Mod ℓ representations of arithmetic fundamental groups II

(A conjecture of A.J. de Jong)

Gebhard Böckle *
Chandrashekhar Khare †

Abstract

We study deformation rings of a n-dimensional representation $\overline{\rho}$, defined over a finite field of characteristic ℓ, of the arithmetic fundamental group $\pi_1(X)$, where X is a geometrically irreducible, smooth curve over a finite field k of characteristic p ($\neq \ell$). We are able to show when $\overline{\rho}$ has large image that the resulting rings are finite flat over $\mathbf{Z}_\ell$. The proof principally uses a Galois-theoretic lifting result of the authors in Part I of this two-part work, a lifting result for cuspidal mod ℓ forms of Ogilvie, Taylor-Wiles systems and the result of Lafforgue. This implies a conjecture of A.J. de Jong in [dJ] for representations of $\pi_1(X)$ with coefficients in power series rings over finite fields of characteristic ℓ, that have this mod ℓ representation $\overline{\rho}$ as their reduction. A proof of all cases of the conjecture for $\ell > 2$ follows from a result announced (conditionally) by Gaitsgory in [Ga]. The methods are different.

*G.B would like to thank the TIFR for its hospitality in the Summer of 2002 during which the first decisive steps in this work were made and also the ETH for its inspirational environment and for its generosity in providing a three year post-doctoral position.

†Some of the work on this paper was done during a visit to Université Paris 7 which was supported by Centre franco-indien pour la promotion de la recherche avancée (CEFIPRA) under Project 2501-1 *Algebraic Groups in Arithmetic and Geometry.*

2000 MSC: 11F80, 11F70, 14H30, 11R34

Contents

1 Introduction

Let X be a geometrically irreducible, smooth curve over a finite field k of characteristic p and cardinality q. Denote by K its function field and by $\widetilde{X}$ its smooth compactification and set $S := \widetilde{X} \setminus X$. Let $\pi_1(X)$ denote the arithmetic fundamental group of X. Thus $\pi_1(X)$ sits in the exact sequence

$$0 \to \pi_1(\overline{X}) \to \pi_1(X) \to G_k \to 0,$$

where $\overline{X}$ is the base change of X to an algebraic closure of k, and G_F denotes the absolute Galois group of any field F. In this paper we study deformation rings of mod ℓ representations of $\pi_1(X)$: fix a continuous, absolutely irreducible representation $\overline{\rho} : \pi_1(X) \to \mathrm{GL}_n(\mathbf{F})$ with $\mathbf{F}$ a finite field of characteristic $\ell \neq p$. We begin with the following conjecture of A. J. de Jong:

Conjecture 1.1 ([dJ], Conj. 1.1) *Let $\rho : \pi_1(X) \to \mathrm{GL}_n(\mathbf{F}[[x]])$ be a continuous representation with residual representation $\overline{\rho}$. Then $\rho(\pi_1(\overline{X}))$ is finite.*

Remark 1.2 (i) In [dJ] de Jong proves the above for $n \leq 2$ by extending Drinfeld's reciprocity theorem in [Dr] to $\mathbf{F}((x))$-coefficients.

(ii) It is an important feature, observed in Lemma 2.12 of [dJ], of the representations considered in Conjecture 1.1 that the image of any inertia group (for a place in S) is finite. We will exploit this several times.

To state a reformulation of the above, we we need some notation. Let $\mathcal{O}$ be the ring of integers of a finite extension of the fraction field of $W(\mathbf{F})$ inside $\overline{\mathbf{Q}}_\ell$, let $\overline{\rho}$ be as above and fix a lift $\eta\colon \pi_1(X) \to \mathcal{O}^*$ of finite order of the 1-dimensional representation $\det \overline{\rho}$. Then in [dJ], following [Ma], it is explained how to attach a deformation ring $R^\eta_{X,\mathcal{O}}(\overline{\rho})$, or simply R^η_X for deformations of $\overline{\rho}$ of determinant η and defined on $\pi_1(X)$. In [dJ] the following is shown:

Theorem 1.3 ([dJ]) *Suppose $\overline{\rho}$ is absolutely irreducible when restricted to $\pi_1(\overline{X})$. Then Conjecture 1.1 is equivalent to R^η_X being finite (as a module) over $\mathbf{Z}_\ell$.*

The theorem combined with the result quoted in Remark 1.2 (a) shows:

Corollary 1.4 ([dJ]) *Suppose $n = 2$ and $\overline{\rho}$ is absolutely irreducible when restricted to $\pi_1(\overline{X})$. Then R^η_X is finite over $\mathbf{Z}_\ell$.*

Remark 1.5 Using obstruction theory, de Jong shows in [dJ] that if R^η_X is finite over $\mathbf{Z}_\ell$, then it is also flat over $\mathbf{Z}_\ell$ and a complete intersection.

1.1 Results

In Theorem 3.1 we prove, under a mild restriction, that the ring R^η_X is finite over $\mathbf{Z}_\ell$. To avoid some technicalities, here we only state the following special case:

Theorem 1.6 *Let $\overline{\rho} : \pi_1(X) \to \mathrm{SL}_n(\mathbf{F})$ be a representation with $\mathbf{F}$ a finite field of characteristic $\ell \neq p$. Assume that $\overline{\rho}$ has full image, $\ell \nmid n$, $|\mathbf{F}| \geq 4$, and $|\mathbf{F}| > 5$ if $n = 2$. Then the ring R^η_X is finite over $\mathbf{Z}_\ell$, and in particular Conjecture 1.1 holds for all ρ with reduction $\overline{\rho}$.*

Corollary 1.7 *Let $\overline{\rho}$ be as in the previous theorem. Then it lifts to an ℓ-adic representation $\rho : \pi_1(X) \to SL_n(\mathcal{O})$ with $\mathcal{O}$ the ring of integers of a finite extension of $\mathbf{Q}_\ell$. The representation ρ arises from a cuspidal eigenform, and hence $\overline{\rho}$ is automorphic. If moreover at any place in S ramification is either tame or of order prime to ℓ, then there exists a lift ρ and a corresponding cuspidal eigenform both of the same conductor as $\overline{\rho}$.*

PROOF of the corollary: We prove the second statement as the first is similar and easier. Let $R_X^{0,\eta}$ denote the quotient of R_X^{η} which parameterizes deformations which are minimal at the places in S. (This is a purely Galois-theoretic requirement. The conditions on ramification are needed so that we can formulate, using [BK1], Props. 5.1 and 5.2, a minimality condition.) By Poitou-Tate and some obstruction theoretic arguments due to Mazur, it is by now standard to show that $R_X^{0,\eta}$ has a presentation $W(\mathbf{F})[[x_1, \ldots, x_n]]/(y_1, \ldots, y_n)$, where some of the y_i could be zero. Because $R_X^{\eta}/(\ell)$ is finite, the same holds for $R_X^{0,\eta}/(\ell)$. From this one deduces easily that $R_X^{0,\eta}$ must be finite flat over $\mathbf{Z}_\ell$. This proves the corollary when combined with the results of [Laf]. ∎

Remark 1.8 The corollary combined with finiteness theorems of Harder about dimensions of cusp forms with bounded conductor and fixed central character has consequences for conjectures in [Ka1], [Mo], [MT]; see [BK2].

1.2 Sketch of proof

The form of Conjecture 1.1, combined with Remark 1.2 (b) and Theorem 1.3, lends itself to proving it not necessarily over X, but over a suitable finite cover Y of it, i.e. to applying base change techniques. We repeatedly make use of this. In a first reduction, base change allows us to pass to a situation where the assumptions of Theorem 1.6 are satisfied, and moreover X is projective.

In a second reduction step, we apply a level lowering technique of Skinner-Wiles in [SW] to the lift of $\overline{\rho}$ constructed in [BK1]. This relies on an important principle that was discovered by Carayol in [Ca] to switch types of automorphic representations that give rise to a given $\overline{\rho}$. The technique of Skinner-Wiles yields, after finite base change, a minimal lift (i.e., a representation of $\pi_1(Y)$ with Y projective) of $\overline{\rho}$ over some finite cover Y of X. (As

the results in [Laf] provide us with all base change results one expects, this does not require solvable base change.)

Thus it suffices to prove that the deformation ring R_Y^η of a representation $\overline{\rho} : \pi_1(Y) \to SL_n(\mathbf{F})$, with large image in the sense of Theorem 1.6, is finite over $\mathbf{Z}_\ell$, where Y is a projective, smooth, geometrically connected curve, and $\overline{\rho}$ lifts to an ℓ-adic representation of $\pi_1(Y)$. (Here R_Y is a minimal deformation ring, i.e., parameterizes equivalence classes of lifts of $\overline{\rho}$, to representations of $\pi_1(Y)$ with a fixed determinant η, defined over certain complete Noetherian $\mathbf{Z}_\ell$-algebras.) This is a significant simplification, if compared to the situation over number fields, as we need no level raising results (which are still not available, at least in any generality).

We prove the finiteness of R_Y^η by constructing Taylor-Wiles systems for $\overline{\rho}$ using the Galois cohomology techniques of Chapter 2 and automorphic methods of Chapter 3. This allows one to prove that the deformation ring R_Y^η for $\overline{\rho}$ is finite over $\mathbf{Z}_\ell$. By what we have said this proves Theorem 1.6.

Our techniques follow closely the original method of Wiles and Taylor in [Wi] and [TW], and later developments [Di], [F], [SW], [HT2], which we have to generalize to our context. In fact most of the work of this paper is devoted to carrying out these generalizations. There is a small modification needed to handle problems arising from "torsion" which may be of relevance even in the number field case: in an appendix we explain this innovation in the context considered in [Wi] and [TW].

1.3 Some remarks

In previous versions of this paper we had a weaker version of Theorem 1.6 with the additional hypothesis that $\overline{\rho}$ was locally irreducible at some place. A result of Ogilvie [Ogilvie] in his University of Chicago thesis, see Theorem 3.7 below, allows us to remove this hypothesis.

A proof of all cases of de Jong's conjecture has been announced conditionally by Gaitsgory in [Ga] for $\ell > 2$. His methods are different from ours. Our proof works in many cases when $\ell = 2$.

There are 2 separate works of Genestier and Tilouine (for GSp_4), and Clozel, Harris and Taylor (for GL_n), on generalizations of [Wi] and [TW] to n-dimensional representations of absolute Galois groups of totally real number fields. It's a comfort to us that we may quote verbatim from Section II of [HT2] for the Hecke action at places that are introduced in building Taylor-Wiles systems. One of the technical differences between the present

work and [HT2] when building Taylor-Wiles systems is that we allow for the possibility that the ℓth roots of 1 are in the base field which entails slight adjustments on the Galois and automorphic side.

The key *qualitative* difference between the mentioned works and ours is that we can prove automorphy of residual representations like $\overline{\rho}$ in the theorem (by the main result of [BK1]), while in the other works this has to be at the moment an important assumption that seems extremely difficult to verify in the number field case. Furthermore our aim is different: we are mainly interested in establishing algebraic properties of deformation rings, while in the number field case these are established *en route* to proving modularity of ℓ-adic representations (which is known in our context by [Laf]!).

Throughout this paper we use the notation of Part I of this work without further mention.

2 Galois cohomology

2.1 On deformations of the determinant

Unlike in part one of this work, we will no longer work with fixed determinants when considering deformation problems. At the same time, we want to keep finite the number of such determinants. The standard way over function fields to achieve this is to require that under any deformation of the determinant a certain *a priori* chosen place is totally split. This is basically what we will be doing – except that the deformation theory, and there the proof of Lemma 2.8 will require a slight twist of this, cf. Remark 2.9. The choice of place is the content of the following lemma:

Lemma 2.1 *There exist infinitely many places $w \in X$ whose residue field k_w satisfies $\ell \not| [k_w : k]$ and $k(\zeta_\ell) \cap k_w = k$.*

Proof: Let K' denote the unique constant field extension of K of degree ℓ. For a place w of K the following three conditions are equivalent: (a) w is split in K'/K, (b) ℓ divides $[k_w : k]$, (c) $\mathrm{Frob}_w \in \mathrm{Gal}(K'/K)$ is trivial. Similarly one has equivalences between (a') $k_w \cap k(\zeta_\ell) = k$, (b') $K(\zeta_\ell)/K$ is inert at w, (c') $\mathrm{Frob}_w \in \mathrm{Gal}(K(\zeta_\ell)/K)$ has maximal order. Since $\mathrm{Gal}(K(\zeta_\ell)/K)$ and $\mathrm{Gal}(K'/K)$ are abelian of relatively prime order, the group $\mathrm{Gal}(K'(\zeta_\ell)/K)$ is the direct product of the above two. Let $\sigma \in \mathrm{Gal}(K'(\zeta_\ell)/K)$ be of maximal

order. By the Čebotarev density theorem there exist infinitely many places $w \in X$ whose Frobenius automorphism maps to σ. Any such w will have the desired properties. ∎

For a place w as above one and $\overline{I}_w := I_w/([G_w, I_w]I_w^\ell)$ one has a split exact sequence

$$0 \longrightarrow \overline{I}_w \longrightarrow G_w^{\mathrm{ab}} \longrightarrow \hat{\mathbf{Z}} \longrightarrow 0 \tag{1}$$

where the group $\overline{I}_w \cong k_w^*/k_w^{*\ell}$ is a quotient of $\mathbf{Z}/(\ell)$ and trivial unless $\zeta_\ell \in K$. We fix a splitting $s_w \colon G_w^{\mathrm{ab}} \to \overline{I}_w$.

