ON NUMBER FIELDS WITH GIVEN RAMIFICATION

GAËTAN CHENEVIER

ABSTRACT: Let E be a CM number field and let S be a finite set of primes of E containing the primes dividing a given prime number l and another prime u split above the maximal totally real subfield of E. If E_S denotes a maximal algebraic extension of E which is unramified outside S, we show that the natural maps $\mathrm{Gal}(\overline{E_u}/E_u) \longrightarrow \mathrm{Gal}(E_S/E)$ are injective. We discuss generalizations of this result.

INTRODUCTION

Let E be a number field and S a nonempty set of places of E. We denote by E_S a maximal algebraic extension of E unramified outside S. Let us fix $u \in S$ and an E-embedding φ of E_S in an algebraic closure $\overline{E_u}$ of E_u. In this paper, we are interested in the following property:

$$(P_{E,S,u}) \qquad\qquad\qquad E_S \text{ is dense in } \overline{E_u},$$

where the identification of E_S with $\varphi(E_S)$ is understood. It is easy to see that $P_{E,S,u}$ is independent of the choice of φ, and equivalent to each of the following properties:

(i) the map $\mathrm{Gal}(\overline{E_u}/E_u) \longrightarrow \mathrm{Gal}(E_S/E)$ induced by φ is injective,

(ii) the E_u-vector space generated by E_S is $\overline{E_u}$,

(iii) for all finite extension K/E_u, there exists a number field E'/E unramified outside S and a place $u'|u$ such that K has a continuous embedding into $E'_{u'}$.

A trivial remark is that if $u \in S' \subset S$, then $P_{E,S',u}$ implies $P_{E,S,u}$. Moreover, a simple argument using Krasner's lemma and a weak approximation theorem shows that a stronger form of $(P_{E,S,u})$ is true[1] if S contains almost all the places of E. However, Minkowski's theorem asserts that $\mathbb{Q}_{\{\infty\}} = \mathbb{Q}$, hence $P_{\mathbb{Q},\{\infty\},\infty}$ is not satisfied. For these reasons and others related to arithmetic geometry which will become clear later, we shall focus our attention on the case where S is a *finite set* containing all the archimedian places

---

[1]Let M be a local field, $d \geq 1$ an integer, and $Q \in M[T]_d$ a separable polynomial of degree d. By continuity of roots and Krasner's lemma, if $R \in M[T]_d$ is sufficiently close to Q, then $M[T]/(R) \simeq M[T]/(Q)$ as M-algebra. Now, let S' be a finite set of places of a number field E, and let us fix for each $x \in S'$ an étale E_x-algebra A_x, each of same degree d. Then the argument above, the primitive element theorem, and the weak approximation for the affine line over E, show that there exists an étale E-algebra A of degree d, with $A \otimes_E E_x \simeq A_x$ for all $x \in S'$. It implies the claim if we take S' to be the set of places x of E such that $x = u$ or $x \notin S$, $A_u := K$, and (for example...) $A_x = E_x^d$ if $x \in S'\backslash\{u\}$. Of course, this simple approach is inefficient when S' is not finite.

of E and all the finite places dividing a given prime number l. As $P_{E,S,u}$ is then obviously true for each archimedian place u (e.g. because of cyclotomic fields), let us assume also that u is finite. At least in this setting, the question of deciding if $P_{E,S,u}$ is true seems to be in the folklore of algebraic number theory[2], and as far as the author knows, there was no example before this paper of such a triple (E, S, u) where the answer was known. Note that although local Galois groups are pro-solvable, it does not seem possible[3] to deduce property $P_{E,S,u}$ by induction from class field theory (or by Grunwald-Wang theorem, [AT][p.105]), the obstructions given by units forcing us to enlarge S at each step (see also prop. 1 §3). Let us mention also that a weak version of $P_{E,S,u}$ is known by the work of Kuz'min and V.G. Mukhamedov ([MU], [NSW] chapter X, §6, thm. 10.6.4 and the last exercise) concerning p-extensions of CM fields. For example, the following result is proved in [MU]. Let p be a prime number and let E be a CM field with maximal totally real subfield F such that each prime v of F dividing p splits in E. If v is such a place, then the canonical maps

$$\mathrm{Gal}(\overline{F_v}/F_v)_p \longrightarrow \mathrm{Gal}(\overline{E}_{\{p,\infty\}}/E)_p,$$

are injective. In this statement, H_p denotes the maximal pro-p-quotient of the profinite group H. However, there seems to be no way to deduce property $P_{E,\{\infty,p\},v}$ from these ones. We come now to our results:

Theorem 1. *Assume that E is a CM field and that u is split above a finite place v of the maximal totally real subfield F of E. If l is a rational prime number which is prime to v, and if S is the set of places of E dividing lv, then $P_{E,S,u}$ holds.*

Corollary 1. *If E and S are as in Theorem 1, then any integer $n \geq 1$ divides the pro-cardinal of $\mathrm{Gal}(E_S/E)$.*

Indeed, this last property is a general consequence of $P_{E,S,u}$ when u is finite, as $\mathrm{Gal}(\overline{E_u}/E_u)$ has then a continuous surjective homomorphism to $\widehat{\mathbb{Z}}$. As Milne pointed out to us, this corollary answers in some cases a question raised in [M, Chap. I §4] (concerning the set P defined there). Note that the hypothesis of Theorem 1 are satisfied for instance if E is a quadratic imaginary field split at a prime number $v = p$, and l is a prime $\neq p$. It has the following consequence for $E = \mathbb{Q}$:

Corollary 2. *Let p be a prime number, N an integer such that $-N$ is the discriminant of an imaginary quadratic field in which p splits, and let S be the set of primes dividing $Np\infty$. Then $P_{\mathbb{Q},S,p}$ holds.*

Explicit examples are given by $(p, N) \in \{(2, 7), (3, 2^3), (3, 11), (5, 2^2), (5, 11), (7, 3), \dots\}$. In fact, as we will see later, we certainly conjecture that if p and l are distinct primes, then $P_{\mathbb{Q},\{\infty,p,l\},p}$ holds:

---

[2]In particular, it had been asked by Ralph Greenberg after a related question raised by James Milne concerning the procardinal of $\mathrm{Gal}(E_S/E)$ (see [M, Chap. I §4] and our corollary 1).

[3]The author confesses that he did not manage to prove that the "the maximal pro-solvable extension of E inside E_S is not dense in $\overline{E}_u$", although it seems reasonable.

Theorem 2. *Let p and l be any distinct prime numbers, and assume hypothesis* 1 *and* 2 *(see §4.1), then $P_{\mathbb{Q},\{\infty,p,l\},p}$ holds.*

Although it is tempting to conjecture that $P_{\mathbb{Q},\{\infty,l\},l}$ holds, we are unfortunately less definite in this case (see §4.2).

Let us describe a bit the strategy of the proofs. First, we have to construct a lot of number fields unramified outside a given set of places S. By a well known result of Grothendieck, the number fields attached to the l-adic étale cohomology of a proper smooth scheme X over E satisfy this property if X has good reduction outside S, and if S contains the primes dividing l. Although it might be very difficult in general to find such an X (S being given), well chosen Shimura varieties give some interesting examples. Even better, their l-adic cohomology is completely described, at least conjecturally, by the Langlands conjectures, in terms of cohomological automorphic forms. By the work of many authors, culminating to Harris and Taylor's proof of local Langlands conjecture for GL_n, a big part of these conjectures is known for the so-called "simple" Shimura varieties, which are attached to some unitary groups. This combined with some other tricks allowed Harris and Taylor to attach an l-adic representation to a wide class of cuspidal automorphic forms for $\mathrm{GL}_n(\mathbb{A}_E)$ ([HT, thm. C]), compatible with the local Langlands correspondence at all finite places not dividing l. Thus, we first show that we can construct cuspidal automorphic forms for $\mathrm{GL}_n(\mathbb{A}_E)$ satisfying Harris-Taylor's conditions, and which are unramified outside S and of given "ramification type" at u. More precisely, we first construct some automorphic forms on well-chosen unitary groups and we apply quadratic base-change to them (§1.1, §1.2). By Harris and Taylor's result, their associated l-adic Galois representations give us number fields with the required local properties and some control at u (§2.1). The local Langlands correspondence shows then that we can produce in this way a lot of such number fields, using unitary groups *of all ranks*. Two little subtleties arise at this point. First, we have little control, of course, on the Weil numbers in the above constructions, i.e. on the *unramified part* of the completion at u of the number fields constructed. The second one is that the automorphic representations we consider must fulfill some conditions so that we may apply to them the results of Harris and Taylor and the known cases of quadratic base change. However, a simple trick (§2.2) allows us to show that we produced sufficiently many number fields to prove Theorem 1.

As the sketch above shows, a question closely related to our initial aim is to ask if there exists pure motives over E with "reduction type" prescribed at each finite place (and say generic Hodge numbers). On the automorphic side, it leads to the purely analytic problem of constructing non trivial, discrete, algebraic automorphic forms for a given reductive $\mathbb{Q}$-group H, with prescribed properties at all finite places. Of course, it is not always possible, e.g. an anisotropic torus has this property if and only if its real points are compact. In §3, we show how to construct these automorphic forms under the following hypothesis on H: its center has finite arithmetic subgroups and $H(\mathbb{R})$ has a holomorphic discrete series. This result was probably known to specialists, but we could not find any convenient reference in this generality. By similar arguments as in the proof of Theorem 1, and using these automorphic representations, we explain in the

last section some consequences concerning property $P_{E,S,u}$ of some standard conjectures in the arithmetic theory of automorphic forms. In particular, we get Theorem 2.

