

Automorphic forms for unitary groups and Galois representations

*Three lectures at the Clay Mathematical Institute Summer School,
Honolulu, Hawaii, 2009*

These modest notes are a shortened version of four lectures given at Hawaii for the CMI summer school on Galois representations. They contain a short survey of the theory of unitary groups over a number field and, in the definite cases, of their automorphic forms, and of the Galois representations that we can attach to those. Very few proofs are given. I hope however that these notes may serve as a quick introduction, and as a very partial summary, of this recent and fundamental achievement that we are now able to construct Galois representations for all automorphic representations of definite unitary groups, and to describe them precisely enough at every local place.

The lectures I gave at Hawaii were more ambitious. The presentation of the results on automorphic forms for unitary groups and Galois representations were just an introduction, and I went on to explain the eigenvarieties of the definite unitary groups, and how one can use them to prove, using the generalizations of Ribet's lemma explained in my previous lectures [B3], some cases of the conjecture of Bloch and Kato [B2]. By lack of time my exposition became more and more sketchy, and I do not think that notes following that exposition would be useful to anyone, and expending them to the size they deserve (at least 100 pages) has proved beyond my energy. Therefore, I redirect the reader to the very nice paper [Buz] for an introduction to the theory of eigenvarieties, to [Ch1], [E1], or [BC2, chapter VII] for eigenvarieties of definite unitary groups, and to [BC2, chapter VIII and IX] for the applications to the Bloch-Kato conjecture I have tried to explain at Hawaii.

Prerequisites: The prerequisites for these lectures are:

- (i) Notions on algebraic groups.
- (ii) If possible, classical modular forms, and their adelic interpretation.

Notations: During most of the lecture, F will be a number field. The ring of adèles will be denoted by \mathbb{A}_F or simply \mathbb{A} . It is a product $\mathbb{A}_F = \mathbb{A}_{F,f} \times \mathbb{A}_{F,\infty}$ of finite adèles $\mathbb{A}_{F,f} = \mathbb{A}_f$ and infinite adèles $\mathbb{A}_{F,\infty} = \mathbb{A}_\infty = F \otimes_{\mathbb{Q}} \mathbb{R}$. When g is an adèle (or an idèle, or an adèle-valued point of a group scheme over F) we denote by

g_f and g_∞ its finite and infinite components. We often identify g_f with the adèle (or idèle, etc.) which has the same finite components and 0 (or 1) at all infinite component, and similarly for g_∞ so that $g = g_f + g_\infty$ (or $g = g_f g_\infty$).

We shall denote by $\bar{\mathbb{Q}}$ the set of complex numbers that are algebraic over \mathbb{Q} . So $\bar{\mathbb{Q}}$ is supposed to be embedded in \mathbb{C} .

CONTENTS

1. Unitary groups	3
1.1. Generalities	3
1.2. Unitary groups on real and p -adic fields	5
1.3. Unitary groups over totally real number fields	7
1.4. Adelic points of G	7
2. Representation of p -adic groups: a very brief review	8
2.1. Brief review on smooth representations	8
2.2. Spherical Hecke algebras and unramified representations	10
3. Automorphic representations for G	12
3.1. Automorphic forms	12
3.2. Automorphic representations	13
3.3. Decomposition of automorphic representations	14
4. Galois representations	14
4.1. set-up	14
4.2. Existence	14
4.3. Properties	15
4.4. Hodge-Tate weights	16
References	17

These notes are about automorphic forms and representations for unitary groups, and their attached Galois representations. The very existence of those attached representations is a recent progress that constitutes one of the most important achievement in the still largely open Langlands' program. It has been the result of a huge collective work of many mathematicians over more than thirty years (realizing an initial sketch, incredibly accurate in retrospect, of Langlands in the seventies). It is absolutely out of question to give or even the sketch the proof of this existence in this paper.

The aim of this lecture is only to provide a short and intuitive introduction to automorphic forms and representations for unitary groups, and to state the existence and main properties of their attached Galois representations. Even simply giving a proper and workable definition of automorphic representations for a general unitary group is a task that cannot be properly done in less than 100 pages.

There are many technical difficulties (especially at the archimedean places), which, though important, are not essential to the intuitive understanding of the notions. To avoid most of those difficulties, I will only consider a special case, namely unitary groups that are definite, that is compact at all archimedean places. While there are many arithmetical applications for which this special case may be sufficient, considering the general case is necessary in many other (including some that might be explained by Chris using Eisenstein series, which only exists for non-definite unitary groups) and moreover, the construction of Galois representations requires to consider non-definite places.

A natural question is: why unitary groups? The short answer is simply: because they are (with a few sporadic other cases, most notably Sp_4) the only algebraic group for which we know, at this point, how to attach Galois representation to most automorphic representations. We should be able to do the same to many other automorphic representations (e.g. all algebraic automorphic representations for GL_n) but it seems that some very difficult new ideas are missing in order to do that.

1. UNITARY GROUPS

1.1. Generalities. Let k be a field of characteristic 0 (for simplicity), and E be an étale algebra of dimension 2 over k (that is to say, E is either $k \times k$ or it is a field of degree 2 over k). The algebra E has only one non-trivial k -automorphism that we shall denote by c . Let V be a free E -module of rank n , and $q : V \times V \rightarrow E$ be a non-degenerate c -Hermitian form. (That is to say, $q(x, y)$ is E -linear in x and c -semi-linear in y , we have $q(x, y) = c(q(y, x))$ for all $x, y \in V$, and $q(x, y) = 0 \forall y \in V$ implies $x = 0$.)

To these data (k, E, V, q) we can attach an algebraic group over k .

Definition 1.1. The *unitary group* G attached to (k, E, V, q) is the algebraic group whose functor of points is

$$G(R) = \{g \in \mathrm{GL}_{E \otimes_k R}(V \otimes_k R), \quad q(gx, gy) = q(x, y) \forall x, y \in V \otimes_k R\}.$$

for every k -algebra R . In the case where E is a field (rather than $k \times k$) we shall say that G is a true unitary group.

Intuitively, this is not very complicated. The k -points of the unitary group are the set of E -linear automorphisms of V that preserve the Hermitian form q . Similarly for R -points.