Lemma 2.2 *Let w, s_w be as above. Let $\overline{\rho} \colon G_w \to \{1\} \in \mathbf{F}$ denote the trivial character and $\rho^w \colon G_w \to \mathrm{GL}_1(R^w)$ the universal deformation of $\overline{\rho}$ for deformations which factors via the splitting s_w. Denote by $L_w \subset H^1(G_w, \mathbf{F})$ the subspace corresponding to the tangent space of the universal deformation.*

Then $\dim L_w = \dim_{\mathbf{F}} H^0(G_w, \mathbf{F}(1)) = \dim_{\mathbf{F}} \mathbf{F}(1)^{\pi_1(X)}$, the subspace L_w is a complement to $H^1_{\mathrm{unr}}(G_w, \mathbf{F})$ in $H^1(G_w, \mathbf{F})$, and $L_w^\perp$ is a complement to $H^1_{\mathrm{unr}}(G_w, \mathbf{F}(1))$ in $H^1(G_w, \mathbf{F}(1))$.

Proof: From the definition of R^w it follows that L_w is a complementary sub vector space for $H^1_{\mathrm{unr}}(G_w, \mathbf{F})$ in $H^1(G_w, \mathbf{F})$. Since local Tate-duality is perfect, $L_w^\perp$ must be a complementary vector space for $H^1_{\mathrm{unr}}(G_w, \mathbf{F}(1))$ in $H^1(G_w, \mathbf{F}(1))$. The fact that L_w is complementary to $H^1_{\mathrm{unr}}(G_w, \mathbf{F})$ also implies that it has the same dimension as $H^2(G_w, \mathbf{F})$. Again by local Tate-duality the latter is equal to the dimension of $H^0(G_w, \mathbf{F}(1))$. Combined with the second assertion in Lemma 2.1 this yields the identities for $\dim_{\mathbf{F}} L_w$. ∎

From now on, for the remainder of this article, we fix a place $w \in X$ as in Lemma 2.1 and a splitting s_w as in (1).

2.2 Removing local ramification

The current section lays the Galois-theoretic ground work for the base change techniques which we will apply repeatedly in the proof of our main result in the subsequent chapter. In this respect the following proposition and corollary will be of much use to us.

Proposition 2.3 *Let R be in $\mathcal{A}$, let $\rho\colon \pi_1(X) \to \mathrm{GL}_n(R)$ a continuous representation and let $S_1 \subset S$ be the set of places at which $\rho(I_v)$ is finite. Let $T_s, T_i \subset \widetilde{X}$ be finite and disjoint and let m be some positive integer. Then there exists a finite (possibly ramified) Galois cover $Y \to X$, say with function field L, such that*

(i) L/K is totally split at all places above of T_s.

(ii) At places in T_i, the residue degree of the extension field L/K is a multiple of m.

(iii) The restriction $\rho_{|\pi_1(Y)}$ is unramified at the places above $S_1 \setminus T_s$.

Note that the assumptions are satisfied for any representation ρ which is unramified outside a finite set of places, provided R is finite or the ring of integers of a local field of positive characteristic, cf. Remark 1.2 (b). Before giving the proof, we state the following important corollary, which will be used in the sequel:

Corollary 2.4 *Suppose R, ρ, S_1 are as in the previous proposition, $T_i \subset \widetilde{X}$ and m some positive integer. Then there exists a finite (possibly ramified) Galois covering $Y \to X$ with corresponding extension L/K of function fields such that*

(i) Y is geometrically connected over k

(ii) $\rho(\pi_1(X)) = \rho(\pi_1(Y))$ $\overline{\rho}(\pi_1(\overline{X})) = \overline{\rho}(\pi_1(\overline{Y}))$,

(iii) $\rho_{|\pi_1(Y)}$ is unramified above the places in S_1.

(iv) at places above T_i, the residue degree of L/K is a multiple of m.

In particular if R is finite or the ring of integers of a local field of positive characteristic, we can ensure that $\rho_{|\pi_1(Y)}$ is unramified everywhere.

Proof of Corollary 2.4: We claim that there is a finite set $T' \subset X$ disjoint from T_i such that the elements $\rho(\mathrm{Frob}_v)$, $v \in T'$, topologically generate $\rho(\pi_1(X))$. Since $\overline{\rho}(\pi_1(X))$ is finite, by the Čebotarev density theorem there exists a finite set $T'' \subset X$ disjoint from T_i with the above property for $\overline{\rho}$. Let $X' \to X$ be the smallest finite Galois covering over which $\overline{\rho}$ becomes trivial. Then $\rho(\pi_1(X'))$ is a pro-ℓ group, and since the pro-ℓ completion

of $\pi_1(X')$ is topologically finitely generated, so is $\rho(\pi_1(X'))$. Therefore its Frattini quotient is finite, and again by the Čebotarev density theorem we may choose a finite set $T''' \subset X$ disjoint from T_i such that the elements $\rho(\mathrm{Frob}_v)$, $v \in T'''$, lie in $\rho(\pi_1(X'))$ and span the Frattini quotient. Therefore by Burnside's basis theorem these elements topologically generate $\rho(\pi_1(X'))$. The claim follows with $T' := T'' \cup T'''$.

Recall that E is the splitting field of $\overline{\rho}$. Let now $T_s \supset T'$ be a finite set of places disjoint from T_i such that

(a) the greatest common divisor of the q_v, $v \in T_s$, is q, and

(b) there exist $w_1, \ldots, w_j \in T_s$ such that $\mathrm{Frob}_{w_i} \in G_E$, $i = 1, \ldots, j$, and such that $\#(E \cap \overline{\mathbf{F}}_p)$ is the greatest common divisor of the q_{w_i}, $i = 1, \ldots, j$.

Applying the above proposition with these data, the corollary follows. (Note that condition (b) guarantees the second part of (ii).) ∎

We first prove the following lemma:

Lemma 2.5 *Let $\widetilde{K}/K$ be finite with constant field k, let u be a place of $\widetilde{K}$ and $\widetilde{K}_u$ the corresponding completion. Suppose $F/\widetilde{K}_u$ is Galois of prime degree e. Then for any set of place T of $\widetilde{K}$ not containing u, there exists a Galois extension L of $\widetilde{K}$ of degree e such that*

(i) all places in T are split,

(ii) there is a unique place u' in L above $\widetilde{K}$, and

(iii) the extension $L_{u'}/\widetilde{K}_u$ is isomorphic to $F/\widetilde{K}_u$.

Proof: Let us first assume that $e = p$. Then $F/\widetilde{K}_u$ is an Artin-Schreier extension, say given by an equation $x^p - x = a$ for some $a \in \widetilde{K}_u$. Using the approximation theorem, we can find $b \in \widetilde{K}$ such that $b - a$ lies in the maximal ideal of the local ring at u and b lies in the maximal ideal of the local rings of places in T. Then the Artin-Schreier extension $L := \widetilde{K}(z)$ with $z^p - z = b$ has all the required properties.

We now suppose $e \neq p$. In this situation, we quote the following result from [Ne], Ex. 6 (the required modifications for the function field case are straightforward): For any finite set T' of places of $\widetilde{K}$, the morphism

$$H^1(G_K, \mathbf{Z}/(e)) \longrightarrow \mathrm{II}_{v \in T'} H^1(G_v, \mathbf{Z}/(e))$$

is surjective. Note that $H^1(G_K, \mathbf{Z}/(e)) = \mathrm{Hom}(G_K, \mathbf{Z}/(e))$. Define $T' := T \cup \{u\}$ and set $\chi_v = 0 \in \mathrm{Hom}(G_v, \mathbf{Z}/(e))$ for $v \in T$ and choose for χ_u a character of G_u whose fixed field is F. Let χ be a global character which maps to the χ_v, $v \in T'$. Then it is easy to see that the fixed field of χ satisfies all the conditions required from L. ∎

PROOF of Proposition 2.3: By possibly shrinking S, we may assume that $\overline{\rho}$ is ramified at all places of S. Let $v_1, \ldots, v_r$ denote the places in S and $v_1, \ldots, v_{r'}$, $r' \leq r$, those in $S_1 \setminus T_s$. The groups $\rho(G_v)$ are all pro-solvable. By repeated application of the above lemma, we first construct a finite extension L_1 over K which is totally split at all places in T_s and such that the local extension of L_1/K above v_1, is Galois with group isomorphic to $\rho(G_{v_1})$ under ρ. Then construct L_2/L_1 which is again totally split at all places of T_s and such that for a place v_2' of L_1 above v_2 in K the local extension of L_2/L_1 above v_1' is Galois with group isomorphic to $\rho(G_{v_2})$ under ρ. One reaches inductively an extension $L_{r'}$ which contains places $w_1, \ldots, w_{r'}$ above $v_1, \ldots, v_{r'}$ such that the restriction of ρ to each G_{w_i} is trivial.

By another repeated application of the lemma, we may construct an extension $L'_{r'}$ of $L_{r'}$, totally split at all places above T_s and such that the residue degree at places in T_i grows by a multiple of m. (Locally at places in T_i one constructs the unramified extensions of degree m.) Then the Galois closure L of $L'_{r'}$ above K has all the desired properties. ∎

Simplifying assumption henceforth: Because of the corollary, and Theorem 1.3, we may and will assume from now on that the curve X in Theorem 1.6 is projective.

2.3 On Taylor-Wiles' auxiliary primes

In Section 3.4, we will construct Taylor-Wiles systems, [TW], in the minimal case. As such they consist of a Galois-theoretic and a Hecke part. The current section provides the Galois-theoretic tools needed. Recall that in [BK1] the extension E/K is defined as the splitting field $\overline{\rho}$.

We begin with the following Lemma:

Lemma 2.6 *Let v be a place such that $q_v \equiv 1 (\mathrm{mod}\ \ell)$, $\overline{\rho}$ is unramified at v and $\overline{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues which are all contained in $\mathbf{F}$. Let $(R, \mathfrak{M})$ be in $\mathcal{A}$ and let $\rho_v : G_v \to \mathrm{GL}_n(R)$ be a lift of $\overline{\rho}_v$. Then up to strict equivalence the image of ρ_v is diagonalizable.*

Recall that $\rho_v, \rho_v' \colon G_v \to \mathrm{GL}_n(R)$ are strictly equivalent if there exists $M \in \mathrm{GL}_n(R)$ congruent to the identity modulo $\mathfrak{M}$ such that $M\rho_v M^{-1} = \rho_v'$.

Note also that ρ_v will factor through the tame quotient $\overline{G}_{q_v}$ of G_v since $\overline{\rho}$ is unramified and the kernel of $\pi \colon \mathrm{GL}_n(R) \to \mathrm{GL}_n(\mathbf{F})$ is prime to p. The lemma implies that in fact ρ_v factors through the abelianization $\hat{\mathbf{Z}} \times \mathbf{Z}/(q_v - 1)$ of $\overline{G}_{q_v}$.

PROOF: Let us assume that $\overline{\rho}_v$ takes its image in the diagonal matrices. This shows in particular, that the exponent e of the cyclic group $\overline{\rho}(G_v)$ is prime to ℓ. Because the kernel of π, defined above, is a pro-ℓ group, the representation $\rho_v \colon \overline{G}_{q_v} \to \mathrm{GL}_n(R)$ must factor via the quotient $G := \mathbf{Z}_\ell(1) \rtimes (\mathbf{Z}_\ell \times \mathbf{Z}/(e))$ of $\overline{G}_{q_v}$.

Let σ be a generator of $\mathbf{Z}/(e)$ and s of $\mathbf{Z}_\ell \times \mathbf{Z}/(e)$. We may regard σ as well as s as elements of G. Because $\overline{\rho}(\sigma)$ has distinct eigenvalues and $\rho_v(\sigma)$ has finite order e, using strict equivalence we may assume that $\rho_v(\sigma)$ is diagonal. Since $\overline{\rho}(\sigma)$ has distinct eigenvalues, the same holds for $\rho_v(\sigma)$. But this implies that $\rho_v(s)$ is diagonal as well, because $\rho_v(s)$ commutes with $\rho_v(\sigma)$.

We now claim by induction on $i \geq 1$ that $\rho_v(t) \pmod{\mathfrak{m}^i}$ is diagonal, the assertion being trivially true for $i = 1$. So let us assume that the assertion holds for i and write $\rho_v(t) = D + B$, where D is a diagonal matrix and B is zero along the diagonal and has entries in $\mathfrak{m}^i$. Because $B^2 \equiv 0 \pmod{\mathfrak{m}^{i+1}}$, the relation $sts^{-1} = t^{q_v}$ yields

$$\rho_v(s)(D+B)\rho_v(s)^{-1} \equiv D^{q_v} + \sum_{i=0}^{q_v-1} D^i B D^{q_v-i-1} \pmod{\mathfrak{m}^{i+1}}.$$

As $D \equiv I \pmod{\mathfrak{m}}$, and $q_v - 1 \in \mathfrak{m}$ the right hand side is congruent to $D^{q_v} + B$ modulo $\mathfrak{m}^{i+1}$. Comparing off-diagonal entries, we see that $B \pmod{\mathfrak{m}^{i+1}}$ commutes with $\rho_v(s) \pmod{\mathfrak{m}^{i+1}}$. This shows that $B \pmod{\mathfrak{m}^{i+1}}$ is diagonal, and hence zero. ∎

For a place v as in the previous lemma, an integer $m \in \mathbf{N}$ such that $\ell^m | (q_v - 1)$, and an eigenvalue λ of $\overline{\rho}(\mathrm{Frob}_v)$, we define the collection of lifts $\mathcal{C}_{v,\lambda,m}$ of $\overline{\rho}_v$ as follows:

Let $s, t \in G_v^{\mathrm{ab}} \cong \mathbf{Z}/(q_v - 1) \times \hat{\mathbf{Z}}$ be such that t generates inertia and s maps to Frob_v in G_v/I_v. Denote by $\lambda_1, \ldots, \lambda_n$ Teichmüller lifts of the eigenvalues if $\overline{\rho}(\mathrm{Frob}_v)$ such that $\lambda \equiv \lambda_1 \pmod{\ell}$. Set

$$R_{v,m} := W(\mathbf{F})[[x_1, \ldots, x_n, y]] / \Big((1+y)^{\ell^m} - 1 \Big),$$

and define $\rho_{v,\lambda,m}\colon G_v \longrightarrow\!\!\!\!\!\rightarrow G_v^{\mathrm{ab}} \longrightarrow \mathrm{GL}_n(R_{v,m})$ by

$$s \mapsto \mathrm{Diag}(\lambda_1(1+x_1),\ldots,\lambda_n(1+x_n)),\ t \mapsto \mathrm{Diag}((1+y),1,1,\ldots,1).$$

