A MILD TCHEBOTAREV THEOREM FOR GL(n)

DINAKAR RAMAKRISHNAN

In memory of Steve Rallis

Introduction

As it is well known, the Tchebotarev density theorem implies that two irreducible ℓ-adic representations ρ_ℓ, ρ'_ℓ of the absolute Galois group of a number field K are isomorphic if the corresponding characteristic polynomials of Frobenius elements agree on a set S of primes of density 1. It is then natural to ask, in view of the Langlands conjectures, whether an analogous assertion holds for cuspidal automorphic representations of $\mathrm{GL}_n(\mathbb{A}_K)$. The object of this Note is to establish such an automorphic analogue for a simple, but useful, class of S of density 1. To be precise, we prove the following:

Theorem A *Let K/k be a cyclic extension of number fields of degree a prime p, and let $\Sigma^1_{K/k}$ denote the set of primes v of K which are of degree 1 over k. Suppose π, π' are cusp forms on $GL(n)/K$ such that $\pi_v \simeq \pi'_v$, for all but a finite number of v in $\Sigma^1_{K/k}$. Then π, π' are twist equivalent. More precisely, they have isomorphic base changes over the cyclotomic extension $K(\zeta)$, where ζ is a non-trivial p-th root of unity.*

We refer to the book [1] for facts on solvable base change for GL(n) due to Arthur and Clozel.

When we say that π, π' are twist equivalent, we mean $\pi' \simeq \pi \otimes \chi$ for a finite order character χ of (the idele classes of) K. In particular, if n is relatively prime to $p-1$, or if the conductors of π, π' are prime to p, we may conclude even that π, π' are isomorphic (over K). When $p = 2$, we thus get the following:

Corollary B *Let K/k be a quadratic extension of number fields. Then any cuspidal automorphic representation π of $GL_n(\mathbb{A}_K)$ is determined (up to isomorphism) by its components π_v for all (but a finite number of) places v of degree 1 over k.*

2000 *Mathematics Subject Classification.* 11F70; 11F80; 22E55.

Partly supported by the NSF grant DMS-0701089.

Clearly, Theorem A refines the strong multiplicity one theorem, which gives the desired global isomorphism if $\pi_v \simeq \pi'_v$ for all but a *finite* number of v. ([4]). For GL(2), there is a stronger result known, requiring the isomorphism $\pi_v \simeq \pi'_v$ only for a set S' of v of density $> 7/8$ ([8]). For GL(n) with $n > 2$, we conjectured elsewhere that such a stronger result should hold with $7/8$ replaced by $1 - 1/2n^2$, which is a theorem for π attached to an ℓ-adic representation ρ_ℓ by an elegant result of Rajan ([6]). We are *far* from such a precise result for those cusp forms π on GL(n), $n \geq 3$, which are not known to be associated to such a ρ_ℓ.

Given a finite cyclic extension K/k, if G, resp. $\tilde{G}$, is a reductive group over k, resp. K, such that $\tilde{G} = G \times_k K$, let us say that a cuspidal automorphic representation π of $G(\mathbb{A}_k)$ admits a *soft base change* to K if there is an automorphic representation Π of $\tilde{G}(\mathbb{A}_K)$ such that for all but a finite number of primes v in $\Sigma^1_{K/k}$, we have $\Pi_v \simeq \pi_u$, where u is the prime of k below v. When $\tilde{G}$ is GL$(n)/K$, Theorem A says that a soft base change Π is unique up to twisting by a character of K which is trivial when pulled back by norm to the p-cyclotomic extension of K; in particular, Π is determined up to isomorphism for $p = 2$ when cuspidal. An initial impetus for it came from a question asked independently by J. Getz and D. Whitehouse. Now Theorem A has been used (for quadratic extensions) by B. Feigon, K. Martin and D. Whitehouse in their paper ([2]) on the periods and non-vanishing of L-functions of GL($2n$), and in Wei Zhang's work on the Gross-Prasad conjecture ([10]).

Now a few words about the proof of Theorem A. A well known, basic theorem of Luo, Rudnick and Sarnak ([5]), which is of importance to us, says that for any cusp form π on GL$(n)/K$, the coefficient a_v of π at any unramified v satisfies the bound $|a_v| < (Nv)^{1/2-1/(n^2+1)}$. (What is essential for us is that a_v is bounded in absolute value by $(Nv)^{1/2-t_n}$ for a fixed positive number t_n independent of v, not the exact shape of t_n.) As it has been noted and used already by Rajan ([7]), feeding this into the known analytic framework, it suffices, under our hypotheses, to prove that for all but a finite number of v whose degree lies in $[2, (n^2+1)/2]$, π_v and π'_v are isomorphic. We cannot achieve this directly, but can show, using some Kummer theory, that it holds for the base changes π_L, π'_L to a carefully chosen solvable extension L of $K' = K(\zeta)$, which will be a compositum (over K) of a finite number of disjoint p^r-extensions $L^{(1)}, L^{(2)}, \dots$ with $2p^r > n^2 + 1$; each $L^{(j)}$ will be a nested chain of cyclic p^2-extensions (see section 4). From this data we prove by descent that $\pi_{K'}$ and $\pi'_{K'}$ are isomorphic. There is an added subtlety if $\pi_{K'}$ or $\pi'_{K'}$ is not cuspidal, and this forces us to work with isobaric sums of unitary cuspidal automorphic representations, which are analogues of semisimple Galois representations of pure weight. These steps together form the core of the argument. It should be stressed that since the basic analytic method is by now standard, given Rajan's work ([7]) making use of [5], what is new here is the use of base change to a suitable chain of p-power extensions to achieve the requisite isomorphism, followed by careful descent.

