Deformations and the rigidity method

by

Gebhard Böckle
Fachbereich Mathematik
Universität Duisburg-Essen
Universitätsstraße 2, 45141 Essen, Germany

e-mail: boeckle@iem.uni-due.de

September 8, 2008

Abstract

In [Ro1, Ro2], Rohrlich proved rigidity for $\mathrm{PSL}_2(\mathbb{Z}_p[[T]])$ for $p > 5$, obtained this group as a Galois group over $\mathbb{C}(t)$ using modular function fields and derived from this interesting consequences for Galois representations attached to the Tate modules of elliptic curves. Furthermore in an unpublished preprint, he established that the corresponding Galois representation $G_{\mathbb{C}(t)} := \mathrm{Gal}(\mathbb{C}(t)^{\mathrm{alg}}/\mathbb{C}(t)) \longrightarrow \mathrm{PSL}_2(\mathbb{Z}_p[[T]])$ is universal.

Here we will turn things around. We first provide a general framework for rigid deformations of (projective) representations of the absolute Galois group of a function field (in one variable) over a separably closed base. Under natural, rather general hypothesis, we will determine the corresponding universal deformation ring. If the residual representation is 'geometrically rigid', which happens to be the case for many surjective representation to $\mathrm{PSL}_2(\mathbb{F}_p)$, $p > 2$, which arise from Belyi triples, then certain universal deformations will be 'geometrically rigid', too. This will give new proofs for most of the results of Rohrlich. Our method also applies to Thompson tuples.

We then go on to give two further applications, which are based on the example computed by Rohrlich. Over $\mathbb{F}_q(t)$, where q is a power of a prime l, we construct infinite p-adic Galois extensions which have finite ramification and whose constant field is finite. Furthermore for $p > 5$ and $p \equiv 1(\mathrm{mod}\ 4)$, we obtain a family of surjective Galois representations $\rho_\zeta : \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q}(\zeta + \zeta^{-1})) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}_p[\zeta + \zeta^{-1}])$, where the parameter ζ runs over all p-power roots of unity. Finally, we exhibit a general class of rigid universal deformation rings which are finite flat over $\mathbb{Z}_p$. In particular this shows that the above examples ρ_ζ of Galois representations are not a singular event, but a general phenomenon.

1 Introduction

The rigidity method has been very important in the study of the inverse Galois problem. For instance, we know due to the work of Belyi and others, cf. [Bel] or [MM], that most simple groups can be realized as Galois groups over suitable abelian extensions of $\mathbb{Q}$. The method was also used in the construction of some infinite Galois extensions, e.g. [FKV]. However no attempts seem to have been made to construct p-adic Galois representations by this method. It is the main objective of this article to introduce a general method which accomplishes precisely this.

To fix ideas, let κ be a finite field of characteristic p, let $n > 1$ be an integer and k a separably closed field of characteristic l such that l is prime to the order of $\mathrm{PGL}_n(\kappa)$. For a finite set of places Σ of the field $k(t)$ let $G_{k(t),\Sigma}$ denote the the maximal Galois extension of $k(t)$ unramified outside Σ. For any field F we denote by $F^{\rm sep}$ its separable closure and by $G_F := \mathrm{Gal}(F^{\rm sep}/F)$ its absolute Galois group. For a profinite group G, let $G^{(l)}$ be its prime-to-l completion. Thus if $S = \{0, 1, \infty\}$, then $G^{(l)}_{k(t),S}$ is the prime-to-l completion of $\langle t_0, t_1, t_\infty : t_0 t_1 t_\infty = 1\rangle$ for suitable topological generators t_i of tame inertia subgroups at $i \in S$.

Let g_0, g_1, g_∞ be a Belyi triple of $\mathrm{PGL}_n(\kappa)$, cf. [MM], p. 99, and let $\bar\rho\colon G^{(l)}_{k(t),S} \longrightarrow \mathrm{PGL}_n(\kappa)$ be the Galois representation defined by $t_i \mapsto g_i$ for $i \in S$. Moreover let F be a field whose separable closure is k so that the triple g_1, g_2, g_3 defines F-rational conjugacy classes, cf. [Ser], § 7.1. Then by the rigidity method there exists a unique representation $\widetilde\rho\colon G_{F(t)} \longrightarrow \mathrm{PGL}_n(\kappa)$ whose restriction to $G_{k(t)}$ is $\bar\rho$. If moreover F is Hilbertian, then there exists a thin subset θ_F of F such that for all $a \in F - \theta_F$ the specialization $t \mapsto a \in F$ yields a surjective representation $G_F \longrightarrow \mathrm{PGL}_n(\kappa)$, where G_F arises as the decomposition group of $G_{F(t)}$ at $t = a$.

Our aim is to generalize the above procedure to obtain p-adic Galois representations. The main tools we develop to extend the rigidity method are

(a) a suitable version of Mazur's theory of deformations of Galois representations, cf. [Ma1], and

(b) a rigidity criterion for such deformations.

The universal deformations from (a) are simple if the ramification allowed is not too small. The conditions in (b) impose strong bounds on ramification. So the interesting cases are those where there is an overlap. For instance, we obtain rigid surjective representations

$$\rho\colon G_{k(t)} \twoheadrightarrow \mathrm{PGL}_n(W(\kappa)[[T_1, \ldots, T_{2n-2}]]),$$

which are ramified at precisely three places – here $W(\kappa)$ is the ring of Witt vectors of κ.

For any integer r prime to the characteristic of k, let ζ_r denote a primitive r-th root of unity. Define $F_m := F(\zeta_{p^m})$ and $F_\infty := \cup_n F_n$. If F is a totally real number field, we define F_m^+ and F_∞^+ as the subfields of F_m and F_∞, resp., of invariants under complex conjugation. Standard methods in rigidity and an idea taken from [Ro1], yields surjective representations

$$\rho_\infty\colon G_{F_\infty(t)} \twoheadrightarrow \mathrm{PGL}_n(W(\kappa)[[T_1, \ldots, T_{2n-2}]]),$$

whose restriction to $G_{k(t)}$ is the above ρ.

Our first application is to the results of Rohrlich in [Ro1], [Ro2] and [Ro3], which heavily rely on the arithmetic of elliptic curves. Most of these results we will recover in Section 8 by an alternate route. One of the benefits of our treatment is that one can more clearly distinguish results which do and which do not depend on the arithmetic of elliptic curves, cf. Remark 8.11.

Other interesting applications are:

(a) The construction of a 'family' of (continuous) surjective Galois representations into $\mathrm{SL}_2(\mathbb{Z}_p[\zeta_{p^m} + \zeta_{p^m}^{-1}])$, cf. Theorem 2.29, parameterized by the p-power roots ζ_{p^m}.

(b) The construction of infinite p-adic analytic Galois extensions of rational function fields of characteristic $l \neq p$ which have finite ramification and whose constant field is finite.

Examples of the latter kind had been constructed previously by different methods in [FKV], [Iha] and [Bö2].

We should also like to mention here that rigidity of p-adic representations in combination with universal deformations has been studied by C. Stewart, [Ste], in relation to a different question.

Acknowledgments: The initial impulse for this article stems from an unpublished preprint of David Rohrlich. It gave a direct proof of the second part of Theorem 2.28, based on [Ro1] and [Ro2]. Furthermore the questions raised in the introduction of [Ro1] were very influential. I would like to thank him for making this preprint accessible and guiding my attention to his results. Without his work, the present article would have never come to existence. The inclusion of deformations of Thompson and not just Belyi tuples into this article, I owe to a suggestion of Michael Dettweiler who stressed their importance. Thanks also to Henri Darmon for some motivating discussions during a stay at McGill University. A number of corrections I owe to Axel Stäbler. Finally, let me thank the referee who did a wonderful job and whose comments and corrections were extremely helpful. Part of this work has been supported by the Deutsche Forschungsgemeinschaft – SFB/TR 45.

2 Results

For a function field K with constant field k denote by g_K its genus. For a finite set Σ of places of K (or of a subfield of finite index which contains k), we denote by $K_\Sigma \subset K^{\rm sep}$ the maximal extension of K unramified outside Σ. By $K_\Sigma^{(l)}$ we denote the fixed field in K_Σ of the kernel of the quotient map $\mathrm{Gal}(K_\Sigma/K) \longrightarrow \mathrm{Gal}(K_\Sigma/K)^{(l)}$. So in particular $K_\Sigma^{(l)}$ is a tame Galois extension of K.

Proofs of the results described in this section are given in the remainder of the article. Each result contains a reference to its proof.

Deformation theory

For the applications to rigidity it is important to work with projective and not with linear representations. Deformations of such do not seem to have been considered in the literature, and so we give a brief introduction to this. As a notational convention, all linear representations will have a prime in the notation, while projective representations are written without a prime. Similarly, matrices in GL_n will always carry a prime, while those in PGL_n will not. All rings in this article will have a unit, and except for group rings, they will all be commutative.

From now on we fix a function field K with constant field k and a residual representation $\bar\rho\colon G_K \longrightarrow \mathrm{PGL}_n(\kappa)$.

Let $E \subset L$ be finite extensions of K such that L is the splitting field of $\bar\rho$ and $\mathrm{Gal}(L/E) \subset \mathrm{Gal}(L/K)$ is a p-Sylow subgroup. Let $\mathrm{Ram}(\bar\rho_{|G_E})$ be the set of places of E at which L/E is ramified. Define S_p as the set of places of K at which the order of the ramification subgroup of L/K is divisible by p, i.e., S_p consists of those places of K which are below those in $\mathrm{Ram}(\bar\rho_{|G_E})$.

Let S be a finite set of places of K. Because S is defined over K and because L is Galois over K, the groups $\mathrm{Gal}(K^{\rm sep}/L_S)$ and $\mathrm{Gal}(K^{\rm sep}/L_S^{(l)})$ are characteristic inside G_K and hence L_S and $L_S^{(l)}$ are Galois over K. The corresponding Galois groups are denoted G_S and $G_S^{(l)}$, respectively. By N_S and $N_S^{(l)}$ we denote $\mathrm{Gal}(L_S/L)$ and $\mathrm{Gal}(L_S^{(l)}/L)$, respectively, and by H the group $\mathrm{Gal}(L/K)$. We often identify H with its image $\mathrm{Im}(\bar\rho)$.

To describe further restrictions of ramification, we define a *ramification datum* $\mathscr{D} := (S, (n_x)_{x\in S})$ to consist of a finite set of places S of K and for each $x \in S$ an element $n_x \in \{p^m : m \in \mathbb{N}_0\} \cup \{\infty\}$. The *support* of $\mathscr{D}$ is defined as $\mathrm{Supp}\,\mathscr{D} := \{x \in S : n_x \neq 1\}$. The *maximal ramification order of* $\mathscr{D}$ is defined as $\mathrm{ord}\,\mathscr{D} := \max\{n_x : x \in S\} \in \mathbb{N}_0 \cup \{\infty\}$.

For any such $\mathscr{D}$, we define the field $L_\mathscr{D}$ as the union of all subextensions F of L_S such that for each place y of L above a place x of S, the ramification index of F/L at y divides the p-power n_x. In particular if $n_x \neq \infty$, then F/L will be at most finitely ramified above x. It is easy to see that $L_\mathscr{D}$ is Galois over K and we define $G_\mathscr{D} := \mathrm{Gal}(L_\mathscr{D}/K)$

and $N_{\mathscr{D}} := \mathrm{Gal}(L_{\mathscr{D}}/L)$. Analogous notions are defined with superscript (l). We depict the situation in the case with superscript (l) in the following diagram:

$$\begin{tikzcd}
L_S^{(l)} \arrow[d, dash] \arrow[dd, dash, bend left, "N_S^{(l)}"] \arrow[dddd, dash, bend left=60, "G_S^{(l)}"] & & & L_z^{(l)} \arrow[dd, dash, "J_x"] \arrow[dddd, dash, bend left, "I_x"] \\
L_{\mathscr{D}}^{(l)} \arrow[d, dash, "N_{\mathscr{D}}^{(l)}"'] \arrow[ddd, dash, bend right=50, "G_{\mathscr{D}}^{(l)}"'] & & & \\
L \arrow[d, dash, "p\text{-Syl.}"'] \arrow[dd, dash, bend left, "H"] & & & L_z \arrow[dd, dash, "H_x"] \\
E \arrow[d, dash] & & & \\
K & & & K_x
\end{tikzcd} \tag{1}$$

On the right, we display the corresponding diagram above a place x of K: here z is a place of L above x; by K_x and L_z we denote the respective local fields; the group J_x is the prime-to-l completion of G_{L_z} and thus isomorphic to the prime-to-l completion of $\mathbb{Z}$; its fixed field is denoted $L_z^{(l)}$; it is Galois over K_x, and the corresponding group is I_x; the ramification subgroup of H at x is H_x; it is isomorphic to I_x/J_x; if H_x is cyclic (which by Remark 2.19 will usually be the case), then the same holds for I_x and by g_x we denote a topological generator of the latter. Since the base field k is algebraically closed, decomposition and inertia groups coincide, and so we will always speak of inertia groups. If we have some places labeled x_i, then, for simplicity, we will denote the corresponding g_{x_i} simply by g_i. In the sequel we identify I_x, J_x, etc., with ramification groups at x. This does require a choice of a place in K^{alg} above x. If a place z in L above x in K is chosen, we sometimes write J_z to indicate the choice.

Let $\mathscr{C}$ denote the category of complete noetherian local rings R with maximal ideal $\mathfrak{m}_R$ and a fixed isomorphism $R/\mathfrak{m}_R \longrightarrow \kappa$. For any ring R in $\mathscr{C}$ its maximal ideal $\mathfrak{m}_R$ will be indexed by that ring. Any $R \in \mathscr{C}$ is naturally a $W(\kappa)$-algebra.

Following [Ma1], we define the functor $\mathrm{Def}_{\mathscr{D}}$ from $\mathscr{C}$ to the category of sets by

$$\mathrm{Def}_{\mathscr{D}}(R) := \{\rho\colon G_{\mathscr{D}} \longrightarrow \mathrm{PGL}_n(R) |\, \rho \equiv \bar{\rho} \pmod{\mathfrak{m}_R} \text{ and } \rho \text{ is continuous}\}/\sim,$$

where two lifts $\rho_1, \rho_2 : G_{\mathscr{D}} \longrightarrow \mathrm{PGL}_n(R)$ are strictly equivalent, $\rho_1 \sim \rho_2$, if and only if there exists an element $A \in \mathrm{PGL}_n(R)$ which reduces to the identity modulo $\mathfrak{m}_R$ such that $\rho_2 = A\rho_1 A^{-1}$. Elements of $\mathrm{Def}_{\mathscr{D}}$ are called *deformations (of type $\mathscr{D}$)* and the equivalence class of a lift ρ is denoted $[\rho]$. If $\mathscr{D}$ is the datum $(S, (\infty)_{x\in S})$, then we shall simply write Def_S for $\mathrm{Def}_{\mathscr{D}}$. The same convention will be applied in all further definitions involving $\mathscr{D}$.

Any $[\rho] \in \mathrm{Def}_{\mathscr{D}}(R)$ factors via $G_{\mathscr{D}}^{(l)}$, since its restriction $\rho_{|N_{\mathscr{D}}}$ factors via the pro-p completion of $N_{\mathscr{D}}$. The pro-p completion of $N_{\mathscr{D}}$ is known to be finitely generated, e.g. Proposition 3.1. By a simple modification of the proof of [Ma1], Prop. 1, one obtains:

Proposition 2.1 *If the centralizer of* $\mathrm{Im}(\bar{\rho})$ *inside* $\mathrm{PGL}_n(\kappa)$ *is trivial then* $\mathrm{Def}_{\mathscr{D}}$ *is representable.*

From now on, we assume that the centralizer of $\mathrm{Im}(\bar{\rho})$ in $\mathrm{PGL}_n(\kappa)$ is trivial.

We write $(R_{\mathscr{D}}, \rho_{\mathscr{D}})$ for a pair $R_{\mathscr{D}} \in \mathscr{C}$ and $\rho_{\mathscr{D}} : G_{\mathscr{D}} \longrightarrow \mathrm{PGL}_n(R_{\mathscr{D}})$ such that $[\rho_{\mathscr{D}}]$ represents the universal object in $\mathrm{Def}_{\mathscr{D}}(R_{\mathscr{D}})$. If we want to stress the residual representation $\bar{\rho}$, we write $R_{\mathscr{D}}(\bar{\rho})$.

To investigate $R_{\mathscr{D}}$, we introduce the following notation. By $\mathrm{ad}_{\bar\rho}$ we denote the representation of $G_{\mathscr{D}}$ on $M_n(\kappa)$ obtained by composing the adjoint representation ad, given by conjugation of $\mathrm{PGL}_n(\kappa)$ on $M_n(\kappa)$, with the representation $\bar\rho$. By $\overline{\mathrm{ad}}$ and $\overline{\mathrm{ad}}_{\bar\rho}$ we denote the quotients of the above representations by the subrepresentation of scalar matrices, by ad^0 the subrepresentation of ad on trace zero matrices. For any $\kappa[G_{\mathscr{D}}]$-module M, we abbreviate $h^i_{\mathscr{D}}(M) := \dim_\kappa H^i(G_{\mathscr{D}}, M)$.

Following the proof of [Ma1], Prop. 2, or [Böl], Thm. 2.4, one has the following:

Proposition 2.2 *Suppose that* $\mathrm{Cent}_{\mathrm{PGL}_n(\kappa)}(\mathrm{Im}(\bar\rho)) = \{1\}$. *Then* $R_{\mathscr{D}}$ *has a presentation*

$$R_{\mathscr{D}} \cong W(\kappa)[[T_1, \ldots, T_m]]/\mathfrak{a},$$

where $m = h^1_{\mathscr{D}}(\overline{\mathrm{ad}})$ *and* $\dim_\kappa \mathfrak{a}/(p, T_1, \ldots, T_m)\mathfrak{a} \le h^2_{\mathscr{D}}(\overline{\mathrm{ad}})$.

For any set S define the sets $\Delta S := \mathrm{Ram}(\bar\rho) - S$ and $S^+ := S \amalg \Delta S = S \cup \mathrm{Ram}(\bar\rho)$. Furthermore, for any place x of K denote by H_x an inertia subgroup in H. The first interesting result regarding the above deformation rings is the following.

Theorem 2.3 (p. 8) *Suppose that* $S \supset S_p$ *is non-empty and that* $\mathrm{Cent}_{\mathrm{PGL}_n(\kappa)}(\mathrm{Im}(\bar\rho)) = \{1\}$. *Then* $h^2_S(\overline{\mathrm{ad}}_{\bar\rho}) = 0$ *and* R_S *is a power series ring over* $W(\kappa)$ *of relative dimension*

$$h^1_S(\overline{\mathrm{ad}}_{\bar\rho}) = (2g_K + |S^+| - 2)(n^2 - 1) - \sum_{x \in \Delta S} \dim \overline{\mathrm{ad}}_{\bar\rho}^{H_x}.$$

For $S = \varnothing$ an explicit example is given in Proposition 9.1.

On the surjectivity of Galois representations

Our next result is a surjectivity criterion for projective universal deformations and will be applied when deforming rigid tuples. It uses a result of Boston, [Bo1], and is inspired by a remark in [Ro1]. The result is independent of our particular set-up and also applies, suitably phrased, to projective representations of the absolute Galois group of number fields or function fields over finite fields.

In the following we identify $H = \mathrm{Im}(\bar\rho)$. We say that a deformation $\rho : G_{\mathscr{D}} \longrightarrow \mathrm{PGL}_n(R)$ has *maximal image* if

$$\mathrm{Im}(\rho) = \{A \in \mathrm{PGL}_n(R) : A \pmod{\mathfrak{m}_R} \in H\}$$

Proposition 2.4 (p. 12) *Let* R *be in* $\mathscr{C}$ *and* $\rho\colon G_{\mathscr{D}} \longrightarrow \mathrm{PGL}_n(R)$ *a lift of* $\bar\rho$. *Assume* $\overline{\mathrm{ad}}$ *is irreducible, the canonical surjection* $\{A \in \mathrm{PGL}_n(W_2(\kappa)) : A \pmod p \in \mathrm{Im}(\bar\rho)\} \twoheadrightarrow H$ *is non-split and* $\rho \pmod{(\mathfrak{m}_R^2, p)}$ *has maximal image. Then* ρ *has maximal image.*

Remark 2.5 Note that if $\overline{\mathrm{ad}}$ is irreducible as an H-module, then $p \nmid n$: Suppose on the contrary that p divides n. Then the trace on $M_n(\kappa)$ is zero on scalar matrices. In other words, ad^0 contains the scalar matrices as an irreducible subrepresentation. But then $\mathrm{ad}^0/\kappa \subset \overline{\mathrm{ad}}$ is a proper non-zero subrepresentation, and so $\overline{\mathrm{ad}}$ is reducible.

Proposition 2.4 yields the following result for universal deformations:

Corollary 2.6 (p. 12) *Suppose the following conditions hold:*

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

(ii) The canonical surjection $\{A \in \mathrm{PGL}_n(W_2(\kappa)) : A \pmod p \in \mathrm{Im}(\bar\rho)\} \twoheadrightarrow H$ *is non-split.*

(iii) The representation $\overline{\mathrm{ad}}$ *is irreducible over* $\mathbb{F}_p[H]$ *and absolutely irreducible over* $\kappa[H]$.

Then for any ramification datum $\mathscr{D}$, the universal projective representation $\rho_{\mathscr{D}}$ has maximal image.

Example 2.7 All the hypotheses of the above proposition are met by representations $\bar{\rho}$ whose image contains $\mathrm{PSL}_n(\kappa)$, provided that $|\kappa| > 5$, if $n = 2$, or $|\kappa| > 3$, if $n > 2$ and $p \not| n$. For the proof of (i) and (ii) see [CPS].

Deforming rigid tuples

We now turn to rigidity, cf. [Ser], Ch. 7,8 for a good account. For elements g, h of a group G, define $g^h := hgh^{-1}$. If we write $\prod g_i$ for elements $g_1, \ldots, g_s$ in a group G, we mean $g_1 g_2 \cdot \ldots \cdot g_s$ in this order. The following generalizes the existing notion of strict rigidity.

Definition 2.8 *Let $\rho \colon G \longrightarrow P$ be a homomorphism of finite groups. Elements $g_1, \ldots, g_s$ of G are called* strictly rigid for ρ*, if the following conditions hold:*

(a) $\prod g_i = 1$ and the g_i generate G.

(b) For any $p_1, \ldots, p_s \in P$ such that $\prod_i \rho(g_i)^{p_i} = 1$, there exists a unique $p \in P$ such that for all i one has $\rho(g_i)^{p_i} = \rho(g_i)^p$.

If ρ is the identity map on G, we simply use the terminology strictly rigid for G.

The above definition agrees with the standard one which can be found for instance in [Ser], § 7.3. Note also that if a homomorphism ρ between finite groups admits a strictly rigid tuple, then the uniqueness assertion in (b) is equivalent to the centralizer of $\rho(G)$ in P being trivial.

Below we provide a generalization of the above definition to profinite groups. The following simple example was important in its formulation.

Example 2.9 If a tuple $g_1, \ldots, g_s$ is strictly rigid for a finite group G, and if N is a normal subgroup of G, the images of the tuple in G/N may no longer form a rigid tuple:

Let κ be a finite field of cardinality q and choose $n \in \mathbb{N}$ which has a common factor with $q-1$. In particular q is at least 3 and n at least 2. Under the latter conditions on n and q, the group $\mathrm{PGL}_n(\kappa)$ admits a strictly rigid tuple – we recall this in Proposition 6.26. Now the determinant map on GL_n induces a natural group epimorphism $\mathrm{PGL}_n(\kappa) \twoheadrightarrow \kappa^*/\kappa^{*n}$. Since κ^*/κ^{*n} is abelian and, under our hypotheses, non-trivial, it does not admit any rigid tuple.

Definition 2.10 *Let $\rho : G \longrightarrow P$ be a continuous homomorphism of profinite groups, and let $N_0 \subset P$ be a normal open subgroup. Elements $g_1, \ldots, g_s$ of G are called* strictly pro-rigid for ρ and N_0*, if for all open normal subgroups $M \trianglelefteq G$ and $N \trianglelefteq P$ with $\rho(M) \subset N \subset N_0$ the elements $g_1 \pmod{M}, \ldots, g_s \pmod{M}$ are strictly rigid for the induced homomorphism $G/M \longrightarrow P/N$ of finite groups.*

As before, if $\rho = \mathrm{id}_G$ we simply use the terminology strictly pro-rigid for G and N_0.

If we have a strictly pro-rigid tuple for a pair (ρ, N_0) as above, by an inverse limit argument one can show that the elements g_i topologically generate G, and that condition (b) of Definition 2.8 holds. In particular we deduce that $\mathrm{Cent}_P(\rho(G)) = 1$. We suspect, that, in general, (a) and (b) for a continuous homomorphism of profinite groups (where in (a) we replace 'generate' by 'topologically generate') together with the assertion that the tuple is strictly rigid for the composite $G \longrightarrow P \longrightarrow P/N_0$, do not suffice to prove strict pro-rigidity for the given tuple and (ρ, N_0).

In this article, we almost exclusively study the following variant of Definition 2.10:

Definition 2.11 *Let R be a complete noetherian local ring with finite residue field, let G be a profinite group and let $\rho\colon G \longrightarrow \mathrm{PGL}_n(R)$ be a continuous projective representation. Elements $g_1, \ldots, g_s$ of G are called* strictly pro-rigid *for ρ if the following conditions hold:*

(a) $\prod g_i = 1$ and the g_i topologically generate G.

(b') For any finite quotient R' of R, for $\rho' := \rho \otimes_R R'$ and for any $A_1, \ldots, A_s \in \mathrm{PGL}_n(R')$ such that $\prod_i \rho'(g_i)^{A_i} = 1$, there exists a unique $A \in \mathrm{PGL}_n(R')$ such that for all i one has $\rho'(g_i)^{A_i} = \rho'(g_i)^A$.

Clearly $g_1, \ldots, g_s$ are strictly pro-rigid for ρ if they satisfy $\prod_i g_i = 1$, are topological generators of G and if for all continuous epimorphisms $R \longrightarrow R'$ with R' finite and for $\rho' := \rho \otimes_R R'$, the tuple $\rho'(g_1), \ldots, \rho'(g_s)$ is strictly rigid for the tautological representation $\mathrm{Im}(\rho') \hookrightarrow \mathrm{PGL}_n(R')$. An inverse limit shows that (b') for a projective representation implies condition (b) of Definition 2.8, and thus $\mathrm{Cent}_{\mathrm{PGL}_n(R)}(\mathrm{Im}(\rho)) = 1$.

For every surjection $R \longrightarrow R'$ in $\mathscr{C}$, set $K^R_{R'} := \mathrm{Ker}(\mathrm{PGL}_n(R) \longrightarrow \mathrm{PGL}_n(R'))$. The following proposition clarifies the relationship between Definitions 2.11 and 2.10:

Proposition 2.12 (p. 11) *Let R and ρ be as in Definition 2.11 with residue field κ_R. Fix a subgroup H of $\mathrm{PGL}_n(\kappa_R)$ and define $P := \{A \in \mathrm{PGL}_n(R) : A \pmod{\mathfrak{m}_R} \in H\}$. If $\overline{\mathrm{ad}}$ is irreducible over $\mathbb{F}_p[H]$ and absolutely irreducible over $\kappa[H]$, then every normal open subgroup N of P which is contained in $K^R_{\kappa_R}$ is of the form $K^R_{R'}$ for some finite R'.*

Corollary 2.13 *If $p \not| n$, then strict pro-rigidity as in Definition 2.11 is a special case of Definition 2.10 for the same ρ and $N_0 = \mathrm{Ker}(\mathrm{PGL}_n(R) \twoheadrightarrow \mathrm{PGL}_n(\kappa_R))$.*

To see that the proposition implies the corollary, take $H = \mathrm{PGL}_n(\kappa_R)$ and observe that for $p \not| n$ the irreducibility hypotheses are indeed satisfied.

Given a strictly (pro-)rigid tuple for ρ (and N_0), we will also be interested in the strict (pro-)rigidity of the image of the tuple inside $\rho(G)$ (and for N_0). For finite R the following gives a relation between the two notions. The simple proof is left to the reader.

Proposition 2.14 *Let R be a finite ring and $\rho : G \longrightarrow \mathrm{PGL}_n(R)$ a representation. Suppose elements $g_1, \ldots, g_s$ are strictly pro-rigid for G and $N_0 = \{1\}$. Then the tuple $\rho(g_1), \ldots, \rho(g_s)$ is strictly rigid for $\rho(G)$ if and only if all A, which satisfy $\rho(g_i)^A \in \rho(g_i)^{\rho(G)}$ for all i, do lie in $\rho(G)$. This holds in particular if $\rho(G) = \mathrm{N}_{\mathrm{PGL}_n(R)}(\rho(G))$.*

Definition 2.15 *If in Definition 2.11 the ring R is a field, we say that the elements $g_1, \ldots, g_s$ are* geometrically rigid *for ρ, if these elements are strictly pro-rigid for the composite of ρ with $\mathrm{PGL}_n(R) \longrightarrow \mathrm{PGL}_n(S)$ for any finite field extension $R \longrightarrow S$.*

Example 2.16 Any Belyi triple is geometrically rigid for the tautological representation, cf. [MM], p. 99, and [Vö], remark after Thm. 5.4. For instance, the triple

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

is geometrically rigid for the tautological representation $\mathrm{PSL}_2(\mathbb{F}_p) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$. An elementary proof can be obtained along the lines of the proof of [Ser], Prop. 7.4.2.

