Lifting mod p representations to characteristics p^2

Gebhard Böckle
ETH Zürich, Departement Mathematik, Rämistrasse 101
8092 Zürich, Switzerland, e-mail: boeckle@math.ethz.ch

January 15, 2003

Abstract

There is an abundance of Galois representations in characteristic p that arise as the mod p reduction of a characteristic zero representation from algebraic geometry. Except for two-dimensional representations there is little known about the set of mod p representations that should arise this way. As a first step in this direction, we consider the problem of finding lifts to characteristic p^2 for a representation $\bar{\rho}\colon G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{GL}_n(\kappa)$, where κ is a finite field of characteristic p, K a local or global field and n any positive integer.

If K is a local field, we can show that such lifts always exist. However if $p|n$, one cannot always fix the determinant of a lift. We also present some partial results for the existence of lifts to characteristic zero.

For global fields K, we can construct lifts only if, vaguely speaking, 'the prime-to-p image of $\bar{\rho}$ is large inside $\mathrm{GL}_n(\kappa)$'. A sufficient condition for this is the vanishing of $H^1(\mathrm{Im}(\bar{\rho}'), M_n(\kappa))$, where $\bar{\rho}'$ is the restriction of $\bar{\rho}$ to $G_{K(\zeta_p)}$ and the action on $M_n(\kappa)$ is the adjoint action. Based on methods of Cline, Parshall and Scott, we will give a group theoretic criterion for this first cohomology group to vanish.

1 Introduction

Throughout κ will be a finite field of characteristic p. We consider representations

$$\bar{\rho}\colon G_K := \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_n(\kappa),$$

where K is a global or local field in the sense of [Neu], § II.5, $\bar{K}$ its separable closure and n is any positive integer. The central question that we will study is the existence of a lift of $\bar{\rho}$ to $W_2(\kappa)$, the ring of Witt vectors of length two. We note right away that for $n = 1$ this question is not a very interesting one, as using Teichmüller lifts, it is immediate that one always has lifts to $W(\kappa)$, the ring of Witt vectors of κ.

A strong motivation for the study of the above question is Serre's conjecture in the case $n = 2$, [Se2]: For $\bar{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\kappa)$ an odd and absolutely irreducible representation and $p > 2$, it predicts the existence of a lift to characteristic zero, which is associated to a modular form of a level computable in terms of $\bar{\rho}$. Despite the fact that this conjecture is still wide open — and only recently a promising approach to its solution was given by R. Taylor, [Tay] — it has served as a major inspirational source and was an important

ingredient in the proof of Fermat's last theorem and the Tanyama-Shimura conjecture, [Wil, TW, BCDT].

More generally, there are many situations in arithmetic geometry where one obtains Galois representations over a finite extension of $\mathbb{Q}_p$ whose mod p reduction is a representation $\bar{\rho}$ as above. In all these cases, the very construction of $\bar{\rho}$ shows the existence of lifts to characteristic zero. Here we want to study a problem in the opposite direction, namely given a mod p representation, under what conditions can one hope to find lifts, at least to characteristic p^2. We now summarize what seems to be known.

In [Kha], Khare proved the existence of lifts to $W(\kappa)$ for any $\bar{\rho}\colon G_K \to \mathrm{GL}_2(\kappa)$ which is reducible and for any field K. Based on this, he gave a proof that for $n = 2$ any $\bar{\rho}\colon G_K \to \mathrm{GL}_2(\kappa)$ admits a lift to $W_2(\kappa)$. For $K = \mathbb{Q}$ (and still $n = 2$), there has been further progress through recent work of Ramakrishna, cf. [Ra1, Ra2]. He proves under very general conditions on $\bar{\rho}$ that there exist lifts to $W(\kappa)$ for $K = \mathbb{Q}$ and $n = 2$. He only needs to exclude a few even cases where the local at p representation is of a certain exceptional shape and imposes some restrictions for small primes $p \leq 5$ — in particular, $p = 2$ is excluded. It also seems likely that some of the results of Ramakrishna can be generalized to other number fields than $\mathbb{Q}$.

If K is a function field of characteristic $l \neq p$, lifts to characteristic zero were obtained by de Jong, [deJ], as a consequence of certain conjectures on the image of the arithmetic fundamental groups of varieties in positive characteristic. In loc. cit. these conjectures are proved for 1- and 2-dimensional representations and they yield the following: Suppose $\bar{\rho}\colon G_K \to \mathrm{GL}_2(\kappa)$ is absolutely irreducible when restricted to $G_{K\bar{\mathbb{F}}_l}$. Let S be a finite set of places outside which $\bar{\rho}$ is unramified. Then there exists a lift to characteristic zero which is unramified outside S.

The above results suggest to investigate the lifting problem also for higher dimensional representations. As a first step towards obtaining lifts to characteristic zero, it seems useful to consider the weaker problem of finding lifts to $W_2(\kappa)$. Already this question provides various interesting problems. Furthermore it would be at the base of any hoped for inductive procedure in the spirit of [Ra1, Ra2] to construct lifts to $W(\kappa)$. We now describe our results in some detail.

Let us fix some notation. By $\mathrm{ad}_{\bar{\rho}}$ we denote the representation of G_K on $M_n(\kappa)$ obtained by composing the adjoint representation ad given by conjugation of $\mathrm{GL}_n(\kappa)$ on $M_n(\kappa)$ with the representation $\bar{\rho}$. By ad^0 and $\mathrm{ad}^0_{\bar{\rho}}$ we the corresponding subrepresentations on matrices of trace zero. It is easy to see that ad is self-dual. For the dual ad^{0*} of ad^0, which can be identified with the quotient of ad by the scalar matrices, we write $\overline{\mathrm{ad}}$, and analogously $\overline{\mathrm{ad}}_{\bar{\rho}}$. By L we denote the splitting field of $\bar{\rho}$, i.e. the fixed field of $\ker(\bar{\rho})$ inside $\bar{K}$. For any representation M of G_K, we denote by $M(i)$ the i-fold Tate twist of it and by M^* the dual representation. Hence any subgroup of $\mathrm{Gal}(L(\zeta_p)/K)$ will act on $\mathrm{ad}_{\bar{\rho}}(1)$ and $\overline{\mathrm{ad}}_{\bar{\rho}}(1)$.

Our first circle of results concerns the lifting of mod p representations in the case where K is a local field. The following will be shown in Section 2:

Theorem 1.1 *For any local field K and any representation $\bar{\rho}\colon G_K \to \mathrm{GL}_n(\kappa)$, there exists a lift to $W_2(\kappa)$.*

Corollary 1.2 *For K and $\bar{\rho}$ as in Theorem 1.1, the following are equivalent.*

(i) Given any lift η of $\det\bar{\rho}$ to $W_2(\kappa)$, there exists a lift ρ of $\bar{\rho}$ to $W_2(\kappa)$ such that $\eta = \det\rho$.

(ii) The natural map $H^0(G_K, \mathrm{ad}_{\bar{\rho}}(1)) \to H^0(G_K, \overline{\mathrm{ad}}_{\bar{\rho}}(1))$ is surjective.

If $p \not| n$ both of the equivalent conditions are satisfied.

Example 2.6 will show how condition (ii) can fail for $p|n$. Example 2.7, will show that for $p|n$ it is in general not even possible to fix the restriction of a lift of the determinant to the inertia subgroup I_K of G_K.

With regards to lifts mod p^l, $l > 2$, or to characteristic zero, we only have partial results for general local fields K, cf. Proposition 2.1 and Remark 2.15. By putting some restrictions on the local fields and on $\bar{\rho}$, in Section 3 we will obtain the following:

Theorem 1.3 *Let K be a local field of residue characteristic different from p. Then any representation $\bar{\rho}\colon G_K \to \mathrm{GL}_n(\kappa)$ for which $\bar{\rho}(I_K)$ is a p-group has a lift to $W(\kappa)$.*

A rather trivial result, whose proof is implicitly contained in that of Lemma 2.4, is the following.

Proposition 1.4 *Let K be a local field and $\bar{\rho}: G_K \to \mathrm{GL}_n(\kappa)$ a representation whose splitting field does not contain a primitive p-th root of unity. Then $\bar{\rho}$ has a lift to $W(\kappa)$.*

For the problem of lifting mod p representations of the absolute Galois group of a global field, we need to set up some more notation. For a number field K denote by S_p the set of places above p, by S_∞ the set of those above infinity, and by S a finite set of places containing $S_p \cup S_\infty$. For a function field K, let S be any finite set of places. $G_{K,S}$ will denote the Galois group of the maximal separable, unramified outside S extension of K. Furthermore, we let $H = \mathrm{Gal}(L(\zeta_p)/K)$ and for each place $\mathfrak{p}$ in S we fix decomposition groups $H_\mathfrak{p} \subset H$ and $G_{K_\mathfrak{p}} \subset G_{K,S}$. Armed with this notation, we obtain the following result on global mod p^2 lifts, which is proved in Section 4.

We call a finite $\kappa[H]$-module X *globally unobstructed (for H^2)* if there exist cyclic subgroups H_i of H such that kernel of the restriction map

$$H^1(H, X^*(1)) \to \coprod_{\mathfrak{p}\in S} H^1(H_\mathfrak{p}, X^*(1)) \sqcup \coprod_i H^1(H_i, X^*(1))$$

is zero. It is easy to see that this condition is independent of the set S chosen, provided S contains $S_p \cup S_\infty$ and all places where $\mathrm{Gal}(L(\zeta_p)/K)$ ramifies. The nomenclature will be explained by Lemma 4.2.

Theorem 1.5 *Let K be a global field of characteristic different from p. Then any representation $\bar{\rho}\colon G_K \to \mathrm{GL}_n(\kappa)$ such that $\mathrm{ad}_{\bar{\rho}}$ is globally unobstructed has a lift to $W_2(\kappa)$.*

In Section 4, we also formulate a similar result for lifts with a fixed determinant using the notion of global unobstructedness for $\mathrm{ad}^0_{\bar{\rho}}$ instead of $\mathrm{ad}_{\bar{\rho}}$, cf. Theorem 4.1.

The above result gives some obvious restrictions when attempting to use the methods of [Ra2], to inductively obtain lifts to $W(\kappa)$. For this another necessary step would be the analysis of local versal deformation problems of representations $G_{K_\mathfrak{p}} \to \mathrm{GL}_n(\kappa)$ at primes $\mathfrak{p}$, which for arbitrary $n, \mathfrak{p}$ seems difficult.

Remark 1.6 For $n = 2$, Theorem 1.5 does not recover the result in [Kha] for global fields, cf. Remark 4.3. After the work of Khare, a rather obvious result is that if there exists a p-Sylow subgroup P of $\bar{\rho}(G_K)$ such that $\{A - I : A \in P\} \subset M_n(\kappa)$ is concentrated in the first row or last column, then there do exist lifts to $W_2(\kappa)$ without assuming global unobstructedness for $\mathrm{ad}_{\bar{\rho}}$. We do think however that the case $n = 2$ is rather special and that general results for $n > 2$ which avoid this assumption should be rather difficult to obtain.

In Section 4, we also prove the following rather simple theorem, based on Artin-Schreier theory:

Theorem 1.7 *Let X be an affine noetherian scheme over $\mathbb{F}_p$ and $\bar{\rho} : \Pi_1(X) \to \mathrm{GL}_n(\kappa)$ a representation of the arithmetic fundamental group $\Pi_1(X)$ of X. Then there exists a lift $\rho\colon \Pi_1(X) \to \mathrm{GL}_n(W(\kappa))$ of $\bar{\rho}$.*

In particular, if K is any *field of characteristic p and $\bar{\rho}\colon G_K \to \mathrm{GL}_n(\kappa)$ any representation, then there exists a lift to $W(\kappa)$. If K is a function field, one can find a lift which is ramified at most at finitely many places.*

Independently, this result is also to be found in [EK], Thm 0.2.

In the final section, we will prove the following result on sufficient conditions for $\mathrm{ad}_{\bar{\rho}}$ to be globally unobstructed:

Proposition 1.8 *Let the notation be as in Theorem 1.5. Under any of the following conditions, $\mathrm{ad}_{\bar{\rho}}$ is globally unobstructed.*

(i) The splitting field L of $\bar{\rho}$ does not contain ζ_p.