Exercise 1.1. This definition implicitly assumes that the functor $R \mapsto G(R)$ is representable by a scheme over k . Prove it.

Exercise 1.2. Assume (k, E) are fixed. We say that (V, q) and (V', q') are equivalent if there is an E -linear isomorphism $f : V \rightarrow V'$ such that $q'(f(x), f(y)) =$

$q(x, y)$ for all $x, y \in V$. We say that (V, q) and (V, q') are *quasi-equivalent* if (V, q) is equivalent to $(V', \alpha q')$ for some $\alpha \in E^*$. Show that if (V, q) and (V', q') are quasi-equivalent, then the unitary groups attached to (k, E, V, q) and (k, E, V', q') are k -isomorphic.

Proposition 1.1. *If E is $k \times k$, then the unitary group G is isomorphic to GL_n . More precisely, once we have chosen one of the two k -morphisms $E \rightarrow k$, there is an isomorphism of k -algebraic groups $G \rightarrow \mathrm{GL}_n$ which is canonical up to inner automorphism of GL_n . Changing the morphism $E \rightarrow k$ amounts to changing the above isomorphism by an outer automorphism of GL_n .*

Proof — Let $p : E \rightarrow k$ be a k -morphism. The choice of p makes the isomorphism $E = k \times k$ (as k -algebra canonical, by saying that p is the first projection on $k \times k$). Let $V_0 = V \otimes_{E,p} k$. We construct a morphism of functors $G(R) \rightarrow \mathrm{GL}_R(V_0 \otimes_k R)$ by sending $g \in G(R)$ (an E -automorphism on $V \otimes_E R$) to its action on $V \otimes_E R \otimes_E k = V_0 \otimes_k R$. We leave to the reader to check that this is an isomorphism. \square

In other words, if a unitary group is not a true unitary group, it is isomorphic to GL_n .

Now, let k' be any extension of k . We can consider $E' = E \otimes_k k'$ which is still an étale algebra over k' (but not that if E was a field, this may fail for E' , hence the interest of the generality adopted), $V' = V \otimes_E E'$ which is still free of rank n over E , and q' the natural extension of q to V' . To the data (k', E', V', q') one can attach a unitary group G' over k' . It is clear from the definition that G' is $G \times_k k'$.

In particular, if $k' = E$, $G \times_k E$ is the unitary group attached to $(E, E \otimes_k E, V', q')$ for some V' and q' . But since $E \otimes_k E$ is isomorphic to $E \times E$, we see by Prop 1.1 that $G \times_k E$ is isomorphic to GL_n . So unitary groups are always *forms* of GL_n .

Exercise 1.3. 1.– Let H be a k -algebraic subgroup of a true unitary group G (attached to (k, E, V, q) as above). Assume that H is a split torus, i.e. isomorphic to \mathbb{G}_m^d for some d . Show that there exists d linearly independent vectors e_1, \dots, e_d in V such that $q(e_i, e_j) = 0$ for all $1 \leq i, j \leq d$. Deduce that $2d \leq \dim V$

2.– Deduce that a true unitary group over k is not isomorphic to GL_n .

3.– Deduce that if the unitary group attached to (k, E, V, q) and to (k, E, V', q') then $E \simeq E'$ as k -algebras.

Exercise 1.4. (easy) This exercise recalls basics of the theory of hermitian form. Let (k, E, V, q) be as usual, with E a field. We say that a vector $v \in V$ is *isotropic* and we say that a subspace H of V is a *hyperbolic plane* if it has a basis v, w with $q(v, v) = q(w, w) = 0$ and $q(v, w) = q(w, v) = 1$.

1.– Let v be a non-zero isotropic vector in V , Show that v belongs to an isotropic subspace of V .

If H is a subspace of V , we call H^\perp the set of $w \in V$ such that $q(v, w) = 0$ for all $v \in H$.

2.– Show that H^\perp is a subspace of V of dimension $\dim V - \dim H$. Show that $(H^\perp)^\perp = H$. Show that if H is a line generated by a non-isotropic vector, or is an hyperbolic plane, then $V = H \oplus H^\perp$.

Remark 1.1. The definition we have given of unitary group is quite intuitive. Unfortunately this not the most general one, nor the most natural from the point of view of the theory of descent. The general definition may be a little bit frightening at first glance, which is why I preferred to use the above "naive" definition. In order to motivate the general definition, let us first reformulate the naive definition. If (k, E, V, q) is as above, then for any endomorphism $u \in \text{End}_E(V)$ there is a unique endomorphism $u^* \in \text{End}_E(V)$ such that

$$q(u(x), y) = q(x, u^*(y)) \text{ for all } x, y \text{ in } V.$$

The application $u \mapsto u^*$ is an anti-involution of the algebra $\text{End}_E(V)$ which induces c on the scalars $E \subset \text{End}_E(V)$. We see easily that our definition of the unitary group G is equivalent to

$$G(R) = \{g \in (\text{End}_E(V) \otimes_k R)^*, g^*g = \text{Id}\}.$$

Now the algebra $\text{End}_E(V)$ is a matrix algebra isomorphic to $M_n(E)$ if $\dim V = n$. We know that an algebra whose base change is a matrix algebra may not be a matrix algebra, but is a central simple algebra. So we are led to the following definition:

Let Δ be a central simple algebra over E , and $u \mapsto u^*$ an anti-involution of the second kind of Δ (that is an additive anti-involution that induces c on the scalars $E \subset \Delta$). Then the unitary group attached to $(k, E, \Delta, *)$ is the group G such that

$$G(R) = \{g \in (\Delta \otimes_k R)^*, g^*g = \text{Id}\}.$$

We thus have a more general notion of unitary group, which reduces to the naive one when Δ is a matrix algebra (exercise). However for simplicity, we will stick to the naive definition.

1.2. Unitary groups on real and p -adic fields. First assume that $k = \mathbb{R}$, $E = \mathbb{C}$, V a space of dimension n over $E = \mathbb{C}$.