Strict and geometric rigidity have strong consequences for the underlying representation of $\mathrm{Im}(\rho)$:

Proposition 2.17 *Suppose ρ admits a strictly pro-rigid tuple and that in addition R is a finite field different from $\mathbb{F}_2$. Consider the (tautological) linear representation of the preimage $\widetilde{G} \subset \mathrm{GL}_n(R)$ of $\rho(G) \subset \mathrm{PGL}_n(R)$ on $V := R^n$. Then $\mathrm{End}_{R[\widetilde{G}]}(V) \cong R$, so that V must be absolutely indecomposable.*

If moreover $\rho(G)$ is of order prime to the characteristic of R, then V is absolutely irreducible.

If the tuple is geometrically rigid, then the above assertions hold for all finite fields.

Proof: Recall that strict pro-rigidity implies that

$$\mathrm{Aut}_{R[\widetilde{G}]}(V) = \mathrm{Aut}_R(V)^{\widetilde{G}} = \mathrm{Cent}_{\mathrm{GL}_n(R)}(\widetilde{G}) = R^*.$$

Suppose first $\#R \geq 3$. Then the $\widetilde{G}$-representation V must be indecomposable, since otherwise we would have $R^* \times R^* \subset \mathrm{Aut}_{R[\widetilde{G}]}(V) = R^*$. By [Ja], Thm. 3.7, it follows that $\mathrm{End}_{R[\widetilde{G}]}(V)$ is a local (not necessarily commutative) R-algebra, whose maximal ideal $\mathfrak{m}$ of non-units consists of nilpotent elements. Then all elements in $1+\mathfrak{m}$ are of finite p-power order but also lie in $\mathrm{Aut}_{\widetilde{G}}(V) = R^*$. We deduce $\mathfrak{m} = 0$. Knowing that $\mathrm{End}_{R[\widetilde{G}]}(V)$ is a skew field and hence by finiteness a field, and that R^* is its set of units, we deduce that the canonical map $R \hookrightarrow \mathrm{End}_{R[\widetilde{G}]}(V)$ is an isomorphism.

If $R = \mathbb{F}_2$ and ρ is geometrically rigid, we apply the previous argument to $\mathbb{F}_4$ and $(\mathrm{PGL}_n(\mathbb{F}_2) \hookrightarrow \mathrm{PGL}_n(\mathbb{F}_4)) \circ \rho$, so that $\mathbb{F}_4 \hookrightarrow \mathrm{End}_{R[\widetilde{G}]}(V \otimes_{\mathbb{F}_2} \mathbb{F}_4)$ is an isomorphism. Since $\mathbb{F}_2 \longrightarrow \mathbb{F}_4$ is flat this implies the same for $\mathbb{F}_2 \hookrightarrow \mathrm{End}_{R[\widetilde{G}]}(V)$. The other assertions are straightforward. ∎

Remark 2.18 If R is as in Definition 2.11 and $\mathfrak{m}_R$ denotes its maximal ideal, then a natural question is, whether it is true that a tuple is strict pro-rigid for a given representation ρ if and only if the tuple is strictly pro-rigid for all the representations $\rho \pmod{\mathfrak{m}_R^m}\colon G \longrightarrow \mathrm{PGL}_n(R/\mathfrak{m}_R^m)$. We assume $p \not| n$:

If for any surjection $R/\mathfrak{m}_R^m \twoheadrightarrow R'$ and for any tuple $A_1, \ldots, A_s$ as in (b') of Definition 2.11 there are lifts $\hat{A}_i$ of the A_i to $R/\mathfrak{m}_R^m$ such that $\prod_i \rho(g_i)^{\hat{A}_i} \equiv 1 \pmod{\mathfrak{m}_R^m}$, then the strict pro-rigidity over $R/\mathfrak{m}_R^m$ implies the existence of some A as asserted for R'. Setting $\widetilde{g}_i = g_1 \cdot \ldots \cdot g_i$ and $\kappa_R := R/\mathfrak{m}_R$, a sufficient condition for such lifts to always exist is

(c) The homomorphism $\overline{\mathrm{ad}}^s \longrightarrow \overline{\mathrm{ad}} : (m_1, \ldots, m_s) \mapsto \sum_{i=1}^s (m_i - m_{i-1})^{\widetilde{g}_{i-1}}$ of $\kappa_R[H]$-modules with $H = \mathrm{Im}(\bar{\rho})$ is surjective, where we identify $m_0 := m_s$,

where $\overline{\mathrm{ad}} = \overline{\mathrm{ad}}_{\bar{\rho}}$ and $\bar{\rho} := \rho \pmod{\mathfrak{m}_R}$.

If the centralizer of $\mathrm{Im}(\bar{\rho})$ in $\mathrm{PGL}_n(\kappa_R)$ is trivial, then the uniqueness over any R' of the matrix A can be deduced from the following condition

(d) The canonical map $\kappa_R \hookrightarrow \mathrm{ad}^G$ is an isomorphism, i.e. $\overline{\mathrm{ad}}^G = 0$.

Both claims can be proved by an inductive argument. The key point is that all subfactors of the kernel of $\mathrm{PGL}_n(R) \twoheadrightarrow \mathrm{PGL}_n(\kappa_R)$ that occur in the induction are isomorphic to $\overline{\mathrm{ad}}$. Since we will never explicitly use the above, we omit the details. Similar arguments are used in the proof of Theorem 6.17.

Both conditions, (c) and (d), are satisfied if the g_i form a geometrically rigid tuple for $\rho \pmod{\mathfrak{m}_R}$ in the sense of Definition 2.15 below and if moreover $\overline{\mathrm{ad}}$ is irreducible: For (d), see Proposition 2.17, for (c), apply Corollary 6.21.

It is possible to formulate a lifting condition in the more general setting of Definition 2.10 provided that N_0 is pro-sovable. The lifting condition can be shown to hold if: (i) the image of the given tuple is strictly pro-rigid for the induced homomorphism $G/\rho^{-1}(N_0) \longrightarrow P/N_0$ and (ii) condition (c) holds for all simple H-module subfactors of N_0. (As groups they are finite abelian.)

Deformations and strict pro-rigidity

For the remainder of the introduction, we assume that $K = k(t)$ and enumerate $S = \{x_1, \ldots, x_s\}$. Then $\mathrm{Gal}(K_S^{(l)}/K)$ is isomorphic to the profinite prime-to-l completion of the group

$$\langle g_1, \ldots, g_s : \prod g_i = 1\rangle,$$

where the g_i are suitable topological generators of an inertia group at x_i. The elements $g_1, \ldots, g_s$ are a natural source of strictly pro-rigid tuples of representations of $\mathrm{Gal}(K_S^{(l)}/K)$. Whenever we will have a representation of this group (for instance one coming from a strictly pro-rigid tuple), then we will have $\mathrm{Gal}(K_S^{(l)}/K) = G_S^{(l)}$. In anticipation of this we will from now on use the notation $G_S^{(l)}$ for $\mathrm{Gal}(K_S^{(l)}/K)$ and along with it, all the other notation displayed in diagram (1).

Remark 2.19 By the definition of $\mathrm{Gal}(K_S^{(l)}/K)$, being the prime-to-$l$ completion, where l is the characteristic of k, its inertia subgroups above all places of $K(t)$ are procylic.

We call an element $A \in \mathrm{PGL}_n(\kappa)$ *regular*, if $\dim \mathrm{ad}^A = n$, where ad^A denotes the subspace of elements of ad which are invariant under the adjoint action of A.

The following is our main result on the pro-rigidity of universal deformations

Theorem 2.20 (p. 23) *Suppose that $K = k(t)$, that $\bar\rho\colon G_S \longrightarrow \mathrm{PGL}_n(\kappa)$ is a continuous representation and that the characteristic l of K is prime to the order of $H = \mathrm{Im}(\rho)$. Let $\Sigma = \mathrm{Ram}(\bar\rho) = \{x_1, \ldots, x_s\}$. For each $i = 1, \ldots, s$, let g_i be a topological generator of an inertia subgroup I_{x_i} of $G_\Sigma^{(l)}$ such that $\prod g_i = 1$ in $G_\Sigma^{(l)}$. Let $\Sigma_{\mathrm{reg}} = \{x_i \in \Sigma : \bar\rho(g_i)$ is regular$\}$ and assume:*

- *(a) The H-representation $\overline{\mathrm{ad}}$ is irreducible.*
- *(b) The elements $g_1, \ldots, g_s$ are geometrically rigid for $\bar\rho$.*
- *(c) Each of the $\bar\rho(g_i)$ is of order prime to p or regular.*
- *(d) For any $x_i \in \Sigma_{\mathrm{reg}}$ and $A_i' \in \mathrm{GL}_n(\kappa)$ a representative of $\bar\rho(g_i) \in \mathrm{PGL}_n(\kappa)$, the matrices $\lambda A_i'$, $\lambda \in \kappa^*$, are pairwise non-conjugate.*
- *(e) $\mathscr{D}$ is a ramification datum such that $\mathrm{Supp}\,\mathscr{D} \subset \Sigma_{\mathrm{reg}}$.*

Then the elements g_i are strictly pro-rigid for $\rho_{\mathscr{D}}$.

If moreover the conditions of Corollary 2.6 hold, then $\rho_{\mathscr{D}}$ has maximal image.

If in addition to all the above, the $\bar\rho(g_i)$ are also strictly rigid for $\mathrm{Im}(\bar\rho)$, then the $\rho_{\mathscr{D}}(g_i)$ are strictly pro-rigid for the group $\mathrm{Im}(\rho_{\mathscr{D}})$ and its subgroup $\mathrm{Ker}(\mathrm{Im}(\rho_{\mathscr{D}}) \longrightarrow \mathrm{Im}(\bar\rho))$.

Condition (d) means that the centralizer of A_i' in $\mathrm{GL}_n(\kappa)$ surjects onto the centralizer of $\bar\rho(g_i)$ in $\mathrm{PGL}_n(\kappa)$. If combined with condition (a), an analogous assertion can be deduced for lifts to any $R \in \mathscr{C}$, cf. Lemma 6.12 (a).

Remark 2.21 In Section 6, Theorem 6.17, we prove a more general result than the above theorem. It relaxes condition (e) to $\mathrm{Supp}\,\mathscr{D} \subset \Sigma$ and does not need (d), but imposes conditions on the deformation types at all $x \in \Sigma$. The deformations considered in Theorem 6.17 will be called **rigid**. Since the preparations to state this theorem are somewhat technical, we chose to present the above simpler form in the introduction.

Only when combined with the concept of ‘rationality’, rigid tuples are useful to attack the inverse Galois problem. We ‘recall’ this notion:

Definition 2.22 ([Ser], Def. 7.1.1) *Let G be a profinite group and F a (discrete!) field. A conjugacy class g^G (of some $g \in G$) is called F-rational if for all F^{sep}-valued (finite dimensional, continuous) characters χ of G one has $\chi(g) \in F$.*

Remark 2.23 If G is finite, the above is the usual definition. If G is infinite profinite, then g^G is F-rational if and only if for any normal open subgroup N in G the conjugacy class $(g \pmod{N})^{G/N}$ in G/N is F-rational. In particular, if for any N the field $F(N)$ denotes the smallest one over which $(g \pmod{N})^{G/N}$ is rational, then g^G is $\cup_N F(N)$-rational – note that $F(N') \supset F(N)$ for $N' \leq N$. From this one easily deduces, e.g. Lemma 6.24, that any class g^G is rational over the maximal abelian extension of F.

Let H' be a subgroup of $\mathrm{PGL}_n(\kappa)$ and assume that $h_1, \ldots, h_s \in H'$ are geometrically rigid for $H' \hookrightarrow \mathrm{PGL}_n(\kappa)$. Let F be a subfield of the separably closed field k and let $\Sigma := \{x_1, \ldots, x_s\}$ be a set of F-rational places of $F(t)$. As before, suppose that the order of $\mathrm{PGL}_n(\kappa)$ is prime to the characteristic of k. Let $g_1, \ldots, g_s$ be topological generators of $\mathrm{Gal}(k(t)_\Sigma^{(l)}/k(t))$ with $\prod g_i = 1$ and such that g_i generates the inertia group at x_i. Then there exists a representation $\bar\rho\colon \mathrm{Gal}(k(t)_\Sigma^{(l)}/k(t)) \longrightarrow \mathrm{PGL}_n(\kappa)$ with $\bar\rho(g_i) = h_i$.

If moreover the conjugacy classes $h_i^{H'}$ are F-rational, then, e.g., by the proof of [Ser], Thm. 8.2.1, the following holds: There exists a unique projective representation $\widetilde\rho\colon \mathrm{Gal}(k(t)_\Sigma^{(l)}/F(t)) \longrightarrow \mathrm{PGL}_n(\kappa)$ whose restriction to $\mathrm{Gal}(k(t)_\Sigma^{(l)}/k(t))$ agrees with $\bar\rho$. The splitting field of $\widetilde\rho$ is (by strict rigidity) a regular cover of $F(t)$ with Galois group isomorphic to H'.

Remark 2.24 Recall that a Galois cover $K/F(t)$ is called *regular* if the natural inclusion $\mathrm{Gal}(KF^{\mathrm{sep}}/F^{\mathrm{sep}}(t)) \hookrightarrow \mathrm{Gal}(K/F(t))$ is an isomorphism. The main use of the word *regular* in this work is with regards to matrices, see after Remark 2.19. On occasion we will need the term regularity also for field extensions. Hopefully, no confusion will arise.

Standard methods of rigidity theory therefore yield the following corollary to Theorem 2.20 (recall that F_m was defined as $F(\zeta_{p^m})$ on page -2):

Corollary 2.25 (cf. Corollary 6.25) *We keep the assumptions and notations of Theorem 2.20. Let m be the maximal ramification order of $\mathscr{D}$ and assume that the conjugacy classes of the $\bar\rho(g_i)$ are F-rational. Then there exists a unique continuous representation*

$$\rho_{\mathscr{D},m}\colon \mathrm{Gal}(k(t)_{\mathscr{D}}^{(l)}/F_m(t)) \longrightarrow \mathrm{PGL}_n(R_{\mathscr{D}})$$

such that the restriction of $\rho_{\mathscr{D},m}$ to $G_{\mathscr{D}}$ is isomorphic to the universal representation $\rho_{\mathscr{D}}$.

If the splitting field of $\widetilde\rho$ is a regular cover of $F(t)$, then so is the splitting field of $\rho_{\mathscr{D},m}$ over $F_m(t)$.

Based on the above we will show the following:

Corollary 2.26 (p. 29) *Let q denote the cardinality of κ and let $n > 1$ be an integer which is prime to q. If $q \neq 2$, there exist infinitely many non-isomorphic Galois extensions of $\mathbb{Q}_\infty(\zeta_{q^n-1})$ with Galois group isomorphic to $\mathrm{PGL}_n(W(\kappa)[[T_1, \ldots, T_{2n-2}]])$.*

The structure of $R_{\mathscr{D}}$ for certain $\mathscr{D}$

As in Theorem 2.20, let $\Sigma = \mathrm{Ram}(\bar\rho)$ and $\Sigma_{\mathrm{reg}} = \{x \in \Sigma : \bar\rho(g_x) \text{ is regular}\}$. The explicit computations and examples of Section 9 raise the question about the general shape of the ring $R_{\mathscr{D}}$ if $\mathrm{Supp}\,\mathscr{D} \subset \Sigma_{\mathrm{reg}}$. In this direction, we have the following result:

Theorem 2.27 (cf. Corollary 7.7) *Suppose that $S_p \subset \Sigma_{\mathrm{reg}}$ and that the conditions of Theorem 2.20 are satisfied. Then the rings $R_{\mathscr{D}}$ with $\mathrm{Supp}\,\mathscr{D} \subset \Sigma_{\mathrm{reg}}$ and $\mathrm{ord}\,\mathscr{D} < \infty$ are reduced, finite flat over $\mathbb{Z}_p$ and complete intersections.*

The proof given in Section 7 consists of two main steps. First, using the rigidity of $\bar{\rho}$ and $\bar{\rho}_{\mathscr{D}}$ we show that $R_{\mathscr{D}}$ is the tensor product of suitably defined local (versal) deformation rings. Second, we can show the above assertions for these local rings 'explicitly'. In fact, in Section 7 we shall prove Theorem 2.27 more generally for all rigid deformations, alluded to in Remark 2.21.

In Section 7, we also explain how parts of these results were motivated by a recent conjecture of de Jong, cf. [deJ].

Applications

Further applications of our results are given in Sections 8 and 9. A large part of Section 8 is dedicated to reproving various of the theorems of Rohrlich, [Ro1] and [Ro2]. At this point we only state one result of Section 8 which, in slightly different form, appeared in an unpublished preprint of Rohrlich.

Let E be an elliptic curve over $k(j)$ with j-invariant j. Let $\bar{\rho}'_{E,p}\colon \mathrm{Gal}(k(j)^{\mathrm{sep}}/k(j)) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ be the representation on the p-torsion points of E. As we assume $l \neq p$, the representation $\bar{\rho}'_{E,p}$ takes its image in $\mathrm{SL}_2(\mathbb{F}_p)$ and surjects onto this group, [Igu], Thm. 4. Let L' be the splitting field of $\bar{\rho}'_{E,p}$. In Section 5, we will construct universal deformations (R'_S, ρ'_S) for deformations ρ' of $\bar{\rho}'_{E,p}$ such that the restriction $\rho'_{|G_{L'}}$ is unramified outside S.

For $k \subset \mathbb{C}$ algebraically closed and $p \geq 7$, in [Ro1], Thm. 3, Rohrlich constructs a surjective lift $\rho' : \mathrm{Gal}_{k(j)} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}_p[[T]])$ which is a deformation of $\bar{\rho}'_{E,p}$ such that $\rho'_{|G_{L'}}$ is unramified outside ∞.

Theorem 2.28 (p. 37) *Let $R'_{\{\infty\}}(\bar{\rho}'_{E,p})$ be the universal ring for deformations ρ' of $\bar{\rho}'_{E,p}$ such that $\rho'_{|G_{L'}}$ is unramified outside ∞, and $\mathrm{Def}'_{\{\infty\}}(\bar{\rho}'_{E,p})$ the corresponding deformation functor. Then for $l, p \geq 5$, the ring $R'_{\{\infty\}} := R'_{\{\infty\}}(\bar{\rho}'_{E,p})$ is isomorphic to $\mathbb{Z}_p[[T]]$, the representation $\rho'_{\{\infty\}}$ takes its image in $\mathrm{SL}_2(R'_{\{\infty\}})$ and for $p > 5$ it is surjective.*

For k as above and $p \geq 7$, the pair $(\mathbb{Z}_p[[T]], \rho')$ is universal for $\mathrm{Def}'_{\{\infty\}}(\bar{\rho}'_{E,p})$.

The second part of the above theorem was proved for $k = \mathbb{C}$ in an unpublished preprint by Rohrlich.

Let $\bar{\rho}_{E,p}$ denote the projective representation attached to $\bar{\rho}'_{E,p}$. In Section 8, we also compute the universal rings $R_{\{\infty\}}$ for all primes p and all l (subject to the condition $l \neq p$).

In Section 9, we give an explicit description of the universal deformation ρ' of Rohrlich. Using it, we explicitly describe $R_{\varnothing}$ if $p \geq 5$ and $l \neq p$ is greater then 3 or equal to zero. Furthermore, we prove the following two results:

Theorem 2.29 (p. 45) *Suppose $p \equiv 1 \,(\mathrm{mod}\ 4)$, $p > 5$. Then there exist*

(a) a surjective representation $\rho_{\infty^+} : G_{\mathbb{Q}^+_\infty} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}_p[[T]])$ which is ramified at most at finitely many primes and

(b) a surjective representation $\rho_\zeta : G_{\mathbb{Q}^+_m} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}_p[\zeta + \zeta^{-1}])$ for each p^m-th root of unity ζ,

such that the restriction $(\rho_\zeta)_{|G_{\mathbb{Q}^+_\infty}}$ agrees with the specialization $T \mapsto \zeta + \zeta^{-1} - 2$ of ρ_{∞^+}.

Theorem 2.30 (p. 46) *Suppose $p > 5$ and $3 < l \not| (p^3 - p)$. Then for any $n \in \mathbb{N}$ there exists an l-adic analytic Galois extension of $\mathbb{F}_l(\zeta_{p^e})(t)$ which has finite ramification, whose constant field is finite, and whose Galois group is isomorphic to $\mathrm{SL}_2(\mathbb{Z}_p[\zeta_{p^e} + \zeta_{p^e}^{-1}])$.*

Because the rings $R_{\mathscr{D}}$ in Theorem 2.27 are finite flat over $\mathbb{Z}_p$ *and* reduced, upon localization at a height one prime and inverting p, they give rise to (projective) n-dimensional p-adic Galois representations. Since for growing $\mathscr{D}$, the rings $R_{\mathscr{D}}$ become larger, too, one obtains infinitely many quotients of $R_{\Sigma_{\mathrm{reg}}}$ which descend to $E(t)$ for some finite extension E (depending on the representation) of the prime field of k. This allows one to state an analog of Theorem 2.30 for higher dimensional representations. As it is straightforward, we omit details.

Constructing higher-dimensional analogs of Theorem 2.29 involves further complications, since we need some condition to ensure that the universal rigid representation descends to a (totally real) finite extension of $\mathbb{Q}$. When attempting to invoke Lemma 6.24, on the rationality of rigid tuples, one is lead to consider deformations for projective symplectic representations. However this case and the statement of the precise analog of Theorem 2.29 remain to be worked out. We note that some complications are to be expected, since $H^1(\mathrm{Im}\,\bar\rho, \overline{\mathrm{ad}})$ is generally non-zero if $\mathrm{Im}\,\bar\rho$ is the full symplectic group, and so the maximality of the image is not immediate. Further questions in this direction will be discussed in Remark 8.11.

3 Universal deformations

In this section, we will prove Theorem 2.3. Let X, Y, Z denote the smooth projective models of the function fields K, E, L, respectively.

For an étale sheaf M on $X-S$, we abbreviate $h^i_{\text{ét}}(X-S, \mathsf{M})$ for $\dim_\kappa H^i_{\text{ét}}(X-S, \mathsf{M})$ and write $\chi_{\text{ét}}(X-S, \mathsf{M})$ for its Euler-Poincaré characteristic $h^0_{\text{ét}}(X, \mathsf{M}) - h^1_{\text{ét}}(X, \mathsf{M}) + h^2_{\text{ét}}(X, \mathsf{M})$. We will regard any $\kappa[H]$-module M as an étale sheaf on X. The notations κ and $\mathbb{F}_p$ are also used for the trivial one-dimensional Galois modules over the respective field. Note that if $\Delta S = \varnothing$, i.e. $\mathrm{Ram}(\bar\rho) \subset S$, then $L_S = K_S$, and so $h^i_S(M) = h^i_{\text{ét}}(X - S, M)$.

We quote the following well-known result from [SGA1], XIII.2.12:

Proposition 3.1 *Let C be a smooth projective curve over k with function field F. If Σ is a finite non-empty set of places of C, then $h^2_{\text{ét}}(C - \Sigma, \mathbb{F}_p) = 0$ and $h^1_{\text{ét}}(C - \Sigma, \mathbb{F}_p) = 2g_F + |\Sigma| - 1$. In particular, the pro-p completion of* $\mathrm{Gal}(F_\Sigma/F)$ *is a free pro-p group on $2g_F + |\Sigma| - 1$ generators.*

If $\Sigma = \varnothing$ and $C \cong \mathbb{P}^1$, then $h^1(C, \mathbb{F}_p) = h^2(C, \mathbb{F}_p) = 0$.

Lemma 3.2 *Suppose that $S \supset S_p$. If either $S \neq \varnothing$ or $S = \varnothing$ and $Y \cong \mathbb{P}^1$, then $h^2_S(M) = 0$ for any $\kappa[H]$-module M.*

Note that in practice the condition $Y \cong \mathbb{P}^1$ (and not $X \cong \mathbb{P}^1$) is less straightforward to verify than $S \neq \varnothing$.

Proof: Note first that $S \supset S_p$ implies that $E_S = L_S$. Because $[E : K]$ is prime to p, the restriction map $H^2(G_S, M) \longrightarrow H^2(\mathrm{Gal}(E_S/E), M)$ is injective, and so it is enough to prove that the latter module vanishes. The action of $\mathrm{Gal}(E_S/E)$ on M is via a p-group. Therefore there exists a decomposition series of M all of whose subquotients are isomorphic to $\mathbb{F}_p$ with trivial Galois action. By devissage it suffices to show that $H^2(\mathrm{Gal}(E_S/E), \mathbb{F}_p) \cong H^2_{\text{ét}}(Y - S(Y), \mathbb{F}_p) = 0$, where $S(Y)$ denotes the places in Y above S. This follows from the previous proposition. ∎

Proof of Theorem 2.3: By Proposition 2.2, the above lemma implies that R_S is a power series ring over $W(\kappa)$ provided that $S \supset S_p$ is non-empty. The following proposition if applied to $M = \overline{\mathrm{ad}}_{\bar\rho}$ gives an explicit expression for the relative dimension $h^1_S(\overline{\mathrm{ad}}_{\bar\rho})$. Since $\mathrm{Cent}_{\mathrm{PGL}_n(\kappa)}(\mathrm{Im}(\bar\rho)) = \{1\}$, we have $\dim_\kappa \overline{\mathrm{ad}}^H = 0$, and so this explicit expression agrees with the expression in Theorem 2.3. ∎

Proposition 3.3 *Suppose that $\varnothing \neq S \supset S_p$. Then for any $\kappa[H]$-module M one has*

$$h^1_S(M) = (2g_K + |S^+| - 2)\dim_\kappa M + \dim_\kappa M^H - \sum_{x\in\Delta S} \dim_\kappa M^{H_x}.$$

If S contains $\mathrm{Ram}(\bar{\rho})$, then a formula for this number is well-known, cf. [Mil], Thm. V.2.18. The only complication that arises is due to the fact that S might be smaller.

The following simple lemma will be crucial in the proof of Proposition 3.3.

Lemma 3.4 *Denote by $Ind^H_{H_x}\mathbb{F}_p$ the representation of H induced by the trivial representation of H_x on $\mathbb{F}_p$. If $S \neq \varnothing$, one has the following short exact sequence of $\mathbb{F}_p[H]$-modules*

$$0 \longrightarrow H^1(N_S,\mathbb{F}_p) \longrightarrow H^1(N_{S^+},\mathbb{F}_p) \longrightarrow Q_{\Delta S} := \coprod_{x\in\Delta S} Ind^H_{H_x}\mathbb{F}_p \longrightarrow 0. \qquad (2)$$

If furthermore $S \supset S_p$, then $Q_{\Delta S}$ is projective, and so the above sequence is split.

Proof: Recall that $S^+ = S \amalg \Delta S$. Therefore the following sequence is left exact

$$0 \longrightarrow H^1(N_S,\mathbb{F}_p) \longrightarrow H^1(N_{S^+},\mathbb{F}_p) \longrightarrow \coprod_{x\in\Delta S}\coprod_{z\mapsto x} H^1(J_z,\mathbb{F}_p),$$

where for each $x \in \Delta S$ we sum over all places $z \in Z$ mapping to x. Each of the $H^1(J_x,\mathbb{F}_p)$ is isomorphic to $\mathbb{F}_p$ and the dimension of $H^1(N_S,\mathbb{F}_p)$ and $H^1(N_{S^+},\mathbb{F}_p)$ are given by Proposition 3.1. Counting dimension now proves the right exactness of the above sequence.

Let us fix $x \in \Delta S$ and consider

$$Q_x := \coprod_{z\mapsto x} H^1(J_z,\mathbb{F}_p) \cong \coprod_{z\mapsto x}\mathbb{F}_p.$$

Let S_x be the set of places in L above x. Then Q_x is the $\mathbb{F}_p$-module $\mathrm{Maps}(S_x,\mathbb{F}_p)$ of all maps from S_x to $\mathbb{F}_p$, and the action of H is given by its natural permutation action on S_x. Thus $Q_x \cong \mathrm{Ind}^H_{H_x}\mathbb{F}_p$.

It remains to prove the projectivity of $Q_{\Delta S} \cong \coprod_{x\in\Delta S} Q_x$ as an $\mathbb{F}_p[H]$-module, provided that $S \supset S_p$. To see this, note that an induced module is projective precisely when the module from which it was induced is projective (over the smaller group ring). So we need to show that $\mathbb{F}_p$ is projective over $\mathbb{F}_p[H_x]$. But for $x \in \Delta S$, i.e., $x \notin S_p$, the groups H_x are of order prime to p, so that any $\mathbb{F}_p[H_x]$-module is projective. ∎

Corollary 3.5 *Suppose that $\varnothing \neq S \supset S_p$. Then for any $\kappa[H]$-module M there is a short exact sequence*

$$0 \longrightarrow H^1(G_S,M) \longrightarrow H^1(G_{S^+},M) \longrightarrow \coprod_{x\in\Delta S} M^{H_x} \longrightarrow 0.$$

Proof: We consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1(H,M) \arrow[r] \arrow[d, equal] & H^1(G_S,M) \arrow[r] \arrow[d, "\gamma"] & H^1(N_S,M)^H \arrow[r] \arrow[d, "\nu"] & H^2(H,M) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & H^1(H,M) \arrow[r] & H^1(G_{S^+},M) \arrow[r] & H^1(N_{S^+},M)^H \arrow[r] & H^2(H,M) \arrow[r] & 0,
\end{tikzcd}$$

whose rows are exact by the inflation-restriction sequence and Lemma 3.2. The maps γ and ν are injective, again since they arise from an inflation restriction sequence and since taking H-invariants is left exact. By the snake lemma, we must have $\mathrm{Coker}(\gamma) \cong \mathrm{Coker}(\nu)$. We now apply the previous lemma to compute $\mathrm{Coker}(\nu)$.

