} are constructed in [BT II, 5.2]. First to the special point v_0 is attached a function $\Phi \to \mathbb{R}$ and its "optimisée" g [BT II, 5.2.3]. Then by the definition of [BT II, 5.2.2] we have, for a in Φ_{red},

$$U_{a,0} = X_{a,g(a)}\ X_{2a,g(2a)}$$

where the $X_{a,u}$, $u \in \mathbb{R}$, are the open compact subgroups of U_a written $U_{a,u}$ in loc. cit (the second term is omitted if $2a$ is not in Φ); the filtration by u in $\mathbb{R}$ is decreasing and one has $zX_{a,u}z^{-1} = X_{a,u+<a,z>}$. In particular, we get

LEMMA.— *Let $a \in \Phi_{red}$.*

(*i*) *For a in Φ_0 or $\Phi_{>0}$, $U_{a,0}$ contains $zU_{a,0}z^{-1}$.*

(*ii*) *For a in Φ_0 or $\Phi_{<0}$, $zU_{a,0}z^{-1}$ contains $U_{a,0}$.*

(*iii*) *$zN_0z^{-1} \subset N_0$, $zN_0^-z^{-1} \supset N_0^-$, $zM_0z^{-1} = M_0$.*

6.12

For use in section 7, we need to describe the image of $K \cap z^{-1}Kz$ in K/K_+. As recalled in 3.7, K/K_+ is the group of points over k_F of the reductive $\bar{\mathcal{G}}_K^{red}$, which we will simply write $\underline{\bar{G}}$. As stated in 6.1, if $\underline{H}$ is an algebraic group over k_F, we put $H = \underline{H}(k_F)$, so that $\bar{G} = K/K_+$.

Let us describe $\underline{\bar{G}}$, following [BT II, 5.3.1], which also refers to [BT II, 4.6].

The schematic closure of $\underline{S}$ in $\mathcal{G}_K$ yields a maximal split torus $\underline{\bar{S}}$ in $\underline{\bar{G}}$, and the schematic closure of $\underline{Z}$ gives a maximal torus $\underline{\bar{Z}}$, which is the centralizer of $\underline{\bar{S}}$ in $\underline{\bar{G}}$. The root system $\bar{\Phi}$ of $\bar{S}$ in $\bar{G}$ is a sub–root system of Φ. As v_0 is a special point, the reflections attached to $\bar{\Phi}$ are the same as those attached to Φ; if a and $2a$ are in Φ, one of them is in $\bar{\Phi}$ and if a is a root in Φ such that neither $2a$ nor $a/2$ is in Φ, then a is in $\bar{\Phi}$.

As in [BT II 4.6.9] we define a function g^* from Φ to the monoid $\tilde{\mathbb{R}} = \mathbb{R} \cup \mathbb{R}_+$, by the rule

$$\begin{array}{lll} g^*(a) = g(a) & \text{if} & g(a) + g(-a) > 0 \\ g^*(a) = g(a)_+ & \text{if} & g(a) + g(-a) \leq 0 \end{array}$$

(note in fact the last inequality is an equality since g is optimal and quasi–concave). By [BT II 4.6.10], (which can be applied by [BT II 5.1.31]) we have for a in Φ_{red}

$$K_+ \cap U_{a,0} = X_{a,g^*(a)}\ X_{2a,g^*(2a)}$$

where for u in $\mathbb{R}$ we have put

$$X_{a,u+} = \bigcup_{v>u} X_{a,u}.$$

In particular, we get

LEMMA.— *For a in $\Phi_{red} \cap \Phi_{>0}$, $zU_{a,0}z^{-1}$ is contained in $K_+ \cap U_{a,0}$ and for a in $\Phi_{red} \cap \Phi_{<0}$, $z^{-1}U_{a,0}z$ is contained in $K_+ \cap U_{a,0}$.*

In fact it also follows from [BT II, 4.6.10] that $\bar{\Phi}$ is the set of a in Φ such that $g(a) + g(-a) = 0$. For a in Φ_{red} the image of $U_{a,0}$ in $\bar{G}$ is the root subgroup $\bar{U}_a$ if a is in $\bar{\Phi}$ (then a is non–divisible in $\bar{\Phi}$) and we put $\bar{a} = a$; if a is not in $\bar{\Phi}$, then $2a$ is and the image of $U_{a,0}$ in $\bar{G}$ is $\bar{U}_{2a}$; we put then $\bar{a} = 2a$. The image of Z_0 in $\bar{G}$ is $\bar{Z}$.

6.13

Let $\underline{\bar{N}}$ be the unipotent subgroup generated by the $\underline{\bar{U}_a}$ for a in $\Phi_{>0} \cap \bar{\Phi}$ and similarly define $\underline{\bar{N}^-}$ and $\underline{\bar{M}}$. Clearly $\bar{N}$ is the image of N_0 in $\bar{G}$, $\bar{N}^-$ is the image of N_0^-, and $\bar{M}$ the image of M_0. The action of z on M_0 by conjugation induces an action on $\bar{M}$, which we write σ.

PROPOSITION.— *The image of $K \cap z^{-1}Kz$ in $\bar{G} \times \bar{G}$ via the map sending k to $(k \mod K_+,\ zkz^{-1} \mod K_+)$ is the set of $(mn, \sigma(m)n_-)$ for m in $\bar{M}$, n in $\bar{N}$, n_- in $\bar{N}^-$.*

In particular, the image of $K \cap z^{-1}Kz$ in K/K_+ is $\bar{M}\bar{N}$.

The group $z^{-1}Kz$ is the parahoric subgroup of G fixing the special point $z^{-1}(v_0)$, image of v_0 under the action of z^{-1}. Consequently $K \cap z^{-1}Kz$ is the subgroup K_Ω of $G \cap \mathrm{Ker} w_G$ fixing the whole geodesic Ω between v_0 and $z^{-1}(v_0)$. By [Ha-Ra, Remark 4], it is the same as the group of points over $\mathcal{O}_F$ of the connected group $\mathfrak{G}_\Omega^0$ of [BT II, 5.2.4] and as such it is generated by Z_0 and $K_\Omega \cap U_a$ for $a \in \Phi_{red}$ (cf. [BTII, 5.24 and 4.6.6 Corollary]).