Exercise 1.5. Show that any non-degenerate hermitian form on V is equivalent to the form

$$q_p((x_1, \dots, x_n), (y_1, \dots, y_n)) = x_1c(y_1) + \dots + x_p c(y_p) - x_{p+1}c(y_{p+1}) - \dots - x_n c(y_n)$$

on \mathbb{C}^n , for some integer p such that $0 \leq p \leq n$. Show that q_p is equivalent (resp. quasi-equivalent) to $q_{p'}$ if and only if $p = p'$ ($p = p'$ or $p = n - p'$).

As a consequence, any true unitary group on \mathbb{R} is equivalent to the unitary group attached to the form q_p , which is denoted by $U(p, n - p)$.

Exercise 1.6. Let p, q be two non-negative integer, with $p + q > 0$. Show that $U(p, q) \simeq U(p', q')$ if and only if $\{p, q\} = \{p', q'\}$. Show that $U(p, q)(\mathbb{R})$ is a compact group if and only if $pq = 0$.

Now we assume that k is a finite extension of \mathbb{Q}_p , and E a quadratic extension of \mathbb{Q}_p , V a space of dimension n .

The following exercise will classify the non-degenerate hermitian forms q over V . For this we need to recall some (probably well-known) notions. A vector v is isotropic for q if $q(v, v) = 0$.

Exercise 1.7. Let q be any non-degenerate hermitian form on V . Set $n = \dim V$.

1.– Recall from Serre that any quadratic form over a space of dimension at least 5 has a non-zero isotropic vector. Deduce that if $\dim V \geq 3$, then q has a non-zero isotropic vector

2.– Assume that V has dimension 1. Show that the values of $q(v, v)$ for v in V form a class in $k^*/N_{E/k}(E^*)$. Deduce that there are 2 equivalence classes of hermitian forms in dimension 1, that are quasi-equivalent

3.– Assume that n is odd, $n = 2m + 1$. Show that V has a decomposition $V = H_1 \oplus \cdots \oplus H_m \oplus L$, where the H_i are hyperbolic plane and L is a line generated by an isotropic vector. Observe that the values $q(v, v)$ for $v \in L$ are in the same class on $k^*/N_{E/k}(E^*)$ that the discriminant of q . Deduce that there are exactly two equivalence classes of non-degenerate c -hermitian form over V , and that those two classes are quasi-equivalent.

3.– Assume that n is even, $n = 2m$. Show that V has either a decomposition $V = H_1 \oplus \cdots \oplus H_m$, or a decomposition $V = H^1 \oplus \cdots \oplus H_{m-1} \oplus L \oplus L'$ where the two Hermitian lines V and V' are not equivalent. Deduce that there are exactly two equivalence class of c -Hermitian form on V , and that they are not quasi-equivalent.

Since quasi-equivalent hermitian forms define isomorphic unitary groups, we see that there is one class of true unitary groups in the odd-dimensional case, and at most 2 in the even-dimensional case.

Exercise 1.8. (difficult) 1.– Assume $\dim V$ is even. Show that the two unitary groups attached to the two classes of hermitian form defined in the above exercise are not isotropic, by showing that only one of them is quasi-split (that is, has a Borel subgroup defined over k).

2.– Assume that $\dim V$ is odd. Show that the unitary group attached to (V, q) is quasi-split.

1.3. Unitary groups over totally real number fields. Let F be a totally real finite extension of \mathbb{Q} , and E be a quadratic extension of F that is totally imaginary. In other words, E is a CM field. Let c be the non-trivial automorphism of E over F . Let V be an E -vector space of dimension n and q be a non-degenerate c -hermitian form on V . To (F, E, V, q) one can attach a (true) unitary group G over F .

To get a better understanding of G we analyze the groups $G_v := G \times_F F_v$ for all places v of F .

If v is **archimedean**, then by assumption v is real, that is $F_v = \mathbb{R}$, and $E_v = \mathbb{C}$, while c induces the complex conjugation on \mathbb{C} . The group G_v is therefore \mathbb{R} -isomorphic to a group $U(p_v, n - p_v)$ for some $0 \leq p_v \leq n$ as in Exercise 1.6.

Definition 1.2. We shall say that G is *definite* if G_v is compact (that is $p_v = 0$ or $p_v = n$) for all real places v of F .

If v is **finite and split** in E , then $E \otimes_F F_v$ is not a field, but is isomorphic to $F_v \times F_v$. Therefore, the group G_v which is the unitary group attached to $(F_v, E \otimes_F F_v, \dots, \dots)$ is by Prop 1.1 isomorphic to GL_n over F_v . The choice of one of the two F_v -morphisms $E \otimes_F F_v$ to F_v , that is of one of the two places of E above v makes this isomorphism canonical, up to conjugation.

If v is *finite and either inert or ramified* in E , then E_v is a quadratic extension of F_v , so G_v is a true unitary group of v . Therefore, there is only one possibility for G_v if $\dim V$ is odd, and two if v is even. In the latter case, G_v can be quasi-split, or not. It is easy to see that it is quasi-split for almost all v .

The point to remember (for beginners) is that even a true unitary group over F becomes GL_n at basically one place of F over two: the places that are split in E . This will be very helpful later.

Slightly more advanced is the following classification theorem:

Theorem 1.1. 1. – If G and G' are two unitary groups such that $G_v \simeq G'_v$ for all place v of F , then $G \simeq G'$.

2. – Let $(G_v)_v$ be a family of unitary groups over F_v , attached to the extension $E \times F_v/F_v$. We assume that G_v is quasi-split for almost all v . Then if $\dim V$ is odd, there is a true unitary group G attached to E/F such that for every place v of F , G_v is the unitary group from the family. If $\dim V = 2m$ is even, the same is true if and only if we have $\prod_v \epsilon_v = 1$, where for v finite $\epsilon_v = 1$ if G_v is quasi-split (including the case where v is split in E), and -1 otherwise, and $\epsilon_v = (-1)^{p_v - m}$ if v is real and $G_v = U(p_v, 2m - p_v)$.