Note first that if we tensor Sequence (2) with M over $\mathbb{F}_p$, we obtain again a split exact sequence. Therefore taking H-invariants yields yet another short exact sequence. Since the actions of N_S and N_{S^+} on M are both trivial, the latter sequence is isomorphic to the short exact sequence

$$0 \longrightarrow H^1(N_S, M)^H \longrightarrow H^1(N_{S^+}, M)^H \longrightarrow (Q_{\Delta S} \otimes M)^H \longrightarrow 0, \tag{3}$$

and so $\mathrm{Coker}(\gamma) \cong (Q_{\Delta S} \otimes M)^H$. Because $Q_{\Delta S}$ is a sum of induced representation, we can simplify the latter expression

$$(Q_{\Delta S} \otimes M)^H \cong \coprod_{x \in \Delta S} \mathrm{Ind}_{H_x}^H (\mathbb{F}_p \otimes \mathrm{Res}_H^{H_x} M)^H \cong \coprod_{x \in \Delta S} (\mathrm{Res}_H^{H_x} M)^{H_x} \cong \coprod_{x \in \Delta S} M^{H_x},$$

and the corollary follows. ∎

Proof of Proposition 3.3: By [Mil], Thm. V.2.18, one has $\chi_{\text{ét}}(X - S^+, M) = (2 - 2g_K - |S^+|) \dim_\kappa M$ for the Euler-Poincaré characteristic of M on $X - S^+$. Lemma 3.2 shows that $h^2_{S^+}(M) = 0$, and the equality $h^0_{S^+}(M) = \dim_\kappa M^H$ is obvious. Since $S^+ \supset \mathrm{Ram}(\bar\rho)$, we have $h^i_{S^+}(M) = h^i_{\text{ét}}(X - S^+, M)$ and therefore

$$h^1_{S^+}(M) = (2g_K - 2 + |S^+|) \dim_\kappa M + \dim_\kappa M^H.$$

The previous corollary yields $h^1_S(M) = h^1_{S^+}(M) - \sum_{x \in \Delta S} \dim_\kappa M^{H_x}$, and the desired dimension formula follows. ∎

For later use, we record the following consequence of Theorem 2.3:

Corollary 3.6 *Suppose $\bar\rho\colon G_{k(t)} \longrightarrow \mathrm{PGL}_n(\kappa)$ is surjective, and ramified precisely at the three places $0, 1, \infty$, and that l is prime to the order of $\mathrm{PGL}_n(\kappa)$. Let g_i be a topological generator of a (pro-cyclic) inertia subgroup I_i of $G^{(l)}_{k(t)}$, for $i = 0, 1, \infty$, and assume that*

(a) $\bar\rho(g_\infty)$ is a regular unipotent element.

(b) $\bar\rho(g_1)$ is a regular semisimple element.

(c) $\bar\rho(g_0)$ has a semisimple lift to $\mathrm{GL}_n(\kappa)$ which has 1 as an $n-1$-fold eigenvalue.

Then $R_{\{\infty\}} \cong W(\kappa)[[T_1, \ldots, T_{n-1}]]$ and $R_{\{1,\infty\}} \cong W(\kappa)[[T_1, \ldots, T_{2n-2}]]$.

Proof: Since a semisimple element of $\mathrm{GL}_n(\kappa)$ has order prime to p, we have $S_p = \{\infty\}$. The genus of $K = k(t)$ is zero. For both, $S = S_p$ and $S = \{1, \infty\}$, we find $S^+ = \mathrm{Ram}(\bar\rho) = \{0, 1, \infty\}$. Our assumptions on the g_i imply that $\dim_\kappa \overline{\mathrm{ad}}_{\bar\rho}^{g_1} = n - 1$ and $\dim_\kappa \overline{\mathrm{ad}}_{\bar\rho}^{g_0} = (n-1)^2$. The result is now immediate from Theorem 2.3. ∎

4 Deformations with maximal image

In this section we will give the proofs of Proposition 2.4 and Corollary 2.6, which gives a sufficient criterion for $\rho_{\mathscr{D}}$ to have maximal image. As a preparation, we also prove Proposition 2.12, which in turn requires the following lemma:

Lemma 4.1 *Let H be a subgroup of $\mathrm{PGL}_n(\kappa)$ such that $\overline{\mathrm{ad}}$ is irreducible over $\mathbb{F}_p[H]$ and absolutely irreducible over $\kappa[H]$. Let V be a vector space over κ with the trivial action of H, and give $V \otimes_\kappa \overline{\mathrm{ad}}$ the diagonal action of H. Then any $\mathbb{F}_p[H]$-submodule of $V \otimes_\kappa \overline{\mathrm{ad}}$ is equal to $W \otimes \overline{\mathrm{ad}}$ for some sub κ-vector space W of V.*

Proof: Since the $\mathbb{F}_p[H]$-span of any vector in $V \otimes \overline{\mathrm{ad}}$ is finite dimensional, we may assume $d := \dim_\kappa V < \infty$. As $V \otimes \overline{\mathrm{ad}}$ is isomorphic to $\overline{\mathrm{ad}}^d$ as an $\mathbb{F}_p[H]$-module, any irreducible $\mathbb{F}_p[H]$-submodule U will be isomorphic to $\overline{\mathrm{ad}}$. Let $r_1, \ldots, r_d$ be a basis of V over κ. It will suffice to show that for any U as above there exist $a_i \in \kappa$ such that $(\sum a_i r_i)\overline{\mathrm{ad}} = U$:

Let $u \in U \subset V \otimes \overline{\mathrm{ad}}$ be non-zero and write it (uniquely) as $\sum w_i r_i$ with $w_i \in \overline{\mathrm{ad}}$. One of the w_i is non-zero, and by possibly reindexing the r_i, we assume $w_1 \neq 0$. Since u is a generator of U, we have $\mathbb{F}_p[H]/\operatorname{Ann}_{\mathbb{F}_p[H]}(u) \cong U \cong \overline{\mathrm{ad}}$. Similarly any non-zero w_i is a generator of $\overline{\mathrm{ad}}$, so that $\mathbb{F}_p[H]/\operatorname{Ann}_{\mathbb{F}_p[H]}(w_i) \cong \mathbb{F}_p[H]w_i \cong \overline{\mathrm{ad}}$ holds for such. The r_i being a basis of V on which H acts trivially, we deduce $\operatorname{Ann}_{\mathbb{F}_p[H]}(u) = \cap_{i:w_i \neq 0} \operatorname{Ann}_{\mathbb{F}_p[H]}(w_i)$. Comparing dimensions over $\mathbb{F}_p$, we find $\operatorname{Ann}_{\mathbb{F}_p[H]}(w_i) = \operatorname{Ann}_{\mathbb{F}_p[H]}(u)$ for any non-zero w_i. In particular $bw_1 \mapsto bw_i$, $b \in \mathbb{F}_p[H]$, is well-defined and an endomorphism of $\overline{\mathrm{ad}}$ for any i. Since $\overline{\mathrm{ad}}$ is absolutely irreducible over $\kappa[H]$, the ring $\operatorname{End}_{\mathbb{F}_p[H]}(\overline{\mathrm{ad}})$ is isomorphic to κ, and so there exist $a_i \in \kappa$, such that $w_i = a_i w_1$ for all i. Thus $U = \mathbb{F}_p[H](\sum_i a_i w_1 r_i) = (\sum_i a_i r_i)\mathbb{F}_p[H]w_1 = (\sum_i a_i r_i)\overline{\mathrm{ad}}$. ∎

Proof of Proposition 2.12: Extending the notation introduced above Proposition 2.12, we set $K_m^R := K_{R/\mathfrak{m}_R^m}^R$, i.e., as the kernel of the epimorphism $\mathrm{PGL}_n(R) \longrightarrow \mathrm{PGL}_n(R/\mathfrak{m}_R^m)$. Let $N \subset \mathrm{PGL}_n(R)$ be open and such that it is contained in K_1^R. Then there exists a smallest $m \in \mathbb{N}$ such that $K_m^R \subset N$. We claim by induction on this m that we can find a surjection $R \longrightarrow R'$ in $\mathscr{C}$ such that $N = K_{R'}^R$. For $m = 1$ there is obviously nothing to prove.

Suppose now that we have proved the claim for m and for all R in $\mathscr{C}$ (without loss of generality we assume $\kappa = \kappa_R$). Suppose that N satisfies $K_{m+1}^R \subset N$ and that $m+1$ is minimal with this property. Then for $N' := N \cap K_m^R$ the quotient N'/K_{m+1}^R is a proper $\mathbb{F}_p[H]$-submodule of

$$K_m^R/K_{m+1}^R \cong \mathfrak{m}_R^m/\mathfrak{m}_R^{m+1} \otimes_\kappa \overline{\mathrm{ad}}.$$

By Lemma 4.1, there exist κ-linearly independent elements $\bar{r}_i$ in $\mathfrak{m}_R^m/\mathfrak{m}_R^{m+1}$, $i = 1, \ldots, t$, such that

$$N'/K_{m+1}^R \cong (\oplus_{i=1}^t \kappa \bar{r}_i) \otimes_\kappa \overline{\mathrm{ad}}.$$

Set $\bar{R} := (R/(\mathfrak{m}_R^{m+1})/(\bar{r}_1, \ldots, \bar{r}_t))$, so that $N' = K_{\bar{R}}^R$.

Next consider the (finite) open normal subgroup $\bar{N} := N/N'$ of $\mathrm{PGL}_n(\bar{R})$ with $\bar{N} \subset K_1^{\bar{R}}$. By construction we also have $K_m^{\bar{R}} \subset \bar{N}$. Thus our induction hypothesis implies that there exists an epimorphism $\bar{R} \longrightarrow R'$ (of artinian rings) in $\mathscr{C}$ such that $\bar{N} = K_{R'}^{\bar{R}}$. But then $N = K_{R'}^R$ and the proof is complete. ∎

We now prove the results on maximal image announced in Section 2. For any ring $R \in \mathscr{C}$ define $R_2 := R/\mathfrak{m}_R^2$ and $\bar{R}_2 := R/(p, \mathfrak{m}_R^2)$. If ρ is a representation into $\mathrm{PGL}_n(R)$, then we also define $\rho_2 := \rho \pmod{\mathfrak{m}_R^2}$ and $\bar{\rho}_2 := \rho \pmod{(p, \mathfrak{m}_R^2)}$. The proof of [Bo1], Prop. 2, easily implies the following:

Lemma 4.2 *Let R be as above, G be a profinite group and $\rho\colon G \longrightarrow \mathrm{PGL}_n(R)$ a continuous representation. If $p \not| n$ and ρ_2 has maximal image, then so does ρ.*

Proof of Proposition 2.4: If $R_2 \cong \bar{R}_2$, the above lemma proves the proposition. Therefore we assume that $0 \neq p \in R_2$. Define $\widetilde{H}_2 := \{A \in \mathrm{PGL}_n(R_2) : A \pmod{\mathfrak{m}_{R_2}} \in \mathrm{Im}(\bar{\rho})\}$ and $\bar{H}_2$ as its reduction modulo p. We consider the short exact sequence

$$1 \longrightarrow \overline{\mathrm{ad}} \longrightarrow \widetilde{H}_2 \xrightarrow{\pi_2} \bar{H}_2 \longrightarrow 1.$$

The map ρ_2 takes its image inside $\widetilde{H}_2$. We claim that it surjects onto $\widetilde{H}_2$. If the claim is shown, the proof is complete by an application of the above lemma.

We assume the contrary, namely that $\mathrm{Im}(\rho_2)$ is properly contained in the group $\widetilde{H}_2$. By our assumption the representation $\bar{\rho}_2$ surjects onto $\bar{H}_2$. Since $\overline{\mathrm{ad}}$ is irreducible, its intersection with $\mathrm{Im}(\rho_2)$ is trivial. Therefore there exists a splitting of π_2. Clearly, $\bar{H}_2 \longrightarrow H$ also has a splitting, and hence there is a splitting of $\widetilde{H}_2 \twoheadrightarrow H$. Choose elements $r_1, \ldots, r_d \in \mathfrak{m}_{R_2}/\mathfrak{m}_{R_2}^2$ such that $p, r_1, \ldots, r_d$ is a basis of this module over κ. Then $R_2/(r_1, \ldots, r_d) \cong W_2(\kappa)$, since otherwise we would have $p \in (r_1, \ldots, r_d)$. If we apply the induced surjective homomorphism $R_2 \longrightarrow W_2(\kappa)$ to the elements of $\widetilde{H}_2$, we obtain a splitting of $\{A \in \mathrm{PGL}_n(W_2(\kappa)) : A \pmod{p} \in H\} \twoheadrightarrow H$, contradicting our assumptions. ∎

Proof of Corollary 2.6: To prove Corollary 2.6 for a general deformation datum $\mathscr{D} = (n_x)_{x\in\Sigma}$, it suffices to prove it in the case where $n_x = \infty$ for all $x \in \mathrm{Supp}\,\mathscr{D}$, i.e. for R_S with $S = \mathrm{Supp}\,\mathscr{D}$. It is then an immediate consequence of Proposition 2.4 and the following lemma. ∎

Lemma 4.3 *Suppose $R = R_S$, $H^1(H, \overline{\mathrm{ad}}) = 0$, $\overline{\mathrm{ad}}$ is irreducible over $\mathbb{F}_p[H]$ and absolutely irreducible over $\kappa[H]$. Then $\bar{\rho}_2$ has maximal image.*

Proof: Let $\bar{H}_2$ be the image of $\bar{\rho}_2$ inside $\mathrm{PGL}_n(\bar{R}_2)$. By Proposition 2.12, there exists an epimorphism $R_2 \longrightarrow \widetilde{R}_2$ (of finite rings) in $\mathscr{C}$, such that $K_{\widetilde{R}_2}^{R_2} = \widetilde{H}_2 \cap K_\kappa^{R_2}$ in the notation from there. Let $\widetilde{\rho}_2 := \rho_2 \otimes_{R_2} \widetilde{R}_2$. By construction we have $\mathrm{Im}(\widetilde{\rho}_2) \cong H$. Since the image of $\widetilde{\rho}_2$ is a subgroup of the central term of the short exact sequence

$$1 \longrightarrow K_\kappa^{\widetilde{R}_2} \longrightarrow \{A \in \mathrm{PGL}_n(\widetilde{R}_2) : A \pmod{\mathfrak{m}_{\widetilde{R}_2}} \in H\} \longrightarrow H \longrightarrow 1,$$

the sequence is split. The left hand term $K_\kappa^{\widetilde{R}_2}$ is isomorphic to a direct sum of $\mathrm{len}(\widetilde{R}_2)-1$ copies of $\overline{\mathrm{ad}}$. The condition $H^1(H, \overline{\mathrm{ad}}) = 0$ therefore implies that the splitting is the trivial one. By the universality of R_S, the trivial splitting can never occur for a quotient of R_S. Hence $\mathrm{len}(\widetilde{R}_2) - 1 = 0$, or in other words $\widetilde{R}_2 \cong \kappa$, and so $\bar{\rho}_2$ has maximal image. ∎

5 Linear and projective representations

For some of the results in the applications, it is necessary to compare deformations of linear and projective representations. We start with a brief discussion on lifting residual projective to linear representation. The following is a simple consequence of obstruction theory. Note again our convention that 'primed' representations are linear and the other ones projective.

Proposition 5.1 *The obstruction to lifting $\bar{\rho}$ to a linear representation $\bar{\rho}'$ is given by an element in $H^2(G_K, \kappa^*)$. If $\bar{\rho}$ takes its image in $\mathrm{PSL}_n(\kappa)$, the obstruction to a lift to $\mathrm{SL}_n(\kappa)$ is an element in $H^2(G_K, \{\pm 1\})$.*

While G_K is not so well understood, the group $G_K^{(l)}$ is. As a simple application of Lemma 3.2, we obtain:

Corollary 5.2 *If $\mathrm{Im}(\bar{\rho}) \subset \mathrm{PSL}_n(\kappa)$, assume that $l > 2$. Otherwise assume that $l \not| |\kappa| - 1$. Then if $S \supset S_p$ is non-empty, any $\bar{\rho}$ has a lift $\bar{\rho}' \colon G_S \longrightarrow \mathrm{GL}_n(\kappa)$.*

From now on, let us assume that we have a lift $\bar{\rho}' \colon G_K \longrightarrow \mathrm{GL}_n(\kappa)$ of $\bar{\rho}$. Let L' denote the splitting field of $\bar{\rho}'$ over K. Furthermore, we fix any lift η of $\det \bar{\rho}'$ whose restriction to $G_{L'}$ is unramified outside S, e.g., we can take the Teichmüller lift of $\det \bar{\rho}'$.

We define the functor Def'_S from $\mathscr{C}$ to the category of sets by

$$\begin{aligned}\mathrm{Def}'_S(R) \quad := \quad & \{\rho' \colon G_K \longrightarrow \mathrm{GL}_n(R) | \, \rho' \equiv \bar{\rho}' \pmod{\mathfrak{m}_R}, \ \rho' \text{ is continuous} \\ & \text{and } \rho'_{|G_{L'}} \text{ is unramified outside } S\}/\sim,\end{aligned}$$

where again $\sim$ is strict equivalence. Def^η_S denotes the subfunctor of Def'_S of deformations whose determinant is equal to η. There are obvious analogs of Propositions 2.1 and 2.2 for these functors, where $\overline{\mathrm{ad}}$ has to be replaced by ad and ad^0, respectively. We omit the precise statements. By (R'_S, ρ'_S) and (R^η_S, ρ^η_S) we denote the universal pairs corresponding to Def'_S and Def^η_S. An analog of Theorem 2.3 holds, too, under the hypotheses that $S \supset S_p$ is non-empty and that $\mathrm{Cent}_{\mathrm{GL}_n(\kappa)}(\mathrm{Im}(\bar{\rho}')) = \kappa^*$.

For any ring R, let $\mathrm{proj} \colon \mathrm{GL}_n(R) \longrightarrow \mathrm{PGL}_n(R)$ denote the canonical surjection.

Proposition 5.3 *Assume that $S \supset S_p$ is non-empty and $p \not| n$. Then the assignment $\rho' \mapsto \mathrm{proj} \circ \rho'$ for $\rho' \in \mathrm{Def}^\eta_S(R)$ defines a natural isomorphism $\mathrm{Def}^\eta_S \cong \mathrm{Def}_S$.*

In particular under the hypothesis of the proposition, one has $(R_S, \rho_S) \cong (R^\eta_S, \mathrm{proj} \circ \rho^\eta_S)$.

Proof: The assignment $\rho' \mapsto \mathrm{proj} \circ \rho'$ is clearly functorial, so we only need to check bijectivity. To see the injectivity, suppose that ρ'_1, ρ'_2 have the same image ρ. Then there exists a continuous character $\chi \colon G_S \longrightarrow R^*$ such that $\rho'_2 = \rho'_1 \otimes \chi$. Because ρ'_1, ρ'_2 are both deformations of $\bar{\rho}'$, the image of χ lies in $1 + \mathfrak{m}_R$. Furthermore, taking determinants yields $\eta = \chi^n \eta$, i.e. $\chi^n = 1$. Because $p \not| n$, elements of $1 + \mathfrak{m}_R$ have unique n-th roots of unity (just write down the power series for $(1+x)^{1/n}$). Hence $\chi = 1$.

For the surjectivity, suppose we are given a deformation ρ to R of $\bar{\rho}$. The obstruction to lifting ρ to a linear representation $\rho' : G_S \longrightarrow \mathrm{GL}_n(R)$ is given by an element $\theta \in H^2(G_S, R^*)$. Because $\bar{\rho}$ lifts to $\bar{\rho}'$, the image of θ in $H^2(G_S, \kappa^*)$ vanishes, so θ lies in $H^2(G_S, 1 + \mathfrak{m}_R)$. Due to our assumption that $S \supset S_p$ is non-empty, Lemma 3.2 implies that $H^2(G_S, \mathbb{F}_p) = 0$. A limit argument shows that $H^2(G_S, 1 + \mathfrak{m}_R) = 0$. Thus we can find a deformation $[\rho'] \in \mathrm{Def}'_S(R)$ such that $\mathrm{proj} \circ \rho' \sim \rho$.

By twisting, we may assume that $\rho' \pmod{p}$ is isomorphic to $\bar{\rho}'$. Then $(\det \rho')\eta^{-1} : G_S \longrightarrow 1 + \mathfrak{m}_R$. As observed above, one can take unique n-th roots inside the one-units of R. So there exists a character $\psi \colon G_S \longrightarrow 1 + \mathfrak{m}_R$ with $\psi^n = (\det \rho')\eta^{-1}$. It follows that $[\rho' \otimes \psi^{-1}] \in \mathrm{Def}^\eta_S$, proving the desired surjectivity. ∎

Remark 5.4 (a) Let Π be any profinite group. Let $\bar{\rho}' : \Pi \longrightarrow \mathrm{GL}_n(\kappa)$ be a linear residual representation and $\bar{\rho} : \Pi \longrightarrow \mathrm{PGL}_n(\kappa)$ the corresponding projective representation. Suppose $\eta : \Pi \longrightarrow W(\kappa)^*$ is a lift of $\det \bar{\rho}'$. Denote by $\mathrm{Def}^{\eta}_{\Pi,\bar{\rho}'}$ the deformation functor for deformations of $\bar{\rho}'$ to $\mathscr{C}$ with determinant η and by $\mathrm{Def}_{\Pi,\bar{\rho}}$ the deformation functor for deformations of $\bar{\rho}$. Then the proof of the above theorem shows that the natural map $\mathrm{Def}^{\eta}_{\Pi,\bar{\rho}'} \longrightarrow \mathrm{Def}_{\Pi,\bar{\rho}}$ defines an isomorphism of functors whenever p does not divide n.

(b) Let us keep the notation of (a) and assume again that p does not define n. Define Def^{1}_{Π} as the deformation functor of deformations of the trivial 1-dimensional representation. Then one easily sees that $\mathrm{Def}^{\eta}_{\Pi,\bar{\rho}'} \hat{\otimes} \mathrm{Def}^{1}_{\Pi} \cong \mathrm{Def}_{\Pi,\bar{\rho}'}$ where the latter functor describes all deformations of $\bar{\rho}'$, and where $\hat{\otimes}$ is the completed tensor product over $W(\kappa)$. If the functors are furthermore representable (or have a hull), then the same relation via the tensor product holds for the corresponding universal (or versal) rings and representations.

For later use we need the following special result:

Proposition 5.5 *If the smooth proper model X of K is isomorphic to $\mathbb{P}^1$, if $S \supset S_p$ consists of a single element and if $p \not| n$, then the natural inclusion of functors $\mathrm{Def}^{\eta}_{S} \hookrightarrow \mathrm{Def}'_{S}$ is an isomorphism. In particular η is the unique lift of $\det \bar{\rho}$.*

Proof: By Remark 5.4 (b), it suffices to show that the universal ring for Def^{1}_{Π} is isomorphic to $W(\kappa)$. Under the stated hypotheses, Proposition 3.1 implies $h^{i}_{\text{ét}}(X - S, \kappa) = 0$ for $i = 1, 2$. The desired structure of the universal ring now follows from obstruction theory, and more specifically the analog of Proposition 2.2 for Def^{1}_{Π}. ∎

6 Rigid deformations

Given a strictly rigid residual representation $\bar{\rho}$, one cannot expect that all of its deformations or in particular the universal deformations ρ_S or $\rho_{\mathscr{D}}$ are again strictly pro-rigid. To preserve rigidity, one needs further local restrictions. This section starts with several pages of preparatory material. This is needed for our definition of a rigid deformation functor $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}$. We prove that this functor is representable and establish that the resulting universal deformation is again strictly pro-rigid. The latter result will include Theorem 2.20 as a special case. In the end, we will also deduce generalizations of Corollaries 2.26 and 2.25.

In the remainder of this article, we assume $K = k(t)$.

Recall that a matrix $\bar{A}$ in $\mathrm{PGL}_n(\kappa)$ or in $\mathrm{GL}_n(\kappa)$ is called *regular*, if $\dim \mathrm{ad}^{\bar{A}} = n$. Let R be in $\mathscr{C}$. A matrix $A \in \mathrm{PGL}_n(R)$ or in $\mathrm{GL}_n(R)$ is called *regular* if and only if its reduction modulo $\mathfrak{m}_R$ is so.

Using the Jordan or rational canonical form one finds:

Lemma 6.1 *Let $\bar{A}'$ be in $\mathrm{GL}_n(\kappa)$ and define on $\bar{V} := \kappa^n$ the structure of a $\kappa[T]$-module via T acting as $\bar{A}'$. Then the following are equivalent:*

(a) $\bar{A}'$ is regular.

(b) Different Jordan blocks in a Jordan decomposition of $\bar{A}'$ have distinct eigenvalues.

(c) The minimal polynomials of T on different indecomposable summands of $\bar{V}$ are relatively prime.

(d) $\bar{V}$ is a cyclic $\kappa[T]$-module.

(e) The characteristic and minimal polynomials of $\bar{A}'$ agree.

(f) $\bar{A}'$ is conjugate to the companion matrix of its characteristic polynomial.

It is our convention that the companion matrix of a monic polynomial $f = \sum_{i=0}^{n} a_i T^i$ of degree n is the matrix whose i-th column is the $(i+1)$-th standard basis vector for $i = 1.\ldots, n-1$, and whose n-th column is the transpose of $(-a_0, \ldots, -a_{n-1})$.

Lemma 6.2 *For $R \in \mathscr{C}$ and $A' \in \mathrm{GL}_n(R)$ the following are equivalent:*

(a) A' is regular

(b) A' is conjugate to the companion matrix of its characteristic polynomial.

(c) The set $\{{A'}^i : i = 0, \ldots, n-1\}$ is part of a basis of $M_n(R)$.

(d) $M_n(R)^{A'}$ is a direct summand of $M_n(R)$ with basis $\{{A'}^i : i = 0, \ldots, n-1\}$.

If either of the above holds, then for any morphism $R \longrightarrow \widetilde{R}$ in $\mathscr{C}$ one has $M_n(R)^{A'} \otimes_R \widetilde{R} \cong M_n(\widetilde{R})^{A'}$ under the canonical isomorphism $M_n(R) \otimes_R \widetilde{R} \cong M_n(\widetilde{R})$.

Proof: (a)⇒(b): Suppose that $\bar{A}'$ is regular. Choose an element $v \in R^n$ whose reduction mod $\mathfrak{m}_R$ is a cyclic vector for $\bar{A}'$. By Nakayama's Lemma it follows that ${A'}^i v$, $i = 0, \ldots, n-1$, is a basis of R^n. With respect to it, the matrix A' has the desired form.

(b)⇒(c): Let $E'_{i,j}$ be the matrix with entry 1 at the place (i,j) and 0 elsewhere. If A' is a companion matrix, then by considering the first columns of the matrices ${A'}^i$, it is clear that the set $\{{A'}^i : i = 0, \ldots, n-1\}$ together with $\{E'_{i,j} : i = 1, \ldots, n, j = 2, \ldots, n\}$ forms a basis of $M_n(R)$.

The implications (c)⇒(a) and (d)⇒(a) are immediate: If $\bar{A}'$ denotes A' (mod $\mathfrak{m}_R$), then either assumption implies that the matrices ${\bar{A}'}^i$, $i = 0, \ldots, n-1$, are linearly independent over κ, so that for $\bar{A}'$ the minimal and characteristic polynomial coincide.

It remains to prove that (a)–(c) imply (d). By (c) the set $\{{A'}^i : i = 0, \ldots, n-1\}$ is part of a basis of $M_n(R)$. Since the set is clearly contained in $M_n(R)^{A'}$, we need to show that it spans $M_n(R)^{A'}$ as an R-module. (This is not completely straightforward, since in general the canonical homomorphism $M_n(R)^{A'} \otimes_R \kappa \longrightarrow M_n(\kappa)^{\bar{A}'}$ is not an isomorphism.) Because $R = \varprojlim R/\mathfrak{m}_R^j$, it suffices to prove (d) in the case where R has finite length, and so we will assume this.

We claim that one has the general bound $\mathrm{len}(M_n(R)^{A'}) \leq \mathrm{len}(M_n(\kappa)^{\bar{A}'}) \,\mathrm{len}(R)$ for the length of $M_n(R)^{A'}$. Using (a) this yields $\mathrm{len}(M_n(R)^{A'}) \leq n \,\mathrm{len}(R) = \mathrm{len}(\sum_{i=0}^{n-1} R{A'}^i)$, and so (d) is shown. For the claim, we choose $e \in \mathbb{N}$ such that $\mathfrak{m}_R^e = 0$ and consider the left exact sequences

$$0 \longrightarrow M_n(\mathfrak{m}_R^{i+1}/\mathfrak{m}_R^e)^{A'} \longrightarrow M_n(\mathfrak{m}_R^i/\mathfrak{m}_R^e)^{A'} \longrightarrow M_n(\mathfrak{m}_R^i/\mathfrak{m}_R^{i+1})^{A'}$$

for $i = 0, \ldots, e-1$. The term on the right is isomorphic to $M_n(\kappa)^{\bar{A}'} \otimes_\kappa \mathfrak{m}_R^i/\mathfrak{m}_R^{i+1}$ and thus has length $\mathrm{len}(M_n(\kappa)^{\bar{A}'}) \,\mathrm{len}(\mathfrak{m}_R^i/\mathfrak{m}_R^{i+1})$. By induction on i, the claim follows.