Finally define $\mathcal{C}_{v,\lambda,m}\colon \mathcal{A} \to \mathbf{Sets}$ by

$$\begin{aligned} R \ \mapsto \ \mathcal{C}_{v,\lambda,m}(R) := \{\rho\colon G_v \to \mathrm{GL}_n(R) \,|\, &\exists \alpha \in \mathrm{Hom}_{\mathcal{A}}(R_{v,m},R), \\ &\exists M \in 1+M_n(\mathfrak{m}_R) : \rho = M(\alpha\circ\rho_{v,\lambda,m})M^{-1}\big\}. \end{aligned}$$

We define $L_{v,\lambda,m} \subset H^1(G_v,\mathrm{ad}(\overline{\rho}))$ as the subspace spanned by the 1-cocycles

$$\left\{ c : g \mapsto \frac{1}{\varepsilon}(\rho(g)\rho_0^{-1}(g) - I) | \rho \in \mathcal{C}_{v,\lambda,m}(\mathbf{F}[\varepsilon]/(\varepsilon^2)) \right\}, \tag{2}$$

where ρ_0 is the tautological lift induced from the splitting $\mathbf{F} \to \mathbf{F}[\varepsilon]/(\varepsilon^2)$. It is easy to see that $\dim L_{v,\lambda,m} = \dim H^1_{\mathrm{unr}}(G_v,\mathrm{ad}(\overline{\rho})) + 1 = n+1$. Moreover $L_{v,\lambda,m}$ is independent of m as long as $m > 0$. Finally, note also that Corollary 4.9 of [BK1] yields:

Lemma 2.7 *Let $\sigma \in \mathrm{Gal}(E(\zeta_\ell)/K)$ be the image of Frob_v. Then the subspace*

$$L^{\perp}_{v,\lambda,m} \subset H^1_{\mathrm{unr}}(G_v,\mathrm{ad}(\overline{\rho})(1)) \cong \mathrm{ad}(\overline{\rho})/(\mathrm{Frob}_v - 1)\mathrm{ad}(\overline{\rho})$$

of codimension one only depends on σ and the choice of λ (among the eigenvalues of $\overline{\rho}(\sigma)$).

Because of the above lemma, we also write $L^{\perp}_{\sigma,\lambda}$ or $L^{\perp}_{v,\lambda}$ for $L^{\perp}_{v,\lambda,m}$. Note that since the cyclotomic character χ is trivial on G_v, the restrictions of $\mathrm{ad}(\overline{\rho})$ and $\mathrm{ad}(\overline{\rho})(1)$ to G_v agree.

The central result of this section is the following which is modeled at [HT2], Thm. IV.5.3. The notation for Selmer groups is the standard one and for instance the one used in [BK1].

Lemma 2.8 *Let $\overline{\rho} : \pi_1(X) \to \mathrm{GL}_n(\mathbf{F})$ be a continuous representation. Define $L_w := H^1_{\mathrm{unr}}(G_v,\mathrm{ad}^0(\overline{\rho}))\oplus L_{w,d}$, where $L_{w,d}$ is the subspace of $H^1(G_w,\mathbf{F})$ considered in Lemma 2.2, and $\mathbf{F} \subset \mathrm{ad}(\overline{\rho})$ via the diagonal embedding. Suppose that*

(i) For any $\pi_1(X)$-subrepresentation V of $\mathrm{ad}(\overline{\rho})$, there exists a regular semisimple $g_V \in \overline{\rho}(\pi_1(\overline{X}))$ such that $V^{g_V} \neq 0$.

(ii) If $\zeta_\ell \in E$, *then* $H^1(\mathrm{Gal}(E/K(\zeta_\ell)), \mathrm{ad}^0(\overline{\rho})) = 0$.

(iii) If $\zeta_\ell \in K$, *then* $\mathrm{ad}^0(\overline{\rho})$ *has no* 1*-dimensional subrepresentation.*

(iv) The image of $\overline{\rho}$ *has no quotient of order* ℓ.

Then for any given $m \in \mathbf{N}$ *there exists a set* Q_m *of* $\dim H^1_{\{L_v\}}(\{w\}, \mathrm{ad}(\overline{\rho}))$ *places of* $X \setminus \{w\}$ *such that*

(a) $q_v \equiv 1 \pmod{\ell^m}$ *for all* $v \in Q_m$,

(b) $\overline{\rho}(\mathrm{Frob}_v)$ *has distinct eigenvalues for each* $v \in Q_m$, *and*

(c) $H^1_{\{L_v^\perp\}}(\{w\} \cup Q_m, \mathrm{ad}(\overline{\rho})(1)) = 0$ *where* $L_v = L_{v,\lambda_v}$ *for each* $v \in Q_m$, *and* λ_v *is some eigenvalue of* $\overline{\rho}(\mathrm{Frob}_v)$.

Moreover $\dim H^1_{\{L_v\}}(\{w\}, \mathrm{ad}(\overline{\rho})) = \dim H^1_{\{L_v\}}(Q_m \cup \{w\}, \mathrm{ad}(\overline{\rho}))$.

The proof in fact shows that the sets Q_m above may be chosen disjoint from any given finite set of places S'. Moreover the proof can be extended, almost verbatim, to the case where one is given a set of deformation conditions $(\mathcal{C}_v, L_v)_{v \in S \cup \{w\}}$ at a finite set S disjoint from $\{w\}$.

PROOF: The proof follows closely the analogous proof given in [HT2] which in turn is similar to that in [TW]. Note first that $L_v = H_{\mathrm{unr}}(G_v, \mathrm{ad}(\overline{\rho}))$ implies that $\dim L_v = h^0(G_v, \mathrm{ad}(\overline{\rho}))$. By Lemma 2.2 we have $\dim L_{w,d} = \dim H^0(G_w, \mathbf{F}(1))$, and so [BK1], Rem. 3.5, yields

$$\dim H^1_{\{L_v\}}(\{w\}, \mathrm{ad}(\overline{\rho})) = \dim H^1_{\{L_v^\perp\}}(\{w\}, \mathrm{ad}(\overline{\rho})(1)). \tag{3}$$

Define $E_m := E(\zeta_{\ell^m})$ and let $Y_m \to X \setminus \{w\}$ be the corresponding Galois cover. We first claim that the composite

$$H^1_{\{L_v^\perp\}}(\{w\},\mathrm{ad}(\overline{\rho})(1)) \hookrightarrow H^1(\pi_1(X\setminus\{w\}),\mathrm{ad}(\overline{\rho})(1)) \to H^1(\pi_1(Y_m),\mathrm{ad}(\overline{\rho})(1))^{\mathrm{Gal}(E_m/K)}$$

is injective, where the second morphism is restriction.

We have $L_w = H^1_{\mathrm{unr}}(G_w, \mathrm{ad}^0(\overline{\rho})) \oplus L_{w,d}$ with $L_{w,d} \subset H^1(G_w, \mathbf{F})$, and so we may prove the claim separately for the subrepresentations $\mathbf{F}$ and $\mathrm{ad}^0(\overline{\rho})$ of $\mathrm{ad}(\overline{\rho})$. We first consider $\mathrm{ad}^0(\overline{\rho})$.

Condition (ii) yields $H^1(\mathrm{Gal}(E_1/K), \mathrm{ad}^0(\overline{\rho})(1))) = 0$, as can be seen by applying for instance by [Bö1], Prop. 1.8 (i),(ii). This proves the claim for

$m = 1$ and $\mathrm{ad}^0(\overline{\rho})$. For $m > 1$, inflation-restriction and taking invariants yields the left-exact sequence

$$0 \to H^1(\mathrm{Gal}(E_m/E_1), \mathrm{ad}^0(\overline{\rho})(1))^{\mathrm{Gal}(E_1/K)} \to H^1(\pi_1(Y_1), \mathrm{ad}^0(\overline{\rho})(1))^{\mathrm{Gal}(E_1/K)}$$
$$\to H^1(\pi_1(Y_m), \mathrm{ad}^0(\overline{\rho})(1))^{\mathrm{Gal}(E_m/K)}.$$

We will show that the left hand term vanishes. Since $K(\zeta_{\ell^m})$ is Galois over K, the group $\mathrm{Gal}(E_m/E_1)$ lies in the center of $\mathrm{Gal}(E_m/K)$. Moreover by the definition of E_1, the action of $\mathrm{Gal}(E_m/E_1)$ on $\mathrm{ad}(\overline{\rho})(1)$ is trivial. Therefore we find

$$\begin{aligned} & H^1(\mathrm{Gal}(E_m/E_1), \mathrm{ad}^0(\overline{\rho})(1))^{\mathrm{Gal}(E_1/K)} \\ = \;& H^1(\mathrm{Gal}(E_m/E_1), \mathbf{F}) \otimes_{\mathbf{F}} (\mathrm{ad}^0(\overline{\rho})(1))^{\mathrm{Gal}(E_1/K)}. \end{aligned}$$

By (iii) the last expression is zero. This proves the claim for the $\mathrm{ad}^0(\overline{\rho})$-component.

We will now consider the diagonal $\mathbf{F}$-component. By inflation-restriction we need to show

$$0 = H^1_{\{L^\perp_{v,d}\}}(\{w\}, \mathbf{F}(1)) \cap H^1(\mathrm{Gal}(E_m/K), \mathbf{F}(1))$$

inside $H^1(\pi_1(X \setminus \{w\}), \mathbf{F}(1))$. Again by inflation-restriction, the second term allows the isomorphism

$$H^1(\mathrm{Gal}(E_m/K), \mathbf{F}(1)) \cong (H^1(\mathrm{Gal}(E_m/K(\zeta_\ell)), \mathbf{F}) \otimes \mathbf{F}(1))^{\mathrm{Gal}(K(\zeta_\ell)/K))}.$$

By assumption (iv) the right hand side is isomorphic to

$$H^1(\mathrm{Gal}(K(\zeta_{\ell^m})/K(\zeta_\ell)), \mathbf{F}) \otimes (\mathbf{F}(1)^{\mathrm{Gal}(K(\zeta_\ell)/K)}).$$

If $\zeta_\ell \notin K$, the proof of the claim is thus complete. In the case $\zeta_\ell \in K$, a non-zero class in $H^1(\mathrm{Gal}(E_m/K), \mathbf{F}(1))$ describes a non-zero character $\mathrm{Gal}(K(\zeta_{\ell^m})/K(\zeta_\ell)) \longrightarrow \mathbf{F}$. Because $\ell \nmid [k_w : k]$, such a class restricts to a non-zero class in $H^1_{\mathrm{unr}}(G_w, \mathbf{F}(1))$. By Lemma 2.2 it maps to a nonzero class in $H^1(G_w, \mathbf{F}(1))/L^\perp_{w,d}$ and so such a class cannot lie in $H^1_{\{L^\perp_{v,d}\}}(\{w\}, \mathbf{F}(1))$. This completes the proof of the claim.

Let now ψ be a 1-cocycle whose class $[\psi] \in H^1_{\{L^\perp_v\}}(\{w\}, \mathrm{ad}(\overline{\rho})(1))$ is non-zero. By the above claim, the restriction of ψ to $\pi_1(Y_m)$ is non-trivial.

Since $\pi_1(Y_m)$ acts trivially on $\mathrm{ad}(\overline{\rho})(1)$, the class $[\psi]$ induces a non-trivial $\mathrm{Gal}(E_m/K)$-equivariant homomorphism $\pi_1(Y_m) \to \mathrm{ad}(\overline{\rho})(1)$. Let E_ψ denote the fixed field of its kernel, and $V(1)$ its image in $\mathrm{ad}(\overline{\rho})(1)$. Then the induced morphism $\mathrm{Gal}(E_\psi/E_m) \to V(1)$ is bijective.

Choose a regular semisimple $g \in \overline{\rho}(\overline{X})$ such that $V^g \neq 0$, and an element $\sigma \in \mathrm{Gal}(E_1/K(\zeta_\ell))$ such that $g = \overline{\rho}(\sigma)$. For such a g we now consider

$$V(1)_g \cong V_g \longhookrightarrow \mathrm{ad}(\overline{\rho})(1)_g \cong \mathrm{ad}(\overline{\rho})_g \cong H^1_{\mathrm{unr}}(G_v, \mathrm{ad}(\overline{\rho})(1)),$$

where $v \in X \setminus \{w\}$ is any place with $\mathrm{Frob}_v \mapsto \sigma$. For an eigenvalue λ of g we denote by $L^\perp_{g,\lambda} \subset \mathrm{ad}(\overline{\rho})(1)_g$ the corresponding subspace as defined in (2). One easily shows $\cap_\lambda L^\perp_{g,\lambda} = 0$, where the intersection ranges over all eigenvalues of g, e.g., by proving the dual assertion. We claim that there exists $x_V \in V_g$ and an eigenvalue λ of g such that

$$\psi(\mathrm{Frob}_v) + x_V \notin L^\perp_{g,\lambda} \subset H^1_{\mathrm{unr}}(G_v, \mathrm{ad}(\overline{\rho})(1)).$$

Assume otherwise. Then $\psi(\mathrm{Frob}_v) + V_g \subset L^\perp_{g,\lambda}$ for all eigenvalues λ. This implies $V_g \subset L^\perp_{g,\lambda}$ for all λ, and therefore $V_g \subset \cap_\lambda L^\perp_{g,\lambda} = 0$, contradicting $V_g \cong V^g \neq 0$.