Notations: If F and G are two subfields of a given field, we denote by $F.G$ the *subfield* generated by F and G. This is also the F-vector space generated by G if G is algebraic over $F \cap G$. If K is a field, $\overline{K}$ denotes a separable algebraic closure of K, and $G_K := \mathrm{Gal}(\overline{K}/K)$ its absolute Galois group, equipped with its Krull topology. If $\rho : G_K \to H$ is any continuous group homomorphism to a topological group H, we will denote by $K(\rho) := \overline{K}^{\mathrm{Ker}(\rho)}$ the algebraic normal extension of K fixed by $\mathrm{Ker}(\rho)$. We will say that $K(\rho)$ is the extension of K *cut out* by ρ. If K is a finite extension of $\mathbb{Q}_p$, $K^{ur} \subset \overline{K}$ denotes its maximal unramified extension, $W_K \subset G_K$ its Weil group, and $I_K = \mathrm{Gal}(\overline{K}/K^{ur}) \subset W_K$ its inertia group. If F is a number field, $\mathbb{A}_F$ denotes the adèle ring of F and $\mathbb{A}_{F,f}$ its quotient of finite ones. If $p + q = n$, we denote by $\mathcal{U}(p,q)$ the real unitary group of signature (p,q), and we set $\mathcal{U}(n) := \mathcal{U}(n,0)$.

Contents

1. Construction of some automorphic forms I

Let E be a CM field as in the statement of Theorem 1. Let us fix a finite place w of F dividing the prime number l (in particular $w \neq v$), and let $n \geq 1$ be an integer.

1.1. **Some unitary groups.** We want to consider unitary groups attached to central division algebras over E, which are quasisplit at each finite place $\neq w, v$, and compact at infinite places for convenience. The relevant "Hasse principle" is known and due to Kneser. We refer to Clozel's paper [C] §2 for a convenient exposition of Kottwitz' interpretation of Kneser's results in the special case of unitary groups.

Lemma 1. *There exists a unitary group* $\mathrm{U}(n)$ *over* F *attached to* E/F *such that for a place* x *of* F, $\mathrm{U}(n)(F_x)$ *is:*

(a) *quasisplit if* x *is a finite place not dividing* wv,

(b) *the group of units of a central division algebra over* F_x *if* $x = v$.

(c) *the compact real unitary group if* x *is real.*

Proof. If n is odd, there is no global obstruction to the existence of such groups by [C][Lemma 2.1]. Assume n is even. By *loc.cit.* (2.2), the global obstruction lies in $\mathbb{Z}/2\mathbb{Z}$ and is the sum of all local ones modulo 2. Assuming given local groups satisfying (a), (b), and (c), we can make the global invariant vanish by requiring, if necessary, that $\mathrm{U}(n)(F_w)$ is either a non-quasisplit unitary group or the units of a division algebra, because such groups have local invariant $\equiv 1 \bmod 2$ by loc.cit. (2.3). This concludes the proof. $\square$

1.2. **Construction of automorphic forms.** Let H/F be the unitary group $\mathrm{U}(n)$ given by Lemma 1. The group $H(F_v)$ is the group of units of a central division algebra D over F_v of rank n^2. Let π be an irreducible, finite dimensional, complex smooth representation of D^*.

Lemma 2. *There exists an irreducible automorphic representation Π of $H(\mathbb{A}_F)$ such that:*

   (a) *If $x \neq v, w$ is finite place, then Π_x is unramified,*

   (b) *$\Pi_v \simeq \pi \otimes \psi$ for some unramified character $\psi : D^* \to \mathbb{C}^*$,*

Proof. We first choose, for each finite place x of F, a particular compact open subgroup J_x of $H(F_x)$. If x is different from v and w, $H(F_x)$ is quasisplit so that we can take for J_x a maximal compact subgroup which is *very special* in the sense of [La, §3.6] (when x does not ramify in E, the hyperspecial compact subgroups of $H(F_x)$ are very special; for almost all x we may and want to take $J_x = H(\mathcal{O}_{F_x})$). For such a place x, an irreducible admissible representation of $H(F_x)$ will be said to be *unramified* if it has a nonzero vector invariant by J_x. If $x = v$, we take $J_x = \mathcal{O}_D^*$ and we fix an irreducible constituent τ_v of $\pi_{|J_v}$. If $x = w$, we take any compact open subgroup of $H(F_x)$ for J_x. Let $J := \prod_x J_x$, it is a compact open subgroup of $H(\mathbb{A}_{F,f})$. Let τ be the trivial extension to J of the representation τ_v of J_v, via the canonical projection $J \to J_v$.

As $H_\infty := H(F \otimes_{\mathbb{Q}} \mathbb{R})$ is compact, the group $H(F)$ is discrete in $H(\mathbb{A}_{F,f})$. In particular, $\Gamma := H(F) \cap J$ is a finite group. For any continuous (finite dimensional), complex representation W of H_∞, we set $W(\tau) := W \otimes \tau^*$, viewed as an $H_\infty \times J$-representation. By the Peter-Weyl theorem, we can find an irreducible W such that $W|\Gamma$ contains a copy of τ, and so a nonzero element $v \in W(\tau)^\Gamma$ (for the diagonal action of Γ). We choose moreover an element $\varphi \in W(\tau)^*$ such that $\varphi(v) = 1$. Let $h : H_\infty \times J \to \mathbb{C}$ be the coefficient of $W(\tau)$ defined by $h(z) := \varphi(z^{-1}.v)$. By construction, h is smooth, left Γ-invariant, and generates copies of $W(\tau)^*$ under the right translations by $H_\infty \times J$, since $W(\tau)$ is irreducible. It is nonzero since $h(1) = 1$. It extends then uniquely to a smooth map $f_h : H(\mathbb{A}_F) \to \mathbb{C}$ null outside the open subset $H(F).(H_\infty \times J)$ and satisfying $f_h(\gamma z) = f_h(z)$, $\forall \gamma \in H(F)$, $z \in H(\mathbb{A}_F)$, i.e. which is an automorphic form for H. Let $\Pi \subset L^2(H(F) \backslash H(\mathbb{A}_F), \mathbb{C})$ be an irreducible constituent of the $H(\mathbb{A}_F)$-representation generated by f_h.

By definition, Π_x is unramified if $x \neq v, w$ is a finite place, hence (a) holds. Moreover, Π_v is an irreducible representation of $H(F_v)$ whose restriction to J_v contains τ_v. As π is supercuspidal and as (J_v, τ_v) is a $[H(F_v), \pi]_{H(F_v)}$-type by [BK, prop. 5.4], π and Π_v

can differ only by a twist by an unramified character of $H(F_v)$, proving (b). We recall the argument for the convenience of the reader. Let $Z = F_v^*$ denote the center of D^*, $\widetilde{J}_v := Z\mathcal{O}_D^* \subset D^*$, and $\widetilde{\tau}$ the natural extension of τ to $\widetilde{J}_v$ which is contained in $\Pi_{v|\widetilde{J}_v}$. Note that any unramified character of Z extends to a unramified character of D^*, hence we may assume that $\pi_{|\widetilde{J}_v}$ contains $\widetilde{\tau}$, by replacing π by some unramified twist if necessary. Note that $D^*/\widetilde{J}_v \simeq \mathbb{Z}/n\mathbb{Z}$ is finite abelian and that its characters are unramified characters of D^*. We conclude as Π_v is a constituent of $\mathrm{Ind}_{\widetilde{J}_v}^{D^*} \pi_{|\widetilde{J}_v} \simeq \pi \otimes_{\mathbb{C}} \mathbb{C}[D^*/\widetilde{J}_v].\square$

2. Proof of Theorem I

2.1. **Construction of S-unramified number fields.** With the assumptions of §1, let S be the set of places of E dividing lv. We fix an embedding $\varphi : E_S \to \overline{F_v}$ extending the F-embedding $E \to \overline{F_v}$ given by u. Let us denote by

$$\mathrm{G}_{E,S} := \mathrm{Gal}(E_S/E).$$

Attached to φ is a group homomorphism $\mathrm{G}_{F_v} \to \mathrm{G}_{E,S}$ (see the introduction for the notations). We keep the assumption of §1.2, and we choose a Π given by Lemma 2. We assume from now that π *corresponds to a supercuspidal representation of* $\mathrm{GL}_n(F_v)$ *by the Jacquet-Langlands correspondence*, that is $\dim_{\mathbb{C}}(\pi) > 1$ if $n > 1$. The local Langlands correspondence (see [HT]) associates to π an continuous, irreducible, representation

$$\psi_\pi : \mathrm{W}_{F_v} \longrightarrow \mathrm{GL}_n(\mathbb{C}).$$

Let $F_v^{ur}(\pi) \subset \overline{F_v}$ be the finite extension of F_v^{ur} which is fixed by $\mathrm{Ker}((\psi_\pi)_{|I_{F_v}})$, that is the extension of F_v^{ur} cut out by $(\psi_\pi)_{|I_{F_v}}$. Recall that l is prime to v and fix embeddings $\iota_l : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}_l}$ and $\iota_\infty : \overline{\mathbb{Q}} \to \mathbb{C}$.