1.4. Adelic points of G . Let G be a unitary group as in the preceding §. Since the ring of adèles $\mathbb{A} = \mathbb{A}_F$ is an F -algebra (via the diagonal embedding), it make sense to talk of the group $G(\mathbb{A}_F)$. Since G is linear, that is a subgroup of GL_m for some m , $G(\mathbb{A}_F) \subset M_m(\mathbb{A}_F) = \mathbb{A}_F^{m^2}$ which allots to give a natural topology on $G(\mathbb{A}_F)$, namely the coarsest that is finer than the topology of $\mathbb{A}_F^{m^2}$ and for which $x \mapsto x^{-1}$

is continuous. This topology is easily seen to be independent of the choices. We shall need a good understanding of this group and of its natural topology.

Let \mathcal{G} be a model of G over $\text{Spec } \mathcal{O}_F[1/f]$ where $f \in \mathcal{O}_F - \{0\}$, that is a group scheme over this scheme whose generic fiber is G . Then for all v prime to f , the model define a subgroup $\mathcal{G}(\mathcal{O}_v)$ of $G(F_v)$ which is compact when v is finite. We can therefore form the restricted product $\prod'_{v \text{ places of } F} G(F_v)$ with respect to the subgroups $\mathcal{G}(\mathcal{O}_v)$.

Lemma 1.1. *This restricted product with its restricted product locally compact topology is independent of the model \mathcal{G} chosen and is naturally isomorphic, as a topological group, with $G(\mathbb{A}_F)$.*

The same lemma of course holds for the finite adèles $G(\mathbb{A}_{F,f}) = \prod'_{v \text{ finite}} G(F_v)$. We have $G(\mathbb{A}_F) = G(\mathbb{A}_{F,f}) \times G(\mathbb{A}_{F,\infty})$.

The group $G(F)$ can be embedded diagonally in $G(\mathbb{A}_F)$. Its image is discrete. If G is definite, then $G(F)$ is discrete in $G(\mathbb{A}_{F,f})$ and the quotient is compact.

2. REPRESENTATION OF p -ADIC GROUPS: A VERY BRIEF REVIEW

In order to understand automorphic representations, we need to remind (without any proof) a very little part of the very important and still active theory of representations of p -adic Lie groups. For a serious introduction to this theory, see [Ca] or [Cas]

2.1. Brief review on smooth representations. In this § only, G will be a group where there is basis of neighborhood of 1 made of compact open subgroups U .

Exercise 2.1. Prove that such a group is locally compact and totally disconnected. What about the converse?

Let k be a field of characteristic 0. By a *smooth representation* V of G over k we mean a k -vector space (not finite dimensional in general) with a linear action of G such that for every $v \in V$, there exists a compact open subgroup U in G such that v is invariant by U .

A smooth representation is *admissible* if for every open subgroup U of G , the subspace V^U of vectors invariant by U is finite dimensional over k .

Let us fix a (left invariant, but since in practice our G will be *unimodular*, this doesn't really matter) Haar measure dg on G , normalized such that the measure of some open compact subgroup U_0 is 1. Then it is easily seen that the measure of any other compact open subgroup will be a rational, hence an element in k .

We denote by $\mathcal{H}(G, k)$ the spaces of function from G to k that are locally constant and have compact support. This space as a natural product : the convolution of functions $(f_1 * f_2)(g) = \int_G f_1(x) f_2(x^{-1}g) dx$. Indeed, since f_1 and f_2 are in $\mathcal{H}(G, k)$, the integral is actually a finite sum, and what is more a finite sum of terms that

are products of a value of f_1 , a value of f_2 , and the measure of a compact open subgroup. So the integral really defines a k -valued function, and it is easy to check that $f_1 * f_2 \in \mathcal{H}(G, k)$. This product makes $\mathcal{H}(G, k)$ a k -algebra, which is not commutative if G is not, and which in general has no unity (the unity would be a Dirac at 1, which is not a function on G if G is not discrete). If V is a smooth representation of G it has a natural structure of $\mathcal{H}(G, k)$ -module by $f.v = \int_G f(g)g.v dg$. The algebra $\mathcal{H}(G, k)$ is called the *algebra of the group G over k* .

Let U be a compact open subgroup of G . Let $\mathcal{H}(G, U, k)$ be the set of functions from G to k that have compact support and that are both left and right invariant by U . This is easily seen to be a subalgebra of $\mathcal{H}(G, k)$, with unity (the unity is the characteristic function of U times a normalization factor depending on the Haar measure). The algebra $\mathcal{H}(G, U, k)$ is called the *Hecke algebra of G w.r.t U over k* . We have $\mathcal{H}(G, k) = \cup_U \mathcal{H}(G, U, k)$ and in particular we see that if G is not commutative, the $\mathcal{H}(G, U, k)$ are not for U small enough. The Hecke algebra are important because of the following trivial property:

Lemma 2.1. *Let V be a smooth representation of G (over k). Then the spaces of invariant V^U has a natural structure of $\mathcal{H}(G, U, k)$ -modules.*

Indeed, if $v \in V^U$, and $f \in \mathcal{H}(G, U, k) \subset \mathcal{H}(G, k)$, $f.v$ is easily seen to be in V^U .

If there is one thing to remember about Hecke algebras it is this lemma, not the definition : the Hecke algebra is what acts on V^U when V is a (smooth) representation of G and U sub-group of G .

We shall apply this theory to groups $G(F_v)$ when G is a unitary group as above and v is a finite place of F .

Exercise 2.2. (easy) Assume that G is finite. Show that $\mathcal{H}(G, k)$ is naturally isomorphic with the algebra $k[G]$. Assume that V is a finite dimensional algebra. Show that the structures of $\mathcal{H}(G, k)$ -module and $k[G]$ -module on V are compatible through that isomorphism.

Hence $\mathcal{H}(G, K)$ is a natural generalization of the classical group algebra of G in the case of a finite G .

Exercise 2.3. (easy) Let U be a normal open subgroup of G , and V be an admissible representation of U . Show that V^U is naturally an admissible representation of G/U . Hence $\mathcal{H}(G/U, k)$ acts on V^U . Show that $\mathcal{H}(G/U, k) = \mathcal{H}(G, U, k)$ and those two algebras have the same action on V^U .