In another paper ([9]), we extend Theorem A non-trivially to the case of an arbitrary Galois extension K/k. The main idea there is quite different and replaces explicit Kummer theory with a fuller use of class field theory, in particular the Tate cohomology and duality. We hope that it is still of interest to have just the cyclic case published, at least because the proof is simpler and more accessible.

We thank the many people who have shown interest in this work over the past few years, especially to those who have used it and have encouraged, like K. Martin, to have it published. Thanks are also due to the NSF for partial support through the grants DMS-0701089 and DMS-1001916. This article is dedicated to the memory of Steve Rallis from whom this author learnt a lot in conversations over the years.

1. Basic Facts: A Review

Let F be a global field with adèle ring $\mathbb{A}_F$. Let Σ_F denote the set of all places of F. If $v \in \Sigma_F$ is finite, let q_v denote the cardinality of the residue field at v. For $n \geq 1$, let $A_0(n, F)$ denote the set of isomorphism classes of irreducible unitary, cuspidal automorphic representations of $\mathrm{GL}(n, \mathbb{A}_F)$. Every π representing a class in $A_0(n, F)$ is (isomorphic to) a tensor product $\otimes_v, \pi_v$, where v runs over all the places of F, such that each π_v is an irreducible generic representation of $\mathrm{GL}(n, F_v)$ and such that π_v is unramified at almost all v. The strong multiplicity one theorem ([4]) asserts that, for any *finite* subset S of Σ_F, π is determined up to isomorphism by the collection $\{\pi_v \,|\, v \notin S\}$.

For any irreducible, automorphic representation π of $GL(n, \mathbb{A}_F)$, let $L(s, \pi) = L(s, \pi_\infty)L(s, \pi_f)$ denote the associated *standard* $L-$function of π; it has an Euler product expansion

$$L(s, \pi) \,=\, \prod_v L(s, \pi_v),$$

convergent in a right-half plane. If v is a finite place where π_v is unramified, there is a corresponding semisimple (Langlands) conjugacy class $A_v(\pi)$ (or $A(\pi_v)$) in $\mathrm{GL}(n, \mathbb{C})$ such that

$$L(s, \pi_v) \,=\, \det(1 - A_v(\pi)T)^{-1}|_{T=q_v^{-s}}.$$

One may find a diagonal representative $\mathrm{diag}(\alpha_{1,v}(\pi), ..., \alpha_{n,v}(\pi))$ for $A_v(\pi)$, which is unique up to permutation of the diagonal entries. Let $[\alpha_{1,v}(\pi), ..., \alpha_{n,v}(\pi)]$ denote the resulting unordered $n-$tuple. One knows (by Godement-Jacquet) that for any non-trivial cuspidal representation π of $\mathrm{GL}(n, \mathbb{A}_F)$, $L(s, \pi)$ is entire.

By Langlands's theory of Eisenstein series, one has a sum operation $\boxplus$, called the isobaric sum ([4]): Given any $m-$tuple of cuspidal representations $\pi_1, ..., \pi_m$ of $\mathrm{GL}(n_1, \mathbb{A}_F), ..., \mathrm{GL}(n_m, \mathbb{A}_F)$ respectively, there exists an irreducible, automorphic representation $\pi_1 \boxplus ... \boxplus \pi_m$ of $\mathrm{GL}(n, \mathbb{A}_F)$, $n = n_1 + ... + n_m$, which is unique up to equivalence, such that for any finite set S of places,

$$L^S(s, \boxplus_{j=1}^m \pi_j) \,=\, \prod_{j=1}^m L^S(s, \pi_j).$$

Call such a (Langlands) sum $\pi \simeq \boxplus_{j=1}^m \pi_j$, with each π_j cuspidal, an *isobaric* representation.

Denote by $\mathcal{A}(n, F)$ the set, up to equivalence, of isobaric automorphic representations of $\mathrm{GL}_n(\mathbb{A}_F)$, and by $\mathcal{A}_u(n, F)$ the subset of isobaric sums of *unitary* cuspidal automorphic representations. If $\pi = \boxplus_{i=1}^m \pi_i$, resp. $\pi' = \boxplus_{j=1}^r \pi'_j$, is in $\mathcal{A}_u(n, F)$, resp. $\mathcal{A}_u(n', F)$, with π_i, π'_j unitary cuspidal, we will need to consider the associated Rankin-Selberg L-function

$$L(s, \pi \times \pi') \,=\, \prod_{i,j} L(s, \pi_i \times \pi'_j),$$

with

$$L(s, \pi_{i,v} \times \pi'_{j,v}) \,=\, \det(1 - A_v(\pi_i) \otimes A_v(\pi'_j)T)^{-1}|_{T=q_v^{-s}}.$$

If $L(s) = \prod_{v \in \sum_\infty \cup \sum_f} L_v(s)$ is any global L-function and Y a set of places of F, then we will denote by $L^Y(s)$ (resp. $L_Y(s)$) the product of $L_v(s)$ over all v outside Y (resp. in Y). We have the following basic result ([4]):