(ii) $\zeta_p \in L$ and $H^1(H', \mathrm{ad}_{\bar{\rho}}) = 0$ where $H' = \mathrm{Gal}(L/K(\zeta_p))$.

(iii) $\zeta_p \in L$ and with respect to a suitable basis of κ^n, the group $H' \cap \mathrm{B}_n(\kappa)$ contains a p-Sylow subgroup of H' and satisfies the conditions of Theorem 1.9.

(iv) $\zeta_p \in L$ and $H = \mathrm{Im}(\bar{\rho})$ contains $\mathrm{SL}_n(\kappa)$ and either $|\kappa| > 5$, or $n > 2$ and $|\kappa| > 3$.

The proof uses a vanishing theorem for $H^1(G, \mathrm{ad})$ and $H^1(G, \overline{\mathrm{ad}})$, based on [CPS], for certain subgroups G of $\mathrm{GL}_n(\kappa)$, which we state below. It may be of independent interest, for example in the theory of deformations of Galois representations.

Denote by $B_n(\kappa)$ and $T_n(\kappa)$ the set of those matrices inside $\mathrm{GL}_n(\kappa)$ which are upper triangular or diagonal, respectively. The subgroup of $B_n(\kappa)$ of matrices with 1's along the diagonal is denoted $U_n(\kappa)$. Also let $\mathrm{ST}_n(\kappa)$ be $T_n(\kappa) \cap \mathrm{SL}_n(\kappa)$. For any subgroup G of $\mathrm{GL}_n(\kappa)$, we denote by $\bar{G}$ its image in $\mathrm{PGL}_n(\kappa) = \mathrm{GL}_n(\kappa)/\kappa^*$. For $1 \leq i, j \leq n$, we let $e_{i,j}$ be the matrix that is one at the spot (i, j) and zero elsewhere, and we let I denote the identity matrix. We say that $(i_1, j_1), \ldots, (i_l, j_l)$ is a *cycle* if after a suitable permutation of the indices one has $j_1 = i_2, j_2 = i_3, \ldots, j_{l-1} = i_l, j_l = i_1$.

The following is obtained by adapting ideas taken from [CPS].

Theorem 1.9 *Let G be a subgroup of $B_n(\kappa)$ that satisfies the following conditions:*

(i) G is the semidirect product $U \rtimes T$ where $U = G \cap U_n(\kappa)$ and $T = G \cap T_n(\kappa)$.

(ii) *There exists a subfield κ' of κ of order at least 7, if $n = 2$, at least 5, if $n = 3$, or at least 4, if $n > 3$, such that $\bar{T}$ contains $\overline{\mathrm{ST}}_n(\kappa')$.*

(iii) *There exist matrices $u_k := I + \alpha_k e_{i_k,j_k} \in U$, $k = 1, \ldots, n'$, $\alpha_k \in \kappa^*$ such that U is generated as a group by the T-conjugates of the elements u_k, $k = 1, \ldots, n'$.*

(iv) *The set $\{(i_m, j_m) | \, m = 1, \ldots, k\}$ contains no cycle.*

Then $H^1(G, \mathrm{ad}) = H^1(G, \overline{\mathrm{ad}}) = 0$.

In particular ([CPS]) $H^1(\mathrm{SL}_n(\kappa), \mathrm{ad}) = 0$, if $|\kappa| \geq 7$ or $|\kappa| \geq 4$ and $n > 2$.

Vaguely speaking, the above says that if G contains a sufficiently 'large' diagonal part and if the unipotent part U is not very 'irregular', then $H^1(G, \mathrm{ad})$ vanishes.

Acknowledgements: I gratefully acknowledge partial support of the Deutsche Forschungsgemeinschaft through a Habilitation grant as well as the hospitality of the University of Illinois that I received while working on this project. My warmest thanks to Chandrashekhar Khare for a conversation which provided the initial impulse for this article and for his continuing interest. Also many thanks to the referee for the extremely careful reading of the original manuscript and many helpful corrections and suggestions.

2 Local lifts

For a p-power $q > 1$ and $m \in \mathbb{N}$, we define the group $D_q(m)$ as the pro-p completion of

$$\langle t_1, \ldots, t_{2m} | t_1^{-1} t_2^{-1-q} t_1 t_2 (t_3, t_4) \ldots (t_{2m-1}, t_{2m}) = 1 \rangle,$$

where for elements s, t in a group, (s, t) will denote the commutator $s^{-1}t^{-1}st$. Furthermore for an integer $f \geq 2$, we define the groups $D_2^{(1,f)}(m)$, $D_2^{(2,f)}(m)$,$D_2^{(3,f)}(m)$, as the pro-2 completion of

$$\langle t_1, \ldots, t_{2m+1} | t_1^2 t_2^{2^f} (t_2, t_3) \ldots (t_{2m}, t_{2m+1}) = 1 \rangle,$$

$$\langle t_1, \ldots, t_{2m} | t_1^{2+2^f} (t_1, t_2)(t_3, t_4) \ldots (t_{2m-1}, t_{2m}) = 1 \rangle,$$

$$\langle t_1, \ldots, t_{2m} | t_1^2 (t_1, t_2) t_3^{2^f} (t_3, t_4) \ldots (t_{2m-1}, t_{2m}) = 1 \rangle,$$

respectively. The groups $D_q(m)$ and $D_2^{i,f}(m)$, are Demuškin groups and are important in the classification of the pro-p completion of the absolute Galois group of a local field, cf. [Lab] and the proof of Theorem 1.1 given below. For any pro-p group P, let $\bar{P}$ denote its maximal p-elementary abelian quotient, and so in particular $\bar{D}_q(m) \cong \mathbb{F}_p^{2m}$.

The main results of this section are the following propositions:

Proposition 2.1 *Let m be any positive integer and $q > 1$ be as above. Let $q = p^\lambda$ for some $\lambda \in \mathbb{N} \cup \{\infty\}$, where $p^\infty := 0$. Any representation $\bar{\tau} \colon D_q(m) \to \mathrm{GL}_n(\kappa)$ has a lift $\tau \colon D_q(m) \to \mathrm{GL}_n(W_{\lambda+1}(\kappa))$.*

Proposition 2.2 *Let $i \in \{1, 2, 3\}$, $f \geq 2$ and $m \in \mathbb{N}$. Any representation $\bar{\tau} \colon D_2^{(i,f)}(m) \to \mathrm{GL}_n(\kappa)$ has a lift $\tau \colon D_2^{(i,f)}(m) \to \mathrm{GL}_n(W_2(\kappa))$.*

Before giving the somewhat technical proofs, we will derive Theorem 1.1. We first prove two lemmas.

Lemma 2.3 *Let $K \in \{\mathbb{R}, \mathbb{C}\}$. Then any representation $\bar{\rho}\colon G_K \to \mathrm{GL}_n(\kappa)$ has a lift to $W(\kappa)$.*

PROOF: For $K = \mathbb{C}$ there is nothing to show, so let $K = \mathbb{R}$ and let g be the generator of the group $C_2 := \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ of order two. If $p \neq 2$, any representation is isomorphic to a direct sum of one-dimensional representations where the image of g lies in $\{\pm 1\}$. Such representation obviously lift.

Suppose therefore $p = 2$. Again any representation is completely reducible. The irreducible representations are the trivial one and $\kappa[C_2]$. The former obviously lifts and the latter has the lift $W(\kappa)[C_2]$. ∎

Lemma 2.4 *Let $K \neq \mathbb{R}, \mathbb{C}$ be a local field and $\bar{\rho}\colon G_K \to \mathrm{GL}_n(\kappa)$ a representation whose image is a p-group. Then $\bar{\rho}$ has a lift to $W_2(\kappa)$.*

PROOF: As the kernel of $\mathrm{GL}_n(W(\kappa)) \to \mathrm{GL}_n(\kappa)$ is a pro-p group, any lift of $\bar{\rho}$ will factor through the pro-p completion $G_K(p)$ of G_K. There are four cases to distinguish:

(i) K is of characteristic p.

(ii) K is of positive characteristic $l \neq p$.

(iii) K is of characteristic 0 and residue characteristic $l \neq p$.

(iv) K is of characteristic 0 and residue characteristic p.

In case (i), the group $G_K(p)$ is a countably generated free pro-p group, cf. [Koc], Satz 10.4. Also, if we are in one of cases (ii)—(iv) and if K does not contain a primitive p-th root of unity, $G_K(p)$ is known to be a free finitely generated pro-p group, cf. [Koc], Sätze 10.1, 10.5. (Note that for $p = 2$, case (iv) is an exception!) Thus in all these cases, $\bar{\rho}$ will clearly admit a lift to $W(\kappa)$.

Let now $q > 1$ be the maximal p-power such that K contains a primitive q-th root of unity. By [Koc], § 9, § 10 and [Lab], for $q > 2$ the group $G_K(p)$ is isomorphic to the group $D_q(m)$ for a suitable m, and for $q = 2$ to one of the groups $D_2^{(i,f)}(m)$ for suitable i, f, m. The theorem now follows from the above propositions. ∎

Remark 2.5 In cases (ii) and (iii), if $\zeta_p \in K$, the group $G_K(p)$ is usually described as the pro-p completion of $\langle s, t | sts^{-1} = t^l \rangle$, where l is congruent to 1 modulo p. It is a simple matter of replacing s by s^u for some $u \in \mathbb{Z}_p^*$ to obtain the presentation we have for $D_q(1)$, where q now is the exact (maximal) p-power dividing $l - 1$.

PROOF OF Theorem 1.1: By Lemma 2.3, we may assume $K \neq \mathbb{R}, \mathbb{C}$. Let F be the splitting field of $\bar{\rho}$, $G := \mathrm{Gal}(F/K)$, P a p-Sylow subgroup of G, and E the fixed field of P in F. The obstruction to lifting $\bar{\rho}$ is given by an element $\theta \in H^2(G_K, \mathrm{ad}_{\bar{\rho}})$, whose well-known construction we now briefly recall for sake of completeness:

Let $\rho_1 \colon G_K \to \mathrm{GL}_n(W_2(\kappa))$ be a continuous set-theoretic lift of $\bar{\rho}$. (One way to obtain such a ρ_1 is to choose for each $\bar{\alpha} \in \mathrm{Im}(\bar{\rho}) \subset \mathrm{GL}_n(\kappa)$ a lift $\beta_{\bar{\alpha}} \in \mathrm{GL}_n(W_2(\kappa))$ and to set $\rho_1(s) := \beta_{\bar{\rho}(s)}$ for $s \in G_K$.) Then for each pair $(s,t) \in G_K$ one defines a unique element $c(s,t) \in M_n(\kappa)$ by the formula

$$\rho_1(s)\rho_1(t)\rho_1(st)^{-1} = I + pc(s,t).$$

The assignment $(s,t) \mapsto c(s,t)$ defines a continuous 2-cocycle of G_K with values in $\mathrm{ad}_{\bar{\rho}}$. Its image θ in $H^2(G_K, \mathrm{ad}_{\bar{\rho}})$ is independent of the choice of ρ_1. Now θ is trivial if and only if it is a 2-coboundary $\mathrm{d}^1 b$ for some continuous 1-cocycle $b \colon G_K \to \mathrm{ad}_{\bar{\rho}}$. Given b, the map $s \mapsto (I - pb(t))\rho_1(s)$ defines a homomorphism $\rho \colon G_K \to \mathrm{GL}_n(W_2(\kappa))$ lifting $\bar{\rho}$. Conversely, if there is a group-theoretic lift, then the associated 2-cocycle and hence also θ are trivial.

Let us now analyze θ. As an additive group, $\mathrm{ad}_{\bar{\rho}}$ is p-primary. Furthermore by the definition of E, the index of G_E in G_K is prime to p, and so the restriction map

$$H^2(G_K, \mathrm{ad}_{\bar{\rho}}) \longrightarrow H^2(G_E, \mathrm{ad}_{\bar{\rho}})$$

is injective. Furthermore, the image of θ under this map is the obstruction to lifting $\bar{\rho}_{|G_E}$. By the above lemma this obstruction vanishes, and hence $\theta = 0$, as desired. ∎

PROOF OF Corollary 1.2: We fix a lift ρ of $\bar{\rho}$ to $W_2(\kappa)$. Let $\mathrm{tr} \colon \mathrm{ad}_{\bar{\rho}} \to \kappa$ be the trace map and $\mathrm{diag} \colon \kappa \to \mathrm{ad}_{\bar{\rho}}$ the map $\lambda \mapsto \lambda I$, where κ is regarded as a trivial G_K-module.