Lemma 3. *(i) There exists a continuous representation*

$$R : \mathrm{G}_{E,S} \to \mathrm{GL}_n(\overline{\mathbb{Q}_l}),$$

such that $R_{|W_{F_v}}$ corresponds to $\Pi_v \otimes |\det|^{(n-1)/2}$ by the local Langlands correspondence,

(ii) $F_v^{ur}.\varphi(E_S) \supset F_v^{ur}(\pi)$.

Proof. This lemma is a consequence of conditional automorphic base change ([C], [CL], [HL]), of Jacquet-Langlands correspondence, and of the main theorem of Harris & Taylor [HT]. Precisely, let us denote by BC the quadratic base change from H to $H' := \mathrm{Res}_{E/F}(H \times_F E)$. By Theorem 3.1.3 of [HL] (generalizing [CL, thm. A.5.2] and [C]), there is a cuspidal automorphic representation Π' of $H'(\mathbb{A}_F)$ such that $\Pi'_x = \mathrm{BC}(\Pi_x)$ for each place $x \neq w$ of F. It applies because Π_∞ is automatically cohomological as $H(F \otimes_{\mathbb{Q}} \mathbb{R})$ is compact, and because H is attached to a division algebra, as $H(F_v)$ is. Note that BC has been defined for unramified representations at the places x such that $H(F_x)$ is a ramified, quasisplit, unitary group, in [La, §3.6, prop. 3.6.4][4]. In

---

[4] As Labesse explained to us, the confusing hypothesis "G is unramified, and K^G is hyperspecial" in prop. 3.6.4 *loc. cit.* should be understood as "G_0 is unramified *over* E_x, and K^G is hyperspecial viewed as a subgroup of $G_0(E_x)$" (for us $G_0 = \mathrm{GL}_n(E_x)$), so as to be of any use, and the same proof applies

particular, Π'_x is unramified if $x \notin S$, $\Pi'_v = \Pi_v \otimes \Pi^*_v$, and Π'_∞ has the base change infinitesimal character. We can then apply[5] Theorem C of [HT] to the image $\mathrm{JL}(\Pi')$ of Π' by the Jacquet-Langlands correspondence (due to Vignéras, see [HT, thm. VI.1.1]), and consider

$$R := R_l(\mathrm{JL}(\Pi'))$$

given by *loc. cit* and the embeddings ι_l, ι_∞, which proves (i).

We check the second assertion. Let us denote by $E_S(R)$ the subfield of E_S fixed by $\mathrm{Ker}(R)$. As $\mathrm{Gal}(\overline{F_v}/(F_v.\varphi(E_S(R)))) = \mathrm{Ker}(R_{|\mathrm{G}_{F_v}})$, Galois theory shows that

$$F_v.\varphi(E_S(R)) = F_v(R_{|\mathrm{G}_{F_v}}).$$

By (i), ψ_{Π_v} is defined over $\iota_\infty(\overline{\mathbb{Q}})$ and $R_{|I_{F_v}} \simeq i_l.i_\infty^{-1}(\psi_{\Pi_v})_{|I_{F_v}}$ (it has finite image), so that $F_v^{ur}(R_{|I_{F_v}}) = F_v^{ur}(\psi_{\Pi_v})$. But by Lemma 2, π and $\Pi_v \otimes |\det|^{(n-1)/2}$ only differ by an unramified twist, hence $\psi_{\Pi_v \otimes |\det|^{(n-1)/2}}$ and ψ_π are equal when restricted to I_{F_v}. In particular, $F_v^{ur}(\pi) := F_v^{ur}(\psi_\pi) = F_v^{ur}(\psi_{\Pi_v})$, and we conclude as $F_v^{ur}.F_v(R_{|\mathrm{G}_{F_v}}) = F_v^{ur}(R_{|I_{F_v}})$.□

2.2. End of the proof.

Lemma 4. *Let $\mathbb{Q}_p \subset M \subset L \subset \overline{M}$ be a tower of field extensions with $M/\mathbb{Q}_p$ finite.*

(i) Assume that L/M is Galois and $M^{ur}.L = \overline{M}$, then $L = \overline{M}$.

(ii) If $\sigma \in \mathrm{G}_M$ acts trivially by conjugation on the tame inertia of I_M, then $\sigma \in I_M$.

(iii) Assume that for all finite Galois extension K/M such that $\mathrm{Gal}(K/M)$ admits an injective, irreducible, complex linear representation, we have $K \subset L$; then $L = \overline{M}$.

Proof. (i) Let $H := \mathrm{Gal}(\overline{M}/L) \subset \mathrm{G}_M$. By assumption, H is normal in Γ and $H \cap I_M = \{1\}$, hence $I_M H \simeq I_M \times H$ is a direct product and (i) (i.e. $H = \{1\}$) is an immediate consequence of (ii), which we now prove.

Let I_M^{tr} be the tame inertia quotient of I_M, recall that there is an isomorphism

$$I_M^{tr} \xrightarrow{\sim} \prod_{l \neq p} \mathbb{Z}_l(1),$$

which means that the action of Γ by conjugation on I_M^{tr}, which factors through the canonical map $\nu : \mathrm{Gal}(M^{ur}/M) \longrightarrow \widehat{\mathbb{Z}}$, is the multiplication by $q^{\nu(\cdot)} \in \prod_{l \neq p} \mathbb{Z}_l^*$, where q is the cardinal of the residue field of K. Let $\gamma \in \Gamma$ such that $q^{\nu(\gamma)} = 1$, we aim to prove that $\nu(\gamma) = 0$. We claim that for any integers $m \geq 2$ and $r \geq 1$, we can find infinitely many primes l such that r divides the order of the image of m in $\mathbb{F}_l^*$. Applying this claim to $m = q$, we get that r divides $\nu(\gamma)$ for all $r \geq 1$, i.e. $\nu(\gamma) = 0$. Let us prove the claim now (see also Van der Waerden's lemma [Lg, chap. X, §2, Lemma 1]). Note

_____

verbatim. If we didn't use these facts, we would be obliged to add, in the set S of the theorem, the places of E ramified above F. Note, however, that this would suffice to get corollary 2.

[5]Note that $\mathrm{JL}(\Pi')$ is cuspidal by Moeglin-Waldspurger's description of the discrete spectrum of GL_n, since $\mathrm{JL}(\Pi')_v = \mathrm{JL}(\Pi'_v)$ is supercuspidal.

that if $P \in \mathbb{Z}[X]$ is such that $P(0) \neq 0$ and $m \geq 2$ is an integer, then the sequence $(P(m^{N!}))_{N \geq 1}$ admits infinitely many prime divisors. Indeed, assuming the assertion it is false, we can find a prime p such that each power of p divides $P(m^{N!})$ for some N. As $P(0) \neq 0$, p is prime to m. Thus if we let N goes to infinity, we get that $P(1) = 0$ in $\mathbb{Z}_p$. This is a contradiction, as $P = X - 1$ certainly satisfies the assertion. The claim follows then from the special case $P := $ the rth cyclotomic polynomial.

We now show (iii). Let K/M be any finite Galois extension, $\rho_1, \ldots, \rho_t$ the irreducible, complex, linear representations of $\mathrm{Gal}(K/M)$, and $K_i \subset K$ the fixed field of $\mathrm{Ker}(\rho_i)$. By assumption, $K_i \subset L$. The existence of the (faithful) regular representation of $\mathrm{Gal}(K/M)$ implies that $\bigcap_i \mathrm{Ker}(\rho_i) = \{1\}$, so that by Galois theory we have $K = K_1 \ldots K_t$, and $K \subset L$. $\square$

Let us finish the proof of Theorem 1. Let K/F_v be a finite Galois extension such that $\mathrm{Gal}(K/F_v)$ admits an irreducible injective representation $\rho : \mathrm{Gal}(K/F_v) \to \mathrm{GL}_n(\mathbb{C})$. The local Langlands correspondence and the Jacquet-Langlands correspondence associate to ρ an irreducible smooth representation π of D^*/F_v such that ψ_π factors through ρ. Lemma 3 (ii) shows that $F_v^{ur}.\varphi(E_S) \supset F_v^{ur}(\pi)$. But $F_v^{ur}(\pi) = F_v^{ur}.K$, as ρ is injective. We have thus shown that $K \subset F_v^{ur}.\varphi(E_S)$. Applying Lemma 4 (iii) to $M = F_v$ and $L = F_v^{ur}.\varphi(E_S)$, we conclude that $F_v^{ur}.\varphi(E_S) = \overline{F_v}$. Applying now Lemma 4 (i) to $M = F_v$ and $L = F_v.\varphi(E_S)$, we get Theorem 1. $\square$

3. Construction of some automorphic forms II

In this section, we generalize some results of §1 concerning the construction of automorphic representations with prescribed properties. Let H be a connected reductive group over $\mathbb{Q}$, J be a compact open subgroup of $H(\mathbb{A}_{\mathbb{Q},f})$, and let τ be a fixed, irreducible, smooth representation of J. We aim to construct discrete, algebraic, automorphic representations Π of H, such that $\Pi_{f|J}$ contains τ. From the point of view of types theory (see [BK]), it allows us to prescribe the inertial equivalence class of each Π_v with v finite. For example, in the case of GL_n over a local field, the inertial equivalent class of a smooth irreducible representation determines the restriction to the inertia group of its Langlands parameter, hence types control the ramification in a strong sense. In general, it seems hard to prescribe more properties of Π_v, as we certainly cannot guess easily its Weil numbers if v is unramified for instance. Note moreover that such a Π may not exist, as the obstruction given by units shows in the example of the torus $H = \mathrm{Res}_{E/\mathbb{Q}}(\mathbb{G}_m/E)$ when $E \neq \mathbb{Q}$ is not quadratic imaginary.