Theorem 1.1 (Jacquet–Piatetski-Shapiro–Shalika, Shahidi) *Let $\pi = \boxplus_{i=1}^m \pi_i$, $\pi' = \boxplus_{j=1}^r \pi'_j$ be in $\mathcal{A}_u(n, F)$, with π_i, π'_j unitary cuspidal. Suppose Y is a finite set of places of F containing the archimedean places such that π, π' are unramified outside Y. Then $L^S(s, \pi \times \overline{\pi}')$ has a pole* *at $s = 1$ iff for some (i, j), π_i is isomorphic to π'_j, in which case the pole of the factor $L(s, \pi_i \times \pi_j)$ is simple.*

Here $\overline{\pi}'$ denotes the complex conjugate representation of π', which, by unitarity, is the contragredient of π'.

The general Ramanujan conjecture predicts that for any $\pi \in \mathcal{A}_u(n, F)$, π_v is tempered at all v. In particular, if v is a finite place where π is unramified, the unordered n-tuple $\{\alpha_{1,v}(\pi), ..., \alpha_{n,v}(\pi)\}$ representing $A_v(\pi)$ should satisfy $|\alpha_{i,v}| = 1$ for every i. This is far from being proved, and the best known bound to date (for general n) is given by the following:

Theorem 1.2 (Luo–Rudnick–Sarnak [5]) *Let $\pi \in \mathcal{A}_u(n, F)$, and v a finite place where π is unramified, with $A_v(\pi) = \{\alpha_{1,v}(\pi), ..., \alpha_{n,v}(\pi)\}$. Then for every $j \leq n$, one has*

$$|\alpha_{j,v}| \, < \, q_v^{\frac{1}{2} - \frac{1}{n^2+1}}.$$

To be precise, Luo, Rudnick and Sarnak only address the case of cusp forms. But for $\pi \in \mathcal{A}_u(n, F)$, any $\alpha_j(\pi)$ must be associated to a cuspidal isobaric constituent π_i on $\mathrm{GL}(n_i)/F$ with $n_i \leq n$, and so the assertion above follows immediately from [5].

We will also need the following (weak) version of the base change theorem for GL(n):

Theorem 1.3 (Arthur–Clozel [1]) *Let M/F be a finite extension of number fields obtained as a succession of cyclic extensions. Then for every $\pi \in \mathcal{A}_u(n, F)$, there exists a corresponding $\pi_M \in \mathcal{A}_u(n, M)$ such that for every finite place v of F where π and M are unramified, and for all places w of M dividing v, we have*

$$A_v(\pi) = \{\alpha_{1,v}, ..., \alpha_{n,v}\} \implies A_w(\pi_M) = \{\alpha_{1,v}^{f_v}, ..., \alpha_{n,v}^{f_v}\},$$

where $f_v = [M_w : F_v]$.

A word of explanation may be helpful. In [1], it is proved that for every cuspidal π, the base change π_M is equivalent to an isobaric sum of unitary cuspidal automorphic representations; when M/F is cyclic of prime degree p, for example, π_M is either cuspidal or of the form $\boxplus_{j=0}^{p-1}(\eta \circ \tau^j)$, where τ is a generator of $\mathrm{Gal}(M/F)$. Since base change is additive relative to isobaric sums, it follows that for any π in $\mathcal{A}_u(n, F)$, π_M lies in $\mathcal{A}_u(n, M)$.

2. A Preliminary Step

Proposition 2.1 *Let F be a number field and $n \geq 1$ an integer. Suppose $\pi, \pi' \in \mathcal{A}_u(n, F)$ are such that for every positive integer $m \leq (n^2+1)/2$, and for all but a finite number of primes v of F of degree m, we have $\pi_v \simeq \pi'_v$. Then π and π' are isomorphic.*

This is essentially an immediate consequence of the bound of Luo-Rudnick-Sarnak, as it has already been noted (and used) by Rajan for cuspidal representations in [7]. For completeness, we quickly go through the relevant points of [8] to make it evident that they carry over, modulo the basic results cited in section 1 and induction on the number of cuspidal isobaric summands, from ($n = 2$; π, π' cuspidal) to (n arbitrary; π, π' isobaric sums of unitary cuspidal representations).

Proof. Denote by X the complement in Σ_F of the union of the archimedean places and the finite places where π or π' is ramified. Given any subset Y of X we set (as in [8]):

$$Z_Y(s) = L_Y(\bar{\pi} \times \pi, s) L_Y(\bar{\pi}' \times \pi', s) / L_Y(\bar{\pi} \times \pi', s) L_Y(\bar{\pi}' \times \pi, s). \tag{2.1}$$

Write

$$\pi = \boxplus_{i=1}^{\ell} m_i \pi_i, \;\; \pi' = \boxplus_{j=1}^{r} m'_j \pi'_j,$$

with $m_i, m'_j \in \mathbb{N}$, and π_i, π'_j unitary cuspidal, with $\pi_i \not\simeq \pi_a$ if $i \neq a$ and $\pi'_j \not\simeq \pi'_b$ if $j \neq b$.