Now for a in Φ_{red} we have $K_\Omega \cap U_a = U_{a,0} \cap z^{-1}U_{a,0}z$, which is $U_{a,0}$ if a is in Φ_0 or $\Phi_{>0}$ and $z^{-1}U_{a,0}z$ if a is in $\Phi_{<0}$. It has image $\bar{U}_{\bar{a}}$ in $\bar{G}$ in the first case, and trivial image in the second. We see already that the image of N_0 in $\bar{G}\times\bar{G}$ is $\bar{N}\times\{1\}$, and reasoning with z^{-1} instead of z we get that the image of N_0^- is $\{1\}\times\bar{N}^-$. Clearly also the image of M_0 is the set of $(m,\sigma(m))$ for m in $\bar{M}$.

Now by loc. cit. K_Ω is generated by $U\cap K_\Omega$, $U^-\cap K_\Omega$ and Z_0, from which it follows that K_Ω is generated by $N\cap K_\Omega$, $N^-\cap K_\Omega$ and $M\cap K_\Omega = M_0$. It is then clear that the image of $K\cap z^{-1}Kz = K_\Omega$ in $\bar{G}\times\bar{G}$ is in the prescribed set.

Remark.— We could have used instead [T, 3.5 and 3.5.1], but that paper does not really give proofs.

7 Satake isomorphisms

7.1

In this section, we finally prove the theorems stated in the introduction. Given the results of sections 5 and 6, we essentially follow Herzig's proofs in [He1].

We use the same notation as in section 6, fixing in particular the maximal split torus $\underline{S}$ of the ambiant group $\underline{G}$, its centralizer $\underline{Z}$, and a minimal parabolic subgroup $\underline{B}$ with Levi component $\underline{Z}$ and unipotent radical $\underline{U}$. We write Δ for the set of simple roots of $\underline{S}$ in $\underline{U}$. We also fix a special vertex v_0 in the apartment A and write K for the corresponding parahoric subgroup, K_+ for its pro–p radical.

As in section 5, we fix a field C of characteristic p, and we consider an absolutely irreducible representation ρ of K/K_+ on a C–vector space V, which we also view as a smooth representation — actually finite dimensional — of K, trivial on K_+.

By 6.5 we have $G = BK$ and $B\cap K = (Z\cap K)(U\cap K)$ so that § 2 gives us a Satake homomorphism (of algebras)

$$\mathcal{S} : \mathcal{H}(G,K,V) \longrightarrow \mathcal{H}(Z, Z\cap K, V^{U\cap K}).$$

We have seen that $\bar{G} = K/K_+$ is the group of k_F–rational points of a reductive $\underline{\bar{G}}$ group over k_F. The image of $B\cap K$ in $\bar{G}$ is the group $\bar{B}$ of points of a Borel subgroup of $\underline{\bar{G}}$, the image $\bar{U}$ of $U\cap K$ is the group of points of its unipotent radical, and the image $\bar{Z}$ of $Z\cap K$ is the group of points of a maximal torus of $\underline{G}$; we have $\bar{B} = \bar{Z}\bar{U}$, of course.

From section 5, we see that $V^{U\cap K}$ has dimension 1, and that $\bar{Z}$ acts on it via a character $\chi : \bar{Z} \to C^\times$, which we also view as a smooth character of $Z \cap K$ trivial on $Z \cap K_+$. As we have seen in § 4, Z acts by conjugation on $Z \cap K$, which is its unique parahoric subgroup; it also acts on the pro–p radical $Z \cap K_+$ of $Z \cap K$, so it acts on $\bar{Z}$ and the support of the algebra $\mathcal{H}(Z, Z \cap K, V^{U\cap K})$ is the stabilizer Z_χ of the character χ in Z.

The set Z_- of anti–dominant elements in Z is a submonoid of Z, containing $Z \cap K$. The main goal of this final section is to prove the following result.

THEOREM.— *The Satake homomorphism $\mathcal{S}$ from $\mathcal{H}(G, K, V)$ to $\mathcal{H}(Z, Z \cap K, V^{U\cap K})$ is injective and its image is the subalgebra made out of functions with support in $Z_- \cap Z_\chi$.*

7.2

Theorem 7.1 is the same as Theorem 1.8, and it includes assertions (i) and (ii) of Theorem 1.5. Before turning to the proof of Theorem 7.1, let us deduce Proposition 1.8, which includes the last assertion of Theorem 1.5. Note that Proposition 1.8 is true when $\underline{G}$ is anisotropic mod. centre, by 4.1 Remark 2. In particular, that applies to Z.

Recall also from 4.1 that Z_χ has finite index in Z, and its subgroup Z'_χ also has finite index in Z (of course $Z = Z_\chi = Z'_\chi$ if χ is trivial). Choose an element s in S with $< a, s >< 0$ for every a in Δ. For every element z in Z, there is a positive integer n such that $s^n z$ is antidominant. We deduce that Z_- generates Z as a group; as Z'_χ contains S, we also see that $Z_- \cap Z'_\chi$ generates Z'_χ, and $Z_- \cap Z_\chi$ generates Z_χ. It then follows from 2.13 that the centre of $\mathcal{H}(Z_-, Z \cap K, V^{U\cap K})$ is $\mathcal{H}(Z_- \cap Z'_\chi, Z \cap K, V^{U\cap K})$; if χ is trivial, $\mathcal{H}(G, K, V)$ is commutative. Finally the finiteness assertions of Proposition 1.8 are consequences of the following lemma, using the same reasoning as in 2.9.