Hence for non-normal U , the Hecke algebra $\mathcal{H}(G, U, k)$ is a generalization of the group algebra of G/U for U normal. In other words, when U is non normal, we can not define G/U as a group, but we do have a substitute for the group algebra of this non-existing group: $\mathcal{H}(G, U, k)$.

Exercise 2.4. Let k' be an extension of k .

a.— Show that if V is a smooth representation of G over k , then $V \otimes_k k'$ is a smooth representation of G over k' .

b.— Show that the formation of V^U commutes to the extensions k'/k .

c.— Show that $\mathcal{H}(G, U, k) \otimes_k k' = \mathcal{H}(G, U, k')$.

Exercise 2.5. Let $\mathcal{C}(G, k)$ and $\mathcal{C}(G/U, k)$ be the space of smooth functions from G and G/U to k .

a.— Show that they both are smooth representation of G (for the left translations)

b.— Show $\mathcal{C}(G, k)^U = \mathcal{C}(G/U, k)$. Therefore $\mathcal{H}(G, U, k)$ acts on $\mathcal{C}(G, U, k)$. Show that this action commutes to the G -action.

c.— Show that $\mathcal{H}(G, U, k)$ is actually naturally isomorphic to $\text{End}_G(\mathcal{C}(G/U, k))$.

Exercise 2.6. a.— Show that $V \mapsto V^U$ is an exact functor from the category of smooth representation of G over k to $\mathcal{H}(G, U, k)$ -module. This functor takes admissible representations to $\mathcal{H}(G, U, k)$ that are finite dimensional.

b.— Let $W = V^U$, $W' \subset W$ a sub- $\mathcal{H}(G, U, k)$ -module, and $V' \subset V$ the sub-representation of V generated by W' . Show that $V'^U = W'$.

c.— Deduce that if V is irreducible as a representation of G , then V^U is irreducible as a $\mathcal{H}(G, U, k)$ -module.

Note that in general the functor defined in a.— above is not fully faithful (even on admissible rep.) and that the converse of c.— is false.

2.2. Spherical Hecke algebras and unramified representations. We now assume that F is a totally real field, E an imaginary quadratic extension of F , and G an unitary group of n -variables attached to E/F .

If v is a finite place of F that splits in E , then $G(F_v) \simeq \text{GL}_n(F_v)$. It is an easy fact that all maximal compact subgroups of $\text{GL}_n(F_v)$ are conjugate (and conjugate to $\text{GL}_n(\mathcal{O}_v)$).

If v is a finite place that does not split in E , then $G(F_v)$ is a true unitary groups. It is not true that all maximal compact subgroups of $G(F_v)$ are conjugate, though there are only finitely many conjugacy class. If v is inert, then there is one class whose elements have maximal volume (for a fixed Haar measure), and we call compact of this class *maximal hyperspecial* compact subgroups of $G(F_v)$. We shall neglect places of F that ramify in E since there only in finite number.

Back to the case v split, we shall call any maximal compact subgroup hyperspecial.

Proposition 2.1 (Tits). *Let \mathcal{G} be a model of G over $\text{Spec } \mathcal{O}_F[1/f]$. Then $\mathcal{G}(\mathcal{O}_v)$ is a maximal compact hyperspecial subgroup of $G(F_v)$ for almost all finite places v .*

Corollary 2.1. *Any compact open subgroup of $G(\mathbb{A}_f)$ contains a compact open subgroup of the form $\prod_v U_v$ with U_v a compact open subgroup of $G(F_v)$ for all v , with U_v maximal hyperspecial for almost all v .*

Let v be a place of F (not ramified in E), and K_v be a maximal compact hyperspecial subgroup of $G(F_v)$. Let k be any field of characteristic 0.

Proposition 2.2. *The algebra $\mathcal{H}(G(F_v), K_v, k)$ is commutative.*

This fact is very important, and certainly not a tautology. As we have seen, $\mathcal{H}(G(F_v), U)$ will certainly be non commutative for small enough compact open subgroups. The fact that it is commutative for K_v a well chosen maximal compact subgroup is what relates ultimately the theory of automorphic forms to commutative algebra, and is at the basis of all modern development ($R = T$. eigenvarieties, etc.) Instance of this phenomenon were first noticed by Poincaré in his paper on the shape of Saturn's rings. The proposition above is due I guess, to Bruhat, and dates back to the early fifties.

Actually we can even determine the structure of the Hecke algebra $\mathcal{H}(G(F_v), K_v, k)$. We shall only need it in the case v split, so $\mathcal{H}(G(F_v), K_v, k) = \mathcal{H}(\mathrm{GL}_n(F_v), \mathrm{GL}_n(\mathcal{O}_v), k)$.

Proposition 2.3 (Satake). *There exists an isomorphism of k -algebras*

$$\mathcal{H}(\mathrm{GL}_n(F_v), \mathrm{GL}_n(\mathcal{O}_v), k) \simeq k[T_1, \dots, T_{n-1}, T_n, T_n^{-1}]$$

that sends T_i to the characteristic function of

$$\mathrm{GL}_n(\mathcal{O}_v) \mathrm{diag}(\pi, \dots, \pi, 1, \dots, 1) \mathrm{GL}_n(\mathcal{O}_v),$$

where the number of π 's is i .

Lemma and Definition 2.1. Let V be a smooth irreducible representation of $G(F_v)$ over k , and K_v a maximal hyperspecial subgroup of G . The statements $V^{K_v} \neq 0$ and $\dim_1 V^{K_v} = 1$ are equivalent. We call V *unramified* if they hold.

Actually this lemma follows from the proposition 2.2 above as follows: we can easily (see exercise 2.4) reduce to the case k algebraically closed and then since if V is irreducible, V^K is as a $\mathcal{H}(G, K_v, k)$ -module (see exercise 2.6), hence has dimension one since the latter is commutative.

Here is an important observation: If V is unramified, V^{K_v} has dimension 1 and $\mathcal{H}(G(F_v), K_v, k)$ acts on V^{K_v} . Therefore, V determines a character

$$(1) \quad \psi_{V,v} : \mathcal{H}(G(F_v), K_v, k) \rightarrow k.$$

It is a theorem (that we shall not use) that V is uniquely determined by ψ_V .