Recall that given ρ, there is a bijection between the set of lifts of $\bar{\rho}$ to $W_2(\kappa)$ modulo conjugation and the set $H^1(G_K, \mathrm{ad}_{\bar{\rho}})$ defined in the following way: For any lift ρ' of $\bar{\rho}$, the map $\rho'\rho^{-1} \colon G_K \to I + pM_n(W_2(\kappa))$ defines a 1-cocycle $c := \frac{1}{p}(\rho'\rho^{-1} - I) \colon G_K \to \mathrm{ad}$. One easily verifies that $\mathrm{tr}(c) \colon G_K \to \kappa$ is the 1-cocycle which arises in the analogous way from $\det \rho' \det \rho^{-1} \colon G_K \to 1 + pW_2(\kappa)$.

Therefore condition (i) of the corollary is clearly equivalent to the surjectivity of the map $H^1(\mathrm{tr}) \colon H^1(G_K, \mathrm{ad}_{\bar{\rho}}) \to H^1(G_K, \kappa)$. The map $H^1(\mathrm{diag}(1))$ in

$$H^0(G_K, \mathrm{ad}(1)) \longrightarrow H^0(G_K, \overline{\mathrm{ad}}(1)) \longrightarrow H^1(G_K, \kappa(1)) \overset{H^1(\mathrm{diag}(1))}{\longrightarrow} H^1(G_K, \mathrm{ad}(1)),$$

which is part of a long exact cohomology sequence, is by Tate local duality dual to $H^1(\mathrm{tr})$. Thus (i) is equivalent to $H^1(\mathrm{diag}(1))$ being injective, which in turn is equivalent to the surjectivity asserted in (ii).

It remains to show that (ii) is satisfied if $p \nmid n$. In this case, however, the sequence $0 \to \kappa \overset{\mathrm{diag}}{\to} \mathrm{ad} \to \overline{\mathrm{ad}} \to 0$ is split exact and so the assertion is obvious. ∎

Example 2.6 Let K be a local field of residue characteristic $l \neq p$ and assume that K contains a p-th root of unity. We choose the presentation $D_q(1)$ for $G_K(p)$ where q is the highest power of p such that K contains a q-th root of unity, i.e., $G_K(p) \cong$

$\langle s,t|sts^{-1} = t^{q+1}\rangle$. Let $A = I + N \in U_p(W_2(\kappa))$ be a simple Jordan block and let $\bar\rho\colon G_K \to G_K(p) \to U_p(\kappa)$ be the (unramified) representation of G_K given by mapping s to $A \pmod p$ and t to I.

A simple computation shows that ad^{G_K} and $\overline{\mathrm{ad}}^{G_K}$ have the same dimension over κ. The left exact sequence $0 \to \kappa^{G_K} \to \mathrm{ad}^{G_K} \to \overline{\mathrm{ad}}^{G_K}$ implies that condition (ii) in Corollary 1.2 is violated. More precisely, we claim that for any lift ρ, which may or may not be ramified, of $\bar\rho$ to $W_2(\kappa)$ the map $\det\rho : G_K \to W_2(\kappa)^*$ is unramified:

Note first that a lift of $\bar\rho$ is given by mapping s to A and t to I. Therefore an arbitrary lift ρ is given by mapping s to $A(1+pM)$ and t to $1+pM'$ where $M, M' \in M_p(W_2(\kappa))$ are subject to the condition

$$A(1+pM)(1+pM')(1-pM)A^{-1} = (1+pM')^{q+1},$$

which is equivalent to $pAM' = pM'A$. The solutions to this equation are the matrices M' which are upper triangular and which on any parallel to the diagonal take a single value. Therefore the trace of pM' is zero since it is p times the value on the diagonal. As asserted it follows that $\det\rho(t) = \det(1+pM') = 1$ for any lift ρ of $\bar\rho$.

Example 2.7 One might argue that the above example is not very interesting since trying to fix a ramified lift of $\det\bar\rho$ for an unramified representation is rather pathological. This opinion is supported even further by some calculations we did, which *suggest* that in the case where $G_K(p)$ is a Demŭskin group on two generators and where the image of $\bar\rho$ is a p-group, the following holds: For any lift η of $\det\bar\rho$ to $W_2(\kappa)$, one can find a lift ρ of $\bar\rho$ with $\det\rho_{|I_K} = \eta_{|I_K}$, where I_K is the inertia subgroup of G_K.

We did not pursue this, as there do exist finite extensions K of $\mathbb{Q}_p$, ramified representations $\bar\rho\colon G_K \to \mathrm{GL}_p(\kappa)$ and lifts η of $\det\bar\rho$ such that for no lift $\rho\colon G_K \to \mathrm{GL}_p(W_2(\kappa))$ one can have $\det\rho_{|I_K} = \eta_{|I_K}$. The following is an example:

Let $q \geq 3$ be a p-power and let K be a finite extension of $\mathbb{Q}_p$ which contains a q-th but not a qp-th root of unity. (The construction can also be carried out in the case where $p = q = 2$.) We choose for $G_K(p)$ the presentation $D_q(m)$ given at the beginning of this section and assume that the subgroup generated by the variables t_{2m-1}, t_{2m} lies inside I_K. We define $\rho'\colon G_K(p) \to \mathrm{GL}_p(W_2(\kappa))$ on the generators t_i of $G_K(p)$ by sending t_{2m} to the matrix A of the previous example and by sending all other t_ν to the identity. Let $\bar\rho$ be the reduction modulo p of ρ'.

Then any lift of $\bar\rho$ is of the form $t_\nu \mapsto Z_\nu := I + pM_\nu$, $\nu = 1, \ldots, 2m-1$, $t_{2m} \mapsto Z_{2m} := A(I + pM_{2m})$, where the M_ν are matrices in $W_2(\kappa)$ subject to the Demuškin relation

$$Z_1^{-1}Z_2^{-1-q}Z_1Z_2(Z_3,Z_4)\ldots(Z_{2m-1},Z_{2m}) = I.$$

In the situation at hand, this relation simplifies to $I + p(A^{-1}M_{2m-1}A - M_{2m-1}) = I$. As in the previous example it follows that $\mathrm{tr}\, pM_{2m-1} = 0$ for all solutions M_{2m-1}, and hence $\det(\rho(t_{2m-1})) = 1$ for all lifts ρ of $\bar\rho$. However as $\det\bar\rho$ is trivial, a possible lift to $W_2(\kappa)$ is given by sending all t_ν except t_{2m-1} to 1 and by sending t_{2m-1} to $1+p$, and we have constructed the desired example.

In the remainder of this section we will prove Proposition 2.1. The proof of Proposition 2.2 is quite analogous, cf. Remark 2.14. Details are left to the reader. From now on,

we simply write D_q for $D_q(m)$. So let $\bar{\tau}\colon D_q \to \mathrm{GL}_n(\kappa)$ be given as in the proposition and let Γ be denote the image of $\bar{\tau}$. As Γ is a p-group, after a suitable change of basis one could assume that it is contained in $U_n(\kappa)$. We will construct a suitable basis of κ^n below.

We now define certain subgroups of $U_n(\kappa)$ which will be important in the combinatorics leading to the proof of Proposition 2.1. We abbreviate $\mathcal{J} := \{(i,j)|1 \leq i < j \leq n\} \subset \mathbb{N}\times\mathbb{N}$. A subset $\mathcal{I}$ of $\mathcal{J}$ is called *admissible*, if for all $(i,j) \in \mathcal{I}$, the elements $(1,j),(2,j),\ldots,(i,j)$ and $(i,j),(i,j+1),\ldots,(i,n)$ lie in $\mathcal{I}$. For an admissible set $\mathcal{I}$, we define the number $s = s(\mathcal{I})$ *of corners of* $\mathcal{I}$ and its *characteristic sequence* $\underline{s} = \underline{s}(\mathcal{I})$ as follows:

s is the number of elements (i,j) of $\mathcal{I}$ such that neither $(i+1,j)$ nor $(i,j-1)$ lies in $\mathcal{I}$, i.e. the number of *corners* towards the diagonal, if one depicts $\mathcal{I}$ in a $n\times n$ grid by marking all the squares with index $(i,j) \in \mathcal{I}$.

$\underline{s}$ is the sequence of such corners. This means that $\underline{s}$ is given by sequences of integers $1 \leq i_1 < i_2 < \ldots < i_s < n$ and $1 < j_1 < j_2 < \ldots < j_s \leq n$ with $i_r < j_r$ for $r = 1,\ldots,s$ such that

$$\mathcal{I} = \{(i,j)|\exists r \in \{1,\ldots,s\} : i \leq i_r \text{ and } j \geq j_r\},$$

and each pair (i_r,j_r) is a corner of $\mathcal{I}$. Clearly there is a bijection between admissible subsets of $\mathcal{J}$ and their characteristic sequences. We always set $j_{s+1} := n+1$.

For an admissible set $\mathcal{I}$ and $r \geq 1$, we define sets $\mathcal{I}^{(r)}$ by

$$\mathcal{I}^{(r)} := \{(l_0,l_r)|\exists l_1,\ldots,l_{r-1} : (l_0,l_1),\ldots,(l_{r-1},l_r) \in \mathcal{I}\}.$$

The sets $\mathcal{I}^{(r)}$ are again admissible. For any ring R, and any admissible set $\mathcal{I}$, we define

$$\begin{aligned} \mathfrak{u}_n^{\mathcal{I}}(R) &:= \{M = (m_{i,j}) \in M_n(R)|m_{i,j} = 0 \text{ if } (i,j) \notin \mathcal{I}\} \text{ and} \\ U_n^{\mathcal{I}}(R) &:= \{M = (m_{i,j}) \in \mathrm{U}_n(R)|M - I \in \mathfrak{u}_n^{\mathcal{I}}(R)\}. \end{aligned}$$

Clearly $U_n^{\mathcal{I}}(R)$ is a normal subgroup of $U_n(R)$ and $\mathfrak{u}_n^{\mathcal{I}}(R)$ a Lie ideal of the Lie algebra $\mathfrak{u}_n(R)$. Often, we simply write $U_n^{\mathcal{I}}$ if the ring R is clear from context, or if the statement is independent of R.

On admissible subsets one defines a partial ordering $\mathcal{I} < \mathcal{I}'$ by the following condition

$$\exists r \in \mathbb{N} : \forall j \leq r\, \forall i : (i,j) \in \mathcal{I} \Rightarrow (i,j) \in \mathcal{I}' \text{ and } \exists i : (i,r) \in \mathcal{I}' - \mathcal{I}.$$

Given an admissible set $\mathcal{I}$, we define various auxiliary admissible subsets from $\mathcal{I}$. First let $r \in \{1,\ldots,s\}$. Define $\mathcal{I}_r \subset \mathcal{I}$ by

$$\mathcal{I}_r := \{(i,j) \in \mathcal{I}| \text{ if } i = i_r, \text{ then } j \geq j_{r+1}\},$$

i.e. in row i_r we erase the entries $j_r,\ldots,j_{r+1}-1$. Next let $(i',j') \in \mathcal{I}$. Define

$$\begin{aligned} \mathcal{I}(i',j') &:= \{(i,j) \in \mathcal{I}|i < i' \text{ or } (i = i' \text{ and } j \geq j')\} \\ \dot{\mathcal{I}}(i',j') &:= \{(i,j) \in \mathcal{I}|i < i' \text{ or } (i = i' \text{ and } j > j')\}. \end{aligned}$$

For future reference, we formulate the following lemma. Note that the groups $\mathfrak{v}(i,j)$, defined therein, will be used below.