LEMMA.— *The monoid $(Z_- \cap Z'_\chi)/(Z \cap K)$ is finitely generated, and has finite index in $(Z_- \cap Z_\chi)/(Z \cap K)$.*

To prove the lemma, recall the homomorphism $v_Z : Z \to X(S) \otimes_{\mathbb{Z}} \mathbb{Q}$. Its image is a lattice and its kernel $Z \cap \tilde{K}$ contains $Z \cap K$ with finite index. The subset Z_- is defined by the equations $< a, z >\leq 0$ for a in Δ. Applying Gordan' lemma 2.11 we get that $Z_-/(Z \cap K)$, $(Z_- \cap Z_\chi)/(Z \cap K)$ and

$(Z_- \cap Z'_\chi)/(Z \cap K)$ are finitely generated commutative monoids. If d is the exponent of χ, we have seen in 2.9 that x^d belongs to Z'_χ if x belongs to Z_χ, and consequently x^d belongs to $Z_- \cap Z'_\chi$ if x belongs to $Z_- \cap Z_\chi$; since $(Z_- \cap Z_\chi)/(Z \cap K)$ is a finitely generated monoid, it follows that $Z_- \cap Z'_\chi$ has finite index in $Z_- \cap Z_\chi$, which proves the lemma.

7.3

Let now turn to the proof of Theorem 7.1. It has several steps, which we turn into lemmas.

Lemma 1.— *Let z in Z_-. Then KzK supports a non–zero function of $\mathcal{H}(G, K, V)$ if and only if z belongs to Z_χ. In that case, the space of such functions has dimension 1 over C, it contains a unique function T_z such that $T_z(z)$ induces the identity on $V^{U\cap K}$.*

Choosing a set of representatives Σ of $\Lambda = Z/Z \cap K$ in Z we get, by the Cartan decomposition, a basis $(T_z)_{z\in\Sigma\cap Z_-\cap Z_\chi}$ for $\mathcal{H}(G, K, V)$

Lemma 2.— *Let z in $\Sigma \cap Z_- \cap Z_\chi$. Then we have $\mathcal{S}(T_z) = \Sigma a_\alpha \tau_\alpha$ for some scalars a_α in C, where the sum is over the set of α in $\Sigma \cap Z_\chi$ such that the images $\bar{z}$ and $\bar{\alpha}$ in Λ verify $A(\bar{\alpha}) \geq A(\bar{z})$. Moreover the only such α such that $A(\bar{\alpha}) = A(\bar{z})$ is $\alpha = z$, and $a_z = 1$.*

Lemma 3.— *Let Φ in $\mathcal{H}(G, K, V)$. Then $\mathcal{S}(\Phi)$ vanishes outside $Z_- \cap Z_\chi$.*

By Lemma 3 the sum in Lemma 2 may be restricted to α in $\Sigma \cap Z_- \cap Z_\chi$.

The proof of Theorem 7.1 from these lemmas follows the usual "triangular" argument : let $\Phi = \Sigma a_z T_z$ be a general non–zero element in $\mathcal{H}(G, K, V)$, with z running through $\Sigma \cap Z_- \cap Z_\chi$. Among the z's with $a_z \neq 0$, choose one, say z_0, such that $A(\bar{z}_0)$ is minimal (for the order on $\mathbb{R}^\Delta$). Evaluate $\mathcal{S}(\Phi)$ at z_0; by Lemma 2, $\mathcal{S}(T_{z_0})(z_0) = 1$. On the other hand, if $a_z \neq 0$ and $\mathcal{S}(T_z)(z_0) \neq 0$ then $A(\bar{z}_0) \geq A(\bar{z})$ by Lemma 2 again; this implies $A(\bar{z}_0) = A(\bar{z})$ by minimality of $A(\bar{z}_0)$ and consequently $z = z_0$ (Lemma 2). In particular $\mathcal{S}(\Phi)(z_0) = a_{z_0} \neq 0$ and $\mathcal{S}$ is **injective**.

Let us turn to sujectivity. For a positive integer r, let $Z_-(r)$ be the set of z in $\Sigma \cap Z_- \cap Z_\chi$ such that the number of elements x in $A(\Lambda)$ with $A(\bar{z}) \leq x \leq 0$ is at most r. By induction on r we prove that τ_z belongs to the image of $\mathcal{S}$ for z in $Z_-(r)$. If z belongs to $Z_-(1)$ then $A(\bar{z}) = 0$ and by Lemma 2 $\mathcal{S}(T_z) = \tau_z$. If z belongs to $Z_-(r + 1)$, then by Lemma 2 $\mathcal{S}(T_z)$ is τ_z plus a linear combination of $\tau_{z'}$ with z' in $Z_-(r)$, so by induction, τ_z is indeed in the image of $\mathcal{S}$. $\square$

7.4

We now prove lemma 1.

Let z in Z_-. To determine the functions in $\mathcal{H}(G, K, V)$ supported on KzK, it is enough to look at their value at z. That value can be any endomorphism φ of V which satisfies

$$(*) \qquad \rho(k_2)\varphi = \varphi\rho(k_1)$$

whenever k_1 and k_2 in K verify $k_2 z = z k_1$. This last condition means that k_1 belongs to $K \cap z^{-1}Kz$ and that $k_2 = zk_1z^{-1}$.

Now by 6.13 Proposition (and using its notation) the image of $K \cap z^{-1}Kz$ in $\bar{G} \times \bar{G}$ is the set of $(mn, \sigma(m)n_-)$ for m in $\bar{M}$ n in $\bar{N}$, n_- in $\bar{N}^-$ — notice that $\bar{N}$ is in $\bar{U}^-$ since z is in Z_-. We can translate (*) into

$$(**) \qquad \rho(\sigma(m)n_-)\varphi = \varphi\rho(mn) \qquad \text{for } m \text{ in } \bar{M},$$

n in $\bar{N}$, n_- in $\bar{N}^-$.