Suppose $\pi_i \not\simeq \pi'_j$ for all i, j. Then, using Theorem 1.1, we see that $Z_X(s)$ is holomorphic at every $s \neq 1$, with

$$-\mathrm{ord}_{s=1} Z_X(s) \; = \; \mu + \mu', \tag{2.2 - a}$$

where

$$\mu = \sum_{i=1}^{\ell} m_i^2, \; \mu' = \sum_{j=1}^{r} {m'_j}^2. \tag{2.2 - b}$$

We note that one knows (see [3]) that $Z_Y(s)$ is of positive type, i.e., $\log Z_Y(s)$ is a Dirichlet series with non-negative coefficients.

As the subproduct of an absolutely convergent Euler product is absolutely convergent, we have the following

Lemma 2.3 *Let S denote the subset of X consisting of finite places v of degree $> \frac{n^2+1}{2}$. Then the incomplete Euler products $L_S(\bar{\pi} \times \pi, s)$ and $L_S(\bar{\pi} \times \pi', s) L_s(\bar{\pi}' \times \pi, s)$ converge absolutely in $\{s \in \mathbb{C} \mid \Re(s) > 1\}$.*

We may write

$$\log(L_Y(\bar\pi \otimes \pi, s)) = \sum_{m \geqq 1} c_m(Y) m^{-s} \tag{2.4}$$

for all subsets Y of X. Then $c_m(Y) = 0$ unless m is of the form Nv^r for some $v \in Y$ and $r \in \mathbb{N}$, and when m is of this form,

$$c_m(Y) = \sum_M \frac{1}{r} \sum_{1 \leqq i,j \leqq 2} \overline{\alpha_{i,v}^r} \alpha_{j,v}^r.$$

where M is the set of pairs $(v, r) \in Y \times \mathbb{N}$ such that $m = Nv^r$.

When $v \in S$, as $Nv > \frac{n^2+1}{2}$, the Luo-Rudnick-Sarnak bound (Theorem 1.2) implies that $\sum_{m \geqq 1} c_m(S) m^{-s}$ converges in $\{\Re(s) \geq 1\}$.

One has a similar statement for $\log(L_S(\bar\pi' \otimes \pi, s))$, $\log(L_S(\bar\pi' \otimes \pi, s))$, and $\log(L_S(\bar\pi' \otimes \pi', s))$. So we get the following

Lemma 2.5 *Let S be as in Lemma 2.3. As s goes to 1 from the right on the real line, we have*

$$\log Z_S(s) \;=\; o\left(\log \frac{1}{s-1}\right).$$

Now, since $\pi_v \simeq \pi'_v$ for all but a finite number of places of X outside S, we get, thanks to this Lemma, the following:

$$\log Z_X(s) \;=\; 4 \log L_X(\bar\pi \otimes \pi, s) + o\left(\log \frac{1}{s-1}\right) \;=\; 4 \log L_X(\bar\pi' \otimes \pi', s) + o\left(\log \frac{1}{s-1}\right). \tag{2.6}$$

Applying (2.2-b), we then get

$$\mu \;=\; \mu', \tag{2.7}$$

and

$$\log Z_X(s) \;=\; 4\mu \log \frac{1}{s-1} + o\left(\log \frac{1}{s-1}\right). \tag{2.8}$$

This contradicts (2.2-a) since $\mu = \mu' \geq 1$.

Thus we must have $\pi_i \simeq \pi'_j$ for *some* (i, j). If π or π' is cuspidal, then both will need to be cuspidal with $\pi = \pi_i \simeq \pi'_j = \pi'$, and so we are done in this case. We may assume that π, π' are non-cuspidal. Consider then the isobaric automorphic representations Π, Π' such that

$$\pi = \Pi \boxplus \pi_i, \; \pi' = \Pi' \boxplus \pi'_j.$$

The Π, Π' satisfy the hypotheses of Proposition 2.1, and we may find as before cuspidal isobaric summands π_k of Π and π'_m of Π' which are isomorphic. Continuing thus, by infinite decent, we arrive finally at the situation when one of the isobaric forms is cuspidal, which we have already taken care of. This proves Proposition 2.1.

□

3. Central character and unitarity

Suppose π, π' are cuspidal automorphic representations of $\mathrm{GL}_n(\mathbb{A}_F)$ of respective central characters ω, ω', such that $\pi_v \simeq \pi'_v$ for all but a finite number of primes v of F of degree 1. Then ω and ω' agree at all (but a finite number of) the degree one places v, which forces the global identity

$$\omega \, = \, \omega'. \tag{3.1}$$

In fact, by Hecke, this conclusion will result as soon as ω and ω' agree at a set of primes of density $> 1/2$.

It is a standard fact that, given a cuspidal π, there is a unique real number $t(\pi)$ such that $\pi \otimes |\cdot|^{-t(\pi)}$ is unitary; here $|\cdot|$ denotes the 1-dimensional representation $g \mapsto |\det(g)|$. Taking central characters, we see then that $\omega|\cdot|^{-nt(\pi)}$ is a unitary character. Thanks to (3.1), we will then get

$$t(\pi) \, = \, t(\pi'). \tag{3.2}$$

This allows us, in the proof of Theorem A, to assume that π, π' are unitary cuspidal automorphic representations.