Lemma 2.8 *Let $\mathcal{I}$ be admissible. Then*

(i) $U_n^{\mathcal{I}^{(2)}}$ *contains the commutator subgroup of* $U_n^{\mathcal{I}}$*, and* $\mathfrak{u}_n^{\mathcal{I}^{(2)}}$ *the commutator ideal of the Lie algebra* $\mathfrak{u}_n^{\mathcal{I}}$*.*

(ii) The group $\bigcap_{r=1}^{s} U_n^{\mathcal{I}_r}$ *contains* $U_n^{\mathcal{I}^{(2)}}$*.*

(iii) For $(i,j) \in \mathcal{I}$ *define* $r \in \{1,\dots,s\}$ *by the condition that* $j_r \le j < j_{r+1}$*. Then* $\mathfrak{u}_n^{\dot{\mathcal{I}}(i,j)}$ *is a Lie ideal in* $\mathfrak{u}_n^{\mathcal{I}(i,j_r)}$*, both stabilized by right and left multiplication by elements of* U_n*. On their quotient* $\mathfrak{v}(i,j)$ *right and left multiplication by elements of* $U_n^{\mathcal{I}}$ *is trivial.*

PROOF: We only prove part (ii) and the second part of (iii), and leave the other parts to the reader. For (ii), observe that it suffices to show that $\bigcap_{r=1}^{s} \mathcal{I}_r \supset \mathcal{I}^{(2)}$. For the latter, it suffices to consider elements (i_r, j), $1 \le r \le s$, since in rows different from the rows i_r, the set $\mathcal{I}$ agrees with $\bigcap_{r=1}^{s} \mathcal{I}_r$ and contains $\mathcal{I}^{(2)}$. More precisely we have to show that if (i_r, j) lies in $\mathcal{I}^{(2)}$, then it lies in $\mathcal{I}_r$: Suppose (i_r, j) lies in $\mathcal{I}^{(2)}$. Then there exists k such that (i_r, k) and (k, j) lie in $\mathcal{I}$. We may clearly assume that $k = j_r$. Since elements of $\mathcal{I}$ 'lie above the diagonal', we have $j_r > i_r$. Because (i_r, j_r) is a corner, the second coordinate of (j_r, j) must be at least that of the following corner, i.e., $j \ge j_{r+1}$, and thus $(i_r, j) \in \mathcal{I}_r$.

For the second part of (iii), let $\tilde{j}$ be in $\{j_r, j_r+1, \dots, j\}$ and fix $x = (x_{k,l}) \in U_n^{\mathcal{I}}$. Then $(x-1)e_{i,\tilde{j}}$ lies in column $\tilde{j}$ above row i, and hence the assertion on left multiplication is clear. (In fact, x could be any element of U_n.)

For right multiplication observe that by the definition of r one has $x_{j,l} - \delta_{j,l} = 0$ if $j > i_r$ and $l < j_{r+1}$. Therefore $e_{i,\tilde{j}}(x-1)$ lies in row i, and on or to the right of column $j_{r+1} > j$. This shows the assertion for right multiplication. ∎

For $A \in \mathrm{GL}_n(\kappa)$, let c_A be the automorphism on $\mathrm{GL}_n(\kappa)$ that sends an element g to $A^{-1}gA$. So the elements c_A are simply given by a change of basis of the vector space κ^n on which $\mathrm{GL}_n(\kappa)$ acts tautologically. A basis of κ^n is called *minimal for* Γ, if there exists an admissible $\mathcal{I}$ with the following property: The group $U_n^{\mathcal{I}}(\kappa)$, whose definition depends on the choice of basis, contains Γ and for all $A \in \mathrm{GL}_n(\kappa)$ and all admissible $\mathcal{I}' < \mathcal{I}$ the group $c_A(\Gamma)$ is not contained in $U_n^{\mathcal{I}'}(\kappa)$. As there always exists a basis with respect to which Γ lies inside $U_n(\kappa)$, and as there are only finitely many admissible sets $\mathcal{I}$, there must exist such a minimal basis. The corresponding $\mathcal{I}$ is called *minimal for* Γ.

Lemma 2.9 *Let* $\mathcal{I}$ *be minimal for* Γ*. For* $r = 1, \dots, s$*, define*

$$\pi_r \colon \bar{D}_q \to V_r = U_n^{\mathcal{I}}(\kappa)/U_n^{\mathcal{I}_r}(\kappa) \cong (\kappa^{j_{r+1}-j_r}, +)$$

as the map induced from $\bar{\tau}$*, where we recall that* $\bar{D}_q \cong \mathbb{F}_p^{2m}$ *is the maximal p-elementary abelian quotient of* D_q*. Then for any* $r = 1, \dots, s$*, the set* $\pi_r(\bar{D}_q)$ *generates* V_r *as a vector space over* κ*.*

Note that it follows easily from parts (i) and (ii) of the previous lemma that $U_n^{\mathcal{I}_r}$ is normal in $U_n^{\mathcal{I}}$ and that the quotient is abelian. So in particular, π_r is a homomorphism.

PROOF: We argue by contradiction. Throughout we regard V_r as vector spaces of row vectors indexed by $j_r, \dots, j_{r+1}-1$. Choose any r such that the κ-span of $\pi_r(\bar{D}_q)$ is not all of V_r. This means that the image lies in a hyperplane of V_r. Therefore we can choose a minimal

$\tilde{j} \in j_r, \ldots, j_{r+1} - 1$ and a row vector $\underline{\alpha} := (0, \ldots, 0, \alpha_{\tilde{j}}, \ldots, \alpha_{j_{r+1}-1}) \in \kappa^{j_{r+1}-\tilde{j}}$ with $\alpha_{\tilde{j}} = 1$ such that $\pi_r(D_q)$ lies in the hyperplane $\{v \in V_r | v \cdot \underline{\alpha}^t = 0\}$. Define $A = (a_{i,j}) \in U_n(\kappa)$ such that A is 1 along the diagonal, $a_{i,\tilde{j}} = \alpha_i$ for $i = \tilde{j} + 1, \ldots, j_{r+1} - 1$, and all other $a_{i,j} = 0$. Applying the automorphism $c_A : g \mapsto A^{-1}gA$ of $\mathrm{GL}_n(\kappa)$ preserves the subgroup $U_n^{\mathcal{I}}(\kappa)$. Furthermore the component $(i_r, \tilde{j})$ of every element of $c_A(\Gamma)$ is zero.

Apply now the automorphism c_P of $\mathrm{GL}_n(\kappa)$ where P is the permutation matrix corresponding to the permutation cycle $(j_r, j_r + 1, \ldots, \tilde{j})$. One can check that c_P maps $U_n^{\mathcal{I}}(\kappa)$ to a subgroup of $U_n(\kappa)$. Let $\mathcal{I}'$ be minimal admissible such that $c_P c_A(\Gamma) \subset U_n^{\mathcal{I}'}(\kappa)$. Then for all $j < j_r$ and all i one has $(i,j) \in \mathcal{I} \Leftrightarrow (i,j) \in \mathcal{I}'$, while the element $(i_r, j_r) \in \mathcal{I} - \mathcal{I}'$. Thus $\mathcal{I}' < \mathcal{I}$, contradicting the minimality of $\mathcal{I}$ for Γ. ∎

From now on, we assume that $\Gamma \subset U_n^{\mathcal{I}}(\kappa)$ where $\mathcal{I}$ is minimal for Γ. In particular, the above lemma applies to all the maps π_l.

Remark 2.10 For the following argument, it is not really necessary that $\mathcal{I}$ is minimal for Γ. We only need an admissible $\mathcal{I}$ such that $\Gamma \subset U_n^{\mathcal{I}}(\kappa)$ and such that all the maps π_r have the property that $\pi_r(D_q)$ generates V_r as a vector space over κ.

Another method to obtain such an $\mathcal{I}$ is to inductively apply the step described in the proof of Lemma 2.9. Starting from the top left to the bottom right and repeating this procedure over and over again until all the maps π_r have the desired property. As there is only a finite number of $\mathcal{I}$'s and as each time we apply this step, $\mathcal{I}$ will become strictly smaller, this process will terminate.

Proof of Proposition 2.1: We proceed by induction on $1 \leq l \leq \lambda$ and assume that we have already found a lift $\tau_l \colon D_q \to U_n^{\mathcal{I}}(W_l(\kappa))$ of $\tau_1 := \bar{\tau}$. We will show that τ_l has a lift to $U_n^{\mathcal{I}}(W_{l+1}(\kappa))$, if $l < \lambda$, and, if $l = \lambda$, to $B_n(W_{l+1}(\kappa))$, the set of upper triangular matrices inside $\mathrm{GL}_n(W_{l+1}(\kappa))$.

Let $X_1, \ldots, X_{2m} \in U_n^{\mathcal{I}}(W_l(\kappa))$ be the images of the elements $t_1, \ldots, t_{2m} \in D_q$ under τ_l, so that they satisfy

$$X_1^{-1} X_2^{-1-q} X_1 X_2 (X_3, X_4) \ldots (X_{2m-1}, X_{2m}) = 1.$$

Let $Y_\nu \in U_n^{\mathcal{I}}(W_{l+1}(\kappa))$ be any lift of X_ν, $\nu = 1, \ldots, 2m$. Consider matrices $M_\nu \in M_n(W_{l+1}(\kappa))$, $\nu = 1, \ldots, 2m$, as variables and define for $\mu = 1, \ldots, m$: $Z_{2\mu} := Y_{2\mu}(I + p^l M_{2\mu-1})$, $Z_{2\mu-1} := Y_{2\mu-1}(I + p^l M_{2\mu})$. We claim that one can choose upper triangular M_ν such that

$$Z_1^{-1} Z_2^{-1-q} Z_1 Z_2 (Z_3, Z_4) \ldots (Z_{2m-1}, Z_{2m}) = 1 \tag{1}$$

and such that furthermore the Z_i lie in the asserted subgroup of $\mathrm{GL}_n(W_{l+1}(\kappa))$.

For matrices $A, B \in M_n(R)$, R a commutative ring, we write $[A, B]$ for $AB - BA$. We state the following simple, if tedious lemma without proof:

Lemma 2.11 *For any (commutative) ring R and $A, B \in \mathrm{GL}_n(R)$ define*

$$F(A,B) := \sum_{j=1}^{q-1} j A^j B A^{q-j-1} \in M_n(R).$$

Then the following hold:

(i) $((I+p^lM)A)^q = A^q + p^lA^{-1}F(A,[M,A])A$ *for* $A, M \in M_n(W_{l+1}(\kappa))$.

(ii)
$$\begin{aligned} & Z_1^{-1}Z_2^{-1-q}Z_1Z_2 \\ = \;& Y_1^{-1}Y_2^{-1-q}Y_1Y_2 + p^lY_1^{-1}[Y_2^{-1-q}Y_1Y_2, M_1] + p^l[Y_1^{-1}Y_2^{-1-q}Y_1, M_2]Y_2 \\ & -p^lY_1^{-1}F(Y_2^{-1},[M_1,Y_2^{-1}])Y_2^{-1}Y_1Y_2. \end{aligned}$$

Note that the expression from part (ii) of the lemma with F replaced by 0, with $q=0$ and indices 1 replaced by $2\mu-1$ and 2 by 2μ, $\mu = 2,\dots,m$ gives the analogous formula for $(Z_{2\mu-1}, Z_{2\mu})$.