Finally, if (a)–(d) hold, then the image of A' under $R \longrightarrow \widetilde{R}$ is again regular, and now the last assertion is a direct consequence of (d). ∎

We will need the following generalization of regularity:

Definition 6.3 *Let R be in $\mathscr{C}$, let A' be in $\mathrm{GL}_n(R)$ and consider $V := R^n$ as an $R[T]$-module by having T act as A'.*

The matrix A' is called block-regular*, if there is an isomorphism $V = \oplus_{i=1}^s W_i^{m_i}$ of $R[T]$-modules such that T is a regular endomorphism on the reduction $\oplus_{i=1}^s W_i \otimes_R \kappa$.*

A matrix $A \in \mathrm{PGL}_n(R)$ is called block-regular*, if it has an block-regular representative in $\mathrm{GL}_n(R)$.*

Note that in the definition of block-regularity the regularity of $\oplus_{i=1}^s W_i \otimes_R \kappa$ implies that the minimal polynomials of the various $W_i \otimes_R \kappa$ are relatively prime.

It is the notion of block-regularity of lifts which will later be important when deforming strictly pro-rigid representations.

Using for instance the rational canonical form, any endomorphism of a vector space can be decomposed into invariant subspaces on which the endomorphism acts via a regular matrix whose minimal polynomial is a power of an irreducible one. Over general rings $R \in \mathscr{C}$ such a decomposition is no longer possible. However one can still decompose endomorphisms into isotypical components for actions prime to p. The point is that for a finite group G of order prime to p the categories of finitely generated $\kappa[G]$-modules and of finitely generated $R[G]$-modules which are free over R are equivalent.

Lemma 6.4 *Suppose $R \in \mathscr{C}$. Let A be in $\mathrm{GL}_n(R)$ and denote by $\bar{A}'$ its reduction modulo $\mathfrak{m}_R$. Let $\widetilde{\kappa} \supset \kappa$ be the smallest overfield which contains all eigenvalues of $\bar{A}'$ and set $\widetilde{q} := |\widetilde{\kappa}|$. Then*

(a) There exists a smallest n_0 such that ${\bar{A}'}^{\widetilde{q}^{n_0}}$ is semisimple, and for any $n_1 \geq n_0$ one has ${\bar{A}'}^{\widetilde{q}^{n_0}} = {\bar{A}'}^{\widetilde{q}^{n_1}}$. Moreover ${\bar{A}'}^{\infty} := {\bar{A}'}^{\widetilde{q}^{n_0}}$ is the semisimplification of $\bar{A}'$.

(b) The limit ${A'}^{\infty} := \lim_{m\longrightarrow\infty} {A'}^{\widetilde{q}^m}$ exists.

(c) The reduction of ${A'}^{\infty}$ is ${\bar{A}'}^{\infty}$.

(d) ${A'}^{\infty}$ and ${\bar{A}'}^{\infty}$ have the same finite order which is prime to p.

(e) If $B' \in \mathrm{GL}_n(R)$ commutes with A', it commutes with ${A'}^{\infty}$.

Proof: Part (a) follows easily by considering the Jordan form of $\bar{A}'$ which is defined over $\widetilde{\kappa}$. To prove (b), we will show that ${A'}^{\widetilde{q}^{n_0+i}} \equiv {A'}^{\widetilde{q}^{n_0+i+1}} \pmod{\mathfrak{m}_R^i}$. The case $i = 1$ has been proved in part (a). For the induction step $i \mapsto i+1$, the inductive hypothesis for i shows that

$$\Delta_i := {A'}^{\widetilde{q}^{n_0+i+1}} - {A'}^{\widetilde{q}^{n_0+i}}$$

lies in $M_n(\mathfrak{m}_R^i)$. By its very definition, it commutes with A'. Raising ${A'}^{\widetilde{q}^{n_0+i}} + \Delta_i$ to the power $\widetilde{q}$ and reducing the result modulo $\mathfrak{m}_R^{i+1}$ yields therefore

$${A'}^{\widetilde{q}^{n_0+i+2}} \equiv {A'}^{\widetilde{q}^{n_0+i+1}} + \widetilde{q}({A'}^{\widetilde{q}^{n_0+i}})^{\widetilde{q}-1}\Delta_i \overset{\widetilde{q}\in\mathfrak{m}_R}{\equiv} {A'}^{\widetilde{q}^{n_0+i+1}} \pmod{\mathfrak{m}_R^{i+1}}.$$

This proves (b). Part (c) is immediate from (a) and the claim just proved.

To prove (d), let e denote the order of ${\bar{A}'}^{\infty}$. It will suffice to show that $({A'}^{\infty})^e$ is the identity in $\mathrm{GL}_n(R)$. Consider

$$({A'}^{\infty})^e = \lim_{m\longrightarrow\infty} ({A'}^{e\,\widetilde{q}^{n_0}})^{\widetilde{q}^m}.$$

Since the reduction of ${A'}^{e\,\widetilde{q}^{n_0}}$ modulo $\mathfrak{m}_R$ is the identity in $\mathrm{GL}_n(\kappa)$, the sequence under the limit converges to the identity in $\mathrm{GL}_n(R)$, proving (d).

The proof of (e) follows straight from the definition of ${A'}^{\infty}$. ∎

Lemma 6.5 *Suppose $R \in \mathscr{C}$ and $\widetilde{A}, \widetilde{A}'$ are matrices in $\mathrm{GL}_n(R)$ of finite order prime to p whose reductions modulo $\mathfrak{m}_R$ agree. Then the two matrices are conjugate over R by a matrix whose reduction modulo $\mathfrak{m}_R$ is the identity.*

Proof: Note first that the two matrices need to have the same order, since for any matrix of $\mathrm{GL}_n(R)$ of order prime to p its order and the order of its reduction mod $\mathfrak{m}_R$ agree. Let e be the common order. The two matrices define homomorphisms $\mathbb{Z}/(e) \longrightarrow \mathrm{GL}_n(R)$ by $\bar{1} \mapsto \widetilde{A}$ and $\bar{1} \mapsto \widetilde{A}'$, respectively, and the reduction modulo $\mathfrak{m}_R$ of these agree. Because e is prime to p, we have $H^i(\mathbb{Z}/(e), \mathrm{ad}) = 0$, for $i = 1, 2$. An inductive argument, writing R as an inverse limit $\varprojlim_{n\in\mathbb{N}} R_n$ such that for all n the kernel of $R_{n+1} \longrightarrow R_n$ is isomorphic to κ, shows that any two homomorphisms of $\mathbb{Z}/(e)$ to $\mathrm{GL}_n(R)$ whose reductions to κ agree are indeed conjugate. ∎

By Lemma 6.5 we may fix a lift of $\bar{A}'^{\infty}$ to $\mathrm{GL}_n(W(\kappa))$ and assume (after conjugating if necessary), that A'^{∞} agrees with the chosen lift to $W(\kappa)$ under the canonical homomorphism $W(\kappa) \longrightarrow R$.

One possible choice for a lift of $\bar{A}'^{\infty}$ to $W(\kappa)$ can be obtained as follows: Suppose $\bar{A}'^{\infty}$ is given in rational canonical form, so that along the diagonal we have square blocks of companion matrices for suitable polynomials in $\kappa[T]$. (If desired, we may assume that the corresponding polynomials are irreducible.) Over $W(\kappa)$, we can write down a matrix of the same shape where the diagonal blocks are the companion matrices, of those polynomials over $W(\kappa)$ whose roots are the Teichmüller lifts of the corresponding polynomials over κ.

In the above lift to $W(\kappa)$ we may group together those companion matrices arising from the same irreducible polynomial. Thereby R^n decomposes into the direct sum of the isotypical components of the action of A'^{∞}. Since A' and B' commute with A'^{∞}, they preserve this direct sum decomposition. In particular this shows:

Corollary 6.6 *Let R be in $\mathscr{C}$, let A' be in $\mathrm{GL}_n(R)$ and define on $V := R^n$ the structure of an $R[T]$-module by having T act as A'^{∞}. Then V is the direct sum $\oplus_i V_i$ of its isotypical components for the $R[T]$-action. Each V_i is preserved under the action of A'.*

Corollary 6.7 *In the definition of block-regularity of a matrix $A' \in \mathrm{GL}_n(R)$ we may assume that each $W_i \otimes_R \kappa$ is indecomposable.*

Proof: If we apply the previous corollary to the W_i in Definition 6.3, then each W_i can be written as a direct sum $W_i = \oplus_j V_{ij}$ where the V_{ij} are isotypical for the action of A'^{∞} and invariant under the action of A'. Since $W_i \otimes_R \kappa \cong \oplus_j V_{ij} \otimes_R \kappa$, the matrix defining the action of A' on each V_{ij} is regular by Lemmas 6.1 and 6.2 and the hypothesis on the action on $W_i \otimes_R \kappa$. Therefore it remains to prove the following: Suppose that A' is a regular matrix and that $V = R^n$ is isotypical for the action of A'^{∞}, then the characteristic polynomial of the reduction $\bar{A}'$ is a power of an irreducible polynomial in $\kappa[T]$.

By Lemma 6.4(a), the characteristic polynomials of the reductions $\bar{A}'$ and $\bar{A}'^{\infty}$ agree. Therefore by Lemma 6.4(c) it suffices to show that for an A'^{∞}-isotypical component the minimal polynomial of $\bar{A}'^{\infty}$ is irreducible. Write the semisimple matrix $\bar{A}'^{\infty}$, with respect to a suitable basis, in block diagonal form, where each block is a companion matrix of an irreducible polynomial $f_i \in \kappa[T]$. Define $F_i \in W(\kappa)[T]$ as the unique polynomial whose roots are the Teichmüller lifts of those of f_i. By Lemma 6.5, the matrix A'^{∞} is conjugate to the block diagonal matrix, where each block is the companion matrix of F_i. Since we assume that V is isotypical for the action of A'^{∞}, all the F_i must agree, and hence so must the f_i. ∎

We now generalize parts of Lemma 6.2 to the block-regular case.

Lemma 6.8 *Suppose R is in $\mathscr{C}$ and $A' \in \mathrm{GL}_n(R)$ is block-regular. Then $M_n(R)^{A'}$ is a direct summand of $M_n(R)$ of rank n and for any morphism $R \longrightarrow R'$ in $\mathscr{C}$ one has $M_n(R)^{A'} \otimes_R R' \cong M_n(R')^{A'}$ under the canonical isomorphism $M_n(R) \otimes_R R' \cong M_n(R')$.*

Proof: Let V, W_i and m_i be as in Definition 6.3, and suppose using Corollary 6.7 that the $W_i \otimes_R \kappa$ are indecomposable $\kappa[T]$-modules. Also, let A'^∞ be as in Lemma 6.4. Let f_i be the minimal polynomial of $\bar{A}'^\infty$ acting on W_i and let $F_i \in W(\kappa)[T]$ be the lift constructed in the proof of the previous corollary. Then the f_i are irreducible and pairwise relatively prime and therefore the pairwise gcd of the polynomials F_i is defined and equal to 1 if the indices are different. We claim that $\mathrm{Hom}_{R[T]}(W_i, W_{i'}) = 0$ whenever $i \neq i'$ for T the action coming from A'^∞:

So let f be such a homomorphism. For any $w_i \in W_i$ we have $F_{i'}(T)f(w_i) = 0$ since $F_{i'}(T)$ is zero on $W_{i'}$. Similarly we have

$$F_i(T)f(w_i) = f(F_i(T)w_i) = f(0) = 0.$$

Because $\gcd(F_i, F_{i'}) = 1$ we deduce $f(w_i) = 0$ for any w_i and hence $f = 0$, as asserted.

Now by the definition of A'^∞ we have $M_n(R)^{A'} \subset M_n(R)^{A'^\infty}$. We apply the above claim to the isomorphism $M_n(R) \cong \oplus_{i,i'} \mathrm{Hom}_R(W_i, W_{i'})^{m_i m_{i'}}$ and infer that

$$M_n(R)^{A'} \cong \oplus_i \Big(M_{m_i}(\mathrm{Hom}_R(W_i, W_i))\Big)^{A'} \cong \oplus_i M_{m_i}(\mathrm{Hom}_R(W_i, W_i)^{A'}).$$

For the individual i, all assertions now follow from Lemma 6.2. ∎

There is a second issue we need to discuss before entering the deformation theory of rigid representations, namely commutators. If one is over a field, the set of matrices commuting with a given one forms a vector subspace of the set of all endomorphisms of the underlying vector space. If instead one considers commutation up to homothety (which one does for PGL_n), the situation is different. To study this, we introduce the following notation: For $R \in \mathscr{C}$ and $A \in \mathrm{PGL}_n(R)$ choose a representative A' of A in $\mathrm{GL}_n(R)$. For any quotient $\widetilde{R} \cong R/\mathfrak{a}$ for some ideal $\mathfrak{a}$ of R, define:

$$Z_A(\widetilde{R}) := \{\zeta \in \widetilde{R}^* \mid \exists B' \in \mathrm{GL}_n(\widetilde{R}) : B'A'B'^{-1} \equiv \zeta A' \pmod{\mathfrak{a}}\},$$

$$C_A(\widetilde{R}) := \{B' \in \mathrm{GL}_n(\widetilde{R}) \mid \exists \lambda \in \widetilde{R}^* : B'A'B'^{-1} \equiv \lambda A' \pmod{\mathfrak{a}}\}.$$

The definitions are clearly independent of the choice of A' (and so interchangeably we write A or A' for the subscript ? of $Z_?$ or $C_?$.), but they do depend on the choice of the surjection $R \longrightarrow \widetilde{R}$ and not just the abstract ring $\widetilde{R}$. For simpler notation, we nevertheless chose to only write the argument $\widetilde{R}$.

The group $C_A(\widetilde{R})$ is the set of representatives in $\mathrm{GL}_n(\widetilde{R})$ of the commutator of the image of A in $\mathrm{PGL}_n(\widetilde{R})$. As an abbreviation, we define $\mathrm{GL}_n(\widetilde{R})^A := M_n(\widetilde{R})^A \cap \mathrm{GL}_n(\widetilde{R})$. For $\widetilde{R} = \kappa$ the following result describes basic properties of $Z_A(\kappa)$ and $C_A(\kappa)$:

Proposition 6.9 *Let A' be in $\mathrm{GL}_n(\kappa)$ and denote by A its image in $\mathrm{PGL}_n(\kappa)$. Then:*

(a) $Z_A(\kappa)$ is a subgroup of the cyclic group κ^*.

(b) If $f(T)$ is the characteristic polynomial of A', then $f(\zeta T) = f(T)$ for all $\zeta \in Z_A(\kappa)$, and so in particular the order of $Z_A(\kappa)$ divides n.

(c) For any ζ in $Z_A(\kappa)$ there exists $B'_0 \in \mathrm{GL}_n(\kappa)$ of the same order as ζ, such that $B'_0 A' B_0'^{-1} = \zeta A'$.

(d) Let ζ be a generator of $Z_A(\kappa)$ and B'_0 be as in (c), and let ζ^i act on $\mathrm{GL}_n(\kappa)^A$ by conjugation with ${B'_0}^i$. Then $C_A(\kappa)$ is isomorphic to the semidirect product $\mathrm{GL}_n(\kappa)^A \rtimes Z_A(\kappa)$.

(e) The matrix B'_0 in (d) can be chosen in such a way that it is conjugate to the diagonal matrix with diagonal $(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$.

Proof: Part (a) is obvious and (b) follows because f is monic of degree n. We now prove (c). It suffices to do this for ζ a generator of $Z_A(\kappa)$. We may assume that A' is given in generalized Jordan form, cf. [SW], p. 340, so that the individual blocks A'_i, $i = 1, \ldots, s$, are of the form

$$\begin{pmatrix} C'_i & & & \\ E'_i & C'_i & & \\ & \ddots & \ddots & \\ & & E'_i & C'_i \end{pmatrix},$$

where C'_i is the companion matrix of an irreducible polynomial $f_i \in \kappa[T]$ and where E'_i is the matrix with entry 1 in the upper right corner and zero elsewhere. That A' and $\zeta A'$ are conjugate means that we may group the blocks in such a way that the following holds: There exist $s_0 = 0 < s_1 < s_2 < \ldots < s_k = s$ such that for $j = 0, \ldots, k-1$ and with $r_j := s_{j+1} - s_j$ the matrix A'_{s_j+i} is conjugate to $\zeta^i A'_{s_{j+1}}$ for $i = 1, \ldots, r_j$, and no two of the matrices A'_{s_j+i} for $i = 1, \ldots, r_j$ are conjugate. Thus for each j the matrix D'_j formed by the blocks A'_{s_j+i}, $i = 1, \ldots, r_j$, is regular and conjugate to $\zeta D'_j$. It suffices therefore to prove (c) under the further hypothesis that A' is regular.

In this situation, by Lemma 6.1(c) we may assume that A' is the companion matrix of its characteristic polynomial. Using (b) for the characteristic polynomial of A', we find $B'_0 A' = \zeta A' B'_0$ for B'_0 the diagonal matrix with diagonal $(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$. This completes the proof of (c) and proves (e) for regular A'.

To see (d), observe that if we identify κ^* with the set of scalar matrices in $GL_n(\kappa)$, then the map $C_A(\kappa) \longrightarrow Z_A(\kappa)$, sending B' to $B'A'{B'}^{-1}{A'}^{-1}$, is well-defined and a surjective group homomorphism with kernel $\mathrm{GL}_n(\kappa)^A$. By (c), $\zeta \mapsto B'_0$ defines a splitting.

Finally, the proof of (e) for general A' is as follows: By the reduction step above for the proof of (c), the matrix A' may be written in block diagonal form where all the blocks are regular matrices and such that each block is conjugate to its product with ζ. Writing A' in this way, the proof of (e) in the general case is immediate from the proof for regular A'. ∎

To ease notation, we make the following convention: Let $\zeta \in W(\kappa)$ denote the Teichmüller lift of some element of κ^*. Any $R \in \mathscr{C}$ is canonically a $W(\kappa)$-algebra. Therefore we write ζ also for its image in R under this canonical homomorphism. (Under this convention ζ is the Teichmüller of the same-named element of κ^*.)

Lemma 6.10 *Let $\varphi\colon R \longrightarrow \widetilde{R}$ be a surjection in $\mathscr{C}$, let A' be block-regular in $\mathrm{GL}_n(R)$ and let $\widetilde{A}' := \varphi(A')$ be its image in $\mathrm{GL}_n(\widetilde{R})$. Let $\zeta \in W(\kappa)$ be the Teichmüller lift of some element of κ^* and suppose that A' and $\zeta A'$ are conjugate in $\mathrm{GL}_n(R)$ and that there is some $\widetilde{B}'_0 \in \mathrm{GL}_n(\widetilde{R})$ of finite order equal to the order of ζ such that $\widetilde{B}'_0 \widetilde{A}' {\widetilde{B}'_0}{}^{-1} = \zeta \widetilde{A}'$. Then there exists $B'_0 \in \mathrm{GL}_n(R)$ of finite order equal to the order of ζ such that $\varphi(B'_0) = \widetilde{B}'_0$ and $B'_0 A' {B'_0}^{-1} = \zeta A'$.*

Proof: Let $B' \in \mathrm{GL}_n(R)$ be such that $B'A'{B'}^{-1} = \zeta A'$ and set $\widetilde{B}' := \varphi(B')$. Since $\widetilde{B}'\widetilde{A}'\widetilde{B}'^{-1} = \widetilde{B}'_0 \widetilde{A}' {\widetilde{B}'_0}{}^{-1} = \zeta \widetilde{A}'$, the matrix $\widetilde{C}' := \widetilde{B}'^{-1}\widetilde{B}'_0$ lies in $M_n(\widetilde{R})^{\widetilde{A}'}$. Therefore by

Lemma 6.8, there exists $C' \in M_n(R)^{A'}$ which reduces to $\widetilde{C}'$. By replacing B' by $B'C'$ we may from now on assume that $\widetilde{B}' = \widetilde{B}'_0$.

Since $\widetilde{B}'_0 = \widetilde{B}'^q_0$ and $\widetilde{B}' = \widetilde{B}'_0$, by Lemma 6.4 (b) and (d), the limit $B'_0 = \lim_i B'^{q^i}$ exists and is a matrix of the same order as $\widetilde{B}'_0$. By continuity, we deduce from $B'^{q^i} A' B'^{-q^i} = \zeta^{q^i} A' = \zeta A'$ also the remaining assertion $B'_0 A' {B'_0}^{-1} = \zeta A'$. ∎

Remark 6.11 Let A' be in $\mathrm{GL}_n(R)$ and suppose that ζ is a generator of the subgroup $Z_A(\kappa) \subset \kappa^*$, cf. Proposition 6.9(a). In Proposition 6.9(e) we have seen that with respect to a suitable basis of κ^n the diagonal matrix $\bar{B}'_0 \in \mathrm{GL}_n(\kappa)$ with diagonal $(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$ satisfies $\bar{B}'_0 \bar{A}' {\bar{B}'_0}^{-1} = \zeta \bar{A}'$ for $\bar{A}'$ the reduction of A' to κ. If ζ also lies in $Z_A(R)$ (with the convention on Teichmüller lifts made above), then by Lemma 6.10 there exists $B'_0 \in \mathrm{GL}_n(R)$ reducing to $\bar{B}'_0$ and of the same order as the reduction such that $B'_0 A' {B'_0}^{-1} = \zeta A'$. Applying Lemma 6.5 we find a basis of R^n (reducing to the given one on κ^n) with respect to which $B'_0 \in \mathrm{GL}_n(R)$ is again the diagonal matrix with diagonal $(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$.

Lemma 6.12 *Let R be in $\mathscr{C}$ and A' in $\mathrm{GL}_n(R)$ be block-regular. Suppose in the Jordan decomposition of $\bar{A}' := A' \pmod{\mathfrak{m}_R}$ at least one block is of size not divisible by p. Then*

(a) $Z_A(R) \cap (1 + \mathfrak{m}_R) = \{1\}$.

(b) Let ζ denote the Teichmüller lift of a generator of $Z_A(\kappa)$, which by Proposition 6.9(a) is a cyclic subgroup of κ^*. If ζ lies in $Z_A(R)$, then for any surjection $R \longrightarrow \widetilde{R}$ in $\mathscr{C}$, the map $C_A(R) \longrightarrow C_A(\widetilde{R})$ is surjective (and a group homomorphism).

Proof: For (a) we argue by contradiction and assume that the stated assertion is wrong. Then it is wrong for $R/\mathfrak{m}_R^i$ for some $i \geq 2$. Hence there is a counterexample for some $R \in \mathscr{C}$ of minimal length, and we may assume the following situation: There is a surjective ring homomorphism $\pi \colon R \longrightarrow \widetilde{R}$ in $\mathscr{C}$ with kernel $\mathfrak{a} = Rx$ for some $x \in R$ such that $\mathfrak{m}_R x = 0$, and moreover $Z_A(R) \cap (1 + \mathfrak{m}_R) \supsetneq \{1\}$ and $Z_A(\widetilde{R}) \cap (1 + \mathfrak{m}_{\widetilde{R}}) = \{1\}$.

Let $B' \in \mathrm{GL}_n(R)$ be such that $B'A'{B'}^{-1} = \lambda A'$ for some $\lambda \in 1 + \mathfrak{m}_R$ with $\lambda \neq 1$. Then $\lambda = 1 + ax$ for some $a \in R - \mathfrak{m}_R$, and $\pi(B')$ and $\pi(A')$ commute. By Lemma 6.8 we may therefore find a matrix $\widetilde{B}' \in \mathrm{GL}_n(R)$ which commutes with A' and such that $B' \equiv \widetilde{B}' \pmod{\mathfrak{a}}$. Set $C' := B'\widetilde{B}'^{-1}$. Then $C' = 1 + x\Delta$ for some $\Delta \in M_n(R)$ and $C'A'{C'}^{-1} = \lambda A'$. The latter identity is equivalent to

$$x(\Delta A' - A'\Delta) = xaA'.$$

Let $\bar{\Delta} := \Delta \pmod{\mathfrak{m}_R}$ and $\bar{a} := a \pmod{\mathfrak{m}_R}$, so that $\bar{a} \neq 0$. Dividing the previous identity by x and reducing modulo $\mathfrak{m}_{\widetilde{R}}$ yields

$$\bar{\Delta}\bar{A}' - \bar{A}'\bar{\Delta} = \bar{a}\bar{A}'. \tag{4}$$

Equation (4) may be viewed as a linear equation over κ in $\bar{a}$ and the coefficients of $\bar{\Delta}$ as unknowns. We claim $\bar{a} = 0$ for any solution over κ^{alg}. This will contradict our hypothesis, and complete the proof.

To prove the claim, we may assume that $\bar{A}'$ is given in Jordan canonical form. It is easy to see that if there is a solution with $\bar{a}$ non-trivial, then for each of the Jordan blocks of $\bar{A}'$ there is a correspondingly sized matrix $\bar{\Delta}'$ such that (4) holds. Let $\bar{J}$ be a Jordan block of size not divisible by p. In this situation, we take the trace of (4) (for $\bar{J}$ and $\bar{\Delta}'$ replacing $\bar{A}'$ and $\bar{\Delta}$). The trace of the commutator on the left hand side is zero. The trace of $\bar{J}$ is non-zero, since $\bar{J}$ is invertible and of size not divisible by p. This shows

$$0 = \bar{a}\,\mathrm{Tr}(\bar{J})$$

with $\mathrm{Tr}(\bar{J}) \neq 0$. It follows that $\bar{a}$ is zero, as asserted.

We now give the proof of (b). Let the underlying basis of R^n be chosen according to Remark 6.11 so that for $B'_0 \in \mathrm{GL}_n(W(\kappa))$ the diagonal matrix with diagonal $(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$ we have $B'_0 A' {B'_0}^{-1} = \zeta A'$. Identifying $\widetilde{R}^*$ with the scalar matrices in $\mathrm{GL}_n(\widetilde{R})$, we first claim that for any $\widetilde{R}$ as in (b) we have a functorial short exact sequence

$$0 \longrightarrow \mathrm{GL}_n(\widetilde{R})^A \longrightarrow C_A(\widetilde{R}) \overset{B' \mapsto B'A'B'^{-1}A'^{-1}}{\longrightarrow} Z_A(\widetilde{R}) = \langle \zeta \rangle \longrightarrow 0,$$

which is split by sending ζ^i to ${B'_0}^i$: The map on the right is well-defined by the definitions of $C_A(\widetilde{R})$ and $Z_A(\widetilde{R})$ (and the identification made above). By the definition of $C_A(\widetilde{R})$, for $B' \in C_A(\widetilde{R})$ the matrix $B'A'B'^{-1}$ is a scalar matrix in $\mathrm{GL}_n(\widetilde{R})$, and from this one deduces that the map on the right is a homomorphism of groups. Its kernel is obviously $\mathrm{GL}_n(\widetilde{R})^A$. Its image is $Z_A(\widetilde{R})$ – by the definition of the latter. In particular $Z_A(\widetilde{R})$ is a subgroup of $\widetilde{R}^*$. By (a) and since ζ is assumed to lie in $Z_A(R)$ we have $Z_A(\widetilde{R}) = \langle \zeta \rangle$.

To complete the proof, we compare the above sequence for a surjective homomorphism $R \longrightarrow \widetilde{R}$. Since on the right hand side we have an isomorphism, it suffices to prove that the functorial homomorphism $\mathrm{GL}_n(R)^{A'} \longrightarrow \mathrm{GL}_n(\widetilde{R})^{A'}$ is surjective. Observe that $\mathrm{GL}_n(R)^A$ consists of those elements of $M_n(R)^A$ whose reduction mod $\mathfrak{m}_R$ lie in $\mathrm{GL}_n(\kappa)$. Therefore the proof is completed by applying Lemma 6.8 which asserts that (by block-regularity of A') the functorial map $M_n(R)^{A'} \longrightarrow M_n(\widetilde{R})^{A'}$ is surjective. ∎

We now come to the definition of *rigid deformation*.

Definition 6.13 *A residual representation $\bar{\rho}$ is called* admissible *if*

(a) the $\kappa[H]$-representation $\overline{\mathrm{ad}}$ is irreducible, and

(b) for any $x \in \mathrm{Ram}(\bar{\rho})$ the element $\bar{\rho}(g_x) \in \mathrm{PGL}_n(\kappa)$ is block-regular.

Remark 6.14 By Remark 2.5, condition (a) implies that p does not divide n, so that the Jordan decomposition of any matrix in $\mathrm{GL}_n(\kappa)$ has a block of size not divisible by p. Hence Lemma 6.12 is applicable to linear lifts of the $\rho(g_x)$, $x \in \mathrm{Ram}(\bar{\rho})$.

For any admissible $\bar{\rho}$ and any $\mathscr{D}$ we define the subfunctor $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}} \subset \mathrm{Def}_{\mathscr{D}}$ of *rigid deformations of $\bar{\rho}$ of type $\mathscr{D}$* as

$$\begin{aligned} \mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}(R) \quad := \quad & \{[\rho] \in \mathrm{Def}_{\mathscr{D}}(R) \mid \forall x \in \mathrm{Supp}\,\mathscr{D} : \rho(g_x) \text{ is block-regular} \\ & \text{and } Z_{\rho(g_x)}(R) \longrightarrow Z_{\bar{\rho}(g_x)}(\kappa) \text{ is an isomorphism}\}. \end{aligned}$$

Elements of $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}$ are called rigid deformations. As before, if $\mathscr{D}$ is the datum $(S, (\infty)_{x \in S})$, we simply write $\mathrm{Def}^{\mathrm{rig}}_S$ for $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}$.