The information containing in $\psi_{V,v}$ (that is the list of values $\psi_V(T_1), \dots, \psi_V(T_n)$ in k , the latter being non-zero), can be summarized in a polynomial, the Satake polynomial.

Definition 2.1. The Satake polynomial of V is the polynomial

$$P_{V,v}(X) = X^n - \psi_{V,v}(T_1)X^{n-1} + \psi_{V,v}(T_2)X^{n-2} - \cdots + (-1)^n \psi_{V,v}(T_n) \in k[X].$$

Important caveat: This is not the correct normalization (for what follows). Actually coefficients should be multiplied by suitable integral power (or perhaps half-integral power) of the cardinality of the residue field. The correct form is to be found in Harris-Taylor's book. Without access to this book here, this would be an excessive effort (so close to the beach) to retrieve the correct coefficients. I'll put them after the conference.

Exercise 2.7. Prove Proposition 2.3 for $n = 2$, as follows. Replace first $\mathrm{GL}_2(K_v)$ by $G = \mathrm{PGL}_2(K_v)$ and K by the image of $\mathrm{GL}_2(\mathcal{O}_v)$ in G . Proceed as follows:

a.– Construct an isomorphism of G -representations $\mathcal{C}(G/K, k) = \mathcal{C}(X, k)$ where X is the tree of $\mathrm{PGL}_2(K_v)$ defined in [B3] and $\mathcal{C}(X, k)$ the set of functions from X to k with finite support. Deduce (use Exercise 2.5) an isomorphism of algebras $\mathcal{H}(G, K, k) \simeq \mathrm{End}_{k[G]}(\mathcal{C}(X, k))$.

b.– Let T_1 be the characteristic function of $K \mathrm{diag}(\pi, 1) K$. Show that this element of $\mathcal{H}(G, K, k)$, seen as an operator on $\mathcal{C}(X, k)$ by the above isomorphism, sends a function f on X to the function $f'(x) = \sum_{y \text{ neighbor of } x} f(y)$.

c.– Deduce that $\mathcal{H}(G, K, k) = \mathbb{C}[T_1]$. Conclude.

3. AUTOMORPHIC REPRESENTATIONS FOR G

We now fix a data (F, E, V, q) as in the preceding § and we assume that the group G is definite.

3.1. Automorphic forms.

Definition 3.1. A function $f : G(\mathbb{A}_F) = G(\mathbb{A}_{F,f}) \times G(\mathbb{A}_{F,\infty}) \rightarrow \mathbb{C}$ is said *smooth*, if it is continuous and if $f(g_f, g_\infty)$ is \mathbb{C}^∞ as a function of g_∞ (for g_f fixed) and is locally constant with compact support as a function of g_f (for g_∞ fixed).

Definition 3.2. A function $f : G(\mathbb{A}_F) \rightarrow \mathbb{C}$ is called *automorphic* (or an *automorphic form*) if it is smooth, left-invariant by $G(F)$, and if it generates a finite dimensional spaces under $G(\mathbb{A}_{F,f})$. The space of all automorphic forms is called $A(G)$.

The space $A(G)$ has a natural hermitian product

$$(f, f') = \int_{G(F) \backslash G(\mathbb{A}_F)} f(g) \bar{f}'(g) dg,$$

, which makes it a pre-Hermitian space (not a Hermitian space, since it is not complete). It has a natural action of $G(\mathbb{A}_F)$ by right translation, which preserves the hermitian product, so $A(G)$ is a pre-unitary representation.

3.2. Automorphic representations. An irreducible representation π of $G(\mathbb{A})$ is said *admissible* if, writing $\pi = \pi_f \otimes \pi_\infty$ where π_f is an irreducible representation of $G(\mathbb{A}_f)$ and π_∞ is an irreducible representation of $G(\mathbb{A}_\infty)$, then π_f is admissible.

Theorem 3.1. *The representation $A(G)$ is the direct sum of irreducible admissible representations of $G(\mathbb{A})$:*

$$(2) \quad A(G) = \bigoplus_{\pi} m(\pi)\pi,$$

where π describes all the (isomorphism classes of) irreducible admissible representations of $G(\mathbb{A})$, and $m(\pi)$ is the (always finite) multiplicity of π in the above space.

It will be convenient to denote by Irr the set (of isomorphism classes) of irreducible complex continuous (hence finite dimensional) representations of $G(\mathbb{A}_{F,\infty})$. For $W \in \text{Irr}$, we define $A(G, W)$ to be the $G(\mathbb{A}_{F,f})$ -representation by right translation on the space of smooth vector valued functions $f : G(\mathbb{A}_{F,f}) \rightarrow W^*$ such that $f(\gamma g) = \gamma_\infty f(g)$ for all $g \in G(\mathbb{A}_{F,f})$ and $\gamma \in G(\mathbb{F})$.

Proof — (Sketch) As $G(\mathbb{A}_{F,\infty})$ is compact the action of this group on $A(G)$ is completely reducible, hence as $G(\mathbb{A}_F) = G(\mathbb{A}_{F,\infty}) \times G(\mathbb{A}_{F,f})$ -representation we have:

$$A(G) = \bigoplus_{W \in \text{Irr}} W \otimes (A(G) \otimes W^*)^{G(\mathbb{A}_{F,\infty})}.$$

But we check at once that the restriction map $f \mapsto f|_{1 \times G(\mathbb{A}_{F,f})}$ induces a $G(\mathbb{A}_{F,f})$ -equivariant isomorphism

$$(A(G) \otimes W^*)^{G(\mathbb{A}_{F,\infty})} \simeq A(G, W).$$

As a consequence, the compactness of $G(F) \backslash G(\mathbb{A}_f)$ shows, by classical arguments that $A(G)$ is admissible, which together with the pre-unitariness of $A(G, W)$ proves the lemma. \square

Definition 3.3. An irreducible representation π of $G(\mathbb{A})$ is said to be *automorphic* if $m(\pi) \neq 0$.

Automorphic representations (for definite unitary groups) are always algebraic, in the following sense.