4. Nested chains of cyclic p^2-extensions

Let p be a prime. We will call an extension L/F of number fields of degree p^r, for some $r \geq 2$, a *nested chain of cyclic* p^2*-extensions* if there is an increasing filtration of fields

$$F = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_{r-2} \subset L_{r-1} \subset L_r = L, \tag{4.1}$$

with

$$[L_j : L_{j-1}] = p, \ \forall\, j \in \{1, 2, \ldots, r\}, \tag{4.2}$$

and

$$L_j/L_{j-2} : \ \text{cyclic}, \ \forall\, j \in \{2, \ldots, r\}. \tag{4.3}$$

An easy example is given by a cyclic p^r extension, while a better example is the following. Let F contain μ_{p^2}. (As usual, we write μ_n for the group of n-th roots of unity in the algebraic closure of F.) Let α be an element of F which is not a p-th power. Put $\alpha_0 = \alpha$ and define α_j, for $j = 1, \ldots, r$, recursively by taking it to be a p-th root of α_{j-1}, and set $L_j = L_{j-1}(\alpha_j)$ and $L_0 = F$. Note that for $j \geq 2$, L_j/L_{j-2} is cyclic of order p^2 by Kummer theory, because $\alpha_j^{p^2} = \alpha_{j-2}$, and $\mu_{p^2} \subset L_{j-2}$, making all the conjugates of α_j over L_{j-2} lie in L_j. (For this example, it is in fact sufficient to have $\mu_p \subset F$ and $\mu_{p^2} \subset L_1$, as seen by the case $L_1 = F(\mu_{p^2})$.)

Lemma 4.4 *Let L/F be a nested chain of cyclic p^2-extensions (of number fields), with $[L : F] = p^r$ and filtration $\{L_j\}$ as above. Suppose v_0 is a finite place of F, unramified in L, which is inert in L_1. Then there exists, for each $j \geq 1$, a unique place v_j of L_j lying over v_{j-1}, so that $Nv_j = (Nv_{j-1})^p$. In particular, $Nv_r = (Nv_0)^{p^r}$.*

Proof. Let us first treat the case when $r = 2$, i.e., when L/F is cyclic of degree p^2. Since v_0 is inert in the intermediate field L_1, we need to check that v_0 does not split into p places in L. Suppose, to the contrary, that it does split that way. Let u be one of the p places of L above v_0. It must then be fixed by a subgroup H of $\mathrm{Gal}(L/F)$ of order p, with H giving the local Galois group $\mathrm{Gal}(L_u/F_{v_0})$. Since v_0 is inert in L_1 with divisor v_1, u necessarily has degree 1 over v_1, and so $H = \mathrm{Gal}(L_{1,v_1}/F_{v_0})$. If σ is a non-trivial element of H, then it acts non-trivially on L_{1,v_1}, and hence on L_1. On the other hand, since L/F is cyclic, it has a unique subgroup of order p, which forces H to be $\mathrm{Gal}(L/L_1)$, implying that σ acts trivially on L_1, yielding a contradiction. Put another way, if v_0 has degree p in L, then the corresponding Frobenius class Fr_{v_0} is given by an element σ of $\mathrm{Gal}(L/F)$ of order p, which has trivial image in the quotient by $H = \langle\sigma\rangle$, making v_0 split in the fixed field L^H of H. Clearly, L^H must be L_1 by the cyclicity of L/F. Either way, the case $r = 2$ is now settled.

Now let $r > 2$, and assume by induction that the Lemma holds for $r - 1$. So for every $j \leq r - 1$, there is a unique place v_j of L_j above v_{j-1} (of L_{j-1}). Now all we have to show is that v_{r-1} is inert in $L = L_r$. Since L_r/L_{r-2} is cyclic of order p^2, and since (by induction) the place v_{r-2} of L_{r-2} is inert in L_{r-1}, we conclude what we want by appealing again to the $r = 2$ scenario.

The assertion about the norm of v_r follows.

□

Lemma 4.5 *Let $L^{(i)}/F$, $1 \leq i \leq k$ be disjoint p^r-extensions. Suppose moreover that every $L^{(i)}$ is a nested chain of cyclic p^2-extensions with respective filtrations*

$$F = L_0^{(i)} \subset L_1^{(i)} \subset \cdots \subset L_r^{(i)} = L^{(i)}.$$

Let $v_0^{(i)}$, $1 \leq i \leq k$, be distinct primes of F, unramified in the compositum $M := L^{(1)}L^{(2)} \dots L^{(k)}$, such that each $v_0^{(i)}$ is inert in $L_1^{(i)}$. Then, if $\tilde{v}^{(i)}$ is a prime of M lying above $v_0^{(i)}$, we have

$$N\tilde{v}^{(i)} \geq (Nv_0^{(i)})^{p^r}, \ \forall i \leq k.$$

Proof. Fix any $i \leq k$. By Lemma 4.4, for each $j \geq 2$, there is a unique prime $v_j^{(i)}$, of $L_j^{(i)}$ lying above $v_{j-1}^{(i)}$. Then $\tilde{v}^{(i)}$ must lie above $v_r^{(i)}$ in the extension $M/L^{(i)}$. So

$$N\tilde{v}^{(i)} \geq Nv_r^{(i)}. \tag{4.6}$$

On the other hand, by Lemma 4.4, we have

$$Nv_r^{(i)} = (Nv_0^{(i)})^{p^r}. \tag{4.7}$$

The assertion of Lemma 4.5 now follows by combining (4.6) and (4.7). □

5. Isomorphism over suitable solvable extensions L/K, $L \supset E$

Let K/k be a cyclic p-extension. For $j \geq 1$, denote by $\Sigma_{K/k}^j$ the set of finite places v of K which are unramified over k and of degree j over k; of course this set is non-empty only for $j \in \{1, p\}$. Let π, π' be cuspidal automorphic representations of $\mathrm{GL}_n(\mathbb{A}_K)$ such that, as in the setup of Theorem A,

$$\pi_v \simeq \pi'_v, \ \text{for all but finitely many } v \in \Sigma_{K/k}^1. \tag{5.1}$$

As noted in section 3, the central characters of π and π' must be the same, and moreover, we may assume that π, π' are unitary.