Remark 6.15 (a) Let ζ_x be a generator of $Z_{\bar{\rho}(g_x)}(\kappa)$ and let $B_x \in \mathrm{PGL}_n(W(\kappa))$ denote the diagonal matrix with diagonal $(1, \zeta_x, \zeta_x^2, \ldots, \zeta_x^{n-1})$. By Remark 6.11 and Lemma 6.12 the second condition for rigid deformations can be phrased as follows: There exists a basis of R^n, depending on x, such that inside $\mathrm{PGL}_n(R)$ the elements B_0 and $\rho(g_x)$ commute. This in turn is equivalent to the assertion that the kernel of $\mathrm{GL}_n(R)^{\rho(g_x)} \longrightarrow \mathrm{PGL}_n(R)^{\rho(g_x)}$ is independent of $R \in \mathscr{C}$.

(b) If x is not in $\mathrm{Ram}(\bar{\rho})$, then any representative of $\bar{\rho}(g_x)$ in $\mathrm{GL}_n(\kappa)$ is a scalar matrix and thus is block-regular. But then any block-regular lift is represented by a scalar matrix in $\mathrm{GL}_n(R)$, and hence is the identity in $\mathrm{PGL}_n(R)$. We deduce $\mathrm{Ram}(\rho) = \mathrm{Ram}(\bar{\rho})$ for rigid deformations $[\rho]$, and so we will always assume $\mathrm{Supp}\,\mathscr{D} \subset \mathrm{Ram}(\bar{\rho})$ in $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}$.

(c) In a previous version of this article, we had no explicit definition of rigid deformations. Implicitly, when combining rigidity and deformations, we always made the assumption that $\operatorname{Supp}\mathscr{D}$ was contained in the set of those places x for which $\bar{\rho}(g_x)$ was regular. Then by Lemma 6.2 any deformation is automatically (block-)regular. The motivation for the present approach was to be able to deform so-called Thompson tuples. Previously we could only deform Belyi tuples. The importance of being able to do so and some first steps for such a more general approach were suggested by M. Dettweiler.

(d) If rigidity for a deformation should be deducible from the residual representation, then the deformation should satisfy similar constraints as the given residual representation. In the following we try to explain why the conditions in the definition of $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}$ seem natural to us:

At various crucial points we will need the surjectivity of $C_A(R) \longrightarrow C_A(R')$ for surjections $R \longrightarrow R'$ in $\mathscr{C}$ as proved in Lemma 6.12 and lifts A of $\bar{\rho}(g_x)$ at places $x \in \operatorname{Supp}\mathscr{D}$. This certainly requires that $Z_A(R) \cap (1 + \mathfrak{m}_R) = \{1\}$, and so we need part (a) of the definition of admissibility for $\bar{\rho}$ (cf. Remark 6.14) as well as the condition that $Z_A(R) \longrightarrow Z_{\bar{\rho}(g_x)}(\kappa)$ be bijective. The other ingredient for this surjectivity is that $M_n(R)^A \longrightarrow M_n(R')^A$ be surjective. For R, R' of finite length this basically amounts to the condition that $M_n(R)^A$ is a free R-module of rank independent of R. Iso-regularity achieves this, and it provides one with good deformation conditions in the most important cases, where either $\bar{\rho}(g_x)$ is regular, or where it is semisimple. Moreover, as we shall see later, cf. Lemma 7.2, locally rigid deformations are unobstructed.

Theorem 6.16 $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}$ *is representable.*

We write $(R^{\mathrm{rig}}_{\mathscr{D}}, \rho^{\mathrm{rig}}_{\mathscr{D}})$ for a pair $R^{\mathrm{rig}}_{\mathscr{D}} \in \mathscr{C}$ and $\rho^{\mathrm{rig}}_{\mathscr{D}} : G_{\mathscr{D}} \longrightarrow \mathrm{GL}_n(R^{\mathrm{rig}}_{\mathscr{D}})$ such that $[\rho^{\mathrm{rig}}_{\mathscr{D}}]$ represents the universal object in $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}(R_{\mathscr{D}})$.

Proof: It suffices to show relative representability of [Ma2], § 19, for the restriction of $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}$ to the inertia groups at places $x \in \mathrm{Ram}(\bar{\rho})$. Since this restriction is completely determined by the image of a fixed topological generator g_x of I_x it is completely describable by lifts of the matrix $\bar{A} := \bar{\rho}(g_x)$. Define $\mathrm{Def}^{\mathrm{rig}}_x(R)$ as the set of strict equivalence classes of those $A \in \mathrm{PGL}_n(R)$ which lift $\bar{A}$, are block-regular and for which $Z_A(R) \longrightarrow Z_A(\kappa)$ is bijective. This is the local deformation problem when the ramification datum at x satisfies $n_x = \infty$. If this is relatively representable, then so will be all the quotients for n_x finite. We need to show that for all diagrams

$$R_1 \xrightarrow{\varphi_1} R_0 \xleftarrow{\varphi_2} R_2$$

of Artin rings in $\mathscr{C}$ such that φ_1 is surjective and for R the ring $\{(r_1, r_2) \in R_1 \times R_2 \mid \varphi_1(r_1) = \varphi_2(r_2)\}$ the homomorphism

$$\mathrm{Def}^{\mathrm{rig}}_x(R) \longrightarrow \mathrm{Def}^{\mathrm{rig}}_x(R_1) \times_{\mathrm{Def}^{\mathrm{rig}}_x(R_0)} \mathrm{Def}^{\mathrm{rig}}_x(R_2)$$

is bijective. Injectivity is clear, and so let A_i be elements in $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}}(R_i)$, $i = 0, 1, 2$ such that $\widetilde{A}_0 := \varphi_1(A_1)$, $\varphi_2(A_2)$ and A_0 are conjugate. In fact we may and will assume from now on that $A_0 = \varphi_2(A_2)$. Let us also fix representatives $A'_i \in \mathrm{GL}_n(R_i)$ of the A_i with the same property. It will suffice to construct $A' \in \mathrm{GL}_n(R)$ mapping to A'_1 and to A'_2 up to strict equivalence.

We first show that for any $A' \in \mathrm{GL}_n(R)$ mapping to $A'_i \in \mathrm{Def}^{\mathrm{rig}}_x(R_i)$, $i = 1, 2$, the homomorphism $Z_{A'}(R) \longrightarrow Z_{\bar{\rho}(g_x)}(\kappa)$ is an isomorphism: Let $\zeta \in \kappa^*$ be a generator of $Z_{\bar{\rho}(g_x)}(\kappa)$ and denote by ζ also its Teichmüller lift to $W(\kappa)^*$. By Lemma 6.10 there exists

$B'_2 \in \mathrm{GL}_n(R_2)$ of the same order as ζ, such that $B'_2 A'_2 {B'_2}^{-1} = \zeta A'_2$. Let B'_0 be the reduction of B'_2 to R_0. Again by Lemma 6.10 there exists $B'_1 \in \mathrm{GL}_n(R_1)$ of the same order as ζ and reducing to B'_0, such that $B'_1 A'_1 {B'_1}^{-1} = \zeta A'_1$. Let $B' \in \mathrm{GL}_n(R)$ be the matrix obtained by gluing B'_1 and B'_2 along B'_0. Clearly $B' A' {B'}^{-1} = \zeta A'$, since this holds after reducing to either R_1 or R_2, and, for the same reason, the order of B' must agree with the order of ζ, as was to be shown.

It remains to show that there exists an block-regular matrix $A' \in \mathrm{GL}_n(R)$ mapping up to strict equivalence to both A'_i, $i = 1, 2$. By decomposing the A'_i into isotypical components according to the lifting of the action of the semisimplification of $\bar{A}' := A'_0 \pmod{\mathfrak{m}_R}$, cf. Lemma 6.4, we may assume that $\bar{A}'$ is a direct sum of identical indecomposable representations. Since the A'_i are block-regular lifts, we may (after conjugation) assume that they are given in block diagonal form where the matrices along the diagonal are identical square matrices, say all equal to C'_i, such that their reductions to κ agree and are regular. By Lemma 6.2(b), we may assume that the C'_i are companion matrices. Since two companion matrices are conjugate if and only if they are identical, the reductions of C'_1 and C'_2 to R_0 agree with C'_0. Hence the A'_i given in this form glue to an block-regular $A' \in \mathrm{GL}_n(R)$, as had to be shown. ∎

Our next aim iths to prove the pro-rigidity of the representations $\rho^{\mathrm{rig}}_{\mathscr{D}}$, more precisely, we want to show the following result:

Theorem 6.17 *Suppose $K = k(t)$, l is prime to the order of H and $\Sigma = \mathrm{Ram}(\bar{\rho}) = \{x_1, \ldots, x_s\}$. For each $i = 1, \ldots, s$, let g_i be a topological generator of an inertia subgroup I_{x_i} of $G^{(l)}_{\Sigma}$ such that $\prod g_i = 1$ in $G^{(l)}_{\Sigma}$. We assume that*

- *(a) the elements $g_1, \ldots, g_s$ are geometrically rigid for $\bar{\rho}$,*
- *(b) $\bar{\rho}$ is admissible in the sense of Definition 6.13.*

Then the elements $g_1, \ldots, g_s$ are strictly pro-rigid for $\rho^{\mathrm{rig}}_{\mathscr{D}}$.

If moreover the conditions of Corollary 2.6 hold, then $\rho^{\mathrm{rig}}_{\mathscr{D}}$ has maximal image.

If in addition to all the above, the $\bar{\rho}(g_i)$ are also strictly rigid for $\mathrm{Im}(\bar{\rho})$, then the $\rho^{\mathrm{rig}}_{\mathscr{D}}(g_i)$ are strictly rigid for the group $\mathrm{Im}(\rho^{\mathrm{rig}}_{\mathscr{D}})$ and its subgroup $\mathrm{Ker}(\mathrm{Im}(\rho^{\mathrm{rig}}_{\mathscr{D}}) \longrightarrow \mathrm{Im}(\bar{\rho}))$.

Proof of Theorem 2.20: The above theorem combined with the following lemma, immediately yields Theorem 2.20. ∎

Lemma 6.18 *Suppose that*

- *(a) As a $\kappa[H]$-module $\overline{\mathrm{ad}}$ is irreducible.*
- *(b) $g_1, \ldots, g_s \in G^{(\ell)}_{\Sigma}$ are geometrically rigid for $\bar{\rho}$.*
- *(c) Each $\bar{\rho}(g_i)$ is of order prime to p or regular.*
- *(d) For each regular $\bar{\rho}(g_i) \in \mathrm{PGL}_n(\kappa)$ and representative $A'_i \in \mathrm{GL}_n(\kappa)$ the matrices $\lambda A'_i$, $\lambda \in \kappa^*$, are pairwise non-conjugate.*
- *(e) $\mathscr{D}$ is a ramification datum such that $\mathrm{Supp}\,\mathscr{D} \subset \Sigma_{\mathrm{reg}}$.*

Then $\bar{\rho}$ is admissible and $\mathrm{Def}^{\mathrm{rig}}_{\mathscr{D}} = \mathrm{Def}_{\mathscr{D}}$.

Proof: By conditions (a) and (c) the representation $\bar{\rho}$ is admissible. By condition (d) we have $Z_{\bar{\rho}(g_i)}(\kappa) = \{1\}$ for all i, and from Lemma 6.12, which needs (a) in the form $p \not| n$ and (c), it follows that $Z_{\rho(g_i)}(R) \longrightarrow Z_{\bar{\rho}(g_i)}(\kappa)$ is an isomorphism for any R in $\mathscr{C}$. Finally (c) and (e) show that any deformation is regular at all places of $\mathrm{Supp}\,\mathscr{D}$. ∎

For the proof of Theorem 6.17, we first need to establish some consequences of geometric rigidity. Let $\rho\colon G \longrightarrow \mathrm{PGL}_n(\kappa)$ be a representation and assume that $\underline{g} := \{g_1, \ldots, g_s\}$ is geometrically rigid for ρ. We define the scheme $V_{\rho,\underline{g}}$ as the locally closed subvariety of $(\mathbb{P}^{n^2-1})^s$ defined by

$$V_{\rho,\underline{g}}(R) := \Big\{(A_1, \ldots, A_s) \in \mathrm{PGL}_n(R)^s : \rho(g_1)^{A_1} \cdot \ldots \cdot \rho(g_s)^{A_s} = 1\Big\}$$

for any κ-algebra R. We also define the scheme C_i as the locally closed subscheme in $\mathbb{P}^{n^2-1}$ defined by

$$C_i(R) := \Big\{A \in \mathrm{PGL}_n(R) : A\rho(g_i) = \rho(g_i)A\Big\}.$$

Our first goal is to show the following proposition:

Proposition 6.19 *Assume that $\underline{g}$ is geometrically rigid for ρ and $\overline{\mathrm{ad}}_\rho$ is irreducible. Then the morphism*

$$\varphi\colon \mathrm{PGL}_n \times \prod_i C_i \longrightarrow V_{\rho,\underline{g}} : (B, B_1, \ldots, B_s) \mapsto (BB_1, \ldots, BB_s)$$

is an isomorphism of algebraic varieties. In particular $V_{\rho,\underline{g}}$ is smooth.

Proof: Geometric rigidity means precisely that on closed points the morphism φ is an isomorphism. The variety PGL_n is an open subvariety of $\mathbb{P}^{n^2-1}$ and hence smooth. Furthermore the C_i are smooth, since they are the intersection of a linear subspace of $\mathbb{P}^{n^2-1}$ with the open subvariety PGL_n. Via φ the scheme $V_{\rho,\underline{g}}$ is therefore a homogeneous space for the smooth group scheme $\mathrm{PGL}_n \times \prod_i C_i$. Since it is principal homogeneous on closed points, φ is an isomorphism if and only if $V_{\rho,\underline{g}}$ is smooth at some closed point.

We consider the point $\mathbb{1} := (1, 1, \ldots, 1)$. The dimension of $V_{\rho,\underline{g}}$ is $s(n^2-1)$ minus the number of algebraically independent equations of the matrix entries in

$$\rho(g_1)^{A_1} \cdot \ldots \cdot \rho(g_s)^{A_s} = 1,$$

which is at most n^2-1, i.e., the dimension of $\overline{\mathrm{ad}}$. By the following lemma, the dimension of the tangent space at $\mathbb{1}$ is $(s-1)(n^2-1)$. This shows that the Krull dimension of the localization of $V_{\rho,\underline{g}}$ at $\mathbb{1}$ is $(s-1)(n^2-1)$ and that this local ring is smooth. ∎

Lemma 6.20 *The dimension of the tangent space of $V_{\rho,\underline{g}}$ at $\mathbb{1}$ is $(s-1)(n^2-1)$.*

Proof: We define matrices $\widetilde{A}_1 := A_s^{-1}A_1$, $\widetilde{A}_2 := A_1^{-1}A_2$, $\ldots$, $\widetilde{A}_s := A_{s-1}^{-1}A_s$ and $\widetilde{A} := A_1$. Then $V_{\rho,\underline{g}}$ is isomorphic to the scheme V' defined by mapping each κ-algebra R to

$$\Big\{(\widetilde{A}, \widetilde{A}_1, \ldots, \widetilde{A}_s) \in \mathrm{PGL}_n(R)^{s+1} : \widetilde{A}_1\rho(g_1)\widetilde{A}_2\rho(g_2)\ldots\widetilde{A}_s\rho(g_s) = 1, \widetilde{A}_1\ldots\widetilde{A}_s = 1\Big\}.$$

Setting $\widetilde{g}_0 = 1$ and $\widetilde{g}_i := g_1 \ldots g_i$ for $i = 1, \ldots, s-1$, implicit differentiation yields the following expression for the tangent space at $\mathbb{1}$:

$$\Big\{(\delta, \delta_1, \ldots, \delta_s) \in \overline{\mathrm{ad}}^{s+1} : \sum_{i=1}^s \delta_i^{\widetilde{g}_{i-1}} = \sum_{i=1}^s \delta_i = 0\Big\}.$$

Note that the $\widetilde{g}_i$ are also topological generators of G. Eliminating δ_1 and using the adjoint action, we rewrite the defining equation of the tangent space as $\sum_{i=1}^{s-1}(\widetilde{g}_i - 1)\delta_{i+1} = 0$. We claim that the map

$$\lambda\colon \overline{\mathrm{ad}}^s \longrightarrow \overline{\mathrm{ad}} : (\delta, \delta_2, \ldots, \delta_s) \mapsto \sum_{i=1}^{s-1}(\widetilde{g}_i - 1)\delta_{i+1}$$

is surjective. If this is shown, then the kernel will have dimension $(s-1)(n^2-1)$, which completes the proof of the lemma.

To prove the claim, observe that for arbitrary $g, h \in G$ and $x \in \overline{\mathrm{ad}}$ one has $(gh-1)x = (g-1)(hx) + (h-1)x$ as well as $h(g-1)x = (hg-1)x - (h-1)x$. Define $W := \sum_{g\in G}(g-1)\,\overline{\mathrm{ad}}$. An inductive argument based on the first formula shows that for any set of generators g'_j of $\rho(G)$ one has $W = \sum_j (g'_j - 1)\,\overline{\mathrm{ad}}$. In particular this shows that the image of λ is W. The second formula shows that W is a G-submodule of $\overline{\mathrm{ad}}$. By the hypotheses of Proposition 6.19, $\overline{\mathrm{ad}}$ is irreducible, and so it remains to show that W is non-zero. However, for any non-identity element $\rho(g)$ the set $(\rho(g)-1)\overline{\mathrm{ad}}$ contains a non-zero element, and so we have proved the claim. ∎

For $g \in G$ we set $\overline{\mathrm{ad}}^g := \{v \in \overline{\mathrm{ad}} : (g-1)v = 0\}$. The following corollary is needed in the proof of Theorem 6.17.

Corollary 6.21 *If $\bar\rho$ is irreducible and admits a geometrically rigid tuple, the sequence*

$$0 \longrightarrow \bigoplus_{i=1}^{s} \overline{\mathrm{ad}}^{g_i} \xrightarrow{(\varepsilon_1,\ldots,\varepsilon_s)\mapsto(\varepsilon_i-\varepsilon_{i-1})_{i=1}^s} (\overline{\mathrm{ad}}^s)^0 \xrightarrow{(\eta_i)_{i=1}^s\mapsto\sum_i \eta_i^{\widetilde{g}_{i-1}}} \overline{\mathrm{ad}} \longrightarrow 0$$

is short exact, where $(\overline{\mathrm{ad}}^s)^0$ denotes the sub vector space of tuples in $\overline{\mathrm{ad}}^s$ which sum to zero.

PROOF: We first prove the exactness of the displayed sequence: The surjectivity of λ in the previous proof is equivalent to the surjectivity of the right hand arrow. For the injectivity of the left hand arrow, suppose that $(\varepsilon_1, \ldots, \varepsilon_s)$ maps to zero. Then we have $\varepsilon_1 = \ldots = \varepsilon_s$. In particular this element is invariant under all g_i and hence under G. It follows that the element lies in $\overline{\mathrm{ad}}^G$ which is zero. To see that the composite of the two arrows is zero, note that $\varepsilon_i = \varepsilon_i^{g_i}$, so that $\varepsilon_i^{\widetilde{g}_{i-1}} = \varepsilon_i^{\widetilde{g}_i}$. Using this, when computing the composite, one sees that it leads to a sum telescoping to zero. It remains to prove exactness in the middle. For this we may simply count dimensions. The dimensions of the terms on the left and right sum to the dimension of the tangent space of $\mathrm{PGL}_n \times \prod C_i$. This we have shown to be $(s-1)(n^2-1)$ which is the dimension of the middle term. ∎

The exactness in the previous corollary, or its proof yield:

Corollary 6.22 *If $(g_1, \ldots, g_s)$ are geometrically rigid for ρ, then $\sum_{i=1}^{s} \dim \overline{\mathrm{ad}}^{g_i} = (s-2)(n^2-1)$.*

The above can be used to bound the size of $\Sigma_{\mathrm{reg}} = \{x \in \Sigma : \bar\rho(g_x) \text{ is regular}\}$:

Corollary 6.23 *One has $|\Sigma_{\mathrm{reg}}| \leq 2$ except in the case $n = 2$ where $|\Sigma_{\mathrm{reg}}| = |\Sigma| = 3$.*

Since (except for $n = 2$) the number of block-regular places, can be significantly larger than 2, the ring R_S^{rig} may capture much more information than the ring $R_{\Sigma^{\mathrm{reg}}} = R_{\Sigma^{\mathrm{reg}}}^{\mathrm{rig}}$ (cf. Lemma 6.18) considered in a previous version of this work.

Proof: By Corollary 6.22, we have

$$(|\Sigma|-2)(n^2-1)=\sum_{x\in\Sigma}\dim\overline{\mathrm{ad}}^{H_x}\leq|\Sigma_{\mathrm{reg}}|(n-1)+(|\Sigma|-|\Sigma_{\mathrm{reg}}|)(n^2-1).$$

It follows that $(|\Sigma_{\mathrm{reg}}|-2)(n+1)\leq|\Sigma_{\mathrm{reg}}|$, or equivalently $|\Sigma_{\mathrm{reg}}|\leq 2+2/n$. The assertion for $n>2$ follows.

If $n=2$, then one must have $\Sigma=\Sigma_{\mathrm{reg}}$, since any non-trivial element of $\mathrm{PGL}_2(\kappa)$ is regular. Then the above equality specializes to $(|\Sigma|-2)3=|\Sigma|\cdot 1$, i.e. $|\Sigma|=3$. ∎

Proof of Theorem 6.17: Let us fix an admissible $\bar{\rho}$. Only then is a universal rigid deformation defined. We deduce that for any $x\in\mathrm{Ram}(\bar{\rho})$ the matrix $\rho^{\mathrm{rig}}_{\mathscr{D}}(g_x)$ is block-regular, and hence so are all its images $A_{x,R}$ under any homomorphism $R^{\mathrm{rig}}_{\mathscr{D}}\longrightarrow R$ in $\mathscr{C}$. Moreover, by Remark 6.14 we may apply Lemma 6.12 to the $A_{x,R}$.

By an inverse limit argument, it will suffice to prove the first assertion of the theorem – in other words, the strict pro-rigidity of $g_1,\ldots,g_s$ for $\rho^{\mathrm{rig}}_{\mathscr{D}}$ – for any finite quotient $R\in\mathscr{C}$ of $R^{\mathrm{rig}}_{\mathscr{D}}$ of finite length, and for this, we will induct on the length μ of R. For $\mu=1$, the result follows from strict rigidity of the g_i for $\bar{\rho}$.

We assume the theorem to be proven for all finite quotients $\widetilde{R}\in\mathscr{C}$ of $R^{\mathrm{rig}}_{\mathscr{D}}$ of length μ. Let $R\in\mathscr{C}$ be a quotient of $R^{\mathrm{rig}}_{\mathscr{D}}$ of length $\mu+1$. Let $x\in\mathfrak{m}_R$ be an non-zero element such that $\mathfrak{m}_R x=0$, and set $\widetilde{R}:=R/(x)$. We write ρ for $\rho^{\mathrm{rig}}_{\mathscr{D}}\otimes_{R^{\mathrm{rig}}_{\mathscr{D}}}R$ and $\widetilde{\rho}$ for $\rho\otimes_R\widetilde{R}$. Condition (a) in Definition 2.11 for ρ is clear from geometric rigidity of $\bar{\rho}$.

For the uniqueness assertion in Definition 2.11 (b'), we need to prove the triviality of $\mathrm{Cent}_{\mathrm{PGL}_n(R)}(\mathrm{Im}(\rho))$. So let A be in this centralizer. By the induction hypothesis, A is representable in the form $1+xD$ for some $D\in M_n(R)$. The element D being centralized by $\mathrm{Im}(\rho)$ means that its reduction modulo $\mathfrak{m}_R$ lies in $\mathrm{ad}^{\mathrm{Im}(\bar{\rho})}$ which consists of scalar matrices only. Hence A is represented by a scalar matrix and thus the identity in $\mathrm{PGL}_n(R)$.

To prove the existence assertion in (b'), suppose that we are given $A_1,\ldots,A_s\in\mathrm{PGL}_n(R)$ such that

$$\rho(g_1)^{A_1}\cdot\ldots\cdot\rho(g_s)^{A_s}=1. \tag{5}$$

Let $\widetilde{A}_i$ denote the image of A_i in $\mathrm{PGL}_n(\widetilde{R})$. By the induction hypothesis, we can find $\widetilde{B}_i\in\mathrm{PGL}_n(\widetilde{R})$ in the centralizer of $\widetilde{\rho}(g_i)$ and a $\widetilde{B}\in\mathrm{PGL}_n(\widetilde{R})$ such that $\widetilde{A}_i=\widetilde{B}\widetilde{B}_i$ for $i=1,\ldots,s$. Let $\hat{B}$ be any lift of $\widetilde{B}$ to $\mathrm{PGL}_n(R)$. By Lemma 6.12 and the definition of rigid deformation, each matrix $\widetilde{B}_i$ is the reduction of some $\hat{B}_i\in\mathrm{PGL}_n(R)$, so that $\hat{B}_i^{-1}\rho(g_i)\hat{B}_i=\rho(g_i)$. Therefore, if we conjugate Equation (5) by $\hat{B}^{-1}$ and rename the variables $\hat{B}^{-1}A_i\hat{B}_i^{-1}$ as A_i, we can and will assume that $A_i\equiv 1 \pmod{xR}$.

Choose $D_i\in M_n(R)$ so that $1+xD_i\in\mathrm{GL}_n(R)$ is a representative for A_i modulo $R^*\cdot 1$. Note that the A_i only depend on $\bar{D}_i:=(D_i \pmod{\mathfrak{m}_R}) \pmod{\kappa\cdot 1}\in\overline{\mathrm{ad}}$. Distributing the terms in Equation (5) and subtracting $1=\rho(g_1)\ldots\rho(g_s)$ from each side we obtain the following equation (essentially in $\overline{\mathrm{ad}}$):

$$x\sum_{i=1}^{s}\rho(g_1)\ldots\rho(g_{i-1})(\rho(g_i)D_i-D_i\rho(g_i))\rho(g_{i+1})\ldots\rho(g_s)=0.$$

We multiply this on the right by $1=\rho(g_s^{-1})\ldots\rho(g_1^{-1})$, and introduce the notation $\widetilde{g}_i=g_1\ldots g_i$. Then the above equation is equivalent to

$$\sum_{i=1}^{s}\widetilde{g}_{i-1}(g_i-1)\bar{D}_i=0 \tag{6}$$

in $\overline{\mathrm{ad}}$ where we use the adjoint action.

We define $\delta_{i+1} := \bar{D}_i - \bar{D}_{i+1}$, $i = 1, \ldots, s-1$, and $\delta_1 = \bar{D}_s - \bar{D}_1$ so that $\sum_{i=1}^{s} \delta_i = 0$. Then Equation (6) can be rewritten as

$$0 = \sum_{i=1}^{s} (\widetilde{g}_i - \widetilde{g}_{i-1})\bar{D}_i = \sum_{i=1}^{s} \widetilde{g}_{i-1}\delta_i.$$

By Corollary 6.21 there now exist elements $\varepsilon_i \in \overline{\mathrm{ad}}^{g_i}$ such that for all $i = 1, \ldots, s-1$ one has $\delta_i = \varepsilon_i - \varepsilon_{i-1}$. This implies that $D := D_i + \varepsilon_i$ is independent of i. But then we have

$$\rho(g_i)^{1+xD_i} = (\rho(g_i)^{1-x\varepsilon_i})^{1+xD} = \rho(g_i)^{1+xD}.$$

for all $i = 1, \ldots, s$. This completes the proof of the rigidity of $\underline{g}$ for ρ.

We now explain the last two assertions of the theorem: By Corollary 2.6 and our hypotheses, $\rho_{\mathscr{D}}$ has maximal image. Hence the same is true for its quotient $\rho^{\mathrm{rig}}_{\mathscr{D}}$.

Finally suppose that in addition the $\bar{\rho}(g_i)$ are strictly rigid for $\mathrm{Im}(\bar{\rho})$, let R be any finite quotient of $R_{\mathscr{D}}$ and set $\rho_R := \rho_{\mathscr{D}} \otimes_{R_{\mathscr{D}}} R$. By Proposition 2.12, to complete the proof of Theorem 6.17, we need to show that the $\rho_R(g_i)$ are strictly rigid for $\mathrm{Im}(\rho_R)$: So let $A_1, \ldots, A_s \in \mathrm{PGL}_n(R)$ such that $\prod_i \rho_R(g_i)^{A_i} = 1$. Since the g_i are strictly rigid for ρ_R, there is a unique $A \in \mathrm{PGL}_n(R)$ such that for all i we have $\rho_R(g_i)^{A_i} = \rho_R(g_i)^{A}$. By the strict rigidity of the $\bar{\rho}(g_i)$ for $\mathrm{Im}(\bar{\rho})$, it follows that the reduction of A modulo $\mathfrak{m}_R$ lies in $\mathrm{Im}(\bar{\rho})$. Since $\rho_{\mathscr{D}}$ has maximal image and hence so does ρ_R, it follows that A itself must lie in $\mathrm{Im}(\rho_R)$. The uniqueness of A is obvious and so the proof is complete. ∎

We note some facts on rationality as introduced in Definition 2.22.

Lemma 6.24 *Let F be a field, G a profinite group and $g \in G$ of finite order m prime to the characteristic of F. Then:*

(a) Any F^{sep}-valued (locally constant finite dimensional) character χ of G satisfies $\chi(g) \in F(\zeta_m)$, and so g^G is $F(\zeta_m)$-rational.

(b) The class g^G is F-rational if and only if $\chi(g) = \chi(g^e)$ for all $e \in (\mathbb{Z}/(m))^*$ for which there exists a $\sigma \in \mathrm{Gal}(F^{\mathrm{sep}}/F)$ with $\sigma(\zeta_m) = \zeta_m^e$.

(c) If g and g^{-1} are conjugate, then g^G is $F(\zeta_m + \zeta_m^{-1})$-rational.

The proof follows easily from [Ser], § 7.1.