Admittedly these expressions do look quite complicated. However in the analysis below, it will turn out that we only need what could be call the 'leading term' and this will be very computable and rather simple. To simplify the notation, we introduce the following abbreviations:

$$\begin{aligned} P_1 &:= Y_1^{-1}Y_2^{-1-q}Y_1Y_2, \\ Q_1 &:= Y_1^{-1}[Y_2^{-1-q}Y_1Y_2, M_1] + [Y_1^{-1}Y_2^{-1-q}Y_1, M_2]Y_2 - Y_1^{-1}F(Y_2^{-1},[M_1,Y_2^{-1}])Y_2^{-1}Y_1Y_2, \\ P_\mu &:= Y_{2\mu-1}^{-1}Y_{2\mu}^{-1}Y_{2\mu-1}Y_{2\mu}, \ \mu = 2,\dots,m, \\ Q_\mu &:= Y_{2\mu-1}^{-1}[Y_{2\mu}^{-1}Y_{2\mu-1}Y_{2\mu}, M_{2\mu-1}] + [Y_{2\mu-1}^{-1}Y_{2\mu}^{-1}Y_{2\mu-1}, M_{2\mu}]Y_{2\mu}, \ \mu = 2,\dots,m. \end{aligned}$$

Using this notation, we can rewrite condition (1) as

$$I - P_1\dots P_m = p^l\sum_{\mu=1}^{m} P_1\dots P_{\mu-1}Q_\mu P_{\mu+1}\dots P_m. \tag{2}$$

By induction hypothesis and the choice of the Y_ν, the expression $I - P_1\dots P_m$ lies in the linear subspace $p^l\mathfrak{u}_n^{\mathcal{I}}(W_{l+1}(\kappa))$. If $p^{l+1}|q$, the expression will in fact be contained in $p^l\mathfrak{u}_n^{\mathcal{I}^{(2)}}(W_{l+1}(\kappa))$, since then $Y_2^{-q} \in U_n^{\mathcal{I}^{(2)}}(W_{l+1}(\kappa))$. Let $p_\mu \in U_n^{\mathcal{I}}(\kappa)$ denote the image of P_μ under the reduction map $W_{l+1}(\kappa) \to \kappa$, and x_ν that of Y_ν, i.e., $x_\nu = \bar{\tau}(t_\nu)$. Let $x \in \mathfrak{u}_n^{\mathcal{I}}(\kappa)$ be the mod p reduction of some matrix in $X \in \mathfrak{u}_n^{\mathcal{I}}(W_{l+1}(\kappa))$ with $p^lX = I - P_1\dots P_m$. Finally for $m_1,\dots,m_{2m} \in M_n(\kappa)$, define

$$\begin{aligned} q_1 &:= x_1^{-1}[x_2^{-1-q}x_1x_2, m_1] + [x_1^{-1}x_2^{-1-q}x_1, m_2]x_2 - x_1^{-1}F(x_2^{-1},[m_1,x_2^{-1}])x_2^{-1}x_1x_2 \\ q_\mu &:= x_{2\mu-1}^{-1}[x_{2\mu}^{-1}x_{2\mu-1}x_{2\mu}, m_{2\mu-1}] + [x_{2\mu-1}^{-1}x_{2\mu}^{-1}x_{2\mu-1}, m_{2\mu}]x_{2\mu}, \ \mu = 2,\dots,m. \end{aligned}$$

Equation (2) is then equivalent to the following equation

$$x = \sum_{\mu=1}^{m} p_1\dots p_{\mu-1}q_\mu p_{\mu+1}\dots p_m, \tag{3}$$

where the q_μ are linear expressions in the m_ν. The following lemma implies that Equation (3) has a solution with m_ν of a form such that the Z_μ lie in the asserted subspace of $\mathrm{GL}_n(W_{l+1}(\kappa))$, and thus it completes the proof of the proposition. ∎

Define $\mathfrak{b}_n(\kappa) := \{A = (a_{i,j}) \in M_n(\kappa) \,|\, \forall i > j : a_{i,j} = 0\}$, i.e., as the set of upper triangular matrices.

Lemma 2.12 *For any $x \in \mathfrak{u}_n^{\mathcal{I}}(\kappa)$, there exist $m_1, \ldots, m_{2m} \in \mathfrak{b}_n(\kappa)$ such that*

$$x = \sum_{\mu=1}^{m} p_1 \ldots p_{\mu-1} q_\mu p_{\mu+1} \ldots p_m.$$

Furthermore, if $x \in \mathfrak{u}_n^{\mathcal{I}^{(2)}}$, one may choose $m_1, \ldots, m_{2m} \in \mathfrak{u}_n^{\mathcal{I}}(\kappa)$.

PROOF: For a pair $(i,j) \in \mathcal{I}$ define i' to be the maximal i such that $(i',j) \in \mathcal{I}$. Let (i',j') be the 'corner' in row i'. Furthermore let r be the number of the corner (i',j'), i.e., $(i',j') = (i_r, j_r)$.

We will prove the following assertion by upward induction in i, and then for fixed i by downward induction on j, thus establishing the first part of the lemma. For all $(i,j) \in \mathcal{I}$, there exist $m_1, \ldots, m_{2m} \in \mathfrak{b}_n(\kappa)$ such that:

(i) All $q_\mu \in \mathfrak{u}_n^{\mathcal{I}(i,j')}(\kappa)$ (and hence $\sum_{\mu=1}^{m} p_1 \ldots p_{\mu-1} q_\mu p_{\mu+1} \ldots p_m \in \mathfrak{u}_n^{\mathcal{I}(i,j')}(\kappa)$).

(ii) Modulo $\mathfrak{u}_n^{\dot{\mathcal{I}}(i,j)}(\kappa)$ one has $e_{i,j} \equiv \sum_{\mu=1}^{m} p_1 \ldots p_{\mu-1} q_\mu p_{\mu+1} \ldots p_m \in \mathfrak{u}_n^{\mathcal{I}(i,j')}(\kappa)$.

The proof of this assertion will use the following sublemma.

Sublemma 2.13 *For any $\alpha \in \kappa$, the map $\pi_{i,j}^{\alpha}$, defined as*

$$\pi_{i,j}^{\alpha} : D_q \longrightarrow \mathfrak{u}_n^{\mathcal{I}}(\kappa) : g \mapsto [\bar{\tau}(g), \alpha e_{i,i'}],$$

takes its values inside $\mathfrak{u}_n^{\mathcal{I}(i,j')}(\kappa)$. The induced map

$$\bar{\pi}_{i,j}^{\alpha} : D_q \longrightarrow \mathfrak{v}(i,j) = \mathfrak{u}_n^{\mathcal{I}(i,j')}(\kappa) / \mathfrak{u}_n^{\dot{\mathcal{I}}(i,j)}(\kappa)$$

factors via $\pi_r \colon D_q \to \bar{D}_q \to V_r$, defined in Lemma 2.9. The resulting map $V_r \to \mathfrak{v}(i,j)$ can be described as follows:
Consider an element $\alpha \in V_r$ as a row vector with entries

$$(\alpha_{i_r,j_r}, \alpha_{i_r,j_r+1}, \ldots, \alpha_{i_r,j_{r+1}-1})$$

and consider elements of $\mathfrak{v}(i,j)$ as row vectors $(\beta_{i,j_r}, \beta_{i,j_r+1}, \ldots, \beta_{i,j})$. Then the map $V_r \to \mathfrak{v}(i,j)$ simply truncates the first vector after position j and multiplies it by $-\alpha$.

PROOF: One has $[\bar{\tau}(g), e_{i,i'}] = (\bar{\tau}(g) - 1)e_{i,i'} - e_{i,i'}(\bar{\tau}(g) - 1)$. Arguing as in the proof of Lemma 2.8 (iii) it follows that $\pi_{i,j}^{\alpha}$ takes its image in $\mathfrak{u}_n^{\mathcal{I}(i,j')}$. The same line of reasoning shows that $U_n^{\mathcal{I}_r}$ maps under $g \mapsto [g, \alpha e_{i,i'}]$ to $\mathfrak{u}_n^{\dot{\mathcal{I}}(i,j)}$. Hence the induced map $\bar{\pi}_{i,j}^{\alpha}$ factors via $\bar{D}_q \to V_r$ as desired, and is therefore a group homomorphism. The explicit shape of $V_r \to \mathfrak{v}(i,j)$ is easily established. ∎

To prove the assertion we take $m_\nu = \alpha_\nu e_{i,i'}$ for suitable α_ν to be determined below. By the sublemma, the expressions $[\bar\tau(g), m_\nu]$ are in $\mathfrak{u}_n^{\mathcal{I}(i,j')}$. From the definitions of the q_μ and the results of Lemma 2.8 it follows that modulo $\mathfrak{u}_n^{\dot{\mathcal{I}}(i,j)}$ one has

$$p_1 \dots p_{\mu-1} q_\mu p_{\mu+1} \dots p_m \equiv \alpha_{2\mu}[x_{2\mu}^{-1}, e_{i,i'}] + \alpha_{2\mu-1}[x_{2\mu-1}, e_{i,i'}]$$

for $\mu = 1, \dots, m$, where we recall that the x_ν are the images under $\bar\tau$ of the generators t_ν of D_q. In the case $q = 2$ and $\mu = 1$, the term $F(.,.)$ intervenes, and one has to add the expression $\alpha_1[x_2^{-1}, e_{i,i'}]$ to the right hand side for the above formula to be true. To avoid this further complication, below we assume that $q > 2$. However, the interested reader can easily adjust the formulas below to see that the proof with minor modifications also works for $q = 2$.

Hence modulo $\mathfrak{u}_n^{\dot{\mathcal{I}}(i,j)}$ we have

$$\sigma := \sum_{\mu=1}^{m} \alpha_{2\mu}[x_{2\mu}^{-1}, e_{i,i'}] + \alpha_{2\mu-1}[x_{2\mu-1}, e_{i,i'}] \equiv \sum_{\mu=1}^{m} p_1 \dots p_{\mu-1} q_\mu p_{\mu+1} \dots p_m \in \mathfrak{v}(i, j'). \quad (4)$$

It may now be clear what we meant by the 'leading term' of the expressions for p_μ, q_μ when introducing them.

Let $\bar x_{2\mu}$ denote the image of $x_{2\mu}^{-1}$ in V_r and $\bar x_{2\mu-1}$ that of $x_{2\mu-1}$, considered as a row vector in V_r, and define $\tilde x_\nu$ by truncating the vector $\bar x_\nu$ after column j. Then the explicit description of $\bar\pi_{i,j}^{\alpha}$ and of the induced map $V_r \to \mathfrak{v}(i,j)$ yields $\sigma = -\sum \alpha_\nu \tilde x_\nu$ as a row vector in $\mathfrak{v}(i,j)$.

The t_ν generate D_q. Hence by Lemma 2.9 the $\bar x_\nu$ span V_r as a vector space over κ. Therefore the $\tilde x_\nu$ generate $\mathfrak{v}(i,j)$ as a vector space over κ, and so we can find suitable α_ν such that $\sigma = (0, 0, \dots, 0, 1)$. This proves the assertion made in (ii).

Finally for $x \in \mathfrak{u}^{\mathcal{I}^{(2)}}$, essentially the same inductive proof as above will work, where however we have to convince ourselves that we can now choose all m_ν in $\mathfrak{u}^{\mathcal{I}}(\kappa)$. In the proof above, we needed for each row index i_r of a corner all the elements e_{i,i_r} with $i \le i_r$ in order to obtain the elements at the spot (i,j) between columns j_r and j_{r+1} on rows up to number i_r. However by its definition $\mathcal{I}^{(2)}$ contains only elements (i_0, j) such that there exists an $(i_1, i_0) \in \mathcal{I}$. In the inductive step for (i_0, j), we need the subspace over κ spanned by e_{i_1,i_0}, and this lies in $\mathfrak{u}^{\mathcal{I}}(\kappa)$, as asserted. ∎

Remark 2.14 The proof of Proposition 2.2 is almost word by word the same as the one we gave for Proposition 2.1. However there are some notational differences, which is the main reason why we did not try to write a uniform proof, the matter already being technical enough.

If one successfully adapted the above proof, one difference that one will encounter is that the expression for σ given in Equation (4) in the proof of Lemma 2.12 takes a slightly different form. Depending on $i = 1, 2, 3$ one obtains the following expressions for $D_2^{i,f}(m)$,

independently of f:

$$\begin{aligned}\sigma &= \alpha_1[x_1, e_{i,i'}] + \sum_{\mu=1}^{m} \alpha_{2\mu+1}[x_{2\mu+1}^{-1}, e_{i,i'}] + \alpha_{2\mu}[x_{2\mu}, e_{i,i'}] \\ \sigma &= \alpha_2[x_1, e_{i,i'}] + \sum_{\mu=1}^{m} \alpha_{2\mu}[x_{2\mu}^{-1}, e_{i,i'}] + \alpha_{2\mu-1}[x_{2\mu-1}, e_{i,i'}] \\ \sigma &= \alpha_2[x_1, e_{i,i'}] + \sum_{\mu=1}^{m} \alpha_{2\mu}[x_{2\mu}^{-1}, e_{i,i'}] + \alpha_{2\mu-1}[x_{2\mu-1}, e_{i,i'}]\end{aligned}$$

The reader who went through the proof of Lemma 2.12, will now easily verify that it is again possible for suitable choices of the $\alpha_\nu \in \kappa$ to obtain $\sigma = (0, 0, \ldots, 0, 1)$. Therefore the proof of the analogue of Lemma 2.12 for the $D_2^{i,f}(m)$ will pose no further problems.

