ON NUMBER FIELDS WITH GIVEN RAMIFICATION

GAËTAN CHENEVIER

1. Introduction

Let E be a number field and S be 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 :

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

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

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

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

(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 simple argument using Krasner's lemma and a weak approximation theorem shows that $(P_{S,u})$ is true if S contains almost all the places of E. Moreover, the example of $E = \mathbb{Q}$ and $S = \{\infty\}$ shows that $P_{S,u}$ is not always satisfied. However, the author doesn't know whether there was a single example of triple (E, S, u) *with S and u finite*, such that $(P_{S,u})$ was known to be true before this paper. In what follows, we shall not attempt to discuss any necessary conditions on (E, S, u) for $(P_{S,u})$ to be true, but we will look for sufficient ones. A trivial remark is that if $u \in S' \subset S$, $(P_{S',u}) \Rightarrow (P_{S,u})$, hence we want to take S as small as possible. The best result we can prove is the following :

Theorem : *Assume that E/F is a CM field split above a finite place v of F and write $v = uu'$ in 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 $(P_{S,u})$ is true.*

This holds 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 : *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 $(P_{S,p})$ holds for $E = \mathbb{Q}$.*

Explicit examples are given by

$$(p, N) \in \{(2, 7), (2, 3.5), (3, 2^3), (3, 2^2.5), (3, 11), (5, 2^2), (5, 11), (7, 3), (11, 2^3)\}$$

The theorem above is related to some results of Kuz'min and V.G. Mukhamedov ([MU], [NSW] chapter X, §6, thm. 10.6.4 and the last exercise) concerning p-extensions. For example, the following result is proved in [MU]. Let p be a prime number and let E/F be a CM field 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 our results from these ones, and our proof is very different. It seems, moreover, that we cannot deduce the above theorem 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.

Let us describe the strategy of the proof. 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[1]. 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 & 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. Thus, we first show that we can construct cohomological automorphic forms for these groups (or related ones) which are unramified outside S and of a given ramification type at u (§2.1, §2.2). Then, applying Harris & Taylor's theorem [HT], we get number fields with the required local properties (§2.3). The local Langlands correspondence shows then that we can produce in this way *a lot of them*, using unitary groups *of all ranks*. Two little subtleties arise at this point. First, we have few control, of course, on the Weil numbers in the above constructions, i.e. on the *unramified part* of the local properties at u of the number fields constructed. The second one is that the automorphic representations we consider must be supercuspidal at u so that we may apply to them the results of Harris & Taylor. However, a simple trick (§2.4) allows us to show that we produced sufficiently many number fields to conclude.

In fact, assuming some standard conjectures in the theory of automorphic forms, we could even get stronger results, as will be explained in a forthcoming sequel of this paper. Ultimately, we believe that $P_{\{\infty,p\},p}$ is true for $E = \mathbb{Q}$. Although it would be natural to hope for a proof of such a statement (or of our theorem) without mentioning any automorphic form, we have no idea how to do it!

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 an algebraic closure of K. If K is a

[1]For instance, $X_1(l^n)$ has good reduction outside l, and its genus goes to ∞ with n. However, it only constructs number fields of GL_2-type in some sense, hence they cannot exhaust $\overline{\mathbb{Q}_l}$.

finite extension of $\mathbb{Q}_p$, we denote by $K^{ur} \subset \overline{K}$ its maximal unramified extension. 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.

2. Proof

Let E/F be a CM field as in the statement of the theorem. 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.

2.1. **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's 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. □

2.2. **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) $\Pi_v \simeq \pi \otimes \psi \cdot \det$ *for some unramified character* $\psi : F_v^* \to \mathbb{C}^*$*,*

(c) If x *is a real place,* Π_x *is cohomological.*

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 finite and 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 [L, §3.6] (when x does not ramify in E, the hyperspecial compact subgroups of $H(F_x)$ are very special). 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. Moreover, Π_v is a 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 $H(F_v)$. The condition (c) is automatic since H_∞ is compact. □

2.3. **Construction of S-unramified number fields.** 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

$$G_{E,S} := \mathrm{Gal}(E_S/E), \ \ G_v := \mathrm{Gal}(\overline{F_v}/F_v).$$

Attached to φ is a group homomorphism $G_v \to G_{E,S}$. We will also denote by $I \subset G_v$ the inertia subgroup of G_v. We keep the assumption of §2.2, 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 n-dimensional, complex representation ψ_π of the Weil group of F_v, whose restriction to I has finite image. Let $F_v^{ur}(\pi) \subset \overline{F_v}$ be the finite extension of F_v^{ur} which is fixed by $\mathrm{Ker}((\psi_\pi)_{|I}) \subset G_v$. Recall that l is prime to v.