This exactly means that φ factors through a linear map

$$\tilde{\varphi} : V_{\bar{N}} \longrightarrow V^{\bar{N}_-}$$

such that

$$\sigma(m)\tilde{\varphi} = \tilde{\varphi}m \quad \text{for } m \text{ in } \bar{M}$$

where we write m for the natural action of m on $V_{\bar{N}}$ or $V^{\bar{N}_-}$. Now by 5.7 (ii) the projection π of $V^{\bar{N}_-}$ onto $V_{\bar{N}}$ is an $\bar{M}$–equivariant isomorphism, so the condition above actually means that $\tilde{\varphi} \circ \pi$ is an endomorphism u of $V^{\bar{N}_-}$ satisfying $\sigma(m)u = um$ for m in $\bar{M}$. The representation of $\bar{M}$ on $V^{\bar{N}_-}$ is absolutely irreducible by 5.7 (i); if V has associated character $\psi(\chi, I)$, it has associated character $\psi(\chi, \Delta_{\bar{M}} \cap I)$. Also, by 5.6 its composition with σ has associated character $\psi(\chi \circ \sigma_Z, \Delta_{\bar{M}} \cap I)$ where σ_Z is the restriction of σ to $Z \cap K$. It follows that a non–zero endomorphism u as above exists if and only if $\chi \circ \sigma_Z = \chi$ i.e. if and only if z belongs to Z_χ, and then there is only a line of such endomorphisms, with a unique one which acts as identity on $V^{\bar{U}}$.

This ends the proof of the first lemma.

7.5

We now turn to the proof of Lemma 2. The last assertion is an immediate consequence of 6.9 Proposition, giving $KzK \cap zU = z(U \cap K)$, and the formula for $\mathcal{S}$ in 2.7, Proposition.

By the same formula, if α in $\Sigma \cap Z_\chi$ is such that $a_\alpha \neq 0$ then $KzK \cap K\alpha U$ is non empty, which by 6.10 Proposition implies $A(\bar{\alpha}) \geq A(\bar{z})$, and even $\alpha = z$ if $A(\bar{\alpha}) = A(\bar{z})$. This gives Lemma 2.

7.6

Let us now turn to the proof of Lemma 3, which closely follows [He1, Proof of Theorem 1.2].

Fix Φ in $\mathcal{H}(G, K, V)$ and z in Z, not in Z_-. We have to show that $\mathcal{S}(\Phi)$ vanishes at z. By assumption there is a root a in Δ such that $< a, z >> 0$. We decompose $\underline{U}$ as a semi–direct product of $\underline{U}_a$ with the invariant subgroup $\underline{U}^a$ generated by the root subgroups $\underline{U}_b$ with b positive and not a multiple of a. The same computation as Herzig's then gives that $\mathcal{S}(\Phi)(z)$ is 0 if $zU_{a,0}z^{-1}$ is a proper subgroup of $U_{a,0} \cap K_+$ (note that by 6.12 Lemma, $U_{a,0} \cap K_+$ indeed contains $zU_{a,0}z^{-1}$).

To conclude, we use Herzig's trick in [He1, Step 5]. We may as well assume $\Phi = T_\xi$ for some ξ in $\Sigma \cap Z_- \cap Z_\chi$.

Let Y be the set of z in Σ with $\mathcal{S}(T_\xi)(z) \neq 0$. If Y is not included in Z_-, there is a root a in Δ and z in Y such that $< a, z >> 0$. Choose a total ordering on Δ starting with a, and choose z in Y such that $(< b, z >)_{b \in \Delta}$ is the greatest possible for the lexicographic ordering on $\mathbb{R}^\Delta$, so that $< a, z >> 0$.

We have $z^2U_{a,0}z^{-2} \subsetneq zU_{a,0}z^{-1} \subseteq U_{a,0} \cap K_+$, so that $z^2U_{a,0}z^{-2}$ is a proper subgroup of $U_{a,0} \cap K_+$. In particular $\mathcal{S}(T_\xi^2)(z^2) = 0$. But on the other hand $\mathcal{S}(T_\xi^2) = \mathcal{S}(T_\xi)^2$ so

$$\mathcal{S}(T_\xi^2)(z^2) = \sum_{t \in \Sigma} \mathcal{S}(T_\xi)(t)\mathcal{S}(T_\xi)(t^{-1}z^2)$$

The term in that sum with $t = z$ is non–zero. If the term with t is not zero then $(< b, t >)_{b \in \Delta}$ and $(< b, t^{-1}z^2 >)_{b \in \Delta}$ are both not greater than $(< b, z >)_{b \in \Delta}$ in $\mathbb{R}^\Delta$. This implies $A(\bar{z}) = A(\bar{t})$ and by 6.10 Proposition $z = t$. This shows $\mathcal{S}(T_\xi^2)(z^2) \neq 0$, a contradiction. $\square$

7.7

For future use, let us now examine what remains of the previous results when we are given another absolutely irreducible representation ρ' of K/K_+ on a C–vector space V'. Write $\psi(\chi, I)$ and $\psi(\chi', I')$ for the parameters of V and V', as in § 5.5.

Let $z \in Z_-$. Then, following the proof of Lemma 1 step by step, we see that KzK supports a non–zero function of $\mathcal{H}(G, K, V, V')$ if and only if conditions (i) and (ii) below are satisfied:

$$(i) \qquad \chi'(x) = \chi(zxz^{-1}) \quad \text{for all } x \text{ in } Z \cap K\,;$$

$$(ii) \qquad \Delta_{\bar{M}} \cap I = \Delta_{\bar{M}} \cap I'\,.$$

(Here we are using the same notation as in 6.11 and 7.5).

When conditions (i) and (ii) are satisfied, the space $\mathcal{F}_z$ of functions in $\mathcal{H}(G, K, V, V')$ supported on KzK is one–dimensional; indeed the map from $\mathcal{F}_z$ to $\mathrm{Hom}_C(V^{U\cap K}, V'^{U\cap K})$ sending Φ to $\mathcal{S}(\Phi)(z)$ is an isomorphism, by 6.9 Proposition and the formula for $\mathcal{S}$ in 2.7.

Let us write $Z_-(\chi, \chi')$ for the set of z in Z_- satisfying conditions (i) and (ii). Choose a basis vector for each of $V^{U\cap K}$ and $V'^{U\cap K}$. Then for z in $Z_-(\chi, \chi')$ there is a unique function T_z in $\mathcal{H}(G, K, V, V')$ sending the basis vector of $V^{U\cap K}$ onto the basis vector of $V'^{U\cap K}$. Recalling the set of representatives Σ of $Z/Z \cap K$ in Z that we have chosen, we get a basis for $\mathcal{H}(G, K, V, V')$ made out of the T_z for z in $\Sigma \cap Z_-(\chi, \chi')$.