Let $\tau \in \pi_1(X \setminus \{w\})$ by any element which acts trivially on E_m and maps to x_V under ψ. Because E_ψ/K is Galois, by the Čebotarev density theorem there exists a place $v' \in X \setminus \{w\}$ such that the image of $\mathrm{Frob}_{v'}$ in $\mathrm{Gal}(E_\psi/K)$ agrees with that of $\tau\mathrm{Frob}_v$. By the above $[\psi] \notin L^\perp_{v',\lambda}$. A simple inductive argument now finishes the proof of the lemma. ∎

Remark 2.9 At two instances the above proof made crucially use of the special choice of w and of the deformation condition on the determinant that we enforce at w. First these choices were needed to obtain formula (3). Second, they were needed to prove the injectivity of the $\mathbf{F}$-component of $\mathrm{ad}(\overline{\rho})$ in the displayed homomorphism below (3). There an important point is that in the function field situation the extension $K(\zeta_{\ell^m})/K(\zeta_\ell)$ is a constant field extension, and hence unramified. The special choice of determinantal deformations at w was then needed to rule out certain unramified characters. In the number field case the extension $K(\zeta_{\ell^m})/K(\zeta_\ell)$ typically is ramified at the prime ℓ, and so a choice of w and a deformation condition is unecessary.

To complement the above lemma, in the particular case in which we are interested, we also prove the following:

Lemma 2.10 *Suppose* $\overline{\rho}\colon \pi_1(X) \to \mathrm{SL}_n(\mathbf{F})$ *is surjective,* $\ell \nmid n$, $|\mathbf{F}| \geq 4$, *and* $|\mathbf{F}| > 5$ *for* $n = 2$. *Then*

(i) $\overline{\rho}(\pi_1(\overline{X})) = \mathrm{SL}_n(\mathbf{F})$ *contains a regular semisimple element.*

(ii) $\mathrm{ad}(\overline{\rho}) = \mathrm{ad}^0(\overline{\rho}) \oplus \mathbf{F}$, $\mathrm{ad}^0(\overline{\rho})$ *is irreducible, and for any regular semisimple* $g \in \mathrm{SL}_n(\mathbf{F})$ *one has* $\mathbf{F}^g = \mathbf{F}$ *and* $M_n^0(\mathbf{F})^g \neq 0$.

(iii) $H^1(\mathrm{SL}_n(\mathbf{F}), M_n^0(\mathbf{F})) = 0$.

(iv) $\mathrm{SL}_n(\mathbf{F})$ *has no quotient isomorphic to* $\mathbf{Z}/(\ell)$.

PROOF: Under our conditions on n and $\mathbf{F}$, the group $\mathrm{SL}_n(\mathbf{F})$ has no abelian quotients, which shows (iv) and $\overline{\rho}(\overline{X}) = \mathrm{SL}_n(\mathbf{F})$. Parts (i) and (ii) are clear and (iii) follows from [CPS]. ∎

3 Automorphic methods

We begin this chapter by briefly reviewing parts of the theory of automorphic forms over function fields. We formulate in Section 3.3 a principle of Carayol, [Ca] in a form suitable for us (cf., the 2 lemmas in the section). Section 3.4 explains how to carry over the method of Taylor-Wiles systems and its later simplification, cf. [TW], [Di], from the number field to the function field case, using crucially results of Section 3.3, assuming that we are in a situation where we have an automorphic lift of $\overline{\rho}$ of minimal level. Thereby we prove isomorphisms between certain universal deformation rings and corresponding Hecke algebras, under this crucial assumption. We present a slight technical improvement over the usual method that might also be useful in the number field case. In Section 3.5, we prove a theorem on 'lowering the level up to base change' for certain cuspidal Hecke eigenforms, which allows us to verify this assumption in a significant number of cases, enough to cover the applications to Theorems 3.1 and 1.6 that are proved in the last section by pulling all the results of this section together. Our method here is that of Skinner-Wiles, [SW], and again relies on results of Section 3.3.

We fix some notation to state the main theorem of the final section: Let $\mathcal{O}$ be a discrete valuation ring finite over $W(\mathbf{F})$ and with maximal ideal $\mathfrak{m}$. For a finite subset T of X, consider a representation $\rho\colon \pi_1(X \setminus T) \to \mathrm{GL}_n(\mathcal{O})$

with residual representation $\overline{\rho} := \rho \pmod{\mathfrak{m}}$. The extension E/K is as in Section 2.3. We say that ρ is *of type*-1 *at a place* $v \in \widetilde{X}$, if $\overline{\rho}$ *is unramified at* v *and* $\rho(I_v)$ *is unipotent of rank* 1.

In the final section, we prove the following theorem and give some further applications of it.

Theorem 3.1 *Let* $\mathcal{O}, T, \rho, \overline{\rho}$ *be as above and suppose they satisfy*

(i) ρ_v *is of type*-1 *at all* $v \in T$,

(ii) For any $\pi_1(X)$*-subrepresentation* V *of* $\mathrm{ad}(\overline{\rho})$*, there exists a regular semisimple* $g_V \in \overline{\rho}(\pi_1(\overline{X}))$ *such that* $V^{g_V} \neq 0$.

(iii) If $\zeta_\ell \in K$*, then* $\mathrm{ad}^0(\overline{\rho})$ *has no* 1*-dimensional subrepresentation,*

(iv) If $\zeta_\ell \in E$*, then* $H^1(\mathrm{Gal}(E/K(\zeta_\ell), \mathrm{ad}^0(\overline{\rho})) = 0$.

(v) The image of $\overline{\rho}$ *has no quotient of order* ℓ.

(vi) $\eta := \det \rho$ *is of finite order,*

Then R^η_X *is finite flat over* $\mathbf{Z}_\ell$.

The proof of this theorem will occupy us in the rest of the paper. Combined with the Galois-theoretic lifting results of [BK1] (Theorem 1.1 and Theorem 2.4 there), the above theorem will easily imply Theorem 1.6 as we see at the very end (see proof of Theorem 4.1).

Note that if $\mathrm{ad}^0(\overline{\rho})$ is (absolutely) irreducible, then so is $\overline{\rho}$. So when we require both assumptions, we only state the former.

Let us fix the following notation for this chapter: For a place v of $\widetilde{X}$ we denote by K_v, A_v, $\mathfrak{M}_v$, k_v and q_v the completion of the function field K of X at v, its ring of integers, the maximal ideal of the latter, its residue field and the cardinality of the latter, respectively. Let $\mathbf{A} = \mathbf{A}_K$ be the adeles over K. The symbols F, $\mathcal{O}$, $\mathbf{F}$, and $\mathfrak{m}$ will denote a finite sufficiently large extension of $\mathbf{Q}_\ell$, its ring of integers, its residue field and the maximal ideal of $\mathcal{O}$, respectively. In the definitions to come, Λ stands for either of the three rings F, $\mathcal{O}$ or $\mathbf{F}$.

Note again that we have chosen a place $w \in X$ and a splitting s_w as in Lemma 2.1 and in the short exact sequence (1). To this splitting corresponds

the choice of a uniformizer π_w of K_w unique up to multiplication by $1+\mathfrak{M}_w$. From now on v will always a place of K different from w.

Let $\overline{U}_0(k_v) \subset \mathrm{GL}_n(k_v)$ be the maximal parabolic which fixes the subspace $e_1 k_v$ and define $U_0(v) := \{g \in \mathrm{GL}_n(A_v) : g \pmod{\mathfrak{M}_v} \in \overline{U}_0(v)\}$. For $\bar{g} \in \overline{U}_0(k_v)$ denote by $a_{11}(\bar{g})$ its $(1,1)$-entry.

Definition 3.2 *For a character $\chi_v : k_v^* \to \Lambda^*$, we denote by $I_1(\chi_v)$ the 1-dimensional representation of $U_0(v)$ defined by*

$$U_0(v) \xrightarrow{(\mathrm{mod}\ \mathfrak{M}_v)} \overline{U}_0(k_v) \xrightarrow{a_{11}} k_v^* \xrightarrow{\chi_v} \Lambda^*.$$

We define $U_{1,m}(v) := \{g \in U_0(v) : a_{11}(g \pmod{\mathfrak{m}}) \in k_v^{*\ell^m}\}$, so that $U_{1,m}(v) \subset \ker(I_1(\chi_v)) \subset U_0(v)$ for any character χ_v of order dividing ℓ^m.

At w We also define the compact open group $U_d(w)$ as the kernel of the composite

$$GL_n(A_w) \overset{\mathrm{mod}\,\mathfrak{M}_w}{\longrightarrow\!\!\!\!\rightarrow} \mathrm{GL}_n(k_w) \overset{\det}{\longrightarrow\!\!\!\!\rightarrow} k_w^* \longrightarrow\!\!\!\!\rightarrow k_w^*/(k_w^{*\ell}).$$

3.1 Automorphic forms over function fields

Our next aim is to define spaces of cusp forms on $\mathrm{GL}_n(\mathbf{A})$.

In the sequel we will often work under the following hypothesis:

Assumption 3.3

- *T is a finite subset of $X \setminus \{w\}$,*
- *$\omega : \mathrm{GL}_1(\mathbf{A}) \to \Lambda^*$ is a character of finite order, unramified outside w, and trivial on $\pi_w^{\mathbf{Z}}(1+\mathfrak{M}_w)k_w^{*\ell}K^*$. (with π_w the uniformizer chosen above.)*
- *for $v \in T$, $\chi_v : k_v^* \to \Lambda^*$ is a character of ℓ-power order ℓ^{m_v}, which may be trivial*

The above set-up will be of use in two different instances, namely in lowering the level of an automorphic cusp form associated to a residual Galois representation and in constructing Taylor-Wiles systems. In the first case, we will use the above notation as stated, in the second, the set T will be denoted by Q or Q_m.

Using the chosen uniformizer $\pi_w \in K_w$ corresponding to s_w, we define for any $m \in \mathbf{N}_0$

$$Z_T^m := K^*\Big(\pi_w^{\mathbf{Z}}(1+\mathfrak{M}_w)k_w^{*\ell} \times \prod_{v\in T}(1+\mathfrak{M}_v)k_v^{*\ell^m} \times \prod_{v\notin T\cup\{w\}} A_v^*\Big).$$

For any $m \in \mathbf{N}$ and any finite (possibly empty) $T \subset X \setminus \{w\}$ we define a compact open subgroup of $\mathrm{GL}_n(\mathbf{A})$ by

$$U_T^m \;:=\; U_d(w) \times \prod_{v\in T} U_{1,m}(v) \times \prod_{v\notin T\cup\{w\}} \mathrm{GL}_n(A_v) \subset \mathrm{GL}_n(\mathbf{A})$$

Under the hypothesis of Assumption 3.3, and for $m \geq \max\{m_v : v \in T\}$, we define $\mathbf{C}_{cusp,T}^{\omega,(\chi_v)}(\Lambda)$ as the space of all functions

$$f\colon \mathrm{GL}_n(K)\backslash\mathrm{GL}_n(\mathbf{A})/U_T^m \to \Lambda$$

with the following properties:

(i) The central action of Z_T^m on f is described by ω,

(ii) for $v \in T$ the right action of $U_0(v)$ on $f(g\cdot\_)$ is via the character $I_1(\chi_v)$, and

(iii) f is cuspidal (cf. [BJ], § 5).

Note that the conditions do completely determine the central action of A_v^*. We define the analogous space $\mathbf{C}_{c,T}^{\omega,(\chi_v)}(\Lambda)$ with the last condition replaced by compact support mod center. By a result of Harder we have an inclusion $\mathbf{C}_{cusp,T}^{\omega,(\chi_v)}(\Lambda) \subset \mathbf{C}_{c,T}^{\omega,(\chi_v)}(\Lambda)$

For any $m \in \mathbf{N}_0$ we define a second space of functions $\mathbf{C}_{cusp,T}^{\omega,m}(\Lambda)$ as the space of all functions

$$f\colon \mathrm{GL}_n(K)\backslash\mathrm{GL}_n(\mathbf{A})/U_T^m \to \Lambda$$

such that for $z \in Z_T^m$ one has $f(zg) = \omega(z)f(g)$, and f is cuspidal. If instead of cuspidal we consider functions that are compact mod center we denote the corresponding space by $\mathbf{C}_{c,T}^{\omega,m}(\Lambda)$.

The following is an immediate consequence of the above definitions:

Proposition 3.4 *Assume that F contains ζ_{ℓ^m}. Then for any $m \in \mathbf{N}_0$*

$$\mathbf{C}^{\omega,m}_{cusp,T}(F) \cong \bigoplus_{(\chi'_v)} \mathbf{C}^{\omega,(\chi'_v)}_{cusp,T}(F),$$

and

$$\mathbf{C}^{\omega,m}_{c,T}(F) \cong \bigoplus_{(\chi'_v)} \mathbf{C}^{\omega,(\chi'_v)}_{c,T}(F),$$

where the (χ'_v) range over all characters of $\Pi_{v\in T}\frac{U_0(v)}{U_{1,m}(v)}$.

Proposition 3.5 *Let $M(\mathcal{O})$ be any of the spaces $\mathbf{C}^{\omega,(\chi_v)}_{cusp,T}(\mathcal{O})$, $\mathbf{C}^{\omega,(\chi_v)}_{c,T}(\mathcal{O})$, $\mathbf{C}^{\omega,m}_{cusp,T}(\mathcal{O})$ or $\mathbf{C}^{\omega,m}_{c,T}(\mathcal{O})$.*

(i) The spaces $M(\mathcal{O})$ are free and when we consider the cuspidal space they are also finitely generated over $\mathcal{O}$.

(ii) The induced morphism $M(\mathcal{O}) \otimes_{\mathcal{O}} \mathbf{F} \to M(\mathbf{F})$ is injective.

PROOF: The modules $\mathbf{C}^{\omega,(\chi_v)}_{c,T}(\mathcal{O})$ and $\mathbf{C}^{\omega,m}_{c,T}(\mathcal{O})$ of compactly supported functions may be viewed as functions on an infinite (discrete) set. Hence they are free $\mathcal{O}$-modules. The other two are submodules of these, and thus they are free as well. This proves (i).