If $p > (n^2+1)/2$, then Theorem A follows immediately from Proposition 2.1. In general, fix a positive integer r such that

$$p^r > (n^2+1)/2. \tag{5.2}$$

The object of this section is to prove the following:

Proposition 5.3 *Let K/k, π, π' be as in Theorem A. Then there is a finite solvable extension L/K containing $E := K(\mu_{p^2})$ such that the base changes π_L, π'_L, satisfy*

$$\pi_L \simeq \pi'_L.$$

In fact the number field L we construct below will be much nicer than just being solvable over K. The extension L/E will turn out to be the compositum of a finite number of of p^r-extensions $L^{(i)}$, with each of them a nested chain of cyclic p^2-extensions. The Galois closure of L over $K(\mu_p)$ will again be a p-power extension, hence nilpotent. We will also have some freedom in the choice of the $L^{(i)}$, and their filtrations, which will become relevant in the next section when we descend to E.

Put $K' = K(\mu_p)$ and $k' = k(\mu_p)$. Then K'/k' is still a cyclic p-extension. The following Lemma is clear since K'/K and k'/k are of degree dividing $p-1$.

Lemma 5.4 *Let $v \in \Sigma^j_{K/k}$, for $j \in \{1, p\}$. Then, for every prime v' of K' above v, we have $v' \in \Sigma^j_{K'/k'}$.*

Consequently, the hypotheses of Theorem A are preserved for K'/k', and we may assume from here on, after replacing k (resp. K) by k' (resp. K'), that

$$\mu_p \subset k. \tag{5.5}$$

Proof of Proposition 5.3 when $K = E$

Since $\mu_p \subset k$, we may realize the cyclic p-extension K as $k(\alpha^{1/p})$, for an element α in k which is not a p-th power (in k). Now fix a positive integer r for which (5.2) holds. Choose a sequence of elements $\alpha_{-1} = \alpha$, $\alpha_0, \ldots, \alpha_r$ in the algebraic closure of K, and the corresponding chain of fields $k = L_{-1}, K = L_0, \ldots, L_r$ such that for each $j \geq 0$,

$$L_j = L_{j-1}(\alpha_j), \text{ with } \alpha_j^p = \alpha_{j-1}. \tag{5.6}$$

Clearly, every L_j/L_{j-1} is cyclic of order p, and so $[L_r : K] = p^r$. Moreover, since $\mu_{p^2} \subset E = K$, each L_j/L_{j-2} is also cyclic by Kummer theory. In other words, L_r/K is a nested chain of cyclic p^2-extensions. In fact, L_r/k is also such a nested chain, but of degree p^{r+1}.

Now put $L = L_r$. Applying Lemma 4.4, we then see that for every prime $\tilde{v}$ in L lying over some v in $\Sigma^p_{K/k}$, the degree of $\tilde{v}$ is p^r over k, hence has degree at least p^r over $\mathbb{Q}$. On the other hand, every other prime $\tilde{u}$ of L unramified over k lies above some u in $\Sigma^1_{K/k}$. So the hypotheses of Theorem A imply (by base change [1]) that $\pi_{L,\tilde{u}} \simeq \pi'_{L,\tilde{u}}$. (Such a $\tilde{u}$ could have small degree, like p, over K, but nevertheless it must lie over a prime u of degree 1 over k, which is all that matters to us.) Putting these together, and applying Proposition 2.1 over L, we get Proposition 5.3 when $K = E$. □

Proof of Proposition 5.3 when $K \neq E$

Here we want to base change and consider the cyclic p-extension

$$E/F, \text{ with } F = k(\mu_{p^2}),\ E = KF. \tag{5.7}$$

Clearly, the (p,p)-extension E/k contains $p+1$ subfields $F^{(i)}$, $0 \leq i \leq p$, of degree p over k, with one of them being K; say $K = F^{(0)}$. We need the following

Lemma 5.8 *Let $v \in \Sigma^p_{K/k}$ be unramified in E. Then v splits into p places $v_1, \dots, v_p$ in E, and there is a (unique) cyclic p-extension $F^{(i)}$ of k (depending on v), $1 \leq i \leq p$, such that each v_j lies in $\Sigma^p_{E/F^{(i)}}$. In other words, if z is the unique place of k below v, then z splits into p places in $F^{(i)}$, each of which is inert in E.*

Proof of Lemma 5.8. Since G :=Gal(E/k) is $\mathbb{Z}/p \times \mathbb{Z}/p$, the decomposition groups are either trivial or of order p. So, if z is the place of k lying below v, its Frobenius class Fr_z in G is given by an element σ of order p (since z is inert in K). So v must split in K. If we put $H = \langle \sigma \rangle$, then K^H is $F^{(i)}$ for a unique $i \in \{1, \dots, p\}$. Then z splits in $F^{(i)}$ and then becomes inert in E, as claimed. □