7.8

We have just seen that $\mathcal{H}(G, K, V, V')$ is non–zero if and only if $Z_-(\chi, \chi')$ is non–empty. This can be expressed more simply.

Proposition.— *$\mathcal{H}(G, K, V, V')$ is non–zero if and only if χ and χ' are conjugate by an element of Z.*

Clearly, by condition (i), if $\mathcal{H}(G, K, V, V')$ is non–zero then χ and χ' are conjugate by an element of Z. Conversely assume that for some z in Z we have $\chi'(x) = \chi(zxz^{-1})$ for all x in $Z \cap K$. We can certainly choose an element s in S such that $< a, sz >< 0$ for all simple roots a in Δ. Then sz belongs to Z_- and the associated Levi subgroup of $\bar{G}$ is $\bar{Z}$ for which $\Delta_{\bar{Z}}$ is empty. It follows that sz belongs to $Z_-(\chi, \chi')$, hence the proposition.

Still with z as above, we get an algebra isomorphism of $\mathcal{H}(Z, Z \cap K, \chi)$ onto $\mathcal{H}(Z, Z \cap K, \chi')$ sending φ to $\varphi' : x \mapsto \varphi(zxz^{-1})$. Since conjugation by z preserves Z_- we obtain an algebra isomorphism of $\mathcal{H}(Z_-, Z \cap K, \chi)$ onto $\mathcal{H}(Z_-, Z \cap K, \chi')$ and, via Theorem 7.1, an algebra isomorphism of $\mathcal{H}(G, K, V)$ onto $\mathcal{H}(G, K', V')$. However, in general it is not clear if we can arrange for such an isomorphism to be given by convolution with a function in $\mathcal{H}(G, K, V, V')$.

7.9

Turning to Lemma 3 now, we note that the first part of its proof is still valid, and gives that for Φ in $\mathcal{H}(G, K, V, V')$, $\mathcal{S}(\Phi)$ vanishes at an element z in Z **provided** $zU_{a,0}z^{-1}$ is a **proper** subgroup of $U_{a,0} \cap K_+$ for some positive root a. But examples [He2, 6.14] show that $\mathcal{S}(\Phi)$ need not vanish on all of $Z - Z_-$. Describing the image of $\mathcal{H}(G, K, V, V')$ under the Satake map $\mathcal{S}$ is a challenging problem.

Nevertheless, we can adapt Lemma 2 to ensure:

Proposition.— *$\mathcal{S}$ is injective on $\mathcal{H}(G, K, V, V')$.*

Indeed, let Φ be a non–zero function in $\mathcal{H}(G, K, V, V')$, and write it as a linear combination $\Sigma a_\alpha T_\alpha$ for α in $\Sigma \cap Z_-(\chi, \chi')$. Among the β's in $\Sigma \cap Z_-(\chi, \chi')$ with $a_\beta \neq 0$, choose one such that $A(\bar{\beta})$ is minimal. For α in $\Sigma \cap Z_-(\chi, \chi')$ such that $a_\alpha \neq 0$, $\mathcal{S}(a_\alpha T_\alpha)$ vanishes at β unless $A(\bar{\beta}) \geq A(\bar{\alpha})$; by the choice of β, $A(\bar{\beta}) \geq A(\bar{\alpha})$ implies $A(\bar{\beta}) = A(\bar{\alpha})$ and by 6.10 Proposition $\alpha = \beta$. In conclusion $\mathcal{S}(a_\alpha T_\alpha)$ vanishes at β unless $\alpha = \beta$. In particular $\mathcal{S}(\Phi)$ does not vanish at β and in particular is non–zero. That proves the Proposition.

7.10

Finally, let us return to the case of trivial coefficients C, justifying now Remarks 1) and 2) in 1.5. We now allow C to be any commutative ring.

Let K' be any group intermediate between the special parahoric subgroup K that we have fixed and the corresponding maximal compact subgroup $\tilde{K}$.

Lemma 1.— *We have $G = BK'$, $U \cap K' = U \cap K$ and $B \cap K' = (Z \cap K')(U \cap K')$.*

Proof. Since $G = BK$, a fortiori $G = BK'$. We saw in Theorem 6.5

that $B \cap \tilde{K} = (Z \cap \tilde{K})(U \cap \tilde{K})$ and $U \cap \tilde{K} = U \cap K$. The equalities $U \cap \tilde{K} = U \cap K' = U \cap K$ and $B \cap K' = (Z \cap K')(U \cap K')$ follow immediately.

By §2 and the lemma, we get a Satake morphism $\mathcal{S}'_C$ from $\mathcal{H}(G, K', C)$ to $\mathcal{H}(Z, Z \cap K', C)$ and we want to compare $\mathcal{S}'_C$ with the Satake morphism $\mathcal{S}_C$ from $\mathcal{H}(G, K, C)$ to $\mathcal{H}(Z, Z \cap K, C)$ that we have considered so far.

We first note that as a vector space, $\mathcal{H}(G, K', C)$ is naturally a subspace of $\mathcal{H}(G, K, C)$, more precisely it is the subspace of functions which are bi–invariant under K'. However the inclusion of $\mathcal{H}(G, K', C)$ into $\mathcal{H}(G, K, C)$ is not, if $K' \neq K$, and algebra isomorphism. Similarly $\mathcal{H}(Z, Z \cap K', C)$ is a subspace, usually not a subalgebra, of $\mathcal{H}(Z, Z \cap V, C)$. Nevertheless we prove:

LEMMA 2.— *By restriction to $\mathcal{H}(G, K', C)$, the Satake morphism $\mathcal{S}_C$ induces $\mathcal{S}'_C$.*

This follows immediately from the equality $U \cap K = U \cap K'$ in Lemma 1 and the formula describing $\mathcal{S}'_C$ and $\mathcal{S}_C$.

Remark.— Assume that $[K' : K]$ is invertible in C. Then the map $\Phi \to [K' : K]^{-1}\Phi$ is an algebra homomorphism of $\mathcal{H}(G, K', C)$ into $\mathcal{H}(G, K, C)$. As the inclusion of $\tilde{Z}$ in $\tilde{K}$ yields an isomorphism of $\tilde{Z}/Z$ into $\tilde{K}/K$, we have $[Z \cap K' : Z \cap K] = [K', K]$ and the map $\varphi \mapsto [K' : K]^{-1}\varphi$ is an algebra homomorphism of $\mathcal{H}(Z, Z \cap K', C)$ into $\mathcal{H}(Z, Z \cap K, C)$. This is coherent with Lemma 2.