The next result is the analog of Corollary 2.25 under the more general hypothesis of Theorem 6.17. It implies the corollary due to Lemma 6.18.

Corollary 6.25 *We keep the assumptions and notations of Theorem 6.17. Let $m := \mathrm{ord}\,\mathscr{D}$ and assume that the conjugacy classes of the $\bar{\rho}(g_i)$ are F-rational. Then there exists a unique continuous representation*

$$\rho^{\mathrm{rig}}_{\mathscr{D},m}\colon \mathrm{Gal}(k(t)^{(l)}_{\mathscr{D}}/F_m(t)) \longrightarrow \mathrm{PGL}_n(R^{\mathrm{rig}}_{\mathscr{D}})$$

whose restriction to $G_{\mathscr{D}}$ is isomorphic to the universal representation $\rho^{\mathrm{rig}}_{\mathscr{D}}$.

If the splitting field of $\widetilde{\rho}\colon \mathrm{Gal}(k(t)^{(l)}_{\Sigma}/F(t)) \longrightarrow \mathrm{PGL}_n(\kappa)$ is a regular cover of $F(t)$, then so is the splitting field of $\rho^{\mathrm{rig}}_{\mathscr{D},m}$ over $F_m(t)$.

Proof: To shorten the notation, we define $\mathfrak{m} := \mathfrak{m}_{R^{\mathrm{rig}}_{\mathscr{D}}}$. Recall that $F_m = F(\zeta_{p^m})$. By Theorem 6.17, the elements g_i are strictly pro-rigid for any of the representations $\rho^{\mathrm{rig}}_{\mathscr{D}} \pmod{\mathfrak{m}^\mu}$, $\mu \in \mathbb{N}$. Let $\hat{h}_i$ denote $\rho^{\mathrm{rig}}_{\mathscr{D}}(g_i)$. By the previous lemma, the conjugacy classes of the $\hat{h}_i$ are F_m-rational. We apply the result quoted above Corollary 2.25 and obtain representations $\rho^{(\mu)}_{\mathscr{D},m}\colon \mathrm{Gal}(k(t)_\Sigma/F_m(t)) \longrightarrow \mathrm{PGL}_n(R^{\mathrm{rig}}_{\mathscr{D}}/\mathfrak{m}^\mu)$ whose restriction to $G_{k(t)}$ agrees with the representation $\rho_{\mathscr{D}} \pmod{\mathfrak{m}^\mu}$ up to conjugation. By an inductive procedure, we can conjugate the $\rho^{(\mu)}_{\mathscr{D},m}$ suitably, so that for all μ we have

$$\rho^{(\mu)}_{\mathscr{D},m} = \rho^{(\mu+1)}_{\mathscr{D},m} \pmod{\mathfrak{m}^\mu}.$$

Then $\rho^{\mathrm{rig}}_{\mathscr{D},m} := \varprojlim_\mu \widetilde{\rho}^{(\mu)}_{\mathscr{D},m}$ satisfies the conditions stated in the corollary.

It remains to prove the second assertion of the corollary. By Corollary 2.6, the image of $\rho^{\mathrm{rig}}_{\mathscr{D},m}$ is maximal. The regularity of the splitting field of $\widetilde{\rho}$ implies that $\widetilde{\rho}$ and $\bar{\rho}$ must have the same image. Combining the two assertions yields that $\rho^{\mathrm{rig}}_{\mathscr{D}}$ and $\rho^{\mathrm{rig}}_{\mathscr{D},m}$ have the same image, and thus the splitting field of $\rho^{\mathrm{rig}}_{\mathscr{D},m}$ is regular over $F_m(t)$. ∎

We end this section by exhibiting two examples of geometrically rigid tuples, and thereby proving Corollary 2.26. We recall the following from [MM]. In the form needed, the result is due to Völklein.

Proposition 6.26 *For $\kappa \neq \mathbb{F}_2$ and any $n \geq 2$, there exists a Belyi triple g_1, g_2, g_3 of $\mathrm{PGL}_n(\kappa)$ (i.e., a strictly rigid triple) which is geometrically rigid for the identity representation of $\mathrm{PGL}_n(\kappa)$ into itself and satisfies*

(a) g_2 and g_3 are regular elements.

(b) g_2 is semisimple and g_3 is unipotent.

(c) g_1 has a semisimple lift to $\mathrm{GL}_n(\kappa)$ which has 1 as an $n-1$-fold eigenvalue.

(d) $Z_{g_1}(\kappa) = \{1\}$.

Proof: We abbreviate $q := |\kappa|$ and let $a \in \mathbb{F}_p^{\mathrm{alg}}$ be an element of exact order $q^n - 1$. Define polynomials $f(t) := \prod_{i=0}^{n-1}(t - a^{q^i})$ and $g(t) := (t-1)^n$, cf. [MM], Remark on p. 105f. Let $\sigma_1, \sigma_2, \sigma_3$ denote the Belyi triple for $\mathrm{GL}_n(\kappa)$ with characteristic polynomials f, g for σ_2^{-1} and σ_3, respectively, as constructed in [MM], Thm. II.2.6. Let g_i be the image of the σ_i in $\mathrm{PGL}_n(\kappa)$. We claim that the g_i have the desired properties:

Part (d) follows from the choice of a and the definition of f, since no two distinct roots of f, if divided by each other, yield an element in κ. Next, a simple adaptation of the proof of [MM], Prop. II.3.1, shows that the σ_i generate $\mathrm{GL}_n(\kappa)$, and hence the g_i generate $\mathrm{PGL}_n(\kappa)$. The result of Belyi, [MM], Thm. I.5.10, implies that the g_i are geometrically rigid for the identity representation of $\mathrm{PGL}_n(\kappa)$ into itself. From the characteristic polynomials of σ_2 and σ_3, part (b) is immediate, and furthermore σ_2 must be semisimple.

[MM], Thm. II.2.6, also asserts that the rank of $1 - \sigma_1$ is one, where $\sigma_1 = \sigma_3^{-1}\sigma_2^{-1}$. Using f, g we compute the determinant of σ_1 to $a^{1+q+\cdots+q^{n-1}}$, which is of order $q-1 > 1$. Therefore σ_1 must have an eigenvalue different from 1, and so part (c) is shown.

It remains to prove that σ_3 is a regular element. The construction of σ_3 is given in [MM], Lem. II.2.5. Following it, it is possible to give an explicit expression for σ_3 in terms of a and q. It shows that σ_3 is unipotent upper triangular and all its upper diagonal entries are non-zero. Hence $\sigma_3 - 1$ is of rank $n-1$ and thus σ_3 is regular unipotent. ∎

Our second result on explicit geometrically rigid tuples goes again back to Völklein:

Proposition 6.27 *Suppose that $q := |\kappa| \geq 5$ and $n \geq 9$. Then there exists a Thompson tuple $(g_0, g_1, \ldots, g_n)$ of $\mathrm{PGL}_n(\kappa)$, i.e., a tuple in $\mathrm{PGL}_n(\kappa)^{n+1}$ which satisfies* *(a) the g_i generate an irreducible subgroup inside* $\mathrm{PGL}_n(\kappa)$*,*

(b) $g_0 g_1 \cdot \ldots \cdot g_n = 1$ *and*

(c) each g_i has a representative in $\mathrm{GL}_n(\kappa)$ *whose eigenspace for the eigenvalue* 1 *has dimension* $n-1$*,*

and such that in addition *the g_i form a generating set for* $\mathrm{PGL}_n(\kappa)$*, are geometrically rigid for the identity representation of* $\mathrm{PGL}_n(\kappa)$ *into itself and are semisimple and non-scalar. In particular $Z_{g_i}(\kappa) = \{1\}$ for all i, since $n \geq 9$.*

Proof: We choose $b_0, b_1, \ldots, b_n, a_n \in \kappa^*$ such that $b_i \neq 1$ for $i = 0, \ldots, n$, $b_i a_n \neq 1$ for $i = 0, \ldots, n-1$, $a_n \neq 1$ and some b_i has order $|\kappa| - 1$ (for instance, we could take $b_0 = \ldots = b_n$ an element of order $|\kappa| - 1 \geq 4$ and $a_n = b_n^2$). Then by [Vö], § 2, there is a tuple $g_0, \ldots, g_n \in \mathrm{GL}_n(\kappa)$ such that the g_i are semisimple, have characteristic polynomial $(T-1)^{n-1}(T-b_i)$ for $i = 0, \ldots, n-1$, and $(T-a_n)^{n-1}(T-b_n)$ for $i = n$, and which form a strictly rigid Thompson tuple in $\mathrm{PGL}_n(\kappa)$, generating the group $\mathrm{PGL}_n(\kappa)$. ■

Proof of Corollary 2.26: Let g_i be topological generators of the (pro-cyclic) inertia subgroups I_i of $G_{\mathbb{Q}^{\mathrm{alg}}(t)}$, $i = 0, 1, \infty$, such that $\prod g_i = 1$. Let us take the geometrically rigid generators of $\mathrm{PGL}_n(\kappa)$ constructed in Proposition 6.26, and call them h_0, h_1, h_∞. Define

$$\bar{\rho} \colon G_{\mathbb{Q}^{\mathrm{alg}}(t)} \longrightarrow \mathrm{PGL}_n(\kappa) : g_i \mapsto h_i.$$

Then $\bar{\rho}$ is ramified precisely at the places of $\Sigma := \{0, 1, \infty\}$. Corollary 3.6 yields that $R_S \cong W(\kappa)[[T_1, \ldots, T_{2n-2}]]$ where $S = \{1, \infty\}$.

We let $F := \mathbb{Q}(\zeta_{(q^n-1)})$. Then Corollary 2.25 provides us with a surjective representation

$$\rho_{S,\infty} \colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}(t)_S / F_\infty(t)) \twoheadrightarrow \mathrm{PGL}_n(R_S),$$

which defines a regular cover of $F_\infty(t)$. Note that by Example 2.7 and Proposition 6.26 all hypotheses of Theorem 2.20, and hence of Corollary 2.25 are met. (The hypothesis that n is not divisible by the characteristic of κ is used twice, in Example 2.7 and in showing $Z_{h_\infty}(\kappa) = 1$ which is needed for Corollary 2.25.)

To complete the proof, we follow [Ro1], pp. 276ff.: Consider $\rho_2 := \rho_{S,\infty} \pmod{\mathfrak{m}_S^2}$. Let F' be a finite extension of F inside F_∞ such that if n_i denotes the order of $\rho_2(g_i)$, then $\zeta_{n_i} \in F'$, for $i = 0, 1, \infty$, e.g. $F' = F_{[\log_p n]+2}$. Then standard arguments in rigidity, similar to those used above Corollary 2.25, show that there exists a surjective representation

$$\hat{\rho}_2 \colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}(t)_\Sigma / F'(t)) \twoheadrightarrow \mathrm{PGL}_n(R_S/\mathfrak{m}_{R_S}^2)$$

whose restriction to $G_{k(t)}$ is $\rho_S \pmod{\mathfrak{m}_{R_S}^2}$ and which is unique up to inner automorphisms of $\mathrm{PGL}_n(R_S/\mathfrak{m}_{R_S}^2)$. Moreover the splitting field of $\bar{\rho}_2$ is a regular cover of $F'(t)$. Let $\theta_{F'}$ be a thin subset of $\mathbb{P}^1(F')$ which contains Σ, cf. [Ser], Thm. 3.4.1. By specializing to suitable places of $\mathbb{P}^1(F') - \theta_{F'}$, one obtains infinitely many different extensions of F' with Galois group isomorphic to $\mathrm{PGL}_n(R_S/\mathfrak{m}_{R_S}^2)$, cf. [Ser], Prop. 3.3.3. Let $\mathscr{S} \subset \mathbb{P}^1(F') - \theta_{F'}$ be an infinite set of such places.

Let D_x be the decomposition group of a point $x \in \mathscr{S}$, inside $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}(t)_\Sigma / F_\infty)$. Then $\rho_{S,\infty}(D_x)$ is a subgroup of $\mathrm{PGL}_n(R_S)$. By the previous paragraph, the quotient modulo $\mathfrak{m}_{R_S}^2$ of $\rho_{S,\infty}(D_x)$ is isomorphic to $\mathrm{PGL}_n(R_S/\mathfrak{m}_{R_S}^2)$. But then, by Proposition 2.4 we must have $\rho_{S,\infty}(D_x) = \mathrm{PGL}_n(R_S)$. Because $x \notin \Sigma$, the specialization of $\rho_{S,\infty}$ at such an x gives a surjective representation $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/F_\infty) \longrightarrow \mathrm{PGL}_n(R_S)$. By the previous paragraph, the specializations at the points $x \in \mathscr{S}$ are pairwise non-isomorphic. ■

Using Proposition 6.27 instead of Proposition 6.26, and Theorem 7.4 (see the next section) with S a set of $n+1$ distinct places instead of Corollary 3.6, and otherwise the same reasoning as above, one finds:

Corollary 6.28 *Let $q := |\kappa|$ and let $n \geq 3$ be an integer prime to q. If $q \geq 5$, there exist infinitely many non-isomorphic Galois extensions of $\mathbb{Q}_\infty(\zeta_{q-1})$ with Galois group isomorphic to $\mathrm{PGL}_n(W(\kappa)[[T_1, \ldots, T_{n+1}]])$.*

Since the g_i in Proposition 6.27 have order dividing $q-1$, $\mathbb{Q}(\zeta_{q-1})$ is a field of rationality for the representation generated by the g_i. In many cases, this field may be taken even smaller, since our prime interest is in the image of the g_i in $\mathrm{PGL}_n(\kappa)$.

7 The structure of the rings $R_{\mathscr{D}}^{(\mathrm{rig})}$

Throughout this section, we assume that $\bar\rho$ is admissible and we have strictly pro-rigid generators for $\bar\rho$ as in Theorem 6.17. In this case, we want to derive a number of ring theoretic properties of the rings $R_{\mathscr{D}}$ and $R_{\mathscr{D}}^{\mathrm{rig}}$ for ramification data $\mathscr{D}$ with $\mathrm{Supp}\,\mathscr{D} \subset \Sigma := \mathrm{Ram}(\bar\rho)$. All these rings will be reduced, flat over $W(\kappa)$ and complete intersections and, for S in place of $\mathscr{D}$ and such that $S_p \subset S \subset \Sigma$, the rings R_S and R_S^{rig} will be power series rings over $W(\kappa)$.

By $\hat\otimes$ we denote the completed tensor product over $W(\kappa)$. Also, let $\bar\rho_x$ denote the restriction of $\bar\rho$ to the inertia group I_x above a place x. The functor that describes the deformations of $\bar\rho_x$ may not be representable, but it has a versal hull. By R_x we denote the corresponding versal deformation ring, and by $R_{x,m}$ the quotient of R_x which parameterizes deformations of $\bar\rho_x$ which are unramified when restricted to $J_x^{p^m}$. Similarly, we will use R_x^{rig} (see also the proof of Theorem 6.16) and $R_{x,m}^{\mathrm{rig}}$.

Lemma 7.1 *Suppose $\bar\rho$ is admissible. Then for $? \in \{\varnothing, \mathrm{rig}\}$ and $S \supset S_p$ the morphism*

$$\widehat{\bigotimes}_{x\in S} R_x^{?} \longrightarrow R_S^{?}$$

induced from restricting a global deformation to its inertia groups at all places in S is surjective.

If $S = \varnothing$, we set $\widehat{\bigotimes}_{x\in S} R_x^{?} := W(\kappa)$.

Proof: Since $R_{S_p}^{\mathrm{rig}}$ is defined by local conditions, for $S \supset S_p$ one has the pushout diagram

$$\begin{tikzcd}
\widehat{\bigotimes}_{x\in S} R_x \arrow[r] \arrow[d] & R_S \arrow[d] \\
\widehat{\bigotimes}_{x\in S_p} R_x^{\mathrm{rig}} \arrow[r] & R_{S_p}^{\mathrm{rig}}
\end{tikzcd}$$

of local rings. By Nakayama's lemma, the upper horizontal homomorphism is surjective if R_S modulo the image of the maximal ideal of $\hat{\bigotimes}_{x\in S} R_x$ is κ. By the pushout property, it suffices to prove $\bar R \cong \kappa$ for $\bar R$ the quotient of $R_{S_p}^{\mathrm{rig}}$ by the ideal generated by the images of all the maximal ideals $\mathfrak{m}_{R_x^{\mathrm{rig}}}$ of the rings R_x^{rig}, $x \in S_p$. So let us assume otherwise.

Note first that $\bar R$ is of characteristic p, since p lies in any of the $\mathfrak{m}_{R_x}$. Therefore $\bar R$ has a quotient $\bar R_\varepsilon \cong \kappa[\varepsilon]/(\varepsilon^2)$. By Theorem 6.17, the elements g_x, $x \in \Sigma$, are strictly pro-rigid for $\rho_{S_p}^{\mathrm{rig}}$ and hence also for the induced representation over the quotient $\bar R_\varepsilon$

$$\bar\rho_\varepsilon \colon G_{k(t)} \longrightarrow \mathrm{PGL}_n(\kappa[\varepsilon]/(\varepsilon^2)).$$

We abbreviate $\bar{h}_x := \bar{\rho}(g_x)$ and $\bar{h}_{x,\varepsilon} := \bar{\rho}_\varepsilon(g_x)$. Because $\mathfrak{m}_{R_x} = 0$ in $\bar{R}_\varepsilon$, the local representations are conjugate to the trivial lift of the residual representation, i.e., there exist matrices $A_x \in \mathrm{PGL}_n(\kappa[\varepsilon]/(\varepsilon^2))$ for all $x \in \Sigma$ such that $\bar{h}_{x,\varepsilon}^{A_x} = \bar{h}_x$. Then

$$\prod h_{x,\varepsilon}^{A_x} = \prod \bar{h}_x = \mathrm{id} \in \mathrm{PGL}_n(\kappa[\varepsilon]/(\varepsilon^2)),$$

and the strict pro-rigidity of the g_x for $\bar{\rho}_\varepsilon$ yields a unique $A \in \mathrm{PGL}_n(\kappa[\varepsilon]/(\varepsilon^2))$ such that

$$\bar{h}_{x,\varepsilon}^{A} = \bar{h}_{x,\varepsilon}^{A_x} = \bar{h}_x \ \forall x \in \Sigma.$$

This means that $\bar{\rho}_\varepsilon^A = \bar{\rho}$, and so $\bar{\rho}_\varepsilon$ is conjugate to the trivial lift of $\bar{\rho}$ to $\kappa[\varepsilon]/(\varepsilon^2)$. By the universality of $(\rho_S^{\mathrm{rig}}, R_S^{\mathrm{rig}})$, the unique morphism $R_S^{\mathrm{rig}} \longrightarrow \kappa[\varepsilon]/(\varepsilon^2)$ inducing $\bar{\rho}_\varepsilon$ factors via κ. This contradicts the construction of $\bar{\rho}_\varepsilon$, and completes the proof of the lemma. ∎

In simple cases, we now compute the Krull dimensions of the rings involved in the previous theorem. We begin with the local cases:

Lemma 7.2 *Suppose $\bar{\rho}$ is admissible. Then for any $x \in \Sigma$ the rings R_x and R_x^{rig} are smooth over $W(\kappa)$.*

Their relative Krull dimensions are given as follows: Write $\bar{\rho}'_x = \oplus_i \bar{\rho}'^{\,n_{x,i}}_{x,i}$ where we represent $\bar{\rho}_x$ by a linear representation and where the $\bar{\rho}'_{x,i}$ are indecomposable of rank $d_{x,i}$ and pairwise non-isomorphic. Let $e_x := |Z_{\bar{\rho}_x(g_x)}(\kappa)|$. Then

$$\dim_{W(\kappa)} R_x = \dim_\kappa H^0(I_x, \overline{\mathrm{ad}}_{\bar{\rho}_x}) = -1 + \sum_i n_{x,i}^2 d_{x,i} \ \textit{and} \ \dim_{W(\kappa)} R_x^{\mathrm{rig}} = -1 + \frac{1}{e_x} \sum_i d_{x,i}.$$

Proof: The assertion for R_x follows straight from obstruction theory: Since $\overline{\mathrm{ad}}$ is of order prime to l and I_x is isomorphic to the prime to l completion of $\mathbb{Z}$, we have $H^2(I_x, \overline{\mathrm{ad}}) = 0$ and $h^0(I_x, \overline{\mathrm{ad}}) = h^1(I_x, \overline{\mathrm{ad}})$. Therefore R_x is smooth over $W(\kappa)$ of relative dimension $h^0(I_x, \overline{\mathrm{ad}})$. The second expression given is simply an evaluation of $h^0(I_x, \mathrm{ad})$, based on the facts that for $i \neq j$ there are no I_x-equivariant homomorphism from $\bar{\rho}'_{x,i}$ to $\bar{\rho}'_{x,j}$ (by the block-regularity of $\bar{\rho}_{x,i}$), while $\mathrm{Hom}_{I_x}(\bar{\rho}'_{x,i}, \bar{\rho}'_{x,i})$ is of dimension $d_{x,i}$ over κ.

For R_x^{rig} the proof is slightly more involved. By Remark 5.4(a) (which requires $p \not| n$, which follows from admissibility), we may consider deformations of a linear representative $\bar{A}'_x$ of $\bar{\rho}(g_x)$. Since the universal ring for deformations of the trivial homomorphism $I_x \longrightarrow \{1\} \subset \kappa^*$ is isomorphic to $W(\kappa)[[T]]$, it will suffice to show that the corresponding universal ring R'^{rig}_x for linear deformations and with no restrictions on the determinant is smooth over $W(\kappa)$ of dimension $\frac{1}{e_x}\sum_i d_{x,i}$.

Let ζ be a generator of $Z_{\bar{A}'_x}(\kappa)$ (or its Teichmüller lift). Using Lemma 6.4, we may group together those $\bar{\rho}'_{x,i}$ which lie in a single ζ-orbit under conjugation by powers of ζ. Then $\bar{A}'_x$ is in block diagonal form, and the blocks corresponding to different ζ-orbits do lift independently. It therefore suffices to prove the assertion in the case of a single ζ-orbit. Since we require the lifts to be block-regular, the multiplicity $n_{x,i}$ will have no effect on the deformation ring, and so it suffices to prove the assertion in the case that all $n_i = 1$. (They are all equal since all $\bar{\rho}'_{x,i}$ lie in a single ζ-orbit.) The following lemma completes the proof, since under the conditions achieved we have $n = \sum d_{x,i}$. ∎

Lemma 7.3 *Suppose $\bar{A}' \in \mathrm{GL}_n(\kappa)$ is regular and let $e = |Z_{\bar{A}'}(\kappa)|$. Then*

(a) The characteristic polynomial of $\bar{A}'$ is of the form $\bar{g}(X) := X^n + \sum_{i=1}^{n/e} X^{(n-i)e}\bar{b}_i$.

(b) Let $g(X) := X^n + \sum_{i=1}^{n/e} X^{(n-i)e} b_i \in W(\kappa)[X]$ *be a lift of* $\bar{g}(X)$*, and denote by* $\sim$ *strict equivalence of matrices. Then the deformation functor*

$$\mathrm{Def}_{\bar{A}'} \colon \mathscr{C} \longrightarrow ((Sets)) : R \mapsto \{A' \in \mathrm{GL}_n(R) \mid A' \mod \mathfrak{m}_R = \bar{A}', Z_{A'}(R) \overset{\cong}{\longrightarrow} Z_{\bar{A}'}(\kappa)\}/\sim$$

is representable by $(R_{\bar{A}'}, A'_{\bar{A}'})$ *with* $R_{\bar{A}'} = W(\kappa)[[T_1, \ldots, T_{n/e}]]$ *and* $A'_{\bar{A}'}$ *the companion matrix of the polynomial* $\widetilde{g}(X) := g(X) + \sum_{i=1}^{n/e} X^{(n-i)e} T_i$*.*

Proof: By Lemma 6.2 we may assume that $\bar{A}'_x$ as well as any lift A'_x are companion matrices. Let $\zeta \in \kappa^*$ be a generator of $Z_{\bar{A}'}(\kappa)$, and denote be ζ also its Teichmüller lift to $W(\kappa)$. Suppose A' is the companion matrix for $f(X) = X^n + \sum_{j=1}^{n} a_i T^{n-i}$. The condition that A' and $\zeta A'$ are conjugate implies that they have the same characteristic polynomials. This leads to $f(X) = f(\zeta X)$. Comparing these polynomials shows that $a_i = 0$ whenever $e \not| i$. In particular this proves part (a). Conversely, if the a_i are zero for $e \not| i$ then the companion matrix of $\zeta A'$ is conjugate to the companion matrix A' (explicitly, by conjugating by the diagonal matrix with entries $(1, \zeta, \ldots, \zeta^{n-1})$) So if we represent all A' as companion matrices for some polynomial f as above, then $\mathrm{Def}_{\bar{A}'}$ is the deformation functor for polynomials f, lifting $\bar{g}$, such that $a_i = 0$ for $e \not| i$. Part (b) is now straightforward. ∎

Theorem 7.4 *Suppose that* $\bar{\rho}$ *is admissible and that* S *is non-empty and satisfies* $S_p \subset S \subset \Sigma$*. Then the homomorphism in Lemma 7.1 is an isomorphism, and the rings* R_S *and* R_S^{rig} *are power series rings over* $W(\kappa)$*.*

Their relative Krull dimensions over $W(\kappa)$ *(in the notation of Lemma 7.2) are*

$$\dim_{W(\kappa)} R_S = -|S| + \sum_{x \in S} \sum_i n_{x,i}^2 d_{x,i} \quad \textit{and} \quad \dim_{W(\kappa)} R_S^{\mathrm{rig}} = -|S| + \sum_{x \in S} \frac{1}{e_x} \sum_i d_{x,i}.$$

Proof: By Theorem 2.3, the ring R_S is a power series ring over $W(\kappa)$ of relative dimension

$$(|\Sigma| - 2)(n^2 - 1) - \sum_{x \in \Sigma - S} \dim \overline{\mathrm{ad}}_{\bar{\rho}}^{H_x}.$$

By Corollary 6.22, we have $\sum_{x \in \Sigma} \dim \overline{\mathrm{ad}}_{\bar{\rho}}^{H_x} = (|\Sigma| - 2)(n^2 - 1)$ if $\bar{\rho}$ has a geometricallly rigid set of generators. Therefore

$$\dim_{W(\kappa)} R_S = \sum_{x \in S} \dim \overline{\mathrm{ad}}_{\bar{\rho}}^{H_x} \overset{\text{Lem. 7.2}}{=} \sum_{s \in S} \dim_{W(\kappa)} R_x.$$

This means that for such S and $? = \varnothing$, in Lemma 7.1 we have smooth rings over $W(\kappa)$ of the same relative Krull dimension on both sides of the displayed homomorphism. Hence the surjective homomorphism in Lemma 7.1 must be an isomorphism. This proves all the claims for the non-rigid global deformation rings.

For rigid deformations observe that we have a pushout diagram of the type displayed in the proof of Lemma 7.1 also for S instead of S_p at the bottom. This proves that the homomorphism in Lemma 7.1 is also an isomorphism for $? = \mathrm{rig}$. The assertion about the relative dimensions are then immediate from Lemma 7.2. ∎

From a pushout diagram as in the proof of Lemma 7.1 and from the first assertion in Theorem 7.4 with $S = \Sigma$, we deduce:

Corollary 7.5 *Let $\mathscr{D} = \{\Sigma : (n_x)_{x\in\Sigma}\}$ and assume that $\bar\rho$ is admissible. Then*

$$\widehat{\bigotimes}_{x\in\Sigma} R^{\mathrm{rig}}_{x,n_x} \longrightarrow R^{\mathrm{rig}}_{\mathscr{D}}$$

is an isomorphism.

To further analyze the structure of $R_{\mathscr{D}}$ and also to complete the proof of Theorem 2.27, in the remainder of this section we prove and discuss the following result:

Theorem 7.6 *For $m \in \mathbb{N}$ and $x \in \Sigma$, the ring $R^{\mathrm{rig}}_{x,m}$ is reduced, finite flat over $W(\kappa)$ and a complete intersection.*

From Theorems 7.6 and Corollary 7.5 we deduce:

Corollary 7.7 *Suppose $\bar\rho$ is regular and p does not divide n. Then for any ramification datum $\mathscr{D}$ (with support in Σ), the ring $R^{\mathrm{rig}}_{\mathscr{D}}$ is reduced, flat over $W(\kappa)$ and a complete intersection. If moreover* $\operatorname{ord}\mathscr{D} < \infty$*, then $R^{\mathrm{rig}}_{\mathscr{D}}$ is a finitely generated $W(\kappa)$-module.*

Suppose $\bar A'_x \in \mathrm{GL}_n(\kappa)$ represents $\bar\rho(g_x)$. Let $R'_{x,m}$ denote the versal ring describing arbitrary deformations of the given representation of $I_{x,m} := I_x/J_x^{p^m}$ with image of $\bar A'_x$ of a fixed generator, and let $R'^{\mathrm{rig}}_{x,m}$ be the quotient for such deformations which are block-regular and so that $Z_A(R) \longrightarrow Z_{\bar A'_x}(\kappa)$ is an isomorphism. As we shall see in the proof of Theorem 7.6, the crucial special case of it is the following result:

Lemma 7.8 *If $\bar A'_x$ acts indecomposably on κ^n with a single eigenvalue, then $R'_{x,m} = R'^{\mathrm{rig}}_{x,m}$ is finite flat over $W(\kappa)$, a complete intersection and reduced.*

Proof of Theorem 7.6: Assuming Lemma 7.8, we indicate the proof of the theorem. Let $p^{m'}$ be the maximal p-power dividing the order of the cyclic group $I_{x,m}$. We proceed as in the proof of Lemma 7.2: Using Remark 5.4, we have $R'^{\mathrm{rig}}_{x,m} \cong R^{\mathrm{rig}}_{x,m} \hat\otimes_{W(\kappa)} R^1_{x,m}$, where $R^1_{x,m} \cong W(\kappa)[[T]]/((1+T)^{p^{m'}} - 1)$ is the universal ring for deformations of the trivial one-dimensional representation. The ring $R^1_{x,m}$ is thus finite flat over $W(\kappa)$, a complete intersection and reduced. One has the following lemma from commutative algebra:

Lemma 7.9 *Let R and R' be in the category $\mathscr{C}$. Suppose R' is finite flat over $W(\kappa)$, a complete intersection and reduced. Then R is finite flat over $W(\kappa)$, a complete intersection and reduced, if and only if this holds for $R' \hat\otimes_{W(\kappa)} R$.*

We sketch a proof: The assertion on finiteness follows easily from the assumed flatness of R' over $W(\kappa)$. Thus one may replace the completed tensor product by the usual one. The assertion on flatness is now easily deduced from R' being a free finitely generated $W(\kappa)$-module and the structure theorem for finitely generated modules over $W(\kappa)$. Having flatness over $W(\kappa)$, the reducedness follows easily by passing to the same rings with p inverted: a ring over $W(\kappa)[1/p]$ which is finite as a module is reduced if and only if it is a product of finite field extensions of $W(\kappa)[1/p]$. For the assertion on complete intersections, we refer to [Mat], p. 308.