3.1. Let H be as above and let Z denote its center. We assume that:

(A) $H(\mathbb{R})$ has a holomorphic discrete series (i.e. the derived Lie algebra of $H(\mathbb{R})$ satisfies (1) of §3.2),

(B) $Z(\mathbb{Q})$ is discrete in $Z(\mathbb{A}_{\mathbb{Q},f})$.

Proposition 1. *Let H be as above, J be a compact open subgroup of $H(\mathbb{A}_{\mathbb{Q},f})$, and let τ be an irreducible smooth representation of J. There exists an irreducible, discrete, automorphic representation Π of $H(\mathbb{A}_{\mathbb{Q}})$ such that Π_∞ is in the holomorphic discrete series, and $\Pi_{f|J}$ contains τ.*

Remarks : Note that by [B1, thm. 8.9], property (B) depends only of the isogeny class of Z. If Z is anisotropic, it holds if and only if $Z(\mathbb{R})$ is compact by thm. 8.7. *loc.cit.* It happens for example when E/F is CM and Z is $(\mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_m)^{N_{E/F}=1}$. It is easy to see that (A) and (B) both hold when H is $\mathrm{GL}_2/\mathbb{Q}$, $\mathrm{GSp}_{2n}/\mathbb{Q}$, the scalar restriction to $\mathbb{Q}$ of a unitary group attached to a CM field, $\mathrm{SO}(n,2)/\mathbb{Q}$, or when $H(\mathbb{R})$ is compact.

Before proving Proposition 1, we mention its following corollary. Let E be a CM field, F its maximal totally real subfield, v a finite place of F which splits in E, and write $v = uu'$.

Corollary 3. *Let π be a supercuspidal, irreducible, representation of $\mathrm{GL}_n(E_u)$. There exists an automorphic cuspidal representation Π of $\mathrm{GL}_n(\mathbb{A}_E)$ satisfying $\Pi^c \simeq \Pi^*$, and such that:*

(a) Π is unramified outside u, u', and Π_u is an unramified twist of π,

(b) for any x archimedian, Π_x has a regular algebraic infinitesimal character.

Proof. By the same reasoning as in the proof of Lemma 1, Hasse's principle shows that there exists a unitary group $\mathrm{U}(n)/F$ attached to E/F which is quasisplit at all finite places $\neq v$, and the group of invertible elements of a central division algebra over $F_v \xrightarrow{\sim} E_u$ at v. In fact, as the local invariant of $\mathcal{U}(m+r, m-r)$ is r mod 2 by [C, lemme 2.2], we could even assume that $\mathrm{U}(n)$ is compact at all archimedian places, except maybe one where it is $\mathcal{U}(n-1,1)$. Then $H := \mathrm{Res}_{E/\mathbb{Q}}\mathrm{U}(n)$ satisfies the hypothesis of Proposition 1, by the remarks above. Let $\pi' := \mathrm{JL}^{-1}(\pi)$ be the finite dimensional representation of $\mathrm{U}(n)(F_v)$ corresponding to π by the Jacquet-Langlands correspondence. By choosing a suitable compact open subgroup J of $H(\mathbb{A}_{\mathbb{Q},f})$ as in the proof of Lemma 2, Proposition 1 produces an automorphic discrete representation Π' of $U(n)/F$ which is unramified outside v, such that Π'_v is a twist of π' by an unramified character, and whose archimedian components are discrete series (hence cohomological by [BW, thm. 5.3. (b)]). As we are in the hypothesis of the "conditional" quadratic base change, we conclude as in the proof of Lemma 3 (i) that $\Pi := \mathrm{JL}(\mathrm{BC}(\Pi'))$ satisfies all the hypothesis of the corollary. $\square$

Note that Proposition 1 is a generalization of Lemma 2, and the same proof as *loc. cit.* would allow us to conclude verbatim when $H(\mathbb{R})$ is compact[6]. The general case relies on more delicate analytic facts. We are very grateful to Laurent Clozel for explaining us an argument using the Selberg trace formula, holding even under the assumption that $H(\mathbb{R})$ has a discrete series. In what follows, we will give an argument using Poincaré

---

[6]For the sake of exposition, and as much of the difficulty disappears in the compact case, we found it convenient to separate the proof. Moreover, Lemma 2 is not only sufficient for the proof of Theorem 1, but also fix some ideas about the general case.

series going back to Poincaré, H. Cartan and Godement (see [B2, ch. 6], [Ca1] §1, [Ca2] §6, §10, and §10 bis, for the detailed case $H_\infty = \mathrm{GSp}_{2g}(\mathbb{R})$, and most of the ideas of the general argument), so that Proposition 1 should certainly not be considered as original. Roughly, the difficulty is twofold. First, we want to use coefficients of square integrable representations of $H(\mathbb{R})$ to ensure the convergence of some Poincaré series. Then, we must have a sufficiently good control on these coefficients to produce some non identically zero automorphic forms. Thus, as a preliminary, will recall in §3.2 some facts about Harish-Chandra's realization of the holomorphic discrete series (due to Harish-Chandra).

3.2. Holomorphic discrete series. In this section, we will follow closely Knapp's book [K, chap. VI]. Let G be a real, connected, reductive Lie group, and K a maximal compact subgroup. Assume that a Cartan decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ satisfies

$$(1) \qquad\qquad\qquad Z_{\mathfrak{g}}(\mathfrak{c}) = \mathfrak{k},$$

where $\mathfrak{c}$ is the center of $\mathfrak{k}$. For example, it is easily seen to be the case for any $\mathcal{U}(p,q)$ and for symplectic groups (see *loc. cit.* §2). Let $\mathfrak{h} \subset \mathfrak{k}$ be a Cartan subalgebra, associated to a Cartan subgroup $T \subset K$, and let $\mathfrak{g}^{\mathbb{C}} = \mathfrak{h}^{\mathbb{C}} \oplus_{\alpha \in \Delta} \mathfrak{g}_\alpha$ be its associated root space decomposition.

Recall that a root $\alpha \in \Delta$ is said to be *noncompact* (resp. *compact*), if $\mathfrak{g}_\alpha \subset \mathfrak{p}^{\mathbb{C}}$ (resp. in $\mathfrak{k}^{\mathbb{C}}$). This notion gives us a partition $\Delta = \Delta_n \coprod \Delta_K$. We fix a *good* ordering on $\mathfrak{h}_{\mathbb{R}}^*$, i.e. with the property that any positive noncompact root is bigger than any compact root. We set $\mathfrak{p}^{\pm} := \oplus_{\alpha \in \Delta_n^{\pm}} \mathfrak{g}_\alpha$, these are abelian Lie subalgebras of $\mathfrak{p}^{\mathbb{C}}$ which are stable by $\mathrm{ad}(\mathfrak{k})$. We fix a complex matrix group $G_{\mathbb{C}}$ whose Lie algebra is $\mathfrak{g}^{\mathbb{C}}$, and we let $K_{\mathbb{C}}$ and $P^{\pm}$ be the complex analytic subgroups of $G_{\mathbb{C}}$ with Lie algebras $\mathfrak{k}^{\mathbb{C}}$ and $\mathfrak{p}^{\pm}$, as in §3 *loc.cit.* By Harish-Chandra's decomposition, the natural product map $P^+ \times K_{\mathbb{C}} \times P^- \to G_{\mathbb{C}}$ is a complex open immersion, and $G K_{\mathbb{C}} P^- \subset G_{\mathbb{C}}$ is an open subset, and so inherits the complex structure of $G_{\mathbb{C}}$. Moreover, there exists a bounded open domain $\Omega \subset P^+ \simeq \mathbb{C}^p$ such that $\Omega K_{\mathbb{C}} P^- = G K_{\mathbb{C}} P^-$. As $G \cap K_{\mathbb{C}} P^- = K$, the G-orbit of $1 \in G_{\mathbb{C}}/K_{\mathbb{C}} P^-$ is $G/K \simeq \Omega$.