7.11

Finally let us turn to a description of the kernel and image of $\mathcal{S}_C$. When C is the field of complex numbers they have been determined by Haines and Rostami [Ha-Ro], thus generalizing the classical results of Satake [Sa] for $\tilde{K}$.

After establishing some notation, we recall the result of [Ha-Ro] and derive our description in general.

We let $\delta : Z \to \mathbb{C}^\times$ be the modulus character of B, restricted to Z; its values are integral powers of the cardinality q of the residue field of F. Since δ is trivial on $Z \cap K$, we may consider it as a character of $\Lambda = Z/Z \cap K$ — we use the same letter δ.

For any commutative ring C, we identify, as we may, the Hecke algebra $\mathcal{H}(Z, Z \cap K, C)$ with the group algebra $C[\Lambda]$; we write e_λ for the basis element of $C[\Lambda]$ corresponding to $\lambda \in \Lambda$. Recalling that W_0 acts on Λ, we get an action of W_0 on the algebra $C[\Lambda]$.

The main result of [Ha-Ro] is that the homomorphism $\delta^{1/2}\mathcal{S}_{\mathbb{C}}$ from $\mathcal{H}(G,K,\mathbb{C})$ to $\mathcal{H}(Z,Z\cap K,\mathbb{C})=\mathbb{C}[\Lambda]$ is injective and its image is the space of W_0–invariant elements of $\mathbb{C}[\Lambda]$: indeed if we take for du the Haar measure on U giving measure 1 to $Z\cap K$, then our map $\mathcal{S}_{\mathbb{C}}$ is exactly the Satake transformation considered in loc. cit, cf. 1.4.

It will be convenient to have a variant characterizing the image of $\mathcal{S}_{\mathbb{C}}$ in terms of a twisted action of W_0 on $\mathbb{C}[\Lambda]$; we follow [ST, §2], where the case where G is split is treated.

For w in W_0 and λ in Λ, we put

$$w\circ e_\lambda=\delta^{1/2}(\lambda/w(\lambda))e_{w(\lambda)}\,,$$

thus getting a linear action $(w,\varphi)\mapsto w\circ\varphi$ on $\mathbb{C}[\Lambda]$.

For an element $\varphi=\Sigma a_\lambda e_\lambda$ in $\mathbb{C}[\Lambda]$, we have

$$\delta^{1/2}\varphi=\Sigma a_\lambda\delta^{1/2}(\lambda)e_\lambda\,,$$

so that $\delta^{1/2}\varphi$ is invariant under w in W_0 if and only if

$$\delta^{1/2}(\lambda)a_\lambda=\delta^{1/2}(w(\lambda))a_{w(\lambda)}\quad\text{for all }\lambda\text{ in }\Lambda$$

that is, exactly when

$$w\circ\varphi=\varphi\,.$$

Consequently, the image of $\mathcal{S}_{\mathbb{C}}$ is the space of elements of $\mathbb{C}[\Lambda]$ invariant under the twisted action of W_0.

7.12

The following lemma shows that the correction factor $\delta^{1/2}(\lambda/w(\lambda))$ is in fact an **integral** power of p, so that the twisted action of W_0 makes sense on $C[\Lambda]$ for any commutative ring C where p is invertible, i.e. any $\mathbb{Z}[1/p]$–algebra cf. [ST, § 2] for the case where G is split.

Recall that $\delta(z)$ for z in Z can be expressed as the normalized absolute value of the determinant of $Ad(z)$ acting on the F–vector space Lie($\underline{U}$). That vector space is the direct sum of the subspaces $L_a=\text{Lie}(\underline{U}_a)$, $a\in\Phi^+_{red}$; accordingly $\delta(z)$ factorizes as a product of $\delta_a(z)$, each an integral power of q.

Lemma.— *Let z in Z have image λ in Λ, and let w in W_0. Then $\delta(\lambda/w(\lambda))$ is the product of $\delta_a(z)^2$ over positive reduced roots a with $w(a)$ negative.*

Proof. Let n in $\mathcal{N}$ have image w in W_0, so that $w(\lambda)$ is the image in Λ of nzn^{-1}. Then for a in Φ^+_{red} we have

$$\det(Ad(nzn^{-1}) \mid L_a) = \det(Ad(z) \mid L_{w^{-1}(a)}) \text{ since } n^{-1}L_a n = L_{w^{-1}(a)} \,.$$

Thus $\delta(\lambda/w(\lambda))$ can be expressed as the product over a in Φ^+_{red}, of $\delta_a(z)\delta_{w^{-1}(a)}(z)^{-1}$.

Now let b be an element of Φ^+_{red}, and look at the occurences of b and $-b$ in that product. If $w(b)$ is positive, there are two terms cancelling each other; if $w(b)$ is negative, then we get a contribution $\delta_b(z)\delta_{-b}(z)^{-1} = \delta_b(z)^2$. This proves the Lemma.

7.13

For each λ in Λ_-, let W_λ be its stabilizer in W_0 and put

$$S_\lambda = \sum_{w \in W_0/W_\lambda} w \circ e_\lambda \,.$$

As λ belongs to Λ_-, each factor in the expression for $\delta(\lambda/w(\lambda))$ given by 7.12 Lemma 2 is a positive integer, so that by the definition of the twisted action, S_λ is an element of $\mathbb{Z}[\Lambda]$. By construction, it is invariant under the twisted action of W_0.

Theorem.— *$\mathcal{S}_\mathbb{Z}$ is injective and the family S_λ, λ in Λ_-, is a basis of its image.*

The proof has several steps, and runs until 7.15.
The first assertion is immediate since $\mathcal{S}_\mathbb{C}$ is injective.
That the S_λ are $\mathbb{Z}$–linearly independent is a consequence of the following statement.