For (ii) note that the argument given in (i) shows that for the spaces describing compactly supported functions the morphism in question is an isomorphism. Since cuspidality is preserved under the reduction map $\mathcal{O} \to \mathbf{F}$ the injectivity also follows in the remaining cases. ∎

By definition, cf. [BJ], one has a smooth admissible automorphic representation $\Pi(f)$ of $\mathrm{GL}_n(\mathbf{A})$ attached to an automorphic form f for GL_n (simply given by $\Lambda[\mathrm{GL}_n(\mathbf{A})]f$). The local constituents of $\Pi(f)$ are denoted $\Pi_v(f)$, so that $\Pi(f) \cong \hat{\otimes}_v \Pi_v(f)$. Conversely, if Π is a smooth admissible cuspidal automorphic representation and U a compact open subgroup of $\mathrm{GL}_n(\mathbf{A})$, then Π^U is a (possibly empty) space of cusp forms.

3.2 Hecke-algebras

For $v \notin T \cup \{w\}$ we define the spherical Hecke algebra $\mathcal{H}_v$ as the algebra of bi-$\mathrm{GL}_n(A_v)$-invariant locally constant compactly supported functions on $\mathrm{GL}_n(K_v)$ with values in $\mathbf{Z}_\ell$, and where multiplication is given by convolution. The algebra $\mathcal{H}_v$ contains naturally defined elements $T_{v,i}$, $i = 1, \ldots, n$, the Hecke-operators at v, and the Satake isomorphism asserts that

$$\mathcal{H}_v \cong \mathbf{Z}_\ell[T_{v,1}, \ldots, T_{v,n}, T_{v,n}^{-1}].$$

For $v \in T$ (T might be empty) and $m_v \in \mathbf{N}_0$, we follow [HT2], Ch. II (there is no difference between the function and the number field case here): So we denote by $V_{v,i}$, $i = 1, \ldots, n-1$, the Hecke-operators in the convolution algebra of $U_{1,m_v}(v)$-bi-invariant locally constant compactly supported functions on $\mathrm{GL}_n(K_v)$ with values in $\mathbf{Z}_\ell$, defined as in [HT2], (II.2.2). By $V_{v,n}$ we denote the *U-operator* from [HT2], II.2.4, which again lies in the above convolution algebra. (We choose the notation $V_{v,n}$, to avoid any conflict with our notation for compact opens.) The commutative subalgebra generated over $\mathbf{Z}_\ell$ by the $V_{v,i}$, $i = 1, \ldots, n$, is denoted by $\mathcal{H}_v^{m_v}$. We consider Hecke action at places in T only when building Taylor-Wiles systems.

To obtain a Hecke action at almost all places (namely outside w), we set

$$\mathcal{H}_T^{ab,m:} = \bigotimes_{v \in T} \mathcal{H}_v^m \otimes \bigotimes_{v \notin \{w\} \cup T} \mathcal{H}_v.$$

This Hecke algebra acts on the spaces of cusp forms $\mathbf{C}_{cusp,T}^{\omega,(\chi_v)}(\Lambda)$, $\mathbf{C}_{cusp,T}^{\omega,m}(\Lambda)$ and the analogous (much larger, infinite-dimensional) space of functions that are compact mod center. For $m \geq \max\{m_v : v \in T\}$, we define $\mathcal{H}_T^m(\Lambda)$, resp. $\mathcal{H}_T^{(\chi_v)}(\Lambda)$ as the image of $\mathcal{H}_T^{ab,m} \otimes_{\mathbf{Z}} \Lambda$ in the endomorphism ring of $\mathbf{C}_{cusp,T}^{\omega,m}(\Lambda)$, resp. $\mathbf{C}_{cusp,T}^{\omega,(\chi_v)}(\Lambda)$. Also define $\mathcal{H}_{c,T}^m(\Lambda)$ and $\mathcal{H}_{c,T}^{(\chi_v)}(\Lambda)$ as the image of $\mathcal{H}_T^{ab,m} \otimes_{\mathbf{Z}} \Lambda$ in the endomorphism ring of $\mathbf{C}_{c,T}^{\omega,m}(\Lambda)$ and $\mathbf{C}_{c,T}^{\omega,(\chi_v)}(\Lambda)$. Because $\mathbf{C}_{cusp,T}^{\omega,m}(\Lambda)$ is a free Λ-module of finite rank, the same holds for $\mathcal{H}_T^m(\Lambda)$ and $\mathcal{H}_T^{(\chi_v)}(\Lambda)$ and one has $\mathcal{H}_T^m(F) \cong \mathcal{H}_T^m(\mathcal{O}) \otimes_{\mathcal{O}} F$ and $\mathcal{H}_T^{(\chi_v)}(F) \cong \mathcal{H}_T^m(\mathcal{O}) \otimes_{\mathcal{O}} F$. (Although $\mathbf{C}_{c,T}^{\omega,m}(\Lambda)$ is *not* a free Λ-module of finite rank, we still have $\mathcal{H}_{c,T}^m(F) \cong \mathcal{H}_{c,T}^m(\mathcal{O}) \otimes_{\mathcal{O}} F$.)

We state the main theorem of [Laf]:

Theorem 3.6 ([Laf]) *For any finite subset T of X, there is a bijection between*

- *smooth irreducible cuspidal automorphic representations* Π *whose central character is of finite order and with* Π_v *unramified for* $v \notin \{w\} \cup T$, *and*

- *irreducible continuous representations* $\rho\colon \pi_1(X \setminus (\{w\} \cup T)) \to \mathrm{GL}_n(\overline{\mathbf{Q}}_\ell)$ *with determinant of finite order.*

Suppose that for Π *as above, the eigenvalues of the operators* $T_{v,i}$, $v \notin \{w\} \cup T$, $i = 1, \ldots, n$, *are* $\alpha_{v,i}$ *(and* $\alpha_{v,0} = 1$*). Then the correspondence is given by the condition*

$$\det\Big(1 - x\rho(\mathrm{Frob}_v)\Big) = \sum_{i=0}^{n} x^{n-i}\alpha_{v,i}. \tag{4}$$

Suppose we are given $\rho\colon \pi_1(X \setminus \{w\} \cup T) \to \mathrm{GL}_n(\mathcal{O})$ with absolutely irreducible residual representation $\overline{\rho}$. Let Π be the corresponding automorphic representation. By the relation (4) the Hecke-eigenvalues $\alpha_{v,i}$, $v \notin \{w\} \cup T$, $i \in 1, \ldots, n$, lie in $\mathcal{O}$, and so they define ring-homomorphisms

$$\mathcal{H}_v \to \mathbf{F} : T_{v,i} \mapsto \ \alpha_{v,i} \pmod{\mathfrak{m}}$$

for $v \notin \{w\} \cup T$.

For $v \in T$ the representation Π_v satisfies $\Pi_v^{U_{1,m_v}(v)} \neq 0$. If this is 1-dimensional then $U_0(v)$ acts on it by a character χ_v. If this character is non-trivial, then Π_v is principal series. (If the dimension is bigger than 1 then Π_v is unramified.)

If $\overline{\rho}$ is unramified at v with n distinct eigenvalues and if $\bar{\lambda}$ is the eigenvalue at the $(1,1)$-entry (this will be the case when the only time we need to consider the Hecke action at T which is when building TW systems), then by [HT2] one has two cases:

1. If Π_v is unramified, then $\dim \Pi_v^{U_{1,m_v}} = n$, the action of $V_{v,n}$ on this space is semisimple, it has a unique eigenvalue which reduces to $\bar{\lambda}$ and the corresponding eigenspaces is 1-dimensional; this 1-dimensional subspace is also an eigenspace for the operators $V_{v,i}$, $i = 1, \ldots, n-1$. The corresponding eigenvalues are denoted $b_{v,i}$ and their mod $\mathfrak{m}$ reductions depend only on $\overline{\rho}(\mathrm{Frob}_v)$.

2. If Π_v is ramified, then $\dim \Pi_v^{U_{1,m_v}} = 1$, and if, we denote by $b_{v,i}$ the eigenvalues for the Hecke-operators $V_{v,i}$, $i = 1, \ldots, n$, their reductions modulo $\mathfrak{m}$ depend only on $\overline{\rho}(\mathrm{Frob}_v)$ (and by the same formulas as in the first

case). Moreover the reduction of $b_{v,n}$ is $\bar{\lambda}$. In either case one obtains a ring homomorphism

$$\mathcal{H}_v^{m_v} \to \mathbf{F} : V_{v,n} \mapsto \bar{\lambda}, V_{v,i} \mapsto b_{v,i} \pmod{\mathfrak{m}} \ (i = 1, \ldots, n-1).$$

The above homomorphisms induce a ring homomorphism $\mathcal{H}_T^{ab,m} \to \mathbf{F}$ whose kernel is a maximal ideal which we denote by $\mathfrak{m}_{\overline{\rho}}$. This notation is justified because the homomorphism depends only on data defined in terms of $\overline{\rho}$. We also denote by $\mathfrak{m}_{\overline{\rho}}$ the image of this ideal in $\mathcal{H}_T^m(\mathcal{O})$, $\mathcal{H}_T^{(\chi_v)}(\mathcal{O})$, $\mathcal{H}_{c,T}^m(\mathcal{O})$ and $\mathcal{H}_{c,T}^{(\chi_v)}(\mathcal{O})$. (Since a priori there is no relation between $\overline{\rho}$ and $\mathbf{C}_{cusp,T}^{\omega,m}(\mathcal{O})$, this image can be all of $\mathcal{H}_T^m(\mathcal{O})$.) For an $\mathcal{H}_T^m$-module M, we denote by $M_{\mathfrak{m}_{\overline{\rho}}}$ its localization at $\mathfrak{m}_{\overline{\rho}}$.

The following theorem is crucial to us, and is proved by David Ogilvie [Ogilvie] in his Chicago thesis. (The referee had also sketched a possible approach to proving the result.)

Theorem 3.7 *(Ogilvie) Compatible with the Hecke action of $\mathcal{H}_T^m$ we have isomorphisms $\mathbf{C}_{cusp,T}^{\omega,(\chi_v)}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}} \simeq \mathbf{C}_{c,T}^{\omega,(\chi_v)}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}$ and $\mathbf{C}_{cusp,T}^{\omega,m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}} \simeq \mathbf{C}_{c,T}^{\omega,m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}$ (and the same statement after dropping the Hecke operators at T).*

3.3 Carayol's principle

The methods of this section, which allow us to change "types" of automorphic forms which give rise to a given $\overline{\rho}$, use a principle discovered by Carayol that occurs in the proof of [Ca] Lemme 1.

We define $N_n(\ell)$ as the order of an ℓ-Sylow subgroup of $\mathrm{GL}_n(k)$.

We may consider the Hecke action without the operators at places in T and will denote the induced maximal ideal of this smaller Hecke algebra by the same symbol.

Lemma 3.8 *We assume the set-up of Assumption 3.3 for sets of characters (χ_v) and (χ'_v) such that*

- *Λ is the fraction field F of $\mathcal{O}$,*
- *for each $v \in T$, the product of $N_n(\ell)$ with the order of $\chi_v^{-1}\chi'_v$, which we assume is a power of ℓ, divides the order of k_v^*.*

Then

$$\mathrm{rank}_{\mathcal{O}}\mathbf{C}^{\omega,(\chi_v)}_{cusp,T}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}} = \mathrm{rank}_{\mathcal{O}}\mathbf{C}^{\omega,(\chi'_v)}_{cusp,T}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}$$

(and the same conclusion holds if we consider the corresponding maximal ideal of the smaller Hecke algebra without the operators at the places in T).

Localization at $\mathfrak{m}_{\overline{\rho}}$ commutes with reduction $\mathcal{O} \to \mathbf{F}$ of the ring of integers of F to its residue field. Furthermore, after reduction on has $\chi_v \equiv \chi'_v \equiv 1$ in $\mathbf{F}$ for all $v \in T$. So in view of Proposition 3.5(i)-(ii) and Theorem 3.7 due to Ogilvie, it suffices to prove the following

Lemma 3.9 *Suppose the hypothesis of Lemma 3.8 hold. Then the submodules $\mathbf{C}^{\omega,(\chi_v)}_{c,T}(\mathcal{O}) \otimes_{\mathcal{O}} \mathbf{F}$ and $\mathbf{C}^{\omega,(\chi'_v)}_{c,T}(\mathcal{O}) \otimes_{\mathcal{O}} \mathbf{F}$ of $\mathbf{C}^{\omega,m}_{c,T}(\mathbf{F})$ agree.*

Proof: By Z we denote the center of GL_n, viewed as an algebraic group over K and we regard Z^m_T as a subgroup of $Z(\mathbf{A})$. Because of the central action and the conditions on the places $v \in T$, elements in $\mathbf{C}^{\omega,(\chi_v)}_{c,T}(\mathcal{O})$ may be thought of as functions with finite support and values in $\mathcal{O}$ on the infinite set $\mathrm{GL}_n(K)Z^m_T\backslash\mathrm{GL}_n(\mathbf{A})/U^0_T$. Choose $g_j \in \mathrm{GL}_n(\mathbf{A})$, $j \in J$, such that

$$\mathrm{GL}_n(\mathbf{A}) = \coprod_{j\in J} \mathrm{GL}_n(K)Z^m_T g_j U^m_T.$$

Let $\mathcal{O}((\chi_v))$ denote $\mathcal{O}$ with the compatible action via ω and the χ_v by $Z^m_T U^0_T/U^m_T Z(K)$. Then $\mathbf{C}^{\omega,(\chi_v)}_{c,T}(\mathcal{O})$ can also be identified with elements of the direct sum $\bigoplus_{j\in J}\mathcal{O}((\chi_v))^{\mathrm{GL}_n(K)\cap Z^m_T g_j^{-1}U^m_T g_j}$, because in addition to the actions by ω and the χ_v, the component at g_j also carries a trivial action by $\mathrm{GL}_n(K)$. We have analogous descriptions for forms with $\mathbf{F}$-coefficients, and for the space $\mathbf{C}^{\omega,(\chi'_v)}_{c,T}(\Lambda)$ with $\Lambda \in \{\mathcal{O}, \mathbf{F}\}$.