Let us fix an analytically integral $\lambda \in \mathfrak{h}_{\mathbb{R}}^*$, which is dominant restricted to Δ_K^+, and let W_λ be the irreducible representation of $K_{\mathbb{C}}$ of highest weight λ. This W_λ gives rise to a complex algebraic vector bundle on the grassmannian $G_{\mathbb{C}}/K_{\mathbb{C}} P^-$, and we want to consider holomorphic, square integrable, sections of this bundle on Ω. Concretely, we fix a definite, K-invariant, hermitian product on W_λ, and we consider the vector space V_λ of W_λ−valued functions f on G satisfying:

(i) $\forall g \in G, \forall k \in K, f(gk) = k^{-1}.f(g),$

(ii) f is holomorphic (see below),

(iii) $\int_G |f(g)|^2 dg < \infty.$

For a map $f : G \to W_\lambda$ satisfying (i), (ii) means that the canonical P^--invariant extension of f to $GK_{\mathbb{C}}P^-$ is holomorphic. Note that V_λ is in a natural way a module over the ring of bounded holomorphic functions on Ω, and a unitary representation L_λ of G by left translation. Let $\delta := \frac{1}{2} \sum_{\alpha \in \Delta^+} \alpha$. We can now state Harish-Chandra's theorem ([K, thm. 6.6][7]):

Theorem: (Harish-Chandra) Assume that $\langle \lambda + \rho, \alpha \rangle < 0$ for all $\alpha \in \Delta_n^+$. Then V_λ is a non zero Hilbert space, and L_λ is an irreducible, square-integrable, G-representation.

We consider now a special case related to the standard jacobian automorphy factor on Ω. Let $\rho_n := \sum_{\alpha \in \Delta_n^+} \alpha \in \mathfrak{h}_{\mathbb{R}}^*$. We claim that ρ_n is analytically integral, dominant, and satisfies:

$$\text{(2)} \qquad \langle \rho_n, \alpha \rangle > 0, \quad \forall \alpha \in \Delta_n^+$$

Indeed, if $p := \dim_{\mathbb{C}} \mathfrak{p}^+$, then ρ_n is the weight of the 1-dimensional representation $\Lambda^p \mathfrak{p}^+$ of $\mathfrak{k}$. In particular, $\forall m \in \mathbb{Z}$, $m\rho_n$ is analytically integral, and dominant with respect to Δ_K^+. Moreover, by definition of the ordering, ρ_n is also the highest weight of the natural representation of $\mathfrak{g}$ on $\Lambda^p \mathfrak{g}^{\mathbb{C}} \supset \Lambda^p \mathfrak{p}^+$, and so is dominant. The last part of the claim follows, as the parabolic subalgebra $\mathfrak{k}^{\mathbb{C}} \oplus \mathfrak{p}^+$ is its own normalizer in $\mathfrak{g}^{\mathbb{C}}$.

As a consequence, we can fix an integer $r > 0$ such that $\delta := -r\rho_n$ satisfies the hypothesis of Harish-Chandra's theorem. Let us fix a an element $j \in V_\delta$ which is an eigenvector for the left translations by K, and satisfies $|j(1)| = 1$. Such an element exists: we can take the one denoted by ψ_λ in [K, Lemma 6.7]. By Harish-Chandra's convolution theorem ([K, cor. 8.41], [B2, cor. 2.22]), K-finite elements of V_λ are bounded on G, and so is j. In particular, if $f \in V_\lambda$ and if $m \geq 0$ is an integer, then $(f \cdot j^m)(g) := f(g) \otimes j^m(g)$ defines an element in $V_{\lambda+m\delta}$. For convenience, we shall often identify the 1-dimensional vector space W_δ with $\mathbb{C}$, taking $j(1)$ as a norm 1 basis element.

Example: Let $G := \mathcal{U}(n-1, 1)$, let K be the diagonal $\mathcal{U}(n-1) \times \mathcal{U}(1)$, and let $T \subset K$ be the diagonal torus. We can choose a good ordering on the roots such that $\sum_{\alpha \in \Delta^+} \mathfrak{g}_\alpha$ is the standard upper Borel subalgebra in $\mathfrak{g}^{\mathbb{C}} = \mathrm{gl}_n(\mathbb{C})$. In this case, $K_{\mathbb{C}}P^-$ identifies with the standard lower parabolic of $G_{\mathbb{C}} = \mathrm{GL}_n(\mathbb{C})$ of type $(n-1, 1)$. The bounded domain Ω identifies with the open unit hermitian ball of $\mathbb{C}^{n-1} = P^+ \subset G_{\mathbb{C}}/K_{\mathbb{C}}P^- = \mathbb{P}^{n-1}(\mathbb{C})$. We define $e_i \in \mathfrak{h}_{\mathbb{R}}^*$ by $e_i(x_1, \ldots, x_n) := x_i$. With these choices, $\Delta_n^+ = \{e_i - e_n, 1 \leq i < n\}$ and $\Delta_K^+ = \{e_i - e_j, 1 \leq i < j < n\}$. Then $\lambda = \sum_{i=1}^n m_i e_i$ satisfies the hypothesis of Harish-Chandra's theorem if, and only if, $m_1 \geq m_2 \geq \cdots \geq m_{n-1}$, $m_n > m_1 + (n-1)$, and $\forall i, m_i \in \mathbb{Z}$. We have $\rho_n = (e_1 + \cdots + e_{n-1}) - (n-1)e_n$, and we can take $\delta = -2\rho_n$.

3.3. Convergence of Poincaré series. We now begin the proof of Proposition 1. Let Z_c denote the maximal compact subgroup of $Z(\mathbb{R})$ (viewed as a real Lie group) and write $Z(\mathbb{R}) = Z_n \times Z_c$ for some closed subgroup Z_n isomorphic to some $\mathbb{R}^m$. Let G denote the

---

[7]The identification of the space we call V_λ with the one *loc.cit.* comes from Borel-Weil-Bott realization of W_λ [K, thm. 5.29].

closed connected subgroup of the Lie group $H(\mathbb{R})$ whose Lie algebra is $\mathfrak{g} = [\mathfrak{h}, \mathfrak{h}] \oplus \mathfrak{z}_{\mathfrak{c}}$. If $H(\mathbb{R})^+$ denotes the neutral component of the real Lie group $H(\mathbb{R})$, then

$$H(\mathbb{R})^+ = Z_n \times G.$$

Let $\Gamma \subset H(\mathbb{R})^+$ be the discrete subgroup $H(\mathbb{Q}) \cap (H(\mathbb{R})^+ \times J)$, let us show that $\Gamma \subset G$. Let C be the $\mathbb{Q}$-torus H/H_{der} and $\det : H \longrightarrow C$ be the canonical $\mathbb{Q}$-morphism. Note that $\det$ induces a $\mathbb{Q}$-isogeny $Z \longrightarrow C$, hence C has finite arithmetic groups by assumption (B) and [B1, thm. 8.9]. In particular, $\det(\Gamma) \subset C(\mathbb{Q})$ is a finite subgroup. But the induced map $\det : H(\mathbb{R})^+ \longrightarrow C(\mathbb{R})$ is injective restricted to Z_n, and $\det(G)$ is compact, hence $\Gamma \subset G$.

The Lie algebra $\mathfrak{g}$ satisfies (1) by assumption (A), so that we can apply to G the constructions (and notations) of §3.2. Let $\lambda \in \mathfrak{h}_{\mathbb{R}}^*$ be as in Harish-Chandra's theorem, we set $V_\lambda(\tau) := V_\lambda \otimes \tau^*$, viewed as a representation of $G \times J$. We will consider coefficients of $V_\lambda(\tau)$ of the following kind. Let $W_\lambda(\tau) := W_\lambda \otimes_\mathbb{C} \tau^*$ viewed as before as a representation of $K \times J$. If $\varphi \in W_\lambda(\tau)^*$, we can see it as a continuous linear form $\tilde{\varphi}$ on $V_\lambda(\tau)$ by $f \mapsto \varphi(f(1))$. We define $h := h_{f,\varphi} : G \times J \to \mathbb{C}$ by $h(z) := \tilde{\varphi}(z^{-1}.f) = \varphi((1 \times z_J^{-1}).f(z_G))$. The Poincaré series $P_h : G \times J \to \mathbb{C}$ is defined by

$$P_h(z) := \sum_{\gamma \in \Gamma} h(\gamma z)$$

We equip $W(\tau)$ with any hermitian norm $|.|$ such that $K \times J$ acts by unitary transformations. As $f \in L^2(G)$, it comes that $P_h \in L^2_{loc}(G \times J)$. Indeed, if $U \subset G \times J$ is a compact set, then $\Gamma \cap (UU^{-1})$ is finite, hence

$$(3) \qquad \sum_{\gamma \in \Gamma} \int_U |h(\gamma g)|^2 dg \le |\Gamma \cap UU^{-1}| \int_{G \times J} |h(g)|^2 dg \le C \int_G |f(g)|^2 dg < \infty,$$

where $C := \mathrm{vol}(I) \cdot |\Gamma \cap UU^{-1}| \cdot ||\varphi|| > 0$. As all the $g \mapsto f(\gamma.g)$ are in V_λ, and in particular holomorphic, P_h converges in fact *uniformly* on any compact subset of $G \times J$, to a holomorphic function on $G \times J$ of right $K \times J$-type $W(\tau)^*$. In particular, we proved the

Lemma 5. *Let $\lambda \in \mathfrak{h}_{\mathbb{R}}^*$ be as in Harish-Chandra's theorem, and let h be a coefficient of $V_\lambda(\tau)$ as above. The Poincaré séries P_h is normally convergent on any compact subset of $G \times J$.*