Using Lemma 7.9, to complete the proof of Theorem 7.6 it suffices to prove all stated assertions for $R'^{\mathrm{rig}}_{x,m}$: We may in $\bar A'_x$ group together those indecomposable pieces which lie in the same orbit under the action of $Z_{\bar A'_x}(\kappa)$. The ring $R'^{\mathrm{rig}}_{x,m}$ will be the (completed) tensor product (over $W(\kappa)$) of the corresponding rings for the individual orbits, and so we will assume that there is a single orbit. By the block-regularity of the lifts, we may, without altering R_x^{rig}, further assume that each indecomposable summand occurs with multiplicity one. This means that $\bar{A}'_x$ is regular.

For regular A'_x the ring R_x^{rig} represents the subfunctor of $\mathrm{Def}_{\bar{A}'_x}$ from Lemma 7.3 of deformations A' for which $A'^{|I_{x,m}|} = 1$. Since the A' may be taken as companion matrices, the latter condition means that $X^{|I_{x,m}|} - 1$ is a multiple of the characteristic polynomial of A'. Let $\widetilde{g}$ be as in Lemma 7.3 and let $f_i \in W(\kappa)[T_1, \ldots, T_{n/e}]$, $i = 0, \ldots, n-1$, be such that $\sum_{i=0}^{n/e-1} X^{ei} f_i$ is the remainder of $X^{|I_{x,m}|} - 1$ modulo $\widetilde{g}$. The above discussion and Lemma 7.3 yield R_x^{rig} as the following quotient of $R_{\bar{A}'_x}$:

Lemma 7.10 $R_x^{\mathrm{rig}} \cong W(\kappa)[[T_1, \ldots, T_{n/e}]]/(f_0, \ldots, f_{n-1})$.

This description makes it obvious that $R_x^{\mathrm{rig}} \otimes_{W(\kappa)} W(\widetilde{\kappa})$ describes the deformations after base change from κ to a finite extension field $\widetilde{\kappa}$. So to prove Theorem 7.6, we may assume that all eigenvalues of $\bar{A}'_x$ lie already in κ.

Then each isotypical component $\bar{A}'_i$ of $\bar{A}'_x$ (acting on κ^n) is indecomposable and has a single eigenvalue and, by the regularity of $\bar{A}'_x$, different components have different eigenvalues. We group them again according to ζ-orbits (after base change orbits may decompose), and then again observe that it suffices to treat the case of a single orbit.

Since $\bar{A}'_i$ has a single eigenvalue, it is not conjugate to $\zeta' \bar{A}'_i$ for $\zeta' \neq 1$. This shows that conjugation by ζ cyclically permutes the $\bar{A}'_i$. The same will hold for lifts. Thus R_x^{rig} is completely determined by the deformations of a single component $\bar{A}'_i$. Moreover any such deformation determines, via the cyclic action of ζ, a deformation of $\bar{A}'_x$. We are thus reduced to the situation of Lemma 7.8. ∎

Proof of Lemma 7.8: We observe first that it suffices to consider the case in which the unique eigenvalue of $\bar{A}'_x$ is one: Suppose it is $\lambda \in \kappa^*$, and denote by λ also the Teichmüller lift of λ. Then multiplication by λ^{-1} yields an isomorphism between the originally given deformation problem and the deformation problem for lifts of $\lambda^{-1}\bar{A}'_x$. Thus from now on we assume $\lambda = 1$.

Lemma 7.10 yields an explicit description of $R'_{x,m}$: In the situation at hand, the deformed matrices A' satisfy $A'^{p^{m'}} = 1$ for $p^{m'}$ the maximal p-power divisor of $|I_{x,m}|$. The polynomial $g(X)$ may be chosen as $(X-1)^n$. The $f_i \in W(\kappa)[T_1, \ldots, T_n]$, $i = 0, \ldots, n-1$, are determined so that $\sum_{i=0}^{n-1} T^i f_i$ is the remainder of $X^{p^{m'}} - 1$ modulo $g(X) + \sum_{i=0}^{n-1} T_i X^i$. Then

$$R'_{x,m} = W(\kappa)[[T_1, \ldots, T_n]]/(f_0, \ldots, f_{n-1}). \tag{7}$$

In particular, the number of relations is at most the number of variables. (One can also give a purely cohomological proof of this.)

We now claim that $R'_{x,m}/(p)$ is finite. Then the argument given in [deJ], 3.14., shows that $(p, f_0, \ldots, f_{n-1})$ forms a system of parameters of the local ring $W(\kappa)[[T_1, \ldots, T_n]]$, and one easily deduces that $R'_{x,m}$ is a complete intersection and finite flat over $W(\kappa)$.

To prove the claim, as in [deJ], it will suffice to show that any deformation of $\bar{A}'_x$ to $\widetilde{\kappa}[[t]]$ is trivial for any finite extension $\widetilde{\kappa}$ of κ. (The reason is that the normalization of any one-dimensional integral quotient of $R'_{x,m}/(p)$ would be of that form.) In other words, we need to show that under any homomorphism $\psi\colon R'_{x,m} \longrightarrow \widetilde{\kappa}[[t]]$ the variables T_i have to map to zero. Let $t_i := \psi(T_i)$. Then in $\widetilde{\kappa}[[t]][X]$ the monic polynomial $h(X) := g(X) + \sum_{i=0}^{n-1} t_i X^i$ divides $(X^{p^{m'}} - 1) = (X-1)^{p^{m'}}$. Because $\widetilde{\kappa}[[t]][X]$ is factorial, $h(X) = (X-1)^n$. But $g(X) = (X-1)^n$, and so all the t_i must be zero, as asserted.

It remains to prove that $R'_{x,m}$ is reduced. By finite flatness over $W(\kappa)$, it suffices to show that $R'_{x,m}[1/p]$ is reduced, i.e., a product of fields. We need the following lemma:

Lemma 7.11 *Let L be a field of characteristic zero and C an artinian local L-algebra with residue field L. Suppose G is a finite group and W a finitely generated $C[G]$-module which is free over C. Then $W \cong V \otimes_L C$ for V the $L[G]$-module $W \otimes_C L$. In particular the characteristic polynomial of any $g \in G$ acting on W lies in the polynomial ring $L[T]$.*

Proof: We prove the assertion by induction on the length of C. For the induction step, let $a \in C$ be a non-zero element which is annihilated by the maximal ideal of C and set $\mathfrak{a} := Ca = La$. Then we have the following extension of $C[G]$-modules:

$$0 \longrightarrow W \otimes_C \mathfrak{a} \longrightarrow W \longrightarrow W \otimes_C C/\mathfrak{a} \longrightarrow 0. \tag{8}$$

By the induction hypothesis the left hand module is isomorphic to V and the right hand module to $V \otimes_L C/\mathfrak{a}$. Using the spectral sequence associated to the composite of functors $M \mapsto \mathrm{Hom}_C(M, V) \mapsto \mathrm{Hom}_C(M, V)^G$, we obtain the left exact sequence

$$0 \longrightarrow H^1(G, \mathrm{Hom}_C(W \otimes_C C/\mathfrak{a}, V)) \longrightarrow \mathrm{Ext}^1_{C[G]}(W \otimes_C C/\mathfrak{a}, V) \xrightarrow{\beta} \mathrm{Ext}^1_C(W \otimes_C C/\mathfrak{a}, V).$$

The module $\mathrm{Hom}_C(W \otimes_C C/\mathfrak{a}, V)$ is an $L[G]$-module isomorphic to $V^* \otimes V$. The category of such modules is semisimple. Thus taking G-invariants is exact, and so the term on the left vanishes. Consequently β is injective. Now both W and, by the induction hypothesis, $V \otimes_L C$ are extensions of V by $W \otimes_C \mathfrak{a}$. Since both are free as C-modules, their classes in $\mathrm{Ext}^1_C(W \otimes_C C/\mathfrak{a}, V)$ coincide. From the injectivity of β we deduce that the extensions W and $V \otimes_L C$ are isomorphic as $C[G]$-modules. The lemma is thus proved. ■

By what we have shown already $R'_{x,m}[1/p]$ is a finite-dimensional (non-zero) algebra over the quotient field of $W(\kappa)$. We apply the lemma with $G := I_{x,m}$, C a component of $R'_{x,m}[1/p]$ and W the representation on C induced from the versal one. Let A'_C be the matrix corresponding to the summand C of $R'_{x,m}[1/p]$. The lemma tells us that the characteristic polynomial of A'_C is defined over the subfield L of the local ring C. At the same time, we deduce from Lemma 6.2(b) that the versal matrix over $R'_{x,m}$ is completely determined by its characteristic polynomial. Hence the subring of $R'_{x,m}$ containing its coefficients is versal as well and must thus agree with $R'_{x,m}$. By flatness over $W(\kappa)$, the ring $R'_{x,m}$ is a subring of $R'_{x,m}[1/p]$, and so $R'_{x,m}$ intersected with C will be contained in L. Since C was chosen arbitrarily, this shows that $R'_{x,m}[1/p]$ is a product of fields. ■

Remark 7.12 It is possible to give a direct proof of the reducedness of $R'_{x,m}$ based on the explicit description in (7). The idea is roughly the same as above. After inverting p, one can consider homomorphisms into $\mathbb{Q}_p^{\mathrm{alg}}[\varepsilon]/(\varepsilon^2)$, and one needs to show that they all take their image in the subring $\mathbb{Q}_p^{\mathrm{alg}}$.

Let us give an interpretation of the reducedness: Since the roots of $X^{p^{m'}} - 1$ in $\mathbb{Q}_p^{\mathrm{alg}}$ are 'known' explicitly, the solutions over $\mathbb{Q}_p^{\mathrm{alg}}$ for the T_i satisfying the equations f_j are given as follows: Let $p_1, \ldots, p_n$ be the elementary symmetric polynomials in n variables. Then $\operatorname{Spec} R'_{x,m}[1/p]$ is the reduced scheme concentrated at the points

$$\Big((-1)^i p_i(\xi_1, \ldots, \xi_n) - \binom{n}{i}\Big)_{i=1,\ldots,n}$$

where $\xi_1, \ldots, \xi_n$ are pairwise distinct $p^{m'}$-th roots of 1.

In principle, one can recursively compute the f_i. We know of no simple general expression for them. For $n = 2$, $p > 2$ and with fixed determinant $\eta = 1$, we now show how to deduce an explicit presentation of the quotient $R^{\eta}_{x,m}$ of $R'_{x,m}$ which describes deformations of determinant one: Fixing the determinant to 1 amounts to setting $T_n = 0$, i.e., to setting $T_2 = 0$. Thus the ring only depends on one indeterminate, the coefficient of X in the characteristic polynomial, or equivalently the trace of the corresponding matrix. Since the ring is a complete intersection, it has the form $R^{\eta}_{x,m} = W(\kappa)[T]/(g_{m'}(T))$ for some polynomial $g_{m'}$ that depends on $m' = m+1$. By flatness over $W(\kappa)$ the reduction mod p of $g_{m'}$ has the same degree as $g_{m'}$, and so we may assume that g is monic. The polynomial $g_{m'}$ is thus determined by its roots over $\mathbb{Q}_p^{\mathrm{alg}}$. We find

$$g_{m'}(T) = \prod_{\zeta}(T - (\zeta + \zeta^{-1} - 2)) \tag{9}$$

where ζ runs through $\{\zeta \in \mathbb{Q}_p^{\mathrm{alg}} \mid \zeta^{p^{m'}} = 1\}/\simeq$ where $\zeta \simeq \zeta^{-1}$. There are recursive formulas for the $g_{m'}(T)$ in [Bo2]. The polynomial $g_{m'}(T)$ completely determines the ring. The corresponding matrix is

$$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 2-T \end{smallmatrix}\right).$$

Let us finish this section, by making some remarks on the genesis of Theorem 2.27. Its starting point was the following conjecture of de Jong, cf. [deJ] (which due to results of Gaitsgory [Ga] is essentially proved for $p \neq 2$), specialized to our situation:

Conjecture 7.13 (de Jong) Suppose K_0 is a function field over a finite field k_0 of characteristic l different from p. Suppose $\bar{\rho} : G_{K_0} \longrightarrow \mathrm{PGL}_n(\kappa)$ is ramified at most at finitely many places S_0 of K_0, and is absolutely irreducible when restricted to $G_{K_0\bar{\mathbb{F}}_l}$. Then the universal deformation ring, call it $R_0(\bar{\rho})$, in the sense of Mazur, for deformations of $\bar{\rho}$ unramified outside S_0 is finite flat over $W(\kappa)$.

Suppose now that the conditions of Theorem 2.20 are satisfied and that we have a set of ramification data $\mathscr{D}$ with $\mathrm{Supp}\,\mathscr{D} \subset \Sigma_{\mathrm{reg}}$ and $\mathrm{ord}\,\mathscr{D} < \infty$. Then Theorem 2.20 yields a representation $\widetilde{\rho}_{\mathscr{D}} : G_{k_0(t)} \longrightarrow \mathrm{PGL}_n(R_{\mathscr{D}})$, where k_0 is a finite extension of the prime field of k.

If k is of positive characteristic, then k_0 is finite and hence there is a morphism $R_0(\bar{\rho}) \longrightarrow R_{\mathscr{D}}$. Using the universality properties of both rings, one can show, by passing to the algebraic closure of k_0, that this morphism is surjective. Hence $R_{\mathscr{D}}$ is finite over $W(\kappa)$ if de Jong's conjecture holds. Now if $R_{\Sigma_{\mathrm{reg}}}$ is a power series ring in $|\Sigma_{\mathrm{reg}}| \cdot (n-1)$ variables, then one can easily show that it has a presentation $W(\kappa)[T_1, \ldots, T_t]/\mathfrak{a}$ where the ideal $\mathfrak{a}$ is generated by at most t variables. By [deJ], 3.14., it then follows that $R_{\mathscr{D}}$ is finite flat over $W(\kappa)$ and a complete intersection.

If k is of characteristic zero, then one observes that $G^{(l)}_{k(t)} \cong G^{(l)}_{k'(t)}$ where k' is an algebraically closed field of characteristic $l \gg 0$. Since $R_{\mathscr{D}}$ only depends on $G^{(l)}_{k(t)}$ (and $\bar{\rho}$), the above assertion follows in the characteristic zero case as well.

8 Applications to results of Rohrlich

We now apply our results to the case where $\bar{\rho}'_{E,p}$ comes from the action of G on the p-torsion points of an elliptic E over $k(j)$ with j-invariant j. Throughout this section, whenever $S = \{\infty\}$, we simply write $R_S = R_\infty$, $\rho_S = \rho_\infty$, etc. We also define $\Lambda := \mathbb{Z}_p[[T]]$.

Lemma 8.1 *If $p \geq 5$ and $l > 3$, then $h^1_\infty(\overline{\mathrm{ad}}_{\bar{\rho}_{E,p}}) = 1$.*

Proof: The representation $\bar{\rho}_{E,p} : G_{k(j)} \longrightarrow \mathrm{PSL}_2(\mathbb{F}_p)$ is a faithful representation of the Galois group attached to the cover $X(p)/\{\pm 1\} \longrightarrow \mathbb{P}^1$, where $X(p)$ is the modular curve for elliptic curves with a choice of a p-torsion basis and the map is the j-invariant.

The map is ramified precisely at those places of $\mathbb{P}^1$, i.e., j-invariants, for which the automorphism group of the reduction at j is non-trivial. This automorphism group is the inertia group at the respective place. For $j \neq \infty$ this automorphism group is determined in [Sil], III.Thm. 10.1, for $j = \infty$, it can be obtained by looking at the Tate curve, [Ka1], A 1.2. One finds that $\bar{\rho}_{E,p}$ is ramified precisely at the three distinct $(l > 3)$ places 0, 1728 $\pmod{l}$ and ∞, and that the orders of the ramification groups are 3, 2 and p, respectively.

Since $\bar{\rho}_{E,p}$ has image $\mathrm{PSL}_2(\mathbb{F}_p)$ whose centralizer in $\mathrm{PGL}_2(\mathbb{F}_p)$ is trivial, we may apply Theorem 2.3 with $S = \{\infty\}$ and $S^+ = \{0, 1728 \pmod{l}, \infty\}$. This yields

$$h^1_\infty(\overline{\mathrm{ad}}_{\bar{\rho}_{E,p}}) = (3-2)\cdot 3 - \dim_\kappa(\overline{\mathrm{ad}}_{\bar{\rho}_{E,p}})^{H_0} - \dim_\kappa(\overline{\mathrm{ad}}_{\bar{\rho}_{E,p}})^{H_{1728}}.$$

The orders of ramification at 0 and 1728 $\pmod{l}$ are 2 and 3, respectively, and it follows easily that

$$\dim_\kappa(\overline{\mathrm{ad}}_{\bar{\rho}_{E,p}})^{H_0} = \dim_\kappa(\overline{\mathrm{ad}}_{\bar{\rho}_{E,p}})^{H_{1728}} = 1.$$

In conclusion, we have $h^1_\infty(\overline{\mathrm{ad}}_{\bar{\rho}_{E,p}}) = 1$ as asserted. ∎

Theorem 8.2 *For $l, p \geq 5$, the ring $R_\infty(\bar{\rho}_{E,p})$ is isomorphic to $\mathbb{Z}_p[[T]]$. For $p > 5$, the representation ρ_∞ surjects onto* $\mathrm{PSL}_2(R_\infty)$.

Proof: By the previous lemma and Theorem 2.3, the assertion on $R_\infty(\bar{\rho}_{E,p})$ is clear. The surjectivity of ρ_∞ follows from Proposition 2.4: In the case at hand we have $\mathrm{Im}(\bar{\rho}_{E,p}) = \mathrm{PSL}_2(\mathbb{F}_p)$, and so all hypotheses of this proposition are satisfied by Example 2.7. ∎

The arguments used in the above proof, can easily be modified to cover the cases excluded in Theorem 2.28, i.e., those where one of l, p is less than 5. The following summarizes the results:

Proposition 8.3 *If $l < 5$ or $p < 5$, then R_{S_p} is a power series rings over $\mathbb{Z}_p$ whose relative dimension is given in the following table. For $p > 5$, the representation ρ_{S_p} has image* $\mathrm{PSL}_2(\mathbb{Z}_p)$.

	$p=2$			$p=3$			$p \geq 5$
	$l=2$	$l=3$	$l \geq 5$	$l=2$	$l=3$	$l \geq 5$	$l \in \{2,3\}$
rel.dimR'_{S_p}	1	1	3	0	0	2	0

We can now identify the representation given by Rohrlich with the universal one.

Proof of Theorem 2.28: Let us first apply Proposition 5.3 and Proposition 5.5 to the previous theorem. This shows that $R'_\infty(\bar{\rho}'_{E,p})$ is isomorphic to $R_\infty(\bar{\rho}_{E,p}) \cong \Lambda$ and that $\det \rho'_S$ is the unique lift of $\det \bar{\rho}'_{E,p} = 1$. Hence the image of ρ'_S must lie in $\mathrm{SL}_2(\Lambda)$.

For $p > 5$, the above theorem says that ρ_∞ is surjective onto $\mathrm{PSL}_2(\Lambda)$. Therefore $\mathrm{Im}(\rho'_\infty)$ is a subgroup of $\mathrm{SL}_2(\Lambda)$ whose image under proj is $\mathrm{PSL}_2(\Lambda)$. Thus one of the matrices $\pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ belongs to $\mathrm{Im}(\rho'_\infty)$ and therefore also its square $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. This implies $\mathrm{Im}(\rho'_\infty) = \mathrm{SL}_2(\Lambda)$.

It remains to identify the pair (Λ, ρ) of Rohrlich with $(R'_\infty, \rho'_\infty)$. By universality there is a unique map $\alpha\colon R'_\infty \cong \Lambda \longrightarrow \Lambda$ such that $\rho' \sim \alpha\rho'_\infty$. Because ρ' surjects onto $\mathrm{SL}_2(\Lambda)$ and the traces of elements of $\mathrm{SL}_2(\Lambda)$ generate Λ, the map α must be surjective. But any surjective endomorphism of a local ring is an isomorphism, for example by the footnote on [Bö1], p. 204. ∎

Remark 8.4 One could also consider rigid deformations for larger ramification sets than $\{\infty\}$. For $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ one has $Z_A(\kappa) = \{\pm 1\}$. Thus for rigid deformations, no ramification can occur at $t = 1728$. However at $t = 0$ one could have further ramification, and indeed Theorem 7.4 yields

$$R^{\text{rig}}_{\{0,1728,\infty\}} = R^{\text{rig}}_{\{0,\infty\}} \cong \mathbb{Z}_p[[T_1, T_2]].$$

For various uses, we now give an explicit description of the universal representation $\rho\colon G_{k(j)} \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z}_p[[T]])$ of Rohrlich, [Ro2]:

Define $\Lambda_0 := \mathbb{Z}_p[\zeta_p + \zeta_p^{-1}]$, $S := \{0, 1728, \infty\}$, choose topological generators g_0, g_{1728}, g_∞ of $G_S^{(l)}$ such that each g_i generates an inertia subgroup I_i and such that $\prod g_i = 1$, and define $h_i := \bar{\rho}_{E,p}(g_i)$.

By [Ser], p. 74, $\mathrm{PSL}_2(\mathbb{F}_p)$ has precisely four conjugacy classes given by the elements of order 2, those of order 3 and by two classes of order p. Over $\mathrm{PGL}_2(\mathbb{F}_p)$ the two classes of order p get combined. Thus by strict rigidity, after conjugating by an element in $\mathrm{PGL}_2(\mathbb{F}_p)$ we may assume that the h_i are the elements in Example 2.16.

As in [Ro2], p. 281, we define matrices

$$t := \begin{pmatrix} 1 & 1 \\ T & 1+T \end{pmatrix} \quad s := \begin{pmatrix} 0 & Y \\ -Y^{-1} & 0 \end{pmatrix} \quad r := t^{-1}s^{-1} \tag{10}$$

in $\mathrm{PSL}_2(\Lambda)$, where $Y \in 1 + T\mathbb{Z}_p[[T]]$ is uniquely determined by the equation $TY^2 + Y - 1 = 0$. The h_i are then the respective matrices modulo (p, T). Thus if we define $\rho\colon G_S^{(l)} \longrightarrow \mathrm{PSL}_2(\Lambda)$ by $g_0 \mapsto r$, $g_{1728} \mapsto s$, $g_\infty \mapsto t$, then $\rho \pmod{(p,T)} = \rho_{E,p}$. Because $s^2 = r^3 = 1$, the representation ρ factors via $G_\infty := G^{(l)}_{\{\infty\}}$.

Note that the same construction also yields a linear representation into $\mathrm{SL}_2(\mathbb{Z}_p[[T]])$ which we denote by ρ'.

Lemma 8.5 *The representation ρ is strictly equivalent to $\rho_{\{\infty\}}(\bar{\rho}_{E,p})$, and similarly ρ' to $\rho'_{\{\infty\}}(\bar{\rho}'_{E,p})$.*

Proof: We only give the proof for the projective representations: The universality of R_∞ shows that ρ arises from ρ_∞ up to conjugation via a unique morphism $R_\infty \cong \Lambda \longrightarrow \Lambda$ that is the identity modulo (p, T).

One easily checks that $\bar{\rho}_2$ has maximal image. Proposition 2.4 and Example 2.7 imply that ρ has maximal image, i.e., that ρ surjects onto $\mathrm{PSL}_2(\Lambda)$. Therefore the map from $R_\infty \cong \Lambda$ to Λ must be surjective, and hence an isomorphism. ∎

In the remainder of this section, we reprove some of main results of [Ro1] using rigidity methods. Let $\mathfrak{M}$ be the compositum of all modular function fields over $\mathbb{C}(j)$, and denote for a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ of finite index by $\mathfrak{M}^\Gamma$ the corresponding modular function field. Let Σ be the set $\{0, 1728, \infty\}$.

Theorem 8.6 ([Ro1], Thm. 1) *There is a unique subfield $\mathfrak{L}$ of $\mathfrak{M}$ which contains $\mathfrak{M}^{\Gamma(p)}$ and is Galois over $\mathbb{C}(j)$ with $\mathrm{Gal}(\mathfrak{L}/\mathbb{C}(j)) \cong \mathrm{PSL}_2(\mathbb{Z}_p[[T]])$. Furthermore $\mathfrak{L}$ is the compositum of all subfields $\mathfrak{K}$ of $\mathfrak{M}$ which contain $\mathfrak{M}^{\Gamma(p)}$ and are Galois over $\mathbb{C}(j)$ with $\mathrm{Gal}(\mathfrak{K}/\mathbb{C}(j)) \cong \mathrm{PSL}_2(\mathbb{Z}/(p^m))$ for some $m \geq 1$.*

Proof: We denote by $\mathfrak{N}$ the fixed field of the kernel of the universal representation ρ_∞ of $\bar{\rho}_{E,p}$. Also let $\mathfrak{L}'$ be the Galois closure of the union of all subfields $\mathfrak{K}$ as in the above theorem. To prove the theorem, it will suffice to show $\mathfrak{L}' = \mathfrak{N}$. Note that each of the fields $\mathfrak{K}$ defines a representation $\rho_{\mathfrak{K}} : G_{\mathbb{C}(j)} \longrightarrow \mathrm{PSL}_2(\mathbb{Z}/(p^m))$ for some $m \geq 1$ whose residual representation agrees with $\bar{\rho}_{E,p}$.

The action of $\mathrm{PSL}_2(\mathbb{Z})$ on the upper half plane completed by the cusps has non-trivial stabilizers precisely at the fourth and sixth roots of unity and at the cusps, i.e. for j-invariants in Σ. Their orders are 2, 3 and ∞. Therefore all the fields $\mathfrak{M}^\Gamma$ are unramified above $\mathbb{C}(j)$ outside Σ, and the ramification orders are 2, 3 and some positive integer. Thus all the deformations $[\rho_{\mathfrak{K}}]$ are in $\mathrm{Def}'(\mathbb{Z}/(p^m))$, and hence $\mathfrak{L}'$ is a subfield of $\mathfrak{N}$.

Because $\mathbb{H} \longrightarrow \mathbb{H}/\Gamma(p)$ is a universal covering, the fixed fields of the representations

$$\{\alpha \circ \rho_\infty : \alpha \colon R'_\infty \longrightarrow \mathbb{Z}/(p^m), m \in \mathbb{N}\}$$

are precisely the fields $\mathfrak{K}$ above. Therefore to show that $\mathfrak{L}' = \mathfrak{N}$, one needs to show that for all $f \in \mathbb{Z}_p[[T]]$, there exists a homomorphism $\alpha \colon \mathbb{Z}_p[[T]] \longrightarrow \mathbb{Z}_p$ such that $\alpha(f) \neq 0$. To prove this, write $f = \sum a_m T^m$ and let m_0 be minimal such that $a_{m_0} \neq 0$. Let $e \in \mathbb{N}_0$ be defined by the condition that a_{m_0}/p^e is a unit in $\mathbb{Z}_p$. Then the homomorphism α defined by $T \mapsto T^{e+1}$ satisfies $0 \not\equiv \alpha(f) \pmod{p^{(e+1)m_0+1}}$. ∎

Theorem 8.7 ([Ro1], Thm. 2) *Suppose $\widetilde{F} \subset \mathbb{C}$ contains all roots of unity of p-power order. Then there exists a unique extension $\mathfrak{L}_{\widetilde{F}}$ of $\widetilde{F}(j)$ contained in $\mathfrak{L}$ such that $\mathfrak{L}_{\widetilde{F}}\mathbb{C} = \mathfrak{L}$ and $\mathbb{C}(j) \cap \mathfrak{L}_{\widetilde{F}} = \widetilde{F}(j)$.*

Proof: Let ρ be as constructed above Lemma 8.5, so that in particular the images of the g_i under $\bar{\rho}_{E,p}$ are the elements described in Example 2.16. By [Ser], p. 87, the conjugacy classes of the elements $\rho_\infty(g_i)$ are rational over $\mathbb{Q}(\sqrt{p^*})$, where $p^* := p(-1)^{\frac{p-1}{2}}$.