Proposition.— *The family T_λ, $\lambda \in \Lambda$, where $T_\lambda = e_\lambda$ if $\lambda \notin \Lambda_-$ and $T_\lambda = S_\lambda$ for λ in Λ_-, is a basis of $\mathbb{Z}[\Lambda]$.*

Proof. Let λ in Λ_-. If for some w in W_0, $w(\lambda)$ is in Λ_-, then $w(\lambda) = \lambda$, so that all the terms in S_λ except e_λ itself are in $\mathbb{Z}e_\mu$ for some μ in $\Lambda - \Lambda_-$.

Assume we have a relation $\Sigma a_\mu T_\mu = 0$ where the a_μ's are integers. Expressing each S_λ in terms of the e_μ, we first get $a_\lambda = 0$ for each λ in Λ_-, and then, obviously, $a_\mu = 0$ for all other μ's. $\square$

Corollary.— (of Proposition) *The family* $(S_\lambda)_\lambda \in \Lambda_-$ *is a basis for the submodule of* $\mathbb{Z}[\Lambda]$ *made out of elements invariant the twisted action of* W_0*.*

Indeed if $\varphi = \sum_{\lambda\in\Lambda} a_\lambda e_\lambda$ is invariant under the twisted action of W_0 then

$$\varphi - \sum_{\lambda\in\Lambda_-} a_\lambda S_\lambda$$

is also invariant, but its support contains no element of Λ_-, so it has to be 0. $\square$

7.14

As the image of $\mathcal{S}_\mathbb{Z}$ is made out of elements invariant under the twisted action of W_0, it remains only to prove that each S_λ, λ in Λ_-, is in the image of $\mathcal{S}_\mathbb{Z}$. For that we use a "triangular" argument again. For $\lambda \in \Lambda_-$ write E_λ for the characteristic function of KzK when z has image λ.

Proposition.— *Let* λ *in* Λ_0*. Then we have* $\mathcal{S}_\mathbb{Z}(E_\lambda) = S_\lambda = e_\lambda$*.*

Proof. Consider $\mathcal{S}_\mathbb{Z}(E_\lambda) - S_\lambda$; it is certainly invariant under the twisted action of W_0 and, by 6.10 Proposition, its support contains no element of Λ_-, so we conclude $\mathcal{S}_\mathbb{Z}(E_\lambda) = S_\lambda$. On the other hand, 6.10 Remark gives $S_\lambda = e_\lambda$. $\square$

For a positive integer r, we let $\Lambda_-(r)$ be the set of λ in Λ_- such that there are at most r elements x in $A(\Lambda)$ with $A(\lambda) \leq x \leq 0$. Clearly $\Lambda_-(1) = \Lambda_0$. By induction on r, we show that for each λ in $\Lambda_-(r)$, S_λ is in the image of $\mathcal{S}_\mathbb{Z}$. The case $r = 0$ is given by the Proposition. Let λ be in $\Lambda_-(r+1)$; by 6.10 Proposition, we have $\mathcal{S}_\mathbb{Z}(E_\lambda) = S_\lambda + \Phi_\lambda$ where Φ_λ is a $\mathbb{Z}$–linear combination of S_μ with μ in $\Lambda_-(r)$ so that by induction S_λ is in the image of $S_\mathbb{Z}$. This ends the proof of 7.13 Theorem.

7.15

Let now C be any commutative ring. From the Theorem and Proposition in 7.13 we immediately get, by tensor product with C:

Theorem.— *The map* $\mathcal{S}_C : \mathcal{H}(G, K, C) \to C[\Lambda]$ *is injective and the family* $1_C \otimes S_\lambda$*,* λ *in* Λ_-*, is a basis of its image (as a* C*–module).*

Remarks.— 1) Assume $p \cdot 1_C = 0$. It follows from our main result with $\mathbb{F}_p$–coefficients (Theorem 1.5), that $1_C \otimes S_\lambda = 1_C \otimes e_\lambda$ for all λ in Λ_-; this can also be seen directly from 7.12 Lemma.

2) Let K' be any group intermediate between K and $\tilde{K}$, and put $\Lambda' = Z/(Z \cap K')$. Then the above theorem translates to this setting: $\mathcal{S}'_C : \mathcal{H}(G, K', C) \to C[\Lambda']$ is injective, and its image has a basis $S_{\lambda'}$, λ' in Λ'_-, where $S_{\lambda'}$ is given by the formula

$$S_{\lambda'} = \sum_{w \in W'/W_{\lambda'}} w \circ e_{\lambda'} \quad \text{with obvious notation} .$$

This can easily be seen from 7.10 and the theorem above.

7.16

As a final comment, let us note the following generalization of the classical results of Satake [Sa].

Theorem.— *For any commutative ring C, the C–algebra $\mathcal{H}(G, K, C)$ is finitely generated.*

It is enough to prove this when C is the ring of integers $\mathbb{Z}$. Applying $\mathcal{S}_\mathbb{Z}$, it amounts to proving that the algebra $\mathbb{Z}[\Lambda]^{W_0}$ of elements in $\mathbb{Z}[\Lambda]$ invariant under the twisted action of W_0, is finitely generated. We imitate [B, VI, §3.4]. By [loc. cit., § 1, n^o 6, Prop. 1.8] we have, for any λ in Λ_- and w in W_0,

$$A(w(\lambda)) \geq A(\lambda) .$$

By 6.10 Proposition, it follows that in the support of $S_\lambda = \sum_{W_0/W_\lambda} w \cdot e_\lambda$, the term e_λ is the only element e_μ with $A(\mu)$ minimal. Choose a finite system of generators $\lambda_1, \ldots, \lambda_r$ of the monoid Λ_-. As in [B, VI, § 3, n^o 2, Lemme 2], if $n_1, \ldots, n_r$ are non–negative integers, then in the support of $S_{\lambda_1}^{n_1} \cdots S_{\lambda_1}^{n_r}$ the only term e_μ with $A(\mu)$ minimal is e_λ where $\lambda = \lambda_1^{n_1} \cdots \lambda_r^{n_r}$. As in 7.14, it follows that the algebra homomorphism from $\mathbb{Z}[X_1, \ldots, X_r]$ to $\mathbb{Z}[\Lambda]^{W_0}$, sending X_i to S_{λ_i} for $i = 1, \ldots, r$, is surjective. □

Note that the analogous result, with the same proof, holds for any group K' intermediate between K and $\tilde{K}$.