Proposition 3.1. *If π is automorphic, the representation π_f has a model over $\bar{\mathbb{Q}}$.*

Proof — Let $W \in \text{Irr}$ and let us restrict it to $G(F) \hookrightarrow G(\mathbb{A}_{F,\infty})$. As is well known W comes from an algebraic representation of G , hence the inclusion $\bar{\mathbb{Q}} \subset \mathbb{C}$ equips W with a $\bar{\mathbb{Q}}$ -structure $W(\bar{\mathbb{Q}})$ which is $G(\bar{\mathbb{Q}})$ -stable. As a consequence, the obviously defined space $A(G, W(\bar{\mathbb{Q}}))$ provides a $G(\mathbb{A}_f)$ -stable $\bar{\mathbb{Q}}$ -structure on $A(G, W)$, and the results follows. \square

Definition 3.4. We say that a compact open subgroup U of $G(\mathbb{A}_f)$ is a *level* for an automorphic form π if $\pi^U \neq 0$. Equivalently $\pi_f^U \neq 0$. Or we say simply that π has level U . The weight of π is simply the finite dimensional representation π_∞ .

Of course, if $U' \subset U$ and then if π has level U it has also level U' .

It is not hard to see that there exists only a finite number of automorphic representations with a fixed level and weight. (We shall not use it, but it fixes the ideas).

3.3. Decomposition of automorphic representations. Recall that if $(V_i)_{i \in I}$ is a family of vector spaces, with $W_i \subset V_i$ a given dimension 1 subspace defined for almost all i (that is for all i except for a finite set J_0 of I), then the restricted tensor product $\bigotimes'_{i \in I} V_i$ is defined as the inductive limit of $\bigotimes'_{i \in J} V_i \otimes \bigotimes_{i \in I-J} W_i$ over the filtering set ordered by inclusion, of finite subsets J (containing J_0) of I .

Theorem 3.2. *Every admissible irreducible representation π_f of $G(\mathbb{A}_{F,f})$ can be written in a unique way as a restricted tensor product $\pi_f = \bigotimes'_{v \text{ finite place}} \pi_v$ where π_v is a irreducible admissible representation of $G(F_v)$, and π_v is unramified for almost all v . More precisely, if $\pi_f^U \neq 0$ where $U = \prod_v U_v$, then $\pi_v^{U_v} \neq 0$.*

In particular, an automorphic representation $\pi = \pi_f \otimes \pi_\infty$ has components π_v at all places v of F : For finite v these are the components π_v of π_f in the above sense, and for infinite v , simply the component of π_∞ in the usual sense. If π_f has level $U = \prod_v U_v$, with U_v hyperspecial for all v except those in a finite set of places Σ , then π_v is unramified for $v \notin \Sigma$.

4. GALOIS REPRESENTATIONS

4.1. set-up. Let π be an automorphic representation of level U , and assume that U contains $\prod_v U_v$. Let $\Sigma(U)$ be the set of places v of F such that

- (i) the place v splits in E
- (ii) U_v is a compact maximal (necessarily hyperspecial) of $G(F_v)$

If $v \in \Sigma(U)$, then π_v is an unramified representation of $G(F_v)$, defined over $\bar{\mathbb{Q}}$. The choice of one of the two places w of v defines an isomorphism (up to conjugacy) $G(F_v) \simeq \mathrm{GL}_n(F_v)$, so allows us to see π_v as a well-determined up to isomorphism representation of $\mathrm{GL}_n(F_v)$. To such a representation one can attach its Satake polynomial, that we shall denote by $P_{\pi,w}(X)$.

4.2. Existence. The following theorem may now be considered as proven (even if some details have not yet appeared in print).

Let us fix an embedding of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_p$.

Theorem 4.1. *Let p be a prime. There exists a unique semi-simple Galois representations $\rho_\pi : G_E \rightarrow \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$ such that at all places v of F in $\Sigma(U)$ such that v does not divide p , then for the two places w of E above v , ρ_π is unramified at w ,*

and the characteristic polynomial of $\rho_\pi(\text{Frob}_w)$ has coefficients in $\bar{\mathbb{Q}}$ and is equal to $P_{\pi,w}$.

Note that the representation ρ_π is a representation of G_E , not of G_F . Let us prove the uniqueness: The set of w above a place in $\Sigma(\pi)$ has density one in G_E . Therefore by Chebotarev, the set of such Frob_w in G_E is dense, and in particular the character of ρ_π is well determined by our condition. Therefore so is ρ_π since it is assumed semi-simple. (the proof of existence is about five thousand times longer).

4.3. Properties. The representation ρ_π enjoys many more properties. Let us give the most important ones.

- (i) The non trivial automorphic $c \in \text{Gal}(E/F)$ induces by conjugation an outer automorphism of G_E , still denoted c . We have $\rho_\pi^c = \rho_\pi^*(1-n)$. In particular ρ_π is polarized in the sense of my notes on Bloch-Kato.

This is easy by looking at the form of the characteristic polynomials $P_{\pi,w}$ and $P_{\pi,w'}$ where w and w' are the two places above v , where v is as in the theorem. Of course, I have not been explicit enough about the normalization so that you can check the details.

- (ii) If v is any place of F where π is unramified, and w is a place of E above v , then ρ_π is unramified at w . (this is contained in the theorem for v split, but this also true for v inert.) In particular ρ_π is unramified almost everywhere.
- (iii) For v split, and w above v , the restriction of ρ_π to G_{E_w} corresponds by Local Langlands to the representation π_v of $G(F_v)$ seen as a representation of $\text{GL}_n(F_v)$ using the isomorphism determined by w . This determines what happens at all split v , for π unramified or not at v . (the analog statement for v non-split is not known in full generality so far).
- (iv) The representations ρ_π is de Rham at all places dividing p and the Hodge-Tate weights are determined by π_∞ . The representation ρ_π is even crystalline at those places w of E that are unramified above places v of F such that π_v is unramified. The crystalline Frobenius slope are determined by π_∞ and $P_{\pi,w}$.
- (v) The representation ρ_π is geometric. (This follows from (ii) and (iv)). In most cases (technically, if π_∞ is regular – see below), it is known by construction that ρ_π actually comes from geometry. If ρ_π is irreducible, it is pure of motivic weight, $1-n$.
- (vi) The L -function $L(\rho_\pi, s)$ satisfy all conjectures about L -functions stated in [B2] (continuation, no zeros on the closure of the domain of convergence, no poles except in trivial cases, functional equation).