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

$$R : G_{E,S} \to \mathrm{GL_n}(\overline{\mathbb{Q}_l}),$$

such that $R_{|G_v}$ corresponds to $\Pi_v \cdot |\det|^{(n-1)/2}$ 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 $H \to H' := \mathrm{Res}_{E/F}(H \times_E F)$. 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 $\Pi'_x = BC(\Pi_x)$ for each place $x \neq w$ of F. It applies because Π_∞ is cohomological, and because H is attached to a division algebra, as is $H(F_v)$. 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 [L, §3.6, prop. 3.6.4][2]. In 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[3] 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*, which proves (i).

We check the second assertion. Let us denote by $E_S(R)$ (resp. $F_v(R)$) the subfield of E_S (resp. $\overline{F_v}$) fixed by $\mathrm{Ker}(R)$ (resp. $\mathrm{Ker}(R_{|G_v})$). As $\mathrm{Gal}(\overline{F_v}/(F_v.\varphi(E_S(R)))) = \mathrm{Ker}(R_{|G_v})$, we have $F_v.\varphi(E_S(R)) = F_v(R)$ by Galois theory. By (i), $F_v^{ur}.F_v(R)$ is exactly the finite extension of F_v^{ur} fixed by the kernel of $(\psi_{\Pi_v})_{|I}$. But by lemma 2, π and $\Pi_v \cdot |\det|^{(n-1)/2}$ only differ by an unramified twist, hence $\psi_{\Pi_v \cdot |\det|^{(n-1)/2}}$ and ψ_π are equal when restricted to I. $\square$

2.4. **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) 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 $M' := L \cap M^{ur}$ and consider the subgroups $I = \mathrm{Gal}(\overline{M}/M^{ur})$ and $H := \mathrm{Gal}(\overline{M}/L)$ of $\Gamma := \mathrm{Gal}(\overline{M}/M')$, we have $IH = \Gamma$. By assumption, H is normal in Γ, hence $H \cap I = \{1\}$ and Γ is the direct product $I \times H$. In particular, $H \simeq \mathrm{Gal}(M^{ur}/M') \subset \widehat{\mathbb{Z}}$ is abelian. As a consequence, all tamely ramified extensions of M containing M' are Galois abelian over M'. Let ω be a uniformizer of M, q be the cardinal of the residue field of $\mathcal{O}_M$, and let $m \geq 1$ be an integer. We apply the previous remark to a splitting field M'_m of $Q_m := X^{q^m-1} - \omega$ over M', which is therefore Galois over M'. As ω is a uniformizer of M', $Q_m \in M'[X]$ is irreducible (Eisenstein criteria). In particular, for each $m \geq 1$, $X^{q^m-1} - 1$ has all its roots in M'_m, and even in M' as M'_m/M' is totally ramified. So $M^{ur} \subset M' \subset L$, and $L = \overline{M}$.

[2]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 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 the corollary.

[3]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.

We now show (ii). Let K/M be any finite Galois extension, $\rho_1, \dots, \rho_t$ 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 $K = K_1 \dots K_t$, and $K \subset L$. □

Let us finish the proof of the theorem. Let K/F_v be a Galois local field 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 (ii) 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 our theorem. □

ACKNOWLEDGMENTS :

The author thanks J. Bellaïche, Y. Benoist, L. Clozel, P. Colmez, L. Fargues, A. Genestier, M. Harris, G. Henniart, J.-P. Labesse, and K. Wingberg, for their remarks or helpful discussions.

Références

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

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

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

[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)

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

[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.

CHENEVIER Gaëtan,
École normale supérieure, DMA,
45, rue d'Ulm,
75005 Paris, France.