Fix an index $i \in \{1, \dots, p\}$. As $\mu_p \subset k \subset F^{(i)}$, we may find an element $\alpha^{(i)}$ in $F^{(i)}$ which is not a p-th power such that

$$E = F^{(i)}((\alpha^{(i)})^{1/p}). \tag{5.9}$$

Choose a sequence of elements $\alpha^{(i)}_{-1} = \alpha^{(i)}, \alpha^{(i)}_0, \dots, \alpha^{(i)}_r$ in the algebraic closure of E, and the corresponding chain of fields $F^{(i)} = L^{(i)}_{-1}, E = L^{(i)}_0, \dots, L^{(i)}_r$ such that for each $j \geq 0$,

$$L^{(i)}_j = L^{(i)}_{j-1}(\alpha^{(i)}_j), \text{ with } (\alpha^{(i)}_j)^p = \alpha^{(i)}_{j-1}. \tag{5.10}$$

By construction, every $L^{(i)}_j / L^{(i)}_{j-1}$ is cyclic of order p, and so $[L^{(i)}_r : E] = p^r$. Moreover, since $\mu_{p^2} \subset E$, each $L^{(i)}_j / L^{(i)}_{j-2}$ is also cyclic by Kummer theory. In other words, $L^{(i)}_r / E$ is a nested chain of cyclic p^2-extensions. In fact, $L^{(i)}_r / F^{(i)}$ is also such a nested chain (of degree p^{r+1}).

This way we get p nested chains $L^{(i)}/E$, disjoint over K from each other. Let L be the compositum of the $L^{(i)}$, as i runs over $\{1, \dots, p\}$. Pick any place v in $\Sigma^p_{K/k}$. Then we know (by Lemma 5.8) that there is a unique $i \leq p$ such that each of the divisors v_k of v in E, $1 \leq k \leq p$, lies in $\Sigma^p_{E/L^{(i)}}$. Then by the $r = 2$ case of Lemma 4.4, v_k is inert in $L^{(1)}$. Applying Lemma 4.5, we then see that every prime $\tilde{v}$ of L lying over some v_k (and hence over v) is of degree $\geq p^r > (n^2+1)/2$. So one may apply Proposition 2.1 and conclude that π_L and π'_L are isomorphic.

□

6. Descent to $E = K(\mu_{p^2})$

Let us preserve the notations of the previous section. Thanks to Proposition 5.3, we know that for the p-power extension L/E we constructed there, one has

$$\pi_L \simeq \pi'_L. \tag{6.1}$$

In order to prove Theorem A, we need to descend this isomorphism down to E. For this we will make use of the fact that there is quite a bit of freedom in choosing L.

Proof of descent when $K = E$

After realizing E as $k(\alpha^{1/p})$ for some α $(= \alpha_{-1})$ in k which is not a p-th power, we chose a sequence of elements $\alpha_j, 0 \leq j \leq r$, with $\alpha_j = \alpha_{j-1}^{1/p}$, and set $L_j = L_{j-1}(\alpha_j)$. We may replace α by $\alpha\beta^p$ for any β in $k - k^p$, which will have the effect of leaving $E = L_0$ intact, but changing L_1 from $E(\alpha_1)$ to $E(\alpha_1\beta_1)$ for a p-th root β_1 of β. Using this we can ensure, for a suitable choice of β, that the discriminant of L_1/E is divisible by a prime P_1 not dividing the conductor of either π_E or π'_E. Next we may choose a $\gamma \in k - k^p$ and put $\alpha_0 = \alpha_0\beta^p\gamma^{p^2}$, which will not change L_0 and L_1, but will change L_2, and we may arrange for the discriminant of the new L_2/L_1 to be divisible by a prime P_2 of L_1 whose norm down to E is relatively prime to $\mathfrak{c}(\pi_E)\mathfrak{c}(\pi'_E)P_1$. This way we may continue and modify all the L_j so that at each stage L_j/L_{j-1}, the relative discriminant is divisible by a new prime P_j of L_{j-1} whose norm down to E is relatively prime to $\mathfrak{c}(\pi_E)\mathfrak{c}(\pi'_E)P_1N_{L_1/E}(P_2)\ldots N_{L_{j-2}/E}(P_{j-1})$.

Now look at the top stage L_r/L_{r-1}. Thanks to (6.1), we know by the properties of base change ([1]) that every cuspidal isobaric component η, say, of $\pi_{L_{r-1}}$ will be twist equivalent to a cuspidal isobaric component η' of $\pi'_{L_{r-1}}$. More precisely, we will need to have, for some integer j mod p,

$$\eta' \simeq \eta \otimes \delta_r^j, \tag{6.2}$$

where δ_r is the character of order p of (the idele classes of) L_{r-1} attached to L_r. But the conductor of δ_r is divisible by the prime P_r, whose norm down to E is, by construction, relatively prime to the conductors of π_E and π'_E and to the discriminant of L_{r-1}/E. This forces $j = 0$, i.e., $\eta \simeq \eta'$. Peeling off this way isomorphic cuspidal components of $\pi_{L_{r-1}}$ and $\pi'_{L_{r-1}}$ one at a time, we conclude that $\pi_{L_{r-1}}$ is isomorphic to $\pi'_{L_{r-1}}$. Next, by induction on $r - j$, we deduce similarly that, for every $j \in \{0, \ldots, r-1\}$,