References

[Ar] J. ARTHUR.— An introduction to the trace formula **in** *Harmonic Analysis, the trace formula, and Shimura varieties*, 1–263, Clay Math. Proc. 4, Amer. Math. Soc., Providence, RI, 2005.

[BL1] L. BARTHEL and R. LIVNÉ.— Irreducible representations of GL_2 of a local field, Duke Math. J. 75 (1994), 261–292.

[BL2] L. BARTHEL and R. LIVNÉ.— Modular representations of GL_2 of a local field : the ordinary, unramified case, J. Number Theory 55 (1995), 1–27.

[Bo] A. BOREL.— Linear Algebraic Groups, Second Enlarged Edition, GTM n^o 126, Springer Verlag (1991).

[B] N. BOURBAKI.— Groupes et algèbres de Lie, Chapitres 4, 5 et 6, Masson, Paris, 1981.

[BTI] F. BRUHAT and J. TITS.— Groupes réductifs sur un corps local, Publ. Math. I.H.E.S. 41 (1972), 5–251.

[BTII] F. BRUHAT and J. TITS.— Groupes réductifs sur un corps local II. Schémas en groupes. Existence d'une donnée radicielle valuée, Publ. Math. I.H.E.S. 60 (1984), 197–376.

[BTIII] F. BRUHAT and J. TITS.— Groupes réductifs sur un corps local. Chapitre III. Compléments et applications à la cohomologie galoisienne, J. Fac. Sci. Univ. Kyoto Sect. IA math. 34 (1987), 671–698.

[Cab] M. CABANES.— Irreducible modules and Levi supplements, J. Algebra 90 (1984), 84–97.

[CE] M. CABANES and M. ENGUEHARD.— *Representation theory of finite reductive groups*, New Mathematical Monographs 1, Cambridge Univ. Press, Cambridge, 2004.

[Carter] R.W. CARTER.— *Finite Groups of Lie Type. Conjugacy classes and complex characters*, Wiley Classics Library, John Wiley & Sons Ltd, Chichester, 1993.

[Cartier] P. CARTIER.— Representations of p–adic groups : a survey, **in** *Automorphic Forms, Representations and L–functions*, P.S.P.M. 33 part I, 1979, 111–155.

[Fu] W. FULTON.— *Introduction to Toric Varieties*, Annals of Math. Studies 131, Princeton Univ. Press, Princeton, 1993.

[Ha] T. HAINES.— Corrigendum : the base change fondamental lemma for central elements of parahoric Hecke algebras, available on the author's web page.

[Ha-Ra] T. HAINES and M. RAPOPORT.— Appendix to Twisted Loop Groups and their affine flag varieties by G. Pappas and M. Rapoport. Advances in Math. 219 (2008), 188–198.

[Ha-Ro] T. HAINES and S. ROSTAMI.— The Satake isomorphism for special maximal parahoric Hecke algebra, Represent. Theory 14 (2010), 264–284.

[HT] M. HARRIS and R. TAYLOR.— *The Geometry and Cohomology of Some Simple Shimura Varieties*, Annals of Math. Studies 151, Princeton Univ. Press, Princeton, 2001.

[H] G. HENNIART.— Une preuve simple des conjectures de Langlands pour $GL(n)$ sur un corps p–adique, Invent. Math. 113 (1993), 339–350.

[He1] F. HERZIG.— A Satake isomorphism in characteristic p, to appear in Compositio Mathematica.

[He2] F. HERZIG.— The Classification of irreducible admissible mod. p representations of a p–adic GL_n, ArXiv : 1005.1713.

[K] R. KOTTWITZ.— Isocrystals with additional structure II, Compositio Mathematica 109 (1997), 255–309.

[Lv] E. LANDVOGT.— *A compactification of the Bruhat–Tits building*, Lecture Notes in Math. 1619, Springer Verlag, Berlin, 1996.

[Ll] R.P. LANGLANDS.— Problems in the theory of automorphic forms **in** *Lectures in modern analysis and Applications* III, Lecture Notes in Math. 170, Springer Verlag, Berlin, 1970, 18–61.

[MS] J.S. Milne and K–Y. Shi.— Conjugates of Shimura Varieties **in** *Hodge Cycles, motives, and Shimura varieties*, Lecture Notes in Math. 900, Springer Verlag, Berlin 1982, 280–356.

[Mo] L. Morris.— Tamely ramified intertwining algebras, Invent. Math. 114 (1993), 1–54.

[O1] R. Ollivier.— Critère d'irréductibilité pour les séries principales en caractéristique p, J. Algebra 304 (2006), 39–72.

[O2] R. Ollivier.— Le foncteur des invariants sous l'action du pro–p–Iwahori de $GL_2(F)$, J. Reine Angew. Math. 635 (2009), 149–185.

[Sa] I. Satake.— Theory of spherical functions on reductive algebraic groups over p–adic fields, Publ. Math. I.H.E.S. 18 (1963) 1–69.

[ST] P. Schneider and J. Teitelbaum.— Banach–Hecke algebras and p–adic Galois representations. Doc. Math. Extra Vol, (2006), 631–684.

[T] J. Tits.— Reductive groups over local fields **in** *Automorphic Forms, Representations, and L–functions*, P.S.P.M. 33, part I, 1979, 29–69.

[V1] M.–F. Vignéras.— *Représentations ℓ–modulaires d'un groupe réductif p–adique avec $\ell \neq p$*, Progress in Mathematics 137, Birkh'auser, 1996.

[V2] M.–F. Vignéras.— On a numerical Langlands correspondence modulo p with the pro–p–Iwahori Hecke ring, Math. Annalen 331 (2005), 523–556. Erratum Math. Annalen 333, 699–701.

[W] J.–L. Waldspurger.— Quelques propriétés arithmétiques de certaines formes automorphes sur $GL(2)$, Compositio Math. 54 (1985), 121–171.