3.4. Construction of non vanishing Poincaré series. It remains to find a λ and an h such that $P_h \ne 0$. Let $\Gamma_0 \subset \Gamma$ be the finite group $\Gamma \cap K$. As in the proof of Lemma 2, we can find a finite dimensional, irreducible, complex representation $W = W_\lambda$ of K such that $W_\lambda(\tau)^{\Gamma_0} \ne 0$. By twisting W_λ by W_δ^m for an integer $m \ge 0$ big enough and divisible by $|\Gamma_0|$, (2) shows that we may assume that $\lambda \in \mathfrak{h}_{\mathbb{R}}^*$ satisfies the hypothesis of Harish-Chandra's theorem. We fix as before an element $v \in W_\lambda(\tau)^{\Gamma_0}$ of norm 1 and we choose a $\varphi \in W(\tau)^*$ of norm 1 such that $\varphi(v) = 1$. By Lemma 5 applied to $\lambda = \delta$ and to the coefficients associated to the function j itself, we get that

$$\Gamma_1 := \{\gamma \in \Gamma, |j(\gamma)| \ge 1\}$$

is a finite subset of Γ, and $\Gamma_0 \subset \Gamma_1$. We claim that we can choose an $f \in V_\lambda(\tau)$ such that

$$f(1) = v, \quad \text{and} \quad \forall \gamma \in \Gamma_1 \backslash \Gamma_0, \ f(\gamma) = 0.$$

As $V_\lambda(\tau)$ is nonzero and stable by the action of $G \times J$, we can find a $f_1 \in V_\lambda(\tau)$, such that $f_1(1) \neq 0$. But by irreducibility of $W_\lambda(\tau)$ as $K \times J$-representation, we can find in $\mathbb{C}[K \times J].f_1$ an element sending 1 to v. We can thus assume that $f_1(1) = v$. Then, we can multiply f_1 by a bounded holomorphic function f_2 on Ω such that $f_2(1) = 1$ and $f_2(\gamma) = 0$ if $\gamma \in \Gamma_1 \backslash \Gamma_0$, which certainly exists (e.g. restrictions to the bounded symmetric domain of polynomials on $P^+ = \mathbb{C}^p$). The function $f = f_1 f_2$ does the trick. This proves the claim.

For any $m \geq 1$ divisible by $|\Gamma_0|$, let us consider the element $v_m := v \otimes 1^{\otimes m} \in W_{\lambda + m\delta}(\tau)^{\Gamma_0}$ and $\varphi_m := \varphi \otimes \mathrm{id}^{\otimes m} \in W_{\lambda + m\delta}(\tau)^*$. We still have $\varphi_m(v_m) = 1$. We define h_m to be the coefficient associated to $f \cdot j^m$ and φ_m. By all the previous choices, $|h_m(\gamma)| \leq |h_0(\gamma)|, \ \forall \gamma \in \Gamma$. As $\sum_{\gamma \in \Gamma} |h_0(\gamma)| < \infty$ by Lemma 5, we get:

$$(4) \qquad\qquad P_{h_m}(1) \underset{|\Gamma_0| \,|\, m, \ m \to \infty}{\longrightarrow} \sum_{\gamma \in \Gamma_0} \varphi(\gamma.v) = |\Gamma_0| \neq 0$$

By (4), we may choose an integer m big enough such that P_{h_m} is not identically zero. We denote again by P_{h_m} its canonical Z_n-invariant extension to $H(\mathbb{R})^+ \times J = G \cdot Z_n \times J$.

Let $f : H(\mathbb{A}_\mathbb{Q}) \to \mathbb{C}$ be the unique map which is $H(\mathbb{Q})$-invariant on the left, zero outside $H(\mathbb{Q}).(H(\mathbb{R})^+ \times J)$, and which coincides with P_{h_m} on the open subset $H(\mathbb{R})^+ \times J$ (note that f is well defined). Then f is smooth, non zero, and belongs to $L^2(H(\mathbb{Q}) \backslash H(\mathbb{A}_\mathbb{Q})/Z_n, \mathbb{C})$ by the estimate (3) (take U a measurable fundamental domain for Γ acting on $G \times J$, they have finite volume). The closure of the $H(\mathbb{A}_\mathbb{Q})$-subrepresentation generated by f is then a finite sum of topologically irreducible representations, any irreducible constituent Π of which satisfies by construction the hypothesis of Proposition 1. $\square$

Remark : As shown by the proof above and by Lemma 6 below, we can even assume that the parameter λ of Π_∞ is as far from the walls of $\mathfrak{h}_\mathbb{R}^*$ as we want.

Lemma 6. *Let Γ be a finite subgroup of a compact connected Lie group K, and let τ be an irreducible complex representation of Γ. For any real $C > 0$, we can find an irreducible representation V of K such that $V_{|\Gamma}$ contains τ, and such that the highest weight of V has distance $\geq C$ from the walls.*

Proof. Using character formulas of Weyl and Kostant, we could even prove that for a dominant weight λ far enough from the walls, $(V_\lambda)_{|\Gamma}$ contains τ if and only if they have the same central character when restricted to Γ. We thank Y. Benoist for explaining us the following quick proof. We fix $\mathfrak{h} \subset \mathfrak{k}$ a Cartan subalgebra, choose a Weyl chamber, and we denote by V_λ the complex irreducible representation of K of highest weight $\lambda \in \mathfrak{h}_\mathbb{R}^*$. By the Peter-Weyl theorem, we can find dominant weights $\lambda_1, \ldots, \lambda_r$ such that $W := \oplus_{i=1} V_{\lambda_i}$ contains, when restricted to Γ, each irreducible finite dimensional complex representation of Γ. Let λ be any dominant weight, then the highest weights of $V_\lambda \otimes_\mathbb{C} W$ lie in the ball of $\mathfrak{h}_\mathbb{R}^*$ centered in λ and of radius $\sup_{i=1}^r |\lambda_i|$ (see [K, IV. §11.13]). As

$\tau \otimes_{\mathbb{C}} W_{|\Gamma}^*$ contains all irreducible representations of Γ by construction, this concludes the proof. $\square$

4. The case $E = \mathbb{Q}$

The problematic in this section is the following: is it possible to reduce property $P_{E,S,u}$ to some standard conjectures in the arithmetic theory of automorphic forms? To fix the ideas, we restrict to the case $E = \mathbb{Q}$. As Proposition 1 does not apply to $\mathrm{GL}_n/\mathbb{Q}$ for $n > 2$, we must use other classical groups, which introduces some obstructions on the L-parameters we can reach with them. It turns out that admitting the (certainly believed!) hypothesis 1 and 2 below, we can prove that $P_{\mathbb{Q},\{\infty,l,p\},p}$ holds for any prime numbers $l \neq p$, which is much stronger than corollary 2. We will end the section by discussing $P_{\mathbb{Q},\{\infty,p\},p}$ for a prime number p, which is the most interesting case in some sense, as its truth would imply all the results of this paper.

4.1. Case $S = \{\infty, l, p\}$, $p \neq l$ **(proof of Theorem 2).** In this section, we give one way (certainly among many others!) to deduce $P_{\mathbb{Q},\{\infty,l,p\},p}$ from some expected properties of automorphic forms for the symplectic groups $\mathrm{GSp}_{2n}/\mathbb{Q}$ for all $n \geq 2$. The proof is very similar to that of Theorem 1, so that we will be rather sketchy on some points. Let $\mathbb{Q}_p^{ab} \subset \overline{\mathbb{Q}_p}$ be the maximal abelian extension of $\mathbb{Q}_p$, note that $\mathbb{Q}_p^{ab} \subset \mathbb{Q}_p^{ur}.\mathbb{Q}_{\{\infty,p\}}$.

Proof. (of Theorem 2 of the introduction) Let $K/\mathbb{Q}_p$ be a finite Galois extension whose Galois group admits an injective irreducible representation $\rho : \mathrm{Gal}(K/\mathbb{Q}_p) \to \mathrm{GL}_n(\mathbb{C})$, we want to prove that $K \subset \mathbb{Q}_p^{ur}.\mathbb{Q}_{\{\infty,p\}}$. The representation ρ extends to an irreducible L-parameter

$$\psi : W_{\mathbb{Q}_p} \to \mathrm{GL}_n(\mathbb{C}).$$

Note that $\mathbb{Q}_p^{ab} \subset \mathbb{Q}_p^{ur}.\mathbb{Q}_{\{\infty,p\}}$ by local class field theory, hence we can replace ψ by any of its twists ψ' by a continuous character $W_{\mathbb{Q}_p} \to \mathbb{C}^*$. We claim that for some well chosen character, the dual of ψ' is not isomorphic to any unramified twist of ψ'. Indeed, as $\psi_{|I_{\mathbb{Q}_p}}$ has a finite image, we can find a $g \in I_{\mathbb{Q}_p} \cap \mathrm{Ker}(\psi)$ acting on $\mathbb{Q}_p(\mu_{p^\infty})$ as an element of infinite order. We can then find a finite order character χ of $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$ such that $\chi^2(g) \neq 1$. Hence $\psi' := \psi \otimes \chi$ does the trick as $\mathrm{tr}(\psi'(g)) = n\chi(g) \neq n\chi(g)^{-1} = \mathrm{tr}(\psi'^*(g))$. We can therefore assume that ψ^* is not isomorphic to any unramified twist of ψ.