By Corollary 2.25, there exists a surjective representation $\widetilde{\rho}_\infty : \mathrm{Gal}(\mathbb{C}(j)_\Sigma/\widetilde{F}) \longrightarrow \mathrm{PSL}_2(R_\infty)$ whose restriction to $G_{\mathbb{C}(j)}$ is ρ_∞. This representation is unique up to inner automorphism of $\mathrm{PSL}_2(R_\infty)$. Define $\mathfrak{L}_{\widetilde{F}}$ to be the splitting field of $\widetilde{\rho}_\infty$.

Because ρ_∞ and $\widetilde{\rho}_\infty$ have the same image, we must have $\mathfrak{L}_{\widetilde{F}}\mathbb{C} = \mathfrak{L}_{\mathbb{C}}$. Furthermore

$$\widetilde{\rho}_\infty(\mathrm{Gal}(\mathfrak{L}_{\widetilde{F}}/\widetilde{F}(j))) = \rho_\infty(\mathrm{Gal}(\mathfrak{L}_{\mathbb{C}}/\mathbb{C}(j))) = \widetilde{\rho}_\infty(\mathrm{Gal}(\mathfrak{L}_{\widetilde{F}}/\mathfrak{L}_{\widetilde{F}} \cap \mathbb{C}(j))),$$

and so we must also have $\mathbb{C}(j) \cap \mathfrak{L}_{\widetilde{F}} = \widetilde{F}(j)$. This proves the existence of $\mathfrak{L}_{\widetilde{F}}$.

For the uniqueness, let $\mathfrak{L}'$ be any field that satisfies the conditions for $\mathfrak{L}_{\widetilde{F}}$. Choose a surjective representation $\rho \colon G_{\widetilde{F}(j)} \longrightarrow \mathrm{PSL}_2(\Lambda)$ with splitting field $\mathfrak{L}'$. Because $\mathfrak{L}'\mathbb{C} = \mathfrak{L}$, the restriction $\rho_{|G_{\mathbb{C}(j)}}$ is isomorphic to ρ_∞. The uniqueness assertion of Corollary 2.25 now implies that $\mathfrak{L}' = \mathfrak{L}_{\widetilde{F}}$. ∎

Theorem 8.8 ([Ro1], Thm. 3) *Let $\widetilde{F}$ be a subfield of $\mathbb{C}$ which contains all p-power roots of unity and let E be an elliptic curve over $\widetilde{F}(j)$ with invariant j. Let $\widetilde{F}(j, E[p^\infty])$ be the splitting field of the representation $\rho_{E,p}$ of $G_{\widetilde{F}(j)}$ on the p-adic Tate-module of E. Then there exists a representative of the universal deformation $(R_\infty \cong \Lambda, \rho_\infty)$ such that the diagram*

$$\begin{tikzcd}
\mathrm{Gal}(\mathfrak{L}_{\widetilde{F}}(E[p^\infty])/\widetilde{F}(j)) \arrow[r, "\rho'_\infty"] \arrow[d, "\pi"'] & \mathrm{SL}_2(\Lambda) \arrow[d, "\pi' : T \mapsto 0"] \\
\mathrm{Gal}(\widetilde{F}(j, E[p^\infty])/\widetilde{F}(j)) \arrow[r, "\rho'_{E,p}"] & \mathrm{SL}_2(\mathbb{Z}_p)
\end{tikzcd}$$

is commutative, where the left vertical map is the natural map from Galois theory.

Proof: For $F = \mathbb{C}$ the universality of $(R'_\infty, \rho'_\infty)$ shows that a diagram as above exists, except for the specific form of the left vertical map. However this form can always be obtained by simply applying a suitable automorphism of Λ.

Let us temporarily pass to projective representations. Then from the previous paragraph and the uniqueness assertion of Corollary 2.25, we obtain the above diagram for arbitrary F provided we look at projective representations.

The quoted corollary also implies that $\rho_{E,p}$ is the unique lift of the restriction of $\rho_{E,p}$ to $G_{\mathbb{C}(j)}$. Therefore $\rho'_{E,p}\pi$ and $\pi'\rho'_\infty$ can at most differ by a character with image in $\{\pm 1\}$. However modulo $\mathfrak{m}_\Lambda$ we have

$$\rho'_{E,p}\pi \equiv \pi'\rho'_\infty \equiv \bar{\rho}'_{E,p},$$

so that this character must be trivial, and thus the diagram commutes. ∎

Let $\lambda_{1/2}$ be the eigenvalues of $\left(\begin{smallmatrix} 1 & 1 \\ T & 1+T \end{smallmatrix}\right)$, i.e., the solutions of $\lambda^2 - (2+T)\lambda + 1 = 0$. The λ_i lie in $1 + T^{1/2}\Lambda[T^{1/2}]$. Thus for any $c \in \mathbb{Z}_p^*$ one has $\beta(c) := \lambda_1^c + \lambda_2^c - 2 = \mathrm{Tr}\left(\begin{smallmatrix} 1 & 1 \\ T & 1+T \end{smallmatrix}\right)^c - 2 \in T\Lambda$. The careful reader can easily check that everything is well-defined. Since $\beta(c) \equiv c^2 T \pmod{T^2\Lambda}$, there exists a unique $\mathbb{Z}_p$-algebra automorphism $\iota_c \colon \Lambda \longrightarrow \Lambda$ mapping T to $\beta(c)$. Below we will show that $\iota \colon \mathbb{Z}_p^* \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(\Lambda) : c \mapsto \iota_c$ is a homomorphism.

We define $\mathrm{sign} \colon \mathbb{Z}_p^* \longrightarrow \mathbb{Z}/(2)$ as the unique homomorphism with kernel $(\mathbb{Z}_p^*)^{\times 2}$ and fix an element $x \in \mathbb{Z}_p^\times \smallsetminus (\mathbb{Z}_p^*)^{\times 2}$. Using sign, ι and x, we define a homomorphism $\mathbb{Z}_p^* \longrightarrow \mathrm{Aut}(\mathrm{PSL}_2(\Lambda))$ via

$$\mathbb{Z}_p^* \times \mathrm{PSL}_2(\Lambda) \mapsto \mathrm{PSL}_2(\Lambda) : (c, A) \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)^{\mathrm{sign}(c)} \iota_c(A) \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)^{\mathrm{sign}(c)}.$$

This yields a semi-direct product $\mathbb{Z}_p^* \ltimes \mathrm{PSL}_2(\Lambda)$. Recall that for any field F of characteristic different from p, we defined F_∞ to be F adjoint all p-power roots of unity. The corresponding cyclotomic character we denote $\chi \colon \mathrm{Gal}(F_\infty/F) \longrightarrow \mathbb{Z}_p^*$. It extends to $\mathrm{Gal}(\mathbb{C}(j)^{\mathrm{alg}}/F(j))$ via the isomorphism $\mathrm{Gal}(F_\infty(j)/F(j)) \cong \mathrm{Gal}(F_\infty/F)$.

Theorem 8.9 ([Ro2], Thm. 3) *Let F be a subfield of $\mathbb{C}$. Then the following hold:*

(a) $\mathfrak{L}_{F_\infty}$ is Galois over $F(j)$.

(b) The map $\iota \colon \mathbb{Z}_p^* \longrightarrow \mathrm{Aut}(\Lambda)$ is a homomorphism.

(c) Via χ and the action of $\mathbb{Z}_p^*$ on $\mathrm{PSL}_2(\Lambda)$, there is an isomorphism

$$\mathrm{Gal}(\mathfrak{L}_{F_\infty}/F(j)) \cong \mathrm{Gal}(F_\infty/F) \ltimes \mathrm{PSL}_2(\Lambda).$$

Proof: The elements $\sigma \in \mathrm{Gal}(\mathbb{C}(j)^{\mathrm{alg}}/F(j))$ act naturally on the representation $\widetilde{\rho}_\infty$ by

$$\sigma \circ \widetilde{\rho}_\infty : g \mapsto \widetilde{\rho}_\infty(\sigma g \sigma^{-1}).$$

The representation $\sigma \circ \widetilde{\rho}_\infty$ is again a representation of $\mathrm{Gal}(\mathbb{C}(j)^{\mathrm{alg}}/F(j))$. By Corollary 2.25, $\sigma \circ \widetilde{\rho}_\infty$ is the unique representation of $\mathrm{Gal}(\mathbb{C}(j)^{\mathrm{alg}}/F(j))$ whose restriction to G_∞ is given by $\sigma \circ \rho_\infty$. The latter representation has the same ramification properties as ρ_∞. Furthermore by strict rigidity of $\bar{\rho}$, the residual representation is a $\mathrm{PGL}_2(\mathbb{F}_p)$ conjugate of $\bar{\rho}$. Thus by the universality of ρ_∞, identifying $R_\infty = \Lambda$ there exists a unique automorphism $\alpha_\sigma \colon \Lambda \longrightarrow \Lambda$ and a matrix $A_\sigma \in \mathrm{PGL}_2(\Lambda)$ such that

$$\sigma \circ \rho_\infty = \alpha_\sigma(A_\sigma \rho_\infty A_\sigma^{-1}). \tag{11}$$

Applying Corollary 2.25 yet another time, we obtain the same equation for $\widetilde{\rho}_\infty$ in place of ρ_∞. From the universality property one also derives that (a) the map

$$\mathbb{Z}_p^* \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(\Lambda) : \sigma \mapsto \alpha_\sigma$$

is a ring homomorphism (because given σ, the map α_σ is unique), and that (b) the assignment

$$\mathrm{Gal}(\mathbb{C}(j)^{\mathrm{alg}}/F(j)) \longrightarrow \mathrm{PGL}_2(\Lambda) : \sigma \mapsto A_\sigma$$

satisfies the 1-cocycle condition $\alpha_{\tau^{-1}}(A_\sigma)A_\tau = A_{\sigma\tau}$. From the strict rigidity of the g_i we moreover deduce that the A_σ are uniquely determined by σ. For $\sigma \in \mathrm{Gal}(\mathbb{C}(j)^{\mathrm{alg}}/F_\infty(j))$ it follows that $\alpha_\sigma = \mathrm{id}$ and $A_\sigma = \widetilde{\rho}_\infty(\sigma)$. Also, the homomorphism from $\mathrm{Gal}(\mathfrak{L}_{F_\infty}/F(j))$ to the automorphism group $\mathrm{Aut}(\mathrm{PSL}_2(\Lambda))$ of $\mathrm{PSL}_2(\Lambda)$ is faithful. As a direct consequence of (11) for $\widetilde{\rho}_\infty$, the splitting field of $\sigma \circ \widetilde{\rho}_\infty$ is independent of σ, i.e., $\mathfrak{L}_{F_\infty}$ is Galois over F which proves (a).

Next we prove (b). As is well known, for any σ one has $\sigma g_\infty \sigma^{-1} = g_\infty^{\chi(\sigma)}$. Therefore applying (11) to g_∞ yields

$$\rho_\infty(g_\infty)^{\chi(\sigma)} = \alpha_\sigma(A_\sigma \rho_\infty(g_\infty) A_\sigma^{-1}).$$

Using the explicit shape of $\rho_\infty(g_\infty)$ and the definition of β, taking traces yields

$$2 + \beta(\chi(c)) = 2 + \alpha_\sigma(T).$$

Therefore we find $\alpha_\sigma = \iota_{\chi(\sigma)}$. Since for $F = \mathbb{Q}$ the map χ is an isomorphism, we deduce (b) from the homomorphism property of $\sigma \mapsto \alpha_\sigma$.

Let now $\sigma_0 \in \mathrm{Gal}(\mathfrak{L}_{F_\infty}/F(j))$ be such that it maps to a topological generator of $\mathrm{Gal}(F_\infty/F)$. Recall that $A_\tau = \widetilde{\rho}(\tau)$ for $\tau \in \mathrm{Gal}(\mathfrak{L}_{F_\infty}/F_\infty(j))$ and that $\widetilde{\rho}$ surjects onto $\mathrm{PSL}_2(\Lambda)$. Replacing σ_0 by $\sigma_0\tau$ for a suitable $\tau \in \mathrm{Gal}(\mathfrak{L}_{F_\infty}/F_\infty(j))$ and using the 1-cocycle condition for $\gamma \mapsto A_\gamma$, we may assume that A_{σ_0} is either id or $\left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)$ – the index $[PGL_2(\Lambda) : \mathrm{PSL}_2(\Lambda)]$ is 2. Both cases can be recognized modulo $\mathfrak{m}_\Lambda$. Now $\widetilde{\rho} \pmod{\mathfrak{m}_\Lambda}$ is equal to the restriction of $\bar{\rho}_{E,p}$ to $\mathrm{Gal}(\mathfrak{L}_{F_\infty}/F_\infty(j))$. The action of σ_0 on $\widetilde{\rho} \pmod{\mathfrak{m}_\Lambda}$ is conjugation by $\bar{\rho}_{E,p}(\sigma_0)$. By our normalization of A_{σ_0} the action is trivial if and only if $\det \bar{\rho}'_{E,p}(\sigma_0)$ is a square in $\mathbb{F}_p^*$. It follows that

$$A_{\sigma_0} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)^{\mathrm{sign}(\chi(\sigma_0))}.$$

Since A_{σ_0} lies in $\mathrm{PGL}_2(\mathbb{Z}_p)$, it is invariant under any automorphism in $\mathrm{Aut}_{\mathbb{Z}_p}(\Lambda)$. Using the 1-cocycle condition one easily deduces that an arbitrary element $\sigma\tau$ with σ in the closure of $\sigma_0^{\mathbb{Z}}$ and $\tau \in \mathrm{Gal}(\mathfrak{L}_{F_\infty}/F_\infty(j))$ acts as

$$\widetilde{\rho}_\infty \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)^{\mathrm{sign}(\chi(\sigma))} \iota_{\chi(\sigma)}(\widetilde{\rho}_\infty(\tau)\widetilde{\rho}_\infty\widetilde{\rho}_\infty(\tau)^{-1}) \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)^{-\mathrm{sign}(\chi(\sigma))}.$$

From this, assertion (c) is straightforward. ∎

The following is an immediate corollary:

Corollary 8.10 *Let $\mathfrak{b}_m$ be the ideal of $\Lambda = \mathbb{Z}_p[[T]]$ generated by the elements $p^{m-i}T^{\frac{p^i-1}{2}}$, $i = 0, \ldots, m$. Then $\mathrm{PGL}_2(\Lambda/\mathfrak{b}_m)$ is the Galois group of a regular cover of $\mathbb{Q}(\zeta_{p^m})(j)$, which is unramified outside $0, 1728, \infty$.*

We leave the simple proof, which consists in checking that $\beta(1+p^m) \equiv X \pmod{\mathfrak{b}_m}$, to the reader.

Remark 8.11 The proofs of this section have amply demonstrated the usefulness of the methods developed in this article. They also show that the results of this section do not really depend on the arithmetic set-up coming from elliptic curves. This was perhaps not so obvious from their original proofs given in [Ro1] and [Ro2].

At this point, we also want to point out that two of the main results of Rohrlich do very much depend on the arithmetic set-up: Assertion (c) in the introduction of [Ro2], needs the fact that the coarse moduli space of elliptic curves is given by $\mathbb{A}^1$ via the j-function. Assertion (d) in loc. cit. uses that for an elliptic curve E defined over a number field and a place $\mathfrak{q}$ of this field not above p and at which E has good reduction, the eigenvalues of Frobenius at $\mathfrak{q}$ acting on the p-adic Tate-module of E are of complex absolute value $(N\mathfrak{q})^{1/2}$.

The work [Ka2] of Katz on rigid local system states that any rigid local system 'comes from geometry'. It would be worthwhile to investigate whether this would yield the following: For any rigid local $\bar{\rho}$ and every $p \neq l$ there is a geometric p-adic Galois representation which deforms $\bar{\rho}$. In Rohrlich's case this is the representation on the Tate module. If so, one could quite generally recover Assertion (d) of [Ro2]. There exists some related work on Katz' results by Dettweiler, Reiter, Völklein and Wewers, e.g. [De].

9 Further Applications

We first give an explicit description of Rohrlich's universal deformation ring for the set of ramification data $\mathscr{D}_m$ defined by $n_\infty = m$ and $n_x = 0$ for $x \neq \infty$. Namely from Remark 7.12 we deduce:

Proposition 9.1 *Suppose $l, p \geq 5$, $l \neq p$ and $m \geq 1$. Define $g_{p^m}(T) \in \mathbb{Z}[T]$ as the monic squarefree polynomial whose roots are the elements $\zeta + \zeta^{-1} - 2$, where ζ runs through the p^m-th roots of unity different from 1. Then $R'_{\mathscr{D}_{m-1}} \cong \mathbb{Z}_p[[T]]/(g_{p^m}(T))$.*

Remark 9.2 Note that by their rigidity property, these representations descend to representation over $k_m(t)$, where k_m is finite over the prime field of k.

Formula (9) implies that $R'_{\mathscr{D}_m}$ is reduced.

For the proof of Theorems 2.29 and 2.30, we need the following lemma:

Lemma 9.3 *Let $3 < l \nmid (p^3 - p)$. Consider the topological generators*

$$t := \begin{pmatrix} 1 & 1 \\ T & 1+T \end{pmatrix} \quad s := \begin{pmatrix} 0 & Y \\ -Y^{-1} & 0 \end{pmatrix} \quad r := t^{-1}s^{-1}$$

of $\mathrm{PSL}_2(\Lambda)$ defined in (10) above Lemma 8.5. Let $\zeta = \zeta_{p^e}$ for some $e \geq 1$. Define $t_\zeta := t_{|T=\zeta+\zeta^{-1}-2}$, and analogously s_ζ and r_ζ. Then the following hold:

(a) The elements $r_\zeta, s_\zeta, t_\zeta$ generate $\mathrm{PSL}_2(\mathbb{Z}_p[\zeta+\zeta^{-1}])$ topologically.

(b) The conjugacy classes of r and s (and so also of r_ζ and s_ζ) are $\mathbb{Q}$- and $\mathbb{F}_l$-rational.

(c) The order of t_ζ is p^e.

(d) The elements t and t^{-1} are conjugate.

(e) The conjugacy class of t_ζ is rational over $\mathbb{Q}(\zeta_{p^e} + \zeta_{p^e}^{-1})$ and $\mathbb{F}_l(\zeta_{p^e} + \zeta_{p^e}^{-1})$.

(f) The conjugacy classes of $r, s, t \pmod{\mathfrak{m}_\Lambda^2}$ are rational over $\mathbb{Q}(\zeta_{p^2})^+$.

Proof: The elements r, s, t are topological generators of $\mathrm{PSL}_2(\Lambda)$. Under the surjective homomorphism $\Lambda \twoheadrightarrow \mathbb{Z}_p[\zeta + \zeta^{-1}]$ given by $T \mapsto \zeta + \zeta^{-1} - 2$, these elements map to $r_\zeta, s_\zeta, t_\zeta$, and whence the latter are topological generators of $\mathrm{PSL}_2(\mathbb{Z}_p[\zeta + \zeta^{-1}])$. This proves (a).

For (b) we apply Lemma 6.24 (b). The assertion on s follows from $s^2 = 1$. For r we shall show that r and r^{-1} are conjugate: Note first that their reductions to $\mathbb{F}_p$ are regular, and so by Lemma 6.2(b) they are both conjugate to their companion matrix. Since r does not deform, its characteristic polynomial is the Teichmüller lift of the characteristic polynomial of its reduction, i.e., of $T^2 + T + 1$. The same holds for r^{-1}. Having the same characteristic polynomials, the regular matrices r, r^{-1} must be conjugate.

For (c) observe first that $\det(t_\zeta) = 1$ (since $\det(t) = 1$) and that $\mathrm{Tr}(t_\zeta) = \zeta + \zeta^{-1}$. Hence the characteristic polynomial $\chi_{t_\zeta}(X)$ of t_ζ is $(X - \zeta)(X - \zeta^{-1})$. It follows that $\chi_{t_\zeta^l}(X) = (X - \zeta^l)(X - \zeta^{-l})$, and thus t_ζ has order p^e as claimed.

The proof of (d) proceeds in the same way as the proof that r and r^{-1} are conjugate.

Part (e) follows from parts (c), (d) and Lemma 6.24 (c).

For (f) we show that $t \pmod{\mathfrak{m}_\Lambda^2}$ has order p^2. Let $a := \left(\begin{smallmatrix} 0 & 1 \\ T & T \end{smallmatrix}\right)$. By explicit computation, one shows that $a^i \equiv 0 \pmod{\mathfrak{m}_\Lambda^2}$ for $i \geq 4$. Also modulo p^2 one has $\binom{p^2}{i} \equiv 0$ for $p \not| i$ and $\binom{p^2}{pi} \equiv \binom{p}{i}$. Since $p \geq 5 \geq 4$ it follows that

$$t^{p^2} = (1 + a)^{p^2} = \sum_{i=0}^{p^2} a^i \binom{p^2}{i} \equiv \sum_{i=0}^{p} a^{pi} \binom{p}{i} = 1 \pmod{\mathfrak{m}_\Lambda^2}. \ \blacksquare$$

We now give the proofs of Theorems 2.29 and 2.30:

Proof of Theorem 2.29: Let $\rho \colon G_{\mathbb{Q}^{\mathrm{alg}}(j)} \longrightarrow \mathrm{SL}_2(\Lambda)$ be the representation constructed in Lemma 8.5, by sending suitable inertial generators of $\mathbb{Q}^{\mathrm{alg}}(j)$ at $0, 1728, \infty$ to r, s, t, respectively. As shown in [Ro1] using strict pro-rigidity (or by applying Corollary 2.25) there exists a unique surjective representation $G_{\mathbb{Q}_\infty(j)} \longrightarrow \mathrm{SL}_2(\Lambda)$ which is unramified outside $0, 1728, \infty$ and whose restriction to $G_{\mathbb{Q}^{\mathrm{alg}}(j)}$ agrees with ρ. In fact, by Lemma 9.3 (d) the associated projective representation descends to $G_{\mathbb{Q}_\infty^+(j)} \longrightarrow \mathrm{PSL}_2(\Lambda)$.

Precisely if $p \equiv 1 \pmod 4$, the residual representation $\bar{\rho}'_{E,p}$ on p-torsion points satisfies $\bar{\rho}'_{E,p}(\mathbb{Q}(\zeta_p)^+(j)) = \mathrm{SL}_2(\mathbb{F}_p)$. Since we assume this, there exists a unique surjective representation $\tau_\infty^+ \colon G_{\mathbb{Q}_\infty^+(j)} \longrightarrow \mathrm{SL}_2(\Lambda)$ which is unramified outside $0, 1728, \infty$ and whose restriction to $G_{\mathbb{C}(j)}$ agrees with ρ.

As in [Ro2] there exists a thin subset θ of $\mathbb{Q}$ such that for all $j_0 \in \mathbb{Q} - \theta$ the specialization $(\tau_\infty^+)_{|j=j_0}$ defines a surjective representation $\tau_{\infty,j_0}^+ : G_{\mathbb{Q}_\infty^+} \longrightarrow \mathrm{SL}_2(\Lambda)$. By [Ro2], p. 280, (d), it follows that each such specialization is unramified outside finitely many primes.

Let now ζ be any non-trivial p-power root of unity, and consider $\widetilde{\tau}_\zeta := \rho_{|T=\zeta+\zeta^{-1}-2}$. By Lemma 9.3 (b) and (e), and by the rigidity method, $\widetilde{\tau}_\zeta$ descends to a representation $\tau_\zeta \colon G_{\mathbb{Q}(\zeta)^+(j)} \longrightarrow \mathrm{SL}_2(\mathbb{Z}_p[\zeta + \zeta^{-1}])$. (The point is that t_ζ has the same order as ζ and is conjugate to its inverse. So its conjugacy class is rational over $\mathbb{Q}(\zeta)^+$.)

The restriction of τ_ζ to $G_{\mathbb{Q}_\infty^+(j)}$ agrees with τ_∞^+ if specialized under $T \mapsto \zeta + \zeta^{-1} - 2$. For $j_0 \in \theta$ define τ_{ζ,j_0} as the specialization $(\tau_\zeta)_{|j=j_0}$. The image of τ_{ζ,j_0} is a subgroup of $\mathrm{SL}_2(\mathbb{Z}_p[\zeta + \zeta^{-1}])$. The restriction of τ_{ζ,j_0} to $G_{\mathbb{Q}_\infty^+(j)}$ agrees by definition with the specialization of τ_{∞,j_0}^+ under $T \mapsto \zeta + \zeta^{-1} - 2$. Since τ_{∞,j_0}^+ is surjective, the same follows for τ_{ζ,j_0}. By taking $\rho_\infty^+ := \tau_{\infty,j_0}^+$ and $\rho_\zeta := \tau_{\zeta,j_0}$, Theorem 2.29 is thus proved. $\blacksquare$

Proof of Theorem 2.30: The argument is similar to, but simpler than that of the previous proof, because we do not need to specialize j: Under our hypothesis on p, l, we obtain from Proposition 8.3 a surjective Galois representation $\rho\colon G_{k(j)} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}_p[[T]])$, where k is the algebraic closure of $\mathbb{F}_l$. Because $l \not| p^3 - p$, the representation is of order prime to p, and hence factors via $G_{k(j)}^{(l)}$.

Again, we obtain an explicit expression for ρ from Lemma 8.5. As in the previous proof, one may specialize T to $\zeta + \zeta^{-1} - 2$. Then the rigidity method implies that the representation descends to a representation

$$\rho_\zeta\colon G_{\mathbb{F}_l(\zeta_{p^e})(j)} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}_p[\zeta + \zeta^{-1}]).$$

This representation is again unramified outside $0, 1728, \infty \pmod{l}$. By the choice of T, the ramification orders at $0, 1728, \infty$ are $3, 2, p^e$, respectively. The assertion follows. ∎

References

[Bel] G. V. Belyi, *On extensions of the maximal cyclotomic field having a given classical Galois group*, J. reine angew. Math. **341** (1983), 147–156.

[Böl] G. Böckle, *A local-to-global principle for deformations of Galois representations*, J. reine angew. Math. **509**, 199-236.

[Bö2] G. Böckle, *Finiteness conjectures for $\mathbb{F}_l[[T]]$-analytic extensions of number fields*, J. Number Theory **96** (2002), no. 2, 257–274.

[Bo1] N. Boston, Appendix to [MW], Compositio Math. **59** (1986), 261–264.

[Bo2] N. Boston, *Families of Galois Representations - Increasing the Ramification*, Duke Math. Journ. **66** vol. 3 (1992), p. 357–367.

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

[De] M. Dettweiler, *Galois realizations of classical groups and the middle convolution*, http://arXiv.org/abs/math/0605381

[FKV] G. Frey, E. Kani, H. Völklein, *Curves with infinite K-rational geometric fundamental group*, in 'Aspects of Galois theory' (Gainesville, FL, 1996), 85–118, LMS Lecture Note Ser. 256, Cambridge Univ. Press, Cambridge, 1999.

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

[Igu] J. Igusa, *Fiber systems of Jacobian varieties*, Amer. J. Math. **81** (1959), 453–476.

[Iha] Y. Ihara, *On unramified extensions of function fields over finite fields*, in 'Galois groups and their representations' (Nagoya, 1981), 89–97, Adv. Stud. Pure Math. 2, North-Holland, Amsterdam-New York, 1983.

[Ja] N. Jacobson, *Basic algebra II*, Second edition. W. H. Freeman and Company, New York, 1989.

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

[Ka1] N. Katz *P-adic properties of modular schemes and modular curves*, in 'Modular Curves of one variable III', 70–189, LNM 350, Springer, 1974.

[Ka2] N. Katz *Rigid local systems*, Ann. of Math. Studies **139**, Princeton University Press, 1996.

[MM] G. Malle, B. H. Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Berlin, 1999.

[Mat] H. Matsumura, *Commutative Algebra*, 2nd ed., Math. Lect. Note Ser. **56**, Benjamin/Cummings Publishing Co., 1980.

[Ma1] B. Mazur, *Deforming Galois representations,* in: Galois groups over $\mathbb{Q}$, Y. Ihara, K. Ribet, J.-P. Serre eds., MSRI Publ. **16**, Springer-Verlag, New-York, Berlin, Heidelberg, 1987, 385-437.

[Ma2] B. Mazur, *An introduction to the deformation theory of Galois representations*, in "Modular forms and Fermat's last theorem" (Boston, MA, 1995), 243–311, Springer, New York, 1997.

[MW] B. Mazur, A. Wiles, *On p-adic analytic families of Galois representations*, Compositio Math. **59** (1986), 231–264

[Mil] J. S. Milne, *Étale Cohomology*, Princeton Math. Series, 33. Princeton University Press, 1980.

[Ro1] D. Rohrlich, *False division towers of elliptic curves*, J. Algebra **229** (2000), no. 1, 249–279.

[Ro2] D. Rohrlich, *A deformation of the Tate module*, J. Algebra **229** (2000), no. 1, 280–313.

[Ro3] D. Rohrlich, *Universal deformations and universal elliptic curves*, preprint (2000), available under `http://math.bu.edu/people/rohrlich`.

[Ser] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics **1**, Jones and Bartlett Publishers, Boston, MA, 1992.

[SGA1] A. Grothendieck et al., *Revêtements étale et groupe fondamental*, Lecture Notes in Math. 224, Springer, Heidelberg, 1971.

[Sil] J. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer, Berlin–New York, 1986.

[Ste] C. Stewart, *Universal deformations, rigidity and Ihara's cocycle*, master's thesis under H. Darmon, McGill University; available under:
`http://www.math.mcgill.ca/darmon/thesis/theses.html`.

[SW] U. Storch, H. Wiebe, *Lehrbuch der Mathematik fr Mathematiker, Informatiker und Physiker. Band II, Lineare Algebra*, Bibliographisches Institut, Mannheim, 1990.

[Vö] H. Völklein, *Rigid generators of classical groups*, Math. Ann. **311**, no. 3, 421–438.