Remark 2.15 There is another case worth mentioning in which one can use the above proof in an inductive argument to construct lifts to characteristic zero. Namely suppose we know that $\bar{\tau}(t_2) - 1$ has rank $n - 1$. In particular, we have $\mathcal{I} = \mathcal{J}$. In each inductive step, we choose lifts of the X_i such that $Y_i \in U_n(W_l(\kappa))$ for $i > 1$ and $Y_1 \in B_n(W_l(\kappa))$ with diagonal $(1, (1+q)^{-1}, \ldots, (1+q)^{1-n})$. With these choices, $I - P_1 \ldots P_m$ will be in $U^{\mathcal{I}}(W_l(\kappa))$. As in the proof of the above proposition, the induction now uses the sharpened version of Lemma 2.12.

3 Local lifts to characteristic zero

Fix a prime-power l with $p \not| l$ and define

$$\hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/(n) \quad \text{and} \quad \mathbb{Z}' := \varprojlim_{n,(n,l)=1} \mathbb{Z}/(n).$$

Note that $\hat{\mathbb{Z}}$ is isomorphic to the infinite product over all $\mathbb{Z}_r$, where r runs through all prime numbers, and $\hat{\mathbb{Z}}'$ is isomorphic to the product over the same groups over all r not dividing l. Finally define $G_l^t := \hat{\mathbb{Z}}' \rtimes \hat{\mathbb{Z}}$, where $x \in \hat{\mathbb{Z}}$ acts on $y \in \hat{\mathbb{Z}}'$ by $y \mapsto l^x y$. The expression l^x is well-defined as an element in $\hat{\mathbb{Z}}'$, since for any $\tilde{x}, \tilde{x}' \in \mathbb{Z}$ with $\tilde{x} \equiv \tilde{x}' \pmod{\phi(n)}$, one has $l^{\tilde{x}} \equiv l^{\tilde{x}'} \pmod{n}$, where $\phi(n)$ is the usual ϕ-function on positive integers. By I_l^t we denote the normal subgroup $\hat{\mathbb{Z}}'$ of G_l^t.

The main result of this section is the following:

Proposition 3.1 *Any representation $\bar{\tau} : G_l^t \to \mathrm{GL}_n(\kappa)$ with $\bar{\tau}(I_l^t)$ a p-group has a lift to $W(\kappa)$.*

We first give an application:

Proof of Theorem 1.3: Let K be a local field whose (finite) residue field is of order l' not divisible by p and let $\bar{\rho}\colon G_K \to \mathrm{GL}_n(\kappa)$ be such that $\bar{\rho}(I_K)$ is a p-group. Let R be any complete noetherian local ring with residue field κ and $\rho\colon G_K \to \mathrm{GL}_n(R)$ be any lift of $\bar{\rho}$. Since the kernel of $\mathrm{GL}_n(R) \to \mathrm{GL}_n(\kappa)$ is a pro-p group, the kernel of $\rho(I_K) \to \bar{\rho}(I_K)$ is a

pro-p group as well, and therefore $\rho(I_K)$ is of order prime to l'. In particular ρ factors via the tame quotient of G_K. This quotient is well-known to be isomorphic to $G^t_{l'}$, and in such a way that I_K maps onto the normal subgroup I^t_l of G^t_l, cf. [Se1], Ex. IV §2.2. The result now follows from Proposition 3.1. ∎

To prove the above proposition, denote by s, t the image of $1 \in \mathbb{Z}$ in $\hat{\mathbb{Z}}$ and $\hat{\mathbb{Z}}'$, respectively, so that s, t topologically generate G^t_l subject to the only relation $sts^{-1} = t^l$, written mulitplicatively. Now any morphism of G^t_l into some profinite group G is determined by the images of s, t, and conversely, given any two elements $S, T \in G$, with $STS^{-1} = T^l$ and T of profinite order prime to l, there exists a unique homomorphism with $s \mapsto T$ and $t \mapsto T$.

We let $a, b \in \mathrm{GL}_n(\kappa)$ denote the images of the generators s, t under $\bar{\rho}$, so that they satisfy the relation $ab = b^l a$. Since $\bar{\rho}(t)$ is of p-power order, all its eigenvalues are equal to 1. By chosing an appropriate basis for κ^n, we may therefore assume that $b \in U_n(\kappa)$ is given in Jordan canonical form. By $B \in U_n(W(\kappa))$ we denote that matrix in Jordan canonical form which reduces to b modulo p, and so in particular the only entries of B are 0 and 1. To prove the above proposition it suffices to construct a lift $A \in \mathrm{GL}_n(W(\kappa))$ of a such that $AB = B^l A$. Define $N = B - I$ and $\bar{N} = b - I$. By rewriting the given relation for A, B, one sees that Proposition 3.1 is a consequence of the following, which we prove below

Proposition 3.2 *There exists a matrix $A \in \mathrm{GL}_n(W(\kappa))$ reducing to a modulo p such that*

$$AN = \left(\sum_{i=1}^{l} \binom{l}{i} N^i \right) A. \tag{5}$$

Proposition 3.2 is an assertion on linear equations. We will need the following lemma on the behavior of solutions to linear equations under 'small' distortions.

Lemma 3.3 *Let R be any commutative ring and $f \in R[x]/(x^m)$ a polynomial such that $f(0) = 0$ and $f'(0)$ is a unit in R. Suppose we are given matrices $C, D, E \in M_m(R)$ such that i) C commutes with D and E, ii) C is nilpotent (hence $C^m = 0$) , and iii) D, E satisfy the relations $DE^i D^i = E^{i-1} D^i$ for all $i \geq 1$. Then there exists an R-linear automorphism T_R of R^m which induces an R-linear isomorphism between the R-modules*

$$V_1(R) := \{v \in R^m : Dv = Cv\} \subset R^m \text{ and}$$

$$V_2(R) := \{v \in R^m : Dv = f(C)v\} \subset R^m.$$

The transformation T_R is given by an explicit expression in terms of f, C, E, which is given in the proof.

Furthermore let $\phi : R \to R'$ be a ring homomorphism and define $V_1(R')$, $V_2(R')$ in the obvious way. Define $T_{R'}$ by substituting $\phi(f), \phi(C), \phi(E)$ for f, C, E, in the expression for T_R. Then $T_{R'}$ is an automorphism of R'^m which induces an R'-linear bijection between $V_1(R')$ and $V_2(R')$.

Proof: Since $f(0) = 0$ and $f'(0)$ is a unit, one can show by induction on m that there exists a unique $h(x) \in R[x]/(x^m)$ such that $f(h(x)) = x$ and $h(f(x)) = x$. Using h, it is easy to find $g \in R[x]/(x^m)$ such that $x = f(x)g(f(x))$.

For suitable, yet to be defined $\alpha_{j,k}$, we define T_R, or simply T, by

$$T := \left(I + \sum_{j=1}^{\infty} \sum_{k=j}^{(m-1)j} \alpha_{j,k} E^j C^k \right).$$

If we succeeded in constructing T so that $(D - f(C))T = D - C$, then the proof would be completed, as T is clearly unipotent (E and C commute and C is nilpotent!), and T maps V_2 to V_1, and T^{-1} the space V_1 to V_2. The lemma would follow. This however is too much to hope for, and it is not quite needed. Vaguely speaking, 'we only need $(D-f(C))T = D-C$ to hold on elements of V_1'.

We define elements $f_i \in R$ by $f(x) = f_1 x + f_2 x + \dots f_{m-1} x^{m-1}$ and $f_i = 0$ for i not in the range $1, \dots, m-1$, and set recursively $\alpha_{1,k} = f_k - \delta_{1,k}$ and

$$\alpha_{j,k} = \sum_{l=j-1}^{(m-1)(j-1)} f_{k-l} \alpha_{j-1,l} \quad \text{for } j > 1.$$

Furthermore define $L := (D - f(C))T - (D - C)$. Based on the above recursive definition of the $\alpha_{j,k}$, one can check that

$$L = \sum_{j=1}^{\infty} \sum_{k=j}^{(m-1)j} \alpha_{j,k} (DE - I) E^{j-1} C^k.$$

Now we are ready to prove the lemma. Let v' be a solution in V_1. Then $(D - C)v = 0$ and hence $C^k v = D^k v$, as C and D commute. By (ii) we have $(DE - I)E^{j-1}D^k = 0$ for all $k \geq j$, so that $Lv = 0$. Therefore

$$0 = Lv = ((D - f(C))T - (D - C))v = (D - f(C))Tv,$$

and so Tv is in V_2. Conversely, say v is a solution in V_2. Then $(D-f(C))v = 0$. We multiply this on the left by $g(f(C))$. Because C and D commute, the equation $x = f(x)g(f(x))$ implies $(Dg(f(C)) - C)v = 0$, and therefore we find

$$C^k v = D^k g(f(C))^k v \quad \forall k \geq 0.$$

We claim that $LT^{-1}v = 0$. As T is unipotent, we can express its inverse as the series $\sum_{i=0}^{\infty} (I - T)^i$. Distributing all the terms in the expression for $LT^{-1}v$, we find that, up to a constant, every term can be written as

$$(I - DE)E^{j_0 - 1} C^{k_0} E^{j_1} C^{k_1} \dots E^{j_l - 1} C^{k_l} v$$

where $1 \leq j_i \leq k_i$. As C, E commute, abbreviating $k = \sum k_i$ and $j = \sum j_i$, we can rewrite the above expression as

$$(I - DE)E^{j-1}C^k v = (I - DE)E^{j-1}D^k g(f(C))^k v$$

with $j \leq k$. By (ii) the latter term is zero, and we find

$$0 = LT^{-1}v = (D - f(C))v - (D - C)T^{-1}v = (D - C)T^{-1}v$$

and thus $T^{-1}v \in V_1$. So T is an R-linear isomorphism between V_2 and V_1 with inverse T^{-1}. The statement about the relation of $T_{R'}$ and T_R under the map $\phi : R \to R'$ is obvious from the construction of T_R. ∎

Remark 3.4 If D is invertible, then our relations among D, E are equivalent to $E = D^{-1}$. But even if D is singular, as we will see below, there are often situations where one can find E, given the matrix D.

PROOF OF Proposition 3.2: We think of (5) as a linear equation in $m = n^2$ indeterminates, the matrix entries of A. We define $R = \mathbb{Z}[1/(l)]$, and take for C the R-linear transformation given by right multiplication with N, and for D, E the R-linear transformations given by left multiplication by N and N^t, respectively. $f(x)$ will be the polynomial $\sum_{i=1}^{l} \binom{l}{i} x^i$. One easily verifies all the conditions of Lemma 3.3. Thus over any R-algebra S we have an isomorphism of the solution spaces $V_1(S) = \{A \in M_n(S) : NA = AN\}$ and $V_2(S) = \{A \in M_n(S) : NA = Af(N)\}$, given by an explicit transformation defined over R.

We now claim that $M_n(R)/V_1(R)$ is flat over R. Let us assume the claim for the moment. As T_R is an R-linear isomorphism, the R-module $M_n(R)/V_2(R)$, too, is flat over R, and hence by base change $M_n(W(\kappa))/V_2(W(\kappa))$ is flat over $W(\kappa)$. This implies that $V_2(\kappa) \cong V_2(W(\kappa)) \otimes_{W(\kappa)} \kappa$. Thus our given solution $a \in V_2(\kappa)$ arises as the mod p reduction of an element $A \in V_2(W(\kappa))$, and the proof of Proposition 3.2 is completed.

To show the flatness of $M_m(R)/V_1(R)$ as an R-module, we will construct an R-basis of $V_1(R)$ and show that it can be completed to an R-basis of $M_m(R)$. Hence $M_m(R)/V_1(R)$ is a free R-module, finishing the proof of the claim. We now construct the respective basis for $V_1(R)$ and $M_n(R)$:

Say N is given by

$$N = \begin{pmatrix} N_1 & 0 & \dots & 0 \\ 0 & N_2 & \dots & 0 \\ .. & .. & .. & .. \\ 0 & 0 & \dots & N_k \end{pmatrix},$$

where the N_i are simple $n_i \times n_i$ Jordan blocks in $U_{n_i}(R)$. We write an $n \times n$ matrix A as

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,k} \\ A_{2,1} & A_{2,2} & \dots & A_{2,k} \\ .... & .... & .. & .... \\ A_{k,1} & A_{k,2} & \dots & A_{k,k} \end{pmatrix},$$

where the submatrix $A_{i,j}$ is of size $n_i \times n_j$. Then the equation $NA = AN$ breaks up into k^2 equations $N_i A_{i,j} = A_{i,j} N_j$.