Note that ρ_π is not irreducible in general. We can construct examples (*endoscopic* forms and *C.A.P* forms) of π for which ρ_π is reducible, and even some where its constituents have not all the same motivic weights (in those cases though, the set of

motivic weights is an arithmetic progression of ratio 1). However, for a large class of representations π called *stable* (defined as those π whose base change to GL_n/E is cuspidal), it is expected that ρ_π is irreducible. It is known so far only if $n \leq 3$ (Blasius-Rogasky for $n = 3$), $n = 4$ if $F = \mathbb{Q}$ and $\pi^c = \pi$ (Ramakrishna) or any n and E but π_v square integrable at some place v of F split in E (Taylor-Yoshida).

4.4. Hodge-Tate weights. We here explain how the weight π_∞ of π determine the HT weights of ρ_π . For simplicity, we do so only in the case where $F = \mathbb{Q}$ and p splits in F . In this case π_∞ is simply a representation of the compact Lie group $U(n)(\mathbb{R})$, necessarily finitely dimensional.

If $\underline{m} := (m_1, \dots, m_n) \in \mathbb{Z}^n$ satisfies $m_1 \geq m_2 \geq \dots \geq m_n$, we denote by $W_{\underline{m}}$ the rational (over \mathbb{Q}), irreducible, algebraic representation of GL_m whose highest weight relative to the upper triangular Borel is the character¹

$$\delta_{\underline{m}} : (z_1, \dots, z_n) \mapsto \prod_{i=1}^n z_i^{m_i}.$$

For any field F of characteristic 0, we get also a natural irreducible algebraic representation $W_{\underline{m}}(F) := W \otimes_{\mathbb{Q}} F$ of $\mathrm{GL}_n(F)$, and it turns out that they all have this form, for a unique \underline{m} .

Let us fix an embedding $E \hookrightarrow \mathbb{C}$, which allows us to see $U(n)(\mathbb{R})$ as a subgroup of $\mathrm{GL}_n(\mathbb{C})$ well defined up to conjugation (see Prop.1.1). So for \underline{m} as above, we can view $W_{\underline{m}}(\mathbb{C})$ as a continuous representation of $U(n)(\mathbb{R})$. As is well known, the set of all $W_{\underline{m}}(\mathbb{C})$ is a system of representatives of all equivalence classes of irreducible continuous representations of $U(m)(\mathbb{R})$. We will say that $W_{\underline{m}}$ has *regular weight* if $m_1 > m_2 > \dots > m_n$.

So by the above $\pi_\infty = W_{\underline{m}}(\mathbb{C})$. The identification depends on an embedding of E to \mathbb{C} hence an embedding of E to the field $\bar{\mathbb{Q}}$ of algebraic number in \mathbb{C} , hence via the chosen embedding of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_p$, an embedding $E \hookrightarrow \bar{\mathbb{Q}}_p$, that is a place w of E above p .

Proposition 4.1. *The Hodge-Tate weights of $(\rho_\pi)_{|G_{E_w}}$ are $k_1 = -m_1 + 1, k_2 = -m_2 + 2, \dots, k_n = -m_n + n$.*

Note that the Hodge-Tate weights are always distinct (this is a consequence of our working with a definite unitary group, analog to the fact that "modular forms of weight 1 (that is of HT weights 0 and 0) are not quaternionic modular forms"). When π_∞ is regular, two Hodge-Tate weights are never consecutive numbers.

Exercise 4.1. a.– If w' is the other place of E above p , what are the Hodge-Tate weights of $(\rho_\pi)_{|G_{E_{w'}}}$?

b.– Is your answer conform to prediction 2.1 of [B2] ?

¹This means that the action of the diagonal torus of GL_n on the unique \mathbb{Q} -line stable by the upper Borel is given by the character above.

REFERENCES

- [B2] J. Bellaïche, *An introduction to the conjecture of Bloch and Kato*, this volume.
- [B3] J. Bellaïche, *Ribet's lemma and pseudocharacters*, this volume.
- [Buz] K. Buzzard, *Eigenvarieties*, proceedings of the LMS Durham Conference on L-functions and arithmetic.
- [BC1] J. Bellaïche & G. Chenevier, *Formes automorphes non tempérées et conjectures de Bloch-Kato*, Annales de l'ENS (2004). Also available on arxiv 02
- [BC2] J. Bellaïche & G. Chenevier, *p-adic Families of Galois representations*, Astérisque, 324, SMF (2009). Also available on arxiv 0602340 (2006).
- [Ca] P. Cartier *Representations of p-adic groups, a survey*, in *Automorphic forms, Representations, and L-functions*, A. Borel & W. Casselman (editors), "Corvallis" PSPM 33, volume 1, A.M.S
- [Cas] W. Casselman, *Introduction to the theory of admissible representations of p-adic reductive groups*, unpublished, see: <http://www.math.ubc.ca/~cass/research/p-adic-book.dvi>.
- [Ch1] G. Chenevier, *Familles p-adiques de formes automorphes pour $GL(n)$* , Journal für die reine und angewandte Mathematik 570 (2004), 143–217.
- [CoBr] O. Brinon & B. Conrad &, *p-adic Hodge theory*, this volume.
- [E1] M. Emerton, *On the interpolation of systems of eigenvalues attached to automorphic Hecke eigenforms*, Invent. Math. 164 no.1 (2006), 1–84.
- [Ki] M. Kisin, *Lectures on deformations of Galois representations*, this volume
- [M] S. Morel, *On the cohomology of certain non-compact Shimura varieties*, to appear in the Annals of Mathematics Studies, available on <http://www.math.ias.edu/morel/>
- [Sh] S. W Shin, *Odd-dimensional Galois representations arising from some compact Shimura varieties*, preprint.

E-mail address: `jbellaic@brandeis.edu`

MATH DEPARTMENT, MS 050, BRANDEIS UNIVERSITY, 415 SOUTH STREET, WALTHAM, MA 02453