$$\pi_{L_j} \simeq \pi'_{L_j}, \tag{6.3}$$

which proves the assertion of Theorem A. □

Proof of descent when $K \neq E$

For each $i = \{1, \ldots, p\}$, we may modify the elements $\alpha_j^{(i)}$ and thus the fields $L_j^{(i)}$ as above, with a new prime divisor $P_j^{(i)}$ of the discriminant of L_j/L_{j-1} popping up at stage j, which is prime to the conductors of π_E, π'_E, and the discriminant of L_{j-1}/E. Now we may, and we will, also choose these primes in such a way that the sets $\{P_1^{(i)}, \ldots, P_r^{(i)}\}$ and $\{P_1^{(k)}, \ldots, P_r^{(k)}\}$ are disjoint whenever $i \neq k$. Now we may realize L as a sequence of cyclic p-extensions, such that at each stage there is a new prime divisor of the relative discriminant. We may then descend each step as above and finally conclude that

$$\pi_E \simeq \pi'_E, \tag{6.4}$$

as asserted. □

7. Descent to $K(\mu_p)$

As before, we may assume that $\mu_p \subset k \subset K$. If $\mu_{p^2} \subset K$, i.e., if $E = K$, then we have already seen above that we have an isomorphism $\pi \simeq \pi'$ over K.

So we may, and we will, assume below that $K \neq E$. Then

$$E = KF,\ k = K \cap F, \ \text{ where } F = k(\mu_{p^2}), \tag{7.1}$$

with

$$[E : F] = [K : k] = [E : K] = [F : k] = p,$$

and by section 6,

$$\pi_E \simeq \pi'_E. \tag{7.2}$$

This implies that if v is any prime of K which splits into p primes $w_1, \ldots, w_p$ in E, then by [1], we have $(\forall j \leq p)$

$$\pi_v \simeq \pi_{w_j} \simeq \pi'_{w_j} \simeq \pi'_v. \tag{7.3}$$

On the other hand, since E/k is a (p,p)-extension, in particular not cyclic of order p^2, any prime u of k which is inert in K must split in E (assuming u is unramified in E). This implies, thanks to (7.3), the following:

$$\pi_v \simeq \pi'_v, \ \forall\, v \in \Sigma^p_{K/k} - \text{finite set}. \tag{7.4}$$

When we combine (7.4) with the hypothesis of Theorem A that

$$\pi_v \simeq \pi'_v, \ \forall\, v \in \Sigma^1_{K/k}, \tag{7.5}$$

we immediately get the desired isomorphism

$$\pi \simeq \pi' \text{ (over } K).$$

We are now done with the proof of Theorem A. The assertion of Corollary B is obvious given Theorem A (since $\mu_2 \subset \mathbb{Q} \subset K$).

□

References

[1] J. Arthur and L. Clozel, *Simple algebras, base change, and the advanced theory of the trace formula*, Annals of Mathematics Studies, vol. 120, Princeton University Press, Princeton, NJ, 1989. MR1007299 (90m:22041)

[2] B. Feigon, K. Martin, and D. Whitehouse, *Periods and nonvanishing of central L-values for GL(2n)*, Preprint (2014), 1–29.

[3] J. Hoffstein and D. Ramakrishnan, *Siegel zeros and cusp forms*, Internat. Math. Res. Notices **6** (1995), 279–308, DOI 10.1155/S1073792895000225. MR1344349 (96h:11040)

[4] H. Jacquet and J. A. Shalika, *On Euler products and the classification of automorphic forms. II*, Amer. J. Math. **103** (1981), no. 4, 777–815, DOI 10.2307/2374050. MR623137 (82m:10050b)

[5] W. Luo, Z. Rudnick, and P. Sarnak, *On the generalized Ramanujan conjecture for* GL(n), Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), Proc. Sympos. Pure Math., vol. 66, Amer. Math. Soc., Providence, RI, 1999, pp. 301–310. MR1703764 (2000e:11072)

[6] C. S. Rajan, *On strong multiplicity one for l-adic representations*, Internat. Math. Res. Notices **3** (1998), 161–172, DOI 10.1155/S1073792898000142. MR1606395 (99c:11064)

[7] C. S. Rajan, *On strong multiplicity one for automorphic representations*, J. Number Theory **102** (2003), no. 1, 183–190, DOI 10.1016/S0022-314X(03)00066-0. MR1994478 (2004f:11050)

[8] D. Ramakrishnan, *A refinement of the strong multiplicity one theorem for* GL(2)*. Appendix to: "l-adic representations associated to modular forms over imaginary quadratic fields. II" by R. Taylor*, Invent. Math. **116** (1994), no. 1-3, 645–649, DOI 10.1007/BF01231576. MR1253208 (95h:11050b)

[9] D. Ramakrishnan, *A theorem on GL(n) à là Tchebotarev*, Preprint, being revised (2012), 1–19.

[10] W. Zhang, *Fourier transform and the global Gan-Gross-Prasad conjecture for unitary groups*, Preprint, to appear in the Annals of Mathematics (2012), 1–73.

Dinakar Ramakrishnan
253-37 Caltech
Pasadena, CA 91125, USA.
dinakar@caltech.edu