Let $d_{i,j} := \min\{n_i, n_j\}$. The solution space of $N_i A_{i,j} = A_{i,j} N_j$ is a free R-module of rank $d_{i,j}$ and a basis for it is given by the matrices

$$M_l := \sum_{i=1}^{d_{i,j}-l} e_{i,n_j-d_{i,j}+i} \text{ for } l = 0, \dots, d_{i,j} - 1.$$

If $n_i < n_j$, a complementary basis is the set of matrices $e_{i,j}$, $i = 1, \dots, n_i$, $j = 1, \dots, n_j - 1$ and, if $n_i \geq n_j$, the set $e_{i,j}$, $i = 1, \dots, n_i - 1$, $j = 1, \dots, n_j$. This finishes the proof of the above claim. ∎

4 Global lifting

With Theorem 1.1 at our disposal, the proof of Theorem 1.5 will follow rapidly. We let K be a global field and $S \supset S_p \cup S_\infty$ a finite set of places outside which $\bar{\rho} : G_K \to \mathrm{GL}_n(\kappa)$ is unramified. We first formulate the analogue of Theorem 1.5 for lifts with fixed determinant:

Theorem 4.1 *Let K be a global field of characteristic different from p, $\bar{\rho}\colon G_K \to \mathrm{GL}_n(\kappa)$ a representation and η a lift of $\det\bar{\rho}$ to $W_2(\kappa)$. Assume that $\mathrm{ad}^0_{\bar{\rho}}$ is globally unobstructed. If $p \not| n$, then $\bar{\rho}$ has a lift $\rho : G_K \to \mathrm{GL}_n(W_2(\kappa))$ with determinant η. If $p|n$, the same assertion holds if one further assumes that for all $\mathfrak{p} \in S$ the representation $\bar{\rho}_{|G_{K_\mathfrak{p}}}$ has a lift to $W_2(\kappa)$ with determinant $\eta_{|G_{K_\mathfrak{p}}}$.*

For any finite $\kappa[G_{K,S}]$-module X, define $Ш^2_S(K,X)$ through the left exact sequence

$$0 \longrightarrow Ш^2_S(K,X) \longrightarrow H^2(G_{K,S},X) \stackrel{\alpha_S(X)}{\longrightarrow} \coprod_{\mathfrak{p}\in S} H^2(G_{K_\mathfrak{p}},X),$$

where the maps $H^2(G_{K,S},X) \to H^2(G_{K_\mathfrak{p}},X)$ are the restriction maps from cohomology, and where for each place $\mathfrak{p}$ one has chosen an embedding $G_{K_\mathfrak{p}} \to G_{K,S}$, i.e., one has singled out a decomposition group in $G_{K,S}$ above $\mathfrak{p}$.

Recall that $H = \mathrm{Gal}(L(\zeta_p)/K)$, where L is the splitting field of $\bar{\rho}$, and that by $H_\mathfrak{p} \subset H$ we denote a decomposition group above a place $\mathfrak{p}$ of K. The following result is easily obtained by the methods in [Bö], §6, where it is only stated in the number field case. It is based on Poitou-Tate duality and the Cebotarov density theorem, cf. [NSW], Thm. 8.6.13, [Neu], Satz 13.4, [Ja]. We omit the proof.

Lemma 4.2 *Suppose the characteristic of K is different from p and X is a finite $\kappa[H]$-module. Then for any sufficiently large finite $S' \supset S$ there is a left exact sequence*

$$0 \longrightarrow Ш^2_{S'}(K,X)^* \longrightarrow H^1(H,X^*(1)) \longrightarrow \coprod_{\mathfrak{p}\in S'} H^1(H_\mathfrak{p},X^*(1)).$$

Note that for places $\mathfrak{p} \in S' - S$ the groups $H_\mathfrak{p}$ are cyclic and that by the Cebotarov density theorem any cyclic subgroup of H occurs infinitely often as a decomposition group. Therefore X is globally unobstructed if and only if $Ш^2_{S'}(K,X) = 0$ for sufficiently large $S' \supset S$.

We use this point to comment on a mistake in loc. cit., where it was erroneously asserted that $\mathrm{ad}^0_{\bar{\rho}}$ is self dual. However this is only the case when $p \not| n$. In general, the dual of $\mathrm{ad}^0_{\bar{\rho}}$ is isomorphic to $\overline{\mathrm{ad}}_{\bar{\rho}}$, i.e., the quotient of $\mathrm{ad}_{\bar{\rho}}$ by the scalar matrices. To correct this, one has to replace in [Bö], p. 223, each occurrence of $\mathrm{ad}^0_{\bar{\rho}}(1)$ by $\mathrm{ad}^{0*}_{\bar{\rho}}(1)$.

Proof of Theorem 1.5: As is well known, the obstruction to finding a lift of $\bar{\rho}$ to $W_2(\kappa)$, unramified outside $S' \supset S$, is given by an element $\theta_{S'} \in H^2(G_{K,S'},\mathrm{ad}_{\bar{\rho}})$. Let $\theta_\mathfrak{p}$ be its image in $H^2(G_{K_\mathfrak{p}},\mathrm{ad}_{\bar{\rho}})$ under the restriction map $\alpha_{S'}(\mathrm{ad}_{\bar{\rho}})$. This is the obstruction to finding a lift to $W_2(\kappa)$ of the restriction $\bar{\rho}_{|G_{K_\mathfrak{p}}}$. By Theorem 1.1 all $\theta_\mathfrak{p}$ vanish and hence $\theta_{S'}$ must be in the kernel $Ш^2_{S'}(K,\mathrm{ad}^0_{\bar{\rho}})$ of $\alpha_{S'}(\mathrm{ad}_{\bar{\rho}})$ for any finite S' containing S.

Let $H_i \subset H$ be cyclic subgroups that are used in showing that $\mathrm{ad}_{\bar{\rho}}$ is globally unobstructed, cf. above Theorem 1.5. By the Cebotarov density theorem there exist places $\mathfrak{p}_i$

not in S such the H_i agree with a decomposition group $H_{\mathfrak{p}_i}$ at $\mathfrak{p}_i$. Let $S' \supset S \cup \{\mathfrak{p}_i : i\}$ be sufficiently large in the sense of the previous lemma. Then by this lemma and global unobstructedness, we have $Ш^2_{S'}(K, \mathrm{ad}^0_{\bar\rho}) = 0$. It follows that $\theta_{S'}$ is zero, as asserted. ∎

The proof of Theorem 4.1 is quite analogous. The obstruction $\theta_{S'}$ to consider lies in $H^2(G_{K,S'}, \mathrm{ad}^0_{\bar\rho})$. For its vanishing, one needs that $\mathrm{ad}^0_{\bar\rho}$ is globally unobstructed which in turn shows that $Ш^2_{S'}(K, \mathrm{ad}^0) = 0$ for any 'sufficiently large finite S'', and also the vanishing of all the local obstructions $\theta_{\mathfrak{p}}$. Details are left to the reader.

Remark 4.3 There are quite simple examples, based on Lemma 4.2 for which $Ш^2_{S'}(K, \mathrm{ad}_{\bar\rho})$ vanishes for no finite S'. Here we give two examples that may be checked using the explicit description of the cohomology of cyclic groups and the inflation-restriction sequence. The first of these in particular shows that the Theorem 1.5 does not recover [Kha]:

Suppose κ is of degree 2 over $\mathbb{F}_p$. Take $n = 2$ and $H = U_2(\kappa)$. Suppose all $H_{\mathfrak{p}}$ are cyclic and that all cyclic groups occur as $H_{\mathfrak{p}}$. Then for no finite S', the group $Ш^2_{S'}(K, \mathrm{ad}_{\bar\rho})$ is zero.

Suppose $\kappa = \mathbb{F}_p$, and H is the subgroup of $U_3(\mathbb{F}_p)$ generated by $I + e_{1,2} + e_{2,3}$ and $I + e_{1,3}$. Suppose each cyclic subgroup of H occurs among the $H_{\mathfrak{p}}$ for some place $\mathfrak{p}$ of S. Then there exists no S' containing S such that $Ш^2_{S'}(K, \mathrm{ad}_{\bar\rho})$ is zero.

The case where K has characteristic p, is rather simple as the following proof of Theorem 1.7 shows.

Proof: Let $\bar\rho\colon \Pi_1(X) \to \mathrm{GL}_n(\kappa)$. We will show that $H^2(\Pi_1(X), \mathrm{ad}_{\bar\rho}) = 0$. The obstruction to lifting a lift $\rho_l : \Pi_1(X) \to \mathrm{GL}_n(W_l(\kappa))$ to $\rho_{l+1} : \Pi_1(X) \to \mathrm{GL}_n(W_{l+1}(\kappa))$ is given by an element in $H^2(\Pi_1(X), \mathrm{ad}_{\bar\rho})$, which by the above claim is zero. Therefore one can inductively construct the desired lift to $W(\kappa)$.

Let P be a p-Sylow subgroup of $\mathrm{Im}(\bar\rho)$ and denote by Y the étale cover of X corresponding to $\bar\rho^{-1}(P)$. As $[\Pi_1(X) : \Pi_1(Y)]$ is of order prime to p, the restriction map $H^2(\Pi_1(X), \mathrm{ad}_{\bar\rho}) \to H^2(\Pi_1(Y), \mathrm{ad}_{\bar\rho})$ is injective, and it will suffice to show that the module $H^2(\Pi_1(Y), \mathrm{ad}_{\bar\rho})$ vanishes.

As $\Pi_1(Y)$ acts via a p-group on $\mathrm{ad}_{\bar\rho}$, the latter Galois module has a decomposition series all of whose subquotients are isomorphic to κ - with necessarily trivial Galois action. Thus by devissage it is enough to show that $H^2(\Pi_1(Y), \kappa) = 0$. The latter now follows by a standard application of Artin-Schreier theory, which shows that $H^i_{\acute et}(Z, \mathbb{F}_p) = 0$ for all $i > 1$ and all affine noetherian schemes Z over $\mathbb{F}_p$, cf. [SGA4], VII.4.3 and IX.3.5. ∎

5 A vanishing criterion for $H^1(H, \mathrm{ad})$

Now we turn to the proof of Theorem 1.9. As an application, we give in Proposition 1.8 a criterion for $\mathrm{ad}_{\bar\rho}$ to be globally unobstructed. In the proof, we closely follow the arguments in [CPS]. Throughout, we use the notation from Theorem 1.9.

For $i, j \in \{1, \ldots, n\}$ we define $\chi_{i,j} : T \to \kappa^*$ to be the character which sends the diagonal matrix $(\lambda_1, \ldots, \lambda_n)$ to λ_i/λ_j. This character factors via $\bar T$. One calls two characters

$\psi, \phi\colon T \to \kappa^*$ equivalent, $\psi \sim \phi$, if there exists $\sigma \in \mathrm{Gal}(\kappa/\mathbb{F}_p)$ such that $\sigma\psi = \phi$. One has the following basic lemma, whose proof we omit.

Lemma 5.1 *Assume that $\bar{T}$ contains $\overline{\mathrm{ST}}_n(\kappa')$ for some field κ' of cardinality at least 7, if $n = 2$, at least 5 if $n = 3$ or at least 4, if $n > 3$. Then for $i \neq j$ and $i' \neq j'$ one has $\chi_{i,j} \sim \chi_{i',j'}$ only if ($i = i'$ and $j = j'$) or ($i = j$ and $i' = j'$).*

The characters $\chi_{i,j}$ appear naturally in the conjugation action of T on

$$U_{i,j} := \Big\{ I + ae_{i,j} | a \in \kappa \Big\} \cong (\kappa, +),$$

because for $t \in T$ and $a \in \kappa$, one has $t(I + ae_{i,j})t^{-1} = I + \chi_{i,j}(t)ae_{i,j}$. For $k \in \{1, \ldots, n'\}$, define $U_k := (U \cap U_{i_k,j_k})$.

For any group $\tilde{G}$ and any $\kappa[\tilde{G}]$-module V, we denote by $B^1(\tilde{G}, V)$ the 1-coboundaries of $\tilde{G}$ with coefficients in V and by $Z^1(\tilde{G}, V)$ the 1-cocycles with coefficients in V. If V is a $\kappa[T]$-module and ψ a character of T, then V_ψ denotes the ψ-isotypical component of V.