Recall now that $M := \mathrm{GL}_n \times \mathrm{GL}_1$ is a Levi factor of the maximal parabolic subgroup of GSp_{2n} stabilizing a maximal isotropic subspace (the so-called *Siegel parabolic*). As the root datum of $\mathrm{GL}_n \times \mathrm{GL}_1$ is selfdual, $\mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_1(\mathbb{C})$ is also a Levi subgroup of $\widehat{\mathrm{GSp}_{2n}} = \mathrm{GSpin}_{2n+1}(\mathbb{C})$. For any unramified characters $\alpha, \beta : W_{\mathbb{Q}_p} \to \mathbb{C}^*$, we can thus consider the L-parameter

$$\psi_{\alpha,\beta} := \psi \otimes \alpha \times \beta : \quad W_{\mathbb{Q}_p} \to \mathrm{GSpin}_{2n+1}(\mathbb{C}),$$

deduced by functoriality. As ψ^* is not isomorphic to any unramified twist of ψ, the centralizer of any $\psi_{\alpha,\beta}$ in $\mathrm{GSpin}_{2n+1}(\mathbb{C})$ is reduced to the center $\mathbb{C}^* \times \mathbb{C}^*$ of $\mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_1(\mathbb{C})$ (it obviously contains it). Indeed, if an element $\gamma \in \mathrm{GSpin}_{2n+1}(\mathbb{C})$ satisfies

$\gamma\psi_{\alpha,\beta}(g)\gamma^{-1} = \psi_{\alpha,\beta}(g)$ for all $g \in W_{\mathbb{Q}_p}$, its image $\overline{\gamma}$ in $\mathrm{PGSpin}_{2n+1}(\mathbb{C}) = \mathrm{SO}_{2n+1}(\mathbb{C})$ self-intertwines

$$(\psi \otimes \alpha) \oplus (\psi \otimes \alpha)^* \oplus 1,$$

and we conclude because this semi-simple representation is multiplicity free by assumption on ψ. As a consequence, we expect that the hypothetical L-packet of $\mathrm{GSp}_{2n}(\mathbb{Q}_p)$ associated to any $\psi_{\alpha,\beta}$ have only one element. Namely, if $\pi_{\alpha,\beta}$ denotes the supercuspidal representation of $M = \mathrm{GL}_n(\mathbb{Q}_p) \times \mathrm{GL}_1(\mathbb{Q}_p)$ attached to $\psi \otimes \alpha \times \beta$ by Harris & Taylor, then the L-packet of $\psi_{\alpha,\beta}$ should consist of the full [8] normalized parabolic induction from M to $\mathrm{GSp}_{2n}(\mathbb{Q}_p)$ of $\pi_{\alpha,\beta}$. We come now to our first hypothesis:

HYPOTHESIS 1: For all supercuspidal representations π of $\mathrm{GL}_n(\mathbb{Q}_p)$ with no selfdual unramified twist, the inertial equivalence class $[M, \pi \times 1]_{\mathrm{GSp}_{2n}(\mathbb{Q}_p)}$ admits a type in the sense of [BK].

By the above hypothesis applied to $\pi \times 1$, and by Proposition 1, we can find a discrete, irreducible, automorphic representation Π of $\mathrm{GSp}_{2n}(\mathbb{A}_{\mathbb{Q}})$ such that Π_l is unramified if $l \notin \{\infty, p\}$, $\Pi_p \in [M, \pi \times 1]_{\mathrm{GSp}_{2n}(\mathbb{Q}_p)}$, and Π_∞ belongs to the holomorphic discrete series. Moreover, by remark 3.4, we may assume that the parameter λ of Π_∞ is far from the walls, hence Π should conjecturally belong to a tempered A-packet. Moreover, by the analysis preceding Hypothesis 1, the L-parameter Ψ_p of Π_p should have the form $\psi_{\alpha,\beta}$ for some α, β. By replacing Π by an unramified twist if necessary, we may assume that Π_∞ is algebraic. Let us fix a complex injective representation $r : \mathrm{GSpin}_{2n+1}(\mathbb{C}) \to \mathrm{GL}_{n_r}(\mathbb{C})$, and embeddings ι_l, ι_∞ as in §2.1. The reasoning above give credits to the following:

HYPOTHESIS 2: For some r as above, there exists a continuous representation

$$R : \mathrm{Gal}(\mathbb{Q}_{\{\infty,p,l\}}/\mathbb{Q}) \to \mathrm{GL}_{n_r}(\overline{\mathbb{Q}_l}),$$

such that the representation $\iota_\infty . \iota_l^{-1} . R_{|I_{\mathbb{Q}_p}} \simeq r \circ \Psi_{p|I_{\mathbb{Q}_p}}$.

Of course, following Langlands, the hypothetical Galois representation R associated to the automorphic representation Π, $\iota_\infty . \iota_l^{-1}$ and r, should satisfy this hypothesis. Assuming the above hypothesis, we obtain by the same reasoning as in the proof of Lemma 3 (ii) that $\mathbb{Q}_p^{ur} . \mathbb{Q}_{\{\infty,p,l\}} \supset K$, which concludes the proof. $\square$

Remarks: (i) Bushnell and Kutzko show in [BK] §8 that Hypothesis 1 would follow from the existence of $\mathrm{GSp}_{2n}(\mathbb{Q}_p)$-covers for the types they have constructed for the supercuspidal representations of $\mathrm{GL}_n(\mathbb{Q}_p)$. Some of theses covers have already been constructed by Blondel in [Bl], but unfortunately only when π has a selfdual unramified twist.

(ii) Hypothesis 2 is known for $n = 1$ (Carayol, Deligne, Langlands).

---

[8]This induced representation is known to be irreducible, see [R].

4.2. Case $l = p$**.** We would like to apply the same reasoning as in §4.1 to prove property $P_{\mathbb{Q}, \{\infty, p\}, p}$, by choosing a K as above and using Π, and using this time the hypothetical p-adic Galois representation R attached to Π. The proof of §4.1 applies verbatim until the statement of hypothesis 2, whose correct form becomes (Π and r are chosen as above):

HYPOTHESIS 2': There exists a continuous representation

$$R : \mathrm{Gal}(\mathbb{Q}_{\{\infty, p\}}/\mathbb{Q}) \to \mathrm{GL}_{n_r}(\overline{\mathbb{Q}_p}),$$

which is potentially semistable at p, and such that $\iota_\infty . \iota_p^{-1}.(R_{|\mathrm{G}_{\mathbb{Q}_p}})^W_{|I_{\mathbb{Q}_p}} \simeq r \circ \Psi_{p|I_{\mathbb{Q}_p}}$.

In the above statement, ρ^W is the representation of $\mathrm{W}_{\mathbb{Q}_p}$ attached by Fontaine to a p-adic *pst* (*i.e.* potentially semistable) representation ρ of $\mathrm{G}_{\mathbb{Q}_p}$ (in fact, in the special situation above, the monodromy operator N is automatically 0). Let $\rho := R_{|\mathrm{G}_{\mathbb{Q}_p}}$. The last step to conclude would be to establish a link between $F_1 := \mathbb{Q}_p^{ur}(\rho_{|I_{\mathbb{Q}_p}})$ (which is also $\mathbb{Q}_p^{ur}.\varphi(\mathbb{Q}_{\{\infty, p\}}(R)))$ and $F_2 := \mathbb{Q}_p^{ur}(\rho^W_{|I_{\mathbb{Q}_p}})$ (which is $\mathbb{Q}_p^{ur}.K$ in the notation of the proof of 4.1). Note that $F_1/\mathbb{Q}_p^{ur}$ (resp. F_2) is in general infinite (resp. always finite), it is the smallest algebraic extension (resp. finite Galois extension) of $\mathbb{Q}_p^{ur}$ over which ρ becomes trivial (resp. semistable, even crystalline here). It turns out that, it is not always the case that $F_2 \subset F_1$, which prevents us from concluding as before. We discuss this point in the following subsection.

Remark: The "modular form case" of hypothesis 2' (i.e. $n = 1$) is known by the work of Carayol, Deligne, Langlands and Takeshi Saito (see the main theorem in [S]). In general, hypothesis 2' would follow from hypothesis 2, the construction of the pure motive attached to Π and the conjectured *independence of l* of the semisimplified Weil-Deligne representation associated to the l-adic cohomology of a given proper smooth scheme X over $\mathbb{Q}_p$ (see [F] §2.4.3).

4.3. Kernels of *pst* representations. Let $l \neq p$ be a prime number, we recall first the l-adic situation. Let $M/\mathbb{Q}_p$ be a local field. We fix a $\varphi \in \mathrm{W}_M$ lifting a geometric Frobenius element, and a non-zero continuous homomorphism $t_l : I_M \to \mathbb{Q}_l$. Let $\rho : \mathrm{G}_M \to \mathrm{GL}_d(\overline{\mathbb{Q}_l})$ be a continuous representation. By Grothendieck's l-adic monodromy theorem, there exists a unique nilpotent matrix $N \in \mathrm{M}_d(\overline{\mathbb{Q}_l})$ such that ρ and the representation of I_M defined by $\gamma \to \exp(t_l(\gamma)N)$ coincide on some open subgroup of I_M. The Weil-Deligne representation attached to ρ is then the isomorphism class of the pair (ρ^W, N) where $\rho^W : \mathrm{W}_M \to \mathrm{GL}_d(\overline{\mathbb{Q}_l})$ is defined by (see [T] §4.2, [F])

$$\rho^W(\varphi^n \gamma) := \rho(\varphi^n \gamma) \exp(-t_l(\gamma)N), \quad \gamma \in I_M, \ n \in \mathbb{Z}.$$

Note that $\rho^W_{|I_M}$ has finite image, hence consists of semisimple elements. In particular, $\mathrm{Ker}(\rho_{|I_M}) \subset \mathrm{Ker}(\rho^W_{|I_M})$, that is

(5) $$M^{ur}(\rho^W_{|I_M}) \subset M^{ur}(\rho_{|I_M}).$$

Obviously, these inclusions are equality if and only if $N = 0$, that is $\rho = \rho^W$. We used implicitly this trivial fact in the proof of Lemma 3 (ii).