Since we prefer to work with the action of the finite group $Z^m_{T,0}/Z(K)\pi^{\mathbf{Z}}_w$, we observe that elements in $\mathbf{C}^{\omega,\ldots}_{c,T}(\ldots)$ may be regarded as functions on the set $\mathrm{GL}_n(\mathbf{A})/Z(K)\pi^{\mathbf{Z}}_w$. By Lemma 3.10 below, the ℓ-part of the exponents of (the finite groups) $(\mathrm{GL}_n(K)\pi^{\mathbf{Z}}_w \cap Z^m_{T,0}g_j^{-1}U^m_T g_j)/Z(K)\pi^{\mathbf{Z}}_w$ divide $N_n(\ell)$ for all j. Using the second hypothesis of Lemma 3.8 we have

$$\mathcal{O}((\chi_v))^{\mathrm{GL}_n(K)\cap Z^m_T g_j U^m_T g_j^{-1}} \cong \mathcal{O}((\chi'_v))^{\mathrm{GL}_n(K)\cap Z^m_T g_j^{-1}U^m_T g_j}$$

for all $j \in J$. Hence for each $j \in J$ either this set is zero, or agrees with $\mathcal{O}$. This completes the proof of Lemma 3.9. ∎

Lemma 3.10 *If $\gamma \in \mathrm{GL}_n(K)/K^*$ is of ℓ-power order, its order divides $N_n(\ell)$.*

PROOF: We have the exact sequence

$$0 \longrightarrow \mathrm{SL}_n(K)/\{x \in K^* : x^n = 1\} \longrightarrow \mathrm{GL}_n(K)/K^* \longrightarrow K^*/K^{*n} \longrightarrow 0.$$

Because the image of γ in K^*/K^{*n} is of ℓ-power order, it must lie in k^*/k^{*n}. Because ℓ is prime to n, the order of this image divides the order of the ℓ-Sylow of k^*. Say the latter order is n_ℓ. Then γ^{n_ℓ} lies in $\mathrm{SL}_n(K)/\{x \in K^* : x^n = 1\}$. Again because n is prime to ℓ, there is an element $\gamma' \in \mathrm{SL}_n(K)$ which maps to γ^{n_ℓ} and whose order is the same as that of γ^{n_ℓ}. Thus it suffices to show that if $\gamma' \in \mathrm{SL}_n(K)$ is of ℓ-power order ℓ^d, then the order of γ' divides the order of an ℓ-Sylow of $\mathrm{SL}_n(k)$.

Let k' be the smallest extension of k which contains a primitive ℓ^d-th root of unity. We assume that γ' is given in rational canonical form over K. We claim that γ' has entries in k. For this we may assume that the rational canonical form consists of a single block, which is thus completely determined by the characteristic polynomial of γ'. But the characteristic polynomial has coefficients in k' and in K and thus in k. Hence γ' has coefficients in k. Thus γ' lies up to conjugation in $\mathrm{SL}_n(k)$, and our last assertion is shown. ∎

3.4 Taylor Wiles systems

Throughout this section, we fix a lift $\rho\colon \pi_1(X) \to \mathrm{GL}_n(\mathcal{O})$ of $\overline{\rho}$ and make the following assumption:

Assumption 3.11 *$\eta := \det \rho$ is of finite order.*

For each $m \in \mathbf{N}$ we also fix a finite subset $Q_m \subset X \setminus \{w\}$ of places such that for all $v \in Q_m$ the matrix $\overline{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues and $q_v \equiv 1 \pmod{\ell^m}$. In this section we will complement the Galois theoretic work in Section 2 by automorphic results that together yield the existence of Taylor-Wiles systems.

Define Δ_m as the maximal quotient of $\prod_{v \in Q_m} k_v^*$ of exponent ℓ^m. Via the projection onto the $(1,1)$-entry, we identify

$$\Delta_m \cong \prod_{v \in Q_m} U_0(v)/U_{1,m}(v).$$

There is a natural ("diamond") action of Δ_m on the spaces $\mathbf{C}^{\omega,m}_{cusp,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}$ and $\mathbf{C}^{\omega,m}_{c,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}$. Using Lemma 3.9 and its proof, we easily show:

Proposition 3.12 *We fix a positive integer m and assume the set-up of Assumption 3.3, with*

(a) the set of places Q_m here playing the role of T there,

(b) Λ a discrete valuation ring $\mathcal{O}$ containing $W(\mathbf{F})[\zeta_{\ell^m}]$,

(c) $\ell^m N_n(\ell)$ dividing the order of k_v^* for all $v \in Q_m$.

Then $\mathbf{C}^{\omega,m}_{cusp,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}$ is free over $\mathcal{O}[\Delta_m]$, and for the invariants under Δ_m one has

$$\left(\mathbf{C}^{\omega,m}_{cusp,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}\right)^{\Delta_m} = \mathbf{C}^{\omega,0}_{cusp,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}.$$

Note that by Proposition 3.4, one has the isomorphism

$$\mathbf{C}^{\omega,m}_{cusp,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}} \otimes F \cong \bigoplus_{(\chi'_v)} \mathbf{C}^{\omega,(\chi'_v)}_{cusp,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}} \otimes F,$$

where the sum is over all characters of (χ'_v) of Δ_m.

Proof: The second assertion is obvious from the definitions. To prove the first, observe that because localization at $\mathfrak{m}_{\overline{\rho}}$ commutes with the action of Δ_m and because of Theorem 3.7, it will suffice to show that $\mathbf{C}^{\omega,m}_{c,Q_m}(\mathcal{O})$ is free over $\mathcal{O}[\Delta_m]$. This follows easily (see proof of Proposition 5.6.1 of [CDT]) from the fact that for all characters (χ_v) of Δ_m, we have $\mathbf{C}^{\omega,(\chi_v)}_{c,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}} \otimes F$ is of the same rank independent of (χ_v) as follows from Lemma 3.9. ∎

We now define universal deformation and Hecke rings corresponding to the above situation.

Choose for each $v \in Q_m$ a Teichmüller lift λ_v of one of the eigenvalues of $\overline{\rho}(\mathrm{Frob}_v)$. Write $\underline{\lambda}$ for $(\lambda_v)_{v\in Q_m}$. Let

$$\rho^{m,\underline{\lambda}}_{X,Q_m} : \pi_1(X \setminus (\{w\} \cup Q_m)) \to \mathrm{GL}_n(R^{m,\underline{\lambda}}_{X,Q_m})$$

denote the universal deformation that parameterizes deformations $\tilde{\rho}\colon \pi_1(X \setminus (\{w\} \cup Q_m)) \to \mathrm{GL}_n(R)$, $R \in \mathcal{A}$, R an $\mathcal{O}$-algebra, of $\overline{\rho}$ such that

- $\det \tilde{\rho}_w$ factors via $G_w \xrightarrow{s_w} \overline{I}_w$ and $\tilde{\rho}_w \otimes (\det \tilde{\rho}_w)^{-1/n}$ is unramified,

- for all $v \in Q_m$, ρ_v is of type $\mathcal{C}_{v,\lambda_v,m}$ as defined above Lemma 2.7.

Note also that from the local conditions at $v \in Q_m$, via the action of I_v one obtains a homomorphism $\mathcal{O}[\Delta_m] \to R^{m,\underline{\lambda}}_{X,\underline{Q}_m}$.

We define $\omega : \mathrm{GL}_1(\mathbf{A}) \to \mathcal{O}^*$ as the Hecke-character corresponding to $\eta = \det \rho$. For $v \in T$ we let $\chi_v : k_v^* \to \mathcal{O}^*$ be the trivial character. Then the above data satisfies Assumption 3.3 for $\Lambda = \mathcal{O}$. Suppose a basis of A_v^n is chosen in such a way that $e_{1,v}$ corresponds to the eigenvalue λ_v. We now define

$$\mathbf{T}^{m,\underline{\lambda}}_{X,\underline{Q}_m} := (\mathcal{H}^m_{Q_m}(\mathcal{O}))_{\mathfrak{m}_{\overline{\rho}}}.$$

Let $\tau_1, \ldots, \tau_s$ be a list of the Galois representations corresponding via Lafforgue's theorem to eigenforms in $\widetilde{\mathbf{C}}^{\omega,m}_{S,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}$. By choice of the maximal ideal and definition of the Hecke action at places in Q_m, using the $\mathbf{C}$-valued theory one finds that the algebra $\mathbf{T}^{m,\underline{\lambda}}_{X,\underline{Q}_m} \otimes_{\mathcal{O}} F$ is semisimple, cf. [HT2], (III.2), second paragraph. We therefore denote by

$$\tau := \tau_1 \oplus \ldots \oplus \tau_s \colon \pi_1(X \setminus Q_m) \longrightarrow \mathrm{GL}_n(\mathbf{T}^{m,\underline{\lambda}}_{X,\underline{Q}_m} \otimes_{\mathcal{O}} F)$$

the corresponding Galois representation.

Proposition 3.13 *The representation τ can be written as the composition of representations*

$$\pi_1(X \setminus Q_m) \overset{\tau^{m,\underline{\lambda}}_{X,\underline{Q}_m}}{\longrightarrow} \mathrm{GL}_n(\mathbf{T}^{m,\underline{\lambda}}_{X,\underline{Q}_m}) \hookrightarrow \mathrm{GL}_n(\mathbf{T}^{m,\underline{\lambda}}_{X,\underline{Q}_m} \otimes_{\mathcal{O}} F).$$

Proof: Because $\overline{\rho}$ is absolutely irreducible, the image of τ lies in the ring of traces. By the Čebotarev density theorem, this ring is spanned by the coefficients of the characteristic polynomials of

$$\tau(\mathrm{Frob}_v), v \notin \{w\} \cup Q_m.$$

Thus by Lafforgue's theorem, it is spanned by the Hecke-eigenvalues of the corresponding eigenforms. Thus the ring of traces lies in $\mathbf{T}^{m,\underline{\lambda}}_{X,\underline{Q}_m}$. ∎

From the definition of $\tau^{m,\underline{\lambda}}_{X,\underline{Q}_m}$ it is clear that it is a representation of the type parameterized by $\rho^{m,\underline{\lambda}}_{X,\underline{Q}_m}$. By universality there arises a unique morphism $R^{m,\underline{\lambda}}_{X,\underline{Q}_m} \to \mathbf{T}^{m,\underline{\lambda}}_{X,\underline{Q}_m}$ such that $\tau^{m,\underline{\lambda}}_{X,\underline{Q}_m}$ is induced from $\rho^{m,\underline{\lambda}}_{X,\underline{Q}_m}$. Both rings are non-zero because of the existence of ρ.

Proposition 3.14 *The induced morphism $R^{m,\underline{\lambda}}_{X,\underline{Q}_m} \to \mathbf{T}^{m,\underline{\lambda}}_{X,\underline{Q}_m}$ is surjective.*

PROOF: By Nakayama's lemma it suffices to prove the assertion modulo $\mathfrak{m}$. It is clear from the Langlands correspondence that the reductions modulo $\mathfrak{m}$ of the Hecke-operators $T_{v,i}$, $v \notin \{w\} \cup T$, and $T'_{w,i}$, $i = 1, \ldots, n$, lie in the image. At places $v \in T$ this again follows from the compatibility of the global Langlands correspondence with the local one, and the explicit decription of the Hecke action at places in T, cf. [HT2] (V.1.5). Namely, the action of $V_{v,n} \pmod{\mathfrak{m}}$ is given by the first eigenvalue $\bar{\lambda}$ of $\overline{\rho}(\mathrm{Frob}_v)$ and the action of $V_{v,i} \pmod{\mathfrak{m}}$, $i = 1, \ldots, n-1$, by the elements $b_{v,i} \pmod{\mathfrak{m}}$ which are expressions in the elementary symmetric polynomials in the remaining eigenvalues of $\overline{\rho}(\mathrm{Frob}_v)$. So in this case, too, the reductions of the Hecke-operators lie in the image of $R^{m,\underline{\lambda}}_{X,\underline{Q}_m}$. ∎

If $Q_m = \emptyset$, we drop it as well as m and $\underline{\lambda}$ from the notation, and add a superscript zero, i.e., the above morphism becomes $R^0_X \to \mathbf{T}^0_X$. We have the following central result:

Theorem 3.15 *Suppose that Assumption 3.11 and the following conditions hold*

(i) For any $\pi_1(X)$-subrepresentation V of $\mathrm{ad}(\overline{\rho})$, there exists a regular semisimple $g_V \in \overline{\rho}(\pi_1(\overline{X}))$ such that $V^{g_V} \neq 0$.

(ii) If $\zeta_\ell \in K$, then $\mathrm{ad}^0(\overline{\rho})$ has no 1-dimensional subrepresentation,

(iii) If $\zeta_\ell \in E$, then $H^1(\mathrm{Gal}(E/K(\zeta_\ell), \mathrm{ad}^0(\overline{\rho})) = 0$.

(iv) $\mathrm{im}(\overline{\rho})$ contains no normal subgroup of index ℓ.

Then $R^0_X \to \mathbf{T}^0_X$ is an isomorphism.

PROOF: The proof is based on the use of Taylor-Wiles system in the improved form due independently to F. Diamond and K. Fujiwara, cf. [Di] and [F]. For each $m \in \mathbf{N}$, use Lemma 2.8 to choose a set $Q_m \subset X$ such that

(a) $\#Q_m = d := \dim H^1_{\{L_v\}}(\{w\}, \mathrm{ad}(\overline{\rho})(1))$

(b) $q_v \equiv 1 \pmod{N_n(\ell)\ell^m}$ for all $v \in Q_m$,

(c) $\overline{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues for each $v \in Q_m$, and

(d) $H^1_{\{L_v^\perp\}}(\{w\} \cup Q_m, \mathrm{ad}(\overline{\rho})) = 0$ where $L_v = L_{v,\lambda_v}$ for each $v \in Q_m$ and λ_v is the Teichmüller lift of some eigenvalue of $\overline{\rho}(\mathrm{Frob}_v)$.

Note that $\dim H^1_{\{L_v\}}(\{w\}, \mathrm{ad}(\overline{\rho})) = \dim H^1_{\{L_v\}}(\{w\} \cup Q_m, \mathrm{ad}(\overline{\rho}))$, and define $\underline{\lambda}_m$ as $(\lambda_v)_{v \in Q_m}$.

We introduce notation similar to [Di], §2. Define

$$\begin{aligned}
\mathbf{R} &:= R^0_X/\mathfrak{m},\ \mathbf{T} := \mathbf{T}^0_X/\mathfrak{m}, \\
\mathbf{R}_m &:= R^{m,\underline{\lambda}_m}_{X,Q_m}/\mathfrak{m},\ \mathbf{T}_m := \mathbf{T}^{m,\underline{\lambda}_m}_{X,Q_m}/\mathfrak{m}, \\
\mathbf{H} &:= \mathrm{Hom}_{\mathcal{O}}(\widetilde{\mathbf{C}}^{0,\omega}_{S,\emptyset}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}, \mathbf{F}), \\
\mathbf{H}_m &:= \mathrm{Hom}_{\mathcal{O}}(\widetilde{\mathbf{C}}^{m,\omega}_{S,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}, \mathbf{F}), \\
\mathbf{A}_m &:= \mathcal{O}[\Delta_m]/\mathfrak{m} \cong \mathbf{F}[[y_1, \ldots, y_d]]/(y_1, \ldots, y_d)^m
\end{aligned}$$

One easily verifies from the preceding work that

(i) Each $\mathbf{R}_m$ is topologically generated by d elements over $\mathbf{F}$,

(ii) $\mathbf{R}_m/\mathfrak{m}^m_{\mathbf{R}_m} \cong \mathbf{F}[[x_1, \ldots, x_d]]/(x_1, \ldots, x_d)^m$,

(iii) there exists a canonical $\mathbf{R}_m$-linear surjection $\pi_m \colon \mathbf{H}_m \longrightarrow\!\!\!\!\!\rightarrow \mathbf{H}$,

(iv) under $\mathbf{R}_m \longrightarrow\!\!\!\!\!\rightarrow \mathbf{R}$ the image of $(y_1, \ldots, y_d)$ is zero,

(v) $\mathbf{H}_m$ is via $\mathbf{A}_m \to \mathbf{R}_m \to \mathbf{T}_m$ a module over $\mathbf{A}_m$ and $\mathbf{R}_m$ and the action of $\mathbf{A}_m$ is the same as that which occurs in Proposition 3.12,

(vi) $\mathbf{H}_m$ is free over $\mathbf{A}_m$ (by Proposition 3.12).

We now verify the following assertion that is also a crucial part of constructing Taylor-Wiles systems:

(vii) The morphism π_m induces an isomorphism $\mathbf{H}_m/(y_1, \ldots, y_d) \cong \mathbf{H}$ where we consider these as modules over $R^{m,\underline{\lambda}_m}_{X,Q_m}$.

In view of Proposition 3.12 and the above definitions it suffices to show that we have an isomorphism

$$\mathbf{C}^{\omega,0}_{cusp,\emptyset}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}} \simeq \mathbf{C}^{\omega,0}_{cusp,Q_m}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}} \tag{5}$$

as modules over $R^{m,\underline{\lambda}_m}_{X,Q_m}$. This follows from the arguments in the proofs of [HT2], Prop. (V.2.3) and (V.2.4), and where the isomorphism above is given by the (exact analog of the) map X_{∞,Q_m} of [HT2]. We give some details. As remarked in *loc. cit.* we need to prove the isomorphism in (5) only after tensoring with $\overline{\mathbf{Q}}_\ell$. We first prove that all forms that contribute to the right hand side are old at places in Q_m.

For this let f be a cuspidal Hecke eigenform for GL_n whose image in the RHS of 5 is non-trivial. Let v be in Q_m. As the ℓ-adic representation ρ_f corresponding to f reduces to $\overline{\rho}$ residually, ρ_f restricted to a decomposition group G_v at v is a lift of $\overline{\rho}_v$ to $\mathcal{O}$. By Lemma 2.6 such lifts are diagonalizable and therefore finite on inertia. Hence by the compatibility of the global Langlands correspondence of [Laf] with the local Langlands correspondence and the unramifiedness of the central character at v, $\Pi_v(f)$ is an unramified principal series representation.

We are now in the situation described on page 21 and quoted from [HT2]. The action of $V_{v,n}$ on $\Pi_v(f)^{U_0(v)}$ is diagonalizable and there is exactly one eigenvalues whose reduction modulo $\mathfrak{m}$ is $\lambda_v \pmod{\mathfrak{m}}$, and it has multiplicity one. Therefore after localization at $\mathfrak{m}_{\overline{\rho}}$ at most a one-dimensional subspace of $\Pi_v(f)^{U_0(v)}$ remains. That the remaining space is indeed 1-dimensional follows from the fact that (5) is injective. We have thus completed the proof of (vii).

It now follows from [Di], Thm 2.1, that $\mathbf{R}$ is a complete intersection of dimension zero and $\mathbf{H}$ is free over $\mathbf{R}$. Since the action of $\mathbf{R}$ on $\mathbf{H}$ factors via $\mathbf{T}$, it follows in particular that $\mathbf{R} \to \mathbf{T}$ must be injective and hence an isomorphism.

Let us now come back to the original question. Because $\mathbf{T}^{m,\underline{\lambda}}_{X,Q_m}$ is $\mathcal{O}$-torsion free and finitely generated, the surjection $R^{m,\underline{\lambda}}_{X,Q_m} \longrightarrow\!\!\!\!\!\rightarrow \mathbf{T}^{m,\underline{\lambda}}_{X,Q_m}$ splits as a map of $\mathcal{O}$-modules. By the above its reduction modulo $\mathfrak{m}$ is an isomorphism. But then the morphism itself must be bijective. ∎

3.5 Lowering the level à la Skinner and Wiles

We have the following 'lowering the level' result as in the work of Skinner and Wiles in [SW].

Theorem 3.16 *Suppose* $\rho\colon \pi_1(X \setminus T) \to \mathrm{GL}_n(\mathcal{O})$ *and* $\overline{\rho} := \rho \pmod{\mathfrak{m}}$ *satisfy the following conditions:*

- $\mathcal{O}$ *contains* ζ_ℓ,
- *for all* $v \in T$, ρ *is of type-*1 *and* $\ell N_n(\ell)$ *divides the order of* k_v^*.

Then there exists a representation $\rho'\colon \pi_1(X \setminus T) \to \mathrm{GL}_n(\mathcal{O})$ *such that*

(i) the residual representations of ρ *and* ρ' *agree,*

(ii) $\rho'(I_v)$ *is finite for* $v \in T$.

Remark 3.17 This theorem is referred to as a level lowering result as from it one deduces that there is a solvable base change $Y \to X$, that one can make disjoint from any given covering of X, such that $\rho'|_{\pi_1(Y)}$ has conductor the conductor of $\overline{\rho}|_{\pi_1(Y)}$. We use this in the section that is coming up!

Proof of Theorem 3.16: We use Lafforgue's theorem to convert the above into an assertion about cusp eigenforms that we have proved in Lemma 3.8: Via Lafforgue's theorem, which is compatible with the local Langlands correspondence, ρ corresponds to a cuspidal Hecke eigenform in $\mathbf{C}^{\omega,(\chi_v)}_{cusp,T}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}$. (In this proof we do not need to consider Hecke action at places in T).

Let now (χ'_v) be such that χ'_v is of exact order ℓ at all $v \in T$. By Lemma 3.8 we find a non-zero cuspidal Hecke eigenform f' in $\mathbf{C}^{\omega,(\chi'_v)}_{cusp,T}(\mathcal{O})_{\mathfrak{m}_{\overline{\rho}}}$. Let ρ' be the corresponding Galois representations, which exists by Lafforgue's theorem. The first assertion is clear from the definition of $\mathfrak{m}_{\overline{\rho}}$. At places in T, it follows from the non-triviality of χ'_v, that $\Pi_v(f')$ is ramified principal series (see 21). This shows the second assertion. ∎

4 Proof of main theorems

We can finally give the proof of our central theorem.

Proof of Theorem 3.1: We argue by contradiction, and, in view of Theorem 1.3, assume that there is a representation $\rho'\colon \pi_1(X) \to \mathrm{GL}_n(\mathbf{F}[[x]])$ with $\overline{\rho} = \rho' \pmod{x}$ and $\rho'(\pi_1(\overline{X}))$ infinite. Because ℓ does not divide n, taking n-th roots is an isomorphism on the 1-units in $\mathbf{F}[[x]]^*$. Therefore the n-th

root of the 1-unit part of $\det \rho'$ is a character, say $\tilde{\eta}$, of $\pi_1(X)$. It has the property $\det(\tilde{\eta} \cdot \rho') = \det \overline{\rho}$. Since the image of $\pi_1(\overline{X})$ under any character of $\pi_1(X)$ is finite, we will from now on assume $\det \rho' = \det \overline{\rho}$.

We now consider the ring $R := \ker(\mathcal{O} \oplus \mathbf{F}[[x]] \longrightarrow\!\!\!\!\!\rightarrow \mathbf{F})$. It lies in $\mathcal{A}$ and affords a representation $\rho'' := \rho \oplus \rho' : \pi_1(X) \to \mathrm{GL}_n(R)$ with determinant η. Set $T_i := T$ the set of places at which ρ is of type-1. Take $m \in \mathbf{N}$ such that $\ell N_n(\ell)$ divides $\#k^*_{w,m}$ for all $w \in T_i$. Then Corollary 2.4 applied to ρ'' provides us with a finite Galois covering $Y \to X$ such that

(i) Y is geometrically connected over k.

(ii) $\rho''(\pi_1(Y)) = \rho''(\pi_1(X))$, $\overline{\rho}(\pi_1(\overline{Y})) = \overline{\rho}(\pi_1(\overline{X}))$,

(iii) ρ is unramified at places not above T_i, and

(iv) $\rho_{|G_{w'}}$ is of type-1 and $\ell \cdot N_n(\ell) | \#k^*_{w'}$ for all w' above a place $w \in T_i$.

Since $\rho_{\pi_1(Y)}$ satisfies all the conditions originally imposed on ρ, we may therefore rename Y to X, assume that ρ' is unramified everywhere and has determinant $\det \overline{\rho}$, and that ρ satisfies the following conditions:

(i) $\overline{\rho} := \rho \pmod{\mathfrak{m}}$ is absolutely irreducible,

(ii) $\overline{\rho}(\pi_1(\overline{X}))$ contains a regular semisimple element,

(iii) $\eta := \det \rho$ is of finite order,

(iv) at places v at which ρ ramifies, ρ_v is of type-1 and $\ell N_n(\ell)$ divides $\#k^*_v$.

Condition (iv) allows us to apply Theorem 3.16 on level lowering. Thereby we may replace (iii) by

(iv)' $\rho(I_v)$ is finite at all places where ρ ramifies and $\overline{\rho}$ does not.

By yet another application of Corollary 2.4 to ρ'' with $T_i = \emptyset$, the latter condition may be replaced by

(iv)" ρ'' is unramified at all places.

Recall that R^0_X is universal for deformations of $\overline{\rho}$ to $\mathcal{O}$-algebras in $\mathcal{A}$ which are unramified outside $\{w\}$, and unramified at w after a twist by a character of order ℓ that factors via s_w. Because ρ' is unramified everywhere, there is

a unique morphism $\phi\colon R^0_X \to \mathbf{F}[[x]]$ which induces ρ'. The ring $\mathbf{F}[[x]]$ is of characteristic ℓ and so ϕ factors via $R^0_X/(\ell)$.

On the other hand by Theorem 3.15, which used the technique of Taylor-Wiles systems, the ring R^0_X is finite over $\mathbf{Z}_\ell$. Therefore $R^0_X/(\ell)$ is finite, and this contradicts our assumption that ρ' has infinite image. ∎

When combined with Lemma 2.10 and [BK1], Prop. 2.6, the following result implies Theorem 1.6. (Note that (i) below implies $\ell \nmid n$, and that we are assuming that X is projective which implies that in the situation of Theorem 1.6 the lifting result of [BK1] is available.)

Theorem 4.1 *Suppose* $\overline{\rho}\colon \pi_1(X) \to \mathrm{GL}_n(\mathbf{F})$ *satisfies*

(i) $\mathrm{ad}^0(\overline{\rho})$ *is absolutely irreducible over* $\mathbf{F}_\ell[\mathrm{im}(\overline{\rho})]$,

(ii) if $\zeta_\ell \in E$, *then* $H^1(\mathrm{Gal}(E/K(\zeta_\ell)), \mathrm{ad}^0(\overline{\rho})) = 0$ *and* $\mathrm{ad}^0(\overline{\rho})$ *is absolutely irreducible over* $\mathbf{F}[\overline{\rho}(\pi_1(Z))]$, *where* $Z \to X$ *corresponds to* $K(\zeta_\ell)/K$,

(iii) $\overline{\rho}$ *admits R-places,*

(iv) $\overline{\rho}(\pi_1(\overline{X}))$ *contains a regular semisimple element.*

Then $R^\eta_{\overline{\rho}}$ *is finite over* $\mathbf{Z}_\ell$, *where* η *is the Teichmüller lift of* $\det\overline{\rho}$.

Proof: To prove the assertion on R^η_X we may, as in the preceeding proof, pass from X to a finite Galois cover provided that we preserve all our original hypothesis.

Using (i)–(iii) we obtain from [BK1], Thm. 2.4, a finite set $T \subset X$ and a representation $\rho\colon \pi_1(X \setminus T) \to \mathrm{GL}_n(W(\mathbf{F}))$ such that ρ is of type-1 at places in T.

Suppose now that $\mathrm{im}(\overline{\rho})$ contains a normal subgroup of index ℓ, and let $\pi : Y \to X$ be the corresponding Galois cover of degree ℓ. Because $\ell \nmid n$, the modular representation theory of finite groups shows that $\mathrm{ad}^0(\overline{\rho})$ is still absolutely irreducible over $\overline{\rho}(\pi_1(Y))$. Also (iv) still holds for $\overline{\rho}|_{\pi_1(Y)}$. We claim that (ii) still holds for $\overline{\rho}_{|\pi_1(Z)}$.

So suppose $\zeta_\ell \in E$. By the reasoning given above, $\mathrm{ad}^0(\overline{\rho})$ will still be absolutely irreducible over $\mathbf{F}[\pi_1(Z_Y)]$ for the pullback $Z_Y \to Y$ of $Z \to X$ along $Y \to X$. Let $K'/K(\zeta_\ell)$ be the field extension corresponding to $Z_Y \to Y$. Inflation-restriction yields

$$0 \to H^1(\mathrm{Gal}(K'/K(\zeta_\ell)), \mathrm{ad}^0(\overline{\rho})^{\mathrm{Gal}(E/K')}) \to H^1(\mathrm{Gal}(E/K(\zeta_\ell), \mathrm{ad}^0(\overline{\rho}))$$
$$\to H^1(\mathrm{Gal}(E/K', \mathrm{ad}^0(\overline{\rho}))^{\mathrm{Gal}(K'/K(\zeta_\ell))} \to H^2(\mathrm{Gal}(K'/K(\zeta_\ell)), \mathrm{ad}^0(\overline{\rho})^{\mathrm{Gal}(E/K')}).$$

The outer terms are zero because $\mathrm{ad}^0(\overline{\rho})^{\mathrm{Gal}(E/K')} = 0$. The second term is zero by assumption. Now any ℓ-group acting on a finite-dimensional non-trivial $\mathbf{F}_\ell$ vector space has a non-trivial set of invariants. Since $\mathrm{Gal}(K'/K(\zeta_\ell)) \cong \mathbf{Z}/(\ell)$, this implies $H^1(\mathrm{Gal}(E/K', \mathrm{ad}^0(\overline{\rho})) = 0$. Thus (ii) holds over Y instead of X.

By induction, we may therefore pass to an extension Y' of X over which (i), (ii) hold, and such that in addition $\overline{\rho}(\pi_1(Y'))$ has no normal subgroup of index ℓ. Over Y' we can now apply Theorem 3.1, and the result follows. (This uses again the formulation of Conjecture 1.1, which makes it obvious that de Jong's conjecture holds for $\overline{\rho}$, if it holds for $\overline{\rho}_{|\pi_1(Y')}$.) ∎

5 Appendix

In the paper we use a modified construction of Taylor-Wiles systems introduced in [TW]. In this appendix we explain this modification in the original context of modular curves of [TW]. We use notation of [Di] to indicate what the problem is and how we handle it. The main point is that when proving freeness of certain cohomology groups it is enough for the purposes of TW systems to prove this over certain group algebras whose group of characters "kill torsion".

A key step in TW systems is to prove, for certain finite set of primes $Q = \{q_1, \cdots, q_r\}$ and any positive integer N prime to the primes in Q, results towards the freeness of the cohomology group $H^1(X_{N,Q}, \mathcal{O})_{\mathsf{m}}$ as a module over $\mathcal{O}[\Delta_Q]$ (under the natural action) with Δ_Q the Sylow ℓ-subgroup (which we may also view as the maximal ℓ-quotient) of $\Pi_{q \in Q}(\mathbf{Z}/q\mathbf{Z})^*$, where m is a mod ℓ maximal ideal of a certain Hecke algebra which satisfies a certain set of conditions, and where $\mathcal{O}$ is a finite flat extension of $\mathbf{Z}_\ell$. Here $X_{N,Q}$ is the modular curve corresponding to the subgroup $\Gamma_0(N) \cap \Gamma_1(q_1 \cdots q_r)$. Further the quotient of $H^1(X_{N,Q}, \mathcal{O})_{\mathsf{m}}$ by the augmentation ideal of $\mathbf{Z}_\ell[\Delta_Q]$ is isomorphic to $H^1(X_0(N), \mathcal{O})_{\mathsf{m}}$ if the primes q_i in addition satisfy the hypothesis that the mod ℓ representation $\overline{\rho}$ corresponding to m is such that it is unramified at q_i and the ratio of the eigenvalues of $\overline{\rho}(\mathrm{Frob}_{q_i})$ are not $q_i^{\pm 1}$.

One of the technical steps in proving the freeness is to impose an auxiliary level structure to avoid problems arising from torsion of $\Gamma_0(N)$. We indicate an argument that bypasses this.

We observe the following proposition which directly follows from the proof of [Ca] Lemme 1:

Proposition 1 *Let e be any integer that kills the torsion of $\Gamma_0(N)$. Let Δ_e^Q be the subgroup of $\mathrm{Hom}(\Delta_Q, \mathbf{Q}_\ell/\mathbf{Z}_\ell)$ that consists of eth powers. Consider the twisted sheaf $\mathcal{O}(\chi)$ for any character $\chi \in \Delta_e^Q$ on $X_0(Nq_1\cdots q_r)$ and assume $\mathcal{O}$ to be large enough to contain all values of χ. Then if k is the residue field of $\mathcal{O}$, the reduction $\mathcal{O}(\chi)\otimes k$ is isomorphic to the constant sheaf k on $X_0(Nq_1\cdots q_r)$.*

As a standard consequence one has:

Corollary 2 *Let Δ_Q^e be the quotient of Δ_Q that is dual to the subgroup Δ_e^Q of $\mathrm{Hom}(\Delta_Q, \mathbf{Q}_\ell/\mathbf{Z}_\ell)$. Let $X_{N,Q,e}$ be the modular curve that corresponds to the congruence subgroup that is the kernel of the natural map $\Gamma_0(Nq_1\cdots q_r) \to \Delta_Q^e$. Let m be a maximal ideal of a certain Hecke algebra (as in [Di]: we drop operators T_r, U_r for r not coprime to $Nq_1\cdots q_n$) acting on $H^1(X_{N,Q,e}, \mathcal{O})$ such that the corresponding residual representation $\overline{\rho}$ of $G_{\mathbf{Q}}$ is not reducible. Then $H^1(X_{N,Q,e}, \mathcal{O})_{\mathsf{m}}$ has a natural action of Δ_Q^e and is a free $\mathcal{O}[\Delta_Q^e]$-module for any $\mathcal{O}$ that is finite flat over $\mathbf{Z}_\ell$.*

Proof of the proposition: For conciseness of notation we denote by Y and X the curves $X_{N,Q,e}$ and $X_0(Nq_1\cdots q_r)$, and we have the natural map $r : Y \to X$ that is the quotient by Δ_Q^e. The sheaf $\mathcal{O}(\chi)$ is described as $\Delta_Q^e\backslash[Y\times\mathcal{O}]$ with Δ_Q^e acting on the constant sheaf $\mathcal{O}$ by χ. The stalk at a point $x \in X$, after choosing a point y in $r^{-1}(x)$, can be identified with the subset of the stalk at y of the constant sheaf, $\mathcal{O}_y$, on which the stabilizer of y in Δ_Q^e acts by χ (thus it is either $\mathcal{O}_y$ or 0). From this description the proposition follows using our assumption on χ. ∎

Proof of the corollary: We first note that as $\overline{\rho}$ is irreducible, the étale H^0 and H^2 of modular curves with coefficients in the twisted sheaves above do not have the maximal ideal m in their support (see Section 3 of [Ca]). Thus from the proposition above, and the long exact sequence of cohomology, it follows that for for any character $\chi \in \Delta_e^Q$ on $X_0(Nq_1\cdots q_r)$ we have a (Hecke equivariant) isomorphism $H^1(X_0(Nq_1\cdots q_r), \mathcal{O}(\chi))_{\mathsf{m}} \otimes k \simeq H^1(X_0(Nq_1\cdots q_r, k)_{\mathsf{m}}$. Then by a standard argument (see proof of Proposition 5.6.1 in [CDT]) the corollary follows. ∎

Let us further assume that for each $n \in \mathbf{N}$ we have sets of primes Q_n of constant cardinality r such that for $q \in Q_n$, q is prime to N, q is 1 mod ℓ^n, and $\overline{\rho}$ is unramified at q with the ratio of the eigenvalues of $\rho(\mathrm{Frob}_q)$ not $q^{\pm 1}$ (such sets exist when $\overline{\rho}$ restricted to the quadratic subfield of $\mathbf{Q}(\mu_\ell)$ is not reducible). Then again $H^1(X_{N,Q,e}, \mathcal{O})_{\mathsf{m}}$ is a free $\mathcal{O}[\Delta_{Q_n}^e]$-module whose quotient by $\Delta_{Q_n}^e$ is isomorphic to $H^1(X_0(N), \mathcal{O})_{\mathsf{m}}$. The group $\Delta_{Q_n}^e$ surjects onto $\mathbf{Z}/(\ell^{n-e})^r$, and thus grows systematically with n. This is enough to construct TW systems as in Section 3.1 of [Di] avoiding imposition of auxiliary level structures.

The modification of this appendix can also be used to avoid imposition of auxiliary level structure needed to bypass torsion problems in the level-lowering method of [SW], as done in the main body of this paper. Here the further remark, in addition to the observation above, is that when base changing to make orders of multiplicative groups of orders of residue fields at some fixed places congruent to 1 modulo high powers of ℓ, one also requires certain other places, chosen in advance, to split completely, so that the ℓ-part of the torsion can't grow much under base change.

References

[Bö1] Böckle, G., *Lifting mod p representations to characteristic p^2*, J. Number Theory **101** (2003), no. 2, 310–337.

[BK1] Böckle, G., Khare, C., *Mod ℓ representations of arithmetic fundamental groups: Part I*, preprint.

[BK2] Böckle, G., Khare, C., *Finiteness results for mod ℓ Galois representations over function fields*, preprint.

[BJ] Borel, A., Jacquet, H., *Automorphic forms and automorphic representations* in "Proc. Sympos. Pure Math., XXXIII", Part 1, pp. 189–207, Amer. Math. Soc., Providence, R.I., 1979.

[Ca] Carayol, H., *Sure les représentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke Math J **59** (1989), 785–801.

[CPS] Cline, E., Parshall, B., Scott, L., *Cohomology of finite groups of Lie type I*, Publ. Math. IHES **45** (1975), 169–191.

[CDT] Conrad, B., Diamond, F., Taylor, R., *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), 521–567.

[Di] Diamond, F., *The Taylor-Wiles construction and multiplicity one*, Invent. Math. **128** (1997), no. 2, 379–391.

[Dr] Drinfeld, V. G., *Two-dimensional ℓ-adic representations of the fundamental group of a curve over a finite field and automorphic forms on* GL(2), Amer. J. Math. **105** (1983), 85–114.

[F] Fujiwara, K., *Deformation rings and Hecke algebras in the totally real case*, unpublised manuscript.

[Ga] D. Gaitsgory, *On de Jong's conjecture*, preprint 2004, available under http://arXiv.org/abs/math/0402184

[dJ] de Jong, A. J., *Conjecture on arithmetic fundamental groups*, Israel J. Math. **121** (2001), 61–84.

[HT1] Harris, M., Taylor, R., *The geometry and cohomology of some simple Shimura varieties*, Annals of Math Studies **151**, Princeton University Press (2001).

[HT2] Harris, M., Taylor, R., *Deformations of automorphic Galois representations*, fourth draft, January 2003, available under `http://www.math.jussieu.fr/ harris/`

[Ka1] Khare, C., *Conjectures on finiteness of mod p Galois representations*, J. Ramanujan Math. Soc. **15** (2000), no. 1, 23–42.

[Laf] Lafforgue, L., *Chtoucas de Drinfeld et correspondance de Langlands*, Invent. Math. **147** (2002), 1–241

[LRS] Laumon, G., Rapoport, M., Stuhler, U., *D-elliptic sheaves and the Langlands correspondence*, Invent. Math. **113** (1993), no. 2, 217–338.

[Ma] Mazur, B., *Deforming Galois representations*, in 'Galois groups over **Q**', 385–437, Math. Sci. Res. Inst. Publ., **16**, Springer, New York, 1989.

[Mo] Moon, H., *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), no. 1, 156–165.

[MT] Moon, H., Taguchi, Y., *Mod p-Galois representations of solvable image*, Proc. Amer. Math. Soc. **129** (2001), no. 9, 2529–2534.

[Ne] Neukirch, J., *Algebraic number theory*, Grundlehren **322**, Springer-Verlag, Berlin, 1999.

[NSW] Neukirch, J., Schmidt, A., Wingberg, K., *Cohomology of number fields*, Grundlehren 323, Springer-Verlag, Berlin, 2000.

[Ogilvie] David Ogilvie, Uiversity of Chicago PhD thesis, 2005.

[SW] Skinner, C. M., Wiles, A. J., *Base change and a problem of Serre*, Duke Math. J. **107** (2001), no. 1, 15–25.

[TW] Taylor, R., Wiles, A., *Ring-theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.

[Wi] Wiles, A., *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141 (1995), 443–551.

Addresses of the authors:
GB: Institut für experimentelle Mathematik, Universität Duisburg-Essen, Standort Essen, Ellernstrasse 29, 45326 Essen, Germany.
e-mail address: `boeckle@iem.uni-due.de`
CK: Dept of Math, University of Utah, 155 S 1400 E, Salt Lake City, UT 84112.
e-mail address: `shekhar@math.utah.edu`
School of Mathematics, TIFR, Homi Bhabha Road, Mumbai 400 005, INDIA.
e-mail addresses: `shekhar@math.tifr.res.in`