Lemma 5.2 *Let L be a $\kappa[U_k \rtimes T]$-module.*

(i) If L is one-dimensional, and if ψ is the character by which T acts on the one-dimensional module L, then

$$\dim_\kappa Z^1(U_k, L)^T = \begin{cases} 1 & \text{if } \psi \sim \chi_{i_k,j_k}, \\ 0 & \text{otherwise.} \end{cases}$$

(ii) For arbitrary L one has

$$\dim_\kappa Z^1(U_k, L)^T \leq \sum_{\psi \sim \chi_{i_k,j_k}} \dim_\kappa L_\psi.$$

Proof: (i) As U_k is a p-group and must therefore act trivially on the one-dimensional κ-module L, we have

$$Z^1(U_k, L)^T = H^1(U_k, L)^T = \mathrm{Hom}_{\mathbb{F}_p}(U_k, L)^T = \mathrm{Hom}_{\mathbb{F}_p[T]}(U_k, L).$$

Let κ'' denote the smallest subfield of κ containing $\chi_{i_k,j_k}(T)$. Then by assumptions (iii) and (iv) the group U_k is isomorphic to κ'' with T acting via the character χ_{i_k,j_k}. A generator over κ'' is given by u_k. Therefore U_k is irreducible as an $\mathbb{F}_p[T]$-module. If $\psi \not\sim \chi_{i_k,j_k}$ we must have $\mathrm{Hom}_{\mathbb{F}_p[T]}(U_k, L) = 0$ by Schur's lemma.

Let us now assume $\psi \sim \chi_{i_k,j_k}$. Then κ'' is also the smallest field containing $\psi(T)$, and if L'' denotes the module κ'' with T acting via ψ, then L is a direct sum of $[\kappa : \kappa'']$ copies of L'' as an $\mathbb{F}_p[T]$-module. Since $\psi \sim \chi_{i_k,j_k}$ it follows that L'' and U_k are isomorphic as $\mathbb{F}_p[T]$-modules. Part (i) now follows from

$$\dim_\kappa \mathrm{Hom}_{\mathbb{F}_p[T]}(U_k, L) = \dim_{\kappa''} \mathrm{Hom}_{\mathbb{F}_p[T]}(U_k, L'') = 1.$$

(ii) For any left exact sequence $0 \longrightarrow V' \longrightarrow V \longrightarrow V''$ of $\kappa[U_k \ltimes T]$-modules, the sequence $0 \to Z^1(U_k, V') \to Z^1(U_k, V) \to Z^1(U_k, V'')$ is left exact. As taking T-invariants is left exact as well, one obtains

$$0 \to Z^1(U_k, V')^T \to Z^1(U_k, V)^T \to Z^1(U_k, V'')^T.$$

Since the exponent of T divides the order of κ^*, every irreducible $\kappa[T]$-module has dimension 1 over κ. As U_k is a normal p-group, every irreducible $\kappa[U_k \rtimes T]$-module will have dimension 1 as well. Hence L has a decomposition series over $\kappa[U_k \rtimes T]$ with one-dimensional subfactors, which is a direct sum decomposition when viewed over $\kappa[T]$. The desired result follows from part (i) and the above left exact sequence. ∎

Proof of Theorem 1.9: Let us first prove $H^1(G, \overline{\mathrm{ad}}) = 0$. By the inflation-restriction sequence combined with the fact that T has order prime to p, we find that

$$\dim_\kappa H^1(G, \overline{\mathrm{ad}}) \quad = \quad \dim_\kappa H^1(U, \overline{\mathrm{ad}})^T.$$

Since T is of order prime to p, taking T-invariants is an exact functor for $\kappa[T]$-modules, and hence we have

$$\dim_\kappa H^1(U, \overline{\mathrm{ad}})^T = \dim_\kappa Z^1(U, \overline{\mathrm{ad}})^T - \dim_\kappa B^1(U, \overline{\mathrm{ad}})^T.$$

To estimate the first term, one observes that

$$Z^1(U, \overline{\mathrm{ad}})^T \to \coprod_k Z^1(U_k, \overline{\mathrm{ad}})^T$$

is injective, as 1-cocycles c are given by the defining property $c(gh) = c(g)h + c(h)$ and as U is generated by the U_k. By the previous lemma we obtain

$$\dim_\kappa Z^1(U, \overline{\mathrm{ad}})^T \leq \sum_{k=1}^{n'} \sum_{\chi_{i,j} \sim \chi_{i_k, j_k}} \dim_\kappa \overline{\mathrm{ad}}_{\chi_{i,j}}.$$

By Lemma 5.1 and condition (ii) of our assumptions, the relation $\chi_{i,j} \sim \chi_{i_k,j_k}$ implies $(i,j) = (i_k, j_k)$ because $i_k < j_k$, and so the term on the right equals n'.

For the second term, one considers the map $\overline{\mathrm{ad}} \to B^1(U, \overline{\mathrm{ad}})$ that sends an element $v \in \overline{\mathrm{ad}}$ to the 1-coboundary $u \mapsto v - vu$. The kernel equals $(\overline{\mathrm{ad}})^U$ and the image is isomorphic to $\overline{\mathrm{ad}}/\overline{\mathrm{ad}}^U$. All maps are maps of $\kappa[T]$-modules. Taking T-invariants, which is (left) exact, one obtains the exact sequence

$$0 \longrightarrow \overline{\mathrm{ad}}^G \longrightarrow \overline{\mathrm{ad}}^T \longrightarrow B^1(U, \overline{\mathrm{ad}})^T.$$

As $\bar{T}$ contains $\overline{\mathrm{ST}}_n(\kappa')$, none of the characters $\chi_{i,j}$, $i \neq j$ is trivial, and thus the set $\overline{\mathrm{ad}}^T$ consists precisely of the set of diagonal matrices in $\overline{\mathrm{ad}}$. For a diagonal matrix d, the condition $u_k d = d u_k$ implies that the entries at the i_k-th and j_k-th spot must agree, and this is still true modulo the set of scalar matrices. Therefore condition (iv) implies that $\dim_\kappa \overline{\mathrm{ad}}^G = (n-1) - n'$. Hence

$$\dim_\kappa B^1(U, \overline{\mathrm{ad}})^T \geq \dim_\kappa \overline{\mathrm{ad}}^T - \dim_\kappa \overline{\mathrm{ad}}^G = (n-1) - (n - n' - 1) = n'.$$

Combining the two estimates, we find that $\dim_\kappa H^1(G, \overline{\mathrm{ad}}) \leq 0$.

To prove $H^1(G, \mathrm{ad}) = 0$, we note first that by the above lemma $Z^1(G, \kappa) = 0$, where we regard κ as a trivial $\kappa[G]$-module. Now the assertion follows easily from the long exact

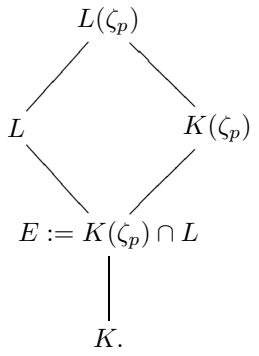
sequence of cohomologies for G which arises from to the short exact sequence $0 \longrightarrow \kappa \longrightarrow \mathrm{ad} \longrightarrow \overline{\mathrm{ad}} \longrightarrow 0$.

For the last part of the theorem, consider $G := \mathrm{SL}_n \cap B_n(\kappa)$. Under the given conditions on κ, this group clearly satisfies all our hypothesis, and so $H^1(G, \mathrm{ad}) = 0$. Since G contains a p-Sylow subgroup of $\mathrm{SL}_n(\kappa)$ and since ad is p-primary, the restriction map

$$H^1(\mathrm{SL}_n(\kappa), \mathrm{ad}) \to H^1(G, \mathrm{ad})$$

is injective, and the proof of Theorem 1.9 is completed. ∎

Proof of Proposition 1.8: For (i) and (ii), we consider the following diagram of fields



As L and $K(\zeta_p)$ are Galois over E and linearly disjoint, it follows that

$$\mathrm{Gal}(L(\zeta_p)/E) \cong \mathrm{Gal}(L(\zeta_p)/L) \times \mathrm{Gal}(L(\zeta_p)/K(\zeta_p))$$

and $\mathrm{Gal}(L(\zeta_p)/K(\zeta_p)) \cong \mathrm{Gal}(L/E)$. As $\mathrm{Gal}(E/K)$ is of order prime to p, we find that

$$\begin{aligned} H^1(\mathrm{Gal}(L(\zeta_p)/K), \mathrm{ad}_{\bar\rho}(1)) &\hookrightarrow H^1(\mathrm{Gal}(L(\zeta_p)/E), \mathrm{ad}_{\bar\rho}(1)) \\ &\cong H^1(\mathrm{Gal}(L(\zeta_p)/K(\zeta_p)), \mathrm{ad}_{\bar\rho})(1)^{\mathrm{Gal}(K(\zeta_p)/E)}. \end{aligned}$$

In case (ii), our assumption says that $H^1(\mathrm{Gal}(L(\zeta_p)/K(\zeta_p)), \mathrm{ad}_{\bar\rho}) = 0$. In case (i), the group $\mathrm{Gal}(K(\zeta_p)/E)$ acts trivially on $H^1(\mathrm{Gal}(L(\zeta_p)/K(\zeta_p)), \mathrm{ad}_{\bar\rho})$, and since it acts non-trivially on $\mathbb{F}_p(1)$, the module of invariants $H^1(\mathrm{Gal}(L(\zeta_p)/K(\zeta_p)), \mathrm{ad}_{\bar\rho})(1)^{\mathrm{Gal}(K(\zeta_p)/E)}$ is zero. In either case we find $H^1(\mathrm{Gal}(L(\zeta_p)/K), \mathrm{ad}_{\bar\rho}(1)) = 0$.

Part (iii) is immediate from (ii) and Theorem 1.9. Finally, assume that H contains $\mathrm{SL}_n(\kappa)$ and that $\zeta_p \in L$. Our conditions on n, κ ensure among other things that $\mathrm{SL}_n(\kappa)$ is simple. The above diagram shows that $H \cong \mathrm{Gal}(L/K)$ contains $H' \cong \mathrm{Gal}(L/K(\zeta_p))$ as a normal subgroup with abelian quotient. As $\mathrm{SL}_n(\kappa) \subset H$ is simple it must therefore be contained in H'. We conclude using Theorem 1.9 and parts (i) and (ii). ∎

References

[Bö] G. Böckle, A local-to-global principle for deformations of Galois representations, J. Reine Angew. Math. **509** (1999), 199–236.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor *On the modularity of elliptic curves over* $\mathbb{Q}$, to appear in the J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

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

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

[EK] M. Emerton, M. Kisin, *Unit L-functions and a conjecture of Katz*, Ann. of Math. (2) **153** (2001), no. 2, 329–354.

[Ja] M. Jarden, *The Čebotarev density theorem for function fields: an elementary approach*, Math. Ann. **261** (1982), no. 4, 467–475.

[Kha] C. Khare, *Base Change, Lifting and Serre's Conjecture*, J. Number Theory **63** (1997), 387–395.

[Koc] H. Koch, *Galoissche Theorie der p-Erweiterungen*, Mathematische Monographien, Band 10, VEB Deutscher Verlag der Wissenschaften, Berlin 1970.

[Lab] J. Labute, *Classification of Demushkin groups*, Can. J. Math. **19** (1966), 106–132.

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

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

[Ra1] R. Ramakrishna, *Lifting Galois representations*, Invent. Math. **138** (1999), no. 3, 537–562.

[Ra2] R. Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur*, Ann. of Math. (2) **156** (2002), no. 1, 115–154.

[Se1] J.-P.Serre, *Local fields*, GTM **67**, Springer-Verlag, New York-Berlin, 1979.

[Se2] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math. Journ. **54** (1987), 179–230.

[SGA4] M. Artin, A. Grothendieck, *Théorie des topos et cohomologie étale des schémas (SGA4)*, Lecture Notes in Math. 269, 270, 305, Springer-Verlag, New-York, Berlin, Heidelberg, 1972-73.

[Tay] R. Taylor, *Remarks on a conjecture by Fontaine and Mazur*, preprint.

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

[Wil] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.