Assume now that $l = p$, and that $\rho : \mathrm{G}_M \to \mathrm{GL}(V)$ is a continuous representation on a finite dimensional $\overline{\mathbb{Q}_p}$-vector space V, which is potentially semistable in the sense of Fontaine [F]. It means that $\mathrm{D}_{\mathrm{pst}}(V) := \bigcup_{L/K \text{finite}} (V \otimes_{\mathbb{Q}_p} B_{st})^{\mathrm{G}_L}$ is free of rank $\dim_{\overline{\mathbb{Q}_p}}(V)$ over $\overline{\mathbb{Q}_p} \otimes_{\mathbb{Q}_p} \mathbb{Q}_p^{nr}$, where B_{st} is the usual Fontaine ring. Fontaine defines then a representation, say ρ^W, of W_M on $\mathrm{D}_{\mathrm{pst}}(V)$, whose restriction to I_M is the obvious one. However, the analogue of the inclusion (5) is not always satisfied in this setting[9]. We are grateful to P. Colmez and T. Saito for explaining us the following example:

Example: Let $M := \mathbb{Q}_p$ and $K \subset \overline{\mathbb{Q}_p}$ be a finite extension of $\mathbb{Q}_p$. Let $\omega : \mathrm{G}_K \to \overline{\mathbb{Q}_p}^*$ be a Lubin-Tate character of K, and $\psi : \mathrm{G}_K \to \overline{\mathbb{Q}_p}^*$ be a continuous character of finite order on I_K, and $\chi := \omega\psi$. It is well known that ω is crystalline, hence χ is *pst*, and the representation $\chi^W_{|I_K}$ on $\mathrm{D}_{\mathrm{pst}}(\chi)$ is $\psi_{|I_K}$. Let $\rho := \mathrm{Ind}_{\mathrm{G}_K}^{\mathrm{G}_{\mathbb{Q}_p}} \chi$. An easy computation shows that $\mathrm{D}_{\mathrm{pst}}(\rho) = \mathrm{Ind}_{\mathrm{W}_K}^{\mathrm{W}_{\mathbb{Q}_p}} \mathrm{D}_{\mathrm{pst}}(\chi)$, hence ρ is *pst* and $\rho^W = \mathrm{Ind}_{\mathrm{W}_K}^{\mathrm{W}_{\mathbb{Q}_p}} \chi^W$.

Let us assume from now that $K/\mathbb{Q}_p$ is Galois to simplify. Let $\mathrm{rec} : \mathcal{O}_K^* \to \mathrm{G}_K^{ab}$ be the reciprocity map of local classfield theory, recall that $\omega \circ \mathrm{rec}$ is the natural map $\mathcal{O}_K^* \to \overline{\mathbb{Q}_p}^*$ induced by some field embedding $K \to \overline{\mathbb{Q}_p}$. We choose now ψ such that $\psi \circ \mathrm{rec}$ is trivial on the pro-p-Sylow of $\mathcal{O}_K^*$, and coincides with $(\omega \circ \mathrm{rec})^{-1}$ on its p'-part. Then, $F_1 := \mathbb{Q}_p^{ur}(\rho^W)$ is the maximal, tamely ramified, abelian extension of K, and is linearly disjoint with $F_2 := \mathbb{Q}_p^{ur}(\rho)$ over K^{ur}. In particular, when $K/\mathbb{Q}_p$ is unramified of degree > 1, it gives examples of p-adic *pst* representations ρ of $\mathrm{G}_{\mathbb{Q}_p}$ such that $\mathbb{Q}_p^{ab}(\rho^W)$ is not included in $\mathbb{Q}_p^{ab}(\rho)$.

Remarks: (i) We do not know if there exists a strict subfield L of $\overline{\mathbb{Q}_p}$ such that the inclusion (5) holds over L for any ρ, or if (5) (or some variant) holds under a mild hypothesis on ρ. For our aim, the only controls we seem to have on ρ are $\rho^W_{|I_M}$ and some information on its set of Hodge-Tate weights. What we do not control at all is the filtration data of $\mathrm{D}_{\mathrm{pst}}(\rho)$. In this direction, we may hope that the p-adic Langlands philosophy initiated by Breuil will allow, in the future, to use the Galois representations attached to p-adic automorphic forms, whose properties at p are less restricted.

(ii) Assuming the extension of T. Saito's theorem [S] to Harris-Taylor's automorphic forms, and using corollary 3, a solution of the above problem of kernels would imply property $P_{E, \{\infty, u, u'\}, u}$ where $E/\mathbb{Q}$ is a quadratic imaginary field and $p = uu'$ a prime number which splits in E. We mention this as the hypothesis we made in §4.1 still seems to be out of reach (especially hypothesis 2).

---

[9]It is however obviously satisfied when $\rho_{|I_M}$ has finite image, as $\rho^W = \rho_{|W_M}$ in this case.

References

[AT]   E. Artin & J. Tate   *Class field theory*
         W. A. Benjamin (1968).

[Bl]   C. Blondel Sp($2N$)-*covers for self-contragredient supercuspidal representations of* GL(N).
         Ann. Sci. École Norm. Sup. (4) **37**, no. 4, p. 533-558 (2004)

[B1]   A. Borel   *Introduction aux groupes arithmétiques*
         Pub. Inst. Math. Strasbourg, Herman (1969)

[B2]   A. Borel   *Automorphic forms on* $\mathrm{SL}_2(\mathbb{R})$
         Cambridge univ. Press **130** (1997)

[BC]   A. Borel & W. Casselman *Automorphic forms, representations, and L-functions.*
         Proc. symp. in pure math. **33**, Corvallis, A.M.S.

[BW]   A. Borel & N. Wallach   *Continuous cohomology, discrete subgroups, and representations
         of reductive groups.*   Annals of math. studies, Princeton univ. press **94** (1980)

[BK]   C. Bushnell & P. Kutzko   *Smooth representations of reductive p-adic groups: structure
         theory via types.*   Proc. Lon. Math. Soc. (3) **77**, p. 582-634 (1998)

[Ca1]   *Variétés analytiques complexes et fonctions automorphes*
         Séminaire H. Cartan, tome 6, E.N.S. Paris (1953/54)

[Ca2]   *Fonctions automorphes.* Séminaire H. Cartan, tome 10, E.N.S. Paris (1957/58)

[C]   L.Clozel *Représentations galoisiennes associées aux représentations automorphes autoduales
         de GL(n).*   Publications math. I.H.E.S. **73**, p. 97-145 (1991)

[CL]   L.Clozel & J.-P. Labesse *Changement de base pour les représentations cohomologiques de
         certains groupes unitaires.*   Appendice à *Cohomologie, stabilisation et changement de base*, SMF,
         Astérisque (1998)

[F]   J.-M. Fontaine *Représentations l-adiques potentiellement semi-stables*
         Periodes p-adiques, exposé VIII, SMF, Astérisque **223** (1994)

[HL]   M. Harris & J.-P. Labesse *Conditional base change for unitary groups*
         To appear in Asian J. Math. (special issue in memory of A. Borel).

[HT]   M. Harris & R.Taylor *The geometry and cohomology of some simple Shimura varieties*
         PUP Annals of Math. Studies **151** (2001)

[K]   A. Knapp   *Representation theory of semisimple groups.*
         Princeton university press (1986)

[La]   J.-P. Labesse   *Cohomologie, stabilisation et changement de base*
         Astérisque **257**, SMF (1998)

[Lg]   S. Lang   *Algebraic number theory*
         Springer GTM **110**

[M]   J. Milne   *Arithmetic duality theorems*
         Perspectives in Mathematics **1**, Academic Press (1986)

[MU]   V.G. Mukhamedov   *Local extensions associated with the l-extensions of number fields with
         restricted ramification.* Zametki 35 (1984) (Russian), Math. Notes **35** No. 3-4 (English transl.)

[NSW]   J.Neukirch, A.Schmidt & K.Wingberg *Cohomology of number fields*
         Grundlehren des mathematischen Wissenschaften 323.

[R]   A. Roche   *Parabolic induction and the Bernstein decomposition*
         Compositio math. **234**, no. 2, p. 113-133 (2002)

[S]   T. Saito *Modular forms and p-adic Hodge theory*
         Invent. Math. **129**, p. 607-620 (1997).

[T]   J.Tate *Number theoretic background*, in *Automorphic forms, representations, and L-functions*,
         P.S.P.M. **33** part 2, Corvallis.

CHENEVIER Gaëtan,

Institut Galilée L.A.G.A., Université Paris 13,
99 Av. J-B. Clément, 93430 Villetaneuse, France,
E-mail: gaetan.chenevier